



CHAPTER 1

Prerequisites

This chapter describes the prerequisites for installing Cisco Unified Operations Manager (with Cisco Unified Service Monitor) on a Windows system. It includes:

- [Server Requirements, page 1-1](#)
- [Client Requirements, page 1-9](#)
- [Cisco Unified Computing System, page 1-10](#)
- [Other System Software, page 1-10](#)
- [System Capacity, page 1-10](#)
- [Supported Devices and Software, page 1-11](#)

For additional requirements before you begin your installation, see [Preparing to Install Operations Manager, page 2-1](#). If you are migrating to Operations Manager 8.0 from an earlier release, see [Preparing to Migrate to Operations Manager 8.0, page 2-16](#). For an overview of the product features and updates, see the *User Guide for Cisco Unified Operations Manager* or the release notes.

Server Requirements

This section covers the server requirements including:

- [Installation Server System Minimum Requirements for Operations Manager, Table 1-1 on page 1-2](#)
- [Coresident Guidelines, page 1-3](#)
- [VMware Guidelines, page 1-5](#)
- [Increasing the Paging File Size, page 1-6](#)
- [Operations Manager Firewall Updates to Avoid Denial of Service Attacks, page 1-7](#)
- [Terminal Server Support for Windows 2003 and 2008, page 1-8](#)

[Table 1-1](#) lists the minimum server system requirements for installing Operations Manager. If you are planning to run Service Monitor or other IP Communications Management software on the same server as Operations Manager or in a virtualization environment, see [Coresident Guidelines, page 1-3](#) and [VMware Guidelines, page 1-5](#) for more information.

For details on supported devices and software, see the *Supported and Interoperable Devices and Software for Cisco Unified Operations Manager 8.0*.

Table 1-1 *Installation Server System Minimum Requirements for Operations Manager*

Requirement Type	Minimum Requirements for Deployment of up to...	
	Up to 10,000 Phones and 1,000 IP Devices	Up to 45,000 Phones and 2,000 IP Devices
Processor	Dual-core processor greater than 2 GHz minimum	One of the following (that add up to four processors): <ul style="list-style-type: none"> • Two dual-core processors greater than 2 GHz minimum • One Quad-core processor greater than 2 GHz minimum
Memory (RAM)	Minimum: 4 GB. ¹ Recommended: 8GB. ²	8 GB.
Page File Space ³	8 GB.	12 GB.
Disk Space ⁴	<ul style="list-style-type: none"> • 84 GB recommended. • NTFS file system (required for secure operation). • At least 16 MB in Windows temporary directory (%TEMP%). 	
Hardware	<ul style="list-style-type: none"> • Color monitor. (For optimum viewing on the Operations Manager display, Cisco recommends that you use the highest native resolution supported by the client PC and monitor. A large, high-resolution display will also allow for less scrolling through information presented and increase operator efficiency. The minimum resolution recommended is 1440 x 900. • CD-ROM drive. • Support for one or two 1-GB NICs (one is required, and the second is for failover support; both NIC cards must have the same IP address). 	
Software ^{5,6,7,8}	<p>One of the following:</p> <ul style="list-style-type: none"> • Windows Server 2003 with Service Pack SP 2 Enterprise Edition (32 bit version). • Windows Server 2003 R2. • Windows Server 2008 with SP2 Standard and Enterprise Edition (32 bit version).⁹ <ul style="list-style-type: none"> • Microsoft .NET Framework must be uninstalled for Operations Manager to work properly. If you have SP2, Microsoft .NET is automatically installed and must be uninstalled permanently. • ODBC Driver Manager¹⁰ 3.5.10 or later. • (Optional) ESX 3.5 and ESXi 4.x—Operations Manager supports ESX for virtualization. For requirements, see VMware Guidelines, page 1-5. • (Optional) NTP—If you are going to use Cisco Unified Service Monitor, configure the server to use Network Time Protocol (NTP) to synchronize with the time server that is used by Cisco Unified Communications Managers in your network. See NTP Configuration Notes, page 2-32. 	

The following list explains the footnotes from [Table 1-1](#), “Installation Server System Minimum Requirements for Operations Manager”:

1. For details on enabling the full 4 GB of RAM on Windows, see [Enabling the Full 4 GB of RAM, page 2-6](#).
2. If Cisco Unified Operations Manager 8.0 is working with Cisco Unified Service Statistics Manager, 8 GB of RAM is highly recommended on the Operations Manager server. In the next release, Operations Manager 8.5 will require 8 GB of RAM for any installation.

3. When configuring the page file, you should set both the minimum and maximum file size parameters to same size. Page size also needs to be changed from automatic to manual. This ensures that Windows creates a page file of the required size. See [Increasing the Paging File Size, page 1-6](#).
4. Do not install Operations Manager on a FAT file system.
5. You must install Operations Manager on a dedicated system. Do not install Operations Manager on a Primary Domain Controller (PDC) or Backup Domain Controller (BDC). Do not install Operations Manager in an encrypted directory. Operations Manager does not support directory encryption.
6. Immediately following installation, the TCP/IP stack should be hardened to avoid denial of service attacks. Ensure these steps are taken before product use. Also see the release notes for information on any additional vulnerabilities.
 - Apply Windows security patches. See Microsoft Security Updates for Denial of Service Attacks for details. The system that you use for your Operations Manager server should meet all the security guidelines that Microsoft recommends for Windows 2003 or 2008 Server. (CSCsy83124) See the NSA website for security guidance: <http://www.nsa.gov>. (Specifically, the TCP/IP stack should be hardened to avoid denial of service attacks.) Search for “Security Consideration for Network Attacks”, in “The Windows Server 2003 - Security Guide, v2.1” for download from this NSA URL. (This website is Copyright © 2010, Microsoft Corporation.)
 - Perform a procedure on their Windows Server 2003 Enterprise Edition or 2008 Standard or Enterprise Edition server to block remote access to all TCP/UDP ports except for those ports used by Operations Manager required for external access. See [Operations Manager Firewall Updates to Avoid Denial of Service Attacks, page 1-7](#).
7. The default locale for your Windows operating system must be set to US-English.
8. Windows Terminal Services is supported in Remote Administration mode only. Use of Windows Terminal Services or Remote Desktop and Virtual Network Computing (VNC) to remotely control the server is not recommended for performing day-to-day operations (for example, running reports, keeping dashboards open, and so on). For more information, see [Terminal Server Support for Windows 2003 and 2008, page 1-8](#).
9. Windows 2008 R2 (64 bit version) is not supported in Operations Manager 8.0.
10. To verify the version of ODBC Driver Manager, from the Windows desktop, select **Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**. Select the **About** tab. If necessary, install Microsoft Data Access Component (MDAC) 2.5 or later.

Coresident Guidelines



Note

For supported configurations in a virtualization environment, see [VMware Guidelines, page 1-5](#).

Operations Manager, Service Monitor, Service Statistics Manager, and Provisioning Manager can be coresident with up to 10,000 phones. [Table 1-2](#) provides the minimum requirements for this type of coresident installation.

Table 1-2 *Installation Server System Minimum Requirements for Coresidence*

Requirement Type	Minimum Requirements for Coresident Deployment of up to 10,000 Phones
Processor	Two-way quad-core processors greater than 3 GHz. A two-way quad-core processor is a system that contains 2 physical processors—each of which is a quad-core processor—effectively containing 8 (2x4) logical CPUs.
Memory (RAM)	16 GB (PAE enabled).
Page File Space ¹	32 GB.
Disk Space ²	<ul style="list-style-type: none"> • 320 GB recommended. (Minimum four SAS drivers.) For optimal I/O throughput, you must have a Battery Backed Write Cache (BBWC); we also recommend two I/O controllers (with two disks on each controller). • NTFS file system (required for secure operation). • At least 16 MB in Windows temporary directory (%TEMP%).
Hardware	<ul style="list-style-type: none"> • Color monitor. (For optimum viewing on the Operations Manager display, Cisco recommends that you use the highest native resolution supported by the client PC and monitor). A large, high-resolution display will also allow for less scrolling through information presented and increase operator efficiency. The minimum resolution recommended is 1440 x 900. • CD-ROM drive. • Support for one or two 1-GB NICs (one is required, and the second is for failover support; both NIC cards must have the same IP address).
Software ^{3,4,5,6}	<ul style="list-style-type: none"> • One of the following: <ul style="list-style-type: none"> – Windows Server 2003 Enterprise Edition SP2. – Windows Server 2008 Enterprise Edition SP2 (32 bit version).⁷ • ODBC Driver Manager 3.5.10 or later.⁸ • (Optional) NTP—If you are going to use Cisco Unified Service Monitor, configure the server to use Network Time Protocol (NTP) to synchronize with the time server that is used by Cisco Unified Communications Managers in your network. See NTP Configuration Notes, page 2-32.

The following list explains the footnotes from [Table 1-2, Installation Server System Minimum Requirements for Coresidence](#):

1. When configuring the page file, you should set both the minimum and maximum file size parameters to 32 GB. This will ensure that Windows creates a 32-GB page file.
2. Do not install Operations Manager on a FAT file system.
3. Do not install Operations Manager on a Primary Domain Controller (PDC) or Backup Domain Controller (BDC). Do not install Operations Manager in an encrypted directory. Operations Manager does not support directory encryption.
4. The system that you use for your Operations Manager server should meet all the security guidelines that Microsoft recommends for Windows 2003 or 2008 Server. See the NSA website for security guidance: <http://www.nsa.gov/>. (Specifically, the TCP/IP stack should be hardened to avoid denial of service attacks.) Search for “Security Consideration for Network Attacks” in *The Windows Server 2003 - Security Guide, v2.1* for download from this NSA URL.
5. The default locale for your Windows operating system must be set to either US-English.

6. Windows Terminal Services is supported in Remote Administration mode only. Use of Windows Terminal Services or Remote Desktop and Virtual Network Computing (VNC) to remotely control the server is not recommended for performing day-to-day operations (for example, running reports, keeping dashboards open, and so on). For more information, see [Terminal Server Support for Windows 2003 and 2008, page 1-8](#).
7. Windows 2008 R2 is not supported in Operations Manager 8.0 as it is a 64-bit version.
8. To verify the version of ODBC Driver Manager, from the Windows desktop, select **Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**. Select the **About** tab. If necessary, install Microsoft Data Access Component (MDAC) 2.5 or later.

To successfully perform coresident installations, follow these recommendations:

Step 1 Install each application along with its databases on a separate drive.

You can install one of the applications on the system drive (C:). However, if you have a sufficient number of drives, we recommend that none of the applications be installed on the system drive.

Step 2 Install applications in this order (recommended, not required):

- a. Operations Manager (includes Service Monitor)
- b. Service Statistics Manager
- c. Provisioning Manager (in Advanced mode)



Note If you have already installed Provisioning Manager, before you install Operations Manager on the same server, perform the tasks in [Preparing a Server Where Provisioning Manager Has Already Been Installed, page 2-4](#).

VMware Guidelines

Operations Manager supports VMware ESX 3.5 and ESXi 4.x. Operations Manager must have the same system resources available to it, inside the virtualization environment that it has for a standard (nonvirtual) installation.

While determining the performance of Operations Manager in your virtual setup, you must take into account that the VMware instance will use some system resources that would normally be available to Operations Manager in a standard installation. Additional requirements for running Operations Manager in a virtualization environment might vary with your environment and system load.

For more information, see *Best Practices for Cisco Unified Communications Management Suite on Virtualization*, at this URL: http://www.cisco.com/en/US/products/ps6535/prod_white_papers_list.html

For details on ordering additional licenses, see http://www.cisco.com/en/US/products/ps6535/prod_bulletins_list.html.

The following configurations are supported for Operations Manager in a virtual environment:

- Each of these products installed on a separate virtual machine:
 - Operations Manager
 - Service Monitor
 - Service Statistics Manager

- Provisioning Manager

Each product should support up to 10,000 phones and 1,000 IP devices. (Running one instance of an application on one virtual machine is the only supported configuration.)

- One instance of Operations Manager supporting up to 45,000 phones and 2,000 IP devices running on its own virtual machine.

For other supported Service Monitor, Service Statistics Manager, and Provisioning Manager configurations in a virtualization environment, see *Best Practices for Cisco Unified Communications Management Suite on Virtualization*, at this URL:

http://www.cisco.com/en/US/products/ps6535/prod_white_papers_list.html.

When setting up Operations Manager in a VMware environment, keep in mind the following guidelines:

- Resources must be reserved at 100% of requirements for the virtual machine.
- To use a licensed Operations Manager in a VMware environment, you must configure your virtual machine with a static MAC address.

You can run Operations Manager in Evaluation mode with a dynamic MAC address. However, before you can run a licensed copy of Operations Manager, you must configure a static MAC address.

To set up a static MAC address, do the following:

-
- Step 1** Power down the virtual machine.
 - Step 2** In the Inventory panel, select the virtual machine.
 - Step 3** Click the **Summary** tab and then click **Edit Settings**.
 - Step 4** In the Hardware list, select **Network Adapter**.
 - Step 5** For MAC address, select **Manual**.
 - Step 6** Change the current MAC address of the virtual machine to a static MAC address in the following range: 00:50:56:00:00:00 to 00:50:56:3F:FF:FF.

While assigning a static MAC address, we recommend choosing a complex address. An example of a complex MAC address is 00:50:56:01:3B:9F. A less complex MAC address is 00:50:56:11:11:11, because of the repeating ones (1).

If you choose a complex address, it is unlikely that you will choose an address being used by another customer. This can prevent accidental licensing overlap between different customers.
 - Step 7** Click **OK**.
-

Increasing the Paging File Size

When installing on Windows Server 2008, you must configure the paging file. You must change the configuration from Auto to Manual and set file sizes as specified in this procedure.

-
- Step 1** From the Windows Start menu, click **Start > Control Panel > System**.
 - Step 2** Select the Advanced tab and under Performance, click **Settings**.
 - Step 3** Select the Advanced tab and under Virtual memory, click **Change**.

- Step 4** Under Paging file size for the selected drive:
- Click **Custom size**
 - Enter the same value in both the Initial size (MB) and Maximum size (MB) boxes.



Note Virtual memory size must be two times the amount of RAM..

- Click **Set**.

- Step 5** Click **OK**.



Note Do not select “Automatically manage paging file size”.

Operations Manager Firewall Updates to Avoid Denial of Service Attacks

If you have Windows Server 2003 or Windows Server 2008, use the following procedure to block remote access to all TCP/UDP ports except for those required for external access by Operations Manager. The ports required for Operations Manager external access is listed in the procedure below in [Step 6](#). Ensure you review the release notes for up-to-date information on denial of service attack vulnerabilities. (CSCsy80792)

- Step 1** Open Control Panel for Windows Firewall.
- Step 2** Select **On** to block all outside sources from connecting to this computer.
The exceptions to this rule are documented in steps below.
- Step 3** Select the Exceptions tab and select any services you may want to open for remote access.
For example, Remote Desktop or File and Print Sharing.
- Step 4** Select the Advanced tab.
To add exemptions for an individual connection, select the network connection that is used for connecting external clients to this server and then click **Settings**.
- Step 5** Click **Add** in the Advanced Settings dialog window to enter your port exceptions.
- Step 6** In the Service Settings dialog, enter each of the following TCP/UDP ports one at a time and click **OK**:

Description of Service	Protocol	Port Number ¹
CUOM Web Server	TCP	1741
CUOM HTTPS	TCP	443
CUSM SFTP Server	TCP	22
CUOM Trap Listener	UDP	161
CUOM Trap Listener	UDP	162
CUOM Syslog Receiver	UDP	514
CUSM Syslog Receiver	UDP	5666

1. Note that external and internal port numbers are the same for all the services that require external access.

Repeat [Step 6](#) until all ports are entered.

Step 7 Click **OK** in the Windows Firewall window to close it.

Step 8 Restart the server for the firewall settings to take effect, if required.

Terminal Server Support for Windows 2003 and 2008

You can install Operations Manager on a system with Terminal Services enabled in Remote Administration mode. However, you must not install Operations Manager on a system with Terminal Services enabled in Application mode.

If you have enabled Terminal Services in Application mode, you should disable the Terminal Server, reboot the system, and start the installation again.

[Table 1-3](#) summarizes the Terminal Services features on a Windows 2003 or 2008 Server.

Table 1-3 *Terminal Services on a Windows 2003 or 2008 Server*

Windows 2003/2008 Server	Features
Terminal Server	Remote access and virtual system. Each client has its own virtual OS environment.
Remote Desktop Administration	Remote access only. All clients use the same (and the only) operating system. Do not use terminal services to perform day-to-day tasks in Cisco Unified Management Communications Suite applications, such as viewing the real-time Fault monitor in Operations Manager or viewing reports in Service Monitor.

Enabling and Disabling Terminal Services on a Windows Server

To enable or disable the Terminal Server, go to **Manage Your Server > Add or Remove a Role > Terminal Server**.

To enable or disable remote desktop administration, go to **Control Panel > System > Remote**.

Enabling and Disabling FIPS on a Windows Server

Sometimes, Federal Information Processing Standard (FIPS)-compliant encryption algorithms are enabled for Group security policy on a Windows server.

When FIPS compliance is enabled, SSL authentication may fail on the Operations Manager server. For Operations Manager to work properly, you must disable FIPS compliance.

To enable or disable FIPS compliance on a Windows server:

Step 1 Go to **Start > Settings > Control Panel > Administrative tools > Local Security Policy**.

The Local Security Policy window appears.

- Step 2** Click **Local Policies > Security Options**.
- Step 3** Select **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.
- Step 4** Right-click the selected policy and select **Properties**.
- Step 5** Select **Enabled** or **Disabled** to enable or disable FIPS-compliant algorithms.
- Step 6** Click **Apply**.

You must reboot the server for the changes to take effect.

Client Requirements

Table 1-4 shows the minimum system requirements for Operations Manager clients.

If a client system is available, it is recommended that you perform all configurations and day-to-day activities on the client system. If a client system is not available, the Operations Manager server must also meet all the system requirements for a client system (see Table 1-4).

Table 1-4 Client System Requirements

Requirement Type	Minimum Requirements
System hardware	<ul style="list-style-type: none"> • Any PC or MAC with an dual-core processor greater than 2.0 GHz minimum. • The minimum screen resolution recommended is 1440 x 900.
System software	<ul style="list-style-type: none"> • One of the following: <ul style="list-style-type: none"> – Windows Server 2003 Enterprise Edition without Windows Terminal Services. – Windows Server 2003 R2. – Windows Server 2008 SP2. – Windows XP Professional with SP2. • Internet Explorer^{1,2} 8.0 or Firefox 3.6 or later. • Adobe Flash Player 9.0 or 10.0. Downloading Flash from the Adobe website requires that you install ActiveX cookies on the system. An offline installation of Flash may be required if Internet Explorer security patches are present on a newly installed Operations Manager server.
Memory (RAM)	2 GB minimum.
Page file space	2 GB.
Environment	<p>Clients must be able to access Operations Manager:</p> <ul style="list-style-type: none"> • From outside a firewall—Refer to documentation for your firewall for how to configure client access. • Across a Virtual Private Network (VPN)—The VPN tunnel should connect the client and a VPN router or similar device.

1. Internet Explorer 6.0 is not supported. The Operations Manager portal does not work with this version. If your Internet Explorer window unexpectedly quits, see the Operations Manager release notes for information on Microsoft updates.
2. Your browser's Internet security level must be set to Medium. To check the current level in Internet Explorer, select **Tools > Internet Options**, and click the **Security** tab.

Cisco Unified Computing System

Operations Manager can be installed on a Cisco Unified Computing System. If you are going to install Operations Manager on a Cisco Unified Computing System, make sure that the system has the latest firmware installed.

For more information, see *Best Practices for Cisco Unified Communications Management Suite on Virtualization*, at this URL:

http://www.cisco.com/en/US/products/ps6535/prod_white_papers_list.html

Other System Software

Ensure that any prerequisites for interoperable software (such as Service Monitor or Service Statistics Manager) are reviewed and acted upon before installing or upgrading Operations Manager 8.0.

For information on preparing to install, see [Preparing the Operations Manager Server, page 2-2](#). See the latest information on supported devices and interoperable software at http://www.cisco.com/en/US/products/ps6535/products_device_support_tables_list.html.

Operations Manager has undergone interoperability testing with McAfee Virus Scan Enterprise 8.0.

While using Operations Manager on a system with virus protection software, it is recommended that you enable virus protection only after the installation is complete. After the installation is complete, we recommend you to exclude the NMSROOT directory from virus scanning.

Problems can arise when Operation Manager files are locked because of virus scanning. You should schedule active scanning of drives and memory to occur during off-peak hours. You may experience delays, and performance may be degraded, when the virus scan software is scanning all files.

System Capacity

[Table 1-5](#) lists the maximum capacity of Operations Manager when it is installed on a system that meets the requirements for the deployment (see [Table 1-1](#)).

Table 1-5 System Capacity

System Parameters	Deployment up to:
	2,000 IP Devices and 45,000 Phones
Voice network IP devices ¹	2,000
Access ports ^{2, 2}	60,000
Trunk ports and interfaces ³	7,500
Cisco Unified Communications Manager (Unified Communications Manager) clusters	Up to 20
Unified Communications Managers	5-10 per cluster (total 150)
Cisco Unified Communications Manager Express and Cisco Unity Express	Up to 600

Table 1-5 System Capacity

System Parameters	Deployment up to:
	2,000 IP Devices and 45,000 Phones
Route lists and route groups	2,200
Phone status tests	1,000
Phone tests ⁴	1,000
Synthetic tests	250
Node-to-node tests/IPSLA tests	500
SRST monitoring	Up to 1,000
Sustained event rate per minute ^{5, 6}	60
High event rate per minute ^{6, 6}	200
Burst events ^{7, 8}	1,500
Concurrent client (browser) logins	10

1. The 500 phone license scales to 100 IP devices. The 1,000 phone license scales to 300 IP devices. The licenses for more than 1,000 phones scale to 2000 IP devices.
2. By default, Operations Manager does not manage access ports; however, it discovers the phones connected to these ports.
3. You can use the `sm_tpmgr` command to view the number of ports and interfaces in your inventory. See the tip below for information on how to use this command in Operations Manager.
4. Phone test scale is for sequential execution in a batch test. Parallel phone tests are not supported in this release.
5. Sustained events are event rates handled by the system on a continuous basis.
6. High events are event rates handled by the system during high activity periods that last for a short duration (up to one hour).
7. Burst events are event rates handled by the system for a one-time high activity period.
8. This is a process event count that includes poll events, traps, syslogs, and service quality traps.

To find out how many trunk and access ports are currently in the Operations Manager inventory, use the `sm_tpmgr` command:

```
# NMSROOT\objects\smarts\bin\sm_tpmgr.exe --server=DFM --sizes
```

Locate the line in the output that is similar to the following:

```
Total Number of Ports: 655 [42/42]
```

In this example, 665 ports were discovered in the server, of which 42 are monitored for connectivity and 42 are monitored for performance.

Supported Devices and Software

Device adapter packages for all supported devices are installed when you install Operations Manager. Information about device support can be found on Cisco.com at http://www.cisco.com/en/US/products/ps6535/products_device_support_tables_list.html.

For details on how to configure Cisco devices to be monitored by Operations Manager, see [Configuring Operations Manager to Monitor Devices, page 3-1](#).

For details on how to configure Cisco software applications (such as Service Monitor, Provisioning Manager, or Service Statistics Manager), see [Adding Cisco Unified Communications Management Server Links from Operations Manager, page 3-22](#).

**Caution**

Be sure to read the important sections on steps to take before installing Operations Manager. For prerequisite installation steps, see [Preparing to Install Operations Manager, page 2-1](#). For prerequisite migration steps, see [Preparing to Migrate to Operations Manager 8.0, page 2-16](#).
