CHAPTER 3

Configuring Service Monitor

The following topics are included:

Note For more information, see Managing Cisco 1040s, page 4-1 and Configuration Checklists and Tips, page A-1.

Configuring Trap Receivers

For the SNMP traps that Service Monitor sends, see MIBs Used and SNMP Traps Generated, page D-1.

Step 1 Select **Administration > 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 *n* and Port fields (where *n* is a number from 1 to 4)	Enter up to 4 trap receivers: • Trap Receiver *n*—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. Change this value to 9005, if you face any issues. When Service Monitor generates SNMP traps, it forwards them to these receivers.

Step 3 Click **OK**.

Understanding and Setting Data Source Credentials

Service Monitor collects data from Unified Communications Manager clusters and sensors (Cisco 1040s and NAMs). You do not need to enter credentials for Cisco 1040s; to enable data collection for them, see Managing Cisco 1040s, page 4-1. However, for NAMs and Unified Communications Manager publisher servers, you must:

- Provide Service Monitor with credentials.
- Keep the credentials up-to-date. (Any time you update credentials on a NAM or on a Unified Communications Manager publisher server, you must also update the corresponding credentials in Service Monitor.)

To view the Data Source Management page, select **Administration > Configuration > Data Source Management**. The Data Source Management page displays:

- As of—The date and time that you opened or last refreshed the page.
- A message if no SMTP server is configured—For more information, see Enabling E-Mail Notifications, page 6-7.

The Data Source Management page also displays the information in the following table.

Columns or Buttons	Description/Action
Display Name	The name that you entered when you added the credentials to Service Monitor.
IP Address	IP address of the cluster or the NAM. To go to the NAM software login page, click the IP address for the NAM.
Type	The data source type; one of these: • CCM—Unified Communications Manager cluster. • NAM—Network Analysis Module.
Version	Unified Communications Manager or NAM software version. For more information, see Supported Data Source Software Versions, page 3-8.
ID	Depends on the data source type: • For CCM—ID assigned to the cluster by Unified Communications Manager. • For NAM—IP address.
Credentials	The status of the credentials that Service Monitor uses to contact the data source (Unified Communications Manager cluster or NAM). Click the status for more information about the credentials; see Viewing Additional Information About Credentials, page 3-4.
Status	The status of data collection: • Configuration Collection—Status of the most recent attempt by Service Monitor to obtain configuration data such as device types and gateways. Click the link for more information; see Viewing More Information About Configuration Collection Status, page 3-5. (Service Monitor collects configuration data from Unified Communications Manager nightly. For more information, see Initiating Configuration Data Collection, page 3-7.) • Call Data—Status or date and time that Service Monitor last received or obtained call data. Click the link for more information; see Viewing More Information About Call Data Status, page 3-5.

Columns or Buttons	Description/Action
Customer	The customer name. This column appears only if you are using Service Monitor in MSP Network Deployment mode.
Buttons	• Add—See Adding Data Source Credentials, page 3-8. • Edit—See Editing Data Source Credentials, page 3-13. • Delete—See Deleting Data Source Credentials, page 3-15. • Verify—Verify credentials for a selected Unified Communications Manager cluster. See Using Data Source Credentials to Troubleshoot Problems and Verify Credentials, page 3-5 and Initiating Configuration Data Collection, page 3-7. • Refresh—Refresh the page. **Note** Do not add, edit, or verify Unified Communications Manager 4.x credentials while Cisco Prime Unified Provisioning Manager (Provisioning Manager) synchronizes with Unified Communications Manager. For more information, see Avoiding Credential Failure When Provisioning Manager Synchronization Runs in Your Network, page 3-13.

Viewing Additional Information About Credentials

This is an example of information displayed when you click the link in the Credentials column:

```
Credential Type: HTTP/S
Current Status: Success
IP Address: 172.25.109.24
Last Contact Time: Wed 03-Feb-2010 14:46:39 PST
Information: Hostname was updated
```

Table 3-1 lists the credential types associated with data sources.

Table 3-1 Credential Types

Data Source Type	Credential Types
CCM	• HTTP/S—Indicates status of authentication to Unified Communications Manager Administration on the publisher server; applicable to Unified Communications Manager 4.x and later. (N/A appears in this column if the data source type is NAM.) • CDR/CDRM DB—Indicates status of authentication to one of these databases: – CDR—Applicable to Unified Communications Manager 4.x. – CDRM—Applicable to Unified Communications Manager 6.x and later. Service Monitor should gain access to the credentials for this database after providing the correct HTTP/S credentials. (N/A appears in this column if the data source type is NAM.)
NAM	• HTTP/S—Indicates the status of authentication to the NAM. (N/A appears in this column if the data source type is CCM.)

Viewing More Information About Configuration Collection Status

This is an example of information displayed when you click the Configuration Collection status link:

```
Type: Configuration Data Collection
Current Status: Success
IP Address: 172.20.119.214
Last Attempt Time: Thu 04-Feb-2010 01:05:00 PST
Last Success Time: Thu 04-Feb-2010 01:05:16 PST
Information:
```

Note If the current status is not Success, check the Information line for help.

For more information, see Initiating Configuration Data Collection, page 3-7.

Viewing More Information About Call Data Status

This is an example of information displayed when you click the Call Data status link:

```
Current Status: Success
IP Address: 172.20.119.214
Last Contact Time: Thu 04-Feb-2010 15:43:00 PST
Last Data Received Time: Tue 02-Feb-2010 12:08:38 PST
Information:
```

If the current status is not Success, check the Information line for help.

For more information, see Using Data Source Credentials to Troubleshoot Problems and Verify Credentials, page 3-5.

Using Data Source Credentials to Troubleshoot Problems and Verify Credentials

Any problem that prevents Service Monitor from contacting and connecting to data sources can interrupt the collection and analysis of call data and configuration data. Use the information on the Data Source Management page to:

- Verify that credentials are valid and that Service Monitor is actively obtaining data.
- Troubleshoot if you notice potential problems with data source credential status or with reports (such as an unusual time gap).

Step 1 Obtain more information by clicking the status links on the Data Source Management page:

- Viewing Additional Information About Credentials, page 3-4
- Viewing More Information About Configuration Collection Status, page 3-5
- Viewing More Information About Call Data Status, page 3-5

The information that you obtain could explain the problem or indicate the need for troubleshooting.

Step 2 Perform some troubleshooting:

- For a NAM—Check whether the:
  - Credentials on a NAM have changed; if so, update the credentials in Service Monitor.
  - NAM is reachable; if not, take steps to ensure that the NAM is reachable.
- For a CCM—Do the following:

- Confirm that the last successful contact Service Monitor had with the cluster was recent. When the last contact status is Success, in some cases, Service Monitor might not be receiving data, but simply waiting to receive data.
- Verify that credentials for the cluster on Unified Communications Manager match those in Service Monitor, and correct, if necessary.
- Verify that DNS parameters are specified correctly on the Service Monitor server and the Unified Communications Manager hostname has been added to DNS. (Service Monitor must be able to resolve the IP address for Unified Communications Manager to obtain the correct name.)
- Check whether any known problems exist that prevent successful data exchange between a cluster and Service Monitor; see *Release Notes for Cisco Prime Unified Service Monitor*.
- Wait or take preventive action when the call data status shows that Service Monitor is discarding data. Service Monitor discards data when receiving old data from Unified Communications Manager 6.x and later. This can happen after the connection between Service Monitor and Unified Communications Manager is reestablished after a break. Unified Communications Manager first sends old files to Service Monitor.

  Note For Unified Communications Manager 7.x and later, you can prevent old data from being sent to Service Monitor. For more information, see Adding Service Monitor to Unified Communications Manager 6.x and Later as a Billing Server, page B-4. For Unified Communications Manager software versions that Service Monitor supports, see *Cisco Prime Unified Service Monitor 8.7 Compatibility Matrix*.

- Credentials that Service Monitor relies upon might change on a Unified Communications Manager platform. If this happens, check with your Unified Communications Manager administrator to obtain the correct credentials. If necessary, update the credentials in Service Monitor.

Step 3 Verify the credentials:

Note Do not verify credentials for Unified Communications Manager 4.x while Provisioning Manager synchronization is running. See Avoiding Credential Failure When Provisioning Manager Synchronization Runs in Your Network, page 3-13.

a. Select **Administration > Configuration > Data Source Management**. The Data Source Management page appears.

b. Select the data source for which you want to verify credentials.

c. Click **Verify**. If the Configuration Data Collection dialog box appears, do one of the following:

   Click **Verify Credentials** to verify credentials only.

   Click **Verify Credentials and Collect Data** to verify credentials and collect configuration data from Unified Communications Manager. For more information, see Initiating Configuration Data Collection, page 3-7.

Sometimes during the addition of CCM or during a scheduled discovery, the following issues are seen:

- CCM is present in Operations Manager, but not in the Data Source Management UI of Service Monitor
- A CCM that is already added, does not respond during a scheduled discovery of devices. The Credentials verification state of the CCM remains in the `Verifying...` state in the Data Source Management UI.

To resolve this problem you must:

- Check the DNS Server configuration to make sure:
  a. DNS Server IP Address is correct
  b. DNS Suffix addition is configured (For Example: `mydomain.com`)
- Delete the CCM in Operations Manager and add it back in case if Service Monitor coresides or coexists with Operations Manager.
- Delete the CCM from Service Monitor and add it back, in case of a standalone Service Monitor Deployment.

For more information, see the following topics:

- Unified Communications Manager Configuration, page B-1
- Understanding and Setting Data Source Credentials, page 3-2

Initiating Configuration Data Collection

Service Monitor collects configuration data from Unified Communications Manager nightly. However, when Unified Communications Manager configuration data has changed and needs to be reflected quickly in Service Monitor, you can initiate configuration data collection.

Note Service Monitor queries the Unified Communications Manager database to collect configuration data; the operation can impact Unified Communications Manager performance.

Examples of Unified Communications Manager configuration data that, when changed, can impact Service Monitor data include:

- The LogCallsWithZeroDuration flag setting
- Offnet/Onnet configuration for gateways, trunks, or system default value
- New devices added

To initiate configuration data collection, use this procedure:

Step 1 Select **Administration > Configuration > Data Source Management**. The Data Source Management page appears.

Step 2 Select the cluster.

Step 3 Click **Verify**. The Configuration Data Collection dialog box appears.

Step 4 Click **Verify Credentials and Collect Data**.

Note This will not appear if Service Monitor and Operations Manager coreside on the same machine.

Supported Data Source Software Versions

For the list of Unified Communications Manager and NAM software versions that Service Monitor supports, see *Cisco Prime Unified Service Monitor 8.7 Compatibility Matrix*.

Adding Data Source Credentials

If Service Monitor is installed in an environment with Operations Manager, Service Monitor uses the Device Credential Repository (DCR) to add and synchronize Unified Communications Manager. See the *Device and Credential Repository* chapter in *Inventory Management in CiscoWorks LAN Management Solution (LMS) 4.0*, for details about the DCR.

Service Monitor and Operations Manager on the Same Server

When Service Monitor is installed on the same server as Operations Manager, Unified Communications Manager publishers added to Operations Manager are automatically added to Service Monitor.

Service Monitor and Operations Manager on Different Servers

When Service Monitor and Operations Manager are installed on separate servers, you must set up the Service Monitor server as the DCR slave to automatically get cluster information from Operations Manager.

We recommend that you review the following CiscoWorks documentation links for detailed information about master-slave configuration:

- DCR Architecture
- Changing DCR Modes
- Master-Slave Configuration Prerequisites and Restore Operations

For detailed information on the DCR master-slave setup, you may also see “Understanding DCR” in the Common Services Online Help. The Common Services online help is only available through the Common Services pages, which are located in the Administration tab. To access the Common Services Online Help, select **Administration > Server Administration (Common Services) > Security**. From the Setting up Security page, click **Help**.

Service Monitor as a Standalone Installation

If Service Monitor is installed in a standalone environment, to obtain and analyze voice data from supported versions of Unified Communications Manager and NAMs, you must:

1. Perform configuration tasks for:
   - Unified Communications Manager—See Unified Communications Manager Configuration, page B-1.
   - NAM—See NAM Configuration, page C-1.
2. Add data source credentials to Service Monitor using the procedure for the appropriate software version:
   - Adding Credentials for NAM 4.x and Later, page 3-9
   - Adding Credentials for Unified Communications Manager 6.x and Later, page 3-10
   - Adding Credentials for Unified Communications Manager 4.x, page 3-11

Note Each cluster that you add to Service Monitor must have a unique cluster ID. You can view the cluster IDs in Service Monitor on the Data Source Management page. To view the cluster ID for a Unified Communications Manager that you plan to add, see Setting Unified Communications Manager Enterprise Parameters, page B-4.

Adding Credentials for NAM 4.x and Later

For the specific NAM hardware platforms and software versions that Service Monitor supports, see *Cisco Prime Unified Service Monitor 8.7 Compatibility Matrix.*

Step 1 Select **Administration > Configuration > Data Source Management**. The Data Source Management page appears.

Step 2 Click **Add**. The Add Credential 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 NAM.
Version	Select NAM 4.x **Note** For more information, see Supported Data Source Software Versions, page 3-8.
IP Address	You must enter one of these: • IP address for the NAM • DNS-resolvable hostname for the NAM. If you enter both an IP address and a hostname, Service Monitor uses the IP address and stores the hostname without verifying or updating it.
Host Name	

Field	Description
Protocol	Select the radio button that corresponds to the web server that is configured on the NAM: • HTTP—If selected, select one of these: – Default Port—Port number is displayed. – Custom Port—Enter the port number. • HTTPS—If selected, select one of these: – Default Port—Port number is displayed. – Custom Port —Enter the port number.
HTTP/S User Name/Password/Re-enter Password	Enter a username and password for a web administrator for the NAM. (For more information, see Enabling http or https Server and Configuring a Web Administrator User, page C-1.)

Step 4 Click **OK**.

Step 5 If an error message is displayed, do the following:

- Ensure that you have the correct credentials for the NAM.
- Ensure that Service Monitor supports the NAM hardware platform and software version; see *Cisco Prime Unified Service Monitor 8.7 Compatibility Matrix*.

Adding Credentials for Unified Communications Manager 6.x and Later

Caution Before adding credentials for a Unified Communications Manager 6.x and later software version cluster, confirm that the cluster ID does not include a space. For more information, see *Release Notes for Cisco Prime Unified Service Monitor 8.7*.

Note For Unified Communications Manager 6.x and later, in addition to adding credentials using the following procedure, you must also provide an SFTP password. See Configuring and Viewing Other Settings, page 3-36. For supported Unified Communications Manager software versions, see Supported Data Source Software Versions, page 3-8.

Step 1 Select **Administration > Configuration > Data Source Management**. The Data Source Management page appears.

Step 2 Click **Add**. The Add Credential 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.
Version	Select this version: CM 6.x and above **Note** For more information, see Supported Data Source Software Versions, page 3-8.
Publisher IP Address Publisher Host Name	You must enter one of these: • Publisher IP address—Enter the IP address for the publisher in the cluster. • Publisher hostname—If you enter only the hostname, it must be DNS-resolvable. If you enter both an IP address and a hostname, Service Monitor uses the IP address and stores the hostname without verifying or updating it.
HTTP/S User Name/Password/Re-enter Password	Enter a username and password that can be used to log in to Unified Communications Manager Administration on the publisher server. The user role must have Standard AXL API Access privilege.

Step 4 Click **OK**.

Note If Service Monitor fails to add the Unified Communications Manager credentials because a duplicate cluster ID exists, change the cluster ID as described in Setting Unified Communications Manager Enterprise Parameters, page B-4 and add the Unified Communications Manager credential again. Every cluster added to Service Monitor must have a unique cluster ID.

Adding Credentials for Unified Communications Manager 4.x

Before you can add credentials to Service Monitor, you must configure the credentials in Unified Communications Manager. See Configuring Database Authentication on Unified Communications Manager 4.x Systems, page B-7.

Note Every cluster that you add to Service Monitor must have a unique cluster ID. You can see the cluster IDs already in use on the Data Source Management page. To view the cluster ID for the Unified Communications Manager that you plan to add, see Setting Unified Communications Manager Enterprise Parameters, page B-4.

When you add credentials to Service Monitor, you must select the database authentication mode that corresponds to the one configured in Unified Communications Manager. See Determining Authentication Mode in Use on a Unified Communications Manager 4.x System, page B-7.

Note Do not add credentials for Unified Communications Manager 4.x while Provisioning Manager synchronization is running. For more information, see Avoiding Credential Failure When Provisioning Manager Synchronization Runs in Your Network, page 3-13.

Step 1 Select **Administration > Configuration > Data Source Management**. The Data Source Management page appears.

Step 2 Click **Add**. The Add Communications Manager dialog box appears.

Step 3 Enter the data described in the following table.

GUI Element	Description/Action
Display Name	Enter a name—up to 20 characters—to describe the cluster.
Version	Select CM 4.x **Note** For more information, see Supported Data Source Software Versions, page 3-8.
Publisher IP Address Publisher Host Name	You must enter one of these: • Publisher IP address—Enter the IP address for the publisher in the cluster. • Publisher hostname—If you enter only the hostname, it must be DNS-resolvable. If you enter both an IP address and a hostname, Service Monitor uses the IP address and stores the hostname without verifying or updating it.
CDR Database (Displayed when you select version CM 4.x)	Select the authentication mode that corresponds to the one used on Unified Communications Manager—see Determining Authentication Mode in Use on a Unified Communications Manager 4.x System, page B-7—and enter any required data: • Windows Authentication • SQL Authentication—When selected, you must also enter data in the SQL User Name and SQL Password/Re-enter SQL password fields. The usernames and passwords that you enter must match those entered for the Microsoft SQL Server account on the Unified Communications Manager publisher node; the account must have access to the CDR database.
HTTP/S User Name/Password/Re-enter password (Displayed when you select version CM 4.x)	Enter a username and password that can be used to log in to Unified Communications Manager Administration on the publisher server.

Step 4 Click **OK**.

Note If Service Monitor fails to add the data source credentials because a duplicate cluster ID exists, change the cluster ID as described in Setting Unified Communications Manager Enterprise Parameters, page B-4 and add the Unified Communications Manager credential again. Every cluster added to Service Monitor must have a unique cluster ID.

Avoiding Credential Failure When Provisioning Manager Synchronization Runs in Your Network

If Provisioning Manager runs in your network, check with your Provisioning Manager administrator to obtain the schedule for synchronization, which is a planned activity. During synchronization, do not add, edit, or verify Unified Communications Manager 4.x credentials in Service Monitor. Otherwise, credentials fail (last contact status displays Failure), data is not collected, and you cannot successfully verify credentials until synchronization completes.

Editing Data Source Credentials

You can change the display name and the HTTP/S username and password for any data source. Otherwise, the information that is displayed and the changes that you can make depend on whether the data source is a cluster or a NAM.

Note Do not edit Unified Communications Manager 4.x credentials while Provisioning Manager synchronization runs in your network. For more information, see Avoiding Credential Failure When Provisioning Manager Synchronization Runs in Your Network, page 3-13.

Step 1 Select **Administration > Configuration > Data Source Management**. The Data Source Management page appears.

Step 2 Select a data source and click **Edit**. The Edit Credential dialog box appears.

Step 3 Enter the data described in the following table. The data that is displayed depends on the software version.

Field	Description
Display Name	Enter a name—up to 20 characters—to describe the data source.
Fields that Are Displayed for a NAM Sensor	
IP Address	This field is dimmed because you cannot edit it.
Hostname	Service Monitor stores any change that you make to the hostname without verifying it.

Field	Description
Protocol	Select the radio button that corresponds to the web server that is configured on the NAM: • HTTP—If selected, select one of these: – Default Port—Port number is displayed. – Custom Port —Enter the port number. • HTTPS—If selected, select one of these: – Default Port—Port number is displayed. – Custom Port —Enter the port number.
HTTP/S Username, Password, Re-enter password	Enter a username and password for a web administrator for the NAM. (For more information, see Enabling http or https Server and Configuring a Web Administrator User, page C-1.)
Fields that Are Displayed for a Unified Communications Manager Cluster	
Publisher IP Address	This field is dimmed because you cannot edit it.
Publisher Host Name	Service Monitor stores any change that you make to the hostname without verifying it.
Windows Authentication SQL Authentication (Displayed if version CM 4.x was selected when adding credentials)	Unified Communications Manager database authentication mode—Select either Windows Authentication or SQL Authentication. **Note** If you are considering changing the authentication mode, see Determining Authentication Mode in Use on a Unified Communications Manager 4.x System, page B-7. If SQL authentication is selected, the usernames and passwords that you enter must match those entered for Microsoft SQL Server accounts on the Unified Communications Manager publisher node: • SQL User Name and Password/Re-enter SQL Password—Enter the username and password for a Microsoft SQL Server account with access to the CDR database on the Unified Communications Manager version 4.x publisher node. • SQL CDR-DB User Name and SQLCDR-DB Password/Re-enter password—Enter the username and password for a Microsoft SQL Server account with access to the CDR database on the Unified Communications Manager version 3.3.x publisher node. For more information, see Adding Microsoft SQLServer User Accounts for Unified Communications Manager 4.x, page B-9.
HTTP/S Username, Password, Re-enter password	Enter a username and password that can be used to log in to Unified Communications Manager Administration on the publisher server. **Note** For Unified Communications Manager 6.x and later, the user role must have Standard AXL API Access privilege.

Step 4 Click **OK**.

For Unified Communications Manager software versions that Service Monitor supports, see Supported Data Source Software Versions, page 3-8.

Deleting Data Source Credentials

After you complete this procedure, Service Monitor can no longer obtain data for the cluster or the NAM. Additionally, the data source no longer appears on the Inventory page. Call data for the data source remains in the database until it is purged. For more information, see Maintaining the Service Monitor Database, page 6-1.

Before you complete this procedure, delete the data source from any CVTQ or sensor threshold groups. See Editing a CVTQ Threshold Group, page 5-6 and Editing a Sensor Group, page 5-11.

Step 1 Select **Administration > Configuration > Data Source Management.** The Data Source Management page appears.

Step 2 Select the check box by the cluster or NAM 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.
- An error message appears, displaying a list of sensor threshold groups to which the NAM belongs. You will need to remove the NAMs from these sensor threshold groups and repeat this procedure.

Step 4 Click **OK**.

Managing the Phone Count

On the Inventory page, you can view the total number of phones that Service Monitor is monitoring. You can also view the names of all sensors (Cisco 1040s and NAMs) and Unified Communications Manager clusters known to Service Monitor to see whether each is monitored. If so, see the number of phones that Service Monitor manages in the cluster or for the sensor.

To manage the phone count, select **Administration > Configuration > Inventory**. The Inventory page appears, displaying the information in the following table.

GUI Element	Description
Phone Licenses	
Used	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 (n) has reached or exceeded licensed limit!`
Total	Number of phones allowed by license.
Cluster/Sensor List	

GUI Element	Description
Cluster/Sensor ID	One of the following: • Cluster ID—The cluster ID is assigned by Unified Communications Manager. • Sensor ID—Sensor MAC address. • NAM—IP address
Name	Display name (if configured in Service Monitor).
IP Address	IP address.
Version	One of these: • Binary image filename for Cisco 1040. • NAM software version. • Unified Communications Manager software version.
Type	One of the following: • Cluster—Unified Communications Manager. • NAM—Network Analysis Module sensor. • 1040—Cisco 1040 Sensor.
State	One of these: • 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: – A user set the state of the cluster or sensor to Suspended. See Suspending and Resuming a Cluster or Sensor from Monitoring, page 3-17. – Service Monitor could not monitor any more newly created clusters or phones when data was received because the phone license count was reached.
Licensed Phone Count	Number of phones in the cluster that are licensed (out of the total phone count).
Total Phone Count	Number of phones configured in the cluster.
Customer	The customer name. This column appears only if you are using Service Monitor in MSP Network Deployment mode.

Suspending and Resuming a Cluster or Sensor from Monitoring

Provided that Unified Communications Manager 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 Unified Communications Manager credentials to Service Monitor. (For more information, see Adding Data Source Credentials, page 3-8.)

Service Monitor learns of a sensor when:

- The Cisco 1040 sensor registers.
- The NAM credentials are added to Service Monitor.

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 Inventory page as Suspended.

Step 1 Select **Administration > Configuration > Inventory**.

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 **Administration > Configuration > Inventory**.

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 Phone Count for a Cluster

Phone count is determined when a cluster is added. Service Monitor counts the number of phones registered to a cluster and applies a license against each phone. The phone count is updated when data discovery is performed overnight or when a device and credential discovery is manually initiated for a cluster.

Configuring Settings for Most-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. If Service Monitor is installed in MSP Network Deployment mode, the report will have Customer name included.

Note The maximum number of records that can be exported to a PDF file is 2,000. The maximum number of records that you can export to CSV is 30,000. For more information, see Configuring Diagnostic Report Search and CSV Export Limit Settings, page 3-38.

Step 1 Select **Administration > Configuration > Export Settings**. The Export Settings (for Most-Impacted Endpoints) 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: • 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: • 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: • Sensor • CVTQ **Note** Separate reports are generated for sensor and CVTQ data. For report filenames, see Table 3-2.

GUI Element	Description/Action
Save at	Enter a location for storing the reports on the server where Service Monitor is installed; a default location is displayed. **Caution** If you configure export settings to save files outside of *NMSROOT*, be sure to also log into the Service Monitor server, create the folder that you entered on the Export Settings page, and provide write permission to the folder for the user *casuser*. If you do not, Service Monitor cannot create the export files. (NMSROOT is the location where Service Monitor is installed. If you used the default location, it is C:\Program Files\CSCOpx.)
E-mail (to)	(Optional) Enter one or more complete e-mail addresses separated by commas. **Note** You should configure another e-mail address to which Service Monitor can send notifications for server process restarts. (Otherwise, Service Monitor sends notifications to the address defined in this field.) For more information, see Configuring a Recipient for E-Mail Notification, page 6-8.
SMTP Server	(Optional) Enter an SMTP server.

E-mail (from)	(Optional) This field does not appear in the Export Settings (for Most-Impacted Endpoints) page.
	
	To configure an e-mail address to appear in the From field, do the following:
	
	1. On the Service Monitor system, go to C:\Program Files\CSCOpx\qovr (if the default location was selected during installation).
	2. Open the qovrExport.properties file.
	3. In the qovrExport.properties file, add EmailFrom=<email address>.
	4. Save and close the file.
	5. Restart the QOVR process. From the command line, enter these commands:
	
	`pdterm QOVR`
	`pdexec QOVR`

Step 2 Click **Apply**.

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

Table 3-2 Most-Impacted Endpoints Exported Reports

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

Configuring Call Classification

This section includes the following topics:

Understanding Call Classification

Service Monitor uses call classification for these purposes:

- To categorize calls in CDR Call Reports. (For more information, see Using CDR Call Reports, page 2-24.)
- To provide categorized call data for Service Statistics Manager reporting (when Service Statistics Manager is installed in the network). For more information, see *User Guide for Cisco Prime Unified Service Statistics Manager.*

Service Monitor categorizes calls using these sets of categories:

- System-defined—Service Monitor places calls into system-defined categories using the criteria shown in Table 3-3; see Understanding How Service Monitor Places a Call into System-Defined Call Categories, page 3-21.
- User-defined—After Service Monitor categorizes a call into the Internal or VG/Trunk-Outgoing system-defined call category, Service Monitor can also evaluate the call against the user-defined dial plan for the cluster, if defined. See Understanding How Service Monitor Places a Call into User-Defined Call Categories, page 3-22.

A call might belong to multiple call categories. For example, an outgoing call through a voice gateway is categorized into the VG/Trunk-Outgoing system-defined category. The same call could also be categorized as a Long Distance call. If so, Service Monitor includes the call in both categories. When you view data for such a call in the CDR Call report, all applicable call categories are listed in the report; see Generating a CDR Call Report, page 2-24 and Understanding a CDR Call Report, page 2-29.

Understanding How Service Monitor Places a Call into System-Defined Call Categories

Service Monitor determines whether a call fits in system-defined categories by analyzing CDRs and other Unified Communications Manager data, such as the following:

- The device types of the source and target endpoints.
- The direction of the call: incoming or outgoing.
- The protocol: H.323, MGCP, or SIP.

Table 3-3 lists system-defined call category types and names, and describes the calls included in the category type.

Table 3-3 System-Defined Call Categories

Category Type	Description	Category Name
Voicemail	Calls to or from voicemail.	Unity Voicemail—Calls that meet system-defined criteria for a voicemail call, such as calls to and from Cisco Unity and Cisco Unity Connection. **Note** You can add user-defined category names to this category type.
Conference	Calls to or from a conferencing system.	Conference Bridge—Calls that meet system-defined criteria for a call involving a conference bridge. **Note** You can add user-defined category names to this category type.
ICT	Calls to or from an intercluster trunk (ICT).	• ICT GK Controlled—ICT calls that are gatekeeper controlled. • ICT Non-GK Controlled—ICT calls that are not gatekeeper controlled.
VG/Trunk-Outgoing	Calls to a voice gateway or a trunk; only OffNet calls are included. (See Understanding OffNet and OnNet Calls, page 3-23.) **Note** User-defined dial plans are applied to calls in the VG/Trunk-Outgoing call category. For more information, see Table 3-4.	• MGCP Gateway Outgoing—Calls to an MGCP voice gateway. • H.323 Gateway Outgoing—Calls to an H.323 voice gateway. • H.323 Trunk Outgoing—Calls to an H.323 trunk. • SIP Trunk Outgoing—Calls to a SIP trunk.

Table 3-3 System-Defined Call Categories (continued)

Category Type	Description	Category Name
VG/Trunk-Incoming	Includes calls from a voice gateway or a trunk; only OffNet calls are included. (See Understanding OffNet and OnNet Calls, page 3-23.)	• MGCP Gateway Incoming—Calls from an MGCP voice gateway. • H.323 Gateway Incoming—Calls from an H.323 voice gateway. • H.323 Trunk Incoming—Calls from an H.323 trunk. • SIP Trunk Incoming—Calls from a SIP trunk.
Tandem	A tandem call occurs when both endpoints are voice gateways or trunks.	Tandem.
OnNet Trunk	Calls where one endpoint is a trunk and the call is not an OffNet call. (See Understanding OffNet and OnNet Calls, page 3-23.) For example, the trunk could be used to connect to WebEx or to a PBX.	• OnNet H.323 Trunk. • OnNet SIP Trunk.
Internal	Calls that do not fall into any of the above categories. For example, calls where one endpoint is an IP phone and the other endpoint is a voice gateway and the call is not an OffNet call. (See Understanding OffNet and OnNet Calls, page 3-23.)	Internal.
Unknown	For system-related reasons, Service Monitor could not determine the device type of the endpoints.	Unknown.

Understanding How Service Monitor Places a Call into User-Defined Call Categories

Service Monitor evaluates whether a call belongs in a user-defined call category, provided that:

- The call has already been categorized as an Internal, VG/Trunk-Outgoing, or OnNet Trunk call (see Understanding How Service Monitor Places a Call into System-Defined Call Categories, page 3-21).
- A user-defined dial plan is assigned to the cluster in which the call occurred. (See Assigning a User-Defined Dial Plan to a Cluster, page 3-32.)

A dial plan includes a prioritized list of dial patterns to which you must assign a user-definable call category name from one of these call category types:

- Conference—No default call category name is provided; you must define one.
- International—The default call category name is International.

- Emergency—The default call category name is Emergency.
- Local—The default call category name is Local.
- Long Distance—The default call category name is Long Distance.
- Service—The default call category name is Service.
- Toll Free—The default call category name is Toll Free.
- Voicemail—No default call category name is provided; you must define one.

Note For more information, see Managing User-Defined Call Categories, page 3-30.

Table 3-4 shows how dial patterns are applied from a user-defined dial plan to a call in the Internal, VG/Trunk-Outgoing, or OnNet Trunk call category.

Table 3-4 How Dial Patterns Are Applied to VG/Trunk-Outgoing, Internal, and OnNet Trunk Calls

Service Monitor Applies Dial Patterns of This Category Type...	To the Directory Number that is the...	In a Call That Is in This System-Defined Category...
• Conference • Emergency • International • Local • Long Distance • Service • Toll Free • Voicemail	Destination	VG/Trunk-Outgoing
• Conference • Voicemail	Source	
• Conference • Voicemail	• Source • Destination	• Internal • OnNet Trunk

Understanding OffNet and OnNet Calls

A call is considered to be OffNet when at least one endpoint is a gateway or a trunk and when any of the following is also true of the endpoint:

- The Call Classification parameter is set to Offnet in the gateway configuration—or the trunk configuration—in Unified Communications Manager (Administration).
- In Unified Communications Manager, both of the following are true:
  - Call Classification parameter is set to System Default in the gateway or trunk configuration.
  - System Default service parameter is set to Offnet.
- The endpoint is an analog gateway.

Any call that does not meet the criteria for an OffNet call is considered to be an OnNet call.

Configuring User-Defined Dial Plans

A dial plan must have a unique name, can include a set of toll-free numbers, and must include a set of dial patterns. A dial pattern identifies a call category name and type and specifies the rule or pattern that a directory number must match for the call to be included in the category.

Service Monitor provides a default dial plan as a starting point from which you can define your own dial plans. The default dial plan includes default dial patterns: call category names, types, and rules. As you configure a dial plan, you can update the call categories and add, modify, and delete the rules that are specified in the default dial plan. For more information, see Understanding the Default Dial Plan, page 3-26.

You can create multiple dial plans. You can assign only one dial plan to each cluster, but you can assign the same dial plan to multiple clusters. To manage dial plans, see the following:

- To add a dial plan, you can use data from one of these:
  - An existing dial plan—See Copying a Dial Plan, page 3-24.
  - The default dial plan—See Adding a Dial Plan, page 3-25.
- To edit a dial plan, see Editing a Dial Plan, page 3-27.
- To delete a dial plan, Deleting a Dial Plan, page 3-28.
- To assign a dial plan, see Assigning a User-Defined Dial Plan to a Cluster, page 3-32.

Copying a Dial Plan

Use this procedure to define a new dial plan by first copying an existing dial plan.

Step 1 Select **Administration > Configuration > Call Classification > Dial Plan Configuration**.

The Dial Plan Configuration page appears.

Step 2 Select a dial plan and click **Copy**. The Add Dial Plan window appears.

Step 3 Update the data described in the following table.

Field	Description
Dial Plan Name	Enter a dial plan name (replacing Copy of *dial plan name*).
Each row in the table comprises a dial pattern, described by these columns: • Condition • No. of Chars • Pattern • Call Category	Update the dial plan by adding, editing, or deleting any dial pattern. For more information, see the following: • Adding a Dial Pattern to a Dial Plan, page 3-28. • Editing a Dial Pattern in a Dial Plan, page 3-29. • Deleting a Dial Pattern from a Dial Plan, page 3-30. **Note** After you add a dial pattern, it has the lowest priority. To change the priority for a dial pattern, see the Priority column in this table.
Priority column	Number dial patterns in the order in which you want them to be applied. 1 is the highest priority.
Toll-Free Numbers	Enter any toll-free numbers, separated by commas.

Step 4 To save the dial plan before continuing to configure it, click **Apply**.

Step 5 To save the dial plan when you are done configuring it, click **OK**. The Dial Plan Configuration page appears.

Adding a Dial Plan

Step 1 Select **Administration > Configuration > Call Classification > Dial Plan Configuration**.

The Dial Plan Configuration page appears.

Step 2 Do one of the following:

- Select an existing dial plan and click **Copy**.
- Click **Add** to add a dial plan based on the default dial plan. (For more information, see Understanding the Default Dial Plan, page 3-26.)

The Add Dial Plan page appears, displaying a dial plan.

Step 3 Enter data described in the following table.

Field	Description
Dial Plan Name	Enter a dial plan name.
Each row in the table comprises a dial pattern, described by these columns: • Condition • No. of Chars • Pattern • Call Category	Update the dial plan by adding, editing, or deleting any dial pattern. For more information, see the following: • Adding a Dial Pattern to a Dial Plan, page 3-28. • Editing a Dial Pattern in a Dial Plan, page 3-29. • Deleting a Dial Pattern from a Dial Plan, page 3-30. **Note** After you add a dial pattern, update the priority for it; see the Priority column in this table.
Priority column	Number the dial patterns in the order in which you want them to be applied in the **Priority** column. 1 is the highest priority.
Toll-Free Numbers	Enter any toll-free numbers, separated by commas.

Step 4 To save the dial plan before continuing to configure it, click **Apply**.

Step 5 To save the dial plan when you are done configuring it, click **OK**. The Dial Plan Configuration page appears.

Understanding the Default Dial Plan

When you add a dial plan, a copy of the default dial plan is displayed for you to update. You can:

- Define your own call category names; however, you must select from the available call category types listed in Table 3-5
- Add, update, or delete dial patterns (each row in Table 3-5 represents a dial pattern)

Changes that you make while configuring a dial plan have no effect on the default dial plan, which is based on the North American Numbering Plan (NANP).

Table 3-5 provides the default dial plan values.

Table 3-5 Default Dial Plan Values

Condition	No. of Chars	Default Pattern	Call Category Name	Call Category Type	Explanation	Priority
>	3	011!	International	International	If the number of digits dialed is greater than 3 and starts with 011, the call is classified as International.	1
=	7	!	Local	Local	If the number of digits dialed is equal to 7 and the pattern is ! (more than one digit; in this case, 7 digits), the call is classified as Local.	2
=	10	T!	Toll Free[1]	Toll Free	If the number of digits dialed is equal to 10 and the pattern is T! (more than one digit; in this case, a 10-digit number that starts with a toll-free number that is defined in the dial plan), the call is classified as Toll Free. To define toll-free numbers in Service Monitor, see Configuring User-Defined Dial Plans, page 3-24.	3
=	10	G!	Local[2]	Local	If the number of digits dialed is equal to 10 and the pattern is G! (more than one digit; in this case, a 10-digit number that starts with a gateway code that has been defined in Service Monitor), the call is classified as Local.	4
=	10	!	Long Distance	Long Distance	If the number of digits dialed is equal to 10 and the pattern is ! (more than one digit; in this case, a 10-digit number), the call is classified as Long Distance.	5
=	11	T!	Toll Free[1]	Toll Free	If the number of digits dialed is equal to 11 and the pattern is T! (more than one digit; in this case, an 11-digit number that starts with a toll-free number that is defined in the dial plan), the call is classified as Toll Free. To define toll-free numbers in Service Monitor, see Configuring User-Defined Dial Plans, page 3-24.	6

Table 3-5 Default Dial Plan Values (continued)

Condition	No. of Chars	Default Pattern	Call Category Name	Call Category Type	Explanation	Priority
=	11	XG!	Local	Local	If the number of digits dialed is equal to 11 and the pattern is XG! (more than one digit; in this case, an 11-digit number that starts with any single digit followed by a gateway code that has been defined in Service Monitor), the call is classified as Local.	7
=	11	!	Long Distance	Long Distance	If the number of digits dialed is equal to 11 and the pattern is ! (more than one digit; in this case, an 11-digit number), the call is classified as Long Distance.	8

1. Service Monitor classifies the call as Toll Free if the toll-free code is defined in the dial plan that is assigned to the cluster. (See Configuring User-Defined Dial Plans, page 3-24.)
2. Service Monitor uses the gateway codes that you define. (See Managing Gateway Codes.)

Editing a Dial Plan

To edit a dial plan name, copy the dial plan, provide the correct name, save the new dial plan, and delete the older dial plan. (See Copying a Dial Plan, page 3-24 and Deleting a Dial Plan, page 3-28.)

Step 1 Select **Administration > Configuration > Call Classification > Dial Plan Configuration**.

Step 2 Select the dial plan to edit and click **Edit**. The Edit Dial Plan window appears.

Step 3 Enter data described in the following table.

Field	Description
Dial Plan Name	Dimmed because you cannot change it.
Each row in the table comprises a dial pattern, described by these columns: • Condition • No. of Chars • Pattern • Call Category	Update the dial plan by adding, editing, or deleting any dial pattern. For more information, see the following: • Adding a Dial Pattern to a Dial Plan, page 3-28. • Editing a Dial Pattern in a Dial Plan, page 3-29. • Deleting a Dial Pattern from a Dial Plan, page 3-30. **Note** After you add a dial pattern, it has the lowest priority. To change the priority for a dial pattern, see the Priority column in this table.
Priority column	Number the dial patterns in the order in which you want them to be applied. 1 is the highest priority.
Toll-Free Numbers	Enter any toll-free numbers, separated by commas.

Step 4 To save the dial plan before continuing to configure it, click **Apply**.

Step 5 To save the dial plan when you are done configuring it, click **OK**. The Dial Plan Configuration page appears.

Deleting a Dial Plan

Note If any cluster is assigned to the dial plan, you cannot delete the dial plan. (See Assigning a User-Defined Dial Plan to a Cluster, page 3-32.)

Step 1 Select **Administration > Configuration > Call Classification > Dial Plan Configuration**.

Step 2 Select the dial plan.

Step 3 Click **Delete**. A confirmation window appears.

Step 4 Click **OK**.

Configuring Dial Patterns in a User-Defined Dial Plan

Use the following procedures to manage dial patterns when you configure a dial plan:

- Adding a Dial Pattern to a Dial Plan, page 3-28
- Editing a Dial Pattern in a Dial Plan, page 3-29
- Deleting a Dial Pattern from a Dial Plan, page 3-30

Adding a Dial Pattern to a Dial Plan

You can add a dial pattern to a dial plan that you are adding or editing.

Step 1 From the Add Dial Plan or Edit Dial Plan page, click **Add**. The Add Dial Pattern dialog box appears.

Step 2 Create a dial pattern by supplying data in these fields:

- Condition—Applies to the number of characters. Select one:
  - Left Arrow (<)—Less than
  - Right Arrow (>) —Greater than
  - Equals symbol (=)—Equal to
- Number of Chars—Enter the total number of digits and non-numeric characters, including plus (+), pound (#), asterisk (*), comma (,), and the at symbol (@).

  Expresses the number of characters in the directory number to which the dial pattern applies.
- Pattern—Enter the pattern to apply to the digits, where:
  - G indicates that the digits identify a gateway code. (For more information, see Managing Gateway Codes, page 3-33.)

  - T indicates that Service Monitor should compare the digits with the toll-free numbers configured in the dial plan.
  - ! signifies multiple digits (any number that is more than 1 digit in length, such as 1234 or 5551234).
  - X signifies a single-digit number (such as 0, 1, or 9).
- Call Category Name—Select one of the following radio buttons and supply data as required:
  - Existing—Select an existing call category name.
  - New—Enter a unique name and select a call category type.

Step 3 Click **OK**. The Add Dial Pattern dialog box closes.

For more information, see the following topics:

- Adding a Dial Plan, page 3-25
- Editing a Dial Plan, page 3-27

Editing a Dial Pattern in a Dial Plan

You can edit a dial pattern when you are adding or editing the dial plan that contains it.

Note When you edit a dial pattern, you cannot change the call category name. To change the call category name, delete the dial pattern and add the dial pattern again; see Deleting a Dial Pattern from a Dial Plan, page 3-30 and Adding a Dial Pattern to a Dial Plan, page 3-28.

Step 1 From the Add Dial Plan or Edit Dial Plan page, click **Edit**. The Edit Dial Pattern dialog box appears.

Step 2 Update data in any of these fields:

- Condition—Applies to the number of characters. Select one:
  - Left Arrow (<)—Less than
  - Right Arrow (>) —Greater than
  - Equals symbol (=)—Equal to
- Number of Chars—Enter the total number of digits and non-numeric characters, including plus (+), pound (#), asterisk (*), comma (,), and the at symbol (@).
- Pattern—Enter the pattern to be used for call classification, where:
  - G indicates that the digits identify a gateway code. (For more information, see Managing Gateway Codes, page 3-33.)
  - T indicates that Service Monitor should compare the digits with the toll-free numbers that are configured in the dial plan.
  - ! signifies multiple digits (any number that is more than 1 digit in length, such as 1234 or 5551234).
  - X signifies a single-digit number (such as 0, 1, or 9).

For examples, see Understanding the Default Dial Plan, page 3-26.

- Call Category Name—This field is dimmed because you cannot change it.

Step 3 Click **OK**. The Edit Dial Pattern dialog box closes.

Deleting a Dial Pattern from a Dial Plan

You can delete a dial pattern when you are adding or editing the dial plan that contains it.

Step 1 Select the dial pattern you want to delete (from the Add Dial Plan or Edit Dial Plan page).

Step 2 Click **Delete**.

Step 3 To save the dial plan, do one of the following

- Click **Apply** to save the dial plan and continue working on the Add Dial Plan or Edit Dial Plan page.
- Click **OK** to save the dial plan and return to the Dial Plan Configuration window.

Managing User-Defined Call Categories

A user-defined call category provides a meaningful name for a dial pattern. When you add or edit a call category name, you can select from these call category types only:

- Conference
- Emergency
- International
- Local
- Long Distance
- Service
- Toll Free
- Voicemail

Call category types are predefined; you cannot change them.

You can create a call category name when you add a dial pattern to a dial plan; see Adding a Dial Pattern to a Dial Plan, page 3-28. You can also add, update, and delete call category names using the procedures in the following topics:

- Adding a Call Category Name, page 3-31
- Editing a Call Category Name, page 3-31
- Deleting a Call Category Name, page 3-31

Adding a Call Category Name

Step 1 Select **Administration > Configuration > Call Classification > Call Category**. The Call Category Configuration page appears.

Step 2 Click **Add**. The Add Call Category dialog box appears.

Step 3 Enter data in the following fields:

- Call Category Name—Enter a unique name.
- Call Category Type—Select one. (For more information, see Managing User-Defined Call Categories, page 3-30.)

Step 4 Click **OK**. The call category is now available for use in dial patterns.

Editing a Call Category Name

Note To change both the call category name and the call category type, add a new call category; see Adding a Call Category Name, page 3-31.

Use this procedure to change a call category name.

Step 1 Select **Administration > Configuration > Call Classification > Call Category**. The Call Category Configuration page appears.

Step 2 Select a call category and click **Edit**. The Edit Call Category dialog box appears.

Step 3 Enter a unique name in the Call Category Name field. (Call Category Type is dimmed because you cannot change it.)

Step 4 Click **OK**. The updated call category is now available for use in dial patterns.

Deleting a Call Category Name

Note You can delete a call category only when it is not used (associated with a dial pattern) in any dial plan.

Deleting a call category deletes the call category name, but does not affect the call category type.

Step 1 Select **Administration > Configuration > Call Classification > Call Category**. The Call Category Configuration page appears.

Step 2 Select a call category and click **Delete**. A confirmation message is displayed.

Step 3 Click **OK**.

Assigning a User-Defined Dial Plan to a Cluster

You can assign the same dial plan to all clusters or assign a different dial plan to each cluster that has been added to Service Monitor. To add a cluster, see Understanding and Setting Data Source Credentials, page 3-2.

Step 1 Select **Administration > Configuration > Call Classification > Dial Plan Assignment**. A list of clusters that have been added to Service Monitor is displayed.

If Service Monitor is installed in MSP Network Deployment mode, a column that lists the Customers is displayed.

Step 2 Select a dial plan or select None for any cluster in the Assign New Dial Plan column.

Note Before you can assign a dial plan to a cluster, you must first configure at least one (see Configuring User-Defined Dial Plans, page 3-24).

Step 3 Click **Update Dial Plan Assignment** to save the assignment.

Configuring Gateway Codes

Service Monitor uses the gateway codes that you configure to determine the call classification for an external call: whether it is local or long distance, for example.

Step 1 Select **Administration > Configuration > Call Classification > Gateway Code**. The Gateway Code Summary page opens, displaying the following information:

- Cluster ID—Cluster identifier that is assigned in Unified Communications Manager.
- Gateway Code Summary—Number of gateways for which gateway codes are configured in Service Monitor and total number of gateways in the cluster.
- Customer—Displayed if Service Monitor is installed in MSP Network Deployment mode.

Note To see the most recent time that Service Monitor checked the gateways in clusters, see Understanding and Setting Data Source Credentials, page 3-2.

Step 2 To configure gateway codes, select a cluster and click **Manage Gateway Code**. The Manage Gateway Code page appears. For more information, see Managing Gateway Codes, page 3-33.

Step 3 To view the gateways for which gateway codes are already configured, select clusters and click **View**. A Gateway Code Configuration Report opens. For more information, see Understanding a Gateway Code Configuration Report, page 3-34.

Managing Gateway Codes

To open the Manage Gateway Code window, see Configuring Gateway Codes, page 3-32. The Manage Gateway Code window displays the information in Table 3-6.

Table 3-6 Manage Gateway Code Window

Field or Button	Description/Action
Cluster ID field	The ID for the selected cluster.
Gateway Code field	Enter gateway codes.
Filtered by field	Filters that are in effect, producing the list of gateways that are displayed in the table.
Gateway Name table column	Name or IP address.
Route Group table column	Name (or blank if the gateway does not belong to a route group in Unified Communications Manager).
Gateway Code table column	Area code that is configured for the gateway in Service Monitor; blank if no code is configured.
Search button	Enables you to update the filters that control which gateways are displayed.
Apply button	Enables you to save changes.

To add, edit, and delete gateway codes, see the following sections:

- Finding the Gateways to Configure, page 3-33
- Updating Gateway Codes, page 3-34

Finding the Gateways to Configure

If the gateways that you are interested in do not appear on the Manage Gateway Code page, use this procedure to find the gateways and place them onto the Manage Gateway Code page.

Step 1 Click **Search**. A Search Criteria dialog box appears, displaying the following fields:

- Cluster Name—The selected cluster. You cannot edit this field.
- Route Group
- Gateway Name
- Gateway Code

Step 2 Enter data as follows:

- To find a specific gateway, enter the gateway name only.
- To find gateways that belong to a specific route group, enter the route group name only.
- To find all gateways on a cluster (this list can be long) leave all entry fields blank.
- To find all gateways for which a particular gateway code is already configured, enter a gateway code only.

Step 3 Click **Search**. The Manage Gateway Code page is displayed again. The Filter by information above the table is updated and the gateways that match the search criteria are added to the table.

Note For information on when Service Monitor last refreshed the list of gateways in a cluster, see Understanding and Setting Data Source Credentials, page 3-2.

Step 4 To update gateway codes, see Updating Gateway Codes, page 3-34.

Updating Gateway Codes

By default, no gateway codes are configured in Service Monitor, and the Manage Gateway Code page displays only gateways for which gateway codes are configured. (For the criteria that are in use for displaying gateways, see the Filter by information above the table.) If the gateway you are interested in does not appear on the Manage Gateway Code page, see Finding the Gateways to Configure, page 3-33.

Use this procedure to add, update, or delete gateway codes for a gateway.

Step 1 Select one or more gateways.

Step 2 Enter codes, separated by commas, in the Gateway Code field, keeping the following in mind:

- Entries in the Gateway Code field completely replace any previously configured gateway codes.
- Leaving the Gateway Code field blank deletes any previously configured gateway codes.

Step 3 Click **Apply**. Changes are saved and appear on the Manage Gateway Code page.

Step 4 Click **Close**. You are returned to the Gateway Code Summary page.

Understanding a Gateway Code Configuration Report

For the selected clusters, the gateway code configuration report displays only the gateways for which gateway codes are configured in Service Monitor. The report includes this information:

- Cluster ID—The name of the selected cluster.
- Gateway Name—DNS name or IP address.
- Route Group—Name; blank if the gateway does not belong to a route group in Unified Communications Manager.
- Gateway Code—Comma-separated list of gateway codes as configured in Service Monitor.

Configuring Trunk Utilization

You can configure the maximum capacity for trunks (maximum concurrent calls) and gateways (maximum channels). You can either configure the maximum capacity for a particular trunk or gateway, or you can use a CSV file to import the trunk utilization configuration data for all clusters.

Configuring the Maximum Capacity for a Trunk or Gateway:

Step 1 Select **Administration > Configuration > Trunk Utilization**. The Trunk Utilization Configuration page appears.

Step 2 Select a cluster.

Step 3 Select one of the following gateway or trunk types:

- MGCP Gateway—Automatically configured with a default setting.
- H.323 Gateway—Not automatically configured.
- H.225 Trunk—Not automatically configured.
- SIP Trunk—Not automatically configured.
- Intercluster Trunk—Not automatically configured.

Step 4 Select the gateway or trunk type, then click **Configure Maximum Capacity**. The corresponding Maximum Capacity Configuration page appears.

Step 5 In the Configure Channels (or Configure Concurrent Calls) field, enter the maximum capacity.

Step 6 Select the gateways or trunks that you want the setting to apply to.

Step 7 Click **Apply**.

Step 8 Click **Close**.

Importing and Exporting Trunk Utilization Data for All Clusters:

Tip The easiest way to create the configuration file is to first use the export function and export to a file. Then modify the data in the file as needed. Since all gateways and trunks are listed in the file, you should need to enter values into the file only.

Step 1 Select **Administration > Configuration > Trunk Utilization**. The Trunk Utilization Configuration page appears.

Step 2 Select a cluster.

Step 3 Click **Bulk Import** (or **Bulk Export**). The Import (Export) Trunk Utilization Configuration dialog box appears.

Step 4 Browse to the location of the CSV file, and then click **Import** (or **Export**). The data is then imported or exported.

Configuring and Viewing Other Settings

Use this procedure to:

- View some settings that are configured outside of the user interface. (See Configuring Diagnostic Report Search and CSV Export Limit Settings, page 3-38 and Configuring Low-Volume Schedule and Database Purging, page 6-2.)
- Configure SFTP settings if you are monitoring calls from Unified Communications Manager version 6.x or later. (For Unified Communications Manager software versions that Service Monitor supports, see Supported Data Source Software Versions, page 3-8.)

Step 1 Select **Administration > System Settings > Other Settings**. The Other Settings page appears.

Step 2 View settings and update SFTP settings as described in the following table.

Fields	Description/Action
Low-Volume Schedule Hours	
<*day*> <*timerange*>; <*timerange*> For example: Mon 0-6; 22-24	For each day of the week, timerange indicates the hours during which Service Monitor processes fewer records, handling a number that is roughly 20% of records processed during a peak period. During the low-volume schedule, Service Monitor performs database maintenance. **Note** A windows user with access to the Service Monitor server can configure this schedule. See Configuring Low-Volume Schedule and Database Purging, page 6-2.
Miscellaneous	
Wait for Diagnostic Report (min)	Number of minutes that Service Monitor continues to search, when there is a large volume of data, before displaying the matching records found so far for a diagnostic report (a Sensor report or a CVTQ report). To configure this setting, see Configuring Diagnostic Report Search and CSV Export Limit Settings, page 3-38.

Report Data Retention Period (days)	Number of days that data is retained in the Service Monitor database before being purged. The default value depends on the configuration:
	
	• Service Monitor alone on a server—7 days.
	• Service Monitor and Operations Manager on a server—3 days.
	
	On the Service Monitor server, a user can change the value of the data-retention-days property in the *NMSROOT*\qovr\qovrconfig.properties file. (NMSROOT is the location where Service Monitor is installed. If you used the default location, it is C:\Program Files\CSCOpx.) To put changes into effect after you edit qovrconfig.properties, you must stop and start the QOVR process. While logged in to the server where Service Monitor is installed, from the command line, enter these commands:
	
	`pdterm QOVR`
	`pdexec QOVR`

Fields	Description/Action
Operations Manager Server	Enter the IP address for the Operations Manager server that Service Monitor is registered to. **Note** Even when Operations Manager and Service Monitor run on the same system, you must replace the default value, localhost, with the correct IP address. Entering the IP address enables users to launch the Detailed Device View page or the Phone Detail window in Operations Manager from Service Monitor reports. (See Understanding Sensor Diagnostic Reports, page 2-8 and Understanding CVTQ Diagnostic Reports, page 2-18.) **Note** To enable users to view Operations Manager windows without logging in to Operations Manager, you can configure single sign-on. For more information, see Enabling Single Sign-On in the Common Services online help. **Note** The Common Services online help is only available through the Common Services pages, which are located in the Administration tab. To access the Common Services Online Help, you can use the following procedure: Select **Administration > Server Administration (Common Services) > Security**. The Setting up Security page appears. Click **Help**.
SFTP	
Username	You cannot change the username from smuser. This same username, smuser, must be configured in Unified Communications Manager. See Adding Service Monitor to Unified Communications Manager 6.x and Later as a Billing Server, page B-4.
Change password check box	Select to change password. **Caution** The default password is smuser. If you change the password here, you must also change the password for smuser in Unified Communications Manager. See Adding Service Monitor to Unified Communications Manager 6.x and Later as a Billing Server, page B-4.
Password	Enter password.
Re-enter password	Re-enter password.

Step 3 Click **Apply**.

Configuring Diagnostic Report Search and CSV Export Limit Settings

Table 3-7 lists properties that affect diagnostic reports. A windows user with access to the Service Monitor server can change the values of these properties in the *NMSROOT*\qovr\qovrconfig.properties file.

Note NMSROOT is the location where Service Monitor is installed. If you used the default location, it is C:\Program Files\CSCOpx.

Table 3-7 Diagnostic Report and Export Settings

Property	Description and Limit
WaitForDiagReport	Number of minutes that Service Monitor continues to search—when there is a large volume of data—before displaying the matching records found so far for a diagnostic report (a Sensor report or a CVTQ report). Default: 2. Maximum: 4. **Note** Service Monitor reports can display up to 2,000 records. To see additional records, you can export a diagnostic report to a CSV file.
ExportCSVLimit	Number of records that Service Monitor exports to a CSV file. The maximum is 30,000.

After you edit qovrconfig.properties, to put changes into effect, you must stop and start the QOVR process. While logged in to the server where Service Monitor is installed, from the command line, enter these commands:

```
pdterm QOVR
pdexec QOVR
```