



# User Guide for Cisco Unified Service Monitor

Cisco Unified Communications Management Suite

Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

Text Part Number: OL-10405-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

*User Guide for Cisco Unified Service Monitor*

© 2005-2006 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

## Getting Started with Service Monitor 1-1

- Overview 1-1
  - Data Collection and Analysis 1-2
  - Thresholds and Traps 1-3
  - Trap Receivers 1-3
- Service Monitor Home Page 1-3
  - Starting Service Monitor 1-4

---

### CHAPTER 2

## Using Reports 2-1

- Overview: Service Monitor Reports 2-1
  - Configuring Service Monitor Initially Before Running Reports 2-2
  - Understanding Report Tool Buttons 2-2
  - Selecting Columns to Display and to Hide on a Service Monitor Report 2-3
  - Specifying IP Addresses or Directory Numbers for Endpoints 2-3
- Using Sensor Reports 2-4
  - Using the Sensor Report Filter to Specify and Generate a Sensor Report 2-4
  - Understanding Sensor Reports 2-5
- Using CVTQ Reports 2-7
  - Using the CVTQ Report Filter to Specify and Generate a CVTQ Report 2-7
  - Understanding CVTQ Reports 2-8
- Using Most-Impacted Endpoints Reports 2-10
  - Generating and Understanding the Sensor Most-Impacted Endpoints Report 2-11
  - Generating and Understanding the CVTQ Most-Impacted Endpoints Report 2-11

---

### CHAPTER 3

## Configuring Service Monitor 3-1

- Configuring Trap Receivers 3-1
- Understanding and Setting Cisco Unified CallManager Credentials 3-2
  - Cisco Unified CallManager Versions Supported 3-4
  - Adding Cisco Unified CallManager Credentials 3-4
  - Editing Cisco Unified CallManager Credentials 3-6
  - Understanding Last Contact Status and When to Verify Credentials 3-7
  - Deleting Cisco Unified CallManager Credentials 3-8
- Selecting Sensors and Clusters to Monitor 3-8
  - Suspending and Resuming a Cluster or Sensor from Monitoring 3-9

- Suspending a Cluster or Sensor 3-10
- Resuming a Cluster or Sensor 3-10
- Updating the Total Known Phone Count for a Cluster 3-10
- Configuring Number of Endpoints and Export Settings for Impacted Endpoints Reports 3-11
- Configuring Other Settings 3-12

CHAPTER 4

**Managing Sensors 4-1**

- Overview: Examining Data From Sensors 4-1
- Performing Initial Configuration in Service Monitor for Sensors 4-2
  - Configuring TFTP Servers for Sensor Configuration and Image Files 4-3
    - Adding a TFTP Server 4-3
    - Copying the Binary Image File to the TFTP Server 4-4
    - Deleting a TFTP Server 4-4
  - Setting Up the Sensor Default Configuration 4-4
- Configuring Sensors in Service Monitor 4-6
  - Understanding the Cisco 1040 Sensor Details Page 4-7
  - Adding a Sensor to Service Monitor 4-8
  - Editing the Configuration for a Specific Sensor 4-10
  - Resetting a Sensor 4-11
  - Deleting a Sensor 4-11
- Viewing the Configuration for a Sensor 4-12
  - Viewing Details in Service Monitor for a Specific Sensor 4-12
  - Viewing the Configuration File on the TFTP Server from a Sensor 4-13
  - Viewing the Configuration Using the Sensor Web Interface 4-13
- Understanding How Sensors Register with Service Monitors 4-14
  - Understanding How a Sensor Registers with Service Monitor 4-15
  - Understanding Sensor Failover to a Secondary Service Monitor 4-15
- Updating Image Files on Sensors 4-15
- Moving a Sensor from One Location to Another 4-16
- Understanding Sensor Call Metrics Archive Files 4-16
- Understanding Cisco 1040 Unreachable Trap 4-17

CHAPTER 5

**Setting Thresholds 5-1**

- Understanding Thresholds and Threshold Groups 5-1
- Configuring Global Thresholds 5-2
- Restoring Global Thresholds to Default Values 5-3
- Configuring CVTQ Groups 5-3
  - Adding a CVTQ Threshold Group 5-4

Editing a CVTQ Threshold Group	5-6
Updating CVTQ Threshold Group Priority	5-8
Deleting a CVTQ Threshold Group	5-8
Configuring Sensor Groups	5-8
Adding a Sensor Group	5-9
Editing a Sensor Group	5-10
Updating Sensor Group Priority	5-11
Deleting a Sensor Group	5-12

## CHAPTER 6

<b>Administering the System and Managing Data</b>	<b>6-1</b>
Understanding Service Monitor Database Purging	6-1
Starting a Database Backup	6-1
Restoring the Database	6-2
Changing the Password for the Service Monitor Database	6-3
Understanding Sensor Archive File Purging	6-3
Managing Log Files	6-3
Understanding Sensor Syslog Handling	6-3
Maintaining the Sensor History Log File	6-4
Managing Log Files and Enabling and Disabling Debugging	6-4
Configuring Users (ACS and Non-ACS)	6-5
Configuring Users Using Non-ACS Mode (CiscoWorks Local Login Module)	6-6
Configuring Users Using ACS Mode	6-6
Using Service Monitor in ACS Mode	6-7
Modifying Roles and Privileges in Cisco Secure ACS	6-8
Starting and Stopping Service Monitor Processes	6-8
Using SNMP to Monitor Service Monitor	6-8
Configuring Your System for SNMP Queries	6-9
Determining the Status of Windows SNMP Service	6-9
Installing and Uninstalling Windows SNMP Service	6-9
Enabling and Disabling Windows SNMP Service	6-10
Configuring Security for SNMP Queries	6-10
Viewing the System Application MIB Log File	6-10
Changing the Hostname on the Service Monitor Server	6-11
Changing the Hostname, Rebooting the Server, and Regenerating the Certificate	6-11
Reconfiguring Service Monitor After a Hostname Change	6-13
Changing the IP Address on the Service Monitor Server	6-13
Changing the Time on the Service Monitor Server	6-14

APPENDIX A

**Configuration Checklists and Tips** A-1

- Initial Configuration Checklist A-1
  - Server and Client Configuration Tasks A-1
- Understanding when You Can Expect to See Results A-2
- Optional Configuration Checklist A-2

APPENDIX B

**Cisco Unified CallManager Configuration** B-1

- Configuration Tasks for Supported Cisco Unified CallManager Versions B-1
- Configuring Cisco Unified CallManager B-2
  - Activating the AXL Web Service on Unified Communications Manager B-3
  - Setting Cisco Unified CallManager Service Parameters B-3
  - Setting Cisco Unified CallManager Enterprise Parameters B-4
  - Adding Service Monitor to Cisco Unified CallManager 5.x as a Billing Server B-4
  - Changing the Password for smuser in Cisco Unified CallManager 5.x B-5
- Configuring MicroSoft SQLServer on Cisco Unified CallManager System B-6
  - Enabling Mixed Authentication in Microsoft SQL Server for CallManager 4.x B-6
  - Adding Microsoft SQLServer User Accounts B-7
- Configuring Voice Gateways When VAD is Enabled B-8

APPENDIX C

**MIBs Used and SNMP Traps Generated** C-1

APPENDIX D

**Licensing** D-1

- Verifying Service Monitor Licensing D-1
- Obtaining and Registering Service Monitor Licenses D-2
- Using an Evaluation License D-3
- Determining License Size Exceeded D-3

APPENDIX E

**Service Monitor Support for SNMP MIBs** E-1

- System Application MIB Implementation E-1
  - System Application Resource MIB Tables E-1
    - Installed Packages E-2
    - Installed Elements E-2
    - Package Status Information E-3
    - Element Status Information E-4
    - Status of Packages when They Ran Previously E-5
    - Status of Elements when They Ran Previously E-5
    - Scalar Variables E-6
    - Process Map E-7

Sample MIB Walk for System Application MIB E-7

---

APPENDIX F

**Security Configuration with Cisco Secure ACS F-1**

Before You Begin: Integration Notes F-1

Configuring Service Monitor on Cisco Secure ACS F-2

Verifying the Service Monitor and Cisco Secure ACS Configuration F-3

---

INDEX





## Preface

---

This manual describes Cisco Unified Service Monitor (Service Monitor) and provides instructions for using and administering it.

## Audience

The audience for this document includes:

- IP communications and IP telephony management personnel.
- Administrative personnel monitoring the overall service levels of their organization.
- Network engineering personnel who evaluate and design IP network infrastructures.

## Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	<b>boldface</b> font
Variables for which you supply values	<i>italic</i> font
Displayed session and system information	screen font
Information you enter	<b>boldface screen</b> font
Variables you enter	<i>italic screen</i> font
Menu items and button names	<b>boldface</b> font
Selecting a menu item in paragraphs	<b>Option&gt;Network Preferences</b>
Selecting a menu item in tables	Option>Network Preferences



**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

---

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

**Warning**

This symbol means danger. You are in a situation that could cause bodily injury.

## Product Documentation

**Note**

The originally published printed and electronic documentation is included with your product. Any changes after original publication are reflected on Cisco.com, where you will find the most up-to-date documentation.

[Table 1](#) describes the product documentation that is available.

**Table 1**      **Product Documentation**

Document Title	Available Formats
<i>Release Notes for Cisco Unified Service Monitor Release 2.0</i>	<ul style="list-style-type: none"> <li>PDF on the product CD.</li> <li>On Cisco.com at <a href="http://cisco.com/en/US/products/ps6536/prod_release_notes_list.html">http://cisco.com/en/US/products/ps6536/prod_release_notes_list.html</a></li> </ul>
<i>Quick Start Guide for Cisco Unified Service Monitor 2.0</i>	<ul style="list-style-type: none"> <li>Printed document that was included with the product.</li> <li>PDF on the product CD.               <ul style="list-style-type: none"> <li>On Cisco.com at <a href="http://cisco.com/en/US/products/ps6536/prod_installation_guides_list.html">http://cisco.com/en/US/products/ps6536/prod_installation_guides_list.html</a></li> </ul> </li> </ul>
<i>User Guide for Cisco Unified Service Monitor</i>	<ul style="list-style-type: none"> <li>PDF on the product CD.</li> <li>On Cisco.com at <a href="http://cisco.com/en/US/products/ps6536/products_user_guide_list.html">http://cisco.com/en/US/products/ps6536/products_user_guide_list.html</a></li> </ul>
Context-sensitive online help	Click the Help link in the upper-right hand corner of the window or the help button in any dialog box.

## Related Documentation

**Note**

The originally published printed and electronic documentation was included with your product. Any changes after original publication are reflected on Cisco.com, where you will find the most up-to-date documentation.

[Table 2](#) describes the additional documentation that is available.

**Table 2**      **Related Documentation**

Document Title	Available Formats
<i>Quick Start Guide for Cisco 1040 Sensor</i>	On Cisco.com at <a href="http://cisco.com/en/US/products/ps6536/prod_installation_guides_list.html">http://cisco.com/en/US/products/ps6536/prod_installation_guides_list.html</a>
<i>Release Notes for Cisco Unified Operations Manager 2.0</i>	On Cisco.com at the following URL: <a href="http://cisco.com/en/US/products/ps6535/prod_release_notes_list.html">http://cisco.com/en/US/products/ps6535/prod_release_notes_list.html</a>
<i>Quick Start Guide for Cisco Unified Operations Manager 2.0</i>	On Cisco.com at the following URL: <a href="http://cisco.com/en/US/products/ps6535/prod_installation_guides_list.html">http://cisco.com/en/US/products/ps6535/prod_installation_guides_list.html</a>
<i>Installation Guide for Cisco Unified Operations Manager</i>	On Cisco.com at the following URL: <a href="http://cisco.com/en/US/products/ps6535/prod_installation_guides_list.html">http://cisco.com/en/US/products/ps6535/prod_installation_guides_list.html</a>
<i>User Guide for Cisco Unified Operations Manager</i>	On Cisco.com at the following URL: <a href="http://cisco.com/en/US/products/ps6535/products_user_guide_list.html">http://cisco.com/en/US/products/ps6535/products_user_guide_list.html</a>
<i>Release Notes for CiscoWorks Common Services 3.0.3 (Includes CiscoView 6.1.2) on Windows</i>	On Cisco.com at the following URL: <a href="http://www.cisco.com/en/US/products/sw/cscowork/ps3996/prod_release_note09186a00805af53a.html">http://www.cisco.com/en/US/products/sw/cscowork/ps3996/prod_release_note09186a00805af53a.html</a>
<i>Readme for Common Services 3.0.4 on Windows</i>	On Cisco.com at the following URL: <a href="http://www.cisco.com/en/US/partner/products/sw/cscowork/ps3996/prod_installation_guide09186a00805f7d64.html">http://www.cisco.com/en/US/partner/products/sw/cscowork/ps3996/prod_installation_guide09186a00805f7d64.html</a>
<i>Installation and Setup Guide for Common Services 3.0.3 (Includes CiscoView) on Windows</i>	<ul style="list-style-type: none"> <li>On Cisco.com at the following URL: <a href="http://www.cisco.com/en/US/partner/products/sw/cscowork/ps3996/products_installation_guide_book09186a00805305cb.html">http://www.cisco.com/en/US/partner/products/sw/cscowork/ps3996/products_installation_guide_book09186a00805305cb.html</a></li> <li>Printed document available by order (part number DOC-7817184=)<sup>1</sup></li> </ul>
<i>User Guide for CiscoWorks Common Services 3.0.3</i>	<ul style="list-style-type: none"> <li>On Cisco.com at the following URL: <a href="http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_book09186a008053eabf.html">http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_book09186a008053eabf.html</a></li> <li>Printed document available by order (part number DOC-7817182=)<sup>1</sup></li> </ul>

1. See the “Obtaining Documentation” section on page xi.

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

### Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

## Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

If you do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

## Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—[security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

---

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

---

## Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

To register as a Cisco.com user, go to this URL:

<http://tools.cisco.com/RPF/register/register.do>

# Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

<http://www.cisco.com/en/US/support/index.html>

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



### Note

Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.



### Tip

#### Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411

Australia: 1 800 805 227

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

**Severity 1 (S1)**—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

**Severity 2 (S2)**—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

**Severity 3 (S3)**—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

**Severity 4 (S4)**—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

<http://www.cisco.com/offer/subscribe>

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:  
<http://www.cisco.com/go/guide>
- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:  
<http://www.cisco.com/go/marketplace/>
- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:  
<http://www.ciscopress.com>
- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:  
<http://www.cisco.com/ipj>
- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:  
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:  
<http://www.cisco.com/discuss/networking>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:  
<http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm>
- World-class networking training is available from Cisco. You can view current offerings at this URL:  
<http://www.cisco.com/en/US/learning/index.html>



# Getting Started with Service Monitor

---

Cisco Unified Service Monitor (Service Monitor) is a product from the Cisco Unified Communications Management Suite that receives and analyzes Mean Opinion Scores (MOSs) from Cisco Unified CallManager clusters and Cisco 1040 Sensors (sensors), sending traps when violations occur.

The following topics are included:

- [Overview, page 1-1](#)
- [Service Monitor Home Page, page 1-3](#)



Note

---

For information on initially configuring Service Monitor, see [Configuration Checklists and Tips, page A-1](#).

---

## Overview

Service Monitor receives and analyzes MOS from Cisco Unified CallManager clusters and Cisco 1040 Sensors. 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 1-3](#) and [Trap Receivers, page 1-3](#).

Service Monitor diagnostic reports display data for calls that occurred during the previous 30 days. You can run reports for cluster-reported data and sensor-reported 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](#).

## Data Collection and Analysis

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

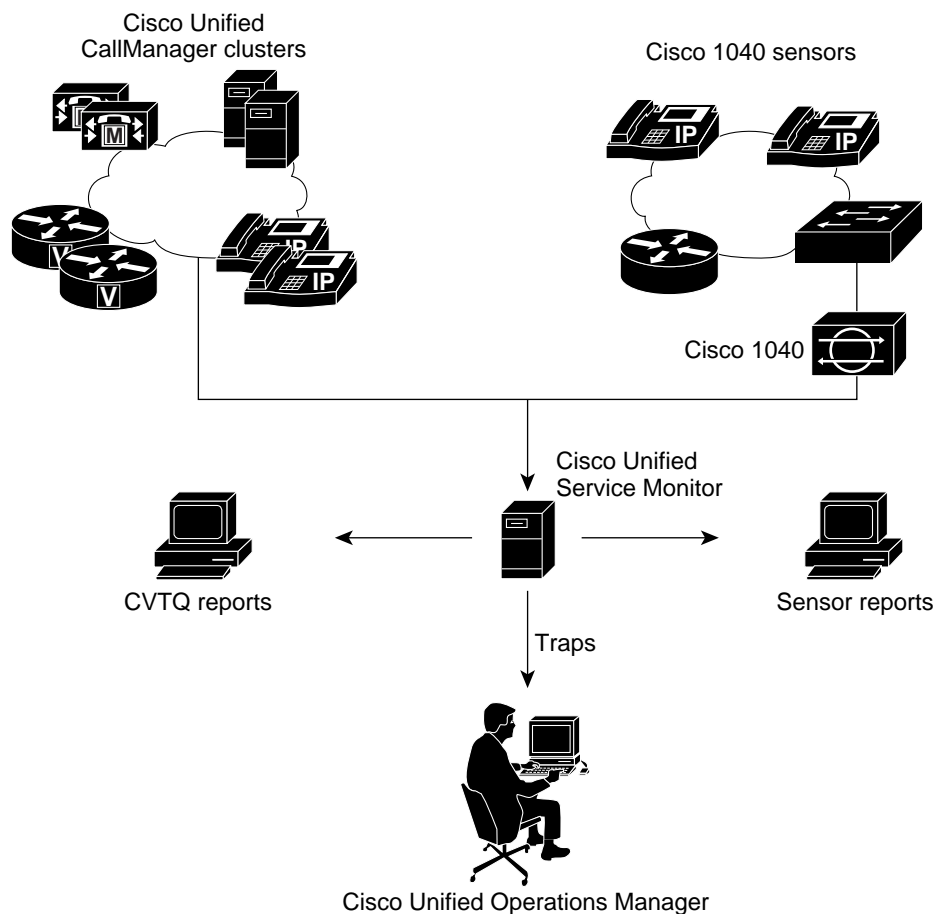
- **Sensors**—Cisco 1040 Sensors compute MOS for each Real-Time Transport Protocol (RTP) stream and send syslog messages to Service Monitor every 60 seconds.
- **CVTQ**—Cisco Unified CallManager collects data from Cisco voice gateways and Cisco IP phones; MOS is calculated on the gateways and phones using the Cisco Voice Transmission Quality (CVTQ) algorithm. At the termination of a call, Cisco Unified CallManager stores the data in Call Detail Records (CDRs) and Call Management Records (CMRs).



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

Figure 1-1 shows Service Monitor receiving data, creating reports, and sending traps.

**Figure 1-1 Service Monitor Overview**



157548

For more information, see these topics:

- [Configuring Service Monitor, page 3-1](#)

- [Managing Sensors, 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 Cisco Unified CallManager 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.

## 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 metrics it receives; when receiving data from:

- **Clusters**—Service Monitor stores information in the database for up to 30 days.
- **Cisco 1040 Sensors**—Service Monitor stores information in the database for up to 30 days. Optionally, Service Monitor stores the call metrics it receives from Cisco 1040s to disk files.

You can configure Cisco 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 event history for up to 30 days

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

## 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 up to the last 30 days.

- [Using Sensor Reports, page 2-4](#)
- [Using CVTQ Reports, page 2-7](#)
- [Using Most-Impacted Endpoints Reports, page 2-10](#)

## Starting Service Monitor

- 
- Step 1** 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. A login page is displayed.
- Step 2** Enter a username and password. If you do not have a username, you can 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 the following topic:

- [Configuring Users \(ACS and Non-ACS\), page 6-5](#)



## Using Reports

---

The following topics are included:

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

### Overview: Service Monitor Reports

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

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

Service Monitor supplies separate reports for data obtained from:

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

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

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

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

## Configuring Service Monitor Initially Before Running Reports

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

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

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





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

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

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


## Understanding Report Tool Buttons

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

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

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

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

- Step 1** In the upper-right corner of a report, click the Tools button . A column selector dialog box appears.
- Step 2** To restore the report to use columns that are displayed by default, click the **Restore Default Columns** button. The column selector dialog box closes and the report window refreshes, displaying the default columns.
- Step 3** To update report columns, do the following:
- To hide a column, place it on the Hidden Column(s) list:
    - Select the column by name from the Displayed Column(s) list.
    - Click the < **Remove** << button. The column appears on the Hidden Column(s) list.



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

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

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



**Note** Your selections are saved and will affect other users.

## Specifying IP Addresses or Directory Numbers for Endpoints

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

**Table 2-1** Endpoint Definition

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

## Using Sensor Reports

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

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


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

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

**Step 2** Do one of the following:

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

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

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

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

## Understanding Sensor Reports

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

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

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

**Table 2-2**      **Sensor Report Contents**

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

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

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

## Using CVTQ Reports

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

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


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

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

**Step 2** Do one of the following:

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

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

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

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

## Understanding CVTQ Reports

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

**Note**

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

**Table 2-3 CVTQ Report Contents**

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

Table 2-3 CVTQ Report Contents (continued)

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

## Using Most-Impacted Endpoints Reports

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

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

This section includes the following topics:

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

## Generating and Understanding the Sensor Most-Impacted Endpoints Report



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

**Step 1** To generate the Cisco 1040 Sensor Most-Impacted Endpoints report, select **Reports > Sensor: Impacted Endpoints**. The report opens in a new window.

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

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

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

## Generating and Understanding the CVTQ Most-Impacted Endpoints Report



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

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

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

**Table 2-5** CVTQ Most-Impacted Endpoints Report Contents

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



# 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)	Enter up to 4 trap receivers: <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul> When Service Monitor generates SNMP traps, it forwards them to these receivers.

**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"> <li>Version—Cisco Unified CallManager software version.</li> <li>ID—ID assigned to the cluster by the Cisco Unified CallManager.</li> </ul>
Last Contact Status	<p>Status for these credentials:</p> <ul style="list-style-type: none"> <li>HTTP/S</li> <li>CDR/CDRM DB</li> <li>Device DB</li> </ul> <p><b>Note</b> 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"> <li>Success—Link. If you click the link, you can check when the last successful contact occurred.</li> </ul> <p><b>Note</b> 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"> <li>Verifying—Click the link for more information.</li> <li>Failure—Click the link for more information.</li> <li>Blank—This credential is not required for Service Monitor to obtain information from this version of the Cisco Unified CallManager.</li> </ul> <p>For more information, see <a href="#">Understanding Last Contact Status and When to Verify Credentials, page 3-7</a>.</p>
Buttons	<ul style="list-style-type: none"> <li>Add—Add credentials for a Cisco Unified CallManager cluster. See <a href="#">Adding Cisco Unified CallManager Credentials, page 3-4</a>.</li> <li>Edit—Edit credentials for a Cisco Unified CallManager cluster. See <a href="#">Adding Cisco Unified CallManager Credentials, page 3-4</a>.</li> <li>Delete—See <a href="#">Deleting Cisco Unified CallManager Credentials, page 3-8</a>.</li> <li>Verify—Verify credentials for a selected Cisco Unified CallManager cluster.</li> <li>Refresh—Refresh the page.</li> </ul>

## 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.  <b>Note</b> 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"> <li>• 3.3.x—Enter the IP address for the publisher</li> <li>• 4.x—Enter the IP address for the publisher</li> <li>• 5.x—Enter the IP address for a publisher or a subscriber</li> </ul>
Version	Select the software version running on the cluster from these: <ul style="list-style-type: none"> <li>• 3.3.x</li> <li>• 4.x</li> <li>• 5.x</li> </ul> <p><b>Note</b> For more information, see <a href="#">Cisco Unified CallManager Versions Supported, page 3-4</a>.</p> <p>Depending on the selected software version, you will need to enter one or more usernames and passwords, described in <a href="#">Step 4</a>.</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. <b>Note</b> If Service Monitor successfully retrieves the hostname from Cisco Unified CallManager, it 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"> <li>• 3.3.x</li> <li>• 4.x</li> <li>• 5.x</li> </ul> <b>Note</b> 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 <a href="#">Determining License Size Exceeded, page D-3</a> .
License limit: ( <i>n</i> )	Number of phones allowed by license.
<b>Cluster/Sensor List</b>	
Cluster/Sensor ID column	One of the following: <ul style="list-style-type: none"> <li>Cluster ID—The cluster ID is assigned by Cisco Unified CallManager.</li> <li>Sensor ID—Sensor MAC address.</li> </ul>
Version column	Software version of Cisco Unified CallManager.
Type	One of the following: <ul style="list-style-type: none"> <li>Cluster</li> <li>Sensor</li> </ul>
State column	One of these: <ul style="list-style-type: none"> <li>Monitored—Service Monitor is collecting and analyzing data from this cluster or sensor and sending traps when violations occur.</li> <li>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"> <li>A user set the state of the cluster or sensor to Suspended. See <a href="#">Suspending and Resuming a Cluster or Sensor from Monitoring, page 3-9</a>.</li> <li>Service Monitor could not monitor any more newly created clusters or phones when data was received because the phone license count was reached.</li> </ul> </li> </ul>
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"> <li>• CSV check box—Save the report in CSV format.</li> <li>• PDF check box—Save the report in PDF format.</li> </ul> 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"> <li>• CSV check box—Save the report in CSV format.</li> <li>• PDF check box—Save the report in PDF format.</li> </ul> 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"> <li>• Sensor</li> <li>• CVTQ</li> </ul> <b>Note</b> Separate reports are generated for sensor and CVTQ data. For report filenames, see <a href="#">Table 3-1</a> .
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 <b>Note</b> Generated on Monday.	CVTQ_Weekly_ddmmyyyy.csv
		CVTQ_Weekly_ddmmyyyy.pdf
Sensors	Daily	Sensor_Daily_ddmmyyyy.csv
		Sensor_Daily_ddmmyyyy.pdf
	Weekly <b>Note</b> 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
<b>SFTP</b>	
Username	You cannot change the username from smuser. This same username, smuser, must be configured in Cisco Unified CallManager. See <a href="#">Adding Service Monitor to Cisco Unified CallManager 5.x as a Billing Server, page B-4</a> .
Change password check box	Select to change password.  <div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <p><b>Caution</b></p> <p>The default password is smuser. If you change the password here, you must also change the password for smuser in Cisco Unified CallManager. See <a href="#">Adding Service Monitor to Cisco Unified CallManager 5.x as a Billing Server, page B-4</a>.</p> </div> </div>
Password	Enter password.
Re-enter password	Re-enter password.

- Step 3** Click **Apply**.



## Managing Sensors

---

The following topics are included:

- [Overview: Examining Data From Sensors, page 4-1](#)
- [Performing Initial Configuration in Service Monitor for Sensors, page 4-2](#)
- [Configuring Sensors in Service Monitor, page 4-6](#)
- [Viewing the Configuration for a Sensor, page 4-12](#)
- [Understanding How Sensors Register with Service Monitors, page 4-14](#)
- [Updating Image Files on Sensors, page 4-15](#)
- [Moving a Sensor from One Location to Another, page 4-16](#)
- [Understanding Sensor Call Metrics Archive Files, page 4-16](#)
- [Understanding Cisco 1040 Unreachable Trap, page 4-17](#)

### Overview: Examining Data From Sensors

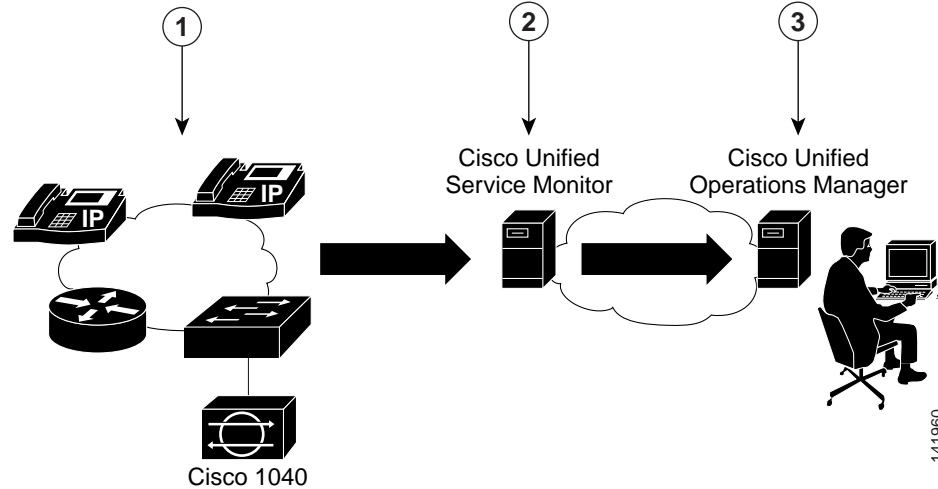
Service Monitor analyzes data that it receives from Cisco 1040 Sensors (Cisco 1040s) installed in your voice network. Each licensed instance of Service Monitor acts as a primary Service Monitor for multiple Cisco 1040s. A Service Monitor can also be configured to act as a secondary Service Monitor for Cisco 1040s that are managed by other licensed instances of Service Monitor. When a Service Monitor becomes unavailable, Cisco 1040s temporarily fail over to secondary Service Monitors until the primary Service Monitor becomes available again.

Service Monitor examines the data it receives from Cisco 1040s, comparing Mean Opinion Scores (MOS)—computed by Cisco 1040s for each RTP stream—against a user-specified threshold value. When MOS drops below the threshold, Service Monitor generates SNMP traps and sends them to up to four trap receivers. Optionally, Service Monitor stores the call metrics it receives from Cisco 1040s to disk files.

To further analyze, display, and act on Service Monitor data, you can use Cisco Unified Operation 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 event history for up to 30 days. For more information, see *User Guide for Cisco Unified Operations Manager*.

[Figure 4-1](#) shows Service Monitor and Cisco 1040s installed with Operations Manager.

Figure 4-1 Service Monitor Deployment



1	Cisco 1040 monitors actual voice calls.	3	Operations Manager presents alert information.
2	Service Monitor evaluates MOS values and sends SNMP traps when a threshold is violated. Service Monitor also sends an SNMP trap when a Cisco 1040 is unreachable.	—	—

For more information, see the following topics:

- [Understanding Cisco 1040 Unreachable Trap, page 4-17](#)
- [MIBs Used and SNMP Traps Generated, page C-1](#)

## Performing Initial Configuration in Service Monitor for Sensors

To configure sensors, do the following:

1. Add one or more TFTP servers for Service Monitor and sensors to use. See [Configuring TFTP Servers for Sensor Configuration and Image Files, page 4-3](#).
2. Copy the binary image file from the Service Monitor server to the TFTP server.
3. Create a default configuration file. See [Setting Up the Sensor Default Configuration, page 4-4](#).

Service Monitor copies sensor configuration files to each TFTP server that you configure. When a sensor connects to the network, it downloads a configuration file from a TFTP server before registering to a service monitor. For more information, see [Understanding How a Sensor Registers with Service Monitor, page 4-15](#).

## Configuring TFTP Servers for Sensor Configuration and Image Files

Service Monitor uses one or more TFTP servers to provide configuration files and binary image files for sensors. You must define at least one TFTP server for Service Monitor to use. You can configure additional TFTP servers either as backup or if you have more than one DHCP scope.

After you add or edit a sensor, Service Monitor updates the configuration file locally, on its server, before copying the configuration file to all known TFTP servers. Keeping copies of the configuration files on each TFTP server enables sensors to fail over efficiently to a secondary Service Monitor.

You can use the configuration files that Service Monitor keeps on the server to recover if there is a write failure on the TFTP server. In this case, you can manually copy configuration files from Service Monitor to each TFTP server that is configured for Service Monitor. (To verify the contents of a configuration file on the TFTP server, see [Viewing the Configuration File on the TFTP Server from a Sensor, page 4-13.](#))

You must copy the binary image file for sensors to each TFTP server that you add to Service Monitor; see [Copying the Binary Image File to the TFTP Server, page 4-4.](#)

- Step 1** Select **Configuration > Sensor > TFTP Servers**. The TFTP Server Setup page appears, displaying the information in the following table.

GUI Element	Description/Action
Check box	Select when you want to delete a TFTP server.
TFTP Server	IP address or DNS name.
Port	The customary port number is 69.
Add button	Click to add a TFTP server.
Delete button	Select a check box and click to delete the selected TFTP server.

### Adding a TFTP Server

To enable sensors to register with Service Monitor, you must define at least one TFTP server where Service Monitor can provide sensor configuration files. You can configure additional TFTP servers; for example, to serve as backup or if you have more than one DHCP scope.



**Note**

You can use a Cisco Unified CallManager 5.x or 4.2 as a TFTP server. Security settings on Cisco Unified CallManager can prevent Service Monitor from uploading configuration files. You must manually copy configuration and image files from Service Monitor to Cisco Unified CallManager TFTP server.

- Step 1** Select **Configuration > Sensor > TFTP Servers**. The TFTP Server Setup page appears.
- Step 2** Click **Add**. The TFTP Server Settings dialog box appears.

- Step 3** Enter data in the following fields:
- TFTP Server—IP address or DNS name.
  - Port Number—The customary port number is 69.
- Step 4** Click **OK**.



**Note** Copy the binary image file to each TFTP server that you add to Service Monitor.

## Copying the Binary Image File to the TFTP Server



**Note** For the binary image files that are supported with Service Monitor 2.0, see *Release Notes for Cisco Unified Service Monitor 2.0* at this URL: [http://www.cisco.com/en/US/partner/docs/net\\_mgmt/cisco\\_unified\\_service\\_monitor/2.0/release/notes/SrvMonRN.html](http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html).

- Step 1** Copy the binary image file, SvcMonAA2\_34.img, from *NMSROOT*\ImageDir on the Service Monitor server to the root location on the TFTP server. (*NMSROOT* is the directory where Service Monitor is installed; its default location is C:\Program Files\CSCOpX.)

## Deleting a TFTP Server

- Step 1** Select **Configuration > Sensor > TFTP Servers**. The TFTP Server Setup page appears.
- Step 2** Select a check box.
- Step 3** Click Delete. A confirmation dialog box appears.
- Step 4** Click **Yes**.

## Setting Up the Sensor Default Configuration

Use this procedure to:

- Enable or disable call metrics archiving—Service Monitor saves MOS data in the database. Optionally, you can also save the data to files.
- View the directory path for the archive data file and the Cisco 1040 image file.
- Create the default configuration file—QOVDefault.CNF specifies the primary and secondary Service Monitor to which a sensor can register.

- Step 1** Select **Configuration > Sensor > Setup**. The Setup page appears.
- Step 2** Update data described in the following table.

GUI Element	Description/Action
Call Metrics Archiving radio buttons	Select one of the following: <ul style="list-style-type: none"> <li>• Enable—After analysis, Service Monitor saves data from Cisco 1040s to disk files.</li> <li>• Disable—After analysis, Service Monitor discards data.</li> </ul> Default: Disable.
Data File Directory	Directory where files are stored if call metrics archiving is enabled. You cannot edit this field. <p><b>Note</b> Call metrics are archived to <i>NMSROOT/DataDir</i>. (<i>NMSROOT</i> is the directory where Service Monitor is installed. Its default location is <i>C:\Program Files\CSCOpX</i>.)</p>
Image File Directory	Directory where sensor binary image file and configuration files are stored locally: <i>NMSROOT/ImageDir</i> — <i>NMSROOT</i> is the directory where Service Monitor is installed; its default location is <i>C:\Program Files\CSCOpX</i> . You cannot edit this field. <p><b>Note</b> For more information, see <a href="#">Updating Image Files on Sensors, page 4-15</a>.</p>
Send traps every <i>n</i> minutes per endpoint	Enter a number greater than or equal to 5. Sensors send data to Service Monitor every 60 seconds. Service Monitor determines whether a violation has occurred and can potentially send a trap-a-minute for that endpoint. Use this setting to reduce the number of traps that Service Monitor sends for each endpoint. For a given endpoint, a trap is sent every <i>n</i> minutes and additional traps during that time are suppressed (not sent).
<b>Default Configuration to TFTP Server</b>	
Image Filename	Enter the image filename if you have downloaded a new image. See <a href="#">Updating Image Files on Sensors, page 4-15</a> . <p><b>Note</b> For the binary image filenames that are supported with Service Monitor 2.0, see <i>Release Notes for Cisco Unified Service Monitor 2.0</i> at this URL: <a href="http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html">http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html</a>.</p>
Primary Service Monitor	IP address or DNS name for the primary Service Monitor.
Secondary Service Monitor	IP address or DNS name for the secondary Service Monitor; blank if not set. (See <a href="#">Editing the Configuration for a Specific Sensor, page 4-10</a> .)

**Step 3** Click **OK**. Service Monitor stores the configuration file locally and copies it to the TFTP servers that are added to Service Monitor. For more information, see [Configuring TFTP Servers for Sensor Configuration and Image Files, page 4-3](#).

**Note**

If you are using Cisco Unified CallManager 5.x or 4.2 as a TFTP server, you must manually upload the default configuration from the image file directory on the Service Monitor server to Cisco Unified CallManager TFTP server.

## Configuring Sensors in Service Monitor

**Note**



You must configure DHCP and DNS correctly for Cisco 1040s to work properly. For more information, see *Quick Start Guide for Cisco 1040 Sensor*.

The following information is available for managing Cisco 1040s:

- [Understanding the Cisco 1040 Sensor Details Page, page 4-7](#)
- [Adding a Sensor to Service Monitor, page 4-8](#)
- [Editing the Configuration for a Specific Sensor, page 4-10](#)
- [Resetting a Sensor, page 4-11](#)
- [Deleting a Sensor, page 4-11](#)

## Understanding the Cisco 1040 Sensor Details Page

**Step 1** Select **Configuration > Sensor > Management**. The Cisco 1040 Sensor Details page displays information listed in the following table.

GUI Element	Description/Action
	Exports data from the Cisco 1040 Sensor Details page to a CSV or PDF file. See <a href="#">Exporting Data to a CSV or PDF File, page 4-8</a> .
	Opens a printer-friendly version of the data in another window; for printing from a browser window.
Check box column	Select Cisco 1040s that you want to edit, reset, or delete.
Name column	Click the name link to view details of the Cisco 1040 configuration. See <a href="#">Viewing Details in Service Monitor for a Specific Sensor, page 4-12</a> .
Sensor Address columns	Displays MAC and IP addresses for Cisco 1040. Click the MAC address link to launch an HTML page on the Cisco 1040. (See <a href="#">Viewing the Configuration Using the Sensor Web Interface, page 4-13</a> .)
Service Monitor columns	<p>Displays the following:</p> <ul style="list-style-type: none"> <li>• Primary—IP address or hostname of the primary Service Monitor defined for the Cisco 1040.</li> <li>• Secondary—IP address or hostname of the secondary Service Monitor defined for the Cisco 1040.</li> <li>• Registered with—IP address or hostname of the Service Monitor to which the Cisco 1040 is currently sending data. If the sensor is not yet registered, Waiting is displayed.</li> </ul> <p><b>Note</b> If you have recently changed the time on your system or, in rapid succession, stopped and started the QOVR process, Service Monitor might display a Cisco 1040 as registered with Waiting, while still receiving and processing syslog messages from the Cisco 1040. To fix this problem, see <a href="#">Restarting Processes to Update Sensor Registration Information in Service Monitor, page 4-8</a>.</p>
Reset Time column	The last date and time the Cisco 1040 was rebooted.
Edit button	Click to edit the Cisco 1040 configuration. See <a href="#">Editing the Configuration for a Specific Sensor, page 4-10</a> .

### Restarting Processes to Update Sensor Registration Information in Service Monitor

Service Monitor might show a Cisco 1040 waiting to register while receiving and processing syslogs from it; this problem can occur after a user does one of the following:

- Uses **pdterm** to stop the QOVR process, and, in quick succession, uses **pdexec** to start it again. To prevent this problem, wait at least 5 minutes between stopping and starting the QOVR process. To correct this problem:
  1. From the command line, stop the QOVR process again, by entering this command:

```
pdterm QOVR
```
  2. Wait at least 5 minutes.
  3. Enter this command:

```
pdexec QOVR
```
- Changes the time on the system where Service Monitor is installed without subsequently stopping and restarting the daemon manager. To correct this problem, stop and start the daemon manager from the command line by issuing the following commands:

```
Net stop crmdmgtd  
Net start crmdmgtd
```

### Exporting Data to a CSV or PDF File

After you click the export icon, a dialog box appears.

- 
- Step 1 Select one radio button: CSV or PDF.
- Step 2 Browse to the location where you want to store the file and click **OK**.
- 

## Adding a Sensor to Service Monitor

If a sensor is already registered with Service Monitor, you must select it and click the Edit button to update it. For more information, see [Editing the Configuration for a Specific Sensor, page 4-10](#).

- 
- Step 1 Select **Configuration > Sensor > Management**. The Cisco 1040 Sensor Detail page appears.
- Step 2 Click **Add**. The Add a Cisco 1040 Sensor dialog box appears.
- Step 3 Enter data listed in the following table.

GUI Element	Description/Action
Sensor Name	Enter up to 20 characters. This name is used on Service Monitor windows, such as reports.  <b>Note</b> Sensor names do not need to be unique. Sensors that register to Service Monitor using the default configuration file each use the name Cisco 1040.
Image File Name	Enter the binary image filename. The filename format is SvcMon<vendor code><Cisco 1040 type><major version>_<minor version><bugfix version>.img. For example:  SvcMonAA2_34.img  For the binary image filenames that are supported with Service Monitor 2.0, see <i>Release Notes for Cisco Unified Service Monitor 2.0</i> at this URL: <a href="http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html">http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html</a> .  For more information, see <a href="#">Viewing the Configuration Using the Sensor Web Interface, page 4-13</a> and <a href="#">Updating Image Files on Sensors, page 4-15</a> .
MAC Address	Enter the MAC address for the Cisco 1040 that you are adding.
Primary Service Monitor	Enter an IP address or DNS name of a host where Service Monitor is installed. The Cisco 1040 sends data to this Service Monitor unless it becomes unreachable.
Secondary Service Monitor	(Optional) Enter an IP address or DNS name of a host where another instance of Service Monitor is installed. The Cisco 1040 sends data to this Service Monitor only if the primary Service Monitor becomes unreachable. For more information, see <a href="#">Viewing the Configuration Using the Sensor Web Interface, page 4-13</a>
Description	Enter up to 80 characters.

- Step 4** Click **OK**. The configuration file is saved on the server where Service Monitor is installed and is copied to all TFTP servers. (See [Configuring TFTP Servers for Sensor Configuration and Image Files, page 4-3](#).) The configuration file is named QOV<MAC address>.CNF, where <MAC address> is the MAC address for the Cisco 1040. (To view the MAC address, see [Viewing the Configuration Using the Sensor Web Interface, page 4-13](#).)



**Note** If you are using Cisco Unified CallManager 5.x or 4.2 as a TFTP server, you must manually upload the MAC-specific configuration file from the image file directory on the Service Monitor server to Cisco Unified CallManager TFTP server. The image file directory is *NMSROOT/ImageDir*; *NMSROOT* is the directory where Service Monitor is installed; its default location is C:\Program Files\CSCOpX.

## Editing the Configuration for a Specific Sensor



**Note** Do not edit a Cisco 1040 configuration file using a text editor. Edit a Cisco 1040 configuration file using this procedure only.

**Step 1** Select **Configuration > Sensor > Management**. (For more information, see [Understanding the Cisco 1040 Sensor Details Page, page 4-7.](#))

**Step 2** Select the check box for a sensor and click **Edit**.

**Step 3** Update any of the following fields.

Fields	Description/Action
Sensor Name	If you want to change the name, enter up to 20 characters. This name is used on Service Monitor windows, such as reports.
MAC Address	Cisco 1040 MAC address. <b>Note</b> You cannot edit this field.
IP Address	Cisco 1040 IP address. <b>Note</b> You cannot edit this field. To update the IP address for a sensor, delete the sensor from Service Monitor and add it again.
Image File Name	Enter the binary image filename. The filename format is SvcMon<vendor code><Cisco 1040 type><major version>_<minor version><bugfix version>.img. For example:  SvcMonAA2_34 .img  Where: <ul style="list-style-type: none"> <li>• A is the vendor code for this Cisco 1040 (for internal use)</li> <li>• A is the Cisco 1040 type (for internal use)</li> <li>• 2 is the major release number</li> <li>• 3 is the minor release number</li> <li>• 4 is the bugfix number</li> </ul> For the binary image filenames that are supported with Service Monitor 2.0, see <i>Release Notes for Cisco Unified Service Monitor 2.0</i> at this URL: <a href="http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html">http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html</a> .  For more information, see <a href="#">Viewing the Configuration Using the Sensor Web Interface, page 4-13</a> and <a href="#">Updating Image Files on Sensors, page 4-15</a> .
Primary Service Monitor	Enter an IP address or DNS name of a host where Service Monitor is installed. The Cisco 1040 sends data to this Service Monitor unless it becomes unreachable.

Fields	Description/Action
Secondary Service Monitor	(Optional) Enter an IP address or DNS name of a host where Service Monitor is installed. The Cisco 1040 sends data to this Service Monitor only if the primary Service Monitor becomes unreachable.
Description	Enter up to 80 characters.

- Step 4** Click **OK**. Service Monitor saves the configuration file on the local server copies it to all TFTP servers. Then Service Monitor resets the sensor, so that it loads the updated configuration.



**Note** If you are using Cisco Unified CallManager 5.x or 4.2 as a TFTP server, you must manually upload the updated configuration file from the image file directory on the Service Monitor server to Cisco Unified CallManager TFTP server. Afterward, you must reset the sensor. (The image file directory is *NMSROOT/ImageDir*; *NMSROOT* is the directory where Service Monitor is installed; its default location is *C:\Program Files\CSCOpX*.)

## Resetting a Sensor

Use this procedure to boot a Cisco 1040. After a Cisco 1040 boots, it first uses DHCP to obtain the IP address of the TFTP server. From the TFTP server, Cisco 1040 obtains a configuration file. If the configuration file specifies a binary image file that is different from the currently installed image, Cisco 1040 also obtains the binary image file from the TFTP server.

- Step 1** Select **Configuration > Sensor > Management**. (For more information, see [Understanding the Cisco 1040 Sensor Details Page, page 4-7](#).)
- Step 2** Select check boxes for the Cisco 1040s that you want to reset.
- Step 3** Click **Reset**.

## Deleting a Sensor

Before you complete this procedure, delete the sensor from any sensor threshold groups. See [Editing a Sensor Group, page 5-10](#).

- Step 1** Delete the configuration file for the Cisco 1040 (*QOVmacaddress.CNF*) from the TFTP servers.
- Step 2** Select **Configuration > Sensors**. The Cisco 1040 Sensor Details page opens. (For more information, see [Understanding the Cisco 1040 Sensor Details Page, page 4-7](#).)
- Step 3** Select check boxes for the Cisco 1040s that you want to delete.
- Step 4** Click **Delete**. One of the following occurs:
- A confirmation dialog box appears.
  - An error message appears, displaying a list of sensor threshold groups to which the sensor belongs. You will need to remove the sensor from these sensor threshold groups and repeat this procedure.

Step 5 Click **OK**.




## Viewing the Configuration for a Sensor

Configuration data for a Cisco 1040 Sensor is stored in Service Monitor, is copied to a configuration file for the sensor on each TFTP server, and is copied down to the sensor (the sensor downloads the configuration from the TFTP server). You can look at the configuration details that are stored for a Cisco 1040 Sensor on each point: Service Monitor, TFTP server, and the sensor itself:

- [Viewing Details in Service Monitor for a Specific Sensor, page 4-12](#)
- [Viewing the Configuration File on the TFTP Server from a Sensor, page 4-13](#)
- [Viewing the Configuration Using the Sensor Web Interface, page 4-13](#)

## Viewing Details in Service Monitor for a Specific Sensor

To open the Cisco 1040 Sensor Detail dialog box, click the name link on the Cisco 1040 Sensor Details page. The Cisco 1040 Sensor Detail dialog box displays the Cisco 1040 Sensor Information table described here.

Field	Description/Action
	Exports data from the Cisco 1040 Sensor Information table to a CSV or PDF file. See <a href="#">Exporting Data to a CSV or PDF File, page 4-8</a> .
	Opens a printer-friendly version of the data in another window; for printing from a browser window.
	Opens context-sensitive online help.
Name link	Cisco 1040 user-entered name—Click to open a web interface on the Cisco 1040. See <a href="#">Viewing the Configuration Using the Sensor Web Interface, page 4-13</a> .
MAC Address	Cisco 1040 MAC address.
IP Address	Cisco 1040 IP address.
Primary Service Monitor	IP address or DNS name for the primary Service Monitor.
Secondary Service Monitor	IP address or DNS name for the secondary Service Monitor; blank if not set. (See <a href="#">Editing the Configuration for a Specific Sensor, page 4-10</a> .)
Registered with	IP address or DNS name for the Service Monitor that this Cisco 1040 is registered with.

Field	Description/Action
Image File Name	<p>Name of the image file installed on the Cisco 1040.</p> <p>For the binary image filenames that are supported with Service Monitor 2.0, see <i>Release Notes for Cisco Unified Service Monitor 2.0</i> at this URL:  <a href="http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html">http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html</a>.</p> <p><b>Note</b> If there is a more recent image file available on the TFTP server, you must edit the configuration file for the Cisco 1040, specifying the filename for the more recent image, and you must reset the Cisco 1040. (See <a href="#">Editing the Configuration for a Specific Sensor</a>, page 4-10.)</p>
Last Reset Time	Date and time that the Cisco 1040 was last reset. (See <a href="#">Resetting a Sensor</a> , page 4-11.)
Description	User-entered description for the Cisco 1040. (See <a href="#">Editing the Configuration for a Specific Sensor</a> , page 4-10.)

## Viewing the Configuration File on the TFTP Server from a Sensor

- 
- Step 1** From your browser, enter `http://<IP address or DNS name>/Communication` where IP address is the address of your Cisco 1040 and DNS name is the DNS name for the Cisco 1040. For example:
- ```
http://Cisco-1040-sj/Communication
```
- Step 2** The Communication Log File window displays the following information from the configuration file on the TFTP server for this Cisco 1040:
- Receiver—IP address or DNS name of each Service Monitor—primary and secondary—defined in the configuration file, separated by semicolons.
  - ID—User-defined name of the Cisco 1040 that uses this configuration file.
  - Image—Name of the binary image file that the Cisco 1040 should download and run from the TFTP server.
  - Last Updated—The last time that this configuration file was updated on the Service Monitor system.
  - CDPGlobalRunState—States whether CDP is enabled (true) or disabled (false).
  - SyslogPort—States the port protocol (UDP) and port number used for sending syslogs to Service Monitor.
  - SkinnyPort—States the port protocol (TCP) and port number used to communicate with Service Monitor.
- 

## Viewing the Configuration Using the Sensor Web Interface

To use the web interface to view the contents of the configuration file for this Cisco 1040 on the TFTP server, see [Viewing the Configuration File on the TFTP Server from a Sensor](#), page 4-13.

You can open a web interface to view the information stored on a Cisco 1040 in one of the following ways:

- Click the **(View)** link on the Cisco 1040 Sensor Details page. See [Understanding the Cisco 1040 Sensor Details Page, page 4-7](#).
- Enter `http://<IP address>` in your browser where IP address is the address of your Cisco 1040.

The Cisco 1040 web interface displays a Cisco 1040 Information window with the following information:

- **ID**—Cisco 1040 MAC address.
- **MAC Address**—Cisco 1040 MAC address.
- **Time stamp**—Current time on the Cisco 1040.
- **Status**—Status of the Cisco 1040; one of the following:
  - operational—Cisco 1040 is receiving RTP streams, analyzing data, and sending data to Service Monitor.
  - not communicating with receiver—The Service Monitor is unreachable.
- **Current Service Monitor**—Name of the Service Monitor to which the Cisco 1040 is sending data; this could be the primary or secondary Service Monitor.
- **TFTP IP Address**—TFTP server from which the Cisco 1040 downloads its binary image file and configuration file.
- **Switch IP Address**—Switch that this Cisco 1040 is connected to.
- **Switch Port**—Switch port that this Cisco 1040 is connected to.
- **Software Version**—Name of the binary image file installed on the Cisco 1040. See [Updating Image Files on Sensors, page 4-15](#).
- **Last Updated**—Last time that the configuration for the Cisco 1040 was updated on Service Monitor. See [Editing the Configuration for a Specific Sensor, page 4-10](#).

## Understanding How Sensors Register with Service Monitors

After you have configured a default sensor configuration file, `QOVDefault.CNF`, sensors can register with Service Monitor automatically. When a sensor registers automatically, Service Monitor uses the information in the default configuration file and creates a MAC-specific configuration file, `QOVmacaddress.CNF`, for the newly registered sensor. After a default sensor configuration file is created, if you want to add a sensor to Service Monitor manually, do so before plugging the sensor in.

After it is connected to a switch, a Cisco 1040 uses DHCP to obtain the IP address of the TFTP server. The Cisco 1040 checks the TFTP server for a configuration file, using the first of the following files that it finds:

- `QOVmacaddress.CNF`—Where MAC address is the MAC address of the Cisco 1040.
- `QOVDefault.CNF`—Default configuration file; used when a specific configuration file for the Cisco 1040 is not found (see [Setting Up the Sensor Default Configuration, page 4-4](#).)

## Understanding How a Sensor Registers with Service Monitor

A newly connected sensor registers to a Service Monitor using a specific configuration file for that sensor, `QOV<MAC address>.CNF` or using the default configuration file, `QOVDefault.CNF`. If using the default configuration file, from it, Service Monitor creates a MAC-specific configuration file, `QOV<MAC address>.CNF`, for the sensor.

There can be only one default configuration file on the TFTP server. The default configuration file specifies the primary Service Monitor. Therefore, sensors that use same TFTP server also use the same default configuration file and register with the same primary Service Monitor.

## Understanding Sensor Failover to a Secondary Service Monitor

A Cisco 1040 sends keepalive messages to the Service Monitor to which it is registered and receives acknowledgements from the Service Monitor. After sending three keepalives without receiving any acknowledgement, a Cisco 1040 starts a failover process to a secondary Service Monitor:

1. The Cisco 1040 sends a keepalive to the secondary Service Monitor that is listed in its configuration file and, upon acknowledgement, registers with that Service Monitor.
2. The secondary Service Monitor obtains the latest configuration file for this Cisco 1040 from the TFTP server, registering the Cisco 1040 as a failover Cisco 1040.
3. The Cisco 1040 starts sending syslog messages to the secondary Service Monitor while continuing to send keepalives to the primary Service Monitor to determine whether it is back up. The secondary Service Monitor processes the syslog messages from the failed-over Cisco 1040.
4. When the primary Service Monitor is back up, the Cisco 1040 unregisters from the secondary Service Monitor and registers to the primary Service Monitor again.

## Updating Image Files on Sensors

For the binary image files that are supported with Service Monitor 2.0, see *Release Notes for Cisco Unified Service Monitor 2.0* at this URL: [http://www.cisco.com/en/US/partner/docs/net\\_mgmt/cisco\\_unified\\_service\\_monitor/2.0/release/notes/SrvMonRN.html](http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html).

- 
- Step 1** When a new image file becomes available, download it from the Cisco software download site:
- a. Point your browser to <http://www.cisco.com>.
  - b. Select **Support > Software Downloads**.
  - c. Click the link for Cisco Unified Service Monitor to see and download available images.
- Step 2** Copy the image file to both of the following:
- The image file directory, `NMSROOT\CSCOpX\ImageDir`—Copy the image file here to retain a local copy as a backup. `NMSROOT` is the directory where Service Monitor is installed; its default location is `C:\Program Files\CSCOpX`.
  - The TFTP server—Copy the file here to provide access to it for Cisco 1040s that are configured to use the image. For TFTP server addresses, see [Configuring TFTP Servers for Sensor Configuration and Image Files](#), page 4-3



**Note** The image filename format is SvcMon<vendor code><Cisco 1040 type><major version>\_<minor version><bugfix version>.img; for example, SvcMonAA2\_34.img.

- Step 3** Modify the configuration for each Cisco 1040, entering the new image filename; see [Editing the Configuration for a Specific Sensor, page 4-10](#).

## Moving a Sensor from One Location to Another



**Warning** Before moving a sensor, read the regulatory compliance and safety information in *Quick Start Guide for Cisco 1040 Sensor*.

- Step 1** (Optional) Perform this step if you want to configure the Cisco 1040 to point to a new primary Service Monitor. Edit the configuration file for the Cisco 1040; for more information, see [Editing the Configuration for a Specific Sensor, page 4-10](#).
- Step 2** Unplug the Cisco 1040.
- Step 3** Plug in the Cisco 1040 at a new location. The Cisco 1040 downloads its configuration file from the TFTP server.



**Note** The Cisco 1040 retains its name after the move.

## Understanding Sensor Call Metrics Archive Files

Service Monitor stores the data it receives from Cisco 1040s in the database, where it remains available for reports for 30 days. Service Monitor can also save the data to files in a directory on the server if you have enabled call metrics archiving. To enable or disable call metrics archiving, see [Setting Up the Sensor Default Configuration, page 4-4](#).

Service Monitor creates a new data file daily at midnight. The data filename is QoV\_YYYYMMDD.csv where YYYY is the 4-digit year, MM is the two-digit month and DD is the two-digit day. For example, QOV\_20061101.csv is a data file for November 1, 2006. Service Monitor also backs up data files that exceed a size limit and deletes older data files; for more information, see [Understanding Sensor Archive File Purging, page 6-3](#).

You can use the data for further analysis or you can disable archiving. (Service Monitor does not send the archived data to other applications.) [Table 4-1](#) lists the format for call metrics data files.

**Table 4-1** Service Monitor Archived Call Metrics File Format

| Description                                            | Value                                                                                                                                                                                                       |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco 1040 MAC address                                 | MAC address of the Cisco 1040 Sensor                                                                                                                                                                        |
| Time stamp                                             | Date and time                                                                                                                                                                                               |
| Source device IP address                               | IPv4 address; for example:<br>172.020.119.043                                                                                                                                                               |
| Destination device IP address                          | IPv4 address, for example:<br>172.020.119.025                                                                                                                                                               |
| Codec of call data record                              | 2: G711Alaw 64k<br>3: G711Alaw 56k<br>4: G711Ulaw 64k<br>5: G711Ulaw 56k<br>6: G722 64k<br>7: G722 56k<br>8: G722 48k<br>10: G728<br>11: G729<br>12: G729AnnexA<br>15: G.729AnnexB<br>16: G729AnnexAwAnnexB |
| Calculated MOS score                                   | 2-digit number with an implied decimal point between the first and second digit                                                                                                                             |
| Primary cause of call degradation                      | J: Jitter<br>P: Packet loss                                                                                                                                                                                 |
| Actual packet loss in the previous minute              | <numeric value>                                                                                                                                                                                             |
| Actual jitter, in milliseconds, in the previous minute | <numeric value>                                                                                                                                                                                             |

**Note**

Call metrics data files remain on disk for 30 days. Service Monitor deletes them thereafter. If you would like to save these files, you must back them up using whatever method you normally use to back up your disk. For more information, see [Understanding Sensor Archive File Purging, page 6-3](#).

## Understanding Cisco 1040 Unreachable Trap

When a Service Monitor stops receiving keepalives from a Cisco 1040 that is registered to it, the Service Monitor generates a Cisco 1040 Unreachable SNMP trap. The Service Monitor sends this trap to up to four recipients. For more information, see [Setting Up the Sensor Default Configuration, page 4-4](#) and [MIBs Used and SNMP Traps Generated, page C-1](#).

**Note**

---

If you configure Operations Manager to receive traps from Service Monitor, the Cisco 1040 Unreachable trap is displayed on the Alerts and Events monitoring dashboard under the unidentified trap device type.

---

For information on Cisco Unified CallManager reachability, see [Understanding Last Contact Status and When to Verify Credentials](#), page 3-7.



## Setting Thresholds

---

The following topics are included:

- [Understanding Thresholds and Threshold Groups, page 5-1](#)
- [Configuring Global Thresholds, page 5-2](#)
- [Restoring Global Thresholds to Default Values, page 5-3](#)
- [Configuring CVTQ Groups, page 5-3](#)
- [Configuring Sensor Groups, page 5-8](#)

## Understanding Thresholds and Threshold Groups

Service Monitor uses thresholds to determine when a MOS value—reported from a sensor or included in CDRs from a Cisco Unified CallManager cluster—has fallen to an unacceptable level. When MOS falls below a threshold, Service Monitor sends a QoVMOSViolation trap to up to four trap receivers.

Service Monitor supplies global thresholds and provides default values for them. Service Monitor can use global thresholds to compare against MOS values reported from sensors or clusters. Since the MOS threshold values might vary depending upon the codec being used in a call, global thresholds include separate values for commonly used codecs such as these:

- G711Alaw64k
- G711Alaw56k
- G711Ulaw64k
- G711Ulaw56k
- G722 64K
- G722 56k
- G722 48k
- G728
- G729
- G729AnnexA
- G729AnnexB
- G729AnnexAwAnnexB

**Note**

For more information about codecs, see [Understanding Codecs: Complexity, Hardware Support, MOS, and Negotiation](http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a00800b6710.shtml) at this URL:  
[http://www.cisco.com/en/US/tech/tk1077/technologies\\_tech\\_note09186a00800b6710.shtml](http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a00800b6710.shtml)

You can update the global threshold default values to reflect MOS values below the average MOS seen in your system. By monitoring Service Monitor reports, you can determine average MOS values and then adjust global thresholds accordingly. You can also easily restore global thresholds to the default values that Service Monitor supplies.

If you would like to use different threshold values for particular sensors, clusters, or groups of endpoints reported on by either sensors or clusters, you can override global thresholds by adding these threshold groups:

- **CVTQ Groups**—A CVTQ group includes one or more clusters, two sets of endpoints, and one or more threshold values for commonly used codecs.
- **Sensor Groups**—A sensor group includes one or more sensors, two sets of endpoints, and one or more threshold values for commonly used codecs.

You can create up to 10 CVTQ groups and up to 10 sensor groups. CVTQ groups are prioritized from highest (one) to lowest (ten), as are sensor groups. In cases where an endpoint is included in more than one CVTQ group or more than one sensor group, Service Monitor compares MOS for the endpoint against the highest priority group that it belongs to.

For more information, see the following topics:

- [Configuring Global Thresholds, page 5-2](#)
- [Configuring CVTQ Groups, page 5-3](#)
- [Configuring Sensor Groups, page 5-8](#)

## Configuring Global Thresholds

Service Monitor compares MOS reported from sensors and clusters against global thresholds when no CVTQ group or sensor group setting is applicable. You cannot delete or clear global thresholds. You can update them and you can restore them to default values. You can override global thresholds by creating user-defined threshold groups; for more information, see [Configuring CVTQ Groups, page 5-3](#) and [Configuring Sensor Groups, page 5-8](#).

Use this procedure to update global thresholds.

- Step 1** Select **Thresholds > Global**. The Global Thresholds page appears, displaying the information in the following table.

| Fields and buttons | Description/Action                                                               |
|--------------------|----------------------------------------------------------------------------------|
| Codec              | Codec name. Grayed out because you cannot edit it.                               |
| <b>MOS</b>         |                                                                                  |
| Suggested Default  | Suggested default value for the codec.<br>Grayed out because you cannot edit it. |
| Current Value      | Enter a value from 0.0 to 5.0.                                                   |

| Fields and buttons                  | Description/Action                                                           |
|-------------------------------------|------------------------------------------------------------------------------|
| Revert to Suggested Defaults button | Click to set the current value of each codec to the suggested default value. |
| Apply button                        | Click to apply changes to current values.                                    |

- Step 2** Enter a new current value for any codec in the table and click **Apply**.
- 

## Restoring Global Thresholds to Default Values

Use this procedure to restore global threshold values to the suggested default values that are displayed on the Global Thresholds page.

- Step 1** Select **Thresholds > Global**. The Global Thresholds page appears.
- Step 2** Click the **Revert to Suggested Defaults** button.
- 

## Configuring CVTQ Groups

A CVTQ group includes one or more Cisco Unified CallManager clusters, two sets of endpoints, and threshold values for one or more commonly used codecs. You can define up to 10 CVTQ threshold groups; Service Monitor prioritizes the CVTQ threshold groups from 1 (highest priority) to 10 (lowest priority), initially reflecting the order in which you create the groups. (You can reprioritize them.) If an endpoint belongs to more than one CVTQ threshold group, Service Monitor uses the thresholds for the highest priority CVTQ threshold group.

- Step 1** Select **Thresholds > CVTQ Groups**. The CVTQ Threshold Groups page appears, displaying up to 10 user-defined CVTQ threshold groups with information described in the following table.

| Fields and Buttons     | Description/Action                                                                                                                                                                                                                            |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Check box column       | Select a CVTQ threshold group if you want to delete it.                                                                                                                                                                                       |
| Name column            | A unique user-defined name for the CVTQ threshold group.                                                                                                                                                                                      |
| Priority column        | A number from 1 to 10, indicating highest to lowest priority. To change priority, enter a different one- or two-digit number for each group in this column for two or more CVTQ threshold groups and click the <b>Update Priority</b> button. |
| Add button             | Click to add a CVTQ threshold group (up to a maximum of 10 CVTQ threshold groups). See <a href="#">Adding a CVTQ Threshold Group, page 5-4</a> .                                                                                              |
| Edit column            | Click the Edit link in this column to update this group. <a href="#">Editing a CVTQ Threshold Group, page 5-6</a> .                                                                                                                           |
| Delete button          | Select one or more check boxes and click the Delete button to delete a CVTQ threshold group.                                                                                                                                                  |
| Update Priority button | Click after entering unique numbers in the Priority column. The page will display again with the CVTQ threshold groups in priority order.                                                                                                     |



## Adding a CVTQ Threshold Group

When you add a CVTQ threshold group, it is assigned the lowest priority among existing CVTQ threshold groups. To adjust its priority, see [Updating CVTQ Threshold Group Priority, page 5-8](#).



**Note** You can add up to 10 CVTQ threshold groups.

- Step 1** Select **Thresholds > CVTQ Groups**. The CVTQ Threshold Groups page appears.
- Step 2** Click **Add**. The Add CVTQ Threshold Group page appears.
- Step 3** Enter data described in the following table.

| GUI Element              | Description/Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group Name field         | Enter a name. The name must be unique among all CVTQ groups.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Select Clusters list     | <p>These words appear in the list box: All current and future clusters.</p> <p><b>Note</b> If you do not select any clusters, the threshold values in this group apply to clusters that are currently managed and will be applied to clusters that are managed in the future.</p> <p>To select clusters:</p> <ol style="list-style-type: none"> <li>1. Click . The Select Clusters dialog box appears, displaying cluster IDs that Service Monitor has obtained from CMRs and CDRs.</li> <li>2. Select check boxes.</li> <li>3. Click <b>OK</b>.</li> </ol> <p>Default: None.</p> |
| Override Thresholds list | <p>Update thresholds:</p> <ol style="list-style-type: none"> <li>1. Click . The MOS Threshold Settings dialog box appears.</li> <li>2. For at least one codec, enter a MOS threshold value.</li> <li>3. Click <b>OK</b>.</li> </ol>                                                                                                                                                                                                                                                                                                                                               |
| Endpoint 1               | <p>Specify a source—or destination—endpoint by selecting one of these radio buttons and entering the appropriate data:</p> <ul style="list-style-type: none"> <li>• DN—Directory number. Enter an exact directory number or use wildcards (x) or a combination of numbers and wildcards to specify a range of directory numbers.</li> <li>• IP—IP address. Enter an exact IP address or use wildcards (*) or a combination of numbers and wildcards to specify a range of IP addresses.</li> </ul> <p><b>Note</b> For more information, see <a href="#">Specifying IP Addresses or Directory Numbers for Endpoints, page 2-3</a>.</p>                              |
| Endpoint 2               | <p>Specify a source—or destination—endpoint by selecting one of these radio buttons and entering the appropriate data:</p> <ul style="list-style-type: none"> <li>• DN—Directory number. Enter an exact directory number or use wildcards (x) or a combination of numbers and wildcards to specify a range of directory numbers.</li> <li>• IP—IP address. Enter an exact IP address or use wildcards (*) or a combination of numbers and wildcards to specify a range of IP addresses.</li> </ul> <p><b>Note</b> For more information, see <a href="#">Specifying IP Addresses or Directory Numbers for Endpoints, page 2-3</a>.</p>                              |

**Step 4** Click **OK**. The CVTQ Threshold Group page appears, displaying the newest CVTQ threshold group last in the list (in the lowest priority position).



## Editing a CVTQ Threshold Group

**Note**

To change CVTQ threshold group priority, see [Updating CVTQ Threshold Group Priority, page 5-8](#).

---

- Step 1** Select **Thresholds > CVTQ Groups**. The CVTQ Threshold Groups page appears.
- Step 2** Select a group and click **Edit**. The Edit CVTQ Threshold Group page appears.
- Step 3** Enter data described in the following table.

| GUI Element              | Description/Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group Name field         | You can change the name if you want to. The name must be unique among all CVTQ groups.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Select Clusters list     | <p>If no clusters are selected, these words appear in the list box: All current and future clusters.</p> <p><b>Note</b> If a cluster is already included in a CVTQ group when credentials for a cluster are deleted, the cluster remains in the group.</p> <p>To select clusters:</p> <ol style="list-style-type: none"> <li>1. Click . The Select Clusters dialog box appears, displaying cluster IDs that Service Monitor has obtained from CMRs and CDRs.</li> <li>2. Select check boxes.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><b>Note</b> If no clusters are selected, the threshold values in this group apply to clusters that are currently managed and will be applied to clusters that are managed in the future.</p> |
| Override Thresholds list | <p>Update thresholds:</p> <ol style="list-style-type: none"> <li>1. Click . The MOS Threshold Settings dialog box appears.</li> <li>2. For at least one codec, enter a MOS threshold value.</li> <li>3. Click <b>OK</b>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Endpoint 1               | <p>Specify a source—or destination—endpoint by selecting one of these radio buttons and entering the appropriate data:</p> <ul style="list-style-type: none"> <li>• DN—Directory number. Enter an exact directory number or use wildcards (x) or a combination of numbers and wildcards to specify a range of directory numbers.</li> <li>• IP—IP address. Enter an exact IP address or use wildcards (*) or a combination of numbers and wildcards to specify a range of IP addresses.</li> </ul> <p><b>Note</b> For more information, see <a href="#">Specifying IP Addresses or Directory Numbers for Endpoints, page 2-3</a>.</p>                                                                                                                                                                                 |
| Endpoint 2               | <p>Specify a source—or destination—endpoint by selecting one of these radio buttons and entering the appropriate data:</p> <ul style="list-style-type: none"> <li>• DN—Directory number. Enter an exact directory number or use wildcards (x) or a combination of numbers and wildcards to specify a range of directory numbers.</li> <li>• IP—IP address. Enter an exact IP address or use wildcards (*) or a combination of numbers and wildcards to specify a range of IP addresses.</li> </ul> <p><b>Note</b> For more information, see <a href="#">Specifying IP Addresses or Directory Numbers for Endpoints, page 2-3</a>.</p>                                                                                                                                                                                 |

## Updating CVTQ Threshold Group Priority

If the directory number or IP address for an endpoint is included in more than one CVTQ group, Service Monitor applies the thresholds for the highest priority CVTQ threshold group.

- 
- Step 1 Select **Thresholds > CVTQ Groups**. The CVTQ Threshold Group page appears, displaying up to 10 user-defined CVTQ threshold groups.
  - Step 2 Enter any unique numbers—up to two digits—in the Priority column.
  - Step 3 Click **Update Priority**. Service Monitor reorders the CVTQ threshold groups and displays them in priority order.
- 

## Deleting a CVTQ Threshold Group

- 
- Step 1 Select **Thresholds > CVTQ Groups**. The CVTQ Threshold Group page appears, displaying up to 10 user-defined CVTQ threshold groups.
  - Step 2 Select the check boxes for the CVTQ threshold groups that you want to delete.
  - Step 3 Click **Delete**. A confirmation dialog box is displayed.
  - Step 4 Click **Yes**. Service Monitor displays any remaining CVTQ threshold groups in priority order.
- 

## Configuring Sensor Groups

A sensor group includes one or more sensors, two sets of endpoints, and threshold values for one or more commonly used codecs. You can define up to 10 sensor threshold groups; Service Monitor prioritizes the sensor threshold groups from 1 (highest priority) to 10 (lowest priority), initially reflecting the order in which you create the groups. (You can reprioritize them.) If an endpoint belongs to more than one sensor threshold group, Service Monitor uses the thresholds for the highest priority sensor threshold group.

- Step 1** Select **Thresholds > Sensor Groups**. The Sensor Threshold Group page appears, displaying up to 10 user-defined sensor groups with information described in the following table.

| GUI Element            | Description/Action                                                                                                                                                                                                                    |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Check box column       | Select a sensor group to update its priority or to delete it.                                                                                                                                                                         |
| Name column            | A unique user-defined name for the sensor group. The name must be unique among all sensor groups.                                                                                                                                     |
| Priority column        | A number from 1 to 10, indicating highest to lowest priority. To change priority, enter a different one- or two-digit number for each group in this column for two or more sensor groups and click the <b>Update Priority</b> button. |
| Add button             | Click to add a sensor threshold group (up to a maximum of 10 CVTQ threshold groups). See <a href="#">Adding a Sensor Group, page 5-9</a> .                                                                                            |
| Edit column            | Click the Edit link in this column to update this group. See <a href="#">Editing a Sensor Group, page 5-10</a> .                                                                                                                      |
| Delete button          | Select one or more check boxes and click the Delete button to delete a CVTQ threshold group.                                                                                                                                          |
| Update Priority button | Click after entering unique numbers in the Priority column. The page will display again with the sensor threshold groups in priority order.                                                                                           |



## Adding a Sensor Group

When you add a sensor group, it is assigned the lowest priority among existing sensor groups. To adjust its priority, see [Updating Sensor Group Priority, page 5-11](#).



**Note** You can add up to 10 sensor groups.

- Step 1** Select **Thresholds > Sensor Groups**. The Sensor Threshold Group page appears.
- Step 2** Click **Add**. The Add Sensor Threshold Group page appears.
- Step 3** Enter data described in the following table.

| GUI Element              | Description/Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group Name field         | Enter a name. The name must be unique among all sensor groups.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Select Sensors list      | <p>These words appear in the list box: All current and future sensors.</p> <p><b>Note</b> If you do not select any sensors, the threshold values in this group apply to sensors that are currently managed and will be applied to sensors that are managed in the future.</p> <p>To select sensors:</p> <ol style="list-style-type: none"> <li>1. Click . The Select Sensors dialog box appears.</li> <li>2. Select check boxes.</li> <li>3. Click <b>OK</b>.</li> </ol> |
| Override Thresholds list | <p>Update thresholds:</p> <ol style="list-style-type: none"> <li>1. Click . The MOS Threshold Settings dialog box appears.</li> <li>2. For at least one codec, enter a MOS threshold value.</li> <li>3. Click <b>OK</b>.</li> </ol>                                                                                                                                                                                                                                      |
| Endpoint 1               | Enter the IP address of a voice gateway or an IP phone. To include a range of IP addresses, enter a partial IP address and use an asterisk (*) to indicate any number. Default: *.*.*.*.                                                                                                                                                                                                                                                                                                                                                                  |
| Endpoint 2               | Enter the IP address of a voice gateway or an IP phone. To include a range of IP addresses, enter a partial IP address and use an asterisk (*) to indicate any number. Default value: *.*.*.*.                                                                                                                                                                                                                                                                                                                                                            |



**Step 4** Click **OK**. The Sensor Threshold Group page appears, displaying the new sensor group threshold group last in the list (in the lowest priority position).

## Editing a Sensor Group



**Note** To change sensor group priority, see [Updating Sensor Group Priority, page 5-11](#).

- Step 1** Select **Thresholds > Sensor Groups**. The Sensor Threshold Group page appears.
- Step 2** Select a group and click the **Edit** link for a sensor group. The Edit Sensor Threshold Group page appears.
- Step 3** Enter data described in the following table.

| GUI Element              | Description/Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group Name field         | You can change the name if you want to. The name must be unique among all sensor groups.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Select Sensors list      | <p>If no sensors are selected, these words appear in the list box: All current and future sensors.</p> <p>To select sensors:</p> <ol style="list-style-type: none"> <li>1. Click . The Select Sensors dialog box appears.</li> <li>2. Select check boxes.</li> <li>3. Click <b>OK</b>.</li> </ol> <p><b>Note</b> If no sensors are selected, the threshold values in this group apply to sensors that are currently managed and will be applied to sensors that are managed in the future.</p> |
| Override Thresholds list | <p>Update thresholds:</p> <ol style="list-style-type: none"> <li>1. Click . The MOS Threshold Settings dialog box appears.</li> <li>2. For at least one codec, enter a MOS threshold value.</li> <li>3. Click <b>OK</b>.</li> </ol>                                                                                                                                                                                                                                                            |
| Endpoint 1               | Enter the IP address for a voice gateway or an IP phone. To include a range of IP addresses, enter a partial IP address and use an asterisk (*) to indicate any number. Enter *.*.*.* to include all IP addresses.                                                                                                                                                                                                                                                                                                                                                              |
| Endpoint 2               | Enter the IP address for a voice gateway or an IP phone. To include a range of IP addresses, enter a partial IP address and use an asterisk (*) to indicate any number. Enter *.*.*.* to include all IP addresses.                                                                                                                                                                                                                                                                                                                                                              |

## Updating Sensor Group Priority

If a sensor is included in more than one sensor group, Service Monitor applies the thresholds for the highest priority sensor threshold group.

- 
- Step 1** Select **Thresholds > Sensor Groups**. The Sensor Threshold Group page appears, displaying up to 10 user-defined sensor groups.
  - Step 2** Enter any unique numbers—up to two digits—in the Priority column.
  - Step 3** Click **Update Priority**. Service Monitor reorders the sensor groups and displays them in priority order.
-

## Deleting a Sensor Group

- 
- Step 1** Select **Thresholds > Sensor Groups**. The Sensor Threshold Group page appears, displaying up to 10 user-defined sensor groups.
  - Step 2** Select the check boxes for the sensor groups that you want to delete.
  - Step 3** Click **Delete**. A confirmation dialog box is displayed.
  - Step 4** Click **Yes**. Service Monitor displays any remaining sensor groups in priority order.
-



## Administering the System and Managing Data

---

This section contains the following topics:

- [Understanding Service Monitor Database Purging, page 6-1](#)
- [Understanding Sensor Archive File Purging, page 6-3](#)
- [Managing Log Files, page 6-3](#)
- [Configuring Users \(ACS and Non-ACS\), page 6-5](#)
- [Starting and Stopping Service Monitor Processes, page 6-8](#)
- [Using SNMP to Monitor Service Monitor, page 6-8](#)
- [Changing the Hostname on the Service Monitor Server, page 6-11](#)
- [Changing the IP Address on the Service Monitor Server, page 6-13](#)
- [Changing the Time on the Service Monitor Server, page 6-14](#)

### Understanding Service Monitor Database Purging

Cisco Unified Service Monitor (Service Monitor) can receive, process, and store call metrics in its database from these sources:

- The Cisco 1040s that are registered to it.
- The Cisco Unified CallManager clusters that are configured to allow database access to Service Monitor or to send data to Service Monitor (when configured as an Application Billing Server). For more information, see [Cisco Unified CallManager Configuration, page B-1](#).

Service Monitor stores the data for 30 days and runs a job daily to purge older data from the database. You can back up and restore the entire Service Monitor database.

- 

### Starting a Database Backup

Use this procedure to perform an immediate backup or a scheduled backup of the Service Monitor database.

- 
- Step 1** Click the CiscoWorks link in the upper-right corner of the Service Monitor home page. A new window opens.
- Step 2** In the Common Services pane, select **Server > Admin > Backup**, click Help, and follow the instructions.
- 

## Restoring the Database

To restore the database, you must use the command-line interface (instructions are available in online help) and you need to know the backup directory structure, which is described in [Table 6-1](#).

Use this procedure to locate the online help for restoring the database.

- 
- Step 1** Click the CiscoWorks link in the upper-right corner of the Service Monitor home page. A new window opens.
- Step 2** In the Common Services pane, select **Server > Admin > Backup**, click Help, and click the Help link to the Restoring Data topic.
- 



### Note

When you restore the database, logging settings return to the default value. As a result, only error messages are written to the log files. If you need additional information written to your log files to debug a problem, reset your logging settings. See [Managing Log Files and Enabling and Disabling Debugging](#), page 6-4.

The backup directory structure for the Service Monitor database includes the suite name, which is *qovr*:

- Format—*/generation\_number/suite[/directory]/filename*
- Example—*/1/qovr/qovr.db*

The backup directory structure is described in [Table 6-1](#).

**Table 6-1** Service Monitor Backup Directory Structure

| Option           | Description                           | Usage Notes                                                                                                                                         |
|------------------|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| generationNumber | Backup number                         | For example, 1, 2, and 3, with 3 being the latest database backup.                                                                                  |
| suite            | Application, function, or module      | When you perform a backup, data for all suites is backed up. The Service Monitor application suite is <i>qovr</i> .                                 |
| directory        | What is being stored                  | Suite applications (if applicable).                                                                                                                 |
| filename         | Specific file that has been backed up | Files include database (.db).<br>For Service Monitor, the following file is listed directly under <i>generationNumber/suite</i> :<br><i>qovr.db</i> |

## Changing the Password for the Service Monitor Database

A command line script is available to change database passwords, including the password for the Service Monitor database, `govr.db`. Instructions are available in online help.

- 
- Step 1** Click the CiscoWorks link in the upper-right corner of the Service Monitor home page. A new window opens.
- Step 2** Click Help. The help window opens.
- Step 3** Select the Index tab, scroll down to the entries for D, and select *database password changes*.
- 

## Understanding Sensor Archive File Purging



### Note

This topic is applicable to systems with sensors.

---

Optionally, Service Monitor archives call metrics data to files in a directory on the server. To enable and disable archiving, see [Setting Up the Sensor Default Configuration, page 4-4](#).

When archiving is enabled, by default, Service Monitor does the following:

- Creates a new data file daily at midnight.
- Creates a new data file whenever the current data file size exceeds 3 MB. When a file reaches this limit, Service Monitor does the following:
  - Backs it up—Appends *.n* to the filetype; for example, `.csv.1`, `.csv.2`, and so on up to the limit of 50 per day.
  - Creates a new data file—Retains the original filetype: `(.csv)`.
- Retains the data files for 30 days before deleting them. If you want to retain the data files for a longer period, you can back up the Service Monitor data files using the same method you use to back up your file system. (Common Services backs up the Service Monitor database only and does not include Service Monitor data files.)

## Managing Log Files

This section includes the following topics:

- [Understanding Sensor Syslog Handling, page 6-3](#)
- [Maintaining the Sensor History Log File, page 6-4](#)
- [Managing Log Files and Enabling and Disabling Debugging, page 6-4](#)

## Understanding Sensor Syslog Handling

Service Monitor receives and processes syslog messages from Cisco 1040s. After processing syslog messages, Service Monitor writes them to the syslog file, `syslog.log`, in `NMSROOT\log\govr`.

## Maintaining the Sensor History Log File

The history log file, `ServiceMonitorHistory.log`, contains records of Cisco 1040 events such as Cisco 1040 reset, configuration update, and errors. The history log file accumulates records and grows in size. If the file becomes too large, you should rename it to enable Service Monitor to start a fresh history log file.



**Note** Service Monitor does not back up the history log file. If you want to back it up, use the same method you use to back up your file system.

## Managing Log Files and Enabling and Disabling Debugging

This information is provided for troubleshooting purposes. Service Monitor log files (see [Table 6-2](#)) are located in the `NMSROOT\log\qovr` directory.



**Note** NMSROOT is the folder where Service Monitor is installed on the server. If you selected the default directory during installation, it is `C:\Program Files\CSCOpX`.

Use this procedure to increase or decrease the type—and quantity—of messages written to log files.

**Step 1** From the Service Monitor home page, select **Logging**. The Logging: Level Configuration page appears.



**Note** You cannot disable logging. Service Monitor always writes error and fatal messages to application log files.

**Step 2** For each Service Monitor functional module, the Error check box is always selected; you cannot deselect it. For a list of modules and related log files, see [Table 6-2](#).

To set all modules to Error, which is the default logging level:

- a. Click the **Default** button. A confirmation page is displayed.
- b. Click **OK**.

To change the logging level for individual modules:

- a. For each module that you want to change, select one (or deselect all) of the following logging levels:
  - Warning—Log error messages and warning messages
  - Informational—Log error, warning, and informational messages
  - Debug—Log error, warning, informational, and debug message



**Note** Deselecting all check boxes for a module returns it to Error, the default logging level.

- b. Review your changes. To cancel your changes, click the **Cancel** button. Otherwise, click the **Apply** button. Clicking the **Apply** button starts immediately resetting the changed logging levels for the Service Monitor functional modules.

Table 6-2 lists Service Monitor log files by function or module. If you request assistance, the Technical Assistance Center (TAC) might ask you to send them some of these log files.

**Table 6-2 Service Monitor Log Files by Module**

| Function/Module      | Log Files                                                                                                                                                            |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Handler         | DataHandler.log<br>DataHandler_stdout.log<br>DataHandler_sterr.log<br>dhError.log<br>LicenseCheck.log<br>ServiceMonitorHistory.log<br>tftpmanager.log<br>trapgen.log |
| Reports              | CVTQReports.log<br>SensorReports.log<br><b>Note</b> These files are located in NMSROOT\log\qovr \reports.                                                            |
| Skinny Communication | SkinnyServer.log                                                                                                                                                     |
| User Interface       | QovrUI.log                                                                                                                                                           |

## Configuring Users (ACS and Non-ACS)

What Service Monitor users can see and do is determined by the user role. There are two different mechanisms or *modes* for authenticating users:

- **Non-ACS**—You select a supported login module to provide authentication and authorization. By default, Common Services uses the CiscoWorks Local login module to assign roles, along with privileges associated with those roles, as described in the Permission Report. (You can generate a Permission Report by clicking the CiscoWorks link in the upper-right corner of the Service Monitor home page and selecting **Common Services > Server > Reports > Permission Report > Generate Report**.) For more information, refer to [Configuring Users Using Non-ACS Mode \(CiscoWorks Local Login Module\)](#), page 6-6.
- **ACS**—In ACS mode, authentication and authorization is provided by Cisco Secure Access Control Server (ACS). Cisco Secure ACS specifies the privileges associated with roles; however, Cisco Secure ACS also enables you to perform device-based filtering, so that users only see authorized devices. To use ACS mode, Cisco Secure ACS must be installed on your network and Service Monitor must be registered with Cisco Secure ACS. For more information, refer to [Configuring Users Using ACS Mode](#), page 6-6.

If Operations Manager uses ACS mode for authentication and authorization and Service Monitor is running on the same system, Service Monitor must also use ACS mode; otherwise, Service Monitor users will not have any permissions.

## Configuring Users Using Non-ACS Mode (CiscoWorks Local Login Module)

To add a user and specify the user role using CiscoWorks Local login module, select **Administration > Add Users**. After the Common Services Local User Setup window opens, click the Help button for information on the configuration steps.

Use the Permission Report to understand how each user role relates to tasks in Service Monitor.

- 
- Step 1** Click the CiscoWorks link in the upper-right corner of the Service Monitor home page. A new window opens.
  - Step 2** Select **Common Services > Server > Reports > Permission Report > Generate Report**.
  - Step 3** Scroll down until you find Cisco Unified Service Monitor.
- 

## Configuring Users Using ACS Mode

To use ACS mode for authentication and authorization, Cisco Secure ACS must be installed on your network and Service Monitor must be registered with Cisco Secure ACS.

- 
- Step 1** Verify the authentication, authorization, and accounting (AAA) mode:
    - a. Click the CiscoWorks link in the upper-right corner of the Service Monitor home page. A new window appears.
    - b. Select **Server > Security > AAA Mode Setup** and check which Type radio button is selected: ACS or Non-ACS.




---

**Note** If you select ACS mode, also select the Register all installed applications with ACS check box. Doing so ensures that Service Monitor tasks are exported to the Cisco Secure ACS server.

---

- Step 2** Verify whether Service Monitor is registered with Cisco Secure ACS (if ACS is selected) by logging in to Cisco Secure ACS.
- Step 3** To modify ACS roles, refer to the Cisco Secure ACS online help (on the Cisco Secure ACS server) for information on modifying roles.




---

**Note** If you modify Service Monitor roles using Cisco Secure ACS, your changes will be propagated to all other instances of Service Monitor that are registered with the same Cisco Secure ACS server.

---

## Using Service Monitor in ACS Mode

Before performing any tasks that are mentioned here, you must ensure that you have successfully completed configuring Cisco Secure ACS with Service Monitor. If you have installed Service Monitor after configuring the CiscoWorks Login Module to ACS mode, then Service Monitor users are not granted any permissions. However, the Service Monitor application is registered to Cisco Secure ACS.



### Note

The System Identity Setup user, defined when you installed Service Monitor, must be added to the Cisco Secure ACS, and this user must have Network Administrator privileges. For more information, click the CiscoWorks link in the upper-right corner of the Service Monitor home page and select **Common Services > Server > Security > Multi-Server Trust Management > System Identity Setup**.

CiscoWorks login modules enable you to add new users using a source of authentication other than the native mechanism (that is, the CiscoWorks Local login module). You can use the Cisco Secure ACS server for this purpose.

By default, the CiscoWorks Local login module authentication scheme has five roles in the ACS mode. They are listed here from least privileged to most privileged:

|                       |                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Help Desk             | User with this role has the privileges to access network status information from the persisted data. User does not have the privilege to contact any device or schedule a job that will reach the network.<br><br>Example: View details for Cisco 1040, setup, and default configuration. (Cannot perform modifications.)                                                     |
| Approver              | User with this role does not have any privileges. (Service Monitor does not assign any tasks to this user role.)                                                                                                                                                                                                                                                              |
| Network Operator      | User with this role has the privilege to perform all tasks that involve collecting data from the network. User does not have write access on the network.<br><br>Example: Set up Service Monitor, add, modify, delete Cisco 1040s.                                                                                                                                            |
| Network Administrator | User with this role has the privilege to change the network. User can also perform Network Operator tasks.<br><br>Example: Same as Network Operator.                                                                                                                                                                                                                          |
| System Administrator  | User with this role has the privilege to perform all system administration tasks. See the Permission report. (Click the CiscoWorks link in the upper-right corner of the Service Monitor home page and select <b>Common Services &gt; Server &gt; Reports &gt; Permission Report &gt; Generate Report</b> .)<br><br>Example: Enable and disable debugging; set logging level. |

Cisco Secure ACS allows you to modify the privileges to these roles. You can also create custom roles and privileges that help you customize Service Monitor to best suit your business workflow and needs. To modify the default privileges, see Cisco Secure ACS online help. (On Cisco Secure ACS, click **Online Documentation > Shared Profile Components > Command Authorization Sets**.)

## Modifying Roles and Privileges in Cisco Secure ACS

If another instance of Service Monitor is registered with the same Cisco Secure ACS, your instance of Service Monitor will inherit those role settings. Furthermore, any changes you make to Service Monitor roles will be propagated to other instances of Service Monitor through Cisco Secure ACS. If you reinstall Service Monitor, your Cisco Secure ACS settings will automatically be applied upon Service Monitor restart.

- 
- Step 1** Select **Shared Profile Components > Cisco Unified Service Monitor** and click the Service Monitor roles that you want to modify.
- Step 2** Select or deselect any of the Service Monitor tasks that suit your business workflow and needs.
- Step 3** Click **Submit**.
- 

## Starting and Stopping Service Monitor Processes

To start and stop Service Monitor processes, select the CiscoWorks link from the upper-right corner of the Service Monitor home page, select **Common Services > Server > Admin > Processes**, and click **Help** for instructions. [Table 6-3](#) provides a complete list of Service Monitor-related processes.

*Table 6-3 Service Monitor-Related Processes*

| Name                | Description                       | Dependency    |
|---------------------|-----------------------------------|---------------|
| QOVR                | Service Monitor server.           | QOVRDbMonitor |
| QOVRDbMonitor       | Service Monitor database monitor. | QOVRDbEngine  |
| QOVRDbEngine        | Service Monitor database.         | —             |
| QOVRMultiProcLogger | Service Monitor process logging.  | —             |
| SSHD                | Service Monitor SFTP server.      | —             |

## Using SNMP to Monitor Service Monitor

Service Monitor supports the system application MIB. This support enables you to monitor Service Monitor using a third-party SNMP management tool, so that you can:

- Consistently monitor multiple platforms—One platform on which Service Monitor resides and one or more on which applications in the Cisco Unified Management Suite reside.
- Assess the application health using the system application MIB, which provides the following information:
  - Applications that Service Monitor installed.
  - Processes associated with applications and current process status.
  - Processes that ran previously and application exit state.

For MIB implementation details and sample MIB walk, see [Appendix E, “Service Monitor Support for SNMP MIBs.”](#)

**Note**

You cannot uninstall the MIB support; however, you can stop Windows SNMP service and set the startup type to either Manual or Disabled. See [Enabling and Disabling Windows SNMP Service, page 6-10](#).

## Configuring Your System for SNMP Queries

To enable SNMP queries, SNMP service must be installed and enabled.

- 
- Step 1** Verify that SNMP service is installed and enabled on the server where Service Monitor is installed. See [Determining the Status of Windows SNMP Service, page 6-9](#).
- Step 2** If you determined that SNMP service was not installed, install Windows SNMP Service; see [Installing and Uninstalling Windows SNMP Service, page 6-9](#).
- 

## Determining the Status of Windows SNMP Service

Windows SNMP service is a Windows component that you can add or remove when you want to. To enable SNMP queries against the MIB that Service Monitor supports, SNMP service must be installed and enabled. You can verify the status of Windows SNMP service as follows.

- 
- Step 1** Open the Windows administrative tool Services window.
- Step 2** Verify the following:
- SNMP Service is displayed on the Windows administrative tool Services window; if so, Windows SNMP service is installed.

**Note**

To install Windows SNMP service, see [Installing and Uninstalling Windows SNMP Service, page 6-9](#).

---

- SNMP Service startup type is Automatic or Manual; if so, Windows SNMP service is enabled.

**Note**

To enable Windows SNMP service, see [Enabling and Disabling Windows SNMP Service, page 6-10](#).

---

## Installing and Uninstalling Windows SNMP Service

Windows online help provides instructions for adding and removing Windows components, such as Windows SNMP service. To locate the instructions, try selecting the Index tab in Windows online help and entering a keyword or phrase, such as *installing SNMP service*.

To uninstall Windows SNMP service, follow instructions in Windows help for removing Windows components.

## Enabling and Disabling Windows SNMP Service

You can enable or disable Windows SNMP service using the Windows administrative tool Services. For instructions to open the Services window, see [Windows online help](#).

---

**Step 1** Locate SNMP Service in the Services window. The status and startup type are displayed.




---

**Note** If SNMP Service is not displayed, Windows SNMP service is not installed; see [Installing and Uninstalling Windows SNMP Service, page 6-9](#).

---

**Step 2** Right-click SNMP Service and select Properties. The SNMP Service Properties window opens:

- To disable SNMP service, set Startup Type to Disable and click **OK**.
- To enable SNMP service, set Startup Type to Automatic or Manual and click **OK**.




---

**Note** To start SNMP service after you enable it, right-click SNMP Service and select Start.

---

## Configuring Security for SNMP Queries

To improve security, the SNMP set operation is not allowed on any object ID (OID). You should also modify the credentials for SNMP service to not use a default or well-known community string.




---

**Note** You do not need to restart SNMP service to modify credentials for it.

---

You can modify SNMP service credentials using the Windows administrative tool Services.

---

**Step 1** Locate SNMP Service in the Services window

**Step 2** Right-click SNMP Service and select Properties. The SNMP Service Properties window opens.

**Step 3** Select the Security tab.

**Step 4** Edit the accepted community names and click **OK**.

---

## Viewing the System Application MIB Log File

The system application MIB log file, SysAppl.log, is located on the server where Service Monitor is installed in *NMSROOT*\log.




---

**Note** NMSROOT is the directory where Service Monitor is installed on your system. If you selected the default directory during installation, it is C:\Program Files\CSCOpX.

---

# Changing the Hostname on the Service Monitor Server

To change the hostname for the Service Monitor server, you must update several files, reboot the server, and regenerate the self-signed security certificate. Afterward, you must update the configuration on Service Monitor.

## Changing the Hostname, Rebooting the Server, and Regenerating the Certificate



**Note** You will reboot the server twice during this procedure. You will also stop the daemon manager to perform some steps.

- Step 1** Change the hostname on the server as follows:
- Stop the daemon manager by entering the following command:  

```
net stop crmdmgtd
```
  - Change the hostname at **My Computer > Properties > Computer Name > Change**.
  - Prevent the daemon manager service from restarting after reboot. From Control Panel, or from Start, open Services and change the startup mode to Manual for the CW2000 Daemon Manager service.
  - Reboot the server.

- Step 2** Change the hostname in the md.properties file (*NMSROOT*\lib\classpath\md.properties).



**Note** *NMSROOT* is the directory where you installed Service Monitor. If you selected the default, it is C:\Program Files\CSCOpX.

- Step 3** Change the hostname in the following registry entries:
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet
  - HKEY\_LOCAL\_MACHINE\SOFTWARE\Cisco\Resource Manager



**Note** Look for all the instances of the old hostname under these registry entries, and replace them with the new hostname.

- Step 4** Change the hostname in these files:
- regdaemon.xml (*NMSROOT*\MDC\etc\regdaemon.xml):
    - Note the old hostname. You will need it to complete [Step 5](#).
    - Enter the new hostname in uppercase letters.
  - web.xml (*NMSROOT*\MDC\tomcat\webapps\classic\WEB-INF\web.xml).

- Step 5** Create a file, *NMSROOT*\conf\cmic\changehostname.info, containing the old hostname and new hostname in uppercase letters in the following format:

```
OLDHOSTNAME:NEWHOSTNAME
```




---

**Note** Hostnames in this file are case-sensitive; they must be entered in uppercase letters; the new hostname must exactly match the hostname entered in `regdaemon.xml`.

---

**Step 6** Delete the `gatekeeper.ior` file from this directory:

`NMSROOT\www\classpath`

**Step 7** If Service Monitor alone is installed on the server, skip to [Step 8](#). If Service Monitor is installed on the same server with Operations Manager, change all occurrences of the old hostname in the following files:

- `NMSROOT\objects\vhmsmarts\local\conf\runcmd_env.sh`
- `NMSROOT\conf\dfm\Broker.info`

**Step 8** If you do not know the password for the cmf database, reset the password as follows:

- a. Open a Command Prompt and go to `NMSROOT\bin`.
- b. Enter the following command:

```
perl dbpasswd.pl dsn=cmf npwd=newpassword
```

where `newpassword` is the new password.




---

**Note** Remember this password. You will need it to complete [Step 9](#).

---

**Step 9** To ensure that devices added before you changed the hostname are properly classified in Device Center, enter the following command:

```
dbisqlc -c "uid=cmfDBA;pwd=dbpassword;eng=cmfEng;dsn=cmf;dbf=NMSROOT\databases\cmf\cmf.db"
-q update PIDM_app_device_map SET app_hostname='NewhostName' where
app_hostname='OldhostName'
```

where:

- `dbpassword` is the Common Services database password.
- `NMSROOT` is the directory where you installed Service Monitor.
- `NewhostName` is the new hostname.
- `OldhostName` is the old hostname.

**Step 10** From the Control Panel, or from Start, open Services and change the startup mode to Automatic for the CW2000 Daemon Manager service.

**Step 11** Reboot the server.

**Step 12** Replace the old hostname with the new hostname in the self-signed security certificate and regenerate it:

- a. Select **Common Services > Server > Security > Certificate Setup**.
- b. For more information, click Help.

**Step 13** Reconfigure Service Monitor. See [Reconfiguring Service Monitor After a Hostname Change, page 6-13](#).


---

## Reconfiguring Service Monitor After a Hostname Change

You must complete this procedure after you complete the procedure [Changing the Hostname, Rebooting the Server, and Regenerating the Certificate](#), page 6-11.

- 
- Step 1** If Service Monitor is configured to send traps to Operations Manager:
- If Operations Manager is installed on the same server as Service Monitor, set up Service Monitor to send traps to the new hostname or IP address. See [Setting Up the Sensor Default Configuration](#), page 4-4.
  - If Operations Manager is installed on another server, on Operations Manager, delete the Service Monitor and add it again. For more information, see Operations Manager online help.
- Step 2** If you have Cisco 1040 sensors in your system, complete these steps:
- a. Change the IP address or hostname in each of the following configuration files:
    - The default configuration file—See [Setting Up the Sensor Default Configuration](#), page 4-4.
    - The specific configuration file for each Cisco 1040 managed by the Service Monitor—See [Editing the Configuration for a Specific Sensor](#), page 4-10.
  - b. Reset the Cisco 1040s. See [Resetting a Sensor](#), page 4-11.
- Step 3** If Service Monitor is monitoring a Cisco Unified CallManager version 5.x, update the IP address for Service Monitor configured as an Application Billing Server. For more information, see [Adding Service Monitor to Cisco Unified CallManager 5.x as a Billing Server](#), page B-4.
- 

## Changing the IP Address on the Service Monitor Server

- 
- Step 1** Stop the daemon manager by entering the following command:
- ```
net stop crmdmgt
```
- Step 2** Delete the gatekeeper.ior file from this directory:
- ```
NMSROOT\www\classpath
```
-  **Note** NMSROOT is the folder where Service Monitor is installed on the server. If you selected the default directory during installation, it is C:\Program Files\CSCOpX.
- 
- Step 3** Change the IP address of the Service Monitor server.
- Step 4** Allow 15 minutes to elapse from the time you completed step 1, then restart the daemon manager by entering the following command:
- ```
net start crmdmgt
```
- Step 5** Reconfigure Service Monitor. See [Reconfiguring Service Monitor After a Hostname Change](#), page 6-13.
-

# Changing the Time on the Service Monitor Server

After you change the time on the server where Service Monitor is installed, stop and start the daemon manager using this procedure.

---

**Step 1** From the command line, issue the following commands:

```
Net stop crmdmgt  
Net start crmdmgt
```

---



## Configuration Checklists and Tips

The following topics are included:

- [Initial Configuration Checklist, page A-1](#)
- [Understanding when You Can Expect to See Results, page A-2](#)
- [Optional Configuration Checklist, page A-2](#)

### Initial Configuration Checklist

[Table A-1](#) lists configuration tasks that you must complete before Service Monitor can start to monitor MOS and send traps.

**Table A-1** *Initial Configuration Task Checklist*

Tasks	Description and Reference
<b>Configuring Service Monitor and Cisco Unified CallManager (when Present in your Network)</b>	
	Configure Cisco Unified CallManager as described in <a href="#">Cisco Unified CallManager Configuration, page B-1</a> .
	Add credentials for Cisco Unified CallManagers to Service Monitor; see <a href="#">Understanding and Setting Cisco Unified CallManager Credentials, page 3-2</a> .
<b>Configuring Service Monitor and Sensors (when Present in your Network)</b>	
	Add at least one TFTP server. See <a href="#">Configuring TFTP Servers for Sensor Configuration and Image Files, page 4-3</a> .
	Set up the sensor default configuration file. See <a href="#">Setting Up the Sensor Default Configuration, page 4-4</a> .
	Copy the binary image file to the root location on the TFTP server. See <a href="#">Copying the Binary Image File to the TFTP Server, page 4-4</a> .
<b>Configuring Trap Receivers</b>	
	Service Monitor can send generated SNMP traps to up to four trap receivers. See <a href="#">Configuring Trap Receivers, page 3-1</a> .

### Server and Client Configuration Tasks

On the Service Monitor server, you should exclude the `NMSROOT\databases` directory from virus scanning. Problems can arise if database files are locked because of virus scanning.

**Note**

*NMSROOT* is the directory where Service Monitor is installed on your system. If you selected the default directory during installation, it is C:\Program Files\CSCOpX.

On Service Monitor clients, you must disable any software that you use to prevent popup windows from displaying. Service Monitor must be able to open multiple windows to display information.

## Understanding when You Can Expect to See Results

After you complete the tasks in [Table A-1](#), Service Monitor starts to receive, analyze, and present data as follows:

- Sensors send a record to Service Monitor every 60 seconds, reporting calculated MOS while a call is in progress. Therefore, Service Monitor can start to generate traps while the call ensues. Similarly, sensor data can be displayed in Service Monitor reports while the call is in progress.
- Call data records (CDRs) are only written by Cisco Unified CallManager after a call has completed. Although Service Monitor might obtain data from Cisco Unified CallManager every 60 seconds, Service Monitor cannot generate traps until the call is over. Similarly, CVTQ data cannot be displayed in Service Monitor reports until a call has completed.

## Optional Configuration Checklist

These tasks enable you to:

- Update and override the default global thresholds—one per codec—that Service Monitor uses to trigger trap generation.
- Generate most-impacted endpoint reports automatically on a nightly and weekly basis.

Tasks	Description and Reference
<b>Updating and Overriding Global Thresholds</b>	
	Update global threshold values. See <a href="#">Configuring Global Thresholds, page 5-2</a> .
	Override global threshold values, providing values for selected sensors. See <a href="#">Configuring Sensor Groups, page 5-8</a> .
	Override global threshold values, providing values for selected clusters. See <a href="#">Configuring CVTQ Groups, page 5-3</a> .
<b>Exporting Most-Impacted Endpoint Reports</b>	
	See <a href="#">Configuring Number of Endpoints and Export Settings for Impacted Endpoints Reports, page 3-11</a> .



# Cisco Unified CallManager Configuration



## Note

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

Service Monitor can collect and analyze data from Cisco Unified CallManagers only if you first configure Cisco Unified CallManager systems as described in these topics:

- [Configuration Tasks for Supported Cisco Unified CallManager Versions](#), page B-1
- [Configuring Cisco Unified CallManager](#), page B-2
- [Configuring MicroSoft SQLServer on Cisco Unified CallManager System](#), page B-6
- [Configuring Voice Gateways When VAD is Enabled](#), page B-8

## Configuration Tasks for Supported Cisco Unified CallManager Versions


For Service Monitor to obtain CVTQ data from a Cisco Unified CallManager, you first need to perform configuration tasks while logged in to:

- Cisco Unified CallManager—To access Cisco Unified CallManager Administration and Cisco Unified CallManager Serviceability.
- The server where Cisco Unified CallManager is installed—To access Microsoft SQLServer.

Depending on the Cisco Unified CallManager version that you use, you need to perform some subset of the tasks listed in this section. Where tasks themselves differ slightly from one Cisco Unified CallManager version to another, version-specific steps are noted in the procedures.

[Table B-1](#) lists the configuration tasks you must complete for each version of Cisco Unified CallManager that you want Service Monitor to obtain CVTQ data from.

Table B-1 Cisco Unified CallManager and Microsoft SQLServer Configuration Tasks

Configuration Task	Perform Task for These Cisco Unified CallManager Versions:		
	5.x	4.x	3.3.x
<b>Configure Cisco Unified CallManager</b>			
<a href="#">Activating the AXL Web Service on Unified Communications Manager, page B-3</a>	X	—	—
<a href="#">Setting Cisco Unified CallManager Service Parameters, page B-3</a>	X	X	X
<a href="#">Setting Cisco Unified CallManager Enterprise Parameters, page B-4</a>	X	X	X
<a href="#">Adding Service Monitor to Cisco Unified CallManager 5.x as a Billing Server, page B-4</a>	X	—	—
<b>Configure Microsoft SQLServer on the Server with Cisco Unified CallManager</b>			
<a href="#">Enabling Mixed Authentication in Microsoft SQL Server for CallManager 4.x, page B-6</a>	—	X	—
			<b>Note</b> Mixed authentication should be configured for 3.3.x by default. If it is not, you can use this procedure to configure mixed authentication for 3.3.x.
<a href="#">Adding Microsoft SQLServer User Accounts, page B-7</a>	—	X	X
 <p><b>Caution</b> Failure to complete this task as documented can prevent Unified Communications Manager from writing CDRs.</p>			
<b>Configure Voice Gateways</b>			
<a href="#">Configuring Voice Gateways When VAD is Enabled, page B-8</a>	X	X	—

## Configuring Cisco Unified CallManager

This section contains the following topics:

- [Activating the AXL Web Service on Unified Communications Manager, page B-3](#)
- [Setting Cisco Unified CallManager Service Parameters, page B-3](#)
- [Setting Cisco Unified CallManager Enterprise Parameters, page B-4](#)

- [Adding Service Monitor to Cisco Unified CallManager 5.x as a Billing Server, page B-4](#)

## Activating the AXL Web Service on Unified Communications Manager

Perform this procedure for Unified Communications Manager versions 5.x and later.

---

**Step 1** Launch Unified Communications Manager Serviceability.

**Step 2** Select **Tools > Service Activation**.

**Step 3** Select a server.




---

**Note** Activate the AXL Web Service on the Publisher node only.

---

**Step 4** Scroll down to Database and Admin Services and select **Cisco AXL Web Service**.

**Step 5** Click **Save**.

---

## Setting Cisco Unified CallManager Service Parameters




---

**Note** Set these parameters on each Cisco Unified CallManager in a cluster.

---

**Step 1** Log in to Cisco Unified CallManager Administration.

**Step 2** Go to the Service Parameters Configuration page as follows:

- For Cisco Unified CallManager 3.3 and 4.x, select **Service > Service Parameters**.
- For Cisco Unified CallManager 5.x, select **System > Service Parameters**.

The Service Parameters Configuration page appears.

**Step 3** Select the server and the service:

- Select the name of the Cisco Unified CallManager server. This is a Cisco Unified CallManager from which Service Monitor will gather data.
- Select the Cisco CallManager service.

**Step 4** Set these parameters:

- For Cisco Unified CallManager versions 3.3.x and 4.x:
  - CDR Enabled Flag—Scroll down to System. Set to **True**.
  - Call Diagnostics Enabled—Scroll down to Clusterwide Parameters (Device - General). Set to **True**.
- For Cisco Unified CallManager 5.x:
  - CDR Enabled Flag—Scroll down to System. Set to **True**.
  - Call Diagnostics Enabled—Scroll down to Clusterwide Parameters (Device - General). Set to **Enable Only When CDR Enabled Flag is True**.

Step 5 Click **Update**.

---

## Setting Cisco Unified CallManager Enterprise Parameters

Perform this procedure for Cisco Unified CallManager versions 3.3, 4.x, and 5.x.

---

- Step 1 Log in to Cisco Unified CallManager Administration.
- Step 2 Select **System > Enterprise Parameters**. The Enterprise Parameters Configuration page appears.
- Step 3 Scroll down to CDR Parameters and set these parameters:
- For Cisco Unified CallManager 3.3 and 4.x:
    - CDR File Time Interval (min)—Set to **1**.
    - CDR Format—Select **CDRs will be inserted into database**.
  - For Cisco Unified CallManager 5.x, set CDR File Time Interval (min) to **1**.
- Step 4 Click **Update**.
- 

## Adding Service Monitor to Cisco Unified CallManager 5.x as a Billing Server



**Note**

- Perform this task on Cisco Unified CallManager version 5.x only.
  - Perform this task only while Service Monitor is up and running.
- 

- Step 1 Launch Cisco Unified CallManager Serviceability.
- Step 2 Select **Tools > CDR Manageability**.
- Step 3 Scroll down to Billing Applications Server Parameters and click **Add New**.
- Step 4 Enter the following:
- Host Name / IP Address—Enter the IP address of the system where Cisco Unified Service Monitor is installed.
  - User Name—Enter smuser.



**Note**

Do not enter any username other than smuser.

---

- Password—Enter a password. The default password is smuser. To change this password:
  - Change it in Service Monitor first. (For more information, see [Configuring Other Settings, page 3-12](#).)
  - Enter the same password that you entered for smuser while configuring other settings in Service Monitor.



**Note** If you changed the password in Service Monitor and Cisco Unified CallManager does not immediately accept the new password, wait one minute and enter the new password again.

- Select SFTP Protocol.
- Directory Path—Enter /home/smuser/.



**Note** Do not enter any directory path other than /home/smuser.

**Step 5** Click **Add**.



**Note** In some cases, for CDR/CMR files to be delivered to a newly added billing server, it is necessary to first restart the CDR Repository Management Service.

- Step 1** From Cisco Unified CallManager Serviceability, select **Tools > Control Center - Network Services**.
- Step 2** From the list of Unified Communications servers, select the publisher.
- Step 3** Scroll down to CDR Services.
- Step 4** Select the **Cisco CDR Repository Manager** radio button.
- Step 5** Click the **Restart** button.

## Changing the Password for smuser in Cisco Unified CallManager 5.x



**Note** Perform this task on Cisco Unified CallManager version 5.x only.

The SFTP password for smuser in Service Monitor and the password for the Service Monitor Applications Billing Server smuser in Cisco Unified CallManager 5.x must be identical. Any time you change one, you must change the other to match. To change the SFTP password for smuser in Service Monitor, see [Configuring Other Settings, page 3-12](#).

Use this procedure to change the password for the Service Monitor Applications Billing Server smuser in Cisco Unified CallManager 5.x.

- Step 1** Launch Cisco Unified CallManager Serviceability.
- Step 2** Select **Tools > CDR Manageability**.
- Step 3** Scroll down to Billing Applications Server Parameters and double-click the link for the Service Monitor.
- Step 4** Enter a new password.




---

**Note** If you changed the password in Service Monitor and Cisco Unified CallManager does not immediately accept the new password, wait one minute and enter the new password again.

---

Do not change the values in any other fields; Host Name / IP Address, User Name, SFTP Protocol, and Directory Path must remain the same.

**Step 5** Click **Update**.

---

## Configuring MicroSoft SQLServer on Cisco Unified CallManager System

Service Monitor needs users accounts configured in Microsoft SQLServer on the Cisco Unified CallManager system to:

- Access CDRs from Cisco Unified CallManager 4.x and 3.3.x
- Access the device database (CCM0300, CCM030n) from Cisco Unified CallManager 3.3.x

## Enabling Mixed Authentication in Microsoft SQL Server for CallManager 4.x

Perform this task for Cisco Unified CallManager 4.x only.

---

- Step 1** Log on to the server where Cisco Unified CallManager is installed.
- Step 2** Select **Start > Programs > Microsoft SQL Server Enterprise Manager**.
- Step 3** Select **Console Root > Microsoft SQL Servers > SQL Server Group** and right-click (**local**). A dialog box appears.
- Step 4** Select the **Security** tab:
- a. Under Authentication, select **SQL Server and Windows**.
  - b. Click **OK**. A message appears, asking whether to restart the SQL server. Click **No**.




---

**Note** If Cisco Security Agent runs on the Unified Communications Manager server, it might block the message that asks whether to restart the SQL server and the change is not applied. To work around this problem, open Windows Services user interface and stop Cisco Security Agent. After you complete steps 4 b and 5, restart Cisco Security Agent.

---

**Step 5** Restart the SQL server.



**Note** Because restarting the SQL server interrupts call processing, you should perform these steps after normal business hours or during a window of time set aside for system maintenance.

- a. Select **Start > Settings > Control Panel > Administrative Tools > Services**. The Services window appears.
- b. Right-click MSSQLSERVER and click **Stop**. A list of services that will be stopped in addition to MSSQLSERVER will be displayed. Note them; you will need to start each one in step 5c.
- c. Right-click MSSQLSERVER and click **Start**. For each of the additional services that were stopped during the previous step, right-click the service and click **Start**.

## Adding Microsoft SQLServer User Accounts

Add Microsoft SQLServer user accounts for Unified Communications Manager 3.x and 4.x as directed in this topic.

Service Monitor needs a Microsoft SQLServer user account to access local databases on the system with Cisco Unified CallManager. Use this procedure to add user accounts on any of these Cisco Unified CallManager versions:

- 4.x—Add an account to enable Service Monitor to access the CDR database.
- 3.3.x—Add an account to enable Service Monitor to access the CDR database and the device database, named CCM030n; for example, CCM0300. Alternatively, add two accounts: one for the CDR database and another for the CCM030n database.

**Step 1** Log on to the server where Cisco Unified CallManager is installed.

**Step 2** Select **Start > Programs > Microsoft SQL Server Enterprise Manager > Security**.

**Step 3** Right-click **Logins** and select **New Login**. A window appears.

**Step 4** On the General tab:

- a. Enter a username.
- b. Select **SQL Authentication** and enter a password.



**Note** Make sure that SQL Authentication is selected and *not* Windows Authentication, which can sometimes be selected by default.

**Step 5** Select the Server Roles tab and select the System Administrators role.



**Caution** You must complete step 5; otherwise, you might prevent Unified Communications Manager from writing CDRs to the database.

**Step 6** Select the Database Access tab and do the following:

a. Select databases as follows:

- For Cisco Unified CallManager version 4.x, check the Permit column for the CDR database.
- For Cisco Unified CallManager version 3.3.x, check the Permit column for the CDR database and for the device database, named CCM030n; for example, CCM0300. Alternatively, select only one database, CDR or the device database, and continue creating the account. After creating one account, repeat the procedure to create another account for the other database.



**Note** Each time you upgrade Cisco Unified CallManager, the *n* in CCM030*n* is increased by 1 and a new device database is created. If there are multiple device databases, choose the most recent one, the one with the highest number; for example, CCM0302. If you upgrade Cisco Unified CallManager 3.3 after you complete this step, you must return to this procedure and repeat this step (Step 6).



**Note** Alternatively, select only one database, CDR or the device database, and continue creating the account. After creating one account, repeat the procedure to create another account for the other database.

At the bottom of the window, database roles for the selected databases are displayed; public is checked by default.

b. Check the db\_owner role (so that public and db\_owner are checked).



**Caution**

You must complete step 6b; otherwise, you can prevent Unified Communications Manager from writing CDRs to the database.

**Step 7** Click **OK**. A confirmation dialog box appears.

**Step 8** Confirm the password (previously entered in step 4b) by entering it again in the dialog box.

## Configuring Voice Gateways When VAD is Enabled

**Note** Enabling voice activation detection (VAD) can save bandwidth, but it can also impact Service Monitor MOS calculations and might cause noticeable or unacceptable clipping of words. VAD is enabled by default in Cisco IOS voice (under dial peer configuration), and disabled by default in Cisco Unified CallManager (under System > Service Parameters).

This information applies when using Cisco Unified CallManager versions 4.2 and later. When VAD is enabled on a voice gateway in a cluster, you can see lower MOS values in CVTQ reports for calls between the voice gateway and IP phones. You need to:

- Configure the comfort noise payload type to 13 (from the default of 19) on H.323, SCCP, and SIP gateways. Doing so enables Cisco IP phones and voice gateways to properly adjust the MOS calculation.



---

**Note** Performing this configuration does not affect the MOS values that are reported in Cisco 1040 Sensor reports.

---

- Be aware that low MOS will be reported for calls between Cisco IP phones and MGCP gateways on CVTQ reports. (Comfort noise payload type is not configurable on MGCP gateways.)





## MIBs Used and SNMP Traps Generated

### MIBS Used

Service Monitor uses the CISCO-SYSLOG-MIB to generate SNMP traps.

### SNMP Traps Generated

Cisco Unified Service Monitor (Service Monitor) generates the following traps:

- MOS violation
- Cisco 1040 unreachable

Trap details are provided as name-value pairs in clogHistMsgText field of the clogMessageGenerated notification. [Table C-1](#) lists details of the MOS violation SNMP trap.

**Table C-1** MOS Violation SNMP Trap

TAG	Description	Value
TT	Trap type	1: Data from sensor 3: Data from Cisco Unified CallManager cluster
01	Cisco 1040 sensor MAC address (when TT = 1) or Cisco Unified CallManager cluster ID (when TT = 3)	Text string.
02	Time stamp	<YYYYMMDDhhmm>
03	Threshold value	Sample value: 3.5.
A	Flag indicating actual or sampled data	0: Actual 1: Sampled (not used)
B	Source device IP address. The source device can be: <ul style="list-style-type: none"> <li>• An IP phone or a voice gateway (when TT = 1 and TT = 3).</li> <li>• A remote Cisco Unified CallManager (when TT = 3 and the call is an intercluster call).</li> </ul>	IPv4 address, for example: 172.20.4.18

Table C-1 MOS Violation SNMP Trap (continued)

TAG	Description	Value
C	Recipient device IP address. The recipient device can be: <ul style="list-style-type: none"> <li>• An IP phone or a voice gateway (when TT = 1 and TT = 3).</li> <li>• A remote Cisco Unified CallManager (when TT = 3 and the call is an intercluster call).</li> </ul>	IPv4 address, for example: 172.20.5.12
D	Codec of call data record (see also CDC in this table).	One of these: 2: G711Alaw 64k 3: G711Alaw 56k 4: G711Ulaw 64k 5: G711Ulaw 56k 6: G722 64k 7: G722 56k 8: G722 48k 10: G728 11: G729 12: G729AnnexA 15: G729AnnexB 16: G729AnnexAwAnnexB
E	MOS score calculated by the sensor (when TT = 1) or CVTQ (when TT = 3).	Sample value: 3.4
F	Primary cause of call degradation.	When TT = 1: <ul style="list-style-type: none"> <li>• J: Jitter</li> <li>• P: Packet Loss</li> </ul> When TT = 3, N/A
G	Actual packet loss in the previous minute.	Sample value: 0.0.
H	Actual jitter in milliseconds in the previous minute.	Sample value: 0 Value is NA when TT = 3

Table C-1 MOS Violation SNMP Trap (continued)

TAG	Description	Value
CDC	Codec of call data record.	One of these: <ul style="list-style-type: none"> <li>• G711Alaw64k</li> <li>• G711Alaw56k</li> <li>• G711Ulaw64k</li> <li>• G711Ulaw56k</li> <li>• G722 64k</li> <li>• G722 56k</li> <li>• G722 48k</li> <li>• G728</li> <li>• G729</li> <li>• G729AnnexA</li> <li>• G729AnnexB</li> <li>• G729AnnexAwAnnexB</li> </ul>
CCR	Cumulative Concealment Ratio—Cumulative ratio of concealment time over speech time observed after starting a call.	Sample value: 0.0 Value is NA when TT = 1
ICR	Interval Concealment Ratio—Interval-based average concealment rate; the ratio of concealment time over speech time for the last three seconds of active speech.	Sample value: 0.0 Value is NA when TT = 1
ICRmx	Interval Concealment Ratio Max—Maximum concealment ratio observed during the call.	Sample value: 0.0 Value is NA when TT = 1
CS	Concealment Seconds—Number of seconds during which some concealment is observed during a call.	Sample value: 0 Value is NA when TT = 1
SCS	Severely Concealed Seconds—Number of seconds during which a significant amount of concealment is observed. If, on average, the observed concealment is greater than fifty milliseconds or approximately five percent, speech is probably not very audible.	Sample value: 0 Value is NA when TT = 1
MLQK	MOS Listening Quality or CVTQ Score—The Cisco Voice Transmission Quality (CVTQ) algorithm provides an objective estimate of the mean opinion score (MOS) for listening quality (LQK), rating it from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream.  <b>Note</b> The CVTQ score can vary based on the type of codec that the Cisco Unified IP Phone uses.	Sample value: 4.5 Value is NA when TT = 1

**Table C-1** MOS Violation SNMP Trap (continued)

TAG	Description	Value
MLQKmn	MOS Listening Quality CVTQ Min—Minimum score observed since the beginning of a call; represents the worst-sounding eight-second interval.	Sample value: 4.1 Value is NA when TT = 1
MLQKmx	MOS Listening Quality CVTQ Max—Maximum score observed since the beginning of a call; represents the best sounding eight-second interval.	Sample value: 4.5 Value is NA when TT = 1
MLQKvr	Version of the CVTQ calculation.	Sample value: .95 Value is NA when TT = 1
DRTN	Duration of the call in seconds.	Sample value: 120 Value is NA when TT = 1
NST	Number of suppressed traps from start time to end time when TT = 1. For more information, see the entry for Send traps every <i>n</i> minutes in <a href="#">Setting Up the Sensor Default Configuration, page 4-4</a> .	Sample value: 9 Value is 0 when TT = 3
ST	Start time when TT = 1. Time when the first trap was sent out for the endpoint.	UTC time Value is 0 when TT = 3
ET	End time when TT = 1. Time when the most recent trap was sent out.	UTC time Value is 0 when TT = 3

[Table C-2](#) lists details of the Cisco 1040 unreachable SNMP trap.

**Table C-2** Cisco 1040 Unreachable SNMP Trap

TAG	Description	Value
TT	Trap type	2
01	Cisco 1040 ID	Cisco 1040 MAC address
02	Time stamp	<YYYYMMDDhhmm>



## Licensing

---

This appendix provides licensing information for Cisco Unified Service Monitor (Service Monitor). It contains the following sections:

- [Verifying Service Monitor Licensing, page D-1](#)
- [Obtaining and Registering Service Monitor Licenses, page D-2](#)
- [Using an Evaluation License, page D-3](#)
- [Determining License Size Exceeded, page D-3](#)

## Verifying Service Monitor Licensing

Use this procedure to determine the status and size (number of phones supported) of the Service Monitor license.

- 
- Step 1** Select the CiscoWorks link in the upper righthand corner of the Service Monitor home page. A new window opens.
- Step 2** Select **Common Services > Server > Admin > Licensing**. The Licensing Information page appears, displaying the information described in the following table.

Column	Description
Name	Abbreviated product name—SM.
Version	Product version— <i>A.b.c</i> , where <i>A</i> is the major version number, <i>b</i> is the minor version number, and <i>c</i> is the service pack number. For example, SM 2.0.0 indicates version 2.0 without service packs.
Size	<p>Limit—Indicates the cumulative number of phones that Service Monitor is licensed to support, up to a maximum of 30,000.</p> <p><b>Note</b> The licensing process permits you to install any valid licenses, even if, as a result, size exceeds the maximum value. To move a license from one Service Monitor server to another, call the Cisco Technical Assistance Center (TAC).</p>
Status	<p>One of the following:</p> <ul style="list-style-type: none"> <li>• Purchased—You have a registered, licensed product.</li> <li>• Evaluation—This license will expire on the expiration date; Service Monitor will stop running.</li> </ul>
Expiration Date	Date on which Service Monitor stops running. Applies to evaluation licenses.

## Obtaining and Registering Service Monitor Licenses

After you have installed Service Monitor, you might want to:

- Upgrade from an evaluation license to a purchased license for the same version of Service Monitor.
- Increase the number of phones that Service Monitor supports, up to a maximum of 30,000.



### Note

For information about licensing Service Monitor during installation or upgrade from an earlier version, see *Quick Start Guide for Cisco Unified Service Monitor 2.0*.

When you purchase Service Monitor software, whether for the product or for incremental support of phones, a Product Authorization Key (PAK) is shipped to you. Use this procedure after you receive a PAK.

**Step 1** Enter the PAK and the MAC address of the server where Service Monitor is installed at the following URL:

<http://www.cisco.com/go/license>

The license file will be e-mailed to you.

**Step 2** Copy the license file to the Service Monitor server with read permission for casuser.



### Note

Service Monitor uses casuser to perform tasks that require Administrator privileges.



**Note** If you copy a folder that contains the license file to the Service Monitor server, be sure to provide read permission for casuser on the folder as well as on the license file.

**Step 3** Register the license file.



**Caution**

This procedure registers a license even when, as a result, license size exceeds the maximum value. Service Monitor manages up to a maximum of 30,000 phones even if license sizes exceed these maximum values.

- a. Click the CiscoWorks link from the upper righthand corner of the Service Monitor home page.
- b. Select **Common Services > Server > Admin > Licensing**. The License Information page appears.
- c. Click the **Update** button. The Select License File dialog box appears.
- d. Browse to and select the license file:
  - Click the **Browse** button.
  - Browse to the location where you copied the license file in [Step 2](#).
  - Select the license file.
  - Click **OK**. The Licensing Information page is updated. For more information, see [Table D-1](#).

**Table D-1** License Registration Result

License registered...	Expected result on Licensing Information page
Upgrade from an evaluation license	Entry in the Status column changes from Evaluation to Purchased.
Increase number of phones supported	Entry in the Size column increases per license size.

## Using an Evaluation License

If you have installed the evaluation version of Service Monitor, when you start Service Monitor, a licensing reminder is displayed. If you fail to upgrade your evaluation license after it expires, access to Service Monitor functionality will be prohibited. To upgrade from an evaluation license, see [Obtaining and Registering Service Monitor Licenses, page D-2](#).

## Determining License Size Exceeded

Service Monitor supports a few more phones than the number specified by your licenses. (See [Verifying Service Monitor Licensing, page D-1](#).) If the number of phones exceeds the license size, you can purchase licenses to increase the number of phones supported—up to 30,000—or purchase an additional software license and install Service Monitor on an additional system. See [Obtaining and Registering Service Monitor Licenses, page D-2](#).

**Caution**

---

Service Monitor monitors up to the number of phones specified by your licenses plus a few more. When the number of phones in Service Monitor exceeds the limit, data from additional phones is not collected or analyzed.

---



## Service Monitor Support for SNMP MIBs

---

Service Monitor implements the system application MIB using SNMP v2 and supplies an SNMP subagent. You can use simple SNMP queries to monitor the health of applications in the Cisco Unified Communications Management suite that supports the MIB.

For information about configuring your system to use SNMP to manage Service Monitor and other Cisco Unified applications, see [Using SNMP to Monitor Service Monitor](#), page 6-8.

### System Application MIB Implementation

The system application MIB, defined in RFC 2287, provides applications installed, processes running for an application, and past run information. You can use the information in the system application MIB to determine the overall health of Service Monitor and drill down to the actual processes running for the application.

For more information about the system application MIB, you can browse MIB information at the following URL:

<http://www.cisco.com/cgi-bin/Support/Mibbrowser/mibinfo.pl?tab=4>

For an example of the data stored in this MIB, see the [Sample MIB Walk for System Application MIB](#), page E-7.

<http://www.cisco.com/cgi-bin/Support/Mibbrowser/mibinfo.pl?tab=4>

### System Application Resource MIB Tables

This section describes MIB tables that contain the following information:

- [Installed Packages](#), page E-2
- [Installed Elements](#), page E-2
- [Package Status Information](#), page E-3
- [Element Status Information](#), page E-4
- [Status of Packages when They Ran Previously](#), page E-5
- [Status of Elements when They Ran Previously](#), page E-5
- [Process Map](#), page E-7
- [Scalar Variables](#), page E-6

## Installed Packages

[Table E-1](#) stores information for installed packages for Service Monitor and other applications in the Cisco Unified Management Suite that support the system application MIB.

**Table E-1** *sysApplInstallPkgTable*

MIB Row Entry	Description from the MIB	Cisco Unified Communications Management Suite Usage
sysApplInstallPkgIndex	Part of the index for this table. An integer used only for indexing purposes. Generally monotonically increasing from 1 as new applications are installed.	Running number for each application registered with the SNMP subagent.
sysApplInstallPkgManufacturer	The manufacturer of the software application package.	Cisco Systems, Inc.
sysApplInstallPkgProductName	The name assigned to the software application package by the manufacturer.	Name provided when the application was registered with the SNMP subagent, such as Cisco Unified Service Monitor 2.0. <b>Note</b> Use this name to select an application to watch.
sysApplInstallPkgVersion	The version number assigned to the application package by the manufacturer of the software.	Version number such as 2.0.2, where 1 is the major version, 0 is the minor version, and 2 is the patch version or incremental device update (IDU) number.
sysApplInstallPkgSerialNumber	The serial number of the software assigned by the manufacturer.	“n/a”
sysApplInstallPkgDate	The date and time this software application was installed on the host.	—
sysApplInstallPkgLocation	The complete pathname where the application package is installed.	<i>NMSROOT</i> —Directory where Service Monitor is installed. If you selected the default directory during installation, it is C:\Program~1\CSCOPx.

## Installed Elements

For each entry in the installed packages table, [Table E-1](#), there can be many entries in the installed element table, [Table E-2](#). The number of installed elements for a package corresponds to the number of processes being monitored for that package.

[Table E-2](#) lists the contents of sysApplInstallElmtTable.

Table E-2 *sysApplInstallElmtTable*

MIB Row Entry	Description from the MIB	Cisco Unified Communications Management Suite Usage
sysApplInstallPkgIndex	Part of the index for this table. This value identifies the installed software package for the application of which this process is a part.	Value from <a href="#">sysApplInstallPkgTable</a> , <a href="#">Table E-1</a> .
sysApplInstallElmtIndex	Unique number across the applications.	Running number.
sysApplInstallElmtName	The name assigned to the software element package by the manufacturer.	Process name used in the daemon manager (not a file or executable name as specified in RFC 2287).
sysApplInstallElmtType	The type of element that is part of the installed application.	Default application(5).
sysApplInstallElmtDate	The date and time that this component was installed on the system.	<b>Note</b> All dates and times are formatted using SNMPv2 textual conventions.
sysApplInstallElmtPath	Install location for this application	<i>NMSROOT</i> —Directory where Service Monitor is installed. If you selected the default directory during installation, it is C:\Program~1\CSCOpX.
sysApplInstallInstallElmtSizeHigh	The installed file size in $2^{32}$ byte blocks.	Default 0 (not implemented).
sysApplInstallInstallElmtSizeLow	The installed file size in $2^{32}$ byte blocks.	Default 0 (not implemented).
sysApplInstallElmtRole	An operator-assigned value used in the determination of application status.	Value used in determining application status: <ul style="list-style-type: none"> <li>required(3)—Process that must run for the application to be considered running.</li> <li>unknown(5)—Optional process.</li> </ul>
sysApplInstallElmtModifyDate	The date and time that this element was last modified.	<b>Note</b> All dates and times are formatted using SNMPv2 textual conventions.
sysApplInstallCurSizeHigh	The current file size in $2^{32}$ byte blocks.	Default 0 (not implemented).
sysApplInstallCurSizeLow	The current file size in $2^{32}$ byte blocks.	Default 0 (not implemented).

## Package Status Information

[Table E-3](#) supplies current application status for Service Monitor and other applications in the Cisco Unified Management Suite that support the system application MIB.

Table E-3 *sysApplRunTable*

MIB Row Entry	Description from the MIB	Cisco Unified Communications Management Suite Usage
sysApplInstallPkgIndex	Part of the index for this table. This value identifies the installed software package for the application of which this process is a part.	Value from <a href="#">sysApplInstallPkgTable</a> , <a href="#">Table E-1</a> .
sysApplRunIndex	Part of the index for this table. An arbitrary integer used only for indexing purposes. Generally, monotonically increasing from 1 as new applications are started on the host, it uniquely identifies application invocations.	Running number.
sysApplRunStarted	The date and time that the application was started.	<b>Note</b> All dates and times are formatted using SNMPv2 textual conventions.
sysApplRunCurrentState	The current state of the running application instance. The possible values are running(1), runnable(2) but waiting for a resource such as CPU, waiting(3) for an event, exiting(4), or other(5).	This value is the measure of application health: <ul style="list-style-type: none"> <li>• running(1)—All required processes are running.</li> <li>• other(5)—One or more required processes are not running.</li> </ul> When all required processes stop or the daemon manager stops, this entry moves to the sysApplPastRun table.

## Element Status Information

[Table E-4](#) provides current status for processes that belong to each application that is currently running.

Table E-4 *sysApplElmtRunTable*

MIB Row Entry	Description from the MIB	Cisco Unified Communications Management Suite Usage
sysApplElmtRunInstallPkg	Part of the index for this table. This value identifies the installed software package for the application of which this process is a part.	Value from <a href="#">sysApplInstallPkgTable</a> , <a href="#">Table E-1</a> .
sysApplElmtRunInvocID	Part of the index for this table. This value identifies the invocation of an application of which this process is a part.	Default 0. <b>Note</b> Service Monitor processes run independently and are not invoked by any other process.
sysApplElmtRunIndex	Part of the index for this table. A unique value for each process running on the host.	Process ID in the operating system.

Table E-4 *sysAppElmtRunTable (continued)*

MIB Row Entry	Description from the MIB	Cisco Unified Communications Management Suite Usage
sysAppElmtRunInstallID	Part of the index for this table. The value of this object is the same value as sysAppInstallElmtIndex for the application element of which this entry represents a running instance.	Value from <a href="#">sysAppInstallElmtTable</a> , <a href="#">Table E-2</a> .
sysAppElmtRunTimeStarted	The time the process was started.	—
sysAppElmtRunState	The current state of the running process. The possible values are running(1), runnable(2) but waiting for a resource such as CPU, waiting(3) for an event, exiting(4), or other(5).	If all processes are running successfully, value is running(1). <b>Note</b> If the process terminates, the process entry moves to the sysElmtPastRun table.
sysAppElmtRunName	The full path and filename of the process.	—
sysAppElmtRunParameters	The starting parameters for the process.	—
sysAppElmtRunCPU	Hundredths of a second of the total system CPU resources consumed by this process.	Obtained from the operating system.
sysAppElmtRunMemory	The total amount of real system memory, measured in kilobytes, currently allocated to this process.	Obtained from the operating system.
sysAppElmtRunNumFiles	The number of regular files that the process currently has open.	Default 0 (not implemented).
sysAppElmtRunUser	The process owner's login name.	Either casuser or SYSTEM.

## Status of Packages when They Ran Previously

[Table E-5](#) contains the status of applications when they ran previously.

Table E-5 *sysAppIPastRunTable*

MIB Row Entry	Description from the MIB
sysAppInstallPkgIndex	Value from <a href="#">sysAppInstallPkgTable</a> , <a href="#">Table E-1</a> .
sysAppIPastRunIndex	Part of the index for this table. An arbitrary integer used only for indexing purposes. Generally monotonically increasing from 1 as new applications are started on the host, it uniquely identifies application invocations.
sysAppIPastRunStarted	The date and time that the application started. <b>Note</b> All dates and times are formatted using SNMPv2 textual conventions.
sysAppIPastExitState	The state of the application instance when it was terminated.
sysAppIPastRunEnded	The date and time the application instance was determined to be no longer running. <b>Note</b> All dates and times are formatted using SNMPv2 textual conventions.

## Status of Elements when They Ran Previously

[Table E-6](#) contains the status of processes when they ran previously.

Table E-6 *sysAppElmtPastRunTable*

MIB Row Entry	Description from the MIB
sysAppElmtPastRunInvocID	Part of the index for this table. Identifies the invocation of an application of which this process is a part.
sysAppElmtPastRunIndex	Part of the index for this table. A unique value for each process running on the host.
sysAppElmtPastRunInstallID	Part of the index for this table. The value of this object is the same value as the sysAppInstallElmtIndex for the application element of which this entry represents a running instance.
sysAppElmtPastRunTimeStarted	The time the process was started.
sysAppElmtPastRunTimeEnded	The time the process was ended.
sysAppElmtPastRunName	The full path and filename of the process.
sysAppElmtPastRunParameters	The starting parameters for the process.
sysAppElmtPastRunCPU	The last known number of hundredths of a second of the total system CPU resources consumed by this process.
sysAppElmtPastRunMemory	The last known total amount of real system memory, measured in kilobytes, allocated to this process before it terminated.
sysAppElmtPastRunNumFiles	The number of regular files that the process currently has open.
sysAppElmtPastRunUser	The process owner's login name.

## Scalar Variables

These variables are used to control MIB table size. You cannot update them.

Table E-7 *Scalars*

MIB Row Entry	Description from the MIB	Default Value
sysApplPastRunMaxRows	Maximum number of entries allowed in the sysApplPastRun table.	2000
sysApplPastRunTableRemItems	Counter for entries removed from the sysApplPastRun table after the maximum number (sysApplPastRunMaxRows) of entries are exceeded.	20 entries
sysApplPastRunTblTimeLimit	Maximum time that an entry in the sysApplPastRun table can exist before being removed.	86400 seconds (1 day)
sysApplElemPastRunMaxRows	Maximum number of entries allowed in the sysApplElmtPastRunTable.	2000 entries
sysApplElemPastRunTableRemItems	Counter for entries removed from the sysApplElmtPastRun table after the maximum number (sysApplElemPastRunMaxRows) of entries are exceeded.	20 entries
SysApplElemPastRunTblTimeLimit	Maximum time that an entry in the sysApplElmtPastRunTable can exist before being removed.	86400 seconds (1 day)
sysApplAgentPollInterval	Minimum interval at which polling to obtain the status of the managed resources occurs.	60 seconds

## Process Map

The sysApplMapTable contains one entry for each process currently running on the system. Table E-8 provides the index mapping from a process identifier to the invoked application, installed element, and installed application package.

**Table E-8** sysApplMapTable

MIB Row Entry	Description from the MIB
sysApplElmtRunIndex	Process identification number.
sysApplElmtRunInvocID	Invoked application (sysApplRunIndex).
sysApplMapInstallElmtIndex	Installed element (sysApplInstallElmtIndex).
sysApplMapInstallPkgIndex	Installed application package (sysApplInstallPkgIndex).

## Sample MIB Walk for System Application MIB

This example shows abridged output from a MIB walk of the SYSAPPL-MIB on a system where Cisco Unified Operations Manager and Service Monitor are installed.

```
***** SNMP QUERY STARTED *****
1: sysApplInstallPkgManufacturer.1 (octet string) Copyright (c) 2004 by Cisco Systems,
   Inc. [43.6F.70.79.72.69.67.68.74.20.28.63.29.20.32.30.30.34.20.62.79.20.43.69.73.63.6F.
   20.53.79.73.74.65.6D.73.2C.20.49.6E.63.2E (hex)]
2: sysApplInstallPkgManufacturer.2 (octet string) Copyright (c) 2004 by Cisco Systems,
   Inc. [43.6F.70.79.72.69.67.68.74.20.28.63.29.20.32.30.30.34.20.62.79.20.43.69.73.63.6F.
   20.53.79.73.74.65.6D.73.2C.20.49.6E.63.2E (hex)]
3: sysApplInstallPkgProductName.1 (octet string) Cisco Unified Service Monitor
   [43.69.73.63.6F.20.55.6E.69.66.69.65.64.20.53.65.72.76.69.63.65.20.4D.6F.6E.69.74.6F.7
   2 (hex)]
4: sysApplInstallPkgProductName.2 (octet string) Cisco Unified Operations Manager and
   Service Monitor
   [43.69.73.63.6F.20.55.6E.69.66.69.65.64.20.4F.70.65.72.61.74.69.6F.6E.73.20.4D.61.6E.6
   1.67.65.72.20.61.6E.64.20.53.65.72.76.69.63.65.20.4D.6F.6E.69.74.6F.72 (hex)]
5: sysApplInstallPkgVersion.1 (octet string) 2.0.0 [32.2E.30.2E.30 (hex)]
6: sysApplInstallPkgVersion.2 (octet string) 2.0.0 [32.2E.30.2E.30 (hex)]
7: sysApplInstallPkgSerialNumber.1 (octet string) n/a [6E.2F.61 (hex)]
8: sysApplInstallPkgSerialNumber.2 (octet string) n/a [6E.2F.61 (hex)]
9: sysApplInstallPkgDate.1 (octet string) 2006-10-12,15:36:45 [07.D6.0A.0C.0F.24.2D (hex)]
10: sysApplInstallPkgDate.2 (octet string) 2006-10-12,15:36:45 [07.D6.0A.0C.0F.24.2D
   (hex)]
11: sysApplInstallPkgLocation.1 (octet string) C:\PROGRA~1\CSCOpX
   [43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78 (hex)]
12: sysApplInstallPkgLocation.2 (octet string) C:\PROGRA~1\CSCOpX
   [43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78 (hex)]
13: sysApplInstallElmtName.1.1 (octet string) QOVR [51.4F.56.52 (hex)]
14: sysApplInstallElmtName.1.2 (octet string) QOVRDbEngine
   [51.4F.56.52.44.62.45.6E.67.69.6E.65 (hex)]
15: sysApplInstallElmtName.1.3 (octet string) QOVRDbMonitor
   [51.4F.56.52.44.62.4D.6F.6E.69.74.6F.72 (hex)]
16: sysApplInstallElmtName.1.4 (octet string) Apache [41.70.61.63.68.65 (hex)]
17: sysApplInstallElmtName.1.5 (octet string) CmfDbEngine
   [43.6D.66.44.62.45.6E.67.69.6E.65 (hex)]
18: sysApplInstallElmtName.1.6 (octet string) JRunProxyServer
   [4A.52.75.6E.50.72.6F.78.79.53.65.72.76.65.72 (hex)]
19: sysApplInstallElmtName.1.7 (octet string) Tomcat [54.6F.6D.63.61.74 (hex)]
20: sysApplInstallElmtName.1.8 (octet string) WebServer [57.65.62.53.65.72.76.65.72 (hex)]
```

21: sysApplInstallElmtName.2.9 (octet string) AdapterServer  
[41.64.61.70.74.65.72.53.65.72.76.65.72 (hex)]

22: sysApplInstallElmtName.2.10 (octet string) Apache [41.70.61.63.68.65 (hex)]

23: sysApplInstallElmtName.2.11 (octet string) CmfDbEngine  
[43.6D.66.44.62.45.6E.67.69.6E.65 (hex)]

24: sysApplInstallElmtName.2.12 (octet string) DCRServer [44.43.52.53.65.72.76.65.72  
(hex)]

25: sysApplInstallElmtName.2.13 (octet string) DfmBroker [44.66.6D.42.72.6F.6B.65.72  
(hex)]

26: sysApplInstallElmtName.2.14 (octet string) DfmServer [44.66.6D.53.65.72.76.65.72  
(hex)]

27: sysApplInstallElmtName.2.15 (octet string) EDS [45.44.53 (hex)]

28: sysApplInstallElmtName.2.16 (octet string) EPMDbEngine  
[45.50.4D.44.62.45.6E.67.69.6E.65 (hex)]

29: sysApplInstallElmtName.2.17 (octet string) EPMServer [45.50.4D.53.65.72.76.65.72  
(hex)]

30: sysApplInstallElmtName.2.18 (octet string) ESS [45.53.53 (hex)]

31: sysApplInstallElmtName.2.19 (octet string) FHDbEngine [46.48.44.62.45.6E.67.69.6E.65  
(hex)]

32: sysApplInstallElmtName.2.20 (octet string) FHServer [46.48.53.65.72.76.65.72 (hex)]

33: sysApplInstallElmtName.2.21 (octet string) GPF [47.50.46 (hex)]

34: sysApplInstallElmtName.2.22 (octet string) INVDbEngine  
[49.4E.56.44.62.45.6E.67.69.6E.65 (hex)]

35: sysApplInstallElmtName.2.23 (octet string) IVR [49.56.52 (hex)]

36: sysApplInstallElmtName.2.24 (octet string) IPIUdbEngine  
[49.50.49.55.44.62.45.6E.67.69.6E.65 (hex)]

37: sysApplInstallElmtName.2.25 (octet string) IPSLAServer  
[49.50.53.4C.41.53.65.72.76.65.72 (hex)]

38: sysApplInstallElmtName.2.26 (octet string) ITMDiagServer  
[49.54.4D.44.69.61.67.53.65.72.76.65.72 (hex)]

39: sysApplInstallElmtName.2.27 (octet string) Interactor [49.6E.74.65.72.61.63.74.6F.72  
(hex)]

40: sysApplInstallElmtName.2.28 (octet string) InventoryCollector  
[49.6E.76.65.6E.74.6F.72.79.43.6F.6C.6C.65.63.74.6F.72 (hex)]

41: sysApplInstallElmtName.2.29 (octet string) IPIUDataServer  
[49.50.49.55.44.61.74.61.53.65.72.76.65.72 (hex)]

42: sysApplInstallElmtName.2.30 (octet string) ITMOGSServer  
[49.54.4D.4F.47.53.53.65.72.76.65.72 (hex)]

43: sysApplInstallElmtName.2.31 (octet string) jrm [6A.72.6D (hex)]

44: sysApplInstallElmtName.2.32 (octet string) LicenseServer  
[4C.69.63.65.6E.73.65.53.65.72.76.65.72 (hex)]

45: sysApplInstallElmtName.2.33 (octet string) NOTSServer [4E.4F.54.53.53.65.72.76.65.72  
(hex)]

46: sysApplInstallElmtName.2.34 (octet string) PTMServer [50.54.4D.53.65.72.76.65.72  
(hex)]

47: sysApplInstallElmtName.2.35 (octet string) PIFServer [50.49.46.53.65.72.76.65.72  
(hex)]

48: sysApplInstallElmtName.2.36 (octet string) QoVMServer [51.6F.56.4D.53.65.72.76.65.72  
(hex)]

49: sysApplInstallElmtName.2.37 (octet string) SRSTServer [53.52.53.54.53.65.72.76.65.72  
(hex)]

50: sysApplInstallElmtName.2.38 (octet string) SIRServer [53.49.52.53.65.72.76.65.72  
(hex)]

51: sysApplInstallElmtName.2.39 (octet string) STServer [53.54.53.65.72.76.65.72 (hex)]

52: sysApplInstallElmtName.2.40 (octet string) Tomcat [54.6F.6D.63.61.74 (hex)]

53: sysApplInstallElmtName.2.41 (octet string) TISServer [54.49.53.53.65.72.76.65.72  
(hex)]

54: sysApplInstallElmtName.2.42 (octet string) TopoServer [54.6F.70.6F.53.65.72.76.65.72  
(hex)]

55: sysApplInstallElmtName.2.43 (octet string) VsmServer [56.73.6D.53.65.72.76.65.72  
(hex)]

56: sysApplInstallElmtName.2.44 (octet string) VHMIntegrator  
[56.48.4D.49.6E.74.65.67.72.61.74.6F.72 (hex)]

57: sysApplInstallElmtName.2.45 (octet string) VHMServer [56.48.4D.53.65.72.76.65.72 (hex)]

58: sysApplInstallElmtName.2.46 (octet string) ITMCTMStartup [49.54.4D.43.54.4D.53.74.61.72.74.75.70 (hex)]

59: sysApplInstallElmtName.2.47 (octet string) IPSLAPurgeTask [49.50.53.4C.41.50.75.72.67.65.54.61.73.6B (hex)]

60: sysApplInstallElmtName.2.48 (octet string) GpfPurgeTask [47.70.66.50.75.72.67.65.54.61.73.6B (hex)]

61: sysApplInstallElmtName.2.49 (octet string) FHPurgeTask [46.48.50.75.72.67.65.54.61.73.6B (hex)]

62: sysApplInstallElmtType.1.1 (integer) application(5)

63: sysApplInstallElmtType.1.2 (integer) application(5)

111: sysApplInstallElmtDate.1.1 (octet string) 2006-10-12,15:36:45 [07.D6.0A.0C.0F.24.2D (hex)]

112: sysApplInstallElmtDate.1.2 (octet string) 2006-10-12,15:36:45 [07.D6.0A.0C.0F.24.2D (hex)]

160: sysApplInstallElmtPath.1.1 (octet string) C:\PROGRA~1\CSCOpX [43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78 (hex)]

209: sysApplInstallElmtSizeHigh.1.1 (integer) 0

258: sysApplInstallElmtSizeLow.1.1 (integer) 0

307: sysApplInstallElmtRole.1.1 (integer) required(3)

356: sysApplInstallElmtModifyDate.1.1 (octet string) 2006-10-12,15:36:45 [07.D6.0A.0C.0F.24.2D (hex)]

405: sysApplInstallElmtCurSizeHigh.1.1 (integer) 0

454: sysApplInstallElmtCurSizeLow.1.1 (integer) 0

503: sysApplRunStarted.1.2 (octet string) 2006-10-18,17:13:24 [07.D6.0A.12.11.0D.18 (hex)]

505: sysApplRunCurrentState.1.2 (integer) running(1)

507: sysApplElmtRunInstallID.0.0.888 (integer) 0

563: sysApplElmtRunTimeStarted.0.0.888 (octet string) 2006-10-18,17:15:35 [07.D6.0A.12.11.0F.23 (hex)]

619: sysApplElmtRunState.0.0.888 (integer) running(1)

675: sysApplElmtRunName.0.0.888 (octet string)  
C:\PROGRA~1\CSCOpX\lib\vbroker\bin\osagent.exe  
[43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78.5C.6C.69.62.5C.76.62.72.6F.6B.65.72.5C.62.69.6E.5C.6F.73.61.67.65.6E.74.2E.65.78.65 (hex)]

731: sysApplElmtRunParameters.0.0.888 (octet string) -p 42342 [2D.70.20.34.32.33.34.32 (hex)]

787: sysApplElmtRunCPU.0.0.888 (timeticks) 0 days 00h:04m:27s.39th (26739)

843: sysApplElmtRunMemory.0.0.888 (integer) 676

899: sysApplElmtRunNumFiles.0.0.888 (integer) 0

955: sysApplElmtRunUser.0.0.888 (octet string) SYSTEM [53.59.53.54.45.4D (hex)]

1000: sysApplElmtRunUser.2.0.9220 (octet string) casuser [63.61.73.75.73.65.72 (hex)]

1011: sysApplElmtPastRunInstallID.2.0.6180 (integer) 44

```

1012: sysAppElmtPastRunTimeStarted.2.0.6180 (octet string) 2006-10-18,17:16:27
      [07.D6.0A.12.11.10.1B (hex)]
1013: sysAppElmtPastRunTimeEnded.2.0.6180 (octet string) 2006-11-5,12:45:49
      [07.D6.0B.05.0C.2D.31 (hex)]
1014: sysAppElmtPastRunName.2.0.6180 (octet string) C:\PROGRA~1\CSCOpX\bin\cwjava.exe
      [43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78.5C.62.69.6E.5C.63.77.6A.61.76.6
      1.2E.65.78.65 (hex)]
1015: sysAppElmtPastRunParameters.2.0.6180 (octet string)
      -Dcom.smarts.conf.clientConnect=C:\PROGRA~1\CSCOpX\objects\smarts\conf\clientConnect.c
      onf
      -Djava.security.policy=C:\PROGRA~1\CSCOpX\lib\jre2\lib\security\java.policy -Xmx128m
      -cw:jre
      C:\PROGRA~1\CSCOpX\lib\jre -cw:xrs -cp:pmf conf\vhm\vhm.classpath
      [2D.44.63.6F.6D.2E.73.6D.61.72.74.73.2E.63.6F.6E.66.2E.63.6C.69.65.6E.74.43.6F.6E.6E.6
      5.63.74.3D.43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78.5C.6F.62.6A.65.63.74.
      73.5C.73.6D.61.72.74.73.5C.63.6F.6E.66.5C.63.6C.69.65.6E.74.43.6F.6E.6E.65.63.74.2E.63
      .6F.6E.66.20.20.2D.44.6A.61.76.61.2E.73.65.63.75.72.69.74.79.2E.70.6F.6C.69.63.79.3D.4
      3.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78.5C.6C.69.62.5C.6A.72.65.32.5C.6C.
      69.62.5C.73.65.63.75.72.69.74.79.5C.6A.61.76.61.2E.70.6F.6C.69.63.79.20.2D.58.6D.78.31
      .32.38.6D.20.20.2D.63.77.3A.6A.72.65.20.43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4
      F.70.78.5C.6C.69.62.5C.6A.72.65.20.20.2D.63.77.3A.78.72.73.20.20.2D.63.70.3A.70.6D.66.
      20.63.6F.6E.66.5C.76.68.6D.5C.76.68.6D.2E.63.6C.61.73.73.70.61.74.68.20.20 (hex)]
1016: sysAppElmtPastRunCPU.2.0.6180 (timeticks) 0 days 00h:01m:52s.06th (11206)
1017: sysAppElmtPastRunMemory.2.0.6180 (integer) 970216
1018: sysAppElmtPastRunNumFiles.2.0.6180 (integer) 0
1019: sysAppElmtPastRunUser.2.0.6180 (octet string) SYSTEM [53.59.53.54.45.4D (hex)]
1020: sysApplPastRunMaxRows.0 (integer) 2000
1021: sysApplPastRunTableRemItems.0 (integer) 20
1022: sysApplPastRunTblTimeLimit.0 (integer) 86400
1023: sysAppElemPastRunMaxRows.0 (integer) 2000
1024: sysAppElemPastRunTableRemItems.0 (integer) 20
1025: sysAppElemPastRunTblTimeLimit.0 (integer) 86400
1026: sysApplAgentPollInterval.0 (integer) 60
1027: sysApplMap.2.888.0.0 (integer) 0

1082: sysApplMap.2.15056.0.28 (integer) 2
***** SNMP QUERY FINISHED *****

```



# Security Configuration with Cisco Secure ACS

This section describes how to configure Service Monitor with Cisco Secure ACS:

- [Before You Begin: Integration Notes, page F-1](#)
- [Configuring Service Monitor on Cisco Secure ACS, page F-2](#)
- [Verifying the Service Monitor and Cisco Secure ACS Configuration, page F-3](#)

## Before You Begin: Integration Notes



### Note

You can integrate Service Monitor with Cisco Secure ACS only if they are installed on separate systems because Service Monitor must be configured as an AAA client for Cisco Secure ACS.

For information about Common Services login modules and user roles, see [Configuring Users \(ACS and Non-ACS\), page 6-5](#).

This section contains the following notes, which you should read before you begin Cisco Secure ACS and Service Monitor integration:

- Multiple instances of the same application using the same Cisco Secure ACS will share settings. Any changes will affect all instances of that application.

For example: You have configured three Service Monitor servers with a Cisco Secure ACS, and you have created a role in Cisco Secure ACS for Service Monitor (say, *SMSU*). This role is shared by licensed versions of Service Monitor running on all three servers.

- A user can have different access privileges for different Cisco Unified Communications Management Suite applications.

For example: A user, *SMSU*, can have the following privileges:

- System Administrator for Service Monitor
- Network Operator for Operations Manager
- Network Administrator for Service Monitor
- Help Desk for Operations Manager

- If an application is configured with Cisco Secure ACS and then that application is reinstalled, it will inherit the old settings.




---

**Note** This is applicable if you are using Cisco Secure ACS version 3.2.3 or earlier.

---

- Using Common Services, you must do the following:
  - Set AAA Mode to ACS—You will need to supply the following information obtained from Cisco Secure ACS to complete this task: IP address or hostname, port, admin username and password, and shared secret key.




---

**Note** When you set Common Services AAA mode to ACS, all Cisco Unified Communications Management Suite applications running on the same server register with Cisco Secure ACS and use it for authentication and authorization. If Service Monitor and Operations Manager are installed on a server in ACS mode, all of the following use Cisco Secure ACS: Service Monitor, Operations Manager, and Common Services.

---

- Set up System Identity Setup username. This user was configured during Service Monitor installation. For more information, click the CiscoWorks link on the Service Monitor home page and select **Common Services > Server > Security > Multi-Server Trust Management > System Identity Setup**.
- On Cisco Secure ACS, you must configure a user with the same username as the System Identity Setup user. For Service Monitor, that user must have Network Administrator privileges on Cisco Secure ACS.
- In ACS mode, fallback is provided for authentication only. (Fallback options allow you to access Service Monitor if the login module fails, or you accidentally lock yourself or others out.) If authentication with ACS fails, Service Monitor does the following:
  1. Tries authentication using non-ACS mode (CiscoWorks local mode).
  2. If non-ACS authentication is successful, presents you with a dialog box with instructions to change the login mode to CiscoWorks local. (You can do so only if you have permission to perform that operation in non-ACS mode.)




---

**Note** You will not be allowed to log in if authentication fails in non-ACS mode.

---

For details on configuring ACS mode, click the CiscoWorks link on the Service Monitor home page and select **Common Services > Server > Security > AAA Mode** and click **Help**.

## Configuring Service Monitor on Cisco Secure ACS

After you complete setting the CiscoWorks server to ACS mode with Cisco Secure ACS, perform the following tasks on Cisco Secure ACS:

1. Click **Shared Profile Components** to verify that the Cisco Unified Service Monitor (Service Monitor) application entry is present.
2. Based on your authentication setting (per user or per group) on Cisco Secure ACS, click either User Setup or Group Setup.

On Cisco Secure ACS, verify the per user or per group setting for Cisco Unified Service Monitor using **Interface Configuration > TACACS + (Cisco IOS)**.

3. Assign the appropriate Service Monitor privileges to the user or group.

For Service Monitor, you must ensure that a user with the same name as the System Identity Setup user is configured on Cisco Secure ACS and has Network Administrator privileges.



**Note** You configured the System Identity Setup user during Service Monitor installation. For more information, click the CiscoWorks link on the Service Monitor home page and select **Common Services > Server > Security > Multi-Server Trust Management > System Identity Setup**.

You can modify roles on Cisco Secure ACS.

- 
- Step 1** Select **Shared Profile Components > Cisco Unified Service Monitor**.
  - Step 2** Click the Service Monitor role that you want to modify.
  - Step 3** Select the Service Monitor tasks that suit your business workflow and needs.
  - Step 4** Click **Submit**.
- 



**Note** If desired, you can also create new roles on Cisco Secure ACS.

## Verifying the Service Monitor and Cisco Secure ACS Configuration

After performing the tasks in [Configuring Service Monitor on Cisco Secure ACS, page F-2](#), verify the configuration as follows:

1. Log in to Service Monitor with the username defined in Cisco Secure ACS.
2. Try to perform tasks, to ensure that you can perform only those tasks that you are entitled to perform based on your privileges on Cisco Secure ACS.

For example: If your privilege is Help Desk, then:

- You should be able to view the Cisco 1040s that are managed by Service Monitor.
- You should not be able to add Cisco 1040s for Service Monitor to manage, and you should not be able to delete them.





---

## A

AAA mode [6-5, F-2](#)

accounts

CallManager Applications Billing Server [B-4](#)

Microsoft SQLServer

CDR database [B-7](#)

device database [B-7](#)

ACS mode

authentication [6-5](#)

Service Monitor, using in [6-8](#)

user roles and privileges, modifying [6-8](#)

users, configuring [6-6](#)

adding

CallManager credentials [3-4](#)

Cisco 1040 [4-8](#)

TFTP server to Service Monitor [4-3](#)

threshold groups

CVTQ [5-4](#)

sensor [5-9](#)

administering Service Monitor

SNMP, using to manage Service Monitor

queries, configuring for [6-9](#)

security, configuring for queries [6-10](#)

system application MIB log file, viewing [6-10](#)

Applications Billing Server. *See* accounts.

archiving call metrics

disabling [4-5](#)

enabling [4-5](#)

audience for this document [i-ix](#)

authentication

ACS

ACS mode [6-5](#)

and authorization [6-5](#)

fallback mode [F-2](#)

Microsoft SQLServer

enabling mixed authentication [B-6](#)

user accounts [B-7](#)

non-ACS mode [6-5](#)

AXL Web Service, activating [B-3](#)

---

## B

backing up

call metrics files [6-3](#)

Service Monitor

database [6-1](#)

data files [6-3](#)

---

## C

CallManager. *See* Cisco Unified CallManager

call metrics

archiving, enabling and disabling [4-5](#)

files [6-3](#)

backing up [6-3](#)

deleting [6-3](#)

cautions

significance of [i-x](#)

Unified Communications Manager database [B-7](#)

CDR database

account [B-7](#)

CallManager credential status [3-3](#)

password [B-7](#)

CDR DB. *See* CDR database

Cisco 1040

- adding 4-8
- deleting 4-11
- editing 4-10
- failover, understanding 4-15
- resetting 4-11
- unreachable, trap 4-17
- web interface 4-13
- Cisco Secure Access Control Server (ACS) 6-5
- Cisco Security Agent B-6
- Cisco Unified CallManager
  - configuring B-1
  - credentials 3-2
  - version used 3-9
- Cisco Unified Operations Manager, as a trap receiver 3-1
- clusters. *See* Cisco Unified CallManager
- codecs
  - in MOS violation SNMP trap C-3
  - reports, generated by 2-4
    - CVTQ report 2-7
    - sensor report 2-11
  - thresholds, setting
    - for CVTQ groups 5-4
    - for sensor groups 5-8
    - global values 5-2
- concealment
  - in CVTQ reports 2-10
  - in SNMP traps C-3
- configuring
  - Cisco 1040 4-10
  - Cisco Unified CallManager B-1
  - DHCP 4-6
  - DNS 4-6
  - sensor
    - default configuration file 4-4
    - primary Service Monitor 4-4
    - secondary Service Monitor 4-4
  - Service Monitor
    - as a billing server B-4
    - initially 2-2

- system, SNMP queries 6-9
- users 6-6
  - CiscoWorks local login module 6-6
  - using ACS mode 6-6
- credentials, CallManager
  - adding 3-4
  - deleting 3-3, 3-8
  - editing 3-6
  - verifying 3-2
- CVTQ
  - reports 2-7
  - threshold group
    - adding 5-4
    - deleting 5-8

---

## D

- daemon manager, starting and stopping 6-14
- database
  - cmf password, changing 6-12
  - directory and virus scanning software A-1
  - Service Monitor
    - backing up 6-1
    - password, changing 6-3
    - purging 6-1
    - restoring 6-2
- debugging, enabling 6-3
- deleting
  - CallManager credentials 3-8
  - Cisco1040 4-11
  - CVTQ group 5-8
  - files from TFTP server 4-11
  - sensor 4-11
  - sensor group 5-12
  - TFTP server from Service Monitor 4-4
- device database
  - account B-7
  - CallManager credential status for 3-3
  - name B-7

password [B-7](#)

device DB. *See* device database

DHCP, configuring [4-6](#)

directory number

- entering, as endpoint [5-11](#)
- wild cards, using in [2-3](#)

disabling

- call metrics archiving [4-5](#)
- debugging [6-3](#)

DN. *See* directory number

DNS, configuring [4-6](#)

documentation [i-x](#)

- audience for this [i-ix](#)
- typographical conventions in [i-ix](#)

downloading sensor image file [4-15](#)

---

## E

editing

- CallManager credentials [3-6](#)
- Cisco 1040
  - configuration [4-10](#)
  - default configuration [4-15](#)
- threshold groups
  - CVTQ [5-4](#)
  - sensor [5-9](#)

enabling

- call metrics archiving [4-5](#)
- debugging [6-4](#)

endpoint

- IP address [5-11](#)
- wild cards, using [2-3](#)

exporting

- most impacted endpoints reports, automatically [3-11](#)
- reports, manually [2-2](#)

---

## F

failover, Cisco 1040 [4-15](#)

filenames

- log files [6-5](#)
- reports, automatically generated [3-11](#)
- sensor configuration
  - default [4-14](#)
  - sensor-specific [4-14](#)
- sensor image [4-9](#)

files

- call metrics [6-3](#)
- configuration
  - sensor default [4-4](#)
  - sensor-specific [4-10](#)
- history log file, maintaining [6-4](#)
- log files [6-3](#)

---

## G

global thresholds [5-2](#)

- restoring default [5-2](#)
- updating [5-2](#)

---

## H

hostname, changing [6-11, 6-13](#)

HTTP

- CallManager credential status [3-3](#)
- username and password [3-6](#)

HTTPS

- CallManager credential status [3-3](#)
- username and password [3-6](#)

---

## I

image file

- downloading [4-15](#)

updating [4-15](#)

version [4-15](#)

#### IP address

entering as endpoint [5-11](#)

Service Monitor system, changing [6-13](#)

wild cards, used when entering [2-3](#)

---

## K

keepalive [4-15](#)

#### known phone count

understanding [3-8](#)

updating [3-10](#)

---

## L

#### license

evaluation, using [D-3](#)

##### file

obtaining [D-2](#)

registering [D-2](#)

limit [3-8](#)

exceeded [D-3](#)

increasing [D-2](#)

upgrading [D-2](#)

#### log files

by module [6-5](#)

debugging, enabling and disabling [6-3](#)

history [6-4](#)

location [6-3](#)

maintaining [6-4](#)

#### login, CiscoWorks

failure [F-2](#)

fallback mode [F-2](#)

login module [F-2](#)

---

## M

managing log files [6-3](#)

#### MIBs

system application, log file [6-10](#)

used by Service Monitor [C-1](#)

---

## N

#### non-ACS mode

authentication [6-5](#)

CiscoWorks Local Login module [6-6](#)

users, configuring [6-6](#)

---

## O

Operations Manager, as a trap receiver [3-1](#)

---

## P

#### password

CDR database [3-4, B-7](#)

CDRM database [3-3](#)

cmf database [6-12](#)

device database [3-4, B-7](#)

Service Monitor database [6-3](#)

SFTP [3-12, B-4](#)

smuser [3-12, B-5](#)

Permission Report [6-5](#)

#### phones

license limit [3-8](#)

monitored [3-8](#)

total known count [3-8](#)

updating known phone count [3-10](#)

popup blockers, disabling [A-1](#)

#### primary Service Monitor

configuring [4-4](#)

setting a [4-8](#)

- updating [4-10](#)
- viewing [4-12](#)

privileges, configuring on Cisco Secure ACS [6-8, F-2](#)

processes

- Service Monitor [6-8](#)
- starting and stopping [6-8](#)

---

## R

registering sensors [4-14](#)

reports

- configuring number of endpoints for [3-11](#)
- filenames, automatically generated [3-11](#)
- most impacted endpoints, exporting [3-11](#)

resetting Cisco 1040 [4-11](#)

resuming

- Cisco Unified CallManager cluster for monitoring [3-9](#)
- sensor for monitoring [3-9](#)

roles, user

- Cisco Secure ACS, configuring [6-8](#)
- Cisco Secure ACS, modifying [6-6](#)

---

## S

secondary Service Monitor

- configuring [4-4](#)
- setting a [4-8](#)
- updating [4-10](#)
- viewing [4-12](#)

security

- certificate [6-12](#)
- SNMP queries [6-10](#)

sensor

- registration explained [4-14](#)
- report [2-4](#)

Service Monitor

- hostname, changing [6-11, 6-13](#)
- IP address, changing [6-13](#)

- processes, stopping and starting [6-8](#)

SFTP

- directory path [B-4](#)
- password [3-12, B-4](#)
- server process [6-8](#)

smuser

- password, updating [B-5](#)
- username [3-12, B-4](#)

SNMP

- queries, configuring security for [6-10](#)
- trap receivers [3-1](#)
- Windows service [6-9](#)

SNMP, using to manage Service Monitor [6-8](#)

- SNMP queries, configuring for [6-9](#)
  - Windows SNMP Service, enabling or disabling [6-10](#)
  - Windows SNMP Service, installing and uninstalling [6-9](#)
  - Windows SNMP Service status, determining [6-9](#)
- SNMP queries, configuring security for [6-10](#)
- system application MIB log file, viewing [6-10](#)

SNMP MIBs, Service Monitor support for [E-1](#)

- sample MIB walk [E-7](#)
- system application MIB implementation [E-1](#)

SQL authentication on Cisco Unified CallManager [B-7](#)

starting

- daemon manager [6-14](#)
- Service Monitor [1-4](#)
- Service Monitor processes [6-8](#)

stopping

- daemon manager [6-14](#)
- QOVR process [4-8](#)
- Service Monitor processes [6-8](#)

suspending

- Cisco Unified CallManager cluster from monitoring [3-9](#)
- sensor from monitoring [3-9](#)

system administration [6-1](#)

system application MIB implementation [E-1](#)

- resource MIB tables [E-1](#)

- element status information [E-4](#)
- installed elements [E-2](#)
- installed packages [E-2](#)
- package status information [E-3](#)
- process map [E-7](#)
- scalar variables [E-6](#)
- status of elements previously run [E-3](#)
- status of packages previously run [E-5](#)
- sample MIB walk [E-7](#)

#### System Identity Setup User

- in Common Services [F-2](#)
- on Cisco Secure ACS [F-3](#)

---

## T

#### TFTP server

- adding to Service Monitor [4-3](#)
- deleting from Service Monitor [4-4](#)

#### thresholds

- global [5-2](#)
- group
  - CVTQ [5-4](#)
  - priority for CVTQ [5-8](#)
  - sensor [5-8](#)
  - sensor priority [5-11](#)

time, updating on the server [6-14](#)

#### trap receivers

- configuring [3-1](#)
- default port number for [3-1](#)
- Operations Manager [3-1](#)

#### traps, SNMP

- Cisco 1040 unreachable
  - definition [C-4](#)
  - understanding [4-17](#)
- from sensors, suppressing [4-5](#)
- MOS violation, definition [C-1](#)

typographical conventions in this document [i-ix](#)

---

## U

#### Unavailable

- device type, reason for [2-6](#)
- MOS, reason for [2-9](#)

#### updating

- image files [4-15](#)
- server time [6-14](#)

#### thresholds

- CVTQ group [5-6](#)
- global [5-2](#)
- sensor group [5-10](#)

#### users

- configuring [6-6](#)
  - using ACS mode [6-6](#)
  - using CiscoWorks local login module [6-6](#)

#### privileges

- modifying [6-8](#)
- Permission Report [6-5](#)

roles [6-8, F-1](#)

System Identity Setup User [F-1](#)

---

## V

verifying CallManager credentials [3-3](#)

#### versions

- Cisco 1040 image file [4-15](#)
- Cisco Unified CallManager [B-1](#)

#### viewing

- CallManager credential status [3-3](#)
- log files by module [6-5](#)
- sensor configuration
  - in Service Monitor [4-12](#)
  - on Cisco 1040 [4-13](#)
  - on TFTP server [4-13](#)

virus scanning software [A-1](#)

---

## W

warnings, significance of [i-x](#)

### Windows SNMP Service

disabling [6-10](#)

enabling [6-10](#)

installing [6-9](#)

status, determining [6-9](#)

uninstalling [6-9](#)

