CHAPTER 1

Getting Started with Service Monitor

Cisco Prime Unified Service Monitor (Service Monitor) is a product from the Cisco Prime Unified Communications Management Suite that receives and analyzes Mean Opinion Scores (MOSs) from Cisco Prime Unified Communications Manager (Unified Communications Manager) clusters and sensors—Cisco 1040 Sensors (Cisco 1040s) and Cisco Network Analysis Modules (NAMs)—sending traps when violations occur.

Note

- Throughout this document, any reference to Unified Communications Manager can also be understood to refer to Cisco Prime Unified CallManager, unless explicitly noted.
- Service Monitor documentation refers you to Common Services features and documentation when they are applicable. Common Services documentation and online help mention CiscoWorks LAN Management Solution and its components, which are products that can be installed elsewhere in your network. Common Services documentation also mentions LMS Portal, LMS Setup Center, and other features that are not applicable to Service Monitor.

The following topics are included:

Note For information on initially configuring Service Monitor, see Configuration Checklists and Tips, page A-1.

Overview

Service Monitor obtains and analyzes MOS from sensors (Cisco 1040s and NAMs) and Unified Communications Manager clusters. Service Monitor supports sensors or clusters or both. For more information, see Data Collection and Analysis, page 1-2.

Service Monitor analyzes the data that it receives and sends traps when MOS falls below a threshold. Service Monitor provides a set of default global thresholds, one per supported codec. Service Monitor enables you to change the default global thresholds and to override them by creating threshold groups: sensor threshold groups and cluster threshold groups. For more information, see Thresholds and Traps, page 1-5 and Trap Receivers, page 1-6.

Service Monitor diagnostic reports display data for calls that occurred during the data retention period (see Configuring and Viewing Other Settings, page 3-36). You can run reports for CVTQ data and sensor data. You can also run reports for the endpoints with the greatest number of violations in a 24-hour or 7-day period. For more information, see Using Reports, page 2-1.

To further analyze, display, and act on Service Monitor data, you can use Cisco Prime Unified Operations Manager (Operations Manager), by configuring it as a trap receiver for Service Monitor. Operations Manager can generate events for Service Monitor traps, display the events on the Service Quality Alerts dashboard, and store and display event history. For more information, see *User Guide for Cisco Prime Unified Operations Manager 8.7.*

Data Collection and Analysis

Service Monitor receives and analyzes MOS from these sources when they are installed in your voice network and configured properly:

- Sensors—Cisco 1040s and NAMs compute MOS for each Real-Time Transport Protocol (RTP) stream. Service Monitor obtains data at 60-second intervals, as a result of:
  - Receiving syslog messages that Cisco 1040s send
  - Polling NAMs for data
- CVTQ—Unified Communications Manager collects data from endpoints that support K-factor; MOS is calculated on the endpoints using the CVTQ algorithm. At the termination of a call, Unified Communications Manager stores the data in Call Detail Records (CDRs) and Call Management Records (CMRs).

Note For endpoints that support K-factor and for Unified Communications Manager versions that Service Monitor supports, see *Cisco Prime Unified Service Monitor 8.7 Compatibility Matrix.*

Table 1-1 provides a high-level comparison among the data sources that Service Monitor uses. Detailed procedures for performing related tasks are provided throughout this document.

Table 1-1 Data Source Comparison

	Sensor		Unified Communications Manager	
Comparison	**1040**	**NAM**	**4.3**	**6.x and Later[1]**
Compatibility determination For more information, see *Cisco Prime Unified Service Monitor 8.7 Compatibility Matrix.*	Binary image filename—SvcMonAB2_102.img	• Network Analysis Module Software version—4.x and 5.x • NAM hardware: NME-NAM NAM-1/NAM-2 NAM 2200 Series Appliances	• Unified Communications Manager version • Support on the voice gateway or Cisco Unified IP Phone for the CVTQ algorithm	
Configuration in Service Monitor	• Add TFTP server • Edit Cisco 1040 Sensor configuration files	Add credentials to Service Monitor		
Configuration outside of Service Monitor	• See *Quick Start Guide for Cisco 1040* • Copy configuration files and binary image to TFTP server	• Configure http or https server and web admin user on the NAM • Configure NTP server in Network Analysis Module Software	Configure accounts and privileges on Unified Communications Manager servers	Configure parameters and application billing server in Unified Communications Manager
Data collection: Push or Pull	Push—Cisco 1040 sends syslog messages	Pull—Service Monitor polls NAMs	Pull—Service Monitor queries the Unified Communications Manager database	Push—Unified Communications Manager sends information to application billing server
MOS Calculation	Based on R-factor		CVTQ algorithm (sometimes referred to as K-factor in Unified Communications Manager documentation)	
Registration or Authentication	Automatic or manual registration—Cisco 1040 registers with a Service Monitor	Authentication—Service Monitor uses credentials to access the data source		
Reports	Sensor Diagnostic Report with link to Sensor Stream Correlation window—Correlates streams from multiple sensors with call detail records (CDR)		• CVTQ Diagnostic Report • CDR Call Report	
	Sensor Most-Impacted Endpoints		CVTQ Most-Impacted Endpoints	

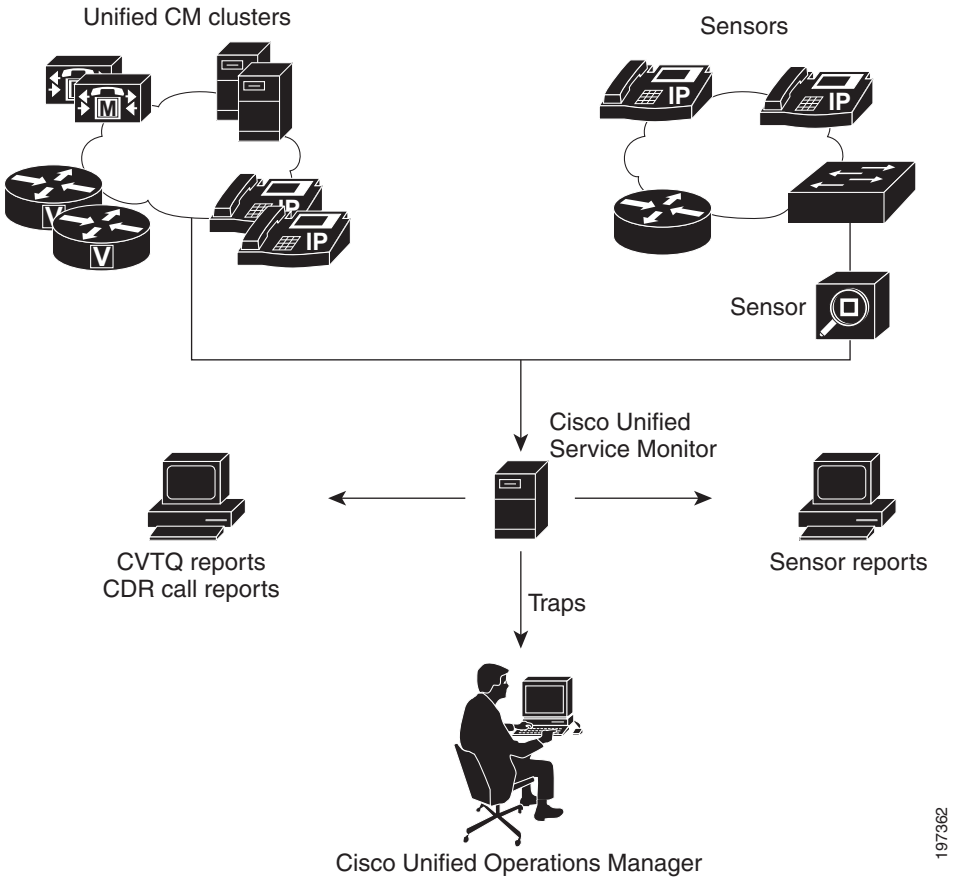
Table 1-1 Data Source Comparison (continued)

	Sensor		Unified Communications Manager	
Comparison	**1040**	**NAM**	**4.3**	**6.x and Later[1]**
Thresholds	Sensor group **Note** Thresholds that you configure in Service Monitor are not propagated to Network Analysis Module software. Likewise, thresholds configured in Network Analysis Module software are not propagated to Service Monitor.		CVTQ group	
	Note If sensor groups or CVTQ are not defined or not applicable, Service Monitor uses global thresholds.			
Time Synchronization	Service Monitor sends hourly time synch to 1040s.	Strong recommendation: Configure NAM to use the NTP server that Service Monitor uses.	Must configure Service Monitor to use the NTP server that Unified Communications Manager uses.	
Timing	Data is pushed or pulled every 60 seconds.		Data available after a call completes.	

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

Figure 1-1 shows sensors and clusters in a network with Service Monitor receiving and obtaining data, creating reports, and sending traps.

Figure 1-1 Service Monitor Overview



For more information, see these topics:

- Configuring Service Monitor, page 3-1
- Managing Cisco 1040s, page 4-1

Thresholds and Traps

Service Monitor examines the data it receives and compares MOS against the applicable threshold from user-defined threshold group settings or global threshold settings. When MOS drops below the threshold, Service Monitor generates SNMP traps and sends them to up to four trap receivers.

You can set thresholds for the following:

- Sensor Groups—Select sensors and endpoints and set a MOS threshold value for one or more supported codecs.
- CVTQ Groups—Select Unified Communications Manager clusters and endpoints and set a MOS threshold value for one or more supported codecs.
- Global Settings—Update default thresholds for one or more supported codecs. Global threshold settings are used when no other thresholds are applicable.

Service Monitor also sends a trap when a sensor is unreachable and another when the same sensor becomes reachable again.

Trap Receivers

Service Monitor examines the data it receives, comparing MOS against a default or user-specified threshold value for the codec. When MOS drops below the threshold, Service Monitor generates SNMP traps and sends them to up to four trap receivers.

Service Monitor also stores the call data it receives (from clusters and sensors) in the database for a configurable number of days. (See Report Data Retention Period in Configuring and Viewing Other Settings, page 3-36.) Optionally, Service Monitor also stores the call data it receives from sensors to disk files. (See Setting Up the Cisco 1040 Sensor Default Configuration, page 4-3.)

You can configure Cisco Prime Unified Operations Manager (Operations Manager) as a trap receiver for Service Monitor. Operations Manager can further analyze, display, and act on Service Monitor data. Operations Manager can:

- Generate events for Service Monitor traps
- Display the events on the Service Quality Alerts dashboard
- Store and display event history

For more information, see *User Guide for Cisco Prime Unified Operations Manager 8.7.*

Service Monitor Home Page

The Reports tab is the home page for Service Monitor, appearing after you log in. From the home page, you can generate reports that provide you with MOS statistics for a configurable number of days. For more information, see the following topics:

- Using Diagnostic Reports, page 2-3
- Generating a CVTQ Diagnostic Report, page 2-14
- Using Most-Impacted Endpoints Reports, page 2-22

Starting Service Monitor

Step 1 Enter the address in your browser:

- If Secure Socket Layer (SSL) is not enabled, enter http://*server_name*:1741 in your browser, where server_name is the DNS name or the IP address of the server where Service Monitor is installed.
- If SSL is enabled, enter https://*server_name:*443.

Note If you changed the HTTPS port during Service Monitor installation, replace 443 with the port number that you entered during installation.

A login page is displayed.

Step 2 Enter a username and password. If you do not have a username, you might be able to use the following:

- Enter *admin* for the user ID.
- Enter the password that you entered for the admin user during installation and press Enter.

The Service Monitor home page appears.

For more information, see Using Reports, page 2-1.

Launching Service Monitor from Operations Manager

To launch Service Monitor from Operations Manager:

Step 1 Select **UC Management Suite**, then select **Launch Home Page** under **Service Monitor.**

The List Service Monitors - Cisco Prime Unified Operations Manager page appears.

Step 2 Click **Add**.

The Add Service Monitor - Cisco Prime Unified Operations Manager page appears.

Step 3 Enter the following:

- IP Address / Hostname—IP address or hostname of the Service Monitor server.
- Protocol—Select **http** or **https** from the drop-down list.
- Port—The port number is 1741.
- Remarks—Enter remarks, if any.
- Username
- Password
- HTTPS Port—The default is 443.

Step 4 Click **Add**.

The Service Monitor server details are displayed on the List Service Monitor page.

Step 5 Select the check box adjacent to the IP address listed, then click **Launch**.

The Service Monitor home page appears.

Step 6 Click **Edit** to edit the Service Monitor details.

Step 7 Click **Configure** to configure trap receiver parameters.

About Enterprise and MSP Deployment Modes

Service Monitor 8.7 can be installed in either of the following modes, based on your requirements:

- Enterprise Network Deployment mode
- Managed Service Provider (MSP) Network Deployment mode

You can specify the mode when you install the product.

Note In MSP Network Deployment mode, Operations Manager and Service Monitor need to coreside on the same machine, that is, Operations Manager and Service Monitor must be installed on the same virtual or physical machine. MSP Network Deployment mode is not applicable for standalone installations of Service Monitor.

In both modes, Service Monitor always works with a unique Operations Manager instance, where both Operations Manager and Service Monitor manage the same set of Unified Communications Managers.

MSP Network Deployment mode enables you to view and manage multiple customers from a single Operations Manager instance in a service provider deployment. You can perform tasks either across multiple customers or for a single customer.

Service Monitor collects and reports CDRs and CMRs from multiple Call Managers. Multiple-customer view support restricts views and actions based on user authorization for the Call Managers that are present in Service Monitor.

Using role-based access control (RBAC), Operations Manager 8.7 provides the ability to authenticate and authorize users based on System Defined Groups used to customize the clusters, applications, and devices per customer.

Customer names defined in Operations Manger are visible in Service Monitor. Users logged in with the permission to view the clusters for a customer in Operations Manger can view the same clusters in Service Monitor. Users are restricted to viewing and executing only what is allowed for their role. See About RBAC for more details on RBAC.

Service Monitor displays the customer name wherever applicable. When Service Monitor is installed in MSP Network Deployment mode along with Operations Manager, the Service Monitor home page shows the list of customers managed under the Customer link at the top-right of the home page. See *User Guide for Cisco Prime Unified Operations Manager 8.7* for more details on MSP Network Deployment mode and multi-customer views.

In a network deployment where NAT-enabled devices exist, Service Monitor does not need to be configured specially for NAT. As long as Service Monitor works with a coresident or coexistent Operation Manager instance, Service Monitor will be able to monitor the clusters for which NAT is in use. See *User Guide for Cisco Prime Unified Operations Manager 8.7* for more details.

Note Cisco 1040 Sensor and NAM are not supported in MSP Network Deployment mode.

About RBAC

Role Based Access Control (RBAC) is a built-in feature in Common Services. Operations Manager 8.7 and Service Monitor 8.7 use the RBAC feature to achieve user role-based authentication and authorization to access groups of devices.

You can create device groups and assign users to roles in Operations Manager, via Common Services. The user roles created via Common Services are common to both Operations Manager and Service Monitor.

Service Monitor mapping of roles to tasks is shared with Operations Manager. This enables you to do either of the following:

- View the tasks assigned to a role
- Select tasks when you create new user roles.

When you create new users via Operations Manager, you can view and select the list of Service Monitor tasks along with other Operations Manager tasks. When Operations Manager and Service Monitor are on the same server, DCR synchronization is automatic, because the Common Services database is shared.

Service Monitor supports the following user roles:

- Super Admin—All privileges of Network Administrator and System Administrator roles.
- System Administrator
- Network Administrator
- Network Operator
- Help desk

See Permissions Report (**Administration > Server Administration (Common Services) > Reports > Permissions Report**) for a list of task to role mapping.

We recommend that you configure security using Cisco Secure ACS, in Enterprise deployment mode.

The following additional information is available:

- For information about configuring users, see the "Configuring Security" section in *Installation Guide for Cisco Prime Unified Service Monitor.*
- For information about configuring Service Monitor to use Cisco Secure ACS for authentication and authorization, see the "Security Configuration with Cisco Secure ACS" appendix in *Installation Guide for Cisco Prime Unified Service Monitor.*
- For information about creating users and assigning roles, see the Adding and Modifying a Local User section in Administration of CiscoWorks LAN Management Solution 4.0.