CHAPTER 2

Installing, Uninstalling, and Upgrading Service Monitor

This section contains the following topics:

Preparing to Install Service Monitor

To ensure a successful Service Monitor installation, do the following before you install Cisco Unified Service Monitor (Service Monitor):

- Make sure that your hardware and software meet the requirements for the server. See Server Requirements, page 1-2.
- Prepare the Service Monitor server for installation. See Preparing the Server, page 2-2.
- Verify that the ports that Service Monitor and Common Services use are not being used. See Ensuring That Required Ports Are Free, page 2-3.
- Gather information that you might need to provide during the Service Monitor installation. See Gathering Information to Provide During Installation, page 2-3.

Preparing the Server

Note 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 NSA website for security guidance (http://www.nsa.gov/ia/guidance/security_configuration_guides/operating_systems.shtml#microsoft).

Specifically, the TCP/IP stack should be hardened to avoid denial of service attacks. Refer to the section "Security Consideration for Network Attacks" on page 103 of the The Windows Server 2003 - Security Guide, v2.1 which can be downloaded from the NSA website.

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 Licensing, page B-1.)

Before installing, reinstalling, or upgrading Service Monitor, do the following:

- Verify that the Primary and Active regional settings on your Windows system are set to either US English or Japanese. Other options are not supported by Service Monitor.

  You can set the Active regional settings in **Control Panel > Regional and Language Options > Regional Options**.
- Set the correct date and time on the system. For more information, see Common Services online help.
- Verify that the drive that you choose to install Service Monitor on is an NTFS file system.
- Verify that the fully qualified domain name of the system on which Service Monitor is installed is Domain Name System (DNS) resolvable. The IP address must be resolvable to the DNS, and the DNS must be resolvable to the IP address (forward and reverse lookup, in DNS terms). To check name resolution on the Service Monitor server, in a command prompt, run the command ***NMSROOT*\bin>smNameRes.exe**.

  Note NMSROOT is the directory where Service Monitor is installed on your system. If you selected the default directory during installation, it is C:\PROGRA~1\CSCOpx.
- Disable the virus scan software on your system. You can restart it after the installation is complete.
- Disable Cisco Security Agent if it is running on your system. You can restart it after the installation is complete.
- Close all open or active programs. Do not run other programs during the installation process.

Do not install Service Monitor on:

- A Primary Domain Controller (PDC) or Backup Domain Controller (BDC).
- An Advanced Server with terminal services enabled in application server mode.

You must install Service Monitor on a system with a static IP address.

You can perform the following tasks either before or after you complete the installation:

- Configure the Service Monitor server to use the same NTP server that Unified Communications Manager uses. See NTP Configuration Notes, page 2-3.
- Obtain the license file or files for Service Monitor. See Licensing, page B-1.

Read through the following installation notes:

- Service Monitor is installed in the default directory *SystemDrive*:\Program Files\CSCOpx

  where *SystemDrive* is the Windows operating system installed directory.

  If you select another directory during installation, the application is installed in that directory.

  The destination folder should not contain the following special characters:

  ! @ # $ % ^ & * ( ) + | } { " [ ] ; ' / ? < > , . ` =

  If errors occur during installation, check the installation log file in the root directory on the drive where the operating system is installed. Each installation creates a new log file; for example:

  C:\Ciscoworks_install_*YYYYMMDD_hhmmss*.log, where *YYYYMMDD* denotes the year, month and date of installation and *hhmmss* denotes the hours, minutes and seconds of installation.

  For example:

  ```
  C:\Ciscoworks_install_20060721_182205.log
  ```

- You can click Cancel at any time to end the installation. However, any changes to your system will not be undone. For example, if any new files were installed or if there were any changes to the system files, you need to manually clean up the installation directories.
- To monitor Service Monitor using a third-party SNMP management tool, see Configuring Your System for SNMP Queries, page 2-18.

Gathering Information to Provide During Installation

During installation, you will need to set passwords for various user accounts and for the database. For more information about the user accounts and for password rules, see Password Information, page A-7. You might need to supply mail settings—such as HTTPS port—and security certificate information. For more information, see User Inputs for Installation, Reinstallation, and Upgrade, page A-1. You will also need to supply the license file location or select Evaluation only. For more information, see Licensing, page B-1.

Ensuring That Required Ports Are Free

The ports that Service Monitor and Common Services use must be free. For a list of ports, see Port Usage, page 1-7.

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 © 2010, Microsoft Corporation.

We also recommend that you configure your NAMs to use the same NTP server that Unified Communications Manager instances use.

Installing Cisco Unified Service Monitor

To ensure that your system is ready for the installation, perform the necessary tasks in Preparing to Install Service Monitor, page 2-1.

Note Windows Management Instrumentation (WMI) services must not run during installation; WMI services can lock processes and cause the installation to terminate unexpectedly. The installation procedure will notify you if WMI services are running and ask permission to stop the services and restart them after installation completes.

Note Cisco recommends that you do not terminate the installation while it is running.

Step 1 As the local administrator, log in to the machine on which you will install the Service Monitor software.

Step 2 Unzip the file that you obtained through the eDelivery system.

Step 3 Click the **setup.exe** file.

The Cisco Unified Service Monitor Setup Program window opens.

Step 4 Read any messages and acknowledge them to continue:

- If WMI Services are running on the system—A message is displayed stating that, for the installation to proceed, the script will stop WMI Services, complete the installation, and restart WMI Services. To continue, click **OK**.
- If IIS is detected (even if it is disabled)—A message is displayed. To avoid port conflict with IIS, click **OK**: in a later step you will be prompted to select an HTTPS port other than 443.

  The Welcome window appears.

Step 5 Click **Next**. The Software License Agreement window appears.

Step 6 Select the **I accept the terms of the license agreement** radio button and click **Next**.

Step 7 The Licensing Information window appears.

Step 8 Select one of the following, and then click **Next**:

- **License File Location**—Browse to enter the location.
- **Evaluation Only**—You can complete the installation and then register the license file later.

Note For instructions on obtaining a license file, see Licensing Process, page B-3.

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**.

If you are installing on a virtual machine with a dynamic MAC address, another warning message will be displayed. Click **Yes**. (Although you can complete the installation, Service Monitor will not be functional. For more information, see VMware Guidelines, page 1-4.)

The Setup Type window appears.

Step 9 Select one of the following radio buttons:

- **Typical**—To install Service Monitor 8.0 while entering the least amount of input.
- **Custom**—To install Service Monitor 8.0, select the 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, Mail Settings, 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 10 Click **Next**. The Select Components window appears.

Step 11 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 your disk space is less than 73000 MB, you can continue with the installation after reading this message:

```
Current disk space <nnnn> MB is less than Recommended disk space 73000 MB and it
may affect performance.
```

Note The disk space displayed in the System Requirements window is the least amount you need to install and start Service Monitor. The Recommended disk space (see Table 1-1 on page 1-2) is the minimum space necessary to use Service Monitor.

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

Step 12 Click **Next**. The Enter Admin Password window appears:

a. Enter a password for the admin user, confirm, and click **Next**.

Note Note the password. You will need it to log in to Service Monitor until you have configured security and created other users.

The Enter 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, Common Services database password, Mail Settings, and self-signed certificate information.
- If you need to change the HTTPS port from 443 to another number, the Mail Settings information page will be displayed.

Step 13 The Summary window appears, displaying the current settings. Click **Install**. As the installation proceeds, additional informational messages are displayed.

Step 14 Click **OK** on additional messages as they are displayed to ensure that the installation progresses:

- 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 2-3.

- 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 Cisco.com within 90 days.
```

A Restart window appears. The Yes, I want to restart my computer now radio button is selected.

Step 15 Click **Finish**. (You must restart your computer before you start Step 16.)

Step 16 After the installation completes:

a. Verify that Service Monitor was installed correctly by starting Service Monitor. See Starting Cisco Unified Service Monitor, page 2-7.

Note You should wait approximately fifteen minutes after the installation completes before starting Service Monitor. This allows all of the process to start. If you do not wait, you may receive the following HTTP Status 500 error message: `The server encountered an internal error () that prevented it from fulfilling this request.`

b. 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.

Starting Cisco Unified Service Monitor

Before starting Service Monitor, do the following:

- Ensure that you restarted your system after you completed the installation or upgrade to Service Monitor 8.0.
- Disable any popup blocker utility that is installed on your client system.

Note By default, SSL is not enabled in Common Services.

Step 1 Enter the appropriate address in your browser as follows:

- If you upgraded to Service Monitor 8.0 and had previously enabled SSL in Common Services, type https://*servername*:*port number* where:
  - servername is the IP address or DNS name of the server where Service Monitor resides
  - port number is either 443 (the default) or the HTTPS port you entered during the upgrade. A login page is displayed.
- If SSL is not enabled, 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.

Preparing to Upgrade to Service Monitor 8.0

This section contains the following information:

Upgrade Paths

You can upgrade to Service Monitor 8.0 from Service Monitor 2.2 or Service Monitor 2.3 only. The upgrade process is not an inline upgrade, meaning you must uninstall the previous version of Service Monitor before you install Service Monitor 8.0.

To save existing call data so that you can continue to run reports against it, you must migrate the call data before you start the upgrade. For more information, see Planning for Data Migration and Migrating Call Data Before the Upgrade, page 2-9.

During the upgrade, configuration data—TFTP servers, trap receivers, credentials, and so on—is automatically migrated.

When you upgrade to Service Monitor 8.0, Common Services upgrades to release 4.0.

Backing Up Service Monitor Files and Database

The upgrade procedure does not back up your system. You should perform a backup before you upgrade.

Step 1 Back up the Service Monitor database:

a. Log in to the system where Service Monitor is installed.

b. Stop the daemon manager using this command:

net stop crmdmgtd

c. From *NMSROOT*\databases\qovr, copy the files qovr.db and qovr.log to a tape, an external drive, or a network directory (not a local directory). Doing so ensures data integrity in case of hardware failure and ensures that backup data does not exhaust local disk space.

d. Restart the daemon manager using the following command:

net start crmdmgtd

Note To restore the database, perform steps 1a and 1b, restore the saved files, and perform step 1c.

Step 2 Back up Service Monitor configuration data using the Common Services backup described in the Common Services online help.

The Common Services online help is only available through the Common Services pages, which are located in the Administration tab.

To access the Common Services online help, you can use the following procedure:

1. Select **Administration > Server Administration (Common Services) > Security**. The Setting up Security page appears.

2. Click **Help**. The online help opens.

Note You must restore the Service Monitor configuration data and additionally restore the database.

To restore both the Service Monitor database and configuration data requires two steps: restoring the database manually and restoring the configuration data (using the procedures referenced in Step 2 b).

Understanding the Effect an Upgrade Has on Your Data

To migrate report data (also know as call data), you must run the call migration tool before you start the upgrade to Service Monitor 8.0. For more information, see Planning for Data Migration and Migrating Call Data Before the Upgrade, page 2-9.

When you upgrade to Service Monitor 8.0:

- Service Monitor configuration data—such as credentials and threshold settings—is retained.
- Common Services data is retained.

Manually Recording Dial Plan Configuration Data from Service Statistics Manager

Note This information is important if you are upgrading to Service Monitor 8.0 and you have Service Statistics Manager in your network.

Service Monitor 8.0 is interoperable with Operations Manager 8.0 and Service Statistics Manager 1.3. Call classification configuration—call categories and dial plans—is introduced in Service Monitor 2.3 and is no longer present in Service Statistics Manager 1.3.

If you are currently using Service Statistics Manager 1.2, you must upgrade to Service Statistics Manager 1.3.

Caution When you upgrade to Service Statistics Manager 1.3, call configuration data is lost.

If you are upgrading from Service Statistics Manager 1.2, before you perform an upgrade, take screenshots or otherwise manually record the dial patterns, gateway codes, toll-free numbers, and service numbers that are configured in Service Statistics Manager 1.2. Save the screenshots or notes that you take to use as a reference when you configure call classification in Service Monitor 8.0.

If you are already using Service Statistics Manager 1.3, this action is not required.

Planning for Data Migration and Migrating Call Data Before the Upgrade

Migrating call data is optional. However, to keep the data, you must migrate it before you start the upgrade to Service Monitor 8.0. You can find the call migration tool in the zip file that contains the Service Monitor product on Cisco.com.

Note The README_QOVR_CMT.TXT. file that is included with the Call Migration Tool provides estimates of the time that data migration takes and the disk space it uses. It also explains the effect that running the tool has on Operations Manager and Service Statistics Manager, if they are installed in your network.

Step 1 Download the zip file (CUSM8_0.zip) that contains the Service Monitor product from Cisco.com. You can navigate to the file as follows:

a. Go to this URL: http://www.cisco.com/en/US/partner/products/ps6536/tsd_products_support_series_home.html.

b. If you have not already logged in to Cisco.com, log in.

c. Click the **Download Software** link.

d. Follow the online instructions to select Cisco Unified Service Monitor 8.0 and download the zip file.

Step 2 Extract the QOVR_CMT.zip file from the \install\CallMigrationTool folder in the CUSM8_0.zip file.

Step 3 Extract the README_QOVR_CMT.TXT file from the QOVR_CMT.zip file and use the information in it to plan for and execute the migration.

Deleting Cisco 1040 Configuration Files from TFTP Servers

We recommend that you delete existing Cisco 1040 configuration and binary image files from your existing TFTP servers before you perform the upgrade. Delete the following files:

- Cisco 1040 Sensor configuration files: One QOVDefault.CNF file and a QoV*MACAddress*.CNF file for each Cisco 1040.
- Binary image file: SvcMonAA2_*nn*.img

Preventing Extra Processing After Upgrade

If you are monitoring calls from Unified Communications Manager 5.x or later, you should consider that:

- During the upgrade to Service Monitor 8.0, all processes are stopped. Service Monitor is not available to receive data files from Unified Communications Manager 5.x or later.
- 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:

- Prevent Unified Communications Manager 7.x and later from sending backlogged data. To do so, edit the billing server and uncheck the Resend on Failure check box. For more information, see Unified Communications Manager Configuration in *User Guide for Cisco Unified Service Monitor 8.0*.
- For Unified Communications Manager software releases earlier than 7.x, prevent them from sending data by deleting the Service Monitor Application Billing Server from Unified Communications Manager and restarting the CDR Repository Manager service. See Removing Service Monitor from

Unified Communications Manager, page 2-11. You can add Service Monitor to Unified Communications Manager and restart the CDR Repository Manager service again after the upgrade completes.

Removing Service Monitor from Unified Communications Manager

This procedure is recommended if you are performing an upgrade to Service Monitor 8.0 and you are monitoring calls from Unified Communications Manager 5.x or 6.x.

Note You can configure Unified Communications Manager 7.x and later to not resend data on failure. For more information, see Unified Communications Manager Configuration in *User Guide for Cisco Unified Service Monitor 8.0*.

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:

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.

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 2-3.

Upgrading to Service Monitor 8.0

Before you perform the upgrade, you must:

- Disable the virus scan software on your system. You can restart it after the upgrade is complete.
- Disable Cisco Security Agent if it is running on your system. You can restart it after the upgrade is complete.

- If you run Service Statistics Manager in your network:
  1. Record call classification data from Service Statistics Manager; (see Manually Recording Dial Plan Configuration Data from Service Statistics Manager, page 2-9).
  2. Stop the Service Statistics Manager server.

Note After you upgrade to Service Monitor 8.0, you must configure dial plans in Service Monitor and then upgrade to Service Statistics Manager 1.3.

Note Immediately after you upgrade, Cisco 1040s are unable register to Service Monitor until you complete the tasks listed in Performing Post-Upgrade Configuration for Cisco 1040s, page 2-14.

Step 1 Change the database password of the Service Monitor 2.x system.

a. On the Service Monitor system, open a command prompt.

b. Stop all processes by entering:

```
net stop crmdmgtd
```

c. Change to the Installation Directory by entering:

```
cd NMSROOT\bin
```

(NMSROOT is the directory where Service Monitor is installed; its default location is C:\Program Files\CSCOpx.)

d. Run `perl dbpasswd.pl dsn=qovr npwd=cisco`. (Changes the password to *cisco*.)

e. Start all processes by entering:

```
net start crmdmgtd
```

Step 2 In a backup folder, make a copy of all the license files located in the NMSROOT\etc\licenses folder.

Step 3 In a backup folder, make a copy of the NMSROOT\qovr\config\ptm\creds file.

Step 4 If you want to migrate call data, see Planning for Data Migration and Migrating Call Data Before the Upgrade, page 2-9.

Step 5 Backup the the Service Monitor database (see Backing Up Service Monitor Files and Database, page 2-8).

Step 6 Uninstall Service Monitor 2.x. As the local administrator, log in to the system where Service Monitor 2.x is installed, and select **Start > All Programs > Cisco Unified Service Monitor > Uninstall Cisco Unified Service Monitor** to start the uninstallation process.

Step 7 Delete the CSCOpx folder.

Step 8 Install Service Monitor 8.0 (see Installing Cisco Unified Service Monitor, page 2-4).

Step 9 A final window is displayed. Select the Yes I want to restart my computer radio button and click **Finish**.

Step 10 After the system has restarted, stop the daemon manager using this command:

```
net stop crmdmgtd
```

Step 11 Change the database password to the same password you set in Service Monitor 2.x.

Step 12 Restore the Service Monitor files and database that you backed up earlier (see Backing Up Service Monitor Files and Database, page 2-8).

Step 13 Copy the previously backed-up creds file to the new installation, in NMSROOT\qovr\config\ptm.

Step 14 In the C:\Program Files\CSCOpx\etc\licenses folder, delete all the files (the VMS folder can remane).

Step 15 Copy the previously backed-up files (in Step 2) to the C:\Program Files\CSCOpx\etc\licenses folder.

Step 16 Restart the daemon manager using the following command:

```
net start crmdmgtd
```

Step 17 Log into Service Monitor. A message appears, stating that your license is invalid.

Step 18 In the message box, click the licensing page link. The Licensing Information page appears.

Step 19 Click update and then enter the location of the upgrade license file.

Note This license file must be an upgrade license for Service Monitor 8.0.

Step 20 Verify that Service Monitor was installed correctly by starting Service Monitor. See Starting Cisco Unified Service Monitor, page 2-7.

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. For more information, see Service Monitor online help.

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 back to Unified Communications Manager.

Note Perform this task on Unified Communications Manager version 5.x and later 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. (For more information, see the 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 for Cisco 1040s

This section provides the minimum steps required to enable Cisco 1040s to register with Service Monitor 8.0. For complete configuration procedures, including how to add NAMs and 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 2-7.

Step 2 Configure the default configuration file:

a. Select **Administration > Configuration > Cisco 1040 > Setup**. The Setup page appears.

b. Update the Default Configuration to TFTP Server fields:

- Image Filename—Enter SvcMonAB2_102.img.
- Primary Service Monitor—Enter an IP address or DNS name.
- Secondary Service Monitor—(Optional) Enter an IP address or DNS name.

Note Occasionally, updated binary image files might be released. For the names of supported binary image files, see *Cisco Unified Service Monitor 8.0 Compliance Matrix*.

c. Click **OK**. Service Monitor stores the default configuration file locally and copies it to the TFTP servers that are configured in Service Monitor.

d. Copy the binary image file, SvcMonAB2_102.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 Cisco 1040 Sensor Configuration Files, page 2-15.

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 2e. After uploading the configuration file, reset the TFTP server on Unified Communications Manager. For more information, see Unified Communications Manager documentation.

Step 3 Wait a few minutes and verify that the Cisco 1040s have registered to Service Monitor. If they have not, reset the Cisco 1040s by disconnecting them from power and connecting them again.

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

Sample Cisco 1040 Sensor Configuration Files

Service Monitor creates these files when you edit the configuration through the user interface and when a Cisco 1040 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 Cisco 1040 Sensor configuration files on the TFTP server.

Default 1040 Sensor 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=SvcMonAB2_102.img
LastUpdated=11_16_2010-6_59_46.78
CDPGlobalRunState=true
SyslogPort=UDP:5666
SkinnyPort=TCP:2000
```

MAC-Specific 1040 Sensor 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=qovr-weekly;;
ID=001120FFCF18
Image=SvcMonAB2_102.img
LastUpdated=11_13_2010-4_3_57.578
CDPGlobalRunState=true
SyslogPort=UDP:5666
SkinnyPort=TCP:2000
```

Uninstalling and Reinstalling Service Monitor

This section contains the following:

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 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 > Uninstall Cisco Unified Service Monitor** to start the uninstallation process.

Note If WMI Services are running on the system, a message is displayed stating that, for the uninstallation to proceed, the script will stop WMI Services, complete the uninstallation, and restart WMI Services. To continue, click **Yes**.

The Uninstallation window appears, listing the components available for uninstallation.

Step 2 Select all check boxes. Click **Next**. The Setup window appears, displaying the components you have selected to uninstall.

Step 3 Click **Next**. Messages that show the progress of the uninstallation appear. The Uninstallation Complete dialog box appears. You must restart your server to complete the uninstallation process. (You can restart your server later by selecting another radio button.)

Step 4 Click **Finish** 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 2-8.

For information about passwords that you will be asked to set during reinstallation, see User Inputs for Installation, Reinstallation, and Upgrade, page A-1. Be sure to read Fixing Problems That Can Occur After You Change Passwords, page A-7.

Use this procedure to install Service Monitor 8.0 on a system where Service Monitor 8.0 is already installed.

Step 1 As the local administrator, log in to the machine on which you will reinstall the Service Monitor software.

Step 2 Unzip the file that you obtained through the eDelivery system.

Step 3 Click the **setup.exe** file.

The Cisco Unified Service Monitor Setup Program window opens.

Step 4 Read any messages and acknowledge them to continue:

- If WMI Services are running on the system—A message is displayed stating that, for the installation to proceed, the script will stop WMI Services, complete the installation, and restart WMI Services. Click **OK**.
- A message is displayed stating that a database backup will not be performed. Click **OK**.

The Welcome window appears.

Step 5 Click **Next**. The Software License Agreement window appears.

Step 6 Select the I accept the terms of the license agreement radio button and click **Next**.

The installation program checks the name lookup and DHCP. The Setup Type dialog box appears.

Step 7 Select the **Typica**l radio button and click **Next**. The Select Applications 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, 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 your disk space is less than 73000 MB, you can continue with the installation after reading this message:

```
Current disk space <nnnn> MB is less than Recommended disk space 73000 MB and it may
affect performance.
```

Note The disk space displayed in the System Requirements window is the least amount you need to install and start Service Monitor. The Recommended disk space (see Table 1-1 on page 1-2) is the minimum space necessary to use Service Monitor.

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

Step 9 Click **Next**. The Change casuser Password window appears.

Step 10 Enter and confirm a password or click **Next** to have the system generate a random password for you. The Summary window appears, displaying the current settings.

Step 11 Click **Install**.

Step 12 The Summary window appears, displaying the current settings.

Step 13 Click **Install**. The reinstallation proceeds and the Setup Complete window appears.

Step 14 Click **Finish**.

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*.