



Using History Reports

These topics explain how to use IP Communications Operations Manager (Operations Manager) Alert and Event History and Service Quality Event History reports:

- [Getting Started with History Reports, page 11-1](#)
- [Getting Started with Alert and Event History, page 11-2](#)
- [Generating Customized Alert and Event History Reports, page 11-3](#)
- [Understanding the Alert History Report, page 11-10](#)
- [Understanding the Event History Report, page 11-12](#)
- [Getting Started with Service Quality Event History Reports, page 11-14](#)
- [Understanding the Service Quality Event History Report, page 11-18](#)

Getting Started with History Reports

Alert and Event History reports and Service Quality History reports enable you to view alerts and events that occurred during the past 31 days. The available information includes alert status and date, related device and device components, annotations (informational text you entered), and event details. Operations Manager purges the Alert History database daily to retain only 31 days of history; see [Viewing Purge Scheduler Status, page 19-13](#).



Note

Service Quality History is useful only if you have purchased a license for CiscoWorks IP Communications Service Monitor (Service Monitor). For more information, see *User Guide for CiscoWorks IP Communications Service Monitor*.




For more information, see the following topics:

- [Getting Started with Alert and Event History, page 11-2](#)
- [Getting Started with Service Quality Event History Reports, page 11-14](#)

History Report Tool Buttons

[Table 11-1](#) explains the tool buttons that appear in the upper-right corner of history reports.

Table 11-1 Alert and Event History Report Window Tool Buttons

Icon	Meaning
	Exports the current report to a PDF or CSV file.
	Opens a printer-friendly version for printing.
	Opens context-sensitive help.

Reports with More than 2,000 Records

The Alert History and 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 or PDF file.

Getting Started with Alert and Event History

You can generate [24-hour context-based reports](#) from various Operations Manager 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 and device components.

24-Hour Context-Based Alert and Event History Reports

On various Operations Manager pages, such as the Alerts and Events display, you can select Alert History or Event History links or menu items. When you click an Alert History or 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 Alert History and Event History reports for a time period that you select and include records based on search criteria that you specify. Alert History and 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 Operations Manager pages. For example, from:

- Service Level View—You can launch an Alert History report for a device.
- Phone Activity display—You can launch a Service Quality Event History report for a phone model.



Note

Operations Manager stores Service Quality event history if you have purchased a license for Service Monitor. For more information, see *User Guide for CiscoWorks IP Communications Service Monitor*.

Customized Alert History and Event History Reports

You might want to generate an Alert History report or an Event History report when:

- A significant alert is shown in the Alerts and Events display, and you want to see how often the alert 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 and alerts other than those you are tracking in your customized Alerts and Events display.

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

- All events that caused an alert.
- Events that occurred on components of a device.
- Occurrences of the same event on different devices.

Generating Customized Alert and Event History Reports

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

- To search for alerts by alert ID, device, or group, see [Getting All Stored Information on an Alert, page 11-3](#).
- To search for events on devices by event ID, device, alert ID, or group, see [Getting All Stored Information on an Event, page 11-6](#).
- 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 11-15](#).

**Note**

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

Getting All Stored Information on an Alert

You can search the Alert History database for alerts using one of the following methods:

- [Searching for Alerts by Alert ID, page 11-4](#)
- [Searching for Alerts by Device, page 11-4](#)
- [Searching for Alerts by Device Group, page 11-4](#)
- [Searching for Alerts by Date, page 11-5](#)

**Note**

Alternatively, to generate a 24-hour report of all alerts in your current view, launch Alert History for the selected view from the Alerts and Events window. See [Using the Alerts and Events Display, page 3-1](#).

Searching for Alerts by Alert ID

To determine how often a specific alert has occurred, search for the alert by its alert ID. The alert ID is displayed in the Alerts and Events display.

-
- Step 1** Select **Reports > Alert and Event History > Alert History > Alert**. The Alert History: Search by Alert ID page appears.
- Step 2** Set your search criteria:
- a. Enter the alert ID.
 - b. Select all alert severity levels that you want to search for.
 - 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 2,000 records match your search criteria, a popup window reports the total number of records found.
- The Alert History report opens. For an explanation of the report contents, see [Understanding the Alert History Report, page 11-10](#).
-

Searching for Alerts by Device

Use this procedure to determine what types of alerts are occurring on a specific device.

-
- Step 1** Select **Reports > Alert and Event History > Alert History > Devices**. The Alert 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).
 - b. Select all alert severity levels that you want to search for.
 - 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 2,000 records match your search criteria, a popup window reports the total number of records found.
- The Alert History report opens. For an explanation of the report contents, see [Understanding the Alert History Report, page 11-10](#).
-

Searching for Alerts by Device Group

To determine what type of alerts are occurring in a specific device group, use this procedure.

-
- Step 1** Select **Reports > Alert and Event History > Alert History > Device Groups**. The Alert History: Search by Group page appears.
- Step 2** Set your search criteria:
- Select the device group. You can also select multiple devices from different groups.
 - Select all alert severity levels that you want to search for.
 - 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 2,000 records match your search criteria, a popup window reports the total number of records found.
- The Alert History report opens. For an explanation of the report contents, see [Understanding the Alert History Report, page 11-10](#).
-

For more information, see the following topics:

- [Customizing Events, page 14-18](#)
- [Events Processed, page D-1](#)

Searching for Alerts by Date

To determine what type of alerts are occurring during a specific day, week, month, or range of dates, use this procedure.

-
- Step 1** Select **Reports > Alert and Event History > Alert History > Date**. The Alert History: Search by Date page appears.
- Step 2** Select the date range and enter:
- Today.
 - 7 days (from *current date* to *date*).
 - One Month (from *current date* to *date*).
 - From: *date* and to: *a date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.).
- Step 3** Click **View**. If more than 2,000 records match your search criteria, a popup window reports the total number of records found. The Alert History report opens. For an explanation of the report contents, see [Understanding the Alert History Report, page 11-10](#).
-

For more information, see the following topics:

- [Customizing Events, page 14-18](#)
- [Events Processed, page D-1](#)

Getting All Stored Information on an Event


Note

For information about Service Quality events, see [Getting All Stored Information on a Service Quality Event, page 11-15](#).

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

- [Searching for Events by Event ID, page 11-6](#)
- [Searching for Events by Device, page 11-6](#)
- [Searching for Events by Alert, page 11-7](#)
- [Searching for Events by Device Group, page 11-8](#)
- [Searching for Events by Date, page 11-8](#)


Note

Alternatively, to generate a 24-hour report of all events on a device component, click the Event History link on the Alerts Detail page. See [Using the Alerts and Events Display, page 3-1](#).

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 Alert Details display.

-
- Step 1** Select **Reports > Alert and Event History > 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 2,000 records match your search criteria, a popup window reports the total number of records found.
- The Event History report opens. For an explanation of the report contents, see [Understanding the Event History Report, page 11-12](#).
-

Searching for Events by Device

Use this procedure to determine what types of events are occurring on a specific device.

-
- Step 1** Select **Reports > Alert and Event History > Event History > Devices**. The Event History: Search by Device page appears.
- Step 2** Set your search criteria:
- Enter a comma-separated list of devices (as they are listed by Device Management). You can select multiple devices from different groups.
 - 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 11-7](#).)
 - 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 2,000 records match your search criteria, a popup window reports the total number of records found.
- The Event History report opens. For an explanation of the report contents, see [Understanding the Event History Report, page 11-12](#).
-

Selecting Event Descriptions for an Event History Report

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

- Step 1** 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:
- Select **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.
-

Searching for Events by Alert

To view the events that correspond to a specific alert, use this procedure.

- Step 1** Select **Reports > Alert and Event History > Event History > Alert**. The Event History: Search by Alert ID page appears.
- Step 2** Set your search criteria:
- Enter the Alert ID.
 - (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 11-7](#).)

- 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 2,000 records match your search criteria, a popup window reports the total number of records found.

The Event History report opens. For an explanation of the report contents, see [Understanding the Event History Report, page 11-12](#).

Searching for Events by Device Group

To determine what types of events are occurring in a specific device group, use this procedure.

Step 1 Select **Reports > Alert and Event History > 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 alert 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 2,000 records match your search criteria, a popup window reports the total number of records found.

The Event History report opens. For an explanation of the report contents, see [Understanding the Event History Report, page 11-12](#).

For more information, see the following topics:

- [History Report Tool Buttons, page 11-1](#)
- [Customizing Events, page 14-18](#)
- [Events Processed, page D-1](#)

Searching for Events by Date

To determine what type of alerts are occurring during a specific day, week, month, or range of dates, use this procedure.

-
- Step 1** Select **Reports > Alert and 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 2,000 records match your search criteria, a popup window reports the total number of records found.
- The Event History report opens. For an explanation of the report contents, see [Understanding the Event History Report, page 11-12](#).
-

For more information, see the following topics:

- [History Report Tool Buttons, page 11-1](#)
- [Customizing Events, page 14-18](#)
- [Events Processed, page D-1](#)

Understanding the Alert History Report

The Alert History report (shown in [Figure 11-1](#)) 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.

Figure 11-1 Alert History Report

	Severity	Alert ID	Device Type	Device Name	Time	Description	Status
1.	Critical	00000S9	Router	172.20.119.89	17-Nov-2005 22:57:44	Reachability	Active
2.	Critical	00000S9	Router	172.20.119.89	17-Nov-2005 22:57:44	Interface	Active
3.	Critical	00000S7	Router	172.20.119.90	17-Nov-2005 22:57:44	Reachability	Active
4.	Critical	00000S7	Router	172.20.119.90	17-Nov-2005 22:57:43	Interface	Active
5.	Critical	00000S4	Router	172.20.119.87	17-Nov-2005 22:57:43	Reachability	Active
6.	Critical	00000S4	Router	172.20.119.87	17-Nov-2005 22:57:43	Interface	Active
7.	Informational	000014M	Router	172.20.119.94	17-Nov-2005 22:57:43	Reachability	Cleared
8.	Critical	00000S6	Router	172.20.119.88	17-Nov-2005 22:57:43	Interface	Active
9.	Critical	00000S6	Router	172.20.119.88	17-Nov-2005 22:57:43	Reachability	Active
10.	Critical	00000S1	Router	172.20.119.91	17-Nov-2005 22:57:42	Reachability	Active
11.	Critical	00000S1	Router	172.20.119.91	17-Nov-2005 22:57:42	Interface	Active
12.	Critical	00000RY	Router	172.20.119.92	17-Nov-2005 22:57:41	Reachability	Active
13.	Critical	00000RY	Router	172.20.119.92	17-Nov-2005 22:57:41	Interface	Active
14.	Critical	00000RV	Router	172.20.119.93	17-Nov-2005 22:57:40	Reachability	Active
15.	Critical	00000RV	Router	172.20.119.93	17-Nov-2005 22:57:40	Interface	Active
16.	Informational	00001XE	PhoneAccessSwitch	seaview-3550.cisco.com	17-Nov-2005 21:55:20	Utilization	Cleared
17.	Critical	00000RV	Content Networking	rme-gw.cisco.com	17-Nov-2005 21:52:13	Utilization	Active
18.	Critical	00000RV	Content Networking	rme-gw.cisco.com	17-Nov-2005 21:52:13	Interface	Active
19.	Critical	00000RV	Content Networking	rme-gw.cisco.com	17-Nov-2005 21:52:13	Utilization	Active
20.	Critical	00000RV	Content Networking	rme-gw.cisco.com	17-Nov-2005 21:48:12	Interface	Active

The Alert History report window provides tools, as shown in [Table 11-1](#).

[Table 11-2](#) describes the contents of the Alert History report.

Table 11-2 Alert History Report—Contents

Heading	Description
Alert ID	Alert identifier number. Clicking this link opens the Event History report (see Figure 11-4 on page 11-14), which contains details about the events associated with the alert.
Device Name	Device name or IP address.
Device	Device type. Inventory Collection in Progress indicates that Operations Manager was discovering the device at the time of the alert. The actual device type is reflected when new events occur. For more information, see Chapter 15, “Using Device Management.”

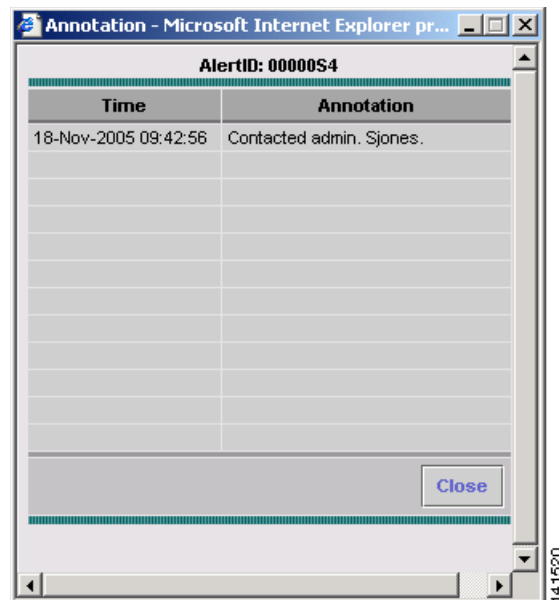
Table 11-2 *Alert History Report—Contents (continued)*

Heading	Description
Description	Alert category, one of the following: Application, Connectivity, Environment, Interface, Other, Reachability, System Hardware, Utilization. For alerts containing multiple events, the report shows the category of the event with the most recent change. For alerts containing multiple events, the report shows the category of the event with the most recent change.
Severity	Critical, Warning, or Informational.
Time	Date and time when the alert was generated.
Status	Alert status, based on last polling. Active Cleared Acknowledged

Viewing User Annotations from an Alert History Report

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

[Figure 11-2](#) shows an alert annotation page, which lists any notes that users have entered using the Alert Details page. (For more information, see [Responding to Alerts, page 3-25.](#))

Figure 11-2 *Alert Annotation Page*

Launching Event History from an Alert History Report

To launch an Event History report from an Alert History report, click the alert ID link that interests you. The Event History report opens in a new window and lists the events that caused the alert to be generated.

Understanding the Event History Report



Note

Service Quality events are reported on Service Quality Event History reports. See [Understanding the Service Quality Event History Report, page 11-18](#).

The Event History report lists events. For each event, the Event History report includes:

- Device on which the event occurred
- Component on which the event occurred
- Time of the event
- Current status of the event
- Event ID link to open the Event Properties page and view current attribute or threshold values compared with the values at the time the event occurred

Figure 11-3 provides an example of an Event History report.

Figure 11-3 Event History Report

Event ID	Device Name	Device Component	Event Description	Time	Status	Alert ID
1. 000417A	172.20.119.90	SNMPAgent-172.20.119.90	Unresponsive	17-Nov-2005 22:57:44	Cleared	00000S7
2. 00041Z9	172.20.119.90	IF-172.20.119.90/3	OperationallyDown	17-Nov-2005 22:57:43	Active	00000S7

The Event History report window provides tool buttons in the upper-right corner of the window; these are described in [Table 11-1](#).

[Table 11-3](#) describes the contents of the Event History report in more detail.

Table 11-3 Event History Report—Contents

Heading	Description
Event ID	Event identifier number. Clicking this link opens the event properties page (see Figure 11-4), which describes the value of MIB attributes currently and at the time of the event.
Device Name	Device name or IP address.
Component	Device element on which the event occurred.

Table 11-3 *Event History Report—Contents (continued)*

Heading	Description	
Description	Operations Manager event name (as described in Appendix D, “Events Processed”). You can also customize the names of events displayed by Event History (and the Alerts and Events display) using the Event Customization feature in Notifications. For more information, see Customizing Events, page 14-18 .	
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 alerts are cleared. When Operations Manager 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 Alerts and Events display.
	Suspended	Device is suspended.
	Resumed	Device is being resumed.
	Deleted	Device has been deleted.
Alert ID	Alert identifier number associated with this event.	

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.

[Figure 11-4](#) shows an example of the event properties page.

Figure 11-4 Event Properties Page

EventID: 0000Y0	
Property	Value
Component	172.20.118.84 [PR-PUB]
InterfaceName	IF-PR-PUB/16777219 [HP NC3163 Fast Ethernet NIC [172.20.118.84]]
InterfaceAdminStatus	UNKNOWN
Address	172.20.118.84
IPStatus	OK
InterfaceType	ETHERNETCSMACD
NetworkNumber	172.20.118.64
InterfaceMode	NORMAL
InterfaceOperStatus	UNKNOWN

Getting Started with Service Quality Event History Reports

This section contains the following topics:

- [Exporting 24-Hour and 7-Day Service Quality Event History Reports](#), page 11-14
- [Getting All Stored Information on a Service Quality Event](#), page 11-15

Exporting 24-Hour and 7-Day Service Quality Event 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) and PDF 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 Event History report:
 - CSV—Saves the report as a comma-separated-values file.
 - PDF—Saves the report in portable document format.



Note 24-hour reports are named ddmmyyyy_Daily.filetype, for example 20Apr2006_Daily.csv.

- All issues for the last 7 days—Select one or more check boxes to generate and save a 7-day Service Quality Event History report:
 - CSV—Saves the report as a comma-separated-values file.
 - PDF—Saves the report in portable document format.



Note 7-day reports are named ddmmYYYY_Weekly.filetype, for example 17Apr2006_Weekly.pdf. 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 Service Monitor server.
 - 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



Note

Service Quality Event History reports are only available if you have purchased a license for Service Monitor. For more information, see *User Guide for CiscoWorks IP Communications Service Monitor*.

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

- [Searching for Service Quality Events by MOS, page 11-15](#)
- [Searching for Service Quality Events by Destination, page 11-16](#)
- [Searching for Service Quality Events by Codec, page 11-16](#)
- [Searching for Service Quality Events by Phone Model, page 11-17](#)
- [Searching for Service Quality Events by Cisco 1040, page 11-17](#)
- [Searching for Service Quality Events by Date, page 11-18](#)

Searching for Service Quality Events by MOS

To view the Service Quality events for MOS less than a value that you supply, use this procedure.

- 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 2,000 records match your search criteria, a popup window reports the total number of records found.

The Service Quality Event History report opens. For an explanation of the report contents, see [Understanding the Service Quality Event History Report, page 11-18](#).

Searching for Service Quality Events by Destination

To view the Service Quality events that correspond to call endpoints, use this procedure.

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 2,000 records match your search criteria, a popup window reports the total number of records found.

The Service Quality Event History report opens. For an explanation of the report contents, see [Understanding the Service Quality Event History Report, page 11-18](#).

Searching for Service Quality Events by Codec

To view the Service Quality events for a particular codec, use this procedure.

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 2,000 records match your search criteria, a popup window reports the total number of records found.

The Service Quality Event History report opens. For an explanation of the report contents, see [Understanding the Service Quality Event History Report, page 11-18](#).

Searching for Service Quality Events by Phone Model

To view the Service Quality events that correspond to specific phone models, use this procedure.

Step 1 Select **Reports > Service Quality History > Event History > Phone Model**. The Service Quality History: Search by Phone Model(s) page appears.

Step 2 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 3 Click **View**. If more than 2,000 records match your search criteria, a popup window reports the total number of records found.

The Service Quality Event History report opens. For an explanation of the report contents, see [Understanding the Service Quality Event History Report, page 11-18](#).

Searching for Service Quality Events by Cisco 1040

To view the Service Quality events that correspond to specific Cisco 1040, use this procedure.

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.



Note 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 2,000 records match your search criteria, a popup window reports the total number of records found.

The Service Quality Event History report opens. For an explanation of the report contents, see [Understanding the Service Quality Event History Report, page 11-18](#).

Searching for Service Quality Events by Date

To view the Service Quality events for specific dates, use this procedure.

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 2,000 records match your search criteria, a popup window reports the total number of records found.

The Service Quality Event History report opens. For an explanation of the report contents, see [Understanding the Service Quality Event History Report, page 11-18](#).

For more information, see the following topics:

- [History Report Tool Buttons, page 11-1](#)
- [Customizing Events, page 14-18](#)
- [Events Processed, page D-1](#)

Understanding the Service Quality Event History Report



Note

Service Quality History is useful only if you have purchased a license for Service Monitor. For more information, see *User Guide for CiscoWorks IP Communications Service Monitor*.

The Service 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 the 2,000 records, click the Export tool button in the upper-right corner of the window.

The Service Quality Event History report window provides tools, as shown in [Table 11-1](#).

[Table 11-4](#) describes the contents of the Service Quality Event History report.

Table 11-4 Service Quality Event History Report—Contents

Heading	Description
Severity	Event severity: <ul style="list-style-type: none"> Warning—MOS is below the MOS threshold configured on Service Monitor. For more information, see <i>User Guide for IP Communications Service Monitor</i>. Critical—MOS is below the MOS threshold configured on Operations Manager. For more information, see Configuring Service Quality Event Settings, page 19-9.
Event ID	Click this link to open the event properties window. See Viewing Service Quality Event Properties, page 11-19 .
Destination Type	One of the following: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Jitter Latency
Time	Date and time that the event occurred.
Codec	One of the following: <ul style="list-style-type: none"> G711 G722 G723 G728 G729
Source Type	One of the following: <ul style="list-style-type: none"> Endpoint IP Phone
Source	IP address or phone extension.
IP Address	Source IP address.

Viewing Service Quality Event Properties

- Step 1** Click an event ID link on the Service Quality Event History report to view properties of the event. See [Understanding the Service Quality Event History Report, page 11-18](#).

Table 11-5 describes the contents of the service quality Event Properties window.

Table 11-5 Service Quality Event Properties Window—Contents

Heading	Description
Destination	Extension number or N/A
Destination IP Address	IP address
Destination Type	One of the following: <ul style="list-style-type: none"> • IP Phone • Endpoint
Destination Model	Phone model or N/A
Switch for Destination	IP address or N/A
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
Source Type	One of the following: <ul style="list-style-type: none"> • IP Phone • Endpoint
Source Model	Phone model or N/A
Switch for Source	IP address or N/A
Source Port	Port type and slot or N/A
Detection Algorithm	Algorithm
MOS	MOS value during event
Critical MOS Threshold	MOS threshold configured on Operations Manager (see Configuring Service Quality Event Settings, page 19-9)
Cause	One of the following: <ul style="list-style-type: none"> • Jitter • Latency • Packet Loss
Codec	Codec in use on the destination; one of the following: <ul style="list-style-type: none"> • G711 • G722 • G723 • G728 • G729
Jitter	Msec
Packet loss	Number of packets.
Cisco 1040 ID	ID consists of a letter and 3 digits; for example, A101.

