



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. A Service Monitor 2.0 license also supports Service Monitor 2.1. 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](#)
- [Upgrading to Cisco Unified Operations Manager 2.1, page 2-10](#)
- [Reinstalling Operations Manager, page 2-20](#)
- [Uninstalling Operations Manager, page 2-21](#)
- [Configuring Your System for SNMP Queries, page 2-22](#)
- [NTP Configuration Notes, page 2-22](#)

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 1-2](#).)
- 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 2-4](#).)
- 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 or upgrading 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.
- Verify that the drive that you choose to install Operations Manager on is an NTFS file system.
- If you are using an IBM server with IBM director installed, 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.
- Verify that the fully qualified domain name of the system on which Operations Manager 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 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:\PROGRA~1\CSCOPx.

- Operations Manager uses ICMP ping to determine the reachability of all devices. Some security applications may detect burst of ICMP pings as being caused by a malicious application. The security application may then block the ping requests. This can cause Operations Manager to generate a flood of false unreachable events. To avoid this situation, you should configure security applications so they do not block bursts of ICMP pings from the Operations Manager server.
- If you have Cisco Security Agent (CSA) installed on your system, and the CS Agent is running, shut it down. If you do not shut it down, you may receive a confirmation message during installation requesting permission to continue with the installation. Select **Yes** and proceed with the installation/upgrade. To shut off the CS Agent, right-click on the Cisco Security Agent. Then select Security Level and select **off**.
- If you plan to install Service Statistics Manager on the Operations Manager server, you must reserve port 1099 and 1100 before installing Operations Manager 2.1. Complete the steps in [Reserving Port 1099 and 1100 for Service Statistics Manager Use, page 2-3.](#)
- Service Statistics Manager stops collecting data from Operations Manager when you reinstall or upgrade Operations Manager and change either of the following:
 - The password for the user "admin."
 - The destination location (the directory in which Operations Manager is installed).

If you change the admin password or the destination location, you can enable data collection by performing procedures that are documented in [Release Notes for Cisco Unified Service Statistics Manager 1.1.](#)

- On 4-GB system, Microsoft Windows detects only 3.5 GB of RAM, even though your system may have 4 GB installed. If you want to choose the medium or large installation when installing Operations Manager, you must first enable all 4 GB of RAM on the system. See [Enabling the Full 4 GB of RAM, page 2-3](#).

**Caution**

If system memory is less than the minimum required to deploy both Operations Manager and Service Monitor a warning displays asking you to upgrade your memory for better performance. If system memory is less than the minimum required, an error displays and the installation cannot continue. You must upgrade system memory to at least 4 GB before you continue with the installation.

Before upgrading or reinstalling Operations Manager, do the following:

- You must back up Operations Manager before an upgrade or reinstallation can be performed. See [Backing Up Data Before the Upgrade or Reinstall, page 2-11](#). During 2.1 upgrade or reinstall, the back up is no longer done due to time limitations.

Enabling the Full 4 GB of RAM

On 4-GB system, Microsoft Windows only detects 3.5 GB of RAM even though your system has 4 GB installed. If you want to choose the medium or large installation when installing or upgrading Operations Manager, you must first enable all the 4 GB of RAM on the system.

-
- Step 1** On the Operations Manager system, in Microsoft Windows, right-click **My Computer**.
 - Step 2** Select **Properties**.
 - Step 3** Select the **Advanced** tab.
 - Step 4** Under Startup and Recovery, click **Settings**.
 - Step 5** Click **Edit**. The boot.ini file opens.
 - Step 6** In the file, add **"/PAE"** to the line that starts with "multi(0)disk(0)rdisk(0)partition(1)\WINDOWS=..."
 - Step 7** Restart the system.
-

Reserving Port 1099 and 1100 for Service Statistics Manager Use

If you plan to install Service Statistics Manager on the Operations Manager server, you must reserve port 1099 and 1100 before installing or upgrading Operations Manager 2.1.

-
- Step 1** Select **Start > Run**.
 - Step 2** Enter regedit and click **OK**. The Registry Editor opens.
 - Step 3** Locate and click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

- Step 4** Right-click ReservedPorts and select **Modify**.

This procedure assumes that the Operations Manager installation process has reserved port 3343 by creating a ReservedPorts multi-string value in the registry with the data 3343-3343 in it. If the ReservedPorts multi-string value does not exist:

- a. Select **Edit > New > Multi-string Value**.
- b. Rename the new value to ReservedPorts.
- c. Double-click ReservedPorts.

Step 5 Add 1099-1099 and 1100-1100 to the value data; enter a space after any preceding value:

3343-3343 1099-1099 1100-1100

Step 6 Click **OK**.

Step 7 Close the Registry Editor.

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 2-4](#).)
- Make sure all processes are running on the Operations Manager system. (See [Actions to Take Before Adding Devices, page 2-5](#).)

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.
- For all 5.x (and greater) Cisco Unified Communication Managers, make sure that the SOAP-Performance Monitoring API is running on all nodes and that the AXL service is activated on the first node (Publisher).
- For all 3.x and 4.x Cisco Unified Communication Managers, make sure that the IIS service is enabled.

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).

- 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:\PROGRA~1\CSCOpx`.

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

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

Port Numbers	Service Name	Application
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
8080	Used to determine if the Cisco Unified Communications Manager 5.0 web service is up. Note 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. Note 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**. An Operations Manager 2.0 license also supports Operations Manager 2.1. You are not required to get a new license.

**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 2-22](#).
- 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. We recommend you exclude the NMSROOT\databases directory from virus scanning. Problems can arise if database files are locked because of virus scanning.
- 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 2-22](#).
- 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 1-2](#).

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 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

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 1-2.](#))
- 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\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.
```

**Caution**

This message may not appear in the foreground and may be minimized in the taskbar. You must click **OK** in this message or your installation time may be significantly impacted.

For more information, see [NTP Configuration Notes, page 2-22](#).

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 > Cisco Unified Operations Manager**.

**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.

Upgrading to Cisco Unified Operations Manager 2.1

This section covers the following topics:

- [Upgrade Paths, page 2-11](#)
- [Backing Up Data Before the Upgrade or Reinstall, page 2-11](#)
- [Before You Begin, page 2-15](#)
- [Upgrading from Operations Manager Releases Prior to 2.0 to Operations Manager 2.0.x, page 2-16](#)
- [Upgrading from Operations Manager 2.0.x to Operations Manager 2.1, page 2-16](#)
- [Restoring Detailed Device View Configuration Data to Operations Manager 2.1, page 2-18](#)
- [Configuring Service Monitor After Upgrading, page 2-18](#)
- [Changes to Notification Event Customization Severity After Upgrade, page 2-20](#)

Upgrade Paths

Operations Manager supports the following upgrade paths:

- Upgrade from a licensed copy of Cisco Unified Operations Manager 2.0.x to a purchased copy of Cisco Unified Operations Manager 2.1.
- Upgrade from a licensed copy of Cisco Unified Operations Manager 2.0.x to an evaluation copy of Cisco Unified Operations Manager 2.1.

There is no full backup run as part of an upgrade or reinstall. This is to allow for a timely upgrade/reinstallation. For instructions on how to run your back ups, see [Backing Up Data Before the Upgrade or Reinstall, page 2-11](#) before performing your upgrade or reinstall.



Caution

There is no direct upgrade from releases prior to 2.0. See [Upgrading from Operations Manager Releases Prior to 2.0 to Operations Manager 2.0.x, page 2-16](#) for details on how to proceed. To download Cisco Unified Operations Manager 2.0.x, go to Cisco.com for the software download at <http://www.cisco.com/cgi-bin/tablebuild.pl/cuom202>.



Note

You cannot upgrade from an evaluation copy of Cisco Unified Operations Manager to a newer evaluation copy of Cisco Unified Operations Manager.

If you have a version of Cisco Unified Operations Manager prior to 2.0.x, see [Upgrading from Operations Manager Releases Prior to 2.0 to Operations Manager 2.0.x, page 2-16](#).

To upgrade from Cisco Unified Operations Manager 2.0.x, see [Upgrading from Operations Manager 2.0.x to Operations Manager 2.1, page 2-16](#).



Note

When you upgrade to Operations Manager, the Service Monitor version changes to 2.1.

There are two levels of functionality that you can purchase for Operations Manager 2.1: Premium Edition and Standard Edition. To get full Operations Manager functionality, you must upgrade to Operations Manager Premium Edition.

Backing Up Data Before the Upgrade or Reinstall

You should back up configuration and data files on the Operations Manager server. This is to ensure you have a backup if corruption occurs.

The following sections cover various backup scenarios for Operations Manager. Refer to each section before making your backup decision.

- [Backing Up and Restoring Detailed Device View Configurations Using Operations Manager Utilities, page 2-12](#)
- [Backing Up and Restoring Using CiscoWorks, page 2-13](#)
- [Handling Sybase Database Issues Before Installation for Operations Manager 2.1, page 2-14](#)

The Detailed Device View configuration is preserved during the 2.1 upgrade; for more information, see [Upgrade Data Scenarios](#).

Table 2-3 describes the data that is stored. Database backup and restore is supported only on the same version of Operations Manager (which includes the database and user configuration data of all Operations Manager modules).

**Caution**

A warning message displays during the upgrade/reinstall procedure. If you have not completed a backup, you can exit the installation to perform your backup.

Table 2-3 Upgrade Data Scenarios

Data	Upgrade Status
Event data	<p>Individual modules (FH, NOS, Event Adapters) copy the updated event lists to their respective configuration files during upgrade.</p> <p>No new events from the removed list are generated after the upgrade. However, you must clear the existing removed events from the system. See Clearing Events After Upgrade, page 2-19. Active events in the Alerts and Events display must be cleared manually.</p>
Device information	<p>Device data.</p> <p>Note Operations Manager does not restore DDV configurations on voice services, system processor, hard disk, virtual memory, and RAM components for Cisco Unified Communications Manager machines. Operations Manager uses RTMT polling, not device MIB polling, to create the above components and therefore does not display the above 2.0.x data in the Operations Manager 2.1 DDV. Operations Manager 2.1 DDV displays voice services, system processor, hard disk, and virtual memory components, but they are different from the components in 2.0.x.</p>
Operations Manager 2.0.x upgrade	See Before You Begin, page 2-15 .

Backing Up and Restoring Detailed Device View Configurations Using Operations Manager Utilities

During the 2.1 upgrade/reinstall the Detailed Device View (DDV) back up is run automatically. The backup utility backs up the states of all components of all types of monitored or partially monitored devices (except for those mentioned below) in the DDV. It does not cover suspended devices. You can also run this script at any time to save your device data if you are using Operations Manager 2.0.3.

**Note**

Operations Manager does not restore DDV configurations on voice services, system processor, hard disk, virtual memory, and RAM components for Cisco Unified Communications Manager boxes. Operations Manager uses RTMT polling, not device MIB polling, to create the above components and therefore does not display the above data in the Operations Manager DDV in 2.1.

**Caution**

Ensure that the daemon processes for this system are up and running to allow for data backup.

The restore utility restores the managed states of nonsuspended devices in the Detailed Device View.

Step 1

If you ran the upgrade or reinstallation program, you do not have to perform this step. To run the backup utility, open a DOS prompt and enter:

```
% PROGRA-1\CSCOpX\objects\vhm\utilities\inventoryBackup default
```

Where *default* saves the managed states of *all* monitored and partially monitored devices in to the inventoryBackup file. There is no user input needed while the script is running.

If you prefer to enter a specific file name or a list specific device IPs, enter:

```
% PROGRA-1\CSCOpX\objects\vhm\utilities\inventoryBackup
```

The script prompts you to enter the file name and device information.

**Caution**

After an Operations Manager 2.1 upgrade, you can run **inventoryRestore** script only after rediscovering all devices from Operations Manager Device Management interface.

Step 2

To run the restore utility, open a DOS prompt and enter:

```
% PROGRA-1\CSCOpX\objects\vhm\utilities\inventoryRestore default
```

Where *default* restores the data saved in the inventoryBackup.xml file. There is no user input needed while the script is running.

If you want to input your own file name enter:

```
% PROGRA-1\CSCOpX\objects\vhm\utilities\inventoryRestore
```

The script prompts you to enter the file name you previously created using the backup utility.

Backing Up and Restoring Using CiscoWorks

When Service Monitor and Operations Manager are installed together, you must use this Common Services database backup procedure. These procedures back up the databases located on the server, including those for Service Monitor, Common Services, and Operations Manager.

This topic also explains how to locate the online help procedures for restoring data.

**Caution**

Backup and restore (including database backup and user configuration data backup) is supported only on the same version of Operations Manager.

Step 1

From the Operations Manager home page, click **CiscoWorks** in the upper right-hand corner of the window. The CiscoWorks home page opens.

Step 2

Under Common Services select **Server > Admin > Backup**. The Backup Job page appears.

Step 3

Click the Help button and follow the instructions for backing up and restoring data.

Database files are stored using the backup directory structure described in [Table 2-4](#).

- Format—/*generation_number/suite/directory/filename*
- Example—/1/itemFh/database/itemFh.db

Table 2-4 Operations Manager Backup Directory Structure

Option	Description	Usage Notes
generationNumber	Backup number	For example, 1, 2, and 3, with 3 being the latest database backup.
suite	Application, function, or module	When you perform a backup, data for all suites is backed up. The CiscoWorks server suite is cmf. The Operations Manager application suites are: <ul style="list-style-type: none"> • dfm—Data collection and analysis for devices in IP infrastructure • itemEpm—Event promulgation • itemFh—Alert history • itemInv—Device inventory • itemIPIU—Phone information • qovr—Service quality • vhm—Data collection and analysis for voice-enabled devices • wpu—Node-to-Node tests.
directory	What is being stored	Each application or suite listed. Directories include database and any suite applications.
filename	File that has been backed up	Files include database (.db), log (.log), version (DbVersion.txt), manifest (.txt), tar (.tar), and data files (datafiles.txt).

Handling Sybase Database Issues Before Installation for Operations Manager 2.1

The Operations Manager 2.0.x database may need to be unloaded and reloaded before the installation/upgrade. There is a Sybase database failure problem where the database can become corrupt, fail to validate, or grows too large (over 10 GB causing the backup procedure to take a long time). If your database shows any of the issues described, use the following procedure to unload and reload the database. You must know your database password to perform this procedure. If you do not know your database password, contact your customer support representative.

Step 1 Stop the daemon manager:

```
% net stop crmdmgt
```



Tip

Ensure you wait until all database processes have stopped running. You can check for running dbeng9 or dbsrv9 processes using the process explorer tool.

Step 2 Unload the database:

```
% dbunload -c "uid=<username>;pwd=<pwd>;dbf=<db name>" <Directory to unload data >
```

For example:

- ```
% dbunload -c "uid=itemFhUser;pwd=<pwd>;dbf=itemFh.db" c:\unload
```
- Step 3** Remove and save the itemFh.db to another directory.
- Step 4** Initialize the new database:
- ```
% dbinit -p 4096 itemFh.db
```
- Step 5** Reload the new database:
- ```
% dbisqlc -c "uid=<default username>;pwd=<default passwd>;dbf=<db name>" reload.sql
```
- For example:
- ```
% dbisqlc -c "uid=dba;pwd=sql;dbf=itemFh.db" reload.sql
```
- Step 6** Delete the *.DAT and *.SQL files newly created, and restart daemon manager.
- ```
% rm *.dat *.sql
% net start crmdmgtd
```
- 

## Before You Begin

- Complete the steps in [Preparing the Operations Manager Server, page 2-2](#)
- Make sure your system meets the system requirements (see [Server Requirements, page 1-2](#)).
- 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 Explorer 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:\PROGRA~1\CSCOPx.

---

- If you will use Service Monitor or plan on to use 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 2-22](#).
  - 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 [Configuring Service Monitor After Upgrading, page 2-18](#).
- If you have Cisco Security Agent installed and running in your system, shut it down before upgrading Operations Manager. If you do not shut it down, you may receive a confirmation message during the upgrade or the upgrade process may fail. (See the *Release Notes for Cisco Unified Operations Manager* on Cisco.com for more details.)
- If you plan to install Service Statistics Manager on the Operations Manager server, you must reserve port 1099 and 1100 before installing or upgrading to Operations Manager 2.1. Complete the steps in [Reserving Port 1099 and 1100 for Service Statistics Manager Use, page 2-3](#). Complete the Operations Manager upgrade first, then install Service Statistics Manager.

- If there is an `inventorybackup.xml` file in `CSCOpX\objects\vhm\utilities` directory before Operations Manager 2.1 upgrade, rename the `inventorybackup.xml` file before you perform the upgrade.
- In order to improve the response times for the Fault History database, run disk defragmentation on the Operations Manager server machine before you install the 2.1 software. The upgrade now allocates 2 GB of disk space to the database and this procedure will ensure faster response times.

## Upgrading from Operations Manager Releases Prior to 2.0 to Operations Manager 2.0.x

There is no direct upgrade from Operations Manager 1.1 to Operations Manager 2.1. If you are upgrading from any of these versions of Operations Manager, you must first upgrade to Operations Manager 2.0.x, then upgrade to Operations Manager 2.1.

To ensure safe migration of your Operations Manager 1.x data, you must upgrade from 1.x to 2.0.x before you upgrade to Operations Manager 2.1. To download Cisco Unified Operations Manager 2.0.x, go to <http://www.cisco.com/cgi-bin/tablebuild.pl/cuom20>.

## Upgrading from Operations Manager 2.0.x to Operations Manager 2.1

The upgrade procedure takes approximately 45 to 90 minutes (depending on your existing database).

- Step 1** As the local administrator, log in to the machine on which you will be upgrading the Operations Manager software. Ensure that the data backup has been performed.



**Note** If there is an `inventorybackup.xml` file in `CSCOpX\objects\vhm\utilities` directory before Operations Manager 2.1 upgrade, rename the `inventorybackup.xml` file before you perform the upgrade.

- Step 2** Insert the Cisco Unified Operations Manager CD-ROM into the CD-ROM drive. The Cisco Unified Operations Manager 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 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**. Click **Next**.

- Step 7** 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 1-2](#).

- Step 8** If you chose Custom installation, you can do any of the following, and then click **Next**:

- Change the user Admin password and Guest password
- Change the system identity account password
- Change the casuser password
- Change the Common Services database password
- Change the HTTPS port, administrator e-mail, or SMTP server settings
- Create a self-signed certificate

This step is not required for Typical installation.

**Step 9** 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

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

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

**Step 11** 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 2-22](#).)

**Step 12** Remove the Cisco Unified Operations Manager CD from the drive.



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

**Step 13** Click **Finish** to reboot the machine.

**Step 14** Wait 30 minutes after the system reboots before starting Operations Manager. This gives all of Operations Manager's processes time to initialize.

**Step 15** Verify the upgrade by starting Operations Manager.

- Step 16** To make sure all existing devices go to the monitored state, you must configure Operations Manager to perform rediscovery after restart. Do the following:
- In Operations Manager, select **Device > Device Management > Modify/Delete Devices**.
  - In the device selector, select the **All Devices** check box.
  - Click **Rediscover**.
- Step 17** To restore the detailed device view configuration, run the restore utility after [Step 16](#) completes. See [Restoring Detailed Device View Configuration Data to Operations Manager 2.1, page 2-18](#). Be sure you have rediscovered your devices before completing this step.
- Step 18** To manually clear the false events that were removed in Operations Manager 2.1, see [Clearing Events After Upgrade, page 2-19](#).

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:\Cisoworks\_setup001.log, the Operations Manager installation might create C:\Cisoworks\_setup002.log, and so forth.) The Cisco Technical Assistance Center (TAC) might ask you to send them the installation log if you encounter problems.

## Restoring Detailed Device View Configuration Data to Operations Manager 2.1

If you upgraded from a previous release of Operations Manager, you must restore the Detailed Device View data that you backed up before the upgrade or reinstallation using the restore utility.

The restore utility restores the managed states of nonsuspended devices in the Detailed Device View.

The utilities are located in CSCOPx\objects\vhm\utilities. To run the restore utility, open a DOS prompt and enter:

```
% CSCOPx\objects\vhm\utilities\inventoryRestore default
```

Where *default* restores the data saved in the inventoryBackup.xml file. No user input is needed while the script is running.

If you want to input your own filename, enter:

```
% CSCOPx\objects\vhm\utilities\inventoryRestore
```

The script prompts you to enter the filename you previously created using the backup utility.

For information on backing up your Detailed Device View after your upgrade and restore is complete, see the online help or [User Guide for Cisco Unified Operations Manager](#).

## Configuring Service Monitor After Upgrading

This section provides the minimum steps required to enable sensors to register with Service Monitor 2.1. 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** Configure the default configuration file:
- Select **Configuration > Sensor > Setup**. The Setup page appears.

- b. Update the Default Configuration to TFTP Server fields:
  - Image Filename—Enter SvcMonAA2\_42.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 are configured in Service Monitor.
- d. Copy the binary image file, SvcMonAA2\_42.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” in the *Quick Start Guide for Cisco Unified Service Monitor* on Cisco.com.

**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. Manually upload the configuration file to the root location on the TFTP server from the Service Monitor image file directory, *NMSROOT*\ImageDir. After uploading the configuration file, reset the TFTP server on Unified Communications Manager. For more information, see the Unified Communications Manager documentation.

---

**Step 3**

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

**Warning**

---

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

---

## Clearing Events After Upgrade

You must to manually clear the following events generated on Cisco Unified Communications Manager that are displayed in Alerts and Events display after the upgrade is complete:

- InsufficientFreeHardDisk
- InsufficientFreeMemory
- InsufficientFreePhysicalMemory
- InsufficientFreeVirtualMemory
- cpuUtilizationExceeded
- ServiceDown
- DBReplicationFailure

These events were removed from the most recent release of Operations Manager and will continue to be displayed in the Alerts and Events display as active. They will not be automatically removed from the display, so must be manually cleared.

## Changes to Notification Event Customization Severity After Upgrade

If you are upgrading from Operations Manager 2.0 or 2.0.1, be aware that the notification event customization changed for 2.0.2 and 2.0.3.

Table 2-5 lists the severity levels, before and after the upgrade.

**Table 2-5 Notification Event Customization Severity**

| Operations Manager 2.0 | Operations Manager 2.0.2/2.0.3/2.1 |
|------------------------|------------------------------------|
| 0—Critical             | 3—Critical                         |
| 1—Warning              | 2—Warning                          |
| 2—Informational        | 1—Informational                    |
| 3—Undefined            | 4—Undefined                        |
| 4—Undefined            | 5—Undefined                        |
| 5—Undefined            | 6—Undefined                        |
| 6—Undefined            | 7—Undefined                        |
| 7—Undefined            | 8—Undefined                        |

## 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**. Click **Next**.
- Step 7** The System Requirements window displays the results of the requirements check and advises whether the reinstallation can continue; click **Next**.
- Step 8** If you chose Custom installation you will be asked to enter the casuser password. This step is not required for Typical installation. Click **Next**.
- Step 9** An information dialog box appears, confirming reinstallation; click **OK**. The Summary window appears, displaying the current settings.
- Step 10** Click **Next**. The installation proceeds.
- Step 11** Remove the Cisco Unified Operations Manager CD from the drive.



---

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

---

- Step 12** Click **Finish** to reboot the machine.
- Step 13** 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 > Cisco Unified Operations Manager**.
- Step 14** To make sure all existing devices go to the monitored state, you must configure Operations Manager to perform rediscovery after restart. Do the following:
- In Operations Manager, select **Device > Device Management > Modify/Delete Devices**.
  - In the device selector, select the **All Devices** check box.
  - Click **Rediscover**.
- Step 15** To restore the detailed device view configuration, run the restore utility after [Step 16](#) completes. See [Restoring Detailed Device View Configuration Data to Operations Manager 2.1, page 2-18](#). Be sure you have rediscovered your devices before completing this step.
- Step 16** To manually clear the false events that were removed in Operations Manager 2.1, see [Clearing Events After Upgrade, page 2-19](#).
- 

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:\Ciscoverks\_setup001.log, the Operations Manager installation might create C:\Ciscoverks\_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 > Uninstall Cisco Unified Operations Manager**.
- 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**.

---

## 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.

---

To enable Operations Manager to manage itself, install and configure SNMP on a local server. 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 © 2008, Microsoft Corporation.

---

