



## CHAPTER 2

# Installing, Uninstalling, and Upgrading Cisco Unified Operations Manager

This chapter describes installing Cisco Unified Operations Manager (with Cisco Unified Service Monitor) on a Windows system.



### Note

Service Monitor is a separately licensed product. If you are going to use Service Monitor, you must install a Service Monitor license after the Operations Manager installation completes. See [Licensing Process, page A-3](#).

This chapter includes the following:

- [Preparing to Install Operations Manager, page 2-1](#)
- [Performing a New Installation, page 2-7](#)
- [Reinstalling Operations Manager, page 2-10](#)
- [Uninstalling Operations Manager, page 2-11](#)
- [Upgrading to Cisco Unified Operations Manager 2.0.1, page 2-12](#)

## Preparing to Install Operations Manager

The information in this section helps you to deploy Operations Manager in your network. Do the following before you install Cisco Unified Operations Manager (Operations Manager):

- Make sure that hardware and software requirements for the server are met. (See [Server Requirements, page 1-3](#).)
- Prepare the Operations Manager server for installation. (See [Preparing the Operations Manager Server, page 2-2](#).)
- Configure devices so that they can be monitored by Operations Manager. ([Preparing Devices for Addition to Operations Manager Inventory, page 2-3](#).)
- Determine whether your existing applications are already using ports that Operations Manager or Cisco Unified Service Monitor (Service Monitor) uses. (Existing applications should not use the ports that Operations Manager or Service Monitor use.) See [Verifying TCP and UDP Ports that Operations Manager Uses, page 2-5](#).
- Gather information that you might need to provide during the Operations Manager installation. (See [Gathering Information to Provide During Installation, page 2-6](#).)

## Preparing the Operations Manager Server

Before installing Operations Manager, do the following:

- Set up the correct date and time on the system. Changing the date and time after installation can cause Operations Manager not to work, because it is perceived as a license violation. Also, the self-signed certificates generated during installation become invalid.
- The drive that you choose to install Operations Manager on must be an NTFS file system.
- If you are using an IBM server with IBM director installed, you must stop the ibm director wmi cim server and change the service to manual, or disable it. If you do not, the Service Level View in Operations Manager will not work.
- Clean the temp directory. You can open the temp directory by typing `%temp%` in a Windows Explorer window.
- 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 2-2](#).
- The fully qualified Domain Name of the system on which Operations Manager is installed must be 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 Operations Manager server; in a command prompt, run the command `<NMSROOT>\bin>smNameRes.exe`.




---

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

---

## Checking for and Temporarily Disabling DEP

---

**Step 1** Log in to the machine on which you will install Operations Manager 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 and, 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.

---

## Enabling DEP

If you disabled DEP before the installation, to turn it on again and enable the installed software to continue to run, use 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 turn off 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 (file with a .exe file extension) and click **OK**.

**Note**

While Operations Manager is running, turn off DEP for cwjava.exe.

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

## Preparing Devices for Addition to Operations Manager Inventory

This section describes actions you must perform before adding devices to Operations Manager device inventory.

Before adding devices to Operations Manager, do the following:

- Configure devices so they can be added to Operations Manager correctly, and so Operations Manager can monitor the devices correctly. (See [Device-Specific Configurations, page 2-3](#).)
- Make sure all processes are running on the Operations Manager system. (See [Actions to Take Before Adding Devices, page 2-4](#).)
- Review the notes for adding devices. (See [Notes on Adding Devices, page 2-4](#).)

## Device-Specific Configurations

### Cisco Unified Communications Manager:

- Make sure that SNMP read access is configured on the Cisco Unified Communications Manager system.
- Provide the HTTP username and password for AXL access. This is the same username and password that is used for the Cisco Unified Communications Manager Administration page.
- If the Cisco Unified Communications Manager Administration page has HTTPS enabled, make sure HTTPS is enabled on all AXL directories.

**Cisco Unified Contact Center and Cisco Unity:**

- Make sure that SNMP read access is configured on the Cisco Unified Contact Center and Cisco Unity systems. You may need to download the Remote Serviceability Kit for certain versions of Cisco Unity (see [www.ciscounitytools.com](http://www.ciscounitytools.com)).
- For Operations Manager to autodiscover Cisco Unified Contact Center devices, each Cisco Unified Contact Center device must be configured with the SNMP v1 read credential (this may be in addition to the SNMP v2c read credentials).

**IPSLA Devices:**

- Make sure that SNMP read and write access is configured on the IPSLA device. The write community string is required to configure tests.
- If the device is used as a target device for the jitter node-to-node test, make sure that the IPSLA responder is enabled.

**All Other Devices:**

- Make sure that SNMP read access is configured.

## Actions to Take Before Adding Devices

- Run `pdshow` to make sure all processes are running except for the transient processes such as the purge tasks.
- Run `<NMSROOT>\objects\smarts\bin\brcontrol` and make sure that you see the message stating that VHM and DFM servers are registered to the broker. If you do not see this message, you must start VHMServer or DFMServer manually.

**Note**


---

NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it is `C:\Program Files\CSCOPx`.

---

## Notes on Adding Devices

- The filtering fields (IP Address, DNS Domain, and SysLocation) in the Discovery Configuration page, are optional. The most effective way to add devices to Operations Manager inventory is to not use these filtering options.
- If you use a ping sweep to add devices, use smaller subnets. Do not use ping sweep on a Class A or Class B address.
- Seed devices must be running CDP.
- If there are many SNMP-unreachable devices in your network and you have to supply multiple device credentials (causing discovery to have to try one or more credentials on each device until it finds the correct credentials for the device), device discovery can take a long time.

This can be caused by the SNMP timeout setting. To fix this situation, you can lower the SNMP timeout and retries setting (default is 3 seconds with 2 retries).

Do the following:

- 
- Step 1** Enter the credentials on the Discovery Configuration page.
  - Step 2** Open the `IPCDiscovery-config.xml` file from `<NMSROOT>\conf\discovery`.

- Step 3** Locate the Credentials section. In this section, for each credential that you entered, you will find a section similar to the following:

```
<SnmpCredential IPAddress="*.*.*.*"> <SNMPv2 Snmpretry="2" Snmptimeout="3000"
Usertag="SNMPv2 Credentials in first line" ROCommunity="/qiJe7XyxpU="
RWCommunity="Byh+1ukjk3I="/> </SnmpCredential>
```

Snmptimeout="3000" indicates that the timeout is 3000 milliseconds, or 3 seconds.

- Step 4** You can lower this value to 1000 milliseconds, or 1 second. You can choose a value based on the SNMP responsiveness in your network.
- Step 5** Save the changes that you made to the file.
- Step 6** Start discovery.



**Note** If you make any further modifications to the credential list from the Discovery Configuration page, you will need to verify the SNMP timeout values in the configuration file. They may have been overwritten.

## Verifying TCP and UDP Ports that Operations Manager Uses

Before installing Operations Manager, make sure that the ports Operations Manager (and Service Monitor) use will only be used by the applications listed in [Table 2-1](#) and [Table 2-2](#).



**Note** If an existing NMS uses port 162, see [Configuring SNMP Trap Receiving and Forwarding, page 3-21](#), for more information.

Operations Manager uses the following TCP and UDP ports.

**Table 2-1** Ports that Operations Manager Uses

Port Numbers	Service Name	Application
161	Simple Network Management Protocol (SNMP)	Common Services
162	Trap receiving (standard port)	Common Services
514	Syslog	Common Services
40000-41000	Used by Common Transport Mechanism for internal application messaging	Operations Manager
42344	Used by Synthetic Testing web service	Operations Manager
42350-42353	Used by messaging software	Operations Manager
43445	Used by Alert History database engine	Operations Manager
43446	Used by inventory service database engine	Operations Manager
43447	Used by event processing database engine	Operations Manager
43449	Used by IP Phone Information Facility database engine	Operations Manager

**Table 2-1** *Ports that Operations Manager Uses (continued)*

Port Numbers	Service Name	Application
8080	Used to determine if the Cisco Unified Communications Manager 5.0 web service is up. <b>Note</b> This port must be made available to Operations Manager.	Operations Manager
9000	Trap receiving CSListener (Operations Manager server if port 162 is occupied)	Operations Manager
9002	DynamID authentication (Operations ManagerBroker)	Operations Manager
9009	Default port number used by the IP telephony server for receiving traps from the device fault server	Operations Manager

**Table 2-2** *Ports that Service Monitor Uses*

Port Numbers	Service Name
53	DNS
67 and 68	DHCP
22	SFTP—Service Monitor uses SFTP to obtain data from Unified Communications Manager 5.x and 6.x.
2000	SCCP—Service Monitor uses SCCP to communicate with Cisco 1040s
43459	Database
5666	Syslog—Service Monitor receives syslog messages from Cisco 1040s.
566-5680	Interprocess communication between user interface and back-end processes. <b>Note</b> These ports must be free.

## Gathering Information to Provide During Installation

You might need to supply the following information while you are installing Operations Manager:



### Note

For more information on creating passwords, see the appendix “Password Information” in *Installation and Setup Guide for Common Services (Includes CiscoView) on Windows*.

- User Admin password
- System Identity Account password
- Casuser password (custom installation only)
- Guest password (custom installation only)
- Common Services database password (custom installation only)
- Web server information (custom installation only)

- License information—Location of the license file. If you have already obtained a license file, provide the path. If not, be sure to obtain one. You can do so before or after you install Cisco Unified Operations Manager; see [Licensing Process, page A-3](#).



**Note** You can determine the status of your license from the Common Services Licensing Information page. From the Operations Manager home page, click **CiscoWorks** in the upper right-hand corner of the window. The CiscoWorks home page opens. Under Common Services, select **Server > Admin > Licensing**.



**Note**

If you are installing Operations Manager for evaluation purposes:

- You do not need to supply a license file.
- You might be interested in the following information:
  - [Licensing Overview, page A-1](#)
  - [Licensing Reminders, page A-5](#)

## Performing a New Installation

The installation process takes approximately sixty minutes to complete.

Follow these guidelines when installing Operations Manager:

- Operations Manager requires a dedicated system; do not install it on a system with:
  - Third-party management software (such as HP OpenView or NetView).
  - Cisco Secure Access Control Server (ACS).
  - Any Cisco applications other than those that are documented to be able to coexist with Operations Manager.
- The system where Operations Manager is to be installed must be configured for DNS.
- If you want to monitor Operations Manager using a third-party SNMP management tool, see [Configuring Your System for SNMP Queries, page 2-17](#).
- Do not install Operations Manager on:
  - A Primary Domain Controller (PDC) or Backup Domain Controller (BDC)
  - A FAT file system.
  - A Windows 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.
- Do not select an encrypted directory. Operations Manager does not support directory encryption.
- Do not install any CiscoWorks Common Services 3.0 service packs on Operations Manager.
- Do not install on any of your voice application servers or on a Cisco Unified Communications Manager server.
- Verify that the system date and time are set properly.

- To speed up installation, disable all virus-scan software while installing.
- You should exclude the NMSROOT/databases directory from virus scanning. Problems can arise if database files are locked because of virus scanning.
- Your system's IP address and hostname should be set before installation.
- If you are going to use Cisco Unified Service Monitor (which is installed when you install Operations Manager), the clocks on Service Monitor and Cisco Unified Communications Manager servers must be synchronized. See [NTP Configuration Notes, page 2-17](#).
- 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 2-2](#).
- Moving your Operations Manager server from Windows Workgroup to Domain is not supported.

---

**Step 1** Make sure your system meets these prerequisites:

- Required (or desired) operating system upgrades have been performed.
- Required service packs are installed.

For system requirements, see [Server Requirements, page 1-3](#).

**Step 2** Close all open or active programs. Do not run other programs during the installation process.

**Step 3** As the local administrator, log in to the machine on which you will install the Operations Manager software, and insert the Cisco Unified Operations Manager CD-ROM into the CD-ROM drive. The Cisco Unified Operations Manager and Service Monitor Setup Program window opens.




---

**Note** 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 4** Click **Install**. The Welcome window appears.

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

**Step 6** Click **Accept**. The Licensing Information window appears.

**Step 7** 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 A-3](#).

---

The Setup Type window appears.

**Step 8** Select **Typical** to install the complete Cisco Unified Operations Manager package, which contains Operations Manager and Service Monitor.

If you choose the *Typical* installation mode, the system automatically provides the following information to the installation process:

- Guest password
- Common Services database password
- Web server information
- Self-signed certificate information

- Username and password for data transport protocol authentication

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

**Step 9** Click **Next**. The Choose Destination Folder window appears.

**Step 10** Do one of the following:

- Click **Next** to accept the default installation directory.
- Browse to the folder where you would like to install Operations Manager, 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 if memory requirements are not met, the installation program displays an error message and stops. (See [Server Requirements, page 1-3](#).)
- If the minimum recommended requirements are not met, the installation program displays a warning message and continues installing.

**Step 11** Click **Next**.

**Step 12** Enter a User Admin password (and confirm), and click **Next**.




---

**Note** If you selected the *Custom* installation mode, during this part of the installation you will be asked to enter all the information that is noted in [Step 8](#).

---

**Step 13** Enter a System Identity Account password (and confirm), and click **Next**.

**Step 14** The Create Casuser dialog box appears; click **Yes** to continue with the installation.

The Summary window appears, displaying the current settings.

**Step 15** Click **Next**. The installation proceeds.

**Step 16** Click **OK** to confirm additional messages if they are displayed:

- If the system has more than one NIC card 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\CSCOp\lib\vbroke\gatekeeper.cfg after the installation is complete.



**Caution**

---

Operations Manager requires only one NIC card and supports only one IP address. Operations Manager does not support two NIC cards with different IP addresses.

---

- If Windows SNMP service is not installed on your system, a message will inform you of this fact.
- If you did not supply a license file during the installation, a message about obtaining a license file is displayed.
- When the installation is complete, the following message appears:

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 2-17](#).

**Step 17** Eject the CD.



**Note** Store the CD in a secure, climate-controlled area for safekeeping.

**Step 18** Click **Finish** to reboot the machine.

**Step 19** Wait 30 minutes after the system reboots before starting Operations Manager. This gives all of the Operations Manager processes time to initialize.

**Step 20** After the installation completes, verify that Operations Manager was installed correctly by starting the application. From the Windows desktop select **Start > All Programs > Cisco Unified Operations Manager and Service Monitor > Cisco Unified Operations Manager and Service Monitor**.

**Step 21** If you disabled DEP before the installation, see [Enabling DEP, page 2-3](#).



**Note** If Enhanced Security is enabled on the Windows 2003 system, you must add the Operations Manager home page to the Internet Explorer Trusted Sites Zone. You will not be able to access the Cisco Unified Operations Manager home page until it is added to the trusted sites. See [Adding the Operations Manager Home Page to the Internet Explorer Trusted Site Zone, page 3-19](#).

If any errors occurred during installation, check the installation log in the root directory on the drive. (For example, the CiscoWorks Common Services installation might create C:\Ciscoworks\_setup001.log, the Operations Manager installation might create C:\Ciscoworks\_setup002.log, and so forth.) The Cisco Technical Assistance Center (TAC) might ask you to send them the installation log.

## Reinstalling Operations Manager

**Step 1** Close all open or active programs. Do not run other programs during the reinstallation process.

**Step 2** As the local administrator, log in to the machine on which you will install the Cisco Unified Operations Manager software, and insert the Cisco Unified Operations Manager CD-ROM into the CD-ROM drive. The installer window appears, asking you if you want to reinstall Cisco Unified Operations Manager.



**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 3** Click **Install**. The Welcome window appears.

**Step 4** Click **Next**. The Software License Agreement window appears.

**Step 5** Click **Accept**. The Setup Type window appears.

**Step 6** Select **Typical** or **Custom**.

**Step 7** Click **Next**. The Backup Data window appears.

**Step 8** Enter or browse to the location where you want the backup of your previous version of Operations Manager stored, and click **Next**.

- Step 9** The System Requirements window displays the results of the requirements check and advises whether the reinstallation can continue; click **Next**.
- Step 10** If you chose Custom installation you will be asked to enter the following:
- Casuser password
  - Username and password for data transport protocol authentication
- This step is not required for Typical installation. Click **Next**.
- Step 11** An information dialog box appears, confirming reinstallation; click **OK**.  
The Summary window appears, displaying the current settings.
- Step 12** Click **Next**. The installation proceeds.
- Step 13** Remove the Cisco Unified Operations Manager CD from the drive.



---

**Note** Store the CD in a secure, climate-controlled area for safekeeping.

---

- Step 14** Click **Finish** to reboot the machine.
- Step 15** After the installation completes, verify that Operations Manager was installed correctly by starting the application. From the Windows desktop select **Start > All Programs > Cisco Unified Operations Manager and Service Monitor > Cisco Unified Operations Manager and Service Monitor**.
- 

If any errors occurred during reinstallation, check the installation log in the root directory on the drive. (For example, the CiscoWorks Common Services installation might create C:\Ciscoworks\_setup001.log, the Operations Manager installation might create C:\Ciscoworks\_setup002.log, and so forth.) The Cisco Technical Assistance Center (TAC) might ask you to send them the installation log.

## Uninstalling Operations Manager



### Caution

---

You must use the Operations Manager uninstallation program to remove Operations Manager from your system. If you try to remove the files and programs manually, you can seriously damage your system.

---



### Note

---

Before uninstalling, be sure to delete all the phone status, node-to-node, and SRST tests from the application. If you do not delete these tests, they will continue to run on the router. To delete these tests, use each test's respective configuration page (see the Cisco Unified Operations Manager online help for information on deleting each test).

---

- Step 1** As the local administrator, log in to the system on which Cisco Unified Operations Manager is installed.
- Step 2** To start the uninstallation process, from the Windows desktop select **Start > All Programs > Cisco Unified Operations Manager and Service Monitor > Uninstall Cisco Unified Operations Manager and Service Monitor**.
- Step 3** Select the components you want to uninstall.

- Step 4** Click **Next** to begin uninstalling the selected components.  
A window appears, listing the components selected for uninstallation.
- Step 5** Click **Next**.  
Messages showing the progress of the uninstallation appear.  
The following message appears:  
Uninstallation is complete. Click OK to finish.
- Step 6** Click **OK**.
- 

## Upgrading to Cisco Unified Operations Manager 2.0.1

Operations Manager supports the following upgrade paths:

- Upgrade from a licensed copy of Cisco Unified Operations Manager 1.1 or 2.0 to a licensed copy of Cisco Unified Operations Manager 2.0.1.
- Upgrade from a licensed copy of Cisco Unified Operations Manager 1.1 or 2.0 to an evaluation copy of Cisco Unified Operations Manager 2.0.1.

**Note**

You cannot upgrade from an evaluation copy of Cisco Unified Operations Manager 1.1 or 2.0 to an evaluation copy of Cisco Unified Operations Manager 2.0.1.

---

To upgrade from Cisco Unified Operations Manager 1.0, see [Upgrading from Operations Manager 1.0 to Operations Manager 2.0.1, page 2-16](#).

To upgrade from IP Telephony Monitor 2.0, see [Moving from IP Telephony Monitor 2.0 to Cisco Unified Operations Manager 2.0.1, page 2-16](#).

**Note**

When you upgrade Operations Manager, you are also upgrading Service Monitor.

---

There are two levels of functionality that you can purchase for Operations Manager 2.0.1: Premium Edition and Standard Edition. If you are upgrading from Operations Manager 1.0 or 1.1 to the Standard Edition of Operations Manager 2.0.1, you will lose some functionality that you previously had in Operations Manager 1.0 and 1.1. You will not be able to use the following diagnostics:

- Phone Status Tests
- Synthetic Tests
- Node-to-Node Tests

Further, you will not have access to the new diagnostic tools that Operations Manager 2.0.1 Premium Edition provides.

To get full Operations Manager functionality, you must upgrade to Operations Manager Premium Edition.

**Before You Begin**

- Before upgrading, back up your existing (Operations Manager 1.1 or 2.0 system) Synthetic Tests and Batch Tests by exporting them to a file. If you lose the tests after upgrade, you can use the backup files to recreate the tests on your upgraded system.
- Make sure your system meets the system requirements (see [Server Requirements, page 1-3](#)).
- Close all open or active programs. Do not run other programs during the upgrade process.
- If Operations Manager has been running for a long period of time and has accumulated a large amount of data (database over 1 GB), you should run an independent backup before upgrading. Also, during installation, do not run the backup data process. You can use Windows Explore to view the database size (Operations Manager's databases are located in the <NMSROOT>\databases folder).




---

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

---

- If you are using Service Monitor or plan on using it, you should be aware of the following:
  - If you plan on using Service Monitor to monitor MOS reported from Cisco Unified Communications Managers, configure the server to use NTP before you upgrade. For more information, see [NTP Configuration Notes, page 2-17](#).
  - It is recommended that you delete existing sensor configuration files—one QOVDefault.CNF file and a QoVMACAddress.CNF file for each sensor—from your existing TFTP servers before you perform the upgrade. Immediately after you upgrade to the Service Monitor 2.0.1 software, sensors are unable register to Service Monitor until you perform post-upgrade configuration steps; for more information, see [Service Monitor Post-Upgrade Configuration, page 2-15](#).
  - If you are upgrading from Service Monitor 1.1, you should make note of the TFTP server that you are using with Service Monitor. You will need the IP address of the TFTP server to add it to Service Monitor after upgrade. (If you are upgrading from 2.0, the TFTP server addresses are retained in the Service Monitor database.)
- 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 2-2](#).

---

**Step 1** As the local administrator, log in to the machine on which you will be upgrading the Operations Manager software.

**Step 2** Stop the daemon manager by running the following command (in a command prompt):

```
net stop crmdmgt
```

**Step 3** Insert the Cisco Unified Operations Manager CD-ROM into the CD-ROM drive. The Cisco Unified Operations Manager and Service Monitor Setup Program window opens.




---

**Note** 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 4** Click **Install**. The Welcome window appears.

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

**Step 6** Click **Accept**. The Licensing Information window appears.

**Step 7** If you are upgrading from Operations Manager 1.1 you will need to enter licensing information (if you are upgrading from Operations Manager 2.0, you will not see this option). 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 A-3](#).

---

The Setup Type window appears.

**Step 8** Select **Typical** or **Custom**.

**Step 9** The System Requirements window displays the results of the requirements check and advises whether the upgrade can continue; click **Next**.




---

**Note** If memory requirements are not met, installation cannot proceed. See [Server Requirements, page 1-3](#).

---

**Step 10** If you chose Custom installation, you can change any of the following:

- User Admin password and Guest password
- System identity account password
- casuser password
- Common Services database password
- HTTPS port, administrator e-mail, or SMTP server settings
- Create a self-signed certificate
- Username and password for data transport protocol authentication

This step is not required for Typical installation. Click **Next**.

**Step 11** The Summary window appears, displaying the current settings. Click **Next**. The installation proceeds.

**Step 12** Click **OK** to confirm additional messages if they are displayed:

- If the system has more than one NIC card 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**

---

Operations Manager requires only one NIC card and supports only one IP address. Operations Manager does not support two NIC cards with different IP addresses.

---

- If Windows SNMP service is not installed on your system, a message will inform you of this fact.
- If you did not supply a license file during the installation, a message about obtaining a license file is displayed.

- When the installation is complete, the following message appears:

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 2-17](#).)

- Step 13** Remove the Cisco Unified Operations Manager CD from the drive.



---

**Note** Store the CD in a secure, climate-controlled area for safekeeping.

---

- Step 14** Click **Finish** to reboot the machine.

- Step 15** Wait 30 minutes after the system reboots before starting Operations Manager. This gives all of Operations Manager's processes time to initialize.

- Step 16** Verify the upgrade by starting Operations Manager.

- Step 17** To make sure all existing devices go to the monitored state, Operations Manager must perform rediscovery. Do the following:

- a. In Operations Manager, select **Device > Device Management > Modify/Delete Devices**.
- b. In the device selector, select the All Devices check box.
- c. Click **Rediscover**.

- Step 18** If you disabled DEP before the installation, see [Enabling DEP, page 2-3](#).
- 

If any errors occur during installation, check the installation log in the root directory on the drive. (For example, the CiscoWorks Common Services installation might create C:\Ciscoworks\_setup001.log, the Operations Manager installation might create C:\Ciscoworks\_setup002.log, and so forth.) The Cisco Technical Assistance Center (TAC) might ask you to send them the installation log.

## Service Monitor 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.

- 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**. Operations Manager 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.

**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*.**

---

## Upgrading from Operations Manager 1.0 to Operations Manager 2.0.1

There is no upgrade from Operations Manager 1.0 to Operations Manager 2.0.1. If you are moving from Operations Manager 1.0, you must first uninstall it before installing Operations Manager 2.0.1.

## Moving from IP Telephony Monitor 2.0 to Cisco Unified Operations Manager 2.0.1

There is no upgrade from IP Telephony Monitor 2.0 to Cisco Unified Operations Manager 2.0.1. If you are moving from IP Telephony Monitor, you must first uninstall it before installing Operations Manager.

# Configuring Your System for SNMP Queries

Operations Manager implements the system application MIB. If you want to use a third-party SNMP management tool to make SNMP queries against the server where Operations Manager 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 installing Operations Manager, you should modify the credentials for Windows SNMP service to not use a default or well-known community string.

It is recommended that you install Windows SNMP service before you install Operations Manager. 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 Operations Manager. 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*.

## NTP Configuration Notes

The clocks on Service Monitor and Cisco 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 Cisco 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](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 Communications 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.

---