



Using Reports

The following topics are included:

- [Overview: Service Monitor Reports, page 2-1](#)
- [Using Sensor Reports, page 2-4](#)
- [Using CVTQ Reports, page 2-7](#)
- [Using Most-Impacted Endpoints Reports, page 2-10](#)

Overview: Service Monitor Reports

Service Monitor reports enable you to examine voice transmission quality in the parts of your network that Service Monitor has monitored during the last 30 days. Service Monitor reports show the times when MOS has been below configured thresholds, the codec in use, and the endpoints on which the violations have occurred. Data for the reports is obtained from Cisco 1040 sensors and Cisco Unified CallManager clusters in your network.

Service Monitor stores the data that it collects from sensors and Cisco Unified CallManagers in the Service Monitor database for 30 days. Service Monitor purges its database every day, retaining only the data for the last 30 days. For more information, see [Understanding Service Monitor Database Purging, page 6-1](#).

Service Monitor supplies separate reports for data obtained from:

- **Sensors**—Sensors send data to Service Monitor every 60 seconds, providing minute-by-minute assessments of MOS.
- **Cisco Unified CallManager clusters**—Service Monitor obtains CVTQ data from clusters every 60 seconds. However, data for a given call becomes available only after it completes. Service Monitor therefore can assess MOS, send traps, and provide information in reports after the call has occurred.

Within sensor reports and CVTQ reports, there are two types of reports:

- **Diagnostic reports**—These reports enable you to specify what you want to report on and generate a report that contains as little as one minute of data or as much as 30 days of data. On the report window itself, you can change the columns that are displayed, including restoring reports to display a default set of columns; see [Selecting Columns to Display and to Hide on a Service Monitor Report, page 2-3](#). For more information, see [Using Sensor Reports, page 2-4](#) and [Using CVTQ Reports, page 2-7](#).

- Most-Impacted Endpoint reports—These reports list the endpoints that have had the most violations reported in the last 24 hours. You can also schedule this report to run automatically; exported reports are then created for the last 24 hours and for the last 7 days. For more information, see [Using Most-Impacted Endpoints Reports, page 2-10](#).

Configuring Service Monitor Initially Before Running Reports

Before you can run Service Monitor reports for the first time, you need to perform some configuration tasks. For Service Monitor to begin monitoring data that is gathered by:

- Cisco Unified CallManager clusters—You need to add credentials to Service Monitor and perform some configuration in Cisco Unified CallManager or on the system where Cisco Unified CallManager resides. For more information, see the following topics:
 - [Understanding and Setting Cisco Unified CallManager Credentials, page 3-2](#)
 - [Cisco Unified CallManager Configuration, page B-1](#)
- Cisco 1040 Sensors—You need to complete the tasks listed in [Performing Initial Configuration in Service Monitor for Sensors, page 4-2](#).

Service Monitor reports include data for up to the last 30 days and for up to the licensed number of phones:





- To generate reports, see:
 - [Using the Sensor Report Filter to Specify and Generate a Sensor Report, page 2-4](#)
 - [Using the CVTQ Report Filter to Specify and Generate a CVTQ Report, page 2-7](#)
- To view the license limit and the total number of phones that Service Monitor is monitoring—after having learned of them from clusters and sensors—see [Selecting Sensors and Clusters to Monitor, page 3-8](#).

While using Service Monitor reports, the following information is useful:

- [Understanding Report Tool Buttons, page 2-2](#)
- [Selecting Columns to Display and to Hide on a Service Monitor Report, page 2-3](#)

Understanding Report Tool Buttons

The following report tool buttons might appear in the upper-right corner of Service Monitor reports.

	Exports the current report to a PDF or CSV file to save on your local system. Note Enables you to export data for all records or a range of record numbers.
	Opens a new window with the report formatted for printing from your browser.
	Opens a column selector dialog box from which you can select those columns of a report to hide and those to display. See Selecting Columns to Display and to Hide on a Service Monitor Report, page 2-3 .
	Opens context-sensitive help.

Selecting Columns to Display and to Hide on a Service Monitor Report

By default, sensor reports and CVTQ reports do not display every possible column of data. You can select the data that you would like to display.

Step 1 In the upper-right corner of a report, click the Tools button . A column selector dialog box appears.

Step 2 To restore the report to use columns that are displayed by default, click the **Restore Default Columns** button. The column selector dialog box closes and the report window refreshes, displaying the default columns.

Step 3 To update report columns, do the following:

- To hide a column, place it on the Hidden Column(s) list:
 - Select the column by name from the Displayed Column(s) list.
 - Click the < **Remove** << button. The column appears on the Hidden Column(s) list.



Note To select adjacent columns, hold down the Shift key. To select columns that are not adjacent, hold down the Ctrl key.

- To display a column, place it on the Displayed Column(s) list:
 - Select it by name from the Hidden Column(s) list.
 - Click the < **Add** << button. It appears on the Displayed Column(s) list.

Click **Update**. The report window refreshes, displaying only those columns from the Displayed Column(s) list.



Note Your selections are saved and will affect other users.

Specifying IP Addresses or Directory Numbers for Endpoints

When adding or editing a threshold group, you must specify an endpoint. To do so, you can enter the complete directory number or IP address—whichever is applicable—and you can use wildcards, specifying a range of directory numbers or IP addresses. [Table 2-1](#) provides some examples.

Table 2-1 Endpoint Definition

Threshold Group Type	Type of Endpoint	Examples
CVTQ	Directory number	<ul style="list-style-type: none"> 500 matches 500 only. 5XXX matches 4-digit numbers that start with 5; for example, 5876. <p>Note Enter uppercase X only.</p>
One of these: <ul style="list-style-type: none"> CVTQ Sensor 	IP address	<ul style="list-style-type: none"> 172.20.119.21 matches 172.20.119.21 only. 172.*.*.* matches all IP addresses 172.0.0.1 through 172.255.255.255.

Using Sensor Reports

After Cisco 1040 sensors in your network register to a Service Monitor, they send data to that Service Monitor every 60 seconds for every call underway. Service Monitor retains the data in its database for up to 30 days. Using sensor report filters, you can generate reports that include data for all calls that have been monitored by the sensors or reports that include a subset of data, such as:

- Where MOS was less than a specific value
- When reported from specific sensors
- Where particular codecs were used
- A set of endpoints
- All sensors or a subset of sensors
- Any given time period—from one minute to 30 days—during the last 30 days


Using the Sensor Report Filter to Specify and Generate a Sensor Report

Step 1 Select **Reports > Sensor Filter**. The Cisco 1040 Sensor Report Filter page appears.

Step 2 Do one of the following:

- Click **Generate Report** to generate the report using the default criteria. A report opens in a new window. See [Understanding Sensor Reports, page 2-5](#).
- Change any of the report inputs listed in this table. To be included in the report, data needs to meet each of the criteria that you specify.

Fields	Description/Action
MOS Less than or Equal to	Enter a value from 0.0 to 5.0.
Jitter Greater than or Equal to	Enter the number of milliseconds.
Packet Loss Greater than or Equal to	Enter the percent of packet loss.
Codec	Select a codec from the list.

Fields	Description/Action
Endpoint 1	<p>Enter an exact IP address or use wildcards (*)—or a combination of numbers and wildcards—to specify a range of IP addresses for one of the following:</p> <ul style="list-style-type: none"> • Cisco IP phone • Cisco conference bridge • Cisco voice gateway <p>Note The report will include voice activity from this endpoint whether it is the called endpoint or the caller endpoint.</p> <p>For more information, see Specifying IP Addresses or Directory Numbers for Endpoints, page 2-3.</p>
Endpoint 2	<p>Enter an exact IP address or use wildcards (*)—or a combination of numbers and wildcards—to specify a range of IP addresses for one of the following:</p> <ul style="list-style-type: none"> • Cisco IP phone • Cisco conference bridge • Cisco voice gateway <p>Note The report will include voice activity from this endpoint whether it is the called endpoint or the caller endpoint.</p>
Sensor ID(s)	<p>To select sensors:</p> <ol style="list-style-type: none"> 1. Click . The Select Sensors dialog box appears. 2. Select check boxes. 3. Click OK.
Date and Time	Enter the From date and time and To date and time for the period that you want to report on.

Step 3 Click **Generate Report**. A report opens in a new window.

Understanding Sensor Reports

Sensors listen to RTP voice traffic on Switch Port Analyzer (SPAN) ports that have been configured to mirror voice traffic. Two RTP streams—ingoing and outgoing—make up a single voice call. Depending on the phone ports and the voice VLANs that a SPAN port mirrors, a sensor might listen to only one or both RTP streams, calculating MOS and sending data to Service Monitor at 60-second intervals.

Sensor reports can display the MOS that a sensor calculated for RTP streams on a minute-by-minute basis. For each 60 seconds, a sensor report displays one or two rows of data, depending on whether only one or both RTP streams were mirrored on the SPAN port. Each row identifies the sensor that collected the data, the endpoints involved, MOS, milliseconds of jitter, and the time stamp.

[Table 2-2](#) lists all possible columns of data that can be displayed in a Cisco 1040 Sensor report; by default, not all are displayed. For more information, see [Selecting Columns to Display and to Hide on a Service Monitor Report](#), page 2-3.

Table 2-2 **Sensor Report Contents**

Column	Description
Sensor Name	Descriptive name for the sensor that collected the data and analyzed the MOS. Note The name Cisco 1040 signifies that the sensor has registered to Service Monitor using the default configuration file. To enter another name, see Editing the Configuration for a Specific Sensor, page 4-10 .
Sensor MAC Address	Sensor MAC address.
Speaker Directory Number	Directory number is displayed when the device (see speaker IP address below) is managed by a Cisco Unified CallManager that: <ul style="list-style-type: none"> • Is added to Service Monitor with the proper credentials • Has not been suspended from monitoring
Speaker IP Address	IP address for a voice gateway or an IP phone.
Speaker Device Type	One of these: <ul style="list-style-type: none"> • Voice gateway or Cisco IP phone model number. • N/A—Some error prevents Service Monitor from obtaining the device type. • Unavailable—This is the first time Service Monitor has seen this phone and the device type is not yet known; or the corresponding Cisco Unified CallManager: <ul style="list-style-type: none"> – Has not been added to Service Monitor. – Did not provide a valid device type to Service Monitor.
Listener Directory Number	Directory number is displayed when the device (see listener IP address below) is managed by a Cisco Unified CallManager that: <ul style="list-style-type: none"> • Is added to Service Monitor with the proper credentials • Has not been suspended from monitoring
Listener IP Address	IP address for a voice gateway or an IP phone.
Listener Device Type	One of these: <ul style="list-style-type: none"> • Voice gateway or Cisco IP phone model number. • N/A—Some error prevents Service Monitor from obtaining the device type. • Unavailable—This is the first time Service Monitor has seen this phone and the device type is not yet known; or the corresponding Cisco Unified CallManager: <ul style="list-style-type: none"> – Has not been added to Service Monitor. – Did not provide a valid device type to Service Monitor.
MOS	Average MOS value during this 60-second period. Note When voice activity detection (VAD) is enabled on a voice gateway, lower MOS values are seen for streams between the gateway and IP phones.

Table 2-2 *Sensor Report Contents (continued)*

Column	Description
Cause	Reason for lowering MOS; one of these: <ul style="list-style-type: none"> • Jitter • Packet loss
Codec	Codec used.
Time Stamp	Date and time at the start of this 60-second period.
Jitter (ms)	Milliseconds of jitter during this 60-second period.
Packet Loss (%)	Percentage of packet loss during this 60-second period.

Using CVTQ Reports

If you have configured Service Monitor to receive data from Cisco Unified CallManager clusters, Service Monitor retains that data in its database for up to 30 days. Using CVTQ report filters, you can generate reports that include all call data from the clusters or reports that include a subset of call data, such as:

- Where MOS was less than a specific value
- When reported from specific clusters
- Where particular codecs were used
- A set of endpoints
- All clusters or a subset of clusters
- Any given time period—from one minute to 30 days—during the last 30 days


Using the CVTQ Report Filter to Specify and Generate a CVTQ Report

Step 1 Select **Reports > CVTQ Filter**. The CVTQ Report Filter page appears.

Step 2 Do one of the following:

- Click **Generate Report** to generate the report using the default values as displayed on the page. A report opens in a new window. See [Understanding CVTQ Reports, page 2-8](#).
- Change any of the report inputs listed in this table. To be included in the report, data needs to meet each of the criteria that you specify.

Fields	Description/Action
MOS Less than or Equal to	Enter a number from 0.0 to 5.0.
Jitter Greater than or Equal to	Enter the number of milliseconds.
Packet Loss Greater than or Equal to	Enter the percent of packet loss.
Codec	Select a codec from the list.

Fields	Description/Action
Concealment seconds Greater than or Equal to	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds, that is total number of seconds that have more than 5 percent concealment frames).
Concealment ratio Greater than or Equal to	Cumulative ratio of concealment frames to total frames observed after starting a call.
Endpoint 1	Specify called or caller endpoints by selecting one of these radio buttons and entering the appropriate data: <ul style="list-style-type: none"> • DN—Directory number. Enter an exact directory number or use wildcards (X)—or a combination of numbers and wildcards—to specify a range of directory numbers. • IP—IP address. Enter an exact IP address or use wildcards (*)—or a combination of numbers and wildcards—to specify a range of IP addresses. <p>Note To enter a wildcard, you must enter uppercase X. For more information, see Specifying IP Addresses or Directory Numbers for Endpoints, page 2-3.</p>
Endpoint 2	Specify called or caller endpoints by selecting one of these radio buttons and entering the appropriate data: <ul style="list-style-type: none"> • DN—Directory number. Enter an exact directory number or use wildcards (X)—or a combination of numbers and wildcards—to specify a range of directory numbers. • IP—IP address. Enter an exact IP address or use wildcards (*)—or a combination of numbers and wildcards—to specify a range of IP addresses. <p>Note To enter a wildcard, you must enter uppercase X.</p>
Cluster ID(s)	To select clusters: <ol style="list-style-type: none"> 1. Click . The Select Clusters dialog box appears. 2. Select check boxes. 3. Click OK.
Call Termination Date and Time	Enter the From date and time and To date and time for the period that you want to report on.

Step 3 Click **Generate Report**. A report opens in a new window. See [Understanding CVTQ Reports](#), page 2-8.

Understanding CVTQ Reports

Table 2-3 lists all possible columns of data that can be displayed in a CVTQ report; by default, not all are displayed. For more information, see [Selecting Columns to Display and to Hide on a Service Monitor Report](#), page 2-3.

**Note**

The report displays two lines for each call: one with data for the listening experience at the called endpoint and another line for the caller endpoint.

Table 2-3 CVTQ Report Contents

Column	Description
Cluster ID	Cisco Unified CallManager cluster ID.
Caller	<ul style="list-style-type: none"> • Directory Number—Directory number where the call was made. • IP Address—IP address from which the call originated. • Device Type—Type of device making the call; one of these: <ul style="list-style-type: none"> – IP address of a voice gateway – Model number of a Cisco IP phone
Called	<ul style="list-style-type: none"> • Directory Number—Directory number where the call was received. • IP Address—Destination IP address for the call. • Device Type—Type of device receiving the call; one of these: <ul style="list-style-type: none"> – IP address of a voice gateway – Model number of a Cisco IP phone
Listener DN/IP	<p>Identifies the endpoint—called or caller—for which MOS and impairment details are relevant; one of these:</p> <ul style="list-style-type: none"> • IP address of the listener • Directory number of the listener
MOS	<p>Average MOS value during the call, or Unavailable if this data was not available from the cluster; not all IP phones, voice gateways, and Cisco Unified CallManager versions provide MOS. For more information, see <i>Release Notes for Cisco Unified Service Monitor 2.0</i>.</p> <p>Note When VAD is enabled on a voice gateway, lower MOS values might be seen on calls between the gateway and IP phones. For more information, see Configuring Voice Gateways When VAD is Enabled, page B-8.</p>
Codec	Codec used in the call.
Time Stamp	Date and time of the call.
Call Duration [h][m]s	Total hours, minutes, and seconds in the call.

Table 2-3 CVTQ Report Contents (continued)

Column	Description
Impairment Details	<ul style="list-style-type: none"> • Jitter (ms)—Milliseconds of jitter during the call. • Packet Loss (%)—Percentage of packet loss during the call. • Concealment Seconds—Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds). • Severely Concealed Seconds—Number of seconds during which a significant amount of concealment (greater than fifty milliseconds) was observed. • Concealment Ratio—Ratio of concealment frames to total frames.
Call Release Code	<ul style="list-style-type: none"> • Caller Termination Cause—Code that indicates why the call was terminated on the caller endpoint. • Called Termination Cause—Code that indicates why the call was terminated on the called endpoint. <p>For more information, see one of the following:</p> <ul style="list-style-type: none"> • Call Release Codes in <i>Call Detail Record Definitions for Cisco Unified CallManager 5.0(2)</i> • Cause Codes in <i>Cisco CallManager 4.2(1) Call Detail Record Definition</i> <p>You can find these documents at this URL:</p> <p>http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html</p>

Using Most-Impacted Endpoints Reports

Every day at 1am Service Monitor analyzes the stored call data to determine the endpoints where the greatest number of violations occurred during the previous day—from 00:00:00 until 23:59:59:999. Service Monitor stores the result of this analysis in the database for display in most-impacted endpoints reports. Subsequent to the analysis, Service Monitor optionally exports daily and weekly (on Monday) most-impacted endpoints reports, storing them on the server.

By default, Service Monitor determines the 10 most-impacted endpoints and does not export the most-impacted endpoints reports. To change the number of most-impacted endpoints that Service Monitor reports on and to configure automatic export, see [Configuring Number of Endpoints and Export Settings for Impacted Endpoints Reports](#), page 3-11.

This section includes the following topics:

- [Generating and Understanding the Sensor Most-Impacted Endpoints Report](#), page 2-11
- [Generating and Understanding the CVTQ Most-Impacted Endpoints Report](#), page 2-11

Generating and Understanding the Sensor Most-Impacted Endpoints Report


Note

By default, 10 endpoints are included on Most-Impacted Endpoints reports. For more information, see [Configuring Number of Endpoints and Export Settings for Impacted Endpoints Reports, page 3-11](#).

Step 1

To generate the Cisco 1040 Sensor Most-Impacted Endpoints report, select **Reports > Sensor: Impacted Endpoints**. The report opens in a new window.

The Cisco 1040 Sensor Most-Impacted Endpoints report displays the data listed in [Table 2-4](#).

Table 2-4 Cisco 1040 Sensor Most-Impacted Endpoint Report Contents

Column	Description
Endpoint	One of these: <ul style="list-style-type: none"> • Directory number. • IP address for an IP phone, voice gateway, or conference bridge.
Device Type	Voice Gateway or, if a phone, the Cisco phone model is displayed. Note Service Monitor displays Unavailable if the corresponding Cisco Unified CallManager has not been added to Service Monitor or has returned an invalid device type.
Cumulative Talk Time (min)	Cumulative duration of speech through this endpoint during the report time period. Note When launched from the Reports tab, the report includes data from the previous day—from 00:00:00 until 23:59:999. If configured, you can examine a weekly report that has been exported to the server. For the location of exported reports, see Configuring Number of Endpoints and Export Settings for Impacted Endpoints Reports, page 3-11 .
Impaired Minutes	Number of minutes during which MOS was below a threshold through this endpoint.
% of Impaired Minutes	Impaired minutes as a percentage of all minutes.
Average MOS	Average MOS value during cumulative talk time. Note When VAD is enabled on a voice gateway, lower MOS values are seen for streams between the gateway and IP phones.

Generating and Understanding the CVTQ Most-Impacted Endpoints Report


Note

For information about configuring the number of endpoints to include in Most-Impacted Endpoints reports, see [Configuring Number of Endpoints and Export Settings for Impacted Endpoints Reports, page 3-11](#).

- Step 1** To generate the CVTQ Most-Impacted Endpoints report, select **Reports > CVTQ: Impacted Endpoints**. The report opens in a new window.

The CVTQ Most-Impacted Endpoints report displays the data listed in [Table 2-5](#).

Table 2-5 CVTQ Most-Impacted Endpoints Report Contents

Column	Description
Endpoint	One of these: <ul style="list-style-type: none"> • Directory number. • IP address for an IP phone, voice gateway, or conference bridge.
IP Address	Endpoint IP address.
Device Type	Voice Gateway or, if a phone, the Cisco phone model is displayed.
Cumulative Talk Time (min)	Cumulative duration of all calls through this endpoint during the report time period. <p>Note When launched from the Reports tab, the report includes data from the previous day—from 00:00:00 until 23:59:59.999. If configured, you can examine a weekly report that has been exported to the server. For the location of exported reports, see Configuring Number of Endpoints and Export Settings for Impacted Endpoints Reports, page 3-11</p>
# of Calls	Number of calls through this endpoint during the report time period.
Impaired Calls	Number of impaired calls through this endpoint during the report time period.
% of Impaired Calls	Impaired calls as a percentage of calls during the report time period.
Average MOS	Average MOS value during cumulative talk time or Unavailable if this data was not available from the cluster; not all IP phones, voice gateways, and Cisco Unified CallManager versions provide MOS. For more information, see <i>Release Notes for Cisco Unified Service Monitor 2.0</i> . <p>Note When VAD is enabled on a voice gateway, lower MOS values might be seen on calls between the gateway and IP phones. For more information, see Configuring Voice Gateways When VAD is Enabled, page B-8.</p>