CHAPTER 6

# Monitoring Service Quality Events and Alerts

Cisco Prime UOM generates events based on SNMP traps sent by Cisco Unified Service Monitor (Service Monitor). To view the Service Quality events in Cisco Prime UOM, you must have a licensed copy of Service Monitor configured to send traps to Cisco Prime UOM and Service Monitor must be added to Cisco Prime UOM.

You can use Fault Monitor, Diagnostic Views, or the Service Quality History Report to view Service Quality event information.

You can also view Service Quality alerts using **Administration > System Settings > Miscellaneous > Service Quality Alerts**.

These topics describe monitoring service quality events and alerts:



## How to View Service Quality Events

Service quality event information can be viewed in various portlets and reports. The following applications, portlets and reports contain service quality event data:

- Fault Monitor
- Device Pool Phone Registration Status
- Service Quality Event History Report

When Cisco Prime UOM receives traps from Service Monitor, Cisco Prime UOM generates an event. The events are shown in any of the Cisco Prime UOM that display service quality data. Service quality events, enables you to view the following windows:

- Service quality history—Reports service quality events generated during the previous 24 hours.
- Fault Monitor—Reports real-time events.
- Service Quality Events Display—Reports real-time service quality events.
- Service Quality Alerts—Displays the Service Quality Alerts display.

Service Quality History reports provide information from the past 24 hours. To generate a Service Quality History report on time spans beyond the last 24 hours, use Service Quality History from the Reports tab by selecting **Reports > Service Quality History**. For more information, see Getting All Stored Information on a Service Quality Event, page 16-11.

To view service quality events, use Fault Monitor. To access the Service Quality Alerts Display, select **Administration > System Settings > Miscellaneous > Service Quality Alerts**. For more details about viewing service quality events in Fault Monitor, see How Events are Handled, page 4-21.

This section contains:



# Viewing Service Quality Events

To view Service Quality event details, you can choose any of the following:

*Table 6-1 Viewing Service Quality Events in Cisco Prime UOM*

| Task | Select |
|---|---|
| Use Fault Monitor to view SQ events | Using Fault Monitor, page 4-1 |
| Use Diagnostics portlets to view SQ events | Viewing Service Quality Events from the Diagnostics Portal, page 6-2 |

To access the Service Quality Alerts Display, select **Administration > System Settings > Miscellaneous > Service Quality Alerts**.

There may be unexpected results in Service Quality event reports if unsupported special characters appear in fields in these displays or reports. See Supported Special Characters List, page 1-25 for details on what characters are supported in Cisco Prime UOM.

## Viewing Service Quality Events from the Diagnostics Portal

To access the Service Quality events from the Diagnostics tab:

**Step 1** Select the **Diagnostics** tab.

**Step 2** Scroll down the Unified Dashboard to view either of the SQ event portlets:

- UCM Cluster Device Pool Summary, page 3-23
- UC Phone Service Quality (SQ) Event Summary, page 3-34

If the portlets are not visible, you can add them to the dashboard using the Add Portlet icon.

# Understanding the Layout of the Service Quality Event Details Display

These topics provide details about the information in the Service Quality Event Details display.


- Tabular Display Pane, page 6-3
- Window Tools Area, page 6-3


### Tabular Display Pane

The tabular display pane is the core of the Service Quality events display. It contains a list of events that occur on the devices in your current view. This pane is refreshed every 60 seconds. For an explanation for all of the items in the tabular display, see Using the Service Quality Events Display, page 6-3.

Icons alert you to what needs attention. For example, the severity icons indicate which views and events require attention. The tabular display pane is scrollable and can display up to 1,000 records.

### Window Tools Area

The top-right corner of the Service Quality events display contains available tools buttons. All buttons are described in Table 6-2.

*Table 6-2 Service Quality Events Display—Window Tools Buttons*

| Icon | Meaning | Described in... |
|---|---|---|
|  | Exports the current display to a PDF file. | — |
|  | Opens a Service Quality Event History report in a separate window. | Understanding the Service Quality History Report, page 16-14 |
|  | Opens a new window with the display reformatted so that it is suitable for printing from your browser. | — |
|  | Opens online help. | — |

# Using the Service Quality Events Display

The Service Quality Events display shows the events that are occurring in your current view. Events are grouped by their severity: critical, warning, or informational. Within these severity groupings, events with the latest change are listed first.

When an event is generated, it remains in the Service Quality Events display until you clear them. Events are cleared every four hours. If a Cleared event reoccurs, a new event is shown. This display is refreshed every 60 seconds.

**Tip** You can generate a 24-hour Service Quality History report on all events that occurred on devices in your view by clicking the Service Quality Event History button in the upper-right corner of the window.

To see details about how Cisco Prime UOM automatically clears service quality events, see Clearing Service Quality Events, page 6-4.

### Clearing Service Quality Events

Cisco Prime UOM automatically clears service quality at a regular interval. When an event is cleared, it no longer appears on the Service Quality Events display. However, a record of the event remains in the database for 31 days and can be displayed from Service Quality History reports. For more information, see Getting Started with Service Quality History Reports, page 16-10.

# Viewing Service Quality Events Details

Use the Service Quality Event Details display to see detailed event information. This section contains:



## Using the Service Quality Event Details Display

The Service Quality Event Details display shows all of the events associated with a specific event. The events are displayed in a table. Events with the latest change are listed first. Events remain in the Service Quality Event Details display until you clear them. The Service Quality Event Details table is refreshed every 60 seconds.

The event name, destination, destination type, and description of the event are displayed above the Service Quality Event Details table. Table 6-3 describes the columns in the Service Quality Event Details table. Table 6-4 describes the command buttons on the Service Quality Event Details display.

This section contains:



*Table 6-3 Service Quality Event Details Display—Contents*

| Column | Description |
|---|---|
| # | Number of events—Events numbered from 1 |
| ! | Severity of event |
|  | Critical—This indicates that the device has at least one critical event. |
|  | Warning—This indicates that the device has at least one warning event. |
|  | Informational—This indicates that the device has at least one informational event. |
| Event ID | Event identifier number. Click this link to open the event properties page (see Viewing Service Quality Event Details, page 6-6). |

*Table 6-3 Service Quality Event Details Display—Contents (continued)*

| Column | Description |
|---|---|
| Customer Name | Customer cluster group name. |
| MOS | .05 through 5.0 |
| Cause | One of the following:<br>• Jitter<br>• Packet Loss |
| Timestamp | Date and time at which the event occurred. |
| Suppressed Traps | Number of violations for the endpoint for which Service Monitor did not generate a trap.<br>You can configure Service Monitor to send traps from sensors every *n* minutes. See *User Guide for Cisco Unified Service Monitor*. |
| Source Type | One of the following:<br>• Endpoint<br>• IP Phone |
| Source | IP address or DNS name or phone extension. |
| Tools | Links to tools that provide more information on the event.<br>The Service Quality Event History button opens a 24-hour Service Quality History report on the component. |

*Table 6-4 Service Quality Event Details Display—Command Buttons*

| Button | Action |
|---|---|
| Refresh | Selects the All Events view and refreshes the data in the display. |
| Notify | Sends e-mail notification of the event. See Sending E-Mail in Response to a Service Quality Event, page 6-5. |
| Close | Closes the Service Quality Event Details display. |

## Sending E-Mail in Response to a Service Quality Event

When you click the **Notify** button on the Service Quality Event Details display, Cisco Prime UOM opens a dialog box that you can complete to manually send an e-mail notification to one or more recipients.

The e-mail notification contains only the text you add; it does not append any event information. If you want to send *automatic* e-mail notifications when events occur on certain devices, use Notifications to set up an e-mail notification subscription. See Understanding Notifications, page 15-1.

To view Service Quality attributes:

**Step 1** From the Service Quality Event Details display, click **Notify**.

The E-Mail Notification Recipients dialog box opens.

**Step 2** In the E-Mail Notification Recipients dialog box:

**a.** Enter a fully qualified DNS name or IP address for an SMTP server.

b. Enter your e-mail address in the Sender Address field.

c. Enter a comma-separated list of e-mail addresses in the Recipient Addresses field.

d. Enter a subject heading in the Subject field.

e. (Optional) Enter a message in the Message field.

**Step 3** Click **Send**.

## Viewing Service Quality Event Details

You can view service quality event details using the following pages:

- Fault Monitor—View events in Events subpane or Events tab. See Viewing Event Details, page 4-25.
- Diagnostics View—UCM Cluster Device Pool Summary. See UCM Cluster Device Pool Summary, page 3-23.
- Reports > Service Quality > Events History—Search events based on criteria you choose. See Getting All Stored Information on a Service Quality Event, page 16-11.

The Service Quality Event Details display provides additional detail about the event, such as the values of MIB attributes at the time of the event such as those included in Table 6-5.

*Table 6-5 Service Quality Event Details Attributes*

| Field | Description |
|---|---|
| Customer Name | Customer cluster group name. |
| 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:<br>• Endpoint<br>• IP Phone<br>• 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 Endpoint | Extension number or IP address |
| Source IP Address | IP address, or N/A if destination type is Endpoint |
| Source Type | One of the following:<br>• IP Phone<br>• 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 |

*Table 6-5 Service Quality Event Details Attributes (continued)*

| Field | Description |
|---|---|
| Detection Algorithm | Algorithm used to calculate MOS. One of these:<br>• ITU G.107—Indicates that MOS is calculated on a Cisco 1040 Sensor<br>• CVTQ—Indicates that MOS is calculated on an IP phone or Cisco voice gateway using the Cisco Voice Transmission Quality algorithm |
| MOS | MOS value during event |
| Cause | One of the following:<br>• Jitter<br>• Packet Loss |
| Codec | Codec in use on the destination; one of the following:<br>• G711<br>• G722<br>• G728<br>• G729 |
| Jitter | Msec |
| Packet loss | Number of packets |
| **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<br>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). |
| 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 |
| 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 you are 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 |

*Table 6-5 Service Quality Event Details Attributes (continued)*

| Field | Description |
|---|---|
| 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 |

# Event Processing for Service Quality Events During High CPU Utilization

During periods of high CPU utilization, Cisco Prime UOM limits the number of service quality events that it processes. When this occurs, a message appears when you open the Fault Monitor display. The message states that event processing is being controlled.

The excess Service Quality events are written to the *NMSROOT*\logs\itemlogs\SQTraps\Traps.log file, and these events:

- Do not appear on the Fault Monitor display.
- Are not stored in the events history database—They do not appear in Service Quality History reports.

**Note** *NMSROOT* is the directory where Cisco Prime UOM is installed on your system. If you selected the default directory during installation, it can be entered as “C:\Program Files\CSCOpx” or C:\PROGRA~1\CSCOpx.

Cisco Prime UOM checks CPU utilization on its server every 60 seconds. When CPU utilization reaches and remains at 50% or greater for two minutes, Cisco Prime UOM limits the number of service quality events processed until utilization drops below 50%. Table 6-6 lists the number of events that Cisco Prime UOM processes.

*Table 6-6 Service Quality Event Processing Rates During HIgh CPU Utilization*

| Cisco Prime UOM CPU Utilization | Number of Service Quality Events Processed Per Minute |
|---|---|
| 50% | 40 |
| 60% | 20 |

For more details on how service quality events are grouped, or aggregated, in Fault Monitor, see Service Quality Events Aggregation, page 6-9.

# Service Quality Events Aggregation

In Cisco Prime UOM, individual service quality (SQ) events are grouped together, or aggregated, based on their threshold criteria settings. service quality event aggregation is completed for registered device pool and Communication Manager Express (CME) devices only.

The aggregated events are displayed in the Fault Monitor. For details on viewing these events in Fault Monitor, see Getting Device and Event Details, page 4-22.

If a service quality event from a phone is not registered with a device pool or Unified CM Express devices, then that event is not aggregated. Such events are displayed as individual events in Fault Monitor window.

For details on service quality event aggregation, see Handling Service Quality Events for Unified CM Express and Device Pools, page 6-9.

## Handling Service Quality Events for Unified CM Express and Device Pools

Voice service quality events for Unified CM Express devices and device pools, are now aggregated before they are reported in Cisco Prime UOM. Instead of reporting individual service quality events, these events are now aggregated based on criteria set by the device thresholds.

You can use the default device or device pool thresholds or customize them. Aggregation of service quality events is performed for Unified CM Express devices or device pools only.

After you set your Unified CM Express or device pool service quality threshold in the Phone Unregistration Default % field, if the number of events cause the percentage you set to be exceeded then a ServiceQualityThresholdCrossed event is sent.

The calculation to determine whether the threshold has exceeded is through the registered phone count at that point of time in the device pool or Unified CM Express.

For more details, see the Viewing and Editing Device Pool Thresholds, page 19-37.

**Note** One cluster can have multiple device pools. Device pools are displayed after you perform a cluster discovery.

### Device Pool Example

For example, if there are 100 registered phones in a Unified CM Express device pool named 1DP and the threshold value of that device pool is set to 10%, when 10% of those 100 registered phones experience service quality events (ten service quality events generated on individual phones registered to 1DP), then one aggregated event is generated.

Each incoming event on an individual phone of 1DP increases the count of impacted endpoints for 1DP increments by one. When that count reaches 10, an aggregated event is generated.

When the threshold goes below your set threshold value (for this example below 10) the same aggregated event is cleared. The service quality event is removed from the count when a Clear is generated for phones that were impacted.

All service quality events have a life span of four hours; after four hours the events get cleared. As the events are cleared, the impacted endpoint value is also decreased. When it goes below 10, an aggregated clear event is generated.

If the phone that sent the event belongs to the device pool, you can use the Device Pool Threshold window to view or edit the threshold percentages for the Unified CM Express or device pool. See Viewing and Editing Device Pool Thresholds, page 19-37 for details on customizing device pool thresholds.

The component for an aggregated event is a device pool (if the event is raised on a device pool) or a Unified CM Express (if the event is raised on a CME). Endpoints experiencing issues is the value set by the user which impacts the phone.

All events of Device Pools and CME are listed in the Fault Monitor window. If a SQ event, which is coming from a phone, is not a Device Pool or a CME, that event will not be considered for any aggregation.

Voice Gateways and Unity do not belong to any device pool or CME. So these events are listed as individual events in Fault Monitor.

# Using the Service Quality Alerts Display

These topics describe the Service Quality Alerts Display:



The Service Quality Alerts display provides real-time information about IP phone service quality. Service Quality Alerts displays are designed so that you can set them up and leave them running. This serves as an ongoing monitoring tool that indicates when something needs attention.

Use the Service Quality Alerts display to view alerts that Cisco Prime UOM generates based on SNMP traps sent by Cisco Unified Service Monitor (Service Monitor).

To use the Service Quality Alerts display, you must have a licensed copy of Service Monitor configured to send traps to Cisco Prime UOM. You must also add Service Monitor to Cisco Prime UOM. See Adding a Service Monitor Link from Operations Manager, page 21-4.

When Cisco Prime UOM receives traps from Service Monitor, Cisco Prime UOM generates an event or events that are rolled up into an alert. The alert is shown on your Service Quality Alerts display. From a Service Quality Alerts display, you can launch other windows to obtain more information, including:

- Event details—Displays details for the events that caused the alert to be generated.
- Service quality history—Reports service quality events generated during the previous 24 hours.

All Service Quality History reports generated from within the Service Quality Alerts display provide information from the past 24 hours.

To generate a Service Quality History report on time spans beyond the last 24 hours, use Service Quality History from the Reports tab by selecting **Reports > Service Quality History**. For more information, see Getting All Stored Information on a Service Quality Event, page 16-11.

## Starting the Service Quality Alerts Display

To start the Service Quality Alerts display, select **Administration > System Settings > Miscellaneous > Service Quality Alerts**. Service quality alerts appears in a new window.

# Understanding the Layout of the Service Quality Alerts Display

These topics provide details about the information in the Service Quality Alerts display.

### Launch Information and View Status Bar Area

The launch information area shows the current time on the server when the Service Quality Alerts display is being viewed. The view status bar lists the selected view, the number of alerts in that view, and, if filters have been applied, displays "(Filtered.)"

### Tabular Display Pane

The tabular display pane is the core of the Service Quality Alerts display. It contains a list of alerts that are occurring on the devices in your current view. This pane is refreshed every 60 seconds. For an explanation for all of the items in the tabular display, see Using the Service Quality Events Display, page 6-3.

Icons alert you to what needs attention; for example, the severity icons indicate which views and alerts require attention. The tabular display pane is scrollable and can display up to 1,000 records.

### Window Tools Area

The top-right corner of the Service Quality Alerts display contains available tools buttons. All buttons are described in Table 6-2.

*Table 6-7 Service Quality Alerts Display—Window Tools Buttons*

| Icon | Meaning | Described in... |
|---|---|---|
|  | Exports the current display to a PDF file. | — |
|  | Opens the Service Quality Alerts Filter dialog box, for refining the data in the Service Quality Alerts display. | Viewing Service Quality Events Details, page 6-4 |
|  | Opens a Service Quality Event History report in a separate window. | Understanding the Service Quality History Report, page 16-14 |
|  | Opens a new window with the display reformatted so that it is suitable for printing from your browser. | — |
|  | Opens online help. | — |

# Using the Service Quality Alerts Display

The Service Quality Alerts display shows the alerts that are occurring in your current view. Alerts are grouped by their severity: critical, warning, or informational. Within these severity groupings, alerts with the latest change are listed first.

When an alert is generated, it remains in the Service Quality Alerts display until it is cleared. Alerts are cleared every 8 hours. While the alert is in the display, if any of its events occur or get updated, the alert is updated.

- If a Cleared alert reoccurs, a new alert with a new alert ID is shown.
- If a Cleared event reoccurs, a new event with a new event ID is shown. This display is refreshed every 60 seconds.

**Tip** You can generate a 24-hour Service Quality History report on all events that occurred on devices in your view by clicking the Service Quality Event History button in the upper-right corner of the window.

***Table 6-8 Service Quality Alerts Display—Contents***

| Heading | Description | |
|---|---|---|
| # | Number of alerts—Alerts numbered from 1 | |
| ! | Severity of alert | |
| |  | Critical |
| |  | Warning |
| |  | Information |
| Check box | Select one or more check boxes to select alerts that you want to clear before clicking the **Clear** button. | |
| ID | Alert identifier number. Click this link to open a Service Quality Alert Details display. | |
| Destination Type | Call destination: one of the following:<br>• IP Phone<br>• Endpoint | |
| Extension | Extension number if the destination type is IP phone. Click this link to open an IP Phone report. See Understanding Audio IP Phone Inventory Reports, page 1-15. | |
| Destination | IP address if the destination type is Endpoint. Click this link to open an IP Phone report. See Understanding Audio IP Phone Inventory Reports, page 1-15. | |
| Latest Event Time | Date and time alert last occurred or was changed. Diamonds indicate alert activity, such as a new event, new user annotation, and so forth; no diamonds indicates that the alert is stale.<br>Alerts are grouped by severity, and within severities, alerts with the latest change are listed first. | |
| |  | Alert was updated within last 15 minutes. |
| |  | Alert was updated within last 16-30 minutes. |
| |  | Alert was updated within last 31-45 minutes. |
| | No diamonds | Alert was updated 46 or more minutes ago. |

## Purging Service Quality Alerts

Cisco Prime UOM automatically purges service quality alerts when all the events in that alert are purged. When an alert is purged, it no longer appears on the Service Quality Alerts display.

## Viewing Service Quality Alert Display

Whenever you launch the Service Quality Alert display, it shows all Service Quality Alerts in the system.

## Filtering Service Quality Alerts

Filters allow you to manipulate the Service Quality Alerts display to show alerts based on their MOS score, destination, phone model, codec, and Cisco 1040 name or Cisco Unified Communications Manager cluster name.

After you apply a service quality alert filter, the filter is applied to all of your views until you change or reset the filter, or close the Service Quality Alerts display. Other clients that access Cisco Prime UOM are not affected. When you close the Service Quality Alerts display, your filter is lost.

**Step 1** Select **Administration > System Settings > Miscellaneous > Service Quality Alerts**.

The Service Quality Alerts display opens.

**Step 2** Click the filtering button at the top-right of the Service Quality Alerts display.

The Service Quality Alerts Filter dialog box appears.

**Step 3** Enter data for only *one* of the following filters:

- **MOS Score**—Enter a value less than 5.0.
- **Destination**—Select one of the following radio buttons and enter the appropriate information:
  - **Extension**—Phone extension being called. Select an operator from the list and enter a number.
  - **IP Address**— For a phone, switch, voice gateway, or Cisco 1040. Select an operator from the list and enter a number. Depending on the operator, you can enter a portion of the IP address or the full IP address.
- **Codec**—Enter any of these in a comma-separated list: G711, G722, G728, or G729.
- **Phone Model**—Click the button to select phone models from a list.
- **Sensor MAC**—Enter a comma-separated list of MAC addresses for Cisco 1040 Sensors.

**Step 4** Click **OK**.

## Resetting Filters on the Service Quality Alerts Display

From the Service Quality Alerts display, you can clear any filters that you have set without changing the selected view.

**Step 1** On the Service Quality Alerts display, click **Reset Filter**.

A confirmation dialog box appears.

**Step 2** Click **Yes**.

The Service Quality Alerts display refreshes, displaying all alerts in the currently selected view.

# Viewing Events Associated with a Service Quality Alert

Use the Service Quality Alert Details display to see the events that are associated with an alert.

## Starting the Service Quality Alert Details Display

The Service Quality Alert Details display provides information about all of the events that were rolled up into a specific alert.

**Step 1** Select **Administration > System Settings > Miscellaneous > Service Quality Alerts**.

The Service Quality Alerts display opens.

**Step 2** Locate the alert you want to investigate and click the alert ID.

The Service Quality Alert Details display opens.

## Using the Service Quality Alert Details Display

The Service Quality Alert Details display shows all of the events associated with a specific alert. The events are displayed in a table and events with the latest change are listed first. Events remain in the Service Quality Alert Details display until you clear them or until you clear the parent alert. The Service Quality Alert Details table is refreshed every 60 seconds.

The alert name, destination, destination type, and description of the alert are displayed above the Service Quality Alert Details table. Table 6-9 describes the columns in the Service Quality Alert Details table. Table 6-10 describes the command buttons on the Service Quality Alert Details display.

*Table 6-9 Service Quality Alert Details Display—Contents*

| Column | Description | |
|---|---|---|
| # | Number of events—Events numbered from 1 | |
| ! | Severity of alert | |
| |  | Critical |
| |  | Warning |
| |  | Informational Unidentified Trap alert |
| | (no icon) | Informational (for all other events) |

*Table 6-9 Service Quality Alert Details Display—Contents (continued)*

| Column | Description |
|---|---|
| Event ID | Event identifier number. Click this link to open the event properties page (see Viewing Service Quality Event Details, page 6-6). |
| Customer Name | Customer cluster group name. |
| MOS | .05 through 5.0 |
| Cause | One of the following:<br>• Jitter<br>• Packet Loss |
| Timestamp | Date and time at which the event occurred. |
| Suppressed Traps | Number of violations for the endpoint for which Service Monitor did not generate a trap.<br>You can configure Service Monitor to send traps from sensors every *n* minutes. See *User Guide for Cisco Unified Service Monitor*. |
| Source Type | One of the following:<br>• Endpoint<br>• IP Phone |
| Source | IP address or DNS name or phone extension. |
| Tools | Links to tools that provide more information on the event.<br>Clicking the Service Quality Event History button opens a 24-hour Service Quality History report on the component. |

*Table 6-10 Service Quality Alert Details Display—Command Buttons*

| Button | Action |
|---|---|
| Refresh | Selects the All Alerts view and refreshes the data in the display. |
| Clear | Clears the service quality alert. See Clearing Service Quality Events, page 6-4. |
| Notify | Sends e-mail notification of the alert. See Sending E-Mail in Response to a Service Quality Event, page 6-5. |
| Close | Closes the Service Quality Alert Details display. |

## Purging a Service Quality Event

At every four hours Cisco Prime UOM purges service quality events that are displayed on the Service Quality Event Settings page. When an event is purged, it no longer appears on the Service Quality Alerts Details display.

However, a record of the event remains in the database for 31 days and can be displayed from Service Quality Event History reports. For more information, see Getting Started with Service Quality History Reports, page 16-10.

## Sending E-Mail in Response to a Service Quality Alert

When you click the **Notify** button on the Service Quality Alert Details display, Cisco Prime UOM opens a dialog box that you can complete to manually send an e-mail notification to one or more recipients. The e-mail notification contains only the text that you add; it does not append any alert or event information.

If you want to send *automatic* e-mail notifications when alerts or events occur on certain devices, use Notifications to set up an e-mail notification subscription. See Understanding Notifications, page 15-1.

**Step 1** From the Service Quality Alert Details display, click **Notify**.

The E-Mail Notification Recipients dialog box opens.

**Step 2** In the E-Mail Notification Recipients dialog box:

**a.** Enter a fully qualified DNS name or IP address for an SMTP server.

**b.** Enter your e-mail address in the Sender Address field.

**c.** Enter a comma-separated list of e-mail addresses in the Recipient Addresses field.

**d.** Enter a subject heading in the Subject field.

**e.** (Optional) Enter a message in the Message field.

**Step 3** Click **Send**.

## Viewing Service Quality Event Attributes

The Service Quality Event Attributes dialog box provides additional detail about the event, such as the values of MIB attributes at the time of the event.

**Step 1** Select **Administration > System Settings > Miscellaneous > Service Quality Alerts**.

The Service Quality Alerts display opens.

**Step 2** Locate the alert you want to investigate and click the alert ID.

The Service Quality Alert Details display appears.

**Step 3** Locate the event you want to investigate, and click the event ID.

The Service Quality Event Attributes dialog box appears, displaying the event ID and the information in Table 6-3 on page 6-4.

| Field | 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:<br>• Endpoint<br>• IP Phone<br>• Media Server |
| Destination Model | Phone model, or N/A if destination type is Endpoint |

| Field | Description |
|---|---|
| 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 Endpoint | Extension number or IP address |
| Source IP Address | IP address, or N/A if destination type is Endpoint |
| Source Type | One of the following:<br>• IP Phone<br>• 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:<br>• ITU G.107—Indicates that MOS is calculated on a Cisco 1040 Sensor<br>• CVTQ—Indicates that MOS is calculated on an IP phone or Cisco voice gateway using the Cisco Voice Transmission Quality algorithm |
| MOS | MOS value during event |
| Cause | One of the following:<br>• Jitter<br>• Packet Loss |
| Codec | Codec in use on the destination; one of the following:<br>• G711<br>• G722<br>• G728<br>• G729 |
| Jitter | Msec |
| Packet loss | Number of packets |
| **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<br>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).<br>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 |

| Field | Description |
|---|---|
| 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 |
| 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 you are 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 |
| Customer Name | Customer group name. |

**Step 4** Click **Close** to dismiss the dialog box.