



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

Software Release 2.0.3

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-16182-04

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.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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.

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

Installation Guide for Cisco Unified Operations Manager

© 2005 - 2008 Cisco Systems, Inc. All rights reserved.

The Software may contain certain software and related user documentation (e.g., Crystal Enterprise Professional, Crystal Reports Professional and/or Crystal Analysis Professional) that are owned by Crystal Decisions, Inc., 895 Emerson Street, Palo Alto, CA 94301 ("Crystal Decisions"). All such software products are the technology of Crystal Decisions. The use of all Crystal Decisions software products is subject to a separate license agreement included with the Software electronically, in written materials, or both. YOU MAY NOT USE THE CRYSTAL DECISIONS SOFTWARE UNLESS AND UNTIL YOU READ, ACKNOWLEDGE AND ACCEPT THE TERMS AND CONDITIONS OF THE CRYSTAL DECISIONS' SOFTWARE LICENSE AGREEMENT. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE CRYSTAL DECISIONS' SOFTWARE LICENSE, YOU MAY RETURN, WITHIN THIRTY (30) DAYS OF PURCHASE, THE MEDIA PACKAGE AND ALL ACCOMPANYING ITEMS (INCLUDING WRITTEN MATERIALS AND BINDERS OR OTHER CONTAINERS) RELATED TO THE CRYSTAL DECISIONS' TECHNOLOGY, TO SMARTS FOR A FULL REFUND; OR YOU MAY WRITE, CRYSTAL WARRANTIES, P.O. BOX 67427, SCOTTS VALLEY, CA 95067, U.S.A.

GNU eTeks PJA Toolkit

Copyright © 2000-2001 Emmanuel PUYBARET/eTeks info@etek.com. All Rights Reserved.

The eTeks PJA Toolkit is resident on the CD on which the Software was delivered to you. Additional information is available at eTeks' web site: <http://www.eteks.com>. The eTeks PJA Toolkit program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License (GPL) as published by the Free Software Foundation; version 2 of the License. The full text of the applicable GNU GPL is available for viewing at <http://www.gnu.org/copyleft/gpl.txt>. You may also request a copy of the GPL from the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA. The eTeks PJA Toolkit program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

For a period of three years from the date of your license for the Software, you are entitled to receive under the terms of Sections 1 and 2 of the GPL, for a charge no more than SMARTS' cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code for the GNU eTeks PJA Toolkit provided to you hereunder by requesting such code from SMARTS in writing: Attn: Customer Support, SMARTS, 44 South Broadway, White Plains, New York 10601.

IBM Runtime for AIX

The Software contains the IBM Runtime Environment for AIX(R), Java™ 2 Technology Edition Runtime Modules © Copyright IBM Corporation 1999, 2000 All Rights Reserved.

HP-UX Runtime Environment for the Java™ 2 Platform

The Software contains the HP-UX Runtime for the Java™ 2 Platform, distributed pursuant to and governed by Hewlett-Packard Co. ("HP") software license terms set forth in detail at: <http://www.hp.com>. Please check the Software to determine the version of Java runtime distributed to you.

DataDirect Technologies

Portions of this software are copyrighted by DataDirect Technologies, 1991-2002.

NetBSD

Copyright © 2001 Christopher G. Demetriou. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed for the NetBSD Project. See <http://www.netbsd.org/> for information about NetBSD.
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. <<Id: LICENSE, v 1.2 2000/06/14 15:57:33 cgd Exp>>

RSA Data Security, Inc.

Copyright © 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved. License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind. These notices must be retained in any copies of any part of this documentation and/or software.

AES

Copyright © 2003, Dr Brian Gladman <brg@gladman.me.uk>, Worcester, UK. All rights reserved.

License Terms:

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;
3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

ALTERNATIVELY, provided that this notice is retained in full, this product may be distributed under the terms of the GNU General Public License (GPL), in which case the provisions of the GPL apply INSTEAD OF those given above.

Disclaimer: This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose.

Issue Date: 26/08/2003



CONTENTS

Preface ix

CHAPTER 1

Prerequisites 1-1

- Product Overview 1-1
- Server Requirements 1-2
- Client Requirements 1-4
 - Other System Software 1-4
- System Capacity 1-5
- Supported Devices 1-6

CHAPTER 2

Installing, Uninstalling, and Upgrading Cisco Unified Operations Manager 2-1

- Preparing to Install Operations Manager 2-1
 - Preparing the Operations Manager Server 2-2
 - Checking for and Temporarily Disabling DEP 2-2
 - Enabling DEP 2-3
 - Preparing Devices for Addition to Operations Manager Inventory 2-3
 - Device-Specific Configurations 2-4
 - Actions to Take Before Adding Devices 2-4
 - Verifying TCP and UDP Ports that Operations Manager Uses 2-5
 - Gathering Information to Provide During Installation 2-6
- Performing a New Installation 2-7
- Reinstalling Operations Manager 2-10
- Uninstalling Operations Manager 2-11
- Upgrading to Cisco Unified Operations Manager 2.0.3 2-12
 - Upgrading from Operations Manager 2.0.2 to Operations Manager 2.0.3 2-13
 - Service Monitor Post-Upgrade Configuration 2-15
 - Upgrading from Operations Manager Releases Prior to 2.0.2 to Operations Manager 2.0.2 2-16
 - Changes to Notification Event Customization Severity After Upgrade 2-16
- Configuring Your System for SNMP Queries 2-17
- NTP Configuration Notes 2-17

CHAPTER 3

Getting Started 3-1

- Configuring Operations Manager to Monitor Devices 3-1

Understanding the DCR	3-3
Configuring the DCR in Master and Slave Mode	3-4
Adding Devices to the DCR	3-5
Configuring Operations Manager Physical Discovery	3-5
Configuring Credentials	3-7
Filtering Operations Manager Physical Discovery	3-7
Importing Devices Into the DCR	3-9
Configuring Automatic Device Selection in Operations Manager	3-10
Adding Devices Manually from the DCR to Operations Manager	3-10
Understanding Device States	3-11
Verifying Devices Added to Operations Manager	3-12
Starting the Service Level View	3-12
Scheduling Inventory Collection	3-12
Editing the Device Inventory Collection Schedule	3-13
Adding a Phone Discovery Schedule	3-13
Troubleshooting Device Import and Inventory Collection	3-13
Understanding Inventory Collection Messages	3-14
Why Does a Device Go into the Partially Monitored State?	3-15
Why Does a Device Go into the Unreachable State?	3-16
Editing Device Configuration and Credentials	3-17
Modifying SNMP Timeout and Retries	3-17
Performing Manual Inventory Collection on Devices	3-18
Starting Operations Manager	3-19
Adding the Operations Manager Home Page to the Internet Explorer Trusted Site Zone	3-19
Adding a Service Monitor to Operations Manager	3-20
Understanding and Configuring Security	3-20
Supported NMS Integration	3-21
Configuring SNMP Trap Receiving and Forwarding	3-21
Updating the SNMP Trap Receiving Port	3-21
Enabling Devices to Send Traps to Operations Manager	3-22
Enabling Cisco IOS-Based Devices to Send Traps to Operations Manager	3-22
Enabling Catalyst Devices to Send SNMP Traps to Operations Manager	3-22
Integrating Operations Manager Trap Receiving with NMSs or Trap Daemons	3-23
Configuring SNMP Trap Forwarding	3-24
Configuring Cisco Unified Communications Manager for Use with Operations Manager	3-24
Setting HTTP Credentials on Cisco Unified Communications Manager	3-24
Viewing Alerts	3-24
What's Next?	3-25

APPENDIX A**Licensing A-1**

- Licensing Overview **A-1**
- Verifying License Status **A-1**
- Licenses that Can Be Purchased **A-2**
- Licensing Scenarios **A-2**
- Licensing Process **A-3**
- Obtaining a PAK **A-4**
- Obtaining a License File **A-4**
- Registering a License File with Operations Manager **A-4**
- Licensing Reminders **A-5**
- Evaluation Version: Before Expiry **A-5**
- Purchased Version: No License File **A-5**
- Purchased Version: Device Limit Exceeded **A-6**

APPENDIX B**Configuring Operations Manager with Cisco Secure ACS B-1**

- Login Module **B-1**
- Authentication Roles **B-2**
- Before You Begin: Integration Notes **B-3**
- Configuring Operations Manager on Cisco Secure ACS **B-4**
- Verifying the Operations Manager and Cisco Secure ACS Configuration **B-4**

INDEX



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	<i>italic</i> font
Displayed session and system information	screen font
Information you enter	boldface screen font
Variables you enter	<i>italic</i> 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 Formats
<i>Supported Devices Table for Cisco Unified Operations Manager 2.0.3</i>	On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps6535/products_device_support_tables_list.html
<i>Release Notes for Cisco Unified Operations Manager 2.0.3</i>	<ul style="list-style-type: none"> • 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
<i>Installation Guide for Cisco Unified Operations Manager (Includes Service Monitor) 2.0.3</i>	<ul style="list-style-type: none"> • 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
<i>User Guide for Cisco Unified Operations Manager 2.0.3</i>	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 Formats
<i>Release Notes for Cisco Unified Service Monitor 2.0.1</i>	<ul style="list-style-type: none"> 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
<i>User Guide for Cisco Unified Service Monitor 2.0.1</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps6536/products_user_guide_book09186a0080628ace.html
<i>Release Notes for CiscoWorks Common Services 3.0.5 (Includes CiscoView 6.1.5) on Windows</i>	On Cisco.com at the following URL: http://cisco.com/en/US/products/sw/cscowork/ps3996/prod_release_note09186a00806f45bf.html
<i>Installation and Setup Guide for Common Services 3.0.5 (Includes CiscoView) on Windows</i>	On Cisco.com at the following URL: http://cisco.com/en/US/products/sw/cscowork/ps3996/products_installation_guide_book09186a00806ab62a.html
<i>User Guide for CiscoWorks Common Services 3.0.5</i>	On Cisco.com at the following URL: http://cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_book09186a00806feda7.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-hand 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

Revised: June 5, 2008

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 1-4](#)
- [System Capacity, page 1-5](#)
- [Supported Devices, page 1-6](#)

For additional requirements before you begin your installation or upgrade, see [Preparing the Operations Manager Server, page 2-2](#) or [Before You Begin, page 2-12](#).

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.

**Note**

For guidelines on deploying both Operations Manager and Service Monitor, see the *Deployment Best Practices Guide for Cisco Unified Operations Manager 2.0* located on Cisco.com at http://www.cisco.com/en/US/products/ps6535/products_installation_and_configuration_guides_list.html.

Table 1-1 Server System Requirements for Operations Manager (with Service Monitor)

Description	Specification		
Server Requirements			
System Parameters	Small Deployment (Up to 1,000 Phones)	Medium Deployment (Up to 10,000 Phones)	Large Deployment (Up to 30,000 Phones)
Processor	<ul style="list-style-type: none"> Intel Pentium or Xeon processor equal to or greater than 2 GHz or AMD Opteron processor equal to or greater than 2 GHz 	<ul style="list-style-type: none"> Dual Intel Pentium or Xeon processor equal to or greater than 3 GHz or Dual AMD Opteron processor equal to or greater than 3 GHz 	<ul style="list-style-type: none"> Dual Intel Pentium or Xeon processor equal to or greater than 3 GHz or Dual AMD Opteron processor equal to or greater than 3 GHz
Memory (RAM)	4 GB.	4 GB.	4 GB.
Page File Space	4 GB.	4 GB.	4 GB.
Disk Space ¹	<ul style="list-style-type: none"> 60 GB recommended. NTFS file system (required for secure operation). At least 16 MB in Windows temporary directory (%TEMP%). 	<ul style="list-style-type: none"> 72 GB recommended. NTFS file system (required for secure operation). At least 16 MB in Windows temporary directory (%TEMP%). 	<ul style="list-style-type: none"> 72 GB recommended. NTFS file system (required for secure operation). At least 16 MB in Windows temporary directory (%TEMP%).
Hardware	<ul style="list-style-type: none"> Color monitor. CD-ROM drive. Support one or two 10/100 NICs (one is required, and the second is for failover support; both NIC cards must have the same IP address). 		
Software ^{2, 3}	<ul style="list-style-type: none"> One of the following: <ul style="list-style-type: none"> Windows Server 2003 with Service Pack (SP) 1 or SP 2, Standard and Enterprise Editions. Windows Server 2003 R2. ODBC Driver Manager⁴ 3.5.10 or later. <p>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 2-17.</p> <p>Note Windows Terminal Services is supported in remote administration mode only.</p>		

- Do not install Operations Manager on a FAT file system.
- 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.
- The default locale for your Windows operating system must be set to either US-English or Japanese.
- 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.

Client Requirements

Table 1-2 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 1-2).

Table 1-2 Client System Requirements

Requirement Type	Minimum Requirements
System hardware	<ul style="list-style-type: none"> Any PC or server platform with a Pentium processor greater than 1.0 GHz. Color monitor with video card set to 24 bits color depth. Screen resolution of 1024 x 768 dpi. <p>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.</p>
System software	<ul style="list-style-type: none"> One of the following: <ul style="list-style-type: none"> Windows XP with Service Pack 2. Windows Server 2003 Standard or Enterprise Edition without Windows Terminal Services. Windows Server 2003 R2 Internet Explorer 6.0.28, or 6.0.37. Adobe Flash Player 7.0 or higher. <p>Note 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.</p>
Memory (RAM)	1 GB recommended.
Page file space	2 GB.
Environment	<p>Clients must be able to access Operations Manager:</p> <ul style="list-style-type: none"> From outside a firewall—Refer to documentation for your firewall for how to configure client access. Across a Virtual Private Network (VPN)—The VPN tunnel should connect the client and a VPN router or similar device.

Other System Software

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, but 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 1-3 lists the maximum capacity of Operations Manager when it is installed on system that meets the system requirements for a large deployment (see Table 1-1).

Table 1-3 System Capacity

System Parameters	Small Deployment (Up to 1,000 Phones)	Medium Deployment (Up to 10,000 Phones)	Large Deployment (Up to 30,000 Phones)
Devices (voice devices).	1,000	2,000	2,000
IP Phones.	<1,000	1,000 to 10,000	10,000 to 30,000
Access ports ^{1,2}	1,000	10,000	30,000
Trunk ports and interfaces. ²	1,500	4,500	7,000
Cisco Unified Communications Manager clusters.	30	30	30
Cisco Unified Communications Manager Express and Cisco Unity Express.	500	500	500
Route lists and route groups.	600	600	600
Phone status tests.	250	500	1000
Synthetic tests.	100	250 (150 end-to-end and 100 dial tone tests)	500
Node-to-Node tests.	100	250	500
SRST monitoring.	100	500	1,000
Sustained events (4 minute polling interval).	75	75	75
Burst events (4 minute polling interval).	300	300	300
Service Quality traps (4 minute polling interval).	75	75	75
Concurrent client (browser) logins.	5	5	5

1. Operations Manager does not manage the access port by default (recommended). However, it discovers the phones connected to these ports.
2. You can use the `sm_tpmgr` command to view the number of ports/interfaces in your inventory. See the tip below for information on how to use this command in Operations Manager.



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.

Supported Devices

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.



CHAPTER 2

Installing, Uninstalling, and Upgrading Cisco Unified Operations Manager

Revised: June 5, 2008

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



Note

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

This chapter includes the following:

- [Preparing to Install Operations Manager, page 2-1](#)
- [Performing a New Installation, page 2-7](#)
- [Reinstalling Operations Manager, page 2-10](#)
- [Uninstalling Operations Manager, page 2-11](#)
- [Upgrading to Cisco Unified Operations Manager 2.0.3, page 2-12](#)

Preparing to Install Operations Manager

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

- Make sure that hardware and software requirements for the server are met. (See [Server Requirements, page 1-2](#).)
- 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 2-3](#).)
- Determine whether your existing applications are already using ports that Operations Manager or Cisco Unified Service Monitor (Service Monitor) uses. (Existing applications should not use the ports that Operations Manager or Service Monitor use.) See [Verifying TCP and UDP Ports that Operations Manager Uses, page 2-5](#).

- Gather information that you might need to provide during the Operations Manager installation. (See [Gathering Information to Provide During Installation, page 2-6.](#))

Preparing the Operations Manager Server

Before installing Operations Manager, do the following:

- Set up the correct date and time on the system. Changing the date and time after installation can cause Operations Manager not to work, because it is perceived as a license violation. Also, the self-signed certificates generated during installation become invalid.
- The drive that you choose to install Operations Manager on must be an NTFS file system.
- If you are using an IBM server with IBM director installed, you must stop the ibm director wmi cim server and change the service to manual, or disable it. If you do not, the Service Level View in Operations Manager will not work.
- Clean the temp directory. You can open the temp directory by typing `%temp%` in a Windows Explorer window.
- If Windows Data Execution Prevention (DEP) is enabled, it can prevent the installation from completing. To check whether DEP is enabled and to disable it, see [Checking for and Temporarily Disabling DEP, page 2-2.](#)
- The fully qualified Domain Name of the system on which Operations Manager is installed must be DNS resolvable. The IP address must be resolvable to the DNS and the DNS must be resolvable to the IP address (Forward and Reverse Lookup, in DNS terms). To check name resolution on the Operations Manager server; in a command prompt, run the command `<NMSROOT>\bin>smNameRes.exe.`



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

- Operations Manager uses ICMP ping to determine the reachability of all devices. Some security applications may detect burst of ICMP pings as being caused by a malicious application. The security application may then block the ping requests. This can cause Operations Manager to generate a flood of false unreachable events. To avoid this situation, you should configure security applications so they do not block bursts of ICMP pings from the Operations Manager server.
- If you have Cisco Secure Agent (CSA) installed on your system, and the CS Agent is running, you must shut it down before installing or upgrading Operations Manager.

Checking for and Temporarily Disabling DEP

Step 1 Log in to the machine on which you will install Operations Manager as an administrator or a member of the Administrators group.



Note If your computer is connected to a network, network policy settings might prevent you from completing this procedure.

Step 2 Open System Properties by right-clicking the My Computer icon on your desktop and selecting Properties.

- Step 3** Click the Advanced tab and, under Performance, click Settings.
- Step 4** Click the Data Execution Prevention tab. If **Turn on DEP for all programs and services except those I select is selected**, DEP is enabled.
- Step 5** Select **Turn on DEP for essential Windows programs and services only**.
- Step 6** Click **OK**.
- Step 7** If you modified any DEP settings, reboot your machine so the new settings take effect.



Note After the installation completes, you can enable DEP.

Enabling DEP

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

-
- Step 1** Log in as an administrator or a member of the Administrators group.
- Step 2** Open System Properties by right-clicking the My Computer icon on your desktop and selecting Properties.
- Step 3** Click the Advanced tab and, under Performance, click **Settings**.
- Step 4** Click the Data Execution Prevention tab.
- Step 5** Select **Turn on DEP for all programs and services except those I select**.
- Step 6** To turn off DEP for a program, select the check box next to the program name and click **OK**. If the name of the program doesn't appear in the list, click **Add**, navigate to your Program Files folder, select the executable file (file with a .exe file extension) and click **OK**.



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

- Step 7** Click **OK**.
- Step 8** If you modified any DEP settings, reboot your system so the new settings take effect.
-

Preparing Devices for Addition to Operations Manager Inventory

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

Before adding devices to Operations Manager, do the following:

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

Device-Specific Configurations

Cisco Unified Communications Manager:

- Make sure that SNMP read access is configured on the Cisco Unified Communications Manager system.
- Provide the HTTP username and password for AXL access. This is the same username and password that is used for the Cisco Unified Communications Manager Administration page.
- If the Cisco Unified Communications Manager Administration page has HTTPS enabled, make sure HTTPS is enabled on all AXL directories.
- For all 5.x (and greater) Cisco Unified Communication Managers, make sure that the SOAP-Performance Monitoring API is running on all nodes and that the AXL service is activated on the first node (Publisher).
- For all 3.x and 4.x Cisco Unified Communication Managers, make sure that the IIS service is enabled.

Cisco Unified Contact Center and Cisco Unity:

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

IPSLA Devices:

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

All Other Devices:

- Make sure that SNMP read access is configured.

Actions to Take Before Adding Devices

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



Note

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

Verifying TCP and UDP Ports that Operations Manager Uses

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


Note

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

Operations Manager uses the following TCP and UDP ports.

Table 2-1 Ports that Operations Manager Uses

Port Numbers	Service Name	Application
161	Simple Network Management Protocol (SNMP)	Common Services
162	Trap receiving (standard port)	Common Services
514	Syslog	Common Services
40000-41000	Used by Common Transport Mechanism for internal application messaging	Operations Manager
42344	Used by Synthetic Testing web service	Operations Manager
42350-42353	Used by messaging software	Operations Manager
43445	Used by Alert History database engine	Operations Manager
43446	Used by inventory service database engine	Operations Manager
43447	Used by event processing database engine	Operations Manager
43449	Used by IP Phone Information Facility database engine	Operations Manager
8080	Used to determine if the Cisco Unified Communications Manager 5.0 web service is up. Note This port must be made available to Operations Manager.	Operations Manager
9000	Trap receiving CSListener (Operations Manager server if port 162 is occupied)	Operations Manager
9002	DynamID authentication (Operations ManagerBroker)	Operations Manager
9009	Default port number used by the IP telephony server for receiving traps from the device fault server	Operations Manager

Table 2-2 Ports that Service Monitor Uses

Port Numbers	Service Name
53	DNS
67 and 68	DHCP

Table 2-2 Ports that Service Monitor Uses (continued)

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

Gathering Information to Provide During Installation

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


Note

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

- User Admin password
- System Identity Account password
- Casuser password (custom installation only)
- Guest password (custom installation only)
- Common Services database password (custom installation only)
- Web server information (custom installation only)
- License information—Location of the license file. If you have already obtained a license file, provide the path. If not, be sure to obtain one. You can do so before or after you install Cisco Unified Operations Manager; see [Licensing Process, page A-3](#).


Note

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


Note

If you are installing Operations Manager for evaluation purposes:

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

Performing a New Installation

The installation process takes approximately sixty minutes to complete.

Follow these guidelines when installing Operations Manager:

- Operations Manager requires a dedicated system; do not install it on a system with:
 - Third-party management software (such as HP OpenView or NetView).
 - Cisco Secure Access Control Server (ACS).
 - Any Cisco applications other than those that are documented to be able to coexist with Operations Manager.
- The system where Operations Manager is to be installed must be configured for DNS.
- If you want to monitor Operations Manager using a third-party SNMP management tool, see [Configuring Your System for SNMP Queries, page 2-17](#).
- Do not install Operations Manager on:
 - A Primary Domain Controller (PDC) or Backup Domain Controller (BDC)
 - A FAT file system.
 - A Windows Advanced Server with Terminal Services enabled in application server mode.
 - A system with Internet Information Services (IIS) enabled.
 - A system that does not have name lookup.
- Do not select an encrypted directory. Operations Manager does not support directory encryption.
- Do not install any CiscoWorks Common Services 3.0 service packs on Operations Manager.
- Do not install on any of your voice application servers or on a Cisco Unified Communications Manager server.
- Verify that the system date and time are set properly.
- To speed up installation, disable all virus-scan software while installing.
- You should exclude the NMSROOT/databases directory from virus scanning. Problems can arise if database files are locked because of virus scanning.
- Your system's IP address and hostname should be set before installation.
- If you are going to use Cisco Unified Service Monitor (which is installed when you install Operations Manager), the clocks on Service Monitor and Cisco Unified Communications Manager servers must be synchronized. See [NTP Configuration Notes, page 2-17](#).
- If Windows Data Execution Prevention (DEP) is enabled, it can prevent the installation from completing. To check whether DEP is enabled and to disable it, see [Checking for and Temporarily Disabling DEP, page 2-2](#).
- Moving your Operations Manager server from Windows Workgroup to Domain is not supported.

Step 1 Make sure your system meets these prerequisites:

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

For system requirements, see [Server Requirements, page 1-2](#).

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

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



Note If the CD-ROM is already in the CD-ROM drive and you stopped the installation process to close programs or if Autostart is disabled, click **Setup.exe** to restart the process.

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

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

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

Step 7 Select one of the following, and then click **Next**:

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



Note For instructions on obtaining a license file, see [Licensing Process, page A-3](#).

The Setup Type window appears.

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

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

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

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

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

Step 10 Do one of the following:

- Click **Next** to accept the default installation directory.
- Browse to the folder where you would like to install Operations Manager, and click **Next**.

The installation program checks dependencies and system requirements.

The System Requirements window displays the results of the requirements check and advises whether the installation can continue. One of the following might occur:

- If there is not enough disk space for the installation, or if memory requirements are not met, the installation program displays an error message and stops. (See [Server Requirements, page 1-2](#).)
- If the minimum recommended requirements are not met, the installation program displays a warning message and continues installing.

Step 11 Click **Next**.

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



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

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

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

The Summary window appears, displaying the current settings.

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

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

- If the system has more than one NIC card and more than one IP address configured, you will see this message:

```
This machine is multihomed. Please update the MULTI-HOME properties section in
C:\PROGRA~2\CSCOpX\lib\vbroker\gatekeeper.cfg after the installation is complete.
```



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

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

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



Caution This message may not display 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 2-17](#).

Step 17 Eject the CD.



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

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

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

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

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

**Note**

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

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

Reinstalling Operations Manager

- Step 1** Close all open or active programs. Do not run other programs during the reinstallation process.
- Step 2** As the local administrator, log in to the machine on which you will install the Cisco Unified Operations Manager software, and insert the Cisco Unified Operations Manager CD-ROM into the CD-ROM drive. The installer window appears, asking you if you want to reinstall Cisco Unified Operations Manager.

**Note**

If the CD-ROM is already in the CD-ROM drive and you stopped the reinstallation process to close programs or if Autostart is disabled, click **Setup.exe** from the top directory of your CD-ROM to restart the process.

- Step 3** Click **Install**. The Welcome window appears.
- Step 4** Click **Next**. The Software License Agreement window appears.
- Step 5** Click **Accept**. The Setup Type window appears.
- Step 6** Select **Typical** or **Custom**.
- Step 7** Click **Next**. The Backup Data window appears.
- Step 8** Enter or browse to the location where you want the backup of your previous version of Operations Manager stored, and click **Next**.
- Step 9** The System Requirements window displays the results of the requirements check and advises whether the reinstallation can continue; click **Next**.
- Step 10** If you chose Custom installation you will be asked to enter the casuser password. This step is not required for Typical installation. Click **Next**.
- Step 11** An information dialog box appears, confirming reinstallation; click **OK**. The Summary window appears, displaying the current settings.
- Step 12** Click **Next**. The installation proceeds.
- Step 13** Remove the Cisco Unified Operations Manager CD from the drive.

**Note**

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

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

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

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

Uninstalling Operations Manager



Caution

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



Note

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

Step 1 As the local administrator, log in to the system on which Cisco Unified Operations Manager is installed.

Step 2 To start the uninstallation process, from the Windows desktop select **Start > All Programs > Cisco Unified Operations Manager > Uninstall Cisco Unified Operations Manager**.

Step 3 Select the components you want to uninstall.

Step 4 Click **Next** to begin uninstalling the selected components.

A window appears, listing the components selected for uninstallation.

Step 5 Click **Next**.

Messages showing the progress of the uninstallation appear.

The following message appears:

Uninstallation is complete. Click OK to finish.

Step 6 Click **OK**.

Upgrading to Cisco Unified Operations Manager 2.0.3

Operations Manager supports the following upgrade paths:

- Upgrade from a licensed copy of Cisco Unified Operations Manager 2.0.2 to an purchased copy of Cisco Unified Operations Manager 2.0.3.
- Upgrade from a licensed copy of Cisco Unified Operations Manager 2.0.2 to an evaluation copy of Cisco Unified Operations Manager 2.0.3.



Caution

There is no direct upgrade from releases prior to 2.0.2. See [Upgrading from Operations Manager Releases Prior to 2.0.2 to Operations Manager 2.0.2, page 2-16](#) for details on how to proceed.



Tip

To download Cisco Unified Operations Manager 2.0.2, go to Cisco.com for the software download at <http://www.cisco.com/cgi-bin/tablebuild.pl/cuom202>.



Note

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

To upgrade from Cisco Unified Operations Manager 2.0.2, see [Upgrading from Operations Manager 2.0.2 to Operations Manager 2.0.3, page 2-13](#).

If you have a version of Cisco Unified Operations Manager prior to 2.0.2, see [Upgrading from Operations Manager Releases Prior to 2.0.2 to Operations Manager 2.0.2, page 2-16](#).



Note

If you are upgrading from Operations Manager 2.0.2, there is no change in the Service Monitor version.

There are two levels of functionality that you can purchase for Operations Manager 2.0.3: Premium Edition and Standard Edition. To get full Operations Manager functionality, you must upgrade to Operations Manager Premium Edition.

Before You Begin

- Before upgrading, back up your existing Synthetic Tests and Batch Tests by exporting them to a file. If you lose the tests after upgrade, you can use the backup files to recreate the tests on your upgraded system.
- Make sure your system meets the system requirements (see [Server Requirements, page 1-2](#)).
- Close all open or active programs. Do not run other programs during the upgrade process.
- If Operations Manager has been running for a long period of time and has accumulated a large amount of data (database over 1 GB), you should run an independent backup before upgrading. Also, during installation, do not run the backup data process. You can use Windows Explore to view the database size (Operations Manager's databases are located in the <NMSROOT>\databases folder).



Note

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

- If you are using Service Monitor or plan on using it, you should be aware of the following:
 - If you plan on using Service Monitor to monitor MOS reported from Cisco Unified Communications Managers, configure the server to use NTP before you upgrade. For more information, see [NTP Configuration Notes, page 2-17](#).
 - It is recommended that you delete existing sensor configuration files—one QOVDefault.CNF file and a QoVMACAddress.CNF file for each sensor—from your existing TFTP servers before you perform the upgrade. Immediately after you upgrade to the Service Monitor 2.0.1 software, sensors are unable register to Service Monitor until you perform post-upgrade configuration steps; for more information, see [Service Monitor Post-Upgrade Configuration, page 2-15](#).
- If Windows Data Execution Prevention (DEP) is enabled, it can prevent the installation from completing. To check whether DEP is enabled and to disable it, see [Checking for and Temporarily Disabling DEP, page 2-2](#).
- If you have Cisco Secure Agent (CSA) installed on your system, and the CS Agent is running, you must shut it down before installing or upgrading Operations Manager.

Upgrading from Operations Manager 2.0.2 to Operations Manager 2.0.3



Note

On a typical 4 GB memory server, Microsoft Windows only detects ~3.3 GB of memory (even though system has 4 GB installed). The installation will warn you that system memory is insufficient. You may ignore this memory warning message when you know your server has sufficient memory installed.

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

Step 2 Insert the Cisco Unified Operations Manager CD-ROM into the CD-ROM drive. The Cisco Unified Operations Manager Setup Program window opens.



Note

If the CD-ROM is already in the CD-ROM drive and you stopped the installation process to close programs or if Autostart is disabled, click **Setup.exe** to restart the process.

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

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

Step 5 Click **Accept**.

The Setup Type window appears.

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

Step 7 The System Requirements window displays the results of the requirements check and advises whether the upgrade can continue; click **Next**.



Note

If memory requirements are not met, installation cannot proceed. See [Server Requirements, page 1-2](#).

Step 8 If you chose Custom installation, you can change any of the following:

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

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

Step 9 The Summary window appears, displaying the current settings. Click **Next**. The installation proceeds.

Step 10 Click **OK** to confirm additional messages if they are displayed:

- If the system has more than one NIC card and more than one IP address configured, you will see this message:

```
This machine is multihomed. Please update the MULTI-HOME properties section in
C:\PROGRA~2\CSCOpX\lib\vbroker\gatekeeper.cfg after the installation is complete.
```



Caution

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

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

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

Click **OK**. (For more information, see [NTP Configuration Notes, page 2-17](#).)

Step 11 Remove the Cisco Unified Operations Manager CD from the drive.



Note

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

Step 12 Click **Finish** to reboot the machine.

Step 13 Wait 30 minutes after the system reboots before starting Operations Manager. This gives all of Operations Manager's processes time to initialize.

Step 14 Verify the upgrade by starting Operations Manager.

Step 15 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 16 If you disabled DEP before the installation, see [Enabling DEP, page 2-3](#).

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

Service Monitor Post-Upgrade Configuration

This section provides the minimum steps required to enable sensors to register with Service Monitor 2.0.1. For complete configuration procedures, including how to add Unified Communications Managers to Service Monitor, see the configuration checklists in *User Guide for Cisco Unified Service Monitor*.

-
- Step 1** Start Service Monitor.
- Step 2** If you are upgrading from Service Monitor 2.0, you can skip to [Step 3](#); otherwise, add at least one TFTP server to Service Monitor:
- Select **Configuration > Sensor > TFTP Servers**. The TFTP Server Setup page appears.
 - Click **Add**. The TFTP Server Settings dialog box appears.
 - Enter data in the following fields:
 - TFTP Server—IP address or DNS name.
 - Port Number—The default port number is 69.
 - Click **OK**.



Note If you want to use a Unified Communications Manager 6.x, 5.x, or 4.2 as a TFTP server, you can do so.

- Step 3** Configure the default configuration file:
- Select **Configuration > Sensor > Setup**. The Setup page appears.
 - Update the Default Configuration to TFTP Server fields:
 - Image Filename—Enter SvcMonAA2_40.img.
 - Primary Service Monitor—Enter an IP address or DNS name.
 - Secondary Service Monitor—(Optional) Enter an IP address or DNS name.
 - Click **OK**. Operations Manager stores the default configuration file locally and copies it to the TFTP servers that you added in [Step 2](#).
 - Copy the binary image file, SvcMonAA2_40.img, from *NMSROOT*\ImageDir on the Service Monitor server to the root location on the TFTP server. (*NMSROOT* is the directory where Service Monitor is installed; its default location is C:\Program Files\CSCOPx.)
 - Verify that the newly created QOVDefault.CNF file is on the TFTP server. If it is not, upload it to the root location on the TFTP server from the Service Monitor image file directory, *NMSROOT*\ImageDir.

**Note**

If you use Unified Communications Manager as a TFTP server, Service Monitor cannot copy configuration files to Unified Communications Manager due to security settings on the latter. You will need to manually upload the configuration file as described in [Step 3](#). After uploading the configuration file, reset the TFTP server on Unified Communications Manager. For more information, see Unified Communications Manager documentation.

Step 4

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

**Warning**

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

Upgrading from Operations Manager Releases Prior to 2.0.2 to Operations Manager 2.0.2

There is no direct upgrade from Operations Manager 1.1, 2.0, or 2.0.1 to Operations Manager 2.0.3. If you are moving from any of these versions of Operations Manager, you must first upgrade to Operations Manager 2.0.2, then upgrade to Operations Manager 2.0.3.

**Caution**

If you do upgrade directly from 2.0.1 to 2.0.3, a warning that this upgrade is not supported should be displayed; however, this message does not appear. The installation completes even though this upgrade should not be allowed. To ensure safe migration of your Operations Manager 2.0.1 data, you must upgrade from 2.0.1 to 2.0.2 before you upgrade to Operations Manager 2.0.3.

**Tip**

Go to <http://www.cisco.com/cgi-bin/tablebuild.pl/cuom202> to download Cisco Unified Operations Manager 2.0.2 before upgrading to 2.0.3.

Changes to Notification Event Customization Severity After Upgrade

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

[Table 2-3](#) list the severity levels for both, before and after upgrade.

Table 2-3 Notification Event Customization Severity

Operations Manager 2.0	Operations Manager 2.0.2/2.0.3
0—Critical	3—Critical
1—Warning	2—Warning
2—Informational	1—Informational
3—Undefined	8—Undefined

Table 2-3 Notification Event Customization Severity (continued)

Operations Manager 2.0	Operations Manager 2.0.2/2.0.3
4—Undefined	4—Undefined
5—Undefined	5—Undefined
6—Undefined	6—Undefined
7—Undefined	7—Undefined

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.

In order for Operations Manager to manage itself, install and configure SNMP in 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 © 2007, 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, page 3-1](#)
- [Starting Operations Manager, page 3-19](#)
- [Understanding and Configuring Security, page 3-20](#)
- [Supported NMS Integration, page 3-21](#)
- [Configuring SNMP Trap Receiving and Forwarding, page 3-21](#)
- [Configuring Cisco Unified Communications Manager for Use with Operations Manager, page 3-24](#)
- [Viewing Alerts, page 3-24](#)
- [What's Next?, page 3-25](#)

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:\Program Files\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
<ul style="list-style-type: none"> Deploying Operations Manager as an independent server. Automatically synchronizing your inventory with the DCR. 	<p>Add devices from the DCR using automatic synchronization. Automatic synchronization is the default setting, and you do not need to do anything.</p> <p>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.</p>
<ul style="list-style-type: none"> Deploying Operations Manager as an independent server. Manually controlling the devices that are added to inventory. 	<p>Manually add devices from the DCR. See Adding Devices Manually from the DCR to Operations Manager, page 3-10.</p>
<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> Deploying Operations Manager with LMS. Synchronizing the Operations Manager DCR with an existing master DCR. Automatically synchronizing your inventory with the DCR. 	<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> Deploying Operations Manager with LMS. Synchronizing the Operations Manager with an existing master DCR. Manually controlling the devices managed by Operations Manager. 	<ul style="list-style-type: none"> 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 all applications.



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.)

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 Select *one* of the following options:

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

- b.** 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	<p>(Optional) Enter comma-separated IP addresses or IP address ranges for devices that you want to:</p> <ul style="list-style-type: none"> • Include—In the auto-discovery process. • Exclude—From the auto-discovery process. <p>You can use wildcards when specifying the IP address range.</p> <p>An asterisk (*) denotes the octet range of 1-255. Also, the octet range can be constrained using the [xxx-yyy] notation.</p> <p>For example:</p> <ul style="list-style-type: none"> • 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]. <p>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.</p>

Table 3-2 Physical Discovery Filters (continued)

Filter	Description
DNS Domain	<p>(Optional) Enter comma-separated DNS domain names for devices that you want to:</p> <ul style="list-style-type: none"> • Include—In auto-discovery processing. • Exclude—From auto-discovery processing. <p>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:</p> <ul style="list-style-type: none"> • *.cisco.com matches any DNS name ending with .cisco.com. • *.?abc.com matches any DNS name ending with .aabc.com, .babc.com, etc.
SysLocation	<p>(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:</p> <ul style="list-style-type: none"> • Include—In auto-discovery processing. • Exclude—From auto-discovery processing. <p>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.</p>

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.	<ul style="list-style-type: none"> SNMP information is not configured. Device is not responding. Device is not reachable. Device credentials are not correct. 	Unreachable.
Inventory collection in progress.	<ul style="list-style-type: none"> The device model is not recognized. The software version is not supported. 	Unsupported

Verifying Devices Added to Operations Manager

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.

Starting the Service Level View

-
- 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, 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, 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. <ul style="list-style-type: none"> • If the IP address is missing: <ul style="list-style-type: none"> – 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 will go into the partially monitored state. Verify that this 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 ccm 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 any of: <ul style="list-style-type: none"> • 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: HTTPSertificateNotImported	The Cisco Unified Communications Manager certificate has failed.	Do the following: <ol style="list-style-type: none"> 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: <code>keytool -list -keystore <NMSROOT>\CSCOpX\lib\jre\lib\security\cacerts</code> 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. This is done through the Modify/Delete Devices page.

**Note**

You can also change device credentials directly through 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, 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 (for client system requirements, see [Table 1-2](#)).

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 a Service Monitor to Operations Manager

Use this procedure to add a locally installed or remotely installed Service Monitor to Operations Manager.

-
- Step 1** Select **Administration > Service Quality Settings > Service Monitors**. 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.
 - 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.
- Security on the CiscoWorks server—You can configure the following aspects of security for the server on which Operations Manager resides: **Local security or Cisco Secure ACS**—Access to tasks within Operations Manager is either controlled by local security, or provided by Common Services or Cisco Security ACS. Local security is enabled on the server by default. Operations Manager supports integration with Cisco Secure ACS. For more information, see [Configuring Operations Manager with Cisco Secure ACS, page B-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. You can enable or disable SSL depending on the need to use secure access. Operations Manager supports SSL between clients and the server.



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

Supported NMS Integration

Operations Manager supports integration with network management systems (NMSs) as follows:

- Operations Manager listens for traps from managed devices on port 162 (the default). If another NMS on the system with Operations Manager uses port 162:
 - The installation script warns you that this is the case.
 - You must specify a different port for Operations Manager trap receiving after the installation completes. See [Integrating Operations Manager Trap Receiving with NMSs or Trap Daemons](#), page 3-23.
- 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*.

If the standard User Datagram Protocol (UDP) trap port (162) is being used by another NMS, you must configure Operations Manager SNMP trap receiving to use a different UDP port, such as port 9000. See [Configuring SNMP Trap Receiving and Forwarding](#), page 3-21.

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 (for example, to port 9000), 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 2-5](#).

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 3-22](#)

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.
 - Step 2** Select **Products & Solutions > Cisco IOS Software**.
 - Step 3** Select the Cisco IOS Software release version used by your Cisco IOS-based devices.
 - Step 4** Select **Technical Documentation** and select the appropriate command reference guide.
-

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 & Solutions > Switches**.
- Step 3** Select the appropriate Cisco Catalyst series switch.
- Step 4** Select **Technical Documentation** and select the appropriate command reference guide.
-

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 another NMS is already listening for traps on the standard UDP trap port (162), you must configure Operations Manager to use another port, such as port 9000. See [Updating the SNMP Trap Receiving Port, page 3-21](#).
- 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.	<ul style="list-style-type: none"> • 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. • 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.	<ul style="list-style-type: none"> • 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 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.

Setting HTTP Credentials on Cisco Unified Communications Manager

Operations Manager uses the AVVID 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 task 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**

Licensing

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

- [Licensing Overview, page A-1](#)
- [Licensing Reminders, page A-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 determine whether Operations Manager is licensed, see [Verifying License Status, page A-1](#). If you do not have a license or you want to upgrade your license, see [Licensing Scenarios, page A-2](#).

Verifying License Status

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

-
- Step 1** Select the CiscoWorks link in the upper right-hand 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— <i>A.b.c</i> , where <i>A</i> is the major version number, <i>b</i> is the minor version number, and <i>c</i> is the service pack number. For example, OM 2.0.0 indicates version 2.0 without service packs.
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: <ul style="list-style-type: none"> • Purchased—You have a registered, licensed product. • Evaluation—This license will expire on the expiration date; Operations Manager 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.

Licensing Scenarios

[Table A-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 A-1 How to Obtain and Register a License

Scenario	What to do
Installing with a purchased license.	<ol style="list-style-type: none"> Before installing, obtain a license file. See Licensing Process, page A-3. <p>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 A-4.</p> <ol style="list-style-type: none"> 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.	<p>During installation, select Evaluation Only. Evaluation versions are active for 90 days, before you are required to purchase a license.</p> <p>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 A-3.</p>
Getting a license for additional devices (either upgrading from an evaluation license, or increasing the number of supported devices).	<p>See Licensing Process, page A-3.</p> <p>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.</p>
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 30,000 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:

- 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 A-4](#).
- 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 A-4](#).

3. Copy the license file to 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 A-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

-
- 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-hand 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 crmdmgmt
net start crmdmgmt
```

Licensing Reminders

Operations Manager provides reminders in the following circumstances:

- [Evaluation Version: Before Expiry, page A-5](#)
- [Purchased Version: No License File, page A-5](#)
- [Purchased Version: Device Limit Exceeded, page A-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 A-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 A-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 **B**

Configuring Operations Manager with Cisco Secure ACS

This section describes how to configure Operations Manager with Cisco Secure ACS:

- [Login Module, page B-1](#)
- [Authentication Roles, page B-2](#)
- [Before You Begin: Integration Notes, page B-3](#)
- [Configuring Operations Manager on Cisco Secure ACS, page B-4](#)
- [Verifying the Operations Manager and Cisco Secure ACS Configuration, page B-4](#)

Login Module

Common Services provides security mechanisms for authenticating users of applications. You can configure the login module to use one of the following modes of user authentication and authorization:

- **Non-ACS**—In this mode, the Operations Manager server provides authentication and authorization services.
- **ACS**—In this mode, a Cisco Secure Access Control Server (ACS) provides authentication and authorization services. To use this mode, you must have a Cisco Secure ACS installed on your network. The supported versions of Cisco Secure ACS for Windows are 3.2, 3.2.3, 3.3.2, 4.0.

If you are using ACS 3.2.3, we recommend that you install the Admin HTTPS PSIRT patch:

1. Go to <http://www.cisco.com/kobayashi/sw-center/ciscosecure/cs-acs.shtml>.
2. Click the Download Cisco Secure ACS Software (Windows) link. You will find the link to the Admin HTTPS PSIRT patch in the table.

You can integrate Operations Manager with Cisco Secure ACS only if they are installed on separate systems, because Operations Manager must be configured as an authentication, authorization, and accounting (AAA) client for Cisco Secure ACS.

In ACS mode, *fallback* is provided for authentication only. (Fallback options allow you to access Operations Manager if the login module fails, or you accidentally lock yourself or others out.) If authentication with ACS fails, Operations Manager does the following:

1. Tries authentication using non-ACS mode (CiscoWorks local mode).

2. If non-ACS authentication is successful, presents you with a dialog box with instructions to change the login mode to CiscoWorks local. (You can do so only if you have permission to perform that operation in non-ACS mode.)



Note You will not be allowed to log in if authentication fails in non-ACS mode.

For more information, see *User Guide for CiscoWorks Common Services* and Common Services online help.

Authentication Roles

In ACS mode, by default the Operations Manager server provides the five roles listed here, from least privileged to most privileged:

- **Help Desk**—A user with this role has the privileges to access network status information from the persisted data. This user does not have the privilege to contact any device or schedule a job that will reach the network.

For example, this user can search the Alert History database.

- **Network Operator**—A user with this role has the privilege to perform all tasks that involve collecting data from the network. The user can also perform all Approver tasks. The user does not have write access on the network.

For example, this user can configure logging parameters.



Note In Operations Manager, a user with this role by default can perform the same Operations Manager tasks as a Network Administrator.

- **Network Administrator**—A user with this role has the privilege to change the network. The user can also perform Network Operator tasks.

For example, this user can add devices to Operations Manager from the DCR.

- **System Administrator**—A user with this role has the privilege to perform all Operations Manager system administration tasks. See the Permissions report. From the Operations Manager home page, click **CiscoWorks** in the upper right-hand corner of the window, the CiscoWorks home page opens. Under Common Services, select Server > Reports > Permission Report.

For example, this user can configure SNMP trap forwarding (Administration > Preferences).



Note If you use Cisco Secure ACS to modify these roles, removing tasks or reassigning tasks from one role to another, the Permissions report will not reflect your changes.

You can modify roles on Cisco Secure ACS.

Step 1 Select **Shared Profile Components > Cisco Unified Operations Manager**.

Step 2 Click the Operations Manager role that you want to modify.

Step 3 Select the Operations Manager tasks that suit your business workflow and needs.

Step 4 Click **Submit**.



Note

If desired, you can also create new roles on Cisco Secure ACS.

Before You Begin: Integration Notes

This section contains notes that you should read before you begin Cisco Secure ACS and Operations Manager server integration:

- Operations Manager server and Cisco Secure ACS integration should be performed only *after* installing all applications.
- If you have installed your application after configuring the CiscoWorks Login Module to ACS mode, then the application users are not granted any permissions; however, the application is registered to Cisco Secure ACS. On the Cisco Secure ACS server, you must assign the appropriate permissions to the application.

See [Configuring Operations Manager on Cisco Secure ACS, page B-4](#).

- Multiple instances of the same application using the same Cisco Secure ACS will share settings. Any changes will affect all instances of that application.
- If an application is configured with Cisco Secure ACS and then that application is reinstalled, it will inherit the old settings.



Note

This is applicable if you are using Cisco Secure ACS version 3.2.3 or earlier.

- You must create roles in Cisco Secure ACS for each Operations Manager application that is running on the Operations Manager server.

For example, you must create roles in Cisco Secure ACS for Cisco Unified Service Monitor. These roles are not shared by any other Operations Manager application.

- The roles that you create in Cisco Secure ACS are shared across all servers that are configured to the same Cisco Secure ACS.

For example, you have configured 10 servers with a Cisco Secure ACS, and you have created a role in Cisco Secure ACS for Operations Manager (say, *CUOMSU*). This role is shared by Operations Manager applications running on all 10 servers.

- A user can have different access privileges for different Operations Manager applications.

For example a user, *CWSU*, can have the following privileges:

- System Administrator for Common Services
- Approver for RME
- Network Operator for Campus Manager
- Network Administrator for Operations Manager
- Help Desk for Internet Performance Monitor (IPM)

- In CiscoWorks, you must do the following:
 - Set AAA Mode to ACS—You will need to supply the following information, obtained from Cisco Secure ACS, to complete this task: IP address or hostname, port, admin username and password, and shared secret key.
 - Set up System Identity Setup username.
- On Cisco Secure ACS, you must configure a user with the same username as the CiscoWorks server System Identity Setup user. For Operations Manager, this user must have Network Administrator privileges on Cisco Secure ACS. For CiscoWorks applications, this user must have System Administrator privileges on Cisco Secure ACS.

See the chapter “Configuring the Server” in *User Guide for CiscoWorks Common Services* for details on configuring the CiscoWorks server in ACS mode.

Configuring Operations Manager on Cisco Secure ACS

After you complete setting the Operations Manager server to ACS mode with Cisco Secure ACS, perform the following tasks on Cisco Secure ACS:

1. Click **Shared Profile Components** to verify that the Cisco Unified Operations Manager application entry is present.

**Note**

If you integrated CiscoWorks Common Services with Cisco Secure ACS *before* installing Operations Manager, you must configure ACS mode again and register all applications with ACS. See the Common Services online help. Also, if Operations Manager is reinstalled, the configurations in Cisco Secure ACS are not lost. After re-registering Operations Manager with Cisco Secure ACS, the configurations available in Cisco Secure ACS will be inherited by Operations Manager.

2. Based on your authentication setting (per user or per group) on Cisco Secure ACS, click either User Setup or Group Setup.

On Cisco Secure ACS, verify the per-user or per-group setting for Cisco Unified Operations Manager using **Interface Configuration > TACACS + (Cisco IOS)**.

3. Assign the appropriate Operations Manager privileges to the user or group.

For Operations Manager, you must ensure that a user with the same name as the CiscoWorks server System Identity Setup user is configured on Cisco Secure ACS and has Network Administrator privileges.

Verifying the Operations Manager and Cisco Secure ACS Configuration

After performing the tasks in [Configuring Operations Manager on Cisco Secure ACS, page B-4](#), verify the configuration as follows:

1. Log in to Operations Manager with the 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 your privileges on Cisco Secure ACS.

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

- You should be able to view the device summary.
 - You should not be able to select devices for Operations Manager to manage.
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.



INDEX

A

adding

devices

manually to Operations Manager [3-10](#)

to the DCR from Operations Manager [3-5](#)

phone discovery schedule [3-13](#)

Adobe flash [1-4](#)

authentication

ACS mode [B-1](#)

non-ACS mode [B-1](#)

C

capacity, system [1-5](#)

Cisco IP Contact Center

preparing to add to Operations Manager [2-4](#)

Cisco Secure ACS [B-1](#)

Operations Manager, integration with [B-1, B-4](#)

Operations Manager, verifying integration [B-4](#)

supported versions [B-1](#)

Cisco Security Agent (CSA) disabling service prior to install or upgrade [2-2](#)

Cisco Unified Communications Manager

preparing to add to Operations Manager [2-4](#)

Cisco Unity

preparing to add to Operations Manager [2-4](#)

client requirements [1-4](#)

environment [1-4](#)

configuring Operations Manager

further configuration tasks [3-25](#)

NMS integration [3-21](#)

security [3-20](#)

SNMP trap receiving and forwarding, configuring

trap forwarding, configuring [3-23](#)

trap receiving port, updating [3-21](#)

traps, enabling devices to send [3-22](#)

to monitor devices [3-1](#)

adding a phone discovery schedule [3-13](#)

adding devices manually to Operations Manager [3-10](#)

adding devices to the DCR from Operations Manager [3-5](#)

configuring automatic device selection in Operations Manager [3-10](#)

configuring manual device selection in Operations Manager [3-10](#)

configuring the DCR in master and slave mode [3-4](#)

device states [3-11](#)

editing the device inventory collection schedule [3-13](#)

scheduling inventory collection [3-12](#)

verifying device import [3-12](#)

with Cisco Secure ACS [B-4](#)

with Cisco Secure ACS, verifying [B-4](#)

D

Data Execution Prevention (DEP)

disabling [2-2](#)

DEP setting [2-3](#)

device import

error messages [3-14](#)

supported NMS environments [3-3](#)

troubleshooting [3-13](#)

verifying [3-12](#)

device inventory collection schedule, editing [3-13](#)

devices

- inventory collection [3-18](#)

- supported [1-6](#)

device selection in Operations Manager [3-10](#)

discovery

- physical, running [3-5, 3-7](#)

DNS resolution [3-14](#)

drive space requirements on the server

- Operations Manager with Service Monitor [1-3](#)

E

editing the device inventory collection schedule [3-13](#)

error messages, inventory collection [3-14](#)

H

hardware requirements

- client [1-4](#)

- Operations Manager with Server Monitor [1-3](#)

- server with Operations Manager and Service Monitor [1-3](#)

I

importing devices (see device import)

installing Operations Manager [2-7 to 2-10](#)

- preparation for [2-1, 2-4, 2-6](#)

- TCP and UDP ports used [2-5](#)

- preparing devices [2-3](#)

- Cisco IP Contact Center [2-4](#)

- Cisco Unified Communications Manager [2-4](#)

- Cisco Unity [2-4](#)

- IPSLA devices [2-4](#)

- preparing the server [2-2](#)

inventory collection, scheduling [3-12](#)

IP SLA devices

- preparing to add to Operations Manager [2-4](#)

IP Telephony Monitor

- moving from [2-13](#)

L

license

- how to obtain and register [A-2](#)

- levels that can be purchased [A-2](#)

- obtaining a license file [A-4](#)

- obtaining a PAK [A-4](#)

- overview [A-1](#)

- process [A-3](#)

- registering [A-4](#)

- registering a license file with Operations Manager [A-4](#)

- reminders [A-5](#)

- scenarios [A-2](#)

- verifying license status [A-1](#)

license file

- obtaining [A-4](#)

- registering [A-4](#)

logs

- Operations Manager installation [2-10](#)

- Operations Manager reinstallation [2-10, 2-11, 2-15](#)

M

memory (RAM) requirements

- client [1-4](#)

- Operations Manager standalone [1-3](#)

monitoring devices

- configuring Operations Manager for [3-1](#)

- configuring supported NMS environments for device import [3-2](#)

- getting started [3-2](#)

N

NMS integration [3-21](#)

NTP

configuration [2-17](#)

O

Operations Manager

installing [2-7 to 2-10](#)

overview [1-1](#)

preparing the server for installation [2-2](#)

reinstalling [2-10 to 2-11](#)

uninstalling [2-11](#)

upgrading from 2.0.2 [2-12 to ??](#)

P

page file

Operations Manager requirements [1-3](#)

space requirements

client [1-4](#)

PAK, obtaining [A-4](#)

Partially Monitored device state

caused by [3-15](#)

physical discovery

and ping sweep [3-5, 3-7](#)

and seed devices [3-5, 3-7](#)

ports

occupied [2-5](#)

viewing command for inventory [1-5](#)

preparing to install Operations Manager

client requirements [1-4](#)

server requirements and recommendations [1-2](#)

supported devices [1-6](#)

processor requirements

Operations Manager with Service Monitor [1-3](#)

R

RAM requirements

Operations Manager standalone [1-3](#)

recommendations

client [1-4](#)

disabling CSA [2-2](#)

server [1-2](#)

registering

license, Operations Manager [A-4](#)

reinstalling Operations Manager [2-10 to 2-11](#)

S

security

configuring [3-20](#)

login module [B-1](#)

server capacity [1-5](#)

server requirements [1-2](#)

drive space [1-3](#)

hardware [1-3, 1-4](#)

software [1-3](#)

service level view, starting [3-12](#)

Service Monitor

adding to Operations Manager [3-20](#)

post-upgrade configuration [2-15](#)

service packs, Windows [1-3](#)

client [1-4](#)

sm_tpmgr command [1-5](#)

SNMP

configuring

retries [3-17](#)

timeout [3-17](#)

timeout [3-14](#)

SNMP queries

configuring [2-17](#)

SNMP trap receiving and forwarding, configuring [3-21](#)

trap receiving port, updating [3-21](#)

traps, enabling devices to send [3-22](#)

traps forwarding, configuring [3-23](#)

software

tested with [1-4](#)

software requirements

- Operations Manager client [1-4](#)
- software server requirements
 - Operations Manager with Service Monitor [1-3](#)
- starting Operations Manager [3-19](#)
 - adding home page to internet explorer's trusted site zone [3-19](#)
- supported
 - Cisco Secure ACS versions [B-1](#)
 - client environments [1-4](#)
 - server environments [1-2](#)
- swap file
 - Operations Manager with Service Monitor [1-3](#)
 - space requirements
 - client [1-4](#)
- system capacity [1-5](#)

- users
 - authentication of [B-2](#)
 - roles [B-3](#)
 - System Identity Setup User [B-3](#)

T

- timeout
 - Data Collector [3-14](#)
 - SNMP [3-14](#)
 - configuring [3-17](#)
- traps, changing port [3-21](#)
- troubleshooting
 - device import [3-13](#)
 - device credentials, changing [3-17](#)
 - SNMP timeout and retries, modifying [3-17](#)

U

- UDP and TCP ports used by Operations Manager [2-5](#)
- uninstalling Operations Manager [2-11](#)
- Unreachable device state
 - caused by [3-16](#)
- upgrading
 - Operations Manager 1.1 [2-12](#)
 - upgrading from 2.0.2 [?? to 2-15](#)
 - upgrading from releases prior to 2.0.2 [2-16](#)
 - upgrading Operations Manager [2-12 to ??](#)