Installation Guide for Cisco Unified Operations Manager (Includes Service Monitor)

Software Release 2.2
Cisco Unified Communications Management Suite

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-19471-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Installation Guide for Cisco Unified Operations Manager

CONTENTS

Preface

This guide describes Cisco Unified Operations Manager (Operations Manager), provides instructions for installing Operations Manager on a Windows system, and offers quick-start steps on the use of Operations Manager.

Audience

This document is for anyone who installs and initially uses Operations Manager.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** `font`
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font
Selecting a menu item in paragraphs	**Option > Network Preferences**
Selecting a menu item in tables	Option > Network Preferences

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Product Documentation

Note The originally published printed and electronic documentation is included with your product. Any changes after original publication are reflected on Cisco.com, where you will find the most up-to-date documentation.

Table 1 describes the product documentation that is available.

Table 1 Product Documentation

Document Title	Available Locations
Supported Devices Table for Cisco Unified Operations Manager 2.2	On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps6535/products_device_support_tables_list.html
Release Notes for Cisco Unified Operations Manager 2.2	• In PDF on the product CD-ROM • On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps6535/prod_release_notes_list.html
Installation Guide for Cisco Unified Operations Manager (Includes Service Monitor) 2.2	• In PDF on the product CD-ROM • On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps6535/prod_installation_guides_list.html
User Guide for Cisco Unified Operations Manager 2.2	• In PDF on the product CD-ROM • On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps6535/products_user_guide_list.html
Context-sensitive online help	• Select an option from the navigation tree, then click **Help** • Click the Help button on the page

Related Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 2 describes the additional documentation that is available.

Table 2 Related Documentation

Document Title	Available Locations
Release Notes for Cisco Unified Service Monitor 2.2	• PDF on the product CD-ROM • On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps6536/prod_release_notes_list.html
User Guide for Cisco Unified Service Monitor 2.2	• PDF on the product CD-ROM. • On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps6536/products_user_guide_list.html
Release Notes for CiscoWorks Common Services 3.2	On Cisco.com at this URL: http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_common_services_software/3.2/release/notes/cs32rel.html
User Guide for CiscoWorks Common Services 3.2	On Cisco.com at this URL: http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_common_services_software/3.2/user/guide/cs32ug.html

Additional Information Online

When a new Incremental Device Update (IDU) becomes available, you can download it from Cisco.com.

IDUs are cumulative; that is, new IDUs contain the contents of any previous IDUs. Use this procedure to determine which version of the IDU is installed on your Operations Manager Server.

Step 1 From the Operations Manager home page, click **CiscoWorks** in the upper-right corner of the window. The CiscoWorks home page opens.

Step 2 From the CiscoWorks home page, select **Software Center > Software Update**. The Software Update page appears in a new window.

Step 3 Scroll down to the Products Installed table and locate Cisco Unified Operations Manager.

Step 4 Examine the version number for Cisco Unified Operations Manager. The version number format is *x.y.z* where:

- *x* is the major version.
- *y* is the minor version.
- *z* is the IDU number.

You can also obtain any published patches from the download site.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

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:

- Product Overview, page 1-1
- Server Requirements, page 1-2
- Client Requirements, page 1-10
- Other System Software, page 1-10
- System Capacity, page 1-11
- Bandwidth Estimation, page 1-12
- Supported Devices and Software, page 1-12

For additional requirements before you begin your installation or upgrade, see Preparing the Operations Manager Server, page 2-2 or Before You Start the Upgrade, page 2-17.

Product Overview

Cisco Unified Operations Manager (Operations Manager) is a product from the Cisco Unified Communications Management Suite, which provides a comprehensive and efficient solution for network management and monitoring of Cisco Unified Communications deployments.

Operations Manager monitors and evaluates the current status of both the IP communications infrastructure and the underlying transport infrastructure in the network. Operations Manager uses open interfaces such as Simple Network Management Protocol (SNMP), Hypertext Transfer Protocol (HTTP), and Windows Management Instrumentation (WMI) to remotely poll data from different devices in the IP communications deployment.

Note Operations Manager does not deploy any agent software on the devices being monitored and thus is nondisruptive to system operations.

Cisco Unified Operations Manager increases productivity of network managers in the following ways:

- Provides contextual diagnostic tools—Enables you to isolate problems more quickly:
  - Diagnostic tests provide performance and connectivity details about different elements of the converged IP communications infrastructure.

  - Synthetic tests replicate end-user activity and verify gateway availability and other configuration and operational aspects of the IP communications infrastructure.
  - IP service-level agreement (SLA)-based diagnostic tests can measure the performance of WAN links and node-to-node network quality.
  - Clickable information in notification messages—Includes context-sensitive links to more detailed information about service outages.
  - Context-sensitive links to other CiscoWorks tools and Cisco tools—For managing IP communications implementations.
- Presents service-quality alerts—Uses information from Cisco Unified Service Monitor, when it is also deployed, to:
  - Display mean opinion scores (MOSs) associated with poor voice quality between pairs of endpoints (Cisco IP Phones, Cisco Unity messaging systems, or voice gateways) involved in a call and other associated details about the voice-quality problem.
  - Enable you to perform a probable path trace between the two endpoints and reports on any outages or problems on intermediate nodes in the path.
- Provides information on current connectivity-related and registration-related outages affecting IP phones (both Session Initiation Protocol and Skinny Client Control Protocol based phones) in the network. In addition, provides contextual information that enables locating and identifying the IP phones involved.
- Tracks IP communications devices and IP phone inventory—Tracks IP phone status changes and creates a variety of reports that document move, add, and change operations on IP phones in the network.
- Provides real-time notifications—Uses SNMP traps, syslog notifications, and e-mail to report the status of the network being monitored to a higher-level entity (typically, to a manager of managers).

Server Requirements

Table 1-1 lists the minimum server system requirements for installing Operations Manager (with Service Monitor). These requirements are for installation only, not for deployment of both Operations Manager and Service Monitor. Depending on your deployment scenario, requirements may vary. For more information, see Coresident Guidelines, page 1-5 and VMware Guidelines, page 1-7.

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

Table 1-1 Installation Server System Minimum Requirements for Operations Manager (without Service Monitor)

Requirement Type	**Minimum Requirements for Deployment of up to...**		
	1,000 IP Devices and 10,000 Phones	**1,000 IP Devices and 30,000 Phones**	**2,000 IP Devices and 45,000 Phones**
Processor	One of the following: • Dual-core Intel Xeon processor equal to or greater than 2 GHz. • Dual-core AMD Opteron processor equal to or greater than 2 GHz.	One of the following: • Two dual-core Intel Xeon processorz equal to or greater than 2 GHz. • Two dual-core AMD Opteron processors equal to or greater than 2 GHz.	Two-way quad-core Xeon X5365 processors at 3 GHz. **Note** A 2-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)	4 GB.[1]	4 GB.[1]	8 GB RAM.
Page File Space[2]	8 GB.	8 GB.	16 GB.
Disk Space[3]	• 72 GB recommended. • NTFS file system (required for secure operation). • At least 16 MB in Windows temporary directory (%TEMP%).		
Hardware	• 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 1024 x 768 on a 17” monitor.) • 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).		

Table 1-1 Installation Server System Minimum Requirements for Operations Manager (without Service Monitor)

Requirement Type	Minimum Requirements for Deployment of up to...		
	1,000 IP Devices and 10,000 Phones	1,000 IP Devices and 30,000 Phones	2,000 IP Devices and 45,000 Phones
Software[4, 5]	• One of the following: – Windows Server 2003 with Service Pack (SP) 2, Standard and Enterprise Editions (32-bit version). – Windows Server 2003 Enterprise R2 Edition SP2 (32-bit version).		• One of the following: – Windows Server 2003 SP2 Enterprise Edition (32-bit version). – Windows Server 2003 SP2 Enterprise R2 Edition (32-bit version).
	Note The system that you use for your Operations Manager server should meet all the security guidelines that Microsoft recommends for Windows 2003 Server. See the Microsoft website for security guidance: http://www.microsoft.com/technet/security/prodtech/WindowsServer2003.mspx (This website is Copyright © 2009, Microsoft Corporation.)		
	Note For virtualization, Operations Manager supports ESX 3.5. For requirements, see VMware Guidelines, page 1-7. • ODBC Driver Manager[6] 3.5.10 or later. **Note** • 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 2-25. • 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 and Service Level View open, and so on). For more information, see Terminal Server Support for a Windows 2003 Server, page 1-8.		

1. For details on enabling the full 4 GB of RAM on Windows, see Enabling the Full 4 GB of RAM, page 2-5.
2. When configuring the page file, you should set both the minimum and maximum file size parameters to same size. This ensures that Windows creates a required-size page file.
3. Do not install Operations Manager on a FAT file system.
4. 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.
5. The default locale for your Windows operating system must be set to either US-English or Japanese.
6. 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 1-7.

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 a 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 Xeon X5365 processors at 3 GHz. **Note** 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]	• 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	• 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 1024 x 768 on a 17" monitor.) • 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]	One of these: • Windows Server 2003 Enterprise Edition SP2 (32-version) • Windows Server 2003 R2 Enterprise Edition SP2 (32-version)
	Note The system that you use for your Operations Manager server should meet all the security guidelines that Microsoft recommends for Windows 2003 Server. See the Microsoft website for security guidance: http://www.microsoft.com/technet/security/prodtech/WindowsServer2003.mspx (This website is Copyright © 2009, Microsoft Corporation.)
	• ODBC Driver Manager[5] 3.5.10 or later. **Note** • 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 2-25. • 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 and Service Level View open, and so on). For more information, see Terminal Server Support for a Windows 2003 Server, page 1-8.

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 default locale for your Windows operating system must be set to either US-English or Japanese.
5. 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.

- Install each application along with its databases on a separate drive. You can install one of the applications on the system drive (C:), but, if you have a sufficient number of drives, we recommend that none of the applications be installed on the system drive.
- Install applications in this order (recommended, not required):
  1. Operations Manager (includes Service Monitor)
  2. Service Statistics Manager
  3. 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. Operations Manager must have the same system resources available to it inside the virtualization environment that it has for a standard (nonvirtual) installation. When 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 CUCMS Virtualization* under this URL:

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

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

- Three instances of Operations Manager, each supporting up to 5,000 phones and 1,000 IP devices
- Each of these products installed on a separate virtual machine:
  - Operations Manager
  - Service Monitor
  - Service Statistics Manager
  - Provisioning Manager

  with each supporting up to 10,000 phones and 1,000 IP devices. (Running one instance of an application in one virtual machine is the only supported configuration.)
- One instance of Operations Manager supporting up to 30,000 phones and 2,000 IP devices

Note For other supported Service Monitor, Service Statistics Manager, and Provisioning Manager configurations in a virtualization environment, see *Best Practices for CUCMS Virtualization* under 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.

  Note 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.

When 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).

Note Choosing a complex address makes it less likely that you will choose an address being used by another customer. This can prevent accidental licensing overlap between different customers.

Step 7 Click **OK**.

Terminal Server Support for a Windows 2003 Server

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 Server.

Table 1-3 Terminal Services on a Windows 2003 Server

Windows 2003 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. **Note** Do not use terminal services to perform day-to-day tasks in Cisco Unified Management Communications Suite applications, such as viewing the Service Level View in Operations Manager or viewing reports in Service Monitor.

Enabling and Disabling Terminal Services on a Windows 2003 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 2003 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 2003 server:

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

The Local Security Policy window appears.

Step 2 Click **Local Polices > Security Options**.

Step 3 Select **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.

Step 4 Right-click the selected policy andselect **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	• Any PC or server platform with an Intel Pentium 4 or Xenon processor greater than 1.0 GHz. • Color monitor with video card set to 24 bits color depth. (For optimum viewing on the Operations Manager display, Cisco recommend 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 1024 x 768 on a 17" monitor.) • Screen resolution of 1024 x 768 dpi. **Note** Not every LCD projector or monitor provides a clear display at the minimum resolution. On LCD projectors and monitors, dot pitch impacts the readability of the screen.
System software	• One of the following: – Windows Server 2003 Standard or Enterprise Edition without Windows Terminal Services. – Windows Server 2003 R2. • Internet Explorer 6.0.28, 6.0.37, or 7.0[1,2]. • Adobe Flash Player 8.0 or 9.0. 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)	1 GB recommended.
Page file space	2 GB.
Environment	Clients must be able to access Operations Manager: • 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] 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**, click the **Security** tab, and click the button.

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 2.2. For information on preparing to install or upgrade, 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.

Note When using Operations Manager on a system with virus protection software, it is recommended that you enable virus protection only after the installation or upgrade is complete. 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

	Deployment up to...		
System Parameters	**1,000 IP Devices and 10,000 Phones**	**1,000 IP Devices and 30,000 Phones**	**2,000 IP Devices and 45,000 Phones**
IP phones	Up to 10,000	Up to 30,000	Up to 45,000
Access ports[1, 2]	15,000	45,000	60,000
Trunk ports and interfaces[2]	4,500	4,500	7,500
Cisco Unified Communications Manager clusters	6	6	Up to 20
Unified Communications Managers	4-8 per cluster (total 30)	4-8 per cluster (total 30)	Up to 150
Cisco Unified Communications Manager Express and Cisco Unity Express	300	300	600
Route lists and route groups	1,000	1,000	2,200
Phone status tests	500	500	1,000
Synthetic tests	100 (50 end-to-end and 50 dial-tone tests)	100	250
Node-to-node tests	100	100	500
SRST monitoring	250	250	1,000
Sustained event rate per minute[3, 6]	25	50	50
High event rate per minute[4, 6]	100	200	200
Burst events[5, 6]	1,000	1,500	1,500
Concurrent client (browser) logins	5	5	5

[1] By default, Operations Manager does not manage access ports; however, it discovers the phones connected to these ports.

[2] 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.

[3] Sustained events are event rates handled by the system on a continuous basis.

[4] High events are event rates handled by the system during high activity periods that last for a short duration (up to one hour).

[5] Burst events are event rates handled by the system for a one-time high activity period.

[6] This is a process event count that includes poll events, traps, syslogs, and service quality traps.

Tip

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.

Bandwidth Estimation

As you plan your deployment, you can obtain an estimate of the bandwidth that Operations Manager requires to manage Cisco Unified Communications network elements. For more information, see the Cisco Unified Operations Manager - Bandwidth Estimator tool available on this Tool Index page: www.cisco.com/en/US/products/prod_tools_index.html.

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.

As additional device adapter packages become available, you can download the IDUs that contain them, by logging into Cisco.com.

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 3-20.

Caution

Be sure to read the important sections on steps to take before installing or upgrading Operations Manager to release 2.2. For prerequisite installation steps, see Preparing the Operations Manager Server, page 2-2. For prerequisite upgrade steps, see Backing Up Data Before the Upgrade or Reinstallation, page 2-14 and Before You Start the Upgrade, page 2-17.

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. 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 2.2. See Licensing Process, page B-3.

This chapter includes the following:

Preparing to Install Operations Manager

The information in this section helps you to deploy Cisco Unified Operations Manager (Operations Manager) in your network. Do the following before you install 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 2-5.)
- 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 2-6.

- Gather information that you might need to provide during the Operations Manager installation. (See Gathering Information to Provide During Installation, page 2-8.)

Preparing the Operations Manager Server

Before installing or upgrading Operations Manager, do the following:

- Before upgrading or reinstalling Operations Manager, you must back up Operations Manager. See Backing Up Data Before the Upgrade or Reinstallation, page 2-14. (The 2.2 upgrade and reinstallation procedures do not perform a backup due to time limitations.)
- 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.
- Set your system's IP address and hostname. (It's not simple to change them after you complete the installation.)
- 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.

- Verify that the drive that you choose to install Operations Manager on is an NTFS file system.

  Note To install Operations Manager on VMware, ensure that you install it on a VMFS 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.
- Operations Manager uses ICMP ping to determine the reachability of all devices. Some security applications may detect a 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.
- Clean the temp directory. You can open the temp directory by typing `%temp%` in a Windows Explorer window.
- 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 2-5.

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

- Verify that the Primary and Active regional settings are set to either US English or Japanese. Other options are not supported by Operations Manager.

  You can set the Active regional settings in **Control Panel > Regional and Language Options > Regional Options**.

- You can install Operations Manager on a system with Terminal Services enabled in Remote Administration mode. However, installation of Operations Manager on a system with Terminal Services enabled in Application mode is not supported.

  If you have enabled Terminal Server in Application mode, disable the Terminal Server, reboot the system, and start the installation again. See Terminal Server Support for a Windows 2003 Server.

- If Internet Information Services (IIS) is detected on your system and if you have continued the installation with IIS services, you cannot use port number 443 for HTTPS. Instead, you must use port numbers ranging from 1026 to 65535 for HTTPS to avoid this conflict.

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

- We recommend that you disable the virus scan software on your system. You can restart it after all installations are completed.

- If you have the Cisco Security Agent installed on your system and it is running, shut it down. If you do not do so, you may receive a confirmation message during installation, requesting permission to continue. Click **Yes** and proceed. To disable the Cisco Security Agent, right-click the Cisco Security Agent icon and select **Security Level > Off**.

- Operations Manager is installed in the default directory: *SystemDrive*:\Program Files\CSCOpx

  Where *SystemDrive* is the drive on which the Windows operating system is installed.

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

  The destination folder should not contain any of the following special characters:

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

- After you click the **Install** button, you can click **Cancel** at any time to end the installation, reinstallation, or upgrade. However, any changes to your system will not be undone.

  For example, if any new files were installed or if any changes were made to the system files, you need to manually clean up the installation directories.

Note We recommend that you do not terminate the installation while it is running.

- If Provisioning Manager is already installed on the server, prevent conflicts that can cause the Operations Manager installation to fail; see Preparing a Server Where Provisioning Manager Has Already Been Installed, page 2-4.

Preparing a Server Where Provisioning Manager Has Already Been Installed

To install Operations Manager and Provisioning Manager on the same server, we recommend that you install Operations Manager first. However, if Provisioning Manager is already installed and running in Secure mode, to install Operations Manager you must prevent SSL-related conflicts. Ensure that:

- Win32 OpenSSL v0.9.8j Light library files are installed correctly.
- Operations Manager will not use port 443. (Provisioning Manager uses port 443 for SSL.)

Ensuring that There Is No Conflict over OpenSSL Library Files

Step 1 In the Windows system directory—which might be C:\WINDOWS and is defined by the %WINDIR% system environment variable—look for these library files:

- ssleay32.dll
- libeay32.dll

If you find them, complete the steps remaining in this procedure.

Step 2 Uninstall Win32 OpenSSL v0.9.8j Light. (You can use Add or Remove Programs from the Control Panel; you can find the program by looking for OpenSSL.)

To install Win32 OpenSSL v0.9.8j Light using the instructions provided in Step 3, download it from this URL: http://www.slproweb.com/products/Win32OpenSSL.html.

Step 3 Install Win32 OpenSSL v0.9.8j Light:

Note If you receive an error message stating that Visual C++ 2008 Redistributables are missing, you must download and install the Visual C++ 2008 Redistributables before proceeding. It is available from this URL: (http://www.slproweb.com/products/Win32OpenSSL.html).

a. During the installation, the “Copy OpenSSL DLLs to” prompt appears and provides two options:

- The Windows System Directory
- The OpenSSL binaries(/bin) directory

Select The OpenSSL binaries(/bin) directory.

b. After the installation, copy the ssleay32.dll and libeay32.dll files:

- From the C:\OpenSSL\bin folder
- To the C:\CUPM\httpd\bin folder

where C:\CUPM is the location where Provisioning Manager is installed and C:\OpenSSL is the location where OpenSSL is installed.

Note Installing Win32 OpenSSL v0.9.8j Light is only the first step to enable SSL on Provisioning Manager.

Step 4 Finish enabling SSL on Provisioning Manager by generating the security certificate and ensuring that the Apache server is correctly configured. For more information, see *Installation Guide for Cisco Unified Provisioning Manager.*

Preventing Conflict over Port 443

When you install Operations Manager, select Custom Installation instead of a Typical Installation. During the custom installation, enter an HTTPS port other than 443.

Enabling the Full 4 GB of RAM

Note If your operating system is Windows 2003 Server Enterprise Edition, /PAE is enabled by default and, therefore, you should not need to perform this procedure.

On a 4-GB system, Microsoft Windows detects only 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 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.

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 2-5.)
- Make sure all processes are running on the Operations Manager system. (See Actions to Take Before Adding Devices, page 2-6.)

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 Communications 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 Communications 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 that Operations Manager (and Service Monitor) uses are free. For the ports that Operations Manager uses, see Table 2-1; for Service Monitor, see Table 2-2.

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[1]
162	Trap receiving (standard port)	Common Services

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

Port Numbers	Service Name	Application
514	Syslog	Common Services
1024-4999	Ephemeral ports	Operations Manager
40000-41000	Used by Common Transport Mechanism for internal application messaging	Operations Manager
42344	Used by Synthetic Testing web service	Operations Manager
42350-42353	Used by messaging software	Operations Manager
43445	Used by Alert History database engine	Operations Manager
43446	Used by inventory service database engine	Operations Manager
43447	Used by event processing database engine	Operations Manager
43449	Used by IP Phone Information Facility database engine	Operations Manager
8080	Used to determine whether 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

[1] For a list of all ports that Common Services uses, see *Installing and Getting Started With CiscoWorks LAN Management Solution 3.2*.

Table 2-2 Ports that Service Monitor Uses

Port Numbers	Service Name
22	SFTP—Service Monitor uses SFTP to obtain data from Unified Communications Manager 5.x and later.
53	DNS.
67 and 68	DHCP.
2000	SCCP—Service Monitor uses SCCP to communicate with Cisco 1040s.
43459	QOVRdatabase.
5666	Syslog—Service Monitor receives syslog messages from Cisco 1040s.
5665-5680	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 information on creating passwords, see Password Information, page A-7.

- User Admin password
- System Identity Account password
- Casuser password (custom installation only)
- Guest password (custom installation only)
- Common Services database password (custom installation only)
- Mail Settings (custom installation and when configuring an HTTPS port other than 443)

  Note If IIS runs on your server, a dialog box will present you with the choice of whether to configure an HTTPS port other than 443 during the installation to avoid port conflict. If you select OK, you will need to enter mail settings.

- 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 B-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 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 2.2. 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 B-1
  - Licensing Reminders, page B-5

Performing a New Installation

The installation process takes approximately 60 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.
- 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 that does not have name lookup.
  - An encrypted directory. Operations Manager does not support directory encryption.
  - A voice application server or Cisco Unified Communications Manager server.
- Do not install any CiscoWorks Common Services 3.2 service packs on Operations Manager.
- Verify that the system date and time are set properly.
- To speed up installation, disable all virus-scan software while installing.
- 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 2-25.
- 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 Read any messages and acknowledge them:

- If Provisioning Manager is running in Secure mode on the system—Messages are displayed telling you to resolve conflicts and to use a port other than 443 for HTTPS. You will not be able to continue the installation; exit the installation and perform tasks in Preparing a Server Where Provisioning Manager Has Already Been Installed, page 2-4.
- If WMI Services are running on the system—A message is displayed stating that, for the installation to proceed, the script will stop WMI Services, complete the installation, and restart WMI Services. To continue, click **OK**.
- If IIS is detected (even if it is disabled)—A message is displayed. To avoid a port conflict with IIS, click **Yes.** In a later step, you will be prompted to select an HTTPS port other than 443.

The Welcome window appears.

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

Step 5 Select the I accept the terms of the license agreement radio button and click **Next**. The Licensing Information window appears.

Step 6 Select one of the following, and then click **Next**:

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

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

The Setup Type window appears.

Step 7 Select **Typical** if you want the system to automatically provide the following information to the installation process:

- Guest password
- Common Services database password
- Mail Settings (also appears if you need to configure an HTTPs port other than 443)
- Self-signed certificate information

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

Step 8 Click **Next**. The Choose Destination Folder window appears.

Step 9 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.

If you are installing on a virtual machine with a dynamic MAC address, another warning message will be displayed. Click **Yes**. (After the installation completes, you can run Operations Manager in Evaluation mode without problems. To license and run Operations Manager, you must configure a static MAC address. For more information, see VMware Guidelines, page 1-7.)

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 10 Click **Next**. You will need to provide input as follows:

a. The Enter Admin Password window appears. Enter a password (and confirm), and click **Next**.

Note Remember the password. You will need it to log in to Operations Manager until you have configured security and created users in addition to admin.

The Enter System Identity Account Password window appears.

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 7.

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

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

d. If IIS is present on your server and you selected **Yes** (to avoid port conflict by reconfiguring the HTTPS port), the Mail Settings window appears. The range of ports that you can use for HTTPS is displayed. After entering data, click **Next**.

e. The Change casuser Password window appears. Do one of the following:

- Click **Next** to automatically generate the password.
- Enter a password and confirm it before clicking **Next**.

The Summary window appears, displaying the current settings.

Step 11 Click **Install**. The installation proceeds.

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

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 2-25.

Step 13 Eject the CD.

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

Step 14 A window appears with the “Yes, I want to restart my computer now” radio button selected. Click **Finish** to reboot the machine.

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

Step 16 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.
- You should exclude the NMSROOT/databases directory from virus scanning. Problems can arise if database files are locked because of virus scanning.

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 2.2

This section covers the following topics:

- Upgrade Paths, page 2-12
- Upgrading from Operations Manager Releases Prior to 2.0.3 to Operations Manager 2.2, page 2-13
- Third-Party Tools and Software Changes, page 2-14
- Backing Up Data Before the Upgrade or Reinstallation, page 2-14
- Before You Start the Upgrade, page 2-17
- (Optional) Planning for (and Running) Service Monitor Call Data Migration Before the Upgrade, page 2-18
- Upgrading to Operations Manager 2.2, page 2-18
- Restoring Detailed Device View Configuration Data to Operations Manager 2.2, page 2-21
- Configuring Service Monitor After Upgrading, page 2-21

Upgrade Paths

Operations Manager supports the upgrade paths listed in Table 2-3.

Table 2-3 Upgrade Paths to Operations Manager 2.2

From this License	To this License	Upgrade to Operations Manager 2.2 Is Supported from These Operations Manager Releases
Purchased	Purchased	2.1 SP1 (2.1.1) 2.1 2.0.3
Purchased	Evaluation	
Evaluation	Evaluation	None

Caution There is no direct upgrade from releases prior to 2.0.3. See Upgrading from Operations Manager Releases Prior to 2.0.3 to Operations Manager 2.2, page 2-13 for details on how to proceed.

Note When you upgrade to Operations Manager 2.2:

- Service Monitor upgrades to release 2.2.
- Common Services upgrades to release 3.2. (For more information, see Third-Party Tools and Software Changes, page 2-14.)

You can purchase two levels of functionality for Operations Manager 2.2: Premium Edition and Standard Edition. To get full Operations Manager functionality, you must upgrade to Operations Manager Premium Edition.

Full backup is not run as part of an upgrade or reinstall, to allow for a short upgrade or reinstallation time. For instructions on how to run your backups, see Backing Up Data Before the Upgrade or Reinstallation, page 2-14 before performing your upgrade or reinstallation.

Upgrading from Operations Manager Releases Prior to 2.0.3 to Operations Manager 2.2

You cannot upgrade directly from Operations Manager releases prior to 2.0.3 to Operations Manager 2.2. If you are running:

- Operations Manager 2.0.2—First upgrade to Operations Manager 2.0.3. To download Operations Manager 2.0.3, go to http://www.cisco.com/cgi-bin/tablebuild.pl/cuom203.
- Operations Manager 2.0 or 2.0.1—First upgrade to Operations Manager 2.1. To download Operations Manager 2.1, go to http://www.cisco.com/cgi-bin/tablebuild.pl/cuom21.
- Operations Manager 1.x—To ensure safe migration of your Operations Manager 1.x data, you must perform these upgrades before you can upgrade to Operations Manager 2.2:
  1. Upgrade from 1.x to 2.0.x. To download Cisco Unified Operations Manager 2.0.x, go to one of these:

     http://www.cisco.com/pcgi-bin/tablebuild.pl/cuom201

     http://www.cisco.com/pcgi-bin/tablebuild.pl/cuom202
  2. Perform the appropriate upgrade:

     From Operations Manager 2.0.1, upgrade to Operations Manager 2.1.

     From Operations Manager, 2.0.2, upgrade to 2.0.3.

For upgrade instructions, see the appropriate installation guide at http://www.cisco.com/en/US/products/ps6535/prod_installation_guides_list.html.

Third-Party Tools and Software Changes

When you upgrade to Operations Manager 2.2, you also upgrade to Common Services 3.2. The following Third-Party components are removed and replaced with open-source components in Common Services 3.2:

- Visigenics, which was used for CORBA communication, is replaced with JACORB.
- Tibco, which was used for event services, is replaced with ActiveMQ.

The following component upgrade is performed in Common Services 3.2:

- Sybase ASA is upgraded to version 10.0.1 from 9.x.
- Java Runtime Environment (JRE) is upgraded to JRE 1.5.0_1; Java Plug-in 1.6.0_05 is provided.

Backing Up Data Before the Upgrade or Reinstallation

To ensure that you have a backup if corruption occurs, you should back up configuration and data files on the Operations Manager server. The following sections cover various backup scenarios for Operations Manager. Depending on your configuration, you might need to perform each of the following:

- Backing Up and Restoring Detailed Device View Configurations Using Operations Manager Utilities, page 2-15
- Backing Up and Restoring Using CiscoWorks, page 2-15
- Backing Up the Service Monitor Database Manually, page 2-16

Because Operations Manager supports the Device Credentials Repository (DCR), you should be aware of the information in these topics in *User Guide for CiscoWorks Common Services 3.2*:

- Effects of Backup-Restore on DCR at http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_common_services_software/3.2/user/guide/admin.html#wp388174
- Master-Slave Configuration Prerequisites and Restore Operations http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_common_services_software/3.2/user/guide/admin.html#wp381835)

During the upgrade to Operations Manager 2.2, the following happens on each component:

- Operations Manager—Detailed Device View configuration is backed up.
- Common Services—All data (such as server settings, usernames, and passwords) is migrated.
- Service Monitor—If you are running Service Monitor on the server, configuration data (such as credentials and threshold settings) is migrated during the upgrade, but report data is not. To migrate report data, you must run the Call Migration Tool before you run the upgrade. See (Optional) Planning for (and Running) Service Monitor Call Data Migration Before the Upgrade, page 2-18.
- Operations Manager, Common Services, and Service Monitor databases—All are upgraded to Sybase 10.

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 or reinstallation procedure. If you have not completed a backup, you should exit the installation to perform your backup.

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

During an upgrade to Operations Manager 2.2 and during a reinstallation, the Detailed Device View (DDV) backup runs automatically. The DDV backup utility backs up the states of all components of all types of monitored or partially monitored devices (except for those mentioned in the note 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 2.2.

Note Operations Manager does not restore DDV configurations on voice services, system processor, hard disk, virtual memory, or RAM components for Cisco Unified Communications Manager systems. Operations Manager uses Real-Time Monitoring Tool (RTMT) polling, not device MIB polling, to create these components and therefore does not display this data in the Operations Manager DDV in release 2.2.

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 to the inventoryBackup file. No user input is needed while the script is running.

If you prefer to enter a specific filename or a list of specific device IP addresses, enter:

```
% PROGRA~1\CSCOpx\objects\vhm\utilities\inventoryBackup
```

The script prompts you to enter the filename and device information.

Caution After an Operations Manager 2.2 upgrade, you can run the **inventoryRestore** script only after rediscovering all devices from the 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 filename enter:

```
% PROGRA~1\CSCOpx\objects\vhm\utilities\inventoryRestore
```

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

Backing Up and Restoring Using CiscoWorks

This procedure backs up the databases for Common Services and Operations Manager. It does not back up:

- The database for Service Monitor—You must back up the Service Monitor database manually;see Backing Up the Service Monitor Database Manually, page 2-16.

- The state of components in the Detailed Device View (DDV)—You must back them up using Backing Up and Restoring Detailed Device View Configurations Using Operations Manager Utilities, page 2-15.

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 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: • 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. (The Service Monitor suite is qovr.)
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).

Backing Up the Service Monitor Database Manually

You must backthe Service Monitor database up manually to nonlocal storage. (The Service Monitor database can potentially grow to greater than 10 GB.)

Step 1 Log in to the system where Service Monitor is installed.

Step 2 Stop the daemon manager using this command:

```
net stop crmdmgtd
```

Step 3 From *NMSROOT*\databases\qovr, copy the files qovr.db and qovrx.log to a tape, an external drive, or a network directory (not a local directory). Doing so ensures data integrity in case of hardware failure and ensures that backup data does not exhaust local disk space.

Step 4 Restart the daemon manager using the following command:

```
net start crmdmgtd
```

Before You Start the Upgrade

Note If you have configured Operations Manager in a master-slave server setup, upgrade the master server before upgrading the slave server.

- 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).
- 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 1.2*.
- If you use Service Monitor, you should be aware of the following:
  - To save existing report data, you should run the Call Migration Tool before you start the upgrade. See (Optional) Planning for (and Running) Service Monitor Call Data Migration Before the Upgrade, page 2-18.
  - It is recommended that you delete existing sensor configuration files—one QOVDefault.CNF file and a QoV*MACAddress*.CNF file for each sensor—from your existing TFTP servers before you perform the upgrade. Immediately after you upgrade to the Service Monitor 2.2 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 2-21.
- To use Service Monitor to monitor MOS reported from Cisco Unified Communications Managers, you should configure the server to use NTP before you upgrade. For more information, see NTP Configuration Notes, page 2-25.
- Close all open or active programs. Do not run other programs during the upgrade process.
- 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 there is an inventorybackup.xml file in CSCOpx\objects\vhm\utilities directory before Operations Manager 2.2 upgrade, rename the inventorybackup.xml file before you perform the upgrade.

- To improve response times for the Fault History database, run disk defragmentation on the Operations Manager server machine before you install the 2.2 software. The upgrade now allocates 2 GB of disk space to the database and defragmenting the disk before the upgrade ensures faster response times.

(Optional) Planning for (and Running) Service Monitor Call Data Migration Before the Upgrade

Migrating call data is optional. However, to keep the data, you must migrate it before you start the upgrade to Operations Manager (includes Service Monitor) 2.2.

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

Step 1 Download the tool (QOVR_CMT.zip) and the readme file from this URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/servmon

Note You will need to log in to Cisco.com.

Step 2 Extract the README_QOVR_CMT.TXT file and use the information in it to plan for and execute the migration.

Note Running the Call Migration Tool migrates only the Service Monitor call data. Service Monitor configuration data migrates automatically during the upgrade to Operations Manager (includes Service Monitor 2.2). After you run the Call Migration Tool, do not run Service Monitor until you complete the upgrade to Operations Manager.

Upgrading to Operations Manager 2.2

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

Note Sometimes the upgrade seems to stall. This happens when files are locked by some processes. You can do either of the following:

- Re-try and wait for processes to release locked files.
- Stop the upgrade and:
  a. Use file explorer to find the processes that are holding file handles under CSCOpx (NMSROOT).
  b. Kill those processes manually and restart the upgrade.

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

a. Ensure that you have completed a backup. (See Backing Up Data Before the Upgrade or Reinstallation, page 2-14.)

b. If there is an inventorybackup.xml file in CSCOpx\objects\vhm\utilities directory before Operations Manager 2.2 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 Read any messages and acknowledge them to continue:

- If WMI Services are running on the system—A message is displayed stating that, for the installation to proceed, the script will stop WMI Services, complete the installation, and restart WMI Services. To continue, click **OK**.
- If IIS is detected (even if it is disabled)—A message is displayed. To avoid port conflict with IIS, click **Yes** and, in a later step, you will be prompted to select an HTTPS port other than 443.
- Acknowledge the message that a database backup will not be performed by clicking **OK**. (If you have not performed a backup, exit the upgrade now and perform a backup.)

  The Welcome window appears.

Step 4 Click **Next**. An upgrade warning appears.

Step 5 To save any Service Monitor report data that you have—and, if you have not run the Call Migration Tool— click **No**, exit, and run the Call Migration Tool to completion before you run the upgrade. Otherwise, click **Yes**.

The Software License Agreement window appears.

Step 6 Select the I accept the terms of the license agreement radio button and click **Next**. The Setup Type window appears.

Step 7 Select **Typical** or **Custom**. (The changes you can make during a Custom installation are listed under Step 9.) Click **Next**.

Step 8 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 9 If you chose Custom installation, windows appear that enable you to do any of the following:

- 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. Click **Next**.

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

Step 11 Click **OK** to confirm additional messages if they are displayed:

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.

- Before database upgrade, the following message is displayed:

```
Rebuilding the database. Please wait. At most, for a 25GB database, it can take up to
an hour.
```

- The following message might appear:

```
Before you reboot this system, configure automatic time synchronization on it using
NTP. Configure this system to use the time server that is used by Cisco Unified
Communications Managers in your network.
```

(For more information, see NTP Configuration Notes, page 2-25.)

- This message is displayed:

```
To make sure all existing devices go to the monitored state, you must configure
Operations Manager to perform rediscovery after restart.
```

- 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.

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 Operations Manager 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:

a. In Operations Manager, select **Device > Device Management > Modify/Delete Devices**.

b. In the device selector, select the **All Devices** check box.

c. Click **Rediscover**.

Step 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 2.2, page 2-21. Be sure that discovery is complete before performing this step.

If any errors occur during installation, check the installation log in the root directory on the drive. (For example, the CiscoWorks Common Services installation might create C:\Ciscoworks_setup001.log, the Operations Manager installation might create C:\Ciscoworks_setup002.log, and so forth.) The Cisco Technical Assistance Center (TAC) might ask you to send them the installation log if you encounter problems.

Restoring Detailed Device View Configuration Data to Operations Manager 2.2

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 Cisco 1040 sensors to register with Service Monitor 2.2. For complete configuration procedures, including how to add Unified Communications Managers and Network Analysis Modules (NAMs) 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:

a. Select **Configuration > Sensor > Setup**. The Setup page appears.

b. Update the Default Configuration to TFTP Server fields:

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

Note To ensure that you use the most up-to-date image file, see *Cisco Unified Service Monitor 2.2 Compatibility Matrix*.

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, SvcMonAB2_102.img, from *NMSROOT*\ImageDir on the Service Monitor server to the root location on the TFTP server. (*NMSROOT* is the directory where Service Monitor is installed; its default location is C:\Program Files\CSCOpx.)

e. Verify that the newly created QOVDefault.CNF file is on the TFTP server. If it is not, upload it to the root location on the TFTP server from the Service Monitor image file directory, *NMSROOT*\ImageDir. For examples of the configuration files, see "Sample 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.***

Reinstalling Operations Manager

Step 1 As the local administrator, log in to the machine on which you will install the Cisco Unified Operations Manager software.

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

Step 3 From the command line, stop the OMHealthMonitor service by entering the following command:

```
net stop OMHealthMonitor
```

Step 4 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 5 Read any messages and acknowledge them to continue:

- If WMI Services are running on the system—A message is displayed stating that, for the installation to proceed, the script will stop WMI Services, complete the installation, and restart WMI Services. To continue, click **OK**.
- Acknowledge the message that a database backup will not be performed by clicking **OK**. (If you have not performed a backup, exit the reinstallation now and perform a backup.)

  The Welcome window appears.

Step 6 Click **Next**. The Software License Agreement window appears.

Step 7 Select the I accept the terms of the license agreement radio button and click **Next**. The Setup Type window appears.

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

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

Step 10 If you chose Custom installation you will be asked to enter:

- Passwords—For admin, guest, system identity account, casuser, database. (In most cases, you can click **Next** to keep the existing password; the casuser password is generated for you if you click **Next**.)
- Security certificate information
- Data transport protocol

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

Step 11 An information dialog box appears, confirming reinstallation; click **OK**.

The Summary window appears, displaying the current settings.

Step 12 Click **Next**. The installation proceeds.

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

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

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

Step 15 After the reinstallation completes, verify that Operations Manager was reinstalled correctly by starting the application. From the Windows desktop select **Start > All Programs > Cisco Unified Operations Manager > Cisco Unified 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:

a. In Operations Manager, select **Device > Device Management > Modify/Delete Devices**.

b. In the device selector, select the **All Devices** check box.

c. Click **Rediscover**.

Step 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 2.2, page 2-21. Be sure you have rediscovered your devices before completing this step.

If any errors occurred during reinstallation, check the installation log in the root directory on the drive. (For example, the CiscoWorks Common Services installation might create C:\Ciscoworks_setup001.log, the Operations Manager installation might create C:\Ciscoworks_setup002.log, and so forth.) The Cisco Technical Assistance Center (TAC) might ask you to send them the installation log.

Uninstalling Operations Manager

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

Before you uninstall Operations Manager, ensure that:

- Remote desktop sessions are not connected to Operations Manager. Remote sessions can lock files; If Operations Manager processes are running, Operations Manager installation will stop.
- You have deleted 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 the respective configuration page for each test; (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 Select **Start > All Programs > Cisco Unified Operations Manager > Uninstall Cisco Unified Operations Manager**.

Step 3 If Windows Management Instrumentation (WMI) is running on the system, this message is displayed:

```
Windows Management Instrumentation (WMI) is running. This locks processes and impedes
installation. To avoid WMI conflicts, this program will stop and immediately restart the
WMI service.stating that WMI impedes the uninstallation and to prevent conflict, the
script will stop WMI services and restart them.
```

You must click **OK**. (To cancel the uninstallation, you can click **Cancel** on the next window that appears.)

Step 4 An Uninstallation window appears, listing the components to uninstall. To continue, click **Next**; otherwise click **Cancel**.

Messages showing the progress of the uninstallation appear.

The following message appears:

```
Uninstallation is complete. Before you install CW200 product, you must restart your
computer and delete any residual files from C:\PROGRA~1\CSCOPX manually.
```

The Yes, I want to restart my computer now radio button is selected. Alternatively, you can select the No, I will restart my computer later radio button.

Note You must restart your computer to finalize the uninstallation.

Step 5 Click **Finish**.

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.

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 © 2009, Microsoft Corporation.

CHAPTER 3

Getting Started

This section provides a minimum number of steps for setting up Cisco Unified Operations Manager (Operations Manager) and viewing diagnostic results. It includes:

Configuring Operations Manager to Monitor Devices

Operations Manager obtains devices to monitor from the CiscoWorks Common Services Device and Credentials Repository (DCR). The DCR is a common repository of devices and their credentials for use by individual applications.

For Operations Manager to monitor a device, it must first be added to the DCR. Once a device is added to the DCR, you can then add it to the Operations Manager inventory, which is separate from the DCR.

Note When Operations Manager is installed, it will automatically synchronize with the DCR and add inventory. This is the default setting.

You can add devices automatically from the DCR to Operations Manager by activating automatic synchronization (the default), or you can add them manually through the Device Selection page. For more information on how Operations Manager is affected by the DCR, see Understanding the DCR, page 3-3.

Note You should exclude the NMSROOT/databases directory from virus scanning. Problems can arise if database files are locked because of virus scanning.

Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it is C:\PROGRA~1\CSCOpx.

Table 3-1 lists some possible deployment scenarios for Operations Manager, and what you will need to do to add devices to Operations Manager inventory.

Table 3-1 Adding Devices to Inventory Scenarios

Deployment Scenario	What to Do
• Deploying Operations Manager as an independent server. • Automatically synchronizing your inventory with the DCR.	Add devices from the DCR using automatic synchronization. Automatic synchronization is the default setting, and you do not need to do anything. If you have changed the synchronization setting from automatic, you will need to change it back. See Configuring Automatic Device Selection in Operations Manager, page 3-10.
• Deploying Operations Manager as an independent server. • Manually controlling the devices that are added to inventory.	Manually add devices from the DCR. See Adding Devices Manually from the DCR to Operations Manager, page 3-10.
• Deploying Operations Manager as an independent server. • You want to use automatic discovery, but not all the devices discovered through automatic discovery need to be managed in Operations Manager.	• Add devices from the DCR using automatic synchronization. • Configure automatic synchronization to select devices based on parameters you set. See Configuring Automatic Device Selection in Operations Manager, page 3-10.
• Deploying Operations Manager with CiscoWorks LAN Management Solution (LMS). • Using the Operations Manager DCR as the master DCR. • Automatically synchronizing your inventory with the DCR.	• Set up the Operations Manager DCR as a master and the LMS DCRs as slaves. Configuring the DCR in Master and Slave Mode, page 3-4. • Run physical discovery. See Adding Devices to the DCR, page 3-5 • Verify that automatic synchronization is configured in Operations Manager. See Configuring Automatic Device Selection in Operations Manager, page 3-10.

Table 3-1 Adding Devices to Inventory Scenarios (continued)

Deployment Scenario	What to Do
• Deploying Operations Manager with LMS. • Synchronizing the Operations Manager DCR with an existing master DCR. • Automatically synchronizing your inventory with the DCR.	• Set up the Operations Manager server DCR as a slave and one of the LMS DCRs as a master. Configuring the DCR in Master and Slave Mode, page 3-4. • Configure Operations Manager to add devices to a master DCR. See Adding Devices to the DCR, page 3-5. • Run physical discovery. See Adding Devices to the DCR, page 3-5 • Verify that automatic synchronization is configured in Operations Manager. See Configuring Automatic Device Selection in Operations Manager, page 3-10.
• Deploying Operations Manager with LMS. • Synchronizing the Operations Manager with an existing master DCR. • Manually controlling the devices managed by Operations Manager.	• Set up the Operations Manager server DCR and the LMS server DCRs as slave and master. Configuring the DCR in Master and Slave Mode, page 3-4. • Configure Operations Manager to add devices to a master DCR. See Adding Devices to the DCR, page 3-5. • Run physical discovery. See Adding Devices to the DCR, page 3-5 • Verify that manual synchronization is configured in Operations Manager. See Configuring Automatic Device Selection in Operations Manager, page 3-10.

Understanding the DCR

The Device and Credentials Repository (DCR) is a centralized device repository for sharing device information across applications. It provides a single place for managing device credentials and attributes, ensuring consistency across applications. Individual applications can query the DCR for a device list, device attributes, and device credentials. Changes to the DCR are propagated to applications that support the DCR, such as Operations Manager and LMS applications. (Service Monitor and Service Statistics Manager neither use nor support the DCR.)

Note A device must be added to the DCR before it can be added to the Operations Manager inventory (see Adding Devices to the DCR, page 3-5).

Once a device is added to the DCR, you can add it to the Operations Manager inventory (the Operations Manager inventory is separate from the DCR). When a device is added to the DCR, the DCR assigns a DCR ID to every managed component. The DCR maps components to devices using either the device name or the IP address. When the device is added to Operations Manager, Operations Manager maps the DCR ID to the device name during inventory collection.

Operations Manager also uses the DCR ID to verify whether the device or component already exists in the Operations Manager inventory. (Further information on how Operations Manager identifies devices—such as whether Operations Manager uses an IP address or DNS name as the device name—is provided in *User Guide For Cisco Unified Operations Manager* or the online help.)

You can add devices automatically from the DCR to Operations Manager by activating automatic synchronization (which is the default), or you can add them selectively by deactivating using the Device Selection page. When a device is deleted it may or may not be deleted from the DCR. Deletion is determined by how Operations Manager is configured with the DCR (for details on deleting devices, see *User Guide For Cisco Unified Operations Manager* or the online help).

The synchronization between the DCR and the Operations Manager inventory is controlled from the Device Selection page.

- For automatic synchronization (this is the default), see Configuring Automatic Device Selection in Operations Manager, page 3-10.
- For manual synchronization (in which you selectively add devices from the DCR to the Operations Manager inventory), see Adding Devices Manually from the DCR to Operations Manager, page 3-10.

Note Do not confuse the Operations Manager physical discovery process (which adds devices to the DCR) or the Operations Manager inventory collection process (which probes devices and updates components in Operations Manager inventory) with the DCR synchronization process. Operations Manager inventory collection is a process that affects only the Operations Manager inventory.

Configuring the DCR in Master and Slave Mode

By default, the DCR on the Operations Manager server is configured as a standalone or independent repository. If you decide to configure the DCR for Operations Manager as a master or a slave, the procedures for doing so are thoroughly documented in the CiscoWorks Common Services online help and in *User Guide for CiscoWorks Common Services*. (To access the CiscoWorks Common Services online help, from the Operations Manager home page, click the CiscoWorks link in the top right corner of the page. The CiscoWorks home page appears; click the Help button.)

Note Ensure that the versions of Operations Manager and Common Services are compatible before configuring the master and slave mode. See the *Supported and Interoperable Devices and Software Table for* Cisco Unified Operations Manager 2.1 for compatibility information.

You must perform prerequisite tasks and you must configure the master and the slave in the proper order. The following procedure can help you get started and locate the information you need in the online help.

Note To start Operations Manager, see Starting Operations Manager, page 3-19.

Step 1 From the Operations Manager home page, click the **CiscoWorks** link in the top right corner of the page. The CiscoWorks home page appears in another window.

Step 2 On the CiscoWorks home page, select **Common Services > Device and Credentials > Admin**. The Administration page appears.

Step 3 Select Mode Settings from the TOC in the left-hand pane. The Mode Settings window appears.

Step 4 Click the Help link in the top right corner of the page. Find the instructions for completing the master-slave configuration prerequisites. These include:

- Adding a peer server user on the system with the master DCR.
- Creating a System Identity User on the system with the slave DCR.
- Copying security certificates.

Follow the instructions in the online help to complete the prerequisites and to configure a master and a slave in the correct order.

Adding Devices to the DCR

Devices are added to the DCR through the Operations Manager Add Devices page (**Devices > Device Management > Add Devices**).

Note To add devices to the DCR using bulk import (importing from an NMS or from a file), see Importing Devices Into the DCR, page 3-9.

Step 1 Select **Devices > Device Management > Add Devices**. The Add Devices page appears.

Step 2 Enter the following:

- IP address or hostname. Multiple devices can be entered at the same time, using a comma-separated list.

  Note When adding multiple devices at the same time, all the devices must be the same type of device and use the same credentials.

- Enter SNMPv2c/SNMPv1 credentials.
- Enter SNMPv3 credentials.
- Enter HTTP credentials (only required for Cisco Unified Communications Manager).
- Windows credentials (only required for Windows-based MCS application servers).

Step 3 Click **OK**.

Configuring Operations Manager Physical Discovery

Step 1 Select **Devices > Device Management > Auto-Discovery Configuration**. The Auto-Discovery Configuration page appears.

Note You can also access the Discovery Configuration page from the Device Management: Summary page, by clicking the Configure button.

Note Discovery requires SNMP and/or SNMPv3 credentials. If the credentials are not configured, when you click **Discovery Configuration**, an empty Discovery Configuration page appears and you will only have the option of configuring credentials. Select the Credentials radio button, then click **Add**; the Configure Credentials page appears (see Configuring Credentials, page 3-7).

Step 2 If the Discovery radio button is not selected, select it.

Step 3 Do *one* of the following:

- Select the **Use Communications Manager or Cisco Discovery Protocol (CDP)** check box, and do one of the following:
  - Enter seed devices using a comma-separated list of IP addresses.

    Note When using a Cisco Unified Communications Manager as the seed device, the following types of devices are discovered:

    - Other Cisco Unified Communications Managers in the network
    - Cisco Unity
    - MGCP Voice Gateways
    - H.323 Voice Gateways
    - Gatekeepers
    - CTI applications configured with CTI ports on the discovered Cisco Unified Communications Managers

    In addition to the Cisco Unified Communications Manager-based discovery, the following types of discoveries occur, resulting in additional devices being added to the inventory:
    - CDP-based discovery
    - ARP-based discovery
    - Route table-based discovery

  - Select the **Use devices currently in the system** check box.
  - Select a hop count.

  Note Discovery may skip more than the number of hops selected. Discovery uses multiple technologies to discover devices, which may result in devices violating L2 or L3 hops. If you are using Hop count to limit discovery, an alternate way of achieving the same objective is to use the *Include* and *Exclude* filters from the Discovery Configuration page (see Filtering Operations Manager Physical Discovery, page 3-7).

  or

- Select the **Use ping sweep check box**. The seed devices and the ping sweep options can be used in an either/or mode.

  When selecting the Use Ping Sweep check box, specify a comma-separated list of IP address ranges using the */netmask* specification.

  For example, use 172.20.57.1/24 to specify a ping sweep range starting from 172.20.57.1 and ending at 172.20.57.255.

Step 4 In the Run pane, configure when physical discovery should run.

- If you want physical discovery to run immediately, select the **now** radio button.
- If you want to schedule physical discovery to run at certain intervals, do one of the following:
  - Select **daily**; enter the time and select the days on which physical discovery should run.
  - Select the **every** radio button; choose how often you want physical discovery to run, enter the times between which you want it to run, and select the day on which it should run.

Step 5 Click **OK**.

Configuring Credentials

Discovery requires SNMP and/or SNMPv3 credentials. If the credentials are not configured when you try to configure discovery, you will only be able to access the Configure Credentials page. You must enter SNMP and/or SNMPv3 credentials before running discovery.

Step 1 Select **Devices > Device Management > Auto-Discovery Configuration > Credentials**. The Configure Credentials page appears.

Step 2 Click **Add**.

Note If you are changing the existing credentials for a device, select the target device and then click **Edit**. Using this edit option only allows you to change the credentials. If you want to change the target device, you must delete the entire row and then re-add all the details.

Step 3 Enter the following:

- IP address or hostname. Multiple devices can be entered at the same time, using a comma-separated list.

  Note When adding multiple devices at the same time, all the devices must be the same type of device and use the same credentials. If you are using wildcard entries, only the following formats are supported: *.*.*.* or 10.76.93.[39-43].

- (Optional) Change the SNMP timeout and retries.
- SNMPv2c/SNMPv1 credentials.
- SNMPv3 credentials.
- HTTP credentials (only required for Cisco Unified Communications Manager).
- Windows credentials (only required for Windows-based MCS application servers).

Step 4 Click **OK**.

Filtering Operations Manager Physical Discovery

You can configure Operations Manager physical discovery to filter out devices. This is optional; it is not required to run physical discovery.

Step 1 Select **Devices > Device Management > Auto-Discovery Configuration > Filters and Schedule**. The Filters and Schedule page appears.

Step 2 Select the **Filters** radio button. Table 3-2 describes the optional filters that are available to you when running physical discovery.

Table 3-2 Physical Discovery Filters

Filter	Description
IP Address	(Optional) Enter comma-separated IP addresses or IP address ranges for devices that you want to: • Include—In the auto-discovery process. • Exclude—From the auto-discovery process. You can use wildcards when specifying the IP address range. An asterisk (*) denotes the octet range of 1-255. Also, the octet range can be constrained using the [xxx-yyy] notation. For example: • To include all devices in the 172.20.57/24 subnet in the auto-discovery process, enter an include filter of 172.20.57.*. • To exclude devices in the IP address range of 172.20.57.224 - 172.20.57.255 from the auto-discovery process, enter an exclude filter of 172.20.57.[224-255]. Both types of wildcards can be used in the same range specification; for example, 172.20.[55-57].*. If both include and exclude filters are specified, the exclude filter is applied first before the include filter. Once a filter is applied to an auto-discovered device, no other filter criterion will be applied to the device. If a device has multiple IP addresses, the device will be processed for auto-discovery as long as it has one IP address that satisfies the include filter.

Table 3-2 Physical Discovery Filters (continued)

Filter	Description
DNS Domain	(Optional) Enter comma-separated DNS domain names for devices that you want to: • Include—In auto-discovery processing. • Exclude—From auto-discovery processing. The DNS names can be specified using wildcards. An asterisk (*) matches any combination of mixed uppercase and lowercase alphanumeric characters, along with the hyphen (-) and underscore (_) characters, of an arbitrary length. A question mark (?) matches a single uppercase or lowercase alphanumeric character or a hyphen or an underscore character. For example: • **.cisco.com* matches any DNS name ending with *.cisco.com.* • **.?abc.com* matches any DNS name ending with *.aabc.com*, *.babc.com*, and so on.
SysLocation	(Optional) Enter comma-separated strings that will match the string value stored in the sysLocation OID in MIB-II, for devices that you want to: • Include—In auto-discovery processing. • Exclude—From auto-discovery processing. The location strings can be specified using wildcards. An asterisk (*) matches, up to an arbitrary length, any combination of mixed uppercase and lowercase alphanumeric characters, hyphen (-), underscore (_), and, white space (spaces and tabs). A question mark (?) wildcard matches a single occurrence of any of the above characters. For example, a SysLocation filter of *San ** will match all SysLocation strings starting with *San Francisco*, *San Jose*, etc.

Step 3 Click **Apply**.

Importing Devices Into the DCR

For bulk import (from an NMS or from a file) Operations Manager provides you a direct link to the DCR (**Devices > Device Management > Import Devices**).

Step 1 Select **Devices > Device Management > Import Devices**. The CiscoWorks Common Services Import Devices page appears.

Step 2 Enter the import information.

Note If you need help importing, click the Help button on the page, and the Common Services online help opens.

Configuring Automatic Device Selection in Operations Manager

Operations Manager uses automatic synchronization by default. Use the following procedure to change manual synchronization to automatic synchronization.

Note If you are running the synchronization process for the first time, it may take several hours for Operations Manager to collect inventory for all of the devices, depending on how many devices are being added to Operations Manager.

Note Devices must exist in the DCR before you can add them to Operations Manager.

Step 1 Select **Devices > Device Management > Device Selection**. The Device Selection page appears.

Step 2 Activate the Automatic radio button.

Step 3 Click **Apply**. Operations Manager will be synchronized with the DCR; any DCR devices currently not in Operations Manager will be added. Operations Manager will perform inventory collection for the new devices that are being added.

Step 4 Verify whether any duplicate devices exist, by selecting **Devices > Device Management > IP Address Report**.

Note If you do not require the duplicate device for your deployment, remove it (for information on deleting devices, see *User Guide For Cisco Unified Operations Manager* or the online help).

Adding Devices Manually from the DCR to Operations Manager

If Operations Manager is configured for automatic device selection, you do not need to perform this procedure. With manual device selection, you need to manually select devices to monitor. You will need to do this periodically after devices have been added to the DCR. For example, if you run Operations Manager physical discovery on a weekly basis, you should consider checking for new devices that you want to monitor after discovery completes.

Note Devices must exist in the DCR before you can add them to Operations Manager.

Step 1 Select **Devices > Device Management** > **Device Selection**. The Device Selection page appears.

Step 2 Select the Manual radio button. All devices that are not in Operations Manager inventory are available through the device selector.

Step 3 Select devices the following ways:

- Entering device names or IP addresses in the Device Display Name, and clicking **Filter**.
- Using the group selector.

Step 4 If you want to see the devices you have selected, click the Selection tab, and a list of devices appears.

Step 5 Click **Select**. Operations Manager will perform inventory collection on the devices that are being added.

Step 6 Verify whether any duplicate devices exist, by selecting **Devices > Device Management > IP Address Report**.

Note If you do not require the duplicate device for your deployment, remove it (for information on deleting devices, see *User Guide For Cisco Unified Operations Manager* or the online help).

For more information, see *User Guide for Cisco Unified Operations Manager*.

Understanding Device States

The Device Management: Summary page lists the device states for all devices in the Operations Manager inventory. The Device Management: Summary page appears when you select **Devices > Device Management**.

Table 3-3 Device States

State	Description
Monitored	The device has been successfully imported, and is fully managed by Operations Manager.
Partially Monitored	The device has been successfully imported by some of the data collectors[1] in Operations Manager, but not all. If a device is in this state, you should take action to ensure that the device becomes monitored.
Monitoring Suspended	Monitoring of the device is suspended.
Inventory Collection in Progress	Operations Manager is probing the device. This is the beginning state, when the device is first added; a device is also in this state during periodic inventory collection. Some of the data collectors may still be gathering device information.
Unreachable	Operations Manager cannot manage the device. See Troubleshooting Device Import and Inventory Collection, page 3-13.
Unsupported	The device is not supported by Operations Manager.

[1] *Data collector* is a term used to refer to all back-end applications that are involved in device discovery and device data collection.

Table 3-4 displays the states that devices go through while they are being added to Operations Manager inventory, and what causes a device to go into a particular device state.

Table 3-4 Transition States of Devices when Being Added to Inventory

Start Inventory Collection	Result of Inventory Collection	Resulting Device State
Inventory collection in progress.	Successfully discovered.	Monitored.
Inventory collection in progress.	Not all credentials were supplied or some services were down.	Partially Monitored.

Table 3-4 Transition States of Devices when Being Added to Inventory (continued)

Start Inventory Collection	Result of Inventory Collection	Resulting Device State
Inventory collection in progress.	• SNMP information is not configured. • Device is not responding. • Device is not reachable. • Device credentials are not correct.	Unreachable.
Inventory collection in progress.	• The device model is not recognized. • The software version is not supported.	Unsupported

Verifying Devices Added to Operations Manager using the Service Level View

One way you can verify that your devices have been added to Operations Manager inventory is by looking at the Service Level View. This also provides you with quick access to many of the Operations Manager tools.

If you find that problems have occurred during inventory collection, see Troubleshooting Device Import and Inventory Collection, page 3-13.

Step 1 Select **Monitoring Dashboard > Service Level View**. The Service Level View display appears, displaying a logical topology view of your IP telephony implementation.

For more information, see *User Guide for Cisco Unified Operations Manager* or the Operations Manager online help.

Scheduling Inventory Collection

There are separate inventory collection schedules for devices and phones. There is only one inventory collection schedule for devices. You cannot create additional schedules; you can only edit the existing schedule. For IP phones, you can create multiple inventory collection schedules.

On the Inventory Collection Schedule page (**Devices > Device Management > Inventory Collection > Device**), you can edit, suspend, or resume the device inventory collection schedule. (See Editing the Device Inventory Collection Schedule, page 3-13.)

On the IP Phone Discovery Schedule page (**Devices > Device Management > Inventory Collection > IP Phone**), you can add, edit, or delete the IP Phone discovery schedules. (See Adding a Phone Discovery Schedule, page 3-13.)

Editing the Device Inventory Collection Schedule

Step 1 Select **Devices > Device Management > Inventory Collection > Device**. The Device Inventory Collection page appears.

Step 2 Click **Edit**. The Inventory Collection Schedule: Edit page appears.

Step 3 Change the desired scheduling information.

Step 4 Click **OK**.

Step 5 Click **Yes**.

Adding a Phone Discovery Schedule

Step 1 Select **Devices > Device Management > Inventory Collection > IP Phone Details**. The IP Phone Discovery Schedule page appears.

Step 2 Click **Add**. The Add Schedule dialog box appears.

Step 3 Enter the following:

- A name for the discovery schedule
- The day of the week when you want discovery to occur
- The time of the day when you want discovery to occur

Step 4 Click **OK**.

Troubleshooting Device Import and Inventory Collection

Problems might occur during physical discovery (Operations Manager adds devices to the DCR) and can also occur during inventory collection (Operations Manager adds devices to its inventory for monitoring).

Note If device inventory collection or discovery is being performed over a slow network connection, or if the devices are unusually slow in responding to SNMP or HTTP requests, you can change the ivr.properties file to prevent Operations Manager from timing out during discovery or inventory collection. The file is located in the NMSROOT/conf/ivr folder.

To increase the time allocated for discovery or inventory collection, change the property messageFactor:6 to messageFactor:10. The higher the number, the longer Operations Manager waits before timing out.

To troubleshoot device inventory collection, try the following:

- If a device is not responding, confirm all device credentials and readd the device. See Editing Device Configuration and Credentials, page 3-17.
- If device inventory collection times out for several devices, increase SNMP timeout settings. See Modifying SNMP Timeout and Retries, page 3-17.

- View device error information on the Modify/Delete Device page. See Performing Manual Inventory Collection on Devices, page 3-18.
- Verify that the device is operational during the import and that it supports MIB II.
- Check the reason for devices being in the Unreachable state. See Starting Operations Manager, page 3-19.
- After troubleshooting the problem, check the device status. See Verifying Devices Added to Operations Manager using the Service Level View, page 3-12.

The Modify/Delete Devices page displays device information and data collection information. You can use Modify/Delete Devices to determine the current state of a device and view data collection errors.

Step 1 Select **Devices > Device Management > Modify/Delete Devices**. The Modify/Delete Devices page opens.

Step 2 Expand the folder that contains your device (according to its inventory collection status; see Verifying Devices Added to Operations Manager using the Service Level View, page 3-12).

Step 3 Click the device name or IP address. The device information is populated.

Step 4 Look under Data Collection Status Information for error information (see Starting Operations Manager, page 3-19).

Step 5 Perform the required actions to clear the error.

Understanding Inventory Collection Messages

Table 3-5 lists messages that might be shown for devices that are in the Unreachable state.

Table 3-5 Inventory Collection Error Messages

Message	Meaning	Action
SNMP Timeout	The device is in the Unreachable state because the SNMP read-only community string for the device is incorrect.	See Editing Device Configuration and Credentials, page 3-17 to enter the correct read community string for the device.
Others: Missing IP Address or Data Collector Timeout	The device is in the Unreachable state because of some other reason. It could be that DNS resolution for the device failed or the data collector timed out.	Click the device on the Modify/Delete Devices page. The error message displays the exact problem. • If the IP address is missing: – Readd the device with the correct IP address. or – Make sure that Operations Manager can resolve the device name: try adding the domain name as part of the device name. • If the data collector times out, restart the daemon manager to get all data collectors in sync.

Why Does a Device Go into the Partially Monitored State?

Table 3-6 explains the possible reasons for the error codes that you see in the Modify/Delete Devices page, that occur for partially monitored devices.

Why Cisco Unified Communications Manager May Go into the Partially Monitored State

- If the incorrect HTTP credentials were entered for a Cisco Unified Communications Manager, it may go into the partially monitored state. When this occurs none of the Perfmon Counters are polled. To change device credentials, see Editing Device Configuration and Credentials, page 3-17.
- If ports 135, 145, and 1025-65000 are not open in a firewall setup, Cisco Unified Communications Manager goes into the partially monitored state. Verify that these ports are open. If you need to open the ports, after doing so, rediscover the device.

Why Certain Voice Applications May Go into the Partially Monitored State

The following devices may go into the partially monitored state:

- Cisco IP Contact Center
- Cisco Unity Connection
- Cisco Unity
- Cisco Personal Assistant

If insufficient windows credentials are provided during the addition of these devices, they become partially monitored, and some of their WMI attributes are not polled. To change device credentials, see Editing Device Configuration and Credentials, page 3-17.

Table 3-6 Error Shown on the Modify/Delete Devices Page

Error Shown on the Modify/Delete Devices Page	Reason	Resolution Steps
Error Code = CCM Authentication Failure Error Message = Success:WrongCredentials	This message indicates that either Unified Communications Manager http credentials are not entered or the credentials provided are incorrect.	Verify that you provided the correct http credentials in the DCR by using the credentials to log in to the Cisco Unified Communications Manager Admin page, and rediscover the device.
Error Code= CCM Authentication Failure Error Message= Success:UnknownCredential Error	This message indicates that SNMP management MIBs are not responding. The MIBs and their associated errors could be one of the following: • MIB-2—The ipAddressTable is not responding. • CISCO-CCM-MIB—The ccmTable is not responding. Specifically the ccmClusterId attribute is not responding. • Inventory collection could not find the ccmVersion detail. This may be because the ccmVersion attribute in the CISCO-CCM-MIB is not responding.	Restart the SNMP Agent on the system and rediscover the device.

Table 3-6 Error Shown on the Modify/Delete Devices Page (continued)

Error Shown on the Modify/Delete Devices Page	Reason	Resolution Steps
Error Code = CCM Authentication Failure Error Message = Success:WebServiceDown	Http service is not running or responding to requests from Operations Manager.	Verify that the web server is running by launching the Cisco Unified Communications Manager Admin page. Check the firewall to see if it is blocking the HTTP/HTTPS connection between Cisco Unified Communications Manager and Operations Manager.

Error Code = CCM Authentication Failure
Error Message = Success: HTTPSCertificateNotImported
	The Cisco Unified Communications Manager certificate has failed.	Do the following:
		1. Check the file IPToHostName.txt in the CSCOpx\lib\jre\lib\security folder. It should contain an entry like the following:
		`deviceip>=<hostname> record for each of the ccm For e.g. 10.76.91.115=blrsd1`
		2. Go to the keytool utility location <NMSROOT>\CSCOpx\lib\jre\bin.
		3. Run the following command:
		`keytool -list -keystore <NMSROOT>\CSCOpx\lib\jre\lib\security\cacerts`
		The downloaded certificates are displayed.
		4. Verify that there is an entry similar to the following for the Cisco Unified Communications Manager:
		`Certificate fingerprint (MD5): AC:B6:94:A5:9C:17:E0:D7:91:52:9B:B1:97:06:A6:E4`
		`cn=ct-sd, ou=nmtg, o=cisco systems, l=bangalore, st=Karnataka, c=in, Oct 26, 200 5, trustedCertEntry`
		5. Rediscover the device.

Why Does a Device Go into the Unreachable State?

Devices may go into the Unreachable state due to the following reasons:

- SNMP timeout
- Data collector timeout

If an SNMP timeout occurs, verify the SNMP access credentials provided during discovery.

If a data collector timeout occurs, verify that the SNMP management interface is not a serial or a generic interface (such as Frame Relay with the subnet mask 255.255.255.252). You should always access SNMP details using an Ethernet interface.

Editing Device Configuration and Credentials

After you add devices, you can change their configuration setup through the Modify/Delete Devices page.

Note You can also change device credentials directly though the DCR device management pages. Operations Manager provides you with a link to the CiscoWorks Common Services Device Management page. From Operations Manager, select **Devices > Device Credentials**. For more details on using CiscoWorks Common Services Device Management, see the CiscoWorks Common Services online help.

Step 1 Select **Devices > Device Management > Modify/Delete Devices**. The Modify/Delete Devices page opens.

Step 2 Expand the folder that contains your devices.

Step 3 Select the device or device group that you want to update.

Step 4 Click **Edit**. The Edit Device Configuration: Change Credentials page appears.

If you select a single device, all the existing credentials for that device are populated in the Edit Device Configuration: Change Credentials page (asterisks populate the field). If you select multiple devices, only a comma-separated list of IP addresses is displayed.

Note The auto-populated credentials (asterisks) do not reflect the actual credentials; they only indicate that credentials are available.

Step 5 You can update the following credentials:

- SNMPv2c/SNMPv1
- SNMPv3
- HTTP
- WMI

Note If you are changing credentials for a device that also has a duplicate, be sure to change the credentials on both devices in case the primary device is deleted.

Step 6 Click **OK**.

Modifying SNMP Timeout and Retries

If an SNMP query does not respond in time, Operations Manager times out. Operations Manager retries contacting the device for as many times as you indicate. The timeout period is doubled for every subsequent retry.

For example, if the timeout value is 4 seconds and the retries value is 3 seconds, Operations Manager waits 4 seconds before the first retry, 8 seconds before the second retry, and 16 seconds before the third retry.

The SNMP timeout and retry values are global settings. Change these values as follows:

Step 1 Select **Devices > Device Management > Inventory Collection > SNMP Configuration**. The SNMP Configuration page appears.

Step 2 Select a new SNMP timeout setting. The default is 4 seconds.

Step 3 Select a new Number of Retries setting. The default is 3 retries.

Step 4 Click **Apply**. Click **Yes** to confirm.

Performing Manual Inventory Collection on Devices

Through the Modify/Delete Devices page, you can manually collect inventory on devices or device groups. When inventory collection takes place, if there are any changes to a device or group configuration, the new settings will overwrite any previous settings.

Note Configuration changes on a device are discovered by Operations Manager only during discovery (inventory collection) of the device. Therefore any changes to a device's configuration are not shown by Operations Manager until the next inventory collection after the configuration change.

Inventory collection occurs only for active devices. Suspended devices do not go through inventory collection. If some of the devices you are selecting for inventory collection are suspended devices, Operations Manager displays messages indicating that only the active devices will go through inventory collection.

Note Do not confuse the Operations Manager physical discovery process (which adds devices to the DCR) or the Operations Manager inventory collection process (which probes devices and updates components in Operations Manager inventory) with the DCR synchronization process. Operations Manager inventory collection is a process that affects only the Operations Manager inventory.

The following events also trigger inventory collection:

- The entire Operations Manager inventory is polled. This is controlled by the inventory collection schedule. (See Scheduling Inventory Collection, page 3-12.)
- Operations Manager is using automatic synchronization with the DCR, and a device is added, or a change is made to a device in the DCR. Such DCR changes include a device being deleted or having its credentials (IP address, SNMP credentials, MDF type) changed.
- Operations Manager is using manual synchronization with the DCR, and a device is added to Operations Manager using the Device Selection page.

Note If you are using the ACS login module, the System Identity user that is configured in ACS should have permission to run all the job management-related tasks in Common Services and the rediscovery task in Operations Manager.

When rediscovery occurs, all devices in the system are discovered. Therefore, this task should be made available only to the person who has access to all devices in the network.

Step 1 Select **Devices > Device Management > Modify/Delete Devices**. The Modify/Delete Devices page appears.

Step 2 Select the device or group for which you want to perform inventory collection.

Step 3 Click **Rediscover**. Inventory collection is started.

Starting Operations Manager

You can access Operations Manager from either the Operations Manager server or a client system.

Note If a client system is available, we recommend that you perform all configuration and day-to-day activities from 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 (for client system requirements, see Table 1-4).

Note

- Disable any popup blocker utility that is installed on your client system before launching Operations Manager.
- By default, SSL is not enabled in Common Services. If you upgraded to Operations Manager 2.2 and SSL was enabled before the upgrade, it remains enabled after the upgrade.

Starting Operations Manager on a Client System

In Internet Explorer, enter the Operations Manager server's IP Address or DNS name followed by the port number 1741. For example, http://<om_server name>:1741.

Starting Operations Manager on the Operations Manager Server

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.

Adding the Operations Manager Home Page to the Internet Explorer Trusted Site Zone

If Enhanced Security is enabled on the Windows 2003 system, you must perform the following procedure before you can access the Operations Manager home page.

Step 1 Open Operations Manager and select **Start > All Programs > Cisco Unified Operations Manager > Cisco Unified Operations Manager**.

Step 2 From the File menu, select **Add this site to**.

Step 3 Click **Trusted Sites Zone**.

Step 4 In the **Trusted Sites** dialog box, click **Add** to move the site to the list.

Step 5 Click **Close**.

Step 6 Refresh the page to view the site from its new zone.

Step 7 Check the Status bar of the browser to confirm that the site is in the **Trusted Sites Zone**.

Adding Cisco Unified Communications Management Server Links from Operations Manager

Use this procedure to add a link to a locally installed or remotely installed Service Monitor server from Operations Manager. For important details about Service Monitor event and trap processing, as well as licensing, see the online help or the *User Guide for Cisco Unified Operations Manager*.

You can also link to Provisioning Manager and Service Statistics Manager servers. See Operations Manager online help or the *User Guide for* Cisco Unified Operations Manager for instructions.

Step 1 Select **UC Management Suite > Service Monitor**. The Service Monitor page appears.

Step 2 Click **Add**. The Add Service Monitor page appears.

Step 3 Enter data in the following fields:

- IP Address—IP address of a remote server where Service Monitor is installed.
- Protocol—HTTP or HTTPS.
- Port—Port by which Service Monitor is accessed. Cannot be left blank.
- Status—Selection for whether to use this Service Monitor as a cross-launch server.
- Remarks—Optional.

Step 4 Click **Add**. The Service Monitor page appears, displaying information for the newly added Service Monitor.

Understanding and Configuring Security

Operations Manager supports the following security-related mechanisms:

- SNMPv3 protocol (Authentication/No-Privacy option)—Operations Manager supports the Authentication/No-Privacy option between the server and the device.
- Local security or Cisco Secure ACS—Access to tasks within Operations Manager is either controlled by local security (Common Services Local login module) or Cisco Secure ACS. Local security is enabled on the server by default. Operations Manager supports integration with Cisco Secure ACS. For more information, see Security Configuration with Cisco Secure ACS, page C-1.

- SSL—Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. It relies upon certificates, public keys, and private keys. (SSL is not enabled in Common Services by default.) You can enable or disable SSL depending on the need to use secure access. Operations Manager supports SSL between clients and the server.

To get started with configuring security, see Setting Up Security in the Configuring the Server chapter of *User Guide for CiscoWorks Common Services*.

Supported NMS Integration

Operations Manager supports integration with network management systems (NMSs) that reside in your network. Operations Manager does not support an NMS residing on the system with Operations Manager.

- Operations Manager listens for traps from managed devices on port 162 (the default). If your network devices are already sending traps to another management application, configure that application to forward traps to Operations Manager.
- Operations Manager forwards traps to destinations that you specify, as follows:
  - To forward pass-through traps, see Configuring SNMP Trap Receiving and Forwarding, page 3-21.
  - To forward processed traps, see “Managing SNMP Trap Notifications” in the “Using Notification Services” chapter of *User Guide for Cisco Unified Operations Manager*.

  For more information on pass-through and processed traps, see the appendix “Processed and Pass-through Traps, and Other Unidentified Traps and Events” in *User Guide for Cisco Unified Operations Manager*.

Configuring SNMP Trap Receiving and Forwarding

Operations Manager can receive traps on any available port and forward them to a list of devices and ports. This capability enables Operations Manager to easily work with other trap processing applications. However, you must enable SNMP on your devices and configure SNMP to send traps either directly to Operations Manager or to one of the following:

- An NMS
- A trap daemon

To send traps directly to Operations Manager, perform the tasks in Enabling Devices to Send Traps to Operations Manager, page 3-22. To integrate SNMP trap receiving with an NMS or a trap daemon, follow the instructions in Integrating Operations Manager Trap Receiving with NMSs or Trap Daemons, page 3-23.

Updating the SNMP Trap Receiving Port

By default, Operations Manager receives SNMP traps on port 162. If you need to change the port, you can do so.

Step 1 Select **Administration > Preferences**. The System Preferences page appears.

Step 2 In the Trap Receiving Port field, enter the port number.

Step 3 Click **Apply**.

For a list of ports that Operations Manager uses, see Verifying TCP and UDP Ports that Operations Manager Uses, page 2-6.

Enabling Devices to Send Traps to Operations Manager

Because Operations Manager uses SNMP MIB variables and traps to determine device health, you must configure devices to provide this information. For any Cisco devices that you want Operations Manager to monitor, SNMP must be enabled and the device must be configured to send SNMP traps to the Operations Manager server.

Make sure your devices are enabled to send traps to Operations Manager by using the command line or GUI interface appropriate for your device:

- Enabling Cisco IOS-Based Devices to Send Traps to Operations Manager, page 3-22
- Enabling Catalyst Devices to Send SNMP Traps to Operations Manager, page 3-23

Enabling Cisco IOS-Based Devices to Send Traps to Operations Manager

For devices running Cisco IOS software, provide the following commands:

```
(config)# snmp-server [community string] ro
(config)# snmp-server enable traps
(config)# snmp-server host [a.b.c.d] traps [community string]
```

where [*community string*] indicates an SNMP read-only community string and [*a.b.c.d*] indicates the SNMP trap receiving host (the Operations Manager server).

For more information, see the appropriate command reference guide.

Step 1 Log in to Cisco.com.

Select **Support > Cisco IOS and NX-OS Software**.

Step 2 Select the Cisco IOS Software release version used by your Cisco IOS-based devices.

Step 3 Under Reference Guides, select the appropriate command reference guide.

Note Periodically, information on Cisco.com is reorganized and, as a result, navigation paths change. If this happens, use Search to look for Cisco IOS Command References.

Enabling Catalyst Devices to Send SNMP Traps to Operations Manager

For devices running Catalyst software, provide the following commands:

```
(enable)# set snmp community read-only [community string]
(enable)# set snmp trap enable all
(enable)# set snmp trap [a.b.c.d] [community string]
```

Where [*community string*] indicates an SNMP read-only community string and [*a.b.c.d*] indicates the SNMP trap receiving host (the Operations Manager server).

For more information, see the appropriate command reference guide.

Step 1 Log in to Cisco.com.

Step 2 Select **Products & Services**.

Step 3 Under Network Systems, select **Switches**.

Step 4 Select the appropriate Cisco Catalyst series switch.

Step 5 In the Support box, select **References**—you might be prompted to log in to Cisco.com—and select the appropriate command reference guide.

Note Periodically, information on Cisco.com is reorganized and, as a result, navigation paths change. If this happens, try using Search to look for Catalyst Command References.

Integrating Operations Manager Trap Receiving with NMSs or Trap Daemons

You might need to complete one or more of the following steps to integrate SNMP trap receiving with other trap daemons and other Network Management Systems (NMSs):

- Add the host where Operations Manager is running to the list of trap destinations in your network devices. See Enabling Devices to Send Traps to Operations Manager, page 3-22. Specify port 162 as the destination trap port.
- If your network devices are already sending traps to another management application, configure that application to forward traps to Operations Manager.

Table 3-7 describes scenarios for SNMP trap receiving and lists the advantages of each.

Table 3-7 Configuration Scenarios for Trap Receiving

Scenario	Advantages
Network devices send traps to port 162 of the host where Operations Manager is running. Operations Manager receives the traps and forwards them to the NMS.	• No reconfiguration of the NMS is required. • No reconfiguration of network devices is required. • Operations Manager provides a reliable trap reception, storage, and forwarding mechanism. • NMS continues to receive traps on port 162 on the host where the NMS is running. • Network devices continue to send traps to port 162.
The NMS receives traps on default port 162 and forwards them to port 162 on the host where Operations Manager is running.	• No reconfiguration of the NMS is required. • No reconfiguration of network devices is required. • Operations Manager does not receive traps dropped by the NMS.

Configuring SNMP Trap Forwarding

By default, Operations Manager does not forward unprocessed SNMP traps. However, you can configure it to do so.

Step 1 Select **Administration > Preferences**. The System Preferences page appears.

Step 2 Under Trap Forwarding Parameters enter:

- An IP address or DNS name for the server.
- A port number on which the server can receive traps.

Step 3 Click the **Apply** button.

Configuring Health Monitor

The Health Monitor utility monitors Operations Manager processes, notes when a process stops and restarts, and can send email updates. To get email updates, perform this procedure.

Step 1 Edit the <*NMSROOT*>/HealthMonitor/conf/HealthMonitor.cfg file.

Step 2 Enter a value for each of these parameters:

- SMTP_Server—SMTP mail server address.
- Receiver_Email_ID—Email ID for the administrator to be notified
- Sender_Email_ID—Email ID that identifies the sender

Step 3 After you update the file, put the updates into effect by restarting the HealthMonitor service. From the comand line, enter these commands:

```
net stop OMHealthMonitor
net start OMHealthMonitor
```

For more information, see *User Guide for Cisco Unified Operations Manager*.

Configuring Cisco Unified Communications Manager for Use with Operations Manager

For Operations Manager to discover and manage Cisco Unified Communications Manager, you must either perform the configurations described in this section or verify that the existing Cisco Unified Communications Manager settings are correct. Incorrect settings cause incomplete monitoring of Cisco Unified Communications Manager, resulting in inconsistent behavior in some Operations Manager features.

This topic contains the following tasks:

- Configuring the Syslog Receiver on Cisco Unified Communications Manager, page 3-25
- Configuring RTMT on Cisco Unified Communications Managers (Optional), page 3-27
- Setting HTTP Credentials on Cisco Unified Communications Manager, page 3-28

You can also see the online help for additional details on how to configure voice application systems and software for use with Operations Manager.

Configuring the Syslog Receiver on Cisco Unified Communications Manager

To successfully receive Cisco Unified Communications Manager syslog messages, you must add the syslog receiver from the device's serviceability web page. Use the following procedure to perform the necessary steps.

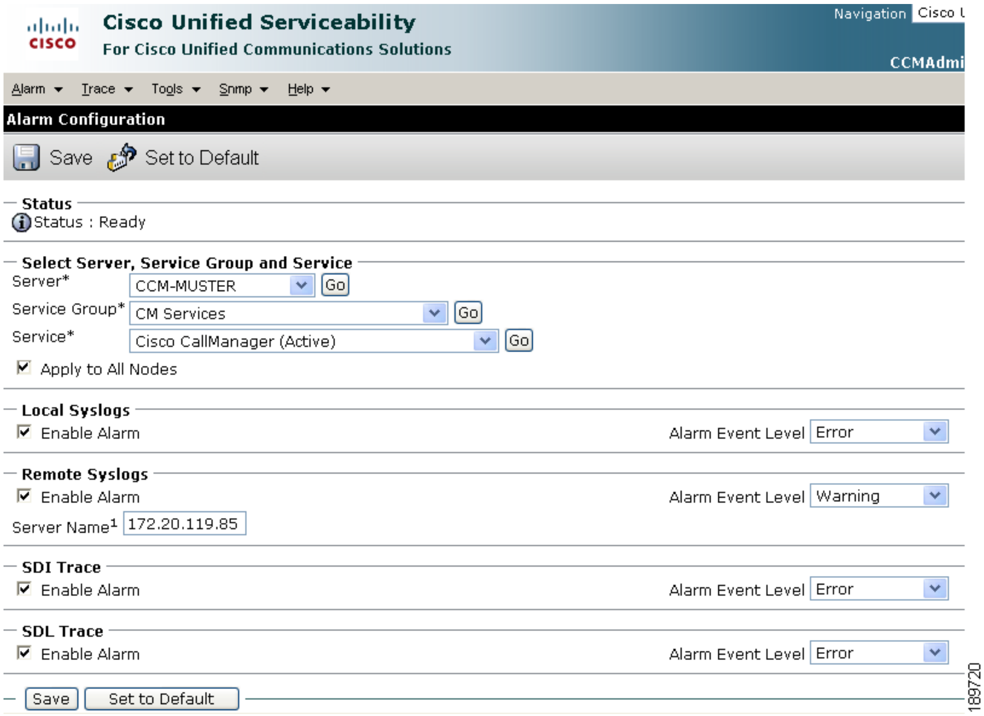
For additional details on what syslog events map to Unified Communications Manager releases, see the Event appendix in the *Cisco Unified Operations Manager User Guide*.

Step 1 On your Cisco Unified Communications Manager, select **Cisco Unified Serviceability** from the Navigation pull-down in the top-right corner of the device's home screen.

Step 2 Select **Alarm > Configuration**.

For an example of the serviceability page for a version 5.x device, see Figure 3-1. The serviceability page may display differently depending on your device version.

Figure 3-1 Unified Serviceability Web Page for CCM Version 6.x Device



Status
Status : Ready

Select Server, Service Group and Service
Server* CCM-MUSTER
Service Group* CM Services
Service* Cisco CallManager (Active)
☑ Apply to All Nodes

Local Syslogs
☑ Enable Alarm — Alarm Event Level: Error

Remote Syslogs
☑ Enable Alarm — Alarm Event Level: Warning
Server Name¹ 172.20.119.85

SDI Trace
☑ Enable Alarm — Alarm Event Level: Error

SDL Trace
☑ Enable Alarm — Alarm Event Level: Error

Caution Do not use the CCM enterprise service parameter to configure the syslog receiver for Operations Manager syslog integration. When the enterprise parameter is enabled, all syslog messages (with matching severity levels) are sent regardless of what is intended to be processed by Operations Manager.

Select the correct alarm configuration elements for your particular machine:

- For Unified Communications Manager 4.x, select **Cisco CallManager**.
- For Unified Communications Manager 5.x, select **Server > Service**:
  - Cisco AMC Service.
  - Cisco CDR Agent.
  - Cisco CDR Repository Manager.
  - Cisco CallManager.
  - Cisco Database Layer Monitoring.
  - Cisco DRF Client.
  - Cisco DRF Master.
- For Unified Communications Manager 6.x and later, select:
  - **Service Group > CM Services**, then **Service > Cisco CallManager.**
  - **Service Group > CDR Service**, then **Cisco CDR Agent** and **Cisco CDR Repository Manager**.
  - **Service Group > Database and Admin Services**, then **Cisco Database Layer Monitoring**.
  - **Service Group > Performance and Monitoring Services**, then **Cisco AMC Service**.

- **Service Group > Backup and Restore**, then **Cisco DRF Client and Cisco DRF Master**.

Step 3 Click the **Enable Alarm** checkbox, select proper Alarm Event Level (see the Alarm Configuration Settings in *Cisco Unified Serviceability Administration Guide for Cisco Unified Communications Manager* on Cisco.com), and enter Operations Manager server name/address in Server Name text box.

For Unified Communications Manager 5.x or later, select AMC Service, and set the alarm event level to **Warning**. For all other devices, set the alarm event level to **Error**. Provide any necessary information based on your Unified Communications Manager.

Step 4 Check **Apply to all nodes**.

Step 5 Click **Save**.

Note Syslog messages have a limitation of 1,024 characters (including the heading). Any syslog-based event details may not contain the full information due this syslog limitation. If the syslog message exceeds this limit, it is truncated to 1,024 characters by the syslog sender.

Activating Events in Operations Manager

Most device events display in the Alerts and Events display after the device has been added to the Operations Manager database. However, several events will not be displayed in Operations Manager out of the box. You must activate the following events in order for Operations Manager to display them:

- Number Of Registered Gateways Increased
- Number Of Registered Gateways Decreased
- Number Of Registered MediaDevices Increased
- Number Of Registered MediaDevices Decreased

Note These events are raised at the cluster level, therefore individual device information might not be available in the event description. To access individual device information use the RTMT Tool. Select Filter > Devices > MediaDevices or Gateway, then select the checkbox for all states and generate the report. This report will display all the registered and unregistered media devices or gateways.

To activate these event pairs, perform the following steps:

1. Open the NMSROOT\conf\seg\sysLogConfig.xml file.
2. Remove the comment for Syslog by removing the lines marked.
3. Restart the SEGServer process.

Configuring RTMT on Cisco Unified Communications Managers (Optional)

Operations Manager uses the same polling rate and threshold settings as RTMT. In normal operation, you do not need to do anything. The default will work properly.

Note This impacts Unified Communications Manager performance and Operations Manager.

If you want to have a lower polling rate, increase the polling rate to monitor in real-time, and then you can update the parameter settings on Cisco Unified Communications Manager. Use the following procedure to perform these steps.

Step 1 To update the polling and threshold parameter settings, go to the Unified Communications Manager Administration page.

Step 2 To change polling rates:

- For CallManager 5.x and later, select **System > Service Parameter > publisher > Cisco AMC Service**, then change the Data Collection Polling rate value.
- For CallManager 4.x, select **Service > Service Parameter > publisher > Cisco RIS Data Collector**, then change the Data Collection Polling rate value.

Step 3 To change threshold parameters, install and launch RTMT, select **AlarmCentral**, then select a specific alert and right-click to launch Alert Property.

Setting HTTP Credentials on Cisco Unified Communications Manager

Operations Manager uses the Administrative XML Layer (AXL) API in addition to SNMP to manage Cisco Communications Manager. This means that Operations Manager makes SOAP calls over HTTP via the AXL interface to collect fault and performance information from Cisco Unified Communications Manager. Operations Manager requires the HTTP username and password in order to execute these queries. The username and password do not need to have administrator privileges. You only need credentials with read-level access to http://server-name/ccmadmin.

Viewing Alerts

You can view alerts using the monitoring dashboard displays. Select **Monitoring Dashboard** and choose from the following displays:

- Service Level View
- Alerts and Events
- Service Quality Alerts
- IP Phone Status

What's Next?

After discovery completes Operations Manager is monitoring your network, Table 3-8 summarizes tasks that you might want to perform to customize Operations Manager for your specific deployment.

Note All these tasks are optional; they are not required for Operations Manager to monitor your network.

Table 3-8 Setting Up Operations Manager

Task	Description
Configure notifications	In addition to learning about alerts by monitoring the Monitoring Dashboard displays, you can subscribe users to receive e-mail and hosts to receive Operations Manager-generated SNMP traps in response to alerts.
Configure views for the Monitoring Dashboard displays	Views are logical groupings of devices that appear in the Monitoring Dashboard displays (Service Level View, Alerts and Events, Phone Activities, and Service Quality Alerts). Whenever you create a new user-defined group on the Group Administration and Configuration page, a corresponding view is created.
Configure polling parameters and thresholds	Operations Manager provides default values for polling parameters and threshold values. However, you can update the values as needed for your network. You should plan to apply the changes when activity on the Operations Manager server is low. By default, Operations Manager does not set the voice utilization polling settings. If you want to use Operations Manager's performance monitoring capabilities, you must first enable voice utilization polling.
Configure purging	By default, Operations Manager purges the database daily at midnight. You can modify the schedule.
Configure inventory collection	Operations Manager provides a single default schedule for inventory collection. You can use that schedule, or you can suspend it.

To use Operations Manager more fully, you might want to perform additional configuration tasks. See the online help or *User Guide for Cisco Unified Operations Manager* for information on using and configuring Operations Manager.

APPENDIX A

User Inputs for Installation, Reinstallation, and Upgrade

This appendix provides information on the user inputs during Operations Manager installation, reinstallation, and upgrade.

This appendix contains:

- User Inputs for Typical Installation
- User Inputs for Custom Installation
- Password Information

User Inputs for Typical Installation

Table A-1 lists information you need to supply when installing Operations Manager for the first time in Typical mode.

Table A-1 User Inputs for New Installation: Typical

Settings	Value
Applications to install	Select the applications you want to install.
Password for *admin* user	No default values. Enter the admin password. For more information on passwords, see Password Information.
Password for System Identity account	No default values. Enter the System Identity account password. For more information on passwords, see Password Information.

Table A-1 User Inputs for New Installation: Typical (continued)

Settings	Value
Password for casuser	The password is generated randomly if you leave the field blank.
Mail Settings: • HTTPS port • Administrator's e-mail address • SMTP server name	**Note** Appears if IIS was detected on your system, and you indicated that you would like to avoid port conflict between IIS and Operations Manager by reconfiguring the default HTTPS port. Otherwise, Mail Settings appears only during a Custom installation The default values are: • Port number 443—Enter a value from the range that is displayed. • *admin@domain.com* • *localhost name*

Table A-2 lists information you need to enter during an upgrade installation in Typical mode.

Table A-2 User Inputs for Upgrade Installation: Typical

Settings	Value
Password for casuser account	The password is generated randomly if you leave the field blank. (See Fixing Problems That Can Occur When You Change Passwords, page A-7.)
Applications to install	Select the applications you want to install.

Table A-3 lists information you need to enter while reinstalling in Typical mode:

Table A-3 User Inputs for Reinstallation: Typical

Settings	Value
Password for casuser account	The password is generated randomly if you leave the field blank. (See Fixing Problems That Can Occur When You Change Passwords, page A-7.)
Applications to install	Select the applications you want to install.

User Inputs for Custom Installation

Table A-4 lists the information you must enter while installing for the first time in Custom mode.

Table A-4 User Inputs for a New Installation: Custom

Settings	Value
Destination folder	The default location is *System drive:*\Program Files\CSCOpx. Select another location if you want to install in a specific location. We recommend that you specify a short path for the destination folder.
Applications to install	Select the applications you want to install.
Password for users *admin* and *guest* (Mandatory)	No default values. Enter the admin and guest password. For more information on passwords, see Password Information.
Password for System Identity account (Mandatory)	No default values. Enter the system identity account password. For more information on passwords, see Password Information.
Password for user *casuser*	The password is generated randomly if you leave the field blank.
Password for the database. (Mandatory)	Enter the database password. For more information on passwords, see Password Information.
Mail Settings: (Mandatory) • HTTPS port • Administrator's e-mail address • SMTP server name	The default values are: • *443*—If IIS is installed on your server, enter a port number from the range displayed. • *admin@domain.com* • *localhost name*
Data for the Self-signed Certificate: (Mandatory) • Country Code • State • City • Organization Name • Organization Unit Name • Host name • E-mail Address	By default, the self-signed certificate is generated using the organization that Windows is registered to, and the host name. You must enter the host name. You can leave the other fields blank. **Note** Common Services allows you to create security certificates to enable SSL communication between your client browser and management server. Self Signed Certificates are valid for five years from the date of creation. When the certificate expires, the browser prompts you to install the certificate again from the server where you have installed Common Services. In the Typical mode, this certificate is automatically generated.

Table A-5 lists the information you must enter during an upgrade installation in Custom mode.

Note If Service Statistics Manager is installed in your network and you change either of the following:

- The password for the user admin
- The destination location (the directory in which Operations Manager is installed)

Service Statistics Manager stops collecting data from Operations Manager. You can reenable data collection by performing the procedures that are documented in *Release Notes for Cisco Unified Service Statistics Manager 12*.

Table A-5 User Inputs for an Upgrade Installation: Custom

Settings	**Value**
Applications to install	Select the applications you want to install.
Password for users *admin* and *guest* (Optional)	You can change the passwords for the admin and guest users. To keep the existing passwords, leave the fields blank. (See Fixing Problems That Can Occur When You Change Passwords, page A-7.)
Password for System Identity account (Mandatory)	No default values. Enter the System Identity account password. For more information on passwords, see Password Information.
Password for the user casuser (Optional)	If you do not enter a password, the setup program generates a random password for you. (See Fixing Problems That Can Occur When You Change Passwords, page A-7.)
Password for the database (Optional)	Leave the fields blank to use the existing password.

Table A-5 User Inputs for an Upgrade Installation: Custom (continued)

Settings	Value
Mail Settings: • HTTPS port • Administrator's e-mail address • SMTP server name (Optional)	You can choose to keep the existing information.
Data for the Self-signed Certificate: (Mandatory) • Country Code • State • City • Organization • Organization Unit Name • E-mail Address	You can change the Self-signed Certificate information. By default, the installation program uses the existing Self-Signed Certificate information. If you want to generate a new certificate, uncheck the Keep Existing Certificate check box, and enter the country code, state, city, company, organization, and host name for HTTPS. You must enter the host name. You can leave the other fields blank. **Note** Common Services allows you to create security certificates to enable SSL communication between your client browser and management server. Self Signed Certificates are valid for five years from the date of creation. When the certificate expires, the browser prompts you to install the certificate again from the server where you have installed Common Services. In the Typical mode, this certificate is automatically generated.

Table A-6 lists the information you must enter while reinstalling in Custom mode.

Note If you have Service Statistics Manager installed and you change either of the following:

- The password for the user admin
- The destination location (the directory in which Operations Manager is installed)

Service Statistics Manager stops collecting data from Operations Manager. You can reenable data collection by performing the procedures that are documented in *Release Notes for Cisco Unified Service Statistics Manager 12*.

Table A-6 User Inputs for Reinstallation: Custom

Settings	Value
Destination folder	The default location is *System drive:*\Program Files\CSCOpx. We recommend that you specify a short path for the destination folder.
Password for users *admin* and *guest* (Optional)	You can change the passwords for the admin and guest users. To keep the existing passwords, leave the fields blank. (If you change the password for the admin user, see Fixing Problems That Can Occur When You Change Passwords, page A-7.)

Table A-6 User Inputs for Reinstallation: Custom (continued)

Settings	Value
Password for System Identity account (Mandatory)	You can change the passwords for the System Identity account. To keep the existing passwords, leave the fields blank.
Password for user casuser (Optional)	If you do not enter a password, the setup program generates a random password for you. (See Fixing Problems That Can Occur When You Change Passwords, page A-7.)
Password for the database (Optional)	Leave the fields blank to retain the existing password.
Mail Settings: • HTTPS port • Administrator's e-mail address • SMTP server name (Optional)	You can choose to keep the existing information.
Data for the Self-signed Certificate: (Mandatory) • Country Code • State • City • Organization Name • Organization Unit Name • Hostname • E-mail Address	By default, the self-signed certificate is generated using the organization that Windows is registered to, and the host name. You must enter the host name. You can leave the other fields blank. **Note** Common Services allows you to create security certificates to enable SSL communication between your client browser and management server. Self Signed Certificates are valid for five years from the date of creation. When the certificate expires, the browser prompts you to install the certificate again from the server where you have installed Common Services. In the Typical mode, this certificate is automatically generated.

Password Information

This topic provides information on the usage of passwords during installation.

It contains:

- Password Rules for New Installation
- Fixing Problems That Can Occur When You Change Passwords
- Password Rules for Upgrade Installation
- Password Rules for Re-installation
- Password Descriptions

Password Rules for New Installation

The following rules apply for a new installation:

- In Typical mode, admin, casuser, and System Identity account passwords are mandatory. The installation program generates guest and database passwords randomly.
- In Custom mode, admin, guest, System Identity account, and database passwords are mandatory. You can either enter the casuser password or allow the installation program to randomly generate it.

Fixing Problems That Can Occur When You Change Passwords

During upgrade and reinstallation, you might change the passwords for the admin user and for the casuser account. Table A-7 lists the problems that can occur and provides steps you can take to resolve them.

Table A-7 Potential Problems

Password Changed	Potential Problem	Workaround
admin	Service Statistics Manager loses contact with Operations Manager and Operations Manager.	If Service Statistics Manager is installed in your network, reestablish contact by performing procedures in *Release Notes for Cisco Unified Service Statistics Manager 1.2*.
casuser	Operations Manager credentials fail when accessing a Unified Communications Manager version 4.x system for which Windows authentication is configured.	The casuser password on the Operations Manager server must match the casuser password on the Unified Communications server. Log in to the Windows server where Unified Communications Manager is installed and update the casuser password. **Note** If you do not know the casuser password on the Operations Manager server, change it; see Changing casuser Password.

Password Rules for Upgrade Installation

During an upgrade installation, the casuser password is requested; other passwords are retained.

Password Rules for Re-installation

The following rules apply for re-installation:

- In Typical mode, the installation program retains passwords for admin, guest, and database.You can either enter the casuser password or allow the installation program to randomly generate it. (See Fixing Problems That Can Occur When You Change Passwords, page A-7.)
- In Custom mode, you can chose to enter new admin, guest, system identity account, and database passwords or retain most existing passwords. You can either enter the casuser password or allow the installation program to randomly generate it. (See Fixing Problems That Can Occur When You Change Passwords, page A-7.)

Password Descriptions

The types of passwords are as follows:

- Common Services admin Password
- System Identity Account Password
- Common Services Guest Password
- Common Services Database Password

Common Services admin Password

While entering the password for the admin user, include a minimum of five characters.

The admin user account is the default administrator; you must use the admin username and password to log in to Operations Manager after initial installation. (Ensure that you have noted down the password.)

You are prompted to enter this password in both Typical and Custom modes of installation.

System Identity Account Password

While entering the System Identity account password, use a minimum of five characters.

You are prompted to enter this password in both Typical and Custom modes of installation.

The System Identity account is used in a multi-server environment. Communication among multiple servers is enabled by a “trust” model addressed by certificates and shared secrets. For more information, see *User Guide for CiscoWorks Common Services.*

Note You need a System Identity account to configure security with Cisco Secure ACS (which must be installed on a separate server) and to configure the DCR in master and slave mode. (Operations Manager supports the DCR; Operations Manager does not support it.)

Common Services Guest Password

While entering the password for the Common Services guest account, use a minimum of five characters.

Use this password to log into the Common Services server as a guest user. You are prompted to enter this password in the Custom mode of installation. In the Typical mode, this password is randomly generated.

Common Services Database Password

While entering database passwords:

- Use a minimum of five characters and a maximum of 15 characters.
- Do not start the password with a number.
- Do not insert spaces between characters.
- Do not use any special characters.

Changing Passwords

These topics explain how to change the passwords for the admin user and the casuser account using utilities (or the Common Services user interface if possible):

- Changing Common Services Admin Password
- Changing casuser Password

Changing Common Services Admin Password

Note If you change the admin password and Service Statistics Manager is in your network, it will lose contact with Operations Manager. To reestablish contact, perform procedures in *Release Notes for Cisco Unified Service Statistics Manager 1.2*.

You can change your Common Services Admin password by using either the Common Services user password recovery utility or from the GUI, if you want to change it.

- Changing Admin Password Using Password Recovery Utility
- Changing Admin Password from Common Services

Changing Admin Password Using Password Recovery Utility

Step 1 Stop the daemon manager by entering the following at the shell prompt:

```
net stop crmdmgtd
```

Step 2 Go to *NMSROOT*\bin directory and enter:

```
NMSROOT\bin\resetpasswd username
```

NMSROOT is the directory where you have installed Operations Manager.

A message appears:

```
Enter new password for username:
```

Step 3 Enter the new password for *username*

Step 4 Start the daemon manager by entering at the command prompt:

```
net start crmdmgtd
```

Changing Admin Password from Common Services

Step 1 Log in with username admin.

Step 2 Select the **CiscoWorks** link in the upper-right corner of the Operations Manager home page.

Step 3 Select **Common Services > Server > Security> Single-Server Management > Local User Setup** in the CiscoWorks home page.

The Local User Setup page appears.

Step 4 Click **Modify My Profile**.

The My Profile pop-up window appears.

Step 5 Enter the password in the Password field.

Step 6 Re-enter the password in the Verify field.

Step 7 Enter the e-mail ID in the E-mail field.

Step 8 Click **OK**.

Changing casuser Password

Caution Changing the casuser password might cause Operations Manager credential failure when accessing a Unified Communications Manager version 4.x system for which Windows authentication is configured. Be prepared to log into the Windows server where Unified Communications Manager is installed to update the casuser password to match the new casuser password that you enter.

Step 1 At the command prompt, enter:

NMSROOT`\setup\support\resetCasuser.exe`

Three options are displayed:

1. Randomly generate the password
2. Enter the password
3. Exit.

Step 2 Enter **2**, and press **Enter**.

A message appears, prompting you to enter the password.

Step 3 Confirm the password.

If a local user policy is configured on the Operations Manager server and you enter a password that does not match the password policy, the application exits with an error message. For more information, see Setting up Local User Policy in *User Guide for CiscoWorks Common Services*.

APPENDIX B

Licensing

This appendix provides licensing information for Cisco Unified Operations Manager (Operations Manager). It contains the following sections:

- Licensing Overview, page B-1
- Licensing Reminders, page B-5

Licensing Overview

Operations Manager features software-based product registration and license key technologies. Licensing ensures that you possess a licensed copy of Operations Manager.

Note

- Licensing uses node-locking technology. The license file can only be used with the MAC address that you supply.
- To license, install, and run Operations Manager on VMware, you must configure a static address for the virtual machine.

To determine whether Operations Manager is licensed, see Verifying License Status, page B-1. If you do not have a license or you want to upgrade your license, see Licensing Scenarios, page B-3.

Verifying License Status

You can use this procedure to verify both Operations Manager and Service Monitor license status.

Step 1 Select the CiscoWorks link in the upper-right corner of the Operations Manager home page. The CiscoWorks home page window opens.

Step 2 Select **Common Services > Server > Admin > Licensing**. The Licensing Information page appears, displaying the information in the following table.

Column	Description
Name	Abbreviated product name—For Operations Manager, this is OM.
Version	Product version—*A.b.c*, where *A* is the major version number, *b* is the minor version number, and *c* is the service pack number. For example, OM 2.0.0 indicates version 2.0 without service packs. Operations Manager 2.0 license also supports Operations Manager 2.2. Service Monitor 2.0 license also supports Service Monitor 2.2.
Size	Limit—Number of IP phones that Operations Manager supports. Registered, unregistered, and suspect phones are counted toward the license limit.
Status	One of the following: • Purchased—You have a registered, licensed product. • Evaluation—This license will expire on the expiration date; Operations Manager and/or Service Monitor will stop running.
Expiration Date	Date on which Operations Manager stops running—Applies to evaluation licenses. The evaluation period lasts for 90 days.

Licenses that Can Be Purchased

The license that you purchase determines which level of Operations Manager (Standard or Premium Edition) you have and the number of phones that Operations Manager can monitor.

Operations Manager provides two levels of feature-based licensing:

- Premium Edition—Full-feature Operations Manager.
- Standard Edition—Limited-feature Operations Manager. The following tools are not accessible:
  - Diagnostics (Phone Status Tests, Synthetic Tests, Batch Tests, and Node-to-Node Tests).
  - Video phone reports.

You can purchase licenses in the following increments:

- Up to 1,000 phones.
- Up to 2,000 phones.
- Up to 5,000 phones.
- Up to 10,000 phones.
- Up to 15,000 phones.
- Up to 20,000 phones.
- Up to 25,000 phones.
- Up to 30,000 phones.

You can combine at 15,000 phone license and a 30,000 phone license to support 45,000 phones on an appropriately sized server.

Licensing Scenarios

Table B-1 describes what to do in different scenarios if you do not have a licensed, registered copy of Operations Manager or if you want to increase device support.

Table B-1 How to Obtain and Register a License

Scenario	What to do
Installing with a purchased license.	1. Before installing, obtain a license file. See *Licensing Process, page B-3*. **Note** You can install Operations Manager without the license file. You can upgrade your license after installation. See Registering a License File with Operations Manager, page B-4. 2. During installation, select License File Location, and provide the location of your license file.
Installing with an evaluation license. **Note** The evaluation license is limited to monitoring 300 devices and 1000 phones.	During installation, select Evaluation Only. Evaluation versions are active for 90 days, before you are required to purchase a license. If you want to upgrade to a purchased license after installation, obtain a PAK and license file for the installed version of Operations Manager. For information on the licensing process, see Licensing Process, page B-3.
Getting a license for additional devices (either upgrading from an evaluation license, or increasing the number of supported devices).	See Licensing Process, page B-3. **Note** When upgrading your license either from an evaluation version or from lower device limits to higher limits, you must restart the daemon manager. If the daemon manager is not restarted, the new device limits will not take effect and the system status reports will not show the correct information.
Moving Operations Manager to another server.	Call the Cisco TAC for assistance.

Licensing Process

The Operations Manager license file includes support for up to 1,000 phones. You can purchase incremental licenses for additional device support and register up to 45,000 phones with a single Operations Manager. For each incremental license that you purchase, you will receive a PAK, and you must use that PAK to obtain a license file. Registered, unregistered, and suspect phones are counted toward the license limit.

Note This licensing process also applies to Service Monitor.

This process applies to new installations and license upgrades:

1. Obtain a Product Authorization Key (PAK)—The PAK is used to register Operations Manager, and any additional device support that you might purchase for Operations Manager, on Cisco.com, and it contains resource limitations. See Obtaining a PAK, page B-4.
2. Obtain a license file—A license file is sent to you after you register the PAK on Cisco.com. See Obtaining a License File, page B-4.
3. Copy the license file—into a directory with read permission for the username casuser or the user group casuser—onto the server where Operations Manager is to be installed. If Operations Manager is already installed and you are upgrading your license file, you must register the license file with Operations Manager. See Registering a License File with Operations Manager, page B-4.

Obtaining a PAK

The PAK is located on the software claim certificate that is shipped with the Operations Manager product CD.

Obtaining a License File

Note To install Operations Manager on a VMware server, you must supply a static MAC address to obtain a license file. Operations Manager does not work with a purchased license when a dynamic MAC address is configured for the virtual machine. For more information, see VMware Guidelines, page 1-7.

Step 1 Register the PAK and the MAC address of the system where Operations Manager is installed with Cisco.com at http://www.cisco.com/go/license. You will be asked to log in. You must be a registered user of Cisco.com to log in.

Note The MAC address is required because licensing uses node-locking technology. The license file can only be used with the MAC address that you supply.

The license file will be e-mailed to you. After you obtain a license file, register the license with the Operations Manager server.

Registering a License File with Operations Manager

Step 1 Copy the license file to the Operations Manager server, into a directory with read permission for the username casuser or the user group casuser.

Step 2 Install the license:

a. From the Operations Manager home page, click **CiscoWorks** in the upper-right corner of the window. The CiscoWorks home page opens. Under Common Services, select **Server > Admin > Licensing**. (For more information, see Common Services online help.)

The Licensing Information page appears.

- **b.** Click **Update**. A file browser dialog box appears.
- **c.** Enter the path to the new license file in the License field, or click **Browse** to locate the license file you copied to the server.
- **d.** Click **OK**.

  The system verifies whether the license file is valid, and updates the license. The updated licensing information appears on the Licensing Information page. If you purchased more than one license, repeat Step 2 to install each additional license.

  If you encounter errors, repeat the steps to license your product.

Step 3 Stop and start the daemon manager from a command prompt by issuing the following commands:

```
net stop crmdmgtd
net start crmdmgtd
```

Licensing Reminders

Operations Manager provides reminders in the following circumstances:

- Evaluation Version: Before Expiry, page B-5
- Purchased Version: No License File, page B-5
- Purchased Version: Device Limit Exceeded, page B-6

Evaluation Version: Before Expiry

If you have installed the evaluation version of Operations Manager, you must obtain the license file from Cisco.com if you want to continue to use the product after the 90-day evaluation period. For details, see Licensing Process, page B-3.

Before expiry of the evaluation license, you will see the following prompt:

```
This software is provided for evaluation purposes only and will expire in XX days. If this
is not an evaluation copy, please click this link for information about obtaining a valid
purchase license. Click here for current licensing information. Otherwise, please contact
your Cisco representative for purchasing information.
```

This message is displayed as an alert after you log in and try to access Operations Manager. If you fail to upgrade your evaluation license, all Operations Manager processes will run, but access to Operations Manager functionality will be prohibited.

Purchased Version: No License File

If you have installed a purchased version of Operations Manager, you must register Operations Manager using the PAK number. For details, see Licensing Process, page B-3. If you fail to register Operations Manager, you will see the following prompt:

```
The license file is invalid. Please click this link for information about obtaining a
valid purchase license. Click here for current licensing information. Otherwise, please
contact your Cisco representative for purchasing information.
```

Operations Manager is fully functional. However, you will continue to receive the alert until you register your license.

Purchased Version: Device Limit Exceeded

If you have a restricted license, Operations Manager notifies you when your device inventory approaches the device limit. Operations Manager counts registered, unregistered, and suspect phones toward the license limit. After the device limit has been reached, Operations Manager displays the following messages:

- Exceeded device limit:

  ```
  You have exceeded the device limit for Cisco Unified Operations Manager. Devices will
  not be managed.
  ```

- Exceeded phone limit:

  ```
  You have exceeded the phone limit for Cisco Unified Operations Manager. Please click
  here for current licensing information. Please contact your Cisco representative to
  determine if additional licenses can be purchased for this server.
  ```

Operations Manager remains functional, but will shortly stop adding devices and phones to managed inventory.

APPENDIX C

Security Configuration with Cisco Secure ACS

To configure Operations Manager to use Cisco Secure ACS for authentication and authorization, work through these topics in order:

- Cisco Secure ACS Support, page C-1
- Operations Manager Integration Notes, page C-1
- CiscoWorks Local Login Module Authentication Roles, page C-2
- Configuring the System Identity User in Common Services, page C-3
- Setting Up the Cisco Secure ACS Server, page C-3
- Changing the AAA Mode to ACS in Common Services, page C-4
- Assigning Roles to Users and User Groups in Cisco Secure ACS, page C-5
- Verifying the Operations Manager and Cisco Secure ACS Configuration, page C-6

Cisco Secure ACS Support

Operations Manager supports the ACS mode of authentication and authorization. To use this mode, you must have a Cisco Secure ACS (Access Control Server), installed in your network on a server separate from the one where Operations Manager is installed. For the supported software version, see For details on supported devices and software, see the *Supported and Interoperable Devices and Software for* Cisco Unified Operations Manager.

Operations Manager Integration Notes

Operations Manager (and Service Monitor, and Common Services) integrate with Cisco Secure ACS as shared profile components. Multiple instances of the same application—for example, Operations Manager—can use the same Cisco Secure ACS server for authentication and authorization.

When you register Cisco Unified Operations Manager (and Cisco Unified Operations Manager, CiscoWorks Common Services) with Cisco Secure ACS, the applications tasks—such as, performing device discovery in Operations Manager—and user roles—such as, Network Administrator—for the application are imported into Cisco Secure ACS.

You only need to register one instance of an application with Cisco Secure ACS for tasks and roles to be imported. If you register an application a second time, any changes that you have made to role settings, such as creating custom roles, are lost.

CiscoWorks Local Login Module Authentication Roles

CiscoWorks login modules enable you to use a source of authentication other than the native mechanism, the CiscoWorks Local login module. You can use the Cisco Secure ACS server for this purpose.

After you authenticate, authorization is controlled by your role. A role is a set of tasks that you have the privilege to perform. By default, the CiscoWorks Local login module authorization scheme has five roles. A sixth role, Super Admin, is available in ACS mode and visible on the Cisco Secure ACS system only. Roles are listed in Table C-1 from least privileged to most privileged.

Table C-1 Common Services User Roles and Privileges

Role	Description
Non-ACS Mode—CiscoWorks Local Login Module	
Help Desk	User with this role has the privileges to view some information in Operations Manager and Common Services. Example: Can search the Alert History database.
Approver	User with this role does not have any privileges. (Operations Manager does not assign any tasks to this user role.)
Network Operator	User with this role has the privilege to perform all Operations Manager tasks and some Common Services tasks. Example: Can configure logging parameters. **Note** A user with this role by default can perform the same Operations Manager tasks as a Network Administrator.
Network Administrator	User with this role has the privilege to perform all Operations Manager tasks and several Common Services tasks. User can also perform Network Operator tasks. Example: Can add devices to Operations Manager from the DCR.
System Administrator	User with this role has the privilege to perform all system administration tasks. Example: Enable and disable debugging; set logging level.
ACS Mode	
Super Admin	User with this role has the privilege to perform all tasks when AAA mode is set to ACS and Cisco Secure ACS is used for authentication. You do not see the Super Admin role when you perform local user setup in Common Services. You can assign a user to this role only when you are logged in to Cisco Secure ACS and only when your CiscoWorks login module is set to ACS.

For tasks that are defined for Operations Manager and Common Services and the roles with privilege to perform the tasks, see the Permission Report in Common Services. (Click the CiscoWorks link in the upper-right corner of the Operations Manager home page and select **Common Services > Server > Reports > Permission Report > Generate Report**.)

Note For more information, see *User Guide for CiscoWorks Common Services 3.2*.

We recommend that you do not modify the default Common Services roles. However, you can create your own custom roles for Operations Manager on Cisco Secure ACS.

Configuring the System Identity User in Common Services

Before you integrate the Operations Manager server with Cisco Secure ACS, ensure that you create and assign all privileges to a System Identity User in Common Services. This topic explains how to set up a local user as the System Identity User. (To use the Common Services admin user as the System Identity User, see the topic Setting up System Identity Account in *User Guide for CiscoWorks Common Services 3.2.)*

1. Create a local user and assign all roles to the user.

   Note If the System Identity User is not configured with all CiscoWorks Local login module roles (see Table C-1), authorization fails when you try perform certain tasks in Operations Manager and Common Services.

2. Update the System Identity User, replacing the username with the one that you created in step 1. (From the CiscoWorks home page **Common Services > Server > Security > Multi-Server Trust Management > System Identity Setup**. For more information, click the Help link.)

For more information, see *User Guide for CiscoWorks Common Services 3.2*.

Setting Up the Cisco Secure ACS Server

Perform these tasks in Cisco Secure ACS before you change the Common Services AAA mode to ACS:

1. Configure ACS Administrators.

   Configure an administrator user with all privileges in Cisco Secure ACS.

   Note If you do not configure the administrator user with all privileges, Operations Manager registration with Cisco Secure ACS fails.

   Note the username and password for the administrator; you will need to enter them when you change the AAA mode to ACS in Common Services.

2. Add the Operations Manager server to Cisco Secure ACS as an AAA Client.

   Configure the Operations Manager server as an AAA client in Cisco Secure ACS and do the following:

   - Select authentication by TACACS + (CISCO IOS).
   - Note the shared secret that you enter; you will need to enter it in Common Services when you change the AAA mode to ACS in Common Services.

3. Add the System Identity User and Common Services users to Cisco Secure ACS.

   You can create a group and add users to it.

4. Note whether the Operations Manager, Service Monitor, and Common Services applications are already registered with Cisco Secure ACS:

   a. To find out, select **Shared Profile Components** and look for:

      Cisco Unified Operations Manager

      Cisco Unified Service Monitor

      CiscoWorks Common Services

   b. Based on your authentication setting (per user or per group) on Cisco Secure ACS, click either User Setup or Group Setup. Verify the per-user or per-group setting for Cisco Unified Operations Manager using **Interface Configuration > TACACS + (Cisco IOS)**.

See the following documents on Cisco.com for details how to perform each of the above tasks:

- *User Guide for Cisco Secure Access Control Server 4.x*

  http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_list.html

- *User Guide for CiscoWorks Common Services 3.2*

  http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_list.html

Changing the AAA Mode to ACS in Common Services

Before you perform this procedure, complete the tasks in Configuring the System Identity User in Common Services, page C-3 and Setting Up the Cisco Secure ACS Server, page C-3.

Step 1 Select **CiscoWorks> Common Services > Server > Security > AAA Mode Setup**.

Step 2 Click **OK**. The AAA Mode Setup page appears.

Step 3 Next to Select a Type, select the ACS radio button. The page refreshes, displaying appropriate options.

Step 4 Under Server Details, enter an IP address for the Cisco Secure ACS server and enter a port.

Step 5 Under Login, enter:

- ACS Admin Name—Enter the name of the administrator you created in step 1 of Setting Up the Cisco Secure ACS Server, page C-3.
- ACS Admin Password—Enter the password for the administrator you created in step 1. (See Setting Up the Cisco Secure ACS Server, page C-3.)
- ACS Shared Secret Key— Enter the shared secret you entered when you added the Operations Manager server to Cisco Secure ACS as an AAA client in step 2. (See Setting Up the Cisco Secure ACS Server, page C-3.)

Step 6 Decide whether to select **Register all installed applications with ACS**.

Note If Operations Manager is registered with ACS and you register it again, you lose any custom roles that were previously configured in Cisco Secure ACS for Operations Manager. The same is true for Service Monitor and Common Services. (To selectively register an application, see Registering an Application to Cisco Secure ACS from the Command Line, page C-5.)

Step 7 Select the appropriate radio button (HTTP or HTTPS) under Current ACS Administrative Access Protocol.

Step 8 Click **Apply** to complete the mode change. An ACS verification status message is displayed; do one of the following:

- Click **OK—**Registers Operations Manager, Service Monitor, and Common Services tasks and users to ACS; overwrites any existing custom roles for Operations Manager, Service Monitor, and Common Services.
- Click **Cancel**—Prevents registration to ACS from occurring.

Step 9 Restart the daemon manager for the changes to take effect. From the command line, enter these commands:

```
net stop crmdmgtd

net start crmdmgtd
```

Registering an Application to Cisco Secure ACS from the Command Line

Registering an application with ACS imports the application tasks and overwrites any custom roles that exist for the application in Cisco Secure ACS. If you did not select **Register all installed applications with ACS** when you changed the AAA mode to ACS in Common Services, you might want to use the information in this section to register an application to Cisco Secure ACS.

A script, <*NMSROOT*>\bin\AcsRegCli.pl, enables you to selectively register applications to Cisco Secure ACS.

Note NMSROOT is the directory where Operations Manager is installed. If you chose the default, it is C:\PROGRA~1\CSCOpx.

Following are the available parameters when running the script from the CLI:

```
AcsRegCli.pl -register <application name>
```

Replace application name with any of the following:

- itm—Registers Operations Manager only
- qovr—Registers Service Monitor only
- cmf—Registers CiscoWorks Common Services only
- all—Registers all applications on the server (Cisco Unified Operations Manager, Cisco Unified Service Monitor, and CiscoWorks Common Services).

Assigning Roles to Users and User Groups in Cisco Secure ACS

You must ensure that the System Identity User in Cisco Secure ACS is assigned all roles and that Common Services users or user groups have been assigned the proper privileges.

In Cisco Secure ACS, select **Shared Profile Components > Cisco Unified** Operations Manager. For more information, see these documents:

- *User Guide for Cisco Secure Access Control Server 4.x*
- *User Guide for CiscoWorks Common Services 3.2* or see Common Services online help. Look for these topics:

- Roles in ACS
- Assigning Roles to Users and User Groups in ACS

Verifying the Operations Manager and Cisco Secure ACS Configuration

After performing the tasks beginning with Assigning Roles to Users and User Groups in Cisco Secure ACS, page C-5 through Configuring the System Identity User in Common Services, page C-3, verify the configuration as follows:

1. Log in to Operations Manager with a username defined in Cisco Secure ACS.
2. Try to perform tasks, to ensure that you can perform only those tasks that you are entitled to perform based on the role assigned to you in Cisco Secure ACS.

   For example: If your privilege is Help Desk, then:

   - You should be able to view Fault History reports.
   - You should not be able to add devices to Operations Manager from the DCR.
3. Based on the Network Device setting for the user or group on Cisco Secure ACS, you can view only certain devices on the Operations Manager server.

Note For a list of Operations Manager displays that perform device-based filtering, see the Operations Manager-specific online help in Cisco Secure ACS.

If you encounter difficulties, see Authentication Failure in ACS Mode in *User Guide for CiscoWorks Common Services.*

INDEX