CHAPTER 16

Using History Reports

These topics explain how to use Cisco Prime Unified Operations Manager (Cisco Prime UOM) Event History and Service Quality History reports:

Getting Started with History Reports

Event History reports and Service Quality History reports enable you to view events that occurred during the past. The available information includes event status and date, related device and device components, annotations (informational text you entered), and event details.

Depending on the criteria you use to generate the report, the Event History reports can display information for both devices and clusters. Cisco Prime UOM purges the Event History database daily to retain only 31 days of history; see Viewing Purge Scheduler Status, page 20-13.

Service Quality History requires statistics collected by Cisco Unified Service Monitor (Service Monitor). Service Monitor is available as part of the Cisco Unified Communications Management Suite product bundles and is also available as a stand-alone application. For more information, see the *User Guide for Cisco Unified Service Monitor* or contact your Cisco sales representative.

This section contains:

Event History Report Tool Buttons

Table 16-1 explains the tool buttons that appear in the upper-right corner of history reports.

Table 16-1 Event History Report Window Tool Buttons

Icon	Meaning
	Exports the current report to a CSV file. **Note** The PDF export option is not available from Event and Service Quality event history reports.
	Opens a printer-friendly version for printing.
	Opens context-sensitive help.

Reports with More than 2,000 Records

The Event History reports display up to 2,000 records that you can scroll or page through. If your report exceeds 2,000 records and you want to view all of them, use the Export tool button to save all of the information to a CSV file.

Getting Started with Event History

You can generate 24-hour context-based reports from various Cisco Prime UOM pages, such as the Topology display. You can also generate customized history reports for which you supply the search criteria and set the date range. You can generate Event History reports for devices, device components, and clusters. You can also export 24-hour and 7-day reports automatically.

The following problem exists in Event History displays:

When over 5,000 events are generated in the network at a time, some events are dropped by Event History. This occurs when Event History processes up to 5,000 events during a burst of more than 5,000 events.

To resolve this, view the events in the Events display. These events are processed by the system and displayed in this display. Note that if the events get cleared they are not displayed on the Events History display after 30 to 60 minutes.

24-Hour Context-Based Event History Reports

On various Cisco Prime UOM pages, such as the Events History display, you can select Event History links or menu items. When you click an Event History link, you generate a *context-based* report that displays relevant history records:

- For which you do not need to enter search criteria.
- For the past 24 hours.

You can also generate customized Event History reports for a time period that you select and include records based on search criteria that you specify. Event History reports include the same type of information whether you generate context-based or customized reports.

You can generate 24-hour context-based history reports from various Cisco Prime UOM pages. For example, from:

- Fault Monitor—You can launch an Event History report via the Device Details.
- Service Level View—You can launch an Event History report for a device or cluster.
- Device Details View
- **Reports > Service Quality Events**

Customized Event History Reports

You might want to generate an Event History report when:

- A significant event is shown in an events display, and you want to see how often the event has been generated in the last month.
- You receive an e-mail notification that an unusual event has occurred.
- You want to search for information on events other than those you are tracking in your customized events display.

You can generate an Event History report to gather information on:

- All events.
- Events that occurred on components of a device.
- Occurrences of the same event on different devices.
- Clusters (which can be selected under device groups).
- Recommended actions to take on event issues.

Exporting 24-Hour and 7-Day Event History Reports

Use this procedure to automatically generate 24-hour Event History reports daily at midnight and 7-day Event History reports weekly at midnight on Monday. You can generate these reports in comma-separated value (CSV) format, save them on disk, and e-mail them.

Step 1 Select **Reports > Event History > Export**.

The automatically Export Event Reports page appears.

Step 2 For each report that you want to generate, select CSV to save the report as a comma-separated-values file.

Reports that you can generate are:

- All events for the last 24 hours—24-hour reports are named EventReports_Daily_ddmmyyyy.filetype, for example EventReports_Daily_20Apr2006.csv
- All events for the last 7 days—7-day reports are named EventReports_Weekly_ddmmyyyy.filetype, for example EventReports_Weekly_17Apr2006.csv. 7-day reports run weekly on Monday at midnight.

Step 3 Enter one or more locations to store or send the report:

- If you want to store the reports on disk, enter (or browse to and select) a location on the server.

Casuser and administrator have write permissions in the default directory. If you change the directory, make sure that the directory has write permission for casuser. If you do not, the export files will not be created.

- If you want to e-mail the reports, enter a fully qualified e-mail address.

Step 4 Click **Apply**.

Generating Customized Event History Reports

To gather historical information on events in the past 31 days, start Event History from the Cisco Prime UOM home page by selecting **Reports > Event History**. The following topics explain how you can apply filters and generate reports based on all information stored in the Event History database:

- To search for events on devices by event ID, device, or group, see Getting All Stored Information on an Event, page 16-4.
- To search for Service Quality events on Cisco 1040s, call endpoints, or phone models, see Getting All Stored Information on a Service Quality Event, page 16-11.

Service Quality History reports are available only if you have purchased a license for Service Monitor.

Getting All Stored Information on an Event

For information about Service Quality events, see Getting All Stored Information on a Service Quality Event, page 16-11.

You can search the Event History database for events using one of the following methods:

- Searching for Events by Event ID, page 16-5
- Searching for Events by Device, page 16-5
- Viewing Specific Events, page 16-6
- Searching for Events by Device Group, page 16-7
- Searching for Events by Date, page 16-7

Alternatively, to generate a 24-hour report of all events on a device component, click the Event History link on the Device Detail page. See Viewing Device Details, page 8-37.

Searching for Events by Event ID

To determine how often a specific event has occurred, search for the event by its event ID. The event ID is displayed on the Device Details display.

To Search for events by event ID:

Step 1 :Select **Reports > Event History > Event**.

The Event History: Search by Event ID page appears.

Step 2 Set your search criteria:

a. Enter the event ID.

b. Select the date range:

- Today.
- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**.

If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Event History report opens. This report contains information on both devices and clusters. For an explanation of the report contents, see Understanding the Event History Report, page 16-8.

Searching for Events by Device

To determine the types of events that occur on a specific device:

Step 1 Select **Reports > Event History > Devices**.

The Event History Search by Device page appears.

Step 2 Set your search criteria:

a. Enter a comma-separated list of devices (as they are listed by Device Management). You can select multiple devices from different groups.

b. Enter the event description by clicking the popup selector box and selecting the events for which you want to search. By default, all events are selected. (See Selecting Event Descriptions for an Event History Report, page 16-6.)

c. Select the date range:

- Today.
- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**.

If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Event History report opens. This report contains information on devices only. For an explanation of the report contents, see Understanding the Event History Report, page 16-8.

Selecting Event Descriptions for an Event History Report

By default all events are selected on the Event Descriptions dialog box.

Note The Event Description filter window under **Reports > Event History > Event History > Device Groups** displays user-defined event names. When the event report is launched, the customized name will be displayed.
To determine the default name for customized events, go to **Administration > System Settings > Event Customization**.

To determine which event descriptions to display:

Step 1 In the Event Descriptions dialog box, deselect events that you do not want to include in the Event History report.

When you deselect an event, if checked, the All check box at the top of the dialog box is also deselected.

Step 2 Do one of the following:

- Click **Select** at the top or bottom of the dialog box to finalize your selections.
- Select **Cancel** at the top or bottom of the dialog box to cancel your selections and return to the default list of all events.

Viewing Specific Events

To view a specific event:

Step 1 Select **Reports > Event History > Event**.

The Event History: Search by Event ID page appears.

Step 2 Set your search criteria:

a. Enter the Event ID.

b. (Optional) Enter the event description by clicking the popup selector box and selecting the events for which you want to search. (See Selecting Event Descriptions for an Event History Report, page 16-6.)

c. Select the date range:

- Today.
- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**.

If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Event History report opens. This report contains information on both devices and clusters. For an explanation of the report contents, see Understanding the Event History Report, page 16-8.

Searching for Events by Device Group

To determine what types of events are occurring in a specific device group:

Step 1 Select **Reports > Event History > Device Groups**.

The Event History: Search by Device Group page appears.

Step 2 Set your search criteria:

a. Select one or more device groups.

b. Enter the event description by clicking the popup selector box and selecting the events for which you want to search.

c. Select all event severity levels that you want to search for.

d. Select the date range:

- Today.
- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**.

If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Event History report opens. This report contains information on devices only. For an explanation of the report contents, see Understanding the Event History Report, page 16-8.

Searching for Events by Date

To determine what type of events are occurring during a specific day, week, month, or range of dates:

Step 1 Select **Reports > Event History > Event History > Date**.

The Event History Search by Date page appears.

Step 2 Select the date range and enter:

- Today.
- 7 days.
- One Month.
- From*: a date* and to: *a date*—Enter or select dates.

Step 3 Click **View**.

If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Event History report opens. This report contains information on both devices and clusters. For an explanation of the report contents, see Understanding the Event History Report, page 16-8.

For more information, see the following topics:

- Getting Started with Event History, page 16-2
- Event History Report Tool Buttons, page 16-1
- Viewing Event Properties from an Event History Report, page 16-10
- Events Processed, page E-1

Understanding the Event History Report

The Event History report (shown in Figure 16-1) is a scrollable table that lists up to 2,000 records, based on your search criteria. To view database contents beyond the 2,000 records, click the Export tool button in the upper-right corner of the window.

When using the Events History display, remember the following:

- If a monitored device is removed from the network, it will continue to be in the Monitored state until the next inventory collection occurs, even though the device is unreachable. The only way that you will know that this device is unreachable, is when an unreachable event appears for this device in the Events display.
- When a device becomes unresponsive, all existing events for that device become cleared and one unresponsive event is generated for the device.

This section contains:

- Viewing User Annotations from an Event History Report, page 16-10
- Viewing Event Properties from an Event History Report, page 16-10

Note Service Quality events are reported on Service Quality History reports. See Understanding the Service Quality History Report, page 16-14.

Figure 16-1 Event History Report

	Severity	Event ID	Device Name	Component Name	Event Name	Last Updated Time	Status
1	Critical	00002A6	cm7-pub.cisco.com	PROC-cm7-pub.cisco.com/_Total	CPUPegging	21-Jul-2010 04:06:29	Active
2	Critical	00002A5	blrsd3.cisco.com	blrsd3.cisco.com	PerformancePollingStopped	21-Jul-2010 04:05:53	Cleared
3	Critical	00002A4	cm7-pub.cisco.com	PROC-cm7-pub.cisco.com/_Total	CPUPegging	21-Jul-2010 04:03:27	Cleared
4	Critical	00002A3	cm7-pub.cisco.com	PROC-cm7-pub.cisco.com/_Total	CPUPegging	21-Jul-2010 04:02:26	Active
5	Critical	00002A2	blrsd3.cisco.com	blrsd3.cisco.com	PerformancePollingStopped	21-Jul-2010 04:02:00	Active
6	Critical	00002A1	10.64.95.162	IF-10.64.95.162/65539 [HP NC324i PCIe Dual Port Gigabit Server Adapter #2]	OperationallyDown	21-Jul-2010 03:56:24	Cleared
7	Critical	00002A0	cm7-pub.cisco.com	PROC-cm7-pub.cisco.com/_Total	CPUPegging	21-Jul-2010 03:51:17	Cleared
8	Critical	000029Z	cm7-pub.cisco.com	PROC-cm7-pub.cisco.com/_Total	CPUPegging	21-Jul-2010 03:50:16	Active
9	Informational	000029Y	VE-cm612-cluster	VE-cm612-cluster	RTMTDataMissing	21-Jul-2010 03:49:07	Active
10	Critical	000029X	blrsd3.cisco.com	blrsd3.cisco.com	PerformancePollingStopped	21-Jul-2010 03:48:03	Cleared

The Event History report window provides tools, as shown in Table 16-1.

Table 16-2 describes the contents of the Event History report.

Table 16-2 Event History Report—Contents

Heading	Description
Severity	Critical, Warning, or Informational.
Event ID	Event identifier number. Clicking this link opens an event properties window (see Figure 16-2 on page 16-10), which contains details about the events.
Device Name	Device name or IP address.
Component Name	Device type. Inventory Collection in Progress indicates that Cisco Prime UOM was discovering the device or cluster at the time of the event. The actual device type is reflected when new events occur. The device type is displayed as N/A during inventory collection. For more information, see Chapter 8, "Using Device Management."
Event Name	Event name.
Last Updated Time	Date and time when the event was generated.
Status	Event status, based on last polling.
	Active—Event is live.
	Cleared—Event is no longer live. Also, when a device is suspended, all events are cleared. When Cisco Prime UOM polling determines that an alarm has been in the Cleared state for 30 minutes or more (from the time of polling), the alarm expires and is removed from the events display.
	Suspended—Device is suspended.
	Resumed—Device is resumed.
	Deleted—Device has been deleted.

Viewing User Annotations from an Event History Report

From an Event History report, click a link in the Status column to open the event annotation page.

The event annotation page, which lists any notes that users have entered, displays. (For more information, see Getting Device and Event Details, page 4-22.) If no annotation is present, a message appears that no annotation is available.

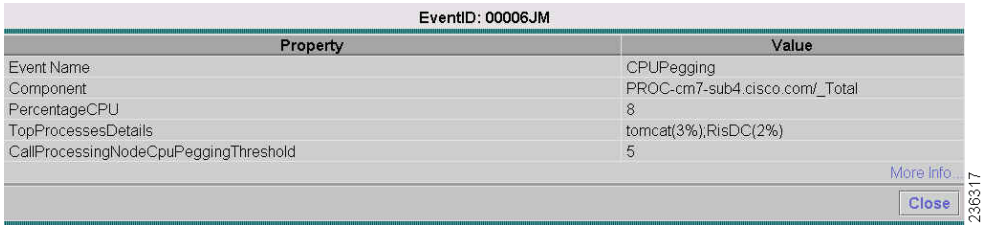
Viewing Event Properties from an Event History Report

From an Event History report, click an event in the Event ID column to open the Event Properties page. The page lists more information about an event, such as the value of MIB attributes, polling and threshold information, and utilization information.

Values at the time of the event are listed alongside current values. For additional event details including recommended actions to resolve the issue, click on the **More Info** button to see the online help.

Figure 16-2 shows an example of the event properties page.

Figure 16-2 Event Properties Page



Getting Started with Service Quality History Reports

This section contains the following topics:

- Exporting 24-Hour and 7-Day Service Quality History Reports, page 16-10
- Getting All Stored Information on a Service Quality Event, page 16-11

Exporting 24-Hour and 7-Day Service Quality History Reports

Use this procedure to automatically generate 24-hour Service Quality History reports daily at midnight and 7-day Service Quality History reports weekly at midnight on Monday. You can generate these reports in comma-separated value (CSV) format, save them on disk, and e-mail them.

Step 1 Select **Reports > Service Quality History > Event History > Export**.

The automatically Export Service Quality Reports page appears.

Step 2 Select one or more reports and report formats:

- All issues for the last 24 hours—Select one or more check boxes to generate and save a 24-hour Service Quality History report as CSV (a comma-separated-values file).

24-hour reports are named ServiceQualityReports_Daily_ddmmyyyy.filetype, for example ServiceQualityReports_Daily_20Apr2006.csv.

- All issues for the last 7 days—Select one or more check boxes to generate and save a 7-day Service Quality History report as CSV.

  7-day reports are named ServiceQualityReports_Weekly_ddmmyyyy.filetype, for example ServiceQualityReports_Weekly_20Apr2006.csv. 7-day reports run weekly on Monday at midnight.

Step 3 Enter one or more locations to store or send the report:

- If you want to store the reports on disk, enter (or browse to and select) a location on the server.

  Casuser and administrator have write permissions in the default directory. If you change the directory, make sure that the directory has write permission for casuser. If you do not, the export files will not be created.

- If you want to e-mail the reports, enter a fully qualified e-mail address.

Step 4 Click **Apply**. The reports will be generated daily at midnight.

Getting All Stored Information on a Service Quality Event

Service Quality History requires statistics collected by Cisco Unified Service Monitor (Service Monitor). Service Monitor is available as part of the Cisco Unified Communications Management Suite product bundles and is also available as a stand alone application.

For more information, see the *User Guide for Cisco Unified Service Monitor* or contact your Cisco Sales Representative.

You can search the Event History database for Service Quality events using one of the following methods:

- Searching for Service Quality Events by MOS, page 16-11
- Searching for Service Quality Events by Destination, page 16-12
- Searching for Service Quality Events by Codec, page 16-12
- Searching for Service Quality Events by Phone Model, page 16-13
- Searching for Service Quality Events by Cisco 1040, page 16-13
- Searching for Service Quality Events by Date, page 16-14

Searching for Service Quality Events by MOS

To view the Service Quality events for MOS less than a value that you supply:

Step 1 Select **Reports > Service Quality History > Event History > MOS**.

The Service Quality History: Search by MOS page appears.

Step 2 Set your search criteria:

a. MOS less than—Enter the lowest value. The range of MOS values is .1 to 4.9.

b. Select the date range:

- Today.
- One Month (from *date* to *date*).

- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**.

If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Service Quality History report opens. For an explanation of the report contents, see Understanding the Service Quality History Report, page 16-14.

Searching for Service Quality Events by Destination

To view the Service Quality events that correspond to call endpoints:

Step 1 Select **Reports > Service Quality History > Event History > Destination**.

The Service Quality History: Search by Destination page appears.

Step 2 Set your search criteria:

a. Select an operator:

- Is exactly
- Begins with
- Contains

b. Enter the destination—IP address for a phone, voice gateway, or Cisco 1040.

c. Select the date range:

- Today.
- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**.

If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Service Quality History report opens. For an explanation of the report contents, see Understanding the Service Quality History Report, page 16-14.

Searching for Service Quality Events by Codec

To view the Service Quality events for a particular codec:

Step 1 Select **Reports > Service Quality History > Event History > Codec**.

The Service Quality History: Search by Codec page appears.

Step 2 Set your search criteria:

a. Select a codec from the list.

b. Select the date range:

- Today.

- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**.

If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Service Quality History report opens. For an explanation of the report contents, see Understanding the Service Quality History Report, page 16-14.

Searching for Service Quality Events by Phone Model

To view the Service Quality events that correspond to specific phone models:

Step 1 Select **Reports > Service Quality History > Event History > Phone Model**.

Step 2 The Service Quality History: Search by Phone Model(s) page appears.

Step 3 Set your search criteria:

a. Click the popup selector box and select the phone models for which you want to search.

b. Select the date range:

- Today.
- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 4 Click **View**.

If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Service Quality History report opens. For an explanation of the report contents, see Understanding the Service Quality History Report, page 16-14.

Searching for Service Quality Events by Cisco 1040

To view the Service Quality events that correspond to specific Cisco 1040:

Step 1 Select **Reports > Service Quality History > Event History > Cisco 1040**.

The Service Quality History: Search by Cisco 1040 page appears.

Step 2 Set your search criteria:

a. Select an operator (Is exactly, Begins with, Contains) and enter a Cisco 1040 ID or portion of a Cisco 1040 ID.

Cisco 1040 IDs include a letter and a 3-digit number.

b. Select the date range:

- Today.

- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**.

If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Service Quality History report opens. For an explanation of the report contents, see Understanding the Service Quality History Report, page 16-14.

Searching for Service Quality Events by Date

To view the Service Quality events for specific dates:

Step 1 Select **Reports > Service Quality History > Event History > Date**.

The Service Quality History: Search by Date page appears.

Step 2 Select one and enter dates if required:

- Today.
- 7 days
- 1 month.
- From*: a date* and to: *a date*—Enter dates.

Step 3 Click **View**.

If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Service Quality History report opens. For an explanation of the report contents, see Understanding the Service Quality History Report, page 16-14.

For more information, see the following topics:

Events Processed, page E-1

Understanding the Service Quality History Report

Service Quality History requires statistics collected by Cisco Unified Service Monitor (Service Monitor). Service Monitor is available as part of the Cisco Unified Communications Management Suite product bundles and is also available as a stand alone application.

For more information, see the *User Guide for Cisco Unified Service Monitor* or contact your Cisco Sales Representative.

The Service Quality History report is a scrollable table that lists up to 2,000 records, based on your search criteria. To view database contents beyond the 2,000 records, click the Export tool button in the upper-right corner of the window.

The Service Quality History report window provides tools, as shown in Table 16-1.

Table 16-3 describes the contents of the Service Quality History report.

Table 16-3 Service Quality History Report—Contents

Heading	Description
Severity	Event severity: • Warning—MOS is below the MOS threshold configured on Service Monitor. For more information, see *User Guide for Cisco Unified Service Monitor*. • Critical—MOS is below the MOS threshold configured on Cisco Prime UOM.
Event ID	Click this link to open the event properties window. See Viewing Service Quality Event Properties, page 16-16.
Destination Type	One of the following: • Endpoint • IP Phone
Destination	IP address or phone extension.
IP Address	Destination IP address.
MOS	Mean Opinion Score that triggered the event.
Cause	One of the following: • Jitter • Latency
Time	Date and time that the event occurred.
Codec	One of the following: • G711Alaw64k • G711Alaw56k • G711Ulaw64k • G711Ulaw56k • G722 64k • G722 56k • G722 48k • G728 • G729 • G729AnnexA • G729AnnexB • G729AnnexAwAnnexB
Source Type	One of the following: • Endpoint • IP Phone
Source	IP address or phone extension.

Table 16-3 Service Quality History Report—Contents (continued)

Heading	Description
IP Address	Source IP address.
Customer	Customer name entered during multiple end-customer's device add procedure.

Viewing Service Quality Event Properties

Click an event ID link on the Service Quality History report to view properties of the event. See Understanding the Service Quality History Report, page 16-14.

Table 16-4 describes the contents of the service quality Event Properties window.

Table 16-4 Service Quality Event Properties Window—Contents

Heading	Description
Destination	Extension number, or N/A if destination type is Endpoint
Destination IP Address	IP address for an endpoint or an IP phone
Destination Type	One of the following: • Endpoint • IP Phone • Media Server
Destination Model	Phone model, or N/A if destination type is Endpoint
Switch for Destination	IP address, or N/A if destination type is Endpoint
Destination Port	Port type and slot; for example Gi1/0/23
Source	Extension number or IP address
Source IP Address	IP address, or N/A if destination type is Endpoint
Source Type	One of the following: • IP Phone • Endpoint
Source Model	Phone model, or N/A if source type is Endpoint
Switch for Source	IP address, or N/A if source type is Endpoint
Source Port	Port type and slot, or N/A if source type is Endpoint
Detection Algorithm	Algorithm used to calculate MOS. One of these: • ITU G.107 - 1040 Sensor based voice quality Indicates that MOS is calculated on a Cisco 1040 Sensor • CVTQ - Phone based voice quality Indicates that MOS is calculated on an IP phone or Cisco voice gateway using the Cisco Voice Transmission Quality algorithm

Table 16-4 Service Quality Event Properties Window—Contents (continued)

Heading	Description
MOS	MOS value during event
Critical MOS Threshold	MOS threshold configured on Cisco Prime UOM.
Cause	One of the following: • Jitter • Latency • Packet Loss
Codec	Codec in use on the destination; one of the following: • G711Alaw64k • G711Alaw56k • G711Ulaw64k • G711Ulaw56k • G722 64k • G722 56k • G722 48k • G728 • G729 • G729AnnexA • G729AnnexB • G729AnnexAwAnnexB
Jitter	Msec
Packet loss	Number of packets
Customer	Customer name.
Details for Events that Are Based on Data from a Sensor	
Sensor MAC	Sensor MAC—Sensor MAC address
Number of suppressed traps	Number of traps that Cisco Unified Service Monitor suppressed between the suppression start time and suppression end time For a given endpoint, Service Monitor sends a trap every *n* (a configurable number) minutes, and additional traps during that time are suppressed (not sent). For more information, see *User Guide for Cisco Unified Service Monitor*.
Suppression start time	Date and time that Service Monitor started to suppress traps for this endpoint
Suppression end time	Date and time that Service Monitor stopped suppressing traps for this endpoint
Details for Events that Are Based on Data from a Cluster	
CVTQ version	Version of CVTQ algorithm used to calculate MOS
Cluster ID	Cisco Unified Communications Manager cluster ID

Table 16-4 Service Quality Event Properties Window—Contents (continued)

Heading	Description
Cumulative Concealment Ratio	Total number of concealment frames divided by the total number of speech frames received from the start of the voice stream
Interval Concealment Ratio	Ratio of concealment frames to speech frames in the preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max Incremental Concealment Ratio	Highest interval concealment ratio from start of the voice stream
Concealment Seconds	Number of seconds during which concealment events (lost frames) occurred since the start of the voice stream (includes severely concealed seconds)
Severely Concealed Seconds	Total number of seconds with more than 5 percent concealment frames
Call duration	Hours, minutes, and seconds, formatted as *n*h *n*m *n*s. For example, a 123-second call would be displayed as 2m 3s.
MOS during last 8 secs	MOS value during the last 8 seconds of the call
Min MOS during call	Minimum MOS value during the call
Max MOS during call	Maximum MOS value during the call