



Configuring Service Monitor

The following topics are included:

- [Configuring Trap Receivers, page 3-1](#)
- [Understanding and Setting Cisco Unified CallManager Credentials, page 3-2](#)
- [Selecting Sensors and Clusters to Monitor, page 3-8](#)
- [Configuring Other Settings, page 3-12](#)



Note

For more information, see [Managing Sensors, page 4-1](#) and [Configuration Checklists and Tips, page A-1](#).

Configuring Trap Receivers

Step 1 Select **Configuration > Trap Receivers**. The Trap Receiver Parameters page appears.

Step 2 Enter the data described in the following table.

GUI Element	Description/Action
SNMP Community String	Enter the SNMP community string for each trap receiver.
Trap Receiver <i>n</i> and Port fields (where <i>n</i> is a number from 1 to 4)	<p>Enter up to 4 trap receivers:</p> <ul style="list-style-type: none"> • Trap Receiver <i>n</i>—Enter the IP address or DNS name of a server. If you want to use Operations Manager to act on and display data from Service Monitor—for example to use the Service Quality Alerts dashboard—specify the IP address for the system with Operations Manager. • Port—Enter the port number on which the receiver listens for SNMP traps. The default is 162; however, a different port might be used for this purpose on this server. <p>When Service Monitor generates SNMP traps, it forwards them to these receivers.</p>

Step 3 Click **OK**.

Understanding and Setting Cisco Unified CallManager Credentials

Service Monitor can obtain and analyze voice data from supported versions of Cisco Unified CallManager. For Service Monitor to do this, you must:

1. Perform configuration tasks either using Cisco Unified CallManager or logged in to the system where Cisco Unified CallManager is installed. See [Cisco Unified CallManager Configuration, page B-1](#).
2. Add Cisco Unified CallManager credentials to Service Monitor using the following procedure.

Step 1 Select **Configuration > CallManager Credentials**. The CallManager Credentials page displays the information in the following table.

Columns or Buttons	Description/Action
Display Name	The user-specified name entered when credentials were added to Service Monitor.
IP Address	Cluster IP address.
Cluster	<ul style="list-style-type: none"> Version—Cisco Unified CallManager software version. ID—ID assigned to the cluster by the Cisco Unified CallManager.
Last Contact Status	<p>Status for these credentials:</p> <ul style="list-style-type: none"> HTTP/S CDR/CDRM DB Device DB <p>Note The CDRM database resides on a Cisco Unified CallManager 5.x system. Service Monitor should have access to the credentials for this database after providing HTTP/S credentials.</p> <p>One of the following statuses will be displayed for each set of credentials:</p> <ul style="list-style-type: none"> Success—Link. If you click the link, you can check when the last successful contact occurred. <p>Note Clicking a status link opens a dialog with more information, including the last time Service Monitor tried to contact the Cisco Unified CallManager and the last time Service Monitor was successful in making contact.</p> <ul style="list-style-type: none"> Verifying—Click the link for more information. Failure—Click the link for more information. Blank—This credential is not required for Service Monitor to obtain information from this version of the Cisco Unified CallManager. <p>For more information, see Understanding Last Contact Status and When to Verify Credentials, page 3-7.</p>
Buttons	<ul style="list-style-type: none"> Add—Add credentials for a Cisco Unified CallManager cluster. See Adding Cisco Unified CallManager Credentials, page 3-4. Edit—Edit credentials for a Cisco Unified CallManager cluster. See Adding Cisco Unified CallManager Credentials, page 3-4. Delete—See Deleting Cisco Unified CallManager Credentials, page 3-8. Verify—Verify credentials for a selected Cisco Unified CallManager cluster. Refresh—Refresh the page.

Cisco Unified CallManager Versions Supported

For the list of Cisco Unified CallManager versions that Service Monitor supports, see *Release Notes for Cisco Unified Service Monitor 2.0*.

Adding Cisco Unified CallManager Credentials



Note

For Cisco Unified CallManager 5.x, in addition to adding credentials using the following procedure, you must also provide an SFTP password. See [Configuring Other Settings, page 3-12](#).



Caution

Before adding credentials for a Cisco Unified CallManager 5.x software version cluster, confirm that the cluster ID does not include a space. For more information, see *Release Notes for Cisco Unified Service Monitor 2.0*.

- Step 1** Select **Configuration > CallManager Credentials**. The CallManager Credentials page appears.
- Step 2** Click **Add**. The Add CallManager dialog box appears.
- Step 3** Enter the data described in the following table.

Field	Description
Display Name	Enter a name—up to 20 characters—to describe the cluster.
Host Name	(Optional) Enter the host name for the server where Cisco Unified CallManager is installed. Note You must enter the host name of the Cisco Unified CallManager if the Service Monitor server cannot resolve the Cisco Unified CallManager host name to an IP address. This problem can occur if incorrect DNS parameters are specified on the Service Monitor server or if the Cisco Unified CallManager host name has not been updated in DNS.

Field	Description
IP Address	Enter the IP address for appropriate node in the cluster; for this software version: <ul style="list-style-type: none"> • 3.3.x—Enter the IP address for the publisher • 4.x—Enter the IP address for the publisher • 5.x—Enter the IP address for a publisher or a subscriber
Version	Select the software version running on the cluster from these: <ul style="list-style-type: none"> • 3.3.x • 4.x • 5.x <p>Note For more information, see Cisco Unified CallManager Versions Supported, page 3-4.</p> <p>Depending on the selected software version, you will need to enter one or more usernames and passwords, described in Step 4.</p>

Step 4 Enter usernames and passwords.

Note When there are multiple Cisco Unified CallManagers in a cluster, you need only supply credentials for the publisher server.

The usernames and passwords that are required vary by Cisco Unified CallManager version:

- 3.3.x:
 - CDR DB User Name and Password/Re-enter password—Enter the username and password for a Microsoft SQLServer account on the server where the Cisco Unified CallManager publisher is installed. This account must have access to the CDR database and, optionally, to the device database. For more information, see [Adding Microsoft SQLServer User Accounts, page B-7](#).
 - Device DB User Name and Password/Re-enter password—Enter the username and password for a Microsoft SQLServer account on the server where the Cisco Unified CallManager publisher is installed; this account must have access to the device database. For more information, see [Adding Microsoft SQLServer User Accounts, page B-7](#).



Note The username and password for the CDR database and the device database will be the same if you have configured one Microsoft SQLServer account to access both databases.

- 4.x:
 - CDR DB User Name and Password/Re-enter password—Enter the username and password for a Microsoft SQLServer account on the server where the Cisco Unified CallManager publisher is installed; this account must have access to the CDR database. For more information, see [Adding Microsoft SQLServer User Accounts, page B-7](#).
 - HTTP/S User Name and Password/Re-enter password—Enter a username and password that can be used to log in to Cisco Unified CallManager Administration.



Note You need only supply this username and password for the Cisco Unified CallManager publisher server.

- 5.x:
 - HTTP/S User Name and Password/Re-enter password—Enter a username and password that can be used to log in to Cisco Unified CallManager Administration on the publisher server. The user role must have Standard AXL API Access privilege.



Note You need only supply this username and password for the Cisco Unified CallManager publisher server.

Step 5 Click **OK**.

Editing Cisco Unified CallManager Credentials

Step 1 Select **Configuration > CallManager Credentials**. The CallManager Credentials page appears.

Step 2 Select a cluster and click **Edit**. The Edit CallManager dialog box appears.

Step 3 Enter the data described in the following table.

Field	Description
Display Name	Enter a name—up to 20 characters—to describe the cluster.
Host Name	Host name for the server where Cisco Unified CallManager is installed. Note If Service Monitor successfully retrieves the hostname from Cisco Unified CallManager, it is displays here, replacing any previously supplied hostname.
IP Address	This field is grayed out because you cannot edit it.
Version	The software version: <ul style="list-style-type: none"> • 3.3.x • 4.x • 5.x Note You cannot change the version by editing.

Step 4 Enter usernames and passwords for the selected Cisco Unified CallManager version:

- 3.3.x:
 - CDR DB User Name and Password/Re-enter password—Enter the username and password for a Microsoft SQLServer account on the server where the Cisco Unified CallManager is installed. This account must have access to the CDR database and, optionally, to the device database. For more information, see [Adding Microsoft SQLServer User Accounts, page B-7](#).

- Device DB User Name and Password/Re-enter password—Enter the username and password for a Microsoft SQLServer account on the server where the Cisco Unified CallManager is installed; this account must have access to the device database. For more information, see [Adding Microsoft SQLServer User Accounts, page B-7](#).



Note The username and password for the CDR database and the device database will be the same if you have configured one Microsoft SQLServer account to access both databases.

- 4.x:
 - CDR DB User Name and Password/Re-enter password—Enter the username and password for a Microsoft SQLServer account on the server where the Cisco Unified CallManager is installed; this account must have access to the CDR database. For more information, see [Adding Microsoft SQLServer User Accounts, page B-7](#).
 - HTTP/S User Name and Password/Re-enter password—Enter a username and password that can be used to log in to Cisco Unified CallManager Administration.
- 5.x:
 - HTTP/S User Name and Password/Re-enter password—Enter a username and password that can be used to log in to Cisco Unified CallManager Administration. The user role must have Standard AXL API Access privilege.

Step 5 Click **OK**.

Understanding Last Contact Status and When to Verify Credentials

Service Monitor needs one or more credentials to obtain Cisco Unified CallManager data successfully. The CallManager Credentials page displays the status of the last contact between Service Monitor and Cisco Unified CallManagers.

In a few cases, you might need to correct credentials on the Cisco Unified CallManager and then verify the credentials from Service Monitor:

- When the last contact status is Successful, in some cases, Service Monitor might not be receiving data, but simply waiting to receive data. To see when the last successful contact occurred, click the status link. If the last contact was not recent, correct any problem with credentials on the Cisco Unified CallManager and verify the credentials from Service Monitor.
- Credentials that Service Monitor relies upon might change on the Cisco Unified CallManager platform. If this happens, check with your Cisco Unified CallManager administrator to obtain the correct credentials. If necessary, update the credentials in Service Monitor. Otherwise, verify the credentials.



Note To determine whether known problems have been identified that could prevent successful data exchange between a cluster and Service Monitor, see *Release Notes for Cisco Unified Service Monitor 2.0*.

Procedure

Step 1 Select **Configuration > CallManager Credentials**. The CallManager Credentials page appears.

- Step 2** Select the Cisco Unified CallManager for which you want to verify credentials.
- Step 3** Click **Verify**.

For more information, see the following topic:

- [Cisco Unified CallManager Configuration, page B-1](#)

Deleting Cisco Unified CallManager Credentials

After you complete this procedure, Service Monitor can no longer obtain voice quality transmission data for the related cluster. Additionally, the cluster will no longer appear on the Monitored Phones page. Call data for the cluster remains in the database until it is purged. For more information, see [Understanding Service Monitor Database Purging, page 6-1](#).

Before you complete this procedure, delete the cluster from any CVTQ threshold groups. See [Editing a CVTQ Threshold Group, page 5-6](#).

-
- Step 1** Select **Configuration > CallManager Credentials**. The CallManager Credentials page appears.
- Step 2** Select the check box by the cluster that you want to delete.
- Step 3** Click **Delete**. One of the following occurs:
- A confirmation dialog box appears.
 - An error message appears, displaying a list of CVTQ threshold groups to which the cluster belongs. You will need to remove the cluster from these CVTQ threshold groups and repeat this procedure.
- Step 4** Click **OK**.
-

Selecting Sensors and Clusters to Monitor

On the Monitored Phones page, you can view the total number of phones that Service Monitor is monitoring. You can also view the names of all sensors and Cisco Unified CallManager clusters known to Service Monitor, see whether each is monitored, and, if so, see the number of phones that Service Monitor manages in the cluster or for the sensor.



Note

Because it is possible for a Cisco Unified CallManager cluster and a sensor to report MOS for some of the same phones:

- The total known phone count displayed on the Monitored Phones page might be less than the sum of known phone counts for clusters/sensors.
 - To decrease the total known phone count, you might need to suspend more than one cluster or sensor.
-

Step 1 Select **Configuration > Monitored Phones**. The Monitored Phones page appears, displaying the information in the following table.

GUI Element	Description
Total known phone count: (<i>n</i>)	Number of phones that Service Monitor is monitoring. If the number of phones equals the license size, the following message is displayed in red: Total known phone count (<i>n</i>) has reached or exceeded licensed limit! For more information, see Determining License Size Exceeded, page D-3 .
License limit: (<i>n</i>)	Number of phones allowed by license.
Cluster/Sensor List	
Cluster/Sensor ID column	One of the following: <ul style="list-style-type: none"> Cluster ID—The cluster ID is assigned by Cisco Unified CallManager. Sensor ID—Sensor MAC address.
Version column	Software version of Cisco Unified CallManager.
Type	One of the following: <ul style="list-style-type: none"> Cluster Sensor
State column	One of these: <ul style="list-style-type: none"> Monitored—Service Monitor is collecting and analyzing data from this cluster or sensor and sending traps when violations occur. Suspended—Service Monitor is not collecting and analyzing data from this cluster or sensor for one of these reasons: <ul style="list-style-type: none"> A user set the state of the cluster or sensor to Suspended. See Suspending and Resuming a Cluster or Sensor from Monitoring, page 3-9. Service Monitor could not monitor any more newly created clusters or phones when data was received because the phone license count was reached.
Known Phone Count	Number of phones that have made calls (in the cluster or monitored by the sensor) and are, therefore, known and being monitored by Service Monitor.

Suspending and Resuming a Cluster or Sensor from Monitoring

Provided that Cisco Unified CallManager is configured properly and Service Monitor license limits are not exceeded, Service Monitor starts to monitor a cluster when it learns of the cluster. Service Monitor learns of a cluster when you add Cisco Unified CallManager credentials to Service Monitor. (For more information, see [Adding Cisco Unified CallManager Credentials, page 3-4](#).)

Service Monitor learns of a sensor when the sensor registers.

If you want to suspend a cluster or a sensor from monitoring—for example, to enable you to monitor phones from a different cluster or sensor—you can do so.

Suspending a Cluster or Sensor

When you suspend a cluster or sensor, the following occurs:

- Data for the suspended cluster or sensor no longer appears in Service Monitor reports.
- The cluster or sensor appears on the Monitored Phones page as Suspended and the known phone count for that cluster or sensor drops to zero (0). If, as a result, the total known phone count also decreases, you are free to monitor additional phones in other clusters or from other sensors (up to your license limit).

-
- Step 1** Select **Configuration > Monitored Phones**.
 - Step 2** Select the check box for the cluster or sensor that you want to suspend.
 - Step 3** Click **Suspend**. A confirmation dialog box appears.
 - Step 4** Click **OK**.
-

Resuming a Cluster or Sensor

-
- Step 1** Select **Configuration > Monitored Phones**.
 - Step 2** Select the check box for a suspended cluster or sensor that you want to monitor.
 - Step 3** Click **Resume**. A confirmation dialog box appears.
 - Step 4** Click **OK**.
-

Updating the Total Known Phone Count for a Cluster

Service Monitor monitors the first n phones that it finds in the data that it receives or obtains from the clusters. If a phone in a cluster fails and is replaced, Service Monitor is not notified and continues to include the failed phone in the total known phone count. To refresh the total known phone count for a cluster, suspend the cluster and resume it.

**Note**

Suspending a cluster resets the phone count to zero for that cluster. The phone count then increases as and when calls come from a phone.

Configuring Number of Endpoints and Export Settings for Impacted Endpoints Reports

Use this procedure to configure:

- The number of endpoints to be included in CVTQ and sensor most-impacted endpoint reports no matter when they run—daily, weekly, or on demand.
- The most-impacted endpoints reports to export—CVTQ or sensor or both. Most-impacted endpoint reports can run daily and weekly, exporting the results to a comma-separated values file (CSV) or a portable document format (PDF) file. You can save the reports on the server and, optionally, automatically send them through e-mail.

Step 1 Select **Configuration > Export Settings**. The Export Settings (for Most Impacted Endpoint) page appears, displaying the information described in the following table.

GUI Element	Description/Action
Number of Endpoints field	Enter the number of endpoints that you want to see on all—exported or directly launched—most-impacted endpoints reports.
Daily at 1:00 AM check boxes	To generate the report every day, select at least one of the following: <ul style="list-style-type: none"> • CSV check box—Save the report in CSV format. • PDF check box—Save the report in PDF format. If neither is selected, Service Monitor does not generate the reports.
Weekly at 1:00 AM Monday check boxes	To generate the report every week, select at least one of the following: <ul style="list-style-type: none"> • CSV check box—Save the report in CSV format. • PDF check box—Save the report in PDF format. If neither is selected, Service Monitor does not generate the reports.
Report Type	Select at least one of the following: <ul style="list-style-type: none"> • Sensor • CVTQ Note Separate reports are generated for sensor and CVTQ data. For report filenames, see Table 3-1 .
Save at	Enter a location for storing the reports on the server where Service Monitor is installed; a default location is displayed.
E-mail to	(Optional) Enter one or more complete e-mail addresses separated by commas.
SMTP Server	(Optional) Enter an SMTP server.

Step 2 Click **Apply**.

Depending on the reports and formats that you have selected, the following reports will be generated.

Table 3-1 Most-Impacted Endpoints Exported Reports


Report Type	When Generated	Report Filenames
CVTQ	Daily	CVTQ_Daily_ddmmyyyy.csv
		CVTQ_Daily_ddmmyyyy.pdf
	Weekly Note Generated on Monday.	CVTQ_Weekly_ddmmyyyy.csv
		CVTQ_Weekly_ddmmyyyy.pdf
Sensors	Daily	Sensor_Daily_ddmmyyyy.csv
		Sensor_Daily_ddmmyyyy.pdf
	Weekly Note Generated on Monday.	Sensor_Weekly_ddmmyyyy.csv
		Sensor_Weekly_ddmmyyyy.pdf

Configuring Other Settings

Configure these settings if you are monitoring calls from a Cisco Unified CallManager version 5.x.

Step 1 Select **Configuration > Other Settings**. The Other Settings page appears.

Step 2 Enter information described in the following table.

Fields	Description/Action
SFTP	
Username	You cannot change the username from smuser. This same username, smuser, must be configured in Cisco Unified CallManager. See Adding Service Monitor to Cisco Unified CallManager 5.x as a Billing Server, page B-4 .
Change password check box	Select to change password. <div style="display: flex; align-items: center;"> <div style="text-align: center; margin-right: 10px;">  Caution </div> <div>The default password is smuser. If you change the password here, you must also change the password for smuser in Cisco Unified CallManager. See Adding Service Monitor to Cisco Unified CallManager 5.x as a Billing Server, page B-4.</div> </div>
Password	Enter password.
Re-enter password	Re-enter password.

Step 3 Click **Apply**.