Cisco Unified Operations Manager

Deployment Best Practices

Authors: Tara Jagannathan, Jay Shivaram, Elvis Hernandez, Prashant P Hegde, Shiva Shankar

July, 2006

Table of Contents

ABBREVIATIONS AND ACRONYMS

ACS	Access Control Server, a CiscoSecure product
IPCC	IP Contact Center
LMS	LAN Management Solution
ODBC	Open Database Connectivity
QoV	Quality of Voice
RME	Resource Manger Essentials, a component of CiscoWorks LMS
IP SLA	Cisco IOS Service Level Agreement
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SRST	Survivable Remote Site Telephony
SSL	Secure Socket Layer
TFTP	Trivial File Transfer Protocol

1 Introduction

This document outlines best practices for a successful deployment of Cisco Unified Communications Operations Manager in enterprise and managed service provider (MSP) environments. It documents different aspects of initial device setup, installation guidelines, server sizing, and best practices for initial setup, ongoing administration, and maintenance of the product.

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. Detailed steps are provided for best practices wherever relevant.

2 Product Overview

Cisco Unified Communications Operations Manager (Operations Manager) provides a unified view of the entire IP communications infrastructure and presents the current operational status of each element of the IP communications network. It continuously monitors the current operational status of different IP communications elements such as Cisco CallManager, Cisco CallManager Express, Cisco Unity, Cisco Unity Express, Cisco IP Contact Center, and Cisco gateways, routers, and phones, and it 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) and Hypertext Transfer Protocol (HTTP) to remotely poll data from different devices in your IP communications deployment. It does not deploy any agent software on the devices being monitored and is nondisruptive to 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.
- Increases productivity of the network managers and enables faster trouble isolation by providing contextual diagnostic tools to enable troubleshooting:
    - Through diagnostic tests, performance, and connectivity details about different elements of the converged IP communications infrastructure
    - Using synthetic tests that replicate end-user activity and verify gateway availability and other configuration and operational aspects of the IP communications infrastructure
    - Through IP service-level agreement (SLA)-based diagnostic tests that can measure the performance of WAN links and measure node-to-node network quality
    - Providing information in notification messages that contain context-sensitive links to more detailed information about service outages
    - Using context-sensitive links to other CiscoWorks tools and Cisco tools for managing IP communications implementations
- Presents service-quality alerts by using the information available through Cisco Unified Communications Service Monitor (when it is also deployed). It displays mean opinion scores 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 problem. 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 enable the location and identification of the IP phones.
- Enables tracking of IP communications devices and IP phone inventory, tracks IP phone status changes, and creates a variety of reports that document move, add, and change operations on IP phones in the network.
- Provides real-time notifications using SNMP traps, syslog notifications, and e-mail that let Operations Manager report the status of the network being monitored to a higher-level entity (typically Manager of Managers).

Figure 1 shows the deployment architecture for Operations Manager.

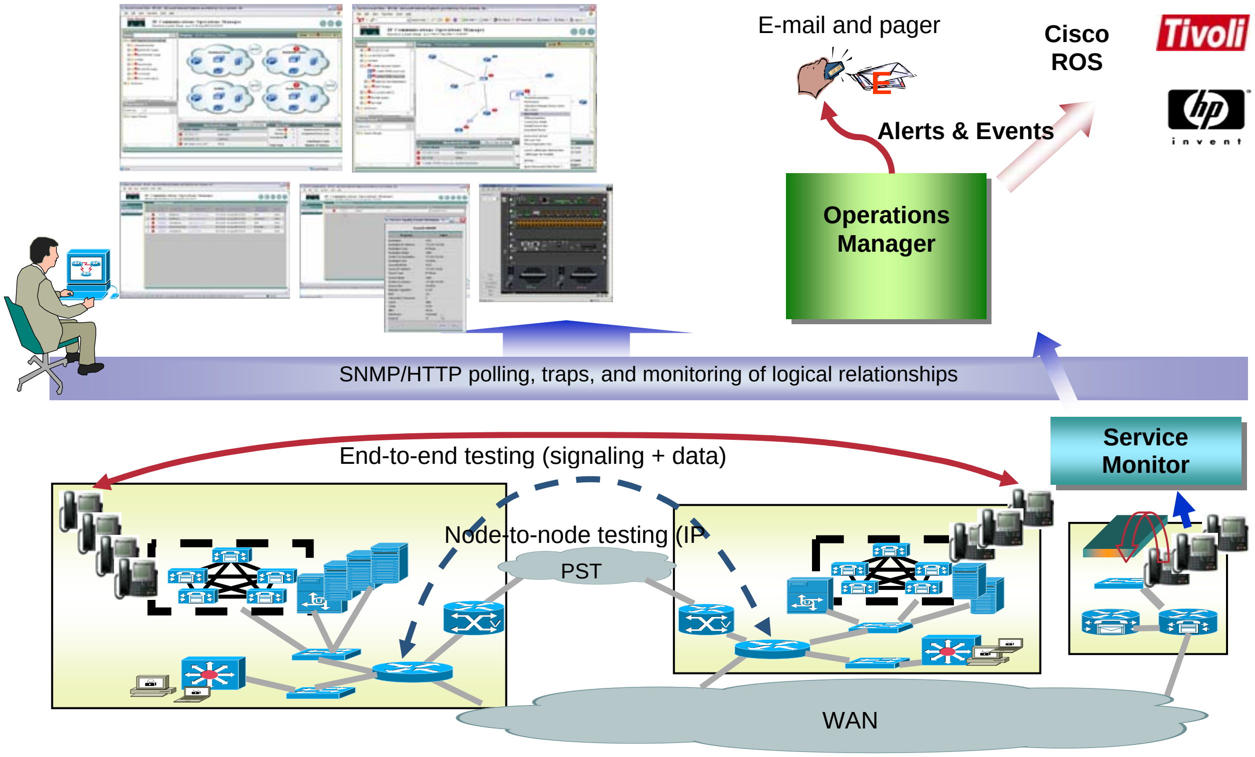


Figure 1: Deployment Architecture

2.1 Deployment Models

2.1.1 Small and Medium Enterprises

For small deployments, (up to 1,000 phones), the software component for Cisco Unified Service Monitor (Service Monitor) can co-reside with Operations Manager on a single platform. A single installation process installs all the necessary components. It provides real-time notifications using SNMP traps, syslog notifications, and e-mail that allow Operations Manager report the status of the network being monitored to a higher-level entity. Figure 2 shows the deployment model for small and medium-size enterprises.

Operations Manager can also share device and credential information with other CiscoWorks tools deployed in the enterprise.

2.1.2 Large Enterprises

For medium and large enterprise deployments (over 1,000 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 Manager of Managers (MOM). Each instance of Operations Manager can manage multi-site and multi-cluster IP communications environments. Operations Manager provides real-time notifications using SNMP traps, syslog notifications, and e-mail that enables Operations Manager to report the status of the network being monitored to a higher-level entity (typically a MOM). It can also share device and credential information with other CiscoWorks tools deployed in the enterprise, resulting in reduced administrative overhead for network managers. Figure 3 shows the deployment model for large enterprises.

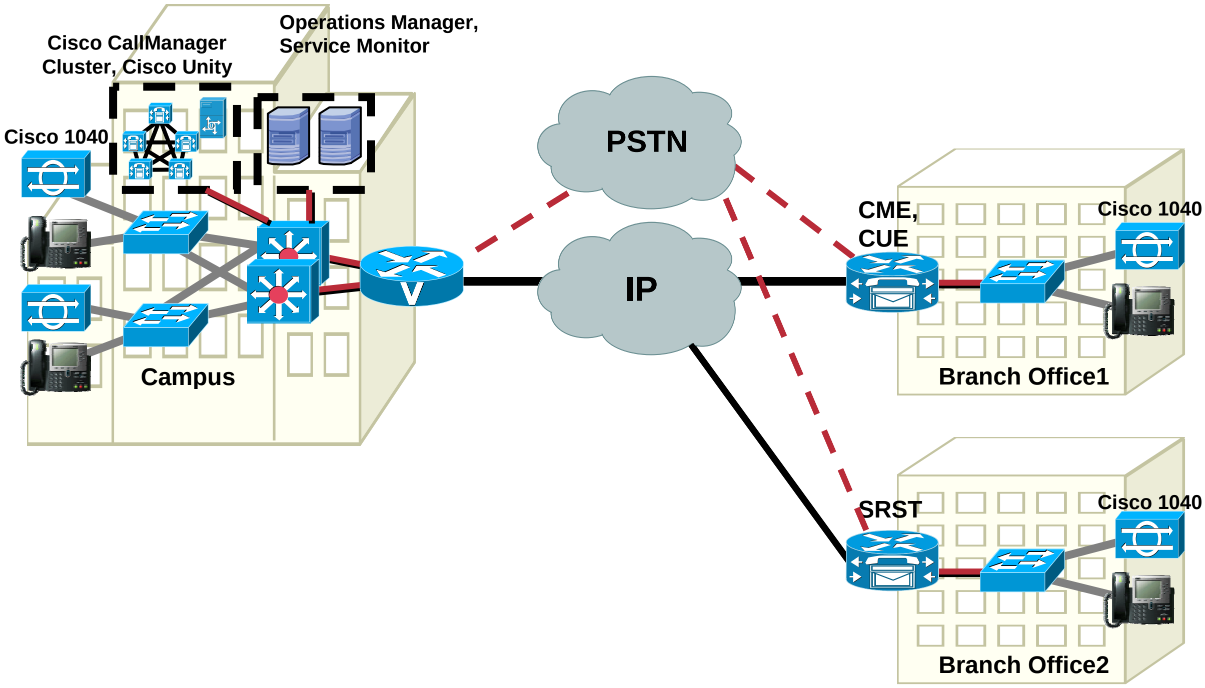


Figure 2: Deployment Model for Small and Medium-Sized Enterprises

2.1.3 Managed Service Providers

A Managed Service Provider (MSP) can deploy one or more instances of Operations Manager to manage its customers' environments. Under certain conditions, a single Operations Manager can successfully manage multiple customer deployments. There should not be any overlap in IP address space between devices in different customer deployments managed by a single Operations Manager server. If there is an overlap, multiple Operations Manager servers may need to be deployed to handle the overlap. Each instance of Operations Manager provides real-time notifications using SNMP traps, syslog notifications, and e-mail that let Operations Manager report the status of the network being monitored to a higher-level entity (typically a Manager of Managers). It can also share device and credential information with other CiscoWorks tools deployed in the network, thereby resulting in reduced administrative overhead for network managers. Figure 3 shows the deployment model for MSPs.

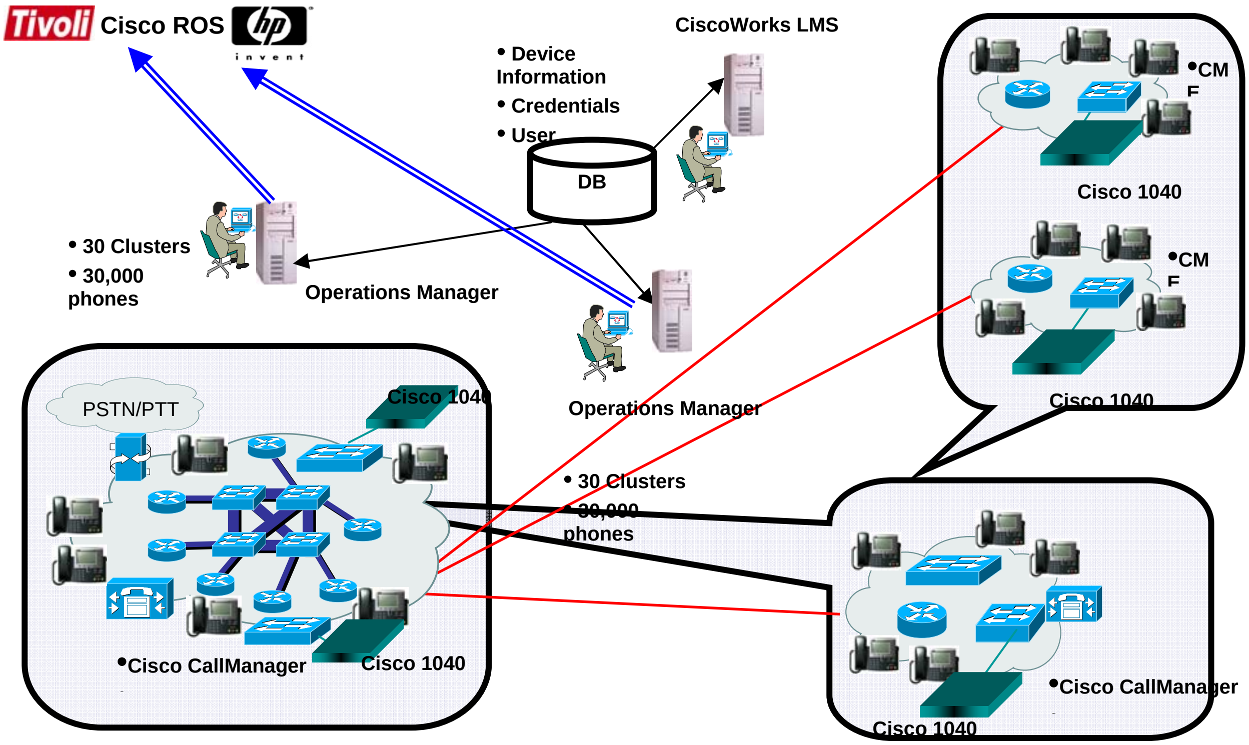


Figure 3: Deployment Model for Large Enterprises

3 Pre-Installation Tasks

This section describes the minimum configuration tasks that should be performed on Cisco IOS®, Cisco Catalyst®, and Cisco Media Convergence Server 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* from Cisco Press as well as Cisco.com.

3.1 Preparing Devices to be Monitored By Operations Manager

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

- SNMP v3 credentials*, or SNMP v2 read community string must be configured on each device.
- SNMP v2 write community string must be configured on each device (needed only for certain Routers and Switches on which IP 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 for Cisco IOS and Cisco Catalyst devices.
- IP connectivity must be verified between the devices and the Operations Manager server.
- For Cisco IOS, 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 CDP should be enabled on all the Cisco devices.
- If CDP is disabled (WAN interfaces usually have CDP disabled), use the ping sweep option. Ensure that you can ping the device from the Operations Manager server.

* SNMP v3 has limited support in Operations Manager. The SNMP v3 support for AUTH=None is not present in Operations Manager. Due to this condition, Operations Manager cannot be used with devices having SNMP V3, AUTH=None.

3.1.1 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
```

3.1.1.1 SNMP v2 Community Strings

Operations Manager can use SNMP v2 read community strings to retrieve fault and performance information from the devices. Some of the features in Operations Manager (Node-to-Node test, Survivable Remote Site Telephony 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 SNMP v2 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
```

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

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

3.1.1.2 SysName Variable

The system name 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 <name>
```

3.1.1.3 Setting up IP SLA on Cisco IOS devices

Certain features within Operations Manager use the IP SLA (formerly known as SAA or Real 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 ensure 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 Survivable Remote Site Telephony (SRST) Monitoring or in Node-to-Node tests. Typically, these are the edge routers in your branch networks and the default gateway for the Cisco CallManager. You can enable the IPSLA responder in the IP SLA router by running the following command (depending on the Cisco IOS 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
```

3.1.2 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.

3.1.2.1 SNMP v2 Community Strings

Operations Manager can use SNMP v2 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 SNMP v2 community strings on a Cisco CatOS 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 ensure that the device can be identified and that SNMP polling can be carried out.

3.1.2.2 Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) 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 network discovery and cannot gather information about Cisco IP Phones connected to these devices. Cisco Discovery Protocol is enabled by default, so you need to enable it only if it has been explicitly disabled. You might also want to disable Cisco Discovery Protocol on devices that are on the borders of your management domain.

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

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

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 DoS attacks. Cisco Discovery Protocol is also relevant to Cisco IOS devices (both routers and switches), because Cisco IOS is being increasingly used on new switches and even on Cisco Catalyst 6500s.

3.1.3 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 CallManager, Cisco Unity, Cisco Unity Connection, Cisco IP Contact Center, Cisco Conference Connection, Cisco Emergency Responder, Cisco IP Contact Center Express, and Cisco Personal Assistant.

3.1.3.1 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**). 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.

3.1.3.2 IBM UM Services

The hardware instrumentation on Cisco MCS on IBM platforms is provided by IBM 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. After this service is stopped, the Service Level View starts normally.

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

3.1.3.3 Windows/MCS SNMP Service

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

To define the SNMP read community string, perform the following steps:

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

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

For Cisco CallManager 5.0, the SNMP community string is configured through the Cisco CallManager Administration user interface. Because Cisco CallManager 5.0 resides on the Linux Operating System, there is no Windows SNMP service to configure.

3.1.3.4 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 for the traps to be sent to.

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

3.1.4 SNMP Management of IP Contact Center

The Microsoft Windows SNMP service is disabled as part of ICM setup and is replaced by the Cisco Contact Center SNMP Management service to process SNMP requests in its place. The Cisco IP Contact Center (IPCC) 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 Editio*n to install the correct SNMP components required for managing IPCC devices using Operations Manager.

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

- Note: In IPCC servers can also move into Partially monitored state
- Check if the Windows Management Interface (WMI) username (with domain Name e.g APAC\shaj) and password is entered in the Primary Credential field in DCR. If not, this needs to be entered. This is the username field when adding a device.

Installing the Cisco SNMP Agent Management Snap-in

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

Step 5 On the IPCC system, select **Start > Run...**

Step 6 In the Start box type, `mmc` and press **ENTER**.

Step 7 From the Console, select **File > Add/Remove Snap-in**. A new window appears.

Step 8 From the Standalone tab, verify that Console Root is selected in the Snap-ins added to: field and click **Add**.

Step 9 In the Add Snap-in window, scroll down and select **Cisco SNMP Agent Management**.

Step 10 Click **Add**.

Step 11 Click **Close**.

Step 12 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

Once you have loaded the Cisco SNMP Agent Management 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 console view.

To do so, select the console and use the Save As function. Select a distinctive filename, making sure to keep the .msc file extension. 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 SNMP v1 and v2c

If you are using SNMP v1 or v2c 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 SNMP v1 and v2c, 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 SNMP v1 or v2c. 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 SNMP v1 or SNMP v2c.

Step 8 (Optional) 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 9 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.

3.1.5 Cisco CallManager

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

3.1.5.1 HTTP Credentials

Operations Manager uses the AVVID XML Layer (AXL) API in addition to SNMP to manage Cisco CallManager. This means that Operations Manager will make SOAP calls over HTTP through the AXL interface to collect fault and performance information from the Cisco CallManager. Operations Manager needs an HTTP username/password to execute these queries. When you add or discover a Cisco CallManager with Operations Manager, you must supply a username/password or that Cisco CallManager will enter the partially monitored state (see section 5.3.3, Device Discovery Process). The username/password do not need to be *administrator* credentials. Any set of credentials with *read* level access that will get authorized for the URL http://server-name/ccmadmin will suffice.

3.1.5.2 HTTPS Configuration and Security Certificates

Cisco CallManager 4.1 or later supports enabling Secure Socket Layers (SSLs) on virtual directories. If you intend to secure the communication between Operations Manager and Cisco CallManager, you will need to enable SSL on the Cisco CallManager 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 CallManager Security Guide* for the appropriate release of Cisco CallManager. Also see the Using Device Manager chapter in *User Guide for Cisco Unified Operations Manager*.

Enabling HTTPS on Cisco CallManager

Step 1 On the Cisco CallManager 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 need to restart IIS service from the Control Panel.

3.1.5.3 Cluster Name of a Cisco CallManager Cluster

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

To change the cluster name of a Cisco CallManager, do the following:

Step 1 Open the Cisco CallManager 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 name. The default is StandAloneCluster. This should be changed so it is unique for every cluster.
Step 4 Click **Update**.

You will need to restart the Cisco CallManager service and the RIS DB Monitor service for these changes to take effect. Restarting these Cisco CallManager services causes a service disruption (of voice). To minimize disruption, be sure to schedule this task for a time when system maintenance is being done.

If OM is already managing the Call Manager and you are changing the cluster name, then the cluster names in the Service Level View will not reflect the new cluster name. You have to delete and readd the CMs in OM again for it reflect the new cluster name.

3.1.6 Cisco CallManager Express and SRST

For Cisco CallManager Express and SRST, the latest Speedbird Cisco IOS MIBs are required (e.g. Version 12.4(3.9)T7).

Go to Cisco.com and download the latest Cisco CallManager Express and Cisco IOS software for SRST which support new SNMP MIBs specific to Cisco CallManager Express and SRST, and their associated phones.

If you have a Cisco CallManager running 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 Speedbird MIB implementation is available on the router.

3.1.7 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.

- Note: In OM, Unity boxes can also move into Partially monitored state
- Check if the WMI username (with domain Name e.g APAC\shaj) and password is entered in the Primary Credential field in DCR. If not, this needs to be entered. This is the username field when adding a device.

3.1.8 Cisco Unity Express

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

The latest version of Cisco Unity Express supports SNMP for the first time, so older versions of Cisco Unity Express must be upgraded. To manage Cisco Unity Express, the latest Cisco Unity Express version (Speedbird) 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 config mode command prompt, the *snmp-server* command is not supported, then you need to upgrade to the latest Cisco Unity Express version.

Setting up Speedbird (Cisco Unity Express)

1) Untar the files.
2) From the NetworkModule boot prompt: config<cr>

TFTP server: <TFTPserverIP>
Default helper-file: aesop_helper

3) boot helper<cr>

The following appears:

```
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 into Cisco Unity Express.
At the Cisco Unity Express prompt, enter the following:

1) conf t<cr>
2) snmp-server community public RO
3) snmp-server community private RW
4) snmp-server host <yourTraphostIP> public
5) end
6) wr

3.2 Preparing the Server for Operations Manager

3.2.1 Operating System

Operations Manager is supported on Windows 2003 Server – Standard Edition and Windows 2003 Server – Enterprise Edition. Other operating systems are not supported. It is recommended that software other than the operating system and anti-virus software not be installed on this computer system. Operations Manager has been tested with Windows 2003 Server – Service Pack 1; hence, it is safe to install Service Pack 1 on the Operations Manager server.

3.2.2 Hostname

It is recommended that you configure the hostname 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 is a very laborious process involving file manipulation and the execution of scripts. *User Guide for Cisco Unified Operations Manager* documents all the steps involved in changing the hostname of the Operations Manager server.

3.2.3 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, visit www.macromedia.com and upgrade the Macromedia Flash Player on the Operations Manager server to Version 8.0.x. 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 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 blocked from the internet.

3.2.4 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.

3.2.5 DNS Settings

It is not mandatory that devices managed by Operations Manager be in DNS. 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 two 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.

Once 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.

3.2.6 Verify Open Database Connectivity (ODBC) Driver Manager

Some components of Operations Manager require the presence of the correct version of ODBC on the Operations Manager server.

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

Step 5 On the Operations Manager server, select **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Data Sources (ODBC)**.

Step 6 Click the **About** tab.

Step 7 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 Microsoft Data Access Component (MDAC).

Note: If the necessary OBDC is not listed, install MDAC 2.5 or higher by referring to the Microsoft website.

3.2.7 Enabling/Installing Windows SNMP Service

Operations Manager reports the status of its components through the host-resources and sysappl MIBs. This support enables 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 ensure 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 not use a default or well-known community string.

To verify that Windows SNMP Service is installed, perform the following steps:

- Open the Windows administrative tool Services window.
- Verify the following:
  - SNMP Service is displayed on the Windows administrative tool Services window (Windows SNMP service is installed).
  - SNMP service status is started (SNMP service is running).

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

3.2.8 Browser Version and Flash Plug-in

The recommended browser is Microsoft Internet Explorer 6.0.2600.0000 or IE 6.0.2800.1106. The browsers must have Macromedia Flash plug-in version 8. To detect and upgrade to Flash version 8, visit http://www.macromedia.com/support/flash/

Also supported is Internet Explorer version 6.0.3, which is shipped along with Windows 2003.

3.2.9 Device Connectivity

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

3.2.10 Terminal Server Services

Remote Desktop Service and/or VNC Services are recommended to remotely manage the Operations Manager server. VNC Services and Remote Desktop can be used to remotely install the Operations Manager (and Service Monitor) software.

3.2.11 Antivirus and Platform Agents

You should enable virus protection on the Operations Manager server, using antivirus software. Active scanning of drives and memory should be performed during off-peak hours. You may experience delays, and performance may be degraded, when the virus scan software is scanning all files. Operations Manager has undergone interoperability testing with the following:

- Third-party virus protection software:
  - Symantec Antivirus Corporate Edition Version 9.0
  - McAfee VirusScan Enterprise 8.0
- Platform Agents:
  - (Optional) Cisco Security Agent 4.0.3 (build 736)

3.2.12 System Capacity

	Maximum #
Number of devices	2,000 (voice devices)
Number of IP telephones	30,000
Number of IP ports	40,000
Number of CallManager clusters	30
Number of standalone CallManagers	150
Number of standalone CMEs/CUEs	500

Number of concurrent logins	10
Number of concurrent IP SLA tests	150
Number of devices on which capacity monitoring data collection is done concurrently	200
Number of concurrent confidence tests	200
Number of phone reachability tests	1000
Number of devices on which SRST monitoring is done concurrently	500

	Capacity		
System Parameter	**Small**	**Medium**	**Large**
Monitored phones	1000	10,000	30,000
Monitored devices	300	1000	2000
Monitored Cisco CallManager clusters	10	15	30
Monitored Cisco CallManager Express routers	100	250	500
Monitored SRST tests	10	100	500
Concurrent synthetic tests	25	100	250
Concurrent Node-to-Node (IP SLA/SAA) tests	25	100	250
Phone reachability tests	50	500	1000
Concurrent client (browser) logins	5	5	5

For IP Communications deployments of more than 30,000 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 a Cisco Secure Access Control Server, 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.

3.2.13 Server Sizing

Description	Specification		
Server Requirements			
System Parameters	**Up to 1,000 phones** **100 devices**	**Up to 10,000 phones** **100 - 1000 devices**	**Up to 30,000 phones** **1000 - 2000 devices**

Processor	Pentium 4 processor > 2 GHz	Pentium 4 or Xeon processor > 3 GHz	Dual Pentium 4 or Xeon processor > 3 GHz
Memory	3 GB RAM	4 GB RAM	4 GB RAM
Swap File	4 GB swap file	4 GB swap file	4 GB swap file
Disk Space	60 GB hard drive	60 GB hard drive	60 GB hard drive
Hardware	Server platform	Server platform	Server platform
Software	Windows 2003 Server	Windows 2003 Server	Windows 2003 Server
Discovery Time	20 – 30 minutes	2 – 2.5 hours	4 – 4.5 hours
Client Requirements			
Processor	Pentium 4 processor > 1 GHz		
Memory	512 MB RAM		
Swap File	1 GB swap file		
Hardware	Any PC/server platform		
Software	Microsoft Internet Explorer 6.0, Windows XP Home, Windows XP Professional, Windows 2003 Server		

The requirements in the previous table outline the minimum hardware configuration needed to operate Cisco Unified Operations Manager at different scalability levels. The client requirements dictate the platform from which the user interfaces (Internet browser-based) are invoked.

3.3 Preparing the Network

3.3.1 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, because it is never down. Ensure that the other interfaces do not have forward lookup pointing to incorrect DNS names.

Ensure 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.*

3.3.2 Configuring Cisco CallManager Security Certificates

Apart from SNMP Polling, Operations Manager runs AXL/SOAP queries on Cisco CallManager to retrieve information from Cisco CallManager. To secure this communication between Operations Manager and Cisco CallManager, Secure Socket Layer (SSL) must be enabled. This option is available for Cisco CallManager 4.1 or later.

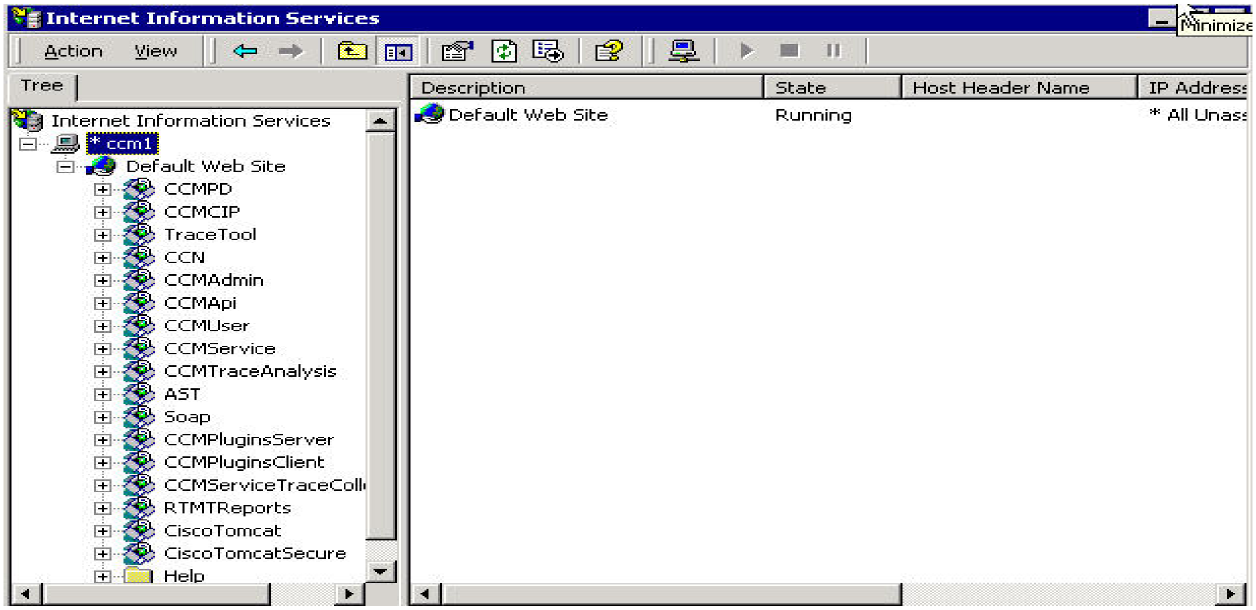
On Cisco CallManager 4.1 or later, enable SSL on these virtual directories:

- 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.

Steps to enable SSL on virtual directories in CallManager 4.1 or later:

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

Step 2 Click **CallManager** to expand it.

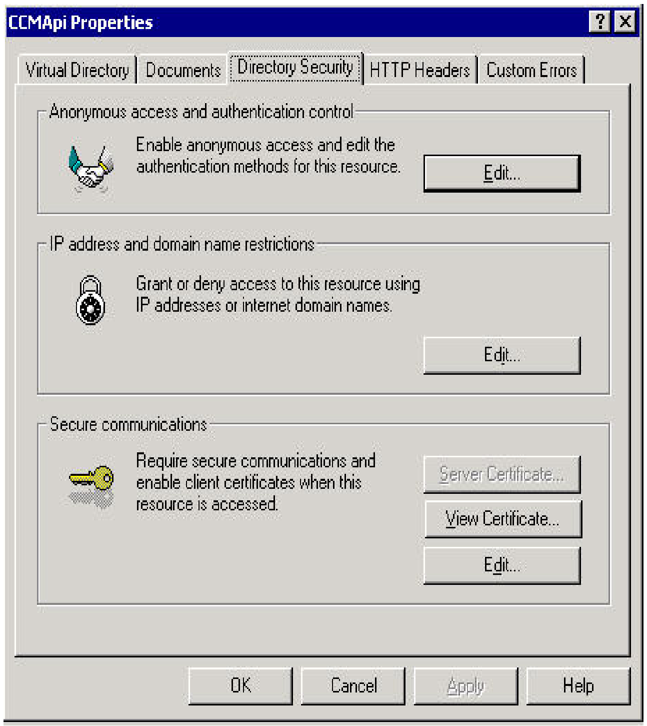


Internet Information Services
* ccm1
Default Web Site
CCMPD
CCMCIP
TraceTool
CCN
CCMAdmin
CCMApi
CCMUser
CCMService
CCMTraceAnalysis
AST
Soap
CCMPluginsServer
CCMPluginsClient
CCMServiceTraceColl
RTMTReports
CiscoTomcat
CiscoTomcatSecure
Help

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.



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

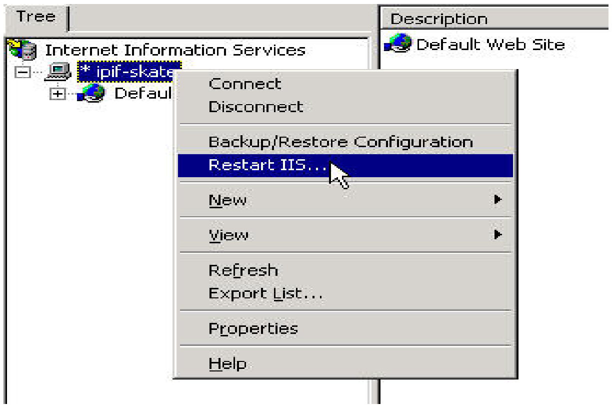
Grant or deny access to this resource using IP addresses or internet domain names.

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**)



Note: For more information, see the Cisco CallManager Security Guide documentation.

From OM version 1.1 onwards, the certificates will be import into OM automatically.

During device addition, please enter HTTP credentials. OM does the rest.

3.3.3 Check Routing and Firewalls

Ensure that any firewalls between the Operations Manager server and the managed devices are configured to allow management traffic through. See Section 3.3.6 for information on which ports should be opened.

Also, ensure 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.

3.3.4 Network Address Translation (NAT)

Operations Manager has limited support for NAT environments. For Operations Manager to support devices behind a NAT firewall, ensure that you have both IP and SNMP connectivity to the NATted IP addresses from the Operations Manager server. You can verify this by using ping commands and using an SNMP MIB browser.

Also, ensure that you do not have duplicate IP addresses across NAT domains that you are trying to manage with the same Operations Manager server. If overlapping IP address ranges exist, then you will need to dedicate different Operations Manager servers to manage these domains.

3.3.5 Network Time Protocol

To be able to correlate events across multiple devices, the devices need to have the same perception of the 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.

3.3.6 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 following TCP and UDP ports.

Table 1 Operations Manager Inbound Ports

Port Number / Type	**Usage**
162 / udp	Default port number used by Operations Manager for receiving traps
1741 / tcp	Used for CiscoWorks HTTP server
9000 / tcp	Trap receiving CSListener (Operations Manager server if port 162 is occupied)
9002 / tcp	Used by the Broker to listen to both the IP telephony server and the device fault manager
9009 / tcp	Default port number used by the IP telephony server for receiving traps from the device fault manager
40000–41000 / tcp	Used by Common Transport Mechanism for internal application messaging
42343 / tcp	Jrun
42344 / tcp	Used by Confidence Testing web service
42350–42353 / tcp	Used by messaging software
43441–43449 / tcp	Used as database ports
57860 / tcp	JRun Server Manager ControlServer - Used for Jrun Administration

Table 2 Operations Manager Outbound Ports

Port Number / Type	**Usage**
161/udp	Standard port for SNMP polling
162/udp	Standard port for SNMP traps
23/tcp	Standard port for Telnet
22/tcp	Standard port for SSH
42340/tcp	CiscoWorks Daemon Manager, the tool that manages server

	processes
42342/udp	Osagent
69/udp	Standard port for TFTP
1683	IIOP port for CiscoWorks gatekeeper
8088	HIOP port for CiscoWorks gatekeeper
514/tcp	RCP port
42351/tcp	Default port; alternate port: 44351/tcp (ESS1 listening port)
42353/tcp	Default port; alternate port: 44353/tcp (ESS routing port)
42350/udp	Default port; alternate port: 44350/udp (ESS service port)

Table 3 Service Monitor Ports

Port Number / Type	Usage
53 / udp	DNS
67 and 68/udp	DHCP
69/udp	TFTP —Service Monitor uses TFTP to find the configuration file for a given Cisco 1040 Sensor
514/udp	Syslog—Service Monitor receives syslog messages from a Cisco 1040
2000 / tcp	SCCP—Service Monitor uses SCCP to communicate with Cisco 1040s
5667	Interprocess communication
43459/tcp	Database

4 Operations Manager Installation

4.1 Preinstallation Checks

- Dual homing (dual NIC), using 2 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 fail-over configuration, in case one of the NIC cards fails) is supported.
- Make sure that you change the default Cisco CallManager cluster ID setting (located at CallManager Administration > Enterprise parameters). The default setting is Stand Alone Cluster. Unless you change this entry, all of the clusters will have the same cluster ID. This causes problems in Operations Manager. Changing the cluster ID requires a restart of RIS Collector service, Windows SNMP service, and the CCMadmin service. Perform these restarts on the publisher and then on the subscribers.

If OM is already managing the Call Manager and you are changing the cluster name, then the cluster names in the Service Level View will not reflect the new cluster name. You have to delete and readd the CMs in OM again for it reflect the new cluster name.

- Make sure that the Operations Manager server's hostname is resolvable using DNS. If DNS is not being used, edit the Windows hosts file and enter Operations Manager hostname and IP address. The hosts file is located at 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
```

4.2 Installation procedures

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

4.3 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.

4.4 Uninstallation

The uninstallation process may display a warning message similar to the following:

```
The uninstallation is waiting for a process to stop, do you
wish to continue to wait?
```

If you see this message, click Yes and continue to wait.

It is a good practice to delete the C:\Program Files\CSCOpx folder 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, from the C:\Program Files\CSCOpx\data folder.

5 Initial Configuration

5.1 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 present 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 the popup windows is eliminated and the buttons at the bottom are visible.

5.2 IP Address or Hostname Changes

Make sure that devices are not entered into Operations Manager or the Common Services Device Credential Repository (DCR) more than once. For example, 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 (by selecting Devices > Device Management) 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.

To avoid discovering the same device multiple times (with different IP addresses), use **Devices > Device Management** and click the **Configure** button (the second button). Enter the IP addresses you want to exclude.

5.3 Network Discovery and Device Management

For Operations Manager to monitor a device, you must first add the device to the Device and Credentials Repository (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 Devices > Device Management > View/Rediscover/Delete.

- The DCR inventory—To view, select Devices > Device Credentials.

Deleting a device in Operations Manager (Devices > Device Management > View/Rediscover/Delete) does not remove it from the DCR.

Deleting a device in the DCR (Devices > Device Credentials) removes it from both the Operations Manager inventory and the DCR.

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

5.3.1 Network Discovery Options

5.3.1.1 CDP-Based Discovery

Operations Manager device discovery is based on CDP, route table, and ARP table using a seed device. Operation Manager uses CDP neighbors, ARP table, and route table entries to discover the network from the seed device.

5.3.1.2 Ping based discovery

You can choose to add a ping sweep (by selecting the use Ping Sweep check box) in addition to or instead of the CDP, 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 CallManager (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 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.

Considerations for using the automatic discovery IP include and exclude filters are described in more detail in Section 5.3.1.3.1.

5.3.1.3 Credential Discovery and MIB II information

Automatic discovery uses the list of credentials configured on the Default Credentials page (Devices > Device Management > Discovery Credentials) to determine the correct SNMP v2/v3 credentials and/or HTTP (or HTTPS) credentials for the device. Once the correct credentials are determined, automatic discovery retrieves MIB II information from the device and populates this information in the DCR.

5.3.1.3.1 Auto-Discovery 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. Once a device IP address satisfies a filter, other filters will not be applied to the device.

For example, if 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 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	Within range	Within range	Not applied

	default *.*.*.*			
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.

5.3.1.3.1.1 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.

5.3.1.3.1.2 DNS Domain Filter

The DNS filter works in a similar manner 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 once 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.

5.3.1.4 Phone Discovery

Phone discovery is performed separately from device discovery. Phone discovery starts after device discovery completes. In Operations Manager, go to **Devices > 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.

5.3.1.5 Cisco Catalyst 6000 Discovery

When discovering a Cisco CallManager, Operations Manager discovers the trunk cards on a Cisco Catalyst as gateways. If the Cisco Catalyst 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 is added and monitored by Operations Manager. When the Cisco Catalyst 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.

5.3.1.6 Troubleshooting Discovery Issues

If you can ping the device from the Operations Manager server and device discovery still 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>
```

5.3.2 Device Import Options

5.3.2.1 Discovery-Based Import

To add devices automatically into Operations Manager, go to **Devices > Device Management**. From the Device Management: Summary page, click the **Configure** button next to Device Selection. From the Device Selection page, select Automatic (the default device selection setting for Operations Manager).

5.3.2.2 Synchronizing with the DCR

Operations Manager uses CiscoWorks Common Services 3.0 as its application framework. The Device and Credentials Repository (DCR), a function of CiscoWorks Common Services 3.0, 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 version 3.0 or later.

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.

For more information, see Sections 2 and 3 in “CiscoWorks Common Services 3.0 Whitepaper” (http://www.cisco.com/application/pdf/en/us/guest/products/ps3996/c1244/cdccont_0900aecd802be11a.pdf).
Note: The document has examples of other CiscoWorks products, such as LAN

Management Solution (LMS), Routed WAN (RWAN) Management Solution, and VPN/Security Management Solution (VMS) bundles. The setup of the DCR is similar to those applications.

5.3.2.3 Manual Device Import

To add a device or devices individually into Operations Manager, go to **Devices > Device Management**. From the Device Management: Summary page, click the **Configure** button next to 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 (RSK) is installed on all Unity and Unity Connection servers.

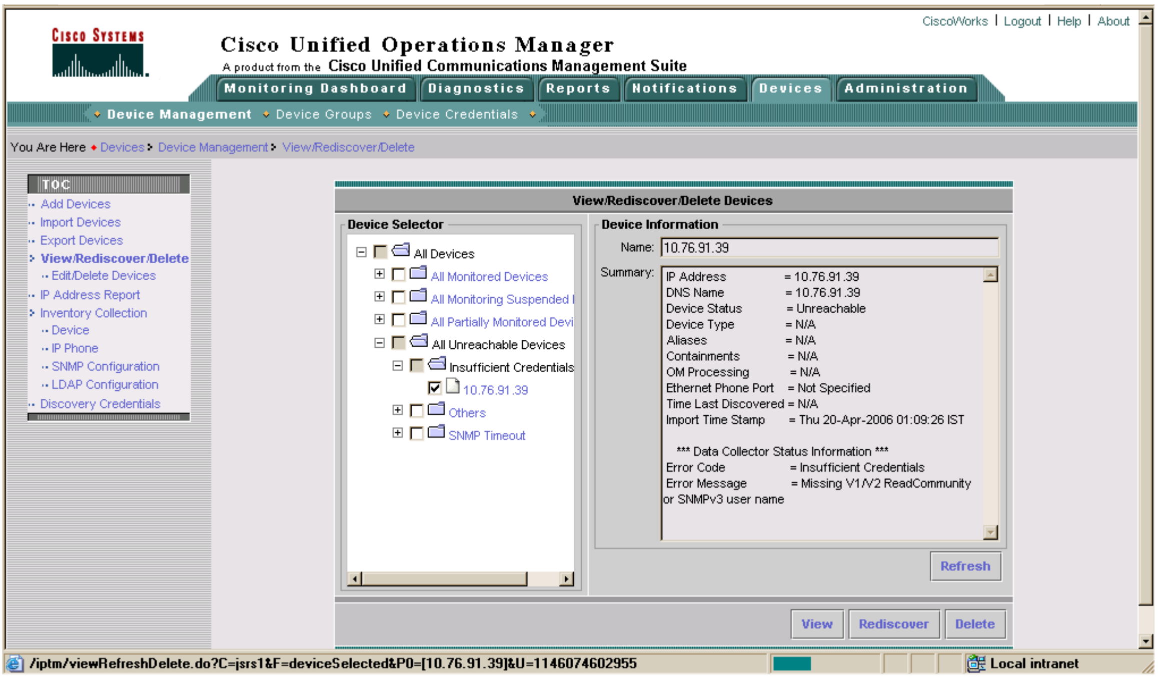
5.3.3 Device Discovery Process

5.3.3.1 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 CallManager 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.
- Monitoring Suspended—Monitoring of the device is suspended.
- Inventory Collection in Progress—Operations Manager is probing the device. This is the beginning state, when the device is first added; a device is also in this state during periodic inventory collection. Some of the data collectors may still be gathering device information.
- Unreachable—Operations Manager cannot manage the device. This can occur if the device cannot be pinged, if SNMP service is not turned on, or if the R/O 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 View/Rediscover/Delete Devices page (Devices > Device Management > View/Rediscover/Delete). In the View/Rediscover/Delete Devices page, open the All Unreachable devices (or Unsupported) folder. Click on the device name/IP address (not the check box). The Data Collector Status Information section provides a detailed error code.



Name: 10.76.91.39

Summary:

```
IP Address          = 10.76.91.39
DNS Name            = 10.76.91.39
Device Status       = Unreachable
Device Type         = N/A
Aliases             = N/A
Containments        = N/A
OM Processing       = N/A
Ethernet Phone Port = Not Specified
Time Last Discovered = N/A
Import Time Stamp   = Thu 20-Apr-2006 01:09:26 IST

  *** Data Collector Status Information ***
Error Code          = Insufficient Credentials
Error Message       = Missing V1/V2 ReadCommunity
or SNMPv3 user name
```

/iptm/viewRefreshDelete.do?C=jsrs1&F=deviceSelected&P0=[10.76.91.39]&U=1146074602955

5.3.3.2 Resolving Discovery Conflict

- Gateways associated with a Cisco CallManager are discovered during the Cisco CallManager discovery process. You may see a grayed-out gateway in the Service Level View. This occurs when a gateway is discovered through Cisco CallManager, 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 CallManager 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. Once 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 CallManager cluster ID setting. The cluster ID is set to Stand Alone Cluster by default. Unless you change this entry, two clusters will have the same cluster ID, which will lead to confusion in Operations Manager. Cluster ID name changes require a restart of the RIS Collector service, Windows SNMP service, and CCM Service, first on the publisher and then on the subscribers.
- Cisco ATA devices will appear in the Service Level View as unmanaged (grey) devices. There is a v1.1 patch that will remove the ATAs from the SLV.

5.4 Diagnostic Tests

5.4.1 Synthetic Tests

The MAC address for synthetic phones must be between 00059a3b7700 and 00059a3b8aff.

Synthetic testing is a mechanism by which Operations Manager emulates a phone. For example, Operations Manager makes phone calls, logs in to conferences, leaves voice mails, makes emergency calls, and downloads TFTP files. When any of these operations fails, Operations Manager flags the failure as an alert, letting the operations personnel know that there could be a problem.

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

5.4.2 Synthetic Test Descriptions and Expected Results

Synthetic Test Descriptions

Synthetic Test	Description	Expected Results
Phone Registration	Opens a connection with the Cisco CallManager/ CallManager Express and registers a simulated IP phone.	Successful registration of the phone.
Off Hook	Simulates an off-hook state to the Cisco CallManager/CallManager Express and checks for receipt of a dial tone.	Receives a dial-tone signal from the Cisco CallManager. The registration of the synthetic phone takes place only for the first time because registration is a costly operation on Cisco CallManager. (However, if the test fails, then synthetic phones are registered again for the next test cycle only.) Once the synthetic phone is registered, Operations Manager checks for a dial-tone signal from the Cisco CallManager.
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

Synthetic Test Descriptions		
Synthetic Test	**Description**	**Expected Results**
		accept the call. **Note** 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 CallManager/ CallManager 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 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.
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.
Unity	Calls the target phone and	Activation of the phone's message-waiting

Synthetic Test Descriptions		
Synthetic Test	**Description**	**Expected Results**
Message Waiting Indicator Test	leaves a voice message in the voice mailbox.	indicator. The message is then deleted and the message-waiting indicator is deactivated.

5.4.3 How Many Simulated IP Phones Do I Need?

The number of simulated IP phones you need to define in the Cisco CallManager/ CallManager Express depends on the number of tests you plan to configure. Different types of confidence tests need a different number of IP phones.

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 a good idea to input the description for these IP phones as "Operations Manager Simulated Phone" when they are configured in the Cisco CallManager/Call Manager Express so that it is distinct from the descriptions of other IP phones in the Cisco CallManager/CallManager Express. The phones to be used in confidence testing must be configured as 7960 phones in the Cisco CallManager/CallManager Express.

Number of Phones Required for Confidence Tests			
Number of Tests	**Type of Test**	**Phones Needed for Test**	**Total Phones Needed**
	Phone Registration	1 (synthetic phone)	1 per Cisco CallManager and CallManager Express
	Off Hook	1 (synthetic phone)	1 per Cisco CallManager and CallManager Express
	End-to-End Call test with real phones	2 (1 synthetic phone and 1 real phone)	2 per Cisco CallManager and CallManager Express
	End-to-End Call test with synthetic phones	2 (synthetic phones)	2 per Cisco CallManager and CallManager Express
	TFTP Receive test	0	
	Emergency Call (without On Site Alert Number)	2 (synthetic phones)	

Number of Phones Required for Confidence Tests			
Number of Tests	**Type of Test**	**Phones Needed for Test**	**Total Phones Needed**
	Emergency Call (with On Site Alert Number)	3 (synthetic phones)	
	Cisco Conference Connection test	2 (synthetic phones)	
	Unity Message-Waiting Indicator test	2 (synthetic phones)	

5.4.3.1 Using an End-to-End Call Test to Monitor the Quality of Voice

You can use the End-to-End Call synthetic test in conjunction with the Cisco 1040 Sensor and Cisco Unified Service Monitor to place a test call and then monitor, in real time, the Mean Opinion Score (MOS) for the test call.

For example, when you receive a complaint about poor voice quality on a phone, you can do the following:

1. In Operations Manager, go to the IP Phones report and find the switch port number that the phone is connected to.
2. Make sure that the switch port is being spanned by the Cisco 1040.
3. Go to the Service Monitor application and configure an appropriate MOS threshold (a value of 4.5 is the highest MOS value which equates to a perfect call). Entering a MOS threshold of 4.5 is useful to temporarily monitor the quality of voice on all calls, regardless of poor quality.
4. In the Operations Manager IP Phones report, right-click the phone with poor voice quality.
5. Create and schedule an End-to-End Call test from Operations Manager to the phone.

   Make sure to “enable RTP” and “Wait for Answer” when creating the test call. Enabling RTP will cause Operations Manager to play a recorded announcement when the test call is answered. Make sure that either someone answers the phone or the phone line is set to “auto answer” in Cisco CallManager.
6. Monitor the Service Quality Alerts page and view the MOS for that test call.

   Do not maintain a MOS threshold of 4.5 or greater in Service Monitor for a long period of time. A MOS threshold of 4.5 is useful as a temporary troubleshooting tool, but may slow the system down.

5.4.4 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 (IP SLA) on any Cisco IOS device across a WAN.

5.4.4.1 Preparing Devices for Node-To-Node Tests

You need to manually enable the IP SLA in Cisco IOS. You may need to configure, depending on the Cisco IOS device, the RTR Responder, or the IP SLA Responder Command Line Interface (CLI).

5.5 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 (CIC), HP OpenView Network Node Manager (NNM), or Tivoli Netview.

The e-mail and e-page notification mechanisms provide additional ways of informing network operations personnel about the alerts in their network. This frees network personnel from having 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. Operations Manager can alert up to 116 events in total. Event sets enable 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:
Allows you to set up notifications based on devices or service quality parameters.

When setting up e-mail notifications, make sure the following are taken care of in the Operations Manager server:

- Port 25 is open for the e-mail notification.
- If Virus Scan is installed, Virus Scan > Properties > Blocking > Block the connection is 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.

5.5.1 CISCO-EPM-NOTIFICATION-MIB

CISCO-EPM-NOTIFICATION-MIB is specifically defined to carry details of the Alerts and Events generated by 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

Alert-Based Notification:
For alert-based notification, the following is the format of values contained in a few key attributes.

cenAlarmInstanceID:

Contains the alphanumeric value assigned to the alert. 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 alert status. The possible cenAlarmStatus values in Operations Manager are 1, 2, and 3.

cenAlarmStatusDefinition contains the <numeric value> <status description> of the alert. 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 up to three of the latest events.

cenAlarmSeverity and cenAlarmSeverityDefinition:

cenAlarmSeverity contains a numeric value associated with the alert 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 field. 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 would be: cenCustomerIdentification- “-“ and cenCustomerRevision – “*”

5.6 Performance and Capacity Monitoring

The performance data is stored in C:\Program Files\CSCOpx\data\gsu_#GSUdata#_ for 72 hours.

The Node-to-Node test results are stored in C:\Program Files\CSCOpx\data\N2Ntests for 31 days.

For more information, see Chapter 7 and Appendix I in *User Guide for Cisco Unified Operations Manager*, and EDCS-437408.

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 first day's file 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.

5.6.1 Enabling Or Disabling Monitoring

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

5.6.1.1 Trending and Alerting

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

5.6.1.2 Capacity Planning Use

Archive the performance data periodically (within 72 hours). Use this data to view longer trends (longer than 72 hours). Excel, for example, can be used to view .csv files. See the user guide appendix for details on the archived files. .

5.6.2 Polling and Thresholds

5.6.2.1 How Do I Change Polling and Threshold Values?

From the Service Level View, right-click a device and select Polling Parameters. You can also access polling parameters from Administration > Polling and Thresholds.

If you change some server settings, e.g. "managed state" to "false" so as monitoring is disabled, upon rebooting the server all settings return to default. To ensure that OM persists these changes, one needs to manually go to the Administration-->Polling And Threshold --> Apply Changes and click on "Apply". [One caveat here is that OM sometimes disallows "Apply" under some conditions. In such cases, one can make an "Apply" to go through by changing some polling settings, and then retrying the "Apply" operation.]

5.6.3 Trap Receiving and Forwarding

Trap receiving and forwarding is configured on the Systems Preferences page (Administration > Preferences).

Do not confuse this feature with SNMP notifications. This feature is to forward traps to a Manager of Managers (MOM).

5.6.4 SRST Monitoring

5.6.4.1 Setting Up and Managing SRST Tests

Survivable Remote Site Telephony (SRST) tests are only configurable on SRST devices. This test will not appear on other device types. You can access SRST tests at 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 *and* the SRST phone becomes unregistered to the Cisco CallManager, Operations Manager determines the branch office to be in SRST mode.

When creating an SRST test, the IP SLA device should be a Cisco IOS device closest to the Cisco CallManager serving that SRST remote office, preferably on the same subnet as the Cisco CallManager. 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.

6 Cisco Unified Communications Service Monitor

When the Cisco 1040 Sensor boots up, it uses DHCP option 150 to TFTP its configuration and image files. Note that the Cisco 1040 does not support CDP and thus does not receive any Auxiliary VLAN information from the switch that it is plugged into. If you are using two VLANs, one for voice and a second for data, make sure that a single VLAN is configured on the switch port that the Cisco 1040 is plugged into. Make sure that this VLAN has a DHCP server configured for that subnet/VLAN.

Similar to the way that an IP phone registers with a Cisco CallManager, a Cisco 1040 Sensor registers (also using SCCP) to the Service Monitor application. On the TFTP server, the Cisco 1040 first looks for its configuration file, named QoV [*Cisco 1040 MAC address*].CNF. If that file does not exist, the Cisco 1040 looks for a file named QOVDefault.CNF. This is a generic configuration file to be used when the “auto registration” option is selected within the Service Monitor application. These .CNF files provide the image filename for the Cisco 1040 to download, in addition to the Service Monitor IP addresses. The Cisco 1040 then downloads this image and registers to the Service Monitor, just like a phone registers to a Cisco CallManager, using SCCP.

The following are some important points that you should be aware of when you are configuring a Cisco 1040:

1. The Cisco 1040 has two Ethernet ports. The first port is for DHCP and TFTP; port #1 is the IP address for the sensor. This port is also for PoE (IEEE PoE).

On a Catalyst 3550, you might need to configure the switch port that is connected to the sensor's port #1. If port #1 on the Cisco 1040 flaps when plugged into a Catalyst 3550 switch port, configure the Catalyst 3550 switch port using the following Cisco IOS CLI: **power inline delay shutdown 20 initial 30**.

2. The 2nd port has no IP address and is used to connect to the switch using a span port that spans phone ports, gateway ports, or VLAN with Real-Time Transport Protocol (RTP), basically spanning any port(s) that has RTP flowing through it. The closer to the phone port, the more consistent the MOS calculated by the Cisco 1040 will be to that of the end user experience. Choose the phones/phone calls that you want to monitor, choose a port to span, and configure that span port. This is an example of performing the configuration using the Cisco IOS CLI:

```
Cisco Internetwork Operating System Software IOS (tm) C3550 Software
monitor session 1 source interface Fa0/18 , Fa0/22 rx
monitor session 1 source interface Fa0/4
monitor session 1 source vlan 1 rx
monitor session 1 destination interface Fa0/9
```

3. Place the image file (.img) and the configuration file (.cnf) on the TFTP server that the phones are using. For Cisco CallManager, it is usually the C:\Program Files\Cisco\TFTPPath directory. For Cisco CallManager Express (CME), it is usually the router’s flash.

The following Cisco IOS CLI commands are used to allow download of these files from a CME router's flash:

tftp-server flash:SvcMonAA2_24.img

tftp-server flash:QOVDefault.cnf

4. Sometimes the .CNF extension gets tied to a "SpeedDial" Windows application and it is a bit tricky to open up this file in Notepad, if editing is required. If this occurs, drag and drop this file into an open Notepad. Change the IP address in the "Receiver=;" entry to the Service Monitor (or to Operations Manager if Service Monitor and Operations Monitor are on the same system) server IP address that you are using in your network. The Cisco 1040 Sensor will send syslogs to this address. Service Monitor then converts this syslog to a trap and forwards this trap northbound (to Operations Manager if Service Monitor and Operations Manager are on the same system, or to a MOM like HPOV, or CIC). (NOTE: Manually editing the .CNF file is not recommended.)

5. You will need to go into the Service Monitor and Operations Manager GUIs to set up MOS thresholds, archiving, and registration of the Cisco 1040.

For example, an end user calls to complain about poor voice quality. Go to the Operations Manager Phone Report page and find the switch port number that the phone is connected to. Make sure that switch port is being spanned by the Cisco 1040. (That is, verify that the switch port that Cisco 1040 port #2 connects to is configured to monitor/span the switch port that the phone is connected to.)

Go to the Service Monitor application and configure an appropriate MOS threshold; a value of 4.5 is the highest MOS value, equating to a perfect call. Entering a MOS threshold of 4.5 is useful to temporarily monitor the quality-of-voice on all calls, regardless of quality.

From the Operations Manager Phone Report page, right-click the phone with poor voice quality. Create and schedule an End-to-End Call test from Operations Manager to the phone. Make sure to “enable RTP” and “Wait for Answer” when creating the test call. Enabling RTP causes Operations Manager to play a recorded announcement when the test call is answered. Make sure that either someone will answer the phone or the phone line is set to “auto answer” in Cisco CallManager. In Operations Manager, monitor the Service Quality Alerts dashboard and view the MOS for that test call.

Note: Do not maintain a MOS threshold of 4.5 or greater in Service Monitor for a long time. A MOS threshold of 4.5 is useful as a temporary troubleshooting tool, but will slow the system down.

You can change the recorded announcement that is played when Operations Manager places an End–to-End Call test with RTP enabled. To do so, back up the tiatc-ulaw.wav file under CSCOpx\objects\ama and delete it. Then copy a G711 ulaw wave file to the CSCOpx\objects\ama folder and rename it to tiatc-ulaw.wav.

Figure 4 illustrates the different states that the Cisco 1040 can be in and shows how the LED on the Cisco 1040 (located on the front panel) indicates the current state through color and by blinking or shining steadily.

Cisco 1040 State Diagram

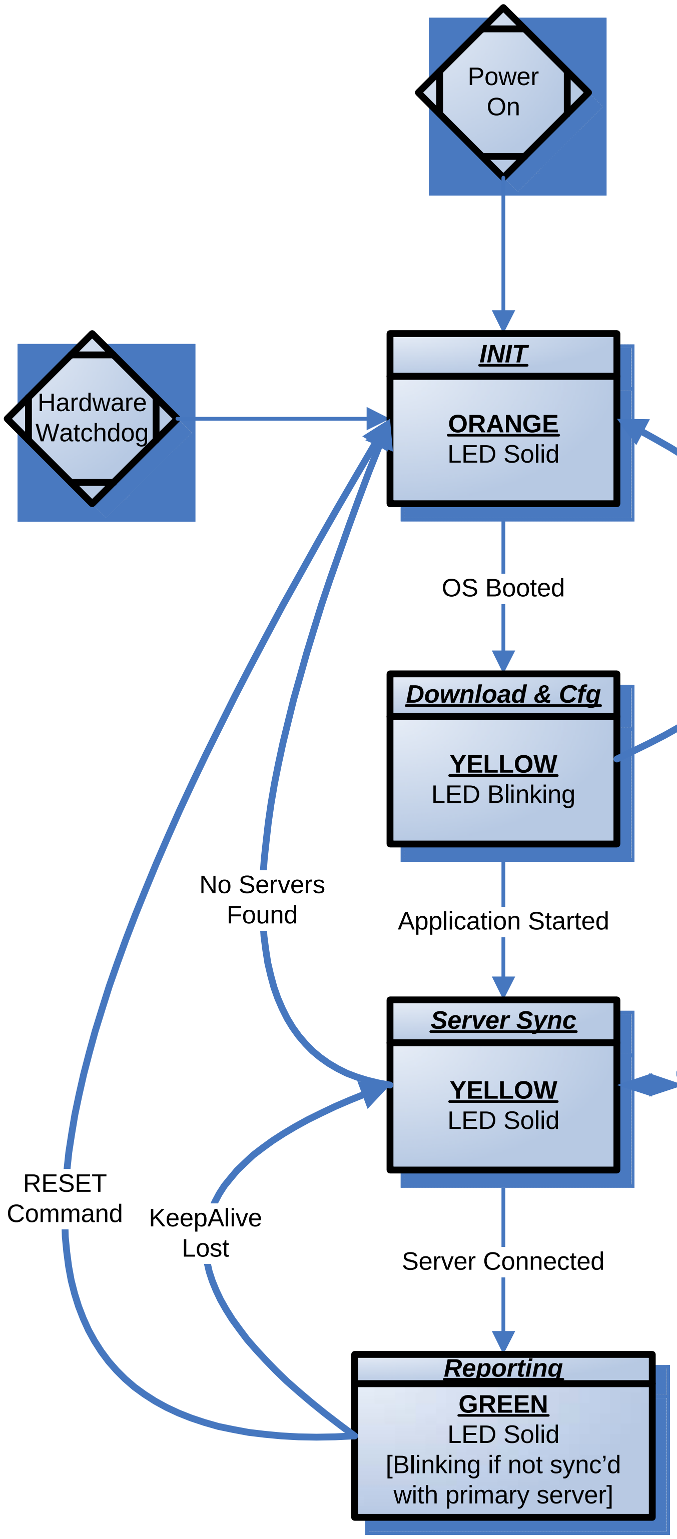


Figure 4. Cisco 1040 State Diagram

You can use the following points to troubleshoot or to simply confirm that everything is configured correctly:

- Check the DHCP server for the Cisco 1040's MAC address.

Enter this command using Cisco IOS CLI:
router#sh ip DHCP bind

```
Bindings from all pools not associated with VRF:
IP address        Client-ID/              Lease expiration          Type
                  Hardware address/
                  User name
10.15.160.115     0012.8200.302a          Mar 01 2000 04:42 AM      Automatic
```

To configure DHCP on a Cisco IOS device (Example):

```
ip DHCP pool probe
  network 192.168.137.128 255.255.255.240
  default-router 192.168.137.129
  domain-name cisco.com
  option 150 ip 192.168.137.129
  dns-server 171.69.2.133 171.68.10.70
  lease 30
```

- Check the TFTP server for file transfer to the Cisco 1040
  For CM, the TFTP directory is C:\Program Files\Cisco\TFTPPath.
  For CME, the TFTP directory is typically the router's flash: "show flash"

- Check the syslog.log file in C:\Program Files\CSCOpx\log. Make sure events are current and being updated. Cisco 1040 syslogs are clearly marked.

Table 4: Syslog Format

Description	**TAG**	**Example**	**Max size i**
Flag	A	0: Actual 1: Sample	1
Source device IP address	B	F0.F0.F0.58	11
Recipient device IP address	C	F0.F0.F0.49	11
Codec of call segment	D	1: Non-standard 2: G711Alaw 64k 3: G711Alaw 56k	3

Description	TAG	Example	Max size i
		4: …… <Refer to appendix A for the complete list>	
Calculated MOS score for call	E	35 (for 3.5) (44 is a perfect call)	2
Primary cause of call degradation	F	J: Jitter P: Packet Loss	1
Actual packet loss	G	9999 (Decimal)	4
Actual jitter	H	9999 (Decimal)	4
Total	—	—	37

- Check the trapgen.log file in C:\Program Files\CSCOpx\log\qovr. Make sure events are current and being updated.
- Enable Call Metrics and check the .csv file in C:\Program Files\CSCOpx\data\CallMetrics and ensure that the files are being created every 60 seconds.
- Check the http pages on the Cisco 1040 sensor: http://<1040 ip address> and http://<1040 IP address>/Communication for device details.
- Ensure that you do not have a port conflict on port 162, the SNMP trap port. Software such as MGSoft will conflict with the Operations Manager QoV trap reception on port 162. Also, disable Windows "SNMP Trap Service" under Administrative Tools > Services and then restart the SNMP Daemon Manager.

Table 5: Data Format for Service Monitor Archived Call Metrics

Description	Value
Cisco 1040 ID	A letter and a 3-digit number; for example, A100
Time stamp	Date and time
Flag indicating actual or sampled data	0: Actual 1: Sampled
Source device IP address	IPv4 address; for example, 172.020.119.043

Description	Value
Destination device IP address	IPv4 address; for example, 172.020.119.025
Codec of call data record	2: G711Alaw 64k 6: G722 64k 9: G7231 10: G728 11: G729
Calculated MOS score	2-digit number with an implied decimal point between the first and second digits
Primary cause of call degradation	J: Jitter P: Packet Loss
Actual packet loss in the previous minute	<numeric value>
Actual jitter, in milliseconds, in the previous minute	<numeric value>

7 Best Practices

7.1 Disabling Hyperthreading

Disabling hyperthreading on the Operations Manager server can substantially improve its performance.

The following procedures may vary, depending on the vendor:

1. Enter the BIOS Configuration and Setup screen by powering up the server and pressing F1 during system startup.
2. Go to **Advance Setup** > **Advance Processor Option** > **Hyperthread**.
3. Select Disabled.
4. Press ESC, to return to the main menu.
5. Select Save Settings, and press Enter.
6. Select Exit Setup, and press Enter, to continue the reboot process with hyperthreading disabled.

7.2 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.

7.3 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.

7.3.1 Preparing for Redundancy

This section describes some pre requisites for redundant OM configurations.

The first step is to have two identical servers available for configuration. One server acts as “Active” and the second a “Standby”. Please refer to the OM installation guide for the hardware specification of these servers. (http://www.cisco.com/en/US/products/ps6535/products_installation_guide_chapter09186a008063d8b5.html#wp1093273)

It is recommended that these servers connect to the network through redundant paths. This ensures that a failure in one part of the network that affects the Active server does not also affect the connectivity of the Standby server.

The instructions given below apply to CUOM 1.1 with SP1 patch. Please contact your TAC representative to obtain a copy of SP1 for CUOM 1.1

Follow this link to get to the SP1 patch:

http://wwwin-nm.cisco.com/Patches/patch-publisher/listbyproduct.cfm?searchbug=CSCsc84584&searchcomponent=&searchfile=&thisfamily=&thisproduct=2.+choose+product&searchProduct=UOM&searchheadline=&searchowner=&fromForm=yes&submit=Submit

7.3.2 Setting up redundancy

Redundant deployment can be considered in four parts.

a) Setting up the Active OM server
b) Setting up the Standby OM server by creating a baseline.
c) Replicate Active OM configuration to Standby OM configuration on a ongoing basis
d) Things to do in case of Failure of Active server.

7.3.3 Setting up the Active OM server

This is the same as setting up a standalone OM 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 (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 north bound notifications
- Configuring Service Monitor to forward traps to OM.
- Configuring Cisco 1040 Probes to register to the Service Monitor

- Configuring System Preferences such as Forwarding Trap Servers, Trap Community strings, SMTP servers for north bound notifications, cross launch-able LMS servers

See the user guide for explanation about each task (http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cuom/cuom1_1/userguid/index.htm)

7.3.3.1 Setting up the Standby server

Once the Active is setup, the Standby server needs to be setup in such a way that it is has the exact same configuration as the Active server. This can be achieved using the “Backup and Restore” feature in OM. The procedure to perform the backup and restore is as follows.

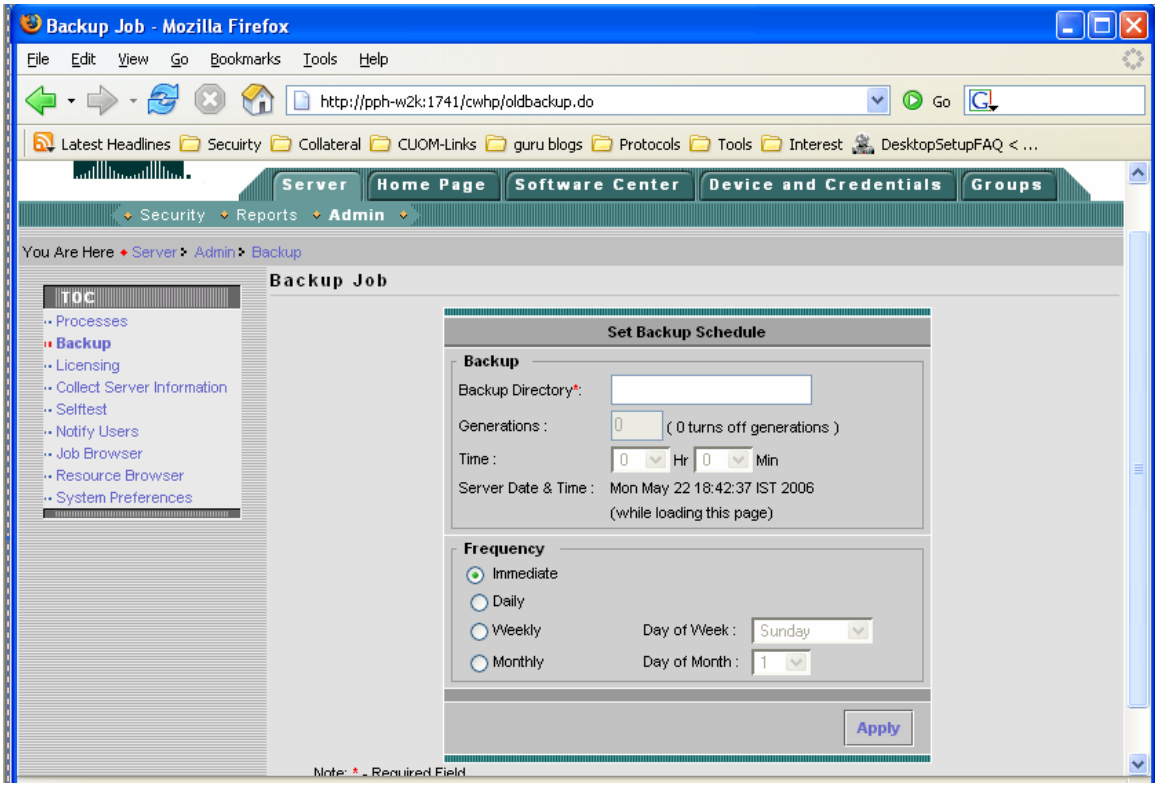
Backup:

Go to the Active OM 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 OM server and copies it into backup directory mentioned. The Number of generation refers to the maximum backups that can be stored under the backup directory. For example, if the number of generations is 2 then two consecutive invocation of this script would create <Backup dir>\0, and <Backup_dir>\1 until it starts wrapping.

Instead of the command line, you could also use the Common Services user interface shown below.



Backup Job

Set Backup Schedule

Backup

Backup Directory*:

Generations : 0 (0 turns off generations)

Time : 0 Hr 0 Min

Server Date & Time : Mon May 22 18:42:37 IST 2006 (while loading this page)

Frequency

● Immediate

○ Daily

○ Weekly Day of Week : Sunday

○ Monthly Day of Month : 1

Apply

Note: * - Required Field

Figure 5 Backing up server data

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.

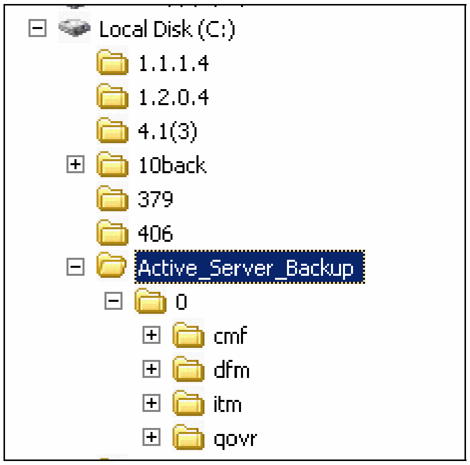
It is recommended that this backed up data directory be kept on a separate system so that it is not affected by disk crashes or any issues associated with the Active server.

Once the data backup is completed, this information needs to be imported to the Standby server using the “Restore Facility” in OM.

Restore:

Go to the Standby Server. Transfer the backup directory from the Active 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 following directory structure.



Copy the entire contents under C:\Active_Server_Backup to the Standby server with the exact same structure.

1. Run 'perl <INSTALL_DIR>\objects\vhm\utilities\dbclean.pl' (This will clean the database)

2. ‘net stop crmdmgtd’ - Start the Daemon manager.

3. ‘net start crmdmgtd’ - Stop the Daemon manager. This is required by the restore script.

4. Run 'perl <INSTALL_DIR>\CSCOpx\bin\restoreBackup.pl -d <backupDir>' - The backup directory is C:\Active_Server_Backup in the example mentioned above.

If the server is integrated with ACS, you may get a question 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 far more easier 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.

5. Restart the daemon manager

5. Wait until “pdshow” lists all the processes running. This will imply that the Daemon manager has completely started.

6. Rediscover all the devices. Go to Devices -> View/Rediscover/Delete

Essentially this creates a baseline for the Standby server. The Standby server would have the complete device list and all the configurations that are identical to the Active.

This also means that Standby would poll the network in exactly the same way as the Active server. If you want to reduce the impact of polling on network bandwidth,

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,** select each group and editing the polling interval values.
3. Go to **Notifications > Notification Criteria**. Select all notification criteria and Select "Suspend"
4. Go to **Diagnostics > Synthetic Tests**. For each test select the "Stop" button. This will stop the Synthetic tests.
5. Go to **Diagnostics > Phone Status Tests**. You will see a list of configured tests. For each test, click on "Edit" and make the schedule to run between "00:00" to "00:00". This essentially stops the test.

6. Suspend monitoring of SRST routers used in SRST tests: Go to **Administration > SRST Poll Settings > SRST Operations**. You will see a list of SRST tests configured. Note down all the target routers. Go to **Devices > Device Management.** You will see the overview of all managed devices. Click on "Monitored Devices". Click on the SRST router IP address in this report, Detailed Device View is launched. In this UI, suspend the device. This will automatically stop the SRST tests.

7.3.4 Continuous data sync up

Once the Active and Standby are in operation, any changes thereon to the Active server need to be propagated to the Standby. Different kinds of data that can change and recommendation for replication are listed below

7.3.4.1 Device List

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

a) Central LMS server as the source of device list for both Primary and Backup. In this case, LMS server acts as a Master repository of devices which pushes any additions or deletions to the device list to the two slaves – Active and the Standby server.

b) Active server as the source of the device list for 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 of the cases, the main idea is setting up the master slave configuration in DCR. The steps are explained below taking the example of Active as the Master DCR and Slave as the Standby DCR.

In the Active Server:

1. Select **Common Services > Server > Security.** The Security Settings page appears.
2. Click **Peer Server Account Setup** in the TOC. The Peer Server Account Setup page appears displaying the list of current users configured.

- To add users, click **Add** in the main window**.** A pop-up appears where you can add the details of the user. In this screen, enter "admin" as the user name and the password of the Standby server.

Now, Go to **Common Services > Server > Multi Server Trust Management > Peer Server certificate.** Import the "Standby" server certificate.

Go to **Common Services > Device and Credentials > Admin > Mode Settings.** Change the mode to "Master"

In the Standby Server:

Go to **Common Services > Server > Multi Server Trust Management > Peer Server certificate. .** Import the "Active" server certificate

Go to **Common Services > Device and Credentials > Admin > Mode Settings.** Change the mode to "Slave", and provide the Master address. Make sure the Master address provided here is identical to the host name 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.

7.3.4.2 User information

It is recommended the Active and Standby is configured to operate in ACS mode. In this mode, all the user and role setup is done on the ACS server, so, the user information is not local to the Active server. Any changes to user information happen centrally and there by automatically propagating to the Active and Standby servers.

7.3.4.3 Other configurations

Any other changes to the configuration to the Active server need to be also done on the Standby server. This includes any new diagnostic tests since the baseline was created, and changes to notification profiles.

If the amount of changes is more, then it is advisable to backup and restore the data so that manually changing the configuration is totally avoided.

7.3.4.4 Failover

Failure of the primary 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. Here are the lists of processes which need to be running for fully functional OM 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
PIFServer	SRSTServer
QoVMServer	STServer
SIRServer	DfmBroker
DfmServer	VHMServer
CmfDbEngine	CmfDbMonitor
DCRServer	CMFOGSServer
ITMOGSServer	GPF
NOTSServer	PTMServer
TopoServer	VsmServer
Jrm	

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

In case the Active server goes down, the standby can be made operational by doing the following

- Using the polling parameters UI, on the standby server, switch over to the default polling interval of 4 minutes.
- Activate Synthetic tests. You can "Start" the tests that are stopped.
- Shift back to the original schedule for Phone Status tests.
- "Resume" the Notification Criteria.
- Verify that you are able to monitor the status of the network and the validity and execution of diagnostic tests and the notification profiles.
- Create a backup of the configuration of the 'newly activated' server
- Decommission the previously active server

7.3.5 Setting up passive redundant server

In some deployments, instead of having Backup server actively polling the network, administrators prefer to have a backup server configured but not online. Using the concepts illustrated earlier in this paper, you can achieve this quite easily.

- Configure a Primary server
- Setup periodic backups on the primary.
- Install a backup server. 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 Primary, restore from the latest backup (or which ever you desire).
- Bring up the Backup server by executing "net start crmdmgtd"
- Wait until all the processes come up.
- Redo any changes to the configuration since the last backup.
- Now, your backup server is ready to be used.

7.4 Operations Manager for MSP Environments

You will need to ensure that you do not have duplicate IP addresses across different network domains that you are trying to manage with the same Operations Manager. If overlapping IP address ranges exist, you will need to dedicate different Operations Manager servers to manage these domains.

7.4.1 ACS Integration for Securing Access to Devices

7.4.1.1 Integrating Operations Manager with the ACS Server

Introduction

CiscoSecure Access Control Server (ACS) provides authentication, authorization, and accounting (AAA) services to network devices that function as AAA clients, such as a network access server, PIXFirewall, or router.

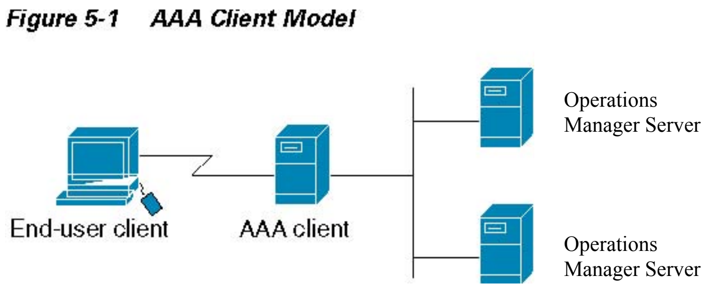


Figure 5-1 AAA Client Model
End-user client
AAA client
Operations Manager Server
Operations Manager Server

Figure 7.1: Cisco Secure Access Control Server

Why Do We Need an ACS?

Operations Manager is integrated with the 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 the ACS server.

Integrating with the ACS Server

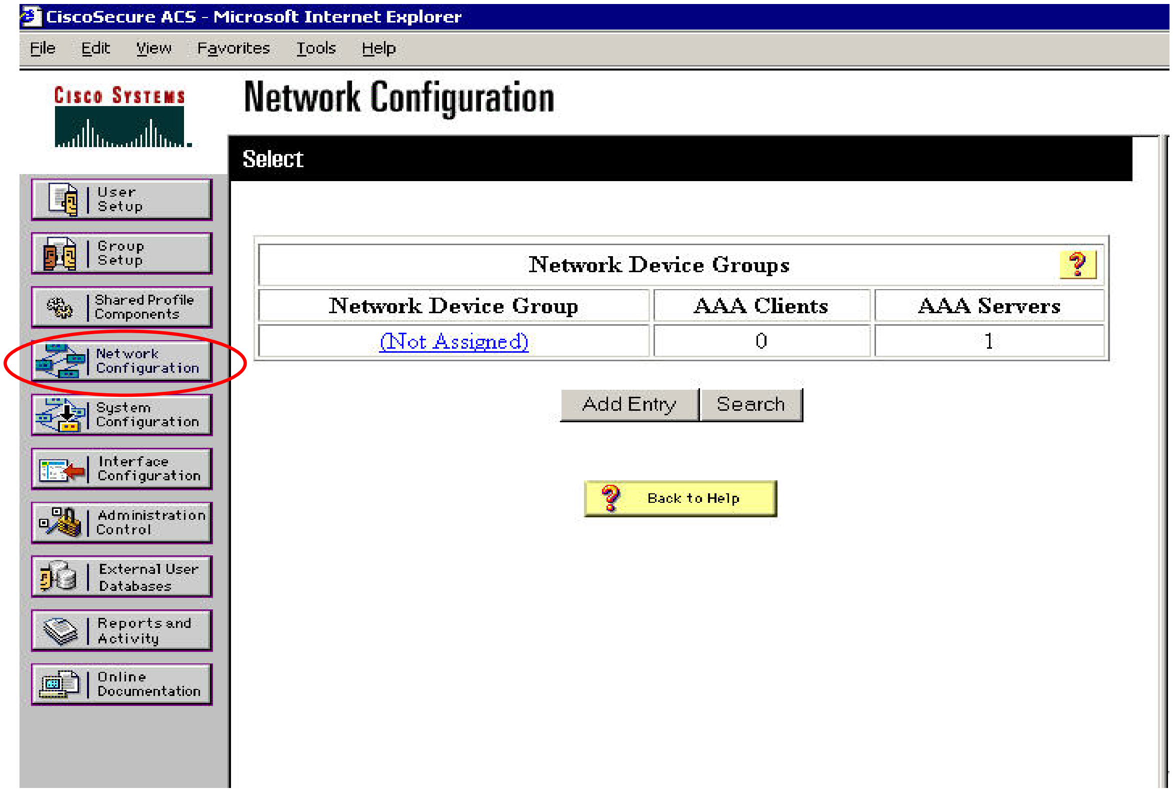
In ACS, network device groups are collections of AAA clients and AAA servers. You can assign AAA clients and AAA servers to the network device groups. For the Network Device Groups table to be displayed in the ACS server, the Network Device Groups option must be enabled.

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**.

To integrate with the ACS server, do the following:

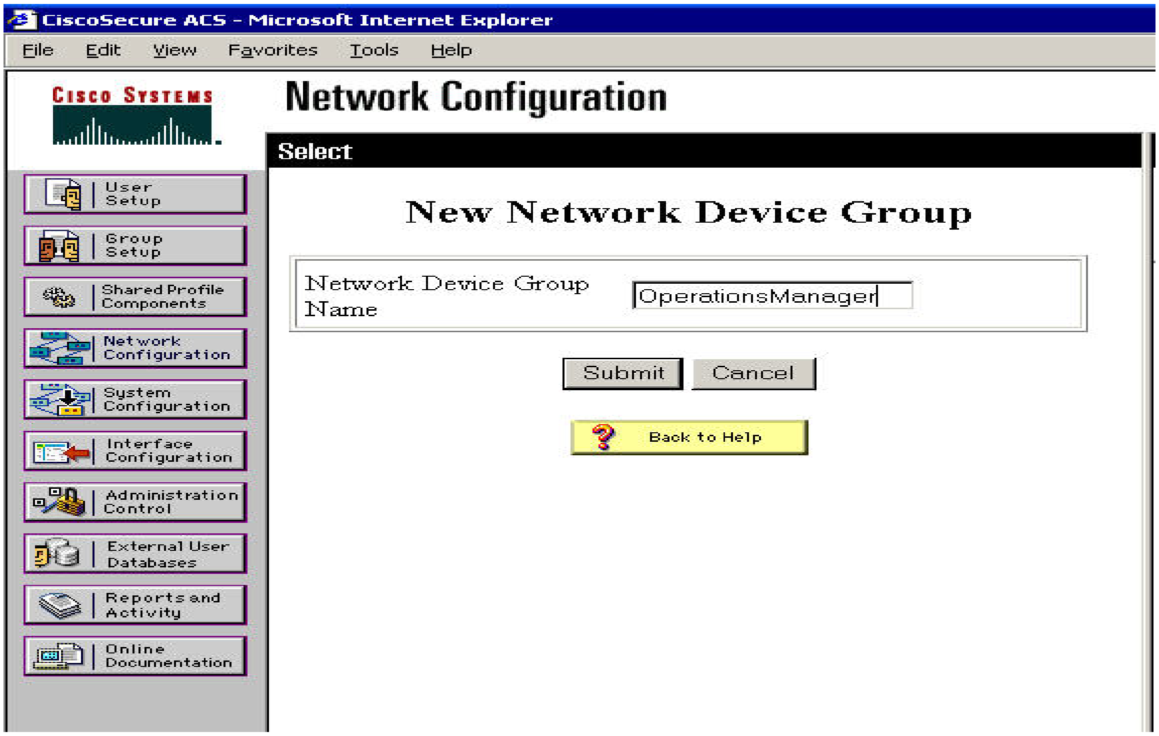
Step 1 From the Cisco Secure ACS login window, log in to the ACS server.
Step 2 From the ACS navigation menu, select **Network Configuration** (see Figure 7.2).



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

Figure 7.2: Network Configuration

Step 3 Under the Network Device Groups table, click **Add Entry**. Enter the network device group name (for example, OperationsManager).



Network Configuration

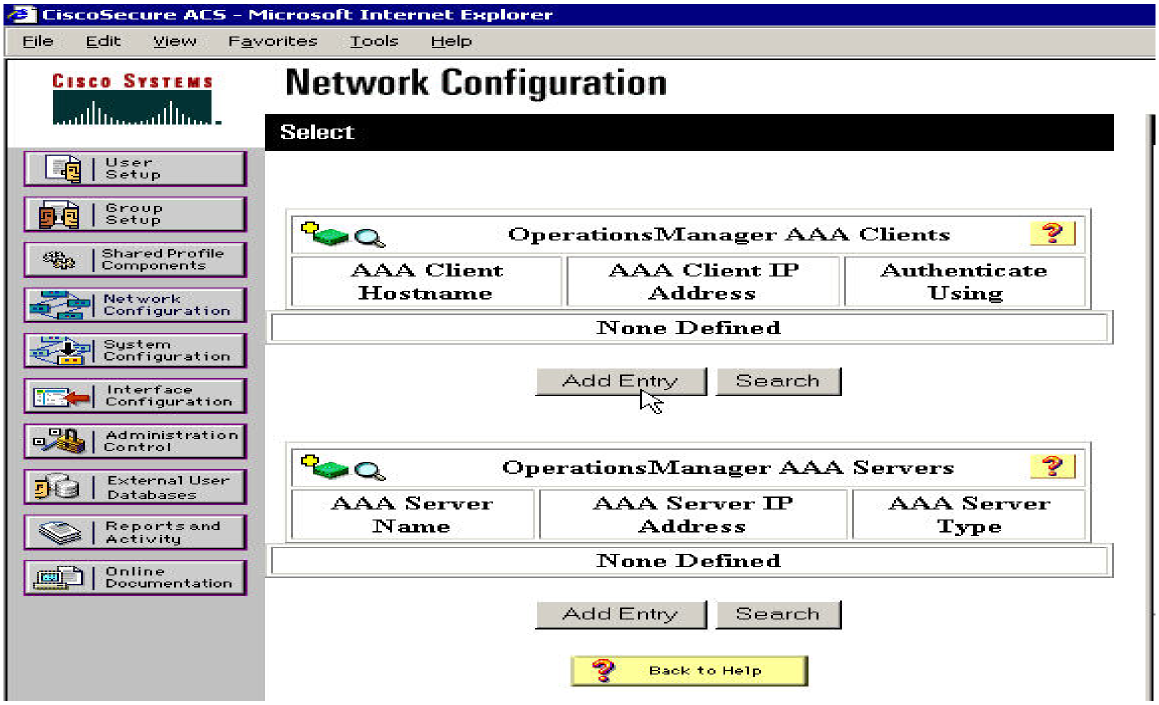
Select

New Network Device Group

Network Device Group Name: OperationsManager

Figure 7.3: Network Device Group

Step 4 Under the Operations Manager AAA Clients table, click **Add Entry**.



Network Configuration

Select

OperationsManager AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		

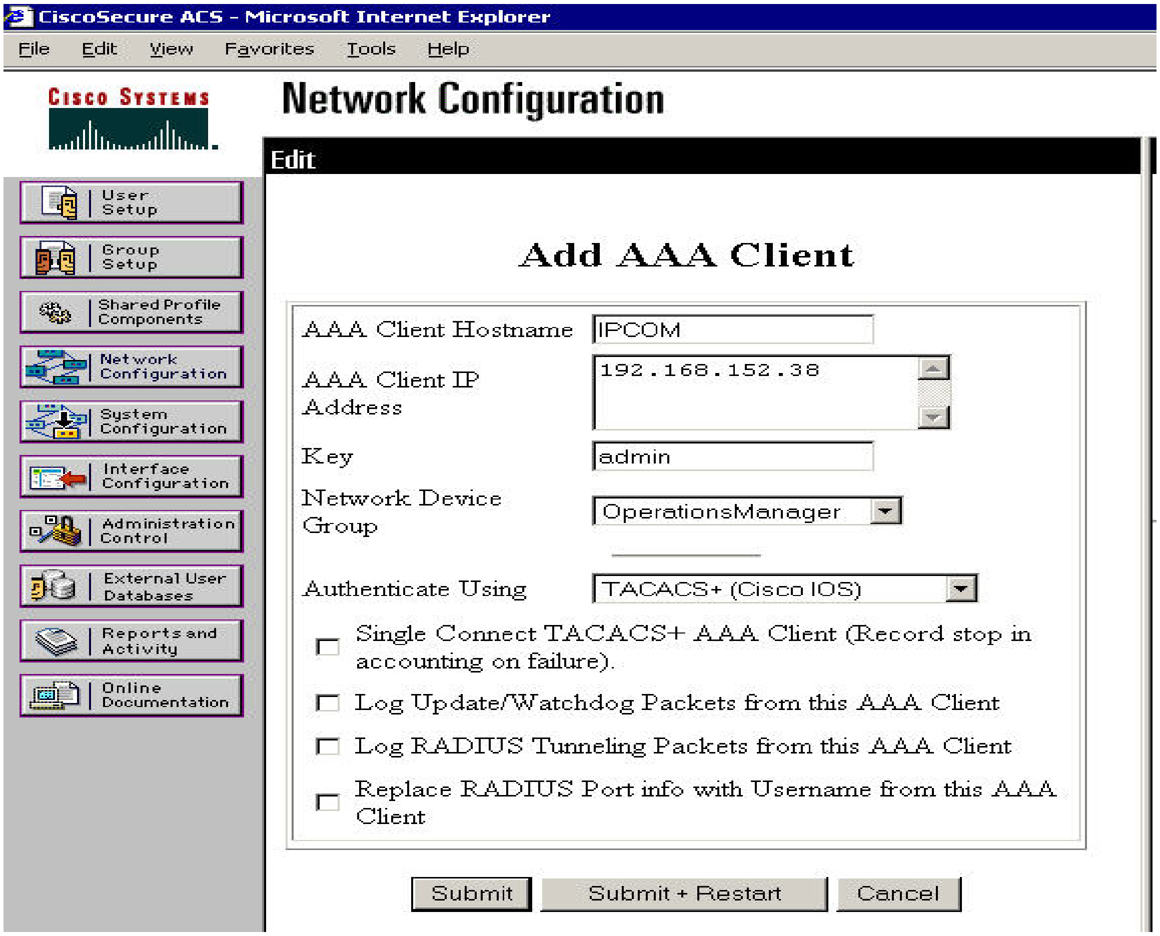
OperationsManager AAA Servers

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

Figure 7.4: Operation Manager AAA Clients

Step 5 In the Add AAA Client dialog box, 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 the ACS server.



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

Figure 7.5: Add AAA Client

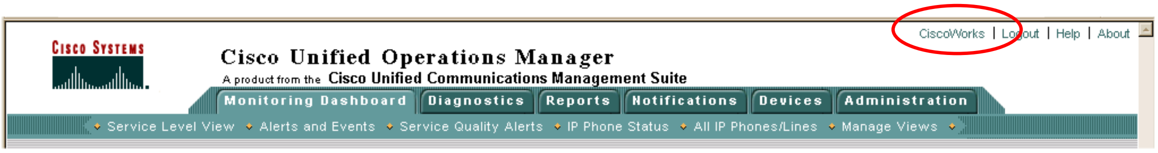
Step 6 Click **Submit+Restart**.

Setting Up the Operations Manager Server

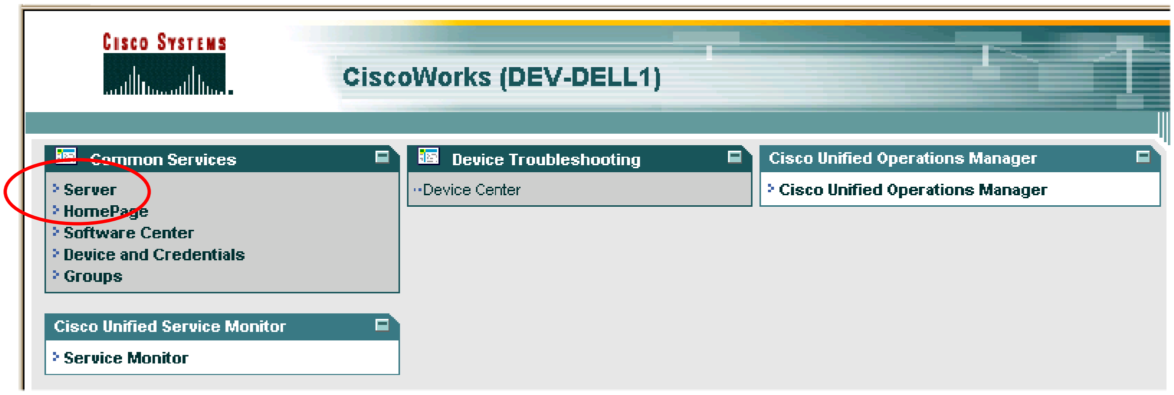
Step 1 Log in to the Operations Manager server.

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

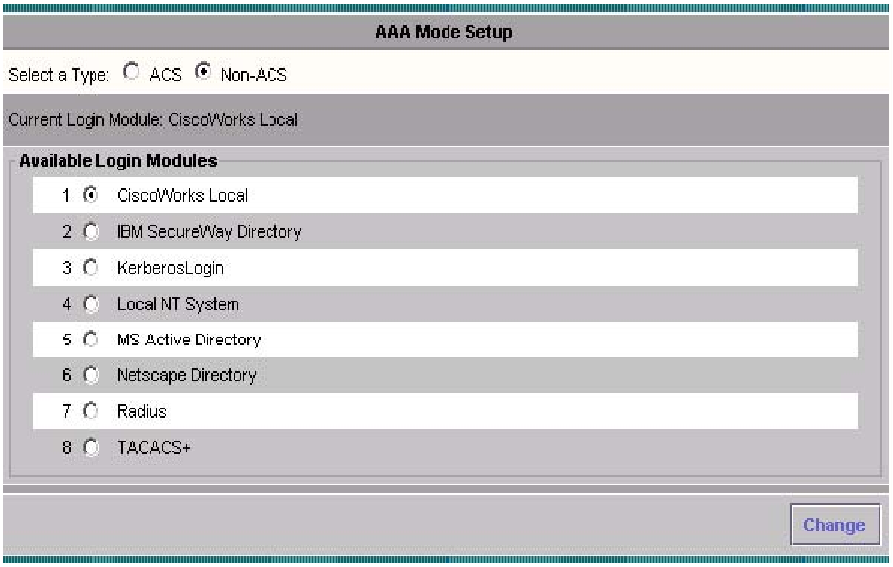
a. Click the **CiscoWorks** link in the top-right corner of the Operations Manager home page.



b. In the Common Service pane, select **Server** > **Security**.



Step 3 From the TOC, select **AAA Mode Setup**. The AAA Mode Setup dialog box appears.



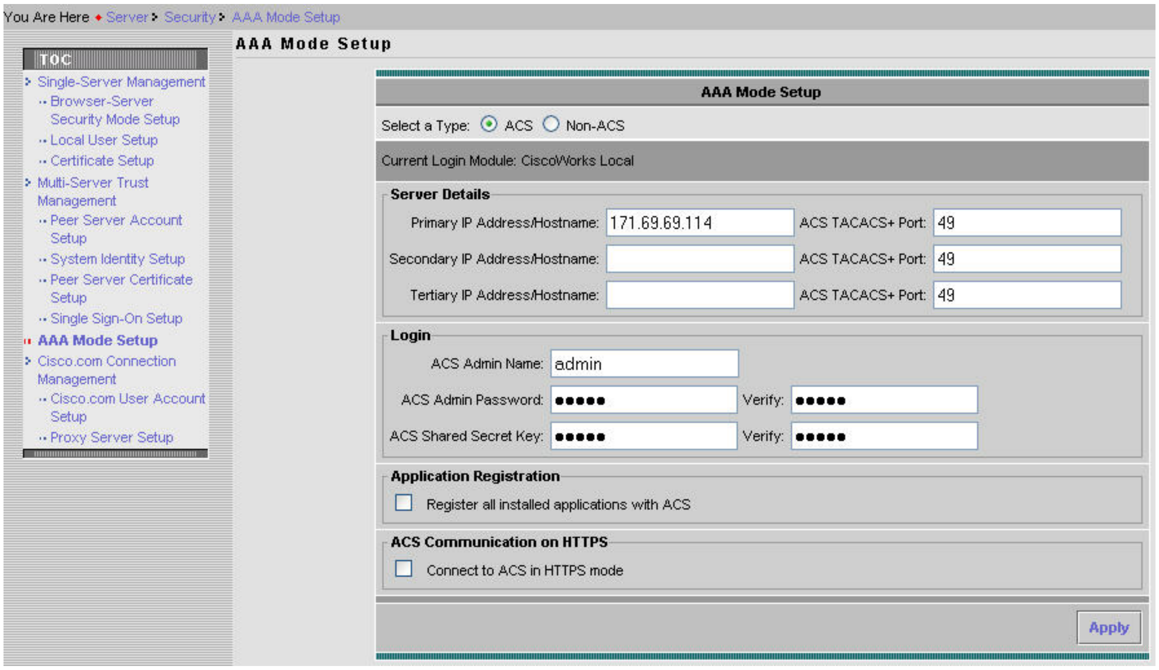
Select a Type: ○ ACS ● Non-ACS

Current Login Module: CiscoWorks Local

Available Login Modules

1 ● CiscoWorks Local
2 ○ IBM SecureWay Directory
3 ○ KerberosLogin
4 ○ Local NT System
5 ○ MS Active Directory
6 ○ Netscape Directory
7 ○ Radius
8 ○ TACACS+

Step 4 Select ACS.


You Are Here • Server > Security > AAA Mode Setup
AAA Mode Setup
TOC
Single-Server Management
Browser-Server Security Mode Setup
Local User Setup
Certificate Setup
Multi-Server Trust Management
Peer Server Account Setup
System Identity Setup
Peer Server Certificate Setup
Single Sign-On Setup
AAA Mode Setup
Cisco.com Connection Management
Cisco.com User Account Setup
Proxy Server Setup
AAA Mode Setup
Apply

Select a Type: ● ACS ○ Non-ACS

Current Login Module: CiscoWorks Local

Server Details

Primary IP Address/Hostname:	171.69.69.114	ACS TACACS+ Port:	49
Secondary IP Address/Hostname:		ACS TACACS+ Port:	49
Tertiary IP Address/Hostname:		ACS TACACS+ Port:	49

Login

ACS Admin Name:	admin		
ACS Admin Password:	●●●●●	Verify:	●●●●●
ACS Shared Secret Key:	●●●●●	Verify:	●●●●●

Application Registration

□ Register all installed applications with ACS

ACS Communication on HTTPS

□ Connect to ACS in HTTPS mode

Step 5 Enter all the ACS server details (including the key value provided in Step 5c of the "Integrating with the ACS Server" section).

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

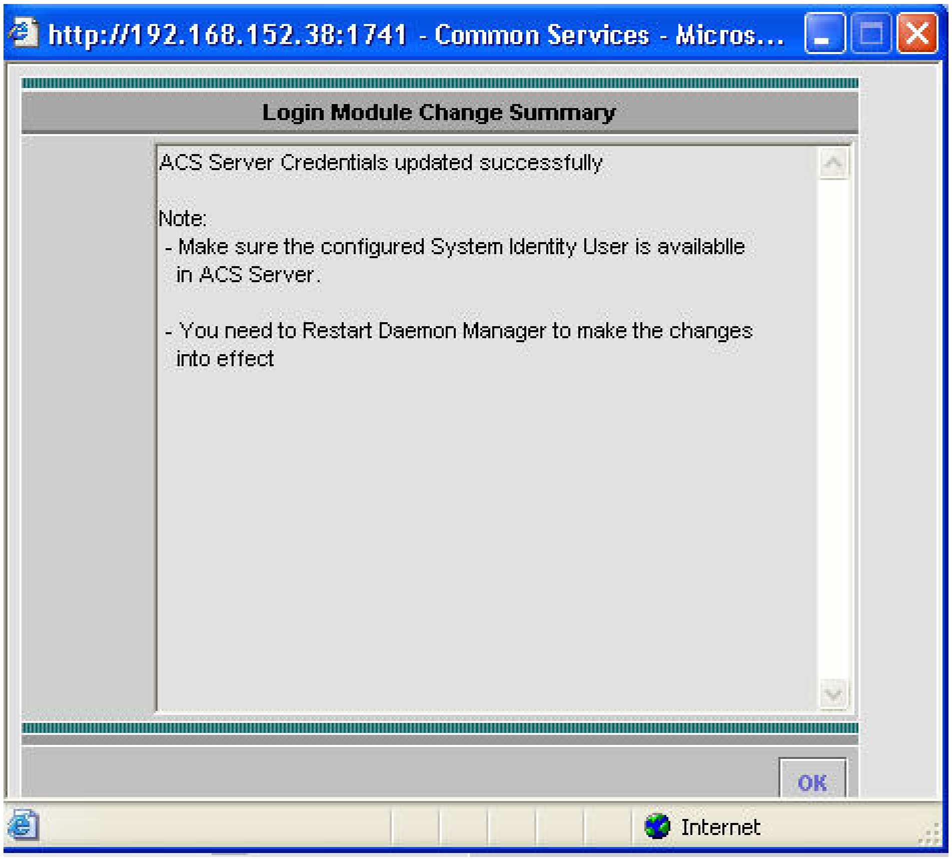
- The values true and false are not acceptable in the Primary, Secondary, and Tertiary IP Address/Hostname fields.

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**.

The following summary screen appears:


http://192.168.152.38:1741 - Common Services - Micros...
Login Module Change Summary
OK
Internet

ACS Server Credentials updated successfully

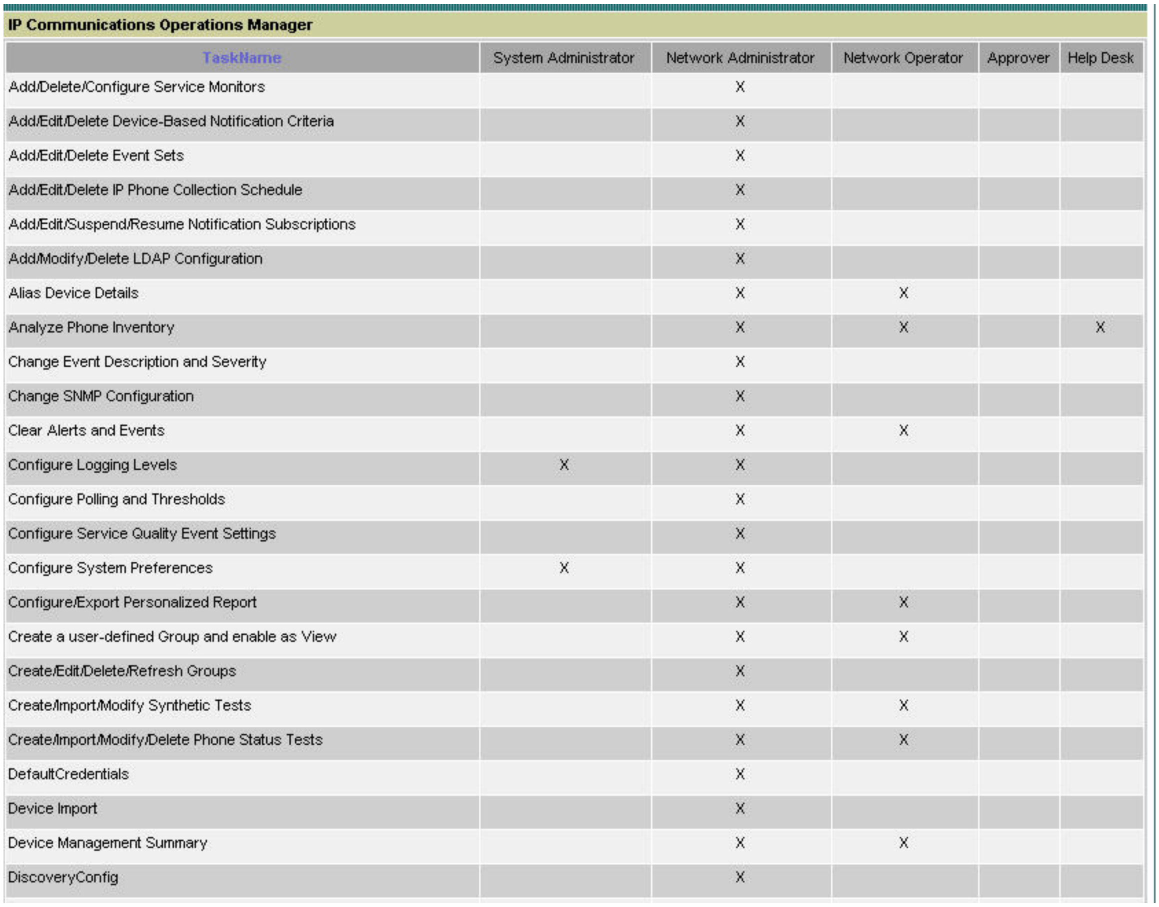
Note:
- Make sure the configured System Identity User is availablle in ACS Server.
- You need to Restart Daemon Manager to make the changes into effect

When you click Apply, the following actions occur:

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

You can access the default mapping in the Operations Manager server by navigating to **Common Services panel > Server > Reports > Permission Report**.



IP Communications Operations Manager

TaskName	System Administrator	Network Administrator	Network Operator	Approver	Help Desk
Add/Delete/Configure Service Monitors		X			
Add/Edit/Delete Device-Based Notification Criteria		X			
Add/Edit/Delete Event Sets		X			
Add/Edit/Delete IP Phone Collection Schedule		X			
Add/Edit/Suspend/Resume Notification Subscriptions		X			
Add/Modify/Delete LDAP Configuration		X			
Alias Device Details		X	X		
Analyze Phone Inventory		X	X		X
Change Event Description and Severity		X			
Change SNMP Configuration		X			
Clear Alerts and Events		X	X		
Configure Logging Levels	X	X			
Configure Polling and Thresholds		X			
Configure Service Quality Event Settings		X			
Configure System Preferences	X	X			
Configure/Export Personalized Report		X	X		
Create a user-defined Group and enable as View		X	X		
Create/Edit/Delete/Refresh Groups		X			
Create/Import/Modify Synthetic Tests		X	X		
Create/Import/Modify/Delete Phone Status Tests		X	X		
DefaultCredentials		X			
Device Import		X			
Device Management Summary		X	X		
DiscoveryConfig		X			

The default mapping between tasks and the roles can be changed in the ACS server, 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`**

Enter **`net start 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 enables 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 into 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 on which can view and act. The same is applicable to Frank as well, where he 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 the ACS server.
Step 2 Click **User Setup**.
Step 3 Enter a username (in this example, Joe), then click **Add/Edit** (see Figure 7.12).

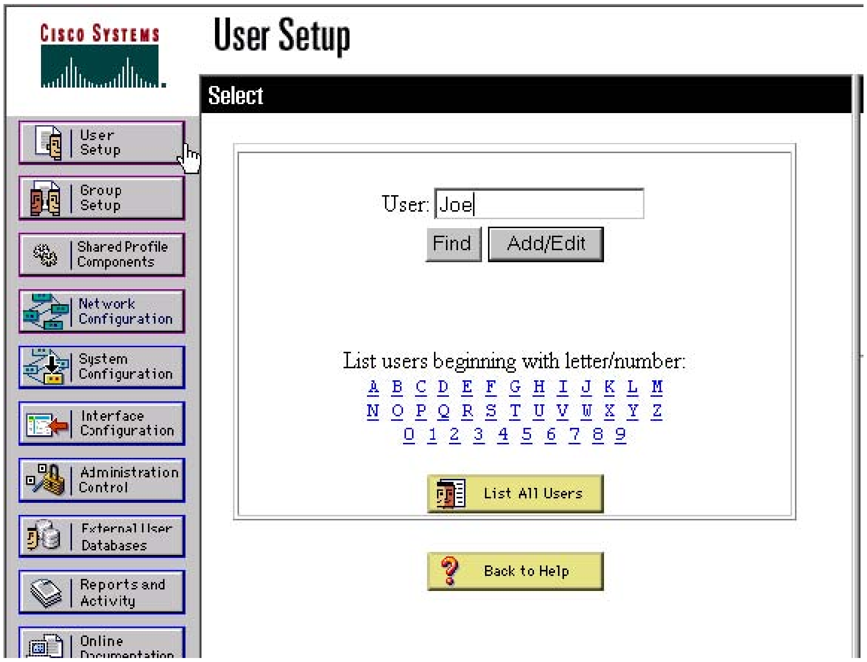
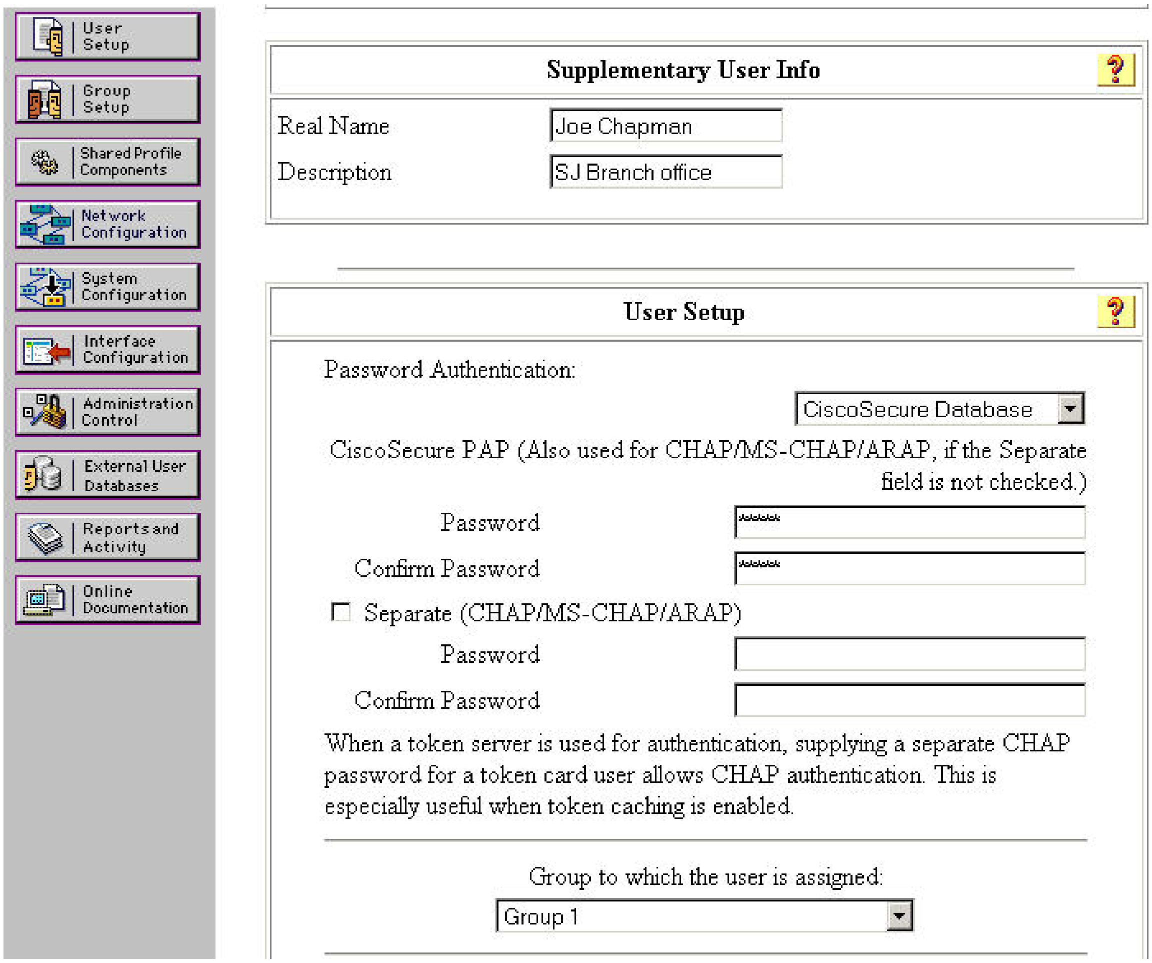


Figure 7.12: ACS User Setup

Step 4 Assign a password for the user *Joe*.
Step 5 Assign Joe to the group named *Group1*, then click **Submit**.



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

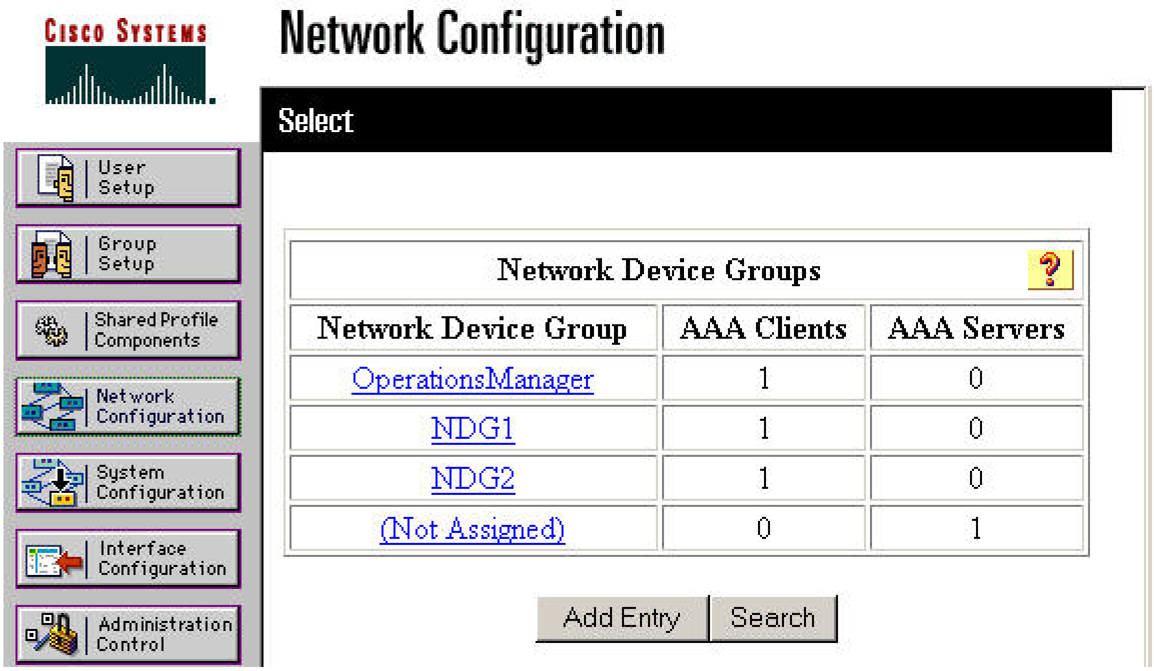
Figure 7.13: User Info

Step 6 Similarly, create a user called Frank and assign him 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.



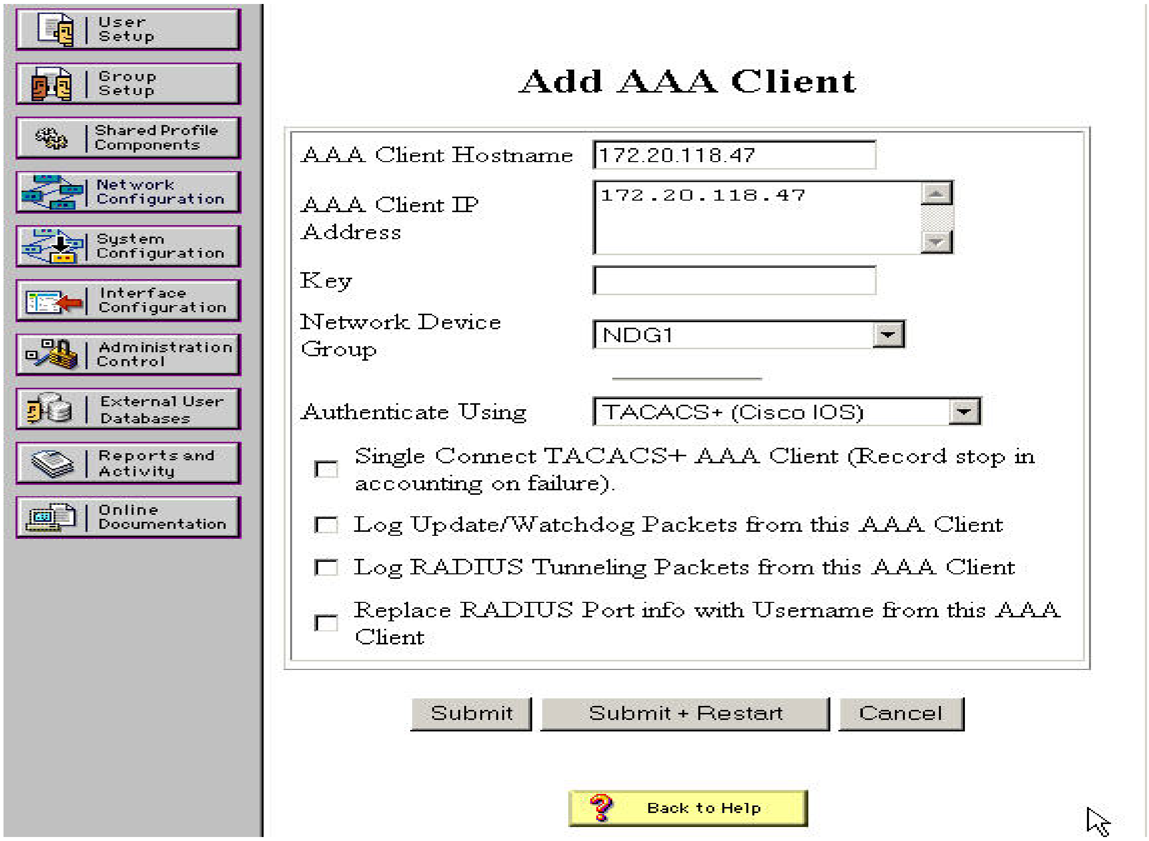
Network Configuration

Select

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

Figure 7.14: Add Entry

d. Click the NDG2 link, and in the Add AAA Client dialog box, add a device D1 with IP address 172.20.118.47.



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

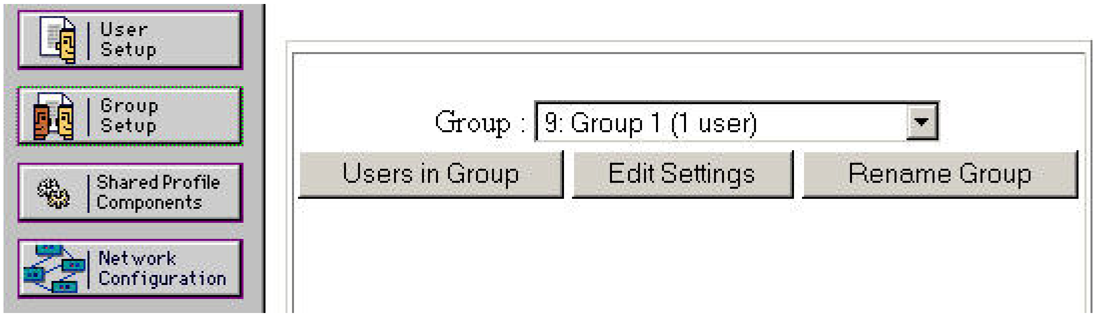
Figure 7.15: Add AAA Client

e. 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**.

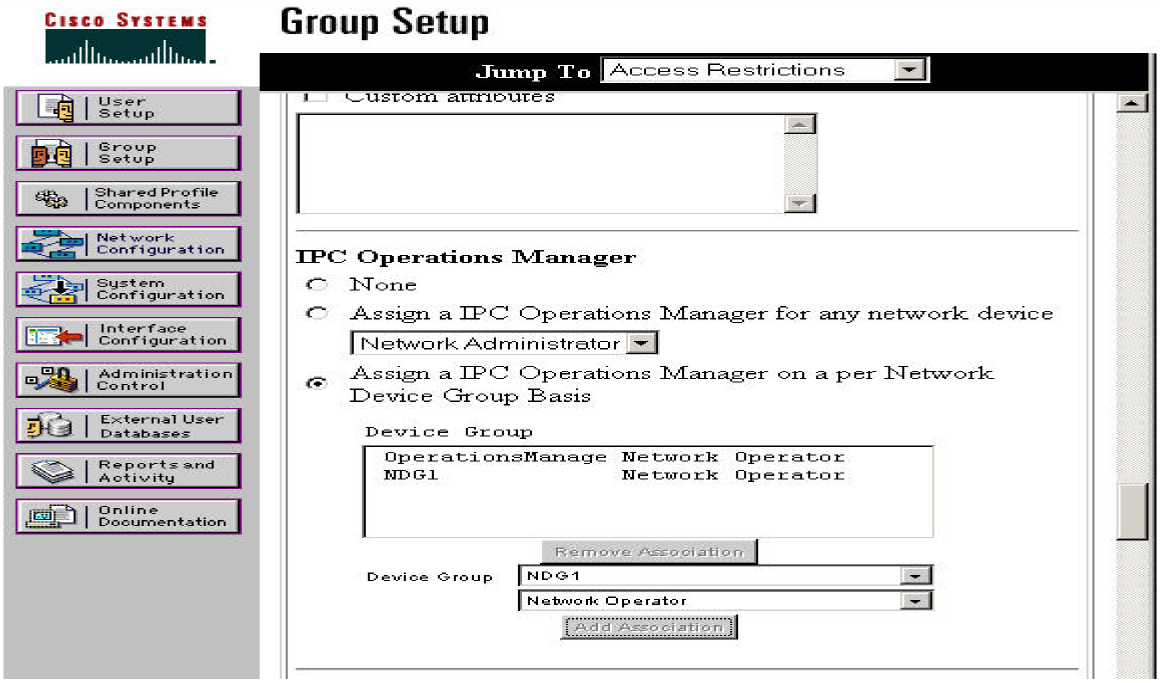
b. Select the group to which the user Joe belongs, then click **Edit Settings**.



Group : 9: Group 1 (1 user)

Figure 7.16: Group Setup

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



Jump To: Access Restrictions

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

Figure 7.17: Group Setup Information

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

Step 10 In the same way, 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.

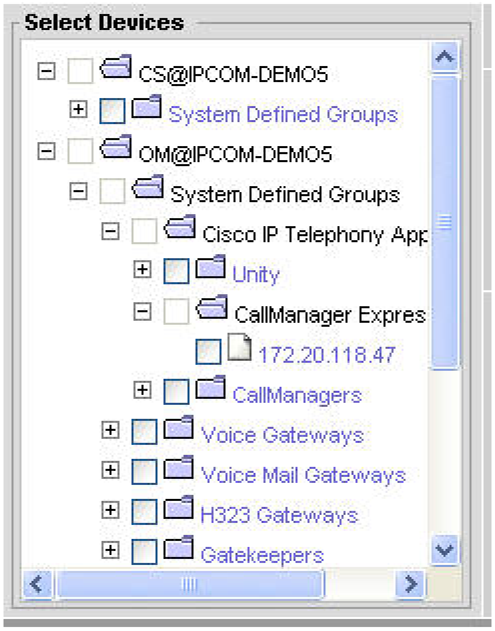
Assume that both Joe and Frank access the Config Editor screen.

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 as follows.



Joe sees only device 172.20.118.47 in the group, and Frank’s login enables him to see only device 172.20.118.48.

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 enable the user to operate in the Network Device Group should be given to this role.

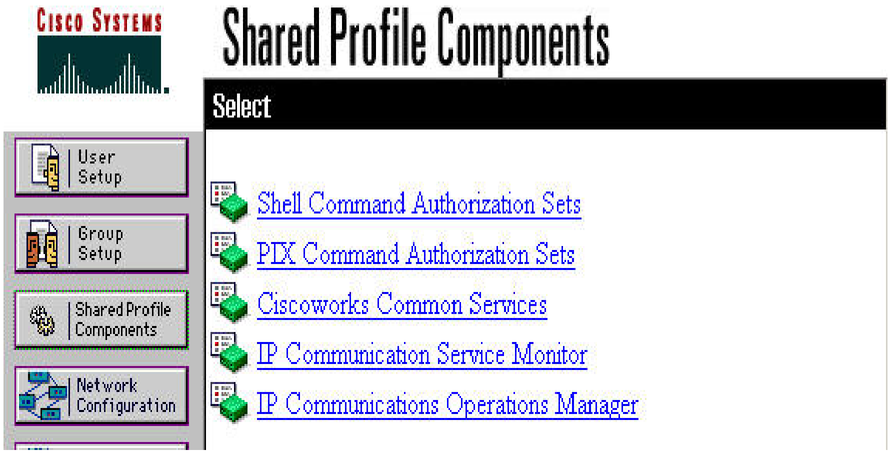
For example, if a user needs both Approver and Network Operator privileges to operate on NDG1, you can create a new role with Network Operator and Approver privileges, and assign the role to the user, so that the user can operate on NDG1.

How to Create a New Role in ACS

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

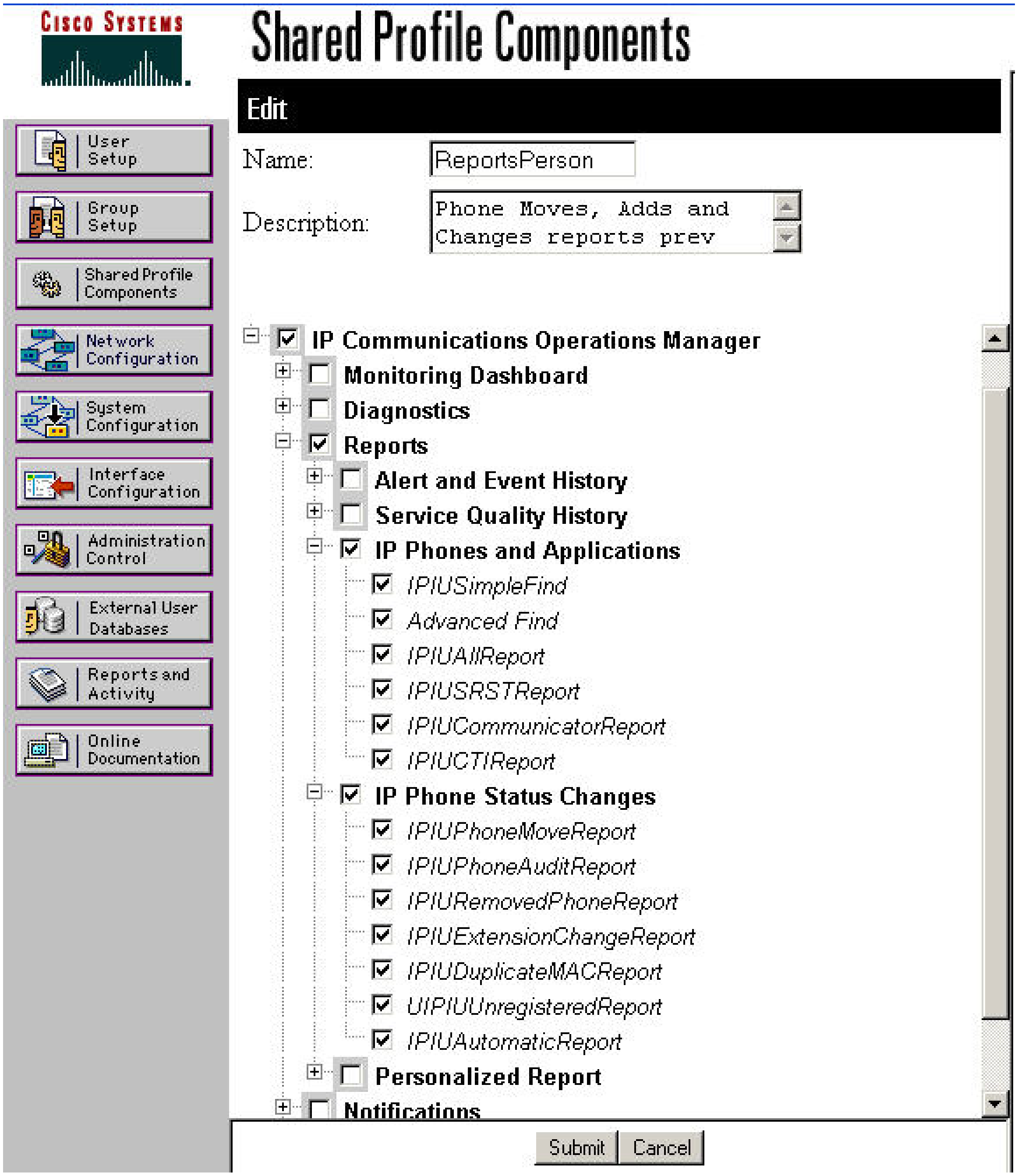
Step 1 Log in to the ACS server.

Step 2 Click **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 following dialog box appears.



Shared Profile Components

Edit

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

Step 5 Enter a new role name and description. select a list of tasks that users with this role can perform.

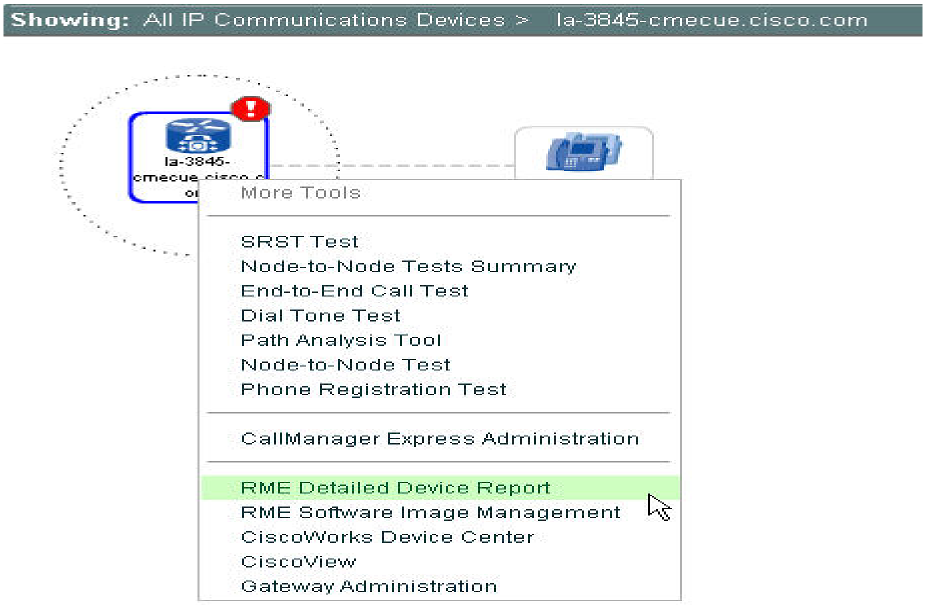
Step 6 When you are satisfied with your settings, click **Submit**.

7.5 LMS Integration

Operations Manager integrates with the following CiscoWorks applications:

- Device Credential Synchronization (see section 5.3, "Network Discovery and Device Management")
- CiscoWorks Resource Manager Essential (RME)
- CiscoWorks Campus Manager (Campus)
- CiscoView

To integrate RME, Campus, or CiscoView with Operations Manager, you must configure the other CiscoWorks applications server's IP address or DNS names in Operations Manager (Administration > Preferences). Make sure that the devices monitored by Operations Manager are also managed in the other CiscoWorks applications that are referenced. Once the integration is complete, a context-sensitive launch point is provide to the appropriate tools from the Service Level View.



7.6 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 ten 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 score is calculated, the MOS score is diluted.

Span as close to the phone switch port as possible for the Cisco 1040 to calculate an accurate MOS.

Configuring the Catalyst Switched Port Analyzer (SPAN) feature:

http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a008015c612.shtml

Configuring Windows 2000 DHCP Server for Cisco CallManager:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00800942f4.shtml

Using One DHCP Server for voice and data networks:

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.

Usually, one of the reasons why the trap may not get forwarded is because of third party SNMP tools installed on the OM server. If you have any SNMP tools installed on the OM server, check to see if the “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 get redirected to this service and OM does not get a copy of the trap and hence OM is not able to process the voice quality trap.

7.6.1 Determine a Quality of Voice Baseline for Your Network

In Service Monitor > Setup, enable call metrics archiving. This archives the MOS parameters for every call. Files are stored in a directory specified during installation. View the MOS values in these archived files and determine the quality of voice (QoV) baseline for your network; that is, the typical MOS value that you are experiencing. Configure the Service Monitor MOS threshold to a value just below your typical value. The Service Monitor MOS threshold will generate a trap when the MOS value falls below this number. For example, a very good MOS score is in the low 4 range. If you typically see a MOS of 4.2 in the archives, then set the MOS threshold to 3.9, for example. You do not need to generate a trap and be alerted for every call, only for the calls that are experiencing poor quality.

Instead of using the archived files, you can use the Operations Manager GUI (when Operations Manager and Service Monitor are co-resident), to assist in determining your QoV baseline. In Service Monitor, configure the Service Monitor MOS threshold to 4.5 (for a short period of time) to determine a QoV baseline for your network. This will generate a QoV trap for every call. Monitor the MOS and determine the typical QoV MOS for your network. Then change the Service Monitor MOS to a lower permanent value based upon your determined baseline.

Instead of using the archived files, you can use the Operations Manager GUI to assist in determining your QoV baseline. You can do this provided that you have configured Service Monitor to send traps to Operations Manager and that you have added Service Monitor to Operations Manager. To determine the QoV baseline:

1. In Service Monitor, configure the Service Monitor MOS threshold to 4.5. As a result, Service Monitor will generate a trap for every call, and Operations Manager will generate alerts.
2. In Operations Manager, launch the Service Quality Alerts display; monitor the MOS and determine the typical QoV baseline MOS for your network.
3. In Service Monitor, configure the MOS threshold to a lower permanent value based upon your determined baseline.
4. In Operations Manager, verify that the MOS threshold for Critical Service Quality Issues (in Service Quality Event Settings) is set lower than the MOS threshold in Service Monitor.

7.6.2 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.

We have to 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, but also the CPU falls short in serving the different processes. The MOS value reported by the sensor gets 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.

7.6.3 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 the same way as with 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 aggregate switch, and the number of RTP streams is below 80, then one sensor per switch would be overkill. This is where RSPAN (Remote Switched Port Analyzer) 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.

7.6.4 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 can be none other than 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.

7.7 Identifying CPU-Intensive Operations

Use the **tasklist** command now available in Windows 2003. Performing the command `tasklist /v /fo CSV > somefile.csv` produces information about processes, memory, etc. This information can be loaded into an Excel spreadsheet.

7.7.1 Boot Up

It takes several minutes for the Operations Manager server to fully restart after a server reboot. The complete boot-up sequence can be traced by going to **Programs > Administrative Tools > Event Viewer** and then double-clicking on the **System** folder.

In the right pane, in the Event column, look for events with the ID 6009 followed by (in time sequence) a 6005. This sequence tells you that the system was restarted. These two events log the fact that the Windows event log was started up, followed by the Windows Release version, and so on.

From this point on in the event log, you can trace the time sequence of when the various system services (such as DCOM, IpSec, TCPIP, telephony, CiscoWorks daemons, Tomcat, Apache, VisiBroker, DbEngines, and so on) were started.

If the Operations Manager system does not seem to be working properly, it could be due to an improper shutdown, perhaps caused by an expected loss of power. Properly shut down and reboot the server before calling the Cisco TAC. A reboot clears up most of these problems.

7.7.2 Device Management Operations

The following script can be used from the Operations Manager Windows command prompt to completely delete the Operations Manager database and clean all devices out of the system.

```
cd C:\Program Files\CSCOpx\objects\vhm\utilities
perl "C:\Program Files\CSCOpx\objects\vhm\utilities\dbclean.pl"
YES
cisco
y
y
y
y
y
net start crmdmgtd
```

7.7.3 High Event Throughput Conditions

In high CPU conditions such as rediscovery, the dashboards can stop refreshing. This can cause the screen to go blank, or it can bring up a browser message stating that a DNS error has occurred. Press F5 and see if the screen refreshes.

If there is a high rate of incoming events on a particular set of devices or destinations and the corresponding alert never gets a chance to go into the Cleared state, high memory consumption can occur. This eventually leads to a build-up of events in the events database, causing systematic degradation and eventual failure of critical services within the Operations Manager server. To avoid this situation, you should manually clear long-lived alerts from the system on a periodic basis.

If this situation occurs, new events will not be shown in the Service Level View, the Service Quality Alert display, or the Alerts and Events display.

To clean the database, do the following:

1. From the command prompt, stop the daemon manager (`net stop crmdmgtd`).
2. Go to the directory <Operations Manager install folder>/CSCOpx/bin on the command line.
3. Execute the command `perl dbRestoreOrig.pl dsn=itemEpm dmprefix=EPM`.
4. Start the Daemon manager (`net start crmdmgtd`).

Alternatively, the dbclean utility mentioned in the Operations Manager FAQ takes care of cleaning all of the Operations Manager databases. It prompts you for each database before cleaning. You should be careful to choose yes only for itemEpm to clean the EPM database.

To clean up data in the system, do the following:

1. Open a command prompt.
2. Run `perl dbclean.pl under \<NMSROOT>\objects\vhm\utilities\`.

For example:

```
C:\Program Files\CSCOpx\objects\vhm\utilities>perl dbclean.pl
```

The following is displayed:

```
dbclean Database cleanup utility.
Copyright (c) 2003 Cisco Systems Inc.
*************************** W A R N I N G ***************************
Running this utility will remove data inside ALL the databases in the
IP Telephony Monitor Application
Type YES if you still want to continue :(type YES)
The CW2000 Daemon Manager service is stopping........................
The CW2000 Daemon Manager service was stopped successfully.
Removing data from databases...StandardDbRegistration .
ama Database initialization is completed.
StandardDbRegistration .
itemInv Database initialization is completed.
StandardDbRegistration .
itemFh Database initialization is completed.
StandardDbRegistration .
itemEpm Database initialization is completed.
StandardDbRegistration .
cmf Database initialization is completed.
```

```
Done.
Now removing repository files...Done.
dbclean utility was run successfully.
The CW2000 Daemon Manager service is starting.
The CW2000 Daemon Manager service was started successfully.
```

Wait several minutes until all daemon processes are up and running.

Do not set the MOS threshold in Service Monitor very high for long periods of time. Internal tests indicate that a high sustained rate of Service Quality Alerts can cause frequent periods of high CPU usage on the Operations Manager server. During these periods of high CPU activity, dashboards and other user interfaces may not respond in a timely manner. The only way to reduce the load on the system in these circumstances is to either lower the MOS thresholds to reduce the rate of Service Quality events being handled by Operations Manager, or reduce the overall load on the system by reducing the number of configured diagnostic tests.

The periodic rediscovery of the entire network (the default is once weekly) is a very CPU-intensive activity, and should preferably be confined to off-peak hours (such as in the middle of the weekend). It is recommended that no users be logged into the system during this period, and if at all possible, dashboards should be closed and diagnostic tests suspended during this interval.

7.7.4 Simultaneous Operations by Multiple Users

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

8 Troubleshooting Tips

See the following sections:

- Section 8.1, Troubleshooting Notes
- Section 8.2, Common Issues
- Section 8.3, Frequently Asked Questions

8.1 Troubleshooting Notes

- Do not place the Operations Manager server on a network restricting SNMP. Check your SNMP access lists and make sure to enter the Operations Manager server. Operations Manager requires SNMP v2 write community strings only to configure the IP SLA for the node-to-node tests.
- Do not place the Cisco 1040 on a network where DHCP is being monitored and restricted. The MAC address of the Cisco 1040 may need to be entered into a DHCP management system application for the Cisco 1040 DHCP to work. Check the switch port configuration of the port that the Cisco 1040 is plugged into.
- The Cisco 1040 currently does not support CDP. Thus, make sure the Cisco 1040 is on a single VLAN; do not use auxiliary VLANs.
- Make sure to open ports on your firewall to allow the Cisco 1040 to be placed on a demilitarized zone (DMZ).

8.2 Common Issues

Installation

1. **What should one check before installing Operations manager?**

A: Check the following before installing Operations Manager

- Make sure you have only one NIC card enabled on the box
- Critical: Check the time on the machine. If you change the time after CUOM installation you may need to reinstall the OS to get CUOM to work.
- Ensure the IP Address to Machine name mapping in DNS and host name of the local machine are the same
    1. In the command prompt run nslookup <ipaddress>. This should show you the hostname of the machine.
    2. Run ipconfig /all and check the hostname and domain name. This should be the same as what you obtained in nslookup
    3. Finally from the command prompt run ping <hostname> where hostname is the fully qualified name of the machine that you got from nslookup.

- If this is a reinstall Click on Start->Run and enter %temp% and delete all files in that folder.
- Ensure that SNMP has been enabled on machine where OM needs to be installed. If it is not enabled then
  1. Go to Control Panel->Add/Remove programs->Add/Remove Windows programs
  2. In the Dialog box look for Management and Monitoring Tools. Enable the check box corresponding to that item
  3. Click on details and ensure that Simple Network Management Provider is checked and enabled.

2. I get a message that one or more files may be locked while upgrading from OM 1.0 or reinstall. What should I do?

- Stop the installation immediately.
- Go to Control panel ->Administrative Tools->Services
- In the Window find the CW2000 Daemon Manager Service. Right click and choose Properties.
- In the dialog find Startup type and change it from "Automatic" to "Manual"
- Reboot the machine and start the upgrade

3. Installation/Unistall of OM failed midway? How do I clean up before trying the install again?

- Delete all files under <NMSROOT> where the product was installed/attempted to be installed
- Go to Start->Run and enter regedit
- Go to HKEY_LOCAL_MACHINE\SOFTWARE\Cisco.
- Delete the following keys
  - MDC
  - Resource Manager

Warning: Registry operations must be done carefully else it can cause unexpected side effects.

4. Why do I see a blank screen on logging into IPCOM 1.0 evaluation version?

A: This means that the license is invalid.

5. When CDP is not working properly, issues can arise on any Windows-based Cisco IP telephony application, such as Cisco CallManager or Cisco Emergency Responder, and so on.

The workaround that follows requires removal of a security patch issued by Microsoft. Cisco recommends that you use the given workaround only if you must use network management software that uses the CDP driver to discover Cisco Emergency Responder; for example, if you use Operations Manager to discover Cisco Emergency Responder servers.

Symptom:

Operations Manager may not be able to discover Cisco Emergency Responder servers. On servers that have Cisco Emergency Responder installed, rebooting causes the operating system to issue an error stating that a driver or service has failed.

The System Event log displays the following message:

```
The CDP Protocol Driver service failed to start due to the
following error:
The I/O operation has been aborted because of either a thread
exit or an application request.
```

Note: Cisco Emergency Responder functionality is not impacted; emergency calling is unaffected.

Conditions:

The problem occurs on Cisco Emergency Responder servers (version 1.2(3)sr2 and earlier) that have the Windows operating version upgraded to 2000.2.7sr3 or 2000.4.1.

The problem is caused by an incompatibility between the CDP driver installed by Cisco Emergency Responder and the Microsoft Security hotfix MS05-019. For more information regarding the hotfix, see:

http://www.microsoft.com/technet/security/bulletin/MS05-019.mspx

Workaround:

You can avoid the problem by uninstalling the software installed as part of MS05-019.

To uninstall the software, do either of the following procedures:

a. Go to **Control Panel** > **Add/Remove Programs**.

b. Scroll down to Windows 2000 Hotfix - KB893066.

c. Click **Change/Remove.**

d. You may be prompted that some other hotfixes may not work. Click **OK**.

e. Reboot the Cisco Emergency Responder server.

Or:

Update the CDP Driver on the Cisco Emergency Responder server:

1. Log in to any Cisco CallManager 4.1 server and copy the following files from Cisco CallManager to the Cisco Emergency Responder server in the c:\program files\cisco\bin folder:
   - CDP.SYS (C:\Program Files\Cisco\Bin)
   - CDPintf.dll (C:\WINNT\system32)
   - CDPInstaller.exe (C:\Program Files\Cisco\Bin)

   – CDP.inf (C:\Program Files\Cisco\Bin)

2. Uninstall the CDP drive from the Cisco Emergency Responder server by running the following command:

   ```
   C:\Program Files\Cisco\Bin> cdpinstaller -v -u CISCO_CDP
   ```

3. Install the new CDP driver by running the following command:

   ```
   C:\program files\Cisco\Bin:> cdpinstaller -v -l "C:\Program
   Files\Cisco\Bin\cdp.inf" -c p -i CISCO_CDP
   ```

4. Reboot the Cisco Emergency Responder server.

After rebooting, open the Alerts and Events display and confirm that the service failure message is not present.

Device management

6. Devices are getting stuck in "In Progress" or "Unreachable" state? How do we debug this?

- If all devices are going into Unreachable state then
  1. Open a command prompt
  2. Execute the command <NMSROOT>\CSCOpx\objects\smarts\bin\brcontrol
  3. The output should look like this

     ```
     C:\Documents and
     Settings\Administrator>c:\progra~1\CSCOpx\objects\sma
     rts\bin\brcontrol
     Broker is located at: ipcomtest-3:9002      Started: May 27
     09:25:34 2006
     Domain        Host Name       Port Proc ID State   Last
     Chg Time
     ------        ---------       ------ ------- -----   -------------
     PollingServer   ipcomtest-3      4345    6592 RUNNING
     May 27 09:27:56 2006
     VHM           ipcomtest-3      4355    6592 RUNNING
     May 27 09:28:02 2006
     DFM           ipcomtest-3      4838    6416 RUNNING May
     27 09:28:43 2006
     ```

  4. Check if you see entries for both DFM and VHM.
  5. If you see an entry for DFM and no entry for VHM then in the command prompt run pdexec VHMServer
  6. If you see no entries in the list it means both DFM and VHM are down. In the command prompt execute
     - pdexec DFMServer
     - pdexec VHMServer
  7. Execute the command mentioned in Step2

8. If you do not see the entries mentioned in step 4 then zip all the logs under <NMSROOT>\log\itemlogs and send it for analysis to development.
9. If both the entries show up then rediscover all the devices by going into Devices -> View/Rediscover/Delete

- If a few devices are going to unreachable state then follow the steps listed below. OM has two SNMP stacks one from Smarts and the other from Cisco. It is necessary that both of them work on a device to be able to get a device managed
  - To check the Cisco stack
    1. Check if snmp credentials are correctly entered. Export the device details from DCR and check the read community string.
    2. Go to http://<serverip>:1741/cwhp/device.center.do?device=<deviceIP>
    3. At the bottom of the page go to Functions Available->Tools-> Management Station to Device
    4. Clicking on it brings up a window. Choose SNMP v1/v2 or SNMP v3 depending on what is configured on the device
    5. Enter the community string in v2(obtained in Step1).. By default public and private are entered in the edit field.
    6. If the device uses SNMPv3 enter the v3 username and password.
    7. Now click ok. If the result shows as failed, then try increasing the SNMP timeout.
    8. If it still does not work recheck the credentials that have been setup on the device.
  - To check the Smarts stack for v1 devices execute the following
    - <NMSROOT>\objects\smarts\bin\sm_snmp -d <deviceName> -s 1 -c <community> walk .1
  - To check the Smarts stack for v1 devices execute the following
    - <NMSROOT>\objects\smarts\bin\sm_snmp -d <deviceName> -s 2c -c <community> walk .1
  - To check the Smarts stack for v1 devices execute the following
    - <NMSROOT>\objects\smarts\bin\sm_snmp -d <deviceName> -s 3 -u <username> -a <authProtocol> -x <authpwd> walk .1

  If the device is reachable through the Smarts stack and not through the Cisco stack, contact development for support.
- Check if the devices are managed through an IP Address that has a net mask of 252(two IP Addresses on a point to point serial link). If yes this is not supported because of a limitation in the Smarts Engine so manage it via another address on the router.
- Go to Devices->View/Rediscover/Delete. Go to the "All Unreachable Devices" and check the group under which the device is listed.
  - If it shows under SNMP Timeout follow the steps listed above.

- If it shows under Data Collector Timeout then rediscover the device and see if it moves to monitored state.
- If it shows under insufficient credentials then it means the SNMP read strings have not been entered.
- Make the corrections and the device will be rediscovered.

7. Why are some devices going into Partially Monitored state?

A: The answer to this varies version of CUOM version installed

For IPCOM 1.0

- Only CCMs can go into partially monitored state in IPCOM 1.0
- Check if you provided the correct http credentials in DCR by using the credentials to login to the CCM Admin page.
- If this is an MLA installation make sure that you are able to login to the device and the user has access to the AXL API.
- Check if the RIS Data Collector Service is running on the CallManager box.
- Check if the AXL API Service is enabled
    - In CCM version < 5.0 enable the following from Control Center
        - Cisco Serviceability Reporter
        - Cisco RIS Data Collector
    - In CCM version > 5.0 enable the following
      From Control Center - Feature Services
        - Database and Admin Services -> Cisco AXL Web Service
        - Performance and Monitoring Services -> Cisco Serviceability Reporter

      From Control Center - Network Services
        - SOAP Services -> SOAP -Real-Time Service APIs
        - SOAP Services -> SOAP -Performance Monitoring APIs
        - CM Services -> Cisco RIS Data Collector
- Now look at the device details under Devices -> View\Rediscover\Delete and check the error and use the table below

S. No	Error shown in Data Collector Status Information	Reason	Resolution steps
1	Error Code = CCM Authentication Failure Error Message = Success:WrongCredentials	This Message indicates that either ccm http credentials are not entered or the credentials provided are incorrect	Check if you provided the correct http credentials in DCR by using the credentials to login to the CCM Admin page and rediscover the device
2	Error Code= CCM Authentication Failure Error Message= Success:UnknownCredentialError	This message indicate some SNMP mgmt mibs are not responding. They could be • MIB-2 →	Restart the SNMP Agent on the box and rediscover the device

		ipAddress Table is not responding • CISCO-CCM-MIB → ccmTable is not responding specifically ccmClusterId attribute is not responding. • Inventory collection module could not find ccmVersion detail, this again because of ccmVersion attribute in CISCO-CCM-MIB is not responding.	
3	Error Code = CCM Authentication Failure Error Message = Success:WebServiceDown	Http service is not running or responding to requests from OM	Check if the Webserver is running by launching the CCM Admin page. Check if the firewall is blocking http/https connection between CCM and OM
4	Error Code = CCM Authentication Failure Error Message = Success: HTTPSCertificateNotImported	Indicates that the CCM certificate download is failed	• Check file IPToHostName.txt under CSCOpx\lib\jre\lib\security, it should contain an entry like deviceip>=<hostname> record for each of the ccm For e.g. 10.76.91.115=blrsd1 • Go to keytool utility location <NMSROOT>\CSCOpx\lib\jre\bin • Execute the command keytool -list -keystore <NMSROOT>\CSCOpx\lib\jre\lib\security\cacerts, it will list the downloaded certificates Check to a see an entry similar to this for the CCM ***Certificate fingerprint (MD5): AC:B6:94:A5:9C:17:E0:D7:91:52:9B:B1:97:06:A6:E4 cn=ct-sd, ou=nmtg, o=cisco systems, l=bangalore, st=Karnataka, c=in, Oct 26, 200 5, trustedCertEntry***, • Rediscover the device

For CUOM 1.1 installations

- For CCMs the steps are the same as listed above
- Note: In CUOM 1.1 IPCC and Unity boxes can also move into Partially monitored state
- Check if the WMI username (with domain Name e.g APAC\shaj) and password is entered in the Primary Credential field in DCR. If not this needs to be entered
- To verify the credentials for any of the boxes on the CUOM box do the following
  - Click on Start->Run. In the dialog box enter wbemtest as the command to run
  - In the dialog that opens click on Connect which opens another dialog
  - Click on connect. If you get an error then it means that
    - Credential is incorrect
    - Unable to connect to the Device
    - Some firewall is blocking the WMI access
  - This will establish if the credentials are correct.

8. What credentials do I need to enter to manage a device?

A: For CCM – HTTP credentials, SNMP Read
For Unity, IPCC – SNMP Read, Primary Credential (WMI)
For All other devices – SNMP Read

.

9. Cisco CallManager 4.2 is going into the partially monitored device state when using Operations Manager 1.0. You may be running into bug CSCsc92859

Action:

Upgrade Operations Manager to version 1.1

10. Why do devices move into unsupported state?

- Check if the device is reachable and it is responding to the SNMP (you can use a standard MIBbrowser)
- Check the SNMP version and credentials
- Check if CDP is enabled on the device and it responds to the cdpCacheGlobalId
- Get the value of the sysobjectid and check if the value is listed in one of the oid*.conf files under <NMSROOT>\CSCOpx\objects\smarts\conf\discovery
- Send the OID with details to TAC.

11. What are the recommendations for Rediscovery of devices?

- Turn off the weekly rediscovery schedule
- When a device is added to OM, then discovery for the specific device happens automatically

- If the user adds new modules to a Cat6k or changes the topology drastically the user can choose all the devices from Device->View\Rediscovery\Delete devices and run a rediscovery

Service Level View

12. When a Cisco CallManager subscriber has lost its CCMadmin service and thus communication with its publisher, the subscriber is not shown in the cluster in the Service Level View.

Action:

Check the Alerts and Events display to see the alert for that subscriber.

The Subscriber icon reappears in the Service Level View once the CCMadmin service is back online.

13. Why do I get an error message when I try to launch SLV immediately after reboot?

A: SLV depends on SIR to complete discovery before showing up the data. So it takes a few minutes after the reboot and system initialization to show up in SIR.

14. The Cisco Unity Express is not shown as being connected to the Cisco CallManager Express.

Action:

Make sure the dial-peer ID number is exactly the same as the voicemail number. For example, if the configured voicemail number is extension 6800, the SIP dial-peer voice ID number associated with the Cisco Unity Express must be 6800.

```
telephony-service
 voicemail 6800

dial-peer voice 6800 voip
 destination-pattern 68..
 session protocol sipv2
 session target ipv4:10.89.154.59
 dtmf-relay sip-notify
```

15. Why does SLV not launch on IBM servers with IBM Director?

A: In IBM machines with IBM Director installed make sure that you shutdown the IBM WMI CIM Server

- Go to Control panel ->Administrative Tools->Services
- Locate the IBM WMI CIM Server in the Services window. Right click and choose Properties.
- In the dialog find Startup type and change it from “Automatic” to “Manual”

- Stop the service
- From a command prompt execute
    - pdterm SIRServer
    - pdexec TopoServer

16. How are T1/E1 ports on Cat6k that are registered to CallManager shown in SLV?

A: In a Cat6k T1 and E1 scenario each port has it's own IP Address and registers with the CCM. However to understand that these ports are part of the same card and chassis the Cat6k that hosts the T1 card needs to be added into CUOM. Then the ports collapse into a single IP Address of the Cat6k in SLV.

17. One of the clusters is not shown in the SLV?

A: At the startup of OM, if the CallManager service was down or the SNMP agent was not responsive on all members in a cluster then the cluster will not be shown in SLV. The easiest way to check this is to see if the ccmTable in CISCO-CCM-MIB in contains the list of all CCMs. Rediscover the Callmanagers that are not shown and they should appear in Topology

18. Some of the CallManagers that belong to the cluster are not shown in SLV?

A: SLV currently needs the CallManager Service to be running on all the Nodes because the SNMP service does no return data when the Call Manager service is down. So these Callmanagers where Callmanager service is not running are not shown currently.

19. SLV is cluttered with a lot of unmanaged devices?

A: If you have a lot of Cat6k T1/E1 ports then see answer to How **are T1/E1 ports on Cat6k that are registered to CallManager shown in SLV?**. If you have ATA's and VG248's that need to be ignored then download a patch.

20. You cannot see the Service Level View; the TopoServer may be down.

Action:

Check the status of TopoServer:

1. Go to **CiscoWorks > Server > Reports > ProessStatus > Generate report**.
2. Verify that TopoServer is running.
3. If the process is stopped, start TopoServer. Go to **CiscoWorks > Server > Admin > Processes > TopoServer > Start**.
4. Launch the Service Level View.

21. The Service Level View only shows All Devices under the tree view, and nothing appears under All IP Communications Devices.

Action:

1. Wait for complete device discovery.
2. Wait for another 10 minutes after complete device discovery, and launch the Service Level View.

Synthetic Testing

22. An End to End call test is failing. How do we debug this?

- Verify that the extension number entered in the Recipient is that of the receiver phone and matches the MAC address configured in CallManager.
- If the call is scheduled to wait for an answer and is run against a real phone, verify that the receiver phone is configured with ForwardNoAnswer to Voicemail.
- Assign the same extension to a real phone within the same CSS and Partition and check if the phone receives the call.
- If it does delete the MAC address from the CCM and readd it and check if it succeeds.
- If the caller and receiver CCM belong to different clusters verify that intercluster trunk is configured and active.

23. I choose a MAC in the synthetic testing UI but the extension field in the GUI is empty and grayed out. How do I fix this?

- Verify that the MAC is configured with an extension in the CCM (Using CCM Administration page).
- Schedule an IP Phone Discovery, wait till it completes and try to access the screen again.

24. A Unity MWI test is failing. How do we debug this?

- Take a real phone and configure it with the same extension and settings as the receiver phone in the MWI test
- If the MWI light is ON use the messages button to delete all the messages in the mailbox and ensure the MWI light goes off
- When the call is received check that the phone rings and a message is left and the MWI comes on.
- If the MWI does not come ON then it can mean that MWI is not being delivered. This needs to be debugged on the Unity box
- If MWI comes ON and does not go OFF then it means that the message is not deleted which means that the menus in the TUI have been customized which cannot be handled by synthetic testing. So setup the default message handler for the receiver phone.

25. How can I backup and restore tests?

- From CUOM 1.1, you can export the tests to a file, delete the tests and use the exported file to import them later.

26. Synthetic Testing results are not visible in the DDV?

- Verify if VHM Server is up and running.(pdshow VHMServer)
- If it is running then it is possible that the tests were created when VHMServer was down
- Export the tests and delete the existing tests.
- Import the tests again

27. What logs should be collected before sending it to development?

- Add the following to CSCOpx/etc/cwsi/AMAServer.properties
  LogMsg.debug=ama:ama.framework:ama.protocol:ama.sms:ama.util:ama.skinny:ama.textual:ama.ipservices
- Restart STServer using the following commands
  - pdterm STServer
  - pdexec STServer
- Enable logging from Administration->Logging. Enable Debug for Synthetic Testing Server
- Wait till the tests are run and status is updated in DDV and send the log file <NMSROOT>\CSCOpx\log\ama-ani.log

IPIF

28. Discovery does not complete and is always in progress?

- Are there many unreachable devices in the network?
- Check if the CCMs have a http server that does not respond for a very long time.
- If there are a large number of phone audit entries then this problem can occur. To fix this use a custom patch from development. Contact TAC for support.

29. Phones registered to a CallManager not shown in IPIF GUI?

- Check the ccmPhoneTable from CISCO-CCM-MIB and see if it has entries for the phones

30. Columns with details like Port and VLAN in the IP Phone reports show NA?

A: Check if the switch is managed in OM and is reachable

31. How do we debug the case of some phones that do not show up in IPIF?

A: Enable logging for IPIF using the Administrator->Logging.

AAD

32. I get an error “Unable to launch AAD. See AAD.log for details” when trying to launch AAD?

- Check the status of the following processes
  - pdshow EPMServer
  - pdshow VSMServer
  - pdshow ITMOGSServer
  - pdshow CMFOGSServer
- If any of the processes are down then restart daemon manager

  - net stop crmdmgtd
  - net start crmdmgtd (20 minutes after previous step)
- If all processes are up go to a command prompt and type epm
- The shell will initialize and connect to the epm process
- Run the following command on the shell “db select * from epm_alarm” to see if any alarms are in the table.
- If all of this is ok send aad.log under <NMSROOT>\log\itemlogs\AAD to development

33. I get a DynAPI error when AAD is open?

- Known issue with one of the jsrs library. Reload/Refresh the page by hitting F5

34. I am not seeing any Alerts in the AAD window?

This can happen when

- There are no alerts in the system.
- The server is in ACS mode and the user is not authorised for devices on which there are alerts in the system.
- You have clicked on one of the user defined views in "Views" tab and there are no alerts in the system on these devices.

Steps:

- Check if the server is in the ACS mode. If yes, check if the user is authorized any devices that have alerts.
- To check which device have alerts go to a command prompt and type epm
- The shell will initialize and connect to the epm process
- Run the following command on the shell “db select * from epm_alarm” to see if any alarms are in the table.

35. What does this entry “Unidentified trap” in AAD window mean?

A: Unidentified traps is a bucket for traps on devices not managed by CUOM.

36. I intermittently get an error when I launch event properties window for some events?

There are some events for which current values of attributes are displayed in the event properties screen. For these events, in some cases there may be an exception when trying to retrieve these current values.

- If you get an exception when trying to launch the event properties window, wait for sometime and then launch this page.
- If you still get an exception, enable logging for AAD at Administration -> Logging -> Alerts and Events Display and send us AAD.log file in log directory (<NMSROOT>\CSCOpx\log\itemLogs\AAD).

SQAAD

37. I don’t see any alerts in SQAAD. What could be the problem?

Ensure the following are done before debugging this problem

- Go to the Service Monitor application and check if the probes are registered and visible in the Service Monitor gui
- Go to Service Monitor setup page and check if the OM address is entered as a trap recipient even if Service Monitor is on the same machine
- In OM go to Administration -> Service Quality and add the Service Monitor even if it is on the same machine
- If these steps are correct then remember that only calls that fall below the SM threshold will shown in AAD.

Now to debug the problem if all the conditions above are met

- Check syslog.log under
    - NMSROOT\CSCOpx\syslog.log in IPCOM 1.0
    - NMSROOT\CSCOpx\log\qovr\syslog.log in CUOM 1.1

  It should contain entries that look like and see if you see recent syslogs. Check the value indicated by D=<value>. This is the MOS score multiplied by a factor of 10. Check if this value is below the threshold multipled by 10.
- If this is true check NMSROOT\log\qovr\trapgen.log

  This should contain the traps that are being generated from the system. If traps are available in this file then it means that the Service Monitor portion is functional and ready. If not the check for exceptions in probemanager.log and datahandler.log

IPC Discovery

Note: Most issues in this section are fixed in CUOM 1.1 SP1 located at http://wwwin-nm.cisco.com/Patches/patch-publisher/listbyproduct.cfm?searchbug=CSCsc84584&searchcomponent=&searchfile=&thisfamily=&thisproduct=2.+choose+product&searchProduct=UOM&searchheadline=&searchowner=&fromForm=yes&submit=Submit

38. Why do I get devices that are outside of the subnet specified in the filter as a part of discovery?

A: You need CUOM 1.1 SP1 to fix this issue.

39. Discovery Filters do not seem to work?

A: You need CUOM 1.1 SP1 to fix this issue.

40. What are the criteria for seed devices?

- Seed devices must be reachable via SNMP
- They should be running CDP and if not ping sweep must be enabled.
- CUOM 1.1 SP1 should be installed for a stable Auto Discovery

41. Why do the CCMs go into partially monitored state even though I specify the HTTP credentials?

- CUOM 1.1 SP1 should be installed.

- If the CCM version is 5.0 and it is configured in SNMP v3, then there is a known issue in 1.1 SP1 that it will go to partially monitored.

42. Why do Unity/IPCC/PA devices go into Partially monitored state?

- CUOM 1.1 SP1 should be installed
- WMI credentials must be specified in the Auto discovery configuration

43. Understanding the fields in the Device Credentials User Interface

- Use Device Credential User interface to provide various types of device credentials.
- These lists of credentials will be used to ascertain the right credentials for the devices discovered. There are 4 types of credentials that can be provided.
  SNMPv1/v2 - Read only and Read Write credentials.
  SNMPv3-User Name/Password and Authentication Protocol
  3) HTTP-HTTP UserName /Password for Cisco Call Manager
  4) WMI - Windows domain\UserName and password for Unity and IPCC (Only with CUOM 1.1 SP1)

Note: Once you provide these credentials they are stored in the system. When you come back to this screen again, you will not see the entered credentials. If you reenter the credentials, the old credentials will be overwritten.

44. Discovery takes too long?

A: There can be multiple reasons for this:

- There are too many unreachable devices. The devices may not be pingable OR may not be SNMP reachable. Its better to exclude specific IP ranges which do not have SNMP manageable devices such as IP Phones, in order to reduce the discovery time.
- Too many credentials. Discovery tries each credential to ascertain the right credential. This processing is sequential, and hence this may prolong the discovery time.
- The SNMP timeout is high. This will compound the problem mentioned in the #2.

45. Sometimes a device's SNMP MIB is not updated. The number of phones may not be updated in the SNMP MIB, causing the number of phones displayed in the Cisco CallManager Administration user interface to be different from the number of phones displayed in Operations Manager.

Action:

Verify that the SNMP MIB on the device is being updated. You can run the command on the Operations Manager server (from a command prompt), or you can use an SNMP MIB browser and compiler to query the Cisco CallManager (or Cisco CallManager Express, Cisco Unity Eexpress, and so on).

On the Operations Manager server, in a command prompt, enter the following command:

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

For example:

```
C:\Program Files\CSCOpx\objects\smarts\bin>sm_snmpwalk.exe -w -c
public 172.20.118.48
```

This command is available in the \CSCOpx\objects\smarts\bin directory. The output file is also present in this directory.

To use a MIB browser, you can download a freeware SNMP package from MG-Soft (http://www.mg-soft.com/download.html#MGMIBBPE) and go to the Cisco SNMP MIB download site and download the appropriate device MIBs: ftp://ftp-sj.cisco.com/pub/mibs/v2.

These MIBs are then compiled into the MIB browser application. This gives you the ability to query that device MIB.

Some MIBs of interest:

- CISCO-CCM-MIB.my
- CISCO-CCME-MIB.my
- CISCO-CDP-MIB.my

Prerequisite MIBs for the previous action:

- CISCO-SMI.my
- CISCO-TC.my
- CISCO-VTP-MIB.my
- IF-MIB.my

46. Discovery says it has "processed x devices", but I don’t see any devices in OM

A: Discovery processes all the devices and then applies the filters. Only after the entire process, the devices will be added to OM.

Notifications

47. What has changed from OM 1.0 to 1.1 in Notifications?

There have been major improvements to the notification GUI in 1.1.

1. In 1.0, notification criteria had to be created and associated with a subscription. Since this mapping is one to one the screens were combined and made one screen to create a notification group, which captures the subscription info as well. It gives the user one consolidated approach of creating/viewing/deleting a notification and subscription group.
2. Support for three states

a. "Inactive" state is when the notification's subscription schedule falls outside the current time. No notifications are forwarded in this state.

b. "Suspended" state is when the subscription has been manually suspended. No notifications are forwarded in this state.

c. "Active" state is when the subscription is operational. Notifications are forwarded in this state.

3. Support for “Always Active” subscriptions

48. How do I decode the trap sent from OM?

A: The trap is standard SNMP format. So any Trap receiver can be used to decode the trap. CISCO's EPM-NOTIFICATION MIB needs to be loaded to find the appropriate varbinds. MG-Soft MIB Browser is one example where the user can decode the trap.

This MIB can be found at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&mibName=CISCO-EPM-NOTIFICATION-MIB

The following will be the content of the trap

S.N	SNMP Variable
1	cenAlarmVersion
2	cenAlarmTimestamp
3	cenAlarmUpdatedTimestamp
4	cenAlarmInstanceID
5	cenAlarmStatus
6	cenAlarmStatusDefinition
7	cenAlarmType
8	cenAlarmCategory
9	cenAlarmCategoryDefinition
10	cenAlarmServerAddressType
11	cenAlarmServerAddress
12	cenAlarmManagedObjectClass
13	cenAlarmManagedObjectAddressType
14	cenAlarmManagedObjectAddress
15	cenAlarmDescription
17	cenAlarmSeverity
18	cenAlarmSeverityDefinition
19	cenAlarmTriageValue
20	cenEventIDList
21	cenUserMessage1
22	cenUserMessage2
23	cenUserMessage3
24	cenAlarmMode
25	cenPartitionNumber
26	cenPartitionName
27	cenCustomerIdentification
28	cenCustomerRevision

49. **User does not receive mail notifications. How do we debug this?**
    - Make sure that there is no email blocking options enabled in the virus scanner or any other firewall programs
    - Check if the configured SMTP server is up and running.

Performance

50. **How do I enable performance polling?**

    A: Performance Polling can be enabled by

    - Choosing the device in SLV and in the context menu that is launched on a right click choose Polling Parameters
    - Go to Administration ->Polling and Thresholds->Polling Parameters

51. **I get a message "No Data available for the last xx minutes" when I try to launch a performance graph. How do I debug this?**

    A: This means that the data for the chosen metric and device was not collected. To debug this

    - Check if data files are being written into <NMSROOT>\CSCOpx\data\gsu_#PerformanceDATA#_
    - If no data is written into the files then check if the device is monitored and up
    - Check for any exceptions in the poller.log
    - Perform the following steps
        - pdterm Performance
        - pdexec Performance
        - Go to Administration ->Polling and Thresholds->Polling Parameters
        - Choose any device group and click edit. In the dialog click apply and ok to the warning message that appears
        - This will cause reconfiguration and resync between Performance and VIC that is required for performance polling

52. **What does the * mean in the data files for Performance?**

    A: * means that data is not available which could be because of

    - Device error
    - Internal CUOM error
    - Metric not valid for the device

8.3 Frequently Asked Questions

1. **The Service Level View shows devices that are not added to Operations Manager in the cluster relationship.**

   These devices are part of the cluster; therefore, they are shown. These devices are grayed out, and no operations can be performed on them.

2. **Sometimes the link from the device ends at the Cisco CallManager and sometimes at the circle.**

   H323 gateways and Gatekeepers are registered to the cluster; links from these devices will end at the circle.

3. **The alert count in the Service Level View does not match the alert count shown in the Alerts and Events display.**

   The Service Level View shows alert counts only for IP telephony devices that are part of the cluster.

4. **The Alerts and Events display shows the informational alert for a device, but the Service Level View does not.**

   Alerts on the device may have been cleared. After some time, a cleared event will also be removed from the Alerts and Events display.

5. **Most Recent Alerts shows alerts for devices, but the Alerts and Events display does not show alerts for any devices.**

   The alerts are in a transient state. Refresh the Service Level View and the alerts will no longer be shown.

6. **For IPCC, devices under instance have alerts, but the alerts are not rolled up to the instance level.**

   Instance alert rollup is based on the alerts that are affecting that specific IPCC instance. If the device is showing the alert, it may be due to an IPCC service being down, which is not affecting this IPCC instance.

7. **The total device count shown in the Service Level View is not the same as the number of devices in Operations Manager.**

   The Service Level View does not include the devices present under All Devices. It only includes the devices that are part of the cluster and not necessarily managed by Operations Manager.

8. **The total phone count shown in the Service Level View is not the same as the number of devices in Operations Manager.**

   The Service Level View phone count does not include the suspected phones.

9. **The Service Level View tree view displays different Cisco Call Manager Express clusters. The map view shows only one Cisco CallManager Express cloud.**

   Check if there are more than 10 Cisco CallManager Expresses. If there are more than 10, all the Cisco CallManager Expresses are grouped under one cloud in the map view.

10. **There are fewer than 10 Cisco CallManager Expresses and the map view still shows only one Cisco CallManager Express cloud.**

    Some Cisco CallManager Expresses may have been deleted after the Cisco CallManager Express grouping occurred. Refresh the screen. Individual CallManager Expresses will appear.

11. **There are fewer than 10 Cisco CallManager Expresses and there are no Cisco CallManager Expresses in the map view.**

    When updating occurs in the existing Service Level View, sometimes the Cisco CallManager Express clouds get deleted from the map view. The tree view should still show the Cisco Call Manager Expresses. To get the Cisco CallManager Expresses to appear in the map view, refresh the Service Level View.

12. **A device group has be modified through the Group Administration and Configuration page.**

    The Service Level View does not handle this case. The workaround is to disable and then re-enable the view using OM > Manage Views.

13. **The Service Level View is open, and a new virtual link has been added. The topology does not show this in the map.**

    New virtual links are not automatically added to the view. Refresh the view, and you will see the newly added virtual links.

14. **Launching connectivity detail displays the following error: "Cannot load connectivity detail information for device..."**

    - Enable CDP on the device and wait for phone rediscovery to occur.
    - In Operations Manager, check the neighboring devices (within five hops) to see if they are in the Monitored or Partially Monitored state.

15. **When the Connectivity Detail window is open, updates to alerts on the device are not shown.**

    Connectivity details are not automatically updated. Refresh the window.

9 Appendix

For the list of all possible events displayed on the Alert Details page, and their descriptions, see:

http://www.cisco.com/en/US/products/ps6535/products_user_guide_chapter09186a008063d8b4.html

For in-depth information about Operations Manager support for the host resources MIB and Operations Manager implementation of system application MIBs, check:

http://www.cisco.com/en/US/products/ps6535/products_user_guide_chapter09186a008063c928.html

For information on ICMP and SNMP polling done by Operations Manager, and the SNMP version supported in Operations Manager, check:

http://www.cisco.com/en/US/products/ps6535/products_user_guide_chapter09186a008063c925.html

For a list of MIBS polled by Operations Manager, check:

http://www.cisco.com/en/US/products/ps6535/products_user_guide_chapter09186a008063c9b9.html

For a list of processed and pass-through traps and other unidentified traps and events, check:

http://www.cisco.com/en/US/products/ps6535/products_user_guide_chapter09186a008063c9ba.html

For information on how Operations Manager calculates repeated *restarts* and *flapping***,** check:

http://www.cisco.com/en/US/products/ps6535/products_user_guide_chapter09186a008063c926.html

10 Useful URLs

10.1 Operations Manager Cisco.com URLs

http://www.cisco.com/en/US/products/ps5747/Products_Sub_Category_Home.html

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

http://www.cisco.com/en/US/products/ps6536/index.html

10.2 Miercom Review of Operations Manager and Service Monitor

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

10.3 CEC URLs

10.3.1 VTG

http://wwwin.cisco.com/voice/products/service_monitor.shtml

http://wwwin.cisco.com/voice/products/operations_manager.shtml

10.3.2 NMTG

http://wwwin-nmbu.cisco.com/fieldportal/products/uom/summary.cfm?family=CiscoWorks&prod=uom

http://wwwin-nmbu.cisco.com/fieldportal/products/usm/summary.cfm?family=CiscoWorks&prod=usm

10.4 VoD—Operations Manager

http://vsearch.cisco.com/

Look for the Video on Demand (VoD) by Tara Jagannathan. This is the Operations Manager demo VoD.

http://wwwin-enged.cisco.com/vod/trainingsession/060214_17542/

10.5 Access to Operations Manager Software for Demonstration

http://wwwin-nmbu.cisco.com/fieldportal/demoserver/index.cfm

http://salt/uom-usm/index.htm

10.6 Training Resources for Operations Manager

http://tools.cisco.com/cmn/jsp/index.jsp?id=49785&redir=YES&userid=(none)

http://wwwin-nmbu.cisco.com/fieldportal/products/uom/index.cfm?Prod=uom&Filetype=Tutorial&tsession=yes&t

http://wwwin-nmbu.cisco.com/fieldportal/products/usm/index.cfm?Prod=usm&Filetype=Tutorial&tsession=yes&t

10.7 Software Downloads

For Cisco employees, to download or request a copy of the software for evaluation:

http://wwwin-nmbu.cisco.com/Evals/mainpage.cfm

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 the "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 to ask-ipc-management@cisco.com.