



## 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 2-11](#)  
[Uninstalling Operations Manager, page 2-12](#)  
[Upgrading to Cisco Unified Operations Manager 2.0.2, 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 2-7](#).)

## 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

Clean the temp directory. You can open the temp directory by typing `%temp%`

Operations Manager server; in a command prompt, run the command  
<NMSROOT>\bin>smNameRes.exe.




---

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.

---

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.

## Checking for and Temporarily Disabling DEP

Step 1



Note

Step 2

Step 3

Step 4

I select is selected

Turn on DEP for all programs and services except those

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

**Step 6** OK



---

If you disabled DEP before the installation, to turn it on again and enable the installed software to continue to run, use this procedure.

---

Log in as an administrator or a member of the Administrators group.

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

Click the Advanced tab and, under Performance, click **Settings**

**Turn on DEP for all programs and services except those I select**

OK

of the program doesn't appear in the list, click **Add**

OK



---

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

---

**Step 7**

---

## Preparing Devices for Addition to Operations Manager Inventory

- [Actions to Take Before Adding Devices](#), page 2-4.)
- 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 2-5.)

## Device-Specific Configurations

### Cisco Unified Communications Manager:

- 
- 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:

- 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:

- 
- 

### All Other Devices:

- 

## Actions to Take Before Adding Devices

- 
- 



Note

## Notes on Adding Devices

- 
- 
- 
- If there are many SNMP-unreachable devices in your network and you have to supply multiple device credentials (causing discovery can take a long time.

---

### Step 1

### Step 2

### Step 3

```
<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.

You can lower this value to 1000 milliseconds, or 1 second. You can choose a value based on the SNMP responsiveness in your network.

Save the changes that you made to the file.

Start discovery.




---

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



### 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
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.  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

**Ports that Service Monitor Uses**

	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.  These ports must be free.

## Gathering Information to Provide During Installation



**Note**

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



CiscoWorks

Server > Admin > Licensing



-  
-

## Performing a New Installation

- 

-

- [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 2-18](#).

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.

---

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](#).

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

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.




---

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.

---

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

Click **Next**

**Accept**

Next



---

---

**Step 8**

*Typical*

*Custom*

**Step 9**

**Step 10**

- 
- 

- 
- 

**Step 11**

**Step 12**



**Note**

---

---

**Step 13**

**Step 14**

**Yes**

Next

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**

- 
- 
- 

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.



**Finish**

**Start > All Programs > Cisco Unified Operations Manager > Cisco Unified 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

Step 2



Note

Step 3

Step 4

Step 5

Step 6

Step 7

Step 8

Step 9

Step 10

Step 11

Step 12

Step 13



Note

Step 14

Step 15

# Uninstalling Operations Manager



---

---



---

---

Step 1

Step 2

Step 3

Step 4

Step 5

Step 6

---

# Upgrading to Cisco Unified Operations Manager 2.0.2

- 
- 



---

---

  
**Note**

---

---

- 
- 
- 

**Before You Begin**

- 
- 
- 
- 

  
**Note**

---

---

- 

*MACAddress*

---

`net stop crmdmgt`



---

---



---

---



---

---



- a. **Device > Device Management > Modify/Delete Devices**
- b.
- c. **Rediscover**

**Step 18**

## **Service Monitor Post-Upgrade Configuration**

d.



Note

Step 3

a.

b.

c.

d.

*NMSROOT*  
*NMSROOT*

*NMSROOT*



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 2.0.2

## Moving from IP Telephony Monitor 2.0 to Cisco Unified Operations Manager 2.0.2

## Changes to Notification Event Customization Severity After Upgrade

*Table 2-3 Notification Event Customization Severity*

Operations Manager 1.1 or 2.0	Operations Manager 2.0.2

## Configuring Your System for SNMP Queries



Note

---



---

---

**Step 1**

a.

b.

•

•

**Step 2****Note**

---

*install SNMP service*

---

## NTP Configuration Notes

1.

*Synchronization: Best Practices,**Cisco IP Telephony Clock**authoritative time server in Windows Server 2003**How to configure an*

---

This website is Copyright © 2007, Microsoft Corporation.

---