



QUICK START GUIDE



Cisco Unified Service Monitor 2.0.1

- 1** SUPPLEMENTAL LICENSE AGREEMENT
- 2** Cisco Unified Service Monitor Overview
- 3** Server and Client System Requirements
- 4** Installation and Upgrade Paths
- 5** Installing Cisco Unified Service Monitor
- 6** Upgrading to Cisco Unified Service Monitor 2.0.1
- 7** Starting Cisco Unified Service Monitor
- 8** Uninstalling and Reinstalling Service Monitor
- 9** Where to Go Next
- 10** Related Documentation
- 11** Obtaining Documentation, Obtaining Support, and Security Guidelines

1 SUPPLEMENTAL LICENSE AGREEMENT

SUPPLEMENTAL LICENSE AGREEMENT FOR CISCO SYSTEMS NETWORK MANAGEMENT SOFTWARE: CISCO UNIFIED SERVICE MONITOR.

IMPORTANT-READ CAREFULLY: This Supplemental License Agreement (“SLA”) contains additional limitations on the license to the Software provided to Customer under the End User License Agreement between Customer and Cisco. Capitalized terms used in this SLA and not otherwise defined herein shall have the meanings assigned to them in the End User License Agreement. To the extent that there is a conflict among any of these terms and conditions applicable to the Software, the terms and conditions in this SLA shall take precedence.

By installing, downloading, accessing or otherwise using the Software, Customer agrees to be bound by the terms of this SLA. If Customer does not agree to the terms of this SLA, Customer may not install, download or otherwise use the Software. When used below, the term “server” refers to central processor unit.

1. ADDITIONAL LICENSE RESTRICTIONS.

- **Installation and Use.** The Software components are provided to Customer solely to install, update, supplement, or replace existing functionality of the applicable Network Management Software product. Customer may install and use the following Software components:
 - CiscoWorks Common Services: Contains shared resources used by other components in this bundle. In many cases, all components in this bundle can be installed on a single server.
 - Cisco Unified Service Monitor: May be installed on one (1) server in Customer's network management environment.
- **Number of IP Phones.** For each Software license granted, Customer may install and run the Software on a single server to manage the number of IP phones specified in the license file provided with the Software, or as specified in the Software License Claim Certificate. Customers whose requirements exceed the IP phone limit must purchase upgrade licenses or additional copies of the Software. The IP phone limit is enforced by license registration.
- **Reproduction and Distribution.** Customer may not reproduce nor distribute the Software.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

Please refer to the Cisco Systems, Inc. End User License Agreement.

2 Cisco Unified Service Monitor Overview

Cisco Unified Service Monitor (Service Monitor), a product from the Cisco Unified Communications Management Suite, receives and analyzes data from these sources when they are installed in your voice network and configured properly:

- Cisco Unified Communications Manager (Unified Communications Manager) clusters—Retain Call Detail Records (CDRs) and Call Management Records (CMRs). CDRs include Mean Opinion Score (MOS) values that were calculated on IP phones and voice gateways using the Cisco Voice Transmission Quality (CVTQ) algorithm.



Note

Starting with versions 4.3, 5.1, and 6.0, the product we formerly referred to as Cisco Unified CallManager will be called Cisco Unified Communications Manager (Unified Communications Manager). Versions earlier than 4.3 and 5.0 retain the Cisco Unified CallManager name. Throughout this document, any reference to Unified Communications Manager can also be understood to refer to Cisco Unified CallManager, unless explicitly noted.

For Unified Communications Manager versions that Service Monitor supports, see *Release Notes for Cisco Unified Service Monitor 2.0.1*. For information about configuring Unified Communications Manager clusters to work with Service Monitor, see *User Guide for Cisco Unified Service Monitor*.

- Cisco 1040 Sensors (sensors)—Compute MOS for each RTP stream; sensors send syslog messages to Service Monitor every 60 seconds.

Each licensed instance of Service Monitor can act as a primary Service Monitor for multiple Cisco 1040s. If you have more than one licensed instance of Service Monitor, Service Monitor can act as secondary backups for each other. Then, when a Service Monitor is unavailable, Cisco 1040s can fail over to a secondary Service Monitor until the primary Service Monitor is once again available.



Note

A Service Monitor that acts as a backup and the Service Monitor that it backs up must both run the same version of Cisco Unified Service Monitor.

Service Monitor compares MOS against a threshold value—default or user-specified—for the codec in use. When MOS drops below the threshold, Service Monitor generates SNMP traps and sends them to up to four recipients. Service Monitor stores the data that it obtains in the database, where it is available for display on Service Monitor reports. Service Monitor purges the database daily to maintain a configurable number of days of data. (For more information, see online help.) Optionally, Service Monitor also stores data obtained from Cisco 1040s in files on disk.

If you configure Cisco Unified Operations Manager (Operations Manager) as a trap receiver for Service Monitor, Operations Manager can further analyze, display, and act on the traps that Service Monitor generates. Operations Manager can generate service quality events, display and track these events on a real-time dashboard, and display and store event history. You can configure additional event settings on Operations Manager to alert you if MOS drops below a threshold or if too many (configurable number) service quality events occur during a period of time (configurable number of minutes). In addition, you can configure Operations Manager to send notifications by e-mail, SNMP trap, and syslog message.

Licensing

Service Monitor features software-based product registration and license key activation technologies. The following table provides information about terminology used in the registration process.



Note A Service Monitor 2.0 license also supports 2.0.1.

Understanding Licensing Terms

Table 1 describes the PAK and the License file and usage of these terms.

Table 1 *Understanding PAK and License File*

Licensing Terms	Description
Product Authorization Key (PAK)	<p>The PAK is printed on the software claim certificate included in product packaging. Use the PAK and the MAC address of the server where Service Monitor will reside to get your license file from Cisco.com. The Service Monitor license file includes support for up to 1,000 phones.</p> <p>You can purchase incremental licenses to support additional IP phones, registering up to 30,000 phones with a single Service Monitor. For each incremental license that you purchase, a PAK is shipped to you, and you must use that PAK to obtain a license file.</p>
License file	<p>When you use the PAK to register your product on the product licensing area of Cisco.com, you will receive a license file. To register, you need to provide both of the following:</p> <ul style="list-style-type: none"> • The MAC address of the server where Service Monitor will reside. • The PAK.

Licensing Your Product During Installation

Before you install the Service Monitor product, you should register the product and obtain a license file.



Note If you are installing Service Monitor for evaluation only, you do not need to perform this procedure.

To license your product, you must:

Step 1 Register the Service Monitor product with Cisco.com using the MAC address of the server on which Cisco Unified Service Monitor 2.0.1 will reside and the PAK.

The PAK is printed on the software claim certificate. Get your license file from:

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



Note You will be asked to log in. You must be a registered user of Cisco.com to log in.

Logging in allows your Cisco user profile information to autopopulate many of the product registration fields. Login is case sensitive.

Step 2 Copy the new license file to the Service Monitor server, into a directory with read permissions for the user name *casuser* or the user group *casusers*.



Note Service Monitor uses a local user, *casuser*, to run processes without having 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 Install the product using the Cisco Unified Service Monitor 2.0.1 product CD; during the installation, when prompted for Licensing Information:

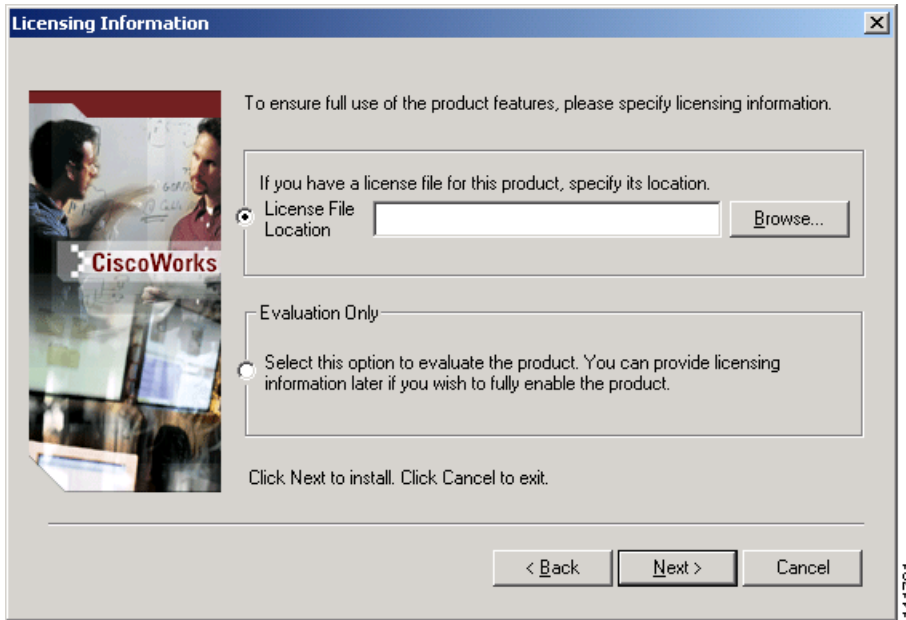
- a. Select the first radio button (see [Figure 1](#)).
- b. Use the browse window to locate the license file directory.
- c. Click **Next** to install the license file.

**Note**

Add any incremental license files that you purchased to support additional IP phones after you install Service Monitor. (See Adding Licenses to an Installed Service Monitor, page 6.)

Figure 1 shows the licensing input dialog box that the installer displays during the installation process.

Figure 1 *Licensing Information Dialog Box*



Adding Licenses to an Installed Service Monitor

After you install or upgrade to Service Monitor 2.0.1, add any new incremental licenses that you have purchased to support additional IP phones. When you purchase an incremental license, you receive a PAK. You must use the PAK to obtain a license file and install the license.

If you installed Service Monitor with an evaluation license, you can subsequently install a purchased license. When you purchase Service Monitor, you receive a PAK. Use it to obtain and install a license file.

To add support for additional IP phones to Service Monitor and to upgrade from an evaluation license to a purchased license, you must:

Step 1 Obtain the license file using the MAC address of the server where Service Monitor is installed and the PAK that you received when you purchased the product. Get your license file from: <http://www.cisco.com/go/license>



Note You will be asked to log in. You must be a registered user of Cisco.com to log in.

Logging in allows your Cisco user profile information to autopopulate many of the product registration fields. Login is case sensitive.

Step 2 Copy the new license file to the Service Monitor server, into a directory with read permissions for the user name *casuser* or the user group *casusers*.



Note Service Monitor uses a local user, *casuser*, to run processes without having Administrator privileges.

Step 3 Install the license:

- a. From Service Monitor, click the CiscoWorks link in the upper-right corner. The CiscoWorks Homepage appears.
- b. Select **Common Services > Server > Admin > Licensing**.
The License Administration page appears.
- c. Click **Update**.
A file browser popup dialog box appears.
- d. Enter the path to the new license file in the License field, or click **Browse** to locate the license file you copied to the server in step 2.
- e. Click **OK**.

The system verifies whether the license file is valid, and updates the license. The updated licensing information appears on the License Information page. If you purchased more than one license, repeat [Step 3](#) to install each additional license.

**Note**

The License Information page displays 2.0 as the supported version. (A Service Monitor 2.0 license supports both 2.0 and 2.0.1.)

If you encounter errors, repeat the steps to license your product.

3 Server and Client System Requirements

Table 2 lists minimum server requirements for installing Service Monitor alone.


Table 3 lists minimum client requirements for Service Monitor.

Table 4 lists browser requirements for Service Monitor.

Table 2 *Minimum Server Requirements*

Component	Minimum Requirement
Hardware	<ul style="list-style-type: none">• Server platform with dual-CPU, Xeon processor, 2.33 GHz or greater <div data-bbox="584 836 638 868" data-label="Image"></div> <div data-bbox="584 873 638 901" data-label="Section-Header">Note</div> <div data-bbox="678 873 1229 1023" data-label="Text"><p>These Cisco products meet the specifications: MCS 7845-H2 and MCS 7845-I2. These come with 4 Serial Attached SCSI (SAS) hard drives, RAID1+0. For ordering information, see Cisco.com.</p></div> <ul style="list-style-type: none">• Color monitor with video card capable of 256 colors or more• CD-ROM drive• SAS disks

Table 2 **Minimum Server Requirements (continued)**


Component	Minimum Requirement
Software for Windows	<p>One of these:</p> <ul style="list-style-type: none"> • Windows Server 2003 Service Pack 1 or 2, Standard or Enterprise edition • Window Server 2003 R2, Standard or Enterprise Edition <p> Note</p> <ul style="list-style-type: none"> • The system that you use for your Service Monitor server should meet all the security guidelines that Microsoft recommends for Windows 2003 Server. See the Microsoft website for security guidance: http://www.microsoft.com/technet/security/prodtech/WindowsServer2003.msp This website is Copyright © 2008, Microsoft Corporation. • It is recommended that Service Monitor not share a platform with other I/O or disk-intensive applications. • Configure the server to use Network Time Protocol (NTP) to synchronize with the time server that is used by Unified Communications Managers in your network. See NTP Configuration Notes, page 11.
Available memory (RAM)	4 GB
Available disk space	<ul style="list-style-type: none"> • 70 GB minimum—SAS disks are required • Virtual memory: 4 GB • NTFS file system¹ required.


1. Install Service Monitor on an NTFS file system. Do not install Service Monitor on a FAT file system. To verify the file system, open My Computer on the Windows desktop, right-click the drive and select **Properties** from the popup menu. The file system field appears in the General tab of the Properties dialog box.

Table 3 **Minimum Client Hardware and Software Requirements**

Component	Minimum Requirement
Hardware/software	<ul style="list-style-type: none">• Any PC or server platform with a Pentium IV processor, 1.0 GHz or greater, running one of the following:<ul style="list-style-type: none">– Windows 2000 (Professional and Server) with Service Pack 3 or Service Pack 4– Windows XP Service Pack 1 or Service Pack 2– Windows 2003 Server (Standard and Enterprise Editions) without Windows Terminal Services• Color monitor with video card set to 256 colors
Available disk space	1 GB virtual memory
Available memory (RAM)	512 MB minimum We recommend that you set virtual memory to twice the size of RAM.

Table 4 **Browser Requirements**

Browser	Version	Platform
Internet Explorer	6.0.28 7.0	Either of the following: <ul style="list-style-type: none"> • Windows 2000 • Windows XP
	6.0.3790.0 7.0	Windows Server 2003
 <p>Note If you use Internet Explorer 6 (or 7) with Service Pack 2 (SP2), the default settings for new security features can prevent file download windows from being displayed.</p>		<p>If you have set the custom level of security in Internet Explorer 6 (or 7) SP2 to medium or higher, the option Automatic prompt to file download is disabled. If you try to download data to a PDF or CSV file from Service Monitor to a desktop that does not have Adobe Acrobat Reader or Microsoft Excel installed, nothing happens. The PDF file or the spreadsheet is not displayed, nor is a window that prompts you to save the file.</p> <p>To enable file download windows to display, do this on your desktop:</p> <ol style="list-style-type: none"> 1. In Internet Explorer, select Tools > Options. 2. Select the Security tab and click Custom Level. 3. Scroll to Downloads, and select Enable for Automatic prompt to file download.

 **Note** When using Service Monitor, disable any software on your desktop that you use to prevent popup windows from displaying. Service Monitor must be able to open multiple windows to display information.

NTP Configuration Notes

The clocks on Service Monitor and Unified Communications Manager servers must be synchronized for Service Monitor reports to include complete and up-to-date information and accurately reflect activity during a given time period. These notes offer a starting point and do not provide complete instructions for configuring NTP.

To get started:

1. Talk with your Unified Communications Manager administrators to determine the time server with which Service Monitor should synchronize. You might find *Cisco IP Telephony Clock Synchronization: Best Practices*, a white paper on Cisco.com, useful; read it at this URL: http://cisco.com/en/US/products/sw/voicesw/ps556/prod_white_papers_list.html.
2. Use your system documentation to configure NTP on the Windows Server 2003 system where Service Monitor will be installed. Configure NTP with the time server being used by Cisco Unified Communication Managers in your network. You might find *How to configure an authoritative time server in Windows Server 2003*, useful; look for it at this URL: <http://support.microsoft.com/kb/816042>.



Note

This website is Copyright © 2007, Microsoft Corporation.

Cisco Unified Service Monitor Port Usage

This section provides a list of ports used by Cisco Unified Service Monitor.




Note

The ports in [Table 5](#) should not be scanned.

Table 5 **Service Monitor Port Usage**

Protocol	Port Number	Service Name
UDP	53	DNS.
UDP	67 and 68	DHCP.
UDP	5666	Syslog—Service Monitor receives syslog messages from Cisco 1040.
TCP	22	SFTP—Service Monitor uses SFTP to obtain data from Unified Communications Manager versions 5.x and 6.x.
TCP	2000	SCCP—Service Monitor uses SCCP to communicate with Cisco 1040s.
TCP	43459	Database.
TCP	5665–5680	Interprocess communication between the user interface and back-end processes.

 **Note** These ports must be free.

**Note**

Service Monitor uses TFTP to find the configuration file for a given Cisco 1040. Service Monitor by default uses port 69 on the TFTP servers.

4 Installation and Upgrade Paths

Table 6 lists the supported installation paths. Table 7 lists the supported upgrade paths.

Table 6 Supported Installation Paths


If you are installing Service Monitor on a system that...	Then do this
<p>Has Operations Manager 2.0.1 (which includes Service Monitor 2.0.1) installed and Service Monitor 2.0.1 is not yet licensed.</p>	<p>To activate Service Monitor 2.0.1:</p> <ol style="list-style-type: none"> 1. Purchase Service Monitor 2.0 and obtain a PAK. <p> Note Service Monitor 2.0 includes 2.0.1.</p> <ol style="list-style-type: none"> 2. Use the PAK and the MAC address of the system where Operations Manager is installed to register your product on Cisco.com and obtain a license file. 3. If you plan to add Unified Communications Managers to Service Monitor, configure the Service Monitor system to use NTP; see NTP Configuration Notes, page 11. 4. Install the license file on the system where Service Monitor 2.0.1 is installed. See Adding Licenses to an Installed Service Monitor, page 6. 5. Perform the tasks in the configuration task checklist in <i>User Guide for Cisco Unified Service Monitor</i>.

Table 6 Supported Installation Paths (continued)

If you are installing Service Monitor on a system that...	Then do this
Has any product other than Operations Manager 2.0.1 installed	<ol style="list-style-type: none"> 1. Uninstall other products; for example, uninstall all CiscoWorks and Network Management System (NMS) products. 2. After you complete the uninstallation, verify that <i>NMSROOT</i>, if it exists, does not contain any files. <i>NMSROOT</i> is the directory where Service Monitor will be installed; its default location is C:\Program Files\CSCOPx. If <i>NMSROOT</i> exists, delete any files from it. 3. Use the instructions in this table for Does not have Operations Manager 2.0.1 installed.
Does not have Operations Manager 2.0.1 installed	<ol style="list-style-type: none"> 1. If you want to manage Service Monitor using a third-party SNMP management tool, install Windows SNMP service. 2. Use the PAK and the MAC address of the Service Monitor server to register your product on Cisco.com and obtain a license file. 3. Copy the license file to the server where you will install Cisco Unified Service Monitor. See <i>Licensing Your Product During Installation</i>, page 5. 4. If you plan to add Unified Communications Manager to Service Monitor, configure the Service Monitor system to use NTP; see <i>NTP Configuration Notes</i>, page 11. 5. Install Cisco Unified Service Monitor 2.0 (includes 2.0.1). 6. Install any incremental license files that you purchased to support additional IP phones. See Adding Licenses to an Installed Service Monitor, page 6. 7. Perform the tasks in the configuration task checklist in <i>User Guide for Cisco Unified Service Monitor</i>.

Table 7 lists the supported upgrade paths.

Table 7 Supported Upgrade Paths

If you are upgrading to Service Monitor 2.0.1 on a system that...	Then do this
Has been upgraded with Operations Manager 2.0.1 (which includes Service Monitor 2.0.1)	If you previously installed a license for Service Monitor 2.0 on this system, it is still valid for Service Monitor 2.0.1. You should: <ul style="list-style-type: none">• Delete existing binary image files (SvcMonAA2_<i>nm</i>.img) from your TFTP servers.• Copy the new binary image file (SvcMonAA2_40.img) to your TFTP servers.• Edit the default sensor configuration file; update the image filename to SvcMonAA2_40.img.• Verify that the newly updated default sensor configuration file is on your TFTP servers.• Reset your sensors.

Table 7 Supported Upgrade Paths (continued)


If you are upgrading to Service Monitor 2.0.1 on a system that...	Then do this
Has a licensed version of Service Monitor 1.1	<ol style="list-style-type: none"> 1. Order Service Monitor 2.0. Service Monitor 2.0.1 and a PAK will be shipped to you. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;">  <p>Note Starting with Service Monitor 2.0, licensing no longer limits the number of sensors that can register. Instead, licensing is based upon the number of phones being monitored.</p> </div> <ol style="list-style-type: none"> 2. Use the PAK and the MAC address of the server where Service Monitor 1.1 is installed to register your product on Cisco.com and obtain a license file. 3. Copy the license file to the server where Service Monitor 1.1 is installed. You will be prompted to supply the license file location during the upgrade procedure. 4. If you plan to add Unified Communications Manager to Service Monitor, configure the Service Monitor system to use NTP; see NTP Configuration Notes, page 11. 5. Make note of the IP addresses for the TFTP server you used with Service Monitor 1.1. You will need to add the TFTP server to Service Monitor 2.0.1 in step 9. 6. From your existing TFTP servers, delete any existing: <ul style="list-style-type: none"> – Sensor configuration files—These include one QOVDefault.CNF file and a QoVMACAddress.CNF file for each sensor. – Binary image files—These are named SvcMonAA2_nm.img. 7. Using the product CD, upgrade to Cisco Unified Service Monitor 2.0.1. 8. If you purchased any new incremental license files, see Adding Licenses to an Installed Service Monitor, page 6. 9. Complete the tasks listed in Performing Post-Upgrade Configuration, page 32.

Table 7 Supported Upgrade Paths (continued)

If you are upgrading to Service Monitor 2.0.1 on a system that...	Then do this
Has a licensed version of Service Monitor 2.0	<ol style="list-style-type: none"> 1. Order an upgrade kit. A product CD for Service Monitor 2.0.1 will be shipped to you. 2. If you plan to add Unified Communications Manager to Service Monitor and you have not yet configured NTP on the Service Monitor system, do so now; see NTP Configuration Notes, page 11. 3. From your existing TFTP servers, delete any existing: <ul style="list-style-type: none"> – Sensor configuration files—These include one QOVDefault.CNF file and a QoVMACAddress.CNF file for each sensor. – Binary image files—These are named SvcMonAA2_nm.img. 4. Using the product CD, upgrade to Cisco Unified Service Monitor 2.0.1. 5. Install any new incremental license files that you have purchased to support additional phones. See Adding Licenses to an Installed Service Monitor, page 6. 6. Complete the tasks listed in Performing Post-Upgrade Configuration, page 32.

5 Installing Cisco Unified Service Monitor

This section includes both of the following:

- Before You Install Service Monitor, page 18
- Performing the Service Monitor Installation, page 20

Before You Install Service Monitor

Service Monitor is *already* installed on a server when you install Operations Manager. To activate Service Monitor on such a server, register your PAK on Cisco.com and install the license file for Cisco Unified Service Monitor. (See Adding Licenses to an Installed Service Monitor, page 6.)

If Windows Data Execution Prevention (DEP) is enabled, it can prevent the installation from completing. To check whether DEP is enabled and to disable it, see Checking for and Temporarily Disabling DEP, page 18.

If you want to monitor Service Monitor using a third-party SNMP management tool, see Configuring Your System for SNMP Queries, page 19.

To get ready for performing the installation, see Preparing Information that You Need to Install Service Monitor, page 20.

Checking for and Temporarily Disabling DEP

Step 1 Log in to the machine on which you will install Service Monitor as an administrator or a member of the Administrators group.



Note If your computer is connected to a network, network policy settings might prevent you from completing this procedure.

Step 2 Open System Properties by right-clicking the My Computer icon on your desktop and selecting Properties.

Step 3 Click the Advanced tab; then, under Performance, click Settings.

Step 4 Click the Data Execution Prevention tab. If **Turn on DEP for all programs and services except those I select** is selected, DEP is enabled.

Step 5 Select **Turn on DEP for essential Windows programs and services only**.

Step 6 Click **OK**.



Note After the installation completes, you can enable DEP.

Configuring Your System for SNMP Queries

Service Monitor implements the system application MIB. If you want to use a third-party SNMP management tool to make SNMP queries against the server where Service Monitor is installed, Windows SNMP service must be installed.



Note To improve security, the SNMP set operation is not allowed on any object ID (OID) in the system application MIB. After installation of Service Monitor, you should modify the credentials for Windows SNMP service to not use a default or well-known community string.

You can install Windows SNMP service before or after you install Service Monitor. Use this procedure to determine whether Windows SNMP service is installed.

Step 1 Verify that Windows SNMP service is installed on the server where you will install Service Monitor. To do so:

- a. Open the Windows administrative tool Services window.
- b. Verify the following:
 - SNMP Service is displayed on the Windows administrative tool Services window; if so, Windows SNMP service is installed.
 - SNMP service status is Started; if so, SNMP service is running.

Step 2 If Windows SNMP service is not installed, install it.



Note 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 *install SNMP service*.

Preparing Information that You Need to Install Service Monitor

To install Service Monitor on a server without Operations Manager, you will need to supply the following information during the installation:

- Licensing information—License file location. See Understanding Licensing Terms, page 4.



Note

If you are installing Service Monitor for evaluation purposes, you do not need to enter licensing information.

- Passwords for the *admin* user and the *system identity* user—Passwords must contain at least 5 characters.



Note

The system identity user enables communication between servers through a trust model and is used, for example, if you want to configure authentication and authorization for Service Monitor using Cisco Secure ACS. For information about configuring Service Monitor with ACS, see *User Guide for Cisco Unified Service Monitor*. For information about the system identity account, see *User Guide for CiscoWorks Common Services 3.0.5*.



Note

If you choose a Typical installation, the program generates passwords randomly for the guest and casuser users, and for the database. If you choose a Custom installation, you will be prompted for these passwords also.

Performing the Service Monitor Installation

Do not install Service Monitor on:

- A Primary Domain Controller (PDC) or Backup Domain Controller (BDC).
- A FAT file system.
- An Advanced Server with terminal services enabled in application server mode.
- A system with Internet Information Services (IIS) enabled.
- A system that does not have name lookup.
- A system with 2 network interface cards (NICs).

We recommend that you:

- Install Service Monitor on a system that has a static IP address.
- Disable the virus scan software on your system. You can restart it after installation is complete.

Before You Begin

Make sure your system meets the prerequisites:

- Required (or desired) operating system upgrades have been performed.
- Required Windows service packs are installed.
- Required minimum amount (or more) of RAM is available.

Close all open or active programs. Do not run other programs during the installation process.

Installing Service Monitor

Step 1 As the local administrator, log in to the machine on which you will install the Service Monitor software, and insert the Service Monitor CD-ROM into the CD-ROM drive. The Cisco Unified Service Monitor 2.0.1 Setup Program window opens.

If the CD-ROM is already in the CD-ROM drive and you stopped the installation process to close programs or if Autostart is disabled, click **Setup.exe** to restart the process.

Step 2 Click **Install**. The Welcome window appears.

Step 3 Click **Next**. The Software License Agreement window appears.

Step 4 Click **Accept**. The Licensing Information window appears.

Step 5 Select one of the following, and then click **Next**:

- **License File Location**—Browse to enter the location. For instructions on obtaining a license file, see Licensing, page 4.
- **Evaluation Only**—You can complete the upgrade and then register the license file later; see Adding Licenses to an Installed Service Monitor, page 6.



Note For instructions on obtaining a license file, see Licensing, page 4.

The installation program checks the name lookup and DHCP. If a static IP address is not configured on your system, the DHCP-Enabled Network Adapters dialog box appears. Click **Yes**.

The Setup Type window appears.

Step 6 Select one of the following radio buttons:

- **Typical**—To install the complete Service Monitor package, which contains Common Services 3.0.5 and Service Monitor 2.0.1.
- **Custom**—To install the complete Service Monitor package, select a destination directory, and enter passwords for user and database.

If you choose the *Typical* installation mode, the following information will be supplied for you for the Common Services installation: guest password, Common Services database password, Web Server information, and self-signed certificate information. The remainder of this procedure is written for a Typical installation.

If you choose the *Custom* installation mode, you will be prompted to enter the above information during the installation process.

Step 7 Click **Next**. The Select Components window appears.

Step 8 Select all radio buttons. Click **Next**.

The installation program checks dependencies and system requirements.

The System Requirements window displays the results of the requirements check and advises whether the installation can continue. One of the following might occur:

- If there is not enough disk space for the installation, or the correct operating system is not present, or the minimum required RAM is not available, the installation program displays an error message and stops.
- If your system has less than 4 GB of RAM, you can continue with the installation after reading this message:

WARNING: System memory is less than the requirement for Cisco Unified Service Monitor system to support high call volume.

Please refer to Service Monitor documentation for more details and upgrade the memory to at least 4GB if you have high call volume.

- If other minimum requirements are not met, the installation program displays an appropriate message and continues installing.

Step 9 Click **Next**. The Change Admin Password window appears:

- a. Enter an admin password, confirm, and click **Next**. The Change System Identity Account Password window appears
- b. Enter a System Identity Account password (and confirm), and click **Next**. The Create casuser dialog box appears.
- c. Click **Yes** to continue with the installation.



Note If you selected the *Custom* installation mode, during this part of the installation you will be asked to enter the following information: guest password, casuser password, Common Services database password, Web server information, and self-signed certificate information.

Step 10 The Summary window appears, displaying the current settings. Click **Next**. The installation proceeds.

Step 11 Click **OK** on additional messages if they are displayed:

If the system has more than one NIC and more than one IP address configured, you will see this message:

```
This machine is multihomed. Please update the MULTI-HOME properties section in
C:\PROGRA~2\CSCOpX\lib\vbroker\gatekeeper.cfg after the installation is complete.
```



Caution

Do not run Service Monitor on this system; uninstall Service Monitor and install it on another system that has only one NIC.

If Windows SNMP service is not installed on your system, you will see this message:

```
Windows SNMP service is not installed on your system. This installation will
continue. To install support for system application and host resources MIBs, you
must install the Windows SNMP service, using Add/Remove Programs from the Control
Panel.
```

If you installed Service Monitor for evaluation only, you will see this message:

```
Please obtain a valid license key from CCO within 90 days.
```

You will see a dialog box with the following message displayed:

```
Before you reboot this system, configure automatic time synchronization on it
using NTP. Configure this system to use the time server that is used by Cisco
Unified Communications Managers in your network.
```

For more information, see [NTP Configuration Notes, page 11](#).

Step 12 A message appears asking whether to reboot your system now. Reboot your system before you start [Step 13](#).

Step 13 After the installation completes:

- a. Verify that Service Monitor was installed correctly by starting Service Monitor. See [Starting Cisco Unified Service Monitor, page 34](#).
 - b. Exclude the databases directory from virus scanning; see [After You Install Service Monitor, page 24](#).
 - c. If you disabled DEP before the installation, see [Enabling DEP, page 24](#).
-

After You Install Service Monitor

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`.

Enabling DEP

If you disabled DEP before the installation, re-enable it and enable the installed software to continue to run, using this procedure.

-
- Step 1** Log in as an administrator or a member of the Administrators group.
 - Step 2** Open System Properties by right-clicking the My Computer icon on your desktop and selecting Properties.
 - Step 3** Click the Advanced tab and, under Performance, click **Settings**.
 - Step 4** Click the Data Execution Prevention tab.
 - Step 5** Select **Turn on DEP for all programs and services except those I select**.
 - Step 6** To disable DEP for a program, select the check box next to the program name and click **OK**. If the name of the program doesn't appear in the list, click **Add**, navigate to your Program Files folder, select the executable file (the file with an `.exe` file extension) and click **OK**.



Note While Service Monitor is running, disable DEP for `cwjava.exe`.

- Step 7** Click **OK**.
-

6 Upgrading to Cisco Unified Service Monitor 2.0.1

This section includes the following:

- Before You Upgrade to Service Monitor 2.0.1, page 25
- Performing the Upgrade to Service Monitor 2.0.1, page 28
- Performing Post-Upgrade Configuration, page 32

Before You Upgrade to Service Monitor 2.0.1



Note Service Monitor software is *already* upgraded to release 2.0.1 on a server where you have upgraded to Operations Manager 2.0.1. For more information, see Installation and Upgrade Paths, page 13.

Performing a Database Backup

The upgrade procedure does not back up your system. See Backing Up Service Monitor Files and Database, page 26.

Understanding the Effect an Upgrade Has on Your Data

Report data is not retained during an upgrade. During an upgrade from 1.*n*, sensor configuration data is not retained. During an upgrade from 2.0, configuration data is retained for sensors as well as for Unified Communications Managers.

Saving TFTP Server Information

If you are upgrading from Service Monitor 1.1, select **Setup** from the Service Monitor home page, note the IP address or DNS name of the TFTP server, and note the port. You need this information to add the TFTP server to Service Monitor after the upgrade. (If you are upgrading from 2.0, TFTP server addresses are retained in the Service Monitor database.)

Deleting Configuration Files from TFTP Servers

It is recommended that you delete existing sensor configuration and binary image files from your existing TFTP servers before you perform the upgrade. Delete the following files:

- Sensor configuration files: One QOVDefault.CNF file and a QoVMACAddress.CNF file for each sensor.
- Binary image file: SvcMonAA2_*nm*.img

Preventing Extra Processing After Upgrade

If you are upgrading from Service Monitor 2.0 and are monitoring calls from Unified Communications Manager 5.*n*, you should consider that:

- During the upgrade from Service Monitor 2.0 to 2.0.1, all processes are stopped. Service Monitor is not available to receive data files from Unified Communications Manager 5.*n*.

- After the upgrade completes:
 - Unified Communications Manager sends all backlogged data files to Service Monitor; this takes time.
 - Service Monitor drops old files.

To avoid this processing, before you upgrade, you can delete the Service Monitor Application Billing Server from Unified Communications Manager and restart the CDR Repository Manager service. See Removing Service Monitor from Unified Communications Manager 5.n, page 27. You can add Service Monitor to Unified Communications Manager and restart the CDR Repository Manager service again after the upgrade completes.

Disabling DEP

If Windows Data Execution Prevention (DEP) is enabled, it can prevent the installation from completing. To check whether DEP is enabled and to disable it, see Checking for and Temporarily Disabling DEP, page 18.

Configuring NTP

If you plan to add Unified Communications Managers to Service Monitor and have not already configured the Service Monitor server to use NTP, do so before or after you upgrade. For more information, see NTP Configuration Notes, page 11.

Backing Up Service Monitor Files and Database

Back up the files on the Service Monitor server using whatever method you normally use. If you are upgrading from 2.0, the database is preserved during the upgrade. As a precaution, perform a database backup before performing the upgrade.



Note If you are upgrading from 1.1, the existing database is not preserved during upgrade and should not be restored on a 2.0.1 system.

If the Service Monitor database—*NMSROOT\databases\qovr\qovr.db*—is larger than 5 GB, it is strongly recommended that you back up the database manually using this procedure.

Step 1 Log in to the system where Service Monitor is installed.

Step 2 Stop the daemon manager using this command:

```
net stop crmdmgt
```

- Step 3** From `NMSROOT\databases\qovr`, copy the files `qovr.db` and `qovrx.log` to a location outside of `NMSROOT`.
- Step 4** Restart the daemon manager using the following command:
- ```
net start crmdmgt
```
- 

Alternatively, for a database that is smaller than 5 GB, you can use this procedure.

---

- 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.
- 

## Removing Service Monitor from Unified Communications Manager 5.n

This procedure is recommended if you are upgrading from Service Monitor 2.0 and you are monitoring calls from Unified Communications Manager 5.n.

---

- Step 1** Launch Unified Communications Manager Serviceability.
- Step 2** Select **Tools > CDR Management**.
- Step 3** Scroll down to Billing Applications Server Parameters and look for the Service Monitor server that you want to upgrade. You can identify the server from entries in the Hostname/IP Address and User Name columns; (smuser will be displayed in the User Name column).
- Step 4** Select the check box for the Service Monitor server that you will upgrade.
- Step 5** Click Delete Selected.
- Step 6** Restart the CDR Repository Service:
- From Unified Communications Manager Serviceability, select **Tools > Control Center - Network Services**.
  - From the list of servers, select the publisher.
  - Scroll down to CDR Services.
  - Select the **Cisco CDR Repository Manager** radio button.
  - Click the **Restart** button.
-

## Performing the Upgrade to Service Monitor 2.0.1



---

**Note** Immediately after you upgrade, sensors are unable register to Service Monitor until you complete the tasks listed in Performing Post-Upgrade Configuration, page 32.

---

The upgrade procedure does *not* perform a backup prior to copying and installing new files on your system. To perform a backup, see Backing Up Service Monitor Files and Database, page 26.

Complete all necessary tasks in Before You Upgrade to Service Monitor 2.0.1, page 25.

---

**Step 1** As the local administrator, log in to the machine on which Service Monitor 1.1 or Service Monitor 2.0 is installed, and insert the Service Monitor 2.0.1 CD-ROM into the CD-ROM drive. The Cisco Unified Service Monitor 2.0.1 Setup Program window opens.

If the CD-ROM is already in the CD-ROM drive and you stopped the installation process to close programs or if Autostart is disabled, click **Setup.exe** to restart the process.

**Step 2** Click **Install**. The Welcome window appears.

**Step 3** Click **Next**. The Software License Agreement window appears.

**Step 4** Click **Accept**. If you are upgrading from 2.0, go to [Step 6](#).

**Step 5** If you are upgrading from 1.1, the Licensing Information window appears. Select one of the following, and then click **Next**:

- **License File Location**—Browse to enter the location. For instructions on obtaining a license file, see Licensing, page 4.
- **Evaluation Only**—You can complete the upgrade and then register the license file later; see Adding Licenses to an Installed Service Monitor, page 6.



---

**Note** For instructions on obtaining a license file, see Licensing, page 4.

---

**Step 6** The installation program checks the name lookup and DHCP. If a static IP address is not configured on your system, the DHCP-Enabled Network Adapters dialog box appears. Click **Yes**.

The Setup Type window appears.

**Step 7** Select one of the following radio buttons:

- **Typical**—To install the complete Service Monitor package, which contains Common Services 3.0.5 and Service Monitor 2.0.1.
- **Custom**—To install the complete Service Monitor package and to enter data that is otherwise entered automatically for you.

If you choose the *Typical* installation mode, the following information will be supplied for you for the Common Services installation: guest password, Common Services database password, Web Server information, and self-signed certificate information.

If you choose the *Custom* installation mode, you will be prompted to enter the above information during the installation process.

**Step 8** Click **Next**. The Select Components window appears.

**Step 9** Select all radio buttons and click **Next**. The installation program checks dependencies and system requirements. The System Requirements window displays the results of the requirements check and advises whether the installation can continue. One of the following might occur:

- If there is not enough disk space for the installation or the minimum required RAM is not available, the installation program displays an error message and stops.
- If your system has less than 4 GB of RAM, but meets the minimum requirement, you can continue with the installation after reading this message:

```
WARNING: System memory is less than the requirement for Cisco Unified Service Monitor system to support high call volume. Please refer to Service Monitor documentation for more details and upgrade the memory to at least 4GB if you have high call volume.
```

- If other minimum requirements are not met, the installation program displays an appropriate message and continues installing.

**Step 10** The Summary window appears, displaying the current settings. Click **Next**. The upgrade proceeds and completes.

**Step 11** Click **OK** on additional messages if they are displayed:

If the system has more than one NIC and more than one IP address configured, you will see this message:

```
This machine is multihomed. Please update the MULTI-HOME properties section in C:\PROGRA~2\CSCOpX\lib\vbroker\gatekeeper.cfg after the installation is complete.
```



---

**Caution**

Do not run Service Monitor on this system; uninstall Service Monitor and install it on another system that has only one NIC.

---

If Windows SNMP service is not installed on your system, you will see this message:

```
Windows SNMP service is not installed on your system. This installation will continue. To install support for system application and host resources MIBs, you must install the Windows SNMP service, using Add/Remove Programs from the Control Panel.
```

**Step 12** From Windows Explorer, delete any files in the folder `NMSROOT\MDC\tomcat\work`.

**Note**

---

Delete files, but not folders within `NMSROOT\MDC\tomcat\work`. `NMSROOT` is the directory where Service Monitor is installed. Its default location is `C:\Program Files\CSCOPx`.

---

**Step 13** A dialog box with the following message is displayed:

Before you reboot this system, configure automatic time synchronization on it using NTP. Configure this system to use the time server that is used by Cisco Unified Communications Managers in your network.

Click **OK**. (For more information, see [NTP Configuration Notes, page 11](#).)

**Step 14** A message is displayed asking whether to reboot the server. Reboot your system before you start [Step 15](#).

**Step 15** After you reboot the server:

- a. Verify the upgrade by starting Service Monitor. See [Starting Cisco Unified Service Monitor, page 34](#).
- b. Complete the tasks listed in [Performing Post-Upgrade Configuration, page 32](#). Sensors will not register to Service Monitor until you complete this step.
- c. If you deleted a Service Monitor Application Billing Server from Unified Communications Manager 5.x, add it. See [Adding Service Monitor to Unified Communications Manager, page 30](#).
- d. Exclude the databases directory from virus scanning; see [After You Install Service Monitor, page 24](#).
- e. If you disabled DEP before the installation, see [Enabling DEP, page 24](#).

**Note**

---

After upgrade, logging settings are returned to their default values. As a result, only error messages are written to Service Monitor log files. If you need additional information in your log files to help you debug a problem, update your logging settings. See the Service Monitor online help for instructions.

---

## Adding Service Monitor to Unified Communications Manager

If you removed a Service Monitor Application Billing Server from Unified Communications Manager before upgrading, add the Service Monitor Application Billing Server to Unified Communications Manager.



---

**Note** Perform this task on Unified Communications Manager version 5.x and 6.x only. Perform this task only while Service Monitor is up and running.

---

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

**Step 2** Select **Tools > CDR Management**.

**Step 3** Scroll down to Billing Applications Server Parameters and click **Add New**.

**Step 4** Enter data in the following fields:

- 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. (Select **Configuration > Other Settings**. For more information, see online help.)
  - 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 Unified Communications Manager 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**. In some cases, for CDR/CMR files to be delivered to a newly added billing server, you must first restart the CDR Repository Management Service:

- a. From Unified Communications Manager Serviceability, select **Tools > Control Center - Network Services**.
- b. From the list of servers, select the publisher.

- c. Scroll down to CDR Services.
  - d. Select the **Cisco CDR Repository Manager** radio button.
  - e. Click the **Restart** button.
- 

## Performing Post-Upgrade Configuration

This section provides the minimum steps required to enable sensors to register with Service Monitor 2.0.1. For complete configuration procedures, including how to add Unified Communications Managers to Service Monitor, see the configuration checklists in *User Guide for Cisco Unified Service Monitor*.

---

- Step 1** Start Service Monitor. See Starting Cisco Unified Service Monitor, page 34.
- Step 2** If you are upgrading from Service Monitor 2.0, you can skip to step 3; otherwise, add at least one TFTP server to Service Monitor:
  - a. Select **Configuration > Sensor > TFTP Servers**. The TFTP Server Setup page appears.
  - b. Click **Add**. The TFTP Server Settings dialog box appears.
  - c. Enter data in the following fields:
    - TFTP Server—IP address or DNS name.
    - Port Number—The default port number is 69.
  - d. Click **OK**.



---

**Note** If you want to use a Unified Communications Manager 6.x, 5.x, or 4.2 as a TFTP server, you can do so.

---

- Step 3** Configure the default configuration file:
  - a. Select **Configuration > Sensor > Setup**. The Setup page appears.
  - b. Update the Default Configuration to TFTP Server fields:
    - Image Filename—Enter SvcMonAA2\_40.img.
    - Primary Service Monitor—Enter an IP address or DNS name.
    - Secondary Service Monitor—(Optional) Enter an IP address or DNS name.
  - c. Click **OK**. Service Monitor stores the default configuration file locally and copies it to the TFTP servers that you added in [Step 2](#).

- d. Copy the binary image file, SvcMonAA2\_40.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*.)
- e. Verify that the newly created *QOVDefault.CNF* file is on the TFTP server. If it is not, upload it to the root location on the TFTP server from the Service Monitor image file directory, *NMSROOT\ImageDir*. For examples of the configuration files, see *Sample Sensor Configuration Files*, page 33.

**Note**

---

If you use Unified Communications Manager as a TFTP server, Service Monitor cannot copy configuration files to Unified Communications Manager due to security settings on the latter. You will need to manually upload the configuration file as described in [Step 3](#). After uploading the configuration file, reset the TFTP server on Unified Communications Manager. For more information, see *Unified Communications Manager* documentation.

---

- Step 4** Wait a few minutes and verify that sensors have registered to Service Monitor. If they have not, reset the sensors by disconnecting them from power and connecting them again.

**Warning**

---

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

---

## Sample Sensor Configuration Files

Service Monitor creates these files when you edit the configuration through the user interface and when a sensor uses the default configuration file to register. These samples are provided to enable you to confirm that the contents of a sensor configuration file are correct.

**Note**

---

Always use the Service Monitor user interface to edit sensor configuration files to ensure that Service Monitor functions properly. Do not edit sensor configuration files on the TFTP server.

---

### Default Configuration File—*QOVDefault.CNF*

In the default configuration file, the ID, A000, is a placeholder; an IP address or alternatively a DNS name is provided for the Receiver. The last updated data and time represent the last time that the default configuration was updated from the Service Monitor user interface.

```
Receiver=10.92.99.22;;
ID=A000
Image=SvcMonAA2_40.img
LastUpdated=11_16_2006-6_59_46.78
```

```
CDPGlobalRunState=true
SyslogPort=UDP:5666
SkinnyPort=TCP:2000
```

## MAC-Specific Configuration File—QOV001120FFCF18.CNF

In a MAC-specific configuration file, the default ID, A000, has been replaced by the sensor MAC address; the receiver DNS name is included, although an IP address could appear instead. The last updated date and time represent the last time that the configuration file was updated; this could be when the sensor registered with Service Monitor or when a user edited the configuration file from the Service Monitor user interface.

```
Receiver=govr-weekly;;
ID=001120FFCF18
Image=SvcMonAA2_40.img
LastUpdated=11_13_2006-4_3_57.578
CDPGlobalRunState=true
SyslogPort=UDP:5666
SkinnyPort=TCP:2000
```

# 7 Starting Cisco Unified Service Monitor

---

- Step 1** In your browser, type `http://servername:1741` where `servername` is the IP address or DNS name of the server where Service Monitor resides. A login page is displayed.
- Step 2** Enter a username and password. If you do not have a username, you can do 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.

---

# 8 Uninstalling and Reinstalling Service Monitor

This section contains the following:

- Uninstalling Service Monitor
- Reinstalling Service Monitor

## Uninstalling Service Monitor



### Caution

---

You must use the Cisco Unified Service Monitor uninstallation program to remove Service Monitor from your system. If you try to remove the files and programs manually, you can seriously damage your system.

---

Use this procedure if you need to uninstall Service Monitor.

- 
- Step 1** As the local administrator, log in to the system on which Service Monitor is installed, and select **Start > All Programs > Cisco Unified Service Monitor 2.0.1 > Uninstall Cisco Unified Service Monitor 2.0.1** to start the uninstallation process. A window appears, listing the components available for uninstallation.
- Step 2** Select all check boxes. Click **Next**. A window appears, displaying the components you have selected to uninstall.
- Step 3** Click **Next**. Messages showing the progress of the uninstallation appear. The Uninstallation Complete dialog box displays this message:
- Before you install Service Monitor product, you must restart your computer.
- Step 4** Click **OK** and restart your system.
- Step 5** Delete any files that remain in the *NMSROOT* directory. *NMSROOT* is the directory where Service Monitor was installed; its default location is `C:\Program Files\CSCOPx`.
- 

## Reinstalling Service Monitor



### Note

---

To reinstall Service Monitor on a system with Operations Manager, you must reinstall both Operations Manager and Service Monitor; see *Installation Guide for Cisco Unified Operations Manager (Includes Service Monitor)*.

---

The existing database is preserved when you reinstall Service Monitor. However, the reinstallation procedure does not perform a backup prior to copying and installing new files on your system. To perform a backup, see *Backing Up Service Monitor Files and Database*, page 26.

Use this procedure if you need to install Service Monitor 2.0.1 on a system where Service Monitor 2.0.1 is already installed.

---

**Step 1** As the local administrator, log in to the machine on which you will reinstall Service Monitor, and insert the Service Monitor CD-ROM into the CD-ROM drive. The installer window appears, asking you if you want to install Service Monitor.



---

**Note** If the CD-ROM is already in the CD-ROM drive and you stopped the reinstallation process to close programs or if Autostart is disabled, click **Setup.exe** from the top directory of your CD-ROM to restart the process.

---

**Step 2** Click **Yes**. The Welcome window appears.

**Step 3** Click **Next**. The Software License Agreement window appears.

**Step 4** Click **Accept**. The installation program checks the name lookup and DHCP.

If a static IP address is not configured on your system, the DHCP-Enabled Network Adapters dialog box appears. Click **Yes**.

The Setup Type dialog box appears.

**Step 5** Select the **Typical** radio button and click **Next**. The Select Components window appears.

**Step 6** Select all radio buttons. Click **Next**.

The installation program checks dependencies and system requirements.

The System Requirements window displays the results of the requirements check and advises whether the installation can continue. One of the following might occur:

- If there is not enough disk space for the installation, the installation program displays an error message and stops.
- If your system has less than 4 GB of RAM, you can continue with the installation after reading this message:

WARNING: System memory is less than the requirement for Cisco Unified Service Monitor system to support high call volume.

Please refer to Service Monitor documentation for more details and upgrade the memory to at least 4GB if you have high call volume.

- If other minimum requirements are not met, the installation program displays an appropriate message and continues installing.

**Step 7** Click **Next**. A message is displayed, informing you that this is a reinstallation and that the database will be preserved.

**Step 8** Click **OK**.

**Step 9** The Summary window appears, displaying the current settings. Click **Next**. The reinstallation proceeds and the Setup Complete window appears.

**Step 10** Click **Finish**.

---

## 9 Where to Go Next

After you have installed Service Monitor, you are ready to configure it and start monitoring IP telephony service quality. For more information, see the following User Guides:

- *User Guide for Cisco Unified Service Monitor*
- *User Guide for Cisco Unified Operations Manager*

You can access these documents:

- In PDF format, in the Documentation directory on the respective product CD-ROM.
- From the online help integrated into the product.



---

**Note** For information about Cisco 1040 Sensor, see *Quick Start Guide for Cisco 1040 Sensor*, shipped with Cisco 1040 and available on Cisco.com.

---

## 10 Related 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.

---

For information about installing, troubleshooting, and using the applications and tools in the Cisco Unified Communications Management Suite, see the sources of information described in [Table 8](#).



---

**Note** To view documents in Adobe Portable Document Format (PDF), Adobe Acrobat 4.0 or later is required.

---

**Table 8**      **Related Documentation**

| <b>To learn more about...</b>        | <b>See this document</b>                                         | <b>In the product package?</b> | <b>On the product CD?</b> | <b>On Cisco.com?</b> | <b>On the Cisco Doc. DVD?</b> | <b>In the online help?</b> |
|--------------------------------------|------------------------------------------------------------------|--------------------------------|---------------------------|----------------------|-------------------------------|----------------------------|
| The known product bugs (DDTs)        | <i>Release Notes for Cisco Unified Service Monitor 2.0.1</i>     | No                             | Yes                       | Yes                  | Yes                           | No                         |
|                                      | <i>Release Notes for Cisco Unified Operations Manager 2.0.1</i>  | No                             | No                        | Yes                  | Yes                           | No                         |
| Performing a typical installation    | <i>Quick Start Guide for Cisco Unified Service Monitor 2.0.1</i> | No                             | Yes                       | Yes                  | Yes                           | No                         |
|                                      | <i>Quick Start Guide for Cisco 1040 Sensor</i>                   | No                             | Yes                       | Yes                  | Yes                           | No                         |
| Features, tasks, and troubleshooting | <i>User Guide for Cisco Unified Service Monitor</i>              | No                             | Yes                       | Yes                  | Yes                           | Yes                        |
|                                      | <i>User Guide for Cisco Unified Operations Manager</i>           | No                             | No                        | Yes                  | Yes                           | No                         |

## 11 Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.htm>





**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Europe Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: 31 0 800 020 0791  
Fax: 31 0 20 357 1100

**Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0809R)

© 2005-2007 Cisco Systems, Inc. All rights reserved.