Cisco Prime Collaboration Assurance Reports

This section explains the following:

- Cisco Prime Collaboration Assurance Reports, on page 1
- Prerequisites to Generate the Cisco Prime Collaboration Assurance Reports, on page 1
- Update Call Detail Records NAM Credentials, on page 2
- Call Classification, on page 7
- Configure SFTP Settings, on page 17
- Administrative Reports, on page 20
- CDR & CMR Call Report, on page 21
- NAM & Sensor Report, on page 32
- Session Reports/Conference Reports, on page 40
- TelePresence Endpoint Reports, on page 42
- Launch CUCM Reports, on page 43
- Miscellaneous Reports, on page 43
- Scheduled Reports, on page 48
- Access Data for Reports that Contain More than 2,000 Records, on page 51
- Troubleshoot File Download Issues, on page 51

Cisco Prime Collaboration Assurance Reports

This chapter provides information on various reports in Cisco Prime Collaboration Assurance Reports.

Prerequisites to Generate the Cisco Prime Collaboration Assurance Reports

You can use the Cisco Prime Collaboration Assurance reports to identify problem areas, locate most commonly used and least used endpoints, and determine ideal locations and required endpoint types for future deployment.

Prerequisites:

- Update data source credentials. See Update Call Detail Records NAM Credentials.
- (For voice call reports) Categorize calls, add Dial Plan, configure Gateway Codes. See Call Classification.

- Configure SFTP. See Configure SFTP Settings.
- Unified CM devices must be in managed state.
- Cisco Prime Collaboration Assurance must be added as billing server in Unified CM.

Update Call Detail Records NAM Credentials

Cisco Prime Collaboration Assurance collects SCS (number of seconds where loss is greater than 5%) from Cisco Unified CM clusters or Cisco Prime Virtual Network Analysis Module (Prime vNAM). It sends SNMP traps when the voice quality of a call fails to meet a user-defined quality threshold.

Cisco Unified CM calculates the MOS value for an entire call using the Cisco Voice Transmission Quality (CVTQ) algorithm. At the termination of a call, Cisco Unified CM stores the data in Call Detail Records (CDRs) and Call Management Records (CMRs) (for more information on CDR and CMR, see the Cisco Unified Communications Manager Call Detail Records Administration Guide.

To provide the credentials for Unified Communications Manager publisher servers, you must:

- Provide Cisco Prime Collaboration Assurance with credentials.
- Keep the credentials up-to-date. (Any time you update credentials on a Unified Communications Manager publisher server, you must also update the corresponding credentials in Cisco Prime Collaboration Assurance.)

To update the credentials, choose **CDR Source Settings** > **Manage Call Quality Data Sources**.

For Cisco Prime Collaboration Release 11.5 and later

To update the credentials, choose **Alarm & Report Administration** > **CDR Source Settings** > **Manage Call Quality Data Sources**.

For Cisco Prime Collaboration Release 12.1 SP3 and later

To update the credentials, choose **Inventory** > **Inventory Management** > **Configure NAM**.

Add Credential for Prime NAM

To add a credential for Prime NAM server:

Step 1 Choose **Assurance Administration** > **CDR Source Settings** > **Manage Call Quality Data Sources**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration** > **CDR Source Settings** > **Manage Call Quality Data Sources**.

For Cisco Prime Collaboration Release 12.1 SP3 and later

Choose **Inventory** > **Inventory Management** > **Configure NAM**.

Step 2 Click **Add**, and enter the required data. Here, every field is mandatory.

Step 3 Click **OK**.

For Cisco Prime Collaboration Release 12.1 SP3 and later

Click **Save**.

Note You can enter either the Hostname or the IP Address in the specified format. Make sure the Hostname is resolvable with the IP address. If it is not resolvable, an error message pops up. The Configure NAM wizard also displays the **Status** of the NAM configurations along with the **Status Reasons**. The various statuses are Success, Verifying, and Failure.

Step 4 Click the **Refresh** button for the credential details to reflect on the user interface.

To edit or delete a credential, check the checkbox of the credential of your choice, and then click **Edit** or **Delete**.

For Cisco Prime Collaboration Release 12.1 SP3 and later

Click **Refresh** icon to view the latest NAM credential status.

To edit a credential, check the checkbox of the credential of your choice, and then make the required changes.

Note **Selected count/<total number of rows> -** Displays the number of rows selected by the total number of rows in the table.

Delete Credentials for Multiple Prime NAMs

Step 1 Choose **Inventory** > **Inventory Management** > **Configure NAM**.

Step 2 Check the checkbox of the credential of your choice.

Step 3 Click **Delete**.

A message pops up indicating that Are you sure you want to delete the selected NAM(s)?

Note If an error occurs, while deleting NAM(s), check the logs.

Verify Credentials for Multiple Prime NAMs

Step 1 Choose **Inventory** > **Inventory Management** > **Configure NAM**.

Step 2 Select the NAM for which you want to verify credentials.

Step 3 Click **Verify**.

Note While the NAM is in “Verifying” state, you can either Verify or Delete a NAM. If you try to verify or delete a NAM, a message appears indicating that NAM Credential(s) cannot be deleted or verified while NAM is in “Verifying” state.

Add Multiple NAM Credentials

You can add multiple NAM credentials, by importing a csv file with Prime NAMs details.

CSV (Comma Separated Values) format is the most common import and export format for spreadsheets and databases.

Preparing the CSV File

The CSV file is based on a default Microsoft Excel-styled CSV file. A CSV file contains a number of rows, each containing a number of columns. Fields are separated by commas and any content that must be treated literally, such as commas and new lines/'carriage returns' themselves are enclosed in quotes.

CSV File Requirements

In addition to being 'well-formed', CSV files have the following requirements.

Each CSV file must possess a heading row.

The CSV file import uses a CSV file's header row to determine how to map data from the CSV file's 2nd row and beyond to fields in the database.

The header row should avoid containing any punctuation (apart from the commas separating each column) or the importer may not work correctly.

CSV supports two types of header file formats: 6 header and 7 header.

- In 12.1 and earlier, it was a 7 header format because HostName and IP Address were two different fields.
- In 12.1 Service Pack 3, it is a 6 header format because it supports both HostName and IP Address in a single field.

The CSV file must contain the following details for each Prime NAM Server:

CSV 6 header file format with HostName

DisplayName	HostName	Protocol	Port	UserName	Password
nam	nam.atlas.local	HTTP	80	admin	Atlas!123

CSV 6 header file format with IPAddress

DisplayName	IPAddress	Protocol	Port	UserName	Password
NAM	10.104.243.11	HTTP	80	admin1	Nam!123

From 12.1 Service Pack 3 and later, it is recommended to use a 6 header file format only for NAM import. If there is an import file prepared in 11.6 and earlier, the same header file can reused in 12.1 Service Pack 3 and later releases.

Note

- Ensure that the rows are not left blank and each record is one line.
- Leading and trailing whitespace is ignored.
- Embedded line-breaks.
- Hostname must be resolvable to IP address.

Import Credentials for Prime NAMs

Step 1 Choose **Inventory** > **Inventory Management** > **Configure NAM**.

Step 2 In the **Import NAM** section, click **Choose File** button to browse to the local csv file, and click **Import** to import the NAM in CSV format.

Step 3 Click **Import**.

Step 4 Click **Refresh** icon to view the latest NAM credential status".

Step 5 Click **Save**.

Credential Verification - Error Messages

Various credential verification error messages are tabulated below. These messages are introduced as part of NAM Import.

Success/Error Message	Condition	Possible Solutions
IMPORT_PROCESS_ SUCCESS_MESSAGE	All the NAM records are successfully imported.	Success message
IMPORT_PROCESS_ SKIPPED_FEW_RECORDS	Failed for one of the following reasons:	
	1. “All the NAM records are not successfully imported. Could not resolve the Hostname for record. Please check the import file. If the problem persists, check the logs.”	
	2. “All the NAM records are not successfully imported. Could not resolve the IP Address for record. Please check the import file. If the problem persists, check the logs.”	
	3. “All the NAM records are not successfully imported. Could not resolve the Hostname or IP Address for record. Please check the import file. If the problem persists, check the logs.”	
IMPORT_PROCESS_FAILURE	"All the NAM records are not successfully imported. Please check the import file. If the problem persists, check the logs.”	Check for duplicates and enter correct data, for example, IP Address.

Success/Error Message	Condition	Possible Solutions
INCORRECT_FILE_FORMAT	"Imported file format is incorrect. Please check the user guide for the exact format and import the file in CSV format only."	Import the file in CSV format only.
IMPORT_FILE_ HEADERS_EMPTY	"File headers are incorrect. Please check the user guide for the exact format."	Choose a file with correct header.
IMPORT_FILE_ CONTENT_EMPTY	"Imported file contents are empty or not proper. Please check the user guide for the exact format."	Enter NAM data.

Use NAM Credentials to Troubleshoot Problems and Verify Credentials

Any problem that prevents Cisco Prime Collaboration Assurance from contacting and connecting to NAM can interrupt the collection and analysis of call data and configuration data. You can perform te following:

- Verify that credentials are valid and that Cisco Prime Collaboration Assurance is actively obtaining data.
- Troubleshoot if you notice potential problems with NAM credential status or with reports (such as an unusual time gap).

Step 1 Perform the following troubleshooting:

For a Cisco Unified CM—Do the following:

- Verify that credentials for the cluster on Cisco Unified CM match those in Cisco Prime Collaboration Assurance, and correct, if necessary.
- Verify that DNS parameters are specified correctly on the Cisco Prime Collaboration Assurance server and the Cisco Unified CM hostname has been added to DNS. (Cisco Prime Collaboration Assurance must be able to resolve the IP address for Cisco Unified CM to obtain the correct name.)
- Check whether any known problems exist that prevent successful data exchange between a cluster and Cisco Prime Collaboration Assurance.
- This can happen after the connection between Cisco Prime Collaboration Assurance and Cisco Unified CM is reestablished after a break. Cisco Unified CM first sends old files to Cisco Prime Collaboration Assurance.
- Credentials that Cisco Prime Collaboration Assurance relies upon might change on a Cisco Unified CM platform. If this happens, check with your Unified CM administrator to obtain the correct credentials. If necessary, update the credentials in Cisco Prime Collaboration Assurance.

Step 2 Verify the credentials:

a) Choose **Assurance Administration** > **CDR Source Settings** > **Manage Call Quality Data Sources**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration** > **CDR Source Settings** > **Manage Call Quality Data Sources**.

For Cisco Prime Collaboration Release 12.1 SP3 and later

Choose **Inventory** > **Inventory Management** > **Configure NAM**.

b) Select the NAM for which you want to verify credentials.
c) Click **Verify**.

Call Classification

Cisco Prime Collaboration Assurance uses call classification to categorize calls in Call Detail Record (CDR) reports.

Cisco Prime Collaboration Assurance determines whether a call fits in system-defined call categories by analyzing the following data:

- Details from CDRs
- Device types of the source and target endpoints
- Direction of the call (incoming or outgoing)
- Protocol (H.323, MGCP, or SIP)

Note CDR reports older than seven days are purged.

The following table lists system-defined call category types and names, and describes the calls included in the category type.

Category Type	Description	Category Name
Voicemail	Calls to or from voicemail.	Unity Voicemail—Calls that meet system-defined criteria for a voicemail call, such as calls to and from Cisco Unity and Cisco Unity Connection. **Note** You can add user-defined category names to this category type.
Conference	Calls to or from a conferencing system.	Conference Bridge—Calls that meet system-defined criteria for a call involving a conference bridge. **Note** You can add user-defined category names to this category type.

ICT	Calls to or from an intercluster trunk (ICT).	• ICT GK Controlled—ICT calls that are gatekeeper controlled. • ICT Non-GK Controlled—ICT calls that are not gatekeeper controlled.
VG/Trunk-Outgoing	Calls to a voice gateway or a trunk; only OffNet calls are included. **Note** User-defined dial plans are applied to calls in the VG/Trunk-Outgoing call category.	• MGCP Gateway Outgoing—Calls to an MGCP voice gateway. • H.323 Gateway Outgoing—Calls to an H.323 voice gateway. • H.323 Trunk Outgoing—Calls to an H.323 trunk. SIP Trunk Outgoing—Calls to a SIP trunk.
VG/Trunk-Incoming	Includes calls from a voice gateway or a trunk; only OffNet calls are included.	• MGCP Gateway Incoming—Calls from an MGCP voice gateway. • H.323 Gateway Incoming—Calls from an H.323 voice gateway. • H.323 Trunk Incoming—Calls from an H.323 trunk. SIP Trunk Incoming—Calls from a SIP trunk.
Tandem	A tandem call occurs when both endpoints are voice gateways or trunks.	Tandem.
OnNet Trunk	Calls where one endpoint is a trunk and the call is not an OffNet call. For example, the trunk could be used to connect to WebEx or to a PBX.	• OnNet H.323 Trunk. • OnNet SIP Trunk.
Internal	Calls that do not fall into any of the above categories. For example, calls where one endpoint is an IP phone and the other endpoint is a voice gateway and the call is not an OffNet call.	Internal.

Unknown	For system-related reasons, Prime Collaboration could not determine the device type of the endpoints.	Unknown.

Cisco Prime Collaboration Assurance places a call in the user-defined call category if:

- The call has already been categorized as an Internal, VG/Trunk-Outgoing, or OnNet Trunk call.
- A user-defined dial plan is assigned to the cluster in which the call occurred.

Understand OffNet and OnNet Calls

A call is considered to be OffNet when at least one endpoint is a gateway or a trunk and when any of the following is also true of the endpoint:

- The Call Classification parameter is set to Offnet in the gateway configuration—or the trunk configuration—in Unified CM (Administration).
- In Unified CM, both of the following are true:

  Call Classification parameter is set to System Default in the gateway or trunk configuration.

  System Default service parameter is set to Offnet.
- The endpoint is an analog gateway.

Any call that does not meet the criteria for an OffNet call is considered to be an OnNet call.

Call Category Creation

You can create a call category when you add a dial pattern to a dial plan.

To add a call category, choose **CDR Analysis Settings** > **Set Call Category**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration** > **CDR Analysis Settings** > **Set Call Category**.

For Cisco Prime Collaboration Release 12.1 SP3 and later

To add a call category, choose **Alarm & Report Administration** > **CDR Analysis Settings** > **Set Call Category**.

Cisco Prime Collaboration Assurance supports a few predefined set of call categories that determine how they are used within Cisco Prime Collaboration Assurance.

The following is a set of predefined call categories: Unity Voicemail, Local, Long Distance, International, Emergency, Service, and Toll Free.

Create Custom Call Category

Cisco Prime Collaboration Assurance also allows you to create custom call category.

Step 1 Click **Alarm & Report Administration** > **CDR Analysis Settings** > **Set Call Category**.

Step 2 Click **Add** button to create a custom call category. A new row is displayed at the end of the table.

Step 3 Choose **Call Category Type** from the drop-down.

Step 4 Click **Save**.

You can create a new call category, select the checkbox to modify the existing call category, or select multiple checkbox(s) to **Delete** the call category.

Dial Plan Addition

A dial plan must have a unique name, can include a set of toll-free numbers, and must include a set of dial patterns. A dial pattern identifies a call category name and type and specifies the rule or pattern that a directory number must match for the call to be included in the category.

Cisco Prime Collaboration Assurance provides a default dial plan as a starting point from which you can define your own dial plans. The default dial plan includes default dial patterns: call category names, types, and rules. As you configure a dial plan, you can add, modify, and delete the rules that are specified in the default dial plan.

You can create multiple dial plans. You can assign only one dial plan to each cluster, but you can assign the same dial plan to multiple clusters.

For Cisco Prime Collaboration Release 11.5 and earlier

To add a dial plan, choose .

For Cisco Prime Collaboration Release 11.5 and later

To add a dial plan, choose **Alarm & Report Administration** > **CDR Analysis Settings** > **Dial Plan Configuration**.

To assign a dial plan, choose **Alarm & Report Administration** > **CDR Analysis Settings** > **Dial Plan Assignment**.

Understand the Default Dial Plan

When you add a dial plan, a copy of the default dial plan is displayed for you to update. You can:

- Select from the existing Call Category names.
- Add, update, or delete dial patterns

For Cisco Prime Collaboration Release 12.1 SP3 and later

- Select from the existing Call Category names.
- Add, update, or delete dial patterns

Changes that you make while configuring a dial plan have no effect on the default dial plan, which is based on the North American Numbering Plan (NANP).

The following table provides the default dial plan values.

Condition	No. of Chars	Default Pattern	Call Category Name	Call Category Type	Explanation	Priority

>	3	011!	International	International	If the number of digits dialed is greater than 3 and starts with 011, the call is classified as International.	1
=	7	!	Local	Local	If the number of digits dialed is equal to 7 and the pattern is ! (more than one digit; in this case, 7 digits), the call is classified as Local.	2
=	10	T!	Toll Free	Toll Free	If the number of digits dialed is equal to 10 and the pattern is T! (more than one digit; in this case, a 10-digit number that starts with a toll-free number that is defined in the dial plan), the call is classified as Toll Free.	3

=	10	G!	Local	Local	If the number of digits dialed is equal to 10 and the pattern is G! (more than one digit; in this case, a 10-digit number that starts with a gateway code that has been defined in Cisco Prime Collaboration Assurance), the call is classified as Local.	4
=	10	!	Long Distance	Long Distance	If the number of digits dialed is equal to 10 and the pattern is ! (more than one digit; in this case, a 10-digit number), the call is classified as Long Distance.	5

=	11	T!	Toll Free	Toll Free	If the number of digits dialed is equal to 11 and the pattern is T! (more than one digit; in this case, an 11-digit number that starts with a toll-free number that is defined in the dial plan), the call is classified as Toll Free.	6
=	11	XG!	Local	Local	If the number of digits dialed is equal to 11 and the pattern is XG! (more than one digit; in this case, an 11-digit number that starts with any single digit followed by a gateway code that has been defined in Cisco Prime Collaboration Assurance), the call is classified as Local.	7

=	11	!	Long Distance	Long Distance	If the number of digits dialed is equal to 11 and the pattern is ! (more than one digit; in this case, an 11-digit number), the call is classified as Long Distance.	8

Note Cisco Prime Collaboration Assurance classifies the call as Toll Free if the toll-free code is defined in the dial plan that is assigned to the cluster.

Add a Dial Plan

You can add a dial plan .

For Cisco Prime Collaboration Release 11.5 and earlier

Step 1 Choose **CDR Analysis Settings** > **Dial Plan Configuration**. Click **Add**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration** > **CDR Analysis Settings** > **Dial Plan Configuration**. Click **Add**.

The **Add Dial Pattern** dialog box is displayed.

For Cisco Prime Collaboration Release 12.1 SP3 and later

Choose **Alarm & Report Administration** > **CDR Analysis Settings** > **Dial Plan Configuration**.

Enter a name to add a new dial plan in **Dial Plan Name** field.

Click **+** (Add) at the end of the table to add a dial pattern.

A new row is created.

Step 2 Create a dial pattern by supplying data in these fields:

- **Condition** - Applies to the number of characters. Select one:
  - Left Arrow (<) - Less than
  - Right Arrow (>) - Greater than
  - Equals symbol (=) - Equal to

- **Number of Chars** - Enter the total number of digits and non-numeric characters, including plus (+), pound (#), asterisk (*), comma (,), and the at symbol (@). Expresses the number of characters in the directory number to which the dial pattern applies.
- **Pattern** - Enter the pattern to apply to the digits, where:
  - G indicates that the digits identify a gateway code.
  - T indicates that Cisco Prime Collaboration Assurance should compare the digits with the toll-free numbers configured in the dial plan.
  - ! signifies multiple digits (any number that is more than 1 digit in length, such as 1234 or 5551234).
  - X signifies a single-digit number (such as 0, 1, or 9).
- **For Cisco Prime Collaboration Release 12.1 SP2 and earlier**

  Call Category Name - Select one of the following radio buttons and supply data as required:
  - **Existing** - Select an existing call category name.
  - **New** - Enter a unique name and select a call category type.
- **For Cisco Prime Collaboration Release 12.1 SP3 and later**

  Call Category Name - Select an existing call category name from the drop-down list that are configured using the "Set Call Category" user interface.

Step 3 Click **OK**.

For Cisco Prime Collaboration Release 12.1 SP3 and later

Click **Save**.

The row is added to the table.

Apply Dial Patterns to VG/Trunk-Outgoing, Internal, and OnNet Trunk Calls

The following table shows how dial patterns are applied from a user-defined dial plan to a call in the Internal, VG/Trunk-Outgoing, or OnNet Trunk call category.

Cisco Prime Collaboration Applies Dial Patterns of This Category Type...	To the Directory Number that is the...	In a Call That Is in This System-Defined Category...
• Conference • Emergency • International • Local • Long Distance • Service • Toll Free • Voicemail	Destination	VG/Trunk-Outgoing
• Conference • Voicemail	Source	
• Conference • Voicemail	• Source • Destination	• Internal • OnNet Trunk

Edit a Dial Plan

You can edit a dial plan. While editing a dial plan, you can add, edit, or delete dial patterns.

Step 1 Choose **Alarm & Report Administration** > **CDR Analysis Settings** > **Dial Plan Configuration**.

Step 2 Click the icon (Edit) to modify a dial pattern.

Step 3 Make the required changes.

Step 4 Follow **Step 3** from “Add a Dial Plan” to modify the existing dial pattern.

Step 5 Click the icon (Save). The row is updated to the table.

Delete a Dial Plan

You can remove a dial plan.

Step 1 Choose the respective row and click the **Delete** button to remove the dial plan.

Step 2 Click **Save** to keep all the changes on the dashlet.

Click **Cancel** to exit.

Configure Gateway Codes

Cisco Prime Collaboration Assurance uses the gateway codes that you configure to determine the call classification for an external call.

Note To view the gateways for which gateway codes are already configured, select clusters and click **View**. The Gateway Code report displays only Media Gateway Control Protocol (MGCP), and H323 gateways. The analog Signaling Connection Control Part (SCCP) gateway is not displayed.

To configure gateway codes:

Step 1 Choose **Assurance Administration** > **CDR Analysis Settings** > **Gateway Code Configuration**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration** > **CDR Analysis Settings** > **Gateway Code Configuration**.

Step 2 On the Gateway Code Summary page, select a cluster and click **Manage Gateway Code**.

Step 3 Enter the gateway code, and then click **Apply**.

Configure SFTP Settings

If you are using Unified Communications Manager to monitor calls, you must configure SFTP settings.

To configure SFTP settings:

Step 1 Choose **Assurance Administration** > **CDR Source Settings** > **CUCM SFTP Credentials**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Alarm & Report Administration** > **CDR Source Settings** > **CUCM SFTP Credentials**.

For Cisco Prime Collaboration Release 12.1 and later

Choose **Inventory** > **Inventory Management** > **CUCM/SFTP Credentials**.

For Cisco Prime Collaboration Release 12.1 SP3 and later

Choose **Inventory** > **Inventory Management**. Click on **CUCM SFTP Credentials** tab.

Step 2 Enter the required information. For field descriptions, see the table for SFTP Settings Page - Field Descriptions.

Step 3 Click **Save**.

A popup message window is displayed to confirm whether you want to update the SFTP credentials across all the managed Unified Communications Manager publishers.

Note Cisco Prime Collaboration Assurance is added as a billing server in the managed Unified Communications Manager publishers.

Step 4 Click **Yes**.

SFTP Settings Page - Field Descriptions

For Cisco Prime Collaboration Release 12.1 SP3 and later

The following table describes the fields in the SFTP Settings page.

Table 1: SFTP Settings Page - Field Descriptions

Fields	Description
Username	You cannot change the username from smuser. This same username, smuser, must be configured in Cisco Unified Communications Manager.
Password	During fresh installation, ensure that the CUCM SFTP Credential is not set by default. You must set the CUCM SFTP password in **Inventory Management** -> **CUCM SFTP Credentials** tab. If credentials is not set, user will not be allowed to add PCA as a CDR Destination in CUCM during device discovery. The application must alert the user to set the CUCM SFTP password stating, "Please configure CUCM SFTP credentials to enable this feature. It can be configured under CUCM SFTP Credentials Tab". **Note** If you want to add PCA as a CDR destination in CUCM, while initiating device discovery, select the “Add the Prime Collaboration server as a CDR Destination in the Unified CM servers" check box in **Discover Devices** -> **Device Discovery** tab under **Auto-Configuration** option. For more information, see the section on “Discovery Methods”. **For Cisco Prime Collaboration Release 12.1 SP3 and earlier** The default password is smuser. If you change the password here, you must also change the password for smuser in Cisco Unified Communications Manager.
Re-enter Password	Enter Password to confirm.

For Cisco Prime Collaboration Release 12.1 SP3 and earlier

The following table describes the fields in the SFTP Settings page.

Table 2: SFTP Settings Page - Field Descriptions

Fields	Description
Low-Volume Schedule Hours	
<day> <timerange>	For each day of the week, timerange indicates the hours during which Cisco Prime Collaboration Assurance processes fewer records. During the low-volume schedule, Cisco Prime Collaboration Assurance performs database maintenance.
Miscellaneous	
Wait for Diagnostic Report (min)	Number of minutes that Cisco Prime Collaboration Assurance continues to search, when there is a large volume of data, before displaying the matching records found for a diagnostic report.
Report Data Retention Period (days)	Number of days that data is retained in the Cisco Prime Collaboration Assurance database before being purged.
SFTP	
Username	You cannot change the username from smuser. This same username, smuser, must be configured in Cisco Unified Communications Manager.

Fields	Description
Change password check box	**For Cisco Prime Collaboration Release 12.1 SP3 and later** During fresh installation, ensure that the CUCM SFTP Credential is not set by default. You must set the CUCM SFTP password in **Inventory Management** -> **CUCM SFTP Credentials** tab. If credentials is not set, user will not be allowed to add PCA as a CDR Destination in CUCM during device discovery. The application must alert the user to set the CUCM SFTP password stating, "Please configure CUCM SFTP credentials to enable this feature. It can be configured under CUCM SFTP Credentials Tab". **Note** If you want to add PCA as a CDR destination in CUCM, while initiating device discovery, select the “Add the Prime Collaboration server as a CDR Destination in the Unified CM servers" check box in **Discover Devices** -> **Device Discovery** tab under **Auto-Configuration** option. For more information, see the section on “Discovery Methods”. **For Cisco Prime Collaboration Release 12.1 SP3 and earlier** The default password is smuser. If you change the password here, you must also change the password for smuser in Cisco Unified Communications Manager.

Administrative Reports

The following administrative reports are available:

Report	Description

System Status Report	Provides information about Inventory, Data Purging, Notifications, Phone Licensing (comprises of Synthetic Tests, Phone Status Tests, and IP SLA Voice Tests), and System Limits.
	It also provides information about Synthetic Tests, Phone Status Tests, and IP SLA Voice Tests for the following test results only:
	• Synthetic Tests: If the test failed to run because of High CPU Utilization in the Cisco Prime Collaboration Assurance server.
	• Phone Status Tests: If the SAA source device is not reachable.
	• IP SLA Voice Tests:
	  • If the configuration is incorrect.
	  • If the device has low memory.
	  • If the source device is not responding.
	  • If the device has rebooted.
	It provides information about phone status test for the following test result:
	• Phone Status test: If the SAA source device is not reachable.
	For the following parameters of System Limits:
	• Port - Ethernet ports are categorized under this parameter.
	• Interfaces - Voice interfaces are categorized under this parameter.

Who Is Logged On Report	Helps you to identify users who are currently logged into Cisco Prime Collaboration Assurance.
Process Status	Shows the status of processes that are currently running on Cisco Prime Collaboration Assurance.

CDR & CMR Call Report

Cisco Prime Collaboration Assurance can process only CDR and CMR data of last 24 hours. CDR reports displays call details such as call category type, call class, call duration, termination type, call release code, and so on. CMR reports can be cross launched from Top 5 Voice Call Quality Location and CDR reports can

be cross launched from Top 5 Call Failure Location. You can also cross launch CMR reports from ServiceQualityThresholdCrossed alarm . The report loads up to 40 records initially, you can scroll down to view more records.

You can select any grade from the generated report to view the details of CMR reports for that particular CDR Record in an inline CMR (popover).

Note CDR reports work only when both Cisco Prime Collaboration Assurance and CUCM are in the same domain.

CMR report generate reports that include all call data from the clusters or reports that include a subset of call data.

The following table describes the fields of CDR call reports.

Field	Description
Grade	Based on voice call grade settings. Select one of the following: • Good—The call value is less than the threshold value of long call SCSR (%) or short call SCSR (%) . The value of this grade appears in green color. • Acceptable—The call value is greater than or equal to threshold value of long call SCSR (%) or short call SCSR (%). The value of this grade appears in orange color. • Poor—The call value is greater than the threshold value of long call SCSR (%) or short call SCSR (%). The value of this grade appears in red color. • N/A—The SCSR (%) value is not available or is negative. • All— Select all the grade.
Cluster ID	Unified Communications Manager cluster.

Caller/Called	• **Directory Number**—Directory number where the call was made. • **Device Type**—Type of device making the call. • **Signaling IP**—IP address of the device that originated the call signaling. For IP Phones, this field specifies the address of the phone. For PSTN calls, this field specifies the address of the H.323 gateway. • **B-Channel**—B-channel number of the MGCP gateway, or NA, if not applicable. • **Media IP**—IP address where the call originated. • **Codec**—Codec name. • **Media Port**—Port through which the call originated. • **Device Pool**—Device pool where the call originated. • **Device Location**—Location where the call originated. When you select the **Quick Filter** from **Show** drop-down menu, search option is available for Caller/Called Device Location. • **Device Name**—Name of the device. • **Termination Cause**—String that describes why the call was terminated.
Caller Video/Called Video	• **Video Codec**— Video Codec name. • **Video Bandwidth**— Bandwidth of the video. • **Video IP**— IP address where the video originated. • **Video Port**— Port through which the video originated. • **Video Resolution**— Resolution of the video.
Call Class	One of these: • Offnet • Onnet **Note** For more information, see Understand OffNet and OnNet Calls, on page 9.

Time Period	Date and time that the call started with respect to the Cisco Prime Collaboration Assurance server local time zone (not the time zone in which Cisco Unified CM resides). The maximum time limit is 7 days. .
Call Duration(s)	Length of the call, in seconds.
Call Category Names	A comma-separated list of the categories to which the call belongs. For more information, see Call Classification, on page 7 and Call Category Creation, on page 9
Call Category Types	A comma-separated list of the category types to which the call categories belongs. For more information see Call Classification, on page 7 and Call Category Creation, on page 9

The following table describes the fields of CMR reports.

Field	**Description**
MOS	Average MOS value during the sample duration. The value might be N/A or not available if the sample duration is very short. MOS reflects the experience of the listener.
Minimum MOS	The minimum MOS score within the sample duration. The value might be N/A or not available if the sample duration is very short.
Grade	Based on voice call grade settings. Select one of the following: • Good—The call value is less than the threshold value of long call SCSR (%) or short call SCSR (%). The value of this grade appears in green color. • Acceptable—The call value is greater than or equal to threshold value of long call SCSR (%) or short call SCSR (%). The value of this grade appears in orange color. • Poor—The call value is greater than the threshold value of long call SCSR (%) or short call SCSR (%). The value of this grade appears in red color. • N/A—The SCSR (%) value is not available or is negative. • All— Select all the grade.

Caller/Called	• **Directory Number**—Directory number where the call was made. • **Device Type**—Type of device making the call. • **Signaling IP**—IP address of the device that originated the call signaling. For IP Phones, this field specifies the address of the phone. For PSTN calls, this field specifies the address of the H.323 gateway. • **B-Channel**—B-channel number of the MGCP gateway, or NA, if not applicable. • **Media IP**—IP address where the call originated. • **Codec**—Codec name. • **Media Port**—Port through which the call originated. • **Device Pool**—Device pool where the call originated. • **Device Location**—Location where the call originated. When you select the **Quick Filter** from **Show** drop-down menu, search option is available for Caller/Called Device Location. • **Device Name**—Name of the device.
Listener DN/IP	Identifies the endpoint-called or caller-for which MOS and impairment details are reported; one of these: • IP address of the listener. • Directory number of the listener.
Jitter (ms)	Milliseconds of jitter during the sample duration.
Packet Loss	Number of packets lost due to network transmission during the sample duration. Computed based on observed RTP sequence number analysis.
Max Jitter (ms)	Maximum milliseconds of jitter during the sample duration.
Conceal Seconds	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely conceal seconds).
Severely Conceal Seconds	Number of seconds during which a significant amount of concealment (greater than fifty milliseconds) was observed.
Conceal Ratio	Ratio of concealment frames to total frames.

Latency	Delay
Cluster	Unified Communications Manager cluster.
Time Period	Date and time that the call started with respect to the Cisco Prime Collaboration Assurance server local time zone (not the time zone in which the Unified Communications Manager resides).
Call Duration(s)	Length of the call, in seconds.
Caller Termination Cause	String that describes why the call was terminated on the caller endpoint
Called Termination Cause	String that describes why the call was terminated on the called endpoint. See Call termination cause codes section in Cisco Unified Communications Manager Call Details Record Administration Guide for the cause codes for failed calls.
Video attributes	Endpoints Report contain video attributes (for video endpoints) such as: • Video duration • Video packets lost • Video jitter • Video round trip time • Video RX Resolution • Video RX Frames Lost
Severely Conceal Seconds Ratio (%)	A metric to measure the voice quality. It is the ratio of Severely Conceal seconds(SCS) and total call duration.
Conceal Seconds Ratio (%)	A metric to measure the network quality. It is the ratio of Conceal seconds(CS) and total call duration.

Note

- All the columns may not appear in CDR & CMR reports by default. To view other fields, click **settings** button and choose **columns**.
- CDR & CMR reports support Jabber.

For Cisco Prime Collaboration Release 11.5 and later

The Location field displays the location that is configured on a device pool instead of the location that is configured on the device, when you set the device location to one of the system locations (Hub_None, Phantom, or Shadow).

Note

- Cisco Prime Collaboration Assurance displays a user defined location instead of Hub_None in Unified Communications Manager for the following features and reports:
  - CDR & CMR Reports
  - Top 5 Poor Voice Call Quality Locations
  - Top 5 Call Failure Locations
  - Unregistered Phone Troubleshooting: Top 5 locations
  - Global Search by location
- If the device location is set to Hub_None and is not associated with any user defined device pool in Unified Communications Manager, Cisco Prime Collaboration Assurance displays the Device Location as Hub_None. Cisco Prime Collaboration Assurance also displays Hub_None as a valid location in Global Search by location option and in Unified Communications Manager troubleshooting view.

You can filter the fields of report using Quick Filter options. For more information, see the Quick Filter section in Filters.

The CDR & CMR report can be exported in both CSV and PDF format. The maximum number of records that can be exported to a PDF file is 30,000. The maximum number of records that you can export to CSV is 200,000.

To export the report, click the **Export** tool button in the right-hand pane of the report window. If your client system seems unresponsive when you try to export files, see Troubleshoot File Download Issues.

The supported video codecs in CDR & CMR report are listed in the following:

- AAC
- G711Alaw 56k
- G711Alaw 64k
- G711Ulaw 56k
- G711Ulaw 64k
- G722 48k
- G722 56k
- G722 64k
- G722.1 24k
- G722.1 32k
- G723.1
- G726 16K
- G726 24K
- G726 32K

- G728
- G729
- G729AnnexA
- G729AnnexAwAnnexB
- G729AnnexB
- GSM
- GSM Enhanced Full Rate
- GSM Full Rate
- GSM Half Rate
- iSAC
- H.264
- H.265

Generate CDR & CMR Reports

To generate CDR & CMR call report:

Note Only an administrator can export CDR/CMR reports. A script must be created to automate the task of exporting on the server.

Step 1 Choose **Assurance Reports** > **CDR & CMR Reports**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports** > **CDR & CMR Reports**.

The CDR & CMR Reports page is displayed.

Step 2 Enter the information in the fields described below:

Table 3:

Field	Description
Display	Select CDR/CMR from the Display
Cluster	Select the Clusters from Cluster. The default value is All.

Field	Description
Location/Devicepool	Select the Location or Devicepool from Location/DevicePool. The default value is Location. If you select Location from Location/DevicePool then select any location from Location. If you select Devicepool from Location/DevicePool then select any devicepool from Devicepool. You can also search Location/Devicepool from the search option available in Location or Devicepool. The default value for Location or Devicepool is Any.
Device Type	Select the devices from Device Type. The default value is Any.
Endpoint	Select Directory Number or IP Address from the Endpoint. The default value is Directory Number.
Caller	Enter the Directory Number or Caller IP address. The default value of Directory Number is * and default value of IP address is *.*.*.*. Directory Number can include any combination of alphanumeric characters and special characters like +,*, @, _, -, . For Directory Number search, use uppercase X as a single-digit wildcard; use * as multiple-digit wildcard. For example 1100X or 11*. For IP address search, the * wildcard applies to the entire octet. For example: 172.30.*.* or 2005:0420:2e00:0094:*:*:*:*.
Called	Enter the Directory Number or Called IP address. The default value of Directory Number is * and default value of IP address is *.*.*.*. Directory Number can include any combination of alphanumeric characters and special characters like +,*, @, _, -, . For Directory Number search, use uppercase X as a single-digit wildcard; use * as multiple-digit wildcard. For example 1100X or 11*. For IP address search, the * wildcard applies to the entire octet. For example: 172.30.*.* or 2005:0420:2e00:0094:*:*:*:*.
Call Category	Select the name or type from the Call Category. The default value is Name.
Category Name/Type	Select the Category name or Category Type. The default value is All.

Field	Description
Grade	Select Good, Acceptable, Poor, All or N/A. The default value is All.
Jitter	Select the range from Jitter and enter the value in milliseconds. The default range is greater than or equal to zero.
Packet Loss	Select the range from Packet Loss and enter the value in the field. The default range is greater than or equal to zero.
Conceal Seconds	Select the range and enter the value in seconds field. The default range is greater than or equal to zero.
Conceal Ratio	Select the range from Conceal ratio and enter the value in the field. The default range is greater than or equal to zero.
Call Type	Select Audio, Video or Any. The default value is Any.
Call Class	Select On-Net, Off-Net, or Any. The default value is Any.
Call Duration	Select the value of call duration from Call Duration and enter the time in secs field. The default value is Any.
Termination Type	Select Success, Failed, or Any. The default value is Any.
Termination Cause Code	Select the cause code from Termination Cause Code. The default value is All.
Time Period	Select **Call Connect Time** or **Call Disconnect Time**. The default value is **Call Connect Time**. In case of cross launch from Top N dashlet, the default value is **Call Disconnect Time**. Call Connect Time—time when the call originates. Call Disconnect Time—time when the call ends. Select Past or Enter the Start Time and End Time. The default value is Past. The default value for the Start Time is one hour less than Current Time and End Time is Current Time. You can select Past in Minutes, Hour(s), or Days. The default value for Past is 1 Hour(s). For example, if you select Past as 8 Hour(s) at 10 p.m today then it displays the records from 2 p.m to 9.59 p.m today. If you select Past as 1 day at 10 a.m today then it displays the records from 12 a.m through 11.59 p.m of previous day.

The Jitter, Packet Loss, Conceal Seconds, Conceal Ratio fields are applicable only for CMR Filter and Call Category, Call Type, Call Class, Call Duration, Termination Type, and Termination Cause Code fields are applicable only for CDR Filter.

Step 3 Click **Apply Filter**.

The CDR & CMR report is generated.

When records are not available for the selected filter, it displays no data available.

CDR & CMR report displays only the records of last 7 days.

Troubleshoot

1. **Issue**: CDR & CMR report displays Grade as N/A.

   Recommended Action: Check if Severely Conceal Seconds Ratio value is not received from the endpoint or CMRs are not present.

2. **Issue**: Severely Conceal Seconds Ratio is x% and call is graded as Poor Call but in actual the call is not a poor call.

   Recommended Action: You can configure threshold values for Severely Conceal Seconds Ratio from Voice Call Grade Page under CDR Analysis Settings.

3. **Issue**: Call grading is incorrect.

   Recommended Action: Cross check the threshold values for Severely Conceal Seconds Ratio against Severely Conceal Seconds Ratio value in the CMR Report for the calls.

4. **Issue**: CDR/CMR Records are not received.

   Recommended Action: Perform one of the following:

   - Add PCA as billing server in the Unified CM, if it is not added.

     When you add PCA as billing server, check the **resend on failure** option in the Unified CM to avoid any failure of CDR delivery.

   - Verify if SFTP username/password is same in Cisco Prime Collaboration Assurance and billing server in Unified CM.
   - Check if CDR repository manager or CDR agent services are up in Unified CM.
   - Check if "CDR Enabled Flag" and "Call Diagnostics Enabled" options are set correctly in Unified CM.
   - Check If any firewall settings blocks the file transfer, if it blocks then correct this at the network infrastructure level.
   - If Data collection of a cluster is in Failed state in Call Quality Data source management page then run rediscovery for that publisher. For a list of Setting Up Devices and Configure Devices for Cisco Prime Collaboration Assurance, see the following:
     - Setting Up Devices for Cisco Prime Collaboration Assurance
     - Configure Devices for Cisco Prime Collaboration Assurance

NAM & Sensor Report

NAM & Sensor report displays the name of the sensor that collected the data, MOS, jitter, and time stamp.

Note This report is not applicable if you have installed Cisco Prime Collaboration Assurance in MSP mode.

To generate NAM & Sensor report, choose **Assurance Reports** > **NAM & Sensor Reports**. Enter the values in required fields and click **Generate Report**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports** > **NAM & Sensor Reports**.

The following table describes the fields of NAM & Sensor reports.

Field	Description
Name	Descriptive name for the sensor that collected the data and analyzed the MOS. **Note** The name Cisco 1040 + < *last 6 digits from MAC address* > identifies a Cisco 1040 that automatically registered with Cisco Prime Collaboration Assurance.
ID	1040 MAC address or Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM) IP address.

Speaker/Listener	Directory Number—Displayed when the device is managed by a Unified Communications Manager that: • Is added to Cisco Prime Collaboration Assurance with the proper credentials • Has not been suspended from monitoring. Device Type—Can provide the device type or one of these: • N/A—Some error prevents Cisco Prime Collaboration Assurance from obtaining the device type. • Unavailable-This is the first time Cisco Prime Collaboration Assurance has seen this phone and the device type is not yet known; or the corresponding Unified CM: • Has not been added to Cisco Prime Collaboration Assurance. • Did not provide a valid device type to Cisco Prime Collaboration Assurance. IP Address—If an IP address is clickable, click it to launch the Detailed Device View page or Phone Detail window. UDP Port—Transport layer port that is the source of the media stream. Device Name.
Time	Time at which the sensor calculated MOS.
TOS	Type of Service (TOS).
MOS	Average MOS value during the sample duration. The value might be N/A or not available if the sample duration is very short. MOS reflects the experience of the listener. Click the value to open a Sensor Stream Correlation window.
Minimum MOS	The minimum MOS score within the sample duration. The value might be N/A or not available if the sample duration is very short.

Primary Degradation Cause	One of these: • Jitter • Packet loss • None—Jitter and packet loss values are both 0 (zero). The value might be N/A or not available if the sample duration is very short.
Grade	Based on voice call grade settings. Select one of the following: • Good—The call value is less than the threshold value of long call SCSR(%) or short call SCSR(%). • Acceptable—The call value is greater than or equal to threshold value of long call SCSR(%) or short call SCSR(%). • Poor—The call value is greater than the threshold value of long call SCSR(%) or short call SCSR(%). • N/A—The SCSR(%) value is not available or is negative. • All— Select all the grade. For more information see Overview of Voice Call Grade Settings.
Jitter (ms)	Milliseconds of jitter during the sample duration.
Packet Loss	Number of packets lost due to network transmission during the sample duration. Computed based on observed RTP sequence number analysis.
Sample Duration(s)	Number of seconds, between the first and last packet that is analyzed. The value is usually 60, but can be less for an initial or final stream.
Max Jitter (ms)	Maximum milliseconds of jitter during the sample duration.
Adjusted Packet Loss(%)	Percentage packet loss due to high jitter. Computed based on a reference jitter buffer with a fixed length delay. This value is not affected by network loss.
Packet Loss (%)	Percent of packet loss. (Packets lost divided by total packets expected expressed as a percent.)
SSRC	Synchronization source ID-Identifies the source of a stream of RTP packets.

Listener DN/IP	Identifies the endpoint-called or caller-for which MOS and impairment details are reported; one of these: • IP address of the listener. • Directory number of the listener.
Cluster	Unified Communications Manager cluster.
Caller/Called	• **Directory Number**—Directory number where the call was made. • **Device Type**—Type of device making the call. • **Signaling IP**—IP address of the device that originated the call signaling. For IP Phones, this field specifies the address of the phone. For PSTN calls, this field specifies the address of the H.323 gateway. • **B-Channel**—B-channel number of the MGCP gateway, or NA, if not applicable. • **Media IP**—IP address where the call originated. • **Media Port**—Port through which the call originated. • **Device Pool**—Device pool where the call originated. • **Location**—Location where the call originated.
Select Time Range	Date and time that the call started with respect to the Cisco Prime Collaboration Assurance server local time zone (not the time zone in which the Unified CM resides). The maximum time limit is 7 days.
Call Duration(s)	Length of the call, in seconds.

Impairment Details	• **Jitter (ms)**—Milliseconds of jitter during the call. • **Packet Loss**—Number of packets lost during the call. • **Concealment Seconds**—Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds). • **Severely Concealed Seconds**—Number of seconds during which a significant amount of concealment (greater than fifty milliseconds) was observed. • **Latency**—Delay • **Concealment Ratio**—Ratio of concealment frames to total frames.
Call Release Code	• **Caller Termination Cause** -String that describes why the call was terminated on the caller endpoint. • **Called Termination Cause** -String that describes why the call was terminated on the called endpoint. See Call termination cause codes section in Cisco Unified Communications Manager Call Details Record Administration Guide for the cause codes for failed calls.
Call Category Names	A comma-separated list of the categories to which the call belongs. For more information, see Call Classification, on page 7 and Call Category Creation, on page 9
Call Category Types	A comma-separated list of the category types to which the call categories belongs. For more information, see Call Classification, on page 7 and Call Category Creation, on page 9
Call Class	One of these: • Offnet • Onnet **Note** For more information, see Understand OffNet and OnNet Calls, on page 9 .
Severely Conceal Seconds Ratio (%)	A metric to measure the voice quality. It is the ratio of Severely Conceal seconds(SCS) and the duration.

Conceal Seconds Ratio (%)	A metric to measure the network quality. It is the ratio of Conceal seconds(CS) and duration.

The NAM & Sensor report can be exported in CSV format.

To export the report, click the **Export** tool button in the right-hand pane of the report window. Select **ALL** or enter the value in **Range** radio button and click **OK**. If your client system seems unresponsive when you try to export files, see Troubleshoot File Download Issues.

Understand Sensor Reports

Two RTP streams—incoming and outgoing—make up a single voice call. Sensors capture voice traffic in various ways:

- Cisco 1040s listen to RTP voice traffic on Switch Port Analyzer (SPAN) ports that have been configured to mirror voice traffic. Depending on the phone ports and the voice VLANs that a SPAN port mirrors, a Cisco 1040 might listen to only one or both RTP streams, calculating MOS and sending data to Cisco Prime Collaboration Assurance at 60-second intervals.
- Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM) can also capture data from SPAN ports. Alternatively, you can configure Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM) to use other means of data capture. For a Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM) to provide the data that Cisco Prime Collaboration Assurance needs, RTP stream monitoring must be enabled on the Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM). Cisco Prime Collaboration Assurance obtains data from Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM) at 60-second intervals.

Sensor reports display the MOS that a sensor calculated for RTP streams on a minute-by-minute basis. For each interval, a sensor report displays one or two rows of data, depending on whether data from only one or both RTP streams was captured. Each row identifies the sensor that collected the data, the endpoints involved, MOS, milliseconds of jitter, and the time stamp.

View Sensor Stream Correlation Data

To launch a Sensor Stream Correlation window, generate a sensor report and click the Grade value for the stream that interests you.

Note If a “Cannot find server” page appears instead of a Sensor Stream Correlation page, see Enable the Sensor Stream Correlation Window to Display.

Cisco Prime Collaboration Assurance correlates data from sensors against one another and against Unified CM call records and displays tables with the following information:

- Stream summary—A subset of the data that was displayed on the sensor report. Additionally, the source synchronization ID (SSRC) for the stream is listed. An SSRC identifies the source of a stream of RTP packets and remains unique during an RTP conference.

Note Another SSRC is assigned to RTP streams sent when the listener endpoint and UDP port are the source of a stream of RTP packets. The Sensor Stream Correlation window correlates data for one SSRC only.

- Call record—Information from the Unified CM CDR that correlates to the stream.

Note If the call is not complete yet, No Call Detail Record found for these streams appears in the table heading.

- Stream details—Details from one or more sensors where the SSRC matches the one in the stream summary.

The following table lists the data that is displayed in the Stream Summary table.

Table 4: Stream Summary

Column	Description

Speaker/Listener	• Directory Number-Displayed when the device is managed by a Unified Communications Manager that:
	  • Is added to Cisco Prime Collaboration Assurance with the proper credentials.
	  • Has not been suspended from monitoring.
	• IP Address-Depending on the device type, an IP Phone Details page or a Detailed Device View opens.
	• UDP Port-Transport layer port that is the source of the media stream.
	• Device Type-Can provide the device type or one of these:
	  • N/A-Some error prevents Cisco Prime Collaboration Assurance from obtaining the device type.
	  • Unavailable-This is the first time that Cisco Prime Collaboration Assurance has seen this phone and the device type is not yet known; or the corresponding Unified CM:
	  • Has not been added to Cisco Prime Collaboration Assurance.
	  • Did not provide a valid device type to Cisco Prime Collaboration Assurance.

TOS	Type of service.
Codec	Codec name.
SSRC	Synchronization Source ID-Identifies the source of a stream of RTP packets.

The following table lists data from the CDR, if available. If the call has not completed yet, No Call Detail Record found for these streams appears in the table heading and the row is blank.

Table 5: Call Record

Column	Description
Call Disconnect	The time that the call disconnected. Zero (0) is displayed if the call never connected.
Cluster ID	Unified CM cluster ID.
Caller Signaling IP	IP address of the device that originated the call signaling. For Cisco Unified IP Phones, this field specifies the address of the phone. For PSTN calls, this field specifies the address of the H.323 gateway.
Caller B-Channel	B-channel number of the MGCP gateway, or NA, if not applicable.
Called Signaling IP	IP address of the device that terminates the call signaling.
Called B-Channel	B-channel number of the MGCP gateway, or NA, if not applicable.
Call Duration (s)	Length of the call, in seconds.
Caller Termination Cause	Populated when the originating party releases the call. **Note** Termination causes might not be populated.
Called Termination Cause	Populated when the terminating party releases the call or the call is rejected. **Note** Termination causes might not be populated.

The following table lists data from streams with an SSRC that matches the one in Stream Summary table.

Table 6: Stream Details

Column	Description
Sensor Name	Display name of the Cisco 1040 or Cisco Prime Network Analysis Module (Prime NAM) or Cisco Prime Virtual Network Analysis Module (Prime vNAM).
Time	Time at which the sensor calculated the MOS.

MOS	Average MOS in the sample duration.
Minimum MOS	Minimum MOS in the sample duration.
Primary Degradation Cause	Jitter, Packet Loss, or None when jitter and packet loss values are zero (0).
Jitter (ms)	Milliseconds of jitter.
Packet Loss	Number of packets lost. (Actual packet loss for the sample duration.)
Sample Duration (s)	Number of seconds elapsed between the first and last packets that are analyzed.
Max Jitter (ms)	Maximum jitter, in milliseconds.
Adjusted Packet Loss (%)	Percentage packet loss due to high jitter. Computed based on a reference jitter buffer with a fixed length delay. This value is not affected by network loss.
Packet Loss (%)	Percentage packet loss. (Actual packets lost divided by total packets expected expressed as a percent.)

Enable the Sensor Stream Correlation Window to Display

When you try to open a Sensor Stream Correlation window, if a window opens displaying a message such as "The page cannot be found", you can resolve the problem by disabling the proxy server setting in your browser. The setting is found in Internet Options on the Connection tab.

Session Reports/Conference Reports

You can use Conference reports to view All Conference Summary report and Conference Detail report.

For Cisco Prime Collaboration Release 12.1 SP2 and later

Prerequisites for Conference Reports

The following are required for conference reports:

- Unified CM and Cisco VCS must be in the Managed state.
- Endpoints and controllers, such as MCU must be in the Managed state.
- Ensure to set the visibility of the devices to "Full Visibility" state.
- JTAPI must be configured on Unified Communications Manager. For information on how to enable JTAPI on Unified Communications Manager, see the Configure Devices for Cisco Prime Collaboration Assurance.
- Cisco Prime Collaboration Assurance server must be registered as a feedback server in Cisco VCS.
- For Conference Diagnostics and Audio Phone Feature Synthetic Tests to work, ensure that CUCM is as per the listed version(s) before applying Cisco Prime Collaboration Assurance Service Pack 1 bundle. For more information, see Supported Devices for Cisco Prime Collaboration Assurance for 12.1 Service Pack 1.

The following reports can be generated for Conference reports:

All Session/Conference Summary Report

The Conference Summary report provides information about the in-progress and completed conferences. The reports are available for four weeks.

This report includes the following information: endpoint name, device ID, total utilization, average duration, and longest conference.

It displays the scheduled duration of the scheduled conference. For an Ad hoc conference this value is displayed as "NA". It also displays utilized scheduled time in % which denotes the scheduled time utilization in percentage.

You can view the following additionally:

- IP address - Displays the IP Address of the selected endpoint that participated in the conference.
- Protocol - Displays the protocol used for the conference. This is displayed in the Participated conferences of Endpoint pane.

Ensure that the visibility of the phones is set to Full, to view the preceding details.

You can view the following additionally

- Received Video DSCP - The last received DSCP value of the video device(s) in the conference. This is only applicable for Cisco Unified IP Phones 8941 and 8945, Cisco DX Series, and Cisco TelePresence TX Series.
- Received Audio DSCP - The last received DSCP value of the audio device in the conference. This is only applicable for Cisco Unified IP Phones 8941 and 8945, Cisco DX Series, and Cisco TelePresence TX Series.
- Peak Packet Loss - The highest value of packet loss (in percentage) that occurred in the conference.

To generate the Conference Summary report, choose **Assurance Reports** > **Session Reports** > **All Session Summary Report** .

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports** > **Conference Reports** > **Conference Summary Report**.

Session/Conference Detail Report

The Conference Detail report provides the following details: conference ID, duration, start/end time, conference type, status, and alarm severity.

To generate the Conference Detail report, choose **Assurance Reports** > **Session Reports** > **Session Detail Report**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports** > **Conference Reports** > **Conference Detail Report**.

TelePresence Endpoint Reports

You can use TelePresence reports to view endpoint utilization, and no show endpoints summary.

For Cisco Prime Collaboration Release 12.1 SP2 and later

Prerequisites for Telepresence Endpoint Reports

The following are required for Telepresence Endpoint Reports:

- Unified CM and Cisco VCS must be in the Managed state.
- Endpoints and controllers, such as MCU must be in the Managed state.
- Ensure to set the visibility of the devices to “Full Visibility” state.
- JTAPI must be configured on Unified Communications Manager. For information on how to enable JTAPI on Unified Communications Manager, see the Configure Devices for Cisco Prime Collaboration Assurance.
- Cisco Prime Collaboration Assurance server must be registered as a feedback server in Cisco VCS.
- For Conference Diagnostics and Audio Phone Feature Synthetic Tests to work, ensure that CUCM is as per the listed version(s) before applying Cisco Prime Collaboration Assurance Service Pack 1 bundle. For more information, see Supported Devices for Cisco Prime Collaboration Assurance for 12.1 Service Pack 1.

The following reports can be generated for TelePresence endpoints:

Endpoint Utilization Report

The Endpoint Utilization report enables you to identify the most utilized and least utilized endpoints.

Average utilization of an endpoint is calculated using the following formula:

- For system-defined (1 day, 1 week, 4 weeks) reports:

  (Total number of utilization in minutes / [maximum utilization * 60]) * 100

- For custom reports:

  (Total number of utilization in minutes / [maximum utilization * 60 * number of days]) * 100

  - 1 day: The maximum utilization is ten hours.
  - 1 week: The maximum utilization is 50 hours.
  - 4 weeks: The maximum utilization is 200 hours.
  - Custom report: The maximum utilization is 7.14 hours per day.

It displays the utilized scheduled time in % which denotes the scheduled time utilization in percentage.

You can customize the endpoint utilization settings. To do so, select an endpoint model (endpoint(s) of a particular model) and then click the **Change Utilization** button. You can select the number of working hours in a day and the number of working days in a week.

To generate the Endpoint Utilization report, choose **Assurance Reports** > **Telepresence Endpoint Reports** > **Endpoints Utilization Report** .

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports** > **Telepresence Endpoint Reports** > **Endpoints Utilization Report**.

No Show Endpoint Summary Report

The No Show Endpoints Summary report provides information about the endpoints that did not participate in the scheduled conferences. This report is generated based on the scheduled completed conferences data.

To generate the No Show Endpoints Summary report, choose **Assurance Reports** > **Telepresence Endpoint Reports** > **No Show Endpoint Summary Report**.

For Cisco Prime Collaboration Release 11.5 and later

To generate the No Show Endpoints Summary report, choose **Reports** > **Telepresence Endpoint Reports** > **No Show Endpoint Summary Report**.

Launch CUCM Reports

Launch CUCM Reports enables you to cross launch to the reporting pages for the Cisco Unified Communications Manager clusters.

Go to **Launch CUCM Reports**, and click a cluster name to open the Cisco Unified Reporting application.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports** > **Launch CUCM Reports**.

Miscellaneous Reports

You can use Miscellaneous reports to view Other Reports, UCM/CME Phone Activity Reports, and Voice Call Quality Event History Reports.

UCM/CME Phone Activity Reports

UCM/CME Phone Activity reports provide information about the audio and video phones that have undergone a status change during the last 30 days.

If you have deployed Cisco Prime Collaboration Assurance in Enterprise mode, the Phone Activity reports display the domain name, except the Export Audio Phones report.

If you have deployed Cisco Prime Collaboration Assurance in MSP mode, the Phone Activity reports display the customer name, except the Export Audio Phones report.

The following Activity reports are available:

Endpoint Move Report

The **Endpoint Move** report displays the details of IP/Video endpoints that have been moved in the last 30 days. It also displays the Extension, Cisco Unified CM address, switch address, and switch ports used before and after the move.

The **Endpoint Move** report shows the time at which the IP/Video endpoint move was detected, and not the time at which the move occurred.

To generate the Endpoint Move report, choose **Reports** > **Miscellaneous Reports** > **Endpoint Move**.

Note **Endpoint Move** report is not supported for the video endpoints that do not support CDP.

Endpoint Audit Report

The Endpoint Audit Report shows the change that have occurred in the managed IP/Video endpoint network.

For example, this report shows you the IP/Video endpoint that have been added or deleted from your network, IP/Video endpoint status, and so on. Endpoint status changes occur, for instance, when an endpoint becomes unregistered with the Cisco Unified CM.

To generate the Endpoint Audit Report, choose **Reports** > **Miscellaneous Reports** > **UCM/CME Phone Activity Reports > Endpoint Audit**.

Note Endpoints appear as "Removed" in the Audit Report when they are unregistered in CUCM for more than 24 hours. For the record, endpoints that are deleted from CUCM while they are registered will first be shown as "Unregistered" in the Audit Report for the next 24 hours, and will be shown as "Removed" beyond that. Note that these will be deleted from Cisco Prime Collaboration Assurance Inventory after the first CDT discovery that happens after the deletion.

Endpoint Remove Report

The Endpoint Remove report lists endpoints that have been removed during the last 30 days.

To generate the Endpoint Remove report, choose **Reports** > **Miscellaneous Reports** > **Endpoint Remove Report**.

Endpoint Extension Report

The Endpoint Extension Report lists the endpoints for which extension numbers were changed during the last 30 days.

To generate the Endpoint Extension Report, choose **Reports** > **Miscellaneous Reports** > **Endpoint Extension Report**.

Note The Endpoint Extension Report is not supported for Cisco Wireless IP Phone 7920.

Understand the Time Period Covered by Audio IP Phone Activity Reports

For Cisco Prime Collaboration Release 11.1 and earlier

When you generate an Audio IP Phone or Video IP Phone Activity report, your results can be affected by the time zones in which each of following resides:

- Your client system—Cisco Prime Collaboration Assurance calculates the time period (previous 24 hours through previous 7 to 30 days, depending on the report) for Phone Activity reports based on the date and time on your client system.
- Prime Collaboration system—Cisco Prime Collaboration Assurance records some audits, such as extension number changes, based on the time that the change is detected on the Cisco Prime Collaboration system.
- Cisco Unified Communications Manager—Cisco Prime Collaboration Assurance records some audits, such as phone moves, based on the time on Cisco Unified CM that changes were detected.

If any of these systems is not in the same time zone as your system, you must take the time zone difference into account when you generate and view Phone Activity reports.

Note If the audit date and time on the Cisco Prime Collaboration Assurance system is inconsistent with those shown in the Audio IP Phone or Video IP Phone Audit report, make sure that all Cisco Unified CM in the network are set to synchronize.

Track Phone Status when Cisco Unified CM Is Down

For Cisco Prime Collaboration Release 11.1 and earlier

If a Cisco Unified CM that is configured with a backup goes down, audio and video IP phones fail over to the backup Cisco Unified CM.

Cisco Prime Collaboration Assurance stores audit records for the phones that register with the backup and these status changes are included in IP Phone and Video Phone Audit reports.

Cisco Prime Collaboration Assurance does not store audit records in the following cases:

- An entire Cisco Unified CM cluster goes down.

  A Cisco Unified CM for which a backup is not configured goes down.

Therefore, status changes for the phones registered to Cisco Unified CM in these situations are not included in Audio IP Phone Status and Video IP Phone Activity reports.

Voice Call Quality Event History Reports

You can search the Event History database for Voice Call Quality events based on:

- MOS
- Destination
- Codec
- Phone model

- Sensor(not applicable if you have installed Cisco Prime Collaboration Assurance in the MSP mode)
- Date
- Export

To generate Call Quality Event History report, choose **Assurance Reports** > **Miscellaneous Reports** > **Voice Call Quality Event History Reports**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports** > **Miscellaneous Reports** > **Voice Call Quality Event History Reports**.

The Voice Call Quality Event History report is a scrollable table that lists up to 2,000 records, based on your search criteria.

To view database contents beyond 2,000 records, choose **Assurance Reports** > **Miscellaneous Reports** > **Voice Call Quality Event History Reports** > **Export**, click Export . If more than 1,000 records match your search criteria, a popup window reports the total number of matching records found.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports** > **Miscellaneous Reports** > **Voice Call Quality Event History Reports** > **Export**.

When you export Voice Call Quality Event History Reports In Internet Explorer browser, the **Windows Security** popup window may prompt for your credentials. The report is downloaded even if you cancel the **Windows Security** popup window.

For the Save at field, enter a location for storing the reports on the server where Cisco Prime Collaboration Assurance is installed; the default location is /opt/emms/cuom/ServiceQualityReports.

Note If you configure export settings to save files outside of default location, be sure to log into the Cisco Prime Collaboration Assurance server, create the folder that you entered on the Export Settings page, and provide write permission to the folder for the user. If you do not perform these tasks, Cisco Prime Collaboration Assurance cannot create the export files.

For the E-mail to field, enter one or more complete e-mail addresses separated by commas.

To download the report, click **Download Report**.

If you have deployed Cisco Prime Collaboration Assurance in the Enterprise mode, the Call Quality Event History reports can be viewed for a specific domain selected from the global selector (drop-down). However, when you export the report, using the export option, the reports are not filtered based on the domain selected from the global selector.

If you have deployed Cisco Prime Collaboration Assurance in the MSP mode, the Call Quality Event History reports contain customer details such as, customer name. The reports can be viewed for a specific customer selected from the global selector (drop-down). However, when you export the report, using the export option, the reports are not filtered based on the customer selected from the global selector. Also, in this mode, you cannot search the Event History database for Voice Call Quality events based on Sensor.

Other Reports

Other reports provide information about CTI applications, Cisco Analog Telephone Adaptor (ATA) devices, and Cisco 1040 sensors if you have deployed Cisco Prime Collaboration Assurance in Enterprise mode.

Note If you have deployed Cisco Prime Collaboration Assurance in MSP mode, you cannot generate reports for Cisco 1040 sensors.

To generate these reports, choose **Assurance Reports** > **Miscellaneous Reports** > **Other Reports** and select a report.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports** > **Miscellaneous Reports** > **Other Reports**.

CTI Applications Report

The CTI Applications report lists CTI applications that are registered with Cisco Unified CM.

The following applications are registered to Cisco Unified CM as CTI devices or CTI ports:

- Cisco Personal Assistant
- Cisco Customer Response Applications
- Cisco IP Contact Center
- Cisco Emergency Responder

ATA Devices Report

The ATA Devices report provides information about the ATA devices that are registered with Cisco Unified CM.

Cisco 1040 Sensors Report

The Cisco 1040 Sensors report provides information about Cisco 1040 sensors that are deployed in your network. Before you generate Cisco 1040 Sensors Report, see prerequisites in Prerequisites to Generate the Cisco Prime Collaboration Assurance Reports.

Note This report is not applicable if you have installed Prime collaboration in MSP mode.

When a web interface is accessible for an IP phone, you can open it from Cisco 1040 sensor report by clicking the hyperlink for one of the following:

- Extension number
- MAC address
- IP address

Conferencing Device Video Port Utilization Report

This report is generated based on the hourly utilization of conferencing devices.

Average Utilization

- 1 day: Average utilization of hour 1 + hour 2 + ... + hour 24) / 24.
- 1 week: Average hourly utilization of each hour in the week is aggregated and divided by (7 x 24).
- 4 weeks: Average hourly utilization of each hour in the 4 weeks is aggregated and divided by (7 x 24 x 4).
- Custom period: Average hourly utilization of each hour in the custom period is aggregated and divided by (24 x number of days in custom period).

Note The utilization is shown as 100% even if the utilization is more than 100%.

Peak Utilization

- 1 day: The peak utilization is analyzed from individual peak values of each of the 24 hours.
- 1 week: The peak utilization is analyzed from individual peak values of each of the 7*24 hours.
- 4 weeks: The peak utilization is analyzed from individual peak values of each of the 7*24*4 hours.
- Custom periods: The peak utilization is analyzed from individual peak values of each hour in the custom period.

To generate the Conferencing Device Utilization report, choose **Assurance Reports** > **Miscellaneous Reports** > **Other Reports** > **Conferencing Device Utilization Report**.

For Cisco Prime Collaboration Release 11.5 and later

Choose **Reports** > **Miscellaneous Reports** > **Other Reports** > **Conferencing Device Utilization Report**.

Click the value of the Average Utilization or Peak Utilization columns to launch the Detailed Video Port Utilization graph. You can choose to view Hourly Average Utilization, Peak Utilization, or actual data (click **All**). You can also use the slider and select a small time interval also (such as a minute) to view actual data for that interval.

Scheduled Reports

Scheduled reports are utilization and inventory reports that you can schedule from the Report Launch Pad. You can generate them according to your scheduling preferences, and download or send them to the configured e-mail ID. These reports can be exported in both CSV and PDF format (except the Conference Detail Report, which can be exported only in CSV format). The data for these reports will be available for 30 days only.

These reports are not enabled by default. You can generate the reports on the spot or enable scheduling to generate them on predefined days.

Choose **Reports** -> **Scheduled Reports** -> **Reports**

The following scheduled reports are available:

Report Title	Description
Utilization Reports (Under Reports selector, select Utilization > Endpoint, and Endpoint No Show to see the Monthly Utilization and Monthly No Show Reports.)	
Monthly Utilization Report	Provides aggregate monthly reports on the utilization of the endpoints. The aggregate value is calculated by *Total utilization for all months* / 12.
Monthly No Show Report	Provides aggregate monthly reports on the nonparticipation of endpoints in scheduled conferences. The average aggregate value is calculated by *Total no show for all months* / 12.
Conference Detail Report	Provides details on the conference statistics for all completed conferences.
Inventory Reports	
Managed Devices Report	Provides information about managed devices. If a device is unknown, only the IP address is displayed. Use this report to find devices for which credentials have been updated.
Unmanaged Devices Report	Provides information about unmanaged devices. Use this report to identify devices for which credentials need to be updated.
Endpoints	Provides information on the endpoints as displayed in the Endpoints Diagnostic page. For more information, see the Endpoint Diagnostics Dashboard section. **Note** The description on Cisco Unified Communications Manager (Call Manager) is mapped with the Endpoint Name column in Endpoint Report. The association of **Endpoint Name** and **User Name** columns helps in identifying the unique Cisco Jabber or Client Services Framework (CSF) devices.
For Cisco Prime Collaboration Release 12.1 SP3 and later Endpoint(s) Reports (Under Reports selector, select **Inventory** -> **Endpoints** to view the following schedule reports: Endpoints Audit, Endpoints Move, Endpoints Remove, and Endpoints Extension Audit.)	

Report Title	Description
	For Cisco Prime Collaboration Release 12.1 SP3 and later You can schedule Endpoints Audit, Endpoints Move, Endpoints Remove, and Endpoints Extension Audit reports and send the generated reports through email notification to the specified email ID. The generated report must list the details of last 1 day. If you have deployed Cisco Prime Collaboration Assurance in MSP Mode, **Customer** name column should be listed.
Event History Reports	
All Events	Provides history of all the events that occurred in last one day, one week, or one month.

Note Scheduled Utilization reports (Monthly Utilization, Monthly No Show, and Conference Detail reports) are applicable for both video phones and TelePresence endpoints. Endpoint details will be populated in these reports based on the license that you purchased.

Generate Scheduled Reports

You can define the reporting period, the report generation date, and the frequency according to your preferences.

To generate a scheduled report:

Step 1 Select a report from the Reports pane.

Step 2 Click the Settings tab under the Report Details pane, and click Enable Scheduling.

Step 3 Schedule the report generation using options in the Scheduler and Settings pane.

Step 4 Do either of the following:

- Click **Save**.
- Generate the report on the spot:
  - Click **Run Now** (adjacent to the report you want to generate).
  - Click the Run History tab under the Report Details pane.
  - Download the report.

To create a customized scheduled report, select a report from the Reports quick display in the left corner only, and click New under the Reports pane. Enter the required information and click Submit. Instances of the run

report are queued as jobs under the Job Management page. You can manage and monitor these jobs from the Job Management page (**System Administration** > **Job Management**).

Access Data for Reports that Contain More than 2,000 Records

Cisco Prime Collaboration Assurance reports display up to 2,000 records. If more than 2,000 records are returned when you generate a report, Cisco Prime Collaboration Assurance displays an informational message before displaying the report.

In this case, you can:

- Enter more specific filters to generate a report with fewer records.
- Export the report data to a CSV file to access the additional records. To open the export window, click the Export icon in the top right of the report window. You can export up to 30,000 records to a CSV file.

Note If your client system seems unresponsive when you try to export files, see Troubleshoot File Download Issues.

Troubleshoot File Download Issues

If you try to export a report or other data to a file from Cisco Prime Collaboration Assurance and either the export dialog box or the window that prompts you to save the export file does not appear, use these procedures to try to fix the problem.

Procedure

	Command or Action	Purpose
Step 1	If you set the custom levels of security in Internet Explorer to medium or greater, the option, Automatic prompt to file download, is disabled. If you try to download a PDF or CSV file to a client system where Adobe Acrobat Reader or Microsoft Excel not installed, nothing happens. The PDF file or the spreadsheet is not displayed nor is a window that prompts you to save the file. To enable file download windows to display, do this on your desktop:	
Step 2	If you are using Internet Explorer, Automatic prompt to file download is enabled, and the window that prompts you to save the file still does not appear, do this:	