Cisco Prime Unified Operations Manager 8.7

Deployment Best Practices

For further information, questions and comments please contact ccbu-pricing@cisco.com

Contents

Introduction 4

Product Overview 4

Small and Medium Enterprises 6
Large Enterprises 7
Managed Service Providers 7

Preinstallation Tasks 7

Preparing Devices to Be Monitored by Operations Manager 8
Cisco IOS Devices 8
Cisco Catalyst Devices 9
Media Convergence Servers 11
SNMP Management of Cisco Unified Contact Center 13
Cisco Unified Communications Manager 15
Voice Gateway and MGCP 17
Cisco Unified Communications Manager Express and SRST 17
Cisco Unity 17
Cisco Unity Express 17
Preparing the Server for Operations Manager 19
Operating System 19
Hardening the Server 19
VMware Deployment 19
Miscellaneous 19
Hostname and IP Address 19
Client PC Macromedia Flash 20
Verify Locale Settings 20
DNS Settings 20
Verify Open Database Connectivity Driver Manager 20
Enabling/Installing Windows SNMP Service 21
Browser Version and Flash Plug-in 21
Device Connectivity 21
Terminal Server Services 21
Antivirus and Platform Agents 22
System Capacity 22
System Requirements 22
Preparing the Network 22
Register Devices and Interfaces in DNS 22
Configuring Cisco Unified Communications Manager Security Certificates 22
Check Routing and Firewalls 25
Network Time Protocol 25
Port Availability 25
Deployment Checklist 26

Operations Manager Installation 28

Preinstallation Checks 28
Installation Procedures 29
Licensing and Registration of the Software 29
Uninstallation 29

Initial Configuration 29

Security and Users 29
IP Address or Hostname Changes 29
Network Discovery and Device Management 29
Network Discovery Options 30
Device Import Options 33
Device Discovery Process 34
Diagnostic Tests 35
Synthetic Tests 35

Synthetic Test Descriptions and Expected Results 36
How Many Simulated IP Phones Do I Need? 37
Node-to-Node Tests 38
Batch Tests 39
Understanding Phone Tests 39
Resolving Batch Test Failure 41
Managing Alerts and Events 41
Notification Services 42
CISCO-EPM-NOTIFICATION-MIB 43
Performance and Capacity Monitoring 45
Enabling or Disabling Monitoring 46
Polling and Thresholds 46
Trap Receiving and Forwarding 47
SRST Monitoring 47

Best Practices 47

Server Maintenance 47
Cold Standby/Redundant Deployments 48
Preparing for Redundancy 48
Setting Up Redundancy 48
Setting Up the Active Operations Manager Server 48
Continuous Data Synchronization 51
Setting Up a Passive Redundant Server 54
Operations Manager for MSP Environments 54
ACS Integration for Securing Access to Devices 54
LMS Integration 65
Cisco Unified Communications Service Monitor Integration 66
Cisco 1040 Sensor in Sampling Mode 67
Cisco 1040 Sensor in a Branch Office 67
Span Port Limitations 67
Simultaneous Operations by Multiple Users 68
Operations Manager System Health Monitor 68

Troubleshooting Tips 69

Useful URLs 69

Cisco.com URLs for Customers and Partners 69
Product Information 69
VoD and Tutorial 69
Deployment Best Practices Guide 69
Training 69
Evaluation Downloads 69
Patch Download 70
Miercom Review of Operations Manager and Service Monitor 70

Abbreviations and Acronyms

ACS	Access Control Server, a Cisco® Secure product
IP SLA	Cisco IOS® Software IP Service Level Agreement
LMS	CiscoWorks LAN Management Solution
MoM	Manager of managers, a high-level network management entity
ODBC	Open Database Connectivity
QoV	Quality of voice
RME	Resource Manager Essentials, a component of CiscoWorks LMS
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SRST	Survivable Remote Site Telephony
SSL	Secure Sockets Layer
TFTP	Trivial File Transfer Protocol

Introduction

This document outlines best practices for a successful deployment of Cisco Prime™ Unified Operations Manager in enterprise and managed service provider (MSP) environments. The document describes pertinent points on initial device setup, installation guidelines, server sizing, and best practices for initial setup, ongoing administration, and maintenance of the product.

Please note that this document is not an alternative to the installation guide or the user guide, as it does not cover all the features or all the steps for the operations suggested. It is a supplement to the installation guide and the user guide. Wherever relevant, this document provides detailed steps for industry-standard best practices.

Product Overview

Cisco Prime Unified Operations Manager (referred to as Operations Manager or UOM, from this point forward) provides a unified view of the entire IP communications infrastructure and presents the current operational status of each element of the IP communications network.

Operations Manager continuously monitors the current operational status of different IP communications elements such as Cisco® Unified Communications (UC) Manager, Cisco Unified Communications Manager Express, Cisco Unity® systems, Cisco Unity Express, Cisco Unity Connection, Cisco Unified Contact Center, Cisco Unified Contact Center Express, Cisco Unified Presence Server, Cisco Emergency Responder, and Cisco Unified MeetingPlace® Express, as well as Cisco gateways, routers, switches, and IP phones. It also provides diagnostic capabilities for faster trouble isolation and resolution.

Operations Manager monitors and evaluates the current status of both the IP communications infrastructure and the underlying transport infrastructure in the network. It 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 your IP communications deployment. Since Operations Manager does not deploy any agent software on the devices being monitored, it is nondisruptive to your system operations.

In addition, Operations Manager does the following:

- Presents the current operational status of your IP communications deployment and provides visualization using service-level views of the network.

- Provides quick at-a-glance, real-time status of all the faults in the Unified Communications network.
- Increases productivity of the network managers and helps enable faster trouble identification and isolation by providing contextual diagnostic tools to facilitate troubleshooting. This is done through:
    - Diagnostic tests, performance, and connectivity details about different elements of the converged IP communications infrastructure.
    - Use of synthetic tests that replicate end-user activity and verify gateway availability as well as other configuration aspects of the Cisco Unified Communications infrastructure. Tests may be run on synthetic phones or real IP phones (both Session Initiation Protocol [SIP]-based and Skinny Client Control Protocol [SCCP]-based phones) deployed in the network.
    - IP service-level agreement (SLA)-based diagnostic tests that can measure the performance of WAN links and measure node-to-node network quality.
    - Information provided in notification messages that contain context-sensitive links to more detailed information about service outages.
    - Use of context-sensitive links to other Cisco Prime tools and Cisco tools for managing IP communications implementations.
- Discovers and reports on the status of different video-enabled IP endpoints (for both SIP- and SCCP-based phones) in the Cisco Unified Communications system and provides additional contextual information to facilitate the location and identification of the IP phones. Operations Manager can also track the status of these endpoints.
- Provides a very powerful set of dynamic phone-testing capabilities that facilitate the use of IP phones (both SIP- and SCCP-based phones) in the Cisco Unified Communications system as test probes to run dial-plan tests, acceptance tests, phone-feature tests, and so on. Such phone-testing capabilities may be used to rapidly troubleshoot issues related to connectivity (signaling/media stream) and voice quality as well as call processing/dial-plan management issues.
- Provides visibility into key performance metrics of different Cisco Unified Communications elements, such as resource usage (CPU, memory, Media Termination Point [MTP] resources, transcoder resources), call statistics (active calls), trunk statistics (trunk usage, port usage, gateway statistics), and so on, that aid in different tasks such as troubleshooting and capacity planning.
- Correlates and presents service-quality alerts by using the information available through Cisco Prime Unified Service Monitor (when it is also deployed). It displays Mean Opinion Scores (MOSs) associated with voice quality between pairs of endpoints (IP phones, Cisco Unity messaging systems, or voice gateways) at specified times in the monitored call segment and other associated details about the voice-quality data. It can also perform a probable path trace between the two endpoints and can report any outages or problems at intermediate nodes in the path.
- Provides current information about connectivity-related and registration-related outages affecting different IP phones in the network and provides additional contextual information to help enable the location and identification of the IP phones.
- Facilitates tracking of IP communications devices and IP phone inventory, tracks IP phone status changes, and creates a variety of reports that document the move, add, and change operations on IP phones in the network.
- Provides real-time notifications using SNMP traps, syslog notifications, and email, thus reporting the status of the network being monitored to a higher-level entity (typically a manager of managers [MoM]).

- Provides a single view to visualize and monitor Unified Communications component status, performance, and test results by logical and physical groupings, and provides the status of the key components on a single screen to make diagnosis of problems much quicker than the previous individual-feature navigation approach.

The following are the new features in Operations Manager Release 8.7:

- Introduction of UC Opsview:

  UC Opsview provides a single view summary of the entire UC phone network status. UC Opsview provides the following dashlets within the UC Opsview:

  - Phone Health Summary
  - Top 5 Call Failure Locations
  - Top 5 WAN Traffic Locations
  - UC Services Health Summary
  - Top 5 Poor Call Quality Location
  - Top 5 Utilized Trunks
- Adding new syslogs:

  Cisco Prime UOM 8.7 allows you to add unsupported syslogs. You must provide the exact syslog name. You need to get the exact syslog details from the device before you use it in Cisco Prime UOM.

The following are the new features in Operations Manager Release 8.6:

- Feature parity of Unified Communications 8.6 applications with functionality from Unified Communications 8.6
- Multicustomer view supporting up to 50 clusters
- Tighter Operations Manager/Service Monitor integration where Service Monitor reports can be launched from the Operations Manager dashboard itself
- Trunk usage summary under diagnostics menu
- Dedicated gateway portal
- Monitoring of Unity Connection cluster
- Presence Server monitoring enhancements
- E-learning video tutorials available from the user interface. You can also view these videos on Cisco.com at http://www.cisco.com/web/learning/le31/le46/nmtg_training/vods/om/om80/pointer.html.

Small and Medium Enterprises

For small deployments (up to 10,000 phones), the software component for Cisco Prime Unified Service Monitor can coreside with Operations Manager on a single platform. A single installation process installs all the necessary components.

Operations Manager provides real-time notifications, using SNMP traps, syslog notifications, and email, that allow Operations Manager to report the status of the network being monitored to a higher-level entity. Operations Manager is also capable of sharing device and credential information with other CiscoWorks tools deployed in the enterprise.

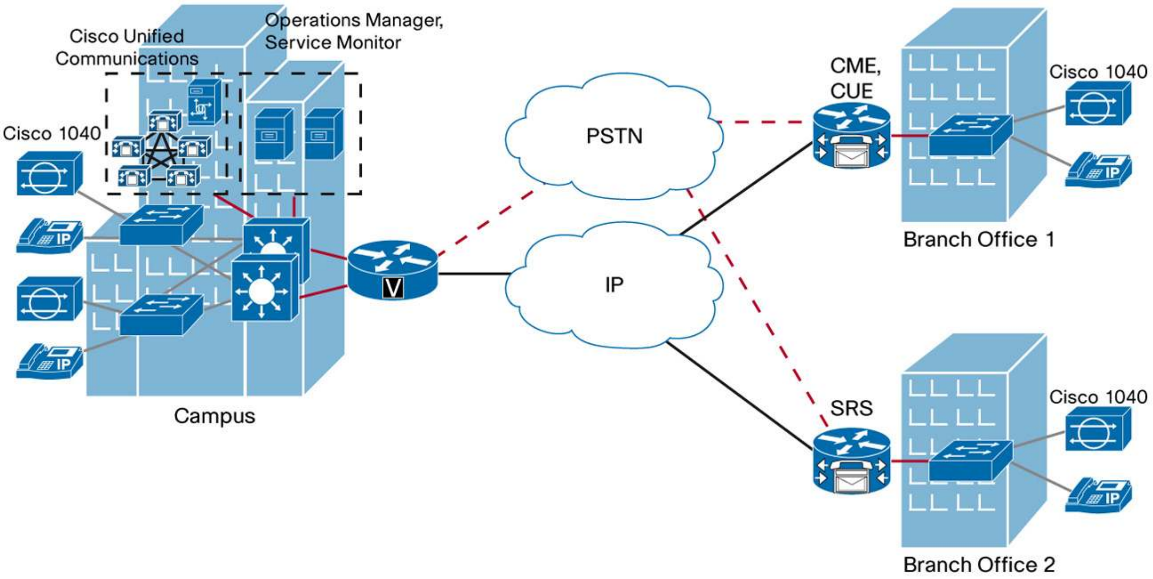
Large Enterprises

For medium and large enterprise deployments (more than 10,000 phones), it is recommended that Operations Manager and the software component Service Monitor be deployed on separate platforms. Operations Manager can be deployed centrally or in a distributed manner to scale to different sizes, using a MoM.

Each instance of Operations Manager can manage multisite and multicluster IP communications environments. Operations Manager provides real-time notifications, using SNMP traps, syslog notifications, and email, that help enable Operations Manager to report the status of the network being monitored to a higher-level entity (typically a MoM).

Since Operations Manager can also share device and credential information with other CiscoWorks tools deployed in the enterprise, this results in reduced administrative overhead for network managers. Figure 1 shows the deployment model for large enterprises.

Figure 1. Deployment Model for Large Enterprises



Managed Service Providers

Operations Manager can manage multiple customers using a single Operations Manager instance. To learn more about it, please go to http://www.cisco.com/en/US/docs/net_mgmt/cisco_unified_operations_manager/8.6/user/guide/intro.html#wp1428397.

Preinstallation Tasks

This section describes the minimum configuration tasks that should be performed on Cisco IOS® Software, Cisco Catalyst®, and Cisco Media Convergence Server (MCS) devices before attempting to manage them using Operations Manager. It should be noted that this is not an exhaustive configuration guide. Depending on the functionality required, further device configuration may be required. For comprehensive information, see Performance and Fault Management, available from Cisco Press as well as on Cisco.com (http://www.cisco.com/en/US/products/sw/netmgtsw/index.html).

Preparing Devices to Be Monitored by Operations Manager

For Operations Manager to manage and monitor devices successfully, the following conditions should be met:

- SNMPv3 credentials[1] or SNMPv2 read community string must be configured on each device.
- SNMPv2 write community string must be configured on each device (needed only for certain routers and switches on which IP service-level agreement, or SLA, tests will be configured).
- IP SNMP access lists should include the IP address of the Operations Manager server.
- The sysName of the device must be the same as the hostname of the devices for Cisco IOS and Cisco Catalyst devices.
- IP connectivity must be verified between the devices and the Operations Manager server.
- For Cisco IOS and Cisco Catalyst devices, one of the interface IP addresses must be designated as the management IP address, and it should be defined as a loopback IP address.
- If Operations Manager is going to discover the network through an automated discovery process, then Cisco Discovery Protocol should be enabled on all the Cisco devices.
- If Cisco Discovery Protocol is disabled (WAN interfaces usually have Cisco Discovery Protocol disabled), use the ping sweep option. Make sure that you can ping the device from the Operations Manager server.

Cisco IOS Devices

This section describes the steps that should be performed to set up Cisco IOS devices for network management.

Note: All steps may not be required, and some steps can be expanded with more functionality.

After performing these steps, save the configuration to nonvolatile random-access memory (NVRAM) by using one of the following commands:

```
write memory
or
copy running-config startup-config
```

SNMPv2 Community Strings

Operations Manager can use SNMPv2 read community strings to retrieve fault and performance information from the devices. Some of the features in Operations Manager (node-to-node tests, Survivable Remote Site Telephony [SRST] monitoring, and phone status tests) also require SNMP write community strings to configure IP SLA (formerly known as the Service Assurance Agent) on certain devices.

If you intend to use these features, be sure to configure SNMP write community strings on these devices. All SNMP community strings must match on the devices and in the Operations Manager default credentials repository.

To configure SNMPv2 community strings on a Cisco IOS device, use the following global configuration commands:

```
snmp-server community <read-community-string> RO
snmp-server community <write-community-string> RW
```

[1] Operations Manager supports SNMPv1, SNMPv2c, and SNMPv3AuthNoPriv mode. SNMPv3 support for AUTH=None is not present in Operations Manager. Due to this condition, Operations Manager cannot be used with devices having SNMPv3, AUTH=None.

These commands help ensure that the device can be identified and that inventory can be carried out.

For Cisco Unified Communications Manager, Cisco Unity products, and other standard IP telephony OS voice applications, the Windows SNMP Service must be enabled and configured with a read-only (RO) community string.

SysName Variable

The system name (sysName) must be unique on every Cisco IOS device for network services to discover all Cisco IOS devices on the network. Network services use this variable to identify each device through Cisco Discovery Protocol. If this value is duplicated on any devices, network services discover only one of the devices. On Cisco IOS Software, the domain name also affects the sysName.

To set the sysName variable on a Cisco IOS device, use the following global configuration command:

```
hostname <text>
```

Setting Up IP SLA on Cisco IOS Devices

Certain features within Operations Manager use the IP SLA (formerly known as SAA or Response Time Responder [RTR]) functionality in Cisco routers and switches. If you intend to use these features (SRST monitoring, phone status tests, and node-to-node tests), you will need to make sure that the IP SLA is enabled on these devices. You will need to enable the IP SLA on all the routers and switches that will be used in SRST monitoring or in node-to-node tests.

Typically, these are the edge routers in your branch networks and the default gateway for Cisco Unified Communications Manager. You can enable the IP SLA responder in the IP SLA router by running the following command (depending on the Cisco IOS Software version) in the global configuration mode:

```
(config #) rtr responder OR ip sla responder
```

Use the **show** command to verify that the responder is running properly:

```
router#show rtr responder
```

Use the following **show** command to verify that the IP SLA feature is available in the Cisco IOS device:

```
router#show rtr application

router#show ip sla?
apm                       IP SLAs Application Performance Monitor
  application             IP SLAs Application
  authentication          IP SLAs Authentication Information
  configuration           IP SLAs Configuration
  enhanced-history        IP SLAs Enhanced History
  group                   IP SLAs Group Scheduling/Configuration
  history                 IP SLAs History
  reaction-configuration  IP SLAs Reaction Configuration
  reaction-trigger        IP SLAs Reaction Trigger
  responder               IP SLAs Responder Information
  statistics              IP SLAs Statistics
```

Cisco Catalyst Devices

This section describes the steps that should be carried out to set up Cisco Catalyst devices for network management.

Note: All steps may not be required, and some steps can be expanded with more functionality.

SNMPv2 Community Strings

Operations Manager can use SNMPv2 read community strings to retrieve fault and performance information from the devices. Some of the features in Operations Manager (node-to-node tests, SRST monitoring, and phone status tests) also require SNMP write community strings to configure the IP SLA on certain devices. If you intend to use these features, be sure to configure SNMP write community strings on these devices. All SNMP community strings must match on the devices and in the Operations Manager default credentials repository.

To configure SNMPv2 community strings on a Cisco Catalyst OS device, use the following global configuration commands:

```
set snmp community read-only <read-community-string>
set snmp community read-write <write-community-string>
```

These commands help ensure that the device can be identified and that SNMP polling can be carried out.

Cisco Discovery Protocol

Cisco Discovery Protocol is a Cisco proprietary protocol that is used by devices to advertise their existence to other devices on the network. Each device that has Cisco Discovery Protocol enabled maintains a table of its neighbors. Operations Manager uses Cisco Discovery Protocol to perform an automated discovery of all the Cisco devices in the network and gather information about Cisco IP Phones connected to these devices.

If Cisco Discovery Protocol is not enabled on a device, Operations Manager cannot perform an automated Cisco Discovery Protocol-based network discovery and cannot populate phone reports with switch-related information. Cisco Discovery Protocol is enabled by default, so you need to enable it only if it has been explicitly disabled. For reasons of information security, it is recommended that Cisco Discovery Protocol be explicitly disabled on devices that are on the borders of your management domain, such as edge routers.

To enable Cisco Discovery Protocol on a Cisco Catalyst device, use the following command:

```
set cdp enable <all | module/port>
```

To enable Cisco Discovery Protocol on a Cisco IOS device, use the following command:

```
cdp run
```

Tips:

- Use the “all” parameter to enable Cisco Discovery Protocol on all ports on the device, or enter specific module and port numbers. A range of ports can also be entered.

  For example, **set cdp enable 2/1-10,3/5-10**.

  To disable Cisco Discovery Protocol on a Cisco Catalyst device, use the command **set cdp disable**.

- Do not run Cisco Discovery Protocol on links that you do not want discovered, such as Internet connections.

Note: Do not enable Cisco Discovery Protocol on links that do not go to Cisco devices. This protects you from Cisco Discovery Protocol denial of service (DoS) attacks. Cisco Discovery Protocol is also relevant to Cisco IOS devices (both routers and switches), because Cisco IOS Software is increasingly being used on new switches and even on Cisco Catalyst 6500s.

Media Convergence Servers

This section describes the steps that should be taken to set up Cisco Media Convergence Servers for network management.

Note: All steps may not be required, and some steps can be expanded with more functionality.

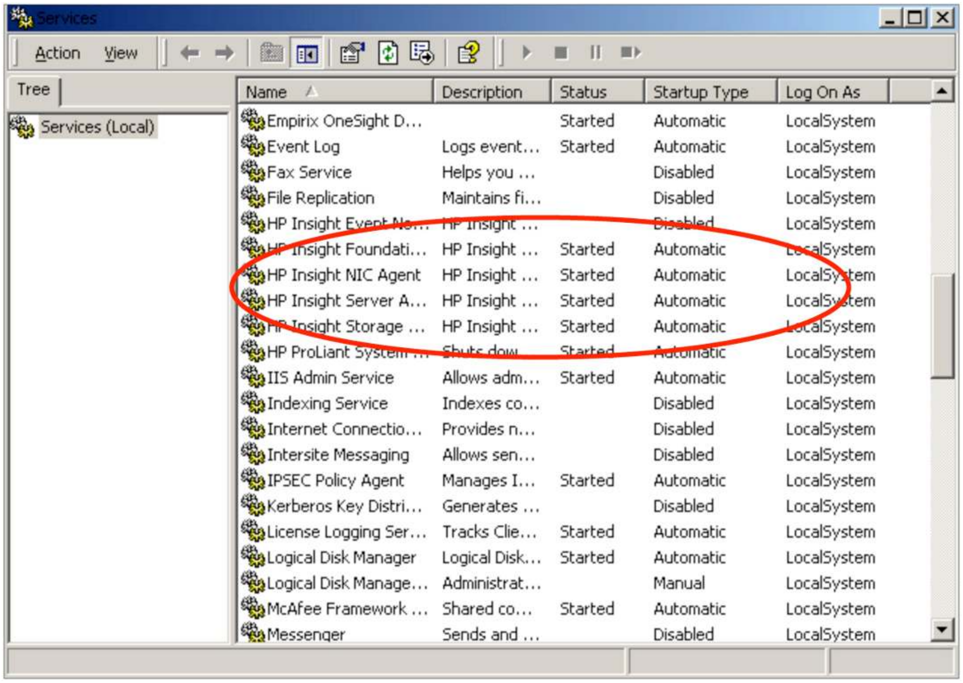
The following section is applicable to all the Cisco IP communication components that run on Cisco MCS platforms. Examples include Cisco Unified Communications Manager, Cisco Unity, Cisco Unity Connection, Cisco Unified Contact Center, Cisco Conference Connection, Cisco Emergency Responder, Cisco Unified Contact Center Express, and Cisco Personal Assistant.

HP Insight Manager Agent Service

The hardware instrumentation on Cisco MCS on HP platforms is provided by the HP Insight Manager software running as a service or a set of services on the system. As a part of the Cisco-provided IP Telephony operating system, these services are automatically installed.

You can verify that these services have been installed by viewing the services' user interface (**Start > Control Panel > Administrative Tools > Services**); see Figure 2. If they have not been installed, you need to install them on the HP system. If these services have been stopped for any reason, restart them.

Figure 2. HP Insight Manager Agent Service



Name	Description	Status	Startup Type	Log On As
Empirix OneSight D...		Started	Automatic	LocalSystem
Event Log	Logs event...	Started	Automatic	LocalSystem
Fax Service	Helps you ...		Disabled	LocalSystem
File Replication	Maintains fi...		Disabled	LocalSystem
HP Insight Event No...	HP Insight ...		Disabled	LocalSystem
HP Insight Foundati...	HP Insight ...	Started	Automatic	LocalSystem
HP Insight NIC Agent	HP Insight ...	Started	Automatic	LocalSystem
HP Insight Server A...	HP Insight ...	Started	Automatic	LocalSystem
HP Insight Storage ...	HP Insight ...	Started	Automatic	LocalSystem
HP ProLiant System ...	Shuts dow...	Started	Automatic	LocalSystem
IIS Admin Service	Allows adm...	Started	Automatic	LocalSystem
Indexing Service	Indexes co...		Disabled	LocalSystem
Internet Connectio...	Provides n...		Disabled	LocalSystem
Intersite Messaging	Allows sen...		Disabled	LocalSystem
IPSEC Policy Agent	Manages I...	Started	Automatic	LocalSystem
Kerberos Key Distri...	Generates ...		Disabled	LocalSystem
License Logging Ser...	Tracks Clie...	Started	Automatic	LocalSystem
Logical Disk Manager	Logical Disk...	Started	Automatic	LocalSystem
Logical Disk Manage...	Administrat...		Manual	LocalSystem
McAfee Framework ...	Shared co...	Started	Automatic	LocalSystem
Messenger	Sends and ...		Disabled	LocalSystem

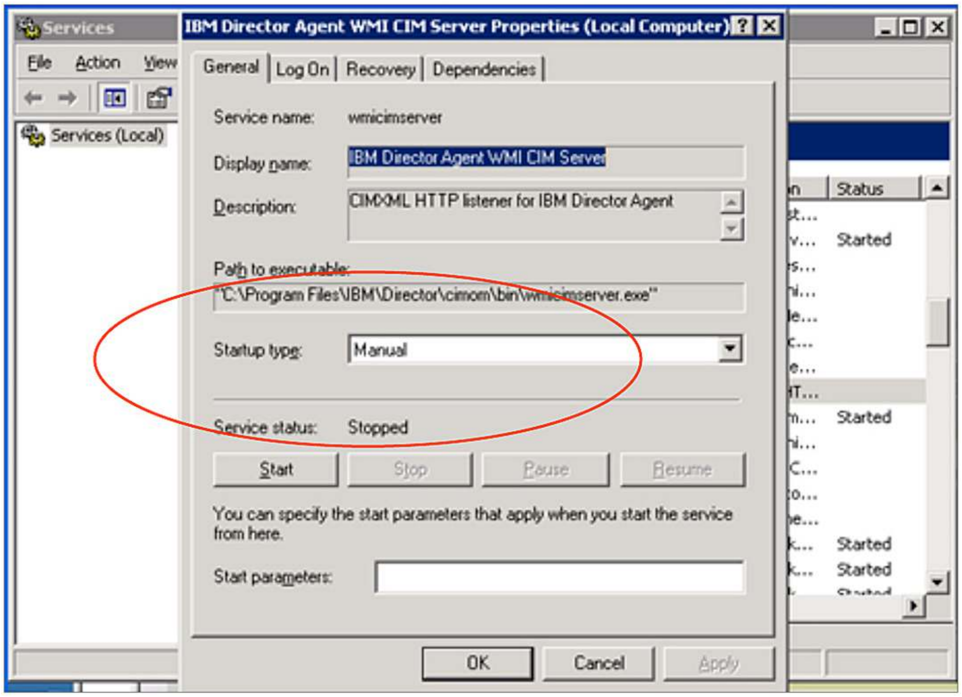
IBM UM Services

The hardware instrumentation on Cisco MCS on IBM platforms is provided by IBM Unified Messaging (UM) Services running as a service or a set of services on the system. As a part of the Cisco-provided IP Telephony operating system, these services are automatically installed. You can verify that these services have been installed by looking at the process umslmsensor in the task manager interface. Search under C:\Program Files for a folder titled UM Services.

The Windows service **ibm director wmi cim server** runs, by default, on IBM servers and prevents the start of Operations Manager service-level view. You need to stop this service and change the startup type to Manual before the installation (Figure 3).

The recommended version of IBM Director is 5.10.1. This is incorporated in the OS build for Communications Manager 2000.4.3.

Figure 3. Stop the IBM Director WMI CIM Server



IBM Director Agent WMI CIM Server Properties (Local Computer)

Service name: wmicimserver

Display name: IBM Director Agent WMI CIM Server

Description: CIMXML HTTP listener for IBM Director Agent

Path to executable:
"C:\Program Files\IBM\Director\cimom\bin\wmicimserver.exe"

Startup type: Manual

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Windows/MCS SNMP Service

As a part of the standard IP telephony OS installation, the SNMP service on the Media Convergence Server is installed, but community strings are not specified. For Operations Manager to manage the device, the device (that is, the Cisco Unified Communications Manager, Cisco Unity, and so on) must have a proper SNMP read community string defined for the SNMP service.

To define the SNMP read community string, do the following:

Step 1. On the MCS, go to **Start > Control Panel > Administrative Tools > Services**.

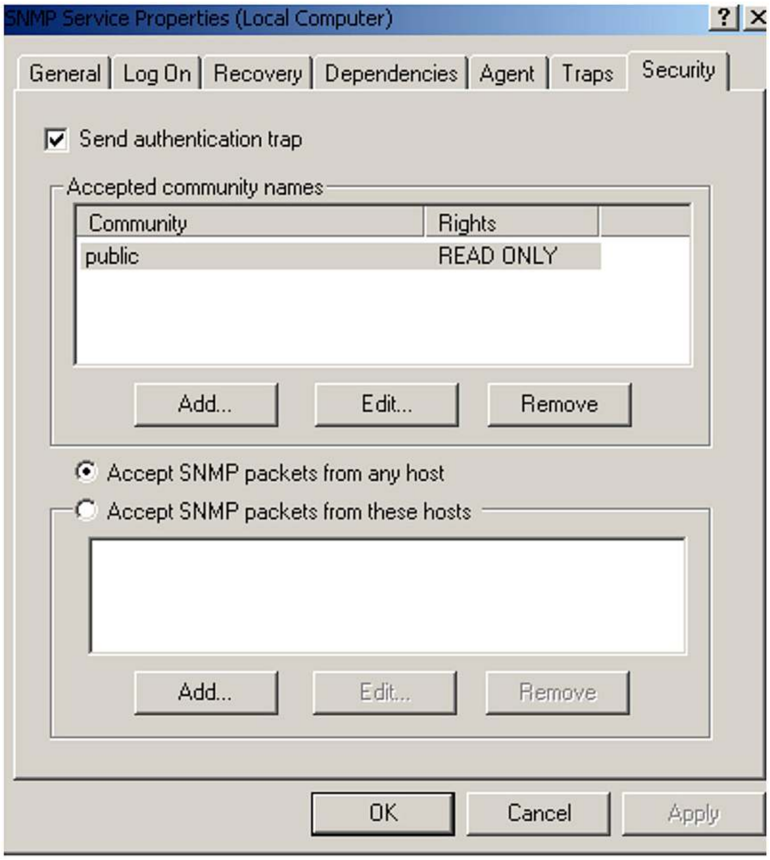
Step 2. Select the **SNMP** service.

Step 3. Double-click the service and select the **Security** tab.

Step 4. Under the **Security** tab, you can define community strings and assign them read permission. (This is not the read community string).

On the same tab, you can also specify which servers (IP addresses) can make SNMP queries to the MCS. In that section, make sure that you add the IP address of Operations Manager as an authorized server to make SNMP queries to the MCS (Figure 4).

Figure 4. Windows/MCS SNMP Service



☑ Send authentication trap

Accepted community names

Community	Rights
public	READ ONLY

● Accept SNMP packets from any host

○ Accept SNMP packets from these hosts

For Cisco Unified Communications Manager 5.0 and later, the SNMP community string is configured through the Cisco Unified Communications Manager Administration user interface. Because Cisco Unified Communications Manager 5.0 and later resides on the Linux operating system, there is no Windows SNMP service to configure. Remember to restart the SNMP Master Agent on Linux-based Communications Manager after SNMP is configured through the user interface.

SNMP Traps

If you want Operations Manager to receive traps from the MCS or the applications installed on the MCS, be sure to specify the IP address of the Operations Manager as a destination on that MCS server. From the SNMP service user interface, go to the traps section and enter the IP address of the Operations Manager as a valid destination in order for the traps to be sent there.

Also, from **Administrative Tools > Services,** disable **Windows SNMP Trap Service** and then restart the SNMP Daemon Manager on the Operations Manager server.

SNMP Management of Cisco Unified Contact Center

The Microsoft Windows SNMP service is disabled as part of Intelligent Contact Management setup and is replaced by the Cisco Contact Center SNMP Management service to process SNMP requests in its place. The Cisco Contact Center SNMP Management service provides for more sophisticated SNMP capabilities than the standard Microsoft SNMP service.

Follow the instructions mentioned in the SNMP Guide for IPCC Enterprise and Hosted Edition to install the correct SNMP components required for managing Cisco Unified Contact Center devices using Operations Manager.

You can configure Cisco SNMP Agent Management settings using the Windows Management Console Snap-in.

Installing the Cisco SNMP Agent Management Snap-in

To add the snap-in and change Cisco SNMP Management settings, do the following:

Step 1. On the Cisco Unified Contact Center system, select **Start > Run**.

Step 2. In the Start box, type **mmc** and press **ENTER**.

Step 3. From the Console, select **File > Add/Remove Snap-in**.

A new window appears.

Step 4. From the Standalone tab, verify that Console Root is selected in the Snap-ins added to: field and click **Add**.

Step 5. In the Add Snap-in window, scroll down and select **Cisco SNMP Agent Management**.

Step 6. Click **Add**.

Step 7. Click **Close**.

Step 8. Click **OK** in the Add/Remove Snap-in window.

The Cisco SNMP Agent Management Snap-in is now loaded in the console.

Saving the Snap-in View

After you have loaded the Cisco SNMP Agent Management Microsoft Management Console (MMC) Snap-in, you can save that console view to a file (with an .msc file extension). The file can be launched directly instead of repeatedly adding the snap-in to a new MMC view.

To do so, select the console and use the **Save As** function. Select a distinctive filename, and make sure that the .msc file extension is maintained. The **Administrative Tools** (**Start**) menu is the default location where the file will be saved, which makes it available for later access through the **Start** menu.

Configuring Community Names for SNMPv1 and SNMPv2c

If you are using SNMPv1 or SNMPv2c you must configure a community name so that network management systems (NMSs) can access the data provided by your server. This name is left blank during installation for security reasons. SNMP community names are used to authenticate data exchange of SNMP information. An NMS can exchange SNMP information only with servers that use the same community name.

To configure the community name for SNMPv1 and SNMPv2c, do the following:

Step 1. Perform the steps in the “Installing the Cisco SNMP Agent Management Snap-in” section.

Step 2. Expand Cisco SNMP Agent Management in the left pane of the MMC plug-in.

Step 3. In the left pane under Cisco SNMP Agent, Management Community Name, and SNMP Version, highlight the community names for SNMPv1 or SNMPv2c.

The **Restricted Access** columns appear in the right pane.

Step 4. Right-click the white space in the right pane and select **Properties**.

A dialog box appears.

Step 5. Click **Add New Community**.

Step 6. In the dialog box, under **Community Information**, provide a community name.

Step 7. Select the SNMP version by selecting the radio box for SNMPv1 or SNMPv2c.

You can enter one or more IP addresses in the **IP Address** field (containing "dots") and click **Insert** to enable access solely for this community from the NMS with the IP address provided.

Step 8. Click **Save**.

The community name appears in the **Configured Communities** section at the top of the dialog box.

Note: You can remove the community name by highlighting the name in the **Configured Communities** section, and clicking **Remove Community**. Changes become effective after you click **OK**.

Cisco Unified Communications Manager

The following configuration options on the Cisco Unified Communications Manager need to be configured for Operations Manager to discover and manage the Cisco Unified Communications Manager. Failure to do so may result in incomplete monitoring of the Cisco Unified Communications Manager and cause some features in Operations Manager to behave inconsistently.

HTTP Credentials

Operations Manager uses the AVVID XML Layer (AXL) API in addition to SNMP to manage Cisco Unified Communications Manager. This means that Operations Manager will make Simple Object Access Protocol (SOAP) calls over HTTP through the AXL interface to collect fault and performance information from the Cisco Unified Communications Manager. Operations Manager needs an HTTP username/password to execute these queries.

When you add or discover a Cisco Unified Communications Manager or Cisco Unified Presence Server with Operations Manager, you must supply a username/password or that Cisco Unified Communications Manager will enter the partially monitored state (see the "Device Discovery Process" section). The username/password need not be administrator credentials. Any set of credentials with read-level access that will get authorized for the URL (http://server-name/ccmadmin) will suffice.

HTTPS Configuration and Security Certificates

Cisco Unified Communications Manager 4.1 or later supports enabling Secure Sockets Layer (SSL) on virtual directories. If you intend to secure the communication between Operations Manager and Cisco Unified Communications Manager, you will need to enable SSL on the Cisco Unified Communications Manager and specifically certain virtual directories.

- CCMApi: Operations Manager uses services in this virtual directory to perform AXL/SOAP database queries.
- SOAP: Operations Manager uses services in this virtual directory to perform AXL/SOAP device queries.

Note: SSL is not enabled on the CCMApi and Soap virtual directories, by default. For information on enabling SSL (using Windows Internet Information Services [IIS]), see **Cisco Unified Communications Manager Security Guide** for the appropriate release of Cisco Unified Communications Manager. Also see the "Using Device Manager" chapter in **User Guide for Cisco Unified Operations Manager**.

Enabling HTTPS on Cisco Unified Communications Manager

To enable HTTPS on Cisco Unified Communications Manager, do the following:

Step 1. On the Cisco Unified Communications Manager system, select **Administrative Tools > Internet Services Manager**.

Step 2. Click the server that is displayed.

Step 3. Right-click the virtual directory (Soap and CCMApi) and click **Properties**.

Step 4. Go to the Directory Security tab and under Secure Communications, click **Edit**.

Step 5. In the dialog box, select the **Require SSL** check box and click **Apply**.

Note: If this procedure does not work, you might have to restart the IIS service from the control panel.

Cluster ID of a Cisco Unified Communications Manager Cluster

Operations Manager relies on the cluster ID of the Cisco Unified Communications Manager cluster to uniquely identify and manage the Cisco Unified Communications Manager deployment. Therefore, if two Cisco Unified Communications Manager deployments belonging to different clusters have the same cluster ID, Operations Manager cannot manage them as two distinct clusters. Cisco Unified Communications Manager (starting with version 3) has a default cluster name of StandAloneCluster. If you are managing multiple Cisco Unified Communications Manager deployments belonging to different clusters within the same Operations Manager, you will need to change the cluster ID of these Cisco Unified Communications Managers so that they have unique names.

To change the cluster ID of a Cisco Unified Communications Manager, do the following:

Step 1. Open the Cisco Unified Communications Manager Administration page.

Step 2. From the menu, select **System**, and choose **Enterprise Parameters**.

The **Enterprise Configuration** page is displayed.

Step 3. In the **Cluster ID** field, enter a new cluster ID.

The default is **StandAloneCluster**. This should be changed so that it is unique for every cluster.

Step 4. Click **Update**.

You will need to restart the Cisco Unified Communications Manager service and the RIS Data Collector service for these changes to take effect. Restarting these Cisco Unified Communications Manager services causes a service disruption (this is for voice services only). To minimize disruption, be sure to schedule this task for a time when system maintenance is being done.

If Operations Manager is already managing Cisco Unified Communications Manager and you are changing the cluster ID, then the cluster IDs in the Service Level View will not reflect the new cluster ID. You have to delete and re-add the Cisco Unified Communications Manager in Operations Manager for it to reflect the new cluster ID.

Verifying Cisco Unified Communications Manager DNS Settings

Operations Manager will be unable to collect the correct monitoring information if it cannot resolve the name using Domain Name System (DNS) for Communications Manager, Unity Connection, and Presence Server. You must verify that these devices are resolvable in DNS.

Configuring Syslog Receiver on Cisco Unified Communications Manager

Cisco Prime Unified Operations Manager has enhanced Cisco Unified Communications Manager fault monitoring by supporting integration with Cisco Real-Time Monitoring Tool (RTMT). To enable this integration, you must add the syslog receiver from the Communications Manager's serviceability web page. For detailed procedures, see the **User Guide for Cisco Prime Unified Operations Manager**, located on Cisco.com at http://www.cisco.com/en/US/products/ps6535/products_user_guide_list.html.

Voice Gateway and MGCP

In order for Operations Manager to collect performance data on Cisco MGCP Voice Gateway, the gateway associated call agent (Cisco Unified Communications Manager) should also be managed using Operations Manager. Also for Operations Manager to discover Media Gateway Control Protocol (MGCP) capability for cases such as MGCP VOIP Service, PRI Backhauling, and Signaling System 7 (SS7) signaling, Cisco MGCP Voice Gateway application should be running on Cisco IOS Software 12.4(16.10), 12.4(16.10)T, or later.

Cisco Unified Communications Manager Express and SRST

For Cisco Unified Communications Manager Express and SRST, the latest Cisco IOS MIBs (CISCO-CCME-MIB and CISCO-SRST-MIB) are required. This CISCO-CCME-MIB and CISCO-SRST-MIB were introduced with Cisco IOS Software Release 12.4(4) T and Cisco Unified Communications Manager Express 3.4 and SRST 3.4. Unless noted otherwise, subsequent releases of that Cisco IOS Software release train also support these MIBs.

Go to Cisco.com and download the latest Cisco Unified Communications Manager Express and Cisco IOS Software for SRST, which supports new SNMP MIBs specific to Cisco Unified Communications Manager Express and SRST and their associated phones (available at http://www.cisco.com/cgi-bin/tablebuild.pl/ip-key).

If you are running Cisco Unified Communications Manager 4.0 (or later) and it has an SRST configured, it will appear in the topology along with the cluster. Operations Manager does not put it in the SRST device folder, but lists it under the associated cluster. This is independent of whether or not the MIB implementation is available on the router.

Cisco Unity

For Cisco Unity and Cisco Unity Connection, the appropriate Remote Serviceability Kit (RSK) must be installed for Operations Manager to manage them properly. You can load the RSK from http://www.ciscounitytools.com/. Cisco Unity Connection 7.x and later does not need RSK installation.

For Cisco Unity, the Event Monitoring Service must be configured to send the traps to Operations Manager. Event Monitoring Service should already be installed if the Remote Serviceability Kit is installed. The events supported through Event Monitoring Service trap in Operations Manager 8.x are HardDiskError, OutOfDiskSpace, and ExchangeLogonFailed.

Cisco Unity Connection must be configured to send the syslogs to Operations Manager. Operations Manager will be unable to collect the correct monitoring information if it cannot resolve the name using DNS for Unity Connection. You must verify that Unity Connection instances are resolvable in DNS.

Cisco Unity Express

You need to add the IP address of the Cisco Unity Express device to the Operations Manager server as if the Cisco Unity Express device is a separate device. Cisco Unity Express has its own SNMP agent and management IP address. Adding Cisco Unified Communications Manager Express does not automatically make Operations Manager aware of Cisco Unity Express.

Cisco Unity Express supports SNMP from version 2.3 onward, so older versions of Cisco Unity Express must be upgraded. To manage Cisco Unity Express, the latest version must be used, and SNMP read-only community strings must be configured.

Go to Cisco.com and download the latest Cisco Unity Express version. If, at the Cisco Unity Express configuration mode command prompt, the **snmp-server** command is not supported, then you need to upgrade to the latest Cisco Unity Express version.

Setting Up Cisco Unity Express

To set up the latest Cisco Unity Express, do the following:

Step 1. Untar the files

Step 2. At the NetworkModule boot prompt, enter: **config**<cr>

TFTP server: <TFTPserverIP>

Default helper-file: aesop_helper

Step 3. Enter **boot helper**<cr>

The following text is displayed on the console:

```
Changing owners and file permissions.
Change owners and permissions complete.
INIT: Switching to runlevel: 4
INIT: Sending processes the TERM signal
STARTED: dwnldr_startup.sh
Welcome to Cisco Systems Service Engine Helper Software
Please select from the following
1 Install software
2 Reload module
3 Disk cleanup
4 Linux shell
(Type '?' at any time for help)
Choice: 1
Package name: package_name.pkg
Server URL: ftp://1.100.20.80/build/2.2.0.9
Username:
Password:
```

Once the software is installed, log in to Cisco Unity Express.

At the Cisco Unity Express prompt, enter the following commands:

1. **conf t**<cr>
2. **snmp-server community** <read-only-community-string> **RO**
3. **snmp-server community** <read-write-community-string> **RW**
4. **snmp-server host** <yourTraphostIP> <read-only-community-string>
5. **end**
6. **wr mem**

Preparing the Server for Operations Manager

Operating System

Operations Manager is supported on Windows 2008 Server Standard Edition with Service Pack 2, Windows 2008 Server Enterprise Edition with Service Pack 2, and Windows 2003 Server with Service Pack 2 Enterprise Edition (32-bit version). Please note that other operating systems are **not** supported. It is recommended that no software or applications other than the operating system and antivirus application be installed on this computer system.

For more information about the system requirements, see the **Installation Guide for Cisco Unified Operations Manager 8.7**, located on Cisco.com at http://www.cisco.com/en/US/products/ps6535/prod_installation_guides_list.html.

Hardening the Server

The system that you use for your Operations Manager server should meet all the security guidelines that Microsoft recommends for Windows Server. See the Microsoft website for security guidance.

You may also want to refer to security guidelines that Adobe and Sybase recommend for their applications.

For Adobe Flash 10.0, you may want to refer to http://www.adobe.com/devnet/flashplayer/articles/flash_player_admin_guide/flash_player_admin_guide.pdf.

For Sybase Database, you may want to refer to http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.help.sas_1s0.0.1/title.htm.

VMware Deployment

For VMware centered deployment, see **Best Practices for Cisco Unified Communications Management Suite Virtualization** at http://www.cisco.com/en/US/products/ps6535/prod_white_papers_list.html.

Miscellaneous

It is recommended that you install the following Microsoft hotfix to avoid Operations Manager system degradation in the long run: http://support.microsoft.com/kb/931311.

Operations Manager requires an entire 4 GB of RAM for optimal performance. A typical Windows configuration allocates 3.5 GB RAM for application activities and reserves the remaining memory for its internal use. Enabling the **PAE flag** requests Windows to release its reserved cache (RAM) for application (Operations Manager) usage. For more information about enabling the PAE flag, you can refer to http://www.microsoft.com/whdc/system/platform/server/pae/default.mspx.

It is recommended that you install a SCSI controller that has Battery Backed Write Cache (BBWC). Enabling BBWC will provide better disk performance of the Operations Manager system.

When installing Operations Manager on Windows Server 2008, page file configuration is mandatory. The page file shouldn’t be set to “Automatically manage paging file size”; the user should specifically define the fixed size.

Hostname and IP Address

It is recommended that you configure the hostname and IP address for the Operations Manager server before you start installing Operations Manager. Specify the hostname when you are installing the operating system or subsequently, using **My Computer > Properties > Computer Name**.

Once Operations Manager is installed, changing the hostname and IP address is a very laborious process involving file manipulation and the execution of scripts. Refer to the **User Guide for Cisco Unified Operations Manager**, which documents all the steps involved in changing the hostname and IP address of the Operations Manager server.

Note: Make sure that the hostname does not contain any underscores.

Client PC Macromedia Flash

For any PC client (or if the Operations Manager server is also going to be used as the Operations Manager client), please visit http://www.adobe.com/ and upgrade the Adobe/Macromedia Flash Player on the Operations Manager server to Version 8 or later.

The client system must be used to access the Internet, and the upgrade is applied directly to that system. There is no way to separately download this file from the Adobe or Macromedia website and apply it. If you are working in a very secure network environment, it is recommended that you upgrade the Macromedia Flash version before installing Operations Manager on a network that is blocked from the Internet.

Verify Locale Settings

Operations Manager only supports the U.S. English and Japanese locales. Using other locales means that you are running on a nonsupported configuration. Further, Operations Manager may display erratic behavior, such as JRunProxyServer services not starting automatically. However, non-U.S. English keyboard layouts should work.

DNS Settings

It is not mandatory that devices managed by Operations Manager be in Domain Name System. However, it is mandatory that Operations Manager itself be reachable through both its fully qualified domain name (server.cisco.com) and its IP address. This can be accomplished in either of these ways:

- Adding a forward and reverse name translation in the DNS server for Operations Manager.
- Adding an entry (with the name-to-IP address mapping) in the hosts file in the Windows\system32\etc\drivers folder.

After this is done, verify forward and reverse lookup using the fully qualified domain name as well as the IP address. Failure to do so will cause errors in device discovery and monitoring.

Verify Open Database Connectivity Driver Manager

Some components of Operations Manager require the presence of the correct version of Open Database Connectivity (ODBC) on the Operations Manager server.

To verify the ODBC Driver Manager version, do the following:

Step 1. On the Operations Manager server, select **Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**.

Step 2. Click the **About** tab.

Step 3. Make sure that all ODBC core components have the same version number (3.5xx or later).

ODBC is not available from Microsoft as a standalone installation but is packaged along with the Microsoft Data Access Component (MDAC).

Note: If the necessary ODBC component is not listed, install MDAC 2.5 or later. To obtain the MDAC, refer to the Microsoft website at http://www.microsoft.com/downloads/details.aspx?FamilyID=83e8f178-94c9-4e7d-b0b6-a8a94c4eb912&DisplayLang=en.

Enabling/Installing Windows SNMP Service

Operations Manager reports the status of its components through the host-resources and sysAppl MIBs. This support helps enable users to monitor the management station (Operations Manager) using a third-party SNMP management tool. To enable SNMP queries, Windows SNMP service must already be installed before you install Operations Manager. If Operations Manager is installed without Windows SNMP service, then to enable SNMP queries, you need to install the Windows SNMP service.

If you have installed Windows SNMP service after installing Operations Manager, then you will need to manually make sure that the SNMP trap service is disabled. If the SNMP trap service is not disabled, then Operations Manager will not be able to receive traps from the devices it manages.

Note: To improve security, the SNMP set operation is not allowed on any object ID (OID) in the sysAppl MIB. After installation of Operations Manager, you should modify the credentials for Windows SNMP service to make sure that no default or well-known community string is used.

To verify that Windows SNMP service is installed, do the following:

Step 1. Open the Windows administrative tool Services window.

Step 2. Verify whether:

- SNMP service is displayed on the Windows Services console (Windows SNMP service is installed).
- SNMP service status is started (SNMP service is running).

If the SNMP service is not installed, follow the Windows online help to install SNMP service. Search for **install SNMP Service** in the Windows online help search.

Browser Version and Flash Plug-in

You can refer to the Operations Manager Installation Guide 8.x at http://www.cisco.com/en/US/products/ps6535/prod_installation_guides_list.html to know the recommended browser and Flash versions. Internet Explorer 8.0 and Firefox 3.x are supported browser versions.

To install/upgrade to Flash version 8 or later, visit http://www.macromedia.com/support/flash/.

Device Connectivity

Before attempting to manage your network using Operations Manager, make sure that you can reach devices in all your subnets from the target Operations Manager server. This will help ensure that there are no IP connectivity issues between the management server and the devices.

Terminal Server Services

Virtual Network Computing (VNC) Services and Remote Desktop can be used to remotely install the Operations Manager (and Service Monitor) software.

Antivirus and Platform Agents

Operations Manager has undergone interoperability testing with McAfee VirusScan Enterprise 8.0. When using Operations Manager on a system with virus protection software, make sure that you enable virus protection only after the installation or upgrade is complete. You should schedule active scanning of drives and memory to occur during off-peak hours. You may experience delays, and performance may be degraded, when the virus scan software is scanning all files. You should exclude the NMSROOT/databases directory from virus scanning. Problems can arise if database files are locked because of virus scanning.

System Capacity

For information on system capacity, see the **Installation Guide for Cisco Unified Operations Manager 8.7**, located on Cisco.com at http://www.cisco.com/en/US/products/ps6535/prod_installation_guides_list.html.

For IP communications deployments of more than 45,000 phones, multiple Operations Manager servers can be used to monitor the deployment. These servers can share device and credential information between them, and administrators can perform centralized device and credential management. By integrating with Cisco Secure Access Control Server (ACS), administrators can centrally control user access. Each of these servers will roll up the status of the network being monitored to a higher-level entity (typically a MoM) through SNMP traps and syslog notifications.

System Requirements

For information on system requirements including coresident deployments, see the **Installation Guide for Cisco Unified Operations Manager 8.7**, located on Cisco.com at http://www.cisco.com/en/US/products/ps6535/prod_installation_guides_list.html.

Preparing the Network

Register Devices and Interfaces in DNS

For the name lookup process to work, devices should be registered in DNS. When the discovery process encounters a device, it performs a reverse lookup on the IP address where the device was encountered to get the hostname for the device. Operations Manager then performs a forward lookup on the hostname to get the preferred management interface for the device. Hence, all interfaces should be registered in reverse DNS, but only the preferred management interface should be registered in the forward lookup.

The loopback interface is an ideal candidate for registration in the forward lookup, because this interface never goes down. Make sure that the other interfaces do not have forward lookup pointing to incorrect DNS names, and make sure that the system names (hostnames) of the Cisco devices are identical to their DNS names.

If registering all the devices in DNS is not an acceptable option, then you will need to define a host file with the lookup names (sysnames) of all the devices and their corresponding IP addresses. In the absence of DNS, Operations Manager will use this as the basis of translation.

If neither the DNS entry nor the host file entry is available, Operations Manager will manage the device using one of its IP addresses. Details about which IP address is used to manage the device can be obtained from the IP Address Report. For further details, refer to the “Using Device Management” chapter in **User Guide for Cisco Unified Operations Manager**.

Configuring Cisco Unified Communications Manager Security Certificates

Apart from SNMP polling, Operations Manager runs AXL/SOAP queries on Cisco Unified Communications Manager to retrieve information from it. To secure this communication between Operations Manager and Cisco Unified Communications Manager, SSL must be enabled. This option is available for Cisco Unified Communications Manager 4.1 or later.

On Cisco Unified Communications Manager 4.1 or later, enable SSL on these virtual directories:

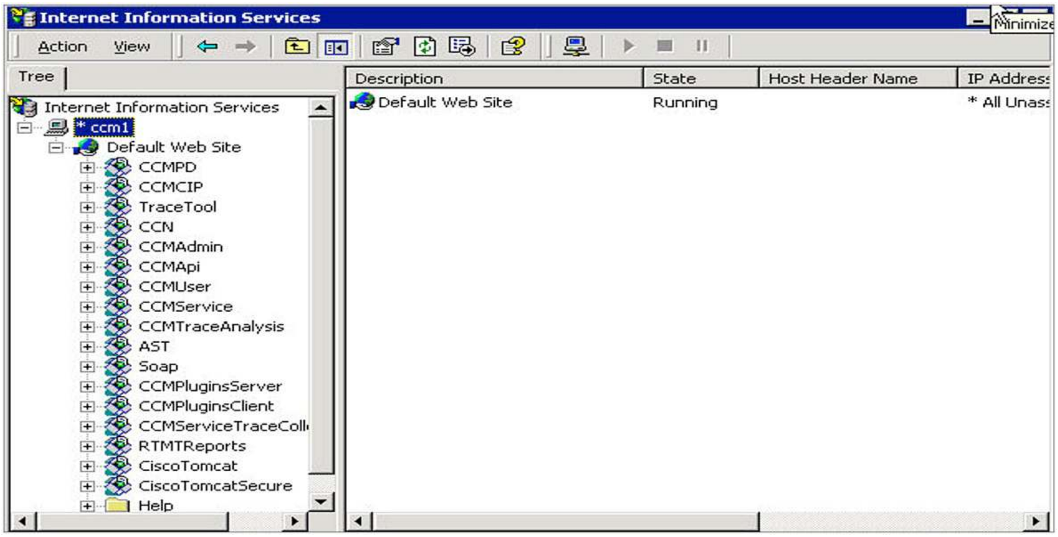
- CCMApi: Operations Manager uses services in this virtual directory to perform AXL/SOAP database queries.
- Soap: Operations Manager uses services in this virtual directory to perform AXL/SOAP device queries.

To enable SSL on virtual directories in Communications Manager 4.1 or later, do the following:

Step 1. On the Cisco Unified Communications Manager server, open Internet Services Manager by navigating to **Start > Programs > Administrator Tools > Internet Services Manager**.

Step 2. Click **CallManager** to expand it (Figure 5).

Figure 5. Communications Manager Internet Service Manager

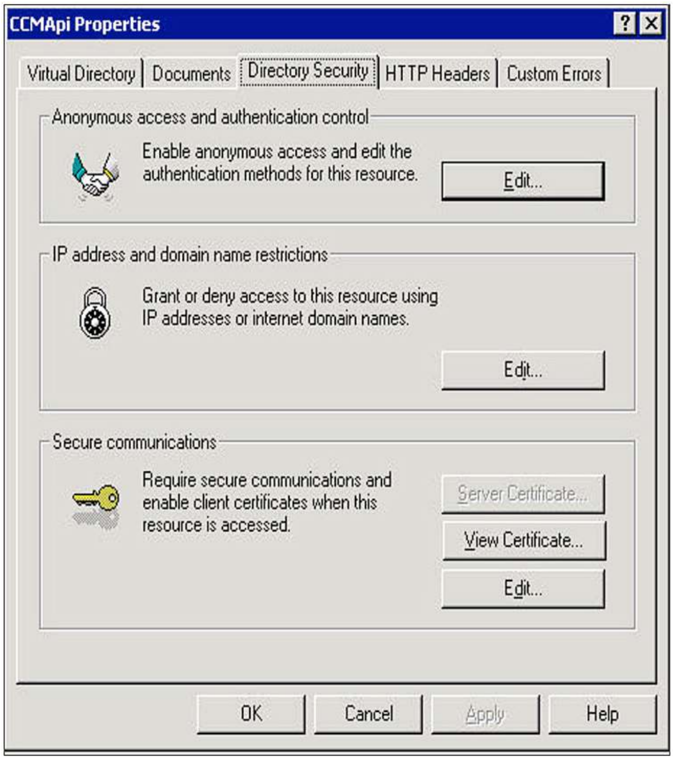


Description	State	Host Header Name	IP Address
Default Web Site	Running		* All Unass

Step 3. Right-click **CCMApi**, then click **Properties**.

Step 4. Select the **Directory** Security tab (Figure 6).

Figure 6. CCMApi Properties



CCMApi Properties

Anonymous access and authentication control

Enable anonymous access and edit the authentication methods for this resource.

IP address and domain name restrictions

Grant or deny access to this resource using IP addresses or internet domain names.

Secure communications

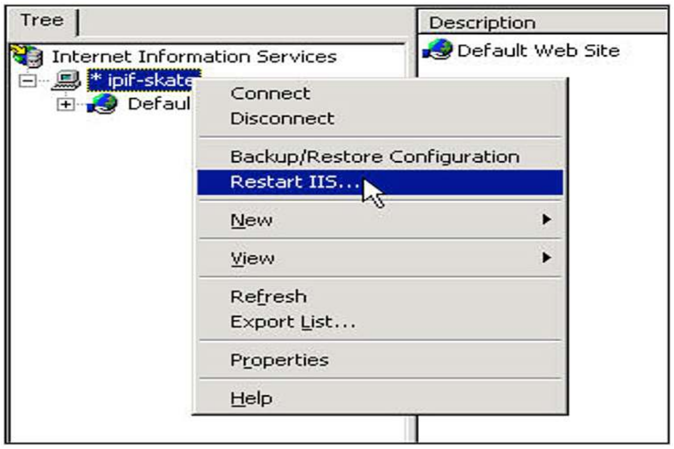
Require secure communications and enable client certificates when this resource is accessed.

Step 5. Under Secure Communications, click **Edit** and **select Require Secure Channel (SSL)**, then close the window.

Step 6. Repeat Step 3 and Step 4 for virtual directory Soap.

Step 7. Restart the web service. (For the select root node, above **Default Web Site**, right-click and select **Restart IIS**; see Figure 7.)

Figure 7. Restart IIS



Note: For more information, see the Cisco Unified Communications Manager Security Guide documentation.

From Operations Manager version 1.1 and later, the certificates are automatically imported into Operations Manager.

While adding devices, enter HTTP credentials. Operations Manager will automatically import the certificate.

Check Routing and Firewalls

Make sure that any firewalls between the Operations Manager server and the managed devices are configured to allow management traffic through. See the "Port Availability" section for information on which ports should be opened.

Also, make sure that there is connectivity between devices to be managed and the Operations Manager server. Even if a route exists to a network behind a managed device, that does not mean that one exists to (and from) the device itself.

Network Time Protocol

To be able to correlate events across multiple devices, the devices need to have the same perception of time. To achieve this, configure the Network Time Protocol (NTP) on the devices. For information on how to configure this functionality, refer to the Cisco device configuration documentation or http://www.cisco.com/univercd. NTP is not required for Operations Manager, but it will make it simpler to correlate real-world events to a real clock, especially across different time zones. NTP is required for Service Monitor and Cisco Unified Communications Manager to synchronize the reporting time for accurate CVTQ reports.

Port Availability

Before installing Operations Manager, make sure that the ports that Operations Manager uses are not already being used by your existing applications. Operations Manager uses the TCP and User Datagram Protocol (UDP) ports listed in the **Installation Guide for Cisco Unified Operations Manager 8.7**, located on Cisco.com at http://www.cisco.com/en/US/products/ps6535/prod_installation_guides_list.html. Table 1 lists the typical ports opened on the firewall.

Table 1. Typical Ports Opened on the Firewall

Port Number/Type	Direction
80/TCP	Operations Manager > Communications Manager, Cisco Unity, and other Unified Communications applications
8080/TCP	Operations Manager > Communications Manager 5.x and later
443/TCP	Operations Manager > Communications Manager 4.x, Cisco Unity, Unified Communications applications
161/UDP	Operations Manager > Communications Manager, Cisco Unity, other Unified Communications applications, and all other devices
162/UDP	Communications Manager, Cisco Unity, other Unified Communications applications, and all other devices > Operations Manager
7/ICMP	Operations Manager > Communications Manager, Cisco Unity, other Unified Communications applications, and all other devices
514/5666/UDP	Communications Manager, Cisco Unity, other Unified Communications applications, and all other devices > Operations Manager/Service Monitor
135 **All high ports between 1024 to 65535**	Operations Manager > Cisco Unity, Unified Communications applications **Note:** This is for WMI access.
22/TCP	Operations Manager/Service Monitor > Communications Manager 5.x and later
8443/TCP	Operations Manager/Service Monitor > Communications Manager 5.x and later

Port Number/Type	Direction
2000/TCP	Service Monitor > Cisco 1040 Sensor
2000/TCP	Operations Manager > Communications Manager **Note:** This is for synthetic tests.
16384 to 32767/UDP	Operations Manager > Target Phones **Note:** This is for synthetic tests.
2748/TCP	Operations Manager > Communications Manager **Note:** This is for JTAPI.
53/TCP	Operations Manager > DNS Server
123/TCP	Operations Manager > NTP Server
25/TCP	Operations Manager > SMTP server
162/UDP	Operations Manager > SNMP Trap Receivers
514/UDP	Operations Manager > Syslog Receivers
1741/TCP	Client Browser > Operations Manager
443/TCP	Client Browser > Operations Manager

Deployment Checklist

Table 2 provides a sample list of the recommended tasks to be carried out before adding devices. The aim of the deployment checklist is primarily to prove that the IP Telephony components are operational and manageable.

Table 2. Deployment Checklist

Task Number	Task Description	Pass/Fail Result
Cisco Unified Communications Manager Cluster		
1.	Configure Windows SNMP read community string in the Windows Local Computer Management MMC	
2.	Configure Communications Manager cluster name in the service parameter settings	
3.	Configure a Communications Manager user in Multilevel Administration (MLA) with READ Access (opsmanager)	
4.	Enable SSL for CCMapi and SOAP in the IIS MMC	
5.	Confirm that network firewall security allows proper connectivity • Communications Manager Admin • SNMP	
6.	Configure SNMP service to only allow Operations Manager server’s IP address	
7.	Configure NTP	
8.	Add Communications Manager publisher to Operations Manager	
9.	Add Communications Manager subscribers to Operations Manager	
Cisco Unity Server		
1.	Configure Windows SNMP read community string in the Windows Local Computer Management MMC	
2.	Install Unity Remote Serviceability Kit from http://www.ciscounitytools.com/ and configure element management systems (EMSs) to send traps to the Unity system	
3.	Configure Windows “opsmanager” user and add to the Administrators group	
4.	Configure NTP	
5.	Confirm that network firewall security allows proper connectivity	
6.	Configure SNMP service to only allow Operations Manager server’s IP address	
7.	Add Cisco Unity Primary/Failover to Operations Manager	
8.	If Cisco Unity has services disabled, change the managed state for the disabled Cisco Unity service in Operations Manager Detailed Device View to False	

Cisco Unified Contact Center Server		
1.	Confirm that the Microsoft SNMP service is disabled on all IPCC servers	
2.	Open the Cisco SNMP MMC and save the profile to the desktop	
3.	Configure windows “opsmanager” user and add to the Administrators group	
4.	Configure Cisco SNMP read community string	
5.	Confirm that firewall security allows proper connectivity	
6.	Configure SNMP service to only allow Operations Manager server’s IP address	
7.	Configure NTP	
8.	Add Contact Center Router servers to Operations Manager	
9.	Add Contact Center Peripheral Gateway servers to Operations Manager	
10.	Add Contact Center Queue Manager server to Operations Manager	
11.	Add Contact Center Historical Data Store server to Operations Manager	
Branch Office Voice Gateway		
1.	Configure access control list (ACL) to allow source IP addresses of Operations Manager servers	
2.	Configure SNMP read and write community strings on the gateway	
3.	Configure NTP	
4.	Confirm that the gateway hostname is unique and the loopback address is registered with DNS	
5.	Confirm that network firewall security allows proper connectivity	
6.	Add the voice gateway to Operations Manager	

Cisco 1040 Sensor		
1.	Configure the Dynamic Host Configuration Protocol (DHCP) scope to provide Option 150 with the IP address of the TFTP server	
2.	Connect Port 1 to a port configured for a single VLAN	
3.	Connect Port 2 to the SPAN port on the switch	
4.	Add the 1040 Sensor to Service Monitor	
5.	Copy the 1040 Sensor image file on the TFTP server	
6.	Copy the 1040 Sensor configuration file to the TFTP server	
7.	Add the 1040 Sensor to Service Monitor	
Cisco IP Phones		
	Confirm that all phones were discovered automatically when the Communications Manager server was added **Note:** Cisco has observed network ACLs preventing Operations Manager from accessing phones over HTTP. This causes IP phone reporting issues.	
Catalyst Switch		
1.	Configure SNMP ACL to allow Operations Manager servers	
2.	Configure SNMP on the switch	
3.	Configure NTP	
4.	Verify that Cisco Discovery Protocol is enabled	
5.	Add the LAN switch to Operations Manager	

Operations Manager Installation

Preinstallation Checks

- Dual homing (dual network interface card [NIC]), using two different IP addresses, is not supported on Operations Manager. If, during installation, you receive a warning message to edit a file named gatekeeper.cfg, then your server is dual homed, and you must disable one of the NIC interfaces before adding any devices to Operations Manager. Using two NICs with a single IP address (a failover configuration, in case one of the NICs fails) is supported.
- If you are using an IBM server, make sure that the Windows service **ibm director wmi cim server** is stopped and changed to Manual before installation. The installation program checks whether the **cim** server is running at the start of the installation process. If the service is running, the installation program displays the error message and stops.
- Net service disturbs some Operations Manager processes causing them not to operate normally. We recommend that you uninstall .Net service from the system before installing Operations Manager.
- Make sure that IIS is disabled before installation. If IIS is enabled when the installation program starts, the installation program displays an error message and stops.
- Make sure that you change the default Cisco Unified Communications Manager cluster ID setting (accessed from **Communications Manager Administration > Enterprise parameters**).

  The default setting is **StandAloneCluster**. Unless this entry is changed, all of the clusters will have the same cluster ID. This will result in problems in Operations Manager. Changing the cluster ID requires a restart of the CCMadmin service on all nodes. Perform these restarts on the publisher and then on the subscribers.

  Note: If Operations Manager is already managing the Cisco Unified Communications Manager and you are changing the cluster ID, then the cluster IDs in the service-level view will not reflect the new cluster ID. You have to delete and add the Cisco Unified Communications Manager in Operations Manager again for it to reflect the new cluster ID.
- Make sure that the Operations Manager server's hostname is resolvable using DNS. If DNS is not being used, edit the Windows host file and enter the Operations Manager hostname and IP address. The default location for the hosts file is C:\Windows\system32\drivers\etc.

```
# This file contains the mappings of IP addresses to hostnames. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding hostname.
# The IP address and the hostname should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
10.1.1.15 Operations Manager server.cisco.com

# add the Operations Manager server IP address and hostname entry
# into the hosts file if DNS is not being used on the network
```

Installation Procedures

If you do not have a license key, then during the installation, select the evaluation version.

Licensing and Registration of the Software

Licensing grants you permission to manage a certain number of phones. You can enter licenses for Operations Manager during installation or add them later. Also, there is a separate license for Service Monitor.

Uninstallation

It is a good practice to delete the C:\Program Files\CSCOpx folder and everything under %temp%, and then reboot the server after the Operations Manager application has been uninstalled from any server. Remember to save any Cisco 1040-related call metrics, performance, or node-to-node archived files that you might want to keep. This data is saved in the following location: C:\Program Files\CSCOpx\data.

Initial Configuration

Security and Users

Add the server name of the Operations Manager system in the local intranet of the client browser that you are accessing.

To add the server name in the local intranet of the client browser, do the following:

Step 1. Click the Internet icon at the bottom-right corner of the status bar on the browser.

The **Internet Security Properties** window appears.

Step 2. Click the **Local Intranet** icon.

Step 3. Click the **Sites** button and add the server URL.

When you do this, the status bar that appears on all popup windows is eliminated and the buttons at the bottom are visible.

IP Address or Hostname Changes

Make sure that the devices are not entered into Operations Manager or the Common Services Device Credential Repository (DCR) more than once. For instance, during device discovery, a router with multiple IP addresses may be discovered more than once, depending on the seed device or number of hops.

If you see the same device, either in Operations Manager or in the DCR, listed twice with two IP addresses, delete the device entirely from the system through the DCR. Add that device individually back into the DCR using a single IP address.

Network Discovery and Device Management

For Operations Manager to monitor a device, you must first add the device to the DCR, which is a function of CiscoWorks Common Services. The DCR can be synchronized with multiple CiscoWorks servers, running the same or different applications. This is called a Management Domain. Devices can be added to the DCR either through synchronization, one at a time, or by importing multiple devices. In Operations Manager, you can enable discovery, which detects devices and adds them to the DCR.

There are two device repository databases located in Operations Manager:

- Operations Manager device inventory: To view, select **Administration > Device Management > Device Configuration > Modify/Delete**.
- The DCR inventory: To view, select **Administration > Device Management > Device Configuration > Device Credentials**.

When you delete a device, it can be removed from either inventory. How Operations Manager is configured with the DCR determines from which inventory a device is deleted. For Operations Manager/DCR configurations, see the “Synchronizing with the DCR” section.

When a device is deleted, the inventory that it is removed from depends on the Operations Manager and DCR configuration:

- Standalone mode: The device is removed from both the Operations Manager and the DCR inventory.
- Master mode: The device is removed from both the Operations Manager and the DCR inventory.
- Slave mode: The device is removed only from the Operations Manager inventory.

After a device is in the DCR, you can select it to be monitored by Operations Manager. Operations Manager performs inventory collection periodically, polling for relevant information from the devices.

Network Discovery Options

There are two network discovery options: Cisco Discovery Protocol-based discovery and ping-based discovery. This section describes both options.

Cisco Discovery Protocol-Based Discovery

Operations Manager device discovery is based on Cisco Discovery Protocol, route table, and Address Resolution Protocol (ARP) table using a seed device. Operations Manager uses Cisco Discovery Protocol neighbors, ARP table, and route table entries to discover the network from the seed device.

Logical Cluster Discovery

Operations Manager device discovery is based on using Cisco Unified Communications Manager as a seed device. Operations Manager uses logical registration relationships to discover the clusterwide devices from the seed device.

When using 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
- Cisco Unified Communications Managers

Ping-Based Discovery

You can choose to add a ping sweep (by selecting the **Ping Sweep** check box) in addition to or instead of the Cisco Discovery Protocol, ARP table, and route table discovery process.

When using a ping sweep discovery, IP phones and other nonvoice devices (for example, network printers, Sun servers, or PCs) with an IP address in the specified ping sweep range will also be discovered. These devices are populated in the DCR and are placed in the unmanaged device state in Operations Manager.

Note that Operations Manager manages and discovers IP phones indirectly. Operations Manager discovers IP phones through querying the Layer 2 switch (to which the phones are connected) and the Cisco Unified Communications Manager (to which the phones are registered). Operations Manager does not directly manage the IP phones, since SNMP is not currently supported on the IP phones. IP phones are discovered because they respond to an Internet Control Message Protocol (ICMP) ping.

To avoid populating the DCR with network printers and other nonvoice network devices, use the IP Exclude filter on the Discovery page.

In IP telephony deployments, phones acquire their IP addresses from a DHCP server. This DHCP server usually has a pool of IP addresses configured for IP phones. The IP phone address pool can be specified in the IP exclude filter, thereby preventing IP phones from being populated in the DCR.

Credential Discovery and MIB II Information

Automatic discovery uses the list of credentials configured on the Credentials page (**Administration > Device Management > Device Configuration > Discovery Configurations > Credentials**) to determine the correct SNMPv2/v3 credentials and/or HTTP (or HTTPS) credentials for the device. After the correct credentials are determined, automatic discovery retrieves MIB II information from the device and populates this information in the DCR.

Autodiscovery IP Address Filters

Both the include and exclude filters can be applied for the automatic discovery process. The exclude filter is applied first, before the include filter. You provide the order of the filters in the include and exclude filter lists, and the filters are applied strictly in this order. After a device IP address satisfies a filter, other filters will not be applied to the device.

For example, suppose that you configure the filters as follows:

Exclude Filter	12.*.*.*, 12.12.*.*
Include Filter	*.*.*.*, 14.*.*.*

In the above case, the filter 12.*.*.* overrides 12.12.*.*, and so 12.12.*.* will never be applied and is thus not required. Similarly, *.*.*.* overrides 14.*.*.*.

The effect of these two filter lists operating in conjunction is that all device IP addresses except those in the range 12.[0-255].[0-255].[0-255] will be discovered and populated in the DCR.

Remember that the exclude filter is applied before the include filter.

Consider three devices with the IP addresses 12.12.12.12, 14.14.14.14, and 20.20.20.20. We show a few examples of filter settings that determine which of these devices are discovered and populated in the DCR, and which are excluded.

The following cases provide examples of possible device discovery filtering scenarios:

Case 1: Configuring using the include and exclude filters.

Device	—	14.14.14.14	20.20.20.20	12.12.12.12
Exclude Filter	12.*.*.*	Out of range	Out of range	Within range
Include Filter	14.*.*.*	Within range	Out of range	Not applied
Result	—	Included	Excluded	Excluded

Case 2: Include filter not specified, so the default (. *.*.*.*) is used.

Device	—	14.14.14.14	20.20.20.20	12.12.12.12
Exclude Filter	12.*.*.* - 13.*.*.*	Out of range	Out of range	Within range
Include Filter	Not specified, use default *.*.*.*	Within range	Within range	Not applied
Result	—	Included	Included	Excluded

Case 3: Exclude filter not specified, so the exclude filter is not applied.

Device	—	14.14.14.14	20.20.20.20	12.12.12.12
Exclude Filter	Not specified	Not applied	Not applied	Not applied
Include Filter	14.*.*.*	Within range	Out of range	Out of range
Result	—	Included	Excluded	Excluded

Case 4: No filters are specified, so all devices are included.

SysLocation Filter

The sysLocation filter is applied after the MIB II system table is queried from a device. Like the IP address filter, you can set include and exclude filters. The exclude filter is applied first. If the sysLocation of a device satisfies any of the specified exclude filters, the device is filtered out. The include filter is applied only if no exclude filters apply to the device. The device will be populated in the DCR if its sysLocation field matches one of the include filters.

DNS Domain Filter

The DNS filter works in a manner similar to the IP address and sysLocation filters. It performs a DNS lookup with a given IP address to resolve a DNS name, then checks the specified include or exclude filters with the DNS domain name. The exclude filter is applied before the include filter.

If multiple filters are specified, the IP address filters are applied first. The sysLocation filter is applied next, and finally, the DNS domain filter is applied. Because other filters are not applied after a filter specification is satisfied for a device, you should not specify a sysLocation filter and/or a DNS domain filter after the IP filters are specified. The sysLocation filter and the DNS domain filters will be applied (in that order) only if the IP address filters are not specified.

Phone Discovery

Phone discovery is performed separately from device discovery. Phone discovery starts after device discovery completes. In Operations Manager, go to **Administration > Device Management > Inventory Collection > IP Phone** to check the status of the last completed phone discovery.

When phones are discovered using a ping device discovery, those phones are placed in the Unknown state.

Cisco Catalyst 6000 Discovery

When discovering a Cisco Unified Communications Manager, Operations Manager discovers the trunk cards on a Cisco Catalyst device as gateways. If the Cisco Catalyst device is not being monitored in Operations Manager, the trunk cards will appear as grayed-out gateways in the service-level view until the Cisco Catalyst device is added and monitored by Operations Manager. When the Cisco Catalyst device is added to Operations Manager, the gateways associated with the trunk cards will be replaced with a single Cisco Catalyst icon in the service-level view.

Troubleshooting Discovery Issues

If you can ping the device from the Operations Manager server and yet device discovery fails, it is typically due to an SNMP problem such as a community string mismatch. Try to ping SNMP from the Operations Manager server.

From the command prompt, enter the following command:

```
sm_snmpwalk.exe -w -c <snmp community string> <device IP>
```

sm_snmpwalk.exe is located under C:\Program Files\CSCOpx\objects\smarts\bin folder on the Operations Manager server. For detailed command syntax, use the following command:

```
sm_snmpwalk.exe --help
```

Device Import Options

Device import can be achieved through the options detailed in the following subsections.

Discovery-Based Import

To add devices automatically into Operations Manager, go to **Administration > Device Management > Device Configuration > DCR Device Selection**. From the Device Selection page, select **Automatic** (the default device selection setting for Operations Manager).

Synchronizing with the DCR

Operations Manager uses CiscoWorks Common Services as its application framework. The DCR, a function of CiscoWorks Common Services, is a common repository of devices, their attributes, and their credentials required to manage devices in a management domain. The DCR lets you share device information among various network management applications.

For example, the device credentials can be shared between:

- Multiple instances of Operations Manager.
- Instances of Operations Manager and any CiscoWorks applications running on Common Services with compatible versions.

To share the device credentials, the DCR server can run in Master mode, Slave mode, or Standalone mode. You can change mode through the user interface or the DCR command-line interface.

To set up CiscoWorks LAN Management Solution (LMS) as DCR Master and Operations Manager as DCR Slave, do the following:

Step 1. Make sure that the hostnames of both machines are DNS/hostname resolvable (check the entries in c:\WINNT\system32\drivers\etc\hosts).

Step 2. Make sure that System Time on both machines is set to the same time zone (it will not work if they are set to different time zones).

There must be a Peer Server Account set up in the Master and a System Identity User set up in the Slave with the same username and password.

The self-signed certificates are present in the Master and Slave based on the information provided during Certificate Setup. Certificate Setup is accessed from **Administration > Server > Security > Single Server Management > Certificate Setup**. (Set up with Hostname/DNS name as Resolvable DNS Name while entering the information in Certificate Setup.)

Step 3. Restart the daemons in both machines.

Step 4. Add the certificates from Master to Slave and vice versa.

You can do this through Peer Server Certificate Setup, accessed from **Administration > Server > Security > Multi-Server Trust Management > Peer Server Certificate Setup**.

Step 5. In the Master, go to **Administration > Device and Credentials > Administration > Mode Settings**, and set it in the Master mode.

Step 6. In the Slave, go to **Administration > Device and Credentials > Administration > Mode Settings** and set it in the Slave mode and add the Master's Hostname.

Manual Device Import

To add one or more devices individually into Operations Manager, go to **Administration > Device Management > Device Configuration > Device Selection**. On the **Device Selection** page, you can add a single device at a time into the system. Make sure that the Cisco Remote Serviceability Kit is installed on all Cisco Unity and Cisco Unity Connection servers.

Device Discovery Process

Device States

- Monitored: The device has been successfully imported and is fully managed by Operations Manager. All devices should be in the Monitored state.
- Partially Monitored: The Cisco Unified Communications Manager has been successfully imported in Operations Manager, but only using SNMP. If a device is in this state, you should check the HTTP credentials and make sure that the device becomes fully monitored. HTTP credentials are needed for Cisco Unified Communications Manager and Cisco Unified Presence Server.
- Monitoring Suspended: Monitoring of the device is suspended.
- Inventory Collection in Progress: Operations Manager is probing the device. This is the initial 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. This can occur if the device cannot be pinged, if SNMP service is not enabled, or if the RO community string provided is incorrect, SNMP may be blocked.
- Unsupported: The device is not supported by Operations Manager. IP phones discovered using a ping sweep will be placed into this category.

The blue number in the Number of Devices column is a hyperlink that brings up device information.

You can determine the reason why a device is unreachable on the Modify/Delete Devices page (**Administration > Device Management > Device Configurations > Modify/Delete Devices**). In the **Modify/Delete Devices** page, open the **All Unreachable** devices (or **Unsupported**) folder. Click the device name/IP address (not the check box). The Data Collector Status Information section provides a detailed error code.

Device Discovery Best Practices

- For small deployment, use a Cisco Unified Communications Manager and a core router as the seeds for discovery using Cisco Discovery Protocol. This will trigger discovery of all clusters, gateways, CTI-based IP Telephony (IPT) applications registered to the clusters, and gatekeepers.
- For big deployment, use publisher IP addresses as the seed device to run Logical Cluster Discovery instead. This will trigger discovery of Communications Managers, Unity servers, gateways, CTI-based IPT applications registered to the clusters, and gatekeepers. The discovery is controlled at cluster level.
- Exclude the devices that you do not wish to locate or discover. This will reduce the pool of unreachable devices.
- Use ping sweep if you see some devices getting excluded in the Communications Manager and core router-based seed discovery.
- Generally, more hops lead to higher discovery time. For all practical purposes, three hops should be considered sufficient.
- If you have many different combinations of community strings, your discovery time will increase.

Resolving Discovery Conflict

- Gateways associated with a Cisco Unified Communications Manager are discovered during the Cisco Unified Communications Manager discovery process. You may see a grayed-out gateway in the service-level view. This occurs when a gateway is discovered through Cisco Unified Communications Manager, but the gateway is not monitored in Operations Manager.
- There are situations when T1 cards on Cisco Catalyst 6000 switches are discovered by Operations Manager, through Cisco Unified Communications Manager discovery, and are represented as individual gateways.

  If a Cisco Catalyst 6000 is not being monitored in Operations Manager, the T1 cards appear in the service-level view as individual, standalone, grayed-out MGCP gateways. After the Cisco Catalyst 6000 is monitored by Operations Manager, these gateways are no longer displayed in the service-level view and are replaced by a single Cisco Catalyst 6000 icon.
- Make sure to change the default Cisco Unified Communications Manager cluster ID setting. The cluster ID is set to **StandAloneCluster** by default. Unless you change this entry, two clusters will have the same cluster ID, which will lead to a problem in Operations Manager. Please note that cluster ID name changes require a restart of Cisco Unified Communications Manager service, first on the publisher and then on the subscribers.

Diagnostic Tests

Synthetic Tests

Synthetic testing is a mechanism by which Operations Manager emulates a phone. For example, Operations Manager makes phone calls, logs into conferences, leaves voice mails, makes emergency calls, and downloads TFTP files.

Note: MAC addresses for synthetic phones must be between 00059a3b7700 and 00059a3b8aff.

When a synthetic test is unsuccessful, it generates one of the following events:

- SyntheticTestFailed: Individual test failed.
- TooManyFailedSyntheticTests: Out of a sample of four tests, the actual percentage of tests that failed exceeds the value of threshold.
- MWIOnTimeExceeded: Number of seconds in which the Cisco Unity message waiting indicator (MWI) light appears exceeds the value of the MWI on-time threshold.
- SyntheticTestsNotRun: Tests were not run for more than 10 minutes on the Operations Manager server (possibly because of insufficient CPU).

Synthetic tests are supported on a variety of applications: Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, TFTP Server, Cisco Conference Connection, Cisco Emergency Response, Cisco Unity, and Cisco Unity Express. The synthetic tests can be scheduled to be run on a periodic basis.

Synthetic Test Descriptions and Expected Results

Table 3 describes the synthetic tests and gives the expected results.

Table 3. Synthetic Test Descriptions

Synthetic Test	Description	Expected Results
Phone Registration	Opens a connection with Cisco Unified Communications Manager/Cisco Unified Communications Manager Express and registers a simulated IP phone.	Successful registration of the phone.
Off-Hook	Simulates an off-hook state to Cisco Unified Communications Manager/Cisco Unified Communications Manager Express and checks for receipt of a dial tone.	Receives a dial-tone signal from Cisco Unified Communications Manager. The registration of the synthetic phone takes place only for the first time because registration is a costly operation on Cisco Unified Communications Manager. However, if the test fails, then synthetic phones are registered again for the next test cycle only. After the synthetic phone is registered, Operations Manager checks for a dial-tone signal from Cisco Unified Communications Manager.
End-to-End Call	Initiates a call to a second simulated or real IP phone.	• Registers, goes off-hook, and places the call. • Ring indication. • Destination phone goes off-hook to accept the call. If **call progress tones and announcements** are configured on the gateway for your end-to-end call, the test may succeed even before the phone rings or after a couple of rings. This indicates that your gateway is working correctly. It can also confirm that the destination route pattern is correct. The registration of the phone occurs only during the first test because registration is a costly operation on Cisco Unified Communications Manager/Cisco Unified Communications Manager Express. However, if the test fails, the registration will occur for the next test cycle only. Enable RTP transmission: Operations Manager plays a recorded announcement upon answer. Use this feature in conjunction with the Cisco 1040 Sensor and Service Monitor to monitor the quality of voice (QoV) of the test call.
TFTP Receive Test	Performs a TFTP get-file operation on the TFTP server.	Successful download of a configuration file from the TFTP server.

Synthetic Test	Description	Expected Results
Emergency Call Test	Initiates a call to the emergency number to test the dynamic routing of emergency calls.	• All calls initiated. • Ring indication on Public Safety Answering Point (PSAP) and On Site Alert Number (OSAN), if configured.
Cisco Conference Connection Test	Creates a conference (meeting) in the Conference Center and connects to the meeting.	• Conference created with the specified meeting ID. • Call initiated. • First person and second person (if configured) successfully connect to the conference.
Cisco Unity Message Waiting Indicator Test	Calls the target phone and leaves a voice message in the voice mailbox.	Activation of the phone's message-waiting indicator. The message is then deleted and the message-waiting indicator is deactivated.

How Many Simulated IP Phones Do I Need?

The number of simulated IP phones you need to define in Cisco Unified Communications Manager/Cisco Unified Communications Manager Express depends on the number of tests you plan to configure. Different types of confidence tests need a different number of IP phones. See Table 4.

A predefined MAC address range has been set aside for these IP phones so that it does not clash with any of the real IP phones or devices in the network. The MAC address range that is available for synthetic testing is between 00059a3b7700 and 00059a3b8aff.

It is recommended that you input the description for these IP phones as **Operations Manager Simulated Phone** when they are configured in Cisco Unified Communications Manager/Cisco Unified Communications Manager Express so that it is distinct from the descriptions of other IP phones in Cisco Unified Communications Manager/Cisco Unified Communications Manager Express. The phones to be used in confidence testing must be configured as 7960 phones in Cisco Unified Communications Manager/Cisco Unified Communications Manager Express.

Table 4. Number of Phones Required for Confidence Tests

Type of Test	Phones Needed for Test	Total Phones Needed
Phone Registration	1 (synthetic phone)	1 per Cisco Unified Communications Manager and Communications Manager Express
Off-Hook	1 (synthetic phone)	1 per Cisco Unified Communications Manager and Cisco Unified Communications Manager Express
End-to-End Call test with real phones	2 (1 synthetic phone and 1 real phone)	2 per Cisco Unified Communications Manager and Cisco Unified Communications Manager Express
End-to-End Call test with synthetic phones	2 (synthetic phones)	2 per Cisco Unified Communications Manager and Cisco Unified Communications Manager Express
TFTP Receive Test	0	
Emergency Call Test (without on-site alert number)	2 (synthetic phones)	
Emergency Call Test (with on-site alert number)	3 (synthetic phones)	
Cisco Conference Connection Test	2 (synthetic phones)	
Cisco Unity Message-Waiting Indicator Test	2 (synthetic phones)	

Creating Synthetic IP Phones in Cisco Unified Communications Manager

To define simulated phones in Cisco Unified Communications Manager for the synthetic tests, do the following:

Step 1. Launch and log in to the Cisco Unified Communications Manager Administration page.

Step 2. From the Cisco Unified Communications Manager Administration tool, select from the menu **Device > Add a New Device**.

Step 3. Change the device type from the drop-down menu to **Phone** and click **Next**.

The phone type for the simulated phone must be Cisco 7960.

Step 4. Select this model as the phone type and click **Next.**

Step 5. In the Phone Configuration window, enter a MAC address between 00059a3b7700 and 00059a3b8aff.

The tool automatically fills in the Description field. Other required fields are Device Pool and Button Template. Keep the default values for these fields.

Step 6. Click **Insert**.

Schedule an IP Phone Discovery; it must complete before the new synthetic IP phone can be used in the synthetic test.

Node-to-Node Tests

Node-to-node tests are typically used to measure jitter, packet loss, and delay on synthetic test traffic generated by the Cisco IOS IP SLA on any Cisco IOS device across a WAN.

Preparing Devices for Node-to-Node Tests

The IP SLA is enabled manually in Cisco IOS Software. You may need to configure, depending on the Cisco IOS device, the RTR Responder, or the IP SLA Responder command-line interface (CLI). The codec type for the jitter test is supported only on certain versions of Cisco IOS Software (specifically, 12.3(4)T and later). Therefore, it is possible that the codec type selection might be grayed out based on the source device you choose.

Node-to-Node Test Events

The events are raised on the source device. A threshold event is generated when the threshold violation occurs for three consecutive polling cycles. The event is cleared if the value falls below the threshold in the following polling cycle.

The following node-to-node events can be generated:

- NodeToNodeTestFailed
- RoundTripResponseTime_ThresholdExceeded
- RingBackResponseTime_ThresholdExceeded
- RegistrationResponseTime_ThresholdExceeded
- AverageLatency_ThresholdExceeded
- PacketLossSD_ThresholdExceeded
- PacketLossDS_ThresholdExceeded

Batch Tests

Batch tests help enable you to test the health and connectivity of a branch office. Batch tests consist of a set of synthetic tests that are run on voice applications (for instance, Cisco Unified Communications Manager Express or Cisco Unity Express) that are deployed in a branch office and a set of phone tests that are run on real phones in the branch office. Batch tests can be run on demand for troubleshooting purposes or on a scheduled basis to verify the health of the voice network in the branch office.

The batch test import file is an XML file. You can find the template of an import file in the <NMSROOT>\Importfiles folder. You should create your own XML file by modifying the template file batchtest.xml, and then create the batch test by importing your XML file (**Diagnostics > Batch Tests > Create**).

If you encounter an error message similar to The batch test import file has fatal errors. Please correct the import file and import again, verify that your seed file is formatted correctly. See the **User Guide for Cisco Unified Operations Managers 8.6** for more details (available at http://www.cisco.com/en/US/products/ps6535/prod_installation_guides_list.html).

Operations Manager saves the data collected by the batch tests to disk. Batch test data is stored on the Operations Manager server in the following location: NMSROOT\data\bt.

Understanding Phone Tests

The phone tests that are run as part of batch testing take control of a real phone in the network and make a call from that phone to another phone. Phone tests use JTAPI credentials. These credentials must be included in the batch test import file.

Note: In a single batch test, do not create phone tests that include both Cisco Unified Communications Manager 4.x and Cisco Unified Communications Manager 5.x. You can create a single batch test that includes different versions of Cisco Unified Communications Manager 4.x, or a single batch test that includes different versions of Cisco Unified Communications Manager 5.x, but do not combine 4.x with 5.x.

Table 5 describes the different phone tests that are used in batch testing.

Table 5. Phone Test Descriptions - Batch Tests

Test	Description
Call	Takes control of a phone and places a call to a given number. The call can be from a real phone to a number, in which case the test is controlling the caller only. Alternatively, the call can be from a real phone to a real phone, in which case the test is controlling both the caller and the receiver.
Call Hold	Takes control of two phones and performs the following: • Places a call from phone A to phone B. • Has phone B put the call on hold. • Disconnects the call.
Call Forward	Takes control of three phones and performs the following: • Places a call from phone A to phone B. • Forwards the call to phone C from phone B. • Verifies that the call is received by phone C. • Disconnects the call.
Call Park	Takes control of three phones and performs the following: • Places a call from phone A to phone B. • Has phone B park the call. The call disappears from phone B and a message is displayed to tell you where the call is parked (for example, Call Park at 80503). • Has phone C dial the number where the call is parked. The parked call is transferred to the phone that you made the call from. • Disconnects the call.

Test	Description
Call Transfer	Takes control of three phones and performs the following: • Places a call from phone A to phone B. • Gets phone B to transfer the call to phone C. • Gets phone C to accept the call. • Disconnects the call.
Conference	Takes control of three phones and performs the following: • Places a call from phone A to phone B. • Places a conference call from phone A to phone C. • Disconnects the call.

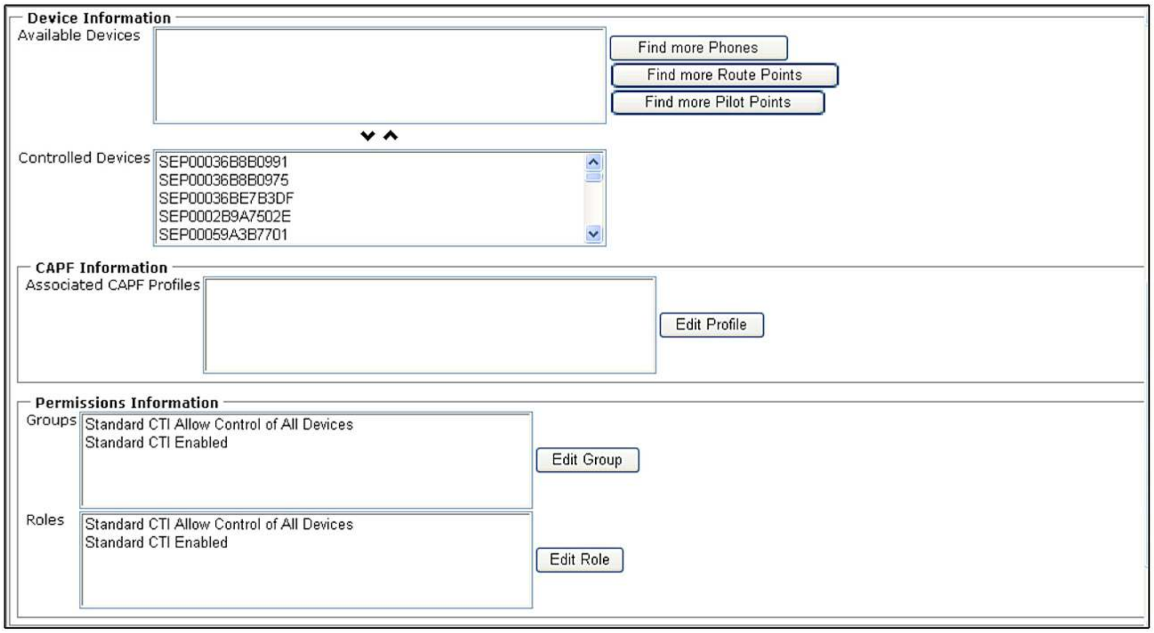
When you are creating a JTAPI application user, make sure of the following:

- Cisco Unified Communications Manager 4.x: All the test phones and test probes need to be associated with the JTAPI application the user created for phone testing (this can be done by using the **Device Association** option). Also make sure that the following options are enabled in the JTAPI User configuration:

  Enable CTI Application Use
  Enable CTI Super Provider
  Call Park Retrieval Allowed
  Enable Calling Party Number Modification

- Communications Manager 5.x/6.x: All the test phones and test probes need to be controlled devices for the JTAPI application the user created for phone testing. Also make sure the JTAPI application user is assigned to the Standard CTI Enabled group and the Standard CTI Allowed Control of All Devices group, as shown in Figure 8.

Figure 8. Communications Manager 5.x JTAPI User Setup



Device Information
Available Devices
Controlled Devices
SEP00036B8B0991
SEP00036B8B0975
SEP00036BE7B3DF
SEP0002B9A7502E
SEP00059A3B7701

CAPF Information
Associated CAPF Profiles

Permissions Information
Groups
Standard CTI Allow Control of All Devices
Standard CTI Enabled
Roles
Standard CTI Allow Control of All Devices
Standard CTI Enabled

You also need to include test phones and test probes in an XML file. Test phones are the phones that actually perform the phone functionality (call, call forward, call conferencing, call park, and call hold). Test probes are the other phones that participate in the phone tests.

For instance, the call conference test would be:

- Place a call from phone A to phone B
- From phone A, conference to phone C

You should define phone A as a test phone and phones B and C as test probes in XML.

The call-forward test would be:

- Place a call from phone A to phone B
- Forward the call to phone C by way of phone B
- Verify that the call is received by phone C

Then, in your XML test file, define phone A as a test phone, and define phones B and C as test probes.

Resolving Batch Test Failure

No events or alerts are generated when a component of a batch test fails. You must use the Batch Test Results report to see the results of a batch test. A new Batch Test Results report is generated every 24 hours for each batch test. The Batch Test Results report provides any error message for the individual tests that are a part of the batch test, and this might help you resolve the batch test failure.

- When the error message displayed is Unable to create provider - Connection refused: connect: Make sure that Cisco Unified Communications Manager CTI service is activated and the JTAPI user is created on Cisco Unified Communications Manager.
- When the error message displayed is Unable to create provider - bad login or password: Make sure that you include the same JTAPI user/password you have defined on Cisco Unified Communications Manager in the XML file.
- When the error message displayed is Invalid phone address XXXX for the CCM XXXX: Make sure that test phones and test probes are associated with the JTAPI user in the Cisco Unified Communications Manager configuration.
- When the error message displayed is Address XXXX is not in provider’s domain: Make sure that test phones and test probes are in your phone inventory. Run the phone inventory collection to bring newly added phones to the Operations Manager inventory.
- When the error message displayed is The test did not complete in the stipulated 30 seconds: Make sure no other synthetic test is run on the same test phones and test probes. It is also recommended that you run the individual test manually if you expect the test to be successful.

Managing Alerts and Events

The Fault Monitor display provides real-time information about the operational status of your network. The displays are designed so that you can set them up and leave them running, providing an ongoing monitoring tool that signals you when something needs attention. When a fault occurs in your network, Operations Manager generates an event and is shown on your Fault Monitor.

You can reduce the number and types of events that you see in any of the following ways:

- Suspend monitoring for the device or device component.
- Suppress events at device level or global level (for more information, refer to **User Guide for Cisco Unified Operations Manager 8.7**., located on Cisco.com at http://www.cisco.com/en/US/products/ps6535/products_user_guide_list.html.
- Filter the events displayed on Fault Monitor.
- Update thresholds; for instance, disable thresholds for interfaces.

For instance, you can stop alerts for an IP telephony application that you have disabled on Cisco Unified Communications Manager intentionally. To do so, do the following:

Step 1. Select **Administration > Device Management > Device Configuration**. The Device Management: Summary page appears. Locate the device state for which you want to view the devices. In the number column that corresponds to the device state, click the number. A report appears, listing the device information. Click a device in the **Device Name** column.

The Detailed Device View opens.

Step 2. In the Detailed Device View, do the following:

a. Select **Voice Services** from the Applications folder.

b. Locate the specific voice application in the table and change the value in the Managed State column to False.

c. Click **Submit**.

The voice application will no longer be monitored.

If you have interfaces that are connected to carrier networks and not routed internally, you can suspend monitoring for an interface by doing the following:

Step 1. From the Device Report, click a device in the Device Name column.

The Detailed Device View opens.

Step 2. In the Detailed Device View, do the following:

a. Select the interface type in the Interfaces folder.

b. Locate the specific interface in the table and change the value in the Managed State column to False.

c. Click **Submit**.

When you stop monitoring a device - changing its monitored state to False - Operations Manager no longer polls that device for information. Subsequent events (including traps) are ignored and no longer processed.

Notification Services

The customization that is available for the northbound notification is extensive. If there is a messaging gateway to the paging system, e-page subscriptions can also be set up.

Most large enterprises have their own domain managers already running in their management systems. Therefore, the SNMP traps generated by Operations Manager are helpful in integrating Operations Manager with other managers such as Cisco Info Center, HP OpenView Network Node Manager (NNM), or Tivoli Netview.

The email and e-page notification mechanisms provide additional ways of informing network operations personnel about the alerts in their network. This helps ensure that network personnel do not have to monitor the real-time fault view throughout the day.

Event Sets

Operations Manager sends notifications based on violation of thresholds as defined in Polling and Thresholds (**Administration > Polling and Thresholds**). Various attributes are constantly polled from all the devices monitored by Operations Manager. Event sets allow you to selectively pick the events of interest and then associate those events to a particular list of devices.

This feature is useful in situations where the support for devices, or device types, or expertise is split across multiple departments or personnel.

Notification Criteria

Notification criteria allow you to set up notifications based on devices or service quality parameters. When setting up email notifications, make sure the following are taken care of in the Operations Manager server:

- Port 25 is open for the email notification.
- If VirusScan is installed, go to **Virus Scan > Properties > Blocking** and make sure **Block the connection** is left unchecked.

Event Customization

Change the default event titles to suit the deployed environment. You can also change the severity level on the event. Several customization features are available for setting up the northbound notification.

CISCO-EPM-NOTIFICATION-MIB

CISCO-EPM-NOTIFICATION-MIB is specifically defined to carry details of events generated by Operations Manager. This MIB needs to be compiled into the manager of managers to decode the SNMP trap received from Operations Manager.

The MIB description covers in detail what each attribute carries. See the online help for information on attributes and possible values (where applicable). Every SNMP Trap PDU generated from Operations Manager contains the following attributes:

- cenAlarmVersion
- cenAlarmTimestamp
- cenAlarmUpdatedTimestamp
- cenAlarmInstanceID
- cenAlarmStatus
- cenAlarmStatusDefinition
- cenAlarmType
- cenAlarmCategory
- cenAlarmCategoryDefinition
- cenAlarmServerAddressType
- cenAlarmServerAddress

- cenAlarmManagedObjectClass
- cenAlarmManagedObjectAddressType
- cenAlarmManagedObjectAddress
- cenAlarmDescription
- cenAlarmSeverity
- cenAlarmSeverityDefinition
- cenAlarmTriageValue
- cenEventIDList
- cenUserMessage1
- cenUserMessage2
- cenUserMessage3
- cenAlarmMode
- cenPartitionNumber
- cenPartitionName
- cenCustomerIdentification
- cenCustomerRevision
- cenAlertID

The following is the format of values contained in a few key attributes:

cenAlarmInstanceID: Contains the alphanumeric value assigned to the event. This is a unique value defined throughout the Operations Manager system at any given time.

cenAlarmStatus and **cenAlarmStatusDefinition:** cenAlarmStatus contains a numeric value associated with the event status. The possible cenAlarmStatus values in Operations Manager are 1, 2, and 3.

cenAlarmStatusDefinition contains the <numeric value> <status description> of the event. The <numeric value> will contain the same value as in cenAlarmStatus. The <status description> provides the string representation of the status.

The possible values for cenAlarmStatusDefinition in Operations Manager are:

- 1-Acknowledged
- 2-Active
- 3-Cleared

cenAlarmCategory and **cenAlarmCategoryDefinition:** cenAlarmCategory contains a numeric value associated with the category under which the latest event was generated for the device. The possible cenAlarmCategory values in Operations Manager are 0 through 9.

cenAlarmCategoryDefinition contains the <numeric value> <category description> of the last processed event. The <numeric value> will contain the same value as in cenAlarmCategory. The < category description > provides the string representation of the category.

The possible values for the Operations Manager are:

- 0-Unknown
- 1-Application
- 2-Environment
- 3-Interface
- 4-Reachability
- 5-Connectivity
- 6-Utilization
- 7-System Hardware
- 8-Security
- 9-Other

cenAlarmDescription: The attribute will contain details for the event.

cenAlarmSeverity and **cenAlarmSeverityDefinition:** cenAlarmSeverity contains a numeric value associated with the event severity. The possible values for the cenAlarmSeverity values in Operations Manager are 1 through 7. cenAlarmSeverityDefinition contains the <numeric value> <severity description> of the alert. The <numeric value> will contain the same value as in cenAlarmSeverity. The <severity description> provides the string representation of the severity.

The possible values for cenAlarmSeverityDefinition in Operations Manager are:

- 1-Informational
- 2-Warning
- 3-Critical
- 4-Undefined
- 5-Undefined
- 6-Undefined
- 7-Undefined

cenCustomerIdentification and **cenCustomerRevision:** These two attributes are free-format text fields. The end users can use it for a further level of customization. These fields are filled in by the user at the time of Notification Criteria setup. If these two fields were not filled in, then the default values are a hyphen "-" for cenCustomerIdentification and an asterisk "*" for cenCustomerRevision.

Performance and Capacity Monitoring

The performance data is stored for a period of 72 hours, in the following location: C:\Program Files\CSCOpx\data\gsu_#GSUdata#_. If the user wants data for more than 72 hours, the comma-separated value (CSV) files have to be manually copied to another location.

The node-to-node test results are stored for 31 days, in the following location: C:\Program Files\CSCOpx\data\N2Ntests. For more information, see Chapter 7 and Appendix I in **User Guide for Cisco Prime Unified Operations Manager**.

A unique file is created for each device per day with a date stamp as part of the filename. At the beginning of every day, a new file is created. If monitoring is done for 4 days starting at 0 hours, on the fourth day there will be three full-day files and one partial-day (in-progress) file. On the fifth day, the file created on the first day is deleted.

If no data is collected for a 24-hour period, a data file will not be created. However, if partial data is collected, a file will be created with "*" filled in for fields that do not have collected data. Partial data collection can happen if the device responded to some queries but not all.

Operations Manager updates these files every polling cycle. The default is every 4 minutes, which can be changed.

Note: While working with performance graphs, we recommend the following:

- If you are not able to collect performance data and you do not see an error message (either a popup message or a message in the log file) indicating the problem, you should verify the status of the device.
- If a gray line or a gray area appears in a graph, hover your mouse over it to obtain a tooltip with an explanation.
- To collect performance data for Cisco Unity Connection, Cisco Unity, or Cisco IP Contact Center, the Windows Management Instrumentation credential is required. When adding these devices to Operations Manager, verify that the WMI username and password are provided.

Enabling or Disabling Monitoring

To enable or disable performance monitoring, you must first enable polling (voice utilization settings) from **Administration > Polling and Thresholds**.

Trending and Alerting

Operations Manager can view performance trends within a 72-hour period. When thresholds are crossed, an alert is generated. See the appendix of the user guide for details on the archived files.

Capacity Planning Use

Archive the performance data periodically (within 72 hours). Use this data to view longer trends (longer than 72 hours). A spreadsheet application such as Microsoft Excel can be used to view CSV files. See the **User Guide for Cisco Prime Unified Operations Manager** appendix for details on the archived files.

Polling and Thresholds

Operations Manager is configured with default settings for polling parameters and threshold values. You can use the default settings, edit them, and restore them to default settings at any time.

How Do I Change Polling and Threshold Values?

You can access polling parameters from **Administration > Polling and Thresholds**.

If you change some server settings - for instance, Managed State to False so monitoring is disabled - upon rebooting the server, all settings return to default.

To make sure that Operations Manager persists these changes, you must manually go to **Administration > Polling and Threshold > Apply Changes** and click **Apply**. (Please note that Operations Manager sometimes disallows **Apply** under certain conditions. In such cases, you can force **Apply** by changing some polling settings and then retrying the "Apply" operation.)

Note: XML files that have the factory default settings for polling frequency and threshold parameters for the various device types and metrics are available in the following location: C:\Program Files\CSCOpx\objects\ptm\config.

PTADefaultSettings_cs.xml has default data settings.

PTADefaultSettings_vhm.xml has default voice health settings.

PTADefaultSettings_gsu.xml has default voice utilization settings.

Trap Receiving and Forwarding

Trap receiving and forwarding are configured on the system preferences page (**Administration > Miscellaneous > Preferences**).

This feature should not be confused with SNMP notifications. This feature is to forward traps to a manager of managers.

SRST Monitoring

Survivable Remote Site Telephony monitoring is achieved by configuring the SAA jitter test between the source router (Head Office Router) and the target router (Branch Office Router) configured for SRST.

Setting Up and Managing SRST Tests

Survivable Remote Site Telephony tests are only configurable on SRST devices. This test will not appear on other device types. You can access SRST tests from **Administration > SRST Poll Setting**.

SRST tests use a ping, originated by an IP SLA device to the SRST gateway device. Also, Operations Manager checks the status of the SRST phone. If the ping to the SRST gateway fails or the SRST phone becomes unregistered from Cisco Unified Communications Manager, Operations Manager determines the branch office to be in SRST mode and displays a list of Cisco IP phones that are in SRST mode on phone reports. When the WAN link is up, Operations Manager generates an SRSTEntered event.

When the WAN link is up and all phones in the branch office are unregistered with the central Cisco Unified Communications Manager, Operations Manager generates an SRSTSuspected event after all SRST phones remain unregistered for two IP phone move tracking cycles. The default IP phone move tracking cycle is 5 minutes.

When creating an SRST test, the IP SLA device should be the Cisco IOS device closest to the Cisco Unified Communications Manager serving that SRST remote office, preferably on the same subnet as the Cisco Unified Communications Manager. The destination router is the SRST gateway. Make sure to choose an SRST remote office phone. You can use the IP phone report to select the phone.

Best Practices

Server Maintenance

A test with a 16-hour polling cycle and a 1-minute sampling interval uses approximately 60 to 100 KB per day. A path echo test with a 16-hour polling cycle, a 1-minute sampling interval, and 12 hops uses approximately 1.2 MB per day.

Disabling Hyperthreading

Hyperthreading may affect inventory collection and device rediscovery performance, as there are many processes and threads involved in these tasks in Operations Manager, leading to an extremely high rate of context switches. Consequently, as the processor switches from one hyperthread to another, cache lines may get invalidated too quickly and too frequently, causing overall degradation in CPU performance.

If performance is found to be inadequate on hyperthreaded processors, disabling hyperthreading on the Operations Manager server may result in better overall performance.

The following procedure may vary, depending on the vendor:

Step 1. Enter the BIOS Configuration and Setup screen by powering up the server and pressing F1 during system startup.

Step 2. Go to **Advance Setup > Advance Processor Option > Hyperthread**.

Step 3. Select **Disabled**.

Step 4. Press **Esc** to return to the main menu.

Step 5. Select **Save Settings**, and press **Enter**.

Step 6. Select **Exit Setup**, and press **Enter** to continue the reboot process with hyperthreading disabled.

Cold Standby/Redundant Deployments

You can use two servers and achieve a cold standby configuration. One Operations Manager server is used as the active server and the other server is left on cold standby and periodically synchronized with the active server using the servers' DCRs. When the active server is taken offline, the cold server will have an up-to-date inventory and can quickly be made active.

Preparing for Redundancy

This section describes some prerequisites for redundant Operations Manager configurations.

The first step is to have two identical servers available for configuration. One server acts as the active server and the second as the standby server. Refer to the Operations Manager installation guide for the hardware specification of these servers. It is recommended that these servers connect to the network through redundant paths. This helps ensure that a failure in one part of the network that affects the active server does not also affect the connectivity of the standby server.

Setting Up Redundancy

Redundant deployment can be considered in four parts:

1. Setting up the active Operations Manager server.
2. Setting up the standby Operations Manager server by creating a baseline.
3. Replicating the active Operations Manager server configuration on the standby Operations Manager server on an ongoing basis.
4. Tasks to be performed in case of failure of the active server.

Setting Up the Active Operations Manager Server

This is the same as setting up a standalone Operations Manager server. Typical tasks include:

- Setting up users and associating roles
- Providing a device list by manually adding devices or syncing up with LMS Device Credential Repository or discovering the network using a seed device
- Setting up the polling intervals based on your monitoring requirements (the default is 4 minutes)
- Creating phone status tests
- Creating synthetic tests

- Creating node-to-node tests
- Setting up SRST polling by creating SRST tests
- Enabling performance polling
- Setting up notification profiles for northbound notifications
- Configuring Service Monitor to forward traps to Operations Manager
- Configuring Cisco 1040 Probes to register to Service Monitor
- Configuring system preferences such as forwarding trap servers, trap community strings, and SMTP servers for northbound notifications and cross-launchable LMS servers

Refer to the user guide for an explanation of each task.

Setting Up the Standby Server

Once the active server is set up, the standby server needs to be set up in such a way that it has exactly the same configuration as the active server. This can be achieved using the Backup and Restore feature in Operations Manager. The procedure to back up and restore files is detailed below.

Backup

Go to the Active Operations Manager server:

```
<INSTALL_DIR>\bin\perl <INSTALL_DIR>\bin\backup.pl <BackUp Dir> <Log file> <Num_Generations>
```

This tool creates a backup of all the data on the active Operations Manager server and copies it into the backup directory mentioned. The number of generations refers to the maximum number of backups that can be stored under the backup directory. For example, if the number of generations is 2, then 2 consecutive invocations of this script will create <Backup dir>\0, and <Backup_dir>\1 until it starts wrapping.

Instead of the command line, you can also use the Common Services user interface (Administration > Server Administration > Administration > Backup).

From the user interface, it is possible to schedule a periodic backup of the active server. Periodic backups allow you to move to the latest backups, if required.

It is recommended that this backed-up data directory be kept on a separate system so that it is not affected by disk crashes or any issues associated with the active server.

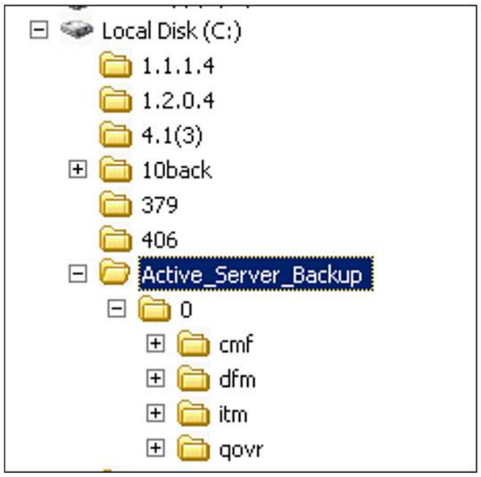
After the data backup is completed, this information must be imported to the standby server using the Restore Facility in Operations Manager.

Restore

Go to the standby server. Transfer the backup directory from the active server to the standby server. The complete directory and its contents should be transferred.

For example, if you have C:\Active_Server_Backup while running the backup script, then you will see the directory structure shown in Figure 9.

Figure 9. Backup Location



Local Disk (C:)
1.1.1.4
1.2.0.4
4.1(3)
10back
379
406
Active_Server_Backup
0
cmf
dfm
itm
qovr

Copy the entire contents under C:\Active_Server_Backup to the standby server with exactly the same structure.

Step 1. Run **perl** <INSTALL_DIR>**\objects\vhm\utilities\dbclean.pl** to clean the database.

Step 2. Run **net stop crmdmgtd** to stop the CiscoWorks Daemon Manager.

Step 3. Run **perl** <INSTALL_DIR>**CSCOpx\bin\restoreBackup.pl -d** <backupDir>.

The backup directory is C:\Active_Server_Backup in the example mentioned above.

Step 4. Copy the qovrx.log from the backup directory; that is, copy C:\Active_Server_Backup to <INSTALL_DIR>\CSCOpx\databases\qovr.

Step 5. Run **net start crmdmgtd** to start the Daemon Manager.

If the server is integrated with Access Control Server, you may get a prompt asking if you want to register your application with ACS.

If you have successfully configured your primary server with ACS (which is recommended because managing centralized users and roles is simplified in a redundancy setup), all your application roles and tasks are already there in ACS. In this case, select **NO** and proceed.

If, in a rare scenario, your configuration in ACS has been wiped out, select **YES**. This will register your application in ACS.

Step 6. Wait until **pdshow** lists all the processes running.

This will imply that the Daemon Manager has completely started.

Step 7. Rediscover all devices, by selecting **Devices > View/Rediscover/Delete**.

Essentially, this creates a baseline for the standby server. The standby server will have the complete device list and all the configurations that are identical to the active server. This also means that the standby server will poll the network in exactly the same way as the active server.

If you want to reduce the impact of polling on network bandwidth, do the following:

Step 1. Increase the polling interval to a very large value (1 hour) to reduce impact on network bandwidth.

You can do this by going to **Administration > Polling Parameters**, selecting each group, and editing the polling interval values.

Step 2. Go to **Administration > Notifications > Notification Criteria**.

Step 3. Select all notification criteria and select **Suspend**.

Step 4. Go to **Administration > Diagnostics Tests > Synthetic Tests**. For each test, select **Stop**.

This will stop the synthetic tests.

Step 5. Go to **Administration > Diagnostics Tests > Phone Status Tests**.

You will see a list of configured tests.

Step 6. For each test, click **Edit** and configure the schedule to run between "00:00" to "00:00."

This essentially stops the test.

Step 7. Suspend monitoring of SRST routers used in SRST tests.

To do this:

a. Go to **Administration > Polling and Thresholds > SRST Operations**.

You will see a list of SRST tests configured.

b. Make a note of all the target routers.

c. Go to **Administration > Device Management > Device Configuration.**

You will see an overview of all managed devices.

d. Click **Monitored Devices**.

e. Click the SRST router IP address in this report.

The Detailed Device View is launched.

f. In this screen, suspend the device.

This will automatically stop the SRST tests.

Continuous Data Synchronization

After the active server and the standby server are operating, any changes to the active server must be propagated to the standby server. Different kinds of data that can change, and recommendations for replication, are listed below.

Device List

Changes to the device list can be propagated by using a central DCR. There are two possibilities:

- Central LMS server as the source of the device list for both active and standby In this case, the LMS server acts as a master repository of devices, which pushes any additions or deletions to the device list to the active and standby servers.
- Active server as the source of the device list for the standby server. In this case, the active server acts as the master device repository. It pushes any changes to the device list to the standby server.

In either case, the main idea is to set up the master-slave configuration in the DCR. The steps are explained below, taking the example of the active server as the master DCR and the standby server as the slave DCR.

In the Active server:

Step 1. Select **Administration > Security > Peer Server Account Setup**.

The Peer Server Account Setup page appears, displaying the list of current users configured.

To add users, click **Add** in the main window. A popup dialog box appears where you can add the details of the user. In this dialog box, enter “admin” as the username and password of the standby server.

Step 2. Go to **Administration > Security > Multi Server Trust Management > Peer Server certificate**.

Step 3. Import the Standby server certificate.

Step 4. Go to **Administration > Device and Credentials > Administration > Mode Settings**.

Step 5. Change the mode to **Master**.

In the Standby server:

Step 1. Change the DCR Group ID in the Standby server.

- Go to <INSTALL_DIR>\CSCOpx\lib\classpath\com\cisco\nm\dcr and change the DCR_Group_ID to any number in dcr.ini. (the DCR_Group_ID of the master and the slave should not be the same).
- Restart the Daemon Manager.

Step 2. Go to **Administration > Server > Security > Multi Server Trust Management > Peer Server certificate**.

Import the Active server certificate.

Step 3. Go to **Administration > Device and Credentials > Administration > Mode Settings**.

Step 4. Change the mode to **Slave**, provide the master address, and restart the Daemon Manager.

Step 5. Make sure the master address provided here is identical to the hostname field in the master’s certificate.

As soon as you do this, the standby is in a slave mode that gets all the device information from the active server.

User Information

It is recommended that the active and standby servers be configured to operate in ACS mode. In this mode, all user and role setup is done on ACS, and the user information is not local to the active server. Any changes to user information happen centrally, thereby automatically propagating to the active and standby servers.

Other Configurations

Any other changes to the configuration of the active server must also be done on the standby server. This includes any new diagnostic tests since the baseline was created, and changes to notification profiles.

Note: If there are many number changes, we recommend that you back up and restore the data so that manually changing the configuration is totally avoided.

Failover

Failure of the active server can be detected by polling sysApplMIB on the primary server. The status of all the processes that are necessary for normal functioning of Operations Manager can be obtained from this MIB. Table 6 lists the processes that need to be running for a fully functional Operations Manager server.

Table 6. List of Processes Required for Operations Manager Server

Tomcat	Apache
TomcatMonitor	QOVRMultiProcLogger
QOVRDbEngine	QOVRDbMonitor
QOVR	LicenseServer
IVR	IPIUDbEngine
IPIUDbMonitor	INVDbEngine
INVDbMonitor	FHDbEngine
FHDbMonitor	ESS
EssMonitor	InventoryCollector
TISServer	IPIUDataServer
ITMDiagServer	VHMIntegrator
EPMDbEngine	EPMDbMonitor
EPMServer	AdapterServer
FHServer	IPSLAServer
PIFServerl	SRSTServer
QoVMServer	STServer
SIRServer	DfmBroker
DfmServer	VHMServer
CmfDbEngine	CmfDbMonitor
DCRServer	CMFOGSServer
ITMOGSServer	GPF
NOTSServer	PTMServer
TopoServer	VsmServer
Jrm	SEGServer

If any of the processes are down, it means that Operations Manager is in an indeterminate state; under such circumstances, you should activate your standby server.

If the active server goes down, the standby server can be made operational by doing the following:

Step 1. On the standby server, go to the Polling Parameters dialog box and change the default polling interval to 4 minutes.

Step 2. Activate Synthetic tests. You can start the tests that are stopped.

Step 3. Shift back to the original schedule for Phone Status tests.

Step 4. Resume the notification criteria.

Step 5. Verify that you are able to monitor the status of the network and the validity and execution of diagnostic tests and notification profiles.

Step 6. Create a backup of the configuration of the newly activated server.

Step 7. Decommission the previously active server.

Setting Up a Passive Redundant Server

In some deployments, instead of having a backup server actively polling the network, administrators prefer to have a backup server configured but not online. Using the procedures described earlier in this document, you can achieve this.

To set up a backup server, do the following:

Step 1. Configure a primary server.

Step 2. Set up periodic backups on the primary.

Step 3. Install a backup server.

Step 4. Shut down the backup server by using **net stop crmdmgtd** at the command line.

This will stop all activity on the backup server.

In the event of a failure of the primary server, restore from the latest backup (or use any other backup you prefer. To do this, do the following:

Step 1. Bring up the backup server by running **net start crmdmgtd**.

Step 2. Wait until all of the processes come up.

Step 3. Redo any changes to the configuration since the last backup.

Your backup server is ready to be used.

Operations Manager for MSP Environments

ACS Integration for Securing Access to Devices

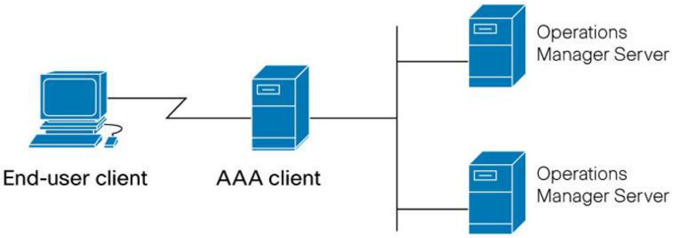
Operations Manager can be integrated with Cisco Secure Access Control Server to secure access to the devices.

Integrating Operations Manager with ACS

Introduction

Cisco Secure Access Control Server provides authentication, authorization, and accounting (AAA) services to network devices that function as AAA clients, such as a network access server, PIX® Firewall, or router (Figure 10).

Figure 10. Cisco Secure Access Control Server



Why Do We Need ACS?

Operations Manager is integrated with ACS to address the following tasks:

- Provide centralized user management for a group of Operations Manager servers or other CiscoWorks servers.
- Provide device-level authorization. Device-level authorization restricts user access to limit users to performing functions only on certain devices. This feature allows you to use Operations Manager in an MSP environment where, with just one Operations Manager instance, you can manage several devices yet allow certain users to act only on certain sets of devices.
- Provide editable user roles. The user roles are mapped to tasks that you have authorized users to perform on the devices. The mapping of roles to tasks can be changed in ACS.

Integrating with ACS 4.0

In ACS, network device groups are collections of AAA clients and AAA servers. You can assign AAA clients and AAA servers to the network device groups. For the Network Device Groups table to be displayed in ACS, the Network Device Groups option must be enabled.

To enable the Network Device Groups table, do the following:

Step 1. From the ACS navigation menu, select **Network Configuration**.

Step 2. Click **Advanced Options**.

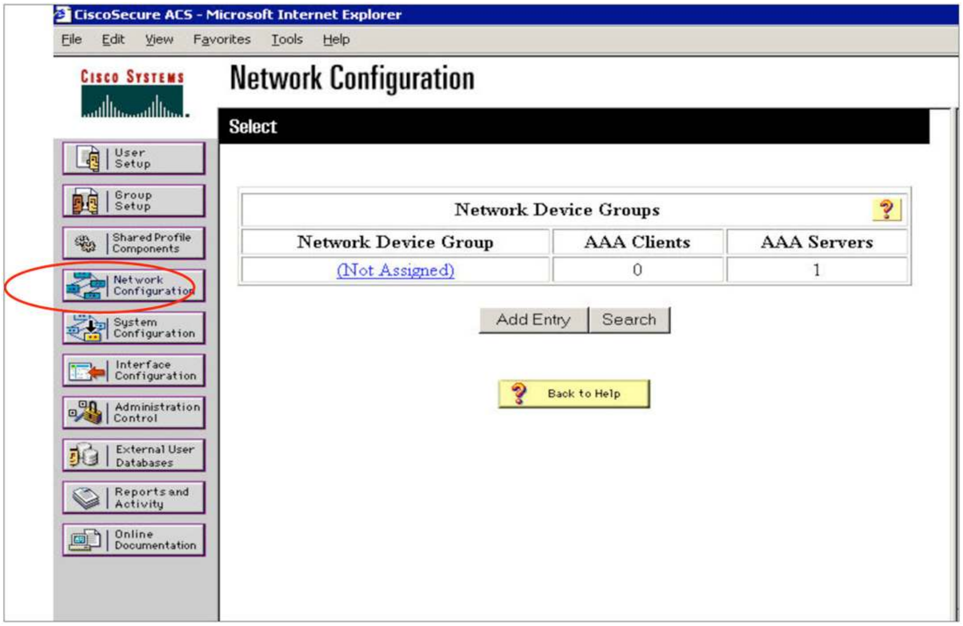
Step 3. Select the **Network Device Groups** check box.

Step 4. Click **Submit+Restart**.

Step 5. From the Cisco Secure ACS login window, log in to ACS.

Step 6. From the ACS navigation menu, select **Network Configuration** (Figure 11).

Figure 11. Network Configuration

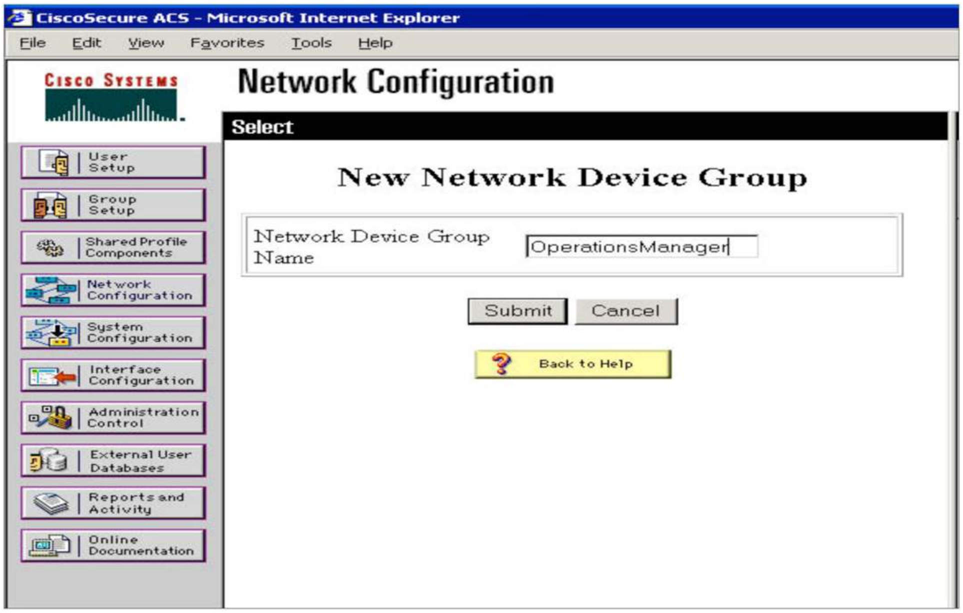


Network Device Groups		
Network Device Group	AAA Clients	AAA Servers
(Not Assigned)	0	1

Step 7. Under the Network Device Groups table, click **Add Entry**.

Step 8. Enter the network device group name (for example, Operations Manager); see Figure 12.

Figure 12. Network Device Group



Network Configuration

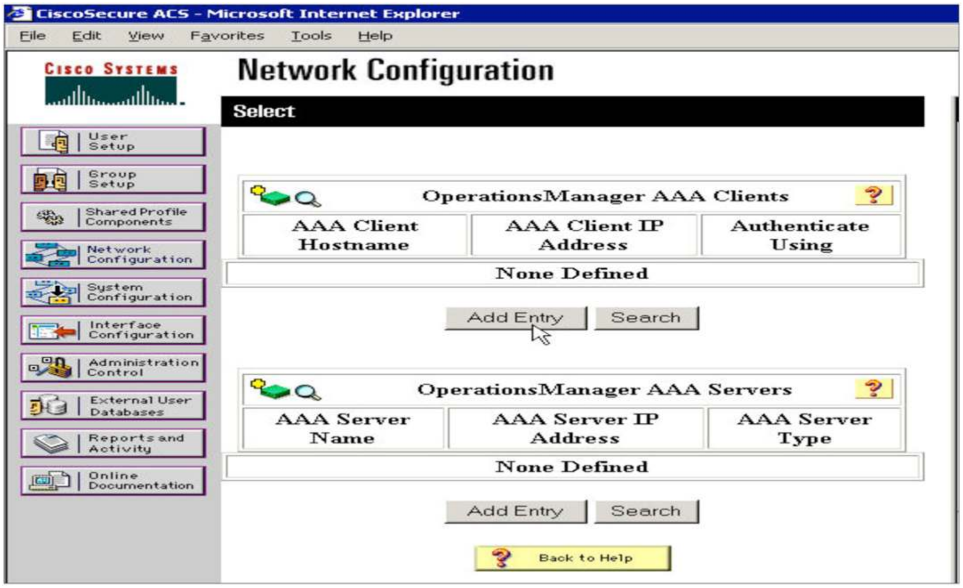
Select

New Network Device Group

Network Device Group Name: OperationsManager

Step 9. Under the Operations Manager AAA Clients table, click **Add Entry** (Figure 13).

Figure 13. Operations Manager AAA Clients



Network Configuration

Select

OperationsManager AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		

OperationsManager AAA Servers

AAA Server Name	AAA Server IP Address	AAA Server Type
None Defined		

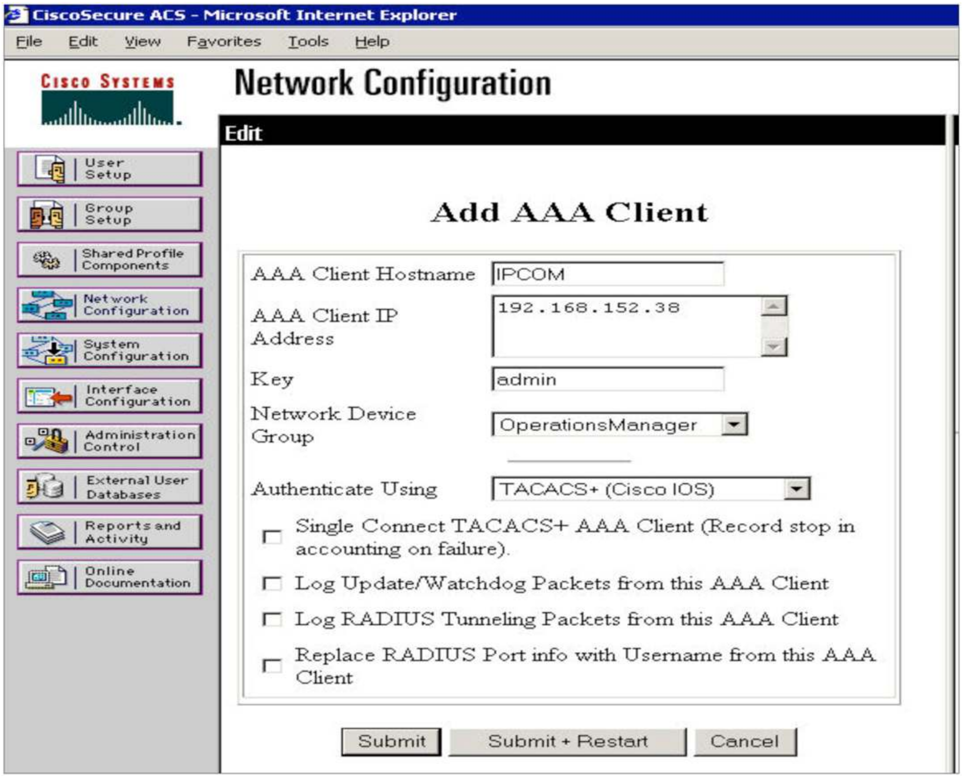
Step 10. In the Add AAA Client dialog box (Figure 14), do the following:

a. Enter the hostname of the Operations Manager server.

b. Enter the IP address of the Operations Manager server.

c. Enter a value in the Key field; this allows this client to contact ACS.

Figure 14. Add AAA Client



Network Configuration

Edit

Add AAA Client

AAA Client Hostname	IPCOM
AAA Client IP Address	192.168.152.38
Key	admin
Network Device Group	OperationsManager
Authenticate Using	TACACS+ (Cisco IOS)

□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

□ Log Update/Watchdog Packets from this AAA Client

□ Log RADIUS Tunneling Packets from this AAA Client

□ Replace RADIUS Port info with Username from this AAA Client

Step 11. Click **Submit+Restart**.

Setting Up the Operations Manager Server

To set up the Operations Manager server, do the following:

Step 1. Log in to the Operations Manager server.

Step 2. Set the login mode of the Operations Manager server.

Step 3. Go to **Administration > Server > Security > AAA Mode Setup**.

The AAA Mode Setup dialog box appears.

Step 4. Select ACS.

Step 5. Enter all the ACS details (including the key value provided in Step 10c of the “Integrating with ACS 4.0” section).

In the corresponding ACS TACACS+ port number fields, the default port is 49. Secondary and tertiary IP address and hostname details are optional.

The values True and False are not acceptable in the Primary, Secondary, and Tertiary IP Address/Hostname fields.

Step 6. Select the **Register all installed applications with ACS** option.

Note: If an application is already registered with ACS, the current registration will overwrite the previous one.

Step 7. Click **Apply**.

When you click **Apply**, the following occurs:

- A list of tasks in the product is registered to ACS.
- A list of default user roles (System Administrator, Network Administrator, Network Operator, Approver, and Help Desk) are registered to ACS.

A mapping of the tasks that the above user roles can execute is registered with the ACS user.

The mapping between user roles and these tasks is registered with the user.

Note: This is a default mapping of user roles and tasks.

The default mapping between tasks and the roles can be changed in ACS, but note that the changed mapping will not be reflected in the permission report.

Step 8. Restart the Daemon Manager. At the command prompt, enter:

```
- net stop crmdmgtd
```

Secure Views

Secure Views allows users access to perform a task on a device or a set of devices that are restricted. Secure Views is applicable only when the Operations Manager server is in ACS Login mode.

Secure Views facilitates filtering of group membership based on the user and the application task context in which a request is made. Filtering is performed only when operating in ACS Login mode. While operating in non-ACS mode, no filtering is performed and evaluating a group results in all devices in that group being returned.

The following example explains secure views:

1. Two users, Joe and Frank, are configured in ACS.
2. Two network device groups, NDG1 and NDG2, are configured in ACS.
3. NDG1 contains device D1.
4. NDG2 contains device D2.
5. The Network Administrator role is mapped to the task **Edit Device Configuration**.
6. Joe has a Network Operator role on NDG1. This means he is authorized to perform the Edit Device Configuration task on device D1 in NDG1.
7. Frank has a Network Operator role on NDG2. This means he is authorized to perform the Edit Device Configuration task on device D2 in NDG2.
8. Group G1 is created in the Operations Manager server. Let us assume that Group G1 has devices D1 and D2 in it.
9. When Joe logs in to the Operations Manager server, he will see only device D1 in group G1. This is because his view of devices in G1 is restricted to only devices that he can view and on which he can act. The same is applicable to Frank as well, who can see only device D2 in group G1.

Creating Users in ACS

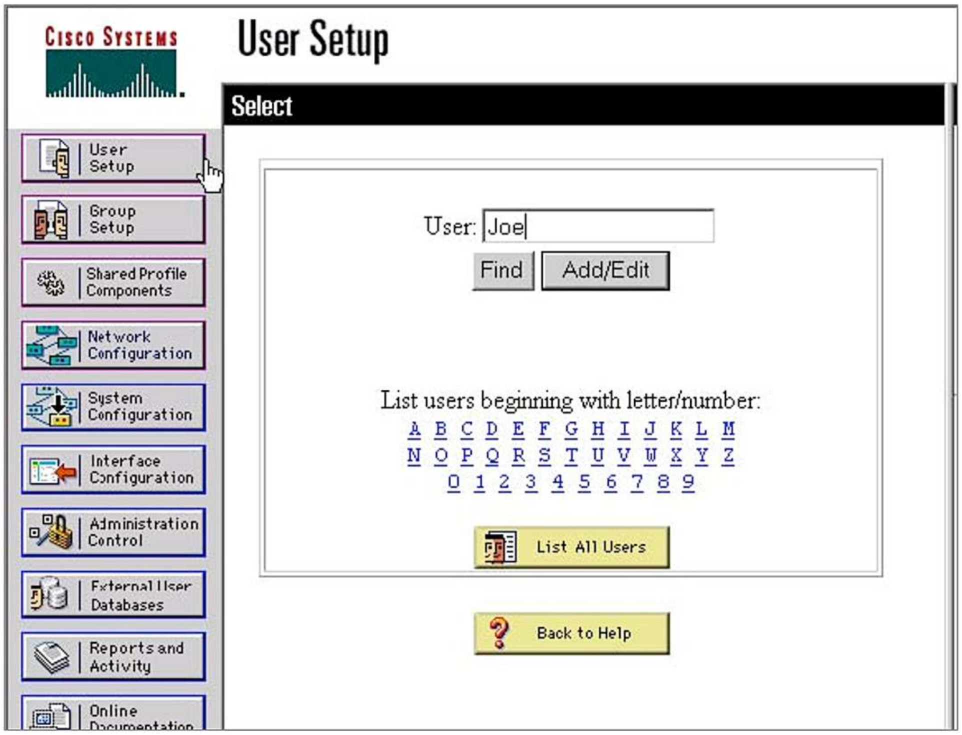
To create two users named Joe and Frank in ACS, do the following:

Step 1. Log in to ACS.

Step 2. Click **User Setup**.

Step 3. Enter a username (in this example, Joe), then click **Add/Edit** (Figure 15).

Figure 15. ACS User Setup



User Setup

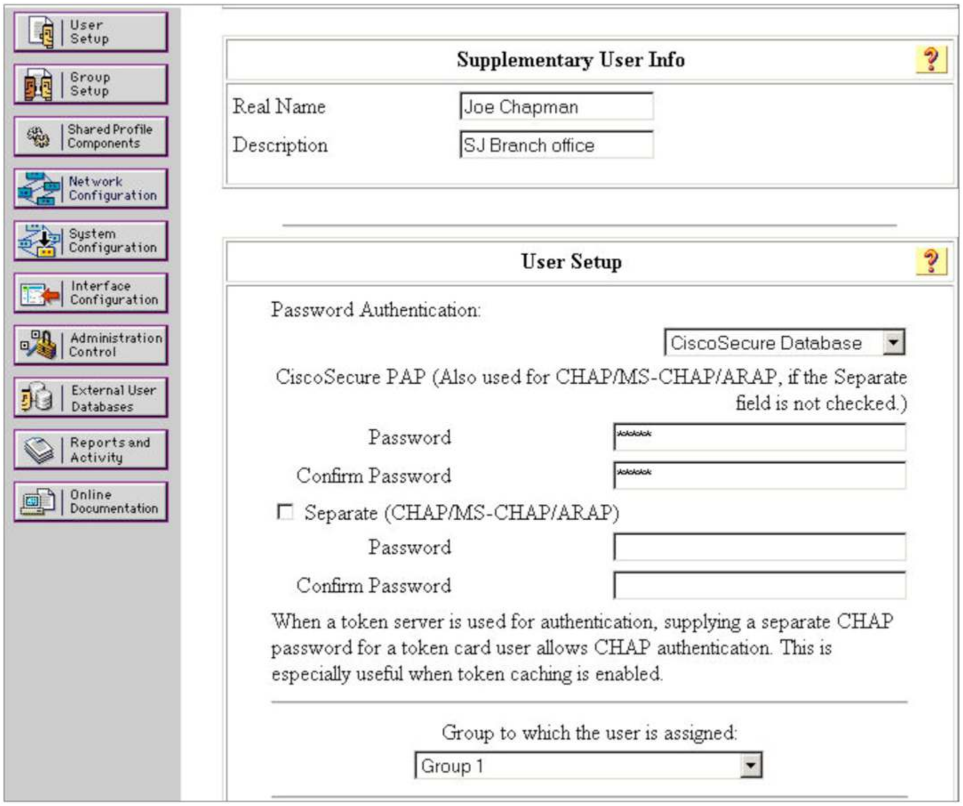
Select

User: Joe

Step 4. Assign a password for the user Joe.

Step 5. Assign Joe to the group named Group1, then click **Submit**. See Figure 16.

Figure 16. User Info



Supplementary User Info

Real Name: Joe Chapman

Description: SJ Branch office

User Setup

Password Authentication: CiscoSecure Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password: *****

Confirm Password: *****

□ Separate (CHAP/MS-CHAP/ARAP)

Password:

Confirm Password:

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned: Group 1

Step 6. Similarly, create a user named Frank and assign the user to **Group2**.

Step 7. Set up the Network Device Groups to contain the following devices:

- D1 (172.20.118.47)
- D2 (172.20.118.48)

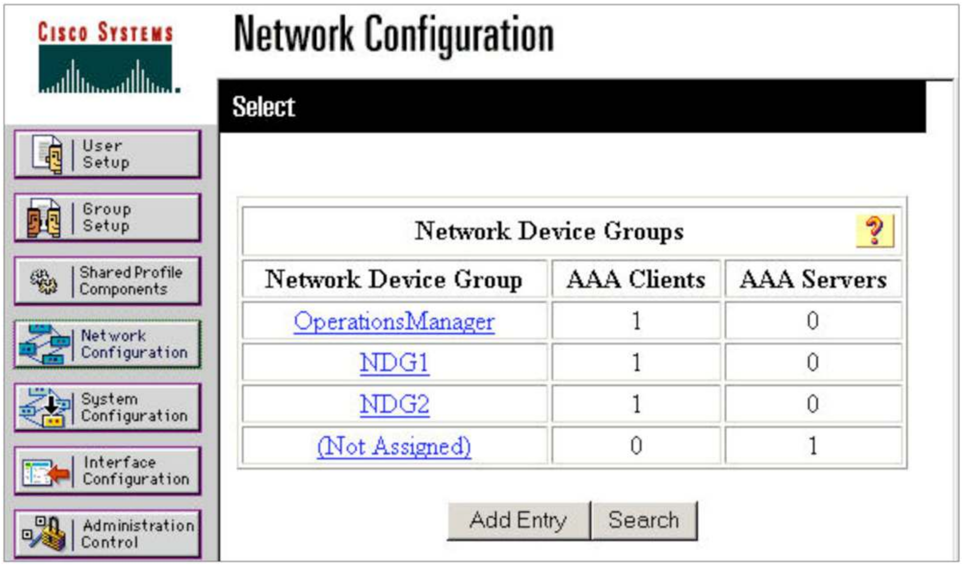
a. Click **Network Configuration**.

The Network Device Groups dialog box appears.

b. Click **Add Entry**.

c. Create two Network Device Groups (**NDG1 and NDG2**) as shown. See Figure 17.

Figure 17. Add Entry

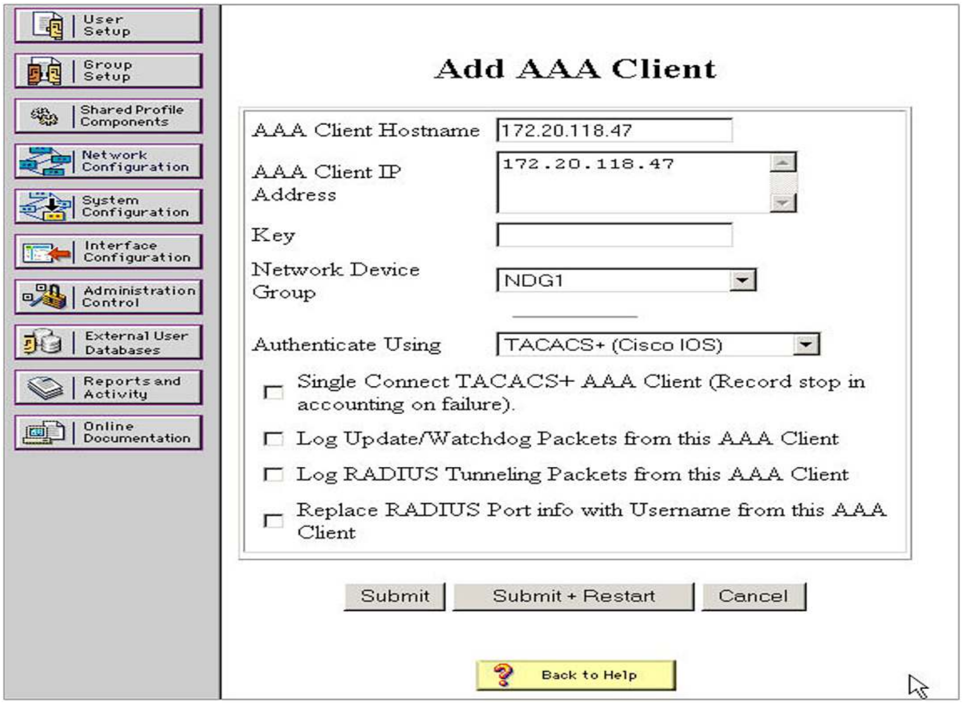


Network Device Groups		
Network Device Group	AAA Clients	AAA Servers
OperationsManager	1	0
NDG1	1	0
NDG2	1	0
(Not Assigned)	0	1

d. Click the NDG2 link.

e. In the Add AAA Client dialog box, add a device D1 with IP address 172.20.118.47 (Figure 18).

Figure 18. Add AAA Client



Add AAA Client

AAA Client Hostname: 172.20.118.47

AAA Client IP Address: 172.20.118.47

Key:

Network Device Group: NDG1

Authenticate Using: TACACS+ (Cisco IOS)

□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

□ Log Update/Watchdog Packets from this AAA Client

□ Log RADIUS Tunneling Packets from this AAA Client

□ Replace RADIUS Port info with Username from this AAA Client

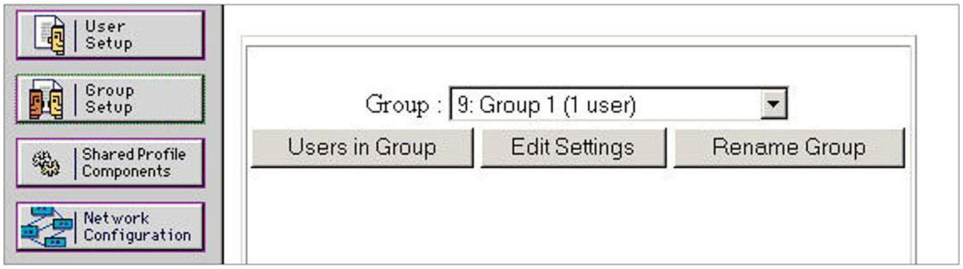
f. Similarly, click NDG2 and add a device D2 with IP address 172.20.118.48.

Step 8. Assign Group1 (Joe's user group) a Network Administrator's role on NDG2:

a. Click **Group Setup**.

b. Select the group to which the user Joe belongs, then click **Edit Settings** (Figure 19).

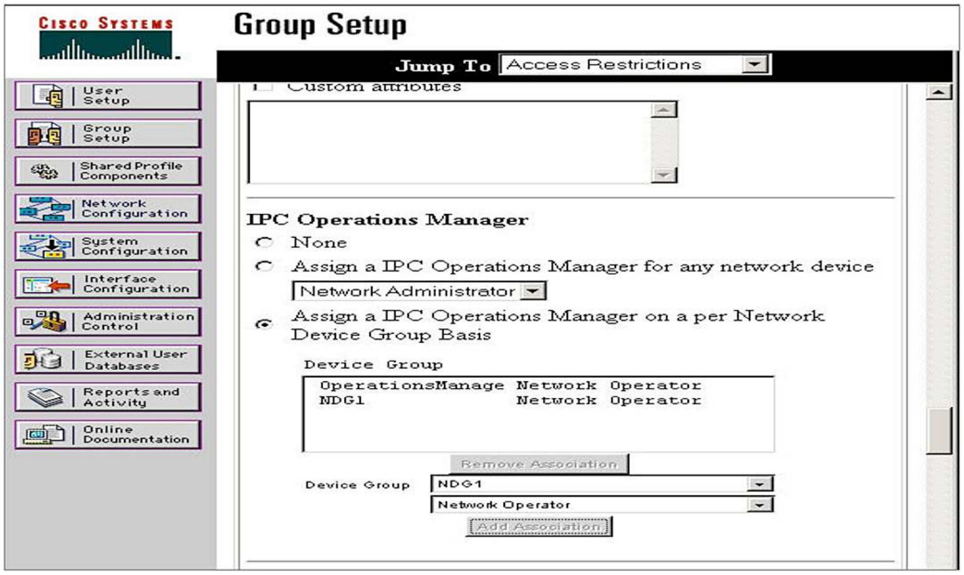
Figure 19. Group Setup



Group : 9: Group 1 (1 user)

c. Create an association for this group with the Network Device Groups that contain the Operations Manager server (NDG1) and device D1 (NDG2). See Figure 20.

Figure 20. Group Setup Information



Group Setup

Jump To Access Restrictions

□ Custom attributes

IPC Operations Manager

○ None

○ Assign a IPC Operations Manager for any network device

Network Administrator

● Assign a IPC Operations Manager on a per Network Device Group Basis

Device	Group
OperationsManage	Network Operator
NDG1	Network Operator

Device Group NDG1

Network Operator

Step 9. To update the settings, click **Submit+Restart**.

Step 10. Similarly, follow the steps to create the association for the group that contains the user Frank and Network Device.

Note: In this example, a user group is assigned a network operator.

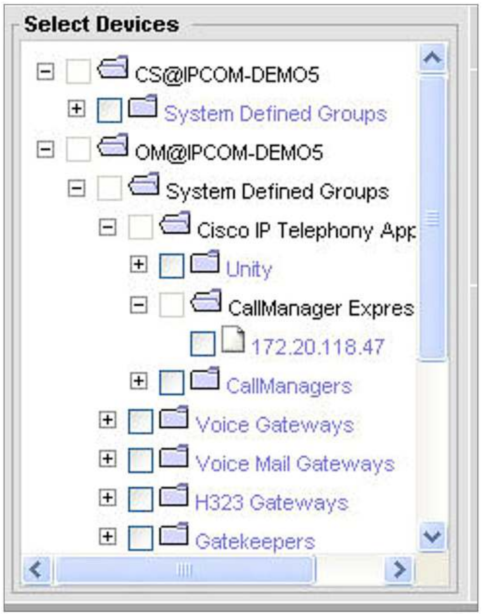
Secured Views is now operational for users Joe and Frank. Assume that both Joe and Frank access the Config Editor screen. In Operations Manager, the group /OM@IPCOM-DEMO5/System Defined Groups/Cisco IP Telephony Applications/Call Manager Express contains two devices:

- 172.20.118.47
- 172.20.118.48

When the two users (Joe and Frank) access the same group in the Config Editor screen, they see different devices in the group.

The view for Joe when he accesses the group /CS@IPCOM-DEMO5/System Defined Groups/Routers/Cisco 7200 Series Routers/Cisco 7204 Router is shown in Figure 21.

Figure 21. Device Group View



Joe sees only device 172.20.118.47 in the group, and Frank's login allows Frank to see only device 172.20.118.48.

Note: If the Operations Manager server is using Access Control Server mode and you want to provide access to a cluster for any user, all the devices in the cluster must be explicitly added into the ACS configuration for that user. It should include Unified Communication Managers, gateways, Unity devices, gatekeepers, and so on.

Why Do We Need to Create a New Role in ACS?

In ACS, the administrator can assign only one role for a user in a network device group. If a user requires privileges other than those associated with the current role to operate on a Network Device Group, a custom role should be created. All necessary privileges to allow the user to operate in the Network Device Group should be given to this role.

For instance, if a user needs both Approver and Network Operator privileges to operate on NDG1, you can create a new role with Network Operator and Approver privileges, and assign the role to the user, so that the user can operate on NDG1.

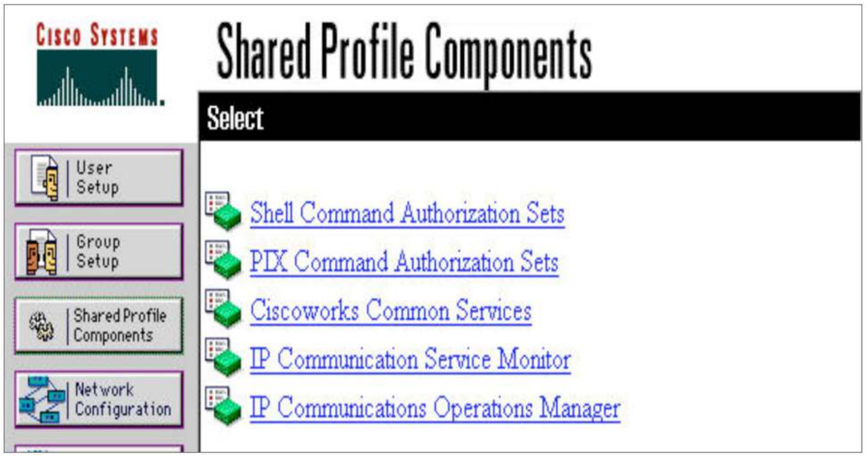
How to Create a New Role in ACS

To create a new role in ACS, do the following:

Step 1. Log in to ACS.

Step 2. Click **Shared Profile Components** (Figure 22).

Figure 22. Shared Profile Components


Cisco Systems
Shared Profile Components
Select
User Setup
Group Setup
Shared Profile Components
Network Configuration
Shell Command Authorization Sets
PIX Command Authorization Sets
Ciscoworks Common Services
IP Communication Service Monitor
IP Communications Operations Manager

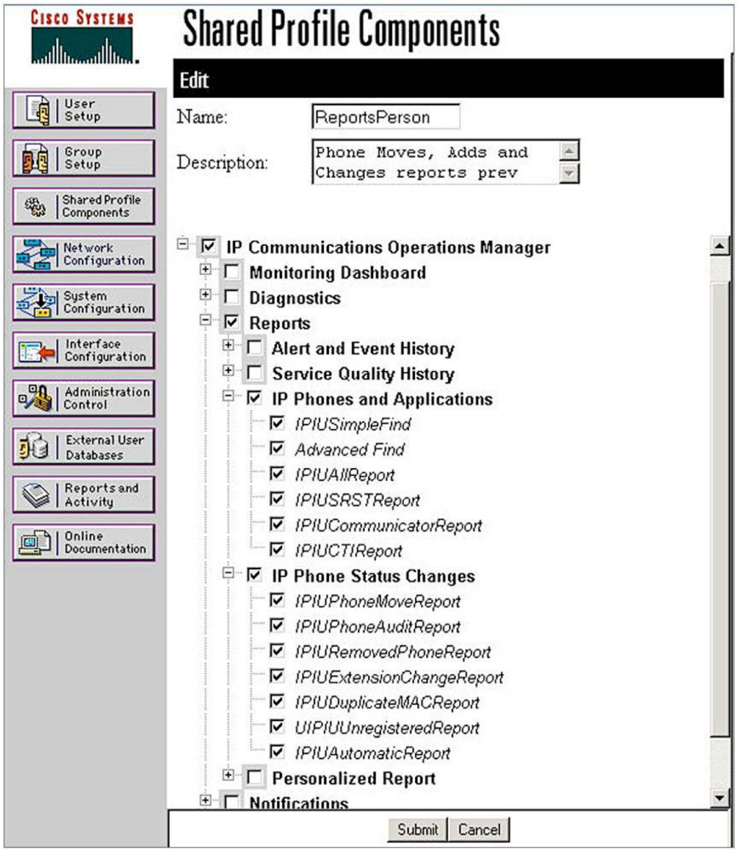
Step 3. Select the shared profile component where you would like to create a new role.

In this example, **Operations Manager** is selected.

Step 4. Click **Add**.

The dialog box shown in Figure 23 appears.

Figure 23. Create a New Role



Name: ReportsPerson

Description: Phone Moves, Adds and Changes reports prev

- ☑ IP Communications Operations Manager
  - ☐ Monitoring Dashboard
  - ☐ Diagnostics
  - ☑ Reports
    - ☐ Alert and Event History
    - ☐ Service Quality History
    - ☑ IP Phones and Applications
      - ☑ *IPIUSimpleFind*
      - ☑ *Advanced Find*
      - ☑ *IPIUAllReport*
      - ☑ *IPIUSRSTReport*
      - ☑ *IPIUCommunicatorReport*
      - ☑ *IPIUCTIReport*
    - ☑ IP Phone Status Changes
      - ☑ *IPIUPhoneMoveReport*
      - ☑ *IPIUPhoneAuditReport*
      - ☑ *IPIURemovedPhoneReport*
      - ☑ *IPIUExtensionChangeReport*
      - ☑ *IPIUDuplicateMACReport*
      - ☑ *UIPIUUnregisteredReport*
      - ☑ *IPIUAutomaticReport*
    - ☐ Personalized Report
  - ☐ Notifications

Reverting Operations Manager to Local CiscoWorks Login Mode

If there is an authorization failure from ACS, most of the Common Services features will be disabled. To recover, you must reset the login module. To do this:

Step 1. Stop the Daemon Manager using:

```
net stop crmdmgtd
or
/etc/init.d/dmgtd stop
```

Step 2. Run the following script:

For Solaris:

/opt/CSCOpx/bin/ResetLoginModule.pl

For Windows:

NMSROOT/bin/perl ResetLoginModule.pl

Step 3. Start the Daemon Manager using:

```
net start crmdmgtd
```

or

```
/etc/init.d/dmgtd start.
```

This helps you to reset the login module and revert back to the local CiscoWorks module.

Multiple instances of the same application (for example, Common Services) using the same ACS instance will share settings. Any changes will affect all instances of that application. If the application is configured with ACS and is reinstalled, the application will inherit the old settings.

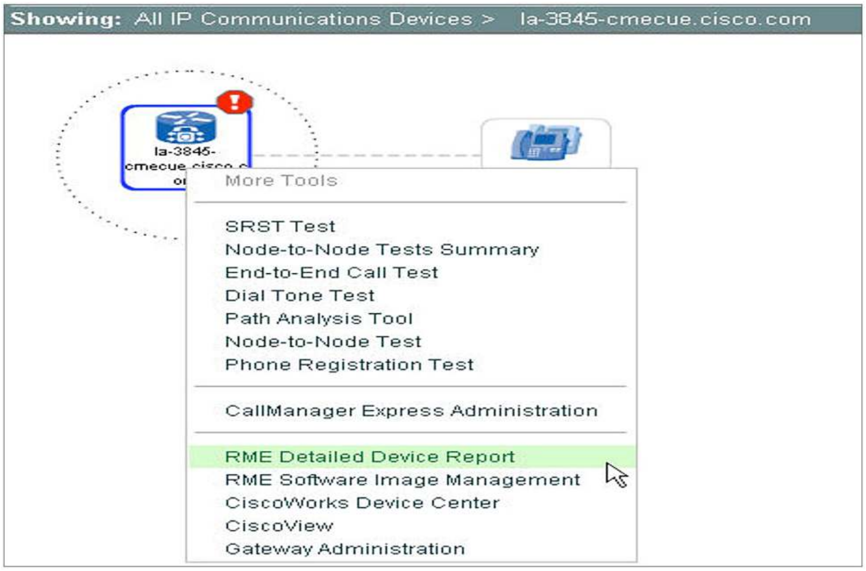
LMS Integration

Operations Manager integrates with the following CiscoWorks applications:

- Device Credential Synchronization (see the “Network Discovery and Device Management” section)
- CiscoWorks Resource Manager Essentials (RME)
- CiscoWorks Campus Manager (Campus)
- CiscoView

To integrate RME, Campus, or CiscoView with Operations Manager, you must configure the other CiscoWorks applications’ server IP addresses or DNS names in Operations Manager (**Administration > Miscellaneous Preferences**). Make sure that the devices monitored by Operations Manager are also managed in the other CiscoWorks applications that are referenced. After the integration is complete, a context-sensitive launch point is provided to the appropriate tools from the Service Level View. See Figure 24.

Figure 24. LMS Integration



Showing: All IP Communications Devices > la-3845-cmecue.cisco.com
la-3845-cmecue.cisco.c om
More Tools
SRST Test
Node-to-Node Tests Summary
End-to-End Call Test
Dial Tone Test
Path Analysis Tool
Node-to-Node Test
Phone Registration Test
CallManager Express Administration
RME Detailed Device Report
RME Software Image Management
CiscoWorks Device Center
CiscoView
Gateway Administration

Cisco Unified Communications Service Monitor Integration

A Cisco 1040 Sensor supports up to 50 active calls (100 RTP streams). At an 8-to-1 ratio (a typical PSTN line-to-user ratio), a Cisco 1040 can monitor approximately 400 phones. The 8:1 ratio is typically used when provisioning phone lines. A Service Monitor supports up to 50 Cisco 1040s (or about 4000 phones); an Operations Manager supports up to 10 Service Monitors (or about 40,000 phones).

If there are more than 100 sessions, some of the RTP streams might not be collected consistently. In this case, since the Cisco 1040 might have missed certain RTP streams, when the MOS value is calculated, the MOS is diluted. Span as close to the phone switch port as possible for the Cisco 1040 to calculate an accurate MOS.

For details on configuring the Catalyst Switched Port Analyzer (SPAN) feature, refer to http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a008015c612.shtml.

For details on configuring the Windows 2000 DHCP Server for Cisco Unified Communications Manager, refer to http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00800942f4.shtml.

For details on using one DHCP server for voice and data networks, refer to http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080114aee.shtml.

Do not set the Service Monitor MOS threshold to values of 4.3 or greater for a prolonged period. This will generate a quality of voice trap for every call. The maximum MOS is 4.5.

If a trap is not forwarded, it is usually because of third-party SNMP tools installed on the Operations Manager server. If you have any SNMP tools installed on the Operations Manager server, check to see if SNMP Trap Service under Windows **Control Panel > Administrative Tools > Services** is running. If it is, stop it and disable it. When the Windows SNMP trap service is running, all traps are redirected to this service and Operations Manager does not get a copy of the trap; hence, Operations Manager is not able to process the voice quality trap.

Similar to the 1040 Sensor, Operations Manager can receive voice quality related SNMP traps from Service Monitor integrated with NAM (Network Analysis Module). NAM can support 100-4000 RTP streams per minute depending upon the Cisco Network Analysis Module platform. For more information refer to http://www.cisco.com/go/nam.

Cisco 1040 Sensor in Sampling Mode

Cisco 1040 Sensors are capable of monitoring 100 RTP streams. If a Cisco 1040 Sensor is deployed on a switch that has more than 100 RTP streams, the sensor will perform sampling, in which case, some of the RTP streams will not be considered for MOS value generation. This situation must be avoided at all times.

In sampling mode, the reported MOS value is diluted, because some of the RTP streams are not considered. The sensor monitors RTP streams and collects the information necessary to compute the MOS value.

This information is stored in a buffer from which the computation process obtains the data to compute the MOS value. If packets arrive at a rate faster than the buffer can be emptied, some of the RTP streams will be dropped before the sensor collects information from them.

Keep in mind that CPU resources will be utilized constantly. Hence, it is not just the buffer that becomes the bottleneck when a sensor is overwhelmed with excess RTP streams; the CPU also falls short in serving the different processes.

The MOS value reported by the sensor is diluted as the number of simultaneous RTP streams increases beyond 100. To avoid this situation, it is important to plan ahead and optimize the span port configuration in the above scenarios.

Cisco 1040 Sensor in a Branch Office

In a branch office, the density of IP phones is less than the density seen on the main campus. Typically, a branch office will contain fixed-configuration switches, and the number of simultaneous calls will be fewer.

In a fairly large branch office, it is common to see multiple fixed-configuration switches stacked to provide more density and avoid the need to run a gigabit uplink to an aggregate switch/router. The Cisco 1040 Sensor fits into this model similar to any other switch. The Cisco 1040 still utilizes a span port to monitor the RTP streams.

In the scenario where the switches are not stacked but have gigabit home run to the aggregate switch and the number of RTP streams is below 80, one sensor per switch is more than what is necessary. This is where Remote Switched Port Analyzer (RSPAN) becomes handy. The configuration done on the switch with respect to SPAN, RSPAN, or ESPAN is transparent to the sensor. The sensor functions normally as long as it sees the RTP stream.

In the scenario where RSPAN is not a desirable configuration, or it is not an approved configuration, a simple active hub can be used to connect the individual SPAN ports from the different switches, and the sensor can be deployed on the hub. It is very important to keep spanning tree loops in mind when such a configuration is attempted. The use of a hub must be selected as the last resort.

Span Port Limitations

The span port is widely used to connect packet sniffers for troubleshooting issues. In the contact center world, the span port is used to record the voice conversation. In the service monitor world, the span port is used to monitor voice quality. It is quite possible that the need may arise to use the span port for packet sniffer, contact center, and service monitor at the same time.

The span port does not allow the configuration of the same source port tied to multiple span destination ports; this is one of the limitations of span port configuration. The only alternative is to use an active splitter that offers one-to-many streams. The simplest splitter must be an active hub that offers one-to-many streams. In this model, the packet sniffer, contact center application, and sensor connect to the hub, and the hub connects to the span destination port on the switch.

Simultaneous Operations by Multiple Users

No more than five simultaneous Operations Manager users are recommended if all users are viewing the portals, performing tests, and creating reports on a constant basis.

Operations Manager System Health Monitor

From Operations Manager 2.2 and later, you can configure and monitor the Operations Manager system health (critical process state). If any of these critical processes go down, a notification is generated and forwarded to the configured email. You can configure the Health Monitor as follows:

Step 1. Access the HealthMonitor.cfg file in the CSCOpx\conf directory to add email-related parameters or change any of the configurable settings, as shown in Table 7.

Table 7. Health Monitor Configuration File Parameters

Configuration File name	Description
HealthMonitor.cfg	This file contains the below configurable parameters: • Max_Retries: Maximum attempts to start a process. • Initial_Delay: Initial delay in seconds when service is started. • Max_Wait_Time: Maximum wait time in seconds to check if processes are up. • Monitoring_Frequency: The frequency at which monitoring is performed (in minutes). • Max_Backups: Maximum backups to maintain per process. • SMTP_Server: SMTP mail server address. • Receiver_Email_ID: Email ID of the administrator. • Sender_Email_ID: Email ID used as identity of the sender. The email-related parameters above (SMTP_Server, Receiver_Email_ID, Sender_Email_ID) do not contain any values. To receive email information when the audit logs are updated, you can add the values for the email-related parameters. An example of file contents is: Max_Retries=3 Initial_Delay=1800 Max_Wait_Time=10 Monitoring_Frequency =300 Max_Backups=3 SMTP_Server=server.domain.com Receiver_Email_ID=admin@domain.com Sender_Email_ID=system@cuom.com

Step 2. Edit the file using your editor and save the changes when you are finished.

Step 3. Stop and restart the OMHealthMonitor service, to make sure that the changes have taken effect:

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

Whenever you have maintenance or debugging tasks to perform, you must stop the OMHealthMonitor Windows Service so that processes that are intentionally shut down are not inadvertently restarted. Run the following commands:

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

Troubleshooting Tips

For more troubleshooting tips and guidelines, please refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_unified_operations_manager/faq/OMFAQ11.html.

Useful URLs

Cisco.com URLs for Customers and Partners

Product Information

- Product Page: http://www.cisco.com/en/US/products/ps6535/index.html
- Supported Devices: http://www.cisco.com/en/US/products/ps6535/products_device_support_tables_list.html
- Release Notes: http://www.cisco.com/en/US/products/ps6535/prod_release_notes_list.html
- Data Sheet: http://www.cisco.com/en/US/products/ps6535/products_data_sheets_list.html
- User Guide: http://www.cisco.com/en/US/products/ps6535/products_user_guide_list.html
- Installation Guide: http://www.cisco.com/en/US/products/ps6535/prod_installation_guides_list.html

VoD and Tutorial

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

Deployment Best Practices Guide

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

Training

Instructor-led Cisco Unified Operations Manager and Service Monitor 2-day training:

- Customers and Partners, send an email message to aeskt_registration@cisco.com

Evaluation Downloads

For Partners and Customers:

Step 1. Go to the Marketplace site at the link below. Note that you must log in with a Cisco employee (CEC) or authorized Cisco Partner login and password: http://www.cisco.com/go/marketplace.

Step 2. Select the **Collateral & Subscription** Store link.

Step 3. Read the notice to Cisco employees and click **Continue**.

Step 4. From the navigation menu at the top-left corner of the page (above the Subscriptions link), select the **Marketing Collateral** link. From the **Marketing Collateral** navigation menu, select **Network Management Evaluation Kits**, and then select the desired evaluation kit.

Step 5. Use “Add to cart” and “Checkout” to place the order for the desired kit, using your ACCESS Visa or personal credit card.

For further questions on Cisco Unified Communications Operations Manager or Cisco Unified Communications Service Monitor, or for any other Cisco Unified Management-related questions, send an email message to ask-ucms@cisco.com.

Patch Download

Go to http://www.cisco.com/kobayashi/sw-center/sw-netmgmt.shtml and look for Operations Manager.

Miercom Review of Operations Manager and Service Monitor

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

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C07-705321-00 04/12