User Guide for Cisco Unified Operations Manager

Software Release 2.1
Cisco Unified Communications Management Suite

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

Text Part Number: OL-16547-02

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

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

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

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

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

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

User Guide for Cisco Unified Operations Manager

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

GNU eTeks PJA Toolkit
Copyright © 2000-2001 Emmanuel PUYBARET/eTeks info@eteks.com. All Rights Reserved.
The eTeks PJA Toolkit is resident on the CD on which the Software was delivered to you. Additional information is available at eTEks' web site: http://www.eteks.com. The eTeks PJA Toolkit program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License (GPL) as published by the Free Software Foundation; version 2 of the License. The full text of the applicable GNU GPL is available for viewing at http://www.gnu.org/copyleft/gpl.txt. You may also request a copy of the GPL from the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA. The eTeks PJA Toolkit program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

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

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

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

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

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

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

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

CONTENTS

Preface

This manual describes Cisco Unified Operations Manager (Operations Manager) and provides instructions for using and administering it.

Audience

The audience for this document includes:

- Network administrators and operators who monitor the status of the IP telephony system and IP fabric
- System administrators who maintain and configure software systems

Conventions

This document uses the following conventions:

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

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

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

Product Documentation

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

Table 1 describes the product documentation that is available.

Table 1 Product Documentation

Document Title	Available Formats
Supported Devices Table for Cisco Unified Operations Manager 2.1	On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps6535/products_device_support_tables_list.html
Release Notes for Cisco Unified Operations Manager 2.1	• In PDF on the product CD-ROM • On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps6535/prod_release_notes_list.html
Installation Guide for Cisco Unified Operations Manager (Includes Service Monitor) 2.1	• In PDF on the product CD-ROM • On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps6535/prod_installation_guides_list.html
User Guide for Cisco Unified Operations Manager 2.1	• In PDF on the product CD-ROM • On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps6535/products_user_guide_list.html
Context-sensitive online help	• Select an option from the navigation tree, then click **Help** • Click the Help button on the page

Related Documentation

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

Table 2 describes the additional documentation that is available.

Table 2 Related Documentation

Document Title	Available Formats
Release Notes for Cisco Unified Service Monitor 2.1	• PDF on the product CD-ROM • On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps6536/prod_release_notes_list.html
User Guide for Cisco Unified Service Monitor 2.1	• PDF on the product CD-ROM. • On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps6536/products_user_guide_list.html
Release Notes for CiscoWorks Common Services 3.0.5 (Includes CiscoView 6.1.5) on Windows	On Cisco.com at the following URL: http://cisco.com/en/US/products/sw/cscowork/ps3996/prod_release_note09186a00806f45bf.html
Installation and Setup Guide for Common Services 3.0.5 (Includes CiscoView) on Windows	On Cisco.com at the following URL: http://cisco.com/en/US/products/sw/cscowork/ps3996/products_installation_guide_book09186a00806ab62a.html
User Guide for CiscoWorks Common Services 3.0.5	On Cisco.com at the following URL: http://cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_book09186a00806feda7.html

Additional Information Online

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

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

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

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

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

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

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

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

Obtaining Documentation and Submitting a Service Request

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

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

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

PART 1

Overview

CHAPTER 1

Introduction

These topics provide an overview of Cisco Unified Operations Manager (Operations Manager):

What Is Operations Manager?

Cisco Unified Operations Manager is a member of the Cisco Unified Communications family of products, which provides a comprehensive and efficient solution for network management, provisioning, and monitoring of Cisco Unified Communications deployments.

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

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

Operations Manager increases productivity of network managers, enabling them to isolate problems more quickly using:

- **Contextual diagnostic tools**:
  - Diagnostic tests provide performance and connectivity details about different elements of the converged IP communications infrastructure.

  - Synthetic tests replicate end-user activity and verify gateway availability and other configuration and operational aspects of the IP communications infrastructure.
  - IP service-level agreement (IP SLA)-based diagnostic tests can measure the performance of WAN links and node-to-node network quality.
  - Phone status tests use IP SLA to monitor the reachability of key phones in the network.
  - Performance graphing allows you to select and examine changes in network performance metrics. You can select, display, and chart network performance data in real time.
  - RTMT (Real-Time Monitoring) Tool monitors real-time behavior of the components (device status, system performance, device discovery, and CTI applications) in a Cisco Unified Communications Manager (formerly known as Cisco CallManager) cluster.
- **Clickable information in notification messages—**Includes context-sensitive links to more detailed information about service outages.
- **Context-sensitive links to other Cisco tools**—For managing IP communications implementations.

Operations Manager also does the following:

- **Presents service-quality alerts**—Uses information from Cisco Unified Service Monitor 1.1, when it is also deployed, to:
  - Display Mean Opinion Scores (MOSs) associated with poor voice quality between pairs of endpoints (Cisco Unified IP Phones, Cisco Unity messaging systems, or voice gateways) involved in a call and other associated details about the voice-quality problem.
  - Enable you to perform a probable path trace between the two endpoints and reports on any outages or problems on intermediate nodes in the path.
- **Highlights current connectivity-related and registration-related outages affecting Cisco Unified IP Phones in the network**—In addition, provides contextual information that enables locating and identifying the IP phones involved.
- **Tracks IP communications devices and IP phone inventory**—Tracks Cisco Unified IP Phone status changes and creates a variety of reports that document move, add, and change operations on Cisco Unified IP Phones in the network.
- **Provides real-time notifications**—Uses SNMP traps, syslog notifications, and e-mail to report the status of the network being monitored to a higher-level entity (typically, to a manager of managers).
- **Provides easy to use, scalable reports**—Displays large networks using visual cues in map views as well as tabular reports to access management details of clusters and devices.
- **Provides Service Level View enhancements**—Automatically groups the Gateways and Application servers if quantity grows beyond a limit. Displays Unified Communications Manager Express and Unity Express information and status in a tabular form rather than in graphical form. Groups unmanaged devices under a single group to reduce the grayed icons clutter.
- **Enables coresidence with other Cisco Unified Communications Management software**—Add links to Operations Manager to launch other Unified Communications management applications using the UC Management Suite tab. You can run Service Monitor, Provisioning Manager, and Service Statistics Manager in standalone mode or as coresident.

Is Operations Manager Ready to Use?

The person or team that installed Operations Manager should have completed the initial configuration before you start working with Operations Manager. The instructions for configuring Operations Manager are included in *Installation Guide for Cisco Unified Operations Manager*.

To use Operations Manager, you must import devices into the Operations Manager inventory as explained in Importing Devices from the DCR, page 16-16.

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

Note When Operations Manager is installed, it automatically synchronizes with the DCR and adds inventory. This is the default setting.

For more detailed information on device management, see Getting Started with Device Management, page 16-1.

Once you have imported devices, Operations Manager is ready to monitor and analyze events, and provide notification of alerts on the Monitoring Dashboard displays (Service Level View, Alerts and Events, Phone Activities, and Service Quality Alerts). Operations Manager uses the default polling parameters and threshold values, default inventory collection and purging schedules, and default views. You should determine whether the default values are adequate for your use.

Note Starting with versions 4.3, 5.1, and 6.0, the product we formerly referred to as Cisco Unified CallManager will be called Cisco Unified Communications Manager. Versions earlier than 4.3 and 5.1 retain the Cisco Unified CallManager name. Throughout this document/online help, any reference to Cisco Unified Communications Manager can also be understood to refer to Cisco Unified CallManager, unless explicitly noted.

Table 1-1 lists tasks that you may attend to, at your discretion, after the initial configuration. The table lists optional configuration tasks and some day-to-day tasks that you may want to address when you first start to use Operations Manager.

Table 1-1 Tasks to Consider when Initially Setting Up Operations Manager

Initial Setup Tasks	Explanation	Reference
Add Monitoring Dashboard views.	Views control which groups of devices are the focus of the Monitoring Dashboard displays (Service Level View, Alerts and Events, Phone Activities, Service Quality Alerts, IP Phone Status, All IP Phones/Lines, Manage Views and Unified CM Express View). There are two default views. You can add more views.	Managing Views, page 6-1
Subscribe users to receive e-mail notification of alerts and subscribe hosts to receive Operations Manager-generated SNMP traps.	Operations Manager displays the operational health of the IP telephony environment and IP fabric on the Alerts and Events display. In addition, you can subscribe users and hosts to receive e-mail or Operations Manager-generated SNMP traps, respectively, in response to alerts.	Using Notifications, page 15-1
Update polling parameters and threshold values.	Operations Manager provides default values. However, you can update the values based on your experience with and knowledge of the IP telephony environment and IP fabric. You should plan to apply the changes during a time of low activity on the network.	Configuring Polling and Thresholds, page 19-1

Table 1-1 Tasks to Consider when Initially Setting Up Operations Manager (continued)

Initial Setup Tasks	Explanation	Reference
Enable the voice utilization polling settings.	By default, the voice utilization polling settings are not enabled. Operations Manager uses the statistics gathered during voice utilization polling for charting network performance.	For information on performance graphing, see Using Performance Graphs, page 7-1. For information on setting polling parameters, see Managing Polling Parameters, page 19-12.
Set up synthetic tests to monitor IP telephony application health.	You can configure various tests to run at intervals against IP telephony elements, such as Cisco Unified Communications Managers.	Using Synthetic Tests, page 9-1
Set up Node-To-Node tests.	Node-To-Node tests monitor the response time and availability of multiprotocol networks on both an end-to-end and a hop-by-hop basis.	Using Node-To-Node Tests, page 11-1
Set up phone status tests to check the availability of key phones.	You can configure Operations Manager to test the availability of key phones in your network.	Using Phone Status Testing, page 8-3
Set up batch tests.	You can test the health and connectivity of a branch office. Batch tests consist of a set of synthetic tests that are run on voice applications and a set of phone tests that are run on real phones in the branch office.	Using Batch Tests, page 10-1
Set up Survivable Remote Site Telephony (SRST) tests.	After you import devices to Operations Manager, import a list identifying the source routers and target SRST routers in Operations Manager inventory. This enables Operations Manager to perform regular tests and to notify you when a branch office fails over to SRST.	Understanding How Operations Manager Monitors SRST, page 18-1
Update the device inventory collection schedules.	Operations Manager provides a single default schedule for device inventory collection. You can use that schedule or suspend it.	Working with the Device Inventory Collection Schedule, page 16-37
Update phone discovery schedules.	Operations Manager provides six default schedules for phone discovery. You can update or delete them; you can also add phone discovery schedules (up to a maximum of ten.)	Working with IP Phone Discovery, page 16-38
Update the Purging Scheduler.	By default, Operations Manager purges the database at midnight. You can edit the schedule.	Setting System-Wide Parameters Using System Preferences, page 20-9
Configure Operations Manager to forward traps to a Network Management System (NMS).	Operations Manager can forward traps to other NMSs, such as HP OpenView and NetView.	Integrating SNMP Trap Receiving with Other Trap Daemons or NMSs, page 20-5
Set up cross-launch capabilities to other Cisco Unified Management products	Operations Manager allows you to create links to other Cisco Unified Management products such as Service Monitor and Service Statistics Manager so that you can run diagnostic reports and access other monitoring functions.	Setting Up Cisco Unified Communications Management Application Links, page 21-1

How Will I Use Operations Manager for Day-to-Day Operations?

These topics briefly describe Operations Manager functions that will be used frequently. On a day-to-day basis, operations personnel are likely to use the Monitoring Dashboard displays (Service Level View, Alerts and Events, Phone Activities, Service Quality Alerts, and Unified CM Express View) to monitor the IP telephony environment.

Network administrators and operators might similarly use the Monitoring Dashboard displays and Alert and Event History to assess network health and the IP Phone reports to solve IP phone problems.

In addition, network administrators and operators will use:

- **Device Management**—To keep the inventory of devices that Operations Manager monitors current.
- **Notification Services**—To ensure that the right users and systems receive e-mail or SNMP traps in response to alerts on selected devices, device groups, and clusters.

To make the most effective use of Operations Manager on a day-to-day basis, network administrators and operators also need to understand the impact of operations on configuration and administration tasks. An overview is provided in Scheduling Operations Manager Tasks, page 20-3.

The Operations Manager functions that support day-to-day operations are further described in the following topics:

About Alerts, Alert Types, and Events Monitored

An alert is a grouping of one or more events for a given device, while an event is the actual issue seen in the network. All events for a device are rolled up under a single alert. Each event is assigned a unique identification number which is displayed in left column in the Alert Display window. When the event changes its state, it is assigned a new event ID, whereas the alert ID for a device continues to remain the same if at least one issue persists continuously. When a new event for a device occurs after all the existing event(s) for that device get cleared and purged from the system, the device gets a new alert ID. There may be a case when you see that there are no events for an alert and the next subsequent event for the same device gets the old alert ID. This can occur when some user cleared events exist in the database. To verify this, use alert history.

Since the same device can have more than one alert ID in the past, use the search by device option rather than the alert ID to search alert history to identify all the previous events for a given device.

When a device is deleted from Operations Manager, all the corresponding events/alerts are also deleted. For more information on events, see Events Processed, page E-1.

Alert Types

There are two types of events, device and service quality events:

1. Device events which are seen under Alert and Events Display and include:
   - Events for a device
   - Cluster events
   - Phone events

   Device, IP phone, and cluster alerts are shown on the Alert and Events Display.
2. Service Quality events are seen in the Service Quality Alerts and Events display (SQAAD). Service quality alerts are shown in the Service Quality Alerts and Display.

Alert States

The alert states include:

1. Active—If there is at least one event for an alert in the active state, the overall alert state is shown as active. This is an indication that there is some issue currently existing for that device.
2. Cleared—If all the events for an alert are either in the Cleared or UserCleared state, the alert is shown as cleared. This is an indication that all the issues for this device are not existing any more in the network. Such alerts are shown on the Alerts and Events display for information for between 30 to 60 minutes. If all the events are in Cleared state, then the alert gets purged from the display and the databases. If at least one event exists in a UserCleared state, then Operations Manager retains it in the database, so that these UserCleared events are not generated again.
3. Acknowledged—If the alert is acknowledged from the display, the status is shown as acknowledged. This is an indication that user is aware of this alert and is working on fixing the issues.

Event States

The event states include:

1. Active—Whenever any issues occur in the network there is a corresponding event generated in Operations Manager.
2. Cleared—There are two types of cleared events.
   a. When the issue gets resolved in the network there is a cleared event generated. The corresponding active event is removed and substituted by a cleared event.
   b. If the corresponding cleared event cannot be generated then Operations Manager generates a auto cleared event. The event details gives this information if it was auto cleared. The time interval for auto cleared event generation varies for different types of events. For event details, see Supported Events, page E-2. Even if a auto cleared event is generated, the issue may not be resolved in the network. The time intervals for generating cleared events is based on the minimum time required by the administrator to look into the issue and fix it. To avoid missing any important events that may have occurred over a weekend, we recommend you check the alert history in the Alert Display window for a duration of around 30 to 60 minutes.

      To identify automatically cleared events, look for the following in the event details: Cleared by: Cisco Unified Operations Manager has automatically cleared this event.
3. UserCleared—When a event is manually cleared from the dashboard, it moves into a UserCleared state. If you are aware of the issue and not interested in seeing it on the dashboard, you can manually clear the event. When the corresponding cleared event is generated, the event will eventually move from UserCleared state to Cleared state. This event change displays in the user interface and can also be seen as part of alert history. UserCleared events are stored in the database to remind you that you are not interested in that instance of the event. It continues to remain in the database until a cleared

event is generated for it. UserCleared event states do not mean that the issue is resolved in the network. The issue may continue to exists in the network. Such events will be shown on the Alert Display window for a duration of around 30 to 60 minutes.

4. Acknowledged—When an event is acknowledged from the user interface, it moves into the acknowledged state. If you are aware of the issue and are currently working on it, it can be acknowledged. When the issue is fixed in the network or if it is time for auto clear, the event moves into the cleared state.

Alert Severities

The alert can have one of the following severity levels:

1. Critical—If there is at least one event for an alert that is marked critical, the alert also become critical.
2. Warning—If all the events for an alert are in warning or a combination of warning and informational severity levels, the alert is assigned a warning severity level.
3. Informational—If all the events for an alert are informational, the alert is assigned a Informational severity level.

Note Customized severities are not reflected for the events and alerts shown in the dashboard. Therefore you may see a difference in the event/alert severities if you performed any event customization. Service Level View shows the same alert severity as seen in the Alerts and Events dashboard.

Alert Age

Alert age is calculated based on the difference between the current time and the oldest event timestamp present for an alert in the database. The oldest event timestamp can be seen in the Alert Details window. If an alert's age is very old and you don't see any events for that alert with older timestamps it may be because the event (which has the oldest timestamp) was user cleared in the past and it is hidden in the database.

What Are the Monitoring Dashboards?

Operations Manager provides you with four monitoring dashboards. See the following sections for a description of each:

- What Is the Service Level View?, page 1-7
- What Is the Alerts and Events Display?, page 1-8
- What Is the Service Quality Alerts Display?, page 1-8
- What Is the Phone Activities Display?, page 1-9

What Is the Service Level View?

The Service Level View displays a logical topology view of your IP telephony implementation. This logical view focuses on the call control relationships.

The Service Level View shows all the Cisco Unified Communications Manager clusters, Unified Communications Express device clouds, associated gateways, gatekeepers, application servers, and Survivable Remote Site Telephony (SRST) enabled devices, as well as their registration status with Cisco Unified Communications Manager.

The Service Level View is designed so that you can set it up and leave it running, providing an ongoing monitoring tool that signals you when something needs attention. When a fault occurs in your network, Operations Manager generates an event or events that are rolled up into an alert. If the alert occurs on an element, it is shown on the Service Level View.

You can use the Service Level View to:

- Display a logical or neighbor topology view of your IP telephony deployment.
- View cluster or device reports.
- View and act on alerts for devices.
- Run other Operations Manager tools.
- Launch administration pages for devices.

What Is the Alerts and Events Display?

The Alerts and Events display provides a consolidated real-time view of the operational status of your IP telephony environment and IP fabric. When a fault occurs in your network, Operations Manager generates an event (or events). Events are rolled up into alerts, one alert for each device with faults.

When an alert occurs on an element in your active view (a logical group of devices), it is displayed on your Alerts and Events display. You, or a user with administrative privileges, can customize your view to include only those device groups (devices or clusters) that are important to you.

From the Alerts and Events display you can also:

- Drill down into an alert to see what events caused the alert, and add alert annotations for other users to read.
- Drill down into specific events for attribute values.
- Open a Detailed Device View to examine device components and suspend or resume monitoring of them.

You can see which components of the device are in the Operations Manager manageable inventory as follows: After you locate the device on the Alerts and Events display, you can click it and open a Detailed Device View. The Detailed Device View displays the manageable components of the device. From the Detailed Device View, a user in a Network Administrator role can suspend monitoring of a device component and, afterwards, resume monitoring of the device component again.

What Is the Service Quality Alerts Display?

The Service Quality Alerts display provides real-time information about IP phone service quality. Service Quality Alerts displays are designed so that you can set them up and leave them running, providing an ongoing monitoring tool that signals you when something needs attention.

When Operations Manager receives traps from Service Monitor, Operations Manager generates an event or events that are rolled up into an alert. The alert is shown on your Service Quality Alerts display. From a Service Quality Alerts display you can launch other windows to obtain more information.

Note Use the Service Quality Alerts display to view alerts that Operations Manager generates based on SNMP traps sent by Cisco Unified Service Monitor (Service Monitor). To use the Service Quality alerts display, you must have a licensed copy of Service Monitor configured to send traps to Operations Manager. You must also add Service Monitor to Operations Manager; see Adding a Service Monitor Link from Operations Manager, page 21-3.

What Is the Phone Activities Display?

The Phone Activities display provides real-time information about the operational status of your IP phones. The displays are designed so that you can set them up and leave them running, providing an ongoing monitoring tool that signals you when something needs attention.

The Phone Activities display shows information about the IP phones in your network that have become disconnected from the switch, are no longer registered to a Cisco Unified Communications Manager, or have gone into SRST mode.

What Are Diagnostics?

Note If you do not have the required software license, you will not be able to use the diagnostic tools. The Diagnostics tab will not appear in Operations Manager.

Operations Manager provides you with three types of diagnostic tools, see the following sections for a description of each:

- What Are Phone Status Tests?, page 1-9
- What Are Synthetic Tests?, page 1-9
- What Are Batch Tests?, page 1-10
- What Are Node-to-Node Tests?, page 1-10

What Are Phone Status Tests?

Phone status testing uses Cisco IOS IP Service Level Agreement (IP SLA) technology to monitor the status of key phones in the network. A phone status test consists of the following:

- A list of IP phones to test, selected by you.
- A testing schedule that you configure.
- IP SLA-based pings from an IP SLA-capable device (for example, a switch, a router, or a voice router) to the IP phones and, optionally, pings from Operations Manager to the IP phones.

What Are Synthetic Tests?

Synthetic tests are used to measure the availability of voice applications. Synthetic tests verify whether the voice application can service requests from a user. For example, you can use synthetic tests to verify that phones can register with a Cisco Unified Communications Manager.

Synthetic tests use synthetic phones to measure the availability of voice applications by emulating your actions. For example, a synthetic test places a call between clusters and then checks to see if the call is successful.

Operations Manager supports synthetic testing for the following:

- Cisco Unified Communications Manager and Cisco Unified Communications Manager Express
- Cisco TFTP Server
- Cisco Emergency Responder
- Cisco Conference Connection
- Cisco Unity and Cisco Unity Express

What Are Batch Tests?

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

What Are Node-to-Node Tests?

Node-To-Node tests monitor the response time and availability of multiprotocol networks on both an end-to-end and a hop-by-hop basis. After collecting this data you can use the Operations Manager graphing function to examine changes in network performance metrics. You can select, display, and chart network performance data in real time.

What Are Reports?

Operations Manager enables you to generate several types of reports, see the following sections for a description of the reports you can access through the Reports tab:

- What Is Alert and Event History?, page 1-10
- What Is Service Quality?, page 1-11
- What Are IP Phones and Applications Reports and IP Phone Status Change Reports?, page 1-11
-
- What Is a Personalized Report?, page 1-11

What Is Alert and Event History?

Alert and Event History provides the history of Operations Manager alerts and events. The stored history includes alert information and annotations (informational text entered by Operations Manager users), and event information and properties (component name and MIB attributes).

The Alert and Event History reports can display information for both devices and clusters.

You can start Alert and Event History in the following ways:

- From the Alerts and Events display.
- From the Service Level View.
- By selecting **Reports > Alert and Event History**. This method provides historical information about all alerts and events in the Alert and Event History database. The Alert and Event History database keeps information for the alerts and events that occurred within the last year.

You can use Alert and Event History to generate customized reports of specific alerts, specific events, specific dates, and specific device groups.

What Is Service Quality?

Service Quality reports enable you to view service quality alerts and events that occurred during the past year. The available information includes alert status and date, related devices, MOS value, codec type, and other event details.

Note Service Quality is useful only if you have purchased a license for Cisco Unified Service Monitor (Service Monitor). For more information, see *User Guide for Cisco Unified Service Monitor.*

What Are IP Phones and Applications Reports and IP Phone Status Change Reports?

An IP phone has a physical relationship with a switch and a logical relationship with a Cisco Unified Communications Manager. IP phone reports provide a combined view of both of these relationships, making it easy for you to track and resolve IP phone problems.

What Is a Personalized Report?

The Personalized Report enables you to configure a report for the devices, phones, and diagnostic tests that interest you. Other users cannot configure or view this report from Operations Manager.

What Are Service Impact Reports?

Service Impact reports provide you with a single report that describes how a particular failure impacts the rest of your IP telephony deployment. The report answers the following:

- How does this failure affect the users?
- Which services are unavailable because of this failure?
- What is the possible cause and location of the failure?

What Are Notifications?

In addition to watching network conditions as they change on the Monitoring Dashboard displays, you can use notification services to automatically notify users and other systems when specific changes occur on selected devices, device groups, and clusters. To do so, you create subscriptions for either e-mail notification or Operations Manager-generated SNMP trap notification.

Subscriptions comprise:

- A list of devices and device groups of interest
- The status and severity of alarms for which you want notification
- One or more recipients

You can add, edit, and delete subscriptions at any time as your need to disseminate the status and severity of alarms changes.

What Is Device Management?

Device Management involves keeping the inventory of devices that Operations Manager monitors up-to-date.

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

Before Operations Manager can start to monitor your network:

- You need to configure the DCR and Operations Manager device selection. Configuring the DCR involves understanding the options and deciding what makes the most sense for your site.
- Operations Manager needs to complete inventory collection.

The following scenario describes the process for managing devices:

Table 1-2 lists all the steps you need to complete.

Table 1-2 How to Start Monitoring Devices

	Description	References
Step 1	Add devices to the DCR. You have three options: • Use Operations Manager to add devices to the DCR. This is called physical discovery • Share a master repository with applications on other servers. • Bulk import using a seed file to import devices into the DCR.	Understanding the Device and Credentials Repository, page 16-4 See the instructions in the Common Services online help.
Step 2	Configure device selection.	• Automatically Importing DCR Devices, page 16-18 • Manually Importing DCR Devices, page 16-19
Step 3	Allow inventory collection to complete and start to monitor devices.	Understanding the Modify/Delete Devices Page, page 16-29
Step 4	Verify device import by using the Service Level View.	Verifying Device Import, page 16-21

How Does Operations Manager Work?

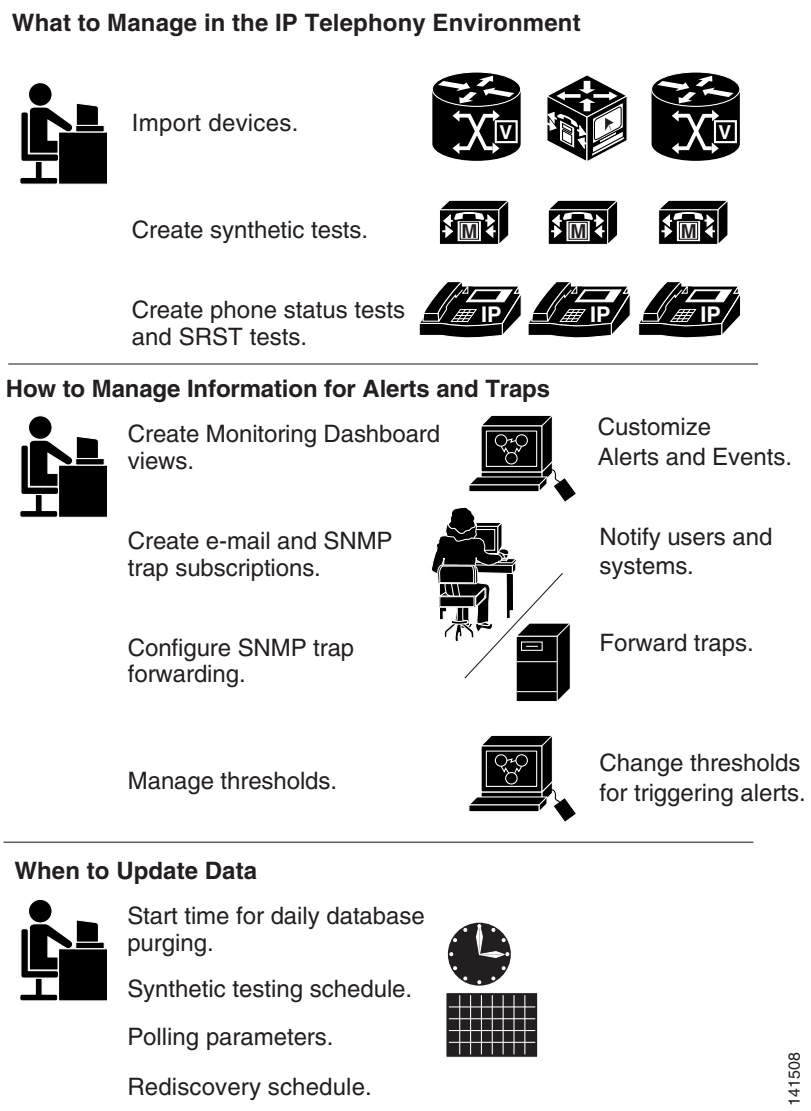
These topics provide a simplified view of Operations Manager user tasks and Operations Manager processing:

- Users Perform Device Management and Configuration, page 1-13
- Operations Manager Performs Ongoing Monitoring, Analysis, and Notification, page 1-14
- Users Respond to Notifications and Alerts, page 1-16

Users Perform Device Management and Configuration

Users supply the information that tells Operations Manager what to monitor. Figure 1-1 shows a user importing devices and phones, and performing optional configuration tasks to optimize Operations Manager.

Figure 1-1 The Role of User Input



Users supply the following information:

- Devices—You must import devices and, as your IP telephony environment and IP fabric change, you must add and delete them accordingly. Operations Manager performs periodic inventory collection, refreshing the inventory of phones, known devices, and device components.

Note Operations Manager monitors supported devices only. To see the device support table for Operations Manager, log in to Cisco.com.

- Phones:
  - Phone Status Tests—To perform phone status tests, you must select the phones to test by importing tests for phones that are already managed by Operations Manager.
  - SRST Monitoring—To determine when phones are running under SRST, you must import information for tests.
- Supported IP telephony applications—Operations Manager polls and rediscovers the devices on which supported IP telephony applications (for example, Cisco Unified Communications Manager) run, just as it does for any other supported device that you import. In addition, you can set up synthetic tests to monitor IP telephony applications such as Cisco Emergency Responder.

You can decide how to manage the information about alerts and traps that Operations Manager produces. For example, you can:

- Create views, enabling users to monitor specific groups of devices on the Monitoring Dashboard displays.
- Create subscriptions to send e-mail and generated SNMP trap notification to users and systems, respectively.
- Determine where to forward traps by configuring the port to which Operations Manager forwards them.

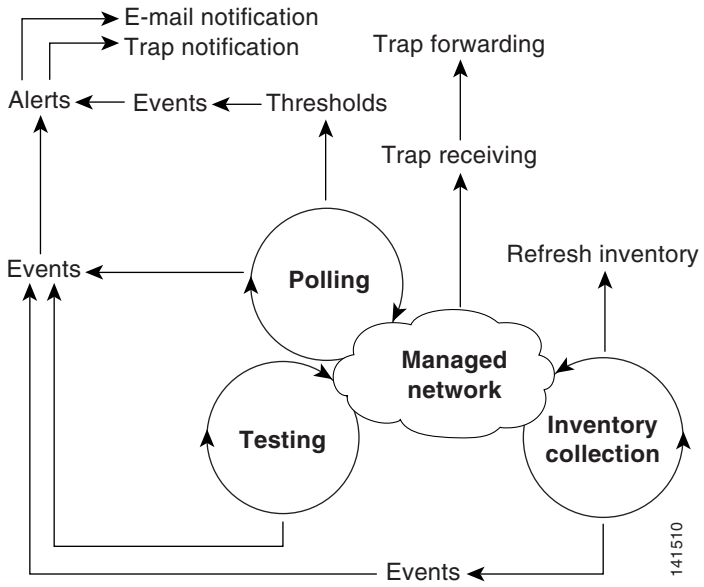
You can also control how often Operations Manager gathers data. Operations Manager receives traps in real time, but you can change the frequency with which it performs the following tasks:

- Polling—You can change the default polling parameters for device groups, altering the polling interval, timeout, and number of retries.
- Device discovery—You can suspend the default discovery schedule.
- Phone discovery—You can add, delete, or edit the schedules for phone discovery.
- Synthetic testing—You can change the frequency with which tests are run. In addition, you can change the range of time during which tests do not run.
- Phone status testing—You can set the interval for phone status tests.
- Node-to-Node testing—You can schedule the frequency with which tests should run.
- SRST monitoring—When you import SRST information, you set the intervals at which tests run. You can update SRST information by importing it again.

Operations Manager Performs Ongoing Monitoring, Analysis, and Notification

Operations Manager continuously gathers information from devices, device groups, clusters, and device components, analyzing and prioritizing events, and raising alerts.

Figure 1-2 Operations Manager Continuously Monitors the IP Fabric



Operations Manager generates alerts based on the following activities:

- Polling—During polling, Operations Manager identifies conditions that warrant generating an event, such as device unreachable or interface down.
- Managing thresholds—After polling, Operations Manager compares the data it collected against threshold values for the devices. If threshold values exceed or do not meet limits, Operations Manager generates the appropriate event. For example, if a T1 port's utilization is higher than 90 percent, Operations Manager raises an event in the Alerts and Events Display. For details on how Operations Manager manages both syslog and real-time monitoring collected thresholds, see Configuring Polling and Thresholds, page 19-1.
- Receiving SNMP traps—Operations Manager listens for traps on the default port or the port that you have configured for SNMP trap receiving. Operations Manager will process the traps from known, supported devices.
- Testing—You can configure Operations Manager to run the following types of tests:
  - Synthetic testing—Synthetic testing of selected functions on a Cisco Unified Communications Manager can uncover problems that Operations Manager reports.
  - Phone status testing—Operations Manager can use IP SLA technology to monitor the reachability of key phones in the network.
  - Node-to-Node testing—Operations Manager can use IP SLA technology to test the response time and availability of multiprotocol networks on both an end-to-end and a hop-by-hop basis.
  - SRST testing—Operations Manager can alert you when a branch office is operating under SRST.

As Operations Manager generates alerts and alert conditions change, Operations Manager determines when to send e-mail notification to subscribers and when to generate SNMP traps to send to other systems.

For additional information, see the following topics:

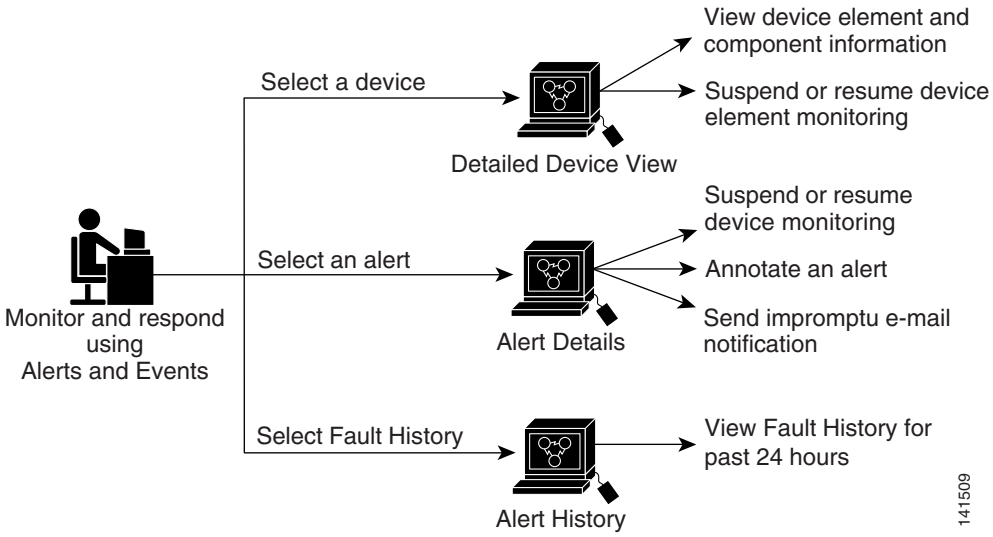
- MIBs Polled and Perfmon Counter Objects Used, page B-1
- Processed and Pass-Through Traps, page C-1

- Events Processed, page E-1
- Polling—SNMP and ICMP, page G-1
- How Operations Manager Calculates Repeated Restarts and Flapping, page H-1

Users Respond to Notifications and Alerts

Most users will monitor the condition of the IP telephony system by using the Alerts and Events display or the Service Level View; others will respond to e-mail. External hosts will receive generated SNMP traps. Figure 1-3 shows how you can respond using the Alerts and Events display.

Figure 1-3 Users Respond to Alerts



Getting Started with Operations Manager

These topics help you to work with and understand the Operations Manager user interface:

- Starting Operations Manager, page 1-17
- Working with Operations Manager Windows, page 1-17
- Using Displays and Reports, page 1-19
- Selecting Objects and Groups, page 1-22
- Understanding Your User Role, page 1-23
- Responding to Security Alerts, page 1-24
- Responding to Messages About Device Limits, page 1-24

Starting Operations Manager

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

Note If a client system is available, it is recommended that you perform all configurations and day-to-day activities on the client system. If a client system is not available, the Operations Manager server must also meet all the system requirements for a client system (for client system requirements, see *Installation Guide for Cisco Unified Operations Manager*).

Starting Operations Manager on a Client System

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

Starting Operations Manager on the Operations Manager Server

From the Windows desktop select **Start > All Programs > Cisco Unified Operations Manager** and **Service Monitor > Cisco Unified Operations Manager and Service Monitor**.

Note If Enhanced Security is enabled on the Windows 2003 system, you must add the Operations Manager home page to the Internet Explorer Trusted Sites Zone. You will not be able to access the Cisco Unified Operations Manager home page until it is added to the trusted sites. (See Adding the Operations Manager Home Page to the Internet Explorer Trusted Site Zone, page 1-17.)

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

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

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

Step 2 In the File menu, click **Add this site to**.

Step 3 Click **Trusted Sites Zone**.

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

Step 5 Click **Close**.

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

Step 7 Check the Status bar of the browser to confirm that the site is in the trusted sites zone.

Working with Operations Manager Windows

This topic focuses on questions you may have when you first start to work with the Operations Manager user interface:

- Why are multiple windows open?, page 1-18
- Why do I see the error "The page cannot be displayed"?, page 1-18

Why are multiple windows open?

For ease of use, Operations Manager opens separate browser windows for many displays. Having multiple windows open allows you to:

- Refer to information from one display to complete a task in another window.
- Rapidly compare information on different displays.

When Operations Manager opens a new browser window, it does not close previously opened windows. You can close browser windows when you are done with them.

Why do I see the error "The page cannot be displayed"?

Operations Manager displays often include links to more detailed information. Right-clicking a link and selecting Open in New Window is not supported. It is expected behavior for this error to appear.

When I press the Enter key, why doesn't Operations Manager complete the current task?

Operations Manager does not accept pressing the Enter key as a substitute for clicking buttons, such as **OK**, **Finish**, or **Next**, on the application page.

Where is the Help button?

The Help button is located in the top right corner of the window. For more information on how to use help, see Using Help, page 1-18.

Using Help

To start help:

1. Click the Help button in the top right corner. If you have a display open, click the question mark icon.

Note If you have selected an option in the navigation tree, the context-sensitive help for that option is displayed.

Help is displayed in a separate browser window that remains open until you close it. Online help includes an index and search capability.

How Are Dates and Times Displayed

Dates and times displayed by Operations Manager reflect the date, time, and time zone set on the server where Operations Manager is installed. If the client system you use to run Operations Manager is located in a time zone other than the time zone set on the server, you will notice the difference; for example:

- Status "as of" the current date and time will not display your local time and time zone and may not match your local date.
- Dates and times shown for previous events are recorded (and displayed) with the server time stamp, which is offset from your local time.

There are no settings that you can change on the client to affect the time zone displayed by Operations Manager. However, you can obtain information about the time zone acronyms and offsets used by Operations Manager in *Release Notes for* Cisco Unified Operations Manager *2.0*. You can view the release notes on Cisco.com.

How Are Phone Counts Displayed in Views and Reports?

The total physical phone count may be displayed differently in some reports and view pages in Operations Manager. Table 1-3 describes how phone lines display in Operations Manager.

Table 1-3 Phone Count Display

Screen or View	Description
Device Management: Summary	Total Phones shows the total number of unique physical phones in the managed network. The count does not include multiple lines for the same phones. Clicking on the number launches a report which shows multiline phones with comma-separated extensions in the same row.
Monitoring DashBoard: All IP Phones/Lines	Shows all the phone lines in the network in a report. Multiline phones are represented by different rows/records.
Reports > IP Phones and Applications > All Phones report	Shows all the phone lines in the network in a report. Multiline phones are represented by different rows/records.
Service Level View: Click to view all phones	Shows all the phone lines in the network in a report. Multiline phones are represented by different rows/records.
Service Level View: Summary Panel	Registered phone count indicates the total number of unique physical phones registered in the selected cluster. Unregistered phone count indicates the total count of unique physical phones unregistered in selected cluster.

Using Displays and Reports

Operations Manager presents information in displays and reports. The displays and reports usually use tables to format the information. The tables ease the task of handling information by providing the following features. Depending on the report, the features available in each report may vary:

- Search—You can search on a string of characters to locate an IP address or hostname.
- Sort—You can sort a display in the order you prefer by clicking any clickable column heading. See Paging and Sorting Displays and Reports, page 1-20.
- Page sizing—You can change the number of rows to view on a page. You must refresh the page in order to view the new page size.
- Direct page access (only in reports)—You can browse a report screen by screen or jump to any screen number in the range by entering a screen number.

Note A report can show up to 2,000 records. If more than 2,000 records exist and you need to access the additional records, you can export all records using the data export icon.

- Data export—You can export data from a display to a comma-separated values (CSV) file, a Portable Document Format (PDF) file, or both, depending upon the display that you are using. See the icon in Table 1-4. Some reports may not be exportable.
- Print-friendly format—You can format the display for a printer and print the result from the browser. Like the display, the print-friendly browser display includes a maximum of 1,000 records (except for the IP Phone Status report which prints the total number of records). See the icon in Table 1-4.

Table 1-4 Displays—Export and Print Icons

Icon	Action
	Exports all data to either a CSV file or a PDF file.
	Reformats the displayed records into print-friendly format, and displays them in a new browser window.

- Add unmanaged devices—From the Unmanaged Devices report you can add devices into the DCR.
- Refresh—Redisplays the table page.
- Clear—Returns the table display to its original state.

Paging and Sorting Displays and Reports

The sort order for any display or report is indicated by the presence of a triangle in the column heading. A triangle pointing down indicates records in descending order, which is the default, while a triangle pointing up indicates records in ascending order.

Step 1 To sort a display, click any blue column heading label.

The first time you click a column heading on a previously unsorted column, data in that column is sorted in descending order. If you click the column heading again, the records will be sorted in the reverse order.

Note When you sort a display or report, if there are more than 1,000 records available, all records are sorted, not just those that are displayed. The first 1,000 records are displayed after sorting. For the Alerts and Events Display, the limit is 1,000 records.

Viewing Data from Reports with Over 2,000 Records

If more than 2,000 records exist, they cannot all be shown in a report. A message will be displayed to notify you when this is the case. If you want to see data for all of the records, you must export the data to a CSV or PDF file. See Exporting Data from a Display or Report, page 1-21.

You may be able to change which of the more than 2,000 records are displayed by sorting the report. See Paging and Sorting Displays and Reports, page 1-20.

Exporting Data from a Display or Report

Most displays and reports can be exported as CSV files and as PDF files (except for the Service Level View).

Note To open a PDF file, you must have Adobe Acrobat Reader 4.0 or higher installed on your client system. However, you can save a file as a PDF file even if you do not have Acrobat Reader on your system.

Step 1 Click the data export icon located on the top-right side of the display or report. See the icon in Table 1-4.

Step 2 If the dialog box Export to appears, select one of the following and click **OK**:

- CSV
- PDF

Step 3 Save the export file in one of the following ways:

- If you selected PDF and have Adobe Acrobat Reader installed on your client system, the PDF file opens. To save the PDF file, select **File > Save as** from the browser and follow the instructions to save the file.
- If you selected PDF and do not have Adobe Acrobat Reader installed, or if you selected CSV, follow the instructions to save the file.

If you use newer versions of Internet Explorer, the default settings for new security features can prevent file download windows from being displayed. For system requirements, see the *Installation Guide for Cisco Unified Operations Manager*.

Tip If you have set the custom levels of security in Internet Explorer to medium or greater, the option automatic prompt to file download is disabled. If you try to download data to a PDF or CSV file from Operations Manager to a client that does not have Adobe Acrobat Reader or Microsoft Excel installed, nothing happens. The PDF file or the spreadsheet is not displayed nor is a window that prompts you to save the file.

To enable file download windows to display, do this on your desktop:

Step 1 In Internet Explorer, select **Tools > Options**.

Step 2 Select the Security tab and click **Custom Level**.

Step 3 Scroll to Downloads and for automatic prompt to file download, select **Enable**.

Printing Displays or Reports

Step 1 Click the printer icon located at the top-right side of the display or report. See the icon in Table 1-4.

A new browser window opens, displaying the data in print-friendly format.

Step 2 Print the display from the new browser window.

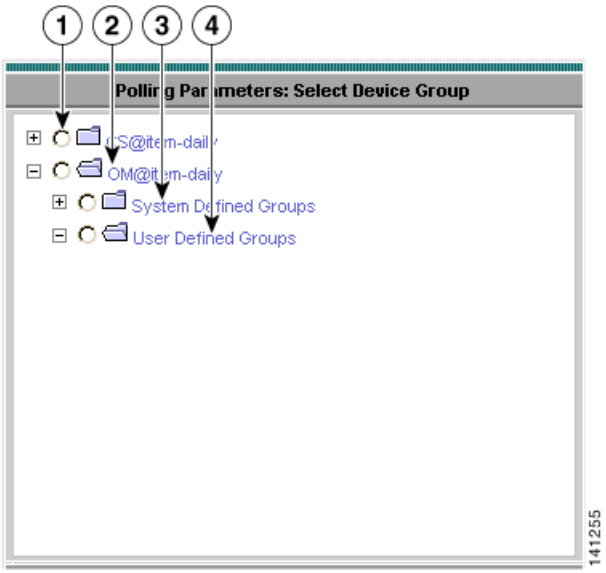
Selecting Objects and Groups

As you use Operations Manager, you will often need to select something—a device or a device group, for example—before you can view information or complete a task. Groups and devices displayed in a selector differ depending upon the application.

This topic explains what is displayed in the selectors, and how to use the selectors.

Figure 1-4 shows a device group selector as it might appear on the Polling Parameters: Select Device Group page.

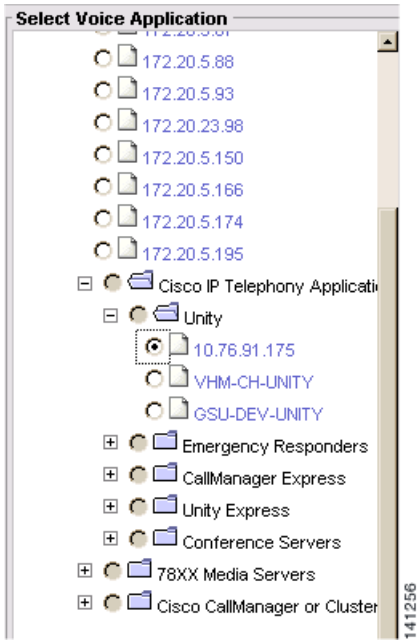
Figure 1-4 Device Group Selector as Displayed on the Polling Parameters: Select Device Group Page



1	CS@item-daily—Groups that are controlled by Common Services. Subgroups are System Defined and User Defined Groups. These groups are different from the Operations Manager groups.	**3**	System Defined Groups—The default grouping of devices in Common Services. System Defined groups cannot be deleted or edited. For a description of each system defined group, see Working with System-Defined Groups, page 17-3.
2	OM@item-daily—Groups that are controlled by Operations Manager.	**4**	User Defined Groups—Groups that you can edit or create to reflect the way you manage the network. Subgroups are System Defined, User Defined, and groups you create. (See Understanding Operations Manager Groups, page 17-1.)

Figure 1-5 shows a device group and device selector as it might appear on the Create Synthetic Test page after a user has expanded the groups and selected a Cisco Unity device. When you select the radio button for a group, you are selecting every device that is a member of the group.

Figure 1-5 Device Group and Device Selector with a Device Selected



Understanding Your User Role

When you log in to Operations Manager, you enter the username and password assigned to you by a System Administrator. Your username is associated with either a CiscoWorks role or a Cisco Secure Access Control Server (ACS) role. By default, CiscoWorks and ACS roles are the same, but an ACS

administrator can edit the ACS roles. User roles control the functions that you are allowed to see and use. If you cannot locate a function in Operations Manager, the task is not permitted for the user role. For more information, do the following:

- View the Permission Report to determine which tasks are permitted for each user role. From the Operations Manager home page, click **CiscoWorks** in the upper right-hand corner of the window. The CiscoWorks home page appears. Under Common Services, select **Server > Reports > Permission Report** and click **Generate Report**.
- View the ACS report by logging into the ACS server and selecting **Shared Profile Components**. Refer to the ACS online help for more information.

For more information, refer to these topics:

- Configuring Users (ACS and Non-ACS), page 20-20
- Using Operations Manager in ACS Mode, page 20-21

Responding to Security Alerts

The first time that you connect to the Cisco Unified Operations Manager server, you will see a Security Alert window displayed. You should install the self-signed security certificate. You should do this once, on each client system you use to access Operations Manager.

Note If you see a Security Alert Window with a message that the certificate has expired, you should contact a user with System Administrator privileges to create a self-signed security certificate. Then install it.

Note If you do not install the self-signed security certificate, you may not be able to access some Operations Manager application pages.

Step 1 Click the **View Certificates** button on the Security Alert window. The Certificate window is displayed.

Step 2 Install the certificate as follows:

a. Click the **Install Certificate** button. The Certificate Import Wizard window is displayed.

b. Follow the instructions provided by the Certificate Import wizard.

Responding to Messages About Device Limits

If you exceed your server's device limit, Operations Manager will continue to work, but it will not allow you to import any more devices. What happens next depends on whether you use automatic synchronization between the Device and Credentials Repository (DCR) and the Operations Manager inventory, or you add DCR devices to the Operations Manager inventory on a device-by-device basis:

- Manual synchronization with DCR—When you use the Device Selector page to move devices from the DCR into Operations Manager, Operations Manager will display a popup message warning you that you cannot import any more devices (see Understanding the Device and Credentials Repository, page 16-4).

- Automatic synchronization with DCR—You will notice that devices are not appearing on Operations Manager pages. You can check the license log for more information (see Accessing and Deleting Log Files, page 20-13).
- For information about device-based licensing, see *Installation Guide for* Cisco Unified Operations Manager.

PART 2

Monitoring Dashboard Displays

CHAPTER 2

Using the Service Level View

These topics describe how to use the Service Level View:

Understanding Service Level and Unified CM Express Views

Cisco Unified Operations Manager's Service Level View displays a logical top-level topology view of your IP telephony implementation. This logical view focuses on call control relationships.

The Service Level View shows Cisco Unified Communications Manager clusters and route groups and route lists in the clusters; Cisco Unified Communications Manager Express clouds, associated gateways, gatekeepers, application servers, and Cisco Unified Contact Centers (and their logical groupings); and SRST-enabled devices; as well as each component's registration status with Cisco Unified Communications Manager. Depending on the numbers of clusters or devices, the relationships may be displayed in a graphic view or a flat table format. Instances of Cisco Unified Communications Manager Express (and their logical groupings) can be viewed by selecting the CME cloud or selecting Unified CM Express Views from the dashboard. Selecting the Unified CM Express Views menu options allows you to access your Communications Manager Express views without launching the Service Level View.

The Service Level View map is designed so that you can set it up and leave it running, providing an ongoing monitoring tool that signals you when something needs attention. Service Level View and Unified CM Express View reports are snapshots of live data and can be manually refreshed to post the most accurate data available. When a fault occurs in your network, Operations Manager generates an event or events that are rolled up into an alert. If the alert occurs on an element, it is shown on the Service Level View.

Note When changing a Cisco Unified Communications application's registration from one Cisco Unified Communications Manager cluster to another, you must remove the registration of the application to the old Cisco Unified Communications Manager cluster in both the application and the old Cisco Unified

Communications Manager cluster. If you do not do this, registration of the application with the old Cisco Unified Communications Manager cluster will continue to appear in the Service Level View in the Down state.

The Service Level View uses tree-based, map-based, and table report displays (depending on the number of devices). If there is an excessive number of Unified Communications Manager clusters or devices that may be too slow to display, use the tree view to navigate to various Unified Communications Manager clusters so that data will display in a flat table format. The table format displays all the IP telephony clusters present in your network. Use the map view to display a logical grouping of device groups and to organize what you want to see. There is one default view called All IP Communications Devices. You can also create your own user-defined views. (For details on managing views, see Managing Views, page 6-1.)\

The Unified CM Express View displays all managed Unified Communications Manager (CM) Express devices and associated Cisco Unity devices in a global-level report. For more information on this report, see Using the Unified Communications Manager Express Report, page 2-16.

The All IP Communications Devices view contains all the Cisco Unified Communications Manager clusters (except for the Unified Communications Manager Express devices), all route lists defined for the cluster, and all the devices associated with the clusters in your network. You cannot add to or edit this default view. The All IP Communications Devices view is what you see the first time you launch the Service Level View.

Note Operations Manager displays route lists and route groups for Cisco Unified Communications Manager version 4.0 and later.

The user-defined views that you create using group management (see Working with User-Defined Groups, page 17-9) can contain any clusters or device groups that you want.

You can specify any user-defined view as the default view, meaning you can specify what view should appear when you open the Service Level View.

You can use the Service Level View to:

- Display a logical or neighbor topology view of your IP telephony deployment. See Starting the Service Level View, page 2-2.
- Navigate from the tree view by selecting clusters to view reports that provide cluster data in a tabular report. See Viewing Large Numbers of Devices and Clusters from the Service Level View, page 2-15.
- View and act on alerts for devices. See Getting Alert Details Using the Service Level View, page 2-14.
- Run other Operations Manager tools. See Launching Operations Manager Tools from the Service Level View, page 2-21.
- Launch administration pages for devices. See Launching Administration Pages for Devices, page 2-31.
- Using the Unified Communications Manager Express Report, page 2-16

Starting the Service Level View

To start the Service Level View, select **Monitoring Dashboard > Service Level View**. Figure 2-1 shows an example of a Service Level View.

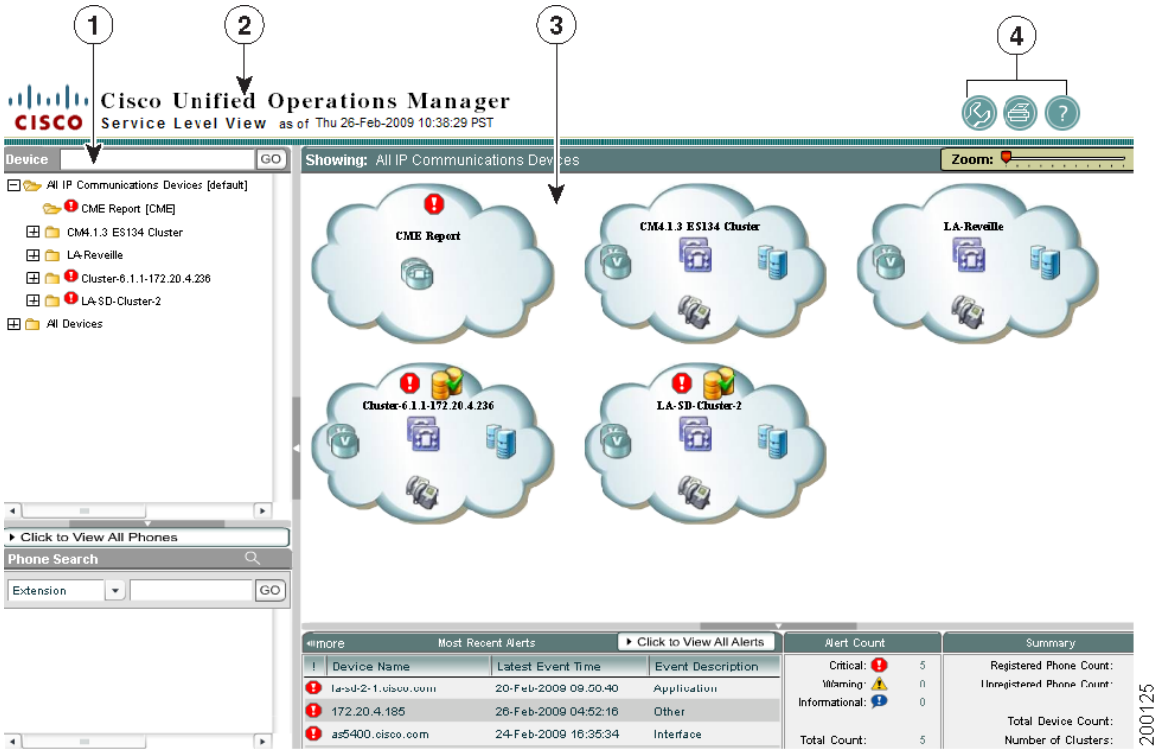
Understanding the Layout of the Service Level View

These topics provide details about the information in the Service Level View:

- Working with the View Pane, page 2-5
- Working with the Map Display Pane, page 2-7
- Setting a Default Service Level View, page 2-9
- Starting the Connectivity Detail View, page 2-10
- Service Level View Legend, page 2-10

Figure 2-1 shows an example of the Service Level View.

Figure 2-1 Service Level View



1	View pane. See View Pane, page 2-4.	**3**	Map display pane. See Map Display Pane, page 2-5.
2	Launch information and view status bar area. See Launch Information and View Status Bar Area, page 2-4.	**4**	Window tools area. See Window Tools Area, page 2-5.

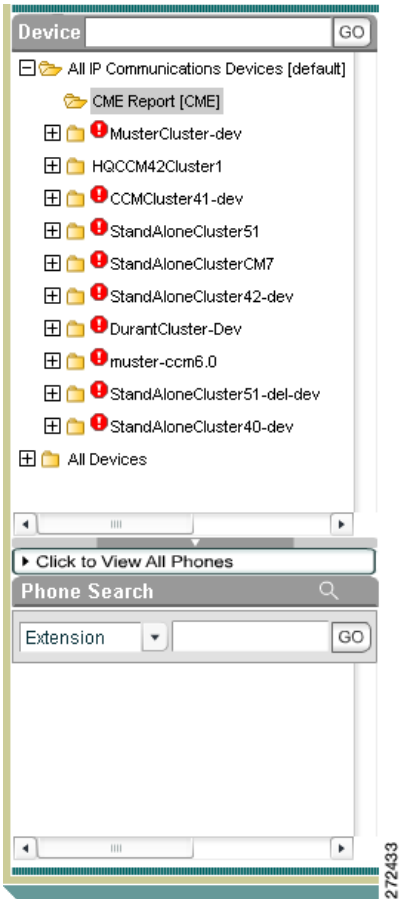
View Pane

The view pane lists the currently available views in a tree-based format. By default, the All IP Communications Devices view is shown, and cannot be deleted from your Service Level View. You can create user-defined views that appear in the view pane. Views must be created and activated before they will be shown in the Service Level View. (To create and activate a view or remove an unwanted view from your display, see Managing Views, page 6-1.)

The current view is highlighted in the view pane. The contents of the current view are shown in a map-based format in the map display pane to the right of the view pane. For details on working with the view pane, see Working with the View Pane, page 2-5.

Figure 2-2 shows two active views; the current view is All IP Communications Devices.

Figure 2-2 Service Level View—View Pane



Launch Information and View Status Bar Area

The launch information area shows the current time on the server when the Service Level View display is being viewed.

The view status bar lists the selected view, which is shown in the map display pane.

Map Display Pane

The map display pane shows a map-based view of the current selected view. It also provides a summary of the view. The summary lists alert information, and the number of phones and devices in the selected view. For details on working with the map display pane, see Working with the Map Display Pane, page 2-7.

Window Tools Area

The top-right corner of the Service Level View contains available tools buttons. All buttons are described in Table 2-1.

Table 2-1 Service Level View—Window Tool Buttons

Icon	Meaning	Described in...
	Opens additional tools, such as the following: • Alert History. • Campus Manager.	Getting All Stored Information on an Alert, page 12-4 Launching Campus Manager—Using the Service Level View, page 2-33
	Opens a printer-friendly version for printing.	Printing Displays or Reports, page 1-22
	Opens the Operations Manager online help.	Using Help, page 1-18

Working with the View Pane

The view pane lists the current active views. The first time you open the Service Level View, the All IP Communications Devices view is displayed. If you do not want All IP Communications Devices to be your default view, you can change it. (See Setting a Default Service Level View, page 2-9.)

If you have created any user-defined groups and enabled the views for the Service Level View, they will also appear in the view pane. (For details on managing views, see Managing Views, page 6-1.)

To drill down to an object in the view pane, click the object; the devices under the object are displayed in either a map-view or table report depending on the number of devices or objects. Large objects with several hundred devices are displayed in a report format to improve performance and ease of use. To understand the types of reports available from the Service Level View, see Viewing Large Numbers of Devices and Clusters from the Service Level View, page 2-15.

You can also see the neighbor connectivity of devices, by using the right-click menu. For every selected device, the next-hop devices physically connected are displayed. See Starting the Connectivity Detail View, page 2-10.

Note If you want to locate a specific device or phone, you can use the search options available in the view pane. Figure 2-2 shows an example of the view pane.

Check boxes in the view pane enable you to act on multiple devices, suspending them, resuming them (if they are suspended), or deleting them.

Using the Search Tool to Locate a Device

In the Service Level View you can search for a specific device.

Step 1 Select **Monitoring Dashboard > Service Level View**.

Step 2 In the search field at the top of the view pane, enter a name or IP address.

Step 3 Click **Go**.

Using the Search Tool to Locate a Phone, Video Endpoint, or TelePresence Endpoint

In the Service Level View you can search for a specific phone, video endpoint, or TelePresence endpoint. When you search for the TelePresence endpoint, two results are displayed: one is the phone and the other is the TelePresence endpoint for the same extension.

Note Video endpoints are displayed only after you have the appropriate software license.

When you click on a phone from the phone/video endpoint search results, the map display pane displays a drilled-down view, with the phone highlighted. The phone will have a logical link to the Cisco Unified Communications Manager to which it is registered.

The following limitations exist for phone search:

- Phone search displays a maximum of 100 phones.
- If more than 100 phones are present, a warning message displays.
- If a matching phone is connected to a Communications Manager Express (CME) device (rather than CCM), then you must use the phone search tree to launch the tools for those phones that display under CME clouds. After Operations Manager 2.1, clicking on the phone no longer displays the phone in the map view; the CME map view is now converted to a table formatted CME report.

Step 1 Select **Monitoring Dashboard > Service Level View**.

Step 2 In the search field located at the bottom of the view pane, select whether you want to search by extension number, IP address, or MAC address. The search allows wild card entries for all of these entries.

Step 3 Enter the appropriate number for the phone.

Step 4 Click **Go**.

Launching an All IP Phones/Lines Report from the Service Level View

Note To launch a report that includes video endpoints, see Generating Video Phone Inventory Reports, page 13-30.

Step 1 Select **Monitoring Dashboard**.

Step 2 In the IP Phone Status pane, select **Click to View All Phones** in the view pane. The All IP Phones/Lines report opens in another window.

For more information, see Understanding IP Phone Inventory Reports, page 13-11. For information on how phone counts are displayed in Operations Manager windows, see How Are Phone Counts Displayed in Views and Reports?, page 1-19.

Launching Service Level View Reports for Large Network Objects

From the Monitoring Dashboard you can access Unified Communications Manager clusters and the devices associated with the clusters in a tabular report.

Step 1 To select Unified Communications Manager Express devices, select **Monitoring Dashboard > Unified CM Express View**. For more details, see Using the Unified Communications Manager Express Report, page 2-16.

Step 2 To select all other IP Communications devices, select **Monitoring Dashboard > Service Level View**. The All IP Communications Devices view (or other customized default view) displays.

Step 3 Select one of the following to access tabular reports:

- A Unified Communications Manager cluster. When you make this selection, similar devices display as a single report icon per cluster or per Unified Communications Manager:
  - MGCP
  - H323
  - APP (application server)
  - SIP APP
  - SRST
- A Unified Communications Manager cluster with unmanaged devices discovered by SIR. When you make this selection, an Unmanaged Devices report displays. No unmanaged devices will be present in the Service Level View map or in the Unified Communications Manager cluster reports.

Note In a cluster that has a primary and secondary Cisco Emergency Responder (CER), Service Level View displays only the primary Cisco Emergency Responder if the Unified Communications Manager is version 4.x. Both the primary and secondary responders are shown if the Unified Communications Manager is version 7.x.

Working with the Map Display Pane

The map display pane shows the registration status of IP telephony devices as well as the SRST status of SRST-enabled devices. This information is displayed in a map-based view. You can drill down to an object in the display pane by clicking the object. The devices under the object are then displayed. Depending on the object you select, the data may be displayed in a map-based view or a report page.

The top view shows Cisco Unified Communications Manager clusters (previously referred to as Communications Manager clusters), Cisco Unified Communications Manager Express groups, and Cisco Unified Contact Center solution groups. If objects are excessively large, they are displayed in a report page when selected. For objects that are easily displayed, you will see the IP telephony devices registered in the group along with registration status.

For Cisco Unified Communications Manager Express, you will see only one Cisco Unified Communications Manager Express cloud in the top level view. You can drill down to see a report that contains the individual Cisco Unified Communications Manager Express details. If there are no Unified Communication Manager Express (CMEs) machines present, then the CME cloud does not display.

If you mouse over the CME cloud, the following details display:

- Total number of CMEs
- Total number of CUEs
- CMEs with Critical Alert
- CUES with Critical Alert
- CME-CUE Links Down

For Cisco Unified Contact Center, the top-level view displays only one Unified CCE cloud. This is to let you know that the system has a Unified CCE solution. When you drill down on this cloud, the individual Unified CCEs appear again as clouds. Drilling down on these clouds shows the individual devices with relevant information.

You can also see the neighbor connectivity of devices, by using the right-click menu. For every selected device, the next-hop devices physically connected are displayed. See Starting the Connectivity Detail View, page 2-10.

Note To enlarge or reduce the size of the map display, use the size slider at the top of the pane. The size slider can be used in either the logical topology view, or the connectivity detail view.

From within the map display pane, you can launch several Operations Manager tools, external applications, reports, and device administration pages.

To access these tools and applications, right-click on an object in the map display and the available options are displayed in a menu box. For details on starting the Operations Manager tools, see Launching Operations Manager Tools from the Service Level View, page 2-21. For details on launching administration pages, see Launching Administration Pages for Devices, page 2-31.

The map display pane also provides a summary of the alerts for the current view at the bottom of the pane (see Working with the Map Display Pane, page 2-7).

Figure 2-3 provides an example of a Service Level View map display.

Figure 2-3 Service Level View Map Display Pane

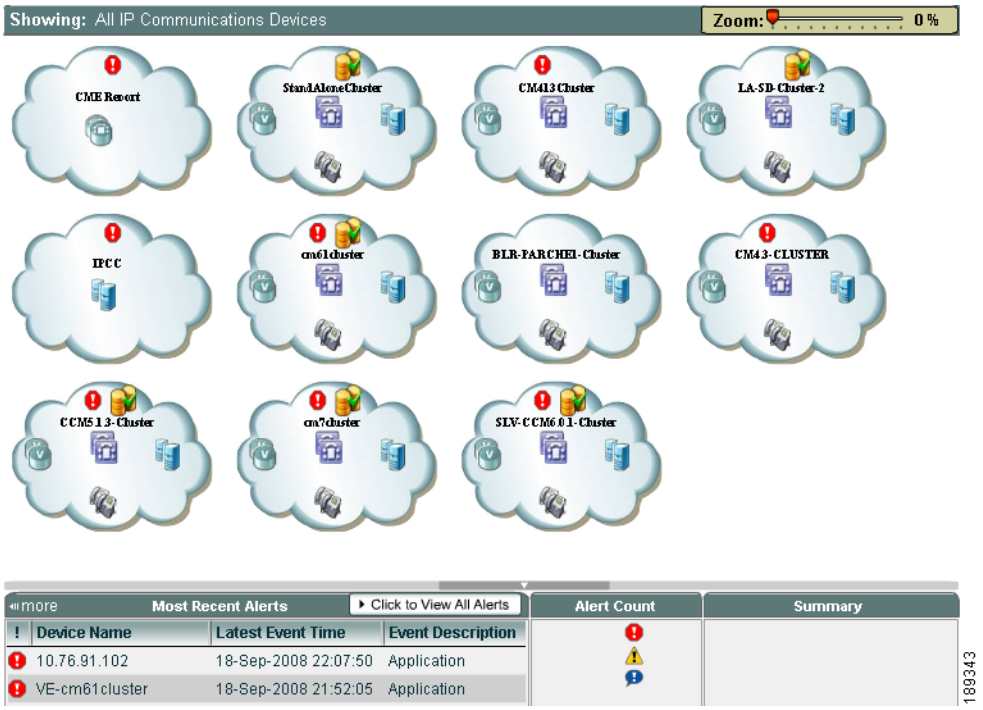


Table 2-2 Map Display Pane—Summary

Button/Heading	Description
Most Recent Alerts	Device name and description.
Click to View All Alerts	Opens the Alerts and Events display.
Alert Count	Lists the number of each type of alert and a total count.
Summary	Lists the number of phones, devices, and clusters.

Setting a Default Service Level View

You can specify any user-defined group as the default view.

Step 1 The user-defined group must be enabled as a view for the Service Level View. For details on enabling views, see Creating a View, page 6-2.

Step 2 In the view pane, locate the user-defined view that you want to make the default view.

Step 3 Right-click on the view.

Step 4 From the menu, select **Set As Default View**.

Step 5 In the information box, click **OK**.

Starting the Connectivity Detail View

The Connectivity Detail View provides a topology view of the neighboring connectivity for the selected devices. For every selected device, the next-hop devices that are physically connected appear. By default the hop count is 1 and cannot be changed.

Step 1 In either the view pane or the map display pane, right-click on the device for which you want to view the connectivity detail.

Step 2 From the menu, select **Connectivity Details**.

The Connectivity Detail View appears.

Working with the Connectivity Detail View

You can use the Connectivity Detail View the same way you use the Map Display Pane (see Working with the Map Display Pane, page 2-7).

Service Level View Legend

Table 2-3, Table 2-4, and Table 2-5 describe the icons, the link status, and the database replication status that can appear in the Service Level View.

Table 2-3 Device Icons for the Service Level View

Icon (Monitored)	Icon (Not Monitored)	Icon (Alert)	Description
			Cisco Unified Communications Manager
	—	—	Cisco Unified Communications Manager Group
			Cisco Unified Communications Manager Express
	—	—	Cisco Unified Communications Manager Express Group

Table 2-3 Device Icons for the Service Level View (continued)

Icon (Monitored)	Icon (Not Monitored)	Icon (Alert)	Description
			Cisco Unified Communications Manager Express/SRST
	—		Voice application server
			Voice gateway
	—	—	IP phone
		—	Group of IP phones
			Cisco Unified Contact Center Enterprise or Unified CCE (formerly IPCC)
			Cisco Unity
			Cisco Unity Express
			Router
			Gatekeeper

Table 2-3 Device Icons for the Service Level View (continued)

Icon (Monitored)	Icon (Not Monitored)	Icon (Alert)	Description
			SIP endpoint
			Switch
			Cisco 1040 Sensor
	—	—	Cisco TelePresence Manager
			Cisco TelePresence endpoints
			MeetingPlace Express
			Rich media appliance
	—	—	Virtual node
	—	—	Virtual node cluster
	—	—	Route list

Table 2-3 Device Icons for the Service Level View (continued)

Icon (Monitored)	Icon (Not Monitored)	Icon (Alert)	Description
		—	Route list cloud This icon is also used to represent a route group on the Route List report. See Viewing the Route List and Route Group Report, page 2-26
	—	—	IP phone group with TelePresence endpoint
	—	—	Voice router group This icon appears in the first-level cloud view and represents the capability of the cluster in the cloud.
	—	—	Group of IP phone applications. This icon appears in the first-level cloud view and represents the capability of the cluster in the cloud.

Table 2-4 Link Type Description for the Service Level View

Link	Description
	Physically connected, but the connection is down.
	Physically connected, but one of the multiple connections is down.
	Physically connected, and the connection is up.
	Logically connected, but registration status is down.
	Logically connected, but one of the multiple connections' registration status is down.
	Logically connected, and registration status is up.

Table 2-4 Link Type Description for the Service Level View (continued)

Link	Description
	A WAN link connecting a remote SRST to a central Cisco Unified Communications Manager site is down.
	A WAN link connecting a remote SRST to a central Cisco Unified Communications Manager site is up.
	Logically related, but the registration status is unavailable.

Table 2-5 Database Replication Status for Cisco Unified Communications Manager Clusters for the Service Level View

Database Icon	Description
	Database replication successful between Cisco Unified Communications Managers in the cluster.
	Database replication error between Cisco Unified Communications Managers in the cluster.

Getting Alert Details Using the Service Level View

In the Service Level View, as shown in Figure 2-1, an alert icon appears next to the device when an alert is generated on the device. The alert severities are critical, warning, or informational. Table 2-6 shows the alert icons.

When an alert is generated, it remains in the Service Level View until it is cleared. The cleared alert is removed from the Alerts and Events display after you invoke the Operations Manager purge operation, which determines that the alarm has been in the cleared state for 30 minutes or longer (from the time of the purge interval). While the alert is in the display, if any of its events recur, the alert is updated.

Table 2-6 shows the alert icons.

Table 2-6 Alert Icons

Icon	Description
	Critical
	Warning
	Informational: Unidentified Trap alert

The Service Level View also lists the number of alerts in the map display pane for the current view (see Working with the Map Display Pane, page 2-7).

How Do I Get Alert Details Using the Service Level View?

You can right-click on the device that has the alert icon displayed next to it, and open an Alert Details page. See Viewing Alert Information, page 2-22.

If you want to see all the alerts for a view, you can open an Alert and Events display by clicking the **Click to View All Alerts** button at the bottom of the map display pane. You can then locate the devices for which you want to view the alert information. See Getting Alert Details Using the Alerts and Events Display, page 3-7.

Viewing Large Numbers of Devices and Clusters from the Service Level View

To view reports that contain large numbers of devices and clusters, there are several options in Operations Manager.

The Service Level View (SLV) shows the logical relationship between all voice devices present in Operations Manager. Because of the need to support hundreds of Unified Communications Manager clouds or hundreds of gateways in a single cluster, the Service Level View provides separate reports that display all device clusters and excessive numbers (over 500) of gateways, APP servers, SIP-APP servers, H323 devices, SRST devices, or Media Gateway Control Protocol (MGCP) devices in a Communications Manager cluster in a flat table format. This report is static and can be manually refreshed.

The Unified CM Express View shows the relationships between Unified CM Express, Unity Express, and associated phones. Use Monitoring Dashboard > Unified CM Express View to view a report with this data.

If you drill down into cloud clusters, and if the number of devices in a cluster is larger than a specified limit, the devices display in a flat table format. If the devices do not exceed the limit, they are displayed graphically.

The default device count limit for reporting is 50. When the number of devices in a cluster (including CCMS) exceeds 50, report icons appear. To change this limit to any value less than 50, modify the DEVICE_MAX_COUNT_FOR_STARTING_REPORT parameter in the CSCOpx\MDC\tomcat\webapps\triveni\topo_flash\topo.properties file.

You can access the following reports using Service Level View or Unified CM Express View:

- Using the Unified Communications Manager Express Report, page 2-16
- Using the MGCP and APP Server Reports, page 2-18
- Using the H323, SIP APP, or SRST Report, page 2-19
- Using the Unmanaged Devices Report, page 2-21

Using the Unified Communications Manager Express Report

The Unified Communications Manager (CM) Express report is a global-level report for all Unified Communications Manager Express devices (CMEs) in Operations Manager. Table 2-7 describes the contents of the Unified CM Express Report.

Table 2-7 Unified Communications Manager Express Report

Field	Description	
CME Name	Route list, route group, or gateway name. The gateway name can be an IP address or a DNS name.	
CME IP Address	IP address for a gateway.	
CME Alert Status	Indicates the severity of an alert, if an alert is present.	
		Critical
		Warning
		Informational Unidentified Trap alert
	(no icon)	Informational (for all other alerts)
	---	No alert present.
Cisco Unity Express (CUE) Registration	The link status between the Communications Manager Express and the Unity Express server. It indicates whether or not Communications Manager Express is still in communication with the voice mail server (CUE).	
CUE Name	Name or IP address for Unity Express.	
CUE IP Address	IP address for Unity Express.	
CUE Alert Status	Indicates the severity of an alert, if an alert is present. See CME Alert Status for icon descriptions.	
Phone Count	Number of registered and unregistered phones associated with this cluster or Communications Manager. For information on how phone counts are displayed in Operations Manager windows, seeHow Are Phone Counts Displayed in Views and Reports?, page 1-19.	

Table 2-7 Unified Communications Manager Express Report

Field	Description	
More Details		
Device State	Shows whether the device is unresponsive or unreachable. (Service Level View previously identified these states with red and gray colors). The values for this field include: • Unresponsive:Active • Unresponsive:Clear • NA—Not applicable (NA). Displays when there is no CUE in the CME cloud or when the other values are not unresponsive:active or clear. Can also display if device is healthy.	
Capability	Lists device features that are applicable to this device, such as voice gateways, Communications Manager Express, voice services, IPSLA, H323, SIP, and routers.	
Managed State	Lists the state the devices are in, from the following possibilities. Is a combination of Device State and Managed State. See Table 16-2 for details on device states. Note that for the CME report only, the unreachable event field overrides the managed state.Other reports will continue to use Device State field to show an unreachable state of the device.	
	Managed	The device has been successfully imported, and is fully managed by Operations Manager.
	Partially Managed	The device has been successfully imported by some of the data collectors[1] in Operations Manager, but not all. If a device is in this state, you should take action to ensure that the device becomes monitored.
	Suspended	Monitoring of the device is suspended.
	NA	Signifies that the device is responsive and has no reachability problems.
CUE Device State	Cisco Unity Express device state. The values for this field include: • Unresponsive:Active • Unresponsive:Clear • NA—Not applicable (NA). Displays when there is no CUE in the CME cloud or when the other values are not unresponsive:active or clear.	
CUE Capability	Cisco Unity Express active features. When there is no CUE in the CME cloud, this field displays NA.	
CUE Managed States	Cisco Unity Express managed device state. Is a combination of CUE Device State and CUE Managed State. When there is no CUE in the CME cloud, this field displays NA.	

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

Using the MGCP and APP Server Reports

MGCP or APP Server reports are specifically launched for every Communications Manager in the cluster.

These reports display information on devices which are registered directly to a particular Communications Manager. MGCP and APP Server devices are included in this report. Table 2-8 contains the details on the MGCP and APP Server reports.

Table 2-8 Service Level View Reports—MGCP and APP Server Reports

Field	Description	
Device Name	Route list, route group, or gateway name. The gateway name can be an IP address or a DNS name.	
Device IP Address	IP address for a gateway.	
Device Alert	Indicates the severity of an alert, if an alert is present.	
		Critical
		Warning
		Informational Unidentified Trap alert
	(no icon)	Informational (for all other alerts)
	---	No alert present.
Device Registration Status with CCM	The link status between the Communications Manager and the device.	
More Details		
Device Capability	Lists device features that are applicable to this device, such as voice gateways, voice services, IPSLA, and routers.	
Protocol	Protocol or gateway. Always displays NA in CME and SRST reports but displays corresponding value in other reports.	
Device State	Shows whether the device is unresponsive or unreachable. (Service Level View previously identified these states with red and gray colors). The values for this field include: • Unresponsive:Active • Unresponsive:Clear • NA—Not applicable (NA). Displays when there the other values are not unresponsive:active or clear. Can also display if device is healthy.	
Managed State	Lists the state the devices are in, from the following possibilities.	

Table 2-8 Service Level View Reports—MGCP and APP Server Reports

Field	Description	
	Managed	The device has been successfully imported, and is fully managed by Operations Manager.
	Partially Managed	The device has been successfully imported by some of the data collectors[1] in Operations Manager, but not all. If a device is in this state, you should take action to ensure that the device becomes monitored.
	Suspended	Monitoring of the device is suspended.
	NA	Signifies that the device is responsive and has no reachability problems.
Device Alert Status	Device state. The values for this field include: • Unresponsive:Active • Unresponsive:Clear • NA—Not applicable (NA). Displays when there the other values are not unresponsive:active or clear.	
Summary Information	Summary information about number of gateways with alerts; number of down registrations; total number of gateways managed; this information is shown at the top of the report.	
Device Tools (click Device Name)	Clicking on the device name allows you to select the various device tools available.	

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

Using the H323, SIP APP, or SRST Report

This report is for all types of devices which can register with the cluster itself without associating itself with any Communications Manager in the cluster. H323, SIP-APP, GK and SRST devices fall under this category. Table 2-9 contains the details on the MGCP and APP Server reports.

Table 2-9 Service Level View Reports—H323, SIP APP and SRST Reports

Field	Description
Device Name	Route list, route group, or gateway name. The gateway name can be an IP address or a DNS name.
Device IP Address	IP address for a gateway.

Table 2-9 Service Level View Reports—H323, SIP APP and SRST Reports

Field	Description	
Device Alert	Indicates the severity of an alert, if an alert is present.	
		Critical
		Warning
		Informational Unidentified Trap alert
	(no icon)	Informational (for all other alerts)
	---	No alert present.
Device Registration Status with Cluster	The link status between the device and the cluster.	
More Details		
Device Capability	Lists device features that are applicable to this device, such as voice gateways, voice services, IPSLA, H323, SIP, and routers.	
Protocol	Protocol or gateway. Always displays NA in SRST reports, but displays the corresponding value in other reports.	
Device State	Shows whether the device is unresponsive or unreachable. (Service Level View previously identified these states with red and gray colors). The values for this field include: • Unresponsive:Active • Unresponsive:Clear • NA—Not applicable (NA). Displays when the other values are not unresponsive:active or clear. Can also display if device is healthy.	
Managed State	Lists the state the devices are in, from the following possibilities.	
	Managed	The device has been successfully imported, and is fully managed by Operations Manager.
	Partially Managed	The device has been successfully imported by some of the data collectors[1] in Operations Manager, but not all. If a device is in this state, you should take action to ensure that the device becomes monitored.
	Suspended	Monitoring of the device is suspended.
	NA	Signifies that the device is responsive and has no reachability problems.
Device Alert Status	Device state. The values for this field include: • Unresponsive:Active • Unresponsive:Clear • NA—Not applicable (NA). Displays when the other values are not unresponsive:active or clear.	

Table 2-9 Service Level View Reports—H323, SIP APP and SRST Reports

Field	Description
Summary Information	Summary information about number of gateways with alerts; number of down registrations; total number of gateways managed; this information is shown at the top of the report.
Device Tools (click Device Name)	Clicking the device name allows you to select the various device tools available.

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

Using the Unmanaged Devices Report

This report contains all the unmanaged devices under a particular cluster. You can select any number of devices and add them to the cluster for management. Table 2-10 contains details displayed in this report:

Note When a device or its components are unmanaged, then the detailed device view would either show the last polled value or N/A, depending on the type of counter. When the device is later managed, these counters would show the newly polled values in the next poll cycle.

Table 2-10 Unmanaged Devices Report

GUI Elements	Description
Field	
Device Name/Device IP Address	Name of unmanaged device.
Device Type	Device is recognized as this type; for example, H323.
Linked to	Cluster or Unified Communications Manager to which this device is associated.
Button	
Search	Locate device information based on a string.
Clear/Refresh	Clear removes search results from the report and loads the original report. Refresh reloads the report from the server. If new data is displayed, any check box selections are reset.
Add	Adds unmanaged devices into the cluster to which the device is associated.

Launching Operations Manager Tools from the Service Level View

The Service Level View can be a central launching point for using Operations Manager. You can access several Operations Manager tools as well as external applications through the Service Level View.

Note You will have access to these tools only if you have proper authorization, according to either the CiscoWorks security model or CiscoSecure Access Control Server security model, depending on which your system is using. See Configuring Users (ACS and Non-ACS), page 20-20.

You can do the following from the Service Level View:

- View alert information for a device (see Viewing Alert Information, page 2-22).
- View alert and event history for a device (see Viewing Alert History, page 2-23).
- View device information (see Viewing Device Information, page 2-23).
- View associated phones for a Cisco Unified Communications Manager (see Viewing Associated Phones, page 2-23).
- View route lists and the route groups and gateways contained in them (see Viewing the Route List and Route Group Report, page 2-26).
- Launch the Path Analysis tool (see Launching the Path Analysis Tool, page 2-24).
- View performance monitoring (see Viewing Performance Monitoring, page 2-25).
- Set up synthetic tests on a device (see Setting Up Synthetic Tests, page 2-27).
- Set up node-to-node tests on a device (see Setting Up Node-To-Node Tests, page 2-28).
- Set up SRST monitoring for a device (see Setting Up SRST Monitoring, page 2-28).
- Edit polling and threshold settings (see Configuring Threshold Settings, page 2-29 and Configuring Polling Settings, page 2-29).
- Create user-defined groups (see Creating User-Defined Groups, page 2-31).
- Launch administration pages for devices (see Launching Administration Pages for Devices, page 2-31).
- Launch external applications (see Launching External Applications—Using the Service Level View, page 2-32).

Viewing Alert Information

Step 1 In either the view pane or the map display pane, right-click on the device for which you want to view alert information.

Step 2 From the menu, select **Alert Details**.

Note If the tool or application you want to launch does not appear in the menu, click the **More Tools** menu item. This launches a secondary menu.

The Alert Details page for the selected device appears. For a description of the Alert Details page, see Starting the Alert Details Page, page 3-9.

Viewing Alert History

Step 1 In either the view pane or the map display pane, right-click on the device for which you want to view alert history.

Step 2 From the menu, select **Alert History**.

Note If the tool or application you want to launch does not appear in the menu, click the **More Tools** menu item. This launches a secondary menu.

An Alert History report for the selected device appears. For a description of the Alert History report, see Understanding the Alert History Report, page 12-10.

Viewing Device Information

Step 1 In either the view pane or the map display pane, right-click on the device for which you want to view information.

Step 2 From the menu, select **Detailed Device View**.

Note If the tool or application you want to launch does not appear in the menu, click the **More Tools** menu item. This launches a secondary menu.

The Detailed Device View for the selected device appears. For a description of the Detailed Device View, see Understanding the Layout of the Detailed Device View, page 3-20.

Viewing Associated Phones

You can view an associated phones report. If you are viewing an associated phones report for a switch, the report displays the phones that are connected to the switch. If you are viewing an associated phones report for a Cisco Unified Communications Manager or Cisco Unified Communications Manager Express, the report displays all the phones that are registered to the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express.

Note The Associated Phones report can be launched from either the Alert Details page, or from the Detailed Device View page using the Tools Launch menu. (See Understanding the Layout of the Alert Details Page, page 3-11, or Understanding the Layout of the Detailed Device View, page 3-20.)

Step 1 In either the view pane or the map display pane, right-click on the phone, Cisco Unified Communications Manager, or Cisco Unified Communications Manager Express for which you want to view associated phones.

Step 2 From the menu, select **Phone Details**.

Note If the tool or application you want to launch does not appear in the menu, click the **More Tools** menu item. This launches a secondary menu.

An Associated Phones report for the selected device appears. For a description of the IP Phone Detail reports, see Understanding IP Phone Inventory Reports, page 13-11.

Launching the Path Analysis Tool

The Path Analysis tool provides hop-by-hop latency information for all the Layer 3 devices. It uses the ping path echo operation of IP SLA. The Path Analysis tool can be launched for any IP SLA-enabled device.

You can select an IP SLA-enabled source and/or a destination device from either the view pane or the map display pane and launch the tool.

Note The Path Analysis tool can also be launched from the Service Quality Alert Detail page using the Tools Launch menu. (See Using the Service Quality Alert Details Display, page 4-6.)

Step 1 In either the view pane or the map display pane, right-click on the device for which you want to run the Path Analysis tool.

Note To select multiple devices, use the Ctrl-click operation to select the devices, and then Ctrl-right click to open the menu.

Step 2 From the menu, select **Path Analysis Tool**. The Path Analysis Tool page appears.

Note If the tool or application you want to launch does not appear in the menu, click the **More Tools** menu item. This launches a secondary menu.

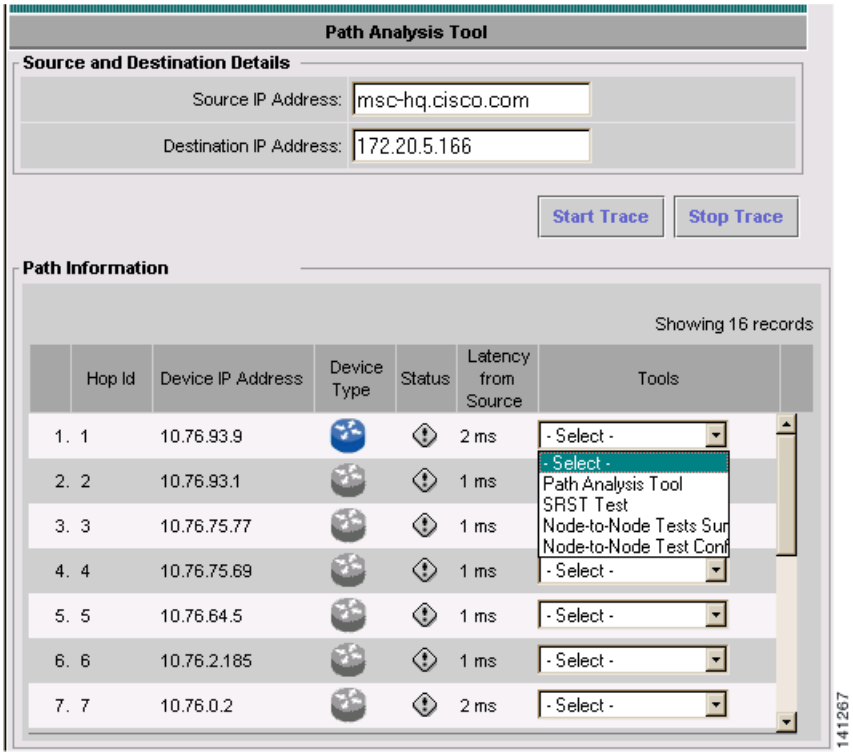
Step 3 Verify that the source and destination devices are correct.

Step 4 Click **Start Trace**. The Credentials for Source Device dialog box appears.

Step 5 Enter source devices' credentials.

Step 6 Click **OK**. The tool runs and the results are displayed on the Path Analysis Tool page. Figure 2-4 shows an example of a Path Analysis tool.

Figure 2-4 Path Analysis Tool



Heading	Description
Hop ID	Hop ID.
Device IP Address	Device's IP address.
Device Type	Icon representing the type of device.
Status	Icon representing the status of the device.
Latency from Source	Latency in milliseconds.
Tools	Other Operations Manager tools that you can run on the device. This list will vary depending on the device. Some examples are: • Node-to-Node tests • SRST tests

Viewing Performance Monitoring

You can select and examine changes in network performance metrics. You can select, display, and chart network performance data in real time.

Step 1 In either the view pane or the map display pane, right-click on the device for which you want to view performance.

Step 2 From the menu, select **Performance**. The Select Metrics dialog box appears.

Note If the tool or application you want to launch does not appear in the menu, click the **More Tools** menu item. This launches a secondary menu.

Step 3 Select the metrics you want to graph. The metrics must have the same units.

Step 4 Click **View Graph**. A performance and capacity planning graph appears. For details about working with the performance graphs, see How to Use Performance Graphs, page 7-1.

Viewing the Route List and Route Group Report

Note Operations Manager displays route lists and route groups for Cisco Unified Communications Manager version 4.0 and later.

Step 1 In the map view pane, click the Route List Cloud icon. A report window opens, displaying the information in Table 2-11.

Note The Route List report window must be manually refreshed.

Table 2-11 Route List and Route Group Report

Field	Description	
Left-most column (contains icons)	• Route List—Expand to view the route groups in the route list. • Route Group—Expand to view the gateways in the route group. • Voice Gateway—View the data for the gateway.	
Name	Route list, route group, or gateway name. The gateway name can be an IP address or a DNS name.	
Alert Status	Indicates the severity of an alert, if an alert is present.	
		Critical
		Warning
		Informational Unidentified Trap alert
	(no icon)	Informational (for all other alerts)
	---	No alert present.
Status	Indicates whether the route list, route group, or gateway is up or down.	
Route Pattern	Route pattern that is associated with the route list. Comprises one or more digits and wildcards (such as *X* which indicates a single digit) that represent a range of directory numbers that are either routed or blocked by the pattern.	
DNS Name	One of the following: • DNS name for a gateway • IP address if the DNS name is not available	
IP Address	IP address for a gateway	
Protocol	Protocol on a gateway: H323 or MGCP	
CCM	DNS name or IP address of the Cisco Unified Communications Manager to which the gateway is registered.	
Tools	Select a tool from the list to get more information or to perform relevant configuration tasks.	

Setting Up Synthetic Tests

Step 1 In either the view pane or the map display pane, right-click on the device for which you want to set up a synthetic test.

Step 2 From the menu, select a synthetic test. Your choices will vary depending on the device. For synthetic test details, see Getting Started with Synthetic Tests, page 9-1.

Note If the tool or application you want to launch does not appear in the menu, click the **More Tools** menu item. This launches a secondary menu.

The Create Synthetic Test page appears. For details on creating synthetic tests, see Creating Synthetic Tests, page 9-6.

Setting Up Node-To-Node Tests

Step 1 In either the view pane or the map display pane, right-click on the device for which you want to set up a node-to-node test.

Step 2 From the menu, select **Node-to-Node Test**.

Note If the tool or application you want to launch does not appear in the menu, click the **More Tools** menu item. This launches a secondary menu.

The Node-To-Node Test Configuration page appears. For details on creating node-to-node tests, see Creating a Single Node-To-Node Test, page 11-2.

Setting Up Node-To-Node Test Graphs

Step 1 In either the view pane or the map display pane, right-click on the device for which you want to set up a node-to-node test graph.

Step 2 From the menu, select **Node-to-Node Test Graphs**.

Note If the tool or application you want to launch does not appear in the menu, click the **More Tools** menu item. This launches a secondary menu.

The Node-To-Node Test Configuration page appears. For details on creating node-to-node tests, see Creating a Single Node-To-Node Test, page 11-2.

Setting Up SRST Monitoring

Step 1 In either the view pane or the map display pane, right-click on the device for which you want to set up SRST monitoring.

Step 2 From the menu, select **Survivable Remote Site Telephony Test**.

Note If the tool or application you want to launch does not appear in the menu, click the **More Tools** menu item. This launches a secondary menu.

The SRST Test Configuration page appears. For details on creating SRST tests, see Configuring a Single SRST Test as Needed, page 18-9.

Configuring Threshold Settings

Step 1 In either the view pane or the map display pane, right-click on the device for which you want to change the threshold settings.

Step 2 From the menu, select **Threshold Parameters**.

Note If the tool or application you want to launch does not appear in the menu, click the **More Tools** menu item. This launches a secondary menu.

The Managing Thresholds: Edit page appears. For details on editing thresholds, see Editing Operations Manager Thresholds, page 19-27.

Configuring Polling Settings

Step 1 In either the view pane or the map display pane, right-click on the device for which you want to change the polling settings.

Step 2 From the menu, select **Polling Parameters**.

Note If the tool or application you want to launch does not appear in the menu, click the **More Tools** menu item. This launches a secondary menu.

The Polling Parameters: Edit page appears. For details on editing polling parameters, see Editing Polling Parameters, page 19-13.

Suspending Devices

Step 1 In either the view pane or the map view pane, select the devices (use Ctrl-click to select the objects) that you want to suspend.

Step 2 Press Ctrl and right-click to open the menu.

Step 3 From the menu, select **Suspend Device**. An informational dialog box appears.

Step 4 Click **OK**.

Resuming Devices

Step 1 In either the view pane or the map view pane, select the devices (use Ctrl-click to select the objects) that you want to resume.

Step 2 Press Ctrl and right-click to open the menu.

Step 3 From the menu, select **Resume Device**. An informational dialog box appears, displaying a message like this one:

```
Monitoring will be resumed for the selected 1 device(s). Be sure to apply your changes
in the PTM UI. Click here to apply the changes.
```

Note If you do not apply changes, the device will not be monitored. If you need to apply changes later, see Applying Changes, page 19-60.

Step 4 Click **OK**.

Adding a Device

If you can see a device that is not monitored in the Service Level View, you can add it to Operations Manager using this procedure.

Step 1 In either the view pane or the map display pane, select the Unmanaged Devices folder. The Unmanaged Devices report displays.

Step 2 Select a device or multiple devices to add and click **Add**. The Add Devices dialog box appears, displaying the IP address (or addresses) for the devices that you selected in the Device Information field.

Step 3 Enter credentials for the device.

Step 4 Click **OK**. The devices are added.

Deleting Devices

Step 1 In either the view pane or the map display pane, select the devices that you want to delete. Use Ctrl-click to select the objects in the View pane.

Step 2 Press Ctrl and right-click to open the menu.

Step 3 From the menu, select **Delete Device**. A confirmation dialog box appears.

Step 4 Click **Yes**. The devices are deleted.

For more information, see Deleting Devices, page 16-36.

Creating User-Defined Groups

The Service Level View provides you with a quick way to create a new user-defined group, by selecting either devices or groups. You cannot edit existing user-defined groups or create rules for populating groups through this page. Administrative grouping activities are performed from the Group Administration and Configuration page (for details, see Managing Groups, page 17-1.)

Step 1 In either the view pane or the map display pane, select the devices or groups (use Ctrl-click to select the objects) that you want to group.

Step 2 Press Ctrl and right-click to open the menu.

Step 3 From the menu, select **Group Devices**. The Create Group menu appears.

Note If the tool or application you want to launch does not appear in the menu, click the **More Tools** menu item. This launches a secondary menu.

Step 4 Do the following:

- Enter a group name
- (Optional) Enter a description
- Select which dashboard displays you want the group to appear in as a view

Step 5 Click **Create**.

Launching Administration Pages for Devices

The Service Level View provides you with links to the administration pages of the monitored devices. The availability of these pages depends on the device type. For example, Cisco Unified Communications Manager and Cisco Unity devices provide access to their administration pages.

Step 1 In either the view pane or the map display pane, right-click on the device whose administration page you want to open.

Step 2 From the menu, select the administration page link.

The following list shows the possible options (depending on the device):

- Cisco Conference Connection Administration
- Cisco Emergency Responder Administration
- Cisco IP Contact Center Administration
- Cisco MeetingPlace Express Administration
- Cisco Unified Communications Manager Administration
- Cisco Unified Communications Manager Express Administration
- Cisco Unified Communications Manager Serviceability

- Cisco Unified Presence Server Administration
- Cisco Unified SIP Proxy Server Administration
- Cisco Unity Administration
- Cisco Unity Connection Administration
- Cisco Unity Express Administration
- Gateway Administration

Note If the tool or application you want to launch does not appear in the menu, click the **More Tools** menu item. This launches a secondary menu.

The administration page opens.

Launching External Applications—Using the Service Level View

The Service Level view provides you with launching points for several external applications. From the Service Level view you can launch the following external applications:

- Launching RME—Using the Service Level View, page 2-32
- Launching Campus Manager—Using the Service Level View, page 2-33
- Launching CiscoView—Using the Service Level View, page 2-33

Note Before you can launch any of these applications, you must register them with Operations Manager (through Administration > Preferences). See Setting System-Wide Parameters Using System Preferences, page 20-9.

Launching RME—Using the Service Level View

Procedure

Step 1 In either the view pane or the map display pane, right-click on the device for which you want to open CiscoWorks Resource Manager Essentials (RME).

Step 2 From the menu, select one of the following:

- Operations Manager Device Center
- Resource Manager Essentials Detailed Device Report
- Resource Manager Essentials Software Image Management

Note If the tool or application you want to launch does not appear in the menu, click the **More Tools** menu item. This launches a secondary menu.

RME opens.

Launching Campus Manager—Using the Service Level View

Procedure

Step 1 Click the tool icon in the Window Tools Area. The Tools dialog box appears.

Step 2 Select one of the following:

- Campus Path Analysis
- Campus Topology

CiscoWorks Campus Manager opens.

Launching CiscoView—Using the Service Level View

Procedure

Step 1 In either the view pane or the map display pane, right-click on the device for which you want to open CiscoView.

Step 2 From the menu, select CiscoView.

Note If the tool or application you want to launch does not appear in the menu, click the **More Tools** menu item. This launches a secondary menu.

CiscoView opens.

Troubleshooting the Service Level View

If devices do not appear in the Service Level View or values do not display properly, you may have not followed the required steps to ensure that your device information is accurate. For details on some things to keep in mind, see Device Prerequisites, page 16-2.

CHAPTER 3

Monitoring Alerts and Events

These topics describe monitoring Alerts and Events:

How to Use the Alerts and Events Display

The Alerts and Events display provides real-time information about the operational status of your network. The displays are designed so that you can set them up and leave them running, providing an ongoing monitoring tool that signals you when something needs attention. When a fault occurs in your network, Cisco Unified Operations Manager (Operations Manager) generates an event or events that are rolled up into an alert. If the alert occurs on an element in your active *view* (a logical grouping of device groups), it is shown on your Alerts and Events display.

After setting up a view, you can customize your Alerts and Events display by selecting specific *views* and using *filters*:

- Views control the events for device groups that appear on the Alerts and Events display. See Selecting Views for Alerts and Events, page 3-2.
- Filters control the *specific device types* you monitor, along with alert *severities* and their *status*. See Filtering Alerts and Events, page 3-2.

You can also change the names of Operations Manager events to names that are more meaningful to you. These customized names are reflected in both the Alerts and Events display and any Alert History reports you generate. Alert History and Alerts and Events displays reflect customized names. For information on changing Operations Manager event names using Notification Customization, see Customizing Events, page 15-23.

You can monitor all devices that Operations Manager supports, once you have added those devices using Device Management and ensured that the devices are in your view.

Note All Alert History reports generated from within the Alerts and Events display provide information from the past 24 hours. To generate an Alert History report on time spans beyond the last 24 hours, use Alert History from the Reports tab by selecting **Reports > Alerts and Event History**. For more information, see 24-Hour Context-Based Alert and Event History Reports, page 12-3.

Selecting Views for Alerts and Events

When you select **Monitoring Dashboard > Alerts and Events** to open the Alerts and Events display, all available views are listed in the view pane on the left side of the display. If the views shown do not meet your needs, you can create a new view as described in Managing Views, page 6-1.

The view pane is updated every two minutes. You can have up to 18 views in the view pane in a single Alerts and Events display. See Activating and Deactivating a View, page 6-2.

Filtering Alerts and Events

Filters allow you to manipulate the Alerts and Events display to show alerts based on their severity, status, and originating device.

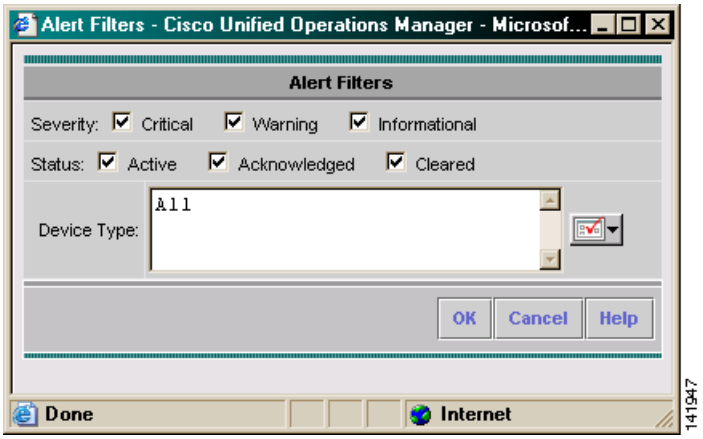
Note Once you use an alert filter, the filter is applied to all of your views until you change the filter; other clients are not affected. When you close the Alerts and Events display, your filters are lost. Filters do not affect severity icons in the view pane.

Step 1 Select **Monitoring Dashboard > Alerts and Events**. The Alerts and Events display opens.

Step 2 Click the filtering button in the tool button area at the top-right of the Alerts and Events display.

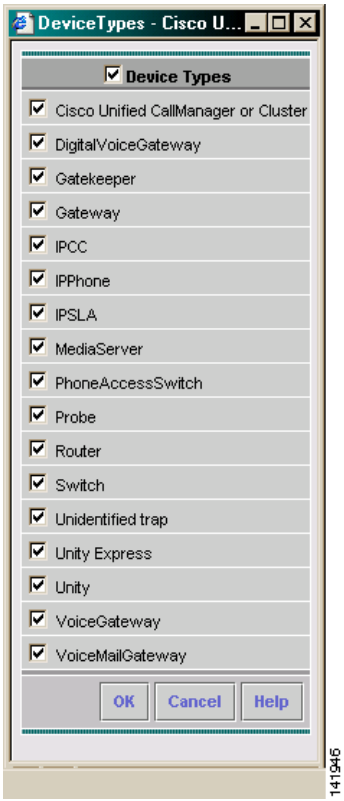
Figure 3-1 shows the Alert Filters page. You can populate the Device Type box by selecting device types from the button to the right of the Device Type box. By default, all device types are selected.

Figure 3-1 Alerts and Events—Alert Filters Dialog Box



Step 3 To see all device types that you can filter, click the button to the right of the Device Type box. A Device Types popup window opens, as shown in Figure 3-2.

Figure 3-2 Alerts and Events—Device Types Dialog Box



Step 4 Verify that only the filtering criteria you want to use are selected.

Step 5 Click **OK**.

Resetting Filters on the Alerts and Events Display

From the Alerts and Events display, you can clear any filters that you have set. As a result, all alerts in the currently selected view are displayed.

Step 1 On the Alerts and Events display, click **Reset Filter**. A confirmation dialog box appears.

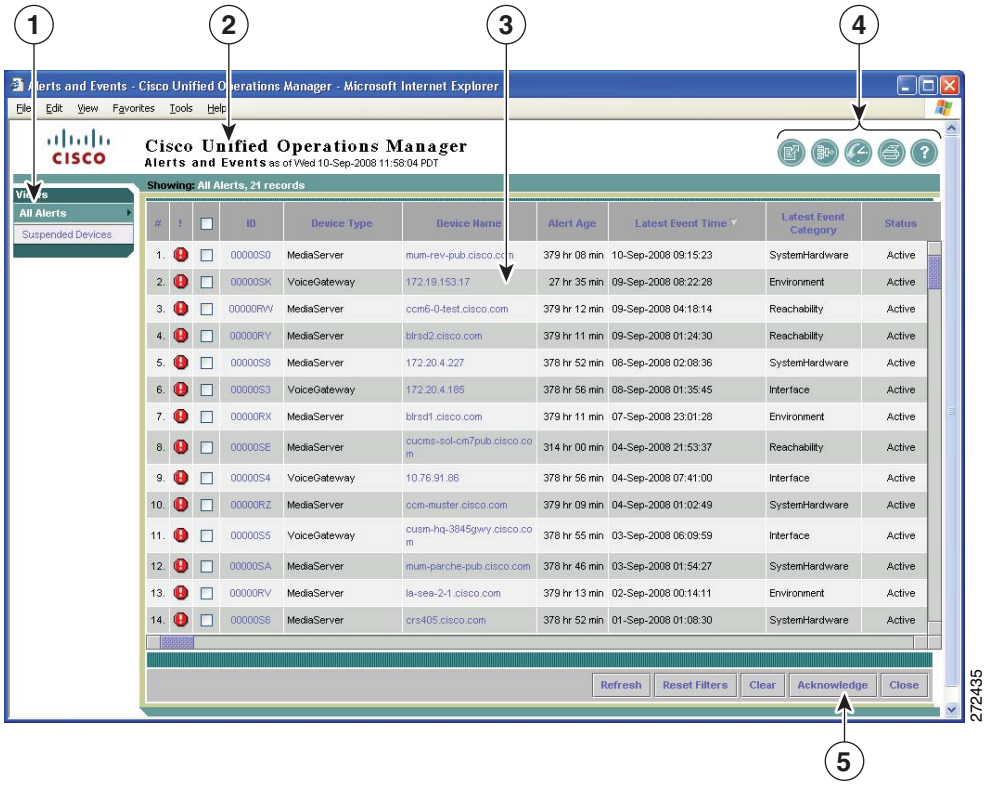
Step 2 Click **Yes**. The Alerts and Events display refreshes, displaying all alerts in the view.

Starting the Alerts and Events Display

To start the Alerts and Events display, select **Monitoring Dashboard > Alerts and Events**. Figure 3-3 shows an example of an Alerts and Events display.

Tip After you become familiar with the Alerts and Events display, you can edit the information it provides as described in Selecting Views for Alerts and Events, page 3-2 and Filtering Alerts and Events, page 3-2.

Figure 3-3 Alerts and Events Display



1	View pane. See View Pane, page 3-5.	**4**	Window tools area. See Window Tools Area, page 3-6.
2	Launch information and view status bar area. See Launch Information and View Status Bar Area, page 3-5.	**5**	Command button area. See Command Button Area, page 3-6.
3	Tabular display pane. See Tabular Display Pane, page 3-5.		

Understanding the Layout of the Alerts and Events Display

These topics provide details about the information in the Alerts and Events display.

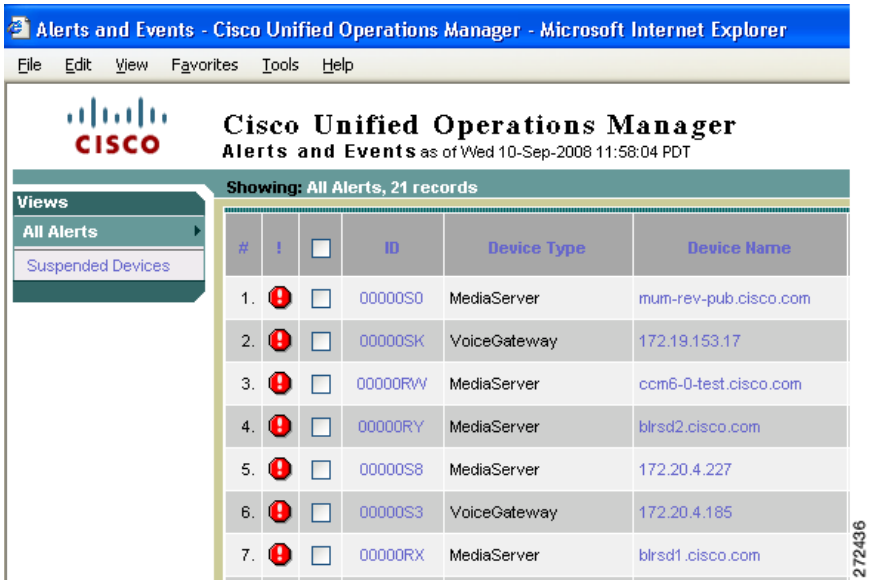
View Pane

The view pane lists the currently available *views*. Views must be created and activated before they are shown in the Alerts and Events display. By default, two views—All Alerts and Suspended Devices—are always shown, and cannot be deleted from your Alerts and Events display. (To create and activate a view or remove an unwanted view from your display, see Managing Views, page 6-1.)

The *current view* is highlighted in the view pane. The contents of the current view are shown in the tabular display pane to the right of the view pane. To select another view, simply click the view name in the view pane.

Figure 3-4 shows four active views; the current view is All Alerts. Icons next to the views indicate the severity of the alerts received from devices in those views, signaling you that the devices may need attention.

Figure 3-4 Alerts and Events Display—View Pane and Severity Icons



For the current view, All Alerts, severity icons also appear next to the alerts in the tabular display, as shown in Figure 3-4, to help you quickly locate a specific alert.

The view pane is updated every two minutes. You can have up to 18 views in the view pane in a single Alerts and Events display.

Launch Information and View Status Bar Area

The launch information area shows the current time on the server when the Alerts and Events display is being viewed.

The view status bar lists the selected view, which is shown in the tabular display pane, and the number of alerts in that view.

Tabular Display Pane

The tabular display pane is the core of the Alerts and Events display. It contains a list of all alerts that are occurring on the devices in your current view. This pane is refreshed every 30 seconds. For an explanation of all of the items in the tabular display, see Getting Alert Details Using the Alerts and Events Display, page 3-7.

Icons alert you to what needs attention; for example:

- The severity icons indicate which views and alerts require attention.
- The diamond symbols in the Latest Event Time column indicate which alerts have experienced recent activity. When no diamonds appear in the Latest Event Time column, it indicates that the alert is older than 45 minutes. The presence of three stars indicates that the alert is older than 15 minutes; two stars that it is older than 30 minutes; and one star that it is older than one minute.

The tabular display pane is scrollable and can store up to 1,000 records.

Window Tools Area

The top-right corner of the Alerts and Events display contains available tools buttons. All buttons are described in Table 3-1.

Table 3-1 Alerts and Events Display—Window Tools Buttons

Icon	Meaning	Described in...
	Exports the current display to a PDF file.	Exporting Data from a Display or Report, page 1-21
	Opens the Filter page, for refining the tabular display in the Alerts and Events display.	Filtering Alerts and Events, page 3-2
	Opens a printer-friendly version for printing.	Printing Displays or Reports, page 1-22
	Opens an Alert History report.	Understanding the Alert History Report, page 12-10
	Opens the online help.	Using Help, page 1-18

Command Button Area

The command buttons on the Alerts and Events display provides you ways to respond to alerts and reset filters.

Table 3-2 Alerts and Events Display—Command Buttons

Button	Action
Refresh	Refreshes the Alerts and Events display.
Reset Filters	Resets the filters set on the Alerts and Events display.
Clear	Clears the alert. See Clearing an Alert—Using the Alert Details Page, page 3-30.
Acknowledge	Changes the alert's status to Acknowledged. See Acknowledging an Alert—Using the Alert Details Page, page 3-30.
Close	Closes the Alerts and Events display.

Table 3-3 Alerts Details Page—Command Buttons

Button	Action
Refresh	Refreshes the contents in the Alerts Details page manually.
Reset Filters	Resets the filters set on the Alerts and Events display.
Clear	Clears the alert. See Clearing an Alert—Using the Alert Details Page, page 3-30.
Acknowledge	Changes the event status to Acknowledged. See Acknowledging an Alert—Using the Alert Details Page, page 3-30.
Close	Closes the Alerts and Events display.

Getting Alert Details Using the Alerts and Events Display

Use the tabular display in the Alerts and Events display to obtain more information about the alerts that are occurring in your current view. In the tabular display, as shown in Figure 3-3, alerts are grouped by their severity: critical, warning, or informational. Within these severity groupings, or *buckets*, alerts with the latest change are listed first.

When an alert is generated, it remains in the Alerts and Events display until it cleared. While the alert is in the display, if any events occur or get updated, the alert is updated. If a cleared event recurs, a new event with a new event ID is shown.

Note When using the Alerts and Events display, remember the following:

- If a monitored device is removed from the network, it will continue to be in the Monitored state until the next inventory collection occurs, even though the device is unreachable. The only way that you will know that this device is unreachable, is when an unreachable alert appears for this device in the Alerts and Events display.
- When a device becomes unresponsive, all existing events for that device become cleared and one unresponsive event is generated for the device.

Table 3-4 defines the Alerts and Events tabular display elements. All elements are updated every 30 seconds.

Tip You can generate a 24-hour Alert History report on all alerts that occurred on devices in your view by opening Alert History from the window tools area of the Alerts and Events display.

Table 3-4 Alerts and Events Tabular Display—Contents

Heading	Description	
	Severity of alert	
		Critical
		Warning
		Informational/Unidentified Trap Alert
ID	Alert identifier number. Clicking this link opens an Alert Details page (see Starting the Alert Details Page, page 3-9).	
Device Type	Type of device. Inventory Collection in Progress indicates that Operations Manager was discovering the device when the alert occurred. The actual device type is reflected when new events occur. The device type is displayed as N/A during inventory collection. For more information, see Using Device Management, page 16-1.	
Device Name	Device name or IP address. Clicking this link opens the Detailed Device View (see Viewing Device Elements in Detail, page 3-22).	
Alert Age	Time span since alert creation, depending upon alert status.	
Latest Event Time	Date and time alert last occurred or was changed. Diamonds indicate alert activity, such as a new event, alert acknowledgement, new user annotation, and so forth; no diamonds indicates that the alert is stale. Alerts are grouped by severity, and within severities, alerts with the latest change are listed first.	
		Alert was updated within last 15 minutes.
		Alert was updated within last 16-30 minutes.
		Alert was updated within last 31-45 minutes.
	No diamonds	Alert was updated 46 or more minutes ago.
Latest Event Category	Event category, one of the following: Application, Connectivity, Environment, Interface, Other, Reachability, and System Hardware. For alerts containing multiple events, the tabular display shows the category of the event with the most recent change.	

Table 3-4 Alerts and Events Tabular Display—Contents (continued)

Heading	Description	
Status	Alert status, based on last polling.	
	Active	Alert is live. (Note that alerts on suspended devices remain active; see Sending E-Mail in Response to an Alert, page 3-31.)
	Cleared	Alert is no longer live.
	Acknowledged	Alert was manually acknowledged by a user (from Alert Details page).
	User Cleared	Alert was manually cleared by a user.

Getting Alert and Event Details

These topics address how to start and use the Alert Details page to get detail information on events:

- Starting the Alert Details Page, page 3-9
- Understanding the Layout of the Alert Details Page, page 3-11
- Viewing Events Associated with an Alert, page 3-14
- Viewing Event Details, page 3-15

Starting the Alert Details Page

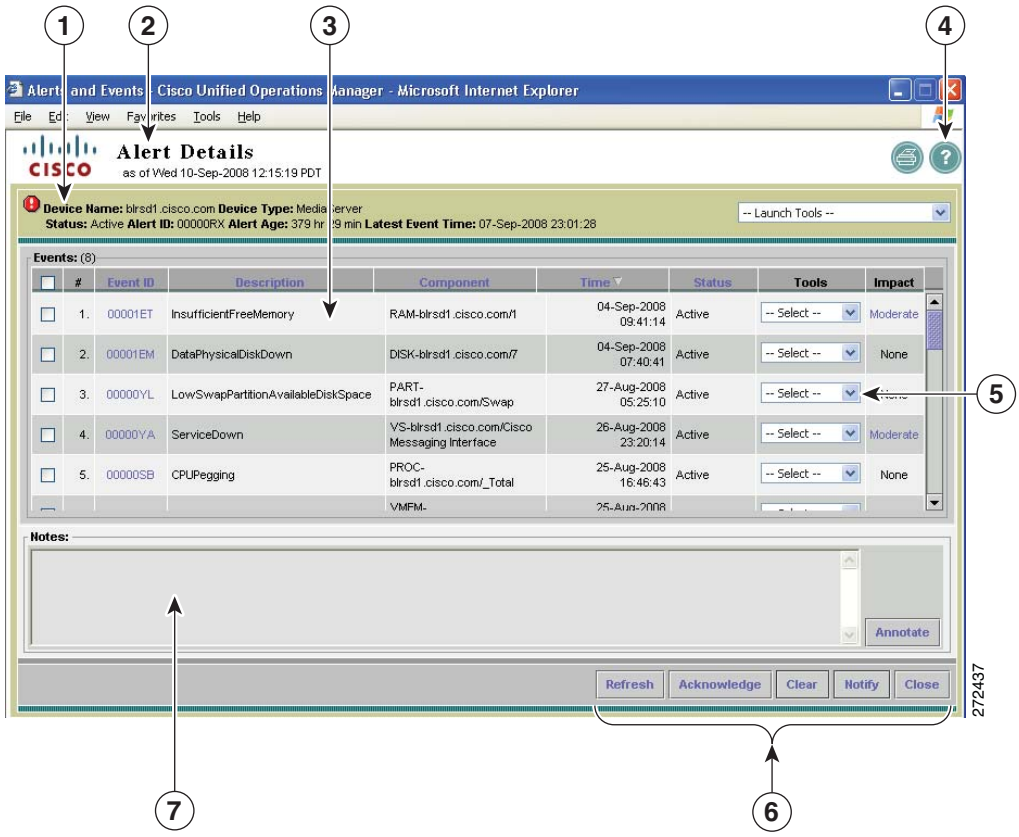
The Alert Details page provides information about all of the events that were rolled up into a specific alert.

Note The Alert Details page can also be opened from the Service Level View. See Viewing Alert Information, page 2-22.

Step 1 Select **Monitoring Dashboard > Alerts and Events**. The Alerts and Events display opens.

Step 2 Locate the alert you want to investigate and click the alert ID. The Alert Details page opens.

Figure 3-5 Alert Details Page



1	Alerts status bar. See Alert Status Bar, page 3-11.	**5**	Tools column list. Select a tool, such as Event History. See Tools Column, page 3-13.
2	Launch information area. See Launch Information Area, page 3-12.	**6**	Command button area. See Command Button Area, page 3-13.
3	Tabular display pane. See Tabular Display Pane, page 3-13.	**7**	Notes pane. See Notes Pane, page 3-13.
4	Window tools area. See Window Tools Area, page 3-13.		

Event Processing for the Alerts and Events Display During High CPU Utilization

During periods of high CPU utilization and alert buildup, Operations Manager stops processing events. You will know when this is occurring by the message that appears in the view status bar of the Alerts and Events display. The message states that alert processing is being controlled, and not every alert is being displayed. The excess Alerts and Events display events are written to the NMSROOT\logs\itemlogs\EPM\EPMDroppedEvents.log file, and these events:

- Do not appear on the Alerts and Events display.
- Are not stored in the Alerts and Events history database.
- Are not sent out as notifications.

Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as "C:\Program Files\CSCOpx" or C:\PROGRA~1\CSCOpx.

Understanding the Layout of the Alert Details Page

These topics provide details about the information on the Alert Details page. These panes are illustrated in Figure 3-5.

Alert Status Bar

The alert status bar lists details about the alert with which the listed events are associated. Table 3-5 explains the contents of the alert status bar area.

Table 3-5 Alert Details Page—Alert Status Bar Contents

Field	Description	
Device Name	Device name or IP address.	
Device	Device type.	
Status	Alert status, based on last polling.	
	Active	Alert is live. (Note that alerts on suspended devices remain active; see Sending E-Mail in Response to an Alert, page 3-31.)
	Cleared	Alert is no longer live.
	Acknowledged	Alert was manually acknowledged by a user (from the Alert Details page).
Alert ID	Alert identifier number	
Alert Age	Time span since alert creation, depending upon alert status:	
	Active or Acknowledged	Time span between alert creation and current server time.
	Cleared	Time span between alert creation and Last Change time (the Last Change time may also represent when the alert was cleared).

Table 3-5 Alert Details Page—Alert Status Bar Contents (continued)

Field	Description
Last Change	Time and date of last alert update (indicates activity, such as an event recurrence, alert acknowledgement, the addition of an annotation, and so forth). Alerts are grouped by severity, and within severities, alerts with the latest change are listed first.
Launch Tools	You can launch Operations Manager tools and external applications. • Alert Details—Opens the Alert Details page (see Starting the Alert Details Page, page 3-9). • Alert History—Opens an Alert History report (see Understanding the Alert History Report, page 12-10). • Associated Phones—Opens an Associated Phones report (see Viewing Associated Phones, page 2-23). • Detailed Device View—Opens a Detailed Device View for the device (see Starting the Detailed Device View, page 3-18). • Performance—Shows performance monitoring (see How to Use Performance Graphs, page 7-1). • Name of Synthetic Test—Opens the Create Synthetic Test page (see Creating Synthetic Tests, page 9-6). The options that appear depend on the device. For synthetic test details, see Getting Started with Synthetic Tests, page 9-1. • Node-To-Node Test—Opens the Node-To-Node Test Configuration page (see Creating a Single Node-To-Node Test, page 11-2). • SRST Test—Opens the SRST Test Configuration page (see Configuring a Single SRST Test as Needed, page 18-9). • Polling Parameters—Opens the Polling Parameters: Edit page (see Editing Polling Parameters, page 19-13). • Threshold Parameters—Opens the Managing Thresholds: Edit page (see Editing Operations Manager Thresholds, page 19-27). • Administrative Pages—Opens the administrative page of the device. The options that appear depend on the device; some examples are Gateway Administration, Unity Administration, Cisco Unified Communications Manager Serviceability, or Cisco Unified Communications Manager Trace Configuration. • Connectivity Details—Opens the Connectivity Detail View (see Working with the Connectivity Detail View, page 2-10). • Path Analysis Tool—Opens the Path Analysis Tool (see Launching the Path Analysis Tool, page 2-24). • Operations Manager Device Center—Opens the Device Center page of the Operations Manager Server (see Using Device Management, page 16-1).

Launch Information Area

The launch information area shows the current time on the server when the Alerts and Events display is being viewed.

Tabular Display Pane

On the Alert Details page, the tabular display pane contains a table that lists details about events. These events are associated with the alert listed in the alert status bar. You can refresh the display by clicking **Refresh** at the bottom of the pane. For an explanation of all of the items in the table, see Getting Alert and Event Details, page 3-9.

The tabular display is scrollable and can store up to 1,000 records. See Viewing Events Associated with an Alert, page 3-14 for actions you can perform from this page.

Window Tools Area

The top-right corner of the Alert Details page contains a printer tool button and an Operations Manager Tools button, as described in Table 3-6.

Table 3-6 Alert Details Page—Window Tools Buttons

Icon	Meaning	Described in...
	Opens a printer-friendly version for printing.	Printing Displays or Reports, page 1-22
	Opens the Operations Manager online help.	Using Help, page 1-18

Tools Column

The tools column includes Alert History. Selecting Event History opens a 24-hour Event History report on the component. See 24-Hour Context-Based Alert and Event History Reports, page 12-3.

Notes Pane

The notes pane lists any alert annotations that users have entered. The notes pane is a convenient tool for making sure that all users see alert information. You can add an annotation by clicking the **Annotate** button. Adding an annotation is described in Annotating an Alert, page 3-31.

Command Button Area

In addition to the Annotate button in the notes pane, the command button area provides other ways to respond to alerts.

Table 3-7 Alert Details Page—Command Buttons

Button	Action
Refresh	Refreshes the tabular display.
Acknowledge	Changes the event status to Acknowledged. See Acknowledging an Alert—Using the Alert Details Page, page 3-30.
Clear	Clears the Alert. See Clearing an Alert—Using the Alert Details Page, page 3-30.
Notify	Sends e-mail notification of the alert. See Sending E-Mail in Response to an Alert, page 3-31.
Close	Closes the Alert Details page.

Viewing Events Associated with an Alert

Use the tabular display in the Alert Details page to obtain more information about all of the events associated with a specific alert. In the tabular display, as shown in Figure 3-6, events with the latest change are listed first.

Events remain on the Alert Details page until the parent alert expires.

Note If you suspend a device, the events remain in the Active state.

If an event recurs, the existing event is not updated. Instead, the recurrence is shown as a new event with a new event ID.

Figure 3-6 provides an example of an Alert Details table. This table is refreshed every 30 seconds.

Figure 3-6 Alert Details Page—Tabular Display

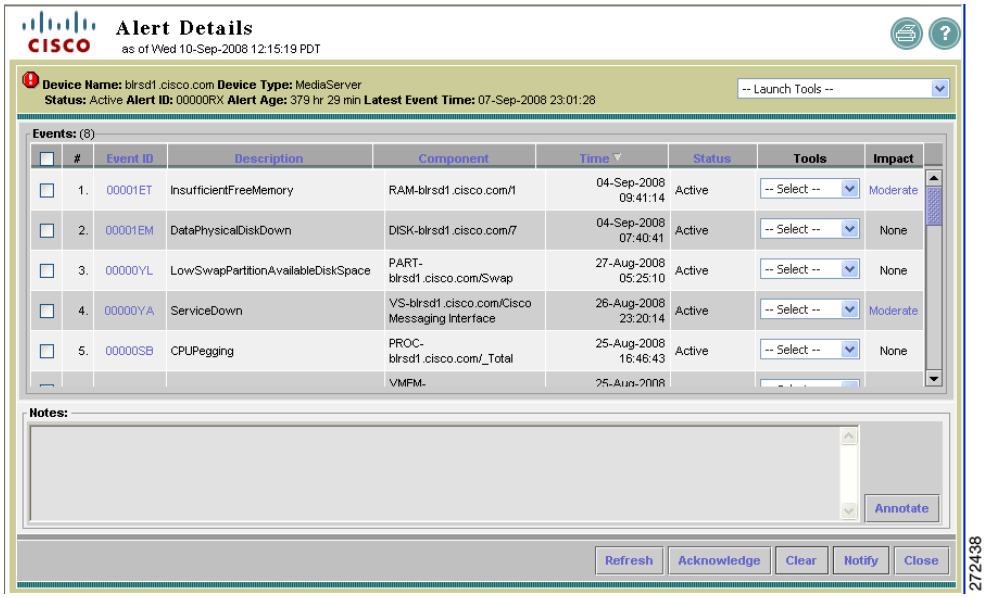


Table 3-8 defines the table elements. Click **Refresh** at the bottom of the pane to refresh the table contents.

Tip Remember that you can generate a 24-hour Alert History report on all events that occurred on a selected component by opening Alert History from the window tools area of the Alerts and Events display.

Table 3-8 Alert Details Tabular Display—Contents

Column	Description	
Event ID	Event identifier number. Clicking this link opens the Event Details page (see Getting Alert and Event Details, page 3-9). Note that this event ID is not the same as the event code provided by Notification Services. For more information, see Customizing Events, page 15-23.	
Description	Operations Manager event name (as described in Events Processed, page E-1). You can also change the names of Operations Manager events to names that are more meaningful to you. For information on changing Operations Manager event names using Notification Customization, see Customizing Events, page 15-23.	
Component	Device element on which the event occurred.	
Time	Time at which the event occurred.	
Status	Event status, based on last polling.	
	Active	Event is live.
	Cleared	Event is no longer live.
	Suspended	Device is suspended.
	Resumed	Device is being resumed.
	Deleted	Device has been deleted.
Tools	Links to tools that allow you to perform additional tasks. For example: • Open an Event History report (see Understanding the Event History Report, page 12-12). • Performance (see How to Use Performance Graphs, page 7-1). • Edit threshold settings (see Editing Operations Manager Thresholds, page 19-27).	
Impact	Options are *None* or *High*. The *High* option is a link that opens a Service Impact Report. See Understanding the Service Impact Report, page 3-16.	

Viewing Event Details

The Event Details page provides additional details about the event, such as the values of MIB attributes at the time of the event, polling and threshold information, and utilization information. The Event Details page also provides ways to respond to events.

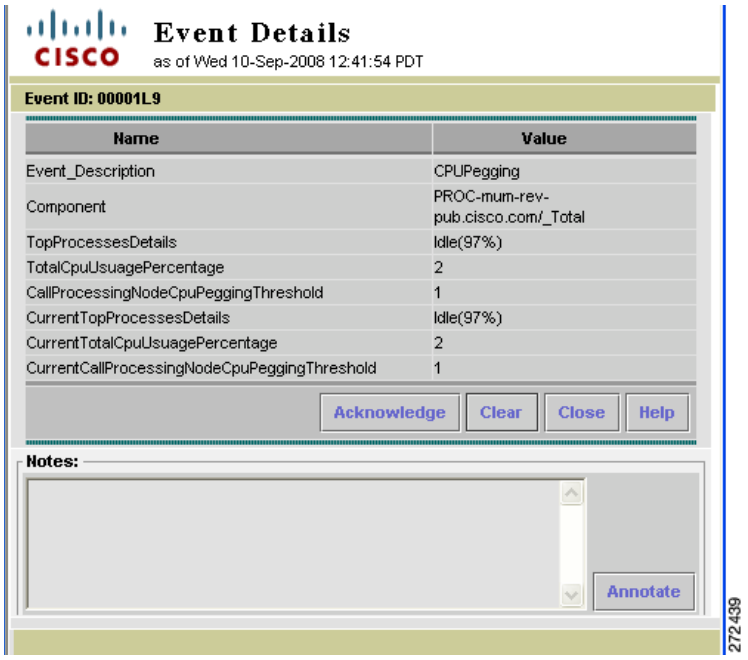
Step 1 Select **Monitoring Dashboard > Alerts and Events**. The Alerts and Events display opens (see Figure 3-7).

Step 2 Locate the alert you want to investigate and click the alert ID. The Alert Details page appears.

Step 3 Locate the event you want to investigate, and click the event ID. The Event Details page appears.

Figure 3-7 shows a typical Event Details page.

Figure 3-7 Event Details Page



The information that is shown in the Event Details page depends on the event description. Table 3-9 describes the Event Details page command buttons.

Table 3-9 Event Details Page—Command Buttons

Button	Action
Acknowledge	Changes the event status to Acknowledged. See Acknowledging an Event—Using the Alert Details Page, page 3-32.
Clear	Moves the event status to UserCleared. See Clearing an Event—Using the Alert Details Page, page 3-32.
Notify	This helps to send email.See Sending E-Mail in Response to an Alert, page 3-31.
Close	Closes the Alerts Details page.
Help	Opens the online help.
Annotate	Add details for other users about event information. See Annotating an Alert, page 3-31.

Understanding the Service Impact Report

Service Impact reports provide you with a single report that describes how a particular failure impacts the rest of your IP telephony deployment. The report answers the following:

- How does this failure affect the users?
- Which services are unavailable because of this failure?
- What is the possible cause and location of the failure?

Viewing a Service Impact Report

Step 1 Select **Monitoring Dashboard > Alerts and Events**. The Alerts and Events display opens.

Step 2 Locate the alert you want to investigate and click the alert ID. The Alert Details page opens.

Step 3 Look in the Impact column. If there is a Service Impact report available, High or Moderate is displayed in the Impact column. If None is displayed, a Service Impact report is not available.

Step 4 Click **High** or **Moderate**. A Service Impact report appears. Figure 3-8 shows an example of a Service Impact report.

Figure 3-8 Service Impact Report

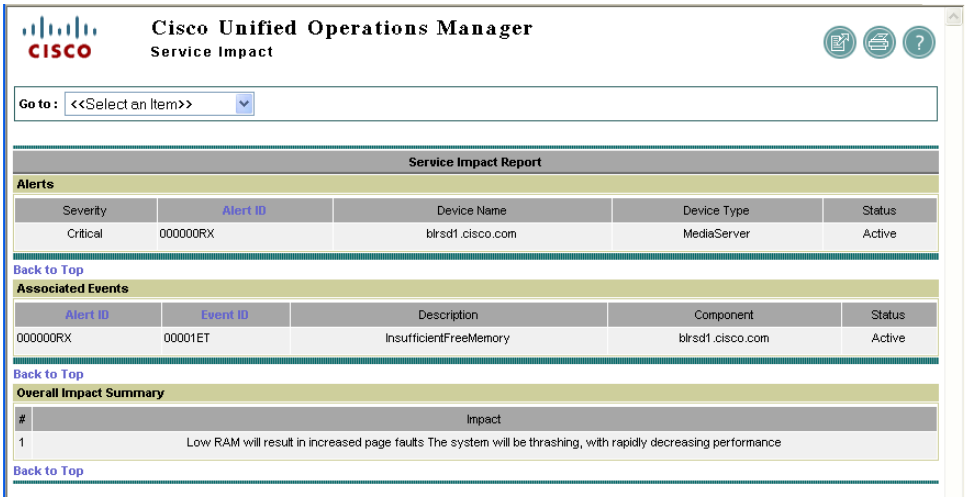


Table 3-10 Service Impact Report Column Descriptions

Column	Description	
Alerts	Severity	Alert severity.
	Alert ID	Alert identification number.
	Device Name	Device name or IP address.
	Device Type	Device type.
	Status	Alert status based on last polling.

Table 3-10 Service Impact Report Column Descriptions (continued)

Column	Description		
Associated Events	Alert ID	Alert identification number for which the event is associated.	
	Event ID	Event identification number.	
	Description	Operations Manager event name (as described in Events Processed, page E-1). You can also change the names of Operations Manager events to names that are more meaningful to you. For information on changing Operations Manager event names using Notification Customization, see Customizing Events, page 15-23.	
	Component	Device element on which the event occurred.	
	Status	Event status, based on last polling.	
		Active	Event is live.
		Cleared	Event is no longer live.
		Suspended	Device is suspended.
		Resumed	Device is being resumed.
		Deleted	Device has been deleted.
Overall Impact Summary	Provides an explanation of the impact that this failure will have on the rest of your IP telephony deployment.		

Getting Device Information

The Detailed Device View provides extensive information on the devices and device components listed in Starting the Detailed Device View, page 3-18. You can view information on devices that Operations Manager is currently monitoring, as well as devices whose monitoring you have suspended.

In the Detailed Device View, you can do the following:

- View hardware and software information on system, environment, connectivity, and interface components
- View hardware and software information on subcomponents of aggregate devices
- View application status for Cisco Unified Communications Manager, Voice Services, Work Flow, and Synthetic Tests.
- Suspend or resume management of a device or a device component so the device is no longer polled, or polling is resumed
- Launch other Operations Manager tools

Starting the Detailed Device View

You can start the Detailed Device View from within the Alerts and Events display, either by clicking a device link, or by starting the Alert Details page and selecting Detailed Device View from the Launch Tools pull-down list.

Note The Detailed Device View page can also be opened from the Service Level View (see Viewing Device Information, page 2-23), as well as from several other locations in Operations Manager. In many reports or pages in Operations Manager, clicking a device name (that is blue) opens a Detailed Device View for the device.

Note You cannot display a Detailed Device View for unidentified trap devices. For more information on unidentified traps, refer to Processed and Pass-Through Traps, page C-1.

Step 1 From the Alerts and Events display, click a device in the Device Name column. The Detailed Device View opens. (See Figure 3-9 for an example.)

Step 2 In the component categories pane, select an item from the device tree. The system information pane is populated with information about the selected item.

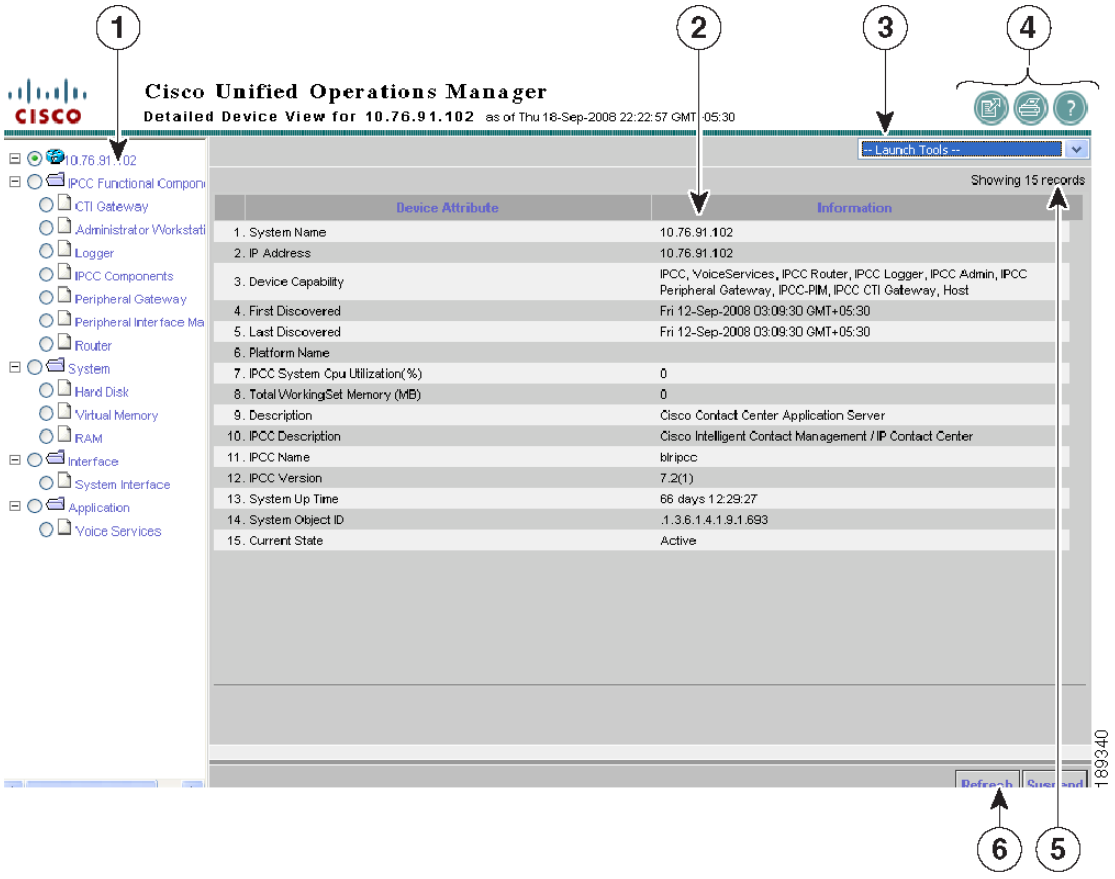
If the item you select is the subdevice of an aggregated device, the Detailed Device View displays the subdevice's managed state and device capability. To display a complete Detailed Device View of the subcomponent, click the **Launch New DDV for This Device** button.

Step 3 If you want to suspend a managed device so it is no longer polled and its traps are no longer processed (or if you want to resume a suspended device):

- Click **Suspend** to change the device's managed state to Suspended. Operations Manager no longer polls any device components, nor does it process any traps. All events and alerts remain in the Active state. The device is moved to the Suspended Devices view. Subsequent events (including traps) are ignored and no longer processed.
- Click **Resume** to change the device's managed state to Active. Operations Manager resumes polling and trap processing on the device, and the device is moved out of the Suspended Devices view and back into its previous view.

Figure 3-9 provides an example of a Detailed Device View.

Figure 3-9 Detailed Device View



1	Component categories pane. See Component Categories Pane, page 3-20.	**4**	Windows tool bar. See Window Tools Area, page 3-22.
2	System information pane. See System Information Pane, page 3-21.	**5**	Command button area. See Command Buttons Area, page 3-22.
3	Tools. See Launch Tools, page 3-21.	**6**	Record count. See Record Count, page 3-22.

Understanding the Layout of the Detailed Device View

These topics provide details about the information in the Detailed Device View.

Component Categories Pane

The component categories pane lists the components of the device or cluster. Selecting a component allows you to view detailed information pertaining to that component, such as CPU usage for a processor, TotalUsedMemory for memory, and so forth.

If the device you are viewing is an aggregate device, the subdevice also appears in the component categories pane. To display a complete Detailed Device View of the subcomponent, click the **Launch New DDV for This Device** button. This button appears after you select the subdevice from the device tree.

System Information Pane

The system information pane provides information such as the system name, IP address, SysUnified Communications ID, system contact, and so forth. Table 3-13 on page 3-23 lists the Detailed Device View information you will see for each device type. See Viewing Device Elements in Detail, page 3-22.

If the system information pane lists an attribute with no value, it is because of one of the following reasons:

- The attribute is not populated.
- The attribute is not configured correctly.
- The attribute does not apply to the device.

You can suspend or resume device or component monitoring by clicking the **Suspend** or **Resume** button (the button shown depends on the component's current managed state). These functions are described in these sections:

- Suspending/Resuming Devices, page 3-26
- Suspending/Resuming a Device Component, page 3-27

Launch Tools

The Launch Tools pull-down list enables you to launch other Operations Manager tools as well as external applications from the Detailed Device View. The tools that are available to you may vary depending on the device type and its configuration.

The following options can be seen in the Launch Tools menu:

- Alert Details—Opens the Alert Details page (see Starting the Alert Details Page, page 3-9).
- Alert History—Opens an Alert History report (see Understanding the Alert History Report, page 12-10).
- Performance—Shows performance monitoring (see How to Use Performance Graphs, page 7-1).
- Name of Synthetic Test—Opens the Create Synthetic Test page (see Creating Synthetic Tests, page 9-6). The options that appear depend on the device. For synthetic test details, see Getting Started with Synthetic Tests, page 9-1.
- Node-To-Node Test—Opens the Node-To-Node Test Configuration page (see Creating a Single Node-To-Node Test, page 11-2).
- SRST Test—Opens the SRST Test Configuration page (see Configuring a Single SRST Test as Needed, page 18-9).
- Polling Parameters—Opens the Polling Parameters: Edit page (see Editing Polling Parameters, page 19-13).
- Threshold Parameters—Opens the Managing Thresholds: Edit page (see Editing Operations Manager Thresholds, page 19-27).
- Administrative Pages—Opens the administrative page of the device. The options that appear depend on the device; some examples are Gateway Administration, Unity Administration, or Communications Manager Serviceability.
- Connectivity Details—Opens the Connectivity Detail View (see Working with the Connectivity Detail View, page 2-10).
- Path Analysis Tool—Opens the Path Analysis Tool (see Launching the Path Analysis Tool, page 2-24).
- Operations Manager Device Center—Opens the Device Center page of the Operations Manager Server (see Using Device Management, page 16-1).

Window Tools Area

The top-right corner of the Detailed Device View contains available tools buttons. All buttons are described in Table 3-11.

Table 3-11 Detailed Device View Page—Window Tools Buttons

Icon	Meaning	Described in...
	Exports the current display to a PDF file.	Exporting Data from a Display or Report, page 1-21
	Opens a printer-friendly version for printing.	Printing Displays or Reports, page 1-22
	Opens the online help.	Using Help, page 1-18

Record Count

The record count lists the number of information types available on the device.

Command Buttons Area

In addition to the Suspend and Resume button in the system information pane, the command button area provides other ways to respond to alerts.

Table 3-12 Detailed Device View—Command Buttons

Button	Action
Suspend or Resume	Either activates or deactivates monitoring of the device. Only one option is available at a time, depending on the state of the device. See Suspending Device Monitoring, page 3-25.
Refresh	Refreshes the Detailed Device View page. (The Detailed Device View is not automatically refreshed; you must do so manually.)

Launch Information

The launch information shows the current time on the server when the Detailed Device View display is being viewed. If you refresh the page, the time is updated.

Viewing Device Elements in Detail

This topic explains what the Detailed Device View displays for different device classes.

Information Shown in the Detailed Device View

Note Unity Connection 2.1 ports are not monitored by Operations Manager. In the Detailed Device View the following Unity Connection port details are displayed as Not Available (N/A):

- Total # of unity connection ports.
- # of ports currently active.
- # inbound ports.
- # outbound ports.
- # inbound ports currently active.
- # outbound ports currently active.

Also, the left pane of the Detailed Device View does not display a Unity Connection Ports option.

Table 3-13 shows the types of device information displayed for the various device types that Operations Manager supports.

Table 3-13 Device Information Provided by the Detailed Device View

Device Type	Status Reported by Detailed Device View					Device-Specific Components Reported by Detailed Device View	Subcomponents Reported by Detailed Device View[1]
	Environment	System	Interface	Connectivity	Application[2]		
Content Networking		X	X				
Digital Voice Gateway			X	X			
Gatekeeper	X	X	X	X			
IPSLA	X	X	X				
MRP		X	X	X			
Personal Assistant					X		
Media Server	X	X	X		X	Cisco Unified Communications Manager Performance Counters[3]	
Phone Access Switch	X	X	X				
Probe	X	X	X				
Routers	X	X	X				RSM, MSM, MSFC
SPE		X			X		
SSP		X	X				

Table 3-13 Device Information Provided by the Detailed Device View (continued)

Device Type	Status Reported by Detailed Device View					Device-Specific Components Reported by Detailed Device View	Subcomponents Reported by Detailed Device View[1]
	Environment	System	Interface	Connectivity	Application[2]		
Switch	X	X	X				RSM, MSM, MSFC
Unified Communications Manager or Cluster							Media Servers, Digital Voice Gateways, Voice Gateways, VoiceMail Gateways
Unified Contact Center Enterprise (formerly IPCC)	X	X	X		X	Functional components: • CTI Gateway • CTI Unified Communications Server • Administrator Workstation • Logger • NIC • Unified CCE Components • Peripheral Gateway • Peripheral Interface Manager • Router Performance Counters[3]	
Unity	X	X	X		X		
Unity Express		X	X		X	Performance Counters[3]	

Table 3-13 Device Information Provided by the Detailed Device View (continued)

Device Type	Status Reported by Detailed Device View					Device-Specific Components Reported by Detailed Device View	Subcomponents Reported by Detailed Device View[1]
	Environment	System	Interface	Connectivity	Application[2]		
Voice Gateway	X	X	X	X	X	Cisco Unified Communications Manager Express, SRST-enabled Cisco Unity Connection IOS GW Performance Counters[3]	RSM, MSM, MSFC
VoiceMail Gateway		X	X	X			

1. You can display a new Detailed Device View for each of these subcomponents.
2. Voice applications and synthetic testing.
3. For descriptions of the Performance Counters, see Performance Counters Shown in the Detailed Device View, page A-1.

The status categories—Environment, System, Interface, and so forth—list different entries depending upon the device class. The following are some examples of what you may see under the status categories:

- Environment: Temperature, fan, power supply, voltage information

Note See the

- System: Hard disk, RAM, processor, virtual memory information
- Interface: Card, interface, port, voice port information

Note The Voice Port entry displays information for T1, E1, FXS, and FXO ports, as well as Ethernet and Gigabit Ethernet ports that have IP phones connected to them. When new Ethernet ports with phones connected to them are discovered, the Voice Port information is updated after a manual refresh of the Detailed Device View.

- Connectivity: Cluster connectivity information such as cluster name, Cisco Unified Communications Manager status, Cisco Unified Communications Manager list, Active Cisco Unified Communications Manager
- Application: Voice Services, Cisco Unified Communications Manager information

Suspending Device Monitoring

You can stop monitoring a device by selecting it and clicking the Suspend button in the Detailed Device View. Conversely, you can resume monitoring by clicking the Resume button. These actions are also available for suspending and resuming specific components. See these topics for more information:

- Suspending/Resuming Devices, page 3-26

- Suspending/Resuming a Device Component, page 3-27

Suspending/Resuming Devices

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

When you suspend a device, the active alerts and events on the device remain in the Active state. Also, a *Suspended* event occurs on the device, which you can view in the device's Alert Details page. This happens to ensure that:

- You cannot mistakenly remove important information from the display when you suspend a device (when alerts are cleared, they are removed from the Alerts and Events display).
- You can easily resume the device.

Step 1 From the Alerts and Events display, start the view that contains your device. (Devices not managed are in the Suspended Devices view.)

Step 2 Click a device in the Device Name column. The Detailed Device View opens. Depending upon the managed state of the device, either the Suspend or the Resume button is shown.

Step 3 Do one of the following:

- Click **Suspend** to change the device's current managed state to Suspended. Operations Manager no longer polls any device components, nor does it process any traps. The device is moved to the Suspended Devices view. Subsequent events (including traps) are ignored and no longer processed.
- Click **Resume** to change the device's current managed state to Active. Operations Manager resumes polling and trap processing on the device, and the device is moved out of the Suspended Devices view and back into its previous view.

  Note When you resume a device, you must also perform the apply changes action in Polling and Thresholds (see Applying Changes, page 19-60).

- Click **Refresh** to redisplay the page.

Figure 3-10 provides an example of the Detailed Device View for a suspended device. Note the Resume button at the bottom of the window.

Figure 3-10 Detailed Device View—Suspended Device

Suspending/Resuming a Device Component

You can unmanage or remanage device components using the Detailed Device View. When you unmanage a component—changing its managed state to false—Operations Manager no longer polls that component for information. Subsequent events (including traps) are ignored and no longer processed.

Note You cannot resume a device component if the parent device is suspended. You must resume the parent device first.

Step 1 From the Alerts and Events display, click a device in the Device Name column. The Detailed Device View opens.

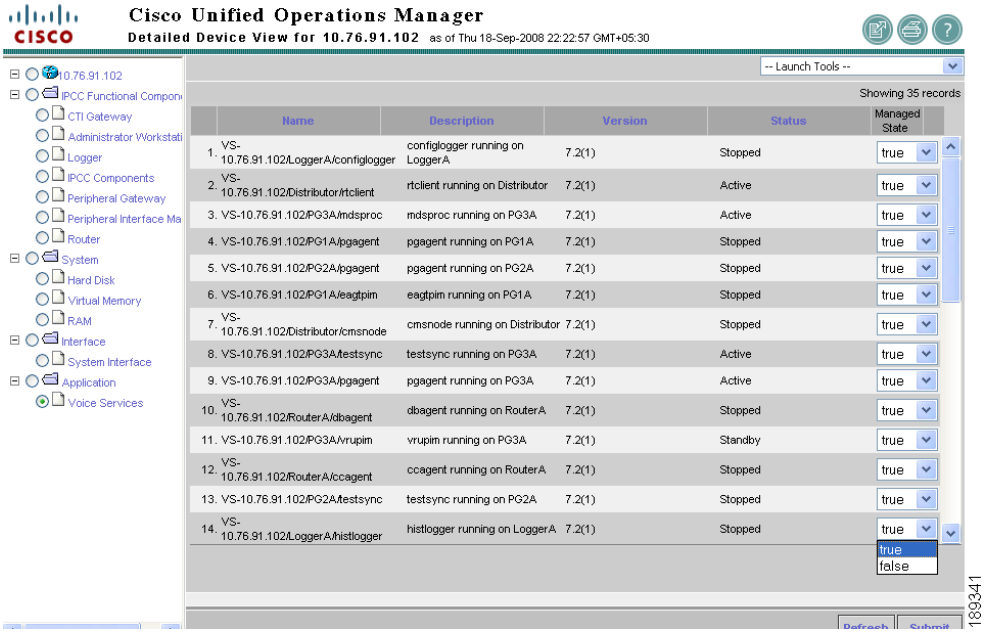
Step 2 Select the component with the instance you want to unmanage.

Step 3 Locate the instance you want to unmanage, and make your change using the list in the Managed State column.

Step 4 Click **Submit**.

Figure 3-11 shows the location of the Managed State column for a managed application (Voice Services).

Figure 3-11 Editing the Managed State of a Device Component



Responding to Alerts

You can respond to alerts from either the Alerts and Events display or the Alert Details page.

- From the Alerts and Events display you can clear or acknowledge an alert (see Responding to Alerts Using the Alerts and Events Display, page 3-28).
- From the Alert Details page you can clear, acknowledge, or annotate an alert. Also, you can send an e-mail in response to an alert (see Responding to Alerts Using the Alert Details Page, page 3-29).

Responding to Alerts Using the Alerts and Events Display

The Alerts and Events Display provides command buttons in the bottom-right corner of the page for you to take action on alerts.

You can perform the following actions:

- Clear an alert (see Clearing an Alert—Using the Alerts and Events Display, page 3-28).
- Acknowledge an alert (see Acknowledging an Alert—Using the Alerts and Events Display, page 3-29).

Clearing an Alert—Using the Alerts and Events Display

Clearing an alert moves the alert to the Cleared state and all the events under it to the user cleared state. Cleared alerts are displayed minimum for 30 minutes and maximum for 60 minutes in the Alerts and Events display.

The alert is purged from database if there are no user cleared events present in the database. As a result, when the next event is raised for the same device, the alert ID remains the same. If all the events are in the cleared state then the alert is purged from the database. As a result, when the next event is raised for the same device, a new alert ID is generated.

When you clear an alert, this status change is populated to all Alerts and Events displays. Once an alert is cleared, the status cannot be changed back. To get the existing state of the events for that device, you must manually delete and re-add the device to Operations Manager. If any new event on the alert recurs, the status reverts to active.

Note The cleared alert is removed from the Alerts and Events display after Operations Manager performs its normal polling and determines that the alarm has been in the cleared state for 30 minutes or longer (from the time of polling). The maximum time that a cleared alert can be seen in the Alerts and Events display is 60 minutes.

Use this procedure to clear one or more alerts from the Alerts and Events display.

Step 1 From the Alerts and Events display, select one or more alerts by selecting check boxes for them.

Step 2 Click **Clear**. A confirmation dialog box appears.

Step 3 Enter your initials.

Step 4 Click **OK**. Operations Manager clears the selected alerts and refreshes the Alerts and Events display.

Acknowledging an Alert—Using the Alerts and Events Display

Acknowledging an active alert signals other users that you are aware of the alert. When you acknowledge an alert, this status change is populated to all Alerts and Events displays.

Use this procedure to acknowledge one or more alerts from the Alerts and Events display.

Step 1 From the Alerts and Events display, select one or more alerts by selecting check boxes for them.

Step 2 Click **Acknowledge**. A confirmation dialog box appears.

Step 3 Enter your initials.

Step 4 Click **OK**. The Alerts and Events display refreshes and the Status column displays acknowledged for the selected devices.

Responding to Alerts Using the Alert Details Page

The Alert Details page provides command buttons in the bottom-right corner of the page (see Figure 3-5). The Suspend button is discussed in Suspending Device Monitoring, page 3-25. This topic explains how you can perform the following actions:

- Acknowledge an alert (see Acknowledging an Alert—Using the Alert Details Page, page 3-30).
- Clear an alert (see Clearing an Alert—Using the Alert Details Page, page 3-30).
- Annotate an alert (see Annotating an Alert, page 3-31).

- Send e-mail in response to an alert (see Sending E-Mail in Response to an Alert, page 3-31).

Acknowledging an Alert—Using the Alert Details Page

Acknowledging an active alert signals other users that you are aware of the alert. When you click the Acknowledge button on the Alert Details page, the alert is acknowledged. To acknowledge all of the events, open the alert, check the Select All check box, and click **Acknowledge**.

If an event on the alert recurs, the alert status reverts to active.

Step 1 From the Alert Details page, select one or more alerts by selecting check boxes for them.

Step 2 Click **Acknowledge**. A confirmation window opens.

Step 3 Click **OK**. In the Alerts and Events display the Status column displays acknowledged for the selected devices.

Clearing an Alert—Using the Alert Details Page

Clearing all active events under an alert changes the alert state in the Alerts and Events display to cleared. You may want to clear an alert when you are receiving erroneous events or are no longer interested in receiving that event. Cleared alerts are displayed minimum for 30 minutes and maximum for 60 minutes in the Alerts and Events display.

The alert is purged from database if there are no user cleared events present in the database. As a result, when the next event is raised for the same device, the alert ID remains the same. If all the events are in the cleared state then the alert is purged from the database. As a result, when the next event is raised for the same device, a new alert ID is generated.

When you click the Clear button after selecting all the events in Alert Details page, the status change is populated to all Alerts and Events displays. The alert status moves into the Cleared state, and the events move into the user cleared state. Once an alert is cleared, the status cannot be changed back. To get the existing state of the device, you must manually delete and re-add the device to Operations Manager.

Note The cleared alert is removed from the Alerts and Events display after Operations Manager performs its normal polling and determines that the alarm has been in the Cleared state for 30 minutes or longer (from the time of polling).

If an event on the alert recurs, the status reverts to Active.

Step 1 From the Alert Details page, select one or more alerts by selecting check boxes for them.

Step 2 Click **Clear**. A confirmation window opens.

Step 3 Click **OK**.

Annotating an Alert

You can annotate an alert by clicking the Annotate button. An editable Annotation dialog box opens; in the dialog box, you can enter up to 255 characters. Any number of annotations can be entered. An annotation is shown whenever other users view the alert from an Alert or Event Details page.

Step 1 From either the Alert or Event Details page or the Event Details page, make a selection on what to annotate and click **Annotate**. The Annotation dialog box opens.

Step 2 Enter your text. Text that exceeds 255 characters is truncated without warning. (If this happens, you can add another annotation.)

Step 3 Click **OK**. The annotated text is displayed in the Notes box.

Sending E-Mail in Response to an Alert

When you click the Notify button in an alert details page (for an alert on a device), Operations Manager opens a dialog box that you can complete to manually send an e-mail notification to multiple recipients. The e-mail notification adds the event/alert details for the selected event. (If you want to send *automatic* e-mail notifications when alerts or events occur on certain devices, use Notification Services to set up an e-mail notification subscription. (See Configuring Notifications, page 15-7.)

Step 1 From the Alert Details page (either for a device alert or a service quality alert), click **Notify**. The E-mail Notification Recipient(s) dialog box opens.

Step 2 Enter a fully qualified DNS name or IP address for an SMTP server.

Step 3 Enter your e-mail address in the Sender Address field.

Step 4 Enter a comma-separated list of e-mail addresses in the Recipient Address(es) field.

Step 5 Enter a subject heading in the Header field.

Step 6 (Optional) Enter a message in the Message field.

Step 7 Click **Send**.

Responding to Events Using the Alert Details Page

The Alert Details page provides command buttons in the bottom-right corner of the page (see Figure 3-5). The Suspend button is discussed in Suspending Device Monitoring, page 3-25. This topic explains how you can perform the following actions:

- Acknowledge an event (see Acknowledging an Event—Using the Alert Details Page, page 3-32).
- Clear an event (see Clearing an Event—Using the Alert Details Page, page 3-32).
- Annotate an event (see Annotating an Event, page 3-32).
- Send e-mail in response to an event (see Sending E-Mail in Response to an Event, page 3-33).

Acknowledging an Event—Using the Alert Details Page

Acknowledging an event signals to other users that you are aware of the event and are working on it.

After the issue gets resolved, it moves to the Cleared state. Cleared events should not be Acknowledged.

Step 1 From the Alert Details page, do one of the following:

- To acknowledge all of the events, open the alert, check the Select All check box.
- To acknowledge a single event, select the check box next to the event.
- To acknowledge multiple events, select the check boxes for the events.

Step 2 Click **Acknowledge**. A confirmation window opens.

Step 3 Click **OK**. In the Alerts and Events display the Status column displays Acknowledged for the selected devices.

Clearing an Event—Using the Alert Details Page

Clearing an event changes the alerts state in the Alerts and Events display to user cleared. When the issue is resolved, the event is moved to the cleared state.

User cleared events do not move to the active state directly. Any subsequent active events are suppressed. If you manually clear an event it signals that you are no longer interested in receiving that event.

Once an event is cleared, the status cannot be changed back. To get the existing state of the device, you must manually delete and re-add the device to Operations Manager. User cleared events are displayed for 30 minutes.

Note The cleared alert is removed from the Alerts and Events display after Operations Manager performs its normal polling and determines that the alarm has been in the Cleared state for 30 minutes or longer (from the time of polling).

If an event on the alert recurs, the status reverts to Active.

Step 1 From the Alert Details page, do one of the following:

- To clear all of the events, open the alert, check the Select All check box.
- To clear a single event, select the check box next to the event.
- To clear multiple events, select the check boxes for the events.

Step 2 Click **Clear**. A confirmation window opens.

Step 3 Click **OK**.

Annotating an Event

You can annotate an alert or an event by clicking the **Annotate** button. An editable Annotation dialog box opens; in the dialog box, you can enter up to 255 characters. Any number of annotations can be entered. An annotation is shown whenever other users view the alert from an Alert or Event Details page.

Step 1 From either the Alert or Event Details page, do one of the following:

- To annotate all of the events, open the alert, check the Select All check box.
- To annotate a single event, select the check box next to the event.
- To annotate multiple events, select the check boxes for the events.

Step 2 Click **Annotate**. The Annotation dialog box opens.

Step 3 Enter your text. Text that exceeds 255 characters is truncated without warning. (If this happens, you can add another annotation.)

Step 4 Click **OK**. The annotated text is displayed in the Notes box.

Sending E-Mail in Response to an Event

When you click the **Notify** button in an alert details page (for an alert on a device), Operations Manager opens a dialog box that you can complete to manually send an e-mail notification to multiple recipients. The e-mail notification adds the event/alert details for the selected event. (If you want to send *automatic* e-mail notifications when alerts or events occur on certain devices, use Notification Services to set up an e-mail notification subscription. (See Configuring Notifications, page 15-7.)

Step 1 From the Alert Details page (either for a device alert or a service quality alert), do one of the following:

- To email notifications for all of the events, open the alert, check the Select All check box.
- To email notification for a single event, select the check box next to the event.
- To email notification for multiple events, select the check boxes for the events.

Step 2 Click **Notify**. The E-mail Notification Recipient(s) dialog box opens.

Step 3 Enter a fully qualified DNS name or IP address for an SMTP server.

Step 4 Enter your e-mail address in the Sender Address field.

Step 5 Enter a comma-separated list of e-mail addresses in the Recipient Address(es) field.

Step 6 Enter a subject heading in the Header field.

Step 7 (Optional) Enter a message in the Message field.

Step 8 Click **Send**.

CHAPTER 4

Monitoring Service Quality Alerts

Note Use the Service Quality Alerts display to view alerts that Operations Manager generates based on SNMP traps sent by Cisco Unified Service Monitor (Service Monitor). To use the Service Quality alerts display, you must have a licensed copy of Service Monitor configured to send traps to Operations Manager. You must also add Service Monitor to Operations Manager; see Adding a Service Monitor Link from Operations Manager, page 21-3.

These topics describe monitoring service quality alerts:

How to Use the Service Quality Alerts Display

The Service Quality Alerts display provides real-time information about IP phone service quality. Service Quality Alerts displays are designed so that you can set them up and leave them running, providing an ongoing monitoring tool that signals you when something needs attention.

When Operations Manager receives traps from Service Monitor, Operations Manager generates an event or events that are rolled up into an alert. The alert is shown on your Service Quality Alerts display. From a Service Quality Alerts display you can launch other windows to obtain more information, including:

- Event details—Displays details for the events that caused the alert to be generated.
- Service quality history—Reports service quality events generated during the previous 24 hours.

Note All Service Quality History reports generated from within the Service Quality Alerts display provide information from the past 24 hours. To generate a Service Quality History report on time spans beyond the last 24 hours, use Service Quality History from the Reports tab by selecting **Reports > Service Quality History**. For more information, see Getting All Stored Information on a Service Quality Event, page 12-15.

Starting the Service Quality Alerts Display

To start the Service Quality Alerts display, select **Monitoring Dashboards > Service Quality Alerts**. Service Quality Alerts appears in a new window.

Tip After you become familiar with the Service Quality Alerts display, you can filter the information it provides as described in Filtering Service Quality Alerts, page 4-5.

Understanding the Layout of the Service Quality Alerts Display

These topics provide details about the information in the Service Quality Alerts display.

View Pane

The view pane lists the currently available *views*, or user-defined device groups, available for Service Quality Alerts. By default, the All Alerts view is always shown and cannot be deleted from your Service Quality Alerts display.

The *current view* is highlighted in the view pane. Alerts for the devices in the current view are shown in the tabular display pane. To select another view, simply click the view name in the view pane.

Icons next to the views indicate the severity of the alerts received from devices in those views, signaling you that the devices may need attention.

For the currently selected view, severity icons also appear next to the alerts in the tabular display to help you quickly locate a specific alert.

The view pane is updated every two minutes. You can have up to 18 views in the view pane in a single Service Quality Alerts display.

Launch Information and View Status Bar Area

The launch information area shows the current time on the server when the Service Quality Alerts display is being viewed. The view status bar lists the selected view, the number of alerts in that view, and, if filters have been applied, displays “(Filtered.)”

Tabular Display Pane

The tabular display pane is the core of the Service Quality Alerts display. It contains a list of alerts that are occurring on the devices in your current view. This pane is refreshed every 60 seconds. For an explanation for all of the items in the tabular display, see Using the Service Quality Alerts Display, page 4-3.

Icons alert you to what needs attention; for example, the severity icons indicate which views and alerts require attention. The tabular display pane is scrollable and can display up to 1,000 records.

Window Tools Area

The top-right corner of the Service Quality Alerts display contains available tools buttons. All buttons are described in Table 4-1.

Table 4-1 Service Quality Alerts Display—Window Tools Buttons

Icon	Meaning	Described in...
	Exports the current display to a PDF file.	—
	Opens the Service Quality Alerts Filter dialog box, for refining the data in the Service Quality Alerts display.	Filtering Service Quality Alerts, page 4-5

Table 4-1 Service Quality Alerts Display—Window Tools Buttons (continued)

Icon	Meaning	Described in...
	Opens a Service Quality Event History report in a separate window.	Understanding the Service Quality History Report, page 12-19
	Opens a new window with the display reformatted so that it is suitable for printing from your browser.	—
	Opens online help.	—

Using the Service Quality Alerts Display

The Service Quality Alerts display shows the alerts that are occurring in your current view. Alerts are grouped by their severity: critical, warning, or informational. Within these severity groupings, alerts with the latest change are listed first.

When an alert is generated, it remains in the Service Quality Alerts display until it is cleared. Alerts are cleared every 8 hours; see Configuring Service Quality Event Settings, page 20-7. While the alert is in the display, if any of its events occur or get updated, the alert is updated. If a Cleared alert reoccurs, a new alert with a new alert ID is shown. If a Cleared event reoccurs, a new event with a new event ID is shown.This display is refreshed every 60 seconds.

Tip You can generate a 24-hour Service Quality History report on all events that occurred on devices in your view by clicking the Service Quality Event History button in the upper-right corner of the window.

Table 4-2 Service Quality Alerts Display—Contents

Heading	Description	
#	Number of alerts—Alerts numbered from 1	
!	Severity of alert	
		Critical
		Warning
		Informational Unidentified Trap alert
	(no icon)	Informational (for all other alerts)
Check box	Select one or more checkboxes to select alerts that you want to clear before clicking the **Clear** button.	
ID	Alert identifier number. Click this link to open a Service Quality Alert Details display.	

Table 4-2 Service Quality Alerts Display—Contents (continued)

Heading	Description	
Destination Type	Call destination: one of the following: • IP Phone • Endpoint	
Extension	Extension number if the destination type is IP phone. Click this link to open an IP Phone report. See Understanding IP Phone Inventory Reports, page 13-11.	
Destination	IP address if the destination type is Endpoint. Click this link to open an IP Phone report. See Understanding IP Phone Inventory Reports, page 13-11.	
Latest Event Time	Date and time alert last occurred or was changed. Diamonds indicate alert activity, such as a new event, new user annotation, and so forth; no diamonds indicates that the alert is stale. Alerts are grouped by severity, and within severities, alerts with the latest change are listed first.	
	◆ ◆ ◆	Alert was updated within last 15 minutes.
	◆ ◆	Alert was updated within last 16-30 minutes.
	◆	Alert was updated within last 31-45 minutes.
	No diamonds	Alert was updated 46 or more minutes ago.

Clearing Service Quality Alerts

Operations Manager automatically clears service quality alerts at a regular interval that is displayed on the Service Quality Event Settings page; for more information, see Configuring Service Quality Event Settings, page 20-7. When an alert is cleared, it no longer appears on the Service Quality Alerts display. However, a record of the alert remains in the database for 31 days and can be displayed from Service Quality History reports. For more information, see Getting Started with Service Quality History Reports, page 12-14.

Use this procedure to manually clear one or more alerts from the Service Quality Alerts display.

Step 1 Select one or more alerts to clear by selecting check boxes for them.

Step 2 Click **Clear**. A confirmation dialog box appears.

Step 3 Click **Yes**. Operations Manager clears the selected alerts and refreshes the Service Quality Alerts display.

Selecting Views for Service Quality Alerts

When you open the Service Quality Alerts display, the All Alerts view is selected in the view pane on the left side of the display. Views control the *device groups* that appear on the Service Quality Alerts display. To select another view, simply click the view name in the view pane.

To add or remove existing views from the view pane, see Activating and Deactivating a View, page 6-2.

To create a new view, first create a user-defined group; see Creating and Editing Groups, page 17-11. Then, use the Manage Views page (see Managing Views, page 6-1) to select the new user-defined group and apply it to Service Quality Alerts. The user-defined group will then be displayed in the view pane. To remove a view from the view pane, deselect it from Service Quality Alerts on the Views page and apply your change.

Note When you add, remove, and update Service Quality Alerts views, you affect all users.

The view pane is updated every two minutes. You can have up to 18 views in the view pane in a single Service Quality Alerts display. For information on how to manage your views, see Managing Views, page 6-1.

Filtering Service Quality Alerts

Filters allow you to manipulate the Service Quality Alerts display to show alerts based on their MOS score, destination, phone model, codec, and Cisco 1040 name or Cisco Unified Communications Manager cluster name.

Note After you apply a service quality alert filter, the filter is applied to all of your views until you change or reset the filter, or close the Service Quality Alerts display. Other clients that access Operations Manager are not affected. When you close the Service Quality Alerts display, your filter is lost.

Step 1 Select **Monitoring Dashboards > Service Quality Alerts**. The Service Quality Alerts display opens.

Step 2 Click the filtering button at the top-right of the Service Quality Alerts display. The Service Quality Alerts Filter dialog box appears.

Step 3 Enter data for only *one* of the following filters:

- **MOS Score**—Enter a value between 1.0 and 5.0.
- **Destination**—Select one of the following radio buttons and enter the appropriate information:
  - **Extension**—Phone extension being called. Select an operator from the list and enter a number.
  - **IP Address**— For a phone, switch, voice gateway, or Cisco 1040. Select an operator from the list and enter a number; depending on the operator, the number that you enter can be a portion of the IP address or the full IP address.
- **Codec**—Enter any of these in a comma-separated list: G711, G722, G728, or G729.
- **Phone Model**—Click the button to select phone models from a list.
- **Sensor MAC**—Enter a comma-separated list of MAC addresses for Cisco 1040 Sensors.

Step 4 Click **OK**.

Resetting Filters on the Service Quality Alerts Display

From the Service Quality Alerts display, you can clear any filters that you have set without changing the selected view.

Step 1 On the Service Quality Alerts display, click **Reset Filter**. A confirmation dialog box appears.

Step 2 Click **Yes**. The Service Quality Alerts display refreshes, displaying all alerts in the currently selected view.

Viewing Events Associated with a Service Quality Alert

Use the Service Quality Alert Details display to see the events that are associated with an alert.

Starting the Service Quality Alert Details Display

The Service Quality Alert Details display provides information about all of the events that were rolled up into a specific alert.

Step 1 Select **Monitoring Dashboard > Service Quality Alerts**. The Service Quality Alerts display opens.

Step 2 Locate the alert you want to investigate and click the alert ID. The Service Quality Alert Details display opens.

Using the Service Quality Alert Details Display

The Service Quality Alert Details display shows all of the events associated with a specific alert. The events are displayed in a table and events with the latest change are listed first. Events remain in the Service Quality Alert Details display until you clear them or until you clear the parent alert. The Service Quality Alert Details table is refreshed every 60 seconds.

The alert name, destination, destination type, and description of the alert are displayed above the Service Quality Alert Details table. Table 4-3 describes the columns in the Service Quality Alert Details table. Table 4-4 describes the command buttons on the Service Quality Alert Details display.

Table 4-3 Service Quality Alert Details Display—Contents

Column	Description	
#	Number of events—Events numbered from 1	
!	Severity of alert	
		Critical
		Warning
		Informational Unidentified Trap alert
	(no icon)	Informational (for all other events)
Event ID	Event identifier number. Click this link to open the event properties page (see Viewing Service Quality Event Attributes, page 4-8).	

Table 4-3 Service Quality Alert Details Display—Contents (continued)

Column	Description
MOS	.05 through 5.0
Cause	One of the following: • Jitter • Packet Loss
Timestamp	Date and time at which the event occurred.
Suppressed Traps	Number of violations for the endpoint for which Service Monitor did not generate a trap. **Note** You can configure Service Monitor to send traps from sensors every *n* minutes. See *User Guide for Cisco Unified Service Monitor.*
Source Type	One of the following: • Endpoint • IP Phone
Source	IP address or DNS name or phone extension.
Tools	Links to tools that provide more information on the event. **Note** Clicking the Service Quality Event History button opens a 24-hour Service Quality History report on the component.

Table 4-4 Service Quality Alert Details Display—Command Buttons

Button	Action
Refresh	Selects the All Alerts view and refreshes the data in the display.
Clear	Clears the service quality alert. See Clearing a Service Quality Alert, page 4-7.
Notify	Sends e-mail notification of the alert. See Sending E-Mail in Response to a Service Quality Alert, page 4-8.
Close	Closes the Service Quality Alert Details display.

Clearing a Service Quality Alert

Operations Manager automatically clears service quality alerts at a regular interval that is displayed on the Service Quality Event Settings page; see Configuring Service Quality Event Settings, page 20-7. When an alert is cleared, it no longer appears on the Service Quality Alerts display. However, a record of the alert remains in the database for 31 days and can be displayed from Service Quality History reports. For more information, see Getting Started with Service Quality History Reports, page 12-14.

You can also clear alerts manually. You can clear multiple alerts simultaneously from the Service Quality Alerts display. See Clearing Service Quality Alerts, page 4-4. Use this procedure to clear a single service quality alert from the Service Quality Alert Details display.

Step 1 From the Service Quality Alert Details display, click **Clear**. A confirmation window opens.

Step 2 Click **OK**.

Sending E-Mail in Response to a Service Quality Alert

When you click the **Notify** button on the Service Quality Alert Details display, Operations Manager opens a dialog box that you can complete to manually send an e-mail notification to one or more recipients. The e-mail notification contains only the text you add; it does not append any alert or event information. (If you want to send *automatic* e-mail notifications when alerts or events occur on certain devices, use Notifications to set up an e-mail notification subscription. See Understanding Notifications, page 15-1.)

Step 1 From the Service Quality Alert Details display, click **Notify**. The E-Mail Notification Recipient(s) dialog box opens.

Step 2 In the E-Mail Notification Recipient(s) dialog box:

a. Enter a fully qualified DNS name or IP address for an SMTP server.

b. Enter your e-mail address in the Sender Address field.

c. Enter a comma-separated list of e-mail addresses in the Recipient Address(es) field.

d. Enter a subject heading in the Subject field.

e. (Optional) Enter a message in the Message field.

f. Click **Send**.

Viewing Service Quality Event Attributes

The Service Quality Event Attributes dialog box provides additional detail about the event, such as the values of MIB attributes at the time of the event.

Step 1 Select **Monitoring Dashboard > Service Quality Alerts**. The Service Quality Alerts display opens.

Step 2 Locate the alert you want to investigate and click the alert ID. The Service Quality Alert Details display appears.

Step 3 Locate the event you want to investigate, and click the event ID. The Service Quality Event Attributes dialog box appears, displaying the event ID and the information in the following table.

Field	Description
Destination	Extension number, or N/A if destination type is Endpoint
Destination IP Address	IP address for an endpoint or an IP phone
Destination Type	One of the following: • Endpoint • IP Phone • Media Server
Destination Model	Phone model, or N/A if destination type is Endpoint
Switch for Destination	IP address, or N/A if destination type is Endpoint
Destination Port	Port type and slot; for example Gi1/0/23
Source Endpoint	Extension number or IP address

Field	Description
Source IP Address	IP address, or N/A if destination type is Endpoint
Source Type	One of the following: • IP Phone • Endpoint
Source Model	Phone model, or N/A if source type is Endpoint
Switch for Source	IP address, or N/A if source type is Endpoint
Source Port	Port type and slot, or N/A if source type is Endpoint
Detection Algorithm	Algorithm used to calculate MOS. One of these: • ITU G.107—Indicates that MOS is calculated on a Cisco 1040 Sensor • CVTQ—Indicates that MOS is calculated on an IP phone or Cisco voice gateway using the Cisco Voice Transmission Quality algorithm
MOS	MOS value during event
Critical MOS Threshold	MOS threshold configured on Operations Manager (see Configuring Service Quality Event Settings, page 20-7)
Cause	One of the following: • Jitter • Packet Loss
Codec	Codec in use on the destination; one of the following: • G711 • G722 • G728 • G729
Jitter	Msec
Packet loss	Number of packets
Details for Events that Are Based on Data from a Sensor	
Sensor MAC	Sensor MAC—Sensor MAC address
Number of Suppressed Traps	The number of traps that Cisco Unified Service Monitor suppressed between the suppression start time and suppression end time **Note** For a given endpoint, Service Monitor sends a trap every *n* (a configurable number) minutes, and additional traps during that time are suppressed (not sent). For more information, see *User Guide for Cisco Unified Service Monitor.*
Suppression Start Time	Date and time that Service Monitor started to suppress traps for this endpoint
Suppression End Time	Date and time that Service Monitor stopped suppressing traps for this endpoint
Details for Events that Are Based on Data from a Cluster	
CVTQ Version	Version of CVTQ algorithm used to calculate MOS

Field	Description
Cluster ID	Cisco Unified Communications Manager cluster ID
Cumulative Concealment Ratio	Total number of concealment frames divided by the total number of speech frames received from the start of the voice stream
Interval Concealment Ratio	Ratio of concealment frames to speech frames in the preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max Incremental Concealment Ratio	Highest interval concealment ratio from start of the voice stream
Concealment Seconds	Number of seconds during which concealment events (lost frames) occurred since the start of the voice stream (includes severely concealed seconds)
Severely Concealed Seconds	Total number of seconds with more than 5 percent concealment frames
Call Duration	Hours, minutes, and seconds, formatted as *n*h *n*m *n*s. For example, a 123-second call would be displayed as 2m 3s.
MOS During Last 8 Secs	MOS value during the last 8 seconds of the call
Min MOS During Call	Minimum MOS value during the call
Max MOS During Call	Maximum MOS value during the call

Step 4 (Optional) To clear the event, click **Clear**. The event no longer appears on the Service Quality Alert Details display.

Step 5 Click **Close** to dismiss the dialog box.

Clearing a Service Quality Event

Use this procedure to remove a single event from a service quality alert.

Step 1 Select **Monitoring Dashboard > Service Quality Alerts**. The Service Quality Alerts display opens.

Step 2 Locate the alert you want to investigate and click the alert ID. The Service Quality Alert Details display appears.

Step 3 Locate the event that you want to clear, and click the event ID.

Step 4 Click **Clear**.

Event Processing for Service Quality Events During High CPU Utilization

During periods of high CPU utilization, Operations Manager limits the number of service quality events that it processes. You will know when this is occurring by the message that appears in the view status bar of the Service Quality Alerts display. The message states that not every alert is being displayed.

The excess Service Quality Alerts display events are written to the NMSROOT\logs\itemlogs\SQTraps\Traps.log file, and these events:

- Do not appear on the Service Quality Alerts display.
- Are not stored in the Alerts and Events history database—They do not appear in Service Quality History reports.

Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as "C:\Program Files\CSCOpx" or C:\PROGRA~1\CSCOpx.

Operations Manager checks CPU utilization on its server every 60 seconds. When CPU utilization reaches and remains at 50% or greater for two minutes, Operations Manager limits the number of service quality events processed until utilization drops below 50%. Table 4-5 lists the number of events that Operations Manager processes.

Table 4-5 Service Quality Event Processing Rates During HIgh CPU Utilization

Operations Manager CPU Utilization	Number of Service Quality Events Processed Per Minute
50%	40
60%	20

CHAPTER 5

Monitoring Phone Activities

These topics describe how to monitor phone activities:

How to Use the Phone Activities Display

The Phone Activities display provides real-time information about the operational status of your IP phones. The displays are designed so that you can set them up and leave them running, providing an ongoing monitoring tool that signals you when something needs attention.

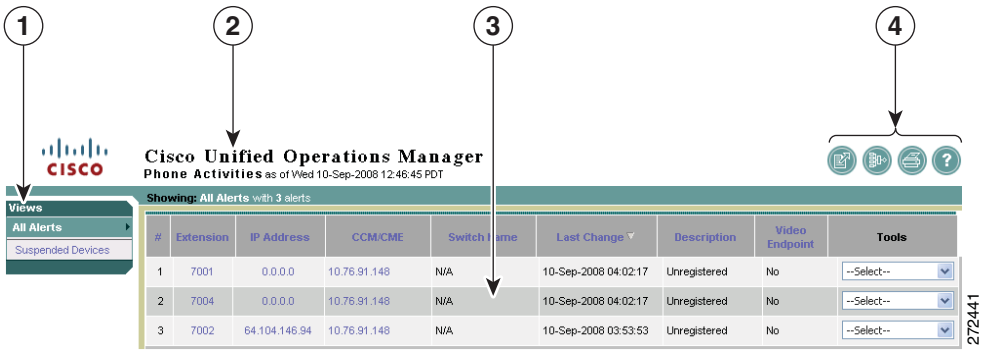
The Phone Activities display shows information about the IP phones in your network that have become disconnected from the switch, are no longer registered to a Cisco Unified Communications Manager, or have gone into SRST mode.

Starting the Phone Activities Display

To start the Phone Activities display, select **Monitoring Dashboard > IP Phone Status**. Figure 5-1 shows an example of a Phone Activities display.

Tip After you become familiar with the Phone Activities display, you can edit the information it provides as described in Customizing the Phone Activities Display, page 5-5.

Figure 5-1 Phone Activities Display



1	View pane. See View Pane, page 5-2.	**3**	Tabular display pane. See Tabular Display Pane, page 5-3.
2	Launch information and view status bar area. See Launch Information and View Status Bar Area, page 5-3.	**4**	Window tools area. See Window Tools Area, page 5-3.

Understanding the Layout of the Phone Activities Display

These topics provide details about the information in the Phone Activities display.

View Pane

The view pane lists the currently available *views*, or logical groupings of devices. Views must be created and activated before they are shown in the Phone Activities display. By default, the All Alerts view is always shown, and cannot be deleted from your Phone Activities display. (To create and activate a view or remove an unwanted view from your display, see Managing Views, page 6-1.)

The *current view* is highlighted in the view pane. The contents of the current view are shown in the tabular display pane to the right of the view pane. To select another view, simply click the view name in the view pane.

Figure 5-2 shows three active views; the current view is All Alerts.

Figure 5-2 Phone Activities Display—View Pane

You can have up to 18 views in the view pane in a single Phone Activities display.

Launch Information and View Status Bar Area

The launch information area shows the current time on the server when the Phone Activities display is being viewed.

The view status bar lists the selected view, which is shown in the tabular display pane.

Tabular Display Pane

The tabular display pane is the core of the Phone Activities display. It contains a list of all the phones that have become disconnected or unregistered, or gone into SRST mode on the devices in your current view. This pane is refreshed every five minutes. For an explanation of all of the items in the tabular display, see Getting Phone Alert Details, page 5-4.

The diamond symbols in the Last Change column indicate which phones have experienced recent activity. When no icon appears in the Last Change column, the alert is no longer current, or *stale*.

The tabular display pane is scrollable and can store up to 1,000 records.

Window Tools Area

The top-right corner of the Phone Activities display contains available tools buttons. All buttons are described in Table 5-1.

Table 5-1 Phone Activities Display—Window Tools Buttons

Icon	Meaning	Described in...
	Exports the current tabular display to a PDF file.	Exporting Data from a Display or Report, page 1-21
	Opens the Filter page, for refining the tabular display in the Phone Activities display.	Filtering Phone Activities, page 5-5
	Opens a printer-friendly version for printing.	Printing Displays or Reports, page 1-22
	Opens the Operations Manager online help.	Using Help, page 1-18

Getting Phone Alert Details

Use the tabular display in the Phone Activities display to obtain more information about the phone alerts that are occurring in your current view.

When a phone alert is generated, it remains in the Phone Activities display as long as the alert is active. In the case where a disconnected phone is moved to a different switch, the phone is removed from the display.

Table 5-2 defines the table elements. All elements are updated every 5 minutes.

Table 5-2 Phone Activities Display—Contents

Heading	Description	
	Severity of alert	
		Critical
		Warning
		Informational Unidentified Trap alert
	(no icon)	Informational (for all other alerts)
Extension	The phone's extension number. Clicking this link opens the IP Phone Detail page (see Understanding IP Phone Inventory Reports, page 13-11).	
IP Address	The phone's IP address. Clicking this link opens the IP phone search page (see Generating the Inventory Analysis Report, page 13-5).	
CCM/CME	The Cisco Unified Communications Manager or Cisco Unified Communications Manager Express that the phone is associated with. Clicking this link opens the Detailed Device View (see the "Viewing Device Elements in Detail" section on page 3-22).	
Switch Name	The switch that the phone is connected to. Clicking this link opens the Detailed Device View (see the "Viewing Device Elements in Detail" section on page 3-22).	
Last Change	Date and time the phone alert last occurred or was changed. Diamonds indicate alert activity, such as a new event, alert acknowledgement, new user annotation, and so forth; no diamonds indicates that the alert is stale. Alerts are grouped by severity, and within severities, alerts with the latest change are listed first.	
		Alert was updated within last 15 minutes.
		Alert was updated within last 16-30 minutes.
		Alert was updated within last 31-45 minutes.
	No diamonds	Alert was updated 46 or more minutes ago.
Description	Registration status of the phone: Registered or Unregistered.	

Table 5-2 Phone Activities Display—Contents (continued)

Heading	Description
Video Endpoint	Yes or No. **Note** Your license controls whether Operations Manager collects data on video endpoints.
Tools	Links to tools that allow you to perform additional tasks. For example: • Run a phone status test (see Using Phone Status Testing, page 8-1). • Configure synthetic tests (see Using Synthetic Tests, page 9-1). • Access the Cisco Unified Communications Manager's administration pages. You must have appropriate permissions to access this information.

Customizing the Phone Activities Display

After setting up a view, you can customize your Phone Activities display by selecting specific *views* and using *filters*:

- Views control the *device groups* that appear on the Phone Activities display. See Selecting Views for the Phone Activities Display, page 5-5.
- Filters control the *specific phone model* you monitor, along with alert *severities* and their *status*. See Filtering Phone Activities, page 5-5.

Selecting Views for the Phone Activities Display

When you select **Monitoring Dashboard > IP Phone Status** to open the Phone Activities display, all available views are listed in the view pane on the left side of the display. If the views shown do not meet your needs, you can create a new view as described in Managing Views, page 6-1.

The view pane is updated every two minutes. You can have up to 18 views in the view pane in a single Phone Activities display. See Managing Views, page 6-1 for information on how to manage your views.

Filtering Phone Activities

Filters allow you to manipulate the Phone Activities display to show alerts based on their extension number, phone model, and activity type.

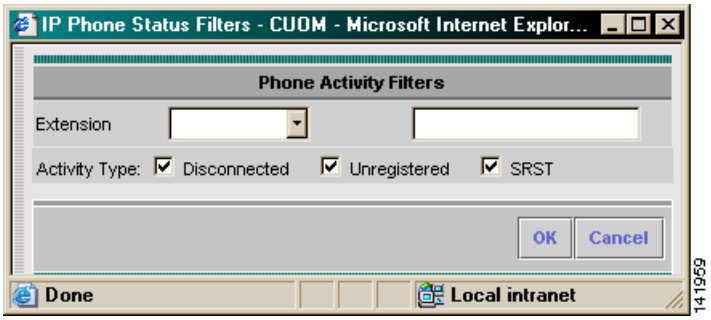
Note Once you use an alert filter, the filter is applied to all of your views until you change the filter; other clients are not affected. When you close the Phone Activities display, your filters are lost. Filters do not affect severity icons in the view pane.

Step 1 Select **Monitoring Dashboard > IP Phone Status**. The Phone Activities display opens.

Step 2 Click the filtering button in the tool button area at the top-right of the Phone Activities display.

Figure 5-3 shows the Phone Activity Filters dialog box.

Figure 5-3 Phone Activity Filters Dialog Box



Step 3 Specify the following filter criteria:

- Extension number
- Activity type

Step 4 Click **OK**.

CHAPTER 6

Managing Views

These topics explain how to work with views in the Monitoring Dashboard displays:

Getting Started with Views

Views are logical groupings of devices that appear in the Monitoring Dashboard displays (Service Level View, Alerts and Events, Phone Activities, Service Quality Alerts, and Unified CM Express). Whenever you create a new User Defined Group in the Group Administration and Configuration page (see Using Group Administration and Configuration, page 17-10), a corresponding view is created.

Once you decide how you want to cluster your devices into a logical set, create and activate a view of these groups so they are shown in the Monitoring Dashboard displays. View elements are not shown until the view is activated and is displayed in the view pane (normally every two minutes).

The Monitoring Dashboard displays can have a maximum of 18 active views.

By default, the Alerts and Events, Phone Activities, and Service Quality Alerts displays contain two default views: All Alerts and Suspended Devices. These views are static and cannot be edited, deactivated, or deleted. The Service Level View contains the All IP Telephony Devices view, which is a default view that cannot be edited, deactivated, or deleted.

Unified CM Express View displays Communications Manager Express device information in a flat table format. This report is also available in Service Level View, but accessing it alone saves you the time that the Service Level View needs to load all the devices if you are only interested in Unified CM Express and Cisco Unity devices.

Creating a View

Views are created when you create a User Defined Group. After you create a User Defined Group, a corresponding view appears in the Views page.

Step 1 Create a User Defined Group using either:

- The Group Administration and Configuration page. (See Managing Groups, page 17-1.)
- Service Level View. (See Using the Service Level View, page 2-1.)

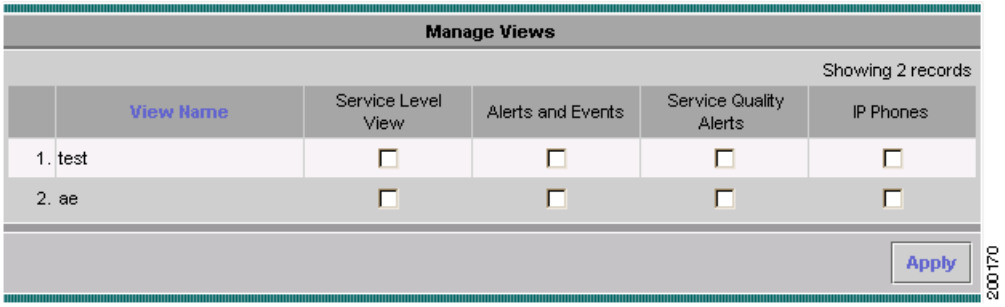
Step 2 Activate the view in the View page. (See Activating and Deactivating a View, page 6-2.)

Activating and Deactivating a View

To include a view in one or more of the Monitoring Dashboard displays (Service Level View, Alerts and Events, Phone Activities, and Service Quality Alerts), you must first activate it. When you activate or deactivate a view, your changes are shown in the appropriate Monitoring Dashboard display when the view pane is refreshed (every two minutes). If you deactivate a view for a particular Monitoring Dashboard display, it is removed from the view once the pane is refreshed. A Monitoring Dashboard display may contain a maximum of 18 active views.

Note You cannot deactivate the All Alerts view or Suspended Devices view.

Step 1 Select **Monitoring Dashboard > Manage Views**. The Manage Views page appears.



Step 2 From the Manage Views page you can do the following:

- Activate views by selecting the radio buttons in the views row that corresponds to the Monitoring Dashboard displays where you want the view to appear.
- Deactivate views by deselecting the radio buttons in the views row that corresponds to the Monitoring Dashboard displays where you do not want the view to appear.

Step 3 Click **Apply**.

Editing a View

You can edit views only by changing the corresponding User Defined Group. Once the User Defined Group is edited, the corresponding view is updated when the view pane is refreshed (normally every two minutes).

You can delete User Defined Groups in the Group Administration and Configuration page. (See Creating and Editing Groups, page 17-11.)

Deleting a View

You can delete views only by deleting the corresponding User Defined Group. Once the User Defined Group is deleted, the corresponding view is deleted when the view pane is refreshed (normally every two minutes).

You can delete User Defined Groups in the Group Administration and Configuration page. (See Deleting Groups, page 17-32.)

Viewing Unified Communications Manager Express Devices

The Unified Communications Manager Express View displays all Cisco Unified Communications Manager Express devices and associated Cisco Unity devices. You can avoid loading the entire Service Level View if you only want to access this information by using Unified CM Express View.

Step 1 To view Unified Communications Manager Express devices, select one of the following:

- **Monitoring Dashboard > Unified CM Express View** loads the table report.
- **Monitoring Dashboard > Service Level View** displays device registration and association for all network devices. Then select the CME Report cloud to view the Unified Communications Manager Express View table report. When you hover over the CME Report cloud you can see CME and CUE details.

Step 2 See Table 2-7 for details on the report fields.

CHAPTER 7

Using Performance Graphs

These topics explain how to use performance graphs:

How to Use Performance Graphs

Cisco Unified Operations Manager (Operations Manager) allows you to select and examine changes in network performance metrics. You can select, display, and chart network performance data in real time. The performance graphs are accessed through the Service Level View, Alert Details page, and Node-to-Node Tests page.

You can create performance graphs from the data that is collected when:

- Voice utilization polling is enabled for devices. (See Editing Polling Parameters, page 19-13.)

  Note Voice utilization polling is disabled by default.

- Data is available on disk from node-to-node tests that you have configured. (See Working with Node-To-Node Tests, page 11-1.)

The following topics describe the data you can graph and help you to understand the information displayed:

What Metrics Can I Include on a Graph?

When you create a performance graph (see Launching a Performance Graph, page 7-6), you select devices and then select among metrics that are appropriate to those devices. Table 7-1 summarizes the types of metrics that you can graph for each device type.

Table 7-2 summarizes the node-to-node test metrics that you can graph.

Table 7-1 Utilization Metrics that You Can Graph by Device Type

Device Type	CPU	Memory	Calls	Port Utilization	Channel Utilization	Device-Specific Usage
Cisco Unified Communications Manager	X	X	X[1]		• BRI • FXS • FXO • T1/E1 PRI • T1 CAS	Cisco Unified Communications Manager Resource Utilization: • MOH multicast • MOH unicast • MTP resource • Transcoder • Hardware conference • Software conference • Percentage conference active • Percentage conference streams active • Location bandwidth available • CTI links active • Registered analog access • Registered MGCP gateways • Registered hardware phones
Cisco Unified Communications Manager Express	X	X	X[2]			• IP phones registered • Key IP phones registered
Cisco Unified Communications Manager-controlled MGCP[3] gateways				• FXS • FXO	• T1/E1 PRI • T1 CAS • BRI[4]	
Cisco Unified Communications Manager or Cluster						
Voice Mail Gateway	X			Voice mail and PBX ports		
Gatekeeper	X	X				Zones[5]
Cisco IOS gateways	X	X	X[6]	• E&M • FXO • FXS	• T1/E1 PRI • T1/E1 CAS[7] • BRI	DSP[8]
SRST	X	X				Minutes in SRST mode

Table 7-1 Utilization Metrics that You Can Graph by Device Type (continued)

Device Type	CPU	Memory	Calls	Port Utilization	Channel Utilization	Device-Specific Usage
Unity	X	X		• Inbound • Outbound		
Unity Express	X					• Capacity utilization • Session utilization • Orphaned mailboxes
Unity Connection	X	X		• Inbound • Outbound • Total number of active ports • Total number of ports • Total number of active inbound ports • Total number of inbound ports • Total number of active outbound ports • Total number of outbound ports		
Unified CCE	X	X				• Number of contact center agents currently logged into Unified CCE • Number of calls in progress in Unified CCE • Number of inbound calls per second

1. Active calls on Cisco Unified Communications Manager.
2. E-phone active call legs.
3. MGCP = Media Gateway Control Protocol.
4. BRI channel status for MGCP gateways is supported only with Cisco Unified Communications Manager 4.1 and later.
5. Zone information includes bandwidth, requests, and errors.
6. Active call legs on Cisco IOS gateway.
7. T1/E1 CAS channel status for Cisco IOS gateways is only reported for Cisco AS5200 Series Universal Access Servers.
8. DSP = Digital signal processor.

The data files for the performance metrics listed in Table 7-1 are located on the server, in the NMSROOT\data\gsu_#GSUdata#_ directory. If you do not have access to the directory, contact a local administrator for the server where Operations Manager is installed. The filenames are created using the device name and the date. These files are kept for 72 hours, after which they are purged.

Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as "C:\Program Files\CSCOpx" or C:\PROGRA~1\CSCOpx.

Table 7-2 Graphable Metrics for Node-to-Node Tests

Node-to-Node Test	Graphable Metrics
UDP Jitter for VoIP	• Source-to-destination packet loss. • Destination-to-source packet loss. • Source to destination jitter. • Destination to source jitter. • Average latency. • Node-to-Node quality.
Ping Echo	Round-trip response time.
Ping Path Echo	Round-trip response time.
UDP Echo	Round-trip response time.
Gatekeeper Registration Delay	Registration response time.

The data files for the performance metrics listed in Table 7-2 are located on the server, in the NMSROOT\data\N2Ntests directory. The data files in this folder are purged after 31 days. If you do not have access to the directory, contact a local administrator for the server where Operations Manager is installed.

Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as "C:\Program Files\CSCOpx" or C:\PROGRA~1\CSCOpx.

Performance Graphing Notes

This section contains information you should be aware of when working with performance graphs.

Table 7-3 Performance Graphing Notes

Summary	Explanation
An MGCP gateway on a Catalyst 6000 switch. When you have all three capabilities (voice gateway, switch, and MGCP) performance graphing cannot graph all the data. Only the common metrics are available for graphing.	When graphing performance metrics for a device that has these three capabilities (voice gateway, switch, and MGCP) you will only be able to graph the common metrics. 1. Select the device for which you want to graph performance metrics. 2. Select **Performance**. A metrics dialog box appears. 3. Select the desired metrics, and click **Next**. A second dialog box appears, listing the MGCP gateway ports. 4. Select a port, and then click **View**. **Note** In the Alert Details page you will not have the option to graph HighUtilization events.
A voice gateway, MGCP, and H323 on a router. When you have all these capabilities on one device, each metric displays two graphs.	When graphing performance metrics for a device that has these capabilities (voice gateway, MGCP, H323, and router), each metric displays two graphs. Also, when graphing multiple devices or devices that have multiple polling intervals, the least common multiple is used to plot the x axis. Real-time graphs will refresh at this common polling interval.
Location Bandwidth Available text box. The location bandwidth is located on the Cisco Unified Communications Manager system.	Enter the location on the Cisco Unified Communications Manager system. This location is configured through Cisco Unified Communications Manager. If you have questions regarding the location bandwidth, see your Cisco Unified Communications Manager documentation. 1. Select the device for which you want to graph the location bandwidth availability. 2. Select **Performance**. A metrics dialog box appears. 3. Select the Location Bandwidth Available check box. 4. Enter the location on the Cisco Unified Communications Manager system where the location bandwidth resides. 5. Click **View**.
Zone Home text box. The zone is located on the gatekeeper system.	Enter the location on the gatekeeper system. This location is configured through the gatekeeper. If you have questions regarding the location bandwidth, see your gatekeeper documentation. 1. Select the device for which you want to graph the zone home. 2. Select **Performance**. A metrics dialog box appears. 3. Select the Zone Home check box. 4. Enter the location on the gatekeeper where the zone home resides. 5. Click **View**.

Table 7-3 Performance Graphing Notes (continued)

Summary	Explanation
In the Select Metrics dialog box for Unified CCE, you will see the following fields: • Agents logged on • Calls in progress • Inbound Calls per second	To view a performance graph for any of these metrics, you must enter the name of the Unified CCE instance for which you want the information, in the field next to Instance Name. Each Unified CCE contains a list of enterprise contact center applications, which are identified by their instance name.
Operations Manager will not display a performance graph for all Unified CCEs.	Operations Manager only collects data for Unified CCEs that have router capabilities. To verify your Unified CCE's capabilities, you can run a device report through device management, and look for *Unified CCE or IPCC Router* in the Device Capabilities column of the Device report. You cannot view a performance graph for Unified CCEs that do not have router capabilities. Instead, you will get a message window stating such.

Launching a Performance Graph

The performance graphs are available through the following:

- Service Level View—See Launching Operations Manager Tools from the Service Level View, page 2-21.
- Route List and Route Group Report—See Viewing the Route List and Route Group Report, page 2-26.
- Alert Details page—See Understanding the Layout of the Alert Details Page, page 3-11.
- Detailed Device View—See Understanding the Layout of the Detailed Device View, page 3-20.
- Node-to-Node Tests page—See Viewing Test Trending, page 11-16.

Before you Begin

- Verify that Operations Manager is monitoring the devices for which you want to collect utilization statistics. This includes the Cisco Unified Communications Manager that the ports are registered to. See Verifying Device Import, page 16-21.
- Enable the voice utilization polling settings. By default the voice utilization polling settings are not enabled. Operations Manager uses the statistics gathered during voice utilization polling for charting network performance. See Voice Utilization Settings—Polling, page 19-23 and Editing Polling Parameters, page 19-13.
- Review the Performance Graphing Notes, page 7-5.

Use this procedure to launch a performance graph from the Service Level View.

Step 1 In the Service Level View (see Using the Service Level View, page 2-1), right-click on the device for which you want to see the performance metrics.

Note If you want to select multiple devices, hold the Ctrl key when clicking the devices in the map view.

Step 2 From the menu select **Performance**. The Select Metrics dialog box appears.

Step 3 Select one or more desired metrics, and click **View Graph**. A performance graph window appears, displaying one or more graphs (see Figure 7-1).

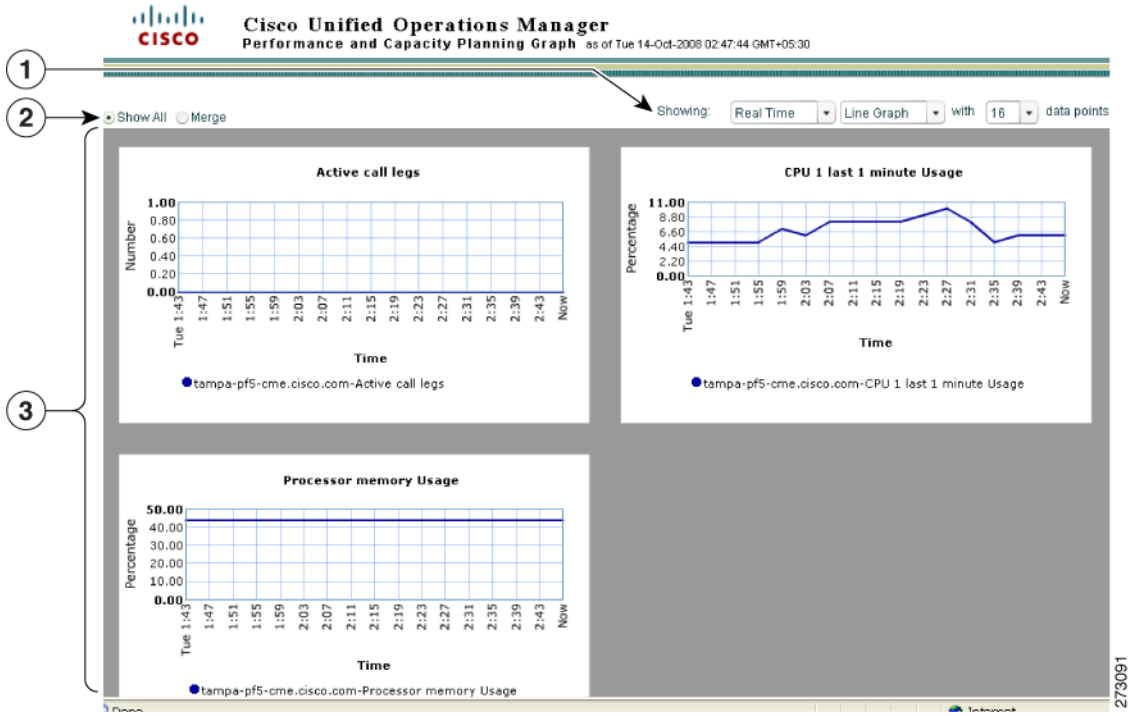
Note If not all expected values are plotted on a graph, the most likely reason is that one or more values are very small in comparison to the maximum value. For example, for the values 250, 2, and 1, the smaller values, 2 and 1, will not be plotted.

Note If you receive errors while creating performance graphs, you can look in the Error.log file for error details. The log file is located in the NMSROOT\data\gsu_#GSUdata#_ directory. Also, see Troubleshooting Performance Graphs, page 7-10.

Working with Graphs

Performance graphs provide real-time information and historical information. When you launch a performance graph, one line graph is displayed for each metric that you select. Each line graph contains 16 data points displayed in real time. All the performance graph windows have the same layout as shown in Figure 7-1.

Figure 7-1 Performance Graph Window Layout



1	Showing Lists. See Showing Lists, page 7-8.	**3**	Graph display pane.
2	Show All and Merge radio buttons. See Show All or Merge, page 7-8.		

Showing Lists

By default, these lists display:

- Real Time—Select the number of hours of data to graph, up to a maximum of 72 hours.

Note If you select a device that does not have data available for the selected time interval, a message appears stating such. An empty graph appears and automatically refreshes periodically. At any time, you can change the time interval to get historical information, if there is any.

- Line Graphs—Select Bar Chart or Area Chart.
- With 16 data points—Select up to a maximum of 240 data points.

Show All or Merge

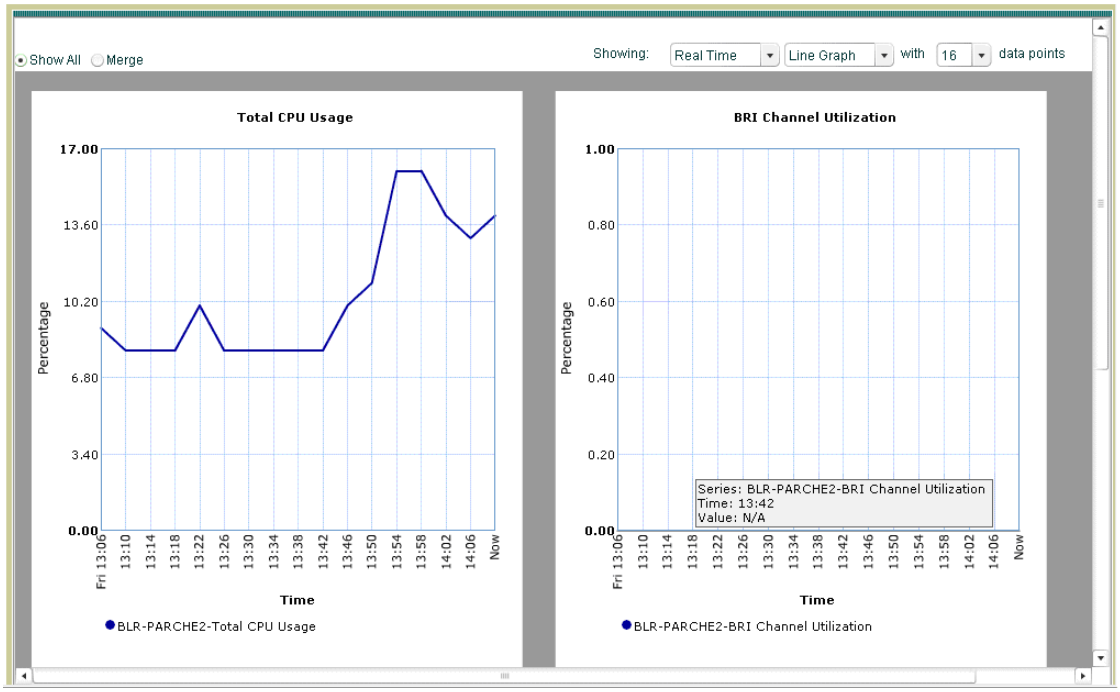
You can show all graphs or merge all graphs regardless of the unit of measure. When you select the Merge radio button, the merged graph is scaled to show all the metrics in the single graph. Also, a new Showing list appears, displaying *Scaled*. You can select Default in place of Scaled from the list. For an example of a merged graph, see Working with a Merged Graph, page 7-9.

Understanding Graphs and Getting More Information

Figure 7-2 shows two graphs, each with the following information:

- Title—Reflects the metric.
- X axis—Shows a time line.
- Y axis—Displays the unit of measure.
- Legend—Includes the name of the device from which the data was gathered and the name of the metric.

Figure 7-2 Default Display of a Performance Graph Window



The BRI Channel Utilization graph, on the right in Figure 7-1, includes a gray line at 0.00 percent. There is no BRI channel utilization data for the device. The gray message box that is shown appears when you hover your cursor over a gray line or gray area in a graph. If you click the gray message box and more information is available, a dialog box will appear.

Working with a Merged Graph

When you select the Merge radio button, individual graphs are merged into a single, scaled graph as shown in Figure 7-3.

Figure 7-3 Merge Scaled Performance Graph

In a merged, scaled graph, the following information is displayed:

- X axis—Shows a time line.
- Y axis—Shows numbers, but no unit of measure. The unit of measure is included in the legend.

- Legend—Includes the name of the device from which the data was gathered, the name of the metric, the ratio by which the data is scaled, and the unit of measure.

To remove scaling from a merged graph, in place of Scaled, select Default. When you select Default, the legend includes only the device name and the metric.

Troubleshooting Performance Graphs

Note For information about what is displayed on graphs, see Understanding Graphs and Getting More Information, page 7-9.

This section contains information that will help you if you encounter problems generating performance graphs.

If you encounter an error, it will likely appear either when you select Performance Graphing from the menu, or when Operations Manager is checking for the data file to graph.

In the first case (when selecting Performance Graphing), you will see an error message that describes the problem and an action to take.

In the second case (when Operations Manager is checking for the data file), an error message saying something like *No data file is available* appears. The error messages appear in the performance graphing log file (Error.log) located at NMSROOT\data\gsu_#GSUdata#_ directory.

Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as “C:\Program Files\CSCOpx” or C:\PROGRA~1\CSCOpx.

Table 7-4 describes the errors and their possible causes, for both of these types of situations. Possible causes for the errors provide a starting point for you to investigate and take corrective action.

Table 7-4 Troubleshooting Performance Graphing Errors

Error	Possible Causes
Cannot collect data.	• Account and credentials are not the same on all Cisco Unified Communications Managers in the cluster. If this is required, see Determining the Media Server Account to Use for Cisco Unified Communications Manager Access, page 16-39. • HTTP server problems: – HTTP server on the device is down. – HTTP server is operational, but the Cisco Unified Communications Manager is down. • Device unreachable due to a network problem. • Performance Monitor process on the media server is down. • The Cisco Unified Communications Manager that the MGCP gateway is registered to is not in Operations Manager inventory. • Device capability is not supported. (Performance graphing supports the following: Cisco Unity, Cisco Unity Express, Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, SRST, H.323 devices, and Voice Mail Gateways.) • Device is suspended or deleted. • Device platform is not support. For device support information, see *Supported Device Table for* Cisco Unified Operations Manager on Cisco.com at http://www.cisco.com/en/US/products/ps6535/products_device_support_tables_list.html.
Cannot collect data because of the following: • The username or password for the device is empty. • The system has the wrong credentials for the device. • The device does not have credential information.	• No credentials in Operations Manager. • Incorrect credentials in Operations Manager. **Note** To add credentials, see Editing Device Configuration and Credentials, page 16-30.

Table 7-4 Troubleshooting Performance Graphing Errors (continued)

Error	Possible Causes
Cannot collect data from the device because of the following: • A processing error occurred. • Parsing or processing errors occurred. • Internal initialization errors occurred. • Initialization problems occurred in the device data collector.	Incorrect Cisco Unified Communications Manager version. Check the following: • The version of the Cisco Unified Communications Manager that is running on the device. • The Cisco Unified Communications Manager version number that is stored in Operations Manager. For instructions, see Viewing Device Details, page 16-32. **Note** If the Cisco Unified Communications Manager version number that is stored in Operations Manager is incorrect, re-add the device. See Understanding the Device and Credentials Repository, page 16-4. For device support information, see *Supported Device Table for* Cisco Unified Operations Manager on Cisco.com at http://www.cisco.com/en/US/products/ps6535/products_device_support_tables_list.html.
Cannot collect WMI counters from the device.	• The device maybe unreachable due to network problems. • An incorrect hostname, username, and/or password was used. • The Remote Procedure Call (RPC) service is not running on the device. • The Current user does not have permission to query WMI.
Cannot collect data from the device. The certificate hostname/IP Address cannot be mapped to the URL hostname/IP Address.	The device is not in DNS.
Incomplete data collected because an error occurred in communicating with the device.	Incorrect Cisco Unified Communications Manager version. Check the following: • The version of the Cisco Unified Communications Manager that is running on the device. • The Cisco Unified Communications Manager version number that is stored in Operations Manager. For instructions, see Viewing Device Details, page 16-32. **Note** If the Cisco Unified Communications Manager version number that is stored in Operations Manager is incorrect, re-add the device. See Understanding the Device and Credentials Repository, page 16-4. For device support information, see *Supported Device Table for* Cisco Unified Operations Manager on Cisco.com at http://www.cisco.com/en/US/products/ps6535/products_device_support_tables_list.html.
Cannot collect data because of the following: • The device returned no data from a required MIB. • The device received no MIB data.	• No data from a required MIB. • A required MIB is not populated on the device. • No MIBs returned data. • Device is unreachable due to a network problem. • Device credentials do not contain a valid SNMP community read string. • SNMP response slow; data collection timed out.

Table 7-4 Troubleshooting Performance Graphing Errors (continued)

Error	Possible Causes
• The rate of queries on the Cisco Unified Communications Manager exceeds the limit. • An error has occurred in the data processing stage.	Too many queries on a Cisco Unified Communications Manager 4.0 or later. **Note** Check the polling settings (see Viewing Polling Parameters, page 19-12); they should not be less than three minutes.
• The Cisco Unified Communications Manager did not have enough time to handle the query requests. • An error has occurred in the data processing stage.	Query exceeded time limit on Cisco Unified Communications Manager 4.0 or later.

Note When working with performance graphs, remember the following:

- If you are not able to collect performance data and you do not see an error message (either a popup message or a message in the log file) indicating the problem, you should verify the status of the device. To do so, use the View/Rediscover/Delete Devices page (see Verifying Device Import, page 16-21). If the device is in the Unreachable state, verify that the device's credentials are correct and rediscover the device (see Performing Manual Inventory Collection on Devices, page 16-31).
- If a gray line or a gray area appears in a graph, hover your mouse over it to obtain a tooltip with an explanation.
- To collect performance data for Cisco Unity Connection, Cisco Unity, or Cisco IP Contact Center, the Windows Management Instrumentation (WMI) credential is required. When adding these devices to Operations Manager, verify that the WMI username and password are provided.

PART 3

Diagnostics

CHAPTER 8

Using Phone Status Testing

Note If you do not have the required software license, you will not be able to use phone status testing.

The following topics describe phone status testing:

Getting Started with Phone Status Testing

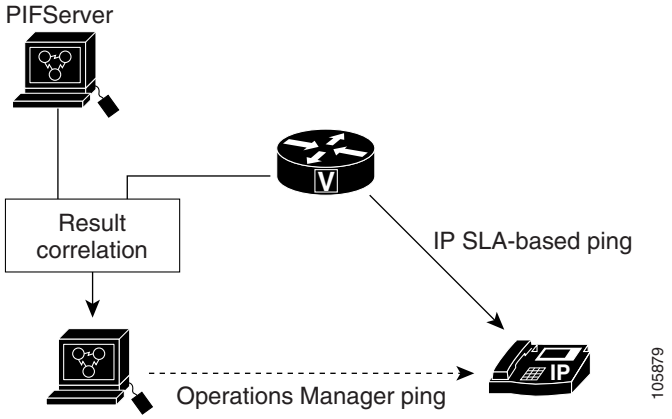
Phone status testing uses Cisco IOS IP SLA (IP SLA) technology to monitor the reachability of key phones in the network. A phone status test consists of the following:

- A list of IP phones to test, selected by you.
- A testing schedule that you configure.
- IP SLA-based pings from an IP SLA-capable device (for example, a switch, a router, or a voice router) to the IP phones and, optionally, pings from Cisco Unified Operations Manager (Operations Manager) to the IP phones.

Note If you ever need to uninstall Operations Manager, be sure to delete all the phone status tests from the application before you uninstall it. If you do not delete these tests, they will continue to run on the router. For instructions on deleting, see Deleting Phone Status Tests, page 8-7.

Figure 8-1 illustrates a phone status test configured on an IP SLA-capable voice router, with Operations Manager ping enabled. Operations Manager configures an echo test on the IP SLA-capable device, provided that the device has enough memory provisioned to allow Operations Manager to do so. Phone status testing also, checks with the phone status process (in the following figure it is referred to as PIFServer, it is used for generating IP phone reports) to verify that the phone is registered.

Figure 8-1 A Phone Status Test



A phone is considered unreachable after there is no response to either an IP SLA-based ping, or an Operations Manager ping, and the phone status is unregistered in the phone status process. Operations Manager generates the PhoneReachabilityTestFailed event. If the phone is not monitored by the phone status process, then a phone is considered unreachable after there is no response to either an IP SLA-based ping, or an Operations Manager ping.

Phone status testing is protocol-independent and can perform tests on phones that operate, for example, under the following protocols:

- MGCP
- SCCP
- SIP

Before You Add a Phone Status Test

You can add phone status tests by using the Create Phone Status test page (see Adding a Phone Status Test—Using the Create Phone Status Test Page, page 8-4), or by using a seed file (see Adding a Phone Status Test—Using a Seed File, page 8-4).

You must be able to provide IP SLA-capable devices and IP phones (extensions and IP addresses) for testing.

Phone status tests do not require information from Operations Manager device inventory. However, when Operations Manager monitors phone-related devices, it can update phone status tests whenever phone information changes.

Maintaining Phone Status Tests

The source device for a phone status test must be monitored in Operations Manager, meaning it must be in Operations Manager inventory for the test to be created.

The following questions and answers supply guidance on how to maintain phone status tests. The answers describe common occurrences and explain whether you need to take action as a result.

Q. What happens when a router is rebooted?

A. When a router is rebooted, the phone status tests are lost. However, Operations Manager reconfigures the test when the router becomes available. While the router is down, the Operations Manager ping continues to run, if you have enabled Operations Manager ping.

Q. What happens after I move a phone to a different Cisco Unified Communications Manager?

A. Phone status tests continue to run, except when phone information (IP address or extension number) changes and phone-related devices are not monitored by Operations Manager (see Table 8-1 for more information); update the seed file and add the test again. If you want to configure the test on the IP SLA-capable device closest to the new Cisco Unified Communications Manager, update the seed file and add the test again.

Using Phone Status Testing

When you open the Phone Status Tests page, you view a table of existing phone status tests with the status for each test. From this page, you can do any of the following:

- Add a phone status test. By using the Create Phone Status test page (see Adding a Phone Status Test—Using the Create Phone Status Test Page, page 8-4), or by using a seed file (see Adding a Phone Status Test—Using a Seed File, page 8-4).
- Configure phone status tests. You can update the schedule for one or more phone status tests and enable or disable the Operations Manager ping. See Editing Phone Status Tests, page 8-6.
- Delete phone status tests. You can delete one or more phone status tests from Operations Manager and from the routers on which the tests run. See Deleting Phone Status Tests, page 8-7.
- View phone status test details. You can view details for one or more phone status tests. See Viewing Phone Status Test Details, page 8-7.

Step 1 Select **Diagnostics > Phone Status Tests**. The following information is displayed.

Note If you do not have the required software license, you will not be able to use phone status testing. The Diagnostic tab will not appear in Operations Manager.

Field	Description
Test Name	Test name—Provide a name for the test when you add it to Operations Manager. See Adding a Phone Status Test—Using a Seed File, page 8-4.
Status	Status can be one of the following: • Started—The test is scheduled to run. • Running—The test is currently running. • Stopped—The test is not scheduled to run.

Adding a Phone Status Test—Using the Create Phone Status Test Page

You can add a phone status test using the Create Phone Status Test page.

Step 1 Select **Diagnostics > Phone Status Tests** and click **Create**. The Create Phone Status Test page appears.

Note Operations Manager provides you with multiple launch points for the Create Phone Status Test page. For example, you can also open the page through a phone report, or the Phone Activities display.

Step 2 In the Source pane, use the device selector to choose a source device, or enter the device's name (or IP address) in the Name field.

Step 3 (Optional) Enter the Interface.

Step 4 Click the **Add from Phone Report** button. The All IP Phones/Lines report opens.

Step 5 On the All IP Phones/Lines report, selected the check box next to the phones you want to add to the test. Click **Select**.

Note If you select a single phone which shares its extension with other phones in the personalized report, the report generated will have details about all the phones (including the selected phone).

Step 6 In the Run area of the Create Phone Status Test page, do the following:

- Schedule when to run the test. Choose an interval time, start and stop times, and the days the test should run.
- Enter a name for the test.
- Choose whether to use ping from the Operations Manager server. By default, phone status testing pings a phone from both the Operations Manager server and the router. Select this check box to disable ping from the Operations Manager server.

Step 7 Click **OK**. One of the following is displayed:

- Informational messages for you to read and acknowledge.
- Errors and recommended actions for you to take.

Adding a Phone Status Test—Using a Seed File

You can add one phone status test at a time by importing a file with a list of extensions to include in the test.

Before you Begin

- Verify that your seed file is formatted correctly. For details, see Formatting an Import File for Phone Status Testing, page 8-5.
- Place the seed file on the server, in the `NMSROOT\ImportFiles` directory. If you do not have access to the directory, contact a local administrator for the server where Operations Manager is installed.

Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as "C:\Program Files\CSCOpx" or C:\PROGRA~1\CSCOpx.

Step 1 Ensure the steps in Before you Begin are complete.

Step 2 Select **Diagnostics > Phone Status Tests** and click **Import**. The Import Phone Status Test page appears.

Step 3 Enter the name of the seed file.

Step 4 In the Run area, do the following:

- Schedule when to run the test. Choose an interval time, start and stop times, and the days the test should run.
- Enter a name for the test.
- Choose whether to use ping from the Operations Manager server. By default, phone status testing pings a phone from both the Operations Manager server and the router. Select this check box to disable ping from the Operations Manager server.

Step 5 Click **OK**. One of the following is displayed:

- Informational messages for you to read and acknowledge.
- Errors and recommended actions for you to take.

Note In some cases, you might need to correct an entry in the seed file. If so, correct the seed file, copy it to the seed file directory, and return to Step 2.

Note Operations Manager does not add a phone status test until all errors are resolved.

Validation of the information in the seed file completes and Operations Manager starts to create tests on the IP SLA-enabled devices. If errors occur during test creation, an error message is displayed. Otherwise, the Phone Status Test Manager window is displayed, showing the newly added test.

Formatting an Import File for Phone Status Testing

A phone status testing import file should list all the phones that you need to create a single test. You can use a six-column or eight-column file format. The first six columns are the same for both file formats.

The information that you must provide for each phone is:

- Extension number.
- IP address.
- MAC address.

You must also provide the IP address and read and write community strings for the router closest to the Cisco Unified Communications Manager that the phone is registered to.

Handle phones with shared lines or multiple extensions as follows:

- Shared lines—Enter one or both phones; Operations Manager can run one test for each phone on a shared line.
- Multiple extensions—No matter how many of the extensions for a phone that you enter, Operations Manager runs only one test for the phone.

Each line of the seed file must contain:

- Six or eight columns. If a column is not used, you must enter a space.
- A colon separating the columns.

Table 8-1 Seed File Format for Phone Status Testing

Column Number	Description
1	Phone extension.
2	Phone MAC address.
3	Phone IP address.
4	IP SLA-enabled device (router, switch, or voice router).
5	Read community string for the IP SLA-enabled device.
6	Write community string for the IP SLA-enabled device.
7	SNMPv3 username (used in the eight-column format only)
8	SNMPv3 password (used in the eight-column format only)

Example 8-1 shows a sample six-column import file. Example 8-2 shows a sample eight-column import file.

Example 8-1 Phone Status Testing Six-Column Import File

```
[Extension]:[MAC Address]:[IPAddress]:[IPSLA Router]:[Read Community]:[Write community]

4000:200000000001:172.20.121.1:10.76.34.194:private:private
```

Example 8-2 Phone Status Testing Eight-Column Import File

```
2) [Extension]:[MAC Address]:[IPAddress]:[SAA Router]:[Read Community]:[Write community]:
[snmpv3UserName]:[snmpv3Passwd]

#4000:200000000001:172.20.121.1:10.76.34.194:!{[NOVALUE]}!:!{[NOVALUE]}!:admin:admin
```

Editing Phone Status Tests

You can change the source device, change phones, update the schedule, or enable or disable the Operations Manager ping for one or more phone status tests. See Getting Started with Phone Status Testing, page 8-1 for information about the Operations Manager ping.

Step 1 Select **Diagnostics > Phone Status Tests**.

Step 2 Select one or more tests and click **Edit**. The Phone Status Test Configuration page appears.

Step 3 Change any of the following.

Field	Description
Source Router	Change the source device.
Selected Phones	Change the phones to monitor.
Select Test Interval	Select the number of minutes (between 1 and 10) from the start of one test to the start of the next test.
Test Time	Select a daily start and end time for tests.
Days of the Week	Select one or more days on which to run tests.
Do not use ping from Operations Manager server	Deselect this check box to enable phone reachability to ping phones from both the Operations Manager server and the router. Select this check box to disable the ping from the Operations Manager server.

Step 4 Click **Finish**.

Deleting Phone Status Tests

You can delete one or more phone status tests.

Step 1 Select **Diagnostics > Phone Status Tests**.

Step 2 Select one or more tests and click **Delete**. A confirmation message is displayed.

Step 3 Click **OK** to delete the tests.

Viewing Phone Status Test Details

Step 1 Select **Diagnostics > Phone Status Tests**.

Step 2 Select a test and click **View**. The Testing Details page appears.

Step 3 The Testing Details page displays the test parameters and schedule and the extension numbers of the tested phones.

CHAPTER 9

Using Synthetic Tests

Note If you do not have the required software license, you will not be able to use synthetic tests.

Synthetic tests are tests that you configure to run periodically. They use voice applications as other devices (phones) normally would, and analyze the behavior of the system. Cisco Unified Operations Manager (Operations Manager) can monitor the information returned from the synthetic tests and generate events based on the results.

The following topics are covered:

Getting Started with Synthetic Tests

Synthetic tests are used to measure the availability of voice applications. Synthetic tests verify whether the voice application can service requests from a user. For example, you can use synthetic tests to verify that phones can register with a Cisco Unified Communications Manager.

Synthetic tests use synthetic phones to measure the availability of voice applications by emulating your actions. For example, a synthetic test places a call between clusters and then checks to see if the call is successful.

If a synthetic test fails, Operations Manager generates a critical event. Such events are displayed in the Alerts and Events display (see Monitoring Alerts and Events, page 3-1).

Operations Manager supports synthetic testing for the following applications:

- Cisco Unified Communications Manager and Cisco Unified Communications Manager Express
- Cisco TFTP Server
- Cisco Emergency Responder
- Cisco Conference Connection

- Cisco Unity, Cisco Unity Express, and Cisco Unity Connection

Table 9-1 lists the synthetic tests and the results that each test must produce to pass.

Note The phones in all scheduled synthetic tests, except for Phone Registration, remain registered unless there is a failure.

Table 9-1 Synthetic Test Descriptions and Expected Results

Synthetic Test	Description	Expected Results
Phone Registration Test	Opens a connection with the Cisco Unified Communications Manager and registers a simulated IP phone.	Successful registration of the phone.
Dial-Tone Test	Simulates an off-hook state to the Cisco Unified Communications Manager and checks for receipt of a dial tone.	Receives a dial tone signal from the Cisco Unified Communications Manager.
End-to-End Call Test	Initiates a call to a second simulated or real IP phone.	• Registers, goes off-hook, and places the call • Ring indication • Destination phone goes off-hook to accept the call **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.
TFTP Download 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.

Table 9-1 Synthetic Test Descriptions and Expected Results (continued)

Synthetic Test	Description	Expected Results
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
Message-Waiting Indicator Test	Calls the target phone and leaves a voice message in the voice mailbox.  **Tip** The destination phone for the Message-Waiting Indicator Test should be configured as Call Forward after X number of rings before moving to voicemail. If it is configured for Call Forward Always, the test will fail.	Activation of the phone's message-waiting indicator. The message is then deleted and the message-waiting indicator is deactivated.

Configuring Synthetic Tests

Step 1 Configure the phones that you will use to run synthetic tests, following the recommendations in Configuring Applications for Synthetic Tests, page 9-3.

Step 2 Configure the synthetic tests, following the instructions in Creating Synthetic Tests, page 9-6.

Configuring Applications for Synthetic Tests

You can configure synthetic tests for each Cisco Unified Communications Manager and Cisco voice application in your network. For each synthetic test, you must configure one or more phones in the related Cisco Unified Communications Manager or Cisco voice application.

Caution Only Cisco 7960 IP Phones are supported for synthetic tests.

When configuring phones:

- Create one phone extension number and one MAC address for each test and use it for that test *only*.
- Make sure that the combination of the phone extension number and the MAC address used in a test is unique across the voice cluster.

Caution Failure to follow these recommendations may result in synthetic test failures.

Before you configure phones, work through Determining How Many Phones You Need, page 9-4 to estimate how many phones you will need based on the tests you want to run.

As you configure phones on each Cisco Unified Communications Manager, use the worksheet in Synthetic Test Worksheets, page 9-25 to simplify data entry into Operations Manager.

Determining How Many Phones You Need

The number of phones you must create in a Cisco Unified Communications Manager for use in synthetic tests depends on:

- The number of synthetic tests you want to configure
- The type of tests you want to run

Table 9-2 provides a worksheet for determining how many phones you need.

Table 9-2 Number of Phones Required for Synthetic Tests

Number of Tests	Type of Test	Phones Needed for Test	Total Phones Needed
	Phone Registration	1 (synthetic phone)	
	Dial-Tone	1 (synthetic phone)	
	End-to-End Call with real phones	2 (1 synthetic phone and 1 real phone)	
	End-to-End Call with synthetic phones	2 (synthetic phones)	
	TFTP Download	0	
	Emergency Call (without On Site Alert Number)	2 (synthetic phones)	
	Emergency Call (with On Site Alert Number)	3 (synthetic phones)	
	Cisco Conference Connection	2 (synthetic phones)	
	Message-Waiting Indicator	2 (synthetic phones)	

Configuring Phones

When you configure phones in a Cisco Unified Communications Manager, you must consider the requirements listed in Meeting the Requirements for Target Phones, page 9-4 and record the phone information as you enter it. A sample worksheet is provided in Synthetic Test Worksheets, page 9-25.

Meeting the Requirements for Target Phones

For the following synthetic tests, there are special requirements for the target phones:

- Message-Waiting Indicator Test—When creating the subscriber on Cisco Unity that you are going to use for synthetic testing, configure the subscriber according to the following:

  - The Set subscriber for self-enrollment at next login check box must be deselected, or you must use a real phone to dial into the Cisco Unity device and complete the personalization process.
  - Set the password option to Password never expires.
  - The destination phone for the Message-Waiting Indicator Test should be configured as CALL FORWARD after X number of rings before moving to voicemail. If it is configured for CALL FORWARD ALWAYS, the test will fail.
- Emergency Call Test—The outgoing PSAP must use a local phone (not 911). Also, for the OSAN, use a synthetic phone only (do not use your local onsite security phone).
- Cisco Conference Connection Test—For Cisco Unified Communications Manager Release 4.0, when you are configuring a route pattern in Cisco Unified Communications Manager to connect to Cisco Conference Connection, you must select the Allow overlap sending option.

Recording Phone Extension Numbers on a Worksheet

As you configure phones, record them on a worksheet similar to those in Table 9-11 through Table 9-14. Use the worksheet that is appropriate for the synthetic test you are configuring.

Note Do not use phone extension numbers that consist of more than twelve digits.

Use a copy of the worksheets to record:

- **Cisco Unified Communications Manager**—You can obtain a list of Cisco Unified Communications Managers from the Create Synthetic Test page. For instructions on opening the Create Synthetic Test page, see Maintaining Synthetic Tests, page 9-5.
- **Phone extension numbers and MAC addresses**—Record the phone extension numbers and MAC addresses you plan to use.
- **Passwords and usernames**—Record the passwords and usernames you plan to use.

Maintaining Synthetic Tests

The Synthetic Tests page lists any synthetic tests that have been set up. To open the Synthetic Tests page, select **Diagnostics > Synthetic Tests**.

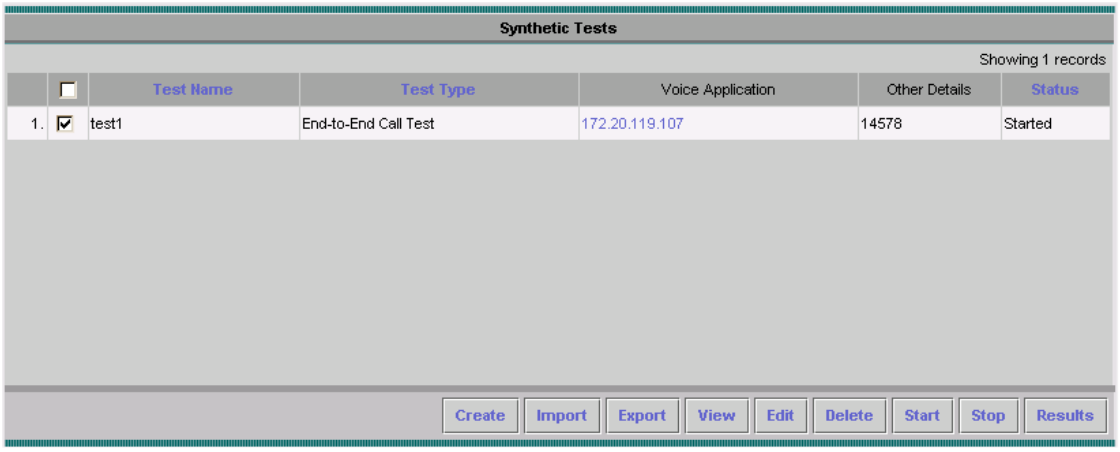
Note If you do not have the required software license, you will not be able to use synthetic tests. The Diagnostic tab will not appear in Operations Manager.

These topics explain how to use the Synthetic Tests page:

- Viewing Synthetic Test Results, page 9-23

Figure 9-1 shows an example of the Synthetic Tests page.

Figure 9-1 Synthetic Tests Page



Heading	Description
Test Name	The name provided by the user.
Test Type	The type of synthetic test that is configured.
Voice Application	The IP address of the server where the application is located.
Status	Test status.
Other Details	Any notes.

Creating Synthetic Tests

Before creating synthetic tests, you must configure phones, following the recommendations in Configuring Applications for Synthetic Tests, page 9-3. When you create synthetic tests, use the worksheet recommended in Configuring Phones, page 9-4 to assist you in entering the correct data.

Note If you do not have the required software license, you will not be able to use synthetic tests.

Note Do not create more than 100 end-to-end call tests that run at one-minute intervals. Configure additional end-to-end call tests to run at various intervals other than one minute.

You can also set up synthetic tests from the Service Level View (see Setting Up Synthetic Tests, page 2-27), as well as from the Launch tools menu that is located on the Detailed Device View and Alert Details page.

The following sections describe the steps for creating synthetic tests:

- Creating a Phone Registration Test, page 9-7

- Creating an End-to-End Call Synthetic Test, page 9-9
- Creating a TFTP Download Synthetic Test, page 9-10
- Creating a Cisco Conference Connection Synthetic Test, page 9-11
- Creating an Emergency Call Synthetic Test, page 9-12
- Creating a Message-Waiting Indicator Synthetic Test, page 9-14

Creating a Phone Registration Test

You can only configure one Phone Registration test per Cisco Unified Communications Manager.

Step 1 Select **Diagnostics > Synthetic Tests**. The Synthetic Tests page appears.

Step 2 Click **Create**. The Create Synthetic Test page appears.

Step 3 From the Test Type pull-down menu, select **Phone Registration Test.**

Step 4 From the group selector in the left pane, select the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express system for which you want to set up the test.

Step 5 Click the arrow button next to the Cisco Unified Communications Manager/Express field to enter the name or IP address of the selected device.

Step 6 Enter the synthetic phone's MAC address. If you used the group selector to choose the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express system, the MAC address field is automatically populated.

Note The MAC address for synthetic phones must be between 00059a3b7700 and 00059a3b8aff and must be in the format 00059a3b7700.

Step 7 Select a protocol type.

Step 8 Select a parameter type:

- If you select Extension, enter the extension for the phone.
- If you select SIP URI, enter the SIP Uniform Resource Identifier (SIP URI).

Note The SIP URI should be in the format sip:extn@ccm; for example, sip:7690@ct-sd.cisco.com.

Step 9 Select a criteria for success, either Registration Success or Registration Failure.

Step 10 If desired, you can change the registration time threshold setting (default is 2000 milliseconds).

Note The phone registration threshold measures the time that it takes for a phone (SIP or SCCP phone) to register with a Cisco Unified Communications Manager. If the threshold is exceeded, a warning event is generated.

Step 11 In the Run pane configure when the test should run.

- If you want the test to run immediately, select the **now** radio button.
- If you want to schedule the test to run at certain intervals, do the following:

- Select the **every** radio button.
- Choose how often you want the test to run.
- Enter the times between which you want the test to run.
- Select the days on which the test should run.
- Enter a test name.

Step 12 Click **Create**.

Creating Dial-Tone Synthetic Tests

You can configure only one dial-tone test per Cisco Unified Communications Manager.

Step 1 Select **Diagnostics > Synthetic Tests**. The Synthetic Tests page appears.

Step 2 Click **Create**. The Create Synthetic Test page appears.

Step 3 From the Test Type pull-down menu, select **Dial-Tone Test.**

Step 4 From the group selector in the left pane, select the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express system for which you want to set up the test.

Step 5 Click the arrow button next to the Cisco Unified Communications Manager/Express field to enter the name or IP address of the selected device.

Step 6 Enter the synthetic phone's MAC address. If you used the group selector to choose the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express system, the MAC address field is automatically populated.

Note The MAC address for synthetic phones must be between 00059a3b7700 and 00059a3b8aff and must be in the format 00059a3b7700.

Step 7 If desired, you can change the dial-tone time threshold setting (default is 500 milliseconds).

Note The dial-tone time threshold measures the time between when an SCCP phone goes offhook to when it receives a dial tone from Cisco Unified Communications Manager. If the threshold is exceeded, a warning event is generated.

Step 8 In the Run pane configure when the test should run.

- If you want the test to run immediately, select the **now** radio button.
- If you want to schedule the test to run at certain intervals, do the following:
  - Select the **every** radio button.
  - Choose how often you want the test to run.
  - Enter the times between which you want the test to run.
  - Select the days on which the test should run.
  - Enter a test name.

Step 9 Click **Create**.

Creating an End-to-End Call Synthetic Test

You have the option of configuring the target phone as a real phone or a synthetic phone. The default setting is a synthetic phone.

Step 1 Select **Diagnostics > Synthetic Tests**. The Synthetic Tests page appears.

Step 2 Click **Create**. The Create Synthetic Test page appears.

Step 3 From the Test Type pull-down menu, select **End-to-End Call Test**.

Step 4 In the Caller pane, do the following:

- Enter the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express system.

  Note You can use the group selector in the left pane to enter a device: Select the device in the group selector, and then click the arrow button next to the Cisco Unified Communications Manager/Express field.

- Enter the synthetic phone's MAC address. If you used the group selector to choose the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express system, the MAC address field is automatically populated.

  Note The MAC address for synthetic phones must be between 00059a3b7700 and 00059a3b8aff and must be in the format 00059a3b7700.

- Select a protocol type.
- Select a parameter type:
  - If you select Extension, enter the extension for the phone.
  - If you select SIP URI, enter the SIP Uniform Resource Identifier (SIP URI).

    Note The SIP URI should be in the format sip:extn@ccm; for example, sip:7690@ct-sd.cisco.com.

Step 5 In the Recipient pane, do the following:

- Select either the Synthetic Phone or Real Phone radio button.
- Enter the name or IP address of the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express system.

  Note You can use the group selector in the left pane to enter a device: Select the device in the group selector, and then click the arrow button next to the Cisco Unified Communications Manager/Express field.

- Enter the phone's MAC address.
- Select a protocol type (if you selected the Real Phone radio button, this option is grayed out).
- Select a parameter type (if you selected the Real Phone radio button, this option is grayed out): If you select Extension, enter the extension for the phone. If you select SIP URI, enter the URI.

Note The Parameters area is grayed out when Synthetic Phone is selected.

Step 6 In the Parameters pane, do the following:

- (Optional) Select **Wait for Answer**. If you selected the Synthetic Phone radio button, this option is grayed out.
- (Optional) Select **Enable RTP transmission**. If you selected the Synthetic Phone radio button, this option is grayed out.
- Choose a criterion for success, either Call Success or Call Failure.
- If desired, you can change the call setup time threshold setting (default is 10000 milliseconds).

Note The call setup time threshold measures the time between when you are done dialing the number to when the Cisco Unified Communications Manager sets up the call (using SIP or SCCP phones). If the threshold is exceeded, a warning event is generated.

Step 7 In the Run pane configure when the test should run.

- If you want the test to run immediately, select the **now** radio button.
- If you want to schedule the test to run at certain intervals, do the following:
  - Select the **every** radio button.
  - Choose how often you want the test to run.
  - Enter the times between which you want the test to run.
  - Select the days on which the test should run.
  - Enter a test name.

Note Do not create more than 100 end-to-end call tests that run at 1-minute intervals. Configure any additional end-to-end call tests to run at various intervals greater than 1 minute.

Step 8 Click **Create**.

Creating a TFTP Download Synthetic Test

You can configure only one TFTP download test for each Cisco Unified Communications Manager.

Step 1 Select **Diagnostics > Synthetic Tests**. The Synthetic Tests page appears.

Step 2 Click **Create**. The Create Synthetic Test page appears.

Step 3 From the Test Type pull-down menu, select **TFTP Download Test**.

Step 4 From the group selector in the left pane, select the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express system for which you want to set up the test.

Step 5 Click the arrow button next to the TFTP Server field, to enter the name or IP address of the selected device.

Step 6 In the Run pane configure when the test should run.

- If you want the test to run immediately, select the **now** radio button.
- If you want to schedule the test to run at certain intervals, do the following:
  - Select the **every** radio button.
  - Choose how often you want the test to run.
  - Enter the times between which you want the test to run.
  - Select the days on which the test should run.
  - Enter a test name.

Step 7 Click **Create**.

Creating a Cisco Conference Connection Synthetic Test

You can configure only one Cisco Conference Connection test for each Cisco Conference Connection Server.

Step 1 Select **Diagnostics > Synthetic Tests**. The Synthetic Tests page appears.

Step 2 Click **Create**. The Create Synthetic Test page appears.

Step 3 From the Test Type pull-down menu, select **Cisco Conference Connection Test**.

Step 4 In the CCC Parameters pane, enter the following:

- Cisco Conference Connection server name or IP address.

  Note You can use the group selector in the left pane to enter a device: Select the device in the group selector, and then click the arrow button next to the Cisco Conference Connection field.

- Username.
- Password.
- Meeting ID.
- Access Number (route pattern between the Cisco Unified Communications Manager and the Cisco Conference Connection server).

Step 5 In the First Caller pane, enter the following:

a. The Cisco Unified Communications Manager where Cisco Conference Connection is configured.

Note You can use the group selector in the left pane to enter a device: Select the device in the group selector, and then click the arrow button next to the Cisco Unified Communications Manager/Express field.

b. The phone's MAC address. Use the format 00059a3b7700. If you used the group selector to choose the Cisco Unified Communications Manager, the MAC address field is automatically populated.

Note The MAC address for synthetic phones must be between 00059a3b7700 and 00059a3b8aff and must be in the format 00059a3b7700. Operations Manager verifies only that the MAC address number entered in the Create Synthetic Test page is syntactically valid. It is your responsibility to make sure the correct numbers are entered, as configured in the Cisco Unified Communications Manager.

Step 6 In the Second Caller pane, enter the following:

a. The name or IP address of the Cisco Unified Communications Manager where Cisco Conference Connection is configured.

Note You can use the group selector in the left pane to enter a device: Select the device in the group selector, and then click the arrow button next to the Cisco Unified Communications Manager/Express field.

b. The phone's MAC address. Use the format 00059a3b7700.

Step 7 In the Run pane configure when the test should run.

- If you want the test to run immediately, select the **now** radio button.
- If you want to schedule the test to run at certain intervals, do the following:
  - Select the **every** radio button.
  - Choose how often you want the test to run.
  - Enter the times between which you want the test to run.
  - Select the days on which the test should run.
  - Enter a test name.

Step 8 Click **Create**.

Creating an Emergency Call Synthetic Test

The Emergency Call synthetic test is supported only on Cisco Emergency Responder Release 1.2.

Step 1 Select **Diagnostics > Synthetic Tests**. The Synthetic Tests page appears.

Step 2 Click **Create**. The Create Synthetic Test page appears.

Step 3 From the Test Type pull-down menu, select **Emergency Call Test**.

Step 4 In the CER Parameters pane, enter the following:

- The name or IP address of the system where Cisco Emergency Responder is installed.

Note You can use the group selector in the left pane to enter a device: Select the device in the group selector, and then click the arrow button next to the Cisco Emergency Responder field.

- Emergency phone number.

Step 5 In the Caller pane, enter the following:

- The name or IP address of the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express for the caller's phone.

Note You can use the group selector in the left pane to enter a device: Select the device in the group selector, and then click the arrow button next to the Cisco Unified Communications Manager/Express field.

- The synthetic phone's MAC address. If you used the group selector to choose the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express system, the MAC address field is automatically populated.

Note The MAC address for synthetic phones must be between 00059a3b7700 and 00059a3b8aff and must be in the format 00059a3b7700. Operations Manager verifies only that the MAC address number entered in the Create Synthetic Test page is syntactically valid. It is your responsibility to make sure the correct numbers are entered, as configured in the Cisco Unified Communications Manager.

Step 6 In the PSAP pane, enter the following:

- The Public Safety Answering Point (PSAP) Cisco Unified Communications Manager or Cisco Unified Communications Manager Express.

Note You can use the group selector in the left pane to enter a device: Select the device in the group selector, and then click the arrow button next to the Cisco Unified Communications Manager/Express field.

- The PSAP phone's MAC address.

Step 7 (Optional) If there is an On Site Alert Number (OSAN), select the On Site Alert Number check box, and enter the following in the OSAN pane:

- The name or IP address of the OSAN Cisco Unified Communications Manager or Cisco Unified Communications Manager Express.

Note You can use the group selector in the left pane to enter a device: Select the device in the group selector, and then click the arrow button next to the Cisco Unified Communications Manager/Express field.

- The OSAN phone's MAC address.

Step 8 In the Run pane configure when the test should run.

- If you want the test to run immediately, select the **now** radio button.
- If you want to schedule the test to run at certain intervals, do the following:
  - Select the **every** radio button.
  - Choose how often you want the test to run.
  - Enter the times between which you want the test to run.

- Select the days on which the test should run.
- Enter a test name.

Step 9 Click **Create**.

Creating a Message-Waiting Indicator Synthetic Test

Ensure that

Step 1 Select **Diagnostics > Synthetic Tests**. The Synthetic Tests page appears.

Step 2 Click **Create**. The Create Synthetic Test page appears.

Step 3 From the Test Type pull-down menu, select **Message-Waiting Indicator Test**.

Step 4 In the Unity Parameters pane, enter a Cisco Unity, Cisco Unity Express, or Cisco Unity Connection system for which you want to set up the test.

Note You can use the group selector in the left pane to enter a device: Select the device in the group selector, and then click the arrow button next to the Cisco Unity/Unity Express/Unity Connection field.

Step 5 In the Caller pane, enter the following:

- The name or IP address of the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express for the caller's phone.

  Note You can use the group selector in the left pane to enter a device: Select the device in the group selector, and then click the arrow button next to the Cisco Unified Communications Manager/Express field.

- The synthetic phone's MAC address. If you used the group selector to choose the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express system, the MAC address field is automatically populated.

  Note The MAC address for synthetic phones must be between 00059a3b7700 and 00059a3b8aff and must be in the format 00059a3b7700. Operations Manager verifies only that the MAC address number entered in the Create Synthetic Test page is syntactically valid. It is your responsibility to make sure the correct numbers are entered, as configured in the Cisco Unified Communications Manager.

Step 6 In the Recipient pane, enter the following:

- The name or IP address of the recipient Cisco Unified Communications Manager or Cisco Unified Communications Manager Express.

  Note You can use the group selector in the left pane to enter a device: Select the device in the group selector, and then click the arrow button next to the Cisco Unified Communications Manager/Express field.

- The phone's MAC address.
- The phone's extension number.
- The voice mail password.

Note Ensure that you do not use the Call Forward All option on this phone or the test will fail. Instead, use the Forward No Answer to Voicemail option for the configuration of the recipient Cisco Unified Communications Manager or Cisco Unified Communications Manager Express.

Step 7 In the Run pane configure when the test should run.

- If you want the test to run immediately, select the **now** radio button.
- If you want to schedule the test to run at certain intervals, do the following:
  - Select the **every** radio button.
  - Choose how often you want the test to run.
  - Enter the times between which you want the test to run.
  - Select the days on which the test should run.
  - Enter a test name.

Step 8 Click **Create**.

Tip After you perform a Cisco Unified Communications Manager version upgrade, Cisco Unity synthetic tests that use the Cisco Unified Communications Manager that you upgraded might stop working. If this problem occurs, you should delete the Cisco Unity synthetic test, and then add the synthetic test again.

Importing Synthetic Tests

You can import multiple synthetic tests at one time by using a comma-separated values (CSV) file.

Before You Begin

- Verify that your seed file is formatted correctly. For details, see Formatting Synthetic Test Import Files, page 9-16.
- Place the seed file on the server, in the `NMSROOT\ImportFiles` directory. If you do not have access to the directory, contact a local administrator for the server where Operations Manager is installed.

Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as "C:\Program Files\CSCOpx" or C:\PROGRA~1\CSCOpx.

Step 1 Select **Diagnostics > Synthetic Tests**. The Synthetic Tests page appears.

Note If you do not have the required software license, you will not be able to use Synthetic tests. The Diagnostic tab will not appear in Operations Manager.

Step 2 Click **Import**. The Import Synthetic Test page appears.

Step 3 Enter the name of the seed file in the Filename field and click **OK**.

Formatting Synthetic Test Import Files

You can find an example of an import file in the <NMSROOT>\Importfiles folder.

Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as "C:\Program Files\CSCOpx" or C:\PROGRA~1\CSCOpx.

The general format for a synthetic test seed file is as follows:

- If you create the import file manually, the import file header should be:

```
Cisco Systems synthetic test import, version=2.0;type=CSV;source=manual
```

- All values must be separated with a vertical bar (|).

The schedule column must use the following formatting:

MONTH,DAYSOFMONTH,DAYSOFWEEK,HOUR,MINUTE

- Month—0-11
- Day of month—1-31
- Day of week—0-6 (0 = sunday)
- Hour—0-23
- Minute—0-59

Each specifier can be a number, a range, comma-separated numbers and a range, or an asterisk.

Month and days of the month fields cannot be changed. You should enter an asterisk (*).

Day of week can have an asterisk to represent all days, or it can have a comma-separated list of days. For Hour, you can enter an asterisk to represent 24 hours, or you can enter a range. Minute can be an asterisk, to represent all, or it can be a range.

Only the following schedule types are supported:

- *;*;*;*;* —All days, 24 hours
- *;*;2-4;*;* —Tuesday to Thursday, 24 hours
- *;*;*;8-20;* —All days between 8:00 a.m. and 8:00 p.m.
- *;*;*;8;20-59:*;*;*;9-19;*:*;*;*;20;0-40 —All days between 8:20 a.m. and 8:40 p.m.

Phone Registration and Dial-Tone Tests

Phone Registration test format:
REGISTRATION|TestName|PollInterval|Schedule|CCMAddress|MACAddress|SrcPhoneProtocol|SIPURI_OR_EXTN

Table 9-3 Import File Format for Phone Registration and Dial-Tone Tests

Column Number	Description
1	Type of test—REGISTRATION
2	Test name.
3	Polling interval.
4	Schedule.
5	Cisco Unified Communications Manager to which the phone is connected.
6	Phone's MAC address.
7	Phone's protocol (SCCP or SIP).
8	SIP URI or extension number.

Example of a Phone Registration test import file:

```
REGISTRATION|reg test|60|*;*;*;*;*|ipif-skate.cisco.com|00059A3B7780|SCCP|4002
```

Dial-Tone Tests

Dial-tone test format:
OFFHOOK|TestName|PollInterval|Schedule|CCMAddress|MACAddress

Table 9-4 Import File Format for Dial-Tone Tests

Column Number	Description
1	Type of test—DIALTONE
2	Test name.
3	Polling interval.
4	Schedule.
5	Cisco Unified Communications Manager to which the phone is connected.
6	Phone's MAC address.

Example of a dial-tone test import file:

```
OFFHOOK|dial-tone|60|*;*;*;*;*|ipif-skate.cisco.com|00059A3B7781
```

End-to-End Call Test

End-to-End Call test format:
ENDTOENDTEST|TestName|PollInterval|Schedule|SrcCCM|SrcMAC|isDestRealPhone|DestCCM|DestMAC|Extn|WaitForAnswer|EnableRTP|SrcPhoneProtocol|SRC_SIPURI_OR_EXTN|DestPhoneProtocol

Table 9-5 File Format for End-to-End Call Test

Column Number	Description
1	Type of test—ENDTOENDTEST
2	Test name.
3	Polling interval.
4	Schedule.
5	Caller Cisco Unified Communications Manager.
6	Caller MAC address.
7	Whether or not the recipient phone is a real phone. Enter true or false.
8	Recipient Cisco Unified Communications Manager.
9	Recipient MAC address.
10	Recipient extension number.
11	Wait for answer. Enter true or false.
12	Enable RTP transmission. Enter true or false.
13	Phone's protocol (SCCP or SIP).
14	SIP URI or extension number.
15	Destinations phone's protocol (SCCP or SIP).

Example of an End-to-End test import file:

```
ENDTOENDTEST|endtoend test|60|*;*;*;*;*|ipif-skate.cisco.com|00059A3B7782|FALSE
|ipif-skate.cisco.com|00059A3B7783|4002|TRUE|FALSE|SCCP|4004|SCCP
```

TFTP Download Test

TFTP test format: TFTP|TestName|PollInterval|Schedule|CCMAddress

Table 9-6 Import File Format for TFTP Download Test

Column Number	Description
1	Type of test—TFTP.
2	Test name.
3	Polling interval.
4	Schedule.
5	Cisco Unified Communications Manager.

Example of a TFTP download test import file:

```
TFTP|tftp download|60|*;*;*;*;*|ipif-skate.cisco.com
```

Message-Waiting Indicator Test

End-to-End Call test format:
MWITEST|TestName|PollInterval|Schedule|UnityAddress|SrcCCM|SrcMAC|DestCCM|DestMAC|Ext
n|Password

Table 9-7 Import File Format for Message-Waiting Indicator Test

Column Number	Description
1	Type of test—MWITEST.
2	Test name.
3	Polling interval.
4	Schedule.
5	Cisco Unity system.
6	Caller Cisco Unified Communications Manager.
7	Caller MAC address.
8	Recipient Cisco Unified Communications Manager.
9	Recipient MAC address.
10	Recipient extension number.
11	Recipient voice mail password.

Example of a Message-waiting indicator test import file:

```
MWITEST|mwi test|300|*;*;*;*;*|10.76.91.155|10.76.91.148|00059A3B7B00|10.76.91.148
|00059A3B7B01|71418001|13579
```

Cisco Conference Connection Test

Cisco Conference Connection Test format:
CCCTEST|TestName|PollInterval|Schedule|CCCAddress|FirstCCM|FirstMAC|SecondCCM|SecondM
AC|CCCUserName|CCCPassword|MeetingID|CCCAccessNum|CCCTargetE164

Table 9-8 Import File Format for Cisco Conference Connection Test

Column Number	Description
1	Type of test—CCCTEST.
2	Test name.
3	Polling interval.
4	Schedule.
5	Cisco Conference Connection system.
6	First caller Cisco Unified Communications Manager.
7	First caller MAC address.
8	Second caller Cisco Unified Communications Manager.
9	Second caller MAC address.

Table 9-8 Import File Format for Cisco Conference Connection Test (continued)

Column Number	Description
10	Cisco Conference Connection username.
11	Cisco Conference Connection password.
12	Meeting ID number.
13	Cisco Conference Connection access number.

Example of a Cisco Conference Connection test import file:

```
CCCTEST|conference conn test|120|*;*;*;*;*|10.76.91.105|10.76.91.99|00059A3B7F00
|10.76.91.99|00059A3B7F01|cccjtapi|cisco|444444|123444444|1234
```

Emergency Call Test

Emergency Call Test format:
EMERGENCYCALLTEST|TestName|PollInterval|Schedule|CERAddress|SrcCCM|SrcMAC|PsapCCM
|PsapMAC|EmergencyNumber|enableOsan|OsanCCM|OsanMAC

Table 9-9 Import File Format for Emergency Call Test

Column Number	Description
1	Type of test—CCCTEST.
2	Test name.
3	Polling interval.
4	Schedule.
5	Cisco Emergency Responder system.
6	Caller Cisco Unified Communications Manager.
7	Caller MAC address.
8	Public Safety Answering Point (PSAP) Cisco Unified Communications Manager.
9	PSAP MAC address.
10	Emergency number.
11	Enable On Site Alert Number (OSAN). Enter true or false.
12	OSAN Cisco Unified Communications Manager.
13	OSAN MAC address.

Example of an Emergency Call test import file:

```
EMERGENCYCALLTEST|emergency call test|600|*;*;*;*;*|10.76.35.211|10.76.93.75|00059A3B7789
|10.76.93.75|00059A3B7790|911|TRUE|10.76.38.111|00059A3B7791
```

Exporting Synthetic Tests

You can export the synthetic tests that you have created to a file on your Operations Manager server. If needed, you can use this file to import your configured synthetic tests back into Operations Manager, or to import the tests into another Operations Manager system.

Step 1 Select **Diagnostics > Synthetic Tests**. The Synthetic Tests page appears.

Step 2 Click **Export**. The Export Synthetic Test page appears.

Step 3 Enter a name for the export file.

Step 4 Click **OK**. All your synthetic tests are exported to a single file.

Editing Synthetic Tests

Note Every time you create or edit a test that requires a phone extension number and a MAC address, you should edit them as a pair. Do not edit one independently of the other.

Step 1 Select **Diagnostics > Synthetic Tests**. The Synthetic Tests page appears.

Step 2 Select the synthetic test you want to edit.

Step 3 Click **Edit**. The Edit Synthetic Test page appears.

Step 4 Enter or change the desired information.

Step 5 Click **Edit**. Your changes will be saved.

Viewing Synthetic Test Details

In the Synthetic Test Details page you can view the parameters that have been configured for a test.

Step 1 Select **Diagnostics > Synthetic Tests**. The Synthetic Tests page appears.

Step 2 Select the synthetic test.

Step 3 Click **View**. The Synthetic Test Details page appears. The details displayed vary depending on the type of test.

Starting and Stopping Synthetic Tests

Synthetic tests can be started or stopped. You can select multiple tests at one time to start or stop. If a test is running while you are trying to stop it, a message appears stating the test's details.

Step 1 Select **Diagnostics > Synthetic Tests**. The Synthetic Tests page appears.

Step 2 Select the synthetic tests that you want to either start or stop.

Step 3 Click **Start** or **Stop** (depending on the desired action). A confirmation box appears.

Step 4 Click **Yes**.

Deleting Synthetic Tests

Step 1 Select **Diagnostics > Synthetic Tests**. The Synthetic Tests page appears.

Step 2 Select the synthetic test you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Yes** in the confirmation box.

Note If you click Cancel before clicking OK, the synthetic tests will not be deleted.

Viewing Synthetic Test Results

You can view the results of synthetic tests in a report format. As with any of the reports in Operations Manager, you can print the report or export it to a file.

The Synthetic Tests Results report provides the following information:

- Test status (passed or failed).
- The day and time that the test finished.
- Any error messages.

Step 1 Select **Diagnostics > Synthetic Tests**. The Synthetic Tests page appears.

Step 2 Select the synthetic test that you want to see the results for.

Step 3 Click **Results**. The Synthetic Tests Results report appears.

Scheduling Synthetic Tests

When you create a synthetic test, you have the option of running the test now, or scheduling the test to run at regular intervals.

If you want to change the time at which the test should run, you must edit the synthetic test in the Edit Synthetic Test page.

Note If the system time of the Operations Manager server is changed backward, the synthetic tests will not execute until the time has elapsed and the system time reaches the original time at which the change was done. For example, if at 10:00 a.m. the system time is changed to 9:00 a.m., the tests will not start executing until the system time is 10:00 a.m.

Note Your login determines whether or not you can perform this task. For information on user security, see Understanding Your User Role, page 1-23.

Step 1 Select **Diagnostics > Synthetic Tests**. The Synthetic Tests page appears.

Step 2 Select the synthetic test you want to edit.

Step 3 Click **Edit**. The Edit Synthetic Test page appears.

Step 4 In the Run area, enter or change the desired schedule information.

Step 5 Click **Edit**. Your changes will be saved.

Synthetic Test Notes

Table 9-10 contains information you should be aware of when working with synthetic tests.

Table 9-10 Synthetic Test Notes

Summary	Explanation

Synthetic tests do not run for 30 minutes after the Operations Manager processes are started. However, during this time, you can still create, edit, or delete tests.	Starting Operations Manager processes places a high load on the system. To prevent synthetic tests from failing during this time, Operations Manager delays starting them.
	You can change the default setting by doing the following:
	1. Add the following default settings in the AMAServer.properties file located in <NMSRoot>\etc\cwsi:
	AMAMonitor.InitialDelay-30
	2. Stop and restart the synthetic transaction server using the following commands:
	`pdterm STServer`
	`pdexec STServer`
	3. Start the VHMSTIntegrator process using the `pdexec VHMSTIntegrator` command.

When the interval of a synthetic test is decreased from a high value to a low value, the first results for the new value may take longer than the new interval to report.	Each synthetic test executes at a time that is controlled by its interval setting. Immediately after you decrease the interval setting for a synthetic test, that transaction might not execute again until a total elapsed time that is longer than the new interval. For example, if you decrease an interval from 180 seconds to 60 seconds, the first results for the new interval may take as long as 240 seconds to report.
One-time synthetic test failures sometimes occur.	Occasionally, one-time synthetic test failures occur. Such failures can be due to high loads on the Operations Manager system or other factors that cause Operations Manager to be unable to receive some events from applications.

Table 9-10 Synthetic Test Notes (continued)

Summary	Explanation
Multiple conferences with the same meeting ID are created and are not deleted, slowing the performance of Cisco Conference Connection database operations.	When synthetic tests for Cisco Conference Connection (CCC) fail, the conferences they create might not be deleted from the CCC Past Conferences database. If a synthetic test fails after a conference is created but before it is stopped and deleted, the next occurrence of the test results in the termination of the conference, but the conference is not deleted. You should periodically delete any old conferences used for synthetic testing. Delete the old conferences through the CCC user interface.
Cisco Unity Message-waiting indicator synthetic tests may fail.	If a Cisco Unity synthetic test fails and the Message-Waiting Indicator light is on, you must configure a real phone with the same extension number used in the test and delete the voice mails manually. Alternatively, you can use the Message Store Manager tool to remove the voice mails. Once this is completed, the test will pass.

Synthetic Test Worksheets

Recording Cisco Unified Communications Manager Information

Table 9-11 Cisco Unified Communications Manager Worksheet for Synthetic Test Configuration

Cisco Unified Communications Manager:			
Synthetic Test	**MAC Address**	**Destination Phone Extension Number**	**Destination Phone Cisco Unified Communications Manager**
Phone Registration		—	—
Dial-Tone		—	—
End-to-End Call—source phone		—	—
End-to-End Call—destination phone (synthetic phone)			
End-to-End Call—destination phone (real phone)	—		—
Phone Registration		—	—
Dial-Tone		—	—
End-to-End Call—source phone		—	—
End-to-End Call—destination phone (synthetic phone)			
End-to-End Call—destination phone (real phone)	—		—
Phone Registration		—	—
Dial-Tone		—	—

Table 9-11 Cisco Unified Communications Manager Worksheet for Synthetic Test Configuration

Cisco Unified Communications Manager:			
Synthetic Test	**MAC Address**	**Destination Phone Extension Number**	**Destination Phone Cisco Unified Communications Manager**
End-to-End Call—source phone		—	—
End-to-End Call—destination phone (synthetic phone)			
End-to-End Call—destination phone (real phone)	—		—

Recording Cisco Emergency Responder Information

Table 9-12 Cisco Emergency Responder Worksheet for Synthetic Test Configuration

Parameter	**Name or Number**
Source	
Cisco Unified Communications Manager	
MAC address	
Destination	
Emergency number	
Public Safety Answering Point	
Cisco Unified Communications Manager	
MAC address	
On Site Alert	
Cisco Unified Communications Manager	
MAC address	

Recording Cisco IP Conference Connection Information

The username, password, and access number are required for the Cisco Conference Connection Test.

Table 9-13 Cisco IP Conference Connection Worksheet for Synthetic Test Configuration

Parameter	**Name or Number**
Cisco Conference Connection	
Username	
Password	
Meeting ID	
Access number	
First Caller	
Cisco Unified Communications Manager	
MAC address	

Table 9-13 Cisco IP Conference Connection Worksheet for Synthetic Test Configuration

Parameter	Name or Number
Cisco Conference Connection	
Username	
Password	
Meeting ID	
Access number	
First Caller	
Second Caller	
Cisco Unified Communications Manager	
MAC address	

Recording Cisco Unity Information

Table 9-14 Cisco Unity Worksheet for Synthetic Test Configuration

Parameter	Name or Number
Caller	
Cisco Unified Communications Manager	
MAC address	
Recipient	
Cisco Unified Communications Manager	
MAC address	
Phone extension number	
Voice Mail	
Password	

CHAPTER 10

Using Batch Tests

Note If you do not have the required software license, you will not be able to use batch tests.

Batch tests enable you to test the health and connectivity of a branch office. Batch tests consist of a set of synthetic tests (see Using Synthetic Tests, page 9-1) that are run on voice applications (for example, Cisco Unified Communications Manager Express or Cisco Unity Express) that are deployed in a branch office and a set of phone tests (see Understanding Phone Tests, page 10-12) that are run on real phones in the branch office. Batch tests can be run once a day to verify the health of the voice network in the branch office. You can also select one or more phones from an All IP Phones/Lines report display and run a phone test on demand.

The following topics are covered:

Working with Batch Tests

This section describes how to create, edit, remove, and analyze batch tests in Operations Manager, as well as how to stop or start batch test operations.

This section includes the following topics:

Creating Batch Tests

You create batch tests by importing an XML file. Each individual batch test consists of multiple synthetic tests and phone tests.

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

Before You Begin

- Verify that your seed file is formatted correctly. For details, see Formatting Batch Test Import Files, page 10-2.
- Place the seed file on the server, in the NMSROOT\ImportFiles directory. If you do not have access to the directory, contact a local administrator for the server where Operations Manager is installed.

  Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as "C:\Program Files\CSCOpx" or C:\PROGRA~1\CSCOpx.

Step 1 Select **Diagnostics > Batch Tests**. The Batch Tests page appears.

Note If you do not have the required software license, you will not be able to use batch tests. The Diagnostic tab will not appear in Operations Manager.

Step 2 Click **Create**. The Create Batch Test page appears.

Step 3 Enter the name of the seed file in the Filename field and click **OK**.

Formatting Batch Test Import Files

The batch test import file is an XML file. You can find an example of an import file in the <NMSROOT>\Importfiles folder.

Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as "C:\Program FilesCSCOpx" or C:\PROGRA~1\CSCOpx.

A batch test import file contains information for one batch test. Each batch test import file contains all the information required to configure the synthetic tests and phone tests for that particular batch test.

- For specific details on what information is required to configure synthetic tests, see Configuring Synthetic Tests, page 9-3.

- For specific details on what information is required to configure phone tests, see Understanding Phone Tests, page 10-12.

When creating a batch test import file, observe the following guidelines for the listed fields:

- TestSchedule—Can have multiple schedule entries.
- Each ScheduleEntry—Must have the following five fields:
  - Month—Not supported.
  - DayOfMonth—Not supported.
  - DayOfWeek—Must be 0 through 6 or asterisk to indicate all days.
  - Hour—Must be between 0 and 23.
  - Minute—Must be between 0 and 59.
- CallAgent—Can be a Cisco Unified Communications Manager or a Cisco Unified Communications Manager Express.
- PhoneMACAddress—The MAC address of a synthetic phone. It must be in the range of 00059A3B7700 to 00059A3B8AFF.
- PhoneProtocol—The protocol of the synthetic phone, either SCCP or SIP.
- PhoneURIorExtension—The extension or URI of a SIP phone. This is ignored for SCCP phones.
- OnsiteAlertNumber—Required only when IsOSANEnabled is set to *true*.
- DialingNumber—Optional. PhoneNumber is used if no input is present. This field is valid for intercluster call only. It must provide the complete number that has to be dialed from source phone to reach destination phone on a different cluster.(for example, just the phone number or the dial pattern/access digits plus the phone number.

Example Batch Test Import FIle

```
<BatchTest name="batch-test1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="BatchTest.xsd">
- <!--

        TestSchedule can have multiple ScheduleEntry's
        Each ScheduleEntry must have the following five fields

            month : Not supported
            dayOfMonth : Not supported
            dayOfWeek : should be 0-6 or * to indicate all days
            hour : hour should be between 0-23
            minute : minute should be between 0-59


  -->
- <TestSchedule>
- <ScheduleEntry>
  <month>*</month>
  <dayOfMonth>*</dayOfMonth>
  <dayOfWeek>*</dayOfWeek>
  <hour>10</hour>
  <minute>10</minute>
  </ScheduleEntry>
- <ScheduleEntry>
  <month>*</month>
  <dayOfMonth>*</dayOfMonth>
  <dayOfWeek>*</dayOfWeek>
  <hour>20</hour>
  <minute>20</minute>
```

```
  </ScheduleEntry>
  </TestSchedule>
  <CiscoCallManager name="CM1" address="ipif-ccm1.cisco.com" jtapiUsername="jtuser"
jtapiPassword="cisco" />
  <CiscoCallManager name="CM2" address="ipif-skate.cisco.com" jtapiUsername="jtuser"
jtapiPassword="cisco" />
- <!--

       CallAgent           : A CallAgent can be a Cisco CallManager or Cisco CallManager
Express
       PhoneMACAddress     : The MAC address of synthetic phone. This should be in the
range
                             00059A3B7700 - 00059A3B8AFF
       PhoneProtocol       : The protocol of synthetic phone. This values can be SCCP or
SIP
       PhoneURIorExtension : The extension of URI of a SIP phone. This is ignored for
SCCP phones


  -->
- <PhoneRegistrationTest name="skinny-reg">
- <Phone>
  <CallAgent>10.76.93.118</CallAgent>
  <PhoneMACAddress>00059A3B7700</PhoneMACAddress>
  <PhoneProtocol>SCCP</PhoneProtocol>
  <PhoneURIorExtension />
  </Phone>
  <SuccessCriteria>RegistrationFailure</SuccessCriteria>
  </PhoneRegistrationTest>
- <PhoneRegistrationTest name="sip-reg">
- <Phone>
  <CallAgent>ipcom-sd1.cisco.com</CallAgent>
  <PhoneMACAddress>00059A3B7800</PhoneMACAddress>
  <PhoneProtocol>SIP</PhoneProtocol>
  <PhoneURIorExtension>sip:7800@ipcom-sd1.cisco.com</PhoneURIorExtension>
  </Phone>
  <SuccessCriteria>RegistrationSuccess</SuccessCriteria>
  </PhoneRegistrationTest>
- <DialToneTest name="dial-tone">
- <Phone>
  <CallAgent>ipcom-sd1.cisco.com</CallAgent>
  <PhoneMACAddress>00059A3B7701</PhoneMACAddress>
  <PhoneProtocol>SCCP</PhoneProtocol>
  <PhoneURIorExtension />
  </Phone>
  </DialToneTest>
- <TftpTest name="tftp-download">
  <TftpServer>ipif-skate.cisco.com</TftpServer>
  </TftpTest>
- <EndToEndTest name="e2e-skinny2real">
- <Caller>
  <CallAgent>ipif-ccm1.cisco.com</CallAgent>
  <PhoneMACAddress>00059A3B7704</PhoneMACAddress>
  <PhoneProtocol>SCCP</PhoneProtocol>
  <PhoneURIorExtension />
  </Caller>
  <IsDestRealPhone>true</IsDestRealPhone>
  <ReceiverURIorExtension>5555</ReceiverURIorExtension>
  <WaitForAnswer>true</WaitForAnswer>
  <EnableRTPTransmission>false</EnableRTPTransmission>
  <SuccessCriteria>CallSuccess</SuccessCriteria>
  </EndToEndTest>
- <EndToEndTest name="e2e-sip2real">
- <Caller>
```

```
  <CallAgent>ipcom-sd1.cisco.com</CallAgent>
  <PhoneMACAddress>00059A3B7801</PhoneMACAddress>
  <PhoneProtocol>SIP</PhoneProtocol>
  <PhoneURIorExtension>sip:7801@ipcom-sd1.cisco.com</PhoneURIorExtension>
  </Caller>
  <IsDestRealPhone>true</IsDestRealPhone>
  <ReceiverURIorExtension>5555</ReceiverURIorExtension>
  <WaitForAnswer>true</WaitForAnswer>
  <EnableRTPTransmission>false</EnableRTPTransmission>
  <SuccessCriteria>CallFailure</SuccessCriteria>
  </EndToEndTest>
- <EndToEndTest name="e2e-skinny2skinny">
- <Caller>
  <CallAgent>10.76.93.118</CallAgent>
  <PhoneMACAddress>00059A3B7702</PhoneMACAddress>
  <PhoneProtocol>SCCP</PhoneProtocol>
  <PhoneURIorExtension />
  </Caller>
  <IsDestRealPhone>false</IsDestRealPhone>
- <Receiver>
  <CallAgent>10.76.93.118</CallAgent>
  <PhoneMACAddress>00059A3B7703</PhoneMACAddress>
  <PhoneProtocol>SCCP</PhoneProtocol>
  <PhoneURIorExtension />
  </Receiver>
  <ReceiverURIorExtension>7703</ReceiverURIorExtension>
  <SuccessCriteria>CallSuccess</SuccessCriteria>
  </EndToEndTest>
- <EndToEndTest name="e2e-sip2sip">
- <Caller>
  <CallAgent>ipcom-sd1.cisco.com</CallAgent>
  <PhoneMACAddress>00059A3B7800</PhoneMACAddress>
  <PhoneProtocol>SIP</PhoneProtocol>
  <PhoneURIorExtension>sip:7800@ipcom-sd1.cisco.com</PhoneURIorExtension>
  </Caller>
  <IsDestRealPhone>false</IsDestRealPhone>
- <Receiver>
  <CallAgent>ipcom-sd1.cisco.com</CallAgent>
  <PhoneMACAddress>00059A3B7801</PhoneMACAddress>
  <PhoneProtocol>SIP</PhoneProtocol>
  <PhoneURIorExtension>sip:7801@ipcom-sd1.cisco.com</PhoneURIorExtension>
  </Receiver>
  <ReceiverURIorExtension>sip:7801@ipif-ccm1.cisco.com</ReceiverURIorExtension>
  <SuccessCriteria>CallSuccess</SuccessCriteria>
  </EndToEndTest>
- <EndToEndTest name="e2e-skinny2sip">
- <Caller>
  <CallAgent>10.76.93.118</CallAgent>
  <PhoneMACAddress>00059A3B7705</PhoneMACAddress>
  <PhoneProtocol>SCCP</PhoneProtocol>
  <PhoneURIorExtension />
  </Caller>
  <IsDestRealPhone>false</IsDestRealPhone>
- <Receiver>
  <CallAgent>10.76.93.118</CallAgent>
  <PhoneMACAddress>00059A3B7802</PhoneMACAddress>
  <PhoneProtocol>SIP</PhoneProtocol>
  <PhoneURIorExtension>sip:7802@ipcom-sd1.cisco.com</PhoneURIorExtension>
  </Receiver>
  <ReceiverURIorExtension>6666</ReceiverURIorExtension>
  <SuccessCriteria>CallSuccess</SuccessCriteria>
  </EndToEndTest>
- <EndToEndTest name="e2e-sip2skinny">
- <Caller>
```

```
  <CallAgent>10.76.93.118</CallAgent>
  <PhoneMACAddress>00059A3B7803</PhoneMACAddress>
  <PhoneProtocol>SIP</PhoneProtocol>
  <PhoneURIorExtension>sip:7803@ipcom-sd1.cisco.com</PhoneURIorExtension>
  </Caller>
  <IsDestRealPhone>false</IsDestRealPhone>
- <Receiver>
  <CallAgent>10.76.93.118</CallAgent>
  <PhoneMACAddress>00059A3B7706</PhoneMACAddress>
  <PhoneProtocol>SCCP</PhoneProtocol>
  <PhoneURIorExtension />
  </Receiver>
  <ReceiverURIorExtension>6666</ReceiverURIorExtension>
  <SuccessCriteria>CallSuccess</SuccessCriteria>
  </EndToEndTest>
- <MWITest name="unity-mwi">
  <VoiceMailSystem>10.76.91.175</VoiceMailSystem>
- <Caller>
  <CallAgent>ipif-ccm1.cisco.com</CallAgent>
  <PhoneMACAddress>00059A3B7707</PhoneMACAddress>
  <PhoneProtocol>SCCP</PhoneProtocol>
  <PhoneURIorExtension />
  </Caller>
- <Receiver>
  <CallAgent>ipif-ccm1.cisco.com</CallAgent>
  <PhoneMACAddress>00059A3B7708</PhoneMACAddress>
  <PhoneProtocol>SCCP</PhoneProtocol>
  <PhoneURIorExtension />
  </Receiver>
  <ReceiverExtension>4000</ReceiverExtension>
  <VoiceMailPassword>123456</VoiceMailPassword>
  </MWITest>
- <ConferenceTest name="ccc">
  <ConferenceServer>10.76.91.151</ConferenceServer>
- <FirstParticipant>
  <CallAgent>ipif-ccm1.cisco.com</CallAgent>
  <PhoneMACAddress>00059A3B7709</PhoneMACAddress>
  <PhoneProtocol>SCCP</PhoneProtocol>
  <PhoneURIorExtension />
  </FirstParticipant>
- <SecondParticipant>
  <CallAgent>ipif-ccm1.cisco.com</CallAgent>
  <PhoneMACAddress>00059A3B7710</PhoneMACAddress>
  <PhoneProtocol>SCCP</PhoneProtocol>
  <PhoneURIorExtension />
  </SecondParticipant>
  <UserName>cccUser</UserName>
  <Password>cisco</Password>
  <MeetingId>444444</MeetingId>
  <ConferenceDialIn>1234</ConferenceDialIn>
  </ConferenceTest>
- <EmergencyCallTest name="cer">
  <EmergencyCallRouter>10.76.91.149</EmergencyCallRouter>
- <Caller>
  <CallAgent>ipif-ccm1.cisco.com</CallAgent>
  <PhoneMACAddress>00059A3B7711</PhoneMACAddress>
  <PhoneProtocol>SCCP</PhoneProtocol>
  <PhoneURIorExtension />
  </Caller>
- <PublicSafetyAnsweringPoint>
  <CallAgent>ipif-ccm1.cisco.com</CallAgent>
  <PhoneMACAddress>00059A3B7712</PhoneMACAddress>
  <PhoneProtocol>SCCP</PhoneProtocol>
  <PhoneURIorExtension />
```

```
  </PublicSafetyAnsweringPoint>
  <EmergencyNumber>911</EmergencyNumber>
  <IsOSANEnabled>false</IsOSANEnabled>
  </EmergencyCallTest>
- <EmergencyCallTest name="cer-with-osan">
  <EmergencyCallRouter>10.76.91.149</EmergencyCallRouter>
- <Caller>
  <CallAgent>ipif-ccm1.cisco.com</CallAgent>
  <PhoneMACAddress>00059A3B7711</PhoneMACAddress>
  <PhoneProtocol>SCCP</PhoneProtocol>
  <PhoneURIorExtension />
  </Caller>
- <PublicSafetyAnsweringPoint>
  <CallAgent>ipif-ccm1.cisco.com</CallAgent>
  <PhoneMACAddress>00059A3B7712</PhoneMACAddress>
  <PhoneProtocol>SCCP</PhoneProtocol>
  <PhoneURIorExtension />
  </PublicSafetyAnsweringPoint>
  <EmergencyNumber>911</EmergencyNumber>
- <!--  OnsiteAlertNumber is required only when IsOSANEnabled is 'true'
  -->
  <IsOSANEnabled>true</IsOSANEnabled>
- <OnSiteAlertNumber>
  <CallAgent>ipif-ccm1.cisco.com</CallAgent>
  <PhoneMACAddress>00059A3B7713</PhoneMACAddress>
  <PhoneProtocol>SCCP</PhoneProtocol>
  <PhoneURIorExtension />
  </OnSiteAlertNumber>
  </EmergencyCallTest>
- <PhoneTest name="pt1" primaryCallManager="CM1">
  <TestPhones>3333,4444,5555,6666</TestPhones>
  <TestProbes>1111,1112,1113,1114</TestProbes>
- <Action name="IntraClusterCall" type="Call">
  <Destination>5555</Destination>
  </Action>
- <Action name="CallToPSTN" type="Call">
  <Destination>918041036116</Destination>
  </Action>
- <Action name="Call to PSTN Negative" type="Call">
  <Destination>918041036116</Destination>
  <SuccessCriteria>CallFailure</SuccessCriteria>
  </Action>
- <Action name="Inter Cluster Call" type="Call">
  <Destination>9999</Destination>
  <DestinationCallManager>CM2</DestinationCallManager>
  </Action>
  <Action name="Call Hold test" type="CallHold" />
  <Action name="Call Forward test" type="CallForward" />
  <Action name="Call Park test" type="CallPark" />
  <Action name="Conference test" type="Conference" />
  </PhoneTest>
+ <PhoneTest name="pt2" primaryCallManager="CM2">
  <TestPhones>3333,4444,5555,6666</TestPhones>
  <TestProbes>1111,1112,1113,1114</TestProbes>
- <Action name="Call to PSTN Negative" type="Call">
  <Destination>918041036116</Destination>
  <SuccessCriteria>CallSuccess</SuccessCriteria>
  </Action>
- <Action name="Inter Cluster Call" type="Call">
  <Destination>8888</Destination>
  <DialingNumber>8888</DialingNumber>
  <DestinationCallManager>CM1</DestinationCallManager>
  <SuccessCriteria>CallFailure</SuccessCriteria>
  </Action>
```

```
<Action name="Call Hold test" type="CallHold" />
<Action name="Call Forward test" type="CallForward" />
<Action name="Call Transfer test" type="CallTransfer" />
</PhoneTest>
</BatchTest>
```

Editing Batch Tests

You can change an existing batch test by importing a new batch test import file. The previous batch test information is overwritten by the new import file. To change the import file, you must manually edit the file (see Formatting Batch Test Import Files, page 10-2).

Step 1 Select **Diagnostics > Batch Tests**. The Batch Tests page appears.

Step 2 Select the batch test that you want to change.

Step 3 Click **Edit**. The Edit Batch Test page appears.

Step 4 Enter the name of the seed file in the Filename field and click **OK**.

Deleting a Batch Test

You can use this function to delete one or more tests. You can delete tests in any state. See Table 10-1 for a description of possible states.

Step 1 Select **Diagnostics > Batch Tests**. The Batch Tests page appears.

Step 2 Select the tests you want to delete, and then click **Delete**. A confirmation dialog box appears.

Step 3 Click **Yes**. Operations Manager deletes the tests you selected.

Viewing Batch Test Details

You can find all the details about a particular batch test on the Test Details page.

As with any of the reports in Operations Manager, you can print the report or export it to a file (see Printing Batch Test Results, page 10-11 and Exporting Batch Test Results, page 10-11).

The Test Details page lists all the synthetic tests and phone tests that are part of the batch test.

Step 1 Select **Diagnostics > Batch Tests**. The Batch Tests page appears.

Step 2 Select the test you want to view, and click **View**. The Test Details page opens.

Note You can jump to any of the tests listed in the Test Details page by selecting the test from the Go to Test menu at the top of the page.

The page contains the following information:

- Test summary:
  - Test name—Name of the batch test.
  - Test details—The number of synthetic and phone tests configured.
  - Test schedule.
- Synthetic tests:
  - Test name—Name of the synthetic test.
  - Test type—Type of synthetic test (see Using Synthetic Tests, page 9-1).
  - Phone details—Call Agent, MAC Address, Protocol, and URI/Extension. The phone information is provided for all phones, whether it is the calling or receiving phone.
- Phone tests:
  - Test name—Name of the phone test.
  - Primary Cisco Unified Communications Manager.
  - Test phones.
  - Test probes.
  - Phone action details—Lists the actions that the phone tests performed.

Note For descriptions of the phone tests, see Understanding Phone Tests, page 10-12.

Verifying the Status of a Test

You can verify whether a test ran and completed correctly. You can also troubleshoot the test if necessary.

Step 1 Select **Diagnostics > Batch Tests**. The Batch Tests page appears. All current batch tests appear on the page. The last column in the table shows the status of each test.

Table 10-1 Test Status Definitions

Test Status	Description
Running	The test is active and collecting data.
Suspended	The test is suspended from data collecting or polling. This occurs because the device was suspended.
Scheduled	Appears after you create or update a test. The status will change to Running at the first polling cycle.

Suspending/Resuming a Batch Test

When you suspend a batch test it no longer runs at its scheduled time. The test is not removed from the system. If you want to remove the test, it must be deleted (see Deleting a Batch Test, page 10-8).

Step 1 Select **Diagnostics > Batch Tests**. The Batch Tests page appears.

Step 2 If the batch test is active and you want to stop it from running, click **Suspend**.

Step 3 If the batch test is suspended and you want it to run it at its scheduled time, click **Resume**.

Scheduling a Batch Test to Run

The scheduled time and day that a batch test is to run is configured in the import file (see Formatting Batch Test Import Files, page 10-2). But if you want to run a batch test on demand, you can use the Run Now button.

Running a Batch Test on Demand

Step 1 Select **Diagnostics > Batch Tests**. The Batch Tests page appears.

Step 2 Select the batch test that you want to run.

Step 3 Click **Run Now**. The batch test runs.

Viewing Batch Test Results

No events or alerts are generated when a component of a batch test fails. You must use the Batch Test Results report to see the results of a batch test. A new Batch Test Results report is generated every 24 hours for each batch test.

As with any of the reports in Operations Manager, you can print the report or export it to a file (see Verifying the Status of a Test, page 10-9 and Exporting Batch Test Results, page 10-11).

The Batch Test Results report provides the following information for the overall batch test:

- Test status.
- The date and time that the test started and finished.

The Batch Test Results report provides the following information for the individual tests that are a part of the batch test:

- Test type.
- Whether or not it is a negative test.
- Test status (passed or failed).
- The date and time that the test finished.
- Any error messages.

Step 1 Select **Diagnostics > Batch Tests**. The Batch Tests page appears.

Step 2 Select the batch test that you want to see the results for.

Step 3 Click **Results**. The Batch Test Results report appears.

Printing Batch Test Results

Step 1 In a batch test report, click the printer icon in the upper-right corner of the window.

The records are reformatted into a print-friendly format and are displayed in a new browser window.

Step 2 Use the print function on your browser to print the display.

Exporting Batch Test Results

Step 1 In a batch test report, click the export icon in the upper-right corner of the window. Select either **CSV** or **PDF** format for export and click **OK**.

Step 2 If you chose CSV in Step 1, do the following:

a. When the File Download dialog box appears, click **Save**.

b. In the Windows folder window, enter the filename and the location where you want to save the file.

c. Click **Save**.

d. In the Download Complete dialog box, click **Close**.

Step 3 If you chose PDF in Step 1, do the following:

a. If a security information dialog box appears, click **Yes**. The records now appear in PDF format.

b. Use the PDF save function to save the file to your system.

Where Is Batch Test Data Stored?

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

Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as “C:\Program Files\CSCOpx” or C:\PROGRA~1\CSCOpx.

Understanding Phone Tests

The phone tests that are run as part of batch testing and on-demand testing take control of a real phone in the network and make a call from that phone to another phone. Phone tests use JTAPI credentials. For batch testing, these credentials must be included in the batch test import file. When running a phone test on demand, the JTAPI credentials must be provided in the phone test creation UI. For the phone test feature in Operations Manager to work properly, the JTAPI credentials need to be configured in Communications Manager as well.

When creating a phone test as part of batch testing, observe these definitions, guidelines, and instructions:

- TestPhones—Phones being tested.
- TestProbes—Phones being used to execute the tests.
- The test phones and test probes must belong to the same Cisco Unified Communications Manager because Operations Manager takes control of these phones and probes through the Communications Manager using JTAPI. If the test phones and test probes belong to a different Cisco Unified Communications Manager, the tests will fail.
- Only when the call test type is an intercluster call can the destination phone belong to a different Cisco Unified Communications Manager. In this instance, the user needs to provide the credentials of the destination Communications Manager in the batch test XML file.
- An example of an import XML file for batch phone testing is provided in C:\Program Files\CSCOpx\ImportFiles\batchPhoneTests.xml.

  See Creating Batch Tests, page 10-2 and Formatting Batch Test Import Files, page 10-2.
- Prior to running the phone tests, verify that the configurations are correct in Communications Manager and that the various phone operations are working using the real phones.

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

Table 10-2 describes the different phone tests that are used in batch testing and on-demand testing.

Note Do not confuse these phone tests with other Operations Manager phone tests (synthetic tests or phone status tests). These phone tests are created as part of batch testing and can also be launched on-demand, from IP Phone reports. These tests take control of real phones to conduct the tests.

Table 10-2 Phone Test Descriptions—Batch and On-Demand Tests

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

Creating and Running a Phone Test on Demand

You can select one or more phones from an All IP Phones/Lines report display and run a phone test on demand. The selected phones must belong to the same Cisco Unified Communications Manager. Phone tests use the JTAPI credential. The JTAPI credential must be configured in Communications Manager.

For information on how phone counts are displayed in Operations Manager windows, seeHow Are Phone Counts Displayed in Views and Reports?, page 1-19.

Step 1 Select **Monitor Dashboard > All IP Phones/Lines** to display all phones.

Step 2 Select the phones you want included in the on-demand phone test.

Step 3 Click **Launch > Phone Test**. The On-Demand Phone Test window appears.

Step 4 Select the items you want included in the on-demand phone test. See Table 10-3 for descriptions.

Step 5 Click **Run.** The on-demand phone test runs.

Table 10-3 On-Demand Phone Test

Item	Description
Cisco Unified Communications Manager	Lists the Communications Manager for the phones selected from the phone report. **Note** You can select a Cisco Unified Communications Manager from the left pane and click the >> button to add it to the Cisco Unified Communications Manager field. The previous Test Phones and Helper Phones selections are cleared; you will need to specify them again.
JTAPI Username and JTAPI Password	Enter the JTAPI username and password configured on the Communications Manager.
Test Phones	To add more phones to Test Phones: • Click **Add from Phone Report**. The phone report window appears. • Select the additional phones to add and click **Select**. **Note** The phones added must belong to the same Cisco Unified Communications Manager provided at the beginning for this test.[1]

Table 10-3 On-Demand Phone Test (continued)

Item	Description
Helper Phones	To add more phones to Helper Phones: • Click **Add from Phone Report**. • Select the additional phones to add and click **Select**. **Note** The phones added must belong to the same Cisco Unified Communications Manager provided at the beginning for this test.[1]
Phone Tests	Select the phone test that you want to see the results for. The following phone tests are available: • Call Hold • Call Forward • Call Park • Call Conference • Call Transfer • Call Test When Call Test is selected, the following fields are enabled: • Call Type • Success Criterion • Phone Number
Call Type	From the drop-down list, choose the call type. When Inter Cluster Call is selected, the following fields are enabled: • Cisco Unified Communications Manager • JTAPI Username • JTAPI Password
Success Criterion	From the drop-down list, choose the success criterion.
Phone Number	The destination phone number to be dialed for the call test needs to be specified in this field.
Dialing Number	When Inter Cluster Call is selected for Call Type, enter the complete phone number that the source phone must dial to reach the destination phone on a different cluster. This may include dial pattern or access digits, for example 94151234567. This field is not mandatory. If left empty the Phone Number field is used instead.

Table 10-3 On-Demand Phone Test (continued)

Item	Description
Cisco Unified Communications Manager	When Inter Cluster Call is selected for Call Type, enter the Cisco Unified Communications Manager for the phone number specified in the Phone Number field.
JTAPI Username and Password	When Inter Cluster Call is selected for Call Type, enter the JTAPI username and password for the Cisco Unified Communications Manager provided in the previous field.

1. If you select a single phone which shares its extension with other phones in the personalized report, the report generated will have details about all the phones (including the selected phone).

Tip If the phone tests fail and display the message "Unable to create provider," verify:

- The JTAPI username and password is created in Communications Manager and that the phones used in the test are assigned to the same JTAPI user. For the phone test feature in Operations Manager to work properly, the JTAPI credentials need to be configured in Communications Manager as well.
- The JTAPI implementation in Communications Manager may have been modified; as a result the JTAPI Java Archive (JAR) files need to be updated in Operations Manager.

To update the JTAPI .JAR files in Operations Manager:

Step 1 Log into Cisco Unified Communications Manager and select **Application > Plugins**.

Step 2 Click **Find** to list the available plugins.

Step 3 From the list, select **Download Cisco JTAPI for Windows** and save the file to your computer.

Step 4 Click the executable file to install the Cisco JTAPI client on your computer.

Step 5 In the directory where Operations Manager is installed on your system, in <Install Directory>\Unified Communications s\bt\lib, look for the directories listed for each Communications Manager version installed.

Step 6 Click the directory for the Communications Manager version that you are currently using. For example, go to directory 5.0 if your current version of Communications Manager is 5.0.x. Replace the .JAR files in the directory with the .JAR files from the newly installed Cisco JTAPI client on your computer.

By default, the .JAR files are in C:\WINNT\java\lib on your computer if the default directory was selected during the Cisco JTAPI client installation.

Viewing On-Demand Phone Test Results

When executed, the On-Demand Phone Test is run immediately and the results are displayed.

Table 10-4 On-Demand Phone Test Results

Item	Description
Action Name	Lists the phone test that was run on the selected phones. The descriptions in Table 10-2 apply to batch tests and on-demand phone tests.
Extension	Phone extension included in on-demand phone test.
Negative Test	Whether or not it is a negative test.
Test Status	Test Status (passed or failed).
Test Start Time	The date and time that the test started.
Test End Time	The date and time that the test finished.
Error Message	Any error messages.

To print an on-demand phone test, see Printing Batch Test Results, page 10-11. To export an on-demand phone test, see Exporting Batch Test Results, page 10-11.

CHAPTER 11

Using Node-To-Node Tests

Note If you do not have the required software license, you will not be able to use node-to-node tests.

Node-to-Node tests monitor the response time and availability of multiprotocol networks on both an end-to-end and a hop-by-hop basis. After collecting this data, you can use the Operations Manager graphing function to examine changes in network performance metrics. You can select, display, and chart network performance data in real time. See Viewing Test Trending, page 11-16. Also, Node-to-Node tests can be configured to trigger events when certain thresholds are crossed. These events appear in the Monitoring Dashboard displays.

This section describes how to create, edit, remove, and analyze Node-to-Node tests in Cisco Unified Operations Manager (Operations Manager).

This section includes the following topics:

Working with Node-To-Node Tests

You can create Node-to-Node tests one at a time, or you can import a file to create more than one test at a time.

Note If you ever need to uninstall Operations Manager, be sure to delete all the node-to-node tests from the application before you uninstall it. If you do not delete these tests, they will continue to run on the router. For instructions on deleting, see Deleting a Test, page 11-15.

This section includes the following topics:

Getting Started: Required Cisco IOS and IP SLA Versions

Node-to-node tests rely upon Cisco IOS IP SLA technology. Table 11-1 lists the versions of IP SLA and Cisco IOS that are required to successfully configure and run each type of node-to-node test.

Table 11-1 IP SLA Mapping for Node-to-Node Tests

	Required Versions	
Test	**IP SLA**	**Cisco IOS**
Ping Echo	2.1.0 and higher	12.0(5)T, 12.1(1), and higher
Ping Path Echo		
UDP Echo		
UDP Jitter for VoIP **Note** Without ICPIF/MOS values.		
UDP Jitter for VoIP **Note** With ICPIF/MOS values.	2.2.0 and higher	12.3(4)T and higher
Gatekeeper Registration Delay		12.3(14)T and higher
Real-Time Transport Protocol	2.20 and higher	• Voice port of type - ds0-group. • DSP of type either C5510 or C549. • IOS version greater than or equal to 12.4(19.12)T

To see device families on which node-to-node tests are supported, see *Supported Devices Table for Cisco Unified* Operations Manager *2.0* on Cisco.com.

Creating a Single Node-To-Node Test

Before you can create a test, the source device must be monitored by Operations Manager. See Using Device Management, page 16-1 for more information.

Note You can also set up Node-to-Node tests from the Service Level View (see Setting Up Node-To-Node Tests, page 2-28).

Step 1 Select **Diagnostics > Node-to-Node Tests**. The Node-to-Node Tests page appears.

Note If you do not have the required software license, you will not be able to use node-to-node tests. The Diagnostic tab will not appear in Operations Manager.

Step 2 Click **Create**. The information required for creating Node-to-Node tests is different for each test operation type. See the following for details:

- UDP Jitter for VoIP, page 11-3—Measures packet loss, round-trip latency, and delay variance (or jitter) in IP networks by generating synthetic UDP traffic.
- Ping Echo, page 11-6—Measures end-to-end response time between a source device and any IP-enabled device.
- Ping Path Echo, page 11-7—Measures hop-by-hop response time between a source device and any IP device on the network by discovering the path using traceroute, and then measuring response time between the source device and each hop in the path.
- UDP Echo, page 11-8—Measures UDP response time between a source device and any IP-enabled device.
- Gatekeeper Registration Delay, page 11-9—Measures the time required for a gateway to register with a gatekeeper.

Note For Gatekeeper Registration Delay tests to run, the source gateway must have SIP or H323 configured on it.

- Real-Time Transport Protocol, page 11-10—Measures voice quality metrics from DSP to DSP by integrating with the DSP software. The operation involves placing a test call from the source gateway to the destination, sending actual RTP packets and then collecting statistics from DSPs.

Note For the Real-time Transport Protocol test to run, the source must have a dsp module type of either C5510 or C549 and must have ds0-group of voice ports configured on it.

UDP Jitter for VoIP

This test uses the UDP protocol to measure latency, one-way jitter, and packet drop. Jitter is interpacket delay. The source device sends a number of packets from the source device to the destination device with a specified interpacket delay. The destination (an IP SLA Responder) time stamps the packet and sends it back. Using this data, the one-way positive and negative jitter (from the source to the destination and back again), packet loss (also from the source to the destination and back again), and round-trip latency are obtained.

Positive jitter occurs when the one-way delay for a packet is longer than the previous packet delay. Negative jitter occurs when the one-way delay for a packet is shorter than the previous packet delay. If the sequence numbers become jumbled, the test reflects the error.

Step 1 Select **Diagnostics > Node-to-Node Tests**. The Node-to-Node Tests page appears.

Step 2 Click **Create**. The Node-to-Node Test Configuration page appears.

Step 3 In the Test Type pull-down menu select **UDP Jitter for VoIP**.

Step 4 In the Source pane, do the following:

- Using the device selector, select a source device.

Note If you cannot find a recently added device, refresh the device groups. See Troubleshooting Note: Selecting a Source Device, page 11-5.

- Select a source interface setting. You can leave it at **Default**, or enter a new setting.

Step 5 In the Destination pane, do the following:

- Using the device selector, select a destination device.
- Enter a UDP port for the destination device (the default value is 16400). This is the port on the destination device to which packets are sent by the source device.

Note If you want to switch the source and destination devices with each other, click the Swap Source and Destination button.

Step 6 In the Parameters pane, you can set the following parameters:

Table 11-2 UDP Jitter for VoIP Test Parameters

Parameter	Default Value	Available Values	Description
Codec Type	—	• G.711ulaw • G.711alaw • G.729	Used to determine the packet interval and the request payload.
Call Duration	8	1 - 59 seconds	Time of the call.
Voice Quality Expectation	Land line	• Land line • Wireless campus • Wireless on the move • Multi-hop	Corresponds to the Access Advantage factor of Mean Opinion Scores (MOS) and Calculated Planning Impairment Factor (ICPIF).
IP QoS	IP Precedence	• IP Precedence • DSCP	Defines the quality of service policies for the IP SLA packets.
	5	• IP Precedence—0 (none) through 7 (high) • DSCP—0 (none) through 8 (CS1), 9, and 10 (AF11)	This is converted to Type of Service (TOS) and set on the device.

Step 7 In the Threshold pane, you can change the following settings:

Table 11-3 UDP Jitter for VoIP Test Threshold Settings

Parameter	Default Value	Available Values	Description
Source to Destination	3 (packet loss) 40 msec (jitter)	Any positive integer[1]	Threshold setting for packet loss and jitter.
Destination to Source	3 (packet loss) 40 msec (jitter)	Any positive integer[1]	Threshold setting for packet loss and jitter.

Table 11-3 UDP Jitter for VoIP Test Threshold Settings

Parameter	Default Value	Available Values	Description
Average Latency	300 m/secs	Any positive integer[1]	Threshold setting for latency.
Node-to-Node Quality	Fair	Excellent, Good, Fair, or Poor	Threshold setting for the test's quality. The values are associated with a MOS score. The value and equivalent MOS are as follows: • Excellent—5 (500) • Good—4 (400-499) • Fair—3 (300-399) • Poor—2 (200-299) • Bad—1 (100-199)

1. Positive integers must be 32 bit.

Step 8 In the Run pane configure when the test should run.

- If you want the test to run only once, select the **Once** radio button.
- If you want to schedule the test to run at certain intervals, do the following:
  - Select the schedule radio button.
  - Choose how often you want the test to run.
  - Enter the time between which you want the test to run.
  - Select the days on which the test should run.
  - Enter a test name. The test name cannot contain tabs, question marks, quotation marks, asterisks, semicolons, commas, colons, forward slashes, straight slashes, or backslashes.

Step 9 Click **OK**.

Troubleshooting Note: Selecting a Source Device

If you recently added an IP SLA-enabled device and it does not appear in the IP SLA Devices group in the selector in the Source pane on the Node-to-Node Test Configuration dialog box, refresh the device group membership.

Step 1 Select **Devices > Device Groups**. The Group Administration and Configuration page appears.

Step 2 In the Group Selector, select the OM@<*server*> group where <server> is the name of your server.

Step 3 Click the **Refresh** button. A confirmation dialog box appears.

Step 4 Click **Yes**. A progress bar appears. A success message is displayed.

Step 5 Click **OK**.

Step 6 If it is open, close the Node-to-Node Test Configuration dialog box. When you open it again, refreshed device groups are displayed in the Source pane.

Ping Echo

This test measures end-to-end latency information using ICMP. The test sends ICMP packets from the source device to the destination device and measures the time it takes to complete the round trip.

Step 1 Select **Diagnostics > Node-to-Node Tests**. The Node-to-Node Tests page appears.

Step 2 Click **Create**. The Node-to-Node Test Configuration page appears.

Step 3 In the Test Type pull-down menu select **Ping Echo**.

Step 4 In the Source pane, do the following:

- Using the device selector, select a source device.

Note If you cannot find a recently added device, refresh the device groups. See Troubleshooting Note: Selecting a Source Device, page 11-5.

- Select a source interface setting. You can leave it at **Default**, or enter a new setting.

Step 5 In the Destination pane, using the device selector, select a destination device.

Note If you want to switch the source and destination devices with each other, click the Swap Source and Destination button.

Step 6 In the Parameters pane, you can set the following parameters:

Table 11-4 Ping Echo Test Parameters

Parameter	Default Value	Available Values	Description
Request Payload	32 bytes	28 to 16384 bytes	A default ICMP Ping packet has 32 bytes. Allows for variably sized operations.
IP QoS	IP Precedence	• IP Precedence • DSCP	Defines the quality of service policies for the IP SLA packets.
	0 (none)	• IP Precedence—0 (none) through 7 (high) • DSCP—0 (none) through 8 (CS1), 9, and 10 (AF11)	This is converted to TOS and set on the device.
Show Link in Service Level View	Not selected	—	Displays this test as a virtual link in the Service Level View.

Step 7 If you want to change the Round-Trip Response Time Threshold, in the Thresholds pane, select the check box and enter a new setting (default is 300 m/secs). The setting must be a positive integer (32 bit).

Step 8 In the Run pane configure when the test should run.

- If you want the test to run only once, select the **Once** radio button.
- If you want to schedule the test to run at certain intervals, do the following:
  - Select the schedule radio button.

- Choose how often you want the test to run.
- Enter the time between which you want the test to run.
- Select the days on which the test should run.
- Enter a test name. The test name cannot contain tabs, question marks, quotation marks, asterisks, semicolons, commas, colons, forward slashes, straight slashes, or backslashes.

Step 9 Click **OK**.

Ping Path Echo

This test measures hop-by-hop latency information using ICMP Ping and traceroute.

Step 1 Select **Diagnostics > Node-to-Node Tests**. The Node-to-Node Tests page appears.

Step 2 Click **Create**. The Node-to-Node Test Configuration page appears.

Step 3 In the Test Type pull-down menu select **Ping Path Echo**.

Step 4 In the Source pane, do the following:

- Using the device selector, select a source device.

Note If you cannot find a recently added device, refresh the device groups. See Troubleshooting Note: Selecting a Source Device, page 11-5.

- Select a source interface setting. You can leave it at **Default**, or enter a new setting.

Step 5 In the Destination pane, using the device selector, select a destination device.

Note If you want to switch the source and destination devices with each other, click the Swap Source and Destination button.

Step 6 In the Parameters pane, you can set the following parameters:

Table 11-5 Ping Path Echo Test Parameters

Parameter	Default Value	Available Values	Description
Request Payload	32 bytes	28 to 16384 bytes	A default ICMP Ping packet has 32 bytes. Allows for variably sized operations.
IP QoS	IP Precedence	• IP Precedence • DSCP	Defines the quality of service policies for the IP SLA packets.
	0 (none)	• IP Precedence—0 (none) through 7 (high) • DSCP—0 (none) through 8 (CS1), 9, and 10 (AF11)	This is converted to TOS and set on the device.

Step 7 If you want to change the Round-Trip Response Time threshold, in the Thresholds pane, select the check box and enter a new setting (default is 300 m/secs). The setting must be a positive integer (32 bit).

Step 8 In the Run pane configure when the test should run.

- If you want the test to run only once, select the **Once** radio button.
- If you want to schedule the test to run at certain intervals, do the following:
  - Select the schedule radio button.
  - Choose how often you want the test to run.
  - Enter the time between which you want the test to run.
  - Select the days on which the test should run.
  - Enter a test name. The test name cannot contain tabs, question marks, quotation marks, asterisks, semicolons, commas, colons, forward slashes, straight slashes, or backslashes.

Step 9 Click **OK**.

UDP Echo

This test measures UDP server latency. The UDP echo test sends a packet with the configured number of bytes to the destination with the specified port number and measures the response time. There are two destination device types for the UDP echo operation: RTR Responders, which use IP SLA, and UDP servers, which do not.

Step 1 Select **Diagnostics > Node-to-Node Tests**. The Node-to-Node Tests page appears.

Step 2 Click **Create**. The Node-to-Node Test Configuration page appears.

Step 3 In the Test Type pull-down menu select **UDP Echo**.

Step 4 In the Source pane, do the following:

- Using the device selector, select a source device.

  Note If you cannot find a recently added device, refresh the device groups. See Troubleshooting Note: Selecting a Source Device, page 11-5.

- Select a source interface setting. You can leave it at **Default**, or enter a new setting.

Step 5 In the Destination pane, using the device selector, select a destination device.

Step 6 Enter the UDP port number (the default value is 7) for the destination device to use when sending response packets.

Note If you want to switch the source and destination devices with each other, click the Swap Source and Destination button.

Step 7 In the Parameters pane, you can set the following parameters:

Table 11-6 UDP Echo Test Parameters

Parameter	Default Value	Available Values	Description
Request Payload	16 bytes	4 to 1500 bytes	Allows for variably sized operations.
IP QoS	IP Precedence	• IP Precedence • DSCP	Defines the quality of service policies for the IP SLA packets.
	0 (none)	• IP Precedence—0 (none) through 7 (high) • DSCP—0 (none) through 8 (CS1), 9, and 10 (AF11)	This is converted to TOS and set on the device.

Step 8 If you want to change the Round-Trip Response Time threshold, in the Thresholds pane, select the check box and enter a new setting (default is 300 m/secs). The setting must be a positive integer (32 bit).

Step 9 In the Run pane configure when the test should run.

- If you want the test to run only once, select the **Once** radio button.
- If you want to schedule the test to run at certain intervals, do the following:
  - Select the schedule radio button.
  - Choose how often you want the test to run.
  - Enter the time between which you want the test to run.
  - Select the days on which the test should run.
  - Enter a test name. The test name cannot contain tabs, question marks, quotation marks, asterisks, semicolons, commas, colons, forward slashes, straight slashes, or backslashes.

Step 10 Click **OK**.

Gatekeeper Registration Delay

This test sends a lightweight Registration Request (RRQ) from an H.323 gateway to an H.323 gatekeeper and receives a Registration Confirmation (RCF) from the gatekeeper. The test then measures the response time.

Note For the Gatekeeper Registration Delay test to run, the source gateway must have SIP or H323 configured on it.

Step 1 Select **Diagnostics > Node-to-Node Tests**. The Node-to-Node Tests page appears.

Step 2 Click **Create**. The Node-to-Node Test Configuration page appears.

Step 3 In the Test Type pull-down menu select **Gatekeeper Registration Delay**.

Step 4 In the Source pane, using the device selector, select a source device.

Note If you cannot find a recently added device, refresh the device groups. See Troubleshooting Note: Selecting a Source Device, page 11-5.

Step 5 If you want to change the Registration Response Time threshold, in the Thresholds pane, select the check box and enter a new setting (default is 300 m/secs). The setting must be a positive integer (32 bit).

Step 6 In the Run pane configure when the test should run.

- If you want the test to run only once, select the **Once** radio button.
- If you want to schedule the test to run at certain intervals, do the following:
  - Select the schedule radio button.
  - Choose how often you want the test to run.
  - Enter the time between which you want the test to run.
  - Select the days on which the test should run.
  - Enter a test name. The test name cannot contain tabs, question marks, quotation marks, asterisks, semicolons, commas, colons, forward slashes, straight slashes, or backslashes.

Step 7 Click **OK**.

Real-Time Transport Protocol

This test provides DSP-to-DSP measurement of voice quality metrics by integrating with the DSP software. Test calls are placed from the source gateway to the source destination, sending actual real-time protocol (RTP) packets and then collecting statistics from DSPs. In some networks, the remote end may not have DSP. In such situations, the real-time protocol test should measure the metrics by making the remote end loop back the RTP stream. The real-time transport protocol test includes delays in the voice path (path from telephony interface to IP interface on originating gateway and path from IP interface to telephony interface on terminating gateway) in these measurements.

Note For the Real-time Transport Protocol test to run, the source must have a DSP module type of either C5510 or C549 and must have ds0-group of voice ports configured on it.

Step 1 Select **Diagnostics > Node-to-Node Tests**. The Node-to-Node Tests page appears.

Step 2 Click **Create**. The Node-to-Node Test Configuration page appears.

Step 3 In the Test Type pull-down menu select **Real-time Transport Protocol**.

Step 4 In the Source pane, using the device selector, select a source device and interface.

Note If you cannot find a recently added device, refresh the device groups. See Troubleshooting Note: Selecting a Source Device, page 11-5.

Step 5 In the Destination pane, using the device selector, select a destination device and interface.

Step 6 Enter the following details:

Field	Description
General Parameters	
General information about a test.	
Codec Type	Used to determine the packet interval and the request payload.
Call Duration	Test duration.
Voice Quality Expectation	Corresponds to the Access Advantage factor of Mean Opinion Scores (MOS) and Calculated Planning Impairment Factor (CPIF).
Threshold Parameters	
Threshold settings for the test.	
Round-Trip time	Threshold Setting. The Destination to Source Conversational Quality (Number) and Destination to Source Listening Quality (Number) metrics are supported.
Interarrival Jitter	Threshold Setting. The Destination to Source Inter-Arrival Jitter (Milliseconds) metric is supported.
Packet Loss	Threshold Setting. The Destination to Source Packet Loss (Number) metric is supported.
R Factor	Threshold Setting. The Destination to Source Listening Quality (Number) metric is supported.
Operation-Specific Parameters	
When and how often the test runs.	
Polling Time	The number of hours in a 24-hour period during which polling occurs.
Occurrence Pattern	Dates on which the test starts and ends, and hours during which the test is scheduled to run. If the test runs weekly, the Schedule parameter displays days of the week when the test is scheduled to run.
Test Name	User-defined test name. Operations Manager also uses the test name to name the folder in which test data is stored. See the description of the Data Directory field in this table.

Step 7 In the Run pane, configure when the test should run.

- If you want the test to run only once, select the **Once** radio button.
- If you want to schedule the test to run at certain intervals, do the following:
  - Select the every X minutes radio button (where X equals the number of minutes).
  - Choose how often you want the test to run.
  - Enter the times between which you want the test to run.
  - Select the days on which the test should run.
  - Enter a test name. The test name cannot contain tabs, question marks, quotation marks, asterisks, semicolons, commas, colons, forward slashes, straight slashes, or backslashes.

Step 8 Click **OK**.

Importing Multiple Tests

You can import up to 64 tests, the maximum that Operations Manager can support, by importing a seed file.

Before You Begin

- Before you can import a test, you must first add the source devices. See Importing Devices into Operations Manager, page 16-16.
- Make sure your seed file is formatted correctly. See Creating a Node-To-Node Test Import File, page 11-12 for more information.
- Place the seed file on the server, in the `NMSROOT\ImportFiles` directory.

Note NMSROOT is the directory where Cisco Unified Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as "C:\Program Files\CSCOpx" or C:\PROGRA~1\CSCOpx.

Step 1 Select **Diagnostics > Node-to-Node Tests**. The Node-to-Node Tests page appears.

Note If you do not have the required software license, you will not be able to use node-to-node tests. The Diagnostic tab will not appear in Operations Manager.

Step 2 Click **Import**. The Import Node-to-Node Tests page appears.

Step 3 In the Seed Filename field, enter the name of the seed file that contains the test information; for example, Node_to_nodetestImport.txt. The file must be located on the server in the directory that is displayed next to the Server Path field name.

Step 4 Click **OK**.

Operations Manager performs the following actions:

- If this is a file you have imported before, Operations Manager checks to see if any of the devices exist in Operations Manager. If all the information in the import file is the same as what already exists in Operations Manager, a message to that effect appears. Click **OK**.
- Operations Manager displays an error message if there are problems with the format of the import file. Click **OK**, then open the file and correct the listed problems. You cannot import the file until all problems are corrected.
- If there are no errors, a confirmation dialog box appears. The dialog box displays the number of new tests created and the number of tests that will be updated. Click **Yes**.

Creating a Node-To-Node Test Import File

You can import up to 64 tests, the maximum that Operations Manager can support at one time. You can find an example of an import file in the <NMSROOT>\Importfiles folder.

Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as “C:\Program Files\CSCOpx” or C:\PROGRA~1\CSCOpx.

For details on formatting test seed files for specific operations, see Formatting Node-To-Node Test Import Files, page 11-13.

All test seed files should have the following information:

- Test name
- Operation type
- Source device name
- Destination device information
- Operation parameters
- Schedule parameters

The general format for a test seed file is as follows:

- If you create the import file manually, the import file header must say:

  ```
  Cisco Systems Node-to-Node test import, version=3.0;type=CSV;source=manual
  ```

- All values must be separated by commas.
- Start and end dates must be formatted as mm/dd/yyyy; for example, 12/01/2004.
- Start and end times must be formatted on a 24-hour clock as hh:mm; for example, 23:30.
- Entering the source-ip-address is optional. This address is the same as the alternate test address.
- Fill in optional fields with double quotation marks; for example, "".
- For all days of the week, enter a one; otherwise, it should be a zero. If the entry for all days of the week is zero, then you need to enter the days of the week. Separate the days of the week with a vertical bar (|); for example, Mon|Tue|Thu|Fri.

Formatting Node-To-Node Test Import Files

Ping Echo test

```
<testName>,Ping-Echo,<source>,<source-ip-address>,<Destination-Name>,<sample-interval>,<IP
QosType><IPQosValue>,<request-payload>,<LSRHop1|LSRop2|LSRHop3|LSRHop4|LSRHop5|LSRHop6|LSR
Hop7|LSRHop8>,<completionTimeThreshold or "">,<start-time>,<end-time>,<AllDaysOfWeek. 1
for all days otherwise 0>,<DaysOfWeek, if AllDaysOfWeek is 0>

echo-import1,Ping-Echo,source-1,"",dest-1,1,DSCP,9,64,lsr-hop1|lsr-hop2,300,09:00,17:00,1
echo-import2,Ping-Echo,source-1,"",dest-1,1,IPPrecedence,4,64,lsr-hop1|lsr-hop2,"",09:00,1
7:00,0,mon|tue|wed|fri
```

LSRHop is an optional field.

Ping Path Echo test

```
<testName>,Ping-Path-Echo,<source>,<source-ip-address>,<Destination-Name>,<sample-
interval>,<IPQosType>,<IPQosValue>,<request-payload>,<completionTimeThreshold or "">
,<start-time>,<end-time>,<AllDaysOfWeek. 1 for all days otherwise 0>,<DaysOfWeek, if
AllDaysOfWeek is 0>
```

```
ping-path-import2,Ping-Path-Echo,source-2,"",dest-2,3,DSCP,10,32,250,17:00,23:00,0,mon|tue
|wed|thu|fri
ping-path-import2,Ping-Path-Echo,source-2,"",dest-2,3,IPPrecedence,5,32,"",17:00,23:00,1
```

UDP Echo test

```
<testName>,UDP-Echo,<source>,<source-ip-address>,<Destination-Name>,<destination-type>,<sa
mple-interval>,<IPQosType>,<IPQosValue>,<destination-port>,<request-payload>,
<completionTimeThreshold or "">,<start-time>,<end-time>,<AllDaysOfWeek. 1 for all days
otherwise 0>,<DaysOfWeek, if AllDaysOfWeek is 0>

udp-import1,UDP-Echo,source-1,"",udp-dest,IPSLA-Responder,1,IPPrecedence,4,2001,
32,300,17:00,23:00,0,mon|tue|wed|thu|fri
udp-import2,UDP-Echo,source-1,"",udp-dest,IPSLA-Responder,1,DSCP,48,2001,32,"",
17:00,23:00,1
```

The destination type can be either UDP-Server or IP SLA-Responder.

UDP Jitter for VoIP test

Without Codec (Node-to-Node Quality) Support:

```
<testName>,Data-Jitter,<source>,<source-ip-address>,<IPSLA-Responder>,<sample-interval>,
<IPQosType>,<IPQosValue>,<request-payload>,<inter-packet-interval>,<number-of-packets>,
<destination-port>,<pktlossSDThreshold or "">,<pktlossDSThreshold or "">,
<jitterSDThreshold or "">,<jitterDSThreshold or "">,<avgLatencyThreshold or "">,
<start-time>,<end-time>,<AllDaysOfWeek. 1 for all days otherwise 0>,<DaysOfWeek, if
AllDaysOfWeek is 0>

jitter-import1,Data-Jitter,source-1,source-1,dest-with-IPSLA-Responder,3,DSCP,24,64,30,20,
2002,30,30,25,25,50,17:00,23:00,0,mon|tue|wed|thu|fri
```

WITH Codec (Node-to-Node Quality) Support, valid for IOS version 12.3(4)T or higher:

```
<testName>,Data-Jitter,<source>,<source-ip-address>,<IPSLA-Responder>,<sample-interval>,
<IPQosType>,<IPQosValue>,<codecType>,<voiceQualityBenchMark>,<number-of-packets>,
<destination-port>,<pktlossSDThreshold or "">,<pktlossDSThreshold or "">,
<jitterSDThreshold or "">,<jitterDSThreshold or "">,<avgLatencyThreshold or "">,
<nodeToNodeQualityThreshold or "">,<start-time>,<end-time>,<AllDaysOfWeek. 1 for all days
otherwise 0>,<DaysOfWeek, if AllDaysOfWeek is 0>

jitter-import2,Data-Jitter,source-1,source-1,dest-with-IPSLA-Responder,3,IPPrecedence,5,G.
711ulaw,LandLine,20,2002,30,30,25,25,50,"",17:00,23:00,1
```

Read-community-string is an optional field. If you specify a community string, Operations Manager validates the IP SLA Responder.

VoIP Gatekeeper Registration Delay test, scheduled daily

```
<testName>,Voip-GKReg-Delay,<source GateWay>,<sample-interval>,
<GatekeeperRegistrationTimeThresholdor "">,<start-time>,<end-time>,<AllDaysOfWeek. 1 for
all days otherwise 0>,<DaysOfWeek, if AllDaysOfWeek is 0>

gkregdelay-import1,Voip-GKReg-Delay,source-gateway,3,50,17:00,23:00,0,mon|tue|wed|thu|fri
gkregdelay-import2,Voip-GKReg-Delay, source-gateway,5,"",17:00,23:00,1
```

Editing Tests

After you have created tests to Operations Manager, you can change test parameters, or, if you want to remove a test from Operations Manager, you can delete it.

You can use this function to edit the parameters of an existing test. For example, you can change the operation parameters of a test or change the schedule. You cannot change the destination device.

Step 1 Select **Diagnostics > Node-to-Node Tests**. The Node-to-Node Tests page appears.

Step 2 Select the test you want to edit, and then click **Edit**. The Edit Node-to-Node Test page appears.

Step 3 You can change the test parameters, including scheduling and threshold settings. See Working with Node-To-Node Tests, page 11-1 for more information.

Step 4 Click **OK** when done.

Deleting a Test

You can use this function to delete one or more tests. You can delete tests in any state. See Table 11-8 for a description of possible states.

Step 1 Select **Diagnostics > Node-to-Node Tests**. The Node-to-Node Tests page appears.

Step 2 Select the tests you want to delete, and then click **Delete**. A confirmation dialog box appears.

Step 3 Click **Yes**. Operations Manager deletes the tests you selected.

Node-To-Node Test Events

The threshold settings that you set during test creation or during modification determine when a node-to-node event is generated. See Working with Node-To-Node Tests, page 11-1.

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

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

- NodeToNodeTestFailed

Note To determine why a Node-to-Node test failed and how to clear it, see the IP SLA documentation located on Cisco.com at the following locations:

- http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_book09186a008043be2d.html
- http://www.cisco.com/en/US/products/ps6350/products_command_reference_book09186a008042df8f.html

- RoundTripResponseTime_ThresholdExceeded
- RingBackResponseTime_ThresholdExceeded
- RegistrationResponseTime_ThresholdExceeded

- AverageLatency_ThresholdExceeded
- PacketLossSD_ThresholdExceeded
- PacketLossDS_ThresholdExceeded
- IAJitterDS_ThresholdExceeded
- RFactorDS_ThresholdExceeded
- MosCQDS_ThresholdExceeded
- MosLQDS_ThresholdExceeded
- RTPPacketLossDS_ThresholdExceeded

For details on the node-to-node events, see Events Processed, page E-1.

Managing Test Operations

The following topics discuss these tasks:

Viewing Test Trending

You can select and examine changes in network performance metrics. You can select, display, and chart network performance data in real time. For details on the types of metrics you can graph, see What Metrics Can I Include on a Graph?, page 7-1.

Step 1 Select **Diagnostics > Node-to-Node Tests**. The Node-to-Node Tests page appears.

Step 2 Select the test you want to trend, and click **Trend**.

- If you select a UDP Jitter for VoIP test, a Select Metrics dialog box appears.
  a. Select the metrics you want to graph. The metrics must have the same units.
  b. Click **View Graph**.
- If you select any of the other tests, a second dialog box does not appear.

A Node-to-Node Test Trend graph appears. For details about working with performance graphs, see How to Use Performance Graphs, page 7-1.

Viewing Test Information

You can find all the details about a particular test on the Test Details page. From this page, you can print or export test information.

Step 1 Select **Diagnostics > Node-to-Node Tests**. The Node-to-Node Tests page appears.

Step 2 Select the test you want to view, and click **View**. The Test Details window opens.

Table 11-7 explains the contents of the window.

Table 11-7 Test Details

Field	Description
General Parameters	
General information about a test.	
Test Name	User-defined test name. Operations Manager also uses the test name to name the folder in which test data is stored. See the description of the Data Directory field in this table.
Operation Type	Type of test operation; for example, Ping Echo.
Source	Name or IP address of the source device.
Source Interface	IP address of an interface on the source device. Can also be listed as *Default*. In the case of *Default*, the IP SLA engine in the source device determines the source interface.
IP SLA Responder	Name of the IP SLA-enabled destination device.
Current Status	The status of the test. See Table 11-8 on page 11-20 for a description of possible states. The state of the test determines whether you can stop or define the test at any given point. The state also determines the state of the data collection. If the status is Config Failed, a description of the cause of the failure appears. If the test status is Config Failed or Config Pending, an explanation appears.
Admin Index	Unique numeric identifier for a test on the source device. See the Note following this table for more information.
Data Directory	Directory in which Operations Manager stores test data. The Data Directory name matches the test name. See Where Is Node-To-Node Test Data Stored?, page 11-20.
Schedule Parameters	
When and how often the test runs.	
Polling Time	The number of hours in a 24-hour period during which polling occurs.
Occurrence Pattern	Dates on which the test starts and ends, and hours during which the test is scheduled to run. If the test runs weekly, the Schedule parameter displays days of the week when the test is scheduled to run.
Operation-Specific Parameters (UDP Jitter for VoIP example)	
Information about the specific kind of operation a test is running. The following part of the table is an example of operation-specific parameters for a UDP Jitter for VoIP test. Other test types will have different operation-specific parameters. For information on operation-specific parameters for other operation types, see Creating a Single Node-To-Node Test, page 11-2.	
Sample Interval (minutes)	The frequency with which the source device polls the destination device and Operations Manager polls the source device.

Table 11-7 Test Details (continued)

Field	Description
Duration	Test duration.
Codec	Used to determine the packet interval and the request payload.
IP QoS Type	The quality of service policies for the IP SLA packets.
IP QoS Value	Quality of service value.
Voice Quality Expectation	Corresponds to the Access Advantage factor of Mean Opinion Scores (MOS) and Calculated Planning Impairment Factor (ICPIF).
Destination Port	The default destination port is 16400.
Threshold Parameters	
Threshold settings for the test.	
Average Latency	Threshold Setting
Packet Loss Source to Destination	Threshold Setting
Packet Loss Destination to Source	Threshold Setting
Jitter Source to Destination	Threshold Setting
Jitter Destination to Source	Threshold Setting
Node-to-Node Quality	Threshold Setting

Note While the test is the Running state, you can view test information directly on the source device. Telnet to the source device and use the command **show rtr configuration** <*admin index*>.

Printing Test Details

You can print all the details about a test shown on the Test Details page.

Step 1 Select **Diagnostics > Node-to-Node Tests**. The Node-to-Node Tests page appears.

Step 2 Select the test you want and click **View**. The Test Details window opens.

Step 3 To print the test details information, click the printer icon in the upper-right corner of the window.

The records are reformatted into a print-friendly format and are displayed in a new browser window.

Step 4 Use the print function on your browser to print the display.

Exporting Test Details

You can export and save all the details about a single test as shown on the Test Details page, including configuration and status. This is not the same thing as exporting the data gathered by a test. To see how to save and export data gathered by a test, see Copying Test Data to Another Server, page 11-21.

Step 1 Select **Diagnostics > Node-to-Node Tests**. The Node-to-Node Tests page appears.

Step 2 Select the test you want and click **View**. The Test Details window opens.

Step 3 To export the test details information, click the export icon in the upper-right corner of the window. Select either **CSV** or **PDF** format for export and click **OK**.

Step 4 If you chose CSV in Step 3, do the following:

a. When the File Download dialog box appears, click **Save**.

b. In the Windows folder window, enter the filename and the location where you want to save the file.

c. Click **Save**.

d. In the Download Complete dialog box, click **Close**.

Step 5 If you chose PDF in Step 3, do the following:

a. If a security information dialog box appears, click **Yes**. The records now appear in PDF format.

b. Use the PDF save function to save the file to your system.

Verifying the Status of a Test

You can verify whether a test ran and completed correctly. You can also troubleshoot the test if necessary.

Step 1 Select **Diagnostics > Node-to-Node Tests**. The Node-to-Node Tests page appears. All current Node-to-Node tests appear in the page. The last column in the table shows the status of each test.

Table 11-8 Test Status Definitions

Test Status	Description
Running	The test is active and collecting data.
Config Pending	Either the device is not responding or configuration of the test is under way.
Delete Pending	Intermediate state, before the test is deleted. No actions can be performed on the test.
Suspended	The test is suspended from data collecting or polling. This occurs because the device was suspended.
Scheduled	Appears after you create or update a test. The status will change to Running at the first polling cycle.
Dormant	The test is active but not currently collecting data. Tests are in the Dormant state between polling cycles.
Config Failed	The test was not configured correctly. Possible problems include incorrect device credentials or low device memory. You can see more information on why the test configuration failed by viewing the Study Details page.

Working with Test Data

Operations Manager saves the data collected by tests to disk.

The following topics provide information you will need to use the data, keep the data safe, and prepare to run additional tests:

- Where Is Node-To-Node Test Data Stored?, page 11-20
- Maintaining Node-To-Node Test Data, page 11-21
- Copying Test Data to Another Server, page 11-21
- What Is the Format of the Node-To-Node Data?, page 11-22

Where Is Node-To-Node Test Data Stored?

Node-to-node test data is stored on the Operations Manager server in the NMSROOT\data\N2Ntests folder.

Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as “C:\Program Files\CSCOpx” or C:\PROGRA~1\CSCOpx.

Table 11-9 shows the two different types of files stored in the data storage directory.

Table 11-9 Test Data Files and Log Files

File Names	Contents
YYYYMMDD.csv	The test data. Each file has multiple records. Each record is a comma-separated values (CSV) record, and there is one record in a file for each polling interval.
StudyInfo.log	The log includes test name, description, polling interval, devices, start date, end date, operation type, polling interval, and status.

Maintaining Node-To-Node Test Data

You should perform all tasks related to maintaining test data, including the following:

- **Verify that there is sufficient disk space to store test data.** Check disk space before a test is scheduled to run. Operations Manager appends data to a test's log files. Operations Manager produces one data file for each running test per day when a test is running. Assess the amount of space used by previous tests to derive an estimate.

  For example, 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.

- **Export and save test data.** Operations Manager purges all data files more than 31 days old. You must save the test to another server to maintain data for more than 31 days. See Copying Test Data to Another Server, page 11-21.

- **Back up the test data.** Operations Manager writes test data to the Data Storage Directory, displayed in the Test Details window. Perform regular backups using the same method you use to back up your file system.

- **Determine when to copy data to another server.** You should copy test data to another server before you examine it.

- **Display and use the data.** You can analyze the results of the test after you import the test data into Microsoft Excel or by using a third-party report-generating tool.

Note Do not open test data files using any application that acquires an exclusive read-only lock on files while the test is in the Running state. If test data files are locked, Operations Manager will not be able to write output data and will instead write errors to the log files. Examples of applications that acquire an exclusive lock are Microsoft Excel and Microsoft Word. You can use these applications when the test is not running.

Copying Test Data to Another Server

You must copy test data to another server before you examine it. You may also want to copy the test data to another server as a means of backup. Test data is in ASCII format. You can copy it to another server using whatever method is available to you; for example, SSH or copy-and-paste. Copy the test data files from the Data Storage Directory. Test data files are those whose names end with .csv, because the test data is written to CSV files.

Note If you use drag-and-drop, you risk moving the test data instead of copying it.

What Is the Format of the Node-To-Node Data?

Operations Manager provides one record type for each type of data collected. The record types are summarized in Table 11-10.

For details on the format of all exported data, see Data File Formats, page J-1.

Table 11-10 Node-To-Node Record Types

Type	Definition
200	Echo—This record format captures end-to-end statistics for the following types of tests: • ICMP Echo • UDP Echo • Gatekeeper Registration Delay
201	Path Echo—This record format captures hop-by-hop statistics for ICMP Path Echo tests. The tests record information from source to destination.
204	Path Echo (Destination Hop)—This record format captures end-to-end statistics for ICMP Path Echo tests. The tests are from the source to the destination.
205	UDP Jitter for VoIP—This record format captures the end-to-end statistics for UDP Jitter for VoIP (Enhanced UDP) tests. The tests record information from source to destination.

PART 4

Reports

CHAPTER 12

Using History Reports

These topics explain how to use Cisco Unified Operations Manager (Operations Manager) Alert and Event History and Service Quality History reports:

Getting Started with History Reports

Alert and Event History reports and Service Quality History reports enable you to view alerts and events that occurred during the past year. The available information includes alert status and date, related device and device components, annotations (informational text you entered), and event details. Depending on the criteria you use to generate the report, the Alert and Event History reports can display information for both devices and clusters. Operations Manager purges the Alert History database daily to retain only 31 days of history; see Viewing Purge Scheduler Status, page 20-11.

Note Service Quality History is useful only if you have purchased a license for Cisco Unified Service Monitor (Service Monitor). For more information, see *User Guide for Cisco Unified Service Monitor.*

For more information, see the following topics:

- Getting Started with Alert and Event History, page 12-2
- Getting Started with Service Quality History Reports, page 12-14

History Report Tool Buttons

Table 12-1 explains the tool buttons that appear in the upper-right corner of history reports.

Table 12-1 Alert and Event History Report Window Tool Buttons

Icon	Meaning
	Exports the current report to a CSV file. **Note** The PDF export option is not available from Alert, Event, and Service Quality event history reports.
	Opens a printer-friendly version for printing.
	Opens context-sensitive help.

Reports with More than 2,000 Records

The Alert History and Event History reports display up to 2,000 records that you can scroll or page through. If your report exceeds 2,000 records and you want to view all of them, use the Export tool button to save all of the information to a CSV file.

Getting Started with Alert and Event History

You can generate 24-hour context-based reports from various Operations Manager pages, such as the Topology display. You can also generate customized history reports for which you supply the search criteria and set the date range. You can generate Event History reports for devices, device components, and clusters. You can also export 24-hour and 7-day reports automatically.

Several conditions exist in Alert and Event History displays as follows:

- The Alert History limit is increased to 2,000 and Alerts and Events Display (AAD) limitation is 1,000.
- **Symptom:** The Alerts and Events View displays only the first 999 alerts and Alerts Display Window (ADV) limitation is 1,000 events.

  Conditions: When over 1,000 events exist for a given alert, the Alerts Display Window displays the first 1,000 events. The remaining events are not displayed, although they exist in the database.

  Workaround: View the remainder of the more than 1,000 events for that alert in the Alert and Event report.
- **Symptom**: When over 5,000 events are generated in the network at a time, some events are dropped by Alert and Event History.

  Conditions: The Alert and Event History processes up to 5,000 events during a burst of more than 5,000 events.

  Workaround: View the events in the Alerts and Events display. These events are processed by the system and displayed in this display.Note that if the events get cleared they are not displayed on the Alerts and Events Display after 30 to 60 minutes.

24-Hour Context-Based Alert and Event History Reports

On various Operations Manager pages, such as the Alerts and Events display, you can select Alert History or Event History links or menu items. When you click an Alert History or Event History link, you generate a *context-based* report that displays relevant history records:

- For which you do not need to enter search criteria.
- For the past 24 hours.

You can also generate customized Alert History and Event History reports for a time period that you select and include records based on search criteria that you specify. Alert History and Event History reports include the same type of information whether you generate context-based or customized reports.

You can generate 24-hour context-based history reports from various Operations Manager pages. For example, from:

- Service Level View—You can launch an Alert History report for a device or cluster.
- Phone Activity display—You can launch a Service Quality History report for a phone model.

Note Operations Manager stores Service Quality history if you have purchased a license for Service Monitor. For more information, see *User Guide for Cisco Unified Service Monitor*.

Customized Alert History and Event History Reports

You might want to generate an Alert History report or an Event History report when:

- A significant alert is shown in the Alerts and Events display, and you want to see how often the alert has been generated in the last month.
- You receive an e-mail notification that an unusual event has occurred.
- You want to search for information on events and alerts other than those you are tracking in your customized Alerts and Events display.

You can generate an Event History report to gather information on:

- All events that caused an alert.
- Events that occurred on components of a device.
- Occurrences of the same event on different devices.
- Clusters (which can be selected under device groups).

Exporting 24-Hour and 7-Day Alert and Event History Reports

Use this procedure to automatically generate 24-hour Alert and Event History reports daily at midnight and 7-day Alert and Event History reports weekly at midnight on Monday. You can generate these reports in comma-separated value (CSV) format, save them on disk, and e-mail them.

Step 1 Select **Reports > Alert and Event History > Export**. The automatically Export Alert and Event Reports page appears.

Step 2 For each report that you want to generate, select CSV to save the report as a comma-separated-values file.

Reports that you can generate are:

- All alerts for the last 24 hours—24-hour reports are named AlertReports_Daily_ddmmyyyy.filetype, for example AlertReports_Daily_20Apr2006.csv
- All alerts for the last 7 days—7-day reports are named AlertReports_Weekly_ddmmyyyy.filetype, for example AlertReports_Weekly_17Apr2006.csv. 7-day reports run weekly on Monday at midnight.
- All events for the last 24 hours—24-hour reports are named EventReports_Daily_ddmmyyyy.filetype, for example EventReports_Daily_20Apr2006.csv.
- All events for the last 7 days—7-day reports are named EventReports_Weekly_ddmmyyyy.filetype, for example EventReports_Weekly_17Apr2006.csv. 7-day reports run weekly on Monday at midnight.

Step 3 Enter one or more locations to store or send the report:

- If you want to store the reports on disk, enter (or browse to and select) a location on the server.

Note Casuser and administrator have write permissions in the default directory. If you change the directory, make sure that the directory has write permission for casuser. If you do not, the export files will not be created.

- If you want to e-mail the reports, enter a fully qualified e-mail address.

Step 4 Click **Apply**.

Generating Customized Alert and Event History Reports

To gather historical information on alerts and events in the past 31 days, start Alert and Event History from the Operations Manager home page by selecting **Reports > Alert and Event History**. The following topics explain how you can apply filters and generate reports based on all information stored in the Alert History database:

- To search for alerts by alert ID, devices, or group, see Getting All Stored Information on an Alert, page 12-4.
- To search for events on devices by event ID, device, alert ID, or group, see Getting All Stored Information on an Event, page 12-7.
- To search for Service Quality events on Cisco 1040s, call endpoints, or phone models, see Getting All Stored Information on a Service Quality Event, page 12-15.

Note Service Quality History reports are available only if you have purchased a license for Service Monitor.

Getting All Stored Information on an Alert

You can search the Alert History database for alerts using one of the following methods:

- Searching for Alerts by Alert ID, page 12-5

- Searching for Alerts by Device, page 12-5
- Searching for Alerts by Device Group, page 12-6
- Searching for Alerts by Date, page 12-6

Note Alternatively, to generate a 24-hour report of all alerts in your current view, launch Alert History for the selected view from the Alerts and Events window. See Monitoring Alerts and Events, page 3-1.

Searching for Alerts by Alert ID

To determine how often a specific alert has occurred, search for the alert by its alert ID. The alert ID is displayed in the Alerts and Events display.

Step 1 Select **Reports > Alert and Event History > Alert History > Alert**. The Alert History: Search by Alert ID page appears.

Step 2 Set your search criteria:

a. Enter the alert ID.

b. Select all alert severity levels that you want to search for.

c. Select the date range:

- Today.
- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**. If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Alert History report opens. This report contains information on both devices and clusters. For an explanation of the report contents, see Understanding the Alert History Report, page 12-10.

Searching for Alerts by Device

Use this procedure to determine what types of alerts are occurring on a specific device.

Step 1 Select **Reports > Alert and Event History > Alert History > Devices**. The Alert History: Search by Device page appears.

Step 2 Set your search criteria:

a. Enter a comma-separated list of devices (as they are listed by Device Management).

b. Select all alert severity levels that you want to search for.

c. Select the date range:

- Today.
- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**. If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Alert History report opens. This report contains information on devices only. For an explanation of the report contents, see Understanding the Alert History Report, page 12-10.

Searching for Alerts by Device Group

To determine what type of alerts are occurring in a specific device group, use this procedure.

Step 1 Select **Reports > Alert and Event History > Alert History > Device Groups**. The Alert History: Search by Group page appears.

Step 2 Set your search criteria:

a. Select the device group. You can also select multiple devices from different groups.

b. Select all alert severity levels that you want to search for.

c. Select the date range:

- Today.
- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**. If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Alert History report opens. This report contains information on devices only. For an explanation of the report contents, see Understanding the Alert History Report, page 12-10.

For more information, see the following topics:

- Customizing Events, page 15-23
- Events Processed, page E-1

Searching for Alerts by Date

To determine what type of alerts are occurring during a specific day, week, month, or range of dates, use this procedure.

Step 1 Select **Reports > Alert and Event History > Alert History > Date**. The Alert History: Search by Date page appears.

Step 2 Select the date range and enter:

- Today.
- 7 days (from *current date* to *date*).
- One Month (from *current date* to *date*).
- From*: date* and to: *a date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.).

Step 3 Click **View**. If more than 1,000 records match your search criteria, a popup window reports the total number of records found. The Alert History report opens. This report contains information on both devices and clusters. For an explanation of the report contents, see Understanding the Alert History Report, page 12-10.

For more information, see the following topics:

- Customizing Events, page 15-23
- Events Processed, page E-1

Getting All Stored Information on an Event

Note For information about Service Quality events, see Getting All Stored Information on a Service Quality Event, page 12-15.

You can search the Alert History database for events using one of the following methods:

- Searching for Events by Event ID, page 12-7
- Searching for Events by Device, page 12-8
- Searching for Events by Alert, page 12-9
- Searching for Events by Device Group, page 12-9
- Searching for Events by Date, page 12-10

Note Alternatively, to generate a 24-hour report of all events on a device component, click the Event History link on the Alerts Detail page. See Monitoring Alerts and Events, page 3-1.

Searching for Events by Event ID

To determine how often a specific event has occurred, search for the event by its event ID. The event ID is displayed on the Alert Details display.

Step 1 Select **Reports > Alert and Event History > Event History > Event**. The Event History: Search by Event ID page appears.

Step 2 Set your search criteria:

a. Enter the event ID.

b. Select the date range:

- Today.
- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**. If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Event History report opens. This report contains information on both devices and clusters. For an explanation of the report contents, see Understanding the Event History Report, page 12-12.

Searching for Events by Device

Use this procedure to determine what types of events are occurring on a specific device.

Step 1 Select **Reports > Alert and Event History > Event History > Devices**. The Event History: Search by Device page appears.

Step 2 Set your search criteria:

a. Enter a comma-separated list of devices (as they are listed by Device Management). You can select multiple devices from different groups.

b. Enter the event description by clicking the popup selector box and selecting the events for which you want to search. By default, all events are selected. (See Selecting Event Descriptions for an Event History Report, page 12-8.)

c. Select the date range:

- Today.
- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**. If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Event History report opens. This report contains information on devices only. For an explanation of the report contents, see Understanding the Event History Report, page 12-12.

Selecting Event Descriptions for an Event History Report

By default all events are selected on the Event Descriptions dialog box.

Note The Event Description filter window under **Reports > Alert and Event History > Device group** displays default event names. When the event report is launched, the customized name will be displayed. To determine the default name is for customized events, go to **Notifications ->Event Customization**.

Step 1 Deselect events that you do not want to include in the Event History report. (When you deselect an event, if checked, the All check box at the top of the dialog box is also deselected.)

Step 2 Do one of the following:

- Click **Select** at the top or bottom of the dialog box to finalize your selections.
- Select **Cancel** at the top or bottom of the dialog box to cancel your selections and return to the default list of all events.

Searching for Events by Alert

To view the events that correspond to a specific alert, use this procedure.

Step 1 Select **Reports > Alert and Event History > Event History > Alert**. The Event History: Search by Alert ID page appears.

Step 2 Set your search criteria:

a. Enter the Alert ID.

b. (Optional) Enter the event description by clicking the popup selector box and selecting the events for which you want to search. (See Selecting Event Descriptions for an Event History Report, page 12-8.)

c. Select the date range:

- Today.
- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**. If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Event History report opens. This report contains information on both devices and clusters. For an explanation of the report contents, see Understanding the Event History Report, page 12-12.

Searching for Events by Device Group

To determine what types of events are occurring in a specific device group, use this procedure.

Step 1 Select **Reports > Alert and Event History > Event History > Device Groups**. The Event History: Search by Device Group page appears.

Step 2 Set your search criteria:

a. Select one or more device groups.

b. Enter the event description by clicking the popup selector box and selecting the events for which you want to search.

c. Select all alert severity levels that you want to search for.

d. Select the date range:

- Today.
- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**. If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Event History report opens. This report contains information on devices only. For an explanation of the report contents, see Understanding the Event History Report, page 12-12.

For more information, see the following topics:

- History Report Tool Buttons, page 12-2
- Customizing Events, page 15-23
- Events Processed, page E-1

Searching for Events by Date

To determine what type of alerts are occurring during a specific day, week, month, or range of dates, use this procedure.

Step 1 Select **Reports > Alert and Event History > Event History > Date**. The Event History: Search by Date page appears.

Step 2 Select the date range and enter:

- Today.
- 7 days.
- One Month.
- From*: a date* and to: *a date*—Enter or select dates.

Step 3 Click **View**. If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Event History report opens. This report contains information on both devices and clusters. For an explanation of the report contents, see Understanding the Event History Report, page 12-12.

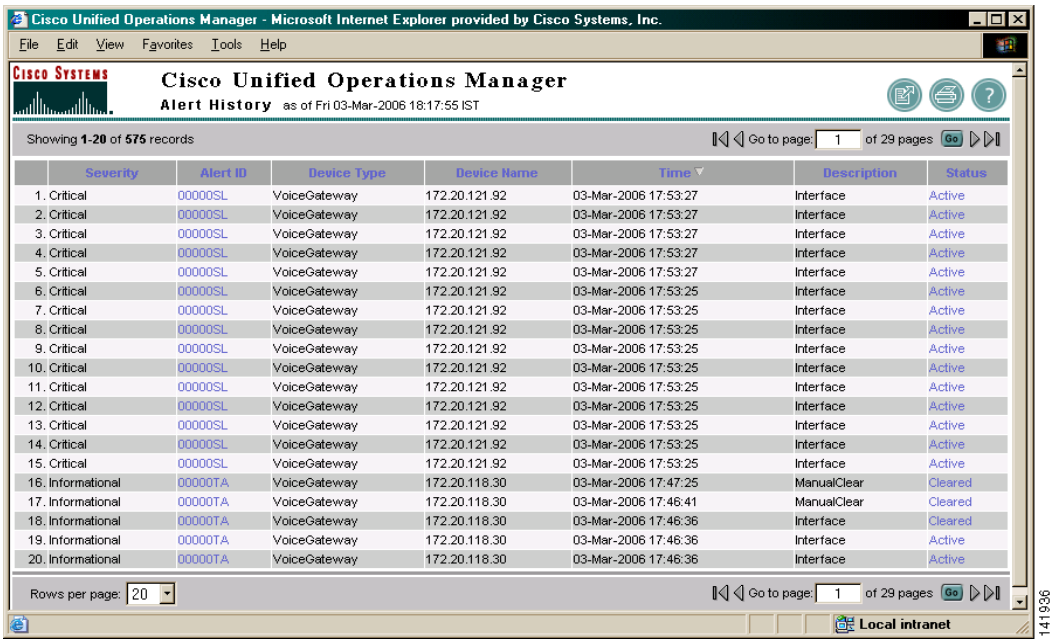
For more information, see the following topics:

- History Report Tool Buttons, page 12-2
- Customizing Events, page 15-23
- Events Processed, page E-1

Understanding the Alert History Report

The Alert History report (shown in Figure 12-1) is a scrollable table that lists up to 1,000 records, based on your search criteria. To view database contents beyond the 1,000 records, click the Export tool button in the upper-right corner of the window.

Figure 12-1 Alert History Report



The Alert History report window provides tools, as shown in Table 12-1.

Table 12-2 describes the contents of the Alert History report.

Table 12-2 Alert History Report—Contents

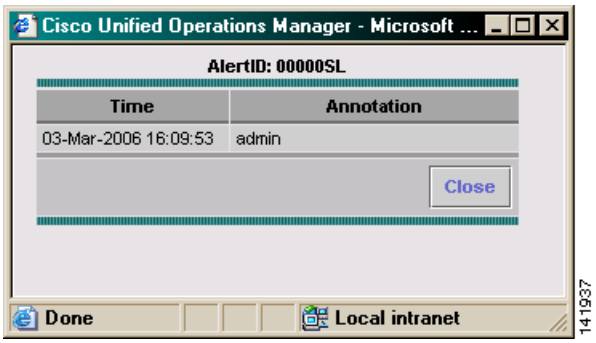
Heading	Description
Alert ID	Alert identifier number. Clicking this link opens the Event History report (see Figure 12-4 on page 12-14), which contains details about the events associated with the alert.
Device Name	Device name or IP address.
Device Type	Device type. Inventory Collection in Progress indicates that Operations Manager was discovering the device or cluster at the time of the alert. The actual device type is reflected when new events occur. The device type is displayed as N/A during inventory collection. For more information, see Chapter 16, "Using Device Management."
Description	Alert category, one of the following: Application, Connectivity, Environment, Interface, Other, Reachability, System Hardware, Utilization. For alerts containing multiple events, the report shows the category of the event with the most recent change. For alerts containing multiple events, the report shows the category of the event with the most recent change.
Severity	Critical, Warning, or Informational.
Time	Date and time when the alert was generated.
Status	Alert status, based on last polling.
	Active
	Cleared
	Acknowledged

Viewing User Annotations from an Alert History Report

From an Alert History report, click a link in the Status column to open the alert annotation page.

Figure 12-2 shows an alert annotation page, which lists any notes that users have entered using the Alert Details page. (For more information, see Responding to Alerts, page 3-28.)

Figure 12-2 Alert Annotation Page



Launching Event History from an Alert History Report

To launch an Event History report from an Alert History report, click the alert ID link that interests you. The Event History report opens in a new window and lists the events that caused the alert to be generated.

Understanding the Event History Report

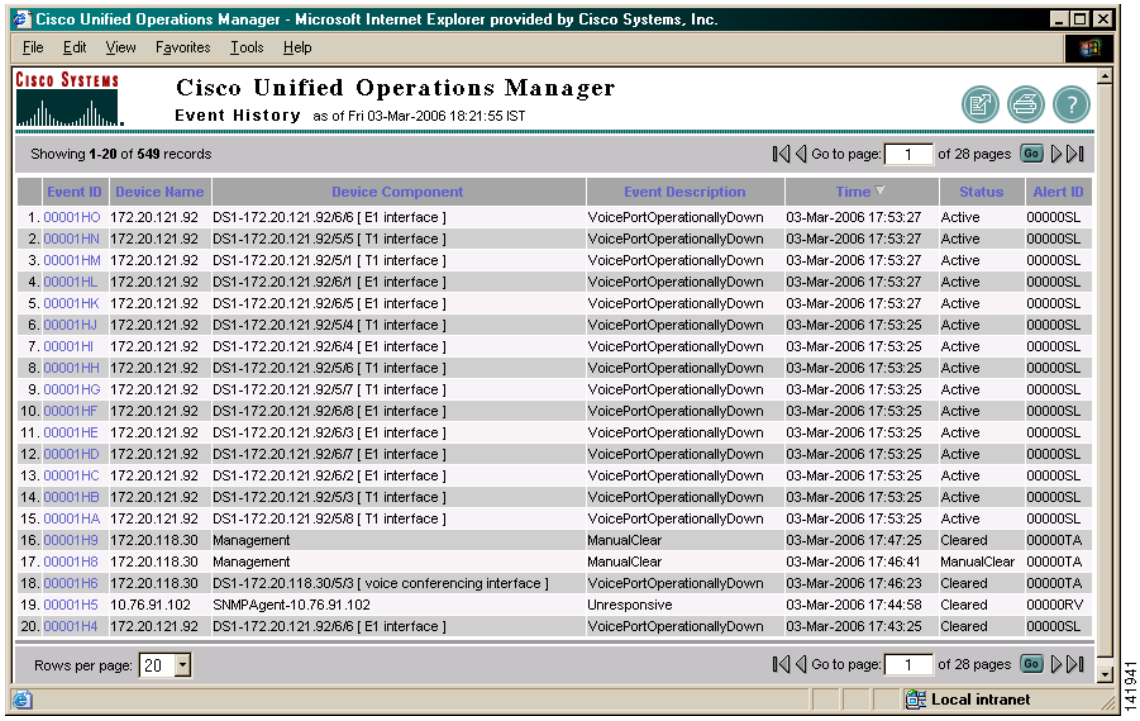
Note Service Quality events are reported on Service Quality History reports. See Understanding the Service Quality History Report, page 12-19.

The Event History report lists events. For each event, the Event History report includes:

- Device on which the event occurred
- Component on which the event occurred
- Time of the event
- Current status of the event
- Event ID link to open the Event Properties page and view current attribute or threshold values compared with the values at the time the event occurred

Figure 12-3 provides an example of an Event History report.

Figure 12-3 Event History Report



The Event History report window provides tool buttons in the upper-right corner of the window; these are described in Table 12-1.

Table 12-3 describes the contents of the Event History report in more detail.

Table 12-3 Event History Report—Contents

Heading	Description
Event ID	Event identifier number. Clicking this link opens the event properties page (see Figure 12-4), which describes the value of MIB attributes currently and at the time of the event.
Device Name	Device name or IP address.
Component	Device element on which the event occurred.
Description	Operations Manager event name (as described in Appendix E, "Events Processed"). You can also customize the names of events displayed by Event History (and the Alerts and Events display) using the Event Customization feature in Notifications. For more information, see Customizing Events, page 15-23.
Time	Date and time when the event was generated.

Table 12-3 Event History Report—Contents (continued)

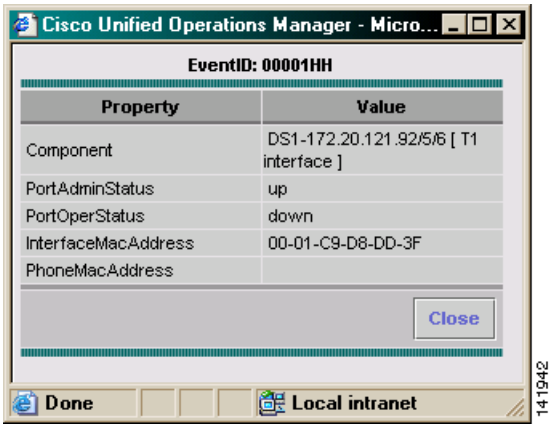
Heading	Description	
Status	Event status, based on last polling.	
	Active	Event is live.
	Cleared	Event is no longer live. Also, when a device is suspended, all alerts are cleared. When Operations Manager polling determines that an alarm has been in the Cleared state for 30 minutes or more (from the time of polling), the alarm expires and is removed from the Alerts and Events display.
	Suspended	Device is suspended.
	Resumed	Device is being resumed.
	Deleted	Device has been deleted.
Alert ID	Alert identifier number associated with this event.	

Viewing Event Properties from an Event History Report

From an Event History report, click an event in the Event ID column to open the Event Properties page. The page lists more information about an event, such as the value of MIB attributes, polling and threshold information, and utilization information. Values at the time of the event are listed alongside current values.

Figure 12-4 shows an example of the event properties page.

Figure 12-4 Event Properties Page



Getting Started with Service Quality History Reports

This section contains the following topics:

- Exporting 24-Hour and 7-Day Service Quality History Reports, page 12-15
- Getting All Stored Information on a Service Quality Event, page 12-15

Exporting 24-Hour and 7-Day Service Quality History Reports

Use this procedure to automatically generate 24-hour Service Quality History reports daily at midnight and 7-day Service Quality History reports weekly at midnight on Monday. You can generate these reports in comma-separated value (CSV) format, save them on disk, and e-mail them.

Step 1 Select **Reports > Service Quality History > Event History > Export**. The automatically Export Service Quality Reports page appears.

Step 2 Select one or more reports and report formats:

- All issues for the last 24 hours—Select one or more check boxes to generate and save a 24-hour Service Quality History report as CSV (a comma-separated-values file).

  Note 24-hour reports are named ServiceQualityReports_Daily_ddmmyyyy.filetype, for example ServiceQualityReports_Daily_20Apr2006.csv.

- All issues for the last 7 days—Select one or more check boxes to generate and save a 7-day Service Quality History report as CSV.

  Note 7-day reports are named ServiceQualityReports_Weekly_ddmmyyyy.filetype, for example ServiceQualityReports_Weekly_20Apr2006.csv. 7-day reports run weekly on Monday at midnight.

Step 3 Enter one or more locations to store or send the report:

- If you want to store the reports on disk, enter (or browse to and select) a location on the server.

  Note Casuser and administrator have write permissions in the default directory. If you change the directory, make sure that the directory has write permission for casuser. If you do not, the export files will not be created.

- If you want to e-mail the reports, enter a fully qualified e-mail address.

Step 4 Click **Apply**. The reports will be generated daily at midnight.

Getting All Stored Information on a Service Quality Event

Note Service Quality History reports are only available if you have purchased a license for Service Monitor. For more information, see *User Guide for Cisco Unified Service Monitor.*

You can search the Alert History database for Service Quality events using one of the following methods:

- Searching for Service Quality Events by MOS, page 12-16
- Searching for Service Quality Events by Destination, page 12-16
- Searching for Service Quality Events by Codec, page 12-17

- Searching for Service Quality Events by Phone Model, page 12-17
- Searching for Service Quality Events by Cisco 1040, page 12-17
- Searching for Service Quality Events by Date, page 12-18

Searching for Service Quality Events by MOS

To view the Service Quality events for MOS less than a value that you supply, use this procedure.

Step 1 Select **Reports > Service Quality History > Event History > MOS**. The Service Quality History: Search by MOS page appears.

Step 2 Set your search criteria:

a. MOS less than—Enter the lowest value. The range of MOS values is .1 to 4.9.

b. Select the date range:

- Today.
- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**. If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Service Quality History report opens. For an explanation of the report contents, see Understanding the Service Quality History Report, page 12-19.

Searching for Service Quality Events by Destination

To view the Service Quality events that correspond to call endpoints, use this procedure.

Step 1 Select **Reports > Service Quality History > Event History > Destination**. The Service Quality History: Search by Destination page appears.

Step 2 Set your search criteria:

a. Select an operator:

- Is exactly
- Begins with
- Contains

b. Enter the destination—IP address for a phone, voice gateway, or Cisco 1040.

c. Select the date range:

- Today.
- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**. If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Service Quality History report opens. For an explanation of the report contents, see Understanding the Service Quality History Report, page 12-19.

Searching for Service Quality Events by Codec

To view the Service Quality events for a particular codec, use this procedure.

Step 1 Select **Reports > Service Quality History > Event History > Codec**. The Service Quality History: Search by Codec page appears.

Step 2 Set your search criteria:

a. Select a codec from the list.

b. Select the date range:

- Today.
- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**. If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Service Quality History report opens. For an explanation of the report contents, see Understanding the Service Quality History Report, page 12-19.

Searching for Service Quality Events by Phone Model

To view the Service Quality events that correspond to specific phone models, use this procedure.

Step 1 Select **Reports > Service Quality History > Event History > Phone Model**. The Service Quality History: Search by Phone Model(s) page appears.

Step 2 Set your search criteria:

a. Click the popup selector box and select the phone models for which you want to search.

b. Select the date range:

- Today.
- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**. If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Service Quality History report opens. For an explanation of the report contents, see Understanding the Service Quality History Report, page 12-19.

Searching for Service Quality Events by Cisco 1040

To view the Service Quality events that correspond to specific Cisco 1040, use this procedure.

Step 1 Select **Reports > Service Quality History > Event History > Cisco 1040**. The Service Quality History: Search by Cisco 1040 page appears.

Step 2 Set your search criteria:

a. Select an operator (Is exactly, Begins with, Contains) and enter a Cisco 1040 ID or portion of a Cisco 1040 ID.

Note Cisco 1040 IDs include a letter and a 3-digit number.

b. Select the date range:

- Today.
- One Month (from *date* to *date*).
- From*: date* and to: *date*—Select dates (or enter dates using this format: dd-Mmm-yyyy, for example, 04-Mar-2006.)

Step 3 Click **View**. If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Service Quality History report opens. For an explanation of the report contents, see Understanding the Service Quality History Report, page 12-19.

Searching for Service Quality Events by Date

To view the Service Quality events for specific dates, use this procedure.

Step 1 Select **Reports > Service Quality History > Event History > Date**. The Service Quality History: Search by Date page appears.

Step 2 Select one and enter dates if required:

- Today.
- 7 days
- 1 month.
- From*: a date* and to: *a date*—Enter dates.

Step 3 Click **View**. If more than 1,000 records match your search criteria, a popup window reports the total number of records found.

The Service Quality History report opens. For an explanation of the report contents, see Understanding the Service Quality History Report, page 12-19.

For more information, see the following topics:

- History Report Tool Buttons, page 12-2
- Customizing Events, page 15-23
- Events Processed, page E-1

Understanding the Service Quality History Report

Note Service Quality History is useful only if you have purchased a license for Service Monitor. For more information, see *User Guide for Cisco Unified Service Monitor.*

The Service Quality History report is a scrollable table that lists up to 1,000 records, based on your search criteria. To view database contents beyond the 1,000 records, click the Export tool button in the upper-right corner of the window.

The Service Quality History report window provides tools, as shown in Table 12-1.

Table 12-4 describes the contents of the Service Quality History report.

Table 12-4 Service Quality History Report—Contents

Heading	Description
Severity	Event severity: • Warning—MOS is below the MOS threshold configured on Service Monitor. For more information, see *User Guide for Cisco Unified Service Monitor.* • Critical—MOS is below the MOS threshold configured on Operations Manager. For more information, see Configuring Service Quality Event Settings, page 20-7.
Event ID	Click this link to open the event properties window. See Viewing Service Quality Event Properties, page 12-20.
Destination Type	One of the following: • Endpoint • IP Phone
Destination	IP address or phone extension.
IP Address	Destination IP address.
MOS	Mean Opinion Score that triggered the event.
Cause	One of the following: • Jitter • Latency
Time	Date and time that the event occurred.

Table 12-4 Service Quality History Report—Contents (continued)

Heading	Description
Codec	One of the following: • G711Alaw64k • G711Alaw56k • G711Ulaw64k • G711Ulaw56k • G722 64k • G722 56k • G722 48k • G728 • G729 • G729AnnexA • G729AnnexB • G729AnnexAwAnnexB
Source Type	One of the following: • Endpoint • IP Phone
Source	IP address or phone extension.
IP Address	Source IP address.

Viewing Service Quality Event Properties

Step 1 Click an event ID link on the Service Quality History report to view properties of the event. See Understanding the Service Quality History Report, page 12-19.

Table 12-5 describes the contents of the service quality Event Properties window.

Table 12-5 Service Quality Event Properties Window—Contents

Heading	Description
Destination	Extension number, or N/A if destination type is Endpoint
Destination IP Address	IP address for an endpoint or an IP phone
Destination Type	One of the following: • Endpoint • IP Phone • Media Server

Table 12-5 Service Quality Event Properties Window—Contents (continued)

Heading	Description
Destination Model	Phone model, or N/A if destination type is Endpoint
Switch for Destination	IP address, or N/A if destination type is Endpoint
Destination Port	Port type and slot; for example Gi1/0/23
Source	Extension number or IP address
Source IP Address	IP address, or N/A if destination type is Endpoint
Source Type	One of the following: • IP Phone • Endpoint
Source Model	Phone model, or N/A if source type is Endpoint
Switch for Source	IP address, or N/A if source type is Endpoint
Source Port	Port type and slot, or N/A if source type is Endpoint
Detection Algorithm	Algorithm used to calculate MOS. One of these: • ITU G.107 - 1040 Sensor based voice quality Indicates that MOS is calculated on a Cisco 1040 Sensor • CVTQ - Phone based voice quality Indicates that MOS is calculated on an IP phone or Cisco voice gateway using the Cisco Voice Transmission Quality algorithm
MOS	MOS value during event
Critical MOS Threshold	MOS threshold configured on Operations Manager (see Configuring Service Quality Event Settings, page 20-7)
Cause	One of the following: • Jitter • Latency • Packet Loss

Table 12-5 Service Quality Event Properties Window—Contents (continued)

Heading	Description
Codec	Codec in use on the destination; one of the following: • G711Alaw64k • G711Alaw56k • G711Ulaw64k • G711Ulaw56k • G722 64k • G722 56k • G722 48k • G728 • G729 • G729AnnexA • G729AnnexB • G729AnnexAwAnnexB
Jitter	Msec
Packet loss	Number of packets
Details for Events that Are Based on Data from a Sensor	
Sensor MAC	Sensor MAC—Sensor MAC address
Number of suppressed traps	The number of traps that Cisco Unified Service Monitor suppressed between the suppression start time and suppression end time **Note** For a given endpoint, Service Monitor sends a trap every *n* (a configurable number) minutes, and additional traps during that time are suppressed (not sent). For more information, see *User Guide for Cisco Unified Service Monitor.*
Suppression start time	Date and time that Service Monitor started to suppress traps for this endpoint
Suppression end time	Date and time that Service Monitor stopped suppressing traps for this endpoint
Details for Events that Are Based on Data from a Cluster	
CVTQ version	Version of CVTQ algorithm used to calculate MOS
Cluster ID	Cisco Unified Communications Manager cluster ID
Cumulative Concealment Ratio	Total number of concealment frames divided by the total number of speech frames received from the start of the voice stream
Interval Concealment Ratio	Ratio of concealment frames to speech frames in the preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max Incremental Concealment Ratio	Highest interval concealment ratio from start of the voice stream
Concealment Seconds	Number of seconds during which concealment events (lost frames) occurred since the start of the voice stream (includes severely concealed seconds)

Table 12-5 Service Quality Event Properties Window—Contents (continued)

Heading	Description
Severely Concealed Seconds	Total number of seconds with more than 5 percent concealment frames
Call duration	Hours, minutes, and seconds, formatted as *n*h *n*m *n*s. For example, a 123-second call would be displayed as 2m 3s.
MOS during last 8 secs	MOS value during the last 8 seconds of the call
Min MOS during call	Minimum MOS value during the call
Max MOS during call	Maximum MOS value during the call

CHAPTER 13

Generating IP Phone and Video Phone Reports

An IP phone has a physical relationship with a switch and a logical relationship with a Cisco Unified Communications Manager. Phone reports provide a combined view of both of these relationships, making it easy for you to track and resolve IP phone and video phone problems. Operations Manager collects phone inventory data as scheduled (see Working with IP Phone Discovery, page 16-38) and collects additional data every 5 minutes to determine whether phone status has changed. IP Phones and Applications reports provide detailed phone inventory and status information. If you have the required software license, you can also view similar reports for video phones.

This section includes the following topics:

Using IP Phones and Applications Reports

Note IP Phones and Applications reports do not include data for video phones. See Using Video Phones Reports, page 13-28.

IP Phones and Applications reports provide inventory and IP status change reports:

- Inventory reports—Provide detailed IP phone data, reflecting the current status of IP phones in your network. These reports enable you to search for a few phones, list a specific set of phones—such as phones connected to a switch, phones in SRST mode and phones that are CTI applications—or view all phones and lines:
  - **Search**—Use Search to view information for a few IP phones or a single IP phone; search enables you to find phones using all or part of an extension number, IP address, or MAC address. See Searching for IP Phones, page 13-3.
  - **Inventory Analysis**—Use the Inventory Analysis report to display IP phones that meet criteria that you specify; for example, IP phones that are registered to a particular Cisco Unified Communications Manager or IP phones that are not connected to particular switches. See Generating the Inventory Analysis Report, page 13-5 and Understanding IP Phone Inventory Reports, page 13-11.

- **All IP Phones/Lines**—Use the All IP Phones/Lines report to view data for all IP phones that Operations Manager is monitoring. See Generating the All IP Phones/Lines Report, page 13-8 and Understanding IP Phone Inventory Reports, page 13-11.
- **SRST IP Phones**—Use the SRST IP phones report to view data for IP phones that are configured for Survivable Remote Site Telephony (SRST) only. See Generating the SRST IP Phones Report, page 13-8 and Understanding IP Phone Inventory Reports, page 13-11.

  Note IP phones that are configured for SRST are also included in the All IP Phones/Lines report and can be included in the Inventory Analysis report.

- **SIP Phones**—Use the SIP Phones report to view data for all SIP phones that Operations Manager is monitoring. See Generating the SIP Phones Report, page 13-9 and Understanding IP Phone Inventory Reports, page 13-11.
- **IP Communicators**—Use the IP Communicators report to view data for IP Communicators. See Generating the IP Communicators Report, page 13-9 and Understanding IP Phone Inventory Reports, page 13-11.

  Note IP Communicators are also included in the All IP Phones/Lines and All CTI Applications reports, and can be included in the Inventory Analysis report.

- **All CTI Applications**—Use the All CTI Applications report to view data for CTI applications. See Generating the All CTI Applications Report, page 13-9.

When a web interface is accessible for an IP phone, you can open it from most IP phone reports by clicking the hyperlink for one of the following:

- Extension number
- MAC address
- IP address

For more information, see Opening an IP Phone Web Interface, page 13-18.

- IP Phone Status Changes reports—Provide data for IP phones that have undergone a status change during the previous 1 to 30 days:
  - **IP Phone Move**—Use the IP Phone Move report to view data for phones that have been connected to a different switch or switch port or that have registered to a different Cisco Unified Communications Manager. See Using the IP Phone Move Report, page 13-21.
  - **Duplicate MAC/IP Address**—See Using the Duplicate MAC/IP Address Report, page 13-26.
  - **Extension Number Change**—See Using the Extension Number Changes Report, page 13-24.
  - **Suspect Phone**—Use the Suspect Phone report to view data for phones that are not registered to a Cisco Unified Communications Manager or that have attempted to register and failed. See Using the Suspect Phone Report, page 13-25.
  - **Removed**—See Using the Removed IP Phones Report, page 13-23.

– **IP Phone Audit**—Use the IP Phone Audit report to obtain a summary of changes, including data for phones that have moved, been removed, undergone an extension number change, appeared in inventory with a duplicate MAC or IP address, or become suspect. See Using the IP Phone Audit Report, page 13-22.

For more information, see the following topics:

- Understanding the Time Period Covered by Phone Status Changes Reports, page 13-20
- Tracking Phone Status Changes when a Cisco Unified Communications Manager Is Down, page 13-21

Generating IP Phone Inventory Reports

This topic includes the following:

Searching for IP Phones

Use Search to find one or only a few IP phones in your network. Search displays information for one phone at a time; you can page back and forth to view information for each phone when multiple phones are found. You can search for phones using all or part of an extension number, IP address, or MAC address.

When you want to find many phones—for example, all phones registered with a Cisco Unified Communications Manager or all phones connected to a switch—use the Inventory Analysis report; see Generating the Inventory Analysis Report, page 13-5.

For information on how phone counts are displayed in Operations Manager windows, seeHow Are Phone Counts Displayed in Views and Reports?, page 1-19.

Step 1 Select **Reports > IP Phones and Applications > Search**. The Find IP Phones page appears.

Step 2 In the Find IP Phones Where pane:

a. Select one of the following:

- Extension number
- IP address
- MAC address

b. Then select one of the following:

- is exactly
- begins with
- contains
- ends with

c. Enter a value.

Step 3 Click **View**. The IP Phone Details dialog box appears, displaying the information described in the following table.

Table 13-1 IP Phone Details

Row	Description
Extension	Extension number of the IP phone; for example, 4000. Click the hyperlink to open the web interface on the IP phone (see Opening an IP Phone Web Interface, page 13-18).
IP Address	IP address of the IP phone; for example, 10.76.38.65. Click the hyperlink to see more details of the IP phone (see Using IP Phones and Applications Reports, page 13-1).
MAC Address	MAC address of the IP phone; for example, 003094c40454, or 00-30-94-c4-04-54. Click the hyperlink to open the web interface on the IP phone (see Using IP Phones and Applications Reports, page 13-1).
CCM Address	Address of the Cisco Unified Communications Manager (CCM) with which the IP phone is registered; for example, 10.76.38.70.
Switch Address	IP address of the switch to which the IP phone is connected; for example, 10.76.29.162.
Switch Name	Switch to which the IP phone is connected.
Switch Port	Switch port to which the IP phone is connected; for example, Fa0/12.
Port Status	Status of the switch port to which the IP phone is connected: up or down.
IP Phone Status	Cisco Unified Communications Manager registration status of the IP phone: • yes—The IP phone is registered with a Cisco Unified Communications Manager. • no—The IP phone is not registered with a Cisco Unified Communications Manager.
IP Phone Model	Cisco IP phone model number; for example, 7902, 7905, 7910, 7912, 7920, 7935, 7940, 7960, or 7970.
Protocol	Protocol the phone is using to communicate with Cisco Unified Communications Manager. **Note** Only SCCP and SIP phones will be discovered. H.323 and MGCP protocols are not currently supported.
VLAN Name	Name of the VLAN in the switch (a user-defined name); for example, voice.
VLAN ID	ID of the VLAN in the switch to which the IP phone is connected; for example, 100.
SRST Router	IP address of the router that the phone is using for SRST.

Table 13-1 IP Phone Details (continued)

Row	Description
SRST Mode	Can be one of the following: • yes—The phone is in SRST mode • no—The phone is not in SRST mode • ?—The phone is suspected to be in SRST mode • –(dash)—The phone is not an SRST phone
Serial No.	IP phone serial number **Note** This information is obtained by phone polling. See Understanding Phone Polling, page 13-28.
Application ID	Identifier of the firmware running on the phone **Note** This information is obtained by phone polling. See Understanding Phone Polling, page 13-28.
Load ID	Identifier of the factory-installed load running on the phone **Note** This information is obtained by phone polling. See Understanding Phone Polling, page 13-28.

Step 4 To display the information in print-friendly format in a new browser window, click **Print**; print the information, using the browser print function.

Step 5 If search results include more than one phone, view them by clicking **Next** or **Prev**.

For more information, see the following topics:

- Launching Tests for Selected IP Phones, page 13-18
- Opening an IP Phone Web Interface, page 13-18
- Obtaining Usernames from LDAP for IP Phone Reports, page 13-18
- Troubleshooting Tips for IP Phones and Applications Reports and Video Phones Reports, page 13-19

Generating the Inventory Analysis Report

Use Inventory Analysis to search for IP phones in your network and display them in a report.

Before You Begin

Inventory Analysis searches for phones using:

- An implicit “or” within each field—If you enter more than one value in a field, Inventory Analysis searches for phones that match any value that you entered.
- An implicit “and” for all fields—If you enter values in more than one field, Inventory Analysis searches for phones that match at least one value from each field.

For example, if you enter two phone models, such as 7910 and 7935, in the IP Phone Model field, the Inventory Analysis report that results includes all phones of these models. If, in addition, you enter a VLAN ID and a switch, Inventory Analysis searches for phones that meet all these criteria; the report that results includes only phones of the models specified that are connected to the switch and in the VLAN that you selected.

Step 1 Select **Reports > IP Phones and Applications > Inventory Analysis**. The Find IP Phones page appears.

Step 2 Enter values in one or more fields, described in the following table.

GUI Element	Description/Action
Find IP Phones Where list boxes and field	From left to right: • Select one of the following: – Extension number – IP Address – MAC Address • Select one of the following: – is exactly – begins with – contains – ends with • Enter a value.
VLAN Name field	Enter the name of the VLAN.
VLAN ID field	Enter the VLAN ID.
IP Phone Status radio buttons	Select one: • Registered • Unregistered • All—Registered and unregistered phones.
SRST radio buttons	Select one: • SRST—Configured to fail over to an SRST router in case of a WAN link failure. • Non-SRST—Not configured for SRST. • All—SRST and non-SRST.
Protocol radio buttons	Select one: • SCCP—Phones using Skinny Client Control Protocol. • SIP—Phones using Session Initiation Protocol. • All—SCCP and SIP.

GUI Element	Description/Action
IP Phone Type field	Enter a comma-separated list of phone models. Edit the entries in the field directly or select from a list of phone types, as follows: 1. Click  . The Select IP Phone Types list appears. 2. Select the desired IP phone types from the list. (Use the Control key or the Shift key to select more than one IP phone type from the list.) 3. Click **OK**.
CCM/CCM Cluster/ CME pane	• Exclude check box—Deselected by default. Select to exclude phones that belong to any Cisco Unified Communications Manager, Cisco Unified Communications Manager cluster, and Cisco Unified Communications Manager Express in the list box. • List box—Enter a comma-separated list of Cisco Unified Communications Managers, Cisco Unified Communications Manager clusters, and instances of Cisco Unified Communications Manager Express, or select them as follows: 1. Click  . The Select CCM/CCM Cluster/CME dialog box appears. 2. In the CCM/CCM Cluster/CME Selector, expand groups and select one or more of the following: Cisco Unified Communications Manager, Cisco Unified Communications Manager Cluster, and Cisco Unified Communications Manager Express. 3. Click **OK**. The dialog box closes and the Find IP Phones screen displays your selections in the CCM/CCM Cluster/CME list box.
Switch pane	• Exclude check box—Deselected by default. Select to exclude phones that are connected to any switch in the list box. • List box—Enter a comma-separated list of switches, or select them as follows: 1. Click  . The Inventory Analysis Switch Selection dialog box appears. 2. In the Switch Selector, expand groups and select switches. 3. Click **OK**. The dialog box closes and the Find IP Phones screen displays your selection in the Switch list box.
SRST Router pane	• Exclude check box—Deselected by default. Select to exclude phones that use any SRST router in the list box. • List box—Enter a comma-separated list of routers, or select them as follows: 1. Click  . The Inventory Analysis Router Selection dialog box appears. 2. In the Router Selector, expand groups and select routers. 3. Click **OK**. The dialog box closes and the Find IP Phones screen displays your selection in the Router list box.

Step 3 Click **View**. The Inventory Analysis Report appears in another window. See Understanding IP Phone Inventory Reports, page 13-11.

You might not be able to see the list of Cisco Unified Communications Manager or switches in the popup window that appears when you click  . This occurs when the PIFServer process is down. Do the following:

- Check the status of PIFServer by using the command **pdshow PIFServer** from the command line.
- If PIFServer is down, use the Common Services start function. To do this:
  1. From the Operations Manager home page, click **CiscoWorks** in the upper right-hand corner of the window. The CiscoWorks home page opens.
  2. Under Common Services, select **Server > Admin > Processes**. The Process Management page appears, displaying process names in a table.
  3. Locate the PIFServer process in the table, select the check box for it, and click **Start**.

Note Alternatively, you can bring PIFServer up using the command **pdexec PIFServer** from the command line. Use this approach if, for example, the web server is down.

Generating the All IP Phones/Lines Report

Step 1 Select **Reports > IP Phones and Applications > All IP Phones/Lines**. The All IP Phones/Lines window appears.

Step 2 Select **IP Phones** from the list, and click **View**. The All IP Phones/Lines report appears, displaying the information described in Understanding IP Phone Inventory Reports, page 13-11.

Note You can also generate the All IP Phones/Lines from the Monitoring Dashboard tab by selecting **Click to View All Phones** in the IP Phone Status pane.

Generating the SRST IP Phones Report

The SRST IP Phones report shows a list of phones that are configured for Survivable Remote Site Telephony (SRST).

Step 1 Select **Reports > IP Phones and Applications > SRST IP Phones**. The SRST IP Phones report appears in a new window, displaying information for the SRST configuration only. For more information, see Understanding IP Phone Inventory Reports, page 13-11.

Generating the SIP Phones Report

The SIP Phones report shows a list of SIP phones.

Step 1 Select **Reports > IP Phones and Applications > SIP Phones**. The SIP Phones report appears in a new window, displaying information for SIP phones only. For more information, see Understanding IP Phone Inventory Reports, page 13-11.

Generating the IP Communicators Report

Note IP Communicators are also included in the All IP Phones/Lines and the All CTI Applications reports and they can be included in the Inventory Analysis report.

Step 1 Select **Reports > IP Phones and Applications > IP Communicators**. The IP Communicators report appears in a new window, displaying information for IP Communicators only. For more information, see Understanding IP Phone Inventory Reports, page 13-11.

Generating the All CTI Applications Report

The All CTI Applications report lists Computer Telephony Interface (CTI) device applications registered with the Cisco Unified Communications Manager that Operations Manager monitors. The following applications are registered to the Cisco Unified Communications Manager as CTI devices or CTI ports:

- Cisco IP Communicators
- Cisco Personal Assistant
- Cisco Customer Response Applications
- Cisco IP Contact Center
- Cisco Emergency Responder

Step 1 Select **Reports > IP Phones and Applications > All CTI Applications**. The All CTI Applications Report appears, displaying the information described in the following table.

Table 13-2 All CTI Applications Report

Column	Description
Extension	Extension of the CTI Application (CTI Port/CTI Route Point).
Application Information	The defined name of the CTI application, as reported by the Cisco Unified Communications Manager. If the application is not registered in CTI, this field displays Not supported.
Registered	Whether or not the CTI Application is registered with the Cisco Unified Communications Manager: Yes or No.
IP Address	• IP address of the CTI application (in case the application is a CTI port) • IP address of the Cisco Unified Communications Manager (in case the application is a CTI Route Point)
CCM Address	Cisco Unified Communications Manager address.
Device Type	Type of the device.
Device Description	Description of the device.

Generating the All ATA Devices Report

The All ATA Devices report lists all Advanced Technology Attachment (ATA) devices registered with the Cisco Unified Communications Manager that Operations Manager monitors.

Step 1 Select **Reports > IP Phones and Applications > All ATA Devices**. The All ATA Devices report appears in a new window, displaying information for all ATA devices only.For more information, see Generating IP Phone Inventory Reports, page 13-3.

Table 13-3 All ATA Devices Report

Columns and Buttons	Description/Action
Device Name	Name of the ATA device
Device Type	ATA device type
CCM Name	Name of the Cisco Unified Communications Manager

Generating the Cisco 1040 Sensors Report

The Cisco 1040 Sensors report lists all Cisco 1040 Sensors connected to the switches that Operations Manager monitors.

Step 1 Select **Reports > IP Phones and Applications > Cisco 1040 Sensors**. The Cisco 1040 Sensors report appears in a new window, displaying information for Cisco 1040 Sensors only.For more information, see Generating IP Phone Inventory Reports, page 13-3.

Table 13-4 Cisco 1040 Sensors Report

Columns and Buttons	Description/Action
Device ID	Device ID of the 1040 Sensor.
IP Address	IP address of the 1040 Sensor.
Switch Name	Name of the switch to which the 1040 Sensor is connected.
Switch Address	IP address of the switch to which 1040 Sensor is connected.
Switch Port	Switch port to which 1040 Sensor is connected.

Understanding the Associated Phone and Phone Detail Reports

You can launch these reports from the Service Level View, the Alert Details page, or the Detailed Device View. Depending on the device that you have selected, the report will list one of the following:

- Phones that are connected to the switch.
- Phones that are registered to Cisco Unified Communications Manager or Cisco Unified Communications Manager Express.

The report contains the data listed in Table 13-5. For information on how phone counts are displayed in Device Management Summary window, see How Are Phone Counts Displayed in Views and Reports?, page 1-19.

Understanding IP Phone Inventory Reports

Table 13-5 describes the data displayed in the following reports:

- Inventory Analysis—Includes phones that match criteria that you specify.
- All IP Phones/Lines—Includes all IP phones, including IP Communicators and IP phones that are configured for SRST.

Note You can filter the All IP Phones/Lines report to include only the phones that you want to see.

- SRST IP Phones—Includes only phones that are configured for SRST.
- SIP Phones—Includes only phones that use Session Initiation Protocol (SIP).
- IP Communicators—Includes IP Communicators only.
- Associated Phones and Phone Details—Includes only phones associated with a selected device; for example, phones connected to a switch or phones registered to Cisco Unified Communications Manager (or Cisco Unified Communications Manager Express).

By default, these reports display only these columns: Extension, User, IP Address, MAC Address, Model, Regd, CCM, Switch Address, and Port. You can hide these columns and select among additional columns to display. See Selecting Columns to Display and to Hide on a Phone Inventory Report, page 13-17.

Table 13-5 describes all possible columns of data that can appear on these reports. For information on how phone counts are displayed in Operations Manager windows, see How Are Phone Counts Displayed in Views and Reports?, page 1-19.

Table 13-5 IP Phone Reports

Columns and Buttons	Description/Action
Number	The row number; starting from 1.
Check box	Select any phones that you would like to: • Print—Include selected phones in a new window in print-friendly format. (See Phones Report Tool Buttons, page 13-13.) • Export to a file—Include selected phones in a PDF or CSV file. (See Phones Report Tool Buttons, page 13-13.) • Launch a test on—Include selected phones in tests that you create from the Launch button when it is present at the bottom of the report. (See Launching Tests for Selected IP Phones, page 13-18.)
Extn.	Extension number of the IP phone; for example, 4000. Click the hyperlink to see more details of the IP phone (see Opening an IP Phone Web Interface, page 13-18).
User	Username obtained using LDAP if you have configured an LDAP server in Operations Manager. See Configuring LDAP, page 16-41 and Obtaining Usernames from LDAP for IP Phone Reports, page 13-18.
IP Address	IP address of the IP phone; for example, 10.76.38.65. Click the hyperlink to see more details of the IP phone (see Opening an IP Phone Web Interface, page 13-18).
MAC Address	MAC address of the IP phone; for example, 003094c40454, or 00-30-94-c4-04-54. Click the hyperlink to see more details of the IP phone (see Opening an IP Phone Web Interface, page 13-18).
Model	Model number of the IP phone; for example, 7902, 7905, 7910, 7912, 7920, 7935, 7940, 7960, or 7970.
Protocol	Protocol the phone is using to communicate with Cisco Unified Communications Manager or Cisco Unified Communications Manager Express. **Note** Only SCCP and SIP phones will be discovered. H.323 and MGCP protocols are not currently supported.
Regd.	Registration status of the IP phone with respect to Cisco Unified Communications Manager or Cisco Unified Communications Manager Express. Displays **yes** if the IP phone is registered or **no** if the IP phone is not registered.
CCM	One of the following: • CCM—Cisco Unified Communications Manager • CCE—Cisco Unified Communications Manager Express
CCM/CME Name	DNS name of the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express with which the IP phone is registered.
CCM/CME Address	IP address of the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express with which the IP phone is registered.
Switch Name	Name of the switch to which the IP phone is connected.

Table 13-5 IP Phone Reports (continued)

Columns and Buttons	Description/Action
Switch Address	IP address of the switch to which the IP phone is connected.
Port	Switch port used by the IP phone; for example, Fa0/12.
Port Status	Status of the port used by the IP phone: up or down.
VLAN Name	Name of the VLAN (user-defined name); for example, voice.
VLAN ID	ID of the VLAN for the IP phone; for example, 100.
SRST Mode	One of the following: • yes—The phone is in SRST mode • no—The phone is not in SRST mode • ?—The phone is suspected to be in SRST mode • —(dash)—The phone is not an SRST phone
SRST Router	One of the following: • IP address of the router that the phone is using for SRST • —(dash)
Serial No.	IP phone serial number **Note** This information is obtained by phone polling. See Understanding Phone Polling, page 13-28.
Application ID	Identifier of the firmware running on the phone **Note** This information is obtained by phone polling. See Understanding Phone Polling, page 13-28.
Load ID	Identifier of the factory-installed load running on the phone **Note** This information is obtained by phone polling. See Understanding Phone Polling, page 13-28.
Launch button	Click and select a menu item to configure tests for the IP phones selected on this report.

For more information, see the following topic:

- Troubleshooting Tips for IP Phones and Applications Reports and Video Phones Reports, page 13-19

Phones Report Tool Buttons

The following report tool buttons might appear in the upper-right corner of IP Phones and Applications or Video Phone reports.

Table 13-6 Phone Report Tool Buttons

	Opens a filter dialog box for refining the report. See Filtering IP Phones and Applications Reports, page 13-14.
	Exports the current report to a PDF or CSV file to save on your local system. **Note** Enables you to export data for all phones, selected phones, or a range of record numbers.
	Opens a new window with the report formatted for printing from your browser.
	Opens a column selector dialog box from which you can select those columns of a report to hide and those to display. See Selecting Columns to Display and to Hide on a Phone Inventory Report, page 13-17.
	Opens context-sensitive help.

Filtering IP Phones and Applications Reports

From an IP Phones and Applications report, click the Filter button  when present. A filter dialog box opens.

Note Filtering is performed using:

- An implicit “or” within each field—If you enter more than one value in a field, phones that match any value are included in the report.
- An implicit “and” for all fields—If you enter values in more than one field, phones that match at least one value from each field are included in the report after filtering.

For example, if you enter two phone models, such as 7910 and 7935, in the IP Phone Model field, the report that results includes all phones of these models. If, in addition, you enter a VLAN ID and a switch, the report is filtered to include only phones of the models specified that are connected to the switch and in the VLAN that you selected.

Step 1 Enter values in one or more fields, described in the following table.

GUI Element	Description/Action
Find IP Phones where list boxes and field	From left to right: • Select one of the following: – Extension number – IP Address – MAC Address • Select one of the following: – is exactly – begins with – contains – ends with • Enter a value.
VLAN Name field	Enter the name of the VLAN.
VLAN ID field	Enter the VLAN ID.
IP Phone Status radio buttons	Select one: • Registered • Unregistered • All—Registered and unregistered phones.
SRST radio buttons	Select one: • SRST—Configured to fail over to an SRST router in case of a WAN link failure. • Non-SRST—Not configured for SRST. • All—SRST and non-SRST.
IP Phone Type field	Enter a comma-separated list of phone models. By default, all supported phone models are included in this field, including IP Communicator. Edit the entries in the field directly or select from a list of phone models, as follows: 1. Click  . The Select IP Phone Types list appears. 2. Select the desired IP phone types from the list. (Use the Control key or the Shift key to select more than one IP phone type from the list.) 3. Click **OK**.

GUI Element	Description/Action
CCM/CME pane	• Exclude check box—Deselected by default. Select to exclude phones that belong to any Cisco Unified Communications Manager, Cisco Unified Communications Manager cluster, and Cisco Unified Communications Manager Express in the list box. • List box—Enter a comma-separated list of Cisco Unified Communications Managers, Cisco Unified Communications Manager clusters, and instances of Cisco Unified Communications Manager Express, or select them as follows: 1. Click  . The Select CCM/CCM Cluster/CME dialog box appears. 2. In the CCM/CCM Cluster/CME Selector, expand groups and select one or more instances of the following: Cisco Unified Communications Manager, Cisco Unified Communications Manager cluster, and Cisco Unified Communications Manager Express. 3. Click **OK**. The dialog box closes and the Find IP Phones screen displays your selections in the CCM/CCM Cluster/CME list box.
Switch pane	• Exclude check box—Deselected by default. Select to exclude phones that are connected to any switch in the list box. • List box—Enter a comma-separated list of switches, or select them as follows: 1. Click  . The Inventory Analysis Switch Selection dialog box appears. 2. In the Switch Selector, expand groups and select switches. 3. Click **OK**. The dialog box closes and the Find IP Phones screen displays your selection in the Switch list box.
SRST Router pane	• Exclude check box—Deselected by default. Select to exclude phones that use any SRST router in the list box. • List box—Enter a comma-separated list of switches, or select them as follows: 1. Click  . The Inventory Analysis Router Selection dialog box appears. 2. In the Router Selector, expand groups and select routers. 3. Click **OK**. The dialog box closes and the Find IP Phones screen displays your selection in the Router list box.

Step 2 Click **OK**. The filter dialog box closes and the IP phone report refreshes. For more information, see Understanding IP Phone Inventory Reports, page 13-11.

You might not be able to see the list of Cisco Unified Communications Manager or switches in the popup window that appears when you click  . This occurs when the PIFServer process is down. Do the following:

- Check the status of PIFServer by using the command **pdshow PIFServer** from the command line.

- If PIFServer is down, use the Common Services start function. To do this:
  1. From the Operations Manager home page, click **CiscoWorks** in the upper right-hand corner of the window. The CiscoWorks home page opens.
  2. Under Common Services, select **Server > Admin > Processes**. The Process Management page appears, displaying process names in a table.
  3. Locate the PIFserver process in the table, select the check box for it, and click **Start**.

Note Alternatively, you can bring PIFServer up using the command **pdexec PIFServer** from the command line. Use this approach if, for example, the web server is down.

Selecting Columns to Display and to Hide on a Phone Inventory Report

By default, phone reports display these columns of data:

- Extension
- User
- IP Address
- MAC Address
- Model
- Regd
- CCM
- Switch Address
- Port

For definitions, see Understanding IP Phone Inventory Reports, page 13-11. Use this procedure to hide any of the default columns and select among additional columns of data to display.

Step 1 In the upper-right corner of a phone report, click the Tools button  . A column selector dialog box appears.

Step 2 To hide a column, place it on the Hidden Column(s) list:

a. Select the column by name from the Displayed Column(s) list.

b. Click the **< Remove <<** button. The column name appears on the Hidden Column(s) list.

Note To select adjacent columns, hold down the Shift key. To select columns that are not adjacent, hold down the Ctrl key.

Step 3 To display a column, place it on the Displayed Column(s) list:

a. Select the column by name from the Hidden Column(s) list.

b. Click the **< Add <<** button. The column name appears on the Displayed Column(s) list.

Step 4 Click **Update**. The report window refreshes, displaying only columns from the Displayed Column(s) list.

Note Your selections do not affect other users and will remain in effect for this report until you log out of Operations Manager or until you change your selections.

Opening an IP Phone Web Interface

You can open an IP phone web interface from an IP Phones and Applications report or a Video Phones report by clicking one of these hyperlinks when available:

- Extension number
- IP address
- MAC address

Another window opens with information directly from the phone, including network configuration details, device, port, and Ethernet information for the specified IP phone.

Obtaining Usernames from LDAP for IP Phone Reports

Operations Manager can supply usernames on IP phone and video phone reports from a corporate LDAP server when the LDAP server is:

- Configured with information for all users.
- Not a secure LDAP server (does not use SSL authentication).
- Added to Operations Manager with the correct credentials and appropriate telephone number. The telephone number can be a phone number or a phone MAC address, depending on the LDAP configuration.

Usernames are updated in Operations Manager when IP phone discovery runs. IP phone discovery obtains users in the corporate directory that have the telephoneNumber attribute, and correlates data for them with information in Cisco Unified Communications Manager.

For more information, see the following topics:

- Understanding IP Phone Inventory Reports, page 13-11
- Working with IP Phone Discovery, page 16-38
- Configuring LDAP, page 16-41

Launching Tests for Selected IP Phones

When the Launch button is present at the bottom right-hand corner of an IP Phones and Applications report or Video Phones report, you can select phones from the report, and configure tests on them using one of the available options:

- SRST Test—Select one or more phones. See Configuring a Single SRST Test as Needed, page 18-9.
- Phone Test—Select one or more phones. See Creating and Running a Phone Test on Demand, page 10-14.
- Synthetic Test—Select one phone only. See Creating Synthetic Tests, page 9-6.
- Phone Status Tests—Select one or more phones. See Adding a Phone Status Test—Using the Create Phone Status Test Page, page 8-4.

Troubleshooting Tips for IP Phones and Applications Reports and Video Phones Reports

This section includes the following tips:

N/A or Not Available Appears in IP Phones and Applications Reports and Video Phone Reports

If N/A or Not Available appears instead of data in a field, it means one of the following:

- The switch or the Cisco Unified Communications Manager is not monitored by Operations Manager. To correct this condition, add the switch or Cisco Unified Communications Manager to Operations Manager.
- Operations Manager cannot get the information from the switch or the Cisco Unified Communications Manager. To correct this condition, check the status of the switch or Cisco Unified Communications Manager in the Alerts and Events display. If the switch or Cisco Unified Communications Manager is unreachable, ensure that the connectivity is restored.
- For IP Phones and Applications reports, if the phone is a Cisco Wireless IP Phone 7920, only logical information from Cisco Unified Communications Manager is displayed. Switch information is not available.

Cisco Wireless IP Phone 7920 Not Displayed in IP Phones and Applications Reports

For the Cisco Wireless IP Phone 7920 to be monitored in Operations Manager, its Aironet access point must also be monitored by Operations Manager. Only logical information from the Cisco Unified Communications Manager is displayed for this phone; switch information for the 7920 appears as N/A or Not Available.

In Cisco Unified Communications Manager releases prior to 4.0, the 7920 appears as a 7960. Therefore, Operations Manager also displays the 7920 as a 7960 for Cisco Unified Communications Manager releases prior to 4.0.

Note IP Phone Status Changes reports, such as IP Phone Audit and Suspect Phone reports, are not supported for the Cisco Wireless IP Phone 7920.

Phones Missing from IP Phones and Applications Reports

If a report does not contain information about an IP phone, the phone might be one of the following:

- A synthetic phone—IP phones configured for synthetic tests (*synthetic phones*) do not appear in IP Phones and Applications reports.
- An IP Communicator—Generate the IP Communicator Report. See Generating the IP Communicators Report, page 13-9.
- A CTI application—These phones appear on the All CTI Applications report. See Generating the All CTI Applications Report, page 13-9.

Using IP Phone Status Changes Reports

IP Phone Status Changes reports supply information for phones that have undergone a status change during the previous 1 to 30 days.

The IP Phone Audit report provides a summary of all of these changes (see Using the IP Phone Audit Report, page 13-22). Additional IP Phone Status Changes reports focus on particular types of changes, as shown in the following table.

Phone Status Change	Details in this Report...
Connection—Connected to a different switch or switch port	Using the IP Phone Move Report, page 13-21
Duplicate IP address or MAC address	Using the Duplicate MAC/IP Address Report, page 13-26
Extension number change	Using the Extension Number Changes Report, page 13-24
Registration with Cisco Unified Communications Manager: • Registered to a different Cisco Unified Communications Manager • Not registered • Attempted to register and failed	Using the IP Phone Move Report, page 13-21 Using the Suspect Phone Report, page 13-25
Removed	Using the Removed IP Phones Report, page 13-23

Understanding the Time Period Covered by Phone Status Changes Reports

When you generate an IP Phone Status Changes or Video Phone Status Changes report, your results can be affected by the time zones in which each of following resides:

- Your client system—Operations Manager calculates the time period (previous 24 hours through previous 7 to 30 days, depending on the report) for Phone Status Changes reports based on the date and time on your client system.
- Operations Manager system—Operations Manager records some audits, such as extension number changes, based on the time that the change is detected on the Operations Manager system.
- Cisco Unified Communications Manager—Operations Manager records some audits, such as phone moves, based on the time on Cisco Unified Communications Manager that changes were detected.

If any of these systems is not in the same time zone as your system, you must take the time zone difference into account when you generate and view Phone Status Changes reports.

Tip If the audit date and time on the Operations Manager system is inconsistent with those shown in the IP Phone Status Changes or Video Phone Status Changes report, make sure that all Cisco Unified Communications Managers in the network are set to synchronize.

Tracking Phone Status Changes when a Cisco Unified Communications Manager Is Down

If a Cisco Unified Communications Manager that is configured with a backup goes down, IP phones and video phones fail over to the backup Cisco Unified Communications Manager. Operations Manager stores audit records for the phones that register with the backup and these status changes are included in IP Phone Status Changes and Video Phone Status Changes reports.

Operations Manager does not store audit records in the following cases:

- An entire Cisco Unified Communications Manager cluster goes down.
- A Cisco Unified Communications Manager for which a backup is not configured goes down.

Therefore, status changes for the phones registered to Cisco Unified Communications Managers in these situations are not included in IP Phone Status Changes and Video Phone Status Changes reports.

Note During the time that Cisco Unified Communications Manager is down, affected phones are:

- Listed on the Phone Activities Monitoring Dashboard where they remain for a minimum of 24 hours. See Getting Phone Alert Details, page 5-4.
- Summarized in the Service Impact report, which provides details for phones that lose registration and do not fail over. The Service Impact report is available from Alert Details for the Cisco Unified Communications Manager while it is down and while the impact of this event remains high; see Understanding the Service Impact Report, page 3-16.

Using the IP Phone Move Report

The IP Phone Move report displays IP phones that have moved, including details about the phone before and after the move. The IP Phone Move report shows the time at which the IP phone move was detected, and not the time at which the move occurred.

Information for the IP Phone Move report is gathered every 5 minutes by IP Phone Movement Tracking (see Understanding IP Phone Movement Tracking, page 13-28). IP Phone Movement Tracking checks all the switches and Cisco Unified Communications Managers, identifies the list of changes, and generates the data on IP phone moves.

Note You obtain fresh data for the IP Phone Move report about once every 5 minutes. Close the report and regenerate it to refresh the data.

Step 1 Select **Reports > IP Phones and Applications > IP Phones and Applications > IP Phone Status Changes > IP Phone Move**. The IP Phone Status Reports page appears.

Step 2 Select the time period (24 hours - 30 days) from the list and click **View**. The IP Phone Move report appears, displaying the information described in the following table.

Column	Description
Extension	Extension number of the IP phone. The Extension column has two subcolumns—Old and New: • **Old**—Extension number of the IP phone before it was moved. • **New**—Extension number of the IP phone after it was moved.
IP Address	IP address of the IP phone.
MAC Address	MAC address of the IP phone.
CCM Address	Cisco Unified Communications Manager address. The CCM Address column has two subcolumns: • **Old**—CCM address of the IP phone before it was moved. • **New**—CCM address of the IP phone after it was moved.
Switch Address	IP address of the switch to which the IP phone is connected. The Switch Address column has two subcolumns: • **Old**—Switch address used by the IP phone before it was moved. • **New**—Switch address used by the IP phone after it was moved.
Switch Port	Switch port used by the IP phone. The Switch Port column has two subcolumns: • **Old—**Switch port used by the IP phone before it was moved. • **New**—Switch port used by the IP phone after it was moved.
Time Stamp	Reflects the date and time that Operations Manager detected the IP phone move.

Tip Phones that have moved and do not run Cisco Discovery Protocol (CDP) do not appear in this report. For example, 30VIP and 12SP+ do not run CDP; you will not see move entries for them.

Using the IP Phone Audit Report

The IP Phone Audit report shows the changes that have occurred in the managed IP phone network. For example, this report shows you the IP phones that have been added to or deleted from your network, or changes in IP phone status. Phone status changes occur, for instance, when a phone becomes unregistered with the Cisco Unified Communications Manager.

You can see what has changed within the last 30 days. Audits are maintained in the database for a period of 30 days, after which they are purged.

Information for the IP Phone Audit report is gathered by IP Phone Movement Tracking (see Understanding IP Phone Movement Tracking, page 13-28). IP Phone Movement Tracking runs every 5 minutes, so you can run the IP Phone Audit report and obtain fresh data about once every 5 minutes. This interval is not configurable.

Step 1 Select **Reports > IP Phones and Applications > IP Phone Status Changes > IP Phone Audit**. The IP Phone Status Reports page appears.

Step 2 Select the time period (24 hours - 30 days) from the list and click **View**. The IP Phone Audit report appears, displaying the information described in the following table.

Column	Description
Extension	Extension number of the IP phone.
IP Address	IP address of the IP phone.
MAC Address	MAC address of the IP phone.
CCM/CME Address	Cisco Unified Communications Manager or Cisco Unified Communications Manager Express address.
Switch Address	IP address of the switch to which the IP phone is connected.
Switch Port	Switch port used by the IP phone.
Time	Time of audit on the Cisco Unified Communications Manager. **Note** Audit date and time are taken directly from Cisco Unified Communications Manager without adjustment for time zone differences, if any exist, between Cisco Unified Communications Manager and Operations Manager systems.
Audit Type	One of the following: • add—Phone added to the network. • remove—Phone removed from the network. • unregistered—From Cisco Unified Communications Manager. • registered—With Cisco Unified Communications Manager.

Note The IP Phone Audit report is not supported for Cisco Wireless IP Phone 7920.

Using the Removed IP Phones Report

The Removed IP Phones report lists phones that have been removed during the previous 1 to 30 days. Operations Manager gathers the information used in this report every 5 minutes (see Understanding IP Phone Movement Tracking, page 13-28.) Therefore, you can run this report and obtain fresh data about once every 5 minutes.

Step 1 Select **Reports > IP Phones and Applications > IP Phone Status Changes > Removed IP Phones**. The IP Phone Status Reports page appears.

Step 2 Select the time period (24 hours - 30 days) from the list and click **View**. The Removed IP Phones report appears in a new window, displaying the information described in the following table.

Column	Description
Extension	Extension number of the IP phone.
IP Address	IP address of the IP phone.
MAC Address	MAC address of the IP phone.
CCM/CME Address	Cisco Unified Communications Manager or Cisco Unified Communications Manager Express address.
Switch Address	IP address of the switch to which the IP phone was previously connected.
Switch Port	Switch port to which the IP phone was previously connected.
Time	Time that the phone was removed from Cisco Unified Communications Manager. **Note** Removal date and time are taken directly from Cisco Unified Communications Manager without adjustment for time zone differences, if any exist, between Cisco Unified Communications Manager and Operations Manager systems.
Indication	Indicates the Cisco Unified Communications Manager registration status of the IP phone: removed.

Note The Removed IP Phone report is not supported for Cisco Wireless IP Phone 7920.

Using the Extension Number Changes Report

The Extension Number Changes report lists phones that have changed extension numbers during the previous 1 to 30 days. Operations Manager gathers the information used in this report every 5 minutes (see Understanding IP Phone Movement Tracking, page 13-28.) Therefore, you can run this report and obtain fresh data about once every 5 minutes.

Step 1 Select **Reports > IP Phones and Applications > IP Phone Status Changes > Extension Number Changes**. The IP Phone Status Reports page appears.

Step 2 Select the time period (24 hours - 30 days) from the list and click **View**. The Extension Number Changes report appears in a new window, displaying the information described in the following table.

Column	Description
Extension	Extension number of the IP phone.
IP Address	IP address of the IP phone.
MAC Address	MAC address of the IP phone.
CCM Address	Cisco Unified Communications Manager address.
Switch Address	IP address of the switch to which the IP phone was previously connected.
Switch Port	Switch port to which the IP phone was previously connected.
Time	Time that Operations Manager determined that the extension number changed.

Note The Extension Number Changes report is not supported for Cisco Wireless IP Phone 7920.

Using the Suspect Phone Report

The Suspect Phone report displays the attributes of all IP phones in your network that:

- Have not registered with a Cisco Unified Communications Manager.
- Have made an unsuccessful attempt to register with a Cisco Unified Communications Manager.

Step 1 Select **Reports > IP Phones and Applications > IP Phone Status Changes > Suspect**. The IP Phone Status Reports page appears.

Step 2 Select the time period (24 hours - 30 days) from the list and click **View**. If there are any suspect IP phones, the Suspect Phone report appears in a new window, displaying the information described in the following table.

Column	Description
Extension	Extension number of the suspect IP phone.
IP Address	IP address of the suspect IP phone.
MAC Address	MAC address of the suspect IP phone.
Switch Address	IP address of the switch to which the suspect IP phone is connected.
Switch Port	Switch port used by the suspect IP phone.
Indication	Indicates the Cisco Unified Communications Manager registration status of the IP phone.

Tip Some IP phones appear marked as Suspect when they are not. To correct this, make sure that the Cisco Unified Communications Manager is managed by Operations Manager. You can check the status of the Cisco Unified Communications Manager on the Device Details report; see Viewing Device Details, page 16-32.

- If the Cisco Unified Communications Manager is not managed by Operations Manager, add it to Operations Manager.
- If the Cisco Unified Communications Manager is managed by Operations Manager but is not reachable, the cause may be loss of connectivity with Operations Manager. Make sure that connectivity with Operations Manager is restored.

Note The Suspect Phone report is not supported for Cisco Wireless IP Phone 7920.

Using the Duplicate MAC/IP Address Report

The Duplicate MAC/IP Address report lists the attributes of all IP phones in your network that have:

- Duplicate MAC addresses; that is, a phone that has the same MAC address as another phone but a different IP address.
- Duplicate IP addresses; that is, a phone that has the same IP address as another phone but a different MAC address.

Operations Manager does not show a multihomed host as a phone with a duplicate MAC address.

Note For the Duplicate MAC/IP Address report to display the correct information, the switch to which the phone is connected must be monitored by Operations Manager. If the switch is not monitored by Operations Manager, the report will not display any information.

Step 1 Select **Reports > IP Phones and Applications > IP Phone Status Changes > Duplicate MAC/IP Address**. The IP Phone Status Reports page appears.

Step 2 Select the time period (24 hours - 30 days) from the list and click **View**. The Duplicate MAC/IP Address IP Phone report appears, displaying the information described in the following table.

Column	Description
Extension	Extension number of the duplicate IP phone.
IP Address	One of the following: • If the problem is a shared MAC address, the IP address of the duplicate IP phone • If the problem is a shared IP address, the IP address in question
MAC Address	One of the following: • If the problem is a shared IP address, the MAC address of the duplicate IP phone • If the problem is a shared MAC address, the MAC address in question
Switch Address	IP address of the switch to which the duplicate IP phone is connected.
Switch Port	Switch port used by the duplicate IP phone.
Indication	Indicates the Cisco Unified Communications Manager registration status of the IP phone: duplicate ip.

Exporting IP Phone Status Changes Reports

Use this procedure to enable Operations Manager to generate IP Phone Status Changes reports once every 24 hours and store them on the Operations Manager system in comma-separated values (CSV) and PDF formats. The creation date and time are used to name the report files. The filename format is typeofreport_date_time.filetype.

Note Operations Manager does not automatically purge these report files. You must remove them manually.

Step 1 Select **Reports > IP Phones and Applications > IP Phone Status Changes > Export**. The automatically Export 24-Hour IP Phone Status Reports page appears, displaying the information described in the following table.

GUI Element	Description/Action
Reports pane	For each IP Phone Status Changes report that you want to generate and save nightly, select at least one of the following: • CSV check box—Save the report in CSV format. • PDF check box—Save the report in PDF format.
Generate pane	• Save at—A default location for storing the reports on the Operations Manager server is displayed; you can enter another location on the server. • E-mail to—(Optional) Enter a complete e-mail address.

Step 2 Click **Apply**.

Understanding IP Phone Movement Tracking

Operations Manager gathers information from switches and Cisco Unified Communications Managers every 5 minutes to identify these types of IP phone moves:

- Intercluster—A phone that was previously registered with one Cisco Unified Communications Manager cluster is now registered with a different cluster.
- Physical—A phone that was physically connected to one switch port is now physically connected to a different switch port.

Operations Manager gathers this information only for phones that run Cisco Discovery Protocol (CDP), such as Cisco Unified IP Phone. For supported models, see the *Supported and Interoperable Devices and Software Table for Cisco Unified* Operations Manager. Operations Manager stores this information for a period of 30 days, after which it is purged from the database. (For information about the daily purging schedule, see Setting System-Wide Parameters Using System Preferences, page 20-9.)

Each time IP Phone Movement Tracking runs, fresh information becomes available for the following reports:

- IP Phone Audit
- IP Phone Move
- Removed IP Phones
- Video Phone Audit
- Video Phone Move
- Removed Video Phones

Understanding Phone Polling

The following information appears in phone reports and is gathered by Operations Manager directly from IP phones, daily beginning at 4 a.m:

- Serial Number—IP phone serial number
- Application Load ID—Identifier of the firmware running on the phone
- Load ID—Identifier of the factory-installed load running on the phone

Using Video Phones Reports

Note If you do not have the required software license, you will not be able to use Video Phones reports.

Video Phones reports provide two types of reports: inventory and video phone status change:

- Inventory reports—Provide detailed video phone data, reflecting the current status of video phones in your network. These reports enable you to search for a few video phones, list a specific set of video phones—such as phones connected to a switch or phones in SRST mode—or view all video phones and lines:
  - **Search**—Use Search to view information for a few video phones or a single video phone; search enables you to find phones using all or part of an extension number, IP address, or MAC address. See Searching for Video Phones, page 13-30.
  - **Inventory Analysis**—Use the Inventory Analysis report to display video phones that meet criteria that you specify; for example, video phones that are registered to a particular Cisco Unified Communications Manager or video phones that are not connected to particular switches. See Generating the Video Phone Inventory Analysis Report, page 13-32 and Understanding Video Phone Reports, page 13-38.
  - **Video Phones/Lines**—Use the Video Phones/Lines report to view data for all video phones that Operations Manager is monitoring. See Understanding the All Video Phones/Lines Report, page 13-35 and Understanding Video Phone Reports, page 13-38.
  - **TelePresence**—Use the TelePresence report to view data for all TelePresence video phone devices and the Cisco Unified IP Phone 7970 associated with the corresponding TelePresence. See Generating the TelePresence Report, page 13-37.
  - **SRST Video Phones**—Use the SRST Video Phones report to view data for video phones that are configured for Survivable Remote Site Telephony (SRST) only. See Generating the SRST Video Phones Report, page 13-38.

    Note Video phones that are configured for SRST are also included in the All Video Phones/Lines report and can be included in the Inventory Analysis report.

  - **SIP Video Phones**—Use the SIP Video Phones report to view data for all SIP video phones that Operations Manager is monitoring. See Generating the SRST Video Phones Report, page 13-38.

  When a web interface is accessible for a video phone, you can open it from most video phone reports by clicking the hyperlink for one of the following:

  - Extension number
  - MAC address
  - Video phone IP address

  For more information, see Opening an IP Phone Web Interface, page 13-18.
- Video Phone Status Changes reports—Provide data for video phones that have undergone a status change during the previous 1 to 30 days:
  - **Video Phone Move**—Use the Video Phone Move report to view data for phones that have been connected to a different switch or switch port or that have registered to a different Cisco Unified Communications Manager. See Using the Video Phone Move Report, page 13-43.
  - **Video Phone Audit**—Use the Video Phone Audit report to obtain a summary of changes, including data for phones that have moved, been removed, undergone an extension number change, appeared in inventory with a duplicate MAC or IP address, or become suspect. See Using the IP Phone Audit Report, page 13-22.
  - **Removed Video Phones**—See Using the Removed Video Phones Report, page 13-45.

- **Extension Number Change**—See Using the Video Phone Extension Number Changes Report, page 13-46.

For more information, see:

- Using Video Phone Status Changes Reports, page 13-43
- Understanding the Time Period Covered by Phone Status Changes Reports, page 13-20
- Tracking Phone Status Changes when a Cisco Unified Communications Manager Is Down, page 13-21

Generating Video Phone Inventory Reports

This topic includes the following:

Searching for Video Phones

Use Search to find one or only a few video phones in your network. Search displays information for one phone at a time; you can page back and forth to view information for each phone when multiple phones are found. You can search for phones using all or part of an extension number, IP address, or MAC address.

When you want to find many phones—for example, all video phones registered with a Cisco Unified Communications Manager or all video phones connected to a switch—use the Inventory Analysis report; see Generating the Inventory Analysis Report, page 13-5.

Step 1 Select **Reports > Video Phones > Search**. The Find Video Phones page appears.

Step 2 In the Find Video Phones Where pane:

a. Select one of the following:

- Extension number
- IP address
- MAC address

b. Then select one of the following:

- is exactly
- begins with
- contains
- ends with

c. Enter a value.

Step 3 Click **View**. The Video Phone Details dialog box appears, displaying the information described in the following table.

Table 13-7 Video Phone Details

Row	Description
Extension	Extension number of the video phone; for example, 4000. Click the hyperlink to open the web interface on the video phone (see Opening an IP Phone Web Interface, page 13-18).
IP Address	IP address of the video phone; for example, 10.76.38.65. Click the hyperlink to see more details of the video phone (see Opening an IP Phone Web Interface, page 13-18).
MAC Address	MAC address of the video phone; for example, 003094c40454, or 00-30-94-c4-04-54. Click the hyperlink to open the web interface on the video phone (see Opening an IP Phone Web Interface, page 13-18).
CCM Address	Address of the Cisco Unified Communications Manager (CCM) with which the video phone is registered; for example, 10.76.38.70.
Switch Address	IP address of the switch to which the video phone is connected; for example, 10.76.29.162.
Switch Name	Switch to which the video phone is connected.
Switch Port	Switch port to which the video phone is connected; for example, Fa0/12.
Port Status	Status of the switch port to which the video phone is connected: up or down.
Video Phone Status	Cisco Unified Communications Manager registration status of the video phone: • yes—The video phone is registered with a Cisco Unified Communications Manager. • no—The video phone is not registered with a Cisco Unified Communications Manager.
Video Phone Model	Cisco video phone model number.
Protocol	Protocol the phone is using to communicate with Cisco Unified Communications Manager. **Note** Only SCCP and SIP phones will be discovered. H.323 and MGCP protocols are not currently supported.
VLAN Name	Name of the VLAN in the switch (a user-defined name); for example, voice.
VLAN ID	ID of the VLAN in the switch to which the video phone is connected; for example, 100.
SRST Router	IP address of the router that the phone is using for SRST.
SRST Mode	Can be one of the following: • yes—The phone is in SRST mode • no—The phone is not in SRST mode • ?—The phone is suspected to be in SRST mode • –(dash)—The phone is not an SRST phone

a. To display the information in print-friendly format in a new browser window, click **Print**; print the information, using the browser print function.

b. If search results include more than one phone, view them by clicking **Next** or **Prev**.

For more information, see the following topic:

- Troubleshooting Tips for IP Phones and Applications Reports and Video Phones Reports, page 13-19

Generating the Video Phone Inventory Analysis Report

Use Inventory Analysis to search for video phones in your network and display them in a report.

Before You Begin

Inventory Analysis searches for phones using:

- An implicit “or” within each field—If you enter more than one value in a field, Inventory Analysis searches for phones that match any value that you entered.
- An implicit “and” for all fields—If you enter values in more than one field, Inventory Analysis searches for phones that match at least one value from each field.

For example, if you enter two video phone models in the Video Phone Model field, the Inventory Analysis report that results includes all phones of these models. If, in addition, you enter a VLAN ID and a switch, Inventory Analysis searches for phones that meet all these criteria; the report that results includes only phones of the models specified that are connected to the switch and in the VLAN that you selected.

Step 1 Select **Reports > Video Phones > Inventory Analysis**. The Find Video Phones page appears.

Step 2 Enter values in one or more fields, described in the following table.

GUI Element	Description/Action
Find Video Phones Where list boxes and field	From left to right: • Select one of the following: – Extension number – IP Address – MAC Address • Then select one of the following: – is exactly – begins with – contains – ends with • Enter a value.
VLAN Name field	Enter the name of the VLAN.
VLAN ID field	Enter the VLAN ID.
Video Phone Status radio buttons	Select one: • Registered • Unregistered • All—Registered and unregistered phones.

GUI Element	Description/Action
SRST radio buttons	Select one: • SRST—Configured to fail over to an SRST router in case of a WAN link failure. • Non-SRST—Not configured for SRST. • All—SRST and non-SRST.
Protocol radio buttons	Select one: • SCCP—Phones using Skinny Client Control Protocol. • SIP—Phones using Session Initiation Protocol. • All—SCCP and SIP.
Video Phone Type field	Enter a comma-separated list of phone models. By default, all supported phone models are included in this field. Edit the entries in the field directly or select from a list of phone models, as follows: 1. Click  . The Select Video Phone Models list appears. 2. Select the desired video phone models from the list. (Use the Control key or the Shift key to select more than one video phone model from the list.) 3. Click **OK**.
CCM/CCM Cluster/ CME pane	• Exclude check box—Deselected by default. Select to exclude phones that belong to any Cisco Unified Communications Manager, Cisco Unified Communications Manager cluster, and Cisco Unified Communications Manager Express in the list box. • List box—Enter a comma-separated list of Cisco Unified Communications Managers, Cisco Unified Communications Manager clusters, and instances of Cisco Unified Communications Manager Express, or select them as follows: 1. Click  . The Select CCM/CCM Cluster/CME dialog box appears. 2. In the CCM/CCM Cluster/CME Selector, expand groups and select one or more of the following: Cisco Unified Communications Manager, Cisco Unified Communications Manager Cluster, and Cisco Unified Communications Manager Express. 3. Click **OK**. The dialog box closes and the Find Video Phones screen displays your selections in the CCM/CCM Cluster/CME list box.

GUI Element	Description/Action
Switch pane	• Exclude check box—Deselected by default. Select to exclude phones that are connected to any switch in the list box. • List box—Enter a comma-separated list of switches, or select them as follows: 1. Click  . The Inventory Analysis Switch Selection dialog box appears. 2. In the Switch Selector, expand groups and select switches. 3. Click **OK**. The dialog box closes and the Find Video Phones screen displays your selection in the Switch list box.
SRST Router pane	• Exclude check box—Deselected by default. Select to exclude phones that use any SRST router in the list box. • List box—Enter a comma-separated list of routers, or select them as follows: 1. Click  . The Inventory Analysis Router Selection dialog box appears. 2. In the Router Selector, expand groups and select routers. 3. Click **OK**. The dialog box closes and the Find Video Phones screen displays your selection in the Router list box.

Step 3 Click **View**. The Inventory Analysis Report appears in another window. See Understanding Video Phone Reports, page 13-38.

You might not be able to see the list of Cisco Unified Communications Managers or switches in the popup window that appears when you click  . This occurs when the PIFServer process is down. Do the following:

- Check the status of PIFServer by using the command **pdshow PIFServer** from the command line.
- If PIFServer is down, use the Common Services start function. To do this:
  1. From the Operations Manager home page, click **CiscoWorks** in the upper right-hand corner of the window. The CiscoWorks home page opens.
  2. Under Common Services, select **Server > Admin > Processes**. The Process Management page appears, displaying process names in a table.
  3. Locate the PIFserver process in the table, select the check box for it, and click **Start**.

Note Alternatively, you can bring PIFServer up using the command **pdexec PIFServer** from the command line. Use this approach if, for example, the web server is down.

Generating the All Video Phones/Lines Report

Step 1 Select **Reports > Video Phones > All Video Phones/Lines**. The All IP Phones/Lines window appears.

Step 2 Select **Video Phones** from the list, and click **View**. The All Video Phones/Lines report appears, displaying the information described in Understanding Video Phone Reports, page 13-38.

Note You can also generate the All Video Phones/Lines from the Monitoring Dashboard tab by selecting **Click to View All Phones** in the Video Phone Status pane.

Understanding the All Video Phones/Lines Report

The All Video Phones/Lines report lists video phones that match the criteria that you entered. By default, these reports display only these columns: Extension, User, IP Address, MAC Address, Model, Regd, CCM, Switch Address, and Port. You can hide these columns and select among additional columns to display. See Selecting Columns to Display and to Hide on a Phone Inventory Report, page 13-17.

Table 13-8 describes all possible columns of data that can appear on the report.

Table 13-8 All Video Phones/Lines Report

Columns and Buttons	Description/Action
Number	The row number; starting from 1.
Check box	Select phones that you would like to: • Print—Include selected phones in a new window in print-friendly format. (See Phones Report Tool Buttons, page 13-13.) • Export to a file—Include selected phones in a PDF or CSV file. (See Phones Report Tool Buttons, page 13-13.) • Launch a test on—Include selected phones in tests that you create from the Launch button when it is present at the bottom of the report. (See Launching Tests for Selected IP Phones, page 13-18.)
Extn.	Extension number of the video phone; for example, 4000. Click the hyperlink to see more details of the video phone (see Opening an IP Phone Web Interface, page 13-18).
User	Username obtained using LDAP if you have configured an LDAP server in Operations Manager. See Configuring LDAP, page 16-41 and Obtaining Usernames from LDAP for IP Phone Reports, page 13-18.
IP Address	IP address of the video phone; for example, 10.76.38.65. Click the hyperlink to see more details of the video phone (see Opening an IP Phone Web Interface, page 13-18).
MAC Address	MAC address of the video phone; for example, 003094c40454, or 00-30-94-c4-04-54. Click the hyperlink to see more details of the video phone (see Opening an IP Phone Web Interface, page 13-18).
Model	Model number of the video phone; for example, 7902, 7905, 7910, 7912, 7920, 7935, 7940, 7960, or 7970.

Table 13-8 All Video Phones/Lines Report

Protocol	Protocol the phone is using to communicate with Cisco Unified Communications Manager or Cisco Unified Communications Manager Express. **Note** Only SCCP and SIP phones will be discovered. H.323 and MGCP protocols are not currently supported.
Regd.	Registration status of the video phone with respect to Cisco Unified Communications Manager or Cisco Unified Communications Manager Express. Displays **yes** if the video phone is registered or **no** if the video phone is not registered.
CCM	One of the following: • CCM—Cisco Unified Communications Manager • CCE—Cisco Unified Communications Manager Express
CCM/CME Name	DNS name of the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express with which the video phone is registered.
CCM/CME Address	IP address of the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express with which the video phone is registered.
Switch Name	Name of the switch to which the video phone is connected.
Switch Address	IP address of the switch to which the video phone is connected.
Port	Switch port used by the video phone; for example, Fa0/12.
Port Status	Status of the port used by the video phone: up or down.
VLAN Name	Name of the VLAN (user-defined name); for example, voice.
VLAN ID	ID of the VLAN for the video phone; for example, 100.
SRST Mode	One of the following: • yes—The phone is in SRST mode • no—The phone is not in SRST mode • ?—The phone is suspected to be in SRST mode • —(dash)—The phone is not an SRST phone
SRST Router	One of the following: • IP address of the router that the phone is using for SRST • —(dash)
Serial No.	IP phone serial number **Note** This information is obtained by phone polling. See Understanding Phone Polling, page 13-28.
Application ID	Identifier of the firmware running on the phone **Note** This information is obtained by phone polling. See Understanding Phone Polling, page 13-28.

Table 13-8 All Video Phones/Lines Report

Load ID	Identifier of the factory-installed load running on the phone **Note** This information is obtained by phone polling. See Understanding Phone Polling, page 13-28.
Launch button	Click and select a menu item to configure tests for the video phones selected on this report.

Generating the TelePresence Report

The TelePresence report shows a list of the TelePresence video phone devices and the Cisco Unified IP Phone 7970 associated with the corresponding TelePresence system.

Step 1 Select **Reports > Video Phones > TelePresence**. The TelePresence report appears in a new window, displaying information for TelePresence video phone devices and the associated Cisco Unified IP Phone 7970. For more information, see Understanding Video Phone Reports, page 13-38.

Table 13-9 TelePresence Report

Columns and Buttons	Description/Action
Number	The row number; starting from 1.
Check box	Select phones that you would like to: • Print—Include selected phones in a new window in print-friendly format. (See Phones Report Tool Buttons, page 13-13.) • Export to a file—Include selected phones in a PDF or CSV file. (See Phones Report Tool Buttons, page 13-13.)
Extn.	Extension number of the video phone; for example, 4000. Click the hyperlink to see more details of the video phone (see Opening an IP Phone Web Interface, page 13-18).
User	Username obtained using LDAP if you have configured an LDAP server in Operations Manager. See Configuring LDAP, page 16-41 and Obtaining Usernames from LDAP for IP Phone Reports, page 13-18.
IP Address	IP address of the video phone; for example, 10.76.38.65. Click the hyperlink to see more details of the video phone (see Opening an IP Phone Web Interface, page 13-18).
MAC Address	MAC address of the video phone; for example, 003094c40454, or 00-30-94-c4-04-54. Click the hyperlink to see more details of the video phone (see Opening an IP Phone Web Interface, page 13-18).
Model	Model number of the video phone.
Regd.	Registration status of the video phone with respect to Cisco Unified Communications Manager or Cisco Unified Communications Manager Express. Displays **yes** if the video phone is registered or **no** if the video phone is not registered.
CCM/CME Address	IP address of the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express with which the video phone is registered.

Table 13-9 TelePresence Report (continued)

Columns and Buttons	Description/Action
Switch Address	IP address of the switch to which the video phone is connected.
Port	Switch port used by the video phone; for example, Fa0/12.

Generating the SRST Video Phones Report

The SRST Video Phones report shows a list of phones that are configured for Survivable Remote Site Telephony (SRST).

Step 1 Select **Reports > Video Phones > SRST Video Phones**. The SRST Video Phones report appears in a new window, displaying information for the SRST configuration only. For more information, see Understanding Video Phone Reports, page 13-38.

Generating the SIP Video Phones Report

The SIP Video Phones report shows a list of SIP video phones.

Step 1 Select **Reports > Video Phones > SIP Video Phones**. The SIP Phones report appears in a new window, displaying information for SIP video phones only. For more information, see Understanding Video Phone Reports, page 13-38.

Understanding Video Phone Reports

Table 13-5 describes the data displayed in the following reports:

- Inventory Analysis—Includes phones that match criteria that you specify.
- All Video Phones/Lines—Includes all video phones, including video phones that are configured for SRST.

Note You can filter the All Video Phones/Lines report to include only the phones that you want to see.

- SRST Video Phones—Includes only phones that are configured for SRST.
- SIP Video Phones—Includes only SIP video phones.

By default, these reports display only these columns: Extension, User, IP Address, MAC Address, Model, Regd, CCM, Switch Address, and Port. You can hide these columns and select among additional columns to display. See Selecting Columns to Display and to Hide on a Phone Inventory Report, page 13-17.

Table 13-10 describes all possible columns of data that can appear on the reports.

Table 13-10 Video Phone Reports

Columns and Buttons	Description/Action
Number	The row number; starting from 1.
Check box	Select phones that you would like to: • Print—Include selected phones in a new window in print-friendly format. (See Phones Report Tool Buttons, page 13-13.) • Export to a file—Include selected phones in a PDF or CSV file. (See Phones Report Tool Buttons, page 13-13.) • Launch a test on—Include selected phones in tests that you create from the Launch button when it is present at the bottom of the report. (See Launching Tests for Selected IP Phones, page 13-18.)
Extn.	Extension number of the video phone; for example, 4000. Click the hyperlink to see more details of the video phone (see Opening an IP Phone Web Interface, page 13-18).
User	Username obtained using LDAP if you have configured an LDAP server in Operations Manager. See Configuring LDAP, page 16-41 and Obtaining Usernames from LDAP for IP Phone Reports, page 13-18.
IP Address	IP address of the video phone; for example, 10.76.38.65. Click the hyperlink to see more details of the video phone (see Opening an IP Phone Web Interface, page 13-18).
MAC Address	MAC address of the video phone; for example, 003094c40454, or 00-30-94-c4-04-54. Click the hyperlink to see more details of the video phone (see Opening an IP Phone Web Interface, page 13-18).
Model	Model number of the video phone.
Protocol	Protocol the phone is using to communicate with Cisco Unified Communications Manager or Cisco Unified Communications Manager Express. **Note** Only SCCP and SIP phones will be discovered. H.323 and MGCP protocols are not currently supported.
Regd.	Registration status of the video phone with respect to Cisco Unified Communications Manager or Cisco Unified Communications Manager Express. Displays **yes** if the video phone is registered or **no** if the video phone is not registered.
CCM	One of the following: • CCM—Cisco Unified Communications Manager. • CCE—Cisco Unified Communications Manager Express.
CCM/CME Name	DNS name of the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express with which the video phone is registered.
CCM/CME Address	IP address of the Cisco Unified Communications Manager or Cisco Unified Communications Manager Express with which the video phone is registered.
Switch Name	Name of the switch to which the video phone is connected.

Table 13-10 Video Phone Reports (continued)

Columns and Buttons	Description/Action
Switch Address	IP address of the switch to which the video phone is connected.
Port	Switch port used by the video phone; for example, Fa0/12.
Port Status	Status of the port used by the video phone: up or down.
VLAN Name	Name of the VLAN (user-defined name); for example, voice.
VLAN ID	ID of the VLAN for the video phone; for example, 100.
SRST Mode	One of the following: • yes—The phone is in SRST mode. • no—The phone is not in SRST mode. • ?—The phone is suspected to be in SRST mode. • —(dash)—The phone is not an SRST phone.
SRST Router	One of the following: • IP address of the router that the phone is using for SRST. • —(dash).
Serial No.	IP phone serial number. **Note** This information is obtained by phone polling. See Understanding Phone Polling, page 13-28.
Application ID	Identifier of the firmware running on the phone. **Note** This information is obtained by phone polling. See Understanding Phone Polling, page 13-28.
Load ID	Identifier of the factory-installed load running on the phone. **Note** This information is obtained by phone polling. See Understanding Phone Polling, page 13-28.
Launch button	Click and select a menu item to configure tests for the video phones selected on this report.

For more information, see the following topic:

- Troubleshooting Tips for IP Phones and Applications Reports and Video Phones Reports, page 13-19

Filtering a Video Phones Report

From a Video Phones report, click the Filter button when present. A filter dialog box opens.

Note Filtering is performed using:

- An implicit “or” within each field—If you enter more than one value in a field, phones that match any value are included in the report.
- An implicit “and” for all fields—If you enter values in more than one field, phones that match at least one value from each field are included in the report after filtering.

For example, if you enter two phone models, such as 7910 and 7935, in the Video Phone Model field, the report that results includes all phones of these models. If, in addition, you enter a VLAN ID and a switch, the report is filtered to include only phones of the models specified that are connected to the switch and in the VLAN that you selected.

Step 1 Enter values in one or more fields, described in the following table.

GUI Element	Description/Action
Find Video Phones where list boxes and field	From left to right: • Select one of the following: – Extension number – IP Address – MAC Address • Then select one of the following: – is exactly – begins with – contains – ends with • Enter a value.
VLAN Name field	Enter the name of the VLAN.
VLAN ID field	Enter the VLAN ID.
Video Phone Status radio buttons	Select one: • Registered • Unregistered • All—Registered and unregistered phones.
SRST radio buttons	Select one: • SRST—Configured to fail over to an SRST router in case of a WAN link failure. • Non-SRST—Not configured for SRST. • All—SRST and non-SRST.
IP Phone Types field	Enter a comma-separated list of phone types. Edit the entries in the field directly or select from a list of phone models, as follows: 1. Click  . The Select IP Phone Types list appears. 2. Select the desired video phone types from the list. (Use the Control key or the Shift key to select more than one video phone type from the list.) 3. Click **OK**.

GUI Element	Description/Action
CCM/CME pane	• Exclude check box—Deselected by default. Select to exclude phones that belong to any Cisco Unified Communications Manager, Cisco Unified Communications Manager cluster, and Cisco Unified Communications Manager Express in the list box. • List box—Enter a comma-separated list of Cisco Unified Communications Managers, Cisco Unified Communications Manager clusters, and instances of Cisco Unified Communications Manager Express, or select them as follows: 1. Click  . The Select CCM/CCM Cluster/CME dialog box appears. 2. In the CCM/CCM Cluster/CME Selector, expand groups and select one or more instances of the following: Cisco Unified Communications Manager, Cisco Unified Communications Manager cluster, and Cisco Unified Communications Manager Express. 3. Click **OK**.
Switch pane	• Exclude check box—Deselected by default. Select to exclude phones that are connected to any switch in the list box. • List box—Enter a comma-separated list of switches, or select them as follows: 1. Click  . The Inventory Analysis Switch Selection dialog box appears. 2. In the Switch Selector, expand groups and select switches. 3. Click **OK**.
SRST Router pane	• Exclude check box—Deselected by default. Select to exclude phones that use any SRST router in the list box. • List box—Enter a comma-separated list of switches, or select them as follows: 1. Click  . The Inventory Analysis Router Selection dialog box appears. 2. In the Router Selector, expand groups and select routers. 3. Click **OK**.

Step 2 Click **OK**. The filter dialog box closes and the video phone report refreshes. For more information, see Understanding IP Phone Inventory Reports, page 13-11.

You might not be able to see the list of Cisco Unified Communications Managers or switches in the popup window that appears when you click  . This occurs when the PIFServer process is down. Do the following:

- Check the status of PIFServer by using the command **pdshow PIFServer** from the command line.
- If PIFServer is down, use the Common Services start function. To do this:
  1. From the Operations Manager home page, click **CiscoWorks** in the upper right-hand corner of the window. The CiscoWorks home page opens.

2. Under Common Services, select **Server > Admin > Processes**. The Process Management page appears, displaying process names in a table.
3. Locate the PIFserver process in the table, select the check box for it, and click **Start**.

Note Alternatively, you can bring PIFServer up using the command **pdexec PIFServer** from the command line. Use this approach if, for example, the web server is down.

Using Video Phone Status Changes Reports

Video Phone Status Changes reports supply information for phones that have undergone a status change during the previous 1 to 30 days.

The Video Phone Audit report provides a summary of all of these changes (see Using the Video Phone Audit Report, page 13-44). Additional Video Phone Status Changes reports focus on particular types of changes, as shown in the following table.

Phone Status Change	Details in this Report…
Connection—Connected to a different switch or switch port	Using the Video Phone Move Report, page 13-43
Extension number change	Using the Video Phone Extension Number Changes Report, page 13-46
Removed	Using the Removed Video Phones Report, page 13-45

Using the Video Phone Move Report

The Video Phone Move report displays video phones that have moved, including details about the phone before and after the move. The Video Phone Move report shows the time at which the video phone move was detected, and not the time at which the move occurred.

Information for the Video Phone Move report is gathered every 5 minutes by Video Phone Movement Tracking (see Understanding IP Phone Movement Tracking, page 13-28). Video Phone Movement Tracking checks all the switches and Cisco Unified Communications Managers, identifies the list of changes, and generates the data on video phone moves.

Note You obtain fresh data for the Video Phone Move report about once every 5 minutes. Close the report and regenerate it to refresh the data.

Step 1 Select **Reports > Video Phones > Video Phone Move**. The Video Phone Status Reports page appears.

Step 2 Select the time period (24 hours - 30 days) from the list and click **View**. The Video Phone Move report appears, displaying the information described in the following table.

Column	Description
Extension	Extension number of the video phone. The Extension column has two subcolumns—Old and New: • **Old**—Extension number of the video phone before it was moved. • **New**—Extension number of the video phone after it was moved.
IP Address	IP address of the video phone.
MAC Address	MAC address of the video phone.
CCM Address	Cisco Unified Communications Manager address. The CCM Address column has two subcolumns: • **Old**—CCM address of the video phone before it was moved. • **New**—CCM address of the video phone after it was moved.
Switch Address	IP address of the switch to which the video phone is connected. The Switch Address column has two subcolumns: • **Old**—Switch address used by the video phone before it was moved. • **New**—Switch address used by the video phone after it was moved.
Switch Port	Switch port used by the video phone. The Switch Port column has two subcolumns: • **Old—**Switch port used by the video phone before it was moved. • **New**—Switch port used by the video phone after it was moved.
Time Stamp	Reflects the date and time that Operations Manager detected the video phone move.

Tip Phones that have moved and do not run Cisco Discovery Protocol (CDP) do not appear in this report. For example, 30VIP and 12SP+ do not run CDP; you will not see move entries for them.

Using the Video Phone Audit Report

The Video Phone Audit report shows the changes that have occurred in the managed video phone network. For example, this report shows you the video phones that have been added to or deleted from your network, or changes in video phone status. Phone status changes occur, for instance, when a phone becomes unregistered with the Cisco Unified Communications Manager.

You can see what has changed within the last 30 days. Audits are maintained in the database for a period of 30 days, after which they are purged.

Information for the Video Phone Audit report is gathered by IP Phone Movement Tracking (see Understanding IP Phone Movement Tracking, page 13-28). IP Phone Movement Tracking runs every 5 minutes, so you can run the Video Phone Audit Detail report and obtain fresh data about once every 5 minutes. This interval is not configurable.

Step 1 Select **Reports > Video Phones > Video Phone Audit**. The Video Phone Status Reports page appears.

Step 2 Select the time period (24 hours - 30 days) from the list and click **View**. The Video Phone Audit report appears, displaying the information described in the following table.

Column	Description
Extension	Extension number of the video phone.
IP Address	IP address of the video phone.
MAC Address	MAC address of the video phone.
CCM/CME Address	Cisco Unified Communications Manager or Cisco Unified Communications Manager Express address.
Switch Address	IP address of the switch to which the video phone is connected.
Switch Port	Switch port used by the video phone.
Time	Time of audit on the Cisco Unified Communications Manager. **Note** Audit date and time are taken directly from Cisco Unified Communications Manager without adjustment for time zone differences, if any exist, between Cisco Unified Communications Manager and Operations Manager systems.
Audit Type	One of the following: • add—Phone added to the network. • remove—Phone removed from the network. • unregistered—From Cisco Unified Communications Manager. • registered—With Cisco Unified Communications Manager.

Using the Removed Video Phones Report

The Removed Video Phones report lists phones that have been removed during the previous 1 to 30 days. Operations Manager gathers the information used in this report every 5 minutes (see Understanding IP Phone Movement Tracking, page 13-28.) Therefore, you can run this report and obtain fresh data about once every 5 minutes.

Step 1 Select **Reports > Video Phones > Removed Video Phones.** The Video Phone Status Reports page appears.

Step 2 Select the time period (24 hours - 30 days) from the list and click **View**. The Removed Video Phones report appears in a new window, displaying the information described in the following table.

Column	Description
Extension	Extension number of the video phone.
IP Address	IP address of the video phone.
MAC Address	MAC address of the video phone.
CCM/CME Address	Cisco Unified Communications Manager or Cisco Unified Communications Manager Express address.
Switch Address	IP address of the switch to which the video phone was previously connected.
Switch Port	Switch port to which the video phone was previously connected.
Time	Time that the phone was removed from Cisco Unified Communications Manager. **Note** Removal date and time are taken directly from Cisco Unified Communications Manager without adjustment for time zone differences, if any exist, between Cisco Unified Communications Manager and Operations Manager systems.
Indication	Indicates the Cisco Unified Communications Manager registration status of the video phone: removed.

Using the Video Phone Extension Number Changes Report

The Extension Number Changes report lists phones that have changed extension numbers during the previous 1 to 30 days. Operations Manager gathers the information used in this report every 5 minutes (see Understanding IP Phone Movement Tracking, page 13-28.) Therefore, you can run this report and obtain fresh data about once every 5 minutes.

Step 1 Select **Reports > Video Phones > Extension Number Changes**. The Video Phone Status Reports page appears.

Step 2 Select the time period (24 hours - 30 days) from the list and click **View**. The Extension Number Changes report appears in a new window, displaying the information described in the following table.

Column	Description
Extension	Extension number of the video phone.
IP Address	IP address of the video phone.
MAC Address	MAC address of the video phone.
CCM Address	Cisco Unified Communications Manager address.
Switch Address	IP address of the switch to which the video phone was previously connected.
Switch Port	Switch port to which the video phone was previously connected.
Time	Time that Operations Manager determined that the extension number changed.

Exporting Video Phone Status Changes Reports

Use this procedure to enable Operations Manager to generate Video Phone Status Changes reports once every 24 hours and store them on the Operations Manager system in comma-separated values (CSV) and PDF formats. The creation date and time are used to name the report files. The filename format is typeofreport_date_time.filetype.

Note Operations Manager does not automatically purge these report files. You must remove them manually.

Step 1 Select **Reports > Video Phones > Export**. The automatically Export 24-Hour Video Phone Status Reports page appears, displaying the information described in the following table.

GUI Element	Description/Action
Reports pane	For each Video Phone Status Changes report that you want to generate and save nightly, select at least one of the following: • CSV check box—Save the report in CSV format. • PDF check box—Save the report in PDF format.
Generate pane	• Save at—A default location for storing the reports on the Operations Manager server is displayed; you can enter another location on the server. • E-mail to—(Optional) Enter a complete e-mail address.

Step 2 Click **Apply**.

Viewing Other Reports

To view Service Level or Unified CM Express View reports, access the reports via the Monitoring Dashboard. See Understanding Service Level and Unified CM Express Views, page 2-1 or Viewing Large Numbers of Devices and Clusters from the Service Level View, page 2-15.

CHAPTER 14

Using the Personalized Report

This section includes the following topics:

Getting Started with the Personalized Report

The Personalized Report enables you to configure a report for the devices, phones, and diagnostic tests that interest you. Other users cannot configure or view this report from Operations Manager.

Note For purposes of the Personalized Report, a user is defined as the username and password combination used to log in to Operations Manager.

Before you can view the Personalized Report, you must select the days on which the Personalized Report should run and the time at which it should run. Optionally, you can export the report to disk when it runs.

The first time you generate a personalized report, the summary information displayed is from the report generated after installation to the time of this request. Subsequent reports display a summary from the time of the previous report generated to the time of last report (the time between subsequent reports).

Configuring a Personalized Report

Step 1 Select **Report > Personalized Report > Configuration**. The Personalized Report Configuration page appears.

Step 2 Enter a name in the Report Name field.

Step 3 In the Configure pane, select one radio button at a time to select the devices, phones, and tests you want included in your report. At any time, click **View** to see a summary of your selections or click **Save** to save your selections. The following table describes how to enter data in the Configure pane.

:

GUI Element	Description/Action
Devices radio button	Expand device folders and select devices from the selector.
Phones radio button	Select the phones that you want to include in your report: • Add phones by entering them or selecting them. To enter phones for which you know the extension number of the MAC address: a. Select **Add > From Known List**. The Add Phone From Known List dialog box appears. b. Enter a comma-separated list of phone extensions and MAC addresses and click Apply. • To select phones from a report: a. Select **Add > From Phone Report**. The All Phone Reports window opens. b. Select phones and click Select. **Note** Phone selection from the Phone report is based on the extension. Personalized reports contain details about all the phones with that extension. Remove phones by selecting them and clicking **Remove**.
Node-to-Node Test radio button	Select tests from the list.
Synthetic Test radio button	Select tests from the list.
Phone Test radio button	Select tests from the list.

Note Clicking **Cancel** cancels all selections, including those for Devices, Phones, Node-to-Node Test, Synthetic Test, and Phone Test.

Step 4 Click **Save**.

Note If you have not yet scheduled the report to run, you must do so. See Scheduling and Exporting the Personalized Report, page 14-13.

Viewing the Personalized Report Configuration Summary

Step 1 Select **Report > Personalized Report > Configuration**. The Personalized Report Configuration page appears.

Step 2 Click **View**. The Report Configuration Summary dialog box opens, displaying the report name and lists:

- Devices selected

- Phones selected
- Node-to-Node tests selected
- Synthetic tests selected
- Phone status tests selected

Step 3 Click **Close**.

Updating the Personalized Report Configuration

Step 1 Select **Report > Personalized Report > Configuration**. The Personalized Report Configuration page appears.

Step 2 Do one of the following:

- Configure a fresh report—Clear all selections by clicking **Reset**. Make new selections; for more information, see Configuring a Personalized Report, page 14-1.

Note After you click Reset, you cannot return to your previous selections. Clicking Reset clears all selections and saves the configuration.

- Update individual selections (see Configuring a Personalized Report, page 14-1) and click **Save**.

The updated configuration is used the next time the Personalized Report runs.

Resetting the Personalized Report Configuration

Use this procedure to clear all selections from the configuration; this is useful when you want to completely reconfigure the Personalized Report.

Note After you click Reset, the configuration is erased. If you do not reconfigure the report (see Configuring a Personalized Report, page 14-1), errors will occur the next time it is scheduled to run. To disable the report, see Enabling and Disabling the Personalized Report, page 14-14.

Step 1 Select **Report > Personalized Report > Configuration**. The Personalized Report Configuration page appears.

Step 2 Click **Reset**.

Viewing the Personalized Report

Note Operations Manager generates the Personalized Report on a schedule; at most, once daily. Operations Manager must generate the report at least once before you can view it. For more information, see Scheduling and Exporting the Personalized Report, page 14-13.

Use this procedure to view a summary and to open report windows for details.

Step 1 Select **Report > Personalized Report > View Report**. The Personalized Report page appears, displaying summaries for the elements that you selected for inclusion in the report:

- **Devices**—Number of selected devices that Operations Manager is monitoring, number of new alerts, and of those, number that are severe. Click the **View** link for details.
- **Phones**—Number of selected phones that Operations Manager is monitoring, number that have lost connectivity, and number that have been moved. Click the **View** link for details.
- **Tests**—Number of selected tests of each type that are running and that have failed. Click the **View** link for details.

Personalized Report for Selected Devices

Note To launch this report, see Viewing the Personalized Report, page 14-4.

This report contains details about devices you have selected for inclusion in your personalized report. The report content is described in the following table.

Field	Description/Action
Go to (list)	Select a section of the report to navigate to it: • Selected Devices Details—Provides succinct status, including alert severity for any alert. • Alerts—Lists details for any alerts on selected devices. • 24-Hour Event History—Lists event history for events related to the alerts.
Selected Devices Details	
Device Type	Type of device.
Device Name	Device name or IP address.
IP Address	Device IP address.

Field	Description/Action
Status	State the device is in with respect to being monitored by Operations Manager: • Monitored • Partially Monitored • Monitoring Suspended • Inventory Collection in Progress • Unreachable • Unsupported For more information, see Understanding the Device Summary and Device States, page 16-14.
First Added	Date and time that the device was first added to Operations Manager.
Last Discovered	Date and time when inventory collection for the device last occurred.
Alert Severity	Critical, Warning, Informational, or, if there are no alerts on the device, Not Available.
Back to Top (link)	Click to return to the top of the report.
Alerts	
Severity	Alert severity—Critical, Warning, or Informational.
Alert ID	Unique identifier for the alert.
Device Type	Type of device.
Device Name	Device name or IP address.
Latest Event Time	Date and time of the most recent event related to the alert.
Latest Event Description	Description of the most recent event. (For event descriptions, see Events Processed, page E-1. Event descriptions can also be customized; see Customizing Events, page 15-23.)
Alert Age	Number of hours that an alert has been in existence.
Status	Alert status—Active, Cleared, or Acknowledged. For more information, see Table 3-4 on page 3-8.
Back to Top (link)	Click to return to the top of the report.
24-Hour Event History	
Event ID	Unique identifier for this event.
Device Type	Type of device.
Device Name	Device name or IP address.
Device Component	Component within the device on which the event occurred.
Event Description	Description of the event. (For event descriptions, see Events Processed, page E-1. Event descriptions can also be customized; see Customizing Events, page 15-23.)
Time	Date and time the event occurred.

Field	Description/Action
Status	Active, Cleared, Suspended, Resumed, or Deleted. For more information, see Table 3-8 on page 3-15.
Alert ID	Unique identifier for the alert that this event is related to.
Back to Top (link)	Click to return to the top of the report.

Personalized Report for Selected Phones

Note To launch this report, see Viewing the Personalized Report, page 14-4.

This report contains details about phones you have selected for inclusion in your personalized report. The report content is described in the following table.

Field	Description/Action
Go to (list)	Select a section of the report to navigate to it: • Phone Details—Provides information for selected phones. • Disconnected/Unregistered Phones in Last 24 Hours—Lists selected phones only if they have been disconnected or unregistered in the previous 24 hours. • Moved Phones in Last 24 Hours—Lists selected phones only if they have moved in the previous 24 hours.
Phone Details	
Extension	Phone extension number.
User	User identified by username, extension, or IP address.
IP Address	IP address for the phone.
MAC Address	MAC address for the phone.
Model	Cisco Unified IP Phone model number.
Protocol	SCCP **Note** H.323 and MGCP protocols are not currently supported.
Regd	Whether the phone is registered to a Cisco Unified Communications Manager or Cisco Unified Communications Manager Express—yes or no.
CCM/CCE Address	Address of the Cisco Unified Communications Manager (CCM) with which the IP phone is registered; for example, 10.76.38.70.
Switch Address	IP address of the switch to which the IP phone is connected; for example, 10.76.29.162.
Switch Name	Name of the switch to which the IP phone is connected.
Port	Switch port used by the IP phone; for example, Fa0/12.
Port Status	Status of the port used by the IP phone; for example, static.
VLAN Name	Name of the VLAN (user-defined name); for example, voice.

Field	Description/Action
VLAN ID	ID of the VLAN for the IP phone; for example, 100.
SRST Mode	One of the following: • yes—The phone is in SRST mode • no—The phone is not in SRST mode • ?—The phone is suspected to be in SRST mode • - (dash)—The phone is not an SRST phone
SRST Router	IP address of the router that the phone is using for SRST.
Back to Top (link)	Click to return to the top of the report.
Disconnected/Unregistered Phones in Last 24 Hours	
Extension	Phone extension number.
IP Address	IP address for the phone.
MAC Address	MAC address for the phone.
Switch Address	IP address of the switch to which the IP phone is connected; for example, 10.76.29.162.
Switch Port	Switch port used by the IP phone; for example, Fa0/12.
Indication	How move was identified.
Back to Top (link)	Click to return to the top of the report.
Moved Phones in Last 24 Hours	
Old Extension	Previous phone extension number.
New Extension	Current phone extension number.
IP Address	IP address for the phone.
MAC Address	MAC address for the phone.
Old CCM	Cisco Unified Communications Manager that the phone was previously registered to.
New CCM	Cisco Unified Communications Manager that the phone is currently registered to.
Old Switch	IP address of the switch to which the IP phone was previously connected; for example, 10.76.29.162.
New Switch	IP address of the switch to which the IP phone is currently connected.
Old Switch Port	Switch port used by the IP phone previously; for example, Fa0/12.
New Switch Port	Switch port used by the IP phone currently.
Deleted Time	Date and time that the old extension was deleted.
Added Time	Date and time that the new extension was added.
Back to Top (link)	Click to return to the top of the report.

Personalized Report for Selected Diagnostic Tests

Note To launch this report, see Viewing the Personalized Report, page 14-4.

This report contains details about diagnostic tests you have selected for inclusion in your personalized report. The report content is described in the following table.

Report Element	Description/Action
Go to (list)	Select a section of the report to navigate to it: • Node-to-Node Tests (Current Status)—Lists most recent node-to-node test results for selected tests. • Node-to-Node Tests (24-Hour History)—Graphs data from node-to-node tests that failed in the previous 24 hours; limited to selected node-to-node tests. • Synthetic Tests (Current Status)—Lists most recent test results for selected tests. • Synthetic Tests (24-Hour Event History)—Lists any test failures for selected synthetic tests. • Phone Status Tests (Current Status)—Lists most recent test results for selected phone status tests. • Phone Status Tests (24-Hour Event History)—Lists any test failures for selected phone status tests.
Node-to-Node Tests (Current Status)	
Test Name	Node-to-node test name. (See Using Node-To-Node Tests, page 11-1.)
Test Type	One of the following: • UDP Jitter for VoIP • Ping Echo • Ping Path Echo • UDP Echo • Gatekeeper Registration Delay • Real Time Transfer
Source	Source device.
Destination	Destination IP-enabled device.
Latest Result	Status for most recent test: pass or fail.
Time Stamp	Date and time of most recent test.
Back to Top (link)	Click to return to the top of the report.

Report Element	Description/Action
Node-to-Node Tests (24-Hour History)	
Graph	A graph is displayed for each node-to-node test included in your Personalized Report that failed in the previous 24 hours. Information about the test is listed above the graph: • Test name. • IP addresses or DNS names of source and destination devices. • Node-to-node test type. • Statistics collected for the test type. The Y axis of each graph: • Adjusts to the maximum value to be displayed. • Displays tick marks at intervals of 40 (the unit of measure is displayed in the legend). The number of values plotted on the graph should match the number of statistics listed above the graph. For example, for a UDP Jitter for VoIP test, the following three statistics could be listed above the graph: Average Latency, Source to Destination, and Destination to Source. Correspondingly, three values should be plotted on the graph. **Note** If not all expected values are plotted on a graph, the most likely reason is that one or more values are very small in comparison to the maximum value. For example, for the values 250, 2, and 1, the smaller values, 2 and 1, will not be plotted.
Synthetic Tests (Current Status)	
Test Name	Name of the synthetic test. For more information about synthetic tests, see Getting Started with Synthetic Tests, page 9-1.
Test Type	One of the following: • End-to-end call test • Phone registration test • Dial-tone test • TFTP download test • Cisco Emergency Responder (CER) test • Cisco Conference Connection (CCC) test • Message Waiting Indicator test
Application	Application involved in the synthetic test: • Cisco Unified Communications Manager (all tests) • Cisco Conference Connection • Cisco Emergency Responder • Cisco Unity (MWI)
Other Details	Additional information.

Report Element	Description/Action
Latest Result	Result of most recent synthetic test: pass or fail.
Time Stamp	Date and time of most recent synthetic test.
Back to Top (link)	Click to return to the top of the report.
Synthetic Tests (24-Hour Event History)	
Event ID	Unique ID for this event.
Event Description	One of the following or a customized description for any of these: • SyntheticTestFailedTests • SyntheticTestsNotRun • TooManyFailedSyntheticTests (For event descriptions, see Events Processed, page E-1. For information about customized events, see Customizing Events, page 15-23.)
Test Name	Name of the synthetic test. For more information about synthetic tests, see Getting Started with Synthetic Tests, page 9-1.
Test Type	One of the following: • End-to-end call test • Phone registration test • Dial-tone test • TFTP download test • Cisco Emergency Responder (CER) test • Cisco Conference Connection (CCC) test • Message Waiting Indicator test
Application	Applications involved in the synthetic test: • Cisco Unified Communications Manager (all tests) • Cisco Conference Connection • Cisco Emergency Responder • Cisco Unity (MWI)
Other Details	Additional information.
Time Stamp	Date and time the synthetic test ran.
Back to Top (link)	Click to return to the top of the report.
Phone Status Tests (Current Status)	
Test Name	Name of the phone status test. For more information about phone status tests, see Getting Started with Phone Status Testing, page 8-1.
Source Phones	IP address of the source phone.
Latest Result	Result of the most recent phone status test: pass or fail.
Time Stamp	Date and time of the most recent phone status test.
Back to Top (link)	Click to return to the top of the report.
Phone Status Tests (24-Hour Event History)	

Report Element	Description/Action
Event ID	ID of the event.
Event Description	PhoneReachabilityTestFailed event or customized event name. (For event descriptions, see Events Processed, page E-1. For information about customized events, see Customizing Events, page 15-23.)
Test Name	Name of the phone status test.
Test Status	Status of the test: pass or fail.
Phone Extension	IP phone extension.
Phone MAC Address	IP phone MAC address.
Time Stamp	Date and time of most recent phone status test.
Back to Top (link)	Click to return to the top of the report.

24-Hour Inventory Update Report—Devices

Note To launch this report, see Viewing the Personalized Report, page 14-4.

This report summarizes all devices in your system that have been added or removed during the last 24 hours. The report content is described in the following table.

Report Element	Description/Action
Go to (list)	Select a section of the report to navigate to it: • Added Devices—Lists devices that have been added. • Removed Devices—Lists devices that have been removed
Added Devices	
Device Type	Type of device.
Device Name	IP address or DNS name.
IP Address	IP address of the device.
Status	State the device is in with respect to being monitored by Operations Manager: • Monitored • Partially Monitored • Monitoring Suspended • Inventory Collection in Progress • Unreachable • Unsupported For more information, see Understanding the Device Summary and Device States, page 16-14.
First Added	Date and time the device was first added to Operations Manager.
Last Discovered	Date and time that inventory collection last occurred on the device.

Report Element	Description/Action
Back to Top (link)	Click to return to the top of the report.
Removed Devices	
Device Type	Type of device.
Device Name	IP address or DNS name.
IP Address	IP address of the device.
Time	Date and time that the device was removed from Operations Manager.
Back to Top (link)	Click to return to the top of the report.

24-Hour Inventory Update Report—Phones

Note To launch this report, see Viewing the Personalized Report, page 14-4.

This report summarizes all IP phones in your system that have been added or removed in during the last 24 hours. The report content is described in the following table.

Report Element	Description/Action
Go to (list)	Select a section of the report to navigate to it: • Added Phones (Last 24 Hours)—Lists phones that have been added. • Removed Phones (Last 24 Hours)—Lists phones that have been removed.
Added Phones (Last 24 Hours)	
Extension	Extension number of the phone.
User	User identified by username, extension, or IP address.
IP Address	IP address for the phone.
MAC Address	MAC address for the phone.
Model	Cisco Unified IP Phone model number
Protocol	SCCP **Note** H.323 and MGCP protocols are not currently supported.
Status	
Regd	Whether the phone is registered to a Cisco Unified Communications Manager or Cisco Unified Communications Manager Express—yes or no.
CCM/CCE Address	Address of the Cisco Unified Communications Manager (CCM) or Cisco Unified Communications Manager Express (CCE) with which the IP phone is registered; for example, 10.76.38.70.
Switch Address	IP address of the switch to which the IP phone is connected; for example, 10.76.29.162.

Report Element	Description/Action
Switch Name	Name of the switch to which the IP phone is connected.
Port	Switch port used by the IP phone; for example, Fa0/12.
Port Status	Status of the port used by the IP phone; for example, static.
VLAN Name	Name of the VLAN (user-defined name); for example, voice.
VLAN ID	ID of the VLAN for the IP phone; for example, 100.
Back to Top (link)	Click to return to the top of the report.

Removed Phones (Last 24 Hours)

The Removed Phones section of the report contains the same fields as the Added Phones section of the report. See Added Phones (Last 24 Hours), page 14-12.

Scheduling and Exporting the Personalized Report

You must create a schedule for the Personalized Report, and optionally, you can export the data to disk.

Creating a Schedule and Optionally Exporting the Personalized Report

Step 1 Select **Reports > Personalized Report > Export**. The automatically Generate Personalized Report page appears.

Step 2 Enter the following:

- (Optional) Export as radio buttons—Select PDF or CSV or both.
- Run:
  - At—Select hour and minute from lists.
  - On—Select one: every day, Sun, Mon, Tue, Wed, Thu, Fri, Sat
- Location:

  Note Location is required only if you have selected export as PDF or CSV.

  - Enter a location including the drive and the folder. For example:

    ```
    C:\MyReport
    ```

  - Select the e-mail check box and enter a fully qualified e-mail address if you want to be notified when the report is created.

Step 3 Click **Apply**. The schedule is created. The Disable button appears.

Updating the Personalized Report Schedule and Export Options

Use this procedure to update the Personalized Report schedule and export options.

Step 1 Select **Reports > Personalized Report > Export**. The automatically Generate Personalized Report page appears.

Note The Apply button is disabled until you change any field on this page. You can update the Personalized Report schedule and export options even when the report is disabled (when the Enable button is active).

Step 2 Update any of the following:

- (Optional) Export as radio buttons—Select PDF or CSV or both.
- Run:
  - At—Select hour and minute from lists.
  - On—Select one: every day, Sun, Mon, Tue, Wed, Thu, Fri, Sat
- Location:

  Note Location is required only if you have selected export as PDF or CSV.

  - Enter a location including the drive and the folder. For example:

    ```
    C:\MyReport
    ```

  - Select the e-mail check box and enter a fully qualified e-mail address if you want to be notified when the report is created.

Step 3 Click **Apply**. The schedule and export options are updated and will be used as soon as possible. If the report is disabled (the Enable button is active), you must enable it to use the new schedule.

Enabling and Disabling the Personalized Report

Use this procedure to stop (disable) the Personalized Report and restart (enable) the report.

Note You cannot enable or disable the Personalized Report if you have not first scheduled it. See Scheduling and Exporting the Personalized Report, page 14-13.

Step 1 Select **Reports > Personalized Report > Export**. The automatically Generate Personalized Report page appears.

Step 2 Click the **Disable** or the **Enable** button.

Note Only one of these buttons is displayed. When you click Enable, the Disable button appears. Similarly, when you click Disable, the Enable button appears.

PART 5

Notification Services

CHAPTER 15

Using Notifications

Cisco Unified Operations Manager (Operations Manager) generates alerts in response to events that occur in the IP Telephony environment and the IP fabric. You can view alerts on Operations Manager dashboards, such as the Alerts and Events display. In addition, you can configure notifications to forward information about alerts and events to SNMP trap daemons on other hosts, syslog daemons, and users.

The following topics explain notifications concepts and provide procedures for managing notifications:

Understanding Notifications

This topic describes how Operations Manager determines when to send a notification and introduces the concepts that you need to be familiar with to configure notifications.

Note Notifications monitor events on device roles, not on device components. For a list of supported events and the device roles on which they can occur, see Appendix E, "Events Processed."

What Causes Operations Manager to Send Notifications?

For each alert or event, Operations Manager compares the event, devices, severity, and state against the configured notification groups and sends a notification when there is a match. Matches can be determined by user-configured event sets and notification criteria. (The procedure for configuring notification criteria is described in Configuring Notifications, page 15-7.)

Operations Manager assigns one severity to each alert or event and changes the state of an alert or event over time, responding to user input and changes on the device. Table 15-1 on page 15-2 lists values for severity and explains how the state of an alert or event changes over time.

Note You can change event names to names that are more meaningful to you. You can also change the event severity sent in notifications from the Operations Manager default value to a user-defined value. See Customizing Events, page 15-23.

Table 15-1 Alert and Event Severity and Status

Operations Manager categorizes alerts and events by severity and status…	
Severity	Critical Warning Informational
Status	Active—The alert or event is live. Acknowledged—A user has manually acknowledged the alert. A user can acknowledge only active alerts or events. Cleared—The alert or event is no longer active. **Note** Alerts or events that have been cleared either expire or, if associated with a suspended device, remain in Operations Manager until a user resumes or deletes the device.

What Are Notification Groups?

A notification group is a user-defined set of rules for generating and sending notifications. A notification group includes:

- Notification criterion—A named set of reasons to generate a notification.
- Notification type—The type of notification to send: SNMP trap, e-mail, or syslog.
- Notification recipients—Hostnames and ports for systems that listen for SNMP traps, syslog messages, or e-mail addresses.
- Daily subscription activity period—The hours during which Operations Manager should use this subscription while monitoring the alerts and events for which to send notifications.

What Are Notification Criteria?

Notification criteria define what you want to monitor for the purpose of sending notifications. A notification criterion is a user-defined, named set of devices or phones, and alerts and events of a particular severity and status. You must specify notification criteria to configure a notification group.

Operations Manager supports two types of notification criteria:

- Device-Based Criteria—Includes the following:
  - Devices—The devices, device groups, or clusters that you want to monitor.
  - Event sets—(Optional). One or more groups of events that you want to monitor. See How Can I Limit Notifications to Those for Specific Events?, page 15-4.
  - Alert severity and status—One or more alert severity levels and status.
  - Event severity and status—One or more event severity levels and status.

Note You can also customize the names and severity of the device-based events displayed by Notifications. See Customizing Events, page 15-23.

- Service Quality-Based Criteria—Includes the following:
  - Phones, endpoints, or probes—Phones, call endpoints, or probes that you want to monitor.
  - Alert severity and status—One or more alert severity levels and status.
  - Event severity and status—One or more event severity levels and status.

  Note You cannot customize the names and severity of the Service Quality-based events displayed by Notifications.

  Service Quality-based criteria are useful when you have purchased a license for Service Monitor and configured Operations Manager as a trap receiver on Service Monitor. Service Quality-based criteria do not include events sets.
- Phone-Based Criteria—Includes the following:
  - Phones—Phones you want to monitor.
  - Alert severity and status—One or more alert severity levels and status.
  - Event severity and status—One or more event severity levels and status.

For additional information, please see the following topics:

- Configuring Event Sets, page 15-4
- Configuring Notifications, page 15-7

What Types of Notifications Can I Send?

Operations Manager provides three types of notification: SNMP trap, e-mail, and syslog. When you configure a notification group, you specify one or more types of notification to send and you must also specify recipients for each type of notification.

SNMP Trap Notifications

Operations Manager generates traps with information about the alert and the events that caused it. CISCO-EPM-NOTIFICATION-MIB defines the trap message format. For more information, see Appendix D, “Notification MIB.”

Note Using SNMP trap notification is different from forwarding raw traps to another server before they have been processed by Operations Manager. For information about the raw traps that Operations Manager can forward, see Appendix C, “Pass-Through and Unidentified Traps.”

E-Mail Notifications

Operations Manager generates e-mail messages containing information about the alert and the events that caused it. CISCO-EPM-NOTIFICATION-MIB defines the message, which is included in the e-mail in text format. When you create an e-mail subscription, you can choose whether to include the subject line only or the complete e-mail message.

Syslog Notifications

Operations Manager generates syslog messages that can be forwarded to syslog daemons on remote systems.

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

Which Systems and Users Can I Notify?

When you configure a notification group, you must specify recipients for each type of notification:

- SNMP trap—Send SNMP traps to a port number on which the host can receive traps. Operations Manager defaults to sending SNMP traps to the port 162. However, you can specify a different port.
- E-Mail—Send e-mail to one or more addresses.
- Syslog—Send syslog messages to a remote system on which the syslog daemon is configured to listen on a specified port. Operations Manager defaults to sending syslog messages to port 514. However, you can specify a different port.

How Can I Limit Notifications to Those for Specific Events?

In some cases, you might want to send notifications for only a subset of the events that Operations Manager monitors. You can set the events that are of interest to you when you define the notification criterion:

- Specify an event set for a device-based notification criterion. You can create as many events sets as you would like.
- Select the events that you want Operations Manager to monitor for Service Quality-based notification criteria. There are few Service Quality-based events and you can select among them when you add or edit Service Quality-based notification criteria.

Configuring Event Sets

Event sets enable you to group the events the you want Operations Manager to monitor for the purpose of sending notifications.

Step 1 Select **Notifications > Event Sets**. The Event Set page appears. The Event Set page displays the following information:

GUI Element	Description/Action
Check Box column	Select one check box to edit, delete, or view an event set.
Event Set column	Event set name.
Description column	Event set description.
Add button	Click to add an event set. See Adding and Editing an Event Set, page 15-5.
Edit button	Click to edit an event set. See Adding and Editing an Event Set, page 15-5.
Delete button	Click to delete an event set.
View button	Click to view an event set. See Viewing an Event Set, page 15-6.

You can use event sets to:

- Limit the number of events that Operations Manager notification monitors. When you do not use event sets, Operations Manager notification monitors all events to determine whether to send a notification.
- Aggregate the notifications that you want to send to different destinations. For example, you can create separate event sets for each of the following purposes:
  - Limit the amount of e-mail notification sent to specific individuals or departments to only those for certain events.
  - Write all occurrences of particular events to syslog.
  - Send SNMP traps when certain events occur.

When you create device-based notification criteria, you must include an event set as one of the criteria. The default event set, All_Events, includes all events.

For additional information, please see the following topic:

- Events Processed, page E-1

Adding and Editing an Event Set

Step 1 Select **Notifications > Event Sets**. The Event Set page appears, displaying the information in the following table.

GUI Element	Description/Action
Event Set column	Event set name.
Description column	Event set description.

Step 2 Do one of the following:

a. Click **Add**

b. Select a check box for an event set and click **Edit**.

Depending on your selection, the **Add Event Set** or **Edit Event Set** page appears.

Step 3 Edit the information on the page, described in the following table.

GUI Element	Description/Action
Event Set Name field	Event set name—Enter or edit the event set name.
Event Set Description field	Event set description—Optional. Enter a description.
Events table	
Number column	Numbers events serially from one.
Check box column	Select to add an event to the event set. Deselect to remove the event from the event set.
Event column	Event description.

Step 4 Click **OK** to save your changes.

For additional information, please see the following topic:

- Viewing an Event Set, page 15-6
- Events Processed, page E-1

Viewing an Event Set

Step 1 Select **Notifications > Event Sets**. The Event Set page appears, displaying the information in the following table.

GUI Element	Description/Action
Event Set column	Event set name.
Description column	Event set description.

Step 2 Select the check box for an event set and click **View**. The Event Set Summary dialog box appears, displaying the following information:

- Event Set Name—User-supplied name.
- Event Set Description—User-supplied description.
- Selected Events—List of events in the event set.

For additional information, please see the following topic:

- Events Processed, page E-1

Deleting an Event Set

Step 1 Select **Notifications > Event Sets**. The Event Set page appears, displaying the information in the following table.

GUI Element	Description
Event Set column	Event set name.
Description column	Event set description.

Step 2 Select the check box next to each event set that you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes** to confirm.

For additional information, please see the following topic:

- Events Processed, page E-1

Configuring Notifications

The Notification Groups page is where notification management activities take place. To open the Notification Groups page, select **Notifications > Notification Criteria**.

These topics explain the activities you can perform from the Notification Groups page:

- Adding and Editing Device Notification Groups, page 15-9
- Adding and Editing Service Quality Notification Groups, page 15-13
- Adding and Editing Phone Notification Groups, page 15-17
- Cloning a Notification Group, page 15-20
- Viewing Notification Group Configuration Details, page 15-21
- Deleting Notification Groups, page 15-21
- Suspending a Notification, page 15-21
- Resuming a Notification, page 15-22
- Mapping Device Types to Values that Display in Events Sent by Devices, page 15-22

Figure 15-1 shows an example of the Notification Groups page.

Figure 15-1 Notification Groups page

Table 15-2 describes the fields in the Notification Groups page.

Table 15-2 Fields on the Notification Groups Page

GUI Element	Description/Action
Check box column	Select one check box to edit or delete a notification.
Name column	Notification group name.
Devices/Device Groups	The devices, device groups, and clusters that are configured for the notification.
Events	The event sets that cause the notification to be sent.
Destinations	The type of notification that will be sent—e-mail, SNMP trap, or syslog message—and the hostnames and e-mail recipients it will be sent to. **Note** The information shown in the destination box is limited. If the information exceeds the limit, an ellipses (...) is displayed. The complete information will be shown in the tooltip.
Operating Interval	The hours of the day during which the subscription is active.
Status	The notification group status; can be any of the following: • Active—Operations Manager is using the notification group while monitoring alerts to determine when to send a notification. • Suspended—The notification has been manually suspended. Operations Manager will not use the notification group unless you resume it. • Inactive—During a period of the day when the notification group is not scheduled to be active.

Table 15-2 Fields on the Notification Groups Page (continued)

GUI Element	Description/Action
Filter drop-down menu/Filter button	Enables you to filter what is displayed on the Notifications Group page.
Add > Device-Based Criterion button	Click to add a device notification group. See Adding and Editing Device Notification Groups, page 15-9.
Add > Service Quality-Based Criterion button	Click to add a Service Quality notification group. See Adding and Editing Service Quality Notification Groups, page 15-13. **Note** A Service Quality-based criterion is useful only if you have purchased a license for Service Monitor.
Clone button	Starts the process of adding a notification group using a current notification group as a template. See Cloning a Notification Group, page 15-20. **Note** Cloning a phone-based notification group is not supported due to the maximum phone limit of 10,000.
Edit button	Click to edit a notification criterion. See Adding and Editing Device Notification Groups, page 15-9 and Adding and Editing Service Quality Notification Groups, page 15-13.
View button	Displays the Notification Group Summary page, where the configuration information for a notification group is displayed.
Suspend button	• Temporarily stops sending notifications to a host. • Temporarily stops sending notifications about a device group. **Note** Overrides scheduled notification's run time. See Suspending a Notification, page 15-21.
Resume button	• Start sending notifications to a host again. • Start sending notifications about a device group using a previously suspended notification. See Resuming a Notification, page 15-22.
Delete button	Click to delete a notification group. See Deleting Notification Groups, page 15-21.

Adding and Editing Device Notification Groups

This section describes the procedure for adding or editing a device notification group.

Note You can use existing notification groups as templates for creating new notification groups. For procedures, see Cloning a Notification Group, page 15-20.

Step 1 Select **Notifications > Notification Criteria**.

Step 2 Do one of the following:

- To add a new criterion, click **Add > Device-Based Criterion**.
- To edit an existing criterion, select the check box for a device notification group and click **Edit**.

Depending on your selection, the Add Device-Based Criterion page or Edit Device-Based Criterion page appears.

  - To add or edit clusters for Notification, select clusters (which are available under the Cisco Unified Communications Manager or Cluster group). The clusters have a VE- prefix in their names.
  - To add or edit phones (which are configured for the Diagnostics test), select phones under System Defined Groups\Phones with tests configured.

Step 3 Edit the information on the page, described in the following table.

Table 15-3 Device-Based Criterion

GUI Element	Description/Action
Device selector pane	Expand device group folders and select check boxes for one or more devices, device groups, or clusters. **Note** If you select a device group, the notification criterion will stay up-to-date when devices are added or deleted from Operations Manager *only* if you also select the Include updates to group membership check box, page 15-11.
Criterion Name field	Enter a name for the notification criterion.
Customer Identification field	Enter any desired identifying information. If you leave this field empty, it is displayed in notifications as follows: • In e-mail and syslog notifications, it is left blank. • In SNMP trap notifications, it is displayed as follows: `Customer ID: -`
Customer Revision field	Enter any desired identifying information. If you leave this field empty, it is displayed in notifications as follows: • In e-mail and syslog notifications, it is left blank. • In SNMP trap notifications, it is displayed as follows: `Customer Revision: *`
Alert Severity check boxes	Select none, one, or more of the following: • Critical. • Warning. • Informational.
Alert Status check boxes	Select none, one, or more of the following: • Active. • Acknowledged. • Cleared.
Event Set Type list box	Select one.

Table 15-3 Device-Based Criterion (continued)

GUI Element	Description/Action
Event Severity check boxes	Select none, one, or more of the following: • Critical. • Warning. • Informational.
Event Status check boxes	Select none, one, or more of the following: • Active. • Acknowledged. • Cleared. **Note** If you select the Cleared check box, you must also select the Informational check box in the Event Severity field. If you do not select the Informational check box, the cleared events will not be forwarded.
Include updates to group membership check box	When selected, if devices are added to or deleted from Operations Manager, the devices are also added to or deleted from the notification criterion. This happens when the notification criterion includes a device group that the devices belong to. Deselect to maintain a static list of devices for any device groups included in the notifications criterion.

Step 4 Click **Next**. The Destination: Edit Device-Based Criterion page appears.

Step 5 Edit the information on this page as described in the following table.

Table 15-4 Edit Device Criteria

GUI Element	Description/Action
Always Active check box	Schedules the notification group to always be active.
Active From: To: fields	Select the hours of the day during which you want this notification group to be active: • From: HH:MM—Select hour and minute that the subscription becomes active. • To: HH:MM—Select the last hour and minute during which the subscription is active. By default, the values are from *00:00* to *00:00* and the subscription is active for 24 hours. **Note** Use this field, for example, to send e-mail notifications to a pager during one shift and not during another.
Include Link to Notification Details check box	Select to include URLs in the notification from which users can directly open the relevant page in Operations Manager for more information. Deselect to omit URLs from notifications.

Table 15-4 Edit Device Criteria (continued)

GUI Element	Description/Action
Subscription Type radio buttons	Select one at a time to enter data for each subscription type that you want to include in this subscription: • Trap—Enter data in the Trap Subscription Type fields, page 15-12. • E-Mail—Enter data in the E-Mail Subscription Type fields, page 15-12. • Syslog—Enter data in the Syslog Subscription Type fields, page 15-12. **Note** Operations Manager does not save the data you enter until you click **Finish** on the Subscription: Summary page. To go to the Subscription: Summary page, click **Next**.
Trap Subscription Type fields	
Hostname editable column	Enter an IP address or DNS name for the host.
Port editable column	Enter a port number on which the host can receive traps. If the port number is left unspecified (empty), the port defaults to 162.
Comments editable column	(Optional) Enter a comment.
E-Mail Subscription Type fields	
SMTP Server field	Enter a fully qualified DNS name or IP address for a Simple Mail Transfer Protocol (SMTP) server. (The name of the default SMTP server might already be displayed.) **Note** To select from any nondefault SMTP servers in use by existing subscriptions, click the SMTP Servers button. **Note** For instructions on how to configure a default SMTP server, see the Setting System-Wide Parameters Using System Preferences, page 20-9.
Sender Address field	Enter the e-mail address that notifications should be sent from. If the sender's e-mail service is hosted on the SMTP server specified, you need enter only the username. You do not need to enter the domain name.
Recipient Address(es) field	Enter one or more e-mail addresses that notifications should be sent to, separating multiple addresses with either a comma or a semicolon. If a recipient's e-mail service is hosted on the SMTP server specified, you need to enter only the username. You do not need to enter the domain name.
Subject Only check box	Select to include only the subject in the e-mail message. Deselect to send a fully detailed e-mail message (default).
Syslog Subscription Type fields	

Table 15-4 Edit Device Criteria (continued)

GUI Element	Description/Action
Facility list	Select a facility from the list (the default is Local Use 0). The Facility field and the event/alert severity are used for the PRI portion of the syslog message, as follows: [*Facility**8][*Severity*] Event/alert severity values are as follows: • Critical = 2 • Warning = 4 • Informational = 6
Location field	(Optional) Enter location information (up to 29 characters). This information will be populated in the syslog message.
Hostname editable column	Enter an IP address or DNS name for the host.
Port editable column	Enter a port number on which the syslog daemon is listening. If the port number is left unspecified (empty), the port defaults to 514. **Note** The syslog daemon on the remote system (hostname) must be configured to listen on a specified port.
Comments editable column	(Optional) A comment.

Step 6 Click **Next**. The Notification Group Summary page appears, displaying all information entered on the previous page.

Step 7 Click **Finish**. The notification information is saved.

Adding and Editing Service Quality Notification Groups

This section describes the procedure for adding or editing a service quality notification group.

Note You can use existing notification groups as templates for creating new notification groups. For procedures, see Cloning a Notification Group, page 15-20.

Step 1 Select **Notifications > Notification Criteria**.

Step 2 Do one of the following:

- To add a new group, click **Add > Service Quality-Based Criterion**.
- To edit an existing group, select the check box next to a service quality notification group and click **Edit**.

Depending on your selection, the Add Service Quality-Based Criterion page or Edit Service Quality-Based Criterion page appears.

Step 3 Edit the information on the page, described in the following table.

Table 15-5 Service Quality-Based Criterion

GUI Element	Description/Action
Notification Criterion field	Enter a name for the notification criterion.
Destination fields	To generate notifications for alerts and events on call destinations, do the following: 1. Select an operator (Is Exactly, Contains, Begins With, Any). 2. Enter an appropriate value: Phone extension or IP address for an endpoint, such as a voice gateway or a phone.
Source fields	To generate notifications for alerts and events on call sources, do the following: 1. Select an operator (Is Exactly, Contains, Begins With, Any). 2. Enter an appropriate value: Phone extension or IP address for a voice gateway or a phone.
Sensor MAC fields	To generate notifications for alerts and events on particular Cisco 1040 Sensors, do the following: 1. Select an operator (Is Exactly, Contains, Begins With, Any). 2. Enter the MAC address for a Cisco 1040 Sensor.
Cluster ID fields	To generate notifications for alerts and events from a particular cluster, do the following: 1. Select an operator (Is Exactly, Contains, Begins With, Any). 2. Enter the cluster ID.
Listener or Speaker Phone Model lists	To generate notifications for alerts and events on particular phone models, enter a comma-separated list of Cisco Unified IP Phone models or select them from a list: 1. Click the icon to open a selector. 2. Select a phone model from the list. To select more than one phone model, hold down **Ctrl** while selecting. 3. Click **OK**.
Alert Severity check boxes	Select any: • Critical. • Warning. • Informational.
Alert Status check boxes	Select any: • Active. • Cleared.
Event Severity check boxes	Select any: • Critical. • Warning. • Informational.

Table 15-5 Service Quality-Based Criterion (continued)

GUI Element	Description/Action
Event Status check boxes	Select any: • Active. • Cleared. **Note** If you select Cleared, you must also select the Informational check box in the Event Severity field. If you do not select the Informational check box, the cleared events will not be forwarded. For more information about event status, see Using the Service Quality Alert Details Display, page 4-6.
Event Description check boxes	Select any: • Critical Service Quality Issue. • Multiple Service Quality Issues. • Service Quality Issue. • Cisco 1040 Sensor Down. **Note** For more information about these events, see Events Processed, page E-1.
Cause check boxes	Select any: • Jitter. • Packet Loss.

Step 4 Click **Next**. The Destination: Edit Qov Criteria page appears.

Step 5 Edit the information on this page as described in the following table.

Table 15-6 Edit Quality-Based Criteria

GUI Element	Description/Action
Always Active check box	Schedules the notification group to always be active.
Active From: To: fields	Select the hours of the day during which you want this subscription to be active: • From: HH:MM—Select hour and minute that the subscription becomes active. • To: HH:MM—Select the last hour and minute during which the subscription is active. By default, the values are from *00:00* to *00:00* and the subscription is active for 24 hours. **Note** Use this field, for example, to send e-mail notifications to a pager during one shift and not during another.
Include Link to Notification Details check box	Select to include URLs in the notification from which users can directly open the relevant page in Operations Manager for more information. Deselect to omit URLs from notifications.

Table 15-6 Edit Quality-Based Criteria (continued)

GUI Element	Description/Action
Subscription Type radio buttons	Select one at a time to enter data for each subscription type that you want to include in this subscription: • Trap—Enter data in the Trap Subscription Type fields, page 15-16. • E-Mail—Enter data in the E-Mail Subscription Type fields, page 15-16. • Syslog—Enter data in the Syslog Subscription Type fields, page 15-16. **Note** Operations Manager does not save the data you enter until you click **Finish** on the Subscription: Summary page. To go to the Subscription: Summary page, click **Next**.
Trap Subscription Type fields	
Hostname editable column	Enter an IP address or DNS name for the host.
Port editable column	Enter a port number on which the host can receive traps. If the port number is left unspecified (empty), the port defaults to 162.
Comments editable column	(Optional) Enter a comment.
E-Mail Subscription Type fields	
SMTP Server field	Enter a fully qualified DNS name or IP address for a Simple Mail Transfer Protocol (SMTP) server. (The name of the default SMTP server might already be displayed.) **Note** To select from any nondefault SMTP servers in use by existing subscriptions, click the SMTP Servers button. **Note** For instructions on how to configure a default SMTP server, see the Setting System-Wide Parameters Using System Preferences, page 20-9.
Sender Address field	Enter the e-mail address that notifications should be sent from. If the sender's e-mail service is hosted on the SMTP server specified, you need enter only the username. You do not need to enter the domain name.
Recipient Address(es) field	Enter one or more e-mail addresses that notifications should be sent to, separating multiple addresses with either a comma or a semicolon. If a recipient's e-mail service is hosted on the SMTP server specified, you need to enter only the username. You do not need to enter the domain name.
Subject Only check box	Select to include only the subject in the e-mail message. Deselect to send a fully detailed e-mail message (default).
Syslog Subscription Type fields	

Table 15-6 Edit Quality-Based Criteria (continued)

GUI Element	Description/Action
Facility list	Select a facility from the list (the default is Local Use 0). The Facility field and the event/alert severity are used for the PRI portion of the syslog message, as follows: [*Facility**8][*Severity*] Event/alert severity values are as follows: • Critical = 2 • Warning = 4 • Informational = 6
Location field	(Optional) Enter location information (up to 29 characters). This information will be populated in the syslog message.
Hostname editable column	Enter an IP address or DNS name for the host.
Port editable column	Enter a port number on which the syslog daemon is listening. If the port number is left unspecified (empty), the port defaults to 514. **Note** The syslog daemon on the remote system (hostname) must be configured to listen on a specified port.
Comments editable column	(Optional) A comment.

Step 6 Click **Next**. The Notification Group Summary page appears, displaying all information entered on the previous page.

Step 7 Click **Finish**. The notification information is saved.

Adding and Editing Phone Notification Groups

This section describes the procedure for adding or editing a phone notification group.

Note The maximum number of phone notification groups allowed is five, and each notification group can contain a maximum of 2,000 phones. Cloning a phone notification group is not supported due to the maximum phone limit of 10,000.

Step 1 Select **Notifications > Notification Criteria**.

Note When Phone-Based Notification Criteria > Phone Report displays, each phone displays two phone entries (which contain two Directory Numbers/Extension Numbers (DNs). To leverage a phone count of 10,000, select one of the two entries.

Step 2 Do one of the following:

- To add a new criterion, click **Add > Phone-Based Criterion**.
- To edit an existing criterion, select the check box for a phone notification group and click **Edit**.

Depending on your selection, the Phone-Based Criterion page or Edit Phone-Based Criterion page appears.

  - To add or edit clusters for Notification, select clusters (which are available under the Cisco Unified Communications Manager or Cluster group). The clusters have a VE- prefix in their names.
  - To add or edit phones (which are configured for the Diagnostics test), select phones under System Defined Groups\Phones with tests configured.

Step 3 Edit the information on the page, described in the following table.

Table 15-7 Phone-Based Criterion

GUI Element	Description/Action
Criterion Name field	Enter a name for the notification criterion.
Unified CM/Unified CM Express-Based Event Threshold	Enter a value for the Unified CM/Unified CM Express-Based Event Threshold. The value should be between 1 and 20. The default value is 5. If the unregistered count of the phone selected in this notification group is more than the Unified CM/Unified CM Express-based event threshold, then a group event for the Unified Communications Manager (PhonesUnregisteredThresholdBased) will be created. If it is less than the threshold, an individual PhoneUnregistered event is created. **Note** Operations Manager displays the MAC address of the phone under the cenEventIdList for the PhoneUnregistered event trap notification (Phone Notification). The same traps used for the Phone Notification traps are used in the CISCO-EPM-Notification events.
Select Phones	Click **Add From Phone Report** to display a phone report. Selected phones will display in this text area. **Note** Adding more than five phone notification groups and adding the same phone to more than one phone notification group is not recommended.
Add From Phone Report button	Displays the All IP Phones/Lines report, from which you can select phones for your criterion. The maximum number of phones per phone-based notification group is 2,000.

Step 4 Click **Next**. A page displays the number of phones selected.

Step 5 Click **OK**. The Destination: Add or Edit Phone-Based Criterion page appears.

Step 6 Edit the information on this page as described in the Table 15-8 on page 15-19.

Table 15-8 Edit Phone Criteria

GUI Element	Description/Action
Always Active check box	Schedules the notification group to always be active.
Active From: To: fields	Select the hours of the day during which you want this notification group to be active: • From: HH:MM—Select hour and minute that the subscription becomes active. • To: HH:MM—Select the last hour and minute during which the subscription is active. By default, the values are from *00:00* to *00:00* and the subscription is active for 24 hours. **Note** Use this field, for example, to send e-mail notifications to a pager during one shift and not during another.
Subscription Type radio buttons	Select one at a time to enter data for each subscription type that you want to include in this subscription: • Trap—Enter data in the Trap Subscription Type fields, page 15-12. • E-Mail—Enter data in the E-Mail Subscription Type fields, page 15-12. • Syslog—Enter data in the Syslog Subscription Type fields, page 15-12. **Note** Operations Manager does not save the data you enter until you click **Finish** on the Subscription: Summary page. To go to the Subscription: Summary page, click **Next**.
Trap Subscription Type fields	
Hostname editable column	Enter an IP address or DNS name for the host.
Port editable column	Enter a port number on which the host can receive traps. If the port number is left unspecified (empty), the port defaults to 162.
Comments editable column	(Optional) Enter a comment.
E-Mail Subscription Type fields	
SMTP Server field	Enter a fully qualified DNS name or IP address for a Simple Mail Transfer Protocol (SMTP) server. (The name of the default SMTP server might already be displayed.) **Note** To select from any nondefault SMTP servers in use by existing subscriptions, click the SMTP Servers button. **Note** For instructions on how to configure a default SMTP server, see the Setting System-Wide Parameters Using System Preferences, page 20-9.
Sender Address field	Enter the e-mail address that notifications should be sent from. If the sender's e-mail service is hosted on the SMTP server specified, you need enter only the username. You do not need to enter the domain name.

Table 15-8 Edit Phone Criteria (continued)

GUI Element	Description/Action
Recipient Address(es) field	Enter one or more e-mail addresses that notifications should be sent to, separating multiple addresses with either a comma or a semicolon. If a recipient's e-mail service is hosted on the SMTP server specified, you need to enter only the username. You do not need to enter the domain name.
Subject Only check box	Select to include only the subject in the e-mail message. Deselect to send a fully detailed e-mail message (default).
Syslog Subscription Type fields	
Facility list	Select a facility from the list (the default is Local Use 0). The Facility field and the event/alert severity are used for the PRI portion of the syslog message, as follows: [*Facility**8][*Severity*] Event/alert severity values are as follows: • Critical = 2 • Warning = 4 • Informational = 6
Location field	(Optional) Enter location information (up to 29 characters). This information will be populated in the syslog message.
Hostname editable column	Enter an IP address or DNS name for the host.
Port editable column	Enter a port number on which the syslog daemon is listening. If the port number is left unspecified (empty), the port defaults to 514. **Note** The syslog daemon on the remote system (hostname) must be configured to listen on a specified port.
Comments editable column	(Optional) A comment.

Step 7 Click **Next**. The Notification Group Summary page appears, displaying all information entered on the previous page.

Step 8 Click **Finish**. The notification information is saved.

Cloning a Notification Group

You can use existing notification groups as templates for creating new notification groups.

Caution Cloning a phone notification group is not supported due to the maximum phone limit of 10,000.

Step 1 Select **Notifications > Notification Criteria**. The Notification Groups page appears.

Step 2 Select the check box next to the notification group that you want to use as the base for your new notification group.

Step 3 Click **Clone**. Depending on your selection, the Clone Device-Based Criterion or Clone Service Quality-Based Criterion page appears.

The rest of the procedures for cloning a notification group are the same as when a notification group is edited. For further instructions, see the following:

- Adding and Editing Device Notification Groups, page 15-9
- Adding and Editing Service Quality Notification Groups, page 15-13

Viewing Notification Group Configuration Details

Step 1 Select **Notifications > Notification Criteria**. The Notification Groups page appears.

Step 2 Select the check box next to a notification group.

Step 3 Click **View**. The Notification Group Summary page appears, displaying the following information:

- Notification Name.
- Notification Group Details—Alert, event, and device type information.
- Destination Details—Trap, e-mail, or syslog destination information.

Deleting Notification Groups

Step 1 Select **Notifications > Notification Criteria**. The Notification Groups page appears.

Step 2 Select the check box next to each notification group that you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes** to confirm.

Suspending a Notification

After you suspend a notification, Operations Manager stops using it until you resume it (see Resuming a Notification, page 15-22).

You can suspend a subscription and resume it at any time. You can also schedule a period during the day when you want a notification to be active. For more information, see Adding and Editing Device Notification Groups, page 15-9.

Note After suspending a notification, the suspend button may still appear enabled. You cannot suspend an already suspended notification. Clicking the Suspend button will have no effect on the notification. You should use the Notification Groups page to determine the status of a notification.

Use this procedure to suspend any type of notification: e-mail, SNMP trap, or syslog.

Step 1 Select **Notifications > Notification Criteria**. The Notifications Group page appears. Select the check box next to each notification group that you want to suspend.

Step 2 Click **Suspend**. A confirmation dialog box appears.

Step 3 Click **Yes** to confirm.

Resuming a Notification

You can resume a notification when its status is Suspended. After resuming a notification it will go into either active or inactive state depending on the time at which the notification group is resumed, and the time of day settings for that notification group.

Resuming a notification group does not override its time of day settings. The group will resume to operate as it did before suspension.

Note You can resume a notification group only after it has been suspended (it is in the Suspended state). You cannot resume a notification group during its inactive time (it is in the Inactive state), even if the Resume button is enabled.

Use this procedure to resume a suspended notification of any type: e-mail, SNMP trap, or syslog.

Step 1 Select **Notifications > Notification Criteria**. The Notification Group page appears.

Step 2 Select the check box next to each notification group that you want to resume.

Step 3 Click **Resume**. A confirmation dialog box appears.

Step 4 Click **Yes** to confirm.

Mapping Device Types to Values that Display in Events Sent by Devices

The device types that appear in Operations Manager are listed in Table 15-9 on page 15-23. The device type seen in the device report is different from the device type seen in the notification. “Device Type” indicates the primary capability of a device in notifications, and is more granular than the device list information). These device types appear as “Device type (MANAGED OBJECT)”. For example, [12] cenAlarmEntry.cenAlarmManagedObjectClass.0 (OctetString): VoiceGateway .

For the most up-to-date list of devices, see the *Supported and Interoperable Devices and Software Table for Cisco Unified Operations Manager*.

The Device Type information is categorized into three types of notification:

- Device-Based Notification, page 15-23
- Service Quality-Based Notification, page 15-23
- Phone-Based Notification, page 15-23

Table 15-9 Notification Device Type Categories

Notification Category	Device Type[1]
Device-Based Notification	• Media Server • Voice Gateway • Router • IPPhone • Switch • Cisco Unified Communications Manager/Unified CM • PhoneAccessSwitch • IPCC • CUE/Unity Express • Customer Voice Portal • Gatekeeper • Cisco Unified Communications Manager or Cluster • Hub • Host • Firewall • MSFC • Bridge • RSM
Service Quality-Based Notification	• Endpoint • Phone
Phone-Based Notification	• IPPhone • Unified CM • Unified CM Express

1. Device types are transmitted directly from the devices and may be subject to change. Please see your device documentation for details if you do not understand your notification message.

Customizing Events

You can customize event description and event severity for any event that is displayed in Operations Manager.

Customizing events is described in the following sections:

- Where Customized Event Descriptions Are Displayed, page 15-24
- Where Customized Event Severity Is Displayed, page 15-24
- Customizing Event Description and Severity, page 15-24

- Restoring Default Event Descriptions and Severities, page 15-25

Where Customized Event Descriptions Are Displayed

When you customize an event description, the new description is reflected in all notifications—e-mail, SNMP traps, and syslog—and on all user interfaces. For example, customized event descriptions are displayed on the Alert Details page and in Alert History and Event History reports.

Note The Event Description filter window under **Reports > Alert and Event History > Device group** displays default event names. When the event report is launched, the customized name will be displayed. To determine the default name is for customized events, go to **Notifications ->Event Customization**.

Where Customized Event Severity Is Displayed

When you customize event severity, it is reflected in all notifications—e-mail, SNMP traps, and syslog. Operations Manager uses only the event severity levels in the following table.

Severity Level	Value that Operations Manager Defines	Value That Operations Manager Writes to Notifications	
		E-Mail and SNMP Traps	Syslog Messages
Critical	3	3	2
Warning	2	2	4
Informational	1	1	6

You can specify a customized event severity level between 1 and 8. When generating traps, the severity level you specify for the event is stored in the CISCO-EPM-NOTIFICATION-MIB and is sent in all notifications.

Note When you customize event severity, Operations Manager continues to process the event based on its default severity. Also, severity levels 4 through 8 are undefined in Operations Manager.

You can quickly and easily restore the default name and severity for any and all events.

Customizing Event Description and Severity

Note Default event names are displayed on the Event Customization page. For default event severity, locate the event in Events Processed, page E-1.

Step 1 Select **Notifications > Event Customization**. The Event Customization page appears, displaying the information shown in the following table.

GUI Element	Description/Action
Number column	Numbers events serially from one.
Check box column	Select to customize an event.
Event Code column	Code number for the event. This number cannot be changed and is used to map default names to customized names.
Default Description column	Default description for the event. This description is not editable.
Current Description column	This is an editable field. For more information, see Where Customized Event Descriptions Are Displayed, page 15-24.
Current Severity column	Select a severity for the event. For more information, see Where Customized Event Severity Is Displayed, page 15-24. **Note** For default event severity levels, locate the event in Events Processed, page E-1.

Step 2 For each event that you want to customize:

a. Select the check box.

b. Enter any changes in the following fields:

- **New Description**—Enter a new description.
- **New Severity—**Select a new severity level from 1 to 8.

Step 3 Click **OK** to save your changes and apply them.

Restoring Default Event Descriptions and Severities

Step 1 Select **Notifications > Event Customization**. The Notification Customization page appears, displaying the information shown in the following table.

GUI Element	Description/Action
Number column	Numbers events serially from one.
Check box column	Select: • The topmost check box to restore default description and severity to all events. • One or more check boxes in rows with events that you want restored to default description and default severity.
Event Code column	Code number for the event. This number cannot be changed and is used to map default names to customized names.
Default Description column	Default description for the event. This description is not editable.

GUI Element	Description/Action
Current Description column	This is an editable field. However, you do not need to enter any changes to restore the default description.
Current Severity column	This is an editable field. However, you do not need to select a value to restore the default severity. **Note** For default event severity levels, locate the event in Events Processed, page E-1.

Step 2 Select the check box for all events or select multiple check boxes for the events that you want to restore to default description and severity.

Step 3 Click **Restore Default Description**.

Step 4 Apply your changes by clicking **Yes** when the confirmation window appears.

For additional information, please see the following topics:

- Getting Alert and Event Details, page 3-9
- Events Processed, page E-1

PART 6

Device Management

CHAPTER 16

Using Device Management

These topics explain how to use Cisco Unified Operations Manager (Operations Manager) Device Management:

Getting Started with Device Management

For Operations Manager to monitor a device, it must first be added to the CiscoWorks Common Services Device and Credentials Repository (DCR). Once a device is added to the DCR, you can then add it to the Operations Manager inventory, which is separate from the DCR.

Note When Operations Manager is installed, it automatically synchronizes with the DCR and adds inventory. This is the default setting.

You can add devices automatically from the DCR to Operations Manager by activating automatic synchronization, or you can add them manually through the Device Selection page. For more information on how Operations Manager is affected by the DCR, see Understanding the Device and Credentials Repository, page 16-4.

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

Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as “C:\Program Files\CSCOpx” or C:\PROGRA~1\CSCOpx.

Using the Operations Manager device management pages, you can perform the following operations:

- Add or import devices into the DCR (see Adding Devices to the DCR, page 16-5, or Importing Devices into the DCR, page 16-11).

- Export device information to a file (see Exporting Device Information from the DCR to a File, page 16-12).
- Edit device configuration (see Editing Device Configuration and Credentials, page 16-30).
- Delete devices (see Deleting Devices, page 16-36).
- Select devices to be added to Operations Manager from the DCR (see Importing Devices from the DCR, page 16-16).
- View device details (see Viewing Device Details, page 16-32).
- Perform inventory collection on devices (see Performing Manual Inventory Collection on Devices, page 16-31).
- Suspend and resume Operations Manager device management (see Suspending/Resuming Devices, page 16-35).

As Operations Manager performs inventory collection on devices, they pass through various *device states* until they are fully recognized by Operations Manager (see Verifying Device Import, page 16-21 for details). Once a device is in Operations Manager inventory, Operations Manager monitors the device and its components according to the polling and threshold settings that apply to the device group (when it is added to the DCR, the DCR assigns the device to a device group).

Device Prerequisites

When working with device management, remember the following:

- If a monitored device is removed from the network, it will continue to be in the Monitored state until the next inventory collection occurs, even though the device is unreachable. The only way that you will know that this device is unreachable, is when an Unreachable alert appears for this device in the Alerts and Events display.
- Configuration changes on a device are discovered by Operations Manager only during the inventory collection process. Therefore any changes to a device's configuration will not be shown by Operations Manager until the next inventory collection after the configuration change.
- If Cisco Discovery Protocol (CDP) is not enabled on a media server (either it is disabled or not responding), Operations Manager will not discover the device correctly and the device will be moved to the Unsupported state.
- If the Operations Manager server is using Access Control Server (ACS) mode, ACS may limit the devices you are permitted to view. For more information, refer to Device-Based Filtering, page 20-22.
- When you add devices, the HTTP (and HTTPS) port numbers are optional. These settings are automatically detected.
- When you add devices that have multiple interfaces and HTTP administrative access, you must manage the device in Operations Manager using the same interface on which you have enabled HTTP administrative access.
- You must enter the Windows username and password when you add Cisco Unified Contact Center, Cisco Unity Connection, Cisco Unity, and Cisco Personal Assistant. These Windows credentials are entered in the Primary Credentials field in the DCR.

- To enable Operations Manager to provide the correct phone count for the Communications Manager Express and Cisco Unity Express (CUE), you must use the following configuration:

```
ephone 8
mac-address 001A.E2BC.3EFB
type 7945
```

  where type is equal to the phone model type. If you are unsure of your model type, see Cisco.com for details on all phone model types, or enter **type ?**.

  For information on how phone counts are displayed in Device Management Summary window, see How Are Phone Counts Displayed in Views and Reports?, page 1-19.

- Starting in release 2.1, for a Cisco Unity Express that is attached to a Unified Communications Manager Express to display in the Service Level View, you must use the following configuration:

```
dial-peer voice 2999 voip  <where voip tag 2999 must be different from voicemail>
destination-pattern 2105  <prefix must be the full E.164 of configured voicemail 2105>
session protocol sipv2
session target ipv4:10.10.1.121
dtmf-relay sip-notify
codec g711ulaw
no vad
!
!
telephony-service
voicemail 2105
```

  where the dial-peer VoIP tag, 2999, is not equal to the voicemail number, and the destination-pattern, 2105, is equal to the voicemail number. This will allow Unity Express to display properly in the Service Level View.

- In order to successfully receive Cisco Unified Communications Manager syslog messages, you must add the syslog receiver from the serviceability web page. See Configuring Syslog Receiver on Cisco Unified Communications Manager, page F-3

Operations Manager manages a device when the device's *management state* is set to True; conversely, Operations Manager does not manage a device when its management state is set to False. A device with a management state set to False is called a *suspended device*. You can also selectively unmanage device components (see Suspending/Resuming a Device Component, page 3-27).

For information on how many devices Operations Manager can manage, refer to *Installation Guide for* Cisco Unified Operations Manager. If the Operations Manager inventory exceeds your device limit, you will see a warning message. For more information, see Responding to Messages About Device Limits, page 1-24.

Types of Devices that Operations Manager Monitors

When devices are added to the DCR, they are assigned to Common Services System Defined Groups. The group to which the DCR assigns the device depends on the device type users specify when they add the device. If a user does not select a device type, or selects the wrong device type, the DCR designates the device as Unsupported, and it is assigned to the Common Services Unsupported group. (For devices with no specified device type, Operations Manager assigns a device type when it performs inventory collection on the device.)

For examples of the types of devices that Operations Manager monitors, see Table 17-1 on page 17-3.

Note For a detailed list of devices that Operations Manager supports, see *Supported Device Table for* Cisco Unified Operations Manager on Cisco.com at http://www.cisco.com/en/US/products/ps6535/products_device_support_tables_list.html.

Ports and Interfaces that Operations Manager Monitors

The following describes the default ports and interfaces that Operations Manager monitors or does not monitor:

- Ports (switches)—By default, Operations Manager monitors trunk ports but does not monitor access ports.
  - An access port is a switch port that is connected to a host or device that Operations Manager does not monitor; that is, an end-station port.
  - A trunk port is a port that connects to a Cisco network device running Cisco Discovery Protocol (CDP). In other words, a trunk port connects to a router, or to a switch that the same Operations Manager server manages.
- Interfaces (routers)—By default, Operations Manager monitors all interfaces listed in the ifTable.
  - During inventory collection only (by default), BRI B-Channel interfaces (for voice) are unmanaged.
  - During inventory collection only (by default), PRI B-Channel interfaces are unmanaged.

Understanding the Device and Credentials Repository

The DCR is a centralized device repository for sharing device information across applications. It provides a single place for managing device credentials and attributes, ensuring consistency across applications. Individual applications can query the DCR for a device list, device attributes, and device credentials. Changes to the DCR are propagated to all applications.

Note A device must be added to the DCR before it can be added to the Operations Manager inventory (see Adding Devices to the DCR, page 16-5).

Once a device is added to the DCR, you can add it to the Operations Manager inventory (the Operations Manager inventory is separate from the DCR). When a device is added to the DCR, the DCR assigns a DCR ID to every managed component.The DCR maps components to devices using either the device name or IP address. When the DCR device is added to Operations Manager, Operations Manager maps the DCR ID to a device name during inventory collection (see Table 16-3 on page 16-17).

Operations Manager also uses the DCR ID to verify if the device or component already exists in the Operations Manager inventory. (Further information on how Operations Manager identifies devices—such as whether Operations Manager uses an IP address or DNS name as the device name—is provided in Importing Devices from the DCR, page 16-16.)

You can add devices from the DCR to Operations Manager automatically by activating automatic synchronization (which is the default), or you can add them selectively by deactivating using the Device Selection page. When a device is deleted it may or may not be deleted from the DCR. Deletion is determined by how Operations Manager is configured with the DCR (see Deleting Devices, page 16-36).

For information on deleting components of aggregate devices, see How Operations Manager Handles Containing and Contained Devices, page 16-17.

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

- For automatic synchronization (this is the default), see Automatically Importing DCR Devices, page 16-18.
- For manual synchronization (in which you selectively add devices from the DCR to the Operations Manager inventory), see Manually Importing DCR Devices, page 16-19.

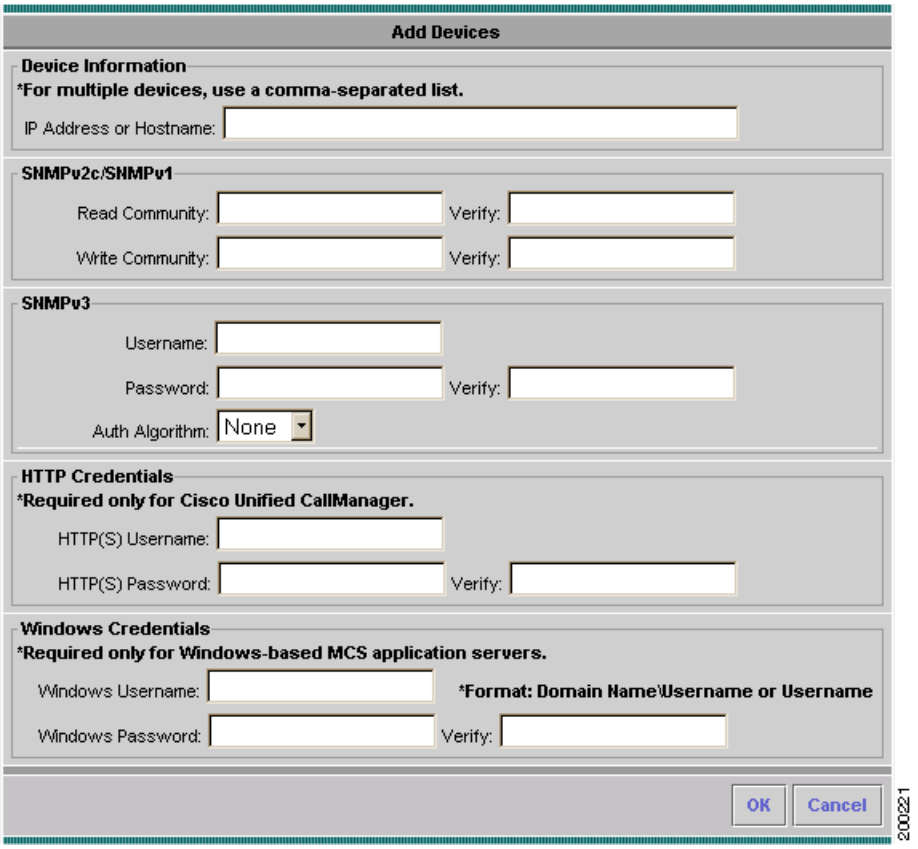
Note Do not confuse the Operations Manager physical discovery process (which adds devices to the DCR) or the Operations Manager inventory collection process (which probes devices and updates components in Operations Manager inventory) with the DCR synchronization process. Operations Manager inventory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

Adding Devices to the DCR

Add devices to the DCR from the Operations Manager Add Devices page (**Devices > Device Management > Add Devices**).

Figure 16-1 shows an example of the Add Devices page.

Figure 16-1 Add Devices Page



Note To add devices to the DCR using bulk import (importing from an NMS or from a file), see Importing Devices into the DCR, page 16-11.

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

Note You can also access the Add Devices page from the Discovered Devices report. (See Viewing the Discovered Devices Report, page 16-14.)

Step 2 Enter the following:

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

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

- SNMPv2c/SNMPv1 credentials
- SNMPv3 credentials
- HTTP credentials (only required for Cisco Unified Communications Manager)
- Windows credentials—Only required for the following devices:
  - Cisco Unified Contact Center
  - Cisco Unity
  - Cisco Unity Connection
  - Cisco Personal Assistant
  - Windows-based versions of Cisco Unified Communications Manager

Step 3 Click **OK**.

Creating a Read-Only Cisco Unified Communications Manager User Account for Polling

Depending on your software, perform one of the following procedures to create a read-only Cisco Unified Communications Manager user account:

- Creating a Read-Only Cisco Unified Communications Manager 4.x User Account (Windows), page 16-6
- Creating a Read-Only Cisco Unified Communications Manager 5.0 and Above User Account (Linux), page 16-6

Creating a Read-Only Cisco Unified Communications Manager 4.x User Account (Windows)

Use the following procedure to set up a read-only user account that allows polling of your Unified Communications Manager device (version 4.x).

Step 1 Create a new read-only user (for example, cuomuser) on the CCMAdmin Page, by selecting **Users > Add a new User**.

Step 2 Create a new user group that contains the new read-only user(for example, CUOM Access) by selecting **User Management > User Group**.

Step 3 Assign the new read-only user to a Read Only user group (CUOM Access) by selecting **Users > Access Rights > Assign Privileges to User Group**.

Step 4 Enable multi-level admin (MLA) on the Cisco Unified Communications Manager by selecting **Users > Access Rights > Configure MLA Parameters**.

Step 5 Restart the Tomcat Web Service on the Communications Manager by selecting **Cisco Unified CallManager Serviceability > Tools > Control Center**.

Step 6 Log into Operations Manager as the read-only user and add the Communications Manager by selecting **Devices > Device Management > Add Devices**.

Creating a Read-Only Cisco Unified Communications Manager 5.0 and Above User Account (Linux)

Use the following procedure to set up a read-only user account that allows polling of your Unified Communications Manager device (version 5.0 and above).

Procedure

Step 1 Create a new read-only user (for example, cuomuser) on the CCMAdmin page by selecting **User Management > Application User**.

Step 2 Create a new user group that contains the new read-only user (for example, CUOM Access) by selecting **User Management > User Group**.

Step 3 Assign the new read-only user to a read-only user group (CUOM Access) by selecting **Users > Access Rights > Assign Privileges to User Group**.

Step 4 Add the Standard AXL API Access role to the read-only user group by selecting **User Management > Role** from the CUCM Admin Page.

The CUOM Access group (or whatever name you assigned) should contain the following roles:
Standard AXL API Access
Standard CCM Admin Users
Standard CCMADMIN Read Only
Standard SERVICEABILITY Read Only

Step 5 Log into Operations Manager as the read-only user and add the Communications Manager by selecting **Devices > Device Management > Add Devices**.

Creating a Read-Only WMI User Account for Polling Cisco Unity Devices

In order to provide a safe and secure environment for files, such as polling logs, you must create a non-administrative user account to perform polling on Windows Management Instrumentation (WMI) for Unity devices.

Procedure

Step 1 Log in to the Unity server with an administrator account.

Step 2 Create a non-administrator or read-only user.

Step 3 Open the WMI Control console by clicking **Start**, click **Run**, type wmimgmt.msc, and then click **OK**.

Step 4 To set the permission for the user, right-click **WMI Control**, click on **Properties**, click on the **Security** tab.

Step 5 Select CIMV2 from namespace navigation window, click on **security**.

Step 6 To add the user just created, click **Add** (or select **Everyone** from the user name window).

Step 7 Select the following permissions from the permission window:

- Execute Method
- Enable Account
- Remote Enable
- Read Security

Step 8 Click **OK**, on the security and WMI control windows and close the WMI management window.

Configuring Operations Manager Physical Discovery

Procedure

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

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

Step 2 Click **Add**. The Configure Credentials page appears (see Configuring Credentials, page 16-8).

Step 3 Enter the following:

- Target devices wild card entry. Multiple devices can be entered at one time, using a comma-separated list.

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

- SNMP timeout and retries
- SNMPv2c/SNMPv1 credentials
- SNMPv3 credentials
- HTTP credentials (only required for Cisco Unified Communications Manager)
- WMI credentials—Only required for the following devices:
  - Cisco Unified Contact Center
  - Cisco Unity
  - Cisco Unity Connection
  - Cisco Personal Assistant

  - Windows-based versions of Cisco Unified Communications Manager

Configuring Credentials

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

Procedure

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

Step 2 Click **Add**.

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

Step 3 Enter the following:

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

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

- (Optional) Change the SNMP timeout and retries
- SNMPv2c/SNMPv1 credentials
- SNMPv3 credentials
- HTTP credentials (only required for Cisco Unified Communications Manager)
- Windows credentials—Only required for the following devices:
  - Cisco Unified Contact Center
  - Cisco Unity
  - Cisco Unity Connection
  - Cisco Personal Assistant
  - Windows-based versions of Cisco Unified Communications Manager

Step 4 Click **OK**.

Filtering Physical Discovery

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

Procedure

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

Step 2 Select *one* of the following options (Discovery or Filters):

- Select the **Discovery** radio button, then:
  - Select the **Cisco Discovery Protocol (CDP),** the **Use Logical Cluster Discovery** check box, or both, and do one of the following:

  a. Enter seed devices using a comma-separated list of IP addresses. The discovery is restricted to one cluster. If you want to perform discovery of multiple clusters, then enter the publisher address for all the clusters, separated by commas, in the Seed device text box.

  Note When using logical cluster discovery, the following types of devices are discovered:

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

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

  b. Select the **Use devices currently in the system** check box.

  Use devices currently in the system is enabled only if Use Cisco Discovery Protocol (CDP) or Use Logical Cluster Discovery is selected.

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

  When selecting the Use Ping Sweep check box, specify a comma-separated list of IP address ranges using the */netmask* specification. For example, use 172.20.57.1/24 to specify a ping sweep range starting from 172.20.57.1 and ending at 172.20.57.255.

  Note Ping sweep cannot be selected with CDP or cluster discovery.

4. Select the **Filters** radio button and enter the filter information. Table 16-1 describes the optional filters that are available to you when running physical discovery. Click **Advanced Filters** to display additional filter options.

Table 16-1 Physical Discovery Filters

Filter	Description
IP Address	(Optional) Enter comma-separated IP addresses or IP address ranges for devices that you want to: • Include—In the auto-discovery process. • Exclude—From the auto-discovery process. You can use wildcards when specifying the IP address range. An asterisk (*) denotes the octet range of 1-255. Also, the octet range can be constrained using the [xxx-yyy] notation. For example: • To include all devices in the 172.20.57/24 subnet in the auto-discovery process, enter an include filter of 172.20.57.*. • To exclude devices in the IP address range of 172.20.57.224 - 172.20.57.255 from the auto-discovery process, enter an exclude filter of 172.20.57.[224-255]. Both types of wildcards can be used in the same range specification; for example, 172.20.[55-57].*. If both include and exclude filters are specified, the exclude filter is applied first before the include filter. Once a filter is applied to an auto-discovered device, no other filter criterion will be applied to the device. If a device has multiple IP addresses, the device will be processed for auto-discovery as long as it has one IP address that satisfies the include filter.
Advanced Filters	
DNS Domain	(Optional) Enter comma-separated DNS domain names for devices that you want to: • Include—In auto-discovery processing. • Exclude—From auto-discovery processing. The DNS names can be specified using wildcards. An asterisk (*) matches any combination of mixed uppercase and lowercase alphanumeric characters, along with the hyphen (-) and underscore (_) characters, of an arbitrary length. A question mark (?) matches a single uppercase or lowercase alphanumeric character or a hyphen or an underscore character. For example: • *.*cisco.com* matches any DNS name ending with *.cisco.com.* • *.*?abc.com* matches any DNS name ending with *.aabc.com*, or *.babc.com*, etc.

Table 16-1 Physical Discovery Filters (continued)

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

Step 3 In the Run pane, specify when physical discovery should run.

- If you want physical discovery to run immediately, select the **now** radio button.
- If you want to schedule physical discovery to run at certain intervals, do one of the following:
  - Select **daily**; enter the time and select the days on which physical discovery should run.
  - Select the **every** radio button; choose how often you want physical discovery to run, then enter the time and select the day on which physical discovery should run.
- If you want cancel a physical discovery that is scheduled to run in the future, select the **disable** radio button.

Step 4 Click **OK**.

Importing Devices into the DCR

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

Procedure

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

Step 2 Enter the import information.

Note To import devices successfully into Operations Manager, the input import CSV file should have Read permission for the USERS group. When importing the CSV file from another directory, ensure that you have casuser permission on the file or import the CSV file directly from the CSCOpx directory. If you need help importing, click the Help button on the page, and the Common Services online help opens.

Tip When you export the devices from Operations Manager, the user permissions to the .csv file are set such that when you import the same file, Operations Manager cannot accept it. Instead, import a copy of the same .csv file, because the permissions are correctly set.

Exporting Device Information from the DCR to a File

To export device information to a file, Operations Manager provides you a direct link to the DCR.

Procedure

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

Step 2 Enter the export information.

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

Tip When you export the devices from Operations Manager, the user permissions to the .csv file are set such that when you import the same file, Operations Manager cannot accept it. Instead, import a copy of the same .csv file, because the permissions are correctly set.

Events that Trigger DCR and Operations Manager Synchronization

The following events will trigger synchronization between the Operations Manager inventory and the DCR:

- Devices are added or deleted, or their credentials (IP address, SNMP credentials, MDF type) are changed in the DCR. (This also triggers a device inventory collection in Operations Manager).
- DCR is changed from:
  - Master to slave
  - Standalone (single server) to slave
- DCR is restored from a different domain.

See these topics for more information:

- Importing Devices from the DCR, page 16-16
- Determining the Media Server Account to Use for Cisco Unified Communications Manager Access, page 16-39

DCR Masters and Slaves

By default, the DCR mode is standalone (single server), and one DCR is supported per server. However, you can configure the DCR to use a master/slave model. In this model, the master DCR is the primary repository residing on a CiscoWorks server. Slave DCRs reside on other CiscoWorks servers, and replicate the DCR master. Any change in the master DCR is propagated to slave DCRs. This allows applications on different servers to use a synchronized device inventory. Using the master/slave model is transparent to Operations Manager.

If the DCR used by your instance of Operations Manager is changed from master to slave, or from standalone to slave, the DCR device list is synchronized with the Operations Manager inventory. First, all devices are removed from the Operations Manager inventory (regardless of DCR synchronization mode). If Operations Manager is configured to use manual synchronization, all DCR devices will appear in the Device Selector (as devices that are not in Operations Manager). For automatic synchronization, all DCR devices are added to the Operations Manager inventory.

Note Whenever the DCR mode is changed (to or from master, slave, or standalone) you must perform a daemon manager restart. Run the following commands:

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

For more information on the DCR master/slave model, refer to the Common Services online help.

Masters and Slaves Configuration for Manual Mode

This section describes the procedures you must perform if you are going to use Operations Manager in a master and slave configuration with manual device selection configured in Operations Manager.

Step 1 In the Device Selection page, set device selection to manual. (See Manually Importing DCR Devices, page 16-19.)

Step 2 Configure Operations Manager as a slave server. (For information on configuring the DCR master/slave model, refer to the Common Services online help.)

All the devices will be present in the local DCR and not in Operations Manager.

Step 3 In the Device Selection page, select the **Manual** radio button.

The CS tree will contain all the devices that are present in the master server. This allows you to select all the devices that are not present in Operations Manager.

Viewing the Discovered Devices Report

The Discovered Devices report lists all the devices that Operations Manager has discovered. It also enables you to select the devices that you want to add to the DCR.

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

Step 2 Next to the Last Discovery field, click **View Report**. The Discovered Devices report opens.

The report lists the following:

- IP address of the device.
- Device Name—This field is populated when a DNS Domain filter is set during discovery configuration. If a DNS Domain filter is not specified, the device name field displays *not available*.
- Has Credentials—Either *True* or *False* appears. This is based on whether discovery was able to discover the credentials.
- Status of the device—There are three possible values: Added to Operations Manager, Updated in Operations Manager, Unreachable.

Note The Add button at the bottom of the report enables you to add the devices that you have selected to the DCR.

Understanding the Device Summary and Device States

The Device Management: Summary page lists the device states for all devices in the Operations Manager inventory. The Device Management: Summary page appears when you select **Devices > Device Management**. Figure 16-2 shows an example of the Device Management: Summary page.

Figure 16-2 Device Management: Summary Page

Table 16-2 describes the information displayed on the Device Management: Summary page.

Table 16-2 Device Management: Summary Page

Heading/Button	Description	
State	Lists the state the devices are in, from the following possibilities:	
	Monitored	The device has been successfully imported, and is fully managed by Operations Manager.
	Partially Monitored	The device has been successfully imported by some of the data collectors[1] in Operations Manager, but not all. If a device is in this state, you should take action to ensure that the device becomes monitored.
	Monitoring Suspended	Monitoring of the device is suspended.
	Inventory Collection in Progress	Operations Manager is probing the device. This is the beginning state, when the device is first added; a device is also in this state during periodic inventory collection. Some of the data collectors may still be gathering device information.
	Unreachable	Operations Manager cannot manage the device. See Troubleshooting Import and Inventory Collection, page 16-22.
	Unsupported	The device is not supported by Operations Manager.
	NA	When there is no Unity Express in the Communications Manager Express cloud, the Unity Express state displays NA.
Total Devices	The number of devices that are in each device state. The blue numbers are links to device reports. When you click a blue number a device report for that specific device state opens. See Understanding Device Reports, page 16-33.	
Total Phones	The number of phones monitored. The blue number links to the All IP Phones/Lines report. See Understanding IP Phone Inventory Reports, page 13-11.	
Device Selection	The current mode for device selection from the DCR. See Importing Devices into Operations Manager, page 16-16.	
Last Discovery	The date and time when last performed physical discovery.	
Next Discovery	The date and time when will next perform physical discovery.	
Configure	To configure physical discovery. See Adding Devices to the DCR, page 16-5.	

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

Importing Devices into Operations Manager

A device must be in the Device and Credentials Repository (DCR) before you can add it to the Operations Manager inventory (see Adding Devices to the DCR, page 16-5). Operations Manager supports two methods of device import from the DCR:

- Using automatic synchronization between the DCR and Operations Manager (see Automatically Importing DCR Devices, page 16-18)

- Using manual synchronization between the DCR and Operations Manager (see Manually Importing DCR Devices, page 16-19)

Note To import devices successfully into Operations Manager, the input import CSV file should have Read permission for the USERS group. When importing the CSV file from another directory, ensure that you have casuser permission on the file or import the CSV file directly from the CSCOpx directory.

Importing Devices from the DCR

Once a device has been added to the DCR, it can be added to the Operations Manager inventory:

- Automatically (whenever there is an addition or change), if Device Selection is set to automatic in the Device Management: Summary page.
- Manually (on a device-by-device basis), if Device Selection is set to Manual in the Device Management: Summary page.

To verify which setting you are using, select **Devices > Device Management**, and check the Device Selection setting.

Note Your login determines whether you can import devices into Operations Manager.

How Operations Manager Identifies Devices Imported from the DCR

When a device is added to Operations Manager from the DCR, Operations Manager attempts to resolve the DNS name (hostname). Operations Manager does not use the DCR Display Name. Table 16-3 shows how Operations Manager names devices, depending on how the devices are added to the DCR.

Table 16-3 How Operations Manager Determines Device Names

When device is added to DCR with...	Operations Manager does the following:
IP address and hostname (DNS name)	• Uses the DNS name, if Operations Manager can resolve it • Uses the IP address, if Operations Manager cannot resolve the DNS name
IP address only	• Uses the DNS name, if Operations Manager can resolve the IP address • Uses the IP address, if Operations Manager cannot resolve the DNS name
DNS name only	Uses the DNS name, even if not resolvable
IP address, and the IP address was already added to the DCR (this is allowed in the DCR)	Chooses one IP address and the other becomes a duplicate. For details on how to determine if you have duplicate devices, see Viewing the IP Address Report Page, page 16-20.
IP address, and the IP address corresponds to two interfaces of the same physical device	Chooses one IP address and the other becomes a duplicate. For details on how to determine if you have duplicate devices, see Viewing the IP Address Report Page, page 16-20.

Note Once a device is added to the DCR with a specified MDF type and sysUnified Communications ID, no one can overwrite it, even if it is incorrect. The only exception is if no sysUnified Communications ID is supplied, as described in the previous table.

For information on how Operations Manager performs polling and discovery, see Appendix G, "Polling—SNMP and ICMP."

How Operations Manager Handles Containing and Contained Devices

Operations Manager supports contained and containing devices (also referred to as aggregate devices). These are devices that have a parent/child relationship with another device, such as a Catalyst switch (parent) containing an MSFC (child). The switch is considered the containing device, and the MSFC is the contained device.

Table 16-4 How Operations Manager Handles Containing and Contained Devices

Action	Effect on Device	
	Containing	Contained
Adding to Operations Manager (regardless of DCR synchronization mode)		
Containing	Added	Added[1]
Contained	N/A	N/A
Inventory Collecting in Operations Manager		
Containing	Inventory collected	Inventory collected
Contained	No effect	Inventory collected
Removing from Operations Manager		
Containing	Deleted	Deleted from Operations Manager (but not deleted from DCR)
Contained	No effect	Deleted
Removing from DCR		
Containing	Deleted	Deleted
Contained	No effect	Deleted
Suspending in Operations Manager		
Containing	Suspended	Suspended
Contained	No effect	Suspended
Resuming in Operations Manager		
Containing	Resumed	Resumed
Contained	No effect	Resumed only if containing device is resumed

1. When a containing device is added to the DCR, the DCR does not recognize the contained devices. However, when the device is added to Operations Manager, the contained devices are probed by Operations Manager and added to the Operations Manager inventory.

Automatically Importing DCR Devices

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

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

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

Step 2 Activate the **automatic** radio button.

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

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

Note If you do not require the duplicate device for your deployment, remove it (see Deleting Devices, page 16-36).

Note If you exceed your device limit, Operations Manager will continue to operate, but you will notice that devices are not being added to Operations Manager. Check the license log as described in Accessing and Deleting Log Files, page 20-13. For information about device-based licensing, see Responding to Messages About Device Limits, page 1-24.

For information about the inventory collection schedule, see Scheduling Inventory Collection, page 16-37.

Manually Importing DCR Devices

Use the following procedure to change automatic synchronization to manual synchronization.

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

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

Step 3 Select devices the following ways:

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

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

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

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

Note If you do not require the duplicate device for your deployment, remove it (see Deleting Devices, page 16-36).

Note If you exceed your device limit, Operations Manager displays a warning message. You can get more information from the license log as described in Accessing and Deleting Log Files, page 20-13. For information about device-based licensing, see Responding to Messages About Device Limits, page 1-24.

For information about how to handle duplicate devices, refer to Viewing the IP Address Report Page, page 16-20.

Determining Which Devices Are in the DCR But Not in Operations Manager

To identify devices that are in the DCR but not in Operations Manager, use the Device Selection page. In the Device Selection page with the Manual radio button selected, the device selector lists the devices that are not in Operations Manager. Devices may not be in Operations Manager for these reasons:

- The devices have not been added to Operations Manager because Operations Manager is using manual DCR synchronization.
- The devices were deleted from Operations Manager. (Devices you delete from Operations Manager are not deleted from the DCR.)

Note Devices you delete can only be added back into Operations Manager using manual import.

See Manually Importing DCR Devices, page 16-19 on how to access the Device Selection page.

For information about moving devices from the DCR into Operations Manager, see Manually Importing DCR Devices, page 16-19. For information about duplicate devices, see Viewing the IP Address Report Page, page 16-20.

Viewing the IP Address Report Page

The IP Address Report page lists all the IP addresses of the devices that are added to Operations Manager. The IP address list includes both the IP addresses of the devices in the DCR (including devices that are not monitored by Operations Manager) and the IP addresses of all the devices in inventory.

The IP Address Report page displays the following:

- The IP addresses for all the devices in the DCR, but not in Operations Manager inventory. The IP Address Report may only display the IP address (if added) and the DCR display name.
- The IP addresses for all the devices in Operations Manager inventory.
- All the IP addresses known for each of the devices in Operations Manager inventory. If there is more than one IP address for a monitored device, all the IP addresses are displayed. The DCR Display Name column displays N/A and the Device Name and Managed IP Address columns will have the same entries for the corresponding device.

- Duplicate device entries from the DCR. If there is more than one entry for the same device in the DCR (this can occur by varying the DCR display name), the IP Address Report identifies the duplicate entries and appends the display names with the corresponding IP address entry in the DCR Display Name column.

Note The duplicate entries in the DCR are identified by having more than one display name in the DCR Display Name column of the IP Address Report.

Step 1 Select **Devices > Device Management > IP Address Report**. The IP Address Report page appears. Figure 16-3 shows an example of the IP Address Report page.

Note For deleting duplicate devices, Deleting Devices, page 16-36.

Figure 16-3 IP Address Report Page

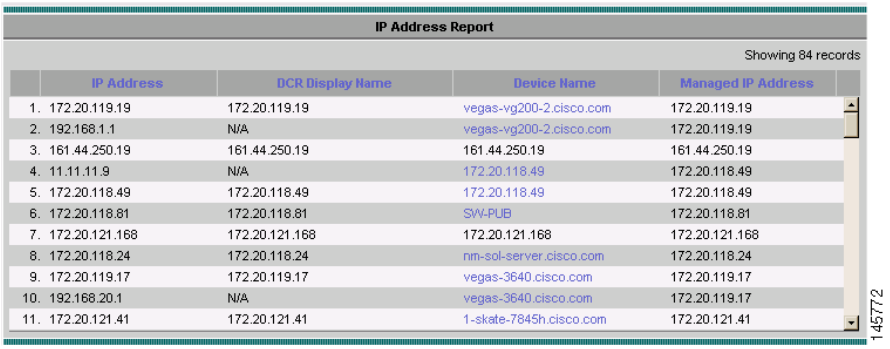


Table 16-5 IP Address Report Page

Heading	Description
IP Address	IP address known to Operations Manager.
DCR Display Name	Display name used when the device was added to the DCR.
Device Name	Device name as seen in Operations Manager. Clicking the device name opens the Detailed Device View page for the device.
Managed IP Address	IP address of the device through which Operations Manager manages the device.

Verifying Device Import

After adding a device, you can verify that it has been imported by using the Modify/Delete Devices page.

Step 1 Select **Devices > Device Management > Modify/Delete Devices**. The Modify/Delete Devices page opens. Figure 16-4 shows an example of the Modify/Delete Devices page.

Step 2 In the device selector, locate the device you added.

Step 3 Click on the device. The device information appears in the right pane. Verify that Device Status is Monitored. A Monitored state on the device indicates that it was imported successfully.

Note For a complete explanation of the device states, see Understanding the Device Summary and Device States, page 16-14.

Step 4 If the device is not in the Monitored state, refer to Troubleshooting Import and Inventory Collection, page 16-22.

Tip If your device appears in the device selector under the All Monitored Devices group, it was fully imported into Operations Manager. Only the devices in the All Partially Monitored Devices group and the All Unreachable Devices group were not imported fully into Operations Manager.

Troubleshooting Import and Inventory Collection

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

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

Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as “C:\Program Files\CSCOpx” or C:\PROGRA~1\CSCOpx.

For information on why you may receive device or license import errors, see the following:

- Why Does the Device or License Import Fail if the CSV File Is Not in CSCOpx?, page 16-22

For information on why your devices are not going into the Monitored state, see the following:

- Why Does a Device Go into the Partially Monitored State?, page 16-23
- Why Does a Device Go Into the Unreachable State?, page 16-28

Step 1 Select **Devices > Device Management > Modify/Delete Devices**. The Modify/Delete Devices page opens. Figure 16-4 shows an example of the Modify/Delete Devices page.

Step 2 Expand the folder that contains your device (according to its inventory collection status; refer to Verifying Device Import, page 16-21).

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

Step 4 Look under Data Collection Status Information for error information.

Step 5 Perform the required actions to clear the error.

Why Does the Device or License Import Fail if the CSV File Is Not in CSCOpx?

If the device or license import file (*.csv) is imported from any folder other than the install-directory CSCOpx, the import fails and gives the following error:

```
ERROR: Import from file failed. REASON: File C:/Documents and
Settings/Administrator/Desktop/backup-csv.csv does not exist. Please check the
permissions of this file/directory.
```

Do the following:

- When you export the devices from Operations Manager, the user permissions to the .csv file are set such that when you import the same file, Operations Manager cannot accept it. Instead, import a copy of the same .csv file, because the permissions are correctly set.
- Ensure that you have casuser permissions.

Why Does a Device Go into the Partially Monitored State?

Table 16-6 explains the possible reasons for the error codes seen on the Modify/Delete Devices page that occur for partially monitored devices.

Why Cisco Unified Communications Manager may go into the partially monitored state

If the incorrect HTTP credentials were entered for a Cisco Unified Communications Manager, it may go into the partially monitored state. When this occurs none of the Perfmon Counters will be polled. To change device credentials, see Editing Device Configuration and Credentials, page 16-30.

Why certain voice applications may go into the partially monitored state

This explanation describes why the following devices may go into the partially monitored state:

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

If insufficient windows credentials are provided during the addition of these devices they will become partially monitored, and some of their WMI attributes will not get polled. To change device credentials, see Editing Device Configuration and Credentials, page 16-30.

Table 16-6 Error Shown on the Modify/Delete Devices Page

Error Shown on the Modify/Delete Devices Page	Reason	Resolution Steps
Error Code = WMI Authentication Failure Error Message = Success: Incorrect WMI Credential or Insufficient Privileges	The message indicates that either the credentials are incorrect or user does not have sufficient privilege to reach the device. WMI credentials are for a user who is not an administrator.	1. Check if the Windows Management Instrumentation (WMI) credentials are correct. 2. If credentials are correct, and the device is in the Partially Monitored State, verify that Operations Manager is able to reach the device with the credentials provided, using the following steps: a. Open the command prompt on the Operations Manager machine, type wbemtest, and click **OK**. b. In the new popup, click **Connect**. c. In the Connect popup for NameSpace text field, enter: \\<ccmip>>\root\cimv2 instead of root\default. d. Enter the User Name and password and click **Login**. Login should succeed for Operations Manager to move the device in to a fully monitored state. 3. If the login fails, check that the Operations Manager machine and CCM are in different domains. If yes, include the domain name when you add a device. 4. If login has failed, see if a firewall may be blocking packets. 5. If login is successful in step 2; a. Try restarting Windows Management Instrumentation service on Cisco Unified Communications Manager. b. Rediscover the device.
Error Code = WMI Authentication Failure Error Message = Success: No Windows Credential for WMI Access	No Windows credential provided.	1. Go to the Modify/Delete screen. 2. Select the device under All Partially Monitored Device ..WMI Authentication Failure category, and click **Edit**. 3. Enter the WMI credential and click **OK**.

Table 16-6 Error Shown on the Modify/Delete Devices Page (continued)

Error Shown on the Modify/Delete Devices Page	Reason	Resolution Steps
Error Code = CCM Authentication Failure Error Message = Success:WrongCredentials	This message indicates that either the Cisco Unified Communications Manager HTTP credentials are not entered or the credentials provided are incorrect.	1. Verify that you provided the correct HTTP credentials in the DCR by using the credentials to log in to the Cisco Unified Communications Manager Admin page. 2. Verify if the same credentials work for https://<CCMIP>/ast/astisapi.dll?QueryService. 3. Rediscover the device.
Error Code= CCM Authentication Failure Error Message= Success:UnknownCredentialError	This message indicates that SNMP management MIBs are not responding. The specific error could be one of the following: • MIB-2—The ipAddressTable is not responding. • CISCO-CCM-MIB—The ccmTable is not responding. Specifically, the ccmClusterId attribute is not responding. • Inventory collection could not find the ccmVersion detail. This may be because the ccmVersion attribute in the CISCO-CCM-MIB is not responding.	1. If the MIB-2 is not responding, restart the SNMP Agent on the system and rediscover the device. 2. If the CISCO-CCM-MIB is not responding, restart the Cisco Unified Communications Manager Service. 3. Rediscover the device.

Table 16-6 Error Shown on the Modify/Delete Devices Page (continued)

Error Shown on the Modify/Delete Devices Page	Reason	Resolution Steps
Error Code = CCM Authentication Failure Error Message = Success:WebServiceDown	HTTP service is not running or responding to requests from Operations Manager.	1. Verify that the web server is running by launching the Cisco Unified Communications Manager Admin page. 2. Check the firewall to see if it is blocking the HTTP/HTTPS connection between Cisco Unified Communications Manager and Operations Manager. 3. For Cisco Unified Communications Manager 5.0, verify that 8433 and 8080 are not blocked.

Table 16-6 Error Shown on the Modify/Delete Devices Page (continued)

Error Shown on the Modify/Delete Devices Page	Reason	Resolution Steps
Error Code = CCM Authentication Failure Error Message = Success: HTTPSCertificateNotImported	The Cisco Unified Communications Manager certificate download has failed.	Do the following: 1. Check the size of the cacerts file located at C:\PROGRA~1\CSCOpx\lib\jre\lib\security\cacerts. If the file size is not zero, then try to delete and add the Cisco Unified Communications Manager node in question. 2. If the file size is zero, then follow the below steps: a. Delete the device [Cisco Unified Communications Manager] completely from Operations Manager and CS [Device .. Device .. Management .. Modify/Delete Devices link]. b. Enter **pdterm InventoryCollector**. c. Copy C:\PROGRA~1\CSCOpx\setup\dependency\jre2\lib\security\cacerts. C:\PROGRA~1\CSCOpx\lib\jre\lib\security\cacerts. d. Change the directory to the following: **cd C:\PROGRA~1\CSCOpx\lib\jre\lib\security** e. Copy IPToHostName.txt IPToHostName.txt.orig. f. Delete IPToHostName.txt. g. Enter **pdexec InventoryCollector**. h. Read the device [Cisco Unified Communications Manager]. i. If after you complete the previous steps, the Cisco Unified Communications Manager nodes are still partially monitored due to insufficient credentials, follow the procedures to manually import the security certificates in Operations Manager. See Cisco Unified Operations Manager *2.0 Deployment Best Practices* on Cisco.com for details on how to repair Cisco Unified Communications Manager nodes that are partially monitored due to insufficient credentials.

Why Does a Device Go Into the Unreachable State?

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

- SNMP timeout
- Data Collector timeout

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

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

Manual Inventory Cleanup

To clean up your inventory, you must delete all devices. This includes all monitored devices, as well as devices in the Unreachable and Unsupported states.

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

Step 2 In the device selector, select the check box next to All Devices.

Step 3 Click **Delete**.

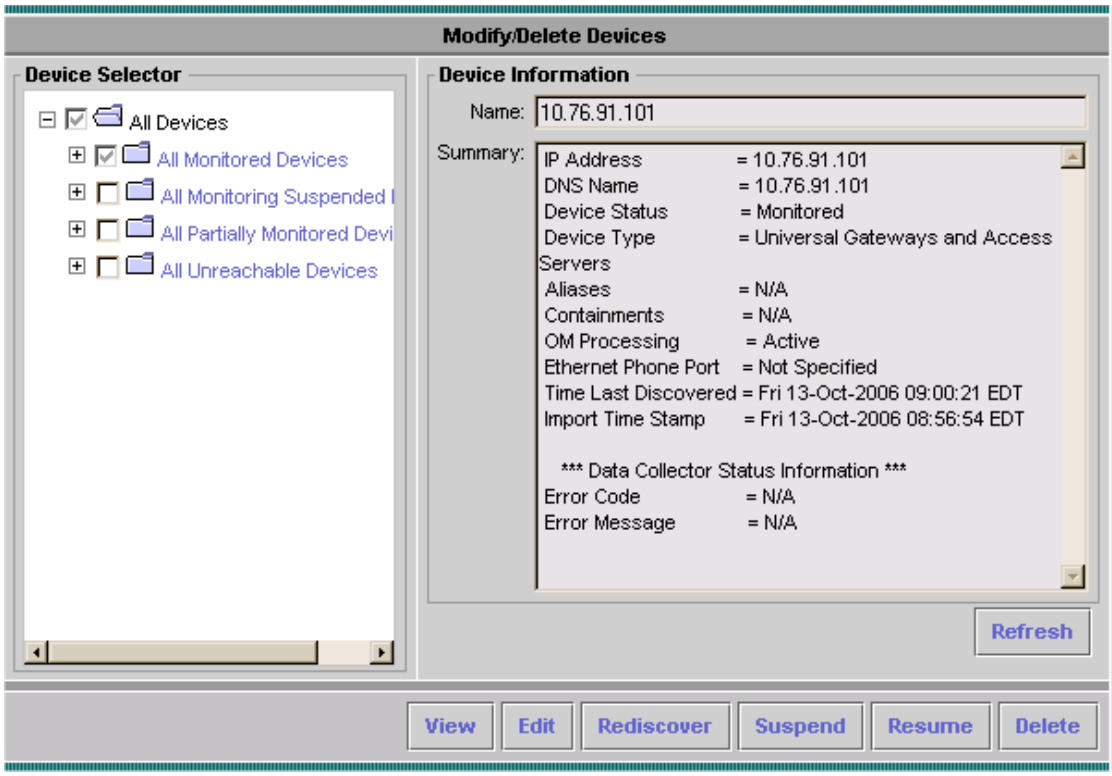
Note It is essential that you delete all of the devices.

Working with Device Management

Understanding the Modify/Delete Devices Page

Performing inventory collection, viewing details, suspending and resuming device monitoring, editing credentials, and deleting devices are controlled by the Modify/Delete Devices page. Figure 16-4 shows the Modify/Delete Devices page.

Figure 16-4 Modify/Delete Devices Page



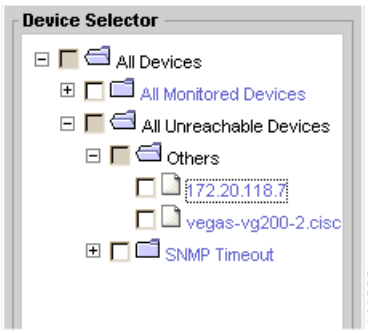
Note If at any time while using the Modify/Delete Devices page, you want to refresh the view, click the **Refresh** button.

The Modify/Delete Devices page contains two panes. The left pane displays a device selector, from which you select the device or group that you want to update or delete. The right pane displays the information for the selected object. Besides displaying device information, the right pane displays data collection information.

Tip If there is an error during device discovery, an error code and error message appear at the bottom of the right pane. For troubleshooting information see Troubleshooting Import and Inventory Collection, page 16-22.

The devices that appear in the device selector are organized in folders, based on whether they are monitored by Operations Manager. The folders appear only if there is a device to go in the folder. Figure 16-5 shows an example of the device selector.

Figure 16-5 Modify/Delete Devices Selector



Under the All Devices folder, devices are placed in the following possible subfolders:

- All Monitored Devices—Contains devices that are fully monitored in the Operations Manager inventory.
- All Monitoring Suspended Devices—Contains devices for which monitoring has been suspended. A user manually suspends monitoring of the device by Operations Manager.
- All Partially Monitored Devices—Contains devices that have been successfully imported by some of the data collectors in Operations Manager (see Why Does a Device Go into the Partially Monitored State?, page 16-23).
- All Unreachable Devices—Contains devices that were not successfully imported into Operations Manager. Descriptions of the errors are displayed in the right pane, next to Error Message (see Why Does a Device Go Into the Unreachable State?, page 16-28).
- All Unsupported Devices—Contains devices that were not imported into Operations Manager because they are not supported.

Details about, and procedures for, performing inventory collection, viewing details, or deleting devices using this page are provided in these topics:

- Performing Manual Inventory Collection on Devices, page 16-31
- Viewing Device Details, page 16-32
- Suspending/Resuming Devices, page 16-35
- Deleting Devices, page 16-36
- Scheduling Inventory Collection, page 16-37

Editing Device Configuration and Credentials

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

Note You can also change device credentials though the Auto Discovery Configuration page. (See Configuring Credentials, page 16-8.)

Step 1 Select **Devices > Device Management > Modify/Delete Devices**. The Modify/Delete Devices page opens. Figure 16-4 shows an example of the Modify/Delete Devices page.

Step 2 Expand the folder that contains your devices.

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

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

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

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

Step 5 You can update the following credentials:

- SNMPv2c/SNMPv1
- SNMPv3
- HTTP
- WMI

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

Step 6 Click **OK**.

Performing Manual Inventory Collection on Devices

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

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

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

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

The following events will also trigger inventory collection:

- The entire Operations Manager inventory is polled. This is controlled by the inventory collection schedule. (See Scheduling Inventory Collection, page 16-37.)

- Operations Manager is using automatic synchronization with the DCR, and a device is added, or a change is made to a device in the DCR. Such DCR changes include a device being deleted or having its credentials (IP address, SNMP credentials, MDF type) changed.
- Operations Manager is using manual synchronization with the DCR, and a device is added to Operations Manager using the Device Selection page.

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

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

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

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

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

Viewing Device Details

You can select devices and view information about them in a report. There are two ways you can generate this report:

- Through the Modify/Delete Devices page, where you can view details about particular devices that you choose. See Using the Modify/Delete Devices Page to Generate a Device Report, page 16-32.
- Through the Device Management: Summary page, where you can view details about all the devices in a particular device state. See Using the Device Management: Summary Page to Generate a Device Report, page 16-33.

The device report provides basic information about the device such as name, IP address, when it was added, and so on. (For a description of a device detail display, see Understanding Device Reports, page 16-33.)

Note If you require more detailed information about a device, use the Detailed Device View. It provides information about device components, including hardware and software information, environment, connectivity, interface components, and so on. (For a description of the Detailed Device View, see Viewing Device Elements in Detail, page 3-22.)

Figure 16-5 shows an example of the Modify/Delete Devices page. Devices are organized in folders according to their device state. (See Understanding the Device Summary and Device States, page 16-14.)

Using the Modify/Delete Devices Page to Generate a Device Report

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

Step 2 For each device for which you want to view details, in the device selector, expand the folders where the device is located.

Step 3 Select a device by clicking the box next to it. Do this for each device for which you want to view details. If you want to view details for all of the devices in a group, click the box next to the group.

Step 4 Click **View**.

A report appears, listing the device information.

Using the Device Management: Summary Page to Generate a Device Report

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

Step 2 Locate the device state for which you want to view the devices.

Step 3 In the number column that corresponds to the device state, click the number.

A report appears, listing the device information.

Note If the number in the column is zero, you will not be able to generate a report.

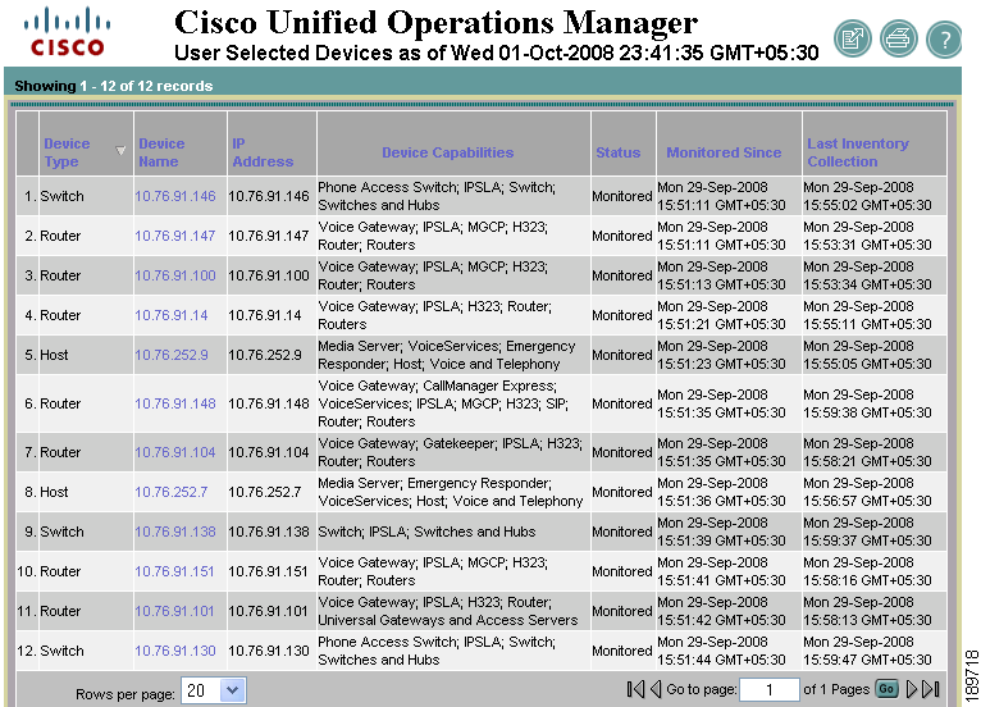
Understanding Device Reports

A device report displays details for the devices that you select. See Viewing Device Details, page 16-32 for information on selecting devices.

Note In the Monitored or Partially Monitored devices reports, a Suspend button appears at the bottom of the report. You can use this button to suspend the monitoring of all the devices in the report. Similarly, the Monitoring Suspended report provides you with a Resume button, so that you can resume monitoring of all the devices in the report.

Figure 16-6 shows an example of a device report.

Figure 16-6 Device Report



Cisco Unified Operations Manager
User Selected Devices as of Wed 01-Oct-2008 23:41:35 GMT+05:30

Showing 1 - 12 of 12 records

	Device Type	Device Name	IP Address	Device Capabilities	Status	Monitored Since	Last Inventory Collection
1.	Switch	10.76.91.146	10.76.91.146	Phone Access Switch; IPSLA; Switch; Switches and Hubs	Monitored	Mon 29-Sep-2008 15:51:11 GMT+05:30	Mon 29-Sep-2008 15:55:02 GMT+05:30
2.	Router	10.76.91.147	10.76.91.147	Voice Gateway; IPSLA; MGCP; H323; Router; Routers	Monitored	Mon 29-Sep-2008 15:51:11 GMT+05:30	Mon 29-Sep-2008 15:53:31 GMT+05:30
3.	Router	10.76.91.100	10.76.91.100	Voice Gateway; IPSLA; MGCP; H323; Router; Routers	Monitored	Mon 29-Sep-2008 15:51:13 GMT+05:30	Mon 29-Sep-2008 15:53:34 GMT+05:30
4.	Router	10.76.91.14	10.76.91.14	Voice Gateway; IPSLA; H323; Router; Routers	Monitored	Mon 29-Sep-2008 15:51:21 GMT+05:30	Mon 29-Sep-2008 15:55:11 GMT+05:30
5.	Host	10.76.252.9	10.76.252.9	Media Server; VoiceServices; Emergency Responder; Host; Voice and Telephony	Monitored	Mon 29-Sep-2008 15:51:23 GMT+05:30	Mon 29-Sep-2008 15:55:05 GMT+05:30
6.	Router	10.76.91.148	10.76.91.148	Voice Gateway; CallManager Express; VoiceServices; IPSLA; MGCP; H323; SIP; Router; Routers	Monitored	Mon 29-Sep-2008 15:51:35 GMT+05:30	Mon 29-Sep-2008 15:59:38 GMT+05:30
7.	Router	10.76.91.104	10.76.91.104	Voice Gateway; Gatekeeper; IPSLA; H323; Router; Routers	Monitored	Mon 29-Sep-2008 15:51:35 GMT+05:30	Mon 29-Sep-2008 15:58:21 GMT+05:30
8.	Host	10.76.252.7	10.76.252.7	Media Server; Emergency Responder; VoiceServices; Host; Voice and Telephony	Monitored	Mon 29-Sep-2008 15:51:36 GMT+05:30	Mon 29-Sep-2008 15:56:57 GMT+05:30
9.	Switch	10.76.91.138	10.76.91.138	Switch; IPSLA; Switches and Hubs	Monitored	Mon 29-Sep-2008 15:51:39 GMT+05:30	Mon 29-Sep-2008 15:59:37 GMT+05:30
10.	Router	10.76.91.151	10.76.91.151	Voice Gateway; IPSLA; MGCP; H323; Router; Routers	Monitored	Mon 29-Sep-2008 15:51:41 GMT+05:30	Mon 29-Sep-2008 15:58:16 GMT+05:30
11.	Router	10.76.91.101	10.76.91.101	Voice Gateway; IPSLA; H323; Router; Universal Gateways and Access Servers	Monitored	Mon 29-Sep-2008 15:51:42 GMT+05:30	Mon 29-Sep-2008 15:58:13 GMT+05:30
12.	Switch	10.76.91.130	10.76.91.130	Phone Access Switch; IPSLA; Switch; Switches and Hubs	Monitored	Mon 29-Sep-2008 15:51:44 GMT+05:30	Mon 29-Sep-2008 15:59:47 GMT+05:30

Rows per page: 20 Go to page: 1 of 1 Pages Go

189718

Table 16-7 describes the information displayed in a device report.

Table 16-7 Device Report

Heading/Button	Description
Device Type	Device type.
Device Name	Device name. Link to the Detailed Device View for the device. Clicking the link opens a Detailed Device View for the device. See Understanding the Layout of the Detailed Device View, page 3-20.
IP Address	Device IP address.
Device Capabilities	Functions that a device can perform; for example, switch, voice gateway, Cisco Unified Communications Manager, Host, and so on.
Status	Current state the device is in.
Monitored Since	The time and date that inventory collection was first completed for the device.
Last Inventory Collection	The time and date that inventory collection was last completed for the device.
	Downloads the Device Details display to a file on your computer.
	Displays the report in a printer-friendly format.

Table 16-7 Device Report (continued)

Heading/Button	Description
	Opens the Operations Manager online help.
Suspend or Resume	Depending on the report, a Suspend button or a Resume button may appear at the bottom of the report. This button enables you to either suspend or resume monitoring of all of the devices in the report. • Suspend—Available in the Monitored and Partially Monitored device report. • Resume—Available in the Monitoring Suspended device report.

Suspending/Resuming Devices

When you stop monitoring a device, Operations Manager no longer polls that device for information. Subsequent events (including traps) are ignored and no longer processed.

When you suspend a device, the active alerts and events on the device are moved to the Cleared state. No suspended management events are generated. The suspended alert information moves from the All Alerts view to the Suspended Devices view. The status of the suspended alert is cleared and the latest event category displays as suspended. The alert is removed within 30 to 60 minutes if the corresponding device status is not resumed within this timeframe.

When you resume a device, Operations Manager resumes the processing of events for that device. No resumed management events are generated on resuming the device. The status of the alert is cleared and the latest event category displays Resumed if there are no active events for that device. An alert for a resumed device is a special case when you can see an alert with zero events. If the resumed device has active events (which means the problem exists in the device), then the status of the resumed alert will be active and latest event category will be updated as per the event category. If you resume a device after a suspended alert has been purged, then a new alert is generated after resuming a device; alternately, the same suspended alert is updated.

Note You can also suspend or resume the monitoring of devices in the following ways:

- From a device report. See Understanding Device Reports, page 16-33.
- Through the Detailed Device View. From here, you can suspend a device or specific device components. For more information on using the Detailed Device View to suspend device monitoring, see the following:
  - Suspending/Resuming Devices, page 3-26
  - Suspending/Resuming a Device Component, page 3-27

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

Step 2 Select the devices that you want to suspend or resume.

Step 3 Do one of the following:

- Click **Suspend** to change the device's current managed state to Suspended. Operations Manager no longer polls any device components, nor does it process any traps. The device is moved to the Suspended Devices view. Subsequent events (including traps) are ignored and no longer processed.
- Click **Resume** to change the device's current managed state to Active. Operations Manager resumes polling and trap processing on the device, and the device is moved out of the Suspended Devices view and back into its previous view.

Note When you resume a device, you must also perform the apply changes action in Polling and Thresholds (see Applying Changes, page 19-60).

Deleting Devices

There are two inventories where devices exist, in Operations Manager and in the DCR, so when you delete a device it can be removed from either inventory. How Operations Manager is configured with the DCR determines from which inventory a device is deleted. For Operations Manager/DCR configurations, see DCR Masters and Slaves, page 16-13.

Which inventory a device is removed from when it is deleted depends on the Operations Manager and DCR configuration as follows:

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

While a device is being deleted, Operations Manager does not allow any inventory collection, suspend operations, or resume operations to be performed on the device. When you delete a containing device, all of the contained devices are deleted.

Guidelines for Deleting Devices

The following guidelines are helpful when you are considering deleting devices from your network:

- If you only want to suspend the managed state of a device, you do not need to delete the device from Operations Manager. For more details on suspending and resuming the managed state of a device, see the Suspending/Resuming Devices, page 16-35.
- Depending upon the load that exists on the system, Operations Manager takes approximately 15 to 40 seconds to delete a device.
- When a Cisco Unity or a Unified Contact Center device is deleted from Operations Manager, RPC keepalive packets will continue to be exchanged between the device and Operations Manager until either the Operations Manager or the device is restarted.
- When you turn off a device in the network and do not want it to be monitored by Operations Manager any longer, you will need to remove the device from Operations Manager or you will be unable to remove alerts and events from the Alerts and Events displays. To remove devices use one of the following procedures:
  - Access Service Level Views and locate the device which you need to remove. Right click the device and select **Delete Device**.

– Select **Devices > Device Management > Modify/Delete Devices**. Select the device by clicking on the checkbox, then click **Delete**. By deleting the device in Operations Manager, all the existing events in the Alerts and Events display will also be removed.

Note Your login determines whether you can perform this operation.

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

Step 2 Select the device or group that you want to delete.

Step 3 Click **Delete**.

Step 4 In the confirmation box, click **Yes**.

Scheduling Inventory Collection

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

In the Inventory Collection Schedule page (**Devices > Device Management > Inventory Collection > Device**), you can edit, suspend, or, resume the device inventory collection schedule. (See Working with the Device Inventory Collection Schedule, page 16-37.)

In the IP Phone Discovery Schedule page (**Devices > Device Management > Inventory Collection > IP Phone**), you can add, edit, or delete the IP phone discovery schedules. (See Working with IP Phone Discovery, page 16-38.)

Working with the Device Inventory Collection Schedule

You can perform the following tasks with the device inventory collection schedule:

- Editing the Device Inventory Collection Schedule, page 16-37
- Suspending and Resuming the Inventory Collection Schedule, page 16-38

Editing the Device Inventory Collection Schedule

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

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

Step 3 Change the desired scheduling information.

Step 4 Click **OK**.

Step 5 Click **Yes**.

Suspending and Resuming the Inventory Collection Schedule

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

Step 2 If the schedule is active and you want to stop it from performing inventory collection, click **Suspend**.

Step 3 If the schedule is not active and you want Operations Manager to perform inventory collection at a scheduled time, click **Resume**.

Working with IP Phone Discovery

When you select **Devices > Device Management > Inventory Collection > IP Phone**, you can perform the following tasks:

- Viewing IP Phone Collection Status, page 16-38
- Adding an IP Phone Discovery Schedule, page 16-38
- Editing an IP Phone Discovery Schedule, page 16-39
- Deleting an IP Phone Discovery Schedule, page 16-39

Viewing IP Phone Collection Status

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

The IP Phone Collection Status pane displays the following:

- Collection Status—Displays the status of the discovery process. The status could be any one of the following:
  - In progress—When you start PIFServer for the first time or restart it, discovery takes place automatically and the status appears as `In Progress`.
  - Complete—The discovery process is complete.
  - Not available. Try after some time—Appears when you start PIFServer for the first time, or restart it, and the discovery process has not yet begun.
- Last Collection Start Time—Displays the start time of the last discovery.
- Last Collection End Time—Displays the end time of the last discovery.

Adding an IP Phone Discovery Schedule

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

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

Step 3 Enter the following:

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

- The time of the day when you want discovery to occur

Step 4 Click **OK**.

Editing an IP Phone Discovery Schedule

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

Step 2 Select the phone discovery schedule that you want to edit.

Step 3 Click **Edit**. The Edit Discovery Schedule dialog box appears.

Step 4 You can change the following:

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

Step 5 Click **OK**.

Step 6 After all your changes are done, click **Apply**.

Deleting an IP Phone Discovery Schedule

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

Step 2 Click **Delete**.

Step 3 In the confirmation box, click **Yes**.

Determining the Media Server Account to Use for Cisco Unified Communications Manager Access

To enable Operations Manager to access a Cisco Unified Communications Manager, you must supply the username and password for an account on the media server. The account to use depends upon the Cisco Unified Communications Manager version and might also depend on whether multilevel administration access (MLA) is enabled for the Cisco Unified Communications Manager. Table 16-8 lists the options.

Table 16-8 Username and Password for Accessing the Cisco Unified Communications Manager

Cisco Unified Communications Manager Version on Media Server	MLA Enabled or Disabled for Cisco Unified Communications Manager	Required Account
Earlier than 4.0	Enabled or disabled	Valid Windows 2000 administrator account on the media server.
4.0 or later	Enabled	A multilevel administration access account with either full access or read-only access to the Standard Serviceability Functional Group.
	Disabled	Valid Windows 2000 administrator account on the media server.

Viewing Discovery Status

In Operations Manager, you can use the Device Management: Summary page to determine the discovery status of the devices that are being added. For details on accessing and understanding the Device Management: Summary page, see Understanding the Device Summary and Device States, page 16-14.

Editing SNMP Timeout and Retries

If an SNMP query does not respond in time, Operations Manager will time out. It will then retry contacting the device for as many times as listed under the snmpretries attribute in the configuration file. The timeout period is doubled for every subsequent retry. For example, if the timeout value is 4 seconds and the retries value is 3, Operations Manager waits for 4 seconds before the first retry, 8 seconds before the second retry, and 16 seconds before the third retry.

The SNMP timeout and retries are global settings.

The default values are:

- Timeout—4 seconds
- Retries—3

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

Step 2 Select a new SNMP timeout setting.

Step 3 Select a new Number of Retries setting.

Step 4 Click **Apply**.

Step 5 In the confirmation box, click **Yes**.

Configuring LDAP

Adding an LDAP Server

Operations Manager can be configured to connect to a Lightweight Directory Access Protocol (LDAP) server, so that Operations Manager can access user information stored in the LDAP server.

Note LDAP servers that use SSL authentication are not supported by Operations Manager.

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

Step 2 Click **Add**. The Add LDAP Server page opens.

Step 3 In the Connection Details area, do the following:

- Enter the LDAP server name or IP address.
- Enter the port number—Port used for LDAP requests on the LDAP server.
- If you want to use anonymous login for authentication, select the Use Anonymous Login check box.
- Enter an admin DN—If your LDAP server requires authentication for lookups, set this to the name of a user who has permission to search the subtree specified in the search base.
- Enter the password for the LDAP server and reconfirm the password.
- Enter a search base—Set this parameter to the search base for LDAP lookups. This search base should include all users who must be returned from the lookup.

Step 4 In LDAP Search Parameters, do the following:

- Enter a name for the search.
- Enter a telephone number—Enter the number as it is stored in the LDAP server.
- Enter a telephone filter—Enter the exact telephone number prefix. This enables Operations Manager to get only extension number details for each person from the LDAP server. This will be correlated with the extension number obtained from Cisco Unified Communications Manager, to display the username.

Step 5 Click **Add**.

Modifying LDAP Server Configuration

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

Step 2 Select the LDAP server that you want to change.

Step 3 Click **Modify**. The Edit LDAP Server Configuration page appears.

Step 4 In the LDAP Server Connection Details area, you can change the following:

- The LDAP server name or IP address.
- The port number—Port used for LDAP requests on the LDAP server.
- Whether to use anonymous login for authentication—Select or deselect the Use Anonymous Login check box.
- An admin DN—If your LDAP server requires authentication for lookups, set this to the name of a user who has permission to search the subtree specified in the search base.
- The password for the LDAP server—Be sure to reconfirm the password.
- A search base—Set this parameter to the search base for LDAP lookups. This search base should include all users who must be returned from the lookup.

Step 5 In the LDAP Search Parameters area, you can change the following:

- Common name.
- Telephone number—Enter the number as it is stored in the LDAP server.
- Telephone filter—Enter the exact telephone number prefix. This enables Operations Manager to get only extension number details for each person from the LDAP server. This will be correlated with the extension number obtained from Cisco Unified Communications Manager, to display the username.

Step 6 Click **Edit**.

Deleting an LDAP Server

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

Step 2 Select the LDAP server that you want to delete.

Step 3 Click **Delete**.

CHAPTER 17

Managing Groups

These topics describe the concepts and processes involved in configuring groups:

Understanding Operations Manager Groups

A group consists of Unified Communications s, where Unified Communications s refer to devices, applications, and groups. Each group has a set of properties (such as a name, description, permission, and so on), but what defines a group are its associated rules. Rules determine the membership of a group, which may change whenever the rule is evaluated.

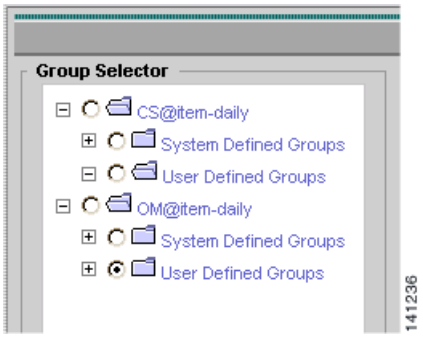
Cisco Unified Operations Manager manages groups in a hierarchical fashion that supports subgrouping. Each child group is a subgroup of a parent group, and its group membership will be a subset of its immediate parent group. For an object to belong to a group, it must satisfy the immediate group rules and the parent group rules.

What you see in the Operations Manager group selector depends on the function you are using. Normally when you view the Operations Manager group selector, some groups are displayed under Operations Manager and other groups under Common Services, as shown in Figure 17-1 on page 17-2.

- Common Services groups are created by Common Services when devices are added to the DCR. These are device groups. The group to which a device belongs is determined by Common Services group rules. Common Services groups include Unified Communications s such as routers, switches, and hubs. All Common Services groups are shared with Operations Manager—in other words, they are shown in the Operations Manager user interface. Groups are only shown when they have members.
- Operations Manager groups are created by Operations Manager. The group to which a device belongs is determined by Operations Manager group rules.

Figure 17-1 shows the object selector, with some groups under Common Services and others under Operations Manager.

Figure 17-1 Group Selector Showing Common Services and Operations Manager Groups

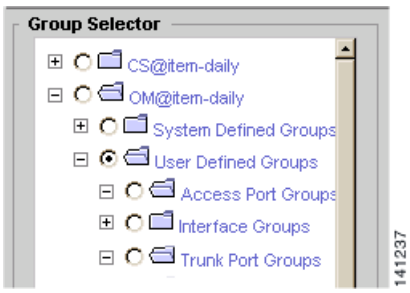


Group	Description
CS@<server-name>	Groups that are controlled by Common Services.
OM@<server-name>	Groups that are controlled by Operations Manager.

As shown in Figure 17-2, the following *types of groups* are supported in Operations Manager:

- System Defined groups—The default grouping of devices in CiscoWorks Common Services. System-defined groups cannot be deleted or edited. For a description of each system-defined group, see the "Working with System-Defined Groups" section on page 17-3.
- User Defined groups—Groups that you edit or create to reflect the way you manage the network. You can edit or create user-defined groups Operations Manager and determine whether they can be viewed by other users. User-defined groups include the following:
  - Access Port Groups—Predefined groups that you can edit for your own purposes. For a detailed description, see Working with User-Defined Groups, page 17-9.
  - Interface Groups—Predefined groups that you can edit for your own purposes. For a detailed description, see Working with User-Defined Groups, page 17-9.
  - Trunk Port Groups—Predefined groups that you can edit for your own purposes. For a detailed description, see Working with User-Defined Groups, page 17-9.
  - Groups you create (to use with views in the Monitoring Dashboard displays, or with notification groups in Notification Services). These are the only groups you can *create*. These appear in the Group Selector under User Defined Groups so you can view the group membership (device groups are created when the devices are added to the Operations Manager inventory).

Figure 17-2 Group Selector Showing Operations Manager Groups



Groups and ACS

The CiscoSecure Access Control Server (ACS) provides device-based filtering for many of the Operations Manager user interfaces that use Group Administration. For more information on ACS, see Device-Based Filtering, page 20-22.

Working with System-Defined Groups

The group selector displays some groups under Operations Manager and other groups under Common Services. The Common Services groups are created by Common Services and are visible when devices are added to the DCR. See Common Services System-Defined Groups, page 17-8 for more information.

The Operations Manager groups are created by Operations Manager. These groups include Access Port Groups, Trunk Port Groups, and Interface Groups. See Table 17-1 for a list of the Operations Manager system-defined groups.

You can control the polling and thresholds settings for these groups using **Administration > Polling and Thresholds**. See Configuring Polling and Thresholds, page 19-1.

Operations Manager System-Defined Groups

The Operations Manager system-defined groups are visible to all users, and are the default groups that are administered by Operations Manager.

Table 17-1 describes the system-defined groups (device types) that come preconfigured in Operations Manager.

Table 17-1 Operations Manager System-Defined Groups /Device Types

Group Name	Definition	Examples
78XX Media Servers	Any Cisco-supported hardware platform that runs Cisco voice applications.	Cisco Media Convergence Servers that are running: • Cisco Unified Communications Manager • Cisco Emergency Responder • Cisco Customer Response Application • Cisco Unity • Cisco Personal Assistant • [and so on]
Access Port Groups • 1 GB Ethernet • 10MB-100MB Ethernet • ATM • Others	A switch port that is connected to a host.	Any switch

Table 17-1 Operations Manager System-Defined Groups (continued)/Device Types

Group Name	Definition	Examples
Cisco Unified Communications Manager or Cluster When a single Cisco Unified Communications Manager or a cluster is added to Operations Manager, Group Management automatically creates a group under the Cisco Unified Communications Manager or Cluster folder. The new group name will be preceded by VE; for example, VE-TEST1-CCM. Under the new folder, the following subfolders appear:	Cisco Unified Communications Manager or cluster. Subgroups of the Cisco Unified Communications Manager or Cluster group contain all of the devices associated with the corresponding instance of the Cisco Unified Communications Manager or cluster.	—
• 78XX Media Servers	All media servers running Cisco Unified Communications Manager in the cluster.	MCS 78XX box
• Digital Voice Gateways	Any DT-24+ or DE-30+ devices that belong to a Cisco Unified Communications Manager or a cluster.	• DT-24+ • DE-30+
• Gatekeepers	Gatekeepers to which a Cisco Unified Communications Manager or cluster is registered.	• Cisco 2600 • Cisco 3640 • Cisco 3660 • Cisco 7200 • [and so on]
• Voice Gateways	Voice gateways whose port (interface) acts as a gateway to a Cisco Unified Communications Manager or a cluster.	• VG-200 • Catalyst 6000 (with a T1, E1, or FXS card) • SIP-Gateway
• Voice Mail Gateways	Any voice mail gateway that belongs to a Cisco Unified Communications Manager or a cluster.	• DPA-7610 • DPA-7639
Cisco Unified Communications Applications Under the All Cisco Unified Communications Applications folder, the following subgroups appear:	Cisco Unified Communications Applications running on a device.	—
• Cisco Unified Presence	Any Cisco Unified Presence Server applications running on a media server.	Cisco Unified Presence Servers
• Communications Manager Business Edition	Any Cisco Unified Communications Manager Business Edition applications running on a media server.	Cisco Unified Communications Manager Business Edition
• Communications Manager Express	Any Cisco Unified Communications Manager Express applications running on a router.	Cisco Unified Communications Manager Express

Table 17-1 Operations Manager System-Defined Groups (continued)/Device Types

Group Name	Definition	Examples
• Communications Managers	Any Cisco Unified Communications Manager applications running on a media server.	Cisco Unified Communications Manager
• Conference Server	Media servers running Cisco Conference Connection.	Cisco Conference Connection
• Customer Response Applications	Any Cisco Customer Response Application (CRA) running on a media server.	Cisco CRA
• Customer Voice Portals	Any Cisco Unified Customer Voice Portal (CVP) application.	Cisco Unified Customer Voice Portal
• Emergency Responders	Any Cisco Emergency Responder running on a media server.	Cisco Emergency Responder
• Expert Advisor	Any Cisco Expert Advisor running on a media server.	Cisco Expert Advisor
• Unified Contact Center Enterprise	Any Cisco Unified CCE running on a media server	Cisco Unified CCE
• Meeting Place	Any Cisco Meeting Place running on a media server.	Cisco Meeting Place
• Meeting Place Express	Any Cisco Meeting Place Express running on a media server.	Cisco Meeting Place Express
• Personal Assistants	Any Cisco Personal Assistant (PA) running on a media server.	Cisco PA
• Unity	Any Cisco Unity application running on a media server.	Cisco Unity
• Unity Connection	Any Cisco Unity Connection application running on a media server.	Cisco Unity Connection
• Unity Express	Any Cisco Unity Express application running on a media server.	Cisco Unity Express
Digital Voice Gateways	Any DT-24+ or DE-30+ devices.	• DT-24+ • DE-30+
Gatekeepers	Gatekeepers that provide address translation, bandwidth control and access control to H323 devices including H323 gateways and Cisco Unified Communications Manager Intercluster Trunks.	• Cisco 2600 • Cisco 3640 • Cisco 3660 • Cisco 7200 • [and so on]

Table 17-1 Operations Manager System-Defined Groups (continued)/Device Types

Group Name	Definition	Examples
H323 Gateways	Switch modules or routers that have voice ports and are configured as H323 gateways.	• Catalyst 4000 with Access Gateway Module • Cisco 1700 • Cisco 2600 • Cisco 2800 • Cisco 3600 • Cisco 3700 • Cisco 3800 • [and so on]
IP SLA Devices	Cisco devices that are running Cisco IOS IP SLA (IP SLA).	IP SLA-capable devices
Interface Groups: • 1 GB Ethernet • 10MB-100MB Ethernet • ATM • Backup • Dial-On-Demand • FDDI • ISDN B channel • ISDN D channel • ISDN physical interface • Others • Serial • Token ring	Devices that represent a logical (typically Layer 2) connection to the network.	Any host, hub, router, or switch
MGCP Gateways	Switch modules or routers that have voice ports and are configured as MGCP gateways.	• Catalyst 6000 with T1/E1/FXS ports • Cisco 1700 • Cisco 2600 • Cisco 2800 • Cisco 3600 • Cisco 3700 • Cisco 3800 • [and so on]

Table 17-1 Operations Manager System-Defined Groups (continued)/Device Types

Group Name	Definition	Examples
Phones with tests configured	Cisco Unified IP Phones that are configured for testing.	• 7910 • 7935 • 7960 • 12SP • 30VIP
SRST Devices	Devices that are configured for Survivable Remote Site Telephony (SRST).	SRST-enabled routers
Switches with phones connected	Cisco switches that have Cisco Unified IP Phones connected to them (through ports on the switch).	• Catalyst 6000 • Catalyst 3500 XL • Catalyst 4000 • Catalyst 2900 • Catalyst 2950 XL
Trunk Port Groups • 1 GB Ethernet • 10MB-100MB Ethernet • ATM • Others	A switch port that is connected to a switch, hub, or bridge.	Any switch, hub, or bridge

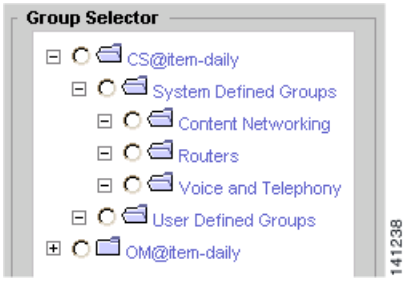
Table 17-1 Operations Manager System-Defined Groups (continued)/Device Types

Group Name	Definition	Examples
Voice Gateways	Any Cisco switch or router that is voice enabled (contains a voice card or voice port and its function is to aid IP Telephony operations).	Switch or router with BRI, E and M, FXS, FXO, T1 or E1 ports. Routers with gatekeeper functions. For example: • Cisco 1700 • Cisco 2600 • Cisco 3600 • Cisco 5300 • Cisco 5400 • Cisco 5800 • Cisco 7200 • Cisco 7500 • Cisco VG-200 • Cisco VG-248 • Catalyst 6000 • Catalyst 4000 • Catalyst 3500 • Catalyst 2900 • [and so on]
Voice Mail Gateways	Any device that connects IP Telephony voice mail systems with legacy voice mail systems.	• DPA-7610 • DPA-7639

Common Services System-Defined Groups

The Common Services system-defined groups, as shown in Figure 17-3, are visible to all users, and are the default groups administered by Common Services. Not all system-defined groups are shown in Figure 17-3 because groups only appear in the group selector when they have device members (in other words, devices in the DCR that belong to that group).

Figure 17-3 Group Selector Showing Common Services System-Defined Groups



The following are the Common Services system-defined groups:

- Broadband Cable
- Content Networking
- DSL and LRE
- Interfaces and Modules
- Network Management
- Optical
- Routers
- Security and VPN
- Storage Networking
- Switches and Hubs
- Universal Gateways and Access Servers
- Unknown
- Voice and Telephony
- Wireless

For more information about Common Services system-defined groups, refer to the Common Services online help.

Working with User-Defined Groups

Because you cannot change the rules for system-defined groups, Operations Manager provides user-defined groups that can contain the devices, ports, or interfaces in which you are interested. Port and interface containment is only seen and used by Polling and Thresholds (see Configuring Polling and Thresholds, page 19-1), but device groups will contain members when devices are added to the Operations Manager inventory. Once you edit or create a group, you can determine whether other users can view the group.

User-defined groups are the basis for the views that appear in the Monitoring Dashboards (Service Level View, Alerts and Events, Phone Activities, and Service Quality Alerts). For every user-defined group you create, a corresponding view is automatically created. For creating user-defined groups, see Creating and Editing Groups, page 17-11.

By default, no devices belong to the predefined user-defined groups. To see membership details for the groups that are created in the Access Port, Interface, and Trunk port folders, you must go to the polling and thresholds pages. (See Configuring Polling and Thresholds, page 19-1.)

Table 17-2 describes the predefined user-defined groups.

Table 17-2 Operations Manager User Defined Groups

Group Name	Use this group to monitor...	Settings you can configure for this group:
Access Port Groups	Access ports	Thresholds
Interface Groups	Interfaces	Thresholds
Trunk Ports Groups	Trunk ports	Thresholds

Using Group Administration and Configuration

The Group Administration and Configuration page is where all group management activities take place. To open the Group Administration and Configuration page, select **Devices > Device Groups**.

These topics explain how to use the Group Administration and Configuration page:

- Creating and Editing Groups, page 17-11
- Viewing Group Details, page 17-29
- Viewing Membership Details, page 17-30
- Refreshing Membership, page 17-31
- Deleting Groups, page 17-32

Figure 17-4 shows an example of the Group Administration and Configuration page.

Figure 17-4 Group Administration and Configuration Page

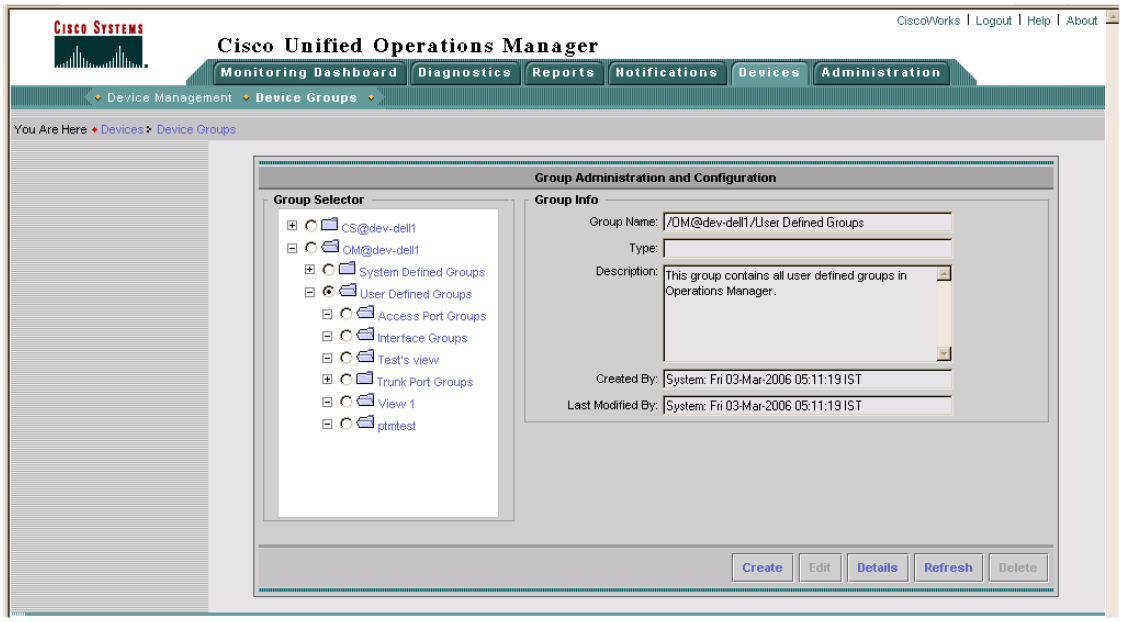


Table 17-3 describes the fields in the Group Administration and Configuration page.

Table 17-3 Fields on Group Administration and Configuration Page

GUI Element	Description
Group selector	A hierarchical display of all available groups.
Group Info pane	When you select an item from the Group Selector, the Group Info pane displays the following information: • Group Name—The name of the group you selected. • Type—The type of Unified Communications s in the selected group. • Description—A text description of the group. • Created By—The person who created the group. • Last Modified By—The last person to edit the group settings.
Create button	Starts the Group Creation Wizard for creating a group, as described in the "Creating a Group" section on page 17-12.
Edit button	Starts the Group Edit Wizard for editing an existing group, as described in the "Editing Group Properties" section on page 17-19.
Details button	Opens the Properties: Details page, as described in the "Viewing Group Details" section on page 17-29.
Refresh button	Refreshes a group's membership, as described in the "Refreshing Membership" section on page 17-31.
Delete button	Deletes a group, as described in the "Deleting Groups" section on page 17-32.

Creating and Editing Groups

The processes for creating and editing groups are similar.

Keep these points in mind:

- You can only *edit* the predefined user-defined group folders (Access Port Groups, Interface Groups, and Trunk Port Groups), which means you cannot remove these folders from the device selector. Once you create a user-defined group under any of these folders, you can edit or delete the group you created. (See Creating an Access Port, Interface, or Trunk Port Group, page 17-15 and Editing an Access Port, Interface, or Trunk Port Group, page 17-21.)
- You can *create or edit* all other user-defined groups (to use with, for example, views in the Monitoring Dashboard displays, or with notification groups in Notification Services). For example, you could create a group called test, which would appear directly under Operations Manager User Defined Groups in the Operations Manager group selector. (See Creating a Group, page 17-12 and Editing Group Properties, page 17-19.)

Operations Manager uses the Group Creation Wizard to guide you through the steps required to create or edit a group. The wizards steps will vary depending on what you are creating. For example, the steps for creating a group using a template (see Creating a Group—Using a Template, page 17-17 and Editing Group Properties—For a Group that Uses a Template, page 17-22) are different from the steps for creating a user-defined group without using a template. Further, if you are creating an Access Port, Interface, or Trunk Port group, the wizard steps are different.

For creating a user-defined group, the wizard consist of four steps:

1. Setting properties (for details, see Creating a Group, page 17-12 and Editing Group Properties, page 17-19).
2. Creating rules (for details, see Understanding Rules, page 17-23).
3. Editing group membership (for details, see Finalizing Group Membership, page 17-28).
4. Viewing the summary (for details, see Viewing the Group Summary, page 17-28).

Note Operations Manager provides you with templates to make it easier for you to create user-defined groups. The four templates that are provided are based on the following:

- Location
- Name
- Subnet
- Service

For instructions on creating groups using the templates, see Creating a Group—Using a Template, page 17-17.

Creating a Group

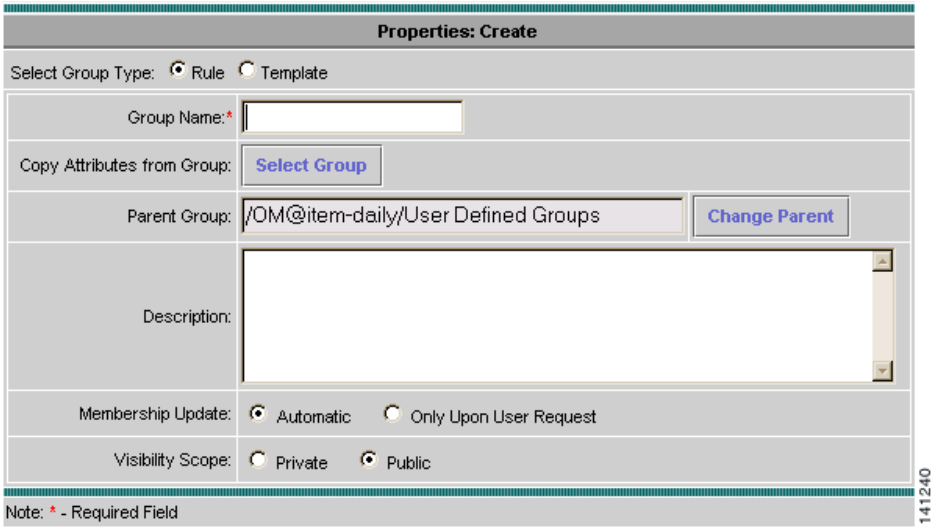
Step 1 Select **Devices > Device Groups**. The Group Administration and Configuration page appears.

Step 2 In the Group Selector, select the parent group under which you want the new group to reside.

Note You must select the User Defined Groups folder or any subfolder. You can only add user-defined groups under the User Defined Groups folder.

Step 3 Click **Create**. The Properties: Create page appears. Figure 17-5 shows an example of the Properties: Create Page.

Figure 17-5 Properties: Create Page



Step 4 In the Select Group Type field, select the Rule radio button.

Step 5 Enter a group name for the new group. The group name cannot contain single quotation marks, dots, or backslashes.

Step 6 If you do not want to copy the attributes of an existing group to your new group, proceed to Step 7. If you want to copy the attributes of an existing group to the new group, do the following:

Note All attributes except the group name are copied to the new group.

a. Click **Select Group**. The Replicate Attributes page appears.

b. Select the group from which you want to copy the attributes.

c. Click **OK**.

Step 7 If you want to change the parent group (the location where the group will reside in the Group Selector), do the following:

a. Click **Change Parent**. The Select Parent page appears.

b. Select the parent group.

c. Click **OK**.

Step 8 (Optional) Enter a description.

Step 9 Choose how you want the group membership updated:

- If you want the membership for this group updated automatically, select automatic.
- If you want the membership for this group updated only when the Refresh button is clicked, select Only Upon User Request.

Step 10 Select a Visibility Scope:

- Private—Available to created user only
- Public—Available to all users

Step 11 Click **Next**. The Rules: Create page appears. (For more information on creating rules, see Understanding Rules, page 17-23.)

Do one of the following:

- To create rules to apply to the group, go to Step 12.
- If you only want to add devices, click **Next** and select the devices on the Membership: Create page. Then go to Step 13.

Note If you need to return to any of the previous pages in the wizard, click **Back**.

Step 12 Create all rules that you want to apply to the group:

a. From the first list, select a logical operator.

Note The list of logical operators is enabled after at least one rule expression is entered.

b. Select an object type.

c. Select a variable.

d. Select an operator.

e. In the Value field, enter a value.

f. Click **Add Rule Expression**. The rule expression appears in the Rule Text box.

Note You can manually add or change any of the text in the Rule Text box. If you enter a single backslash (\), an error is displayed. To enter a single backslash in the Rule Text box, you must type two backslashes (\\) in place of the single backslash. You should always check the syntax after changing a rule expression.

g. If you have added complex rules (containing both AND and OR conditions), you must manually enter parentheses, as in the following example:

```
(:AccessPort.Mode equals "" OR
:AccessPort.Mode contains "BACKUP" OR
:AccessPort.Mode contains "NORMAL") AND
(:AccessPort.DuplexMode contains "HALFDUPLEX" OR
:AccessPort.DuplexMode contains "FULLDUPLEX")
```

h. To verify that the rule syntax is correct, click **Check Syntax**. A dialog box appears, stating that the syntax is valid. Click **OK**.

i. If you want to view the rules for the parent group, select **View Parent Rules**.

Note All rules assigned to a parent group also apply to any of its subgroups.

j. Click **Next**. The Membership: Create page appears.

Step 13 You can add or remove specific Unified Communications s from the group membership (not supported for port and interface groups).

Note The group's rule captures the list of Unified Communications s that are added to or deleted from the group. The rule will contain an Includelist and/or Excludelist section to reflect this.

Although it is acceptable for a rule to have more than one Includelist or Excludelist, the recommended practice is to consolidate them, forming one Includelist and one Excludelist. Check for duplicates across both lists and ensure that no device is both included and excluded.

Note Some IPSLA devices do not automatically appear in the Unified Communications s Matching Membership column, even though they belong to the created group. You will have to manually move these devices from the Unified Communications s from Parent Group column to the Unified Communications s Matching Membership column in the Membership: Create page.

To add an Unified Communications :

a. In the Unified Communications s from Parent Group column, select the device to add.

b. Click **Add**.

To delete an Unified Communications :

a. In the Unified Communications s Matching Membership column, select the device to remove.

b. Click **Remove**.

Step 14 Click **Next**. The group's information appears on the Summary: Create page.

Step 15 Click **Finish**.

Creating an Access Port, Interface, or Trunk Port Group

Step 1 Select **Devices > Device Groups**. The Group Administration and Configuration page appears.

Step 2 In the Group Selector, select the parent group under which you want the new group to reside.

Note You must select one of the following folders: Access Port Groups, Interface Groups, or Trunk Port Groups.

Step 3 Click **Create**. The Properties: Create page appears.

Step 4 Enter a group name for the new group.

Note When you enter the group name; if you want to use special characters, the only allowable special characters are periods, underscores, and dashes.

Step 5 If you do not want to copy the attributes of an existing group to your new group, proceed to Step 7. If you want to copy the attributes of an existing group to the new group, do the following:

Note All attributes except the group name are copied to the new group.

a. Click **Select Group**. The Replicate Attributes page appears.

b. Select the group from which you want to copy the attributes.

c. Click **OK**.

Step 6 If you want to change the parent group (the location where the group will reside in the Group Selector), do the following:

a. Click **Change Parent**. The Select Parent page appears.

b. Select the parent group.

c. Click **OK**.

Step 7 (Optional) Enter a description.

Step 8 Select a Visibility Scope:

- Private—Available to created user only
- Public—Available to all users

Step 9 Click **Next**. The Rules: Create page appears. (For more information on creating rules, see Understanding Rules, page 17-23.)

Note If you need to return to any of the previous pages in the wizard, click **Back**.

Step 10 Create all rules that you want to apply to the group:

a. From the first list, select a logical operator.

Note The list of logical operators is enabled after at least one rule expression is entered.

b. Select an object type. You will have only one choice. This is dictated by which parent group you selected in Step 2.

c. Select a variable.

d. Select an operator.

e. In the Value field, enter a value.

f. Click **Add Rule Expression**. The rule expression appears in the Rule Text box.

Note You can manually add or change any of the text in the Rule Text box. If you enter a single backslash (\), an error is displayed. To enter a single backslash in the Rule Text box, you must type two backslashes (\\) in place of the single backslash. You should always check the syntax after changing a rule expression.

g. If you have added complex rules (containing both AND and OR conditions), you must manually enter parentheses, as in the following example:

```
(:AccessPort.Mode equals "" OR
:AccessPort.Mode contains "BACKUP" OR
:AccessPort.Mode contains "NORMAL") AND
(:AccessPort.DuplexMode contains "HALFDUPLEX" OR
:AccessPort.DuplexMode contains "FULLDUPLEX")
```

h. To verify that the rule syntax is correct, click **Check Syntax**. A dialog box appears, stating that the syntax is valid. Click **OK**.

i. If you want to view the rules for the parent group, select **View Parent Rules**.

Note All rules assigned to a parent group also apply to any of its subgroups.

j. Click **Next**. The group's information appears on the Summary: Create page.

Step 11 Click **Finish**.

Creating a Group—Using a Template

To simplify the group creation process, Operations Manager provides you with templates to help you create a group. The groups you create can only be listed in the group selector under the User Defined Groups folder.

Note The groups that you create using these templates can only be based on the single attribute of the template. If you need to create a group using multiple attributes, you must create a rule. See Creating a Group, page 17-12.

Operations Manager provides the following templates:

- Location based—Creates a group based on device locations. In the group creation wizard you can enter a comma-separated list of locations, and all the devices in the listed locations will appear in the group.
- Name based—Creates a group based on device names. In the group creation wizard you can enter a comma-separated list of device names, and all the devices with the specified names will appear in the group.
- Subnet based—Creates a group based on the devices's subnet. In the group creation wizard you can enter a comma-separated list of subnets, and all the devices in those subnets will appear in the group.
- Service based—Creates a group based on the type of service the device provides. In the group creation wizard you can enter a comma-separated list of device services, and all the devices that provide the specified services will appear in the group. There are specific services that you can enter to create a service based group. You can only use the services that appear in the following list:

  Note The service name must be entered just as it appears in this list.

  - callmanager
  - IPSLA

- callmanager express
- unity express
- conference connection
- unity connection
- emergency responder
- unity
- SRST
- gatekeeper
- h323
- mgcp
- Unified CCE

Step 1 Select **Devices > Device Groups**. The Group Administration and Configuration page appears.

Step 2 In the Group Selector, select the parent group under which you want the new group to reside.

Note You must select the User Defined Groups folder or any subfolder. You can only add user-defined groups under the User Defined Groups folder.

Step 3 Click **Create**. The Properties: Create page appears.

Step 4 In the Select Group Type field, select the Template radio button.

Step 5 Enter a group name for the new group.

Note When you enter the group name; if you want to use special characters, the only allowable special characters are periods, underscores, and dashes.

Step 6 If you want to change the parent group (the location where the group will reside in the Group Selector), do the following:

a. Click **Change Parent**. The Select Parent page appears.

b. Select the parent group.

c. Click **OK**.

Step 7 (Optional) Enter a description.

Step 8 Choose how you want the group membership updated:

- If you want the membership for this group updated automatically, select automatic.
- If you want the membership for this group updated only when the Refresh button is clicked, select Only Upon User Request.

Step 9 Select a Visibility Scope:

- Private—Available to the creator only
- Public—Available to all users

Step 10 Click **Next**. The Templates: Create page appears.

Step 11 In the Template Name field, select the template you want to base your group selection on.

Step 12 (Optional) Enter a description.

Step 13 In the List of Values field, enter the values that you want to use for filtering. For example, if you choose the name-based template, you can enter a list of device names.

Note Wild cards are not supported. Also, the operator that is being used for filtering is contains. For example, if you enter *test*, all devices that contain *test* anywhere in their name will be displayed.

Step 14 Click **Next**. The Membership: Create page appears. You can view the members of the group, but you cannot make any changes.

Step 15 Click **Next**. The group's information appears on the Summary: Create page.

Step 16 Click **Finish**.

Editing Group Properties

Step 1 Select **Devices > Device Groups**. The Group Administration and Configuration page appears.

Step 2 In the Group Selector, select the group you want to edit.

Step 3 Click **Edit**. The Properties: Edit page appears.

Step 4 You can edit the following in the Properties: Edit page:

- Group Name

Note When you enter the group name; if you want to use special characters, the only allowable special characters are periods, underscores, and dashes.

- Description
- Membership update type (not supported for port and interface groups)
- Visibility Scope

Note The parent group is displayed, but it cannot be edited.

Step 5 Click **Next**. The Rules: Edit page appears. For more information on creating rules, see Understanding Rules, page 17-23.

Note If you need to return to any of the previous pages in the wizard, click **Back**.

Step 6 You can add new rules or delete existing rules in the Rules: Edit page.

To add a new rule:

a. From the first list, select a logical operator.

Note The list of logical operators is enabled after at least one rule expression is entered.

b. From the Object Type list, select an object type.

c. From the Variable list, select a variable.

d. From the Operator list, select an operator.

e. In the Value field, enter a value.

f. Click **Add Rule Expression**. The rule expression appears in the Rule Text box.

Note You can manually add or change any of the text in the Rule Text box. If you enter a single backslash (\), an error is displayed. To enter a single backslash in the Rule Text box, you must type two backslashes (\\) in place of the single backslash. You should always check the syntax after changing a rule expression.

g. If you have added complex rules (containing both AND and OR conditions), you must manually enter parentheses, as in the following example:

```
(:AccessPort.Mode equals "" OR
:AccessPort.Mode contains "BACKUP" OR
:AccessPort.Mode contains "NORMAL") AND
(:AccessPort.DuplexMode contains "HALFDUPLEX" OR
:AccessPort.DuplexMode contains "FULLDUPLEX")
```

h. To verify that the syntax of the rule is correct, click **Check Syntax**. A dialog box appears, stating that the syntax is valid. Click **OK**.

i. If you want to view the rules for the parent group, select **View Parent Rules**.

Note All rules assigned to a parent group also apply to any of its subgroups.

j. Click **Next**. The Membership: Edit page appears.

To delete a rule:

a. In the Rule Text box, select the entire rule text and press the **Delete** key.

After deleting the rule, you must click the page so that the page can refresh, removing the list of logical operators.

b. Click **Next**. The Membership: Edit page appears.

Step 7 You can add or remove specific Unified Communications s from the group membership (not supported for port and interface groups).

Note The group's rule captures the list of Unified Communications s that are added to or deleted from the group. The rule will contain an Includelist and/or Excludelist section to reflect this.

Although it is acceptable for a rule to have more than one Includelist or Excludelist, the recommended practice is to consolidate them, forming one Includelist and one Excludelist. Check for duplicates across both lists and ensure that no device is both included and excluded.

Note Some IPSLA devices do not automatically appear in the Unified Communications s Matching Membership column, even though they belong to the created group. You will have to manually move these devices from the Unified Communications s from Parent Group column to the Unified Communications s Matching Membership column in the Membership: Create page.

To add an Unified Communications :

a. In the Available Unified Communications s from Parent Group column, select the device to add.

b. Click **Add**.

To remove an Unified Communications :

a. In the Unified Communications s Matching Membership Criteria column, select the device to remove.

b. Click **Remove**.

Step 8 Click **Next**. The group's information appears on the Summary: Edit page.

Step 9 Click **Finish**.

Editing an Access Port, Interface, or Trunk Port Group

Step 1 Select **Devices > Device Groups**. The Group Administration and Configuration page appears.

Step 2 In the Group Selector, select the access port group, interface group, or trunk port group that you want to edit.

Step 3 Click **Edit**. The Properties: Edit page appears.

Step 4 You can edit the following in the Properties: Edit page:

- Description
- Visibility scope

Step 5 Click **Next**. The Rules: Edit page appears. (For more information on creating rules, see Understanding Rules, page 17-23.)

Note If you need to return to any of the previous pages in the wizard, click **Back**.

Step 6 You can add new rules or delete existing rules in the Rules: Edit page.

To add a new rule:

a. From the first list, select a logical operator.

Note The list of logical operators is enabled after at least one rule expression is entered.

b. From the Object Type list, select an object type.

c. From the Variable list, select a variable.

d. From the Operator list, select an operator.

e. In the Value field, enter a value.

f. Click **Add Rule Expression**. The rule expression appears in the Rule Text box.

Note You can manually add or change any of the text in the Rule Text box. If you enter a single backslash (\), an error is displayed. To enter a single backslash in the Rule Text box, you must type two backslashes (\\) in place of the single backslash. You should always check the syntax after changing a rule expression.

g. If you have added complex rules (containing both AND and OR conditions), you must manually enter parentheses, as in the following example:

```
(:AccessPort.Mode equals "" OR
:AccessPort.Mode contains "BACKUP" OR
:AccessPort.Mode contains "NORMAL") AND
(:AccessPort.DuplexMode contains "HALFDUPLEX" OR
:AccessPort.DuplexMode contains "FULLDUPLEX")
```

h. To verify that the syntax of the rule is correct, click **Check Syntax**. A dialog box appears, stating that the syntax is valid. Click **OK**.

i. If you want to view the rules for the parent group, select **View Parent Rules**.

Note All rules assigned to a parent group also apply to any of its subgroups.

j. Click **Next**. The Membership: Edit page appears.

To delete a rule:

a. In the Rule Text box, select the entire rule text and press the **Delete** key.

After deleting the rule, you must click the page so that the page can refresh, removing the list of logical operators.

b. Click **Next**. The group's information appears on the Summary: Edit page.

Step 7 Click **Finish**.

Editing Group Properties—For a Group that Uses a Template

Step 1 Select **Devices > Device Groups**. The Group Administration and Configuration page appears.

Step 2 In the Group Selector, select the group you want to edit.

Step 3 Click **Edit**. The Properties: Edit page appears.

Step 4 You can edit the following in the Properties: Edit page:

- Group Name

Note When you enter the group name; if you want to use special characters, the only allowable special characters are periods, underscores, and dashes.

- Description
- Membership update type (not supported for port and interface groups)

- Visibility Scope

Note The parent group is displayed, but it cannot be edited.

Step 5 Click **Next**. The Templates page appears.

Step 6 You can change the following in the Templates page:

- Template
- Description
- List of Values

Step 7 Click **Next**. The Membership: Edit page appears. You can view the members of the group, but you cannot make any changes.

Step 8 Click **Next**. The group's information appears on the Summary: Edit page.

Step 9 Click **Finish**.

Understanding Rules

Every group is defined by a set of rules. A rule set contains a Boolean combination of individual rule expressions.

Rules are created to filter in the objects that you want to belong to the group, and to filter out those that you do not want in the group. When determining which Unified Communications s belong to a group, Group Management compares object information to the rule. If an Unified Communications 's information satisfies all of the rule's requirements, it is placed in the group.

One or more rule expressions can be applied to form a rule.

Each rule expression contains the following:

<object type>.<variable> <operator> <value>

For example:

```
:Gatekeeper.Cisco_CommunicationManager_or_Cluster.Name equals "ccm test1"
```

Rules are defined through the Group Creation Wizard on the Rules: Create page.

You can define the following:

- OR, AND, EXCLUDE—Logical operators. This field appears after a rule expression is added in the Rule Text box.
  - OR—Include devices that fulfill the requirements of either rule.
  - AND—Include only devices that fulfill the requirements of both rules.

Note When using the AND operator, the rule expressions cannot contain different types of devices. For example, you cannot use the AND operator with the following rule expressions:

```
:Gatekeeper
:MediaServer
```

In this example, you would have to use the OR operator.

  - EXCLUDE—Do not include these devices.

- Object Type—The type of object that is used to form a group. The object can be all devices, a group, or a type of device.

  In the Object Type field you will see the following choices:

  - AccessPort
  - Device
  - CUE
  - DigitalVoiceGateway
  - Gatekeeper
  - Unified CCE
  - MediaServer
  - PhoneAccessSwitch
  - VoiceGateway
  - VoiceMailGateway
  - Interfaces
  - PRPhone
  - SRSTDevice
  - TrunkPort

- Variable—An attribute of the selected object type to be used for the rule. The list of possible variables changes based on the object type that is selected.
- Operator—The operator to be used in the rule. The list of possible operators changes based on the object type and the variable selected.

  Note When using the *equals* operator the rule is case-sensitive.

- Value—The value of the rule expression. The possible values depend upon the object type, variable, and operator selected. Depending on the operator selected, the value may be free-form text or a list of values.

Some devices (Object Types) cannot be grouped using certain attributes (Variables), because the attributes for these devices do not exist. Table 17-4 lists the devices and the attributes.

Table 17-4 Devices and Attributes that Cannot Be Used for Grouping

Device (Object Type)	Attributes (Variables)
DigitalVoiceGateway	• IP.Address • IP.Netmask • Location • Type • SystemObjectID
Any device with these attributes	• VoiceInterface.Type • VoicePort.Type

Note After you have defined the rule, you should verify the syntax. You can do this on the Rules: Create page.

Figure 17-6 shows an example of the Rules: Create page.

Figure 17-6 Rules: Create Page

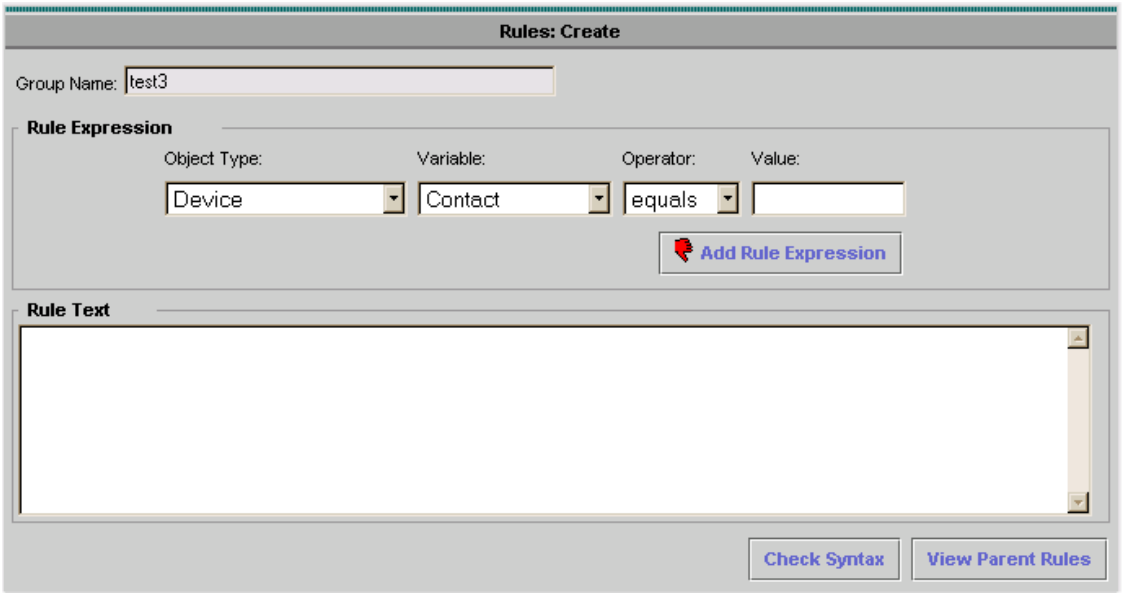


Table 17-5 describes the fields on the Rules: Create page of the Group Creation Wizard.

Table 17-5 Fields on the Rules: Create Page

GUI Element	Description
OR, AND, EXCLUDE drop down list	Logical operators. • OR—Include devices that fulfill the requirements of either rule. • AND—Include only devices that fulfill the requirements of both rules. • EXCLUDE—Do not include these devices. This field is present only after a rule expression is added in the Rule Text box.
Object Type drop down list	The type of object that is used to form the group.
Variable drop down list	The attribute of the selected object type to be used for the rule.
Operator drop down list	The operator to be used in the rule.
Value field	The value of the rule expression.
Add Rule Expression button	Used to add the rule expression to the group rules.
Rule Text field	Displays the rule.
Check Syntax button	Verifies that the rule syntax is correct.
View Parent Rules button	Used to view the parent group rules. **Note** All parent group rules apply to the subgroups.

Understanding What to Enter in the Value Field

Most of the values that can be entered in the Value field of the Rules: Create page are self-evident, but some of the Unified Communications s in the Variables field have special meanings or restrictions on how to enter the related attribute in the Value field.

Table 17-6 describes the Unified Communications s that appear in the Variable field of the Rules: Create page that might need further explanation.

Table 17-6 Explanations of Special Variables

Variable	Explanation
Cisco_CommunicationManager_Or_Cluster.Name	The name of the cluster to which the device belongs. You can find the cluster names by opening the Group Configuration page and selecting the Cisco_CommunicationManager_Or_Cluster group. A list of cluster group names appears. Use these names in the Value field of the Rules: Create page.
Type	The capability of the device. In the Value field of the Rules: Create page, use the following corresponding values for the device: • MediaServer—MediaServer • VoiceMailGateway—VoiceMailGateway • PhoneAccessSwitch—SWITCH or ROUTER • VoiceGateway—SWITCH, ROUTER, or VG248 • Gatekeeper—ROUTER, SWITCH • Router—ROUTER • Switch—SWITCH **Note** When using the *equals* operator in the rule, enter the values exactly as indicated.
ClassName	In the Value field of the Rules: Create page, use the following corresponding values: • VoiceGateway—VoiceGateway • MediaServer—MediaServer • VoiceMailGateway—VoiceMailGateway
Interfaces	In the Value field of the Rules: Create page, use the following corresponding values: • LAPD • DS1 • FXS/FXO • FXS/FXO,DS1

Examples of Rules

Example 1

You want to create a group that contains all of the media servers in the vegas cluster. Form the following rule:

```
:MediaServer.Cisco_CommunicationManager_or_Cluster.Name contains "VEGAS"
```

- Object Type—MediaServer
- Variable—Cisco_CommunicationManager_or_Cluster.Name

- Operator—contains
- Value—“VEGAS”

Example 2

You want to create a group that contains all of the voice gateways that have 172 as part of their IP address.

```
:VoiceGateway.IP.Address contains "172"
```

- Object Type—VoiceGateway
- Variable—IP.Address
- Operator—contains
- Value—“172”

Example 3

You want to create a group that contains all of the phone access switches in the San Jose location.

```
:PhoneAccessSwitch.Location equals "San Jose"
```

- Object Type—PhoneAccessSwitch
- Variable—Location
- Operator—equals
- Value—“San Jose”

Note To help you to better understand group rules, you may want to look at the rules used for system-defined groups. These rules appear in the Properties: Details page. For a description of the Properties: Details page, see Viewing Group Details, page 17-29.

Finalizing Group Membership

After the group rules have been defined, they are evaluated, and you can view the group’s members. In addition, the group membership can be modified by adding or removing specific Unified Communications s. The group rule will be automatically modified to reflect the Unified Communications s that were added or removed from the group. You add or remove specific Unified Communications s from a group’s membership in the Membership: Create page of the Create Group Wizard.

Note If you used a template to create your group, you can only view membership details. You cannot add or remove Unified Communications s from a group’s membership in the Membership: Create page.

Viewing the Group Summary

The final step in the Create Group Wizard is a summary page that displays the new group’s definition. Figure 17-7 shows an example of the Summary: Create page.

Figure 17-7 Summary: Create Page

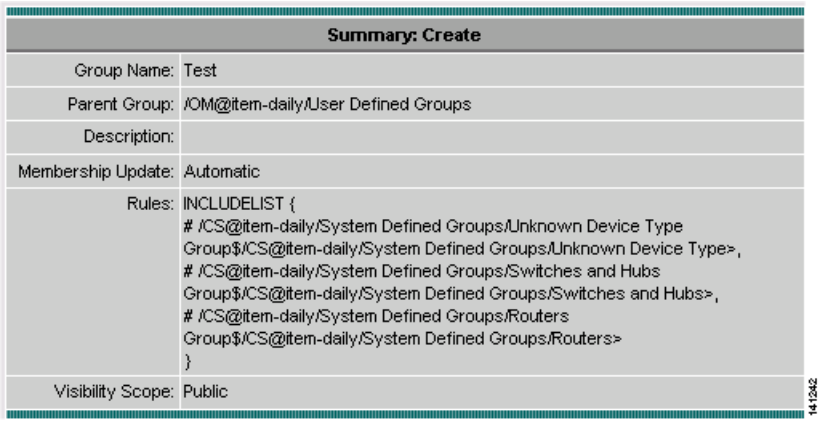


Table 17-7 describes the fields on the Summary: Create page of the Group Creation Wizard.

Table 17-7 Fields on the Group Summary Page

Heading/Button	Description
Group Name	Name of the group you are creating.
Parent Group	The parent group of the group you are creating.
Description	A text description of the group.
Membership Update	How group membership is updated. Membership updates can be automatic (updated every time the group is accessed) or can be upon user request only (updated only when you click the Refresh button).
Rules	The rules used to filter group membership.
Visibility Scope	Setting that determines whether all users or only the created user can view the group.

Viewing Group Details

A group's information is displayed on the Properties: Details page.

Step 1 Select **Devices > Device Groups**. The Group Administration and Configuration page appears.

Step 2 In the Group Selector, select the group for which you want to view details.

Step 3 Click **Details**. The Properties: Details page appears (see Figure 17-8).

Figure 17-8 Properties: Details Page

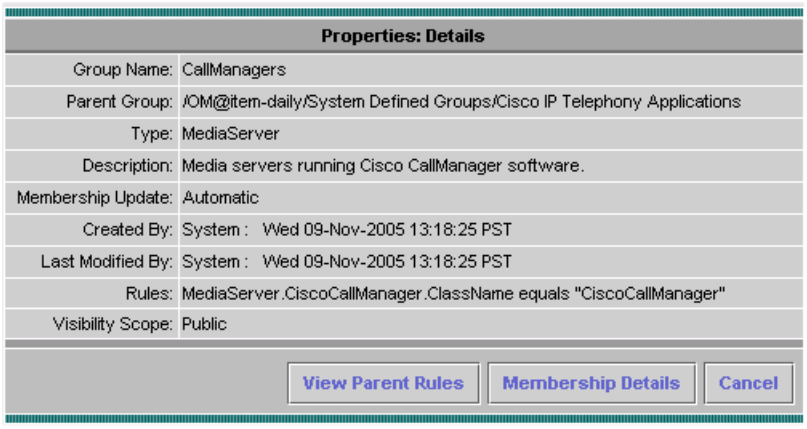


Table 17-8 describes the fields on the Properties: Details page.

Table 17-8 Fields on the Properties: Details Page

Heading/Button	Description
Group Name	Name of the group you are viewing.
Parent Group	The parent group of the group you are viewing.
Type	The type of the Unified Communications s that belong to the group.
Description	A text description of the group.
Membership Update	How group membership is updated. Membership updates can be automatic (updated every time the group is accessed) or can be upon user request only (updated only when you click the Refresh button).
Created By	The person who created the group.
Last Modified By	The last person to edit the group.
Rules	The rules used to filter group membership.
Visibility Scope	Setting that determines whether all users or only the created user can view the group.
View Parent Rules	Used to view the parent group rules. **Note** All parent group rules apply to the subgroups.
Membership Details	Used to view membership details. See Viewing Membership Details, page 17-30.
Cancel	Closes the page and takes you back to the Group Administration and Configuration page.

Viewing Membership Details

You can view a list of the Unified Communications s that belong to a group by accessing the Membership: Details page.

Step 1 **Select Devices > Device Groups**. The Group Administration and Configuration page appears.

Step 2 In the Group Selector, select the group for which you want to view details.

Step 3 Click Details. The Properties: Details page appears.

Step 4 Click **Membership Details**. The Membership: Details page appears.

Figure 17-9 shows an example of the Membership: Details page.

Figure 17-9 Membership: Details Page

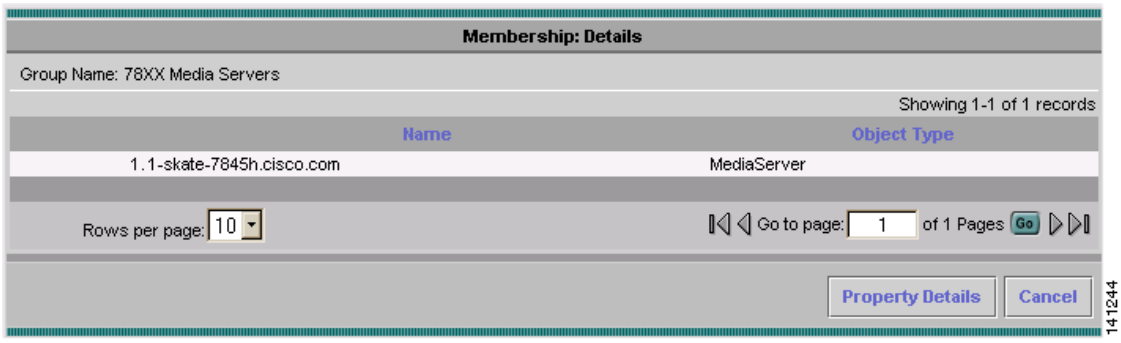


Table 17-9 describes the fields on the Membership: Details page.

Table 17-9 Fields on the Membership: Details Page

Heading/Button	Description
Name	Name of the device for which you want to view membership details.
Object Type	The type of object for which you want to view details.
Property Details	Takes you back to the Properties: Details page.
Cancel	Closes the page and takes you back to the Group Administration and Configuration page.

Refreshing Membership

Refreshing a group's membership forces the group to recompute its membership by reevaluating its rules and obtaining membership information from the data collectors. Port and interface group membership listings are not supported, because these groups are only used for polling and threshold purposes.

Step 1 Select **Devices > Device Groups**. The Group Administration and Configuration page appears.

Step 2 In the Group Selector, select the group you want to refresh.

Step 3 Click **Refresh**.

Step 4 In the confirmation dialog box, click **Yes**. In the next dialog box, click **OK**.

Deleting Groups

You can only delete user-defined groups. This includes any Access Port, Interface, or Trunk Port groups that you created. You cannot delete the Access Port Groups, Interface Groups, or Trunk Port Groups folders.

Step 1 Select **Devices > Device Groups**. The Group Administration and Configuration page appears.

Step 2 In the Group Selector, select the group you want to delete.

Step 3 Click **Delete**.

Step 4 In the confirmation dialog box, click **Yes**. In the next dialog box, click **OK**.

Note Edit, Refresh, and Delete cause internal processes to start. For this reason, Operations Manager could experience a period of high CPU utilization after these processes are triggered.

CHAPTER 18

Configuring SRST Poll Settings

The following topics describe using SRST:

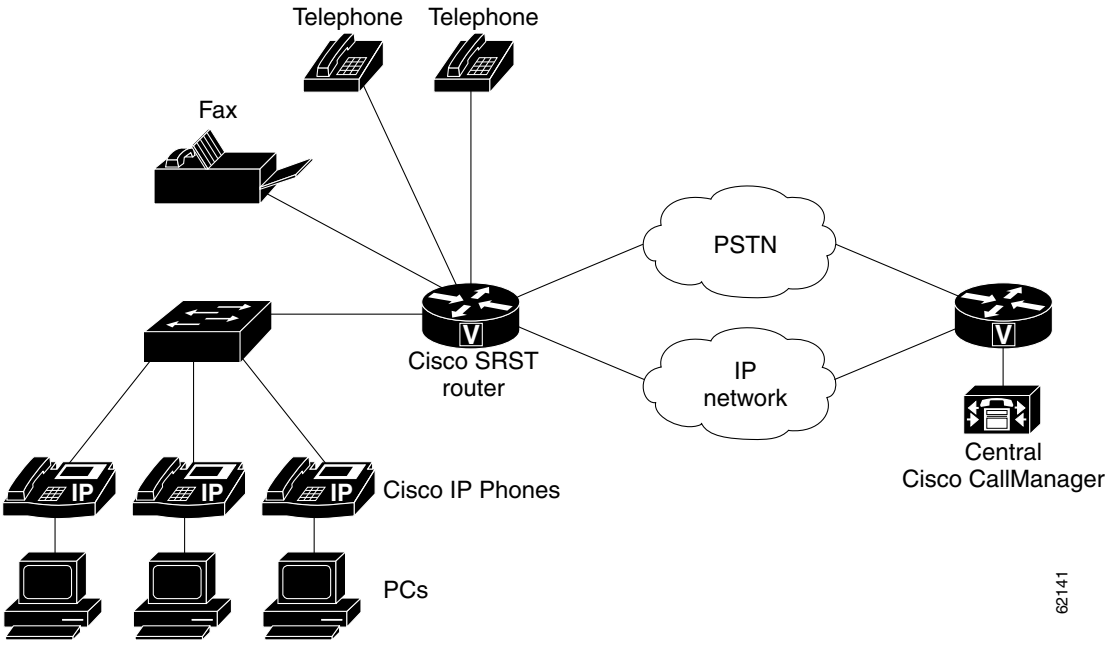
Understanding How Operations Manager Monitors SRST

Figure 18-1 shows a branch office configured for Survivable Remote Site Telephony (SRST). The branch office normally relies on a central Cisco Unified Communications Manager for call processing. If the Cisco Unified Communications Manager becomes inaccessible, phones can use a Cisco voice router for call processing. Phones go into SRST mode when either of the following happens:

- The WAN link to the Cisco Unified Communications Manager at the central site goes down
- The connection to the Cisco Unified Communications Manager is lost

SRST allows phones in branch offices to continue to function until the WAN link comes up or until the phones can register with a Cisco Unified Communications Manager again.

Figure 18-1 Branch Office Cisco Unified IP Phones Connected to a Remote Central Cisco Unified Communications Manager



For Operations Manager to display phones in SRST mode and generate related alerts, you must configure SRST poll settings, identifying the SRST components for Operations Manager to test. Operations Manager does the following:

- Configures IP SLA jitter tests on the source router (at the central Cisco Unified Communications Manager site). Jitter tests run from the source router to detect the reachability of the target SRST router (at the branch office).
- Generates an SRSTEntered event when a jitter test fails, which happens in response to the WAN link being down. See Appendix E, "Events Processed," for information about the SRSTEntered and SRSTSuspected events.
- Displays a list of Cisco Unified IP Phones that are in SRST mode on phone reports. See Generating the SRST IP Phones Report, page 13-8 and Generating the All IP Phones/Lines Report, page 13-8.

Before you configure SRST poll settings, review the recommendations for your deployment of SRST.

Note If you ever need to uninstall Operations Manager, be sure to delete all the SRST tests from the application before you uninstall it. If you do not delete these tests, they will continue to run on the router. For instructions on deleting, see Deleting SRST Poll Settings, page 18-5.

Requirements and Recommendations for SRST Poll Settings

Note This topic does not explain how to configure Cisco Unified Communications Manager, Cisco routers, or Cisco Unified IP Phones for SRST. See the documentation for these products at http://www.cisco.com.

Table 18-1 lists recommendations and requirements for selecting the source router, near the central Cisco Unified Communications Manager, and configuring the SRST target router, at the branch office. See Figure 18-1 for an illustration of a sample configuration.

Table 18-1 Choosing and Configuring Source and Target Routers

Router	Requirements	Recommendations
Source	Choose the source router in such a way that the following paths are the same: • Path of the IP phone TCP keepalive message to the central site Cisco Unified Communications Manager • IP SLA jitter test packet path	Select a source router that is as close to the Cisco Unified Communications Manager as possible.
Target	Enable Cisco IOS IP SLA (IP SLA) Responder on the SRST target router.	**Note** If you disable IP SLA Responder on the target router, spurious SRSTEntered events might occur. See the SRSTEntered event in Appendix E, "Events Processed."

Note Operations Manager creates IP SLA tests on the source routers. These routers must have adequate probe capacity for Operations Manager to successfully create the IP SLA tests.

Monitoring SRST when Source or Target Routers Are Down

Table 18-2 shows how Operations Manager handles SRST activities when devices are down or unreachable.

Table 18-2 Creating SRST Poll Settings or Monitoring for SRST when Devices Are Down

Device Down or Unreachable	During the following SRST activity	Result
Source or target router	Import SRST information	The poll setting will be imported successfully, but will not be created on the routers. **Workaround**: Import SRST poll settings again after the routers become reachable.
	Create SRST poll setting	The poll setting will not be created. **Workaround**: Import SRST poll settings again after the routers become reachable.
Source router	SRST polling	Operations Manager cannot retrieve SRST results. Operations Manager does not detect SRST or generate SRST events. **Note** Operations Manager will generate appropriate events for devices that are unreachable.

Viewing SRST-Related Event Details

When Operations Manager generates an SRSTEntered or SRSTSuspected event, an alert appears on the Alerts activities window. You can drill down through the Alert Details page to view event details. Although multiple phones might be included in an SRST poll setting, only one MAC address and one phone extension are displayed in the Event Properties window.

For more information, see the following topics:

- Viewing Events Associated with an Alert, page 3-14
- Viewing Event Details, page 3-15
- Events Processed, page E-1

Maintaining SRST Poll Settings

When you configure SRST poll settings, based on the poll settings name you provide, Operations Manager either adds a new SRST poll setting or updates an existing SRST poll setting. Operations Manager also creates or updates IP SLA jitter tests on source routers, as needed.

To remove existing SRST poll settings, you must delete them; see Deleting SRST Poll Settings, page 18-5.

Note Be sure to edit SRST poll settings after you change the SRST configuration in your network. For example, if you change MAC addresses or extension numbers on IP phones, you must reconfigure SRST poll settings.

You can configure:

- A single SRST poll setting from various launch points in the Operations Manager user interface. See Configuring a Single SRST Test as Needed, page 18-9.
- Multiple SRST poll settings by importing them from a seed file. See Importing SRST Poll Settings, page 18-5.

Viewing SRST Poll Setting Status

Step 1 Select **Administration > SRST Poll Settings > SRST Operations**. The SRST Operations page appears with the following information.

Field	Description
Test Name	SRST poll setting name
Source Router	Router in the central site on which the IP SLA test is created
Target Router	Router in the branch office
Status	• Active—SRST poll setting is running as configured. • Pending—SRST poll setting is briefly in a transient state after you click Delete. **Note** If device monitoring is suspended for a source router, any associated SRST poll setting is also suspended. See Suspending Device Monitoring, page 3-25.

Deleting SRST Poll Settings

This procedure explains how to delete one or more SRST poll settings.

Note If you delete an IP SLA router from Operations Manager device inventory, any associated SRST poll settings are automatically deleted; see Deleting Devices, page 16-36.

Step 1 Select **Administration > SRST Poll Settings > SRST Operations**. The SRST Operations page appears.

Step 2 Select any of the following:

- Check box in the table heading—Select to delete all SRST poll settings.
- One or more individual check boxes—Select individual SRST poll settings that you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears, asking if you want to continue with the deletion.

Step 4 Click **OK**.

Importing SRST Poll Settings

When you import SRST information, Operations Manager adds any new poll settings from the seed file and updates any existing poll settings that you edited. To remove existing poll settings, you must delete them; see Deleting SRST Poll Settings, page 18-5.

Note Be sure to edit SRST poll settings after you change the SRST configuration in your network. For example, if you change MAC addresses or extension numbers on IP phones, do one of the following:

- Update the seed file and import SRST information again.
- Update poll settings from the Service Level View or an IP Phones and Applications report. See Configuring a Single SRST Test as Needed, page 18-9.

Before You Begin

- Verify that your deployment of SRST meets the requirements specified in Table 18-1.
- Verify that Operations Manager monitors the devices to be polled. See Verifying that Devices Are Monitored by Operations Manager Before Import, page 18-9.
- Verify that the phones that are listed in your seed file have been discovered. To view IP phone discovery status, select **Devices > Device Management > Inventory Collection > IP Phone**.
- Verify that your seed file is formatted correctly. For details, see Formatting an SRST Monitoring Seed File, page 18-6.
- Place the seed file on the server, in the NMSROOT\ImportFiles directory. If you do not have access to the directory, contact a local administrator for the server where Operations Manager is installed.

Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as "C:\Program Files\CSCOpx" or C:\PROGRA~1\CSCOpx.

Step 1 Select **Administration > SRST Poll Settings > SRST Import**. The Import SRST Information page appears.

Step 2 Enter the name of the seed file in the Filename field and click **OK**.

Operations Manager verifies that the data in the seed file is syntactically correct and formatted properly. If there are errors in the seed file, an error dialog box is displayed:

a. Check the srst_import.log file at NMSROOT\logs\itemlogs\srst for details.

b. Correct the problems in the seed file and import the SRST information again.

If the seed file is correct, an information dialog box is displayed.

Step 3 Click **OK**. Operations Manager verifies that the routers are reachable and then creates IP SLA jitter tests on the routers. This might take some time.

Step 4 Verify that all IP SLA jitter tests were created successfully, by examining the srst_test_creation_results.log file in NMSROOT\logs\itemlogs\srst.

Note If you do not have access to this directory, contact a local administrator for the Operations Manager server.

Step 5 If IP SLA jitter tests were not successfully created, do the following:

a. Use the log file to identify problems.

b. Make corrections in the import file and return to Step 1 to import SRST information again.

Formatting an SRST Monitoring Seed File

Note The read and write community strings that you supply in the SRST seed file are used only when community strings for the source or target device do not exist in the Device and Credentials Repository (DCR). For more information, see Editing Device Configuration and Credentials, page 16-30.

Operations Manager supports two seed file formats:

- Table 18-3 lists the preferred format. In general, you should use this format.
- Table 18-4 lists another supported format.

To format the seed file correctly, do the following:

- Include up to 256 poll settings in the seed file, one poll setting per line.

  Note If you include more than 256 poll settings, Operations Manager discards the excess poll settings.

- Include the following for each poll setting:
  - A name
  - A unique combination of source and target router
  - Up to 48 phones

    Note If you include more than 48 phones, Operations Manager discards the excess phones.

  - Information for all columns listed in Table 18-3 (or Table 18-4), delimited by a comma (,)

Table 18-3 SRST Seed File–Preferred Format

Column Number	Description
1	SRST poll settings name—Must be unique.
2	IP address or DNS name of the source router—Source router and target router (column 5) combination must be unique.
3	Read community string of the source router. **Note** If no read community string exists in the DCR for the device, Operations Manager updates the DCR with this string.
4	Write community string of the source router. **Note** If no write community string exists in the DCR for the device, Operations Manager updates the DCR with this string.
5	Username—Enter a username for the source router (if you are supplying SNMPV3 credentials).
6	Password—Enter the password for the source router (if you are supplying SNMPV3 credentials).
7	IP address or DNS name of the SRST target router—Source router (column 2) and target router combination must be unique.
8	Read community string of the SRST target router. **Note** If no read community string exists in the DCR for the device, Operations Manager updates the DCR with this string.
9	Write community string of the SRST target router. **Note** If no write community string exists in the DCR for the device, Operations Manager updates the DCR with this string.

Table 18-3 SRST Seed File–Preferred Format (continued)

Column Number	Description
10	Phone extension numbers of IP telephones associated with SRST target router, delimited by a colon (:).
11	MAC addresses of IP telephones associated with SRST target router, delimited by a colon (:). **Note** MAC addresses must be sequenced in corresponding order with the phone extensions (see column 10).
12	Polling interval—Default (!{[NOVALUE]}!) = 30 seconds (minimum value).
13	Interpacket interval in milliseconds—Default (!{[NOVALUE]}!) = 30 milliseconds (minimum value).
14	Number of packets in each poll setting—Default (!{[NOVALUE]}!) = 10 packets (minimum value).

Example 18-1 shows a sample seed file.

Example 18-1 Sample SRST Seed File in Preferred Format

```
SRST2,10.76.34.194,public,private,admin,admin,10.76.34.222,public,private,0009e847060e:00049afc920b,
4013:4017,30,30,20
```

Table 18-4 SRST Seed File—Secondarily Supported Format

Column Number	Description
1	SRST poll settings name—Must be unique.
2	IP address or DNS name of the source router—Source router and target router (column 5) combination must be unique.
3	Read community string of the source router. **Note** If no read community string exists in the DCR for the device, Operations Manager updates the DCR with this string.
4	Write community string of the source router. **Note** If no write community string exists in the DCR for the device, Operations Manager updates the DCR with this string.
5	IP address or DNS name of the SRST target router—Source router (column 2) and target router combination must be unique.
6	Read community string of the SRST target router. **Note** If no read community string exists in the DCR for the device, Operations Manager updates the DCR with this string.
7	Write community string of the SRST target router. **Note** If no write community string exists in the DCR for the device, Operations Manager updates the DCR with this string.
8	MAC addresses of IP telephones associated with SRST target router, delimited by a colon (:).

Table 18-4 SRST Seed File—Secondarily Supported Format (continued)

Column Number	Description
9	Phone extension numbers of IP telephones associated with SRST target router, delimited by a colon (:). **Note** Phone extensions must be sequenced in corresponding order with the MAC addresses (see column 8).
10	Sample interval specification—Default (!{[NOVALUE]}!) = 30 seconds (minimum value).
11	Interpacket interval in milliseconds—Default (!{[NOVALUE]}!) = 30 milliseconds (minimum value).
12	Number of packets in each poll setting—Default (!{[NOVALUE]}!) = 10 packets (minimum value).

Example 18-2 shows a sample seed file.

Example 18-2 Sample SRST Seed File in Secondarily Supported Format

```
Test1,10.76.34.194,public,private,10.76.34.218,public,private,0009e8470515:00075079c2da,4015:1016,30,30,10
```

Verifying that Devices Are Monitored by Operations Manager Before Import

Before you import SRST poll settings, verify that the following devices are monitored by Operations Manager:

- The media server that runs the Cisco Unified Communications Manager at the central site. (Phones at the remote site are registered to this Cisco Unified Communications Manager.)
- Switches to which the phones at the remote site are connected.
- Source and target routers.

Configuring a Single SRST Test as Needed

You can create an SRST poll setting wherever the SRST Test menu item is available, in either of the following ways:

- On a right-click menu—For example, when you right-click an appropriate device in the Service Level View.
- From a Launch button or Launch Tools menu—For example, when you open the Alert Details window from Alerts and Events for an appropriate device.

When you select the SRST Test menu item, the SRST Test Creation window opens.

Note SRST test names must be unique. If you enter an existing test name, the existing test will be updated. To see a list of existing tests, open the SRST Operations page; for more information, see Viewing SRST Poll Setting Status, page 18-4.

Step 1 Specify a source device that is IP SLA-enabled by entering or selecting the following:

- Name—IP address or DNS name of a device. This field might already contain a name; this might happen, for example, if you select a device on a monitoring dashboard and launch an SRST test for it. You can:
  - Enter an IP address or DNS name for an IP SLA-enabled device.
  - Expand device groups in the selector and select a device.
- Interface—(Optional) Enter an IP address or DNS name to set up the test from a particular interface on the device.

The IP SLA test will be created on the source device.

Note You can switch the name and interface for the source device with those for the destination device by clicking the **Swap Source and Destination** button.

Step 2 Select a destination SRST device by entering or selecting the following:

- Name—Enter an IP address or DNS name or select one from the device selector.
- Interface—(Optional) Enter an IP address or DNS name to set up the test from a particular interface on the device.

Step 3 Add phones to the Selected Phones list in one of the following ways:

- Click **Add > From Known List**. The Add Phone From Known List dialog box appears:
  - Enter phone extensions and MAC addresses formatted like the following:

    ```
    extension:MAC, extension:MAC
    ```

  - Click **Apply**. The dialog box closes and the Selected Phones list is updated.
- Click **Add > From Phone Report**. The All Phones Display window opens.
  - Select a check box for each phone that you want to add to the test.
  - Scroll to the bottom right corner of the window and click **Select**. The All Phones Display closes and the Selected Phones list is updated.
- Type directly into the Selected Phones list to add or remove phones.

Step 4 Enter a test name in the Test Name field.

Step 5 Click **OK**. Additional windows might appear:

- If there are no credentials in the DCR for the source or target device, the SRST Get Credentials dialog box appears:
  - Enter the requested (Read or Write) community string twice.
  - Click **OK**.
- An informational dialog box appears, displaying a message similar to the following:

  ```
  Number of tests updated =0.
  Number of new tests =1.
  For details on errors and validation, see
  NMSROOT/log/itemlogs/srst/srst_import_errors.log.
  Test creation is in progress.
  ```

Note In this example, one new test is being created.

Step 6 Verify that the test was created successfully:

a. Select **Administration > SRST Polling Settings > SRST Operations**. The SRST Operations page appears.

b. Locate the test in the Test Name column. If you cannot locate the test, see the *NMSROOT*\log\itemlogs\srst\srst_import_errors.log file.

NMSROOT is the directory where you installed **Operations Manager**. If you accepted the default installation directory, NMSROOT is C:\Progra~1\CSCOpx.

PART 7

Administration

CHAPTER 19

Configuring Polling and Thresholds

These topics describe the process for configuring polling settings and threshold values:

Overview of Polling and Thresholds

Operations Manager now uses two modules to poll and collect MIB information on devices, device interfaces, and device ports: AMC Services syslog receiver and the Real-Time Monitoring Tool (RTMT).

- Syslog—Operations Manager can receive the syslog-based events from AMC services. You can receive most of these events without any additional configuration. If you want to receive Unified Communications Manager syslog messages, you must configure the Unified Communications Manager to send them to Operations Manager. See Configuring Syslog Receiver on Cisco Unified Communications Manager, page F-3 for more details.
- RTMT—Operations Manager leverages pre-collected cluster-wide performance data from the Real-Time Monitoring Tool (RTMT). OM uses the RTMT on the publisher. You can receive these events without any additional configuration. If you want to change the thresholds settings for the CCM-based events, you must configure Configuring RTMT on Cisco Unified Communications Manager (Optional), page F-4. For more information on the RTMT supported events, see Table 19-10 on page 19-33.

Managing Groups, page 17-1, describes how Group Administration organizes devices, device interfaces, and device ports into different groups. The Common Services system-defined groups include groups such as Cisco Interfaces and Module, Content Networking, Routers, Voice and Telephony, and so forth. These groups have specific polling and threshold settings, while the Broadband Cable device type has different polling and threshold settings. Because a device can belong to multiple groups, the device uses the polling and threshold settings of the *overriding group*.

The Operations Manager polling and threshold function creates its own corresponding groups based on Common Services and Operations Manager groups:

- *Polling* groups that determine how often group members are polled for data.
- *Threshold* groups that determine acceptable levels of performance and utilization for group members.

When group objects are polled and any object's data shows that threshold values have been exceeded, or values have fallen below acceptable levels, Operations Manager generates the appropriate events.

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

In many cases, it might be acceptable to use the default settings for polling parameters. However, depending on how important a device group is, you can increase or decrease the polling interval to accomplish either of the following objectives:

- Minimize the impact on the polled devices
- Enhance the resolution of the collected data

In addition, you can enhance the performance and utilization of devices by adjusting thresholds, taking into account the following information:

- Location of the devices in the IP fabric
- Resource constraints

Which Settings Are Applied to Devices, Ports, and Interfaces?

Every device, device port, and device interface belongs to at least one system-defined group; in fact, they can belong to several. When a device belongs to several groups, Operations Manager uses the settings of the *overriding group*. The overriding group is the highest priority device group to which the device belongs. For more information, see Setting Priorities, page 19-3 which explains how to change group priorities and lists default group priorities.

Which Polling Settings Are Applied?

You can set and apply polling parameters to device groups (not for individual devices). When a device is polled, its ports and interfaces are also polled; therefore, port and interface polling is controlled at the device level.

Every device belongs to at least one system-defined device group. See Working with System-Defined Groups, page 17-3, for information about how devices are assigned to system-defined groups. If a device belongs to more than one group, Operations Manager uses the polling settings of the overriding group (with the highest priority, as described in Setting Priorities, page 19-3).

Which Threshold Settings Are Applied?

You can set and apply threshold parameters to device, interface, and port groups. When a device is polled, Operations Manager compares the new data against the threshold settings. If a threshold value has been exceeded, or a value has fallen below acceptable levels, Operations Manager generates the appropriate event.

If a device, port, or interface belongs to more than one group, Operations Manager uses the threshold settings of the overriding group (the group you determine to have the highest priority, as described in Viewing the Overriding Group—Examples, page 19-6).

Setting Priorities

Note A device group can have different overriding polling and threshold groups.

You can set the priority for each of the following:

- Device polling groups
- Device threshold groups
- Interface threshold groups
- Access port threshold groups
- Trunk port threshold groups

Step 1 Select **Administration > Polling and Thresholds > Priorities**. The Setting Priority: Queue page appears, displaying the groups in priority order.

Step 2 Select the radio button that corresponds to the group type, one of the following:

Note A device can have different overriding polling and threshold groups.

- Polling groups:
  - Device Polling Groups
- Threshold groups:
  - Device Threshold Groups
  - Interface Threshold Groups
  - Access Port Threshold Groups
  - Trunk Port Threshold Groups

Step 3 Rearrange the groups according to your preference (the closer the group is to the top of the list, the higher its priority):

a. Select a group.

b. Move the group up or down using the Up and Down buttons.

Step 4 Click **Save**. The changes are now saved in the database.

Note The changes do not take effect until you apply them to Operations Manager. See Applying Changes, page 19-60.

Because devices, ports, and interfaces can belong to multiple groups, Operations Manager uses the highest priority group to which the device belongs to determine which polling and threshold parameters to use. Operations Manager prioritizes groups as follows, in descending order of priority:

- Access and Trunk Port Group Priorities for Thresholds, Table 19-1 on page 19-4
- Interface Group Priorities for Thresholds, Table 19-2 on page 19-4

- Device Group Priorities for Polling and Thresholds, Table 19-3 on page 19-5

Note To find the overriding group for a device, you can select any device group to which the device belongs and view a Polling Parameters report or a Thresholds report for the group.

By default, Operations Manager gives highest priority to Access Port Groups and Trunk Port Groups, listed in Table 19-1.

Table 19-1 Access and Trunk Port Group Priorities for Thresholds

Access and Trunk Port Groups in Priority Order	Parameters to Set
System Defined Groups	None
Access Port Groups	None
1 GB Ethernet	Threshold
10MB-100MB Ethernet	
ATM	
Others	
Trunk Port Groups	None
1 GB Ethernet	Thresholds
10MB-100MB Ethernet	
ATM	
Others	

Table 19-2 Interface Group Priorities for Thresholds

Interface Groups in Priority Order	Parameters to Set
System Defined Groups	None
Interface Groups	None
1GB Ethernet	Threshold
10MB-100MB Ethernet	Threshold
ATM	Threshold
Token Ring	Threshold
ISDN Physical Interface	Threshold
ISDN B Channel	Threshold
ISDN D Channel	Threshold
Serial	Threshold
FDDI	Threshold
Backup	Threshold
Dial-On-Demand	Threshold
Others	Threshold

Table 19-3 Device Group Priorities for Polling and Thresholds

Device Groups in Priority Order	Parameters to Set[1]
System Defined Groups	None
Cisco Unified Communications Applications	None
Unified Communications Managers	Polling and thresholds
Unified Communications Manager Express	Polling and thresholds
Unity	Polling and thresholds
Unity Express	Polling and thresholds
Unity Connection	Polling and thresholds
Personal Assistants	Polling and thresholds
Meeting Place Express	Polling and thresholds
Meeting Place	Polling and thresholds
IP Contact Center	Polling and thresholds
Expert Advisor	Polling and thresholds
78XX Media Servers	Polling and thresholds
SRST capable Devices	Polling and thresholds
H323 Gateways	Polling and thresholds
Gatekeepers	Polling and thresholds
Voice Mail Gateways	Polling and thresholds
Voice Gateways	Polling and thresholds
Security and VPN	Polling and thresholds
Content Networking	Polling and thresholds
Voice and Telephony	Polling and thresholds
Wireless	Polling and thresholds
Universal Gateways and Access Servers	Polling and thresholds
Broadband Cable	Polling and thresholds
Routers	Polling and thresholds
Storage Networking	Polling and thresholds
Optical Networking	Polling and thresholds
Switches and Hubs	Polling and thresholds
DSL and Long Reach Ethernet (LRE)	Polling and thresholds
Cisco Interfaces and Modules	Polling and thresholds
Network Management	Polling and thresholds

1. A device can have different overriding polling and threshold groups.

Viewing the Overriding Group—Examples

The Polling Parameter and Threshold reports provide information on the overriding groups for all devices in a specific group. Locating the overriding group for a port or interface is a bit more complex, as described in the following procedures.

Viewing the Overriding Polling or Threshold Group for a Device

Use the Polling Parameter report or Thresholds report to identify a device's overriding group.

Step 1 Select **Administration > Polling and Thresholds**.

Step 2 Do one of the following:

- To view the overriding polling groups, select **Polling Parameters**.
- To view the overriding threshold group, select **Thresholds**.

Note A device can have different overriding polling and threshold groups.

Step 3 Select a device group that the device is a member of and click **View**. The appropriate report opens. Locate the device in which you are interested, and look at the Overriding Group column.

Viewing the Overriding Threshold Group for a Port or Interface

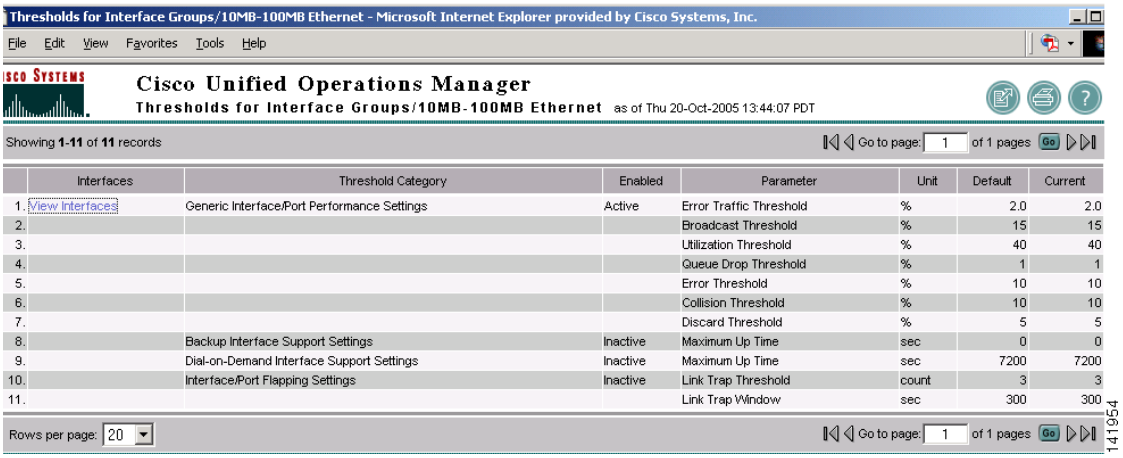
Step 1 Select **Administration > Polling and Thresholds**.

Step 2 Consider the port or interface type and check the appropriate system-defined group for that type, and select **Thresholds**.

Step 3 Select the port or interface group and click **View**.

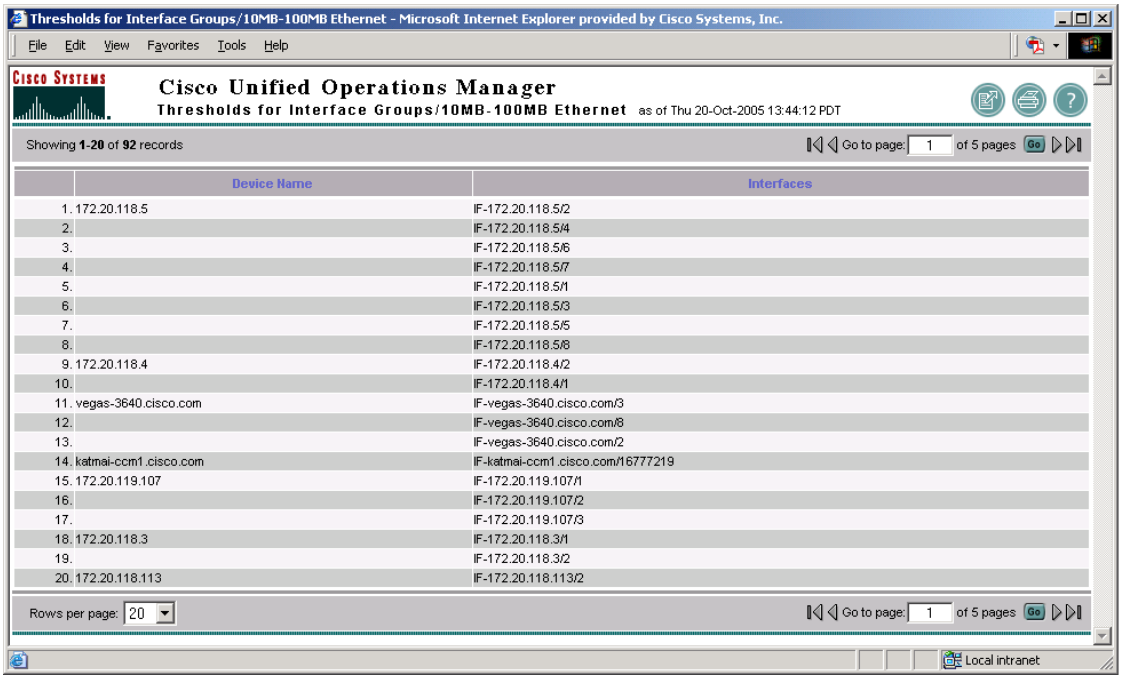
For example, if you think an interface is in the 10MB-100MB Ethernet interface group, you would select **Thresholds**, choose that group, and click **View**, and Figure 19-1 would open.

Figure 19-1 Viewing the 10MB-100MB Ethernet Interface Group —Step 1 (of 2)



Step 4 Click **View Interfaces**. A complete list of interfaces is displayed. See Figure 19-2. (If you were searching for a port, the link would say **View Ports**.)

Figure 19-2 Viewing the 10MB-100MB Ethernet Interface Group —Step 2 (of 2)



a. If the interface or port appears as a member, that group is the overriding group. (Ports and interfaces are only listed as members in the overriding group.)

b. If the interface or port does not appear, repeat this process for all subgroups of port and interface groups until you locate the port or interface.

How Can I Set Parameters for a Device, Interface, or Port?

There are several ways in which you can control the parameters for a device, interface, or port. Polling and thresholds are always applied on a group level, not on a specific device, port, or interface level.

Note Be careful when you change settings for a system-defined group. Your changes will affect the settings of all devices in the group.

Note To apply settings to a device or component that belongs to multiple groups, make sure the group with the desired settings is the overriding group (has the highest priority), as described in Setting Priorities, page 19-3.

To configure *polling and threshold* settings for a *device*:

- Adjust the polling and threshold settings for any system-defined group to which the device belongs (and verify the overriding group, if applicable). This changes the settings for all devices in that system-defined group.
- Create an Operations Manager (OM@*server)* user-defined group and edit it. Apply the desired polling and threshold settings to the group and verify the overriding group. In this way, you can create a group of specific devices in which you are interested, and specify settings for them.

To configure *polling* on *interfaces and ports*:

- Adjust the polling settings defined by the Operations Manager (OM@*server*) system-defined group (and verify the overriding group, if applicable). This changes the polling settings for all interfaces and ports on devices in that system-defined group.
- Create a user-defined group and edit it. Apply the desired polling and threshold settings to the group and verify the overriding group. In this way, only the ports and interfaces on specific devices are affected.

To configure *thresholds* on *interfaces and ports*:

- Adjust the threshold settings defined by the Operations Manager system-defined port or interface group (and verify the overriding group, if applicable). (Make sure the port or interface belongs to that group, as described in Viewing the Overriding Threshold Group for a Port or Interface, page 19-6.) This changes the threshold settings for all interfaces and ports in that system-defined group.
- Create a user-defined interface or port group and edit it. Apply the desired threshold settings, and verify the overriding group. In this way, only the ports and interfaces on specific devices are affected.

For additional information, see the following topics:

- Editing Polling Parameters, page 19-13
- Editing Operations Manager Thresholds, page 19-27

Updating Polling Parameters and Thresholds

Operations Manager is preconfigured with default settings for polling parameters and thresholds for each system-defined device, port, and interface group. Optionally, you can change them. The following steps describe the basic process for updating polling parameters and thresholds.

	Task	Procedures
Step 1	Enable or disable polling for selected polling settings or parameters; change polling parameter values for device, port, interface, or application groups contained within the following: • Operations Manager (OM@*server*) system-defined groups and user-defined groups • Common Services (CS@*server*) system-defined group **Note** At any time, you can go back to Operations Manager default values for polling.	Editing Polling Parameters, page 19-13 Restoring Default Polling Parameters, page 19-16
Step 2	Enable or disable thresholds; change threshold values for device, port, interface, or application groups contained within the following: • Operations Manager (OM@*server*) system-defined groups and user-defined groups • Common Services (CS@*server*) system-defined group • RTMT (Real-Time Monitoring Tool) **Note** At any time you can go back to Operations Manager default threshold values and threshold settings.	Editing Device Group Threshold Settings, page 19-27 Editing Access Port, Trunk Port, and Interface Group Threshold Settings, page 19-30 Customizing Operations Manager Threshold Settings, page 19-29 Restoring Default Thresholds, page 19-31 Viewing RTMT Thresholds, page 19-32 Configuring RTMT Thresholds, page 19-32 Synchronizing RTMT Thresholds, page 19-36
Step 3	Change the default priority for the following: • Device polling groups—Place device groups in priority order for polling. • Device threshold groups—Place device groups in priority order for thresholds. **Note** Device groups can have different overriding polling and threshold groups. • Access port threshold groups—Place access port groups in priority order for thresholds. • Trunk port threshold groups—Place trunk port groups in priority order for thresholds. • Interface threshold groups—Place interface groups in priority order for thresholds.	Setting Priorities, page 19-3
Step 4	When you are done with all changes, if possible, select a time of low activity on the network to update the IP fabric with these changes. The new values will not be used until you apply your changes.	Applying Changes, page 19-60

Selecting Groups

The first thing you must do when you use polling and threshold options is select a group for which parameters exist. Generally, this is a group that does not contain subgroups.

Table 19-4 lists groups in the order in which they are displayed in the group selector and notes whether applicable parameters exist for the group. The group selector you see might not display all of the device groups listed in Table 19-4; device groups are displayed when they have members.

Table 19-4 Device Groups as Displayed in the Device Selector

Device Groups in Display Order	Parameters to Set
CS@*server*	None
System Defined Groups	None
Broadband Cable	Polling and thresholds
Cisco Interfaces and Modules	Polling and thresholds
Content Networking	Polling and thresholds
DSL and Long Reach Ethernet (LRE)	Polling and thresholds
Network Management	Thresholds
Optical Networking	Polling and thresholds
Routers	Polling and thresholds
Security and VPN	Polling and thresholds
Storage Networking	Polling and thresholds
Switches and Hubs	Polling and thresholds
Universal Gateways and Access Servers	Polling and thresholds
Voice and Telephony	Polling and thresholds
Wireless	Polling and thresholds
OM@*server*	
System Defined Groups	None
78XX Media Servers	Polling and thresholds
Access Port Groups	None
1GB Ethernet	Thresholds
10MB-100MB Ethernet	Thresholds
ATM	Thresholds
Others	Thresholds
Cisco Unified Communications Manager or Cluster	None
Cluster name (the name Cisco Unified Communications Manager provides for the cluster)	Polling and thresholds
Cisco Unified Communications Applications	None
Expert Advisor	Polling and thresholds
IP Contact Center	Polling and thresholds
Meeting Place	Polling and thresholds
Meeting Place Express	Polling and thresholds

Table 19-4 Device Groups as Displayed in the Device Selector (continued)

Device Groups in Display Order	Parameters to Set
Personal Assistants	Polling and thresholds
Unified Communications Manager	Polling and thresholds
Unified Communications Manager Express	Polling and thresholds
Unity	Polling and thresholds
Unity Express	Polling and thresholds
Unity Connection	Polling and thresholds
Gatekeepers	Polling and thresholds
H323 Gateways	Polling and thresholds
Interface Groups	None
1GB Ethernet	Thresholds
10MB-100MB Ethernet	Thresholds
ATM	Thresholds
Backup	Thresholds
Dial-on-Demand	Thresholds
FDDI	Thresholds
ISDN B Channel	Thresholds
ISDN D Channel	Thresholds
ISDN Physical Interface	Thresholds
Others	Thresholds
Serial	Thresholds
Token Ring	Thresholds
Trunk Port Groups	None
1GB Ethernet	Thresholds
10MB-100MB Ethernet	Thresholds
ATM	Thresholds
Others	Thresholds
Voice Gateway	Polling and thresholds
Voice Mail Gateway	Polling and thresholds

For additional information, see the following topics:

- Viewing Polling Parameters, page 19-12
- Editing Polling Parameters, page 19-13
- Viewing Operations Manager Thresholds, page 19-26

Managing Polling Parameters

Most port and interface polling is controlled at the device level. However, you can set polling parameters for voice ports and voice interfaces for some voice-enabled device groups. For a list of device groups and related polling parameters, see Parameter Types, Device Groups, and Polling Settings, page 19-17.

From the Polling Parameters page, you can perform any of the following tasks:

- Viewing Polling Parameters, page 19-12
- Editing Polling Parameters, page 19-13
- Restoring Default Polling Parameters, page 19-16

Viewing Polling Parameters

When you view polling parameters for a device group, you can see the devices that are members of the device group, and see the default as well as current values for the polling parameters. Devices that belong to multiple groups use the polling settings of the overriding group. Interface and port polling is controlled at the device level; in other words, switches have a specific polling setting, and that setting determines when the switch ports are polled.

Note If Operations Manager is set to ACS mode for authentication, Cisco Secure ACS may limit the devices you are permitted to view when you generate a Polling Parameters report. For more information, refer to Device-Based Filtering, page 20-22.

Step 1 Select **Administration > Polling and Thresholds > Polling Parameters**.

Step 2 Select a device group for which you can set polling parameters. Generally, this is a device group that does not contain subgroups.

Step 3 Click the **View** button. The Polling Parameters report opens in a separate window. This display provides the following information.

Field	Explanation
Device Name	IP address or DNS name of a device.
Parameter Type	One of the following: • Data Settings—Control polling for devices and those ports and interfaces that are not voice-enabled. • Voice Health Settings—Control polling for voice-enabled devices, ports, interfaces, and applications. • Voice Utilization Settings—Control polling for performance and capacity data; disabled by default.
Parameter	Name of the polling setting to which the values apply.
Polling Enabled	Enabled or Disabled.
Default Value (sec)	Default number of seconds between successive polls for the setting.
Default Retries	Default number of times to retry a failed poll request.
Default Timeout (msec)	Default number of milliseconds before a poll request times out.

Field	Explanation
Current Value (sec)	Current number of seconds between successive polls for the setting.
Current Retries	Current number of times to retry a failed poll request.
Current Timeout (msec)	Current number of milliseconds before a poll request times out.
Overriding Group	Device group from which polling parameter values are applied. (This is the highest priority device polling group to which the device belongs.) If you want to change the polling parameters for a device, edit the settings for the overriding group. See Editing Polling Parameters, page 19-13.

Step 4 When you are done viewing polling parameters, close the window.

For additional information, see the following topics:

- Viewing the Overriding Group—Examples, page 19-6
- Viewing Data from Reports with Over 2,000 Records, page 1-20
- Printing Displays or Reports, page 1-22

Editing Polling Parameters

When you edit Operations Manager polling parameters, you edit settings that are associated with device groups, not with individual devices. When you have finished all changes to polling parameters (and thresholds and priorities), apply all changes. For more information, see Understanding What Happens When You Apply Changes, page 19-16.

Step 1 Select **Administration > Polling and Thresholds > Polling Parameters**.

Step 2 Select a device group for which you can set polling parameters. Generally, this is a device group that does not contain subgroups. (For more information, see Selecting Groups, page 19-9.)

Step 3 Click the **Edit** button. The Polling Parameters: Edit page appears, displaying the following information.

GUI Element	Action/Description
Group Name	Complete group name. Grayed out because you cannot edit it.
Parameter Type list box	One of the following: • Data Settings—Control polling for devices and those ports and interfaces that are not voice-enabled. • Voice Health Settings—Control polling for voice-enabled devices, ports, and interfaces. • Voice Utilization Settings—Control polling for performance and capacity data; disabled by default.
Parameter table	The parameter settings for the selected parameter type are displayed.

Note Enable GSU Performance Polling for users to see the HighPortUtilization event.

Step 4 To edit all parameters, repeat the following steps for each parameter type:

a. Select a parameter type.

b. Change the parameters appropriately for each setting as described in this table.

Field	Description
Parameter	Parameter setting name. Grayed out because you cannot edit it. Each setting controls how frequently devices are polled for a particular type of data; for example, reachability.
Interval (sec)	Current polling interval. Grayed out because you cannot edit it.
New Interval (sec)	Enter the number of seconds between successive polls for the setting: • Data Settings: – Minimum value: 30 – Maximum value: 3600 – Increment: 1 • Voice Health Settings: – Minimum value: 30 for most settings and 240 for the following settings: Digital Voice Gateway-to-Cluster Connectivity Settings Gatekeeper-to-Cluster Connectivity Settings Voice Gateway-to-Cluster Connectivity Settings – Maximum value: 3600 – Increment: 1 • Voice Utilization Settings: – For Cluster UtilizationSettings: Minimum value: 7 Maximum value: 36 Increment: 1 – For all other settings: Minimum value: 1 Maximum value: 60 Increment: 1
Timeout (msec)	Current value for timeout. Grayed out because you cannot edit it.

Field	Description
New Timeout (msec)	Enter the number of milliseconds allowed for a poll request before it times out: • Data Settings and Voice Health Settings: – Minimum value: 10 – Maximum value: 60000 – Increment: 1 • Voice Utilization Settings – Minimum value: 1 – Maximum value: 60 – Increment: 1
Retry	Current value for retry. Grayed out because you cannot edit it.
New Retry	Enter the number of times to retry a failed poll request: • Data Settings and Voice Health Settings: – Minimum value: 0 – Maximum value: 10 – Increment: 1 • Voice Utilization Settings – Minimum value: 0 – Maximum value: 3 – Increment: 1
Defaults	To reset the values for the setting to the defaults, select this check box. To view default values, see Viewing Polling Parameters, page 19-12. **Note** Selecting or deselecting the Defaults check box in the table heading causes all Defaults check boxes to be correspondingly selected or deselected.
Polling Enabled	To disable polling for this setting, deselect this check box. To enable polling, select it. **Note** Selecting or deselecting the Polling Enabled check box in the table heading causes all Polling Enabled check boxes to be correspondingly selected or deselected.

Step 5 To save the settings, do one of the following:

- Click **Save**; your changes are saved in the database. Click **Cancel**; the Polling Parameters: Edit dialog box closes. Your changes will not go into effect until you have applied them. See Applying Changes, page 19-60.
- Click **Apply** to save the settings, close the Polling Parameters: Edit dialog box, and apply changes to the system. When a confirmation dialog box appears, click **Yes**. See Understanding What Happens When You Apply Changes, page 19-16.

Understanding What Happens When You Apply Changes

After you adjust polling and threshold settings, you must apply changes to have Operations Manager start using your changes. The following explains the difference between saving your changes and applying your changes.

When you *save* changes, Operations Manager performs the following tasks:

- Sets the polling and threshold settings in the selected group.

When you *apply* changes, Operations Manager performs the following tasks:

- Recalculates group membership, based on group priority.
- Uses the new polling and threshold settings to gather information from the devices.

You must also apply changes after resuming a device, so that Operations Manager will begin polling the device depending on the appropriate settings.

You can apply changes by selecting **Administration > Polling and Thresholds > Apply Changes**. You can also apply changes by clicking Apply on the Polling Parameters: Edit page or the Thresholds: Edit page.

Restoring Default Polling Parameters

You can restore all parameter settings for a device group to default values using this procedure. If, instead, you want to restore only a few functions or settings, see Editing Polling Parameters, page 19-13.

Before You Begin

To review default polling settings before you apply them, view the Polling Parameter Summary for the device group. See Viewing Polling Parameters, page 19-12. Current settings along with the default settings are displayed.

Step 1 Select **Administration > Polling and Thresholds > Polling Parameters**.

Step 2 Select a device group for which you can restore polling parameters. Generally, this is a device group that does not contain subgroups. (For more information, see Selecting Groups, page 19-9.)

Step 3 Click the **Revert to Default Settings** button. A confirmation dialog box appears.

Step 4 Click **Yes**.

Note The settings are stored in the database, but not yet applied to the IP fabric. See Applying Changes, page 19-60.

Parameter Types, Device Groups, and Polling Settings

This section provides information on polling settings for each parameter type:

Data Settings—Polling

Data settings enable you to poll for device reachability, environment, ports and interfaces, and processor and memory utilization. Table 19-5 lists all data settings and polling intervals for each setting.

Table 19-5 Data Settings—Polling Settings and Default Polling Intervals

Data Polling Settings	Intervals (in seconds)	Usage Notes
Access Port Settings	• 30 minimum. • 3600 maximum. • 1200 default —You can adjust the default polling interval in 1-second increments.	To enable polling for Access Port Settings, you must enable polling for Connector Port and Interface Settings. The same timeout and retry values are used for Access Port Settings and Connector Port and Interface Settings. When you update the timeout and retry value for either of these settings, Polling updates the values for both.
Connector Port and Interface Settings	• 60 minimum. • 3600 maximum. • 240 default —You can adjust the default polling interval in 1-second increments.	
Environment Settings		Environment Settings and Processor and Memory Utilization Settings are not available for all device groups. Some voice-enabled device groups (noted in Table 19-6) have similar settings available for Voice Health Settings parameter type.
Processor and Memory Utilization Settings		
Reachability Settings		—

Table 19-6 lists data polling settings and indicates their applicability to device groups.

Table 19-6 Data Settings—Polling Settings by Device Group

Data Polling Settings/ Device Groups	Access Port Settings	Connector Port and Interface Settings	Environment Settings	Processor and Memory Utilization Settings	Reachability Settings
OM@*server* System Defined Groups					
78XX Media Servers	Disabled by default		See Voice Health Settings (Voice Health Settings—Polling, page 19-19.)		X
Expert Advisor	X	X	Disabled by default		X
Gatekeepers	X	X	X	X	X
H323 Gateways	X	X	X	X	X
IP Contact Center	Disabled by default				X
Meeting Place	X	X	Disabled by default		X
Meeting Place Express	X	X	Disabled by default		X
Personal Assistants	Disabled by default				X
SRST Devices	X	X	X	X	X
Unified Communications Managers	Disabled by default		See Voice Health Settings (Voice Health Settings—Polling, page 19-19.)		X
Unified Communications Manager Express	X	X	X	X	X
Unity	Disabled by default		See Voice Health Settings.		X
Unity Connection	Disabled by default				X
Unity Express	Disabled by default				X
Voice Gateways	X	X	X	X	X
Voice Mail Gateways	Disabled by default		See Voice Health Settings.		X
OM@*server* User Defined Groups (Disabled by default)					
CS@*server* System Defined Groups					
Broadband Cable	X	X	X	X	X
Cisco Interfaces and Modules	Disabled by default		See Voice Health Settings.		X
Content Networking	X	X	X	X	X
DSL and Long Reach Ethernet (LRE)	X	X	X	X	X
Network Management	Disabled by default		Not applicable.		X
Optical Networking	X	X	X	X	X
Routers	X	X	X	X	X
Security and VPN	X	X	X	X	X
Storage Networking	X	X	X	X	X
Switches and Hubs	X	X	X	X	X

Table 19-6 Data Settings—Polling Settings by Device Group (continued)

Data Polling Settings/ Device Groups	Access Port Settings	Connector Port and Interface Settings	Environment Settings	Processor and Memory Utilization Settings	Reachability Settings
Universal Gateways and Access Servers	X	X	X	X	X
Voice and Telephony	X	X	X	X	X
Wireless	X	X	X	X	X

Note

- Polling for voice-enabled ports and interfaces is controlled by voice health settings.
- Polling is disabled by default for user-defined groups. To enable polling for user defined groups, see Editing Polling Parameters, page 19-13.

Voice Health Settings—Polling

Voice health settings control polling for voice-enabled devices, ports, interfaces, and Cisco Unified Communications Applications. Data that is collected includes Cisco Unified Communications Manager cluster connectivity and processor and memory utilization on Media Convergence Servers (MCS) and on voice gateways. Voice health settings default polling intervals (in seconds) are:

- Minimum:
  - 240—For clusters in the Cisco Unified Communications Manager or Cluster device group.
  - 30—For all other device groups.
- Maximum—3600.
- Default—240. You can adjust the default polling interval in 1-second increments.

Table 19-7 lists device groups and the voice health settings that are applicable to them.

Table 19-7 Voice Health Settings—Polling Settings by Device Group

Device Group	Polling Settings for Voice Health Settings
OM@*server* System-Defined Device Groups	
78XX Media Servers	Application Polling Settings Cisco Unity Polling Settings Environment - Power Supply, Fan, and Temperature Sensor Settings Hard Disk and Virtual Memory Settings MCS Ethernet Interface Settings MCS Processor and Memory Utilization Settings
Expert Advisor	Application Polling Settings Environment - Power Supply, Fan, and Temperature Sensor Settings Hard Disk and Virtual Memory Settings MCS Processor and Memory Utilization Settings

Table 19-7 Voice Health Settings—Polling Settings by Device Group (continued)

Device Group	Polling Settings for Voice Health Settings
Gatekeepers	DS1 Voice Port Settings E1 Voice Port Settings FXX Interface Settings
H323 Gateways	Application Polling Settings Cisco Unified Communications Manager Express Settings DS1 Voice Port Settings E1 Voice Port Settings FXX Interface Settings
IP Contact Center	Application Polling Settings Cisco IP Contact Center Polling Settings Hard Disk and Virtual Memory Settings MCS Processor and Memory Utilization Settings
Meeting Place	Application Polling Settings Environment - Power Supply, Fan, and Temperature Sensor Settings Hard Disk and Virtual Memory Settings MCS Processor and Memory Utilization Settings
Meeting Place Express	Application Polling Settings Environment - Power Supply, Fan, and Temperature Sensor Settings Hard Disk and Virtual Memory Settings MCS Processor and Memory Utilization Settings
Personal Assistants	Application Polling Settings MCS Processor and Memory Utilization Settings Personal Assistant Polling Settings
SRST Devices	DS1 Voice Port Settings E1 Voice Port Settings FXX Interface Settings
Unified Communications Manager Express	Application Polling Settings Cisco Unified Communications Manager Express Settings DS1 Voice Port Settings E1 Voice Port Settings FXX Interface Settings

Table 19-7 Voice Health Settings—Polling Settings by Device Group (continued)

Device Group	Polling Settings for Voice Health Settings
Unified Communications Managers	Application Polling Settings
	Environment - Power Supply, Fan, and Temperature Sensor Settings
	Hard Disk and Virtual Memory Settings
	MCS Ethernet Interface Settings
	MCS Processor and Memory Utilization Settings
Cisco Unified Communications Manager or Cluster	Digital Voice Gateway-to-Cluster Connectivity Settings
	Gatekeeper-to-Cluster Connectivity Settings
	Voice Gateway-to-Cluster Connectivity Settings
Unity	Application Polling Settings
	Cisco Unity Polling Settings
	Environment - Power Supply, Fan, and Temperature Sensor Settings
	Hard Disk and Virtual Memory Settings
	MCS Ethernet Interface Settings
	MCS Processor and Memory Utilization Settings
Unity Connection	Application Polling Settings
	Cisco Unity Polling Settings
	Environment - Power Supply, Fan, and Temperature Sensor Settings
	Hard Disk and Virtual Memory Settings
	MCS Ethernet Interface Settings
	MCS Processor and Memory Utilization Settings
Unity Express	Application Polling Settings
	Cisco Unity Express Polling Settings
Voice Gateways	Application Polling Settings
	Cisco Unified Communications Manager Express Settings
	DS1 Voice Port Settings
	E1 Voice Port Settings
	FXX Interface Settings
	VG248 Processor and Memory Utilization Settings
	VG248 Ports-to-Cluster Connectivity Settings
Voice Mail Gateways	DPA Ethernet Interface Settings
	DPA Port Settings
	DPA Processor and Memory Utilization Settings
	DPA-to-Cisco Unified Communications Manager Connectivity Settings
OM@*server* User Defined Groups (Disabled by Default)	
CS@*server* System Defined Groups	

Table 19-7 Voice Health Settings—Polling Settings by Device Group (continued)

Device Group	Polling Settings for Voice Health Settings
Cisco Interfaces and Modules	Application Polling Settings
	Cisco Unity Express Polling Settings
Routers	Application Polling Settings
	Cisco Unified Communications Manager Express Settings
	DS1 Voice Port Settings
	E1 Voice Port Settings
	FXX Interface Settings
Switches and Hubs	DS1 Voice Port Settings
	E1 Voice Port Settings
	FXX Interface Settings
Universal Gateways and Access Servers	DS1 Voice Port Settings
	E1 Voice Port Settings
	FXX Interface Settings
Voice and Telephony	Application Polling Settings
	Cisco IP Contact Center Polling Settings
	Cisco Unity Polling Settings
	DPA Ethernet Interface Settings
	DPA Port Settings
	DPA Processor and Memory Utilization Settings
	DPA-to-Cisco CommunicationManager Connectivity Settings
	DS1 Voice Port Settings
	E1 Voice Port Settings
	Environment - Power Supply, Fan, and Temperature Sensor Settings
	FXX Interface Settings
	Hard Disk and Virtual Memory Settings
	MCS Ethernet Interface Settings
	MCS Processor and Memory Utilization Settings
	VG248 Ports-to-Cluster Connectivity Settings
	VG248 Processor and Memory Utilization Settings

Note Polling is disabled by default for user-defined groups. To enable polling for user defined groups, see Editing Polling Parameters, page 19-13.

Voice Utilization Settings—Polling

Voice Utilization Settings control performance polling. Performance polling collects utilization and capacity planning data from Cisco IOS gateways, gatekeepers, SRST devices, Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, Cisco IP Contact Center, Cisco Unity, Cisco Unity Connection, and Cisco Unity Express. Performance polling is disabled by default.

When performance polling is enabled, Operations Manager collects performance and capacity data that:

- Is accessible from monitoring dashboards in the form of performance graphs; see How to Use Performance Graphs, page 7-1.
- Is also stored in data files on disk for further analysis; for information about data files, see Performance Polling Record Formats, page J-2.
- Is measured against Voice Utilization Settings thresholds. When thresholds are violated, Operations Manager generates events related to performance and capacity problems in an application, on an interface, or on a device; for example, high utilization of ports, channel, and resources of a device.

For information on enabling Voice Utilization Settings, see Editing Polling Parameters, page 19-13.

Voice Utilization Settings default polling interval values (in seconds) are:

- 30 minimum
- 3600 maximum
- 240 default—You can adjust the default polling interval in 1-second increments.

Table 19-8 lists device groups and the Voice Utilization Settings that are applicable to them.

Table 19-8 Voice Utilization Settings—Polling Settings by Device Group

Device Group	Voice Utilization Polling Settings
OM@server	
78XX Media Server	Cisco CommunicationManager and Registered MGCP Gateway Utilization
CommunicationManager	Cisco CommunicationManager and Registered MGCP Gateway Utilization
CommunicationManager Express	Cisco CommunicationManager Express Utilization Cisco SRST Utilization Gatekeeper Utilization H323 Gateway Utilization
Cisco Interfaces and Modules	Cisco Unity Express Utilization
Cisco Unified Communications Manager or Cluster	None
Cluster name (the name Cisco Unified Communications Manager provides for the cluster)	
Gatekeepers	Cisco CommunicationManager Express Utilization Cisco SRST Utilization Gatekeeper Utilization H323 Gateway Utilization

Table 19-8 Voice Utilization Settings—Polling Settings by Device Group (continued)

Device Group	Voice Utilization Polling Settings
H323 Gateways	Cisco CommunicationManager Express Utilization Cisco SRST Utilization Gatekeeper Utilization H323 Gateway Utilization
Unified Contact Center Enterprise	Unified CCE Router Utilization
Routers	Cisco CommunicationManager Express Utilization Cisco SRST Utilization Gatekeeper Utilization H323 Gateway Utilization
SRST Devices	Cisco CommunicationManager Express Utilization Cisco SRST Utilization Gatekeeper Utilization H323 Gateway Utilization
Unity	Cisco Unity Utilization
Unity Connection	Cisco Unity Connection Utilization
Unity Express	Cisco Unity Express Utilization
Universal Gateways and Access Servers	H323 Gateway Utilization
Voice and Telephony	Cisco CommunicationManager and Registered MGCP Gateway Utilization Cisco CommunicationManager Express Utilization Cisco SRST Utilization H323 Gateway Utilization Gatekeeper Utilization Voice Mail Gateway Utilization
Voice Gateways	Cisco CommunicationManager Express Utilization Cisco SRST Utilization Gatekeeper Utilization H323 Gateway Utilization
Voice Mail Gateways	Voice Mail Gateway Utilization

Table 19-9 lists the types of ports and resources that are polled on each device group.

Table 19-9 Voice Utilization Settings—Supported Ports and Resources

Device Group	Analog Ports	Digital Ports	Other Ports	Resources
CommunicationManager Express	—	—	—	IP phone registered
Cisco Unified Communications Manager or Cluster	—	—	—	Location bandwidth
Gatekeeper	—	—	—	Total and Interzone bandwidth
Media Server	FXS FXO	T1/E1 PRI, T1 CAS BRI	Unity inbound and outbound	CommunicationManager MOH Multicast/Unicast, MTP, Transcoder, HW/SW conference
Unity Express	—	—	—	Session, Capacity, Orphaned mailbox
VoiceGateway	FXS FXO E&M	T1/E1 PRIT1/ E1 CASBRI	—	DSP
VoiceMailGateway	—	—	PBX, VM	—

Managing Thresholds

Use Operations Manager to view, edit, and customize your Operations Manager thresholds as well as view, synchronize and configure Real-Time Monitoring (RTMT) thresholds.

Operations Manager does not need to install the RTMT plug-in to poll the device data (for example, memory usage) via RTMT. Operations Manager uses the default settings for these events. If you want to change the threshold settings for specific events, you must install the RTMT plug-in.

From the Thresholds page, you can perform any of the following tasks:

- Viewing Operations Manager Thresholds, page 19-26
- Editing Operations Manager Thresholds, page 19-27
- Restoring Default Thresholds, page 19-31
- Viewing RTMT Thresholds, page 19-32
- Configuring RTMT Thresholds, page 19-32
- Synchronizing RTMT Thresholds, page 19-36

From the Thresholds menu, you have access to either Operations Manager or Real-Time Monitoring Tool (RTMT) thresholds. Select **Administration > Polling and Thresholds > Thresholds** and then select which threshold you wish to access.

For a list of device groups and related threshold settings, see Parameter Types, Device Groups, and Threshold Categories, page 19-36.

Viewing Operations Manager Thresholds

You can view the thresholds that are associated with device groups, trunk port groups, access port groups, and interface groups. Because the numbers of ports and interfaces can be very large, the Thresholds report provides a link through which you can launch a separate page that lists all the ports and interface members of the group. Optionally, you can save the Thresholds report in a comma-separated value (CSV) file.

If the Operations Manager server is using ACS mode for authentication, Cisco Secure ACS may limit the devices you are permitted to view when you generate a Thresholds report. For more information, refer to Device-Based Filtering, page 20-22.

Step 1 Select **Administration > Polling and Thresholds > Thresholds > Operations Manager**.

Step 2 Select a device group for which you can set thresholds. Generally, this is a device group that does not contain subgroups.

Step 3 For more information, see Selecting Groups, page 19-9.

Step 4 Click the **View** button. The Thresholds report window opens and displays the following information.

Field	Explanation
Displayed for an Access Port Group, Trunk Port Group, or Interface Group	
View *xxxxxx* link	Launches a port or interface report, where *xxxxxx* is Access Ports, Interfaces, or Trunk Ports.
Displayed for a Device Group	
Device Name	IP address or DNS name of the device.
Parameter Type	One of the following: • Data Settings—Control thresholds for device reachability, processor and memory, and environment. • Voice Health Settings—Control thresholds for voice-enabled devices, device elements, and Cisco Unified Communications applications. • Voice Utilization Settings—Control thresholds for performance and capacity data collected on voice-enabled devices.
Displayed for All Groups	
Threshold Category	Threshold category name.
Enabled	One of the following: • Active—All threshold settings are enabled for the threshold category. • Inactive—All threshold settings are disabled for the threshold category.
Parameter	Threshold name.
Unit	Unit of measurement for the threshold: • %—Percent. • count—Number of occurrences. • min—Number of minutes. • sec—Number of seconds.
Default	Default setting for the threshold.

Field	Explanation
Current	Current value for the threshold.
Overriding Group	Group from which threshold parameter values are applied. (This is the highest priority group to which the element belongs.)

Step 5 When you are done viewing the threshold report, close the window.

For additional information, see the following topic:

- Viewing the Overriding Group—Examples, page 19-6

Editing Operations Manager Thresholds

When you edit thresholds, the values that you update are associated with groups, not with individual devices, ports, or interfaces. When you have finished all changes to thresholds (and polling parameters and priorities), apply all changes. For more information, see Understanding What Happens When You Apply Changes, page 19-16.

Editing Device Group Threshold Settings

To edit threshold settings for Access Port Groups, Trunk Port Groups, and Interface Groups, see Editing Access Port, Trunk Port, and Interface Group Threshold Settings, page 19-30. To selectively enable and disable threshold settings for a device group, see Customizing Operations Manager Threshold Settings, page 19-29.

This procedure explains how to set thresholds for a selected device group.

Step 1 Select **Administration > Polling and Thresholds > Thresholds > Operations Manager**.

Step 2 Select a device group for which you can set thresholds. Generally, this is a device group that does not contain subgroups. (For more information, see Selecting Groups, page 19-9.)

Step 3 Click the **Edit** button. The Thresholds: Edit dialog box appears, displaying the following information.

Field	Description
Group Name	Complete group name. Grayed out because you cannot edit it.
Parameter Type field or list	One or more of the following: • Data Settings—Control thresholds for device reachability, processor and memory, and environment. • Voice Health Settings—Control thresholds for voice-enabled devices, device elements, and Cisco Unified Communications applications. • Voice Utilization Settings—Control thresholds for performance and capacity data collected on voice-enabled devices. Performance polling is disabled by default. **Note** Only parameter types that are applicable for the selected device group are displayed.

Field	Description
Threshold Category list	One or more threshold categories for the parameter type.
Parameter table	The thresholds for the selected parameter type and threshold category.

Step 4 Repeat these steps until you are done editing thresholds for the selected group:

a. Select a parameter type from the Parameter Type list. (If there is only one parameter type, it is already selected and grayed out because you cannot select another.)

b. Select a threshold category from the Threshold Category list.

c. Update the Parameter table:

- Default check box in the table heading—Select this check box to reset default values for *all* thresholds in the category. Selecting or deselecting this check box does the same to all Default check boxes in this column.
- Parameter—Threshold name; grayed out because you cannot edit it.
- Current Value—Grayed out because you cannot edit it.
- New Value—Update this field.
- Default check box in the row—Select this check box to restore this parameter to its default value. This check box is already selected if the current value matches the default value or if you selected the Default check box in the table heading.

Caution Your changes will be lost if you select another threshold category or parameter type before you click Save.

d. Click **Save**. Although the changes to polling parameters are saved in the database, they are not yet applied to the IP fabric. See Applying Changes, page 19-60.

Step 5 Do one of the following:

- Click **Save**; your changes are saved in the database. Click **Cancel**; the Thresholds: Edit dialog box closes. Your changes will not go into effect until you have applied them. See Applying Changes, page 19-60.
- Click **Apply**. A confirmation dialog box appears. For more information, see Understanding What Happens When You Apply Changes, page 19-16. To apply changes to the system, click **Yes**. The Thresholds: Edit dialog box closes. Operations Manager applies changes.

For additional information, see the following topics:

- Threshold Definitions for Data Settings, page 19-42
- Threshold Definitions for Voice Health Settings, page 19-47
- Threshold Definitions for Voice Utilization Settings, page 19-50
- Understanding What Happens When You Apply Changes, page 19-16

Customizing Operations Manager Threshold Settings

You can selectively disable threshold settings, moving them from an active settings list to an inactive settings list. Operations Manager does not monitor threshold parameters for threshold settings that are on an inactive settings list.

Note To disable or enabled *all* threshold settings for a subgroup of Access Port Groups, Trunk Port Groups, and Interface Groups, see Editing Access Port, Trunk Port, and Interface Group Threshold Settings, page 19-30.

Step 1 Select **Administration > Polling and Thresholds > Thresholds > Operations Manager**.

Step 2 Select a group for which you can set thresholds. Generally, this is a group that does not contain subgroups. (For more information, see Editing Operations Manager Thresholds, page 19-27.)

Step 3 Click the **Edit** button. The Managing Thresholds: Edit page appears.

Step 4 Click the **Customize Settings** button. The Thresholds: Customize Settings dialog box appears, displaying the following information.

Field	Explanation
Group Name	Complete group name. Grayed out because you cannot edit it.
The following fields are displayed for each parameter type that is applicable to the selected group.	
Parameter Type	One of the following, grayed out because you cannot edit it: • Data Settings • Voice Health Settings • Voice Utilization Settings
Inactive Settings list	Threshold settings that are currently disabled.
Active Settings list	Threshold settings that are currently enabled.

Step 5 To update the Active Settings list for a particular parameter type, scroll to the parameter type and do the following:

a. Update the inactive and active settings lists:
   - Select threshold settings from the Inactive Settings list and click the **> Add >>** button.
   - Select threshold settings from the Active Settings list and click the **<< Remove <** button.

b. Scroll to the bottom of the window and click **Save**.

Step 6 To reset *all* parameter types with Operations Manager default settings:

a. Click **Revert to Default Settings**. A confirmation dialog box appears.

b. Click **Yes**. The confirmation dialog box and the Thresholds: Customize Settings dialog box close. The Thresholds: Edit dialog box remains open.

c. Close the Thresholds: Edit dialog box.

Note Customized settings have already been saved. To close the Thresholds: Edit dialog box, simply click **Cancel**.

Note The settings are stored in the database, but not yet applied to the IP fabric. See Applying Changes, page 19-60.

Editing Access Port, Trunk Port, and Interface Group Threshold Settings

This procedure explains how to set parameters for threshold settings that are applicable for a selected access port group, trunk port group, or interface group.

Step 1 Select **Administration > Polling and Thresholds > Thresholds > Operations Manager**.

Step 2 Select a subgroup from Access Port Groups, Trunk Port Groups, or Interface Groups.

Step 3 Click the **Edit** button. The Thresholds: Edit dialog box appears, displaying the following information.

Field	Explanation
Group Name	Complete group name. Grayed out because you cannot edit it.
Disable All Threshold Settings check box	When selected, all threshold settings are disabled. To selectively enable and disable threshold settings, see Customizing Operations Manager Threshold Settings, page 19-29.
Threshold Category list	One or more threshold categories for the parameter type.
Parameter table	The thresholds for the selected threshold category.

Step 4 To disable all threshold settings:

a. Select the Disable All Threshold Settings check box.

b. Click **Save**.

c. Go to Step 6.

Step 5 To update thresholds, repeat these steps until you are done editing thresholds for the selected group.

a. Select a threshold category from the Threshold Category list.

b. Update the Parameter table:

- Default check box in the table heading—Select this check box to reset default values for *all* thresholds in the category. Selecting or deselecting this check box does the same to all Default check boxes in this column.
- Parameter—Threshold name; grayed out because you cannot edit it.
- Current Value—Grayed out because you cannot edit it.

- New Value—Update this field.
- Default check box in the row—Select this check box to restore this parameter to its default value. This check box is already selected if the current value matches the default value or if you selected the Default check box in the table heading.

Caution Your changes will be lost if you select another threshold category before you click Save.

c. Click **Save**. Although the polling parameters are saved in the database, they are not yet applied to the IP fabric. See Applying Changes, page 19-60.

Step 6 Do one of the following:

- Click **Save**; your changes are saved in the database. Click **Cancel**; the Thresholds: Edit dialog box closes. Your changes will not go into effect until you have applied them. See Applying Changes, page 19-60.
- Click **Apply**. A confirmation dialog box appears. For more information, see Understanding What Happens When You Apply Changes, page 19-16. To apply changes to the system, click **Yes**. The Thresholds: Edit dialog box closes. Operations Manager applies changes.

Restoring Default Thresholds

Use this procedure to reset the values of parameters in all active threshold settings in all threshold categories for a selected group. (For information on active threshold settings, see Customizing Operations Manager Threshold Settings, page 19-29.)

Before You Begin

To see default threshold values before you apply them, view the Thresholds report; see Viewing Operations Manager Thresholds, page 19-26.

Step 1 Select **Administration > Polling and Thresholds > Thresholds > Operations Manager**.

Step 2 Select a group for which you can set thresholds. Generally, this is a group that has no subgroups. (For more information, see Selecting Groups, page 19-9.)

Step 3 Click the **Revert to Default Settings** button. A confirmation dialog box appears.

Step 4 Click **Yes**.

Note The settings are stored in the database, but not yet applied to the IP fabric. See Applying Changes, page 19-60.

For additional information, see Viewing Operations Manager Thresholds, page 19-26.

Viewing RTMT Thresholds

You can view real-time monitoring threshold (RTMT) parameters for Cisco Unified Communications Manager devices. You can save the RTMT thresholds report in a comma-separated value (CSV) file.

Step 1 Select **Administration > Polling and Thresholds > Thresholds > RTMT**.

Step 2 If you want up-to-the minute data when viewing cluster-specific information, select the **Synchronize** icon in the RTMT Threshold: Select Voice Cluster window to update the information in *all* clusters. Synchronizing the thresholds with RTMT may take a few minutes to complete. If you prefer to see the data now, skip this step and go to Step 3.

Step 3 Select a voice cluster for which you can view thresholds. For more information, see Selecting Groups, page 19-9.

Step 4 Click the **View** button. The Thresholds report window opens and displays the following information for all clusters or Unified Communications Manager devices. The information is updated each hour.

Field	Explanation
Cluster Name	IP address or DNS name of the device or cluster.
Threshold Name	Threshold category name.
Threshold Value	Current value for the threshold.
Unit	Unit of measurement for the threshold: • %—Percent. • count—Number of occurrences. • min—Number of minutes. • sec—Number of seconds.
Last Synchronized Time Stamp	Date and time thresholds were last checked.

Step 5 When you are done viewing the threshold report, close the window.

Configuring RTMT Thresholds

You can edit some of the real-time monitoring threshold (RTMT) parameters for Cisco Unified Communications Manager devices. For example, you may want to change the polling rate or a threshold setting if you do not want to use the default settings in Operations Manager.

To change the threshold setting for the supported events, you must install the RTMT plug-in. The RTMT plug-in is a free tool that comes with the Cisco Unified Communications Manager devices. Operations Manager does not need to install the RTMT plug-in to poll the device data (for example, memory usage) via the RTMT interface. Operations Manager uses the default threshold settings for these events.

Table 19-10 contains a list of the supported thresholds that can be configured in RTMT that will be updated in Operations Manager. These event parameters are fine-tuned based on your device version, so be sure you are familiar with how to configure threshold parameters before doing so.

Table 19-10 Threshold Mappings for Real-Time Monitoring Tool

Event Name in Operations Manager	Threshold Checked for Unified CM 4.x	Threshold Checked for Unified CM 5.x or Later
LowActivePartitionAvailableDiskSpace	Not applicable.	LowActivePartitionAvailableDiskSpace
LogPartitionLowWaterMarkExceeded	Not applicable.	LogPartitionLowWaterMarkExceeded
CPUPegging	CallProcessingNodeCpuPegging	CallProcessingNodeCpuPegging
LowInactivePartitionAvailableDiskSpace	Not applicable.	LowInactivePartitionAvailableDiskSpace
LowSwapPartitionAvailableDiskSpace	Not applicable.	LowSwapPartitionAvailableDiskSpace
LogPartitionHighWaterMarkExceeded	Not applicable.	LogPartitionHighWaterMarkExceeded
LowAvailableVirtualMemory	LowAvailableVirtualMemory	LowAvailableVirtualMemory
LowAvailableDiskSpace	LowAvailableDiskSpace	Not applicable.

For additonal details on the events above, see Supported Events, page E-2.

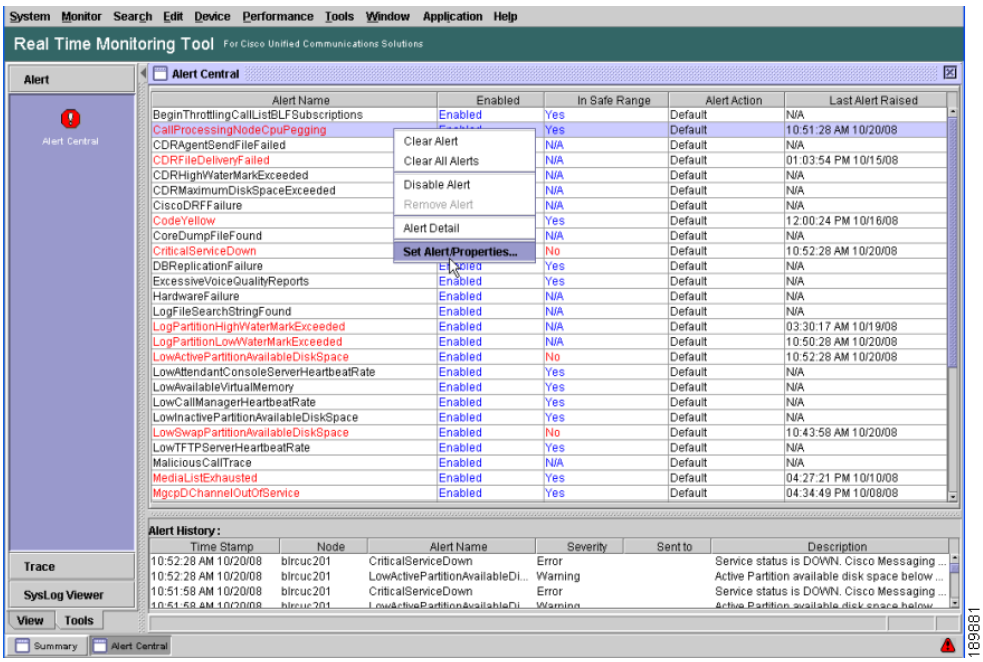
Step 1 On your Cisco Unified Communications Manager, you must have installed the Real-Time Monitoring Tool (RTMT) in order to configure the threshold setting of RTMT poll-based events. To install RTMT, you can download the plug-in from your Cisco Unified Communications Manager device (also called Cisco Unified CallManager depending on your device version). Select **Administration > Application > Plugins**. The plugin name is Cisco Unified CM Real-Time Monitoring Tool - Linux.

For more details, see *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide* on Cisco.com for instructions on how to download this plug-in.

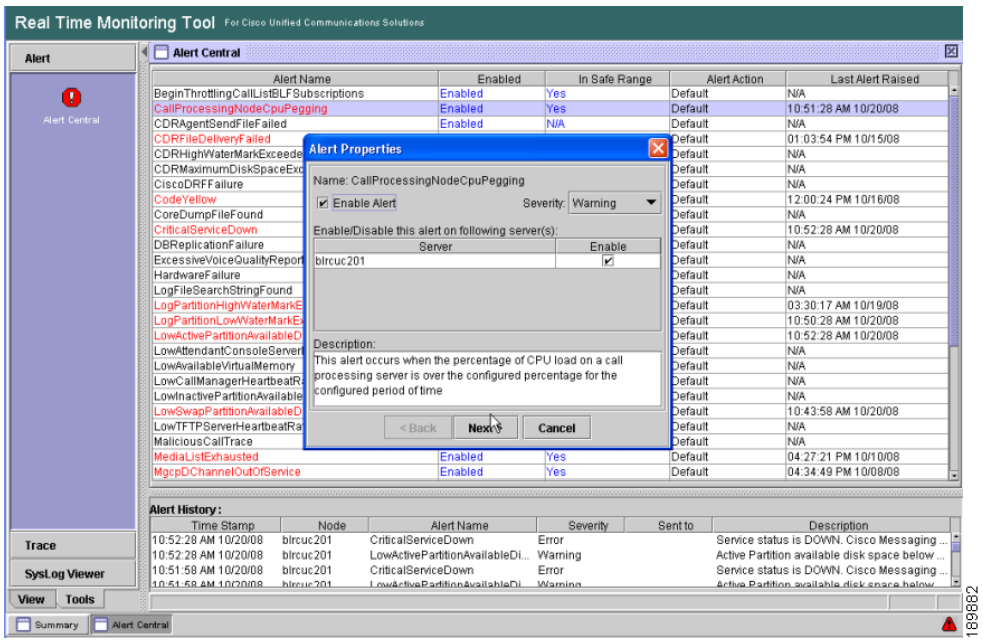
Step 2 Open the RTMT client from and select **Alert > Alert Central**. The Alert Central window appears.

Note The example screens in this procedure are from a Unified Communications Manager, version 5.1.3. For other Unified Communication Manager versions, RTMT plugin download location and interface may vary. See your associated documentation for your Unified Communications Manager version.

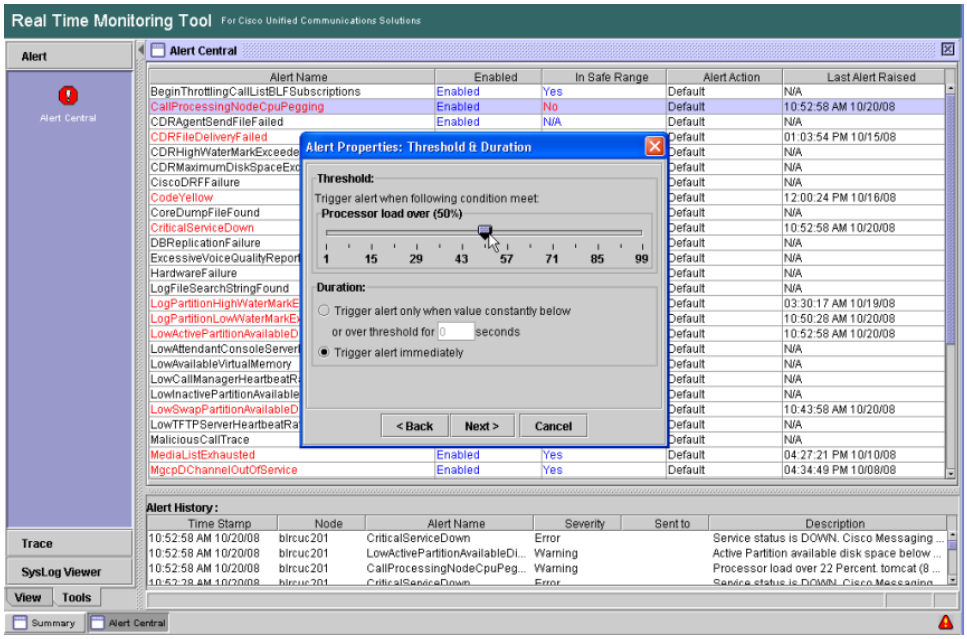
Step 3 Right click on the alert that you want to edit, then select **Set Alert Properties**.



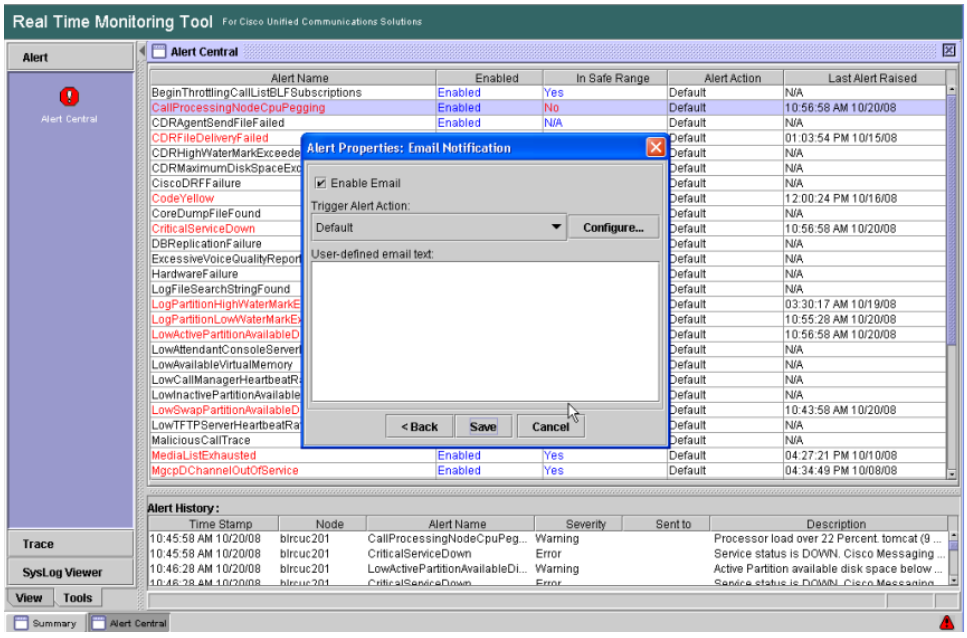
Step 4 Follow the steps in the Alert Properties window to edit the threshold.



Step 5 Enter the appropriate information and click **Next**.



Step 6 Enter the appropriate information and click **Save** to complete the configuration.



Synchronizing RTMT Thresholds

You can synchronize real-time monitoring tool (RTMT) threshold parameters for clusters and Cisco Unified Communications Manager devices. You may want to do this when you do not want to wait for the next scheduled polling. You can also save the RTMT thresholds report in a comma-separated value (CSV) file.

Step 1 Select **Administration > Polling and Thresholds > Thresholds > RTMT Thresholds**.

Step 2 To synchronize thresholds for all voice clusters, click **Synchronize**.

Note There is no option to synchronize individual voice clusters.

Parameter Types, Device Groups, and Threshold Categories

This section provides information on threshold categories for each parameter type:

- Data Settings—Threshold Categories, page 19-36
- Voice Health Settings—Threshold Categories, page 19-38
- Voice Utilization Settings—Threshold Categories, page 19-40

For additional information, see:

- Threshold Definitions for Data Settings, page 19-42
- Threshold Definitions for Voice Health Settings, page 19-47
- Threshold Definitions for Voice Utilization Settings, page 19-50
- Threshold Parameter Values and Events, page 19-56

Data Settings—Threshold Categories

Table 19-12 lists threshold categories for Access Port Groups, Trunk Port Groups, and Interface Groups. Table 19-11 lists data settings threshold categories for all other device groups. An *X* in a column indicates that the setting is applicable to the group.

Table 19-11 Device Settings Threshold Categories by Device Group

	Threshold Categories		
Device Group	**Environment Settings**	**Processor and Memory Settings**	**Reachability Settings**
OM@*server* System Defined Groups			
78XX Media Servers	See Voice Health Settings threshold categories (Voice Health Settings—Threshold Categories, page 19-38.)		X
Expert Advisor	See Voice Health Settings threshold categories.		X
Gatekeepers	X	X	X
H323 GatewayS	X	X	X

Table 19-11 Device Settings Threshold Categories by Device Group

Device Group	Threshold Categories		
	Environment Settings	**Processor and Memory Settings**	**Reachability Settings**
IP Contact Center	X	X	X
Others	X	X	X
Meeting Place	See Voice Health Settings threshold categories.		X
Meeting Place Express	See Voice Health Settings threshold categories.		X
Personal Assistants	See Voice Health Settings threshold categories.		X
SRST Devices	X	X	X
Unified Communication Manager Express	X	X	X
Unified Communication Managers	See Voice Health Settings threshold categories.		X
Unity	See Voice Health Settings threshold categories.		X
Unity Connection	See Voice Health Settings threshold categories.		X
Unity Express	N/A	N/A	X
CS@*server* System Defined Groups			
Broadband Cable	X	X	X
Cisco Interfaces and Modules	N/A	N/A	X
Content Networking	X	X	X
DSL and Long Reach Ethernet (LRE)	X	X	X
Network Management	N/A	N/A	X
Optical Networking	X	X	X
Routers	X	X	X
Security and VPN	X	X	X
Storage Networking	X	X	X
Switches and Hubs	X	X	X
Universal Gateways and Access Servers	X	X	X
Voice and Telephony	X	X	X
Wireless	X	X	X

Table 19-12 lists threshold categories for Operations Manager port and interface groups. For these groups, some threshold categories are disabled by default, indicated by a *D* in the settings column. To enable these settings, see Customizing Operations Manager Threshold Settings, page 19-29.

Note To disable all threshold settings for an interface or port group by selecting a single check box, see Editing Access Port, Trunk Port, and Interface Group Threshold Settings, page 19-30.

Entries in this table are:

- D—Indicates the setting is applicable and disabled by default.
- N/A—Indicates the setting is not applicable.
- X—Indicates the setting is applicable and enabled by default.

Table 19-12 Data Settings Threshold Categories for Access Port, Trunk Port, and Interface Groups

Device Groups	Threshold Categories			
	Backup Interface Support Settings	Dial-on-Demand Interface Support Settings	Generic Interface/Port Performance Settings	Interface/Port Flapping Settings
OM@*server* System Defined Groups				
Access Port Groups/Trunk Port Groups				
1 GB Ethernet	N/A	N/A	X	D
10MB-100MB Ethernet	N/A	N/A	X	D
ATM	N/A	N/A	X	D
Others	N/A	N/A	X	D
Interface Groups				
1 GB Ethernet	D	D	X	D
ATM	D	D	X	X
Backup	X	D	D	D
Dial-On-Demand	D	X	D	D
FDDI	D	D	X	D
ISDN B channel	X	D	D	D
ISDN D channel	D	D	D	X
ISDN physical interface	D	D	X	X
Others	D	D	X	X
Serial	D	D	X	X
Token ring	D	D	X	D

Voice Health Settings—Threshold Categories

Table 19-13 lists threshold categories for voice health settings and the device groups for which they are available.

Table 19-13 Voice Health Settings Threshold Categories by Device Group

Device Group	Voice Health Settings Threshold Categories
OM@server System Defined Groups	
78XX Media Servers	Cisco CommunicationManager Threshold Settings Cisco Unity Threshold Settings Disk Usage and Virtual Memory Settings Environment - Temperature Sensor Settings MWI Threshold Settings Processor and Memory Settings
Expert Advisor	Disk Usage and Virtual Memory Settings Environment - Temperature Sensor Settings Processor and Memory Settings
IP Contact Center	Disk Usage and Virtual Memory Settings Processor and Memory Settings
Meeting Place	Disk Usage and Virtual Memory Settings Environment - Temperature Sensor Settings Processor and Memory Settings
Meeting Place Express	Disk Usage and Virtual Memory Settings Environment - Temperature Sensor Settings Processor and Memory Settings
Personal Assistants	Personal Assistant Threshold Settings Processor and Memory Settings
Unified Communication Manager Express	Cisco CommunicationManager Threshold Settings MWI Threshold Settings
Unified Communication Manager	Disk Usage and Virtual Memory Settings Environment - Temperature Sensor Settings MWI Threshold Settings Processor and Memory Settings
Unity	Cisco Unity Services Settings Cisco Unity Threshold Settings Disk Usage and Virtual Memory Settings Environment - Temperature Sensor Settings MWI Threshold Settings Processor and Memory Settings

Table 19-13 Voice Health Settings Threshold Categories by Device Group (continued)

Device Group	Voice Health Settings Threshold Categories
Unity Connection	Disk Usage and Virtual Memory Settings Environment - Temperature Sensor Settings Processor and Memory Settings MWI Threshold Settings
Unity Express	Cisco Unity Express Threshold Settings MWI Threshold Settings
Voice Gateways	Cisco CommunicationManager Threshold Settings Processor and Memory Settings
Voice Mail Gateways	Processor and Memory Settings
OM@*server* User Defined Groups	
User Defined Groups	Cisco CommunicationManager Threshold Settings Cisco Unity Express Threshold Settings Cisco Unity Threshold Settings Disk Usage and Virtual Memory Settings Environment - Temperature Sensor Settings MWI Threshold Settings Processor and Memory Settings **Note** These settings are disabled by default. To enable them, see Customizing Operations Manager Threshold Settings, page 19-29.
CS@*server* System Defined Groups	
Cisco Interfaces and Modules	Cisco Unity Express Threshold Settings MWI Threshold Settings
Routers	Reachability Settings
Voice and Telephony	Cisco Unity Threshold Settings Disk Usage and Virtual Memory Settings Environment - Temperature Sensor Settings Processor and Memory Settings

Voice Utilization Settings—Threshold Categories

Voice Utilization Settings threshold categories contain thresholds that measure port utilization and resource utilization. Performance polling, which is disabled by default, collects the necessary data for these measurements. To enable performance polling, see Voice Utilization Settings—Polling, page 19-23 and Editing Polling Parameters, page 19-13.

Table 19-14 lists the Voice Utilization Settings threshold categories and the device groups for which they are available.

Table 19-14 Voice Utilization Settings Threshold Categories by Device Group

Device Group	Threshold Categories
OM@*server* System Defined Groups	
78XX Media Servers	Cisco CommunicationManager Port Utilization, page 19-51 MGCP Gateway Port Utilization, page 19-55
CommunicationManager Express	Cisco CommunicationManager Express Utilization, page 19-51 Gatekeeper Utilization, page 19-53 H323 Gateway Port Utilization, page 19-54
CommunicationManagers	Cisco CommunicationManager Port Utilization, page 19-51 MGCP Gateway Port Utilization, page 19-55
Cisco Unified Communications Manager or Cluster	None
Gatekeepers	Cisco CommunicationManager Express Utilization, page 19-51 Gatekeeper Utilization, page 19-53 H323 Gateway Port Utilization, page 19-54
H323 Gateways	Cisco CommunicationManager Express Utilization, page 19-51 Gatekeeper Utilization, page 19-53 H323 Gateway Port Utilization, page 19-54
SRST Devices	Cisco CommunicationManager Express Utilization, page 19-51 Gatekeeper Utilization, page 19-53 H323 Gateway Port Utilization, page 19-54
Unity	Cisco Unity Utilization, page 19-53
Unity Connection	Cisco Unity Connection Utilization, page 19-53
Unity Express	Cisco Unity Express Utilization, page 19-53
Voice Gateways	Cisco CommunicationManager Express Utilization, page 19-51 Gatekeeper Utilization, page 19-53 H323 Gateway Port Utilization, page 19-54
Voice Mail Gateways	Voice Mail Gateway Utilization, page 19-55
OM@*server* User Defined Groups	

Table 19-14 Voice Utilization Settings Threshold Categories by Device Group (continued)

Device Group	Threshold Categories
User Defined Groups	Cisco CommunicationManager Express Utilization, page 19-51 Cisco CommunicationManager Port Utilization, page 19-51 Cisco Unity Utilization, page 19-53 Gatekeeper Utilization, page 19-53 H323 Gateway Port Utilization, page 19-54 MGCP Gateway Port Utilization, page 19-55 Cisco Unity Express Utilization, page 19-53 Voice Mail Gateway Utilization, page 19-55
CS@*server* System Defined Groups	
Cisco Interfaces and Modules	Cisco Unity Express Utilization, page 19-53
Routers	Cisco CommunicationManager Express Utilization, page 19-51 Gatekeeper Utilization, page 19-53 H323 Gateway Port Utilization, page 19-54
Universal Gateways and Access Servers	H323 Gateway Port Utilization, page 19-54
Voice and Telephony	Cisco CommunicationManager Express Utilization, page 19-51 Cisco CommunicationManager Port Utilization, page 19-51 Gatekeeper Utilization, page 19-53 H323 Gateway Port Utilization, page 19-54 MGCP Gateway Port Utilization, page 19-55 Voice Mail Gateway Utilization, page 19-55

Threshold Definitions for Data Settings

This section contains threshold definitions for the following Data Settings threshold categories:

- Disk Usage and Virtual Memory Settings (Data Settings), page 19-43
- Environment Settings (Data Settings), page 19-43
- Generic Interface/Port Performance Settings, page 19-43
- Interface/Port Flapping Settings, page 19-44
- Backup Interface Support Settings, page 19-45
- Dial-On-Demand Interface Support Settings, page 19-45
- Processor and Memory Settings (Data Settings), page 19-45
- Reachability Settings, page 19-46

Disk Usage and Virtual Memory Settings (Data Settings)

Note For voice-enabled devices, see Disk Usage and Virtual Memory Settings (Voice Health), page 19-49.

Disk Usage and Virtual Memory Settings monitors the performance of disk usage and virtual memory elements. Events such as high disk utilization and high virtual memory utilization are controlled by these parameters.

Drive Array Faults Threshold

Count of drive array faults.

Free Hard Disk Threshold

Minimum amount of hard disk space, expressed as a percentage of the total hard disk memory.

Free Memory Threshold

Minimum amount of free virtual memory, expressed as a percentage of total virtual memory.

Environment Settings (Data Settings)

Note For voice-enabled devices, see Environment - Temperature Sensor Settings (Voice Health Settings), page 19-49.

Relative Temperature Threshold

Indicates how close the current temperature value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value. For example, if the shutdown temperature is 50° C and the Relative Temperature Threshold is 10%, the OutofRange event occurs if the temperature exceeds 45° C.

Relative Voltage Threshold

Indicates how close the current voltage value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value. For example, if the shutdown value is +30V and the Relative Voltage Threshold is 10%, the OutofRange event occurs if the voltage exceeds +27V.

Generic Interface/Port Performance Settings

These threshold categories configure the monitoring of a adapter's performance characteristics. The categories include basic parameters—such as utilization, errors, broadcast, and packet drops—common to all media types.

Broadcast Threshold

The upper broadcast traffic, expressed as a percentage of the total bandwidth.

Collision Threshold

The upper threshold for collisions, expressed as a percentage of the total number of output packets. This threshold applies only to Ethernet settings for ports, trunks, and interfaces.

Discard Threshold

The upper dropped packets, expressed as a percentage of the total number of packets.

Error Threshold

The upper packet errors, expressed as a percentage of the total number of packets. Operations Manager generates the HighErrorRate event when both Error Threshold and Error Traffic Threshold are reached or exceeded.

Error Traffic Threshold

The upper packet rate, expressed as a percentage of the total bandwidth. Operations Manager generates the HighErrorRate event when both Error Threshold and Error Traffic Threshold are reached or exceeded. The value for Error Traffic Threshold can include up to two decimal places.

Queue Drop Threshold

The acceptable percentage of packets dropped because of full queues, expressed as a percentage of the total number of packets.

Utilization Threshold

The upper link utilization, expressed as a percentage of the total bandwidth.

Interface/Port Flapping Settings

These settings control the analysis of network adapters (ports and interfaces) that are continually going up and down, or flapping. Flapping analysis monitors SNMP link down traps to identify a flapping network adapter. Operations Manager reports flapping as a fault condition. For more information, see Appendix H, "How Operations Manager Calculates Repeated Restarts and Flapping."

Note Interface/Port Flapping Settings are disabled by default for some port and interface groups. For more information, see Table 19-12.

Link Trap Threshold

The number of SNMP link down traps that must be received within the Link Trap Window for Operations Manager to consider the interface or port flapping. A value of 0 disables flapping analysis.

Link Trap Window

The amount of time used to monitor flapping analysis of a port or interface. If the number of link down traps meets or exceeds the Link Trap Threshold during this window of time, the interface or port is considered to be flapping.

Backup Interface Support Settings

Backup Interface Support Settings configures an interface as a backup. When an interface is identified as a backup:

- The InterfaceOperationallyDown event is not generated if the interface is down.
- The ExceededMaximumUptime event is generated if the interface stays up too long.

Note Backup Interface Support Settings are disabled by default for some port and interface groups. For more information, see Table 19-12.

The following parameter is included in the Backup Interface Support Settings threshold category.

Maximum Up Time

The maximum length of time, in seconds, that the interface might be up before the ExceededMaximumUptime event is generated. If the value of this parameter is 0, the ExceededMaximumUptime event is disabled.

The minimum value is 0, and the maximum value is 86400.

Dial-On-Demand Interface Support Settings

The Dial-On-Demand Interface Support settings identifies an interface as dial-on-demand. In this case:

- The InterfaceOperationallyDown event is not generated if the interface is down.
- The ExceededMaximumUptime event is generated if the interface stays up too long.

Note Dial-on-Demand Interface Settings are disabled by default for some port and interface groups. For more information, see Table 19-12.

Maximum Up Time

The maximum length of time that the interface may be up before the ExceededMaximumUptime event is generated. If the value of this parameter is 0, the ExceededMaximumUptime event is disabled.

The minimum value is 0, and the maximum value is 86400.

Processor and Memory Settings (Data Settings)

Note For voice-enabled devices, see Processor and Memory Settings (Voice Health), page 19-50.

The Processor and Memory Settings control the performance monitoring of a system's processor and its associated memory elements.

Backplane Utilization Threshold

The upper threshold for a switch’s backplane utilization, expressed as a percentage of the total backplane bandwidth.

Free Memory Threshold

The lower threshold for the acceptable amount of free memory, as measured by the ratio of free memory to the total memory.

Memory Buffer Miss Threshold

The upper threshold for the number of buffer misses, expressed as a percentage of the total number of buffer requests.

Memory Buffer Utilization Threshold

The upper threshold for the number of buffers used, expressed as a percentage of the total number of buffers.

Memory Fragmentation Threshold

The lower threshold for memory fragmentation. The fragmentation value is the ratio of the largest number of contiguous unallocated bytes to the total amount of free memory. For example, a value of 5 indicates that the largest free buffer must be at least 5% of the free memory.

Processor Utilization Threshold

The upper threshold for processor utilization, expressed as a percentage of the total capacity of the processor.

Reachability Settings

The reachability settings configure reachability parameters for network adapters (ports and interfaces). They also control the analysis of systems that repeatedly restart, triggering Repeated Restarts and Flapping events. The following parameters are included in the Reachability Settings threshold category.

Restart Trap Threshold

The number of SNMP cold or warm start traps that must be received within the amount of time set by the Restart Trap Window parameter for Operations Manager to consider a system to be performing excessive restarts. A value of 0 disables restart analysis. For more information, see Appendix H, "How Operations Manager Calculates Repeated Restarts and Flapping."

Note If you want cold and warm start traps to generate events to be displayed immediately in the Alerts and Activities display, set the value of Restart Trap Threshold to 1.

Restart Trap Window

The amount of time used to monitor a system's repeated restarts. If the number of start traps meets or exceeds the Restart Trap Threshold during this window of time, the system is considered to be performing excessive restarts.

The minimum value is 30 seconds, and the maximum value is 3600 seconds.

Threshold Definitions for Voice Health Settings

This section contains threshold definitions for voice health settings threshold categories:

Cisco CommunicationManager Threshold Settings

This threshold category measures resource usage on the Cisco Unified Communications Manager platform.

Attendant Console Heartbeat Threshold

Lower threshold for the number of Cisco Unified Communications Manager attendant heartbeats per minute.

CCM Line Link Threshold

Value indicating that the line link state information has been received from Cisco Unified Communications Manager.

Messaging Interface Heartbeat Threshold

Lower threshold for the number of Cisco Messaging interface heartbeats per minute.

Outbound Busy Attempts Threshold

Lower threshold for the number of seconds during which a call through this analog access was attempted when no ports were available.

Ports Active Threshold

Upper threshold for the number of active ports.

Ports Out of Service Threshold

Upper threshold for the number of ports that are out of service.

Cisco CommunicationManager Heartbeat Threshold

Lower threshold for number of Cisco Unified Communications Manager heartbeats per minute.

MOH Out of Resources Threshold

Upper threshold for number of times that an attempt was made to allocate a Music On Hold (MOH) resource when all MOH servers were active or when no MOH servers were registered.

MTP Out of Resources Threshold

Upper threshold for the number of times an attempt was made to allocate an MTP resources.

MOH Connections Lost Threshold

Upper limit for the number of MOH servers that have lost connection with the Cisco Unified Communications Manager.

TFTP Heartbeat Threshold

Lower threshold for the number of Cisco TFTP Service heartbeats per minute.

Hardware Conference Out of Resources Threshold

Upper threshold for number of times in an interval that a conference was requested when none was available.

Software Conference Out of Resources Threshold

Upper threshold for number of times in an interval that a conference was requested when none was available.

High Priority Queue Size Threshold

Upper threshold for size of the high priority queue.

Normal Priority Queue Size Threshold

Upper threshold for size of the normal priority queue.

Low Priority Queue Size Threshold

Upper threshold for size of the low priority queue.

TFTP Aborted Requests Threshold

Upper threshold for number of TFTP aborted requests.

Location Out of Resources Threshold

Upper threshold for number of times the node is out of location bandwidth resources.

Cisco Unity Express Threshold Settings

This threshold measure mailbox time used against allocated capacity.

Total Time Used Threshold

Upper limit on total time used in minutes for greetings and messages in all mailboxes, expressed as a percentage of total allocated capacity.

Cisco Unity Services Settings

This threshold category measures Cisco Unity voice services.

CPU Utilization Threshold

CPU utilization threshold for Cisco Unity voice services.

Cisco Unity Threshold Settings

This threshold category measures Cisco Unity port usage.

Unity License Threshold

Upper limit on the number of Unity licenses in use.

Unity Inbox License Threshold

Upper limit on the number of Unity inbox licenses in use.

Disk Usage and Virtual Memory Settings (Voice Health)

Disk usage and virtual memory settings monitor the performance of disk usage and virtual memory elements. Events such as high disk utilization and high virtual memory utilization are controlled by these parameters.

Free Hard Disk Threshold

Minimum amount of hard disk space, expressed as a percentage of the total hard disk memory.

Free Virtual Memory Threshold

Minimum amount of free virtual memory, expressed as a percentage of total virtual memory.

Environment - Temperature Sensor Settings (Voice Health Settings)

This setting measures temperature on voice-enabled devices. For definitions of environment thresholds that you can set on infrastructure devices, see Environment Settings (Data Settings), page 19-43.

Relative Temperature Threshold

Indicates how close the current temperature value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value. For example, if the shutdown temperature is 50° C and the Relative Temperature Threshold is 10%, the OutofRange event occurs if the temperature exceeds 45° C.

MWI Threshold Settings (Voice Health Settings)

This threshold category specifies how quickly the Unity message waiting indicator light must appear.

MWI On-Time Threshold

Number of seconds within which the Unity message waiting indicator (MWI) light must appear.

Cisco Personal Assistant Threshold Settings (Voice Health Settings)

CPA Login Failure

Total number of failed Cisco Personal Assistant login attempts.

CPA Transfer Failed

Number of times that Cisco Personal Assistant tried and failed to transfer a call.

CPA Voice Mail

The total number of times that callers tried to access voice mail or the total number of voice mail login failures.

Processor and Memory Settings (Voice Health)

The Processor and Memory Settings control the performance monitoring of a system's processor and its associated memory elements.

Free Physical Memory Threshold

The lower threshold for free physical memory, expressed as a percentage of total physical memory.

Processor Utilization Threshold

The upper threshold for processor utilization, expressed as a percentage of the total capacity of the processor.

Threshold Definitions for Voice Utilization Settings

This section contains definitions for thresholds in the following Voice Utilization Settings threshold categories:

- Cisco CommunicationManager Express Utilization, page 19-51
- Cisco CommunicationManager Port Utilization, page 19-51
- Cisco Unity Connection Utilization, page 19-53
- Cisco Unity Express Utilization, page 19-53
- Cisco Unity Utilization, page 19-53
- Gatekeeper Utilization, page 19-53
- H323 Gateway Port Utilization, page 19-54

- MGCP Gateway Port Utilization, page 19-55
- Voice Mail Gateway Utilization, page 19-55

Cisco CommunicationManager Express Utilization

This utilization setting measures the number of IP phones and key IP phones against the maximum numbers for each.

Registered IP Phones Threshold

The number of IP phones that are registered to Cisco Unified Communications Manager Express, expressed as a percentage of the maximum allowable number of phones.

Registered Key IP Phones Threshold

The number of key IP phones that are registered to Cisco Unified Communications Manager Express, expressed as a percentage of the maximum allowable number of key IP phones.

Cisco CommunicationManager Port Utilization

Cisco CommunicationManager Port Utilization settings measure MGCP port and resource utilization on the system where Cisco Unified Communications Manager is installed.

FXS Port Utilization Threshold

Upper threshold on the number of active FXS ports, expressed as a percentage of total FXS ports configured on the Cisco Unified CommunicationManager platform.

FXO Port Utilization Threshold

Upper threshold on the number of active FXO ports, expressed as a percentage of total FXO ports configured on the Cisco Unified CommunicationManager platform.

BRI Channel Utilization Threshold

Upper threshold on the number of active BRI ports, expressed as a percentage of total BRI ports configured on the Cisco Unified CommunicationManager platform.

T1 PRI Channel Utilization Threshold

Upper threshold on the number of active T1 PRI channels, expressed as a percentage of total T1 PRI channels configured on the Cisco Unified Communications Manager platform.

E1 PRI Channel Utilization Threshold

Upper threshold on the number of active E1 PRI channels, expressed as a percentage of total E1 PRI channels configured on the Cisco Unified Communications Manager platform.

T1 CAS Channel Utilization Threshold

Upper threshold on the number of active T1 CAS channels, expressed as a percentage of total T1 CAS channels configured on the Cisco Unified Communications Manager platform.

MOH Multicast Resources Active Threshold

Upper threshold on the number of Music on Hold (MOH) multicast resources that are active, expressed as a percentage of total multicast resources available.

MOH Unicast Resources Active Threshold

Music on Hold (MOH) unicast resources that are active, expressed as a percentage of total unicast resources available.

MTP Resources Active Threshold

Media Termination Point (MTP) resources that are active, expressed as a percentage of total MTP resources available.

Transcoder Resources Active Threshold

Transcoder resources that are active, expressed as a percentage of total Transcoder resources available.

Hardware Conference Resources Active Threshold

Hardware conference resources that are active, expressed as a percentage of total hardware conference resources available.

Software Conference Resources Active Threshold

Software conference resources that are active, expressed as a percentage of total software conference resources available.

Conferences Active Threshold

Number of conferences that are active, expressed as a percentage of total number of supported conferences.

Conference Streams Active Threshold

Number of conferences streams that are active, expressed as a percentage of total number of supported conference streams.

MOH Streams Active Threshold

Number of MOH streams that are active, expressed as a percentage of total number of supported MOH streams.

MTP Streams Active Threshold

Number of MTP streams that are active, expressed as a percentage of total number of supported MTP streams.

Location Bandwidth Available Threshold

The lower acceptable location-based bandwidth available, expressed as a percentage of total location-based bandwidth.

Cisco Unity Connection Utilization

Inbound Port Utilization Threshold

The upper threshold on the number of active inbound ports, expressed as a percentage of the total inbound ports.

Outbound Port Utilization Threshold

The upper threshold on the number of active outbound ports, expressed as a percentage of the total outbound ports.

Cisco Unity Express Utilization

Cisco Unity Express Utilization settings measure voicemail usage, active sessions, and orphaned mailboxes.

Capacity Utilization Threshold

Upper threshold for total number of voicemail minutes used (sum of all user mailboxes), expressed as a percentage of maximum minutes of voicemail capacity.

Session Utilization Threshold

Upper threshold for number of active sessions, expressed as a percentage of maximum number of sessions.

Orphaned Mailboxes Threshold

Lower threshold for current number of mailboxes that are not associated with an owner, expressed as a percentage of total mailboxes.

Note A mailbox is said to be *orphaned* when a user is deleted, but the mailbox is not. The mailbox will continue to take up its defined allocated capacity on the storage media.

Cisco Unity Utilization

Cisco Unity Utilization settings measure inbound and outbound port utilization.

Inbound Port Utilization Threshold

Upper threshold on the number of active inbound ports, expressed as a percentage of total inbound ports.

Outbound Port Utilization Threshold

Upper threshold on the number of active outbound ports as a percentage of total outbound ports.

Gatekeeper Utilization

Gatekeeper Utilization measures total bandwidth and interbandwidth utilization for the local zone.

Note If bandwidth limitation is not set on the gatekeeper, there will be no gatekeeper utilization data.

Total Bandwidth Utilization for Local Zone Threshold

If bandwidth limitation is set, upper bandwidth, expressed as a percentage of bandwidth allocated for the local zone.

Interzone Bandwidth Utilization for Local Zone Threshold

If bandwidth limitation is set, upper interzone bandwidth, expressed as a percentage of interzone bandwidth allocated for the local zone.

H323 Gateway Port Utilization

H323 Gateway Port Utilization measures port usage on H323 gateways.

FXS Port Utilization Threshold

Upper threshold for number of active FXS ports, expressed as a percentage of total FXS ports configured on the H323 gateway.

FXO Port Utilization Threshold

Upper threshold for number of active FXO ports, expressed as a percentage of total FXO ports configured on the H323 gateway.

EM Port Utilization Threshold

Upper threshold for number of active ear and mouth (E&M) ports, expressed as a percentage of total E&M ports configured on the H323 gateway.

BRI Channel Utilization Threshold

Upper threshold for number of BRI channels that are in use, expressed as a percentage of total BRI channels configured on the H323 gateway.

T1 PRI Channel Utilization Threshold

Upper threshold for number of T1 PRI channels that are in use, expressed as a percentage of total T1 PRI channels configured on the H323 gateway.

E1 PRI Channel Utilization Threshold

Upper threshold for number of E1 PRI channels that are in use, expressed as a percentage of total E1 PRI channels configured on the H323 gateway.

T1 CAS Channel Utilization Threshold

Upper threshold for number of T1 CAS channels that are in use as a expressed percentage of total T1 CAS channels configured on the H323 gateway.

E1 CAS Channel Utilization Threshold

Upper threshold for number of E1 CAS channels that are in use, expressed as a percentage of total E1 CAS channels configured on the H323 gateway.

DSP Utilization Threshold

Upper threshold for the number of active channels on digital signal processor (DSP), expressed as a percentage of total channels on DSP on the H323 gateway.

MGCP Gateway Port Utilization

Media Gateway Control Protocol (MGCP) Gateway Port Utilization settings measure port utilization on MGCP gateways registered to a Cisco Unified Communications Manager.

FXS Port Utilization Threshold

Upper threshold for number of active FXS ports, expressed as a percentage of total FXS ports configured on the MGCP gateway.

FXO Port Utilization Threshold

Upper threshold for number of active FXO ports, expressed as a percentage of total FXO ports configured on the MGCP gateway.

BRI Channel Utilization Threshold

Upper threshold for number of BRI channels that are in use, expressed as a percentage of total BRI channels configured on the MGCP gateway.

T1 PRI Channel Utilization Threshold

Upper threshold for number of T1 PRI channels that are in use, expressed as a percentage of total T1 PRI channels configured on the MGCP gateway.

E1 PRI Channel Utilization Threshold

Upper threshold for number of E1 PRI channels that are in use, expressed as a percentage of total E1 PRI channels configured on the MGCP gateway.

T1 CAS Channel Utilization Threshold

Upper threshold for number of T1 CAS channels that are in use as a expressed percentage of total T1 CAS channels configured on the MGCP gateway.

Voice Mail Gateway Utilization

This threshold category measures port utilization on a voice mail gateway.

Voice Mail Port Utilization Threshold

Upper threshold for the number of active voice mail ports as a percentage of total voice mail ports configured on the voice mail gateway.

PBX Port Utilization Threshold

Upper threshold for the number of active PBX ports, expressed as a percentage of total PBX ports configured on the voice mail gateway.

Threshold Parameter Values and Events

Table 19-15 lists threshold categories, the threshold parameters in each category, minimum and maximum values for the threshold parameters, and the events that Operations Manager generates when values pass the threshold.

Note Most thresholds are upper thresholds, representing the highest acceptable value. Lower thresholds are the exception and are footnoted as such.

Table 19-15 Minimum and Maximum Threshold Parameter Values and Related Events

Threshold Category	Threshold Parameter (with unit of measure)	Min	Max	Events	Parameter Type
Backup Interface Support Settings	Maximum Up Time (seconds)	0	86400	ExceededmaximumUptime	Data Settings
Cisco Communication Manager Express Utilization	Registered IP Phones Threshold (%)	1	100	HighResourceUtilization	Voice Utilization Settings
	Registered Key IP Phones Threshold (%)			HighResourceUtilization	

Table 19-15 Minimum and Maximum Threshold Parameter Values and Related Events (continued)

Threshold Category	Threshold Parameter (with unit of measure)	Min	Max	Events	Parameter Type
Cisco Communication Manager Port Utilization	FXS Port Utilization Threshold (%)			HighAnalogPortUtilization	
	FXO Port Utilization Threshold (%)				
	BRI Channel Utilization Threshold (%)			HighDigitalPortUtilization	
	T1 PRI Channel Utilization Threshold (%)				
	E1 PRI Channel Utilization Threshold (%)				
	T1 CAS Channel Utilization Threshold (%)			HighResourceUtilization	Voice Utilization Settings
	MOH Multicast Resources Active Threshold (%)				
	MOH Unicast Resources Active Threshold (%)				
	MTP Resources Active Threshold (%)				
	Transcoder Resources Active Threshold (%)				
	Hardware Conference Resources Active Threshold (%)				
	Software Conference Resources Active Threshold (%)				
	Conferences Active Threshold (%)				
	Conference Streams Active Threshold (%)				
	MOH Streams Active Threshold (%)				
	MTP Streams Active Threshold (%)				
	Location Bandwidth Available Threshold (%)				
Cisco Unity Connection Utilization	Inbound Port Utilization Threshold (%)	1	100	HighPortUtilization	Voice Utilization Settings
	Outbound Port Utilization Threshold (%)				
Cisco Unity Express Threshold Settings	Total Time Used Threshold (%)	0	100	TotalTimeUsedThresholdExceeded	Voice Health Settings

Table 19-15 Minimum and Maximum Threshold Parameter Values and Related Events (continued)

Threshold Category	Threshold Parameter (with unit of measure)	Min	Max	Events	Parameter Type
Cisco Unity Express Utilization	Capacity Utilization Threshold (%) Session Utilization Threshold (%) Orphaned Mailboxes Threshold (%)	1	100	HighResourceUtilization	Voice Utilization Settings
Cisco Unity Services Settings	CPU Utilization Threshold (%)			cpuUtilizationExceeded	Voice Health Settings
Cisco Unity Threshold Settings [1]	Unity License Threshold (count) Unity Inbox License Threshold (count)			AvailableLicenseLow AvailableInboxLicenseLow	Voice Health Settings
	Hung Port Threshold (seconds)	1800	7200	UnityPortHung	
Cisco Unity Utilization	Inbound Port Utilization Threshold (%) Outbound Port Utilization Threshold (%)	1	100	HighPortUtilization	Voice Utilization Settings
Dial-On-Demand Interface Support Settings	Maximum Up Time (seconds)	0	86400	ExceededmaximumUptime	Data Settings
Disk Usage and Virtual Memory Settings	Drive Array Faults Threshold (%)	0	100	ExcessiveDAFaults	Voice Health Settings
	Free Hard Disk Threshold (%) Free Virtual Memory Threshold (%)			InsufficientFreeHardDisk InsufficientFreeVirtualMemory	Data Settings/ Voice Health Settings
Environment - Temperature Sensor Settings	Relative Temperature Threshold (%)			OutofRange TemperatureHigh TemperatureSensorDegraded	Voice Health Settings
Environment Settings	Relative Temperature Threshold (%) Relative Voltage Threshold (%)				Data Settings
Gatekeeper Utilization	Total Bandwidth Utilization for Local Zone Threshold (%) Interzone Bandwidth Utilization for Local Zone Threshold (%)	1	100	HighResourceUtilization	Voice Utilization Settings

Table 19-15 Minimum and Maximum Threshold Parameter Values and Related Events (continued)

Threshold Category	Threshold Parameter (with unit of measure)	Min	Max	Events	Parameter Type
Generic Interface/Port Performance Settings	Broadcast Threshold (%)	0	100	HighBroadcastRate	Data Settings
	Collision Threshold (%)			HighCollisionRate	
	Discard Threshold (%)			HighDiscardRate	
	Error Threshold (%)				
	Error Traffic Threshold (%)	0.00	100.00	HighErrorRate	
	Queue Drop Threshold (%)	0	100	HighQueueDropRate	
	Utilization Threshold (%)			HighUtilization	
H323 Gateway Port Utilization	FXS Port Utilization Threshold (%)	1	100	HighAnalogPortUtilization	Voice Utilization Settings
	FXO Port Utilization Threshold (%)				
	EM Port Utilization Threshold (%)				
	BRI Channel Utilization Threshold (%)			HighDigitalPortUtilization	
	T1 PRI Channel Utilization Threshold (%)				
	E1 PRI Channel Utilization Threshold (%)				
	T1 CAS Channel Utilization Threshold (%)				
	E1 CAS Channel Utilization Threshold (%)				
	DSP Utilization Threshold (%)			HighResourceUtilization	
Interface/Port Flapping Settings	Link Trap Threshold (count)	0	10	Repeated Restarts	Data Settings
	Link Trap Window (sec)	30	3600	Flapping	
MGCP Gateway Port Utilization	FXO Port Utilization Threshold (%)	1	100	HighAnalogPortUtilization	Voice Utilization Settings
	FXS Port Utilization Threshold (%)				
	BRI Channel Utilization Threshold (%)			HighDigitalPortUtilization	
	T1 PRI Channel Utilization Threshold (%)				
	E1 PRI Channel Utilization Threshold (%)				
	T1 CAS Channel Utilization Threshold (%)				
MWI Threshold Settings	MWI On-Time Threshold (seconds)	5	240	MWIOnTimeExceeded	Voice Health Settings

Table 19-15 Minimum and Maximum Threshold Parameter Values and Related Events (continued)

Threshold Category	Threshold Parameter (with unit of measure)	Min	Max	Events	Parameter Type
Personal Assistant Threshold Settings	CPA Login Failure (count) CPA Transfer Fail (count) CPA Voice Mail (count)	0	100	CPALoginFailureThresholdExceeded CPATransferFailedThreshold Exceeded CPAVoicemailThresholdExceeded	Voice Health Settings
Processor and Memory Settings	Backplane Utilization Threshold (%) Free Memory Threshold (%) Memory Buffer Miss Threshold (%) Memory Buffer Utilization Threshold (%) Memory Fragmentation Threshold (%) Processor Utilization Threshold (%)	0	100	HighBackplaneUtilization InsufficientFreeMemory HighBufferMissRate HighBufferUtilization ExcessiveFragmentation HighUtilization	Data Settings
Processor and Memory Settings	Free Physical Memory Threshold (%) Processor Utilization Threshold (%)	0	100	InsufficientFreePhysicalMemory HighUtilization	Voice Health Settings
Reachability Settings	Restart Trap Threshold (count) Restart Trap Window (seconds)	0 30	10 3600	RepeatedRestarts Flapping	Data Settings
Voice Mail Gateway Utilization	Voice Mail Port Utilization Threshold (%) PBX Port Utilization Threshold (%)	0	100	HighPortUtilization	Voice Utilization Settings

1. For details on which events to use instead of obsolete events, see Obsolete Events, page E-33.

Applying Changes

Changes to polling parameters and threshold values do not take effect until you apply changes, thereby reconfiguring Operations Manager to use the new values. Similarly, after you resume devices or device components that were suspended from polling, you must apply changes for the device elements to be polled.

Before You Begin

Applying changes is a CPU-intensive event that might take between one and five minutes to complete. Therefore, to minimize system impact, consider doing the following when possible:

- Consolidating changes to polling parameters and threshold values, thereby limiting the number of times you will need to apply them.
- Applying changes during a low-usage time.

Note Synthetic tests do not run while Operations Manager applies changes.

You can apply changes while you are editing polling parameters or thresholds. See:

- Editing Polling Parameters, page 19-13
- Editing Device Group Threshold Settings, page 19-27
- Editing Access Port, Trunk Port, and Interface Group Threshold Settings, page 19-30.

Alternatively, you can apply changes using this procedure.

Step 1 Select **Administration > Polling and Thresholds > Apply Changes**. The Apply Changes page appears.

Step 2 Click **Yes** to apply the changes:

- If another user has already initiated applying changes, a message is displayed and changes are not applied again.
- If, since the last time changes were applied, polling parameter settings or threshold values have not changed and devices have not been suspended and then resumed, changes will not be applied.

Tip You cannot directly verify that changes have been applied. However, you can do so indirectly. For example, in response to an event, you change a threshold value and apply changes. After Operations Manager finishes applying changes, you can see whether Operations Manager clears the event.

For more information, see the following topics:

- Viewing Events Associated with an Alert, page 3-14
- Suspending/Resuming Devices, page 3-26
- Configuring Polling and Thresholds, page 19-1

CHAPTER 20

Administering Operations Manager

This chapter includes the following topics:

Performing Operations Manager Administration Tasks

From the Cisco Unified Operations Manager (Operations Manager) Administration tab, you can perform the tasks listed in Table 20-1.

Table 20-1 Operations Manager Administration Tasks

Tasks	Description
Polling and Thresholds See Configuring Polling and Thresholds, page 19-1.	From Polling and Thresholds, you can: • Change polling intervals, timeouts, and retries by device group • Enable and disable polling settings • Change thresholds, resetting the limits against which polled data will be compared • Customize threshold settings • Reprioritize groups for polling and thresholds • Apply polling and threshold changes to the system—After you apply changes, Operations Manager configures data collectors to: – Start using updated polling parameters and threshold values – Resume polling for devices or device elements that were previously suspended • Synchronize and view thresholds for Cisco Unified Communications Manager clusters.
SRST Poll Settings See Maintaining SRST Poll Settings, page 18-4.	From the SRST Poll Settings page, you can configure SRST monitoring.
Service Quality Settings See Configuring Service Quality Event Settings, page 20-7.	From the Service Quality Settings page, you can set a MOS threshold. **Note** For Operations Manager to process traps from a Service Monitor, you must add the Service Monitor to Operations Manager *and* you must use Service Monitor to configure Operations Manager as a trap receiver. To add Service Monitors to Operations Manager, see Adding a Service Monitor Link from Operations Manager, page 21-3.
System Status See Generating and Understanding the System Status Report, page 20-8.	From the System Status page, you can generate a System Status report.
Logging See Using Logging to Enable and Disable Debugging, page 20-11.	From the Logging page, you can change the type—and quantity—of messages written to log files, enabling and disabling debugging, for example.

Table 20-1 Operations Manager Administration Tasks (continued)

Tasks	Description
System Preferences See Setting System-Wide Parameters Using System Preferences, page 20-9.	From the System Preferences page, you can configure the following: • SNMP trap receiving—Change the port on which Operations Manager listens for SNMP traps • SNMP trap forwarding—(Optional) Set a host and port number as a recipient for pass-through traps • Default SMTP server—Change or enter a default server to use for e-mail notifications. • Purging schedule—Select the time when database purging occurs daily. • Common Services Servers—Enter remote servers running other CiscoWorks products, such as: – Resource Manager Essentials (RME) – Campus Manager – CiscoView
Add Users See Configuring Users (ACS and Non-ACS), page 20-20.	Launches a Common Services window that opens to the Local User Setup page.
Back Up and Restore See Backing Up and Restoring Operations Manager Data, page 20-25	Provides available options to back up and restore Operations Manager.

For more information, see the following additional topics:

- Configuring SNMP Trap Receiving and Forwarding, page 20-4
- Viewing Purge Scheduler Status, page 20-11

Scheduling Operations Manager Tasks

When Operations Manager is first installed, most tasks listed in Table 20-2 are scheduled by default to ensure that they do not run concurrently. You can configure the schedules for these tasks to meet the requirements of your site. However, you should still avoid running them concurrently.

Table 20-2 Scheduling Considerations

Scheduling Task	Default Schedule	Comments and Notes
Database purging	Run daily at midnight.	The amount of time it takes to purge the database depends on the size of the database.

Table 20-2 Scheduling Considerations (continued)

Scheduling Task	Default Schedule	Comments and Notes
Phone discovery	Run daily at midnight, 04:00, 08:00, 12:00, 16:00, and 20:00.	You should determine how long the last phone discovery took to complete by comparing at the start and end times for the last collection on the IP Phone Discovery Schedule page. See Working with IP Phone Discovery, page 16-38. Knowing how long phone discovery normally takes to complete will help you to schedule.
Inventory collection	Run weekly on Monday at 2:00 a.m.	By default, inventory collection starts 2 hours after database purging.

In addition to configuring schedules with Operations Manager, a system administrator can schedule database backups. You should be careful to coordinate the database backup schedule to avoid running concurrently with the tasks listed in Table 20-2.

For more information about schedules, see the following topics:

- Viewing Purge Scheduler Status, page 20-11
- Backing Up and Restoring Operations Manager Data, page 20-25

Configuring SNMP Trap Receiving and Forwarding

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

- Configure SNMP to send traps directly to Operations Manager
- Integrate SNMP trap receiving with an NMS or a trap daemon

To send traps directly to Operations Manager, perform the tasks in the Enabling Devices to Send Traps to Operations Manager, page 20-4. To integrate SNMP trap receiving with an NMS or a trap daemon, follow the instructions in Integrating SNMP Trap Receiving with Other Trap Daemons or NMSs, page 20-5.

Enabling Devices to Send Traps to Operations Manager

Note If your devices send SNMP traps to a Network Management System (NMS) or a trap daemon, see Integrating SNMP Trap Receiving with Other Trap Daemons or NMSs, page 20-5.

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

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

- Enabling Cisco IOS-Based Devices to Send Traps to Operations Manager, page 20-5
- Enabling Catalyst Devices to Send SNMP Traps to Operations Manager, page 20-5

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

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

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

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

For more information, refer to the appropriate command reference guide.

Step 1 Log in to Cisco.com.

Step 2 Select **Products & Services > Cisco IOS Software**.

Step 3 Select the Cisco IOS software release version used by your Cisco IOS-based devices.

Step 4 Select **Technical Documentation** and select the appropriate command reference guide.

Enabling Catalyst Devices to Send SNMP Traps to Operations Manager

For devices running Catalyst software, provide the following commands:

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

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

For more information, refer to the appropriate command reference guide.

Step 1 Log in to Cisco.com.

Step 2 Select **Products & Services > Cisco Switches**.

Step 3 Select the appropriate Cisco Catalyst series switch.

Step 4 Select **Technical Documentation** and select the appropriate command reference guide.

Integrating SNMP Trap Receiving with Other Trap Daemons or NMSs

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

- Add the host where Operations Manager is running to the list of trap destinations in your network devices. See Enabling Devices to Send Traps to Operations Manager, page 20-4. Specify port 162 as the destination trap port.

  If another NMS is already listening for traps on the standard UDP trap port (162), you must configure Operations Manager to use another port, such as port 9000. See Setting System-Wide Parameters Using System Preferences, page 20-9.
- If your network devices are already sending traps to another management application, configure that application to forward traps to Operations Manager.

Table 20-3 describes scenarios for SNMP trap receiving and lists the advantages of each.

Table 20-3 Configuration Scenarios for Trap Receiving

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

Ports and Protocols that Operations Manager Uses

Operations Manager uses the following protocols:

- SNMP
- ICMP
- TCP/IP
- SMTP
- RMI
- HTTP

Operations Manager uses the TCP and UDP ports described in Table 20-4.

Table 20-4 Operations Manager Incoming Ports

Port Number	Usage
162	Default port number used by Operations Manager for receiving traps
40000–41000	Used by Common Transport Mechanism for internal application messaging
42344	Used by Synthetic Testing web service
42350–42353	Used by messaging software
43441–43459	Used as database ports: • Operations Manager uses the following ports: – 43445—Used by Alert History database engine – 43446—Used by inventory service database engine – 43447—Used by event processing database engine – 43449—Used by IP Phone Information Facility database engine – 43459—Used by Service Monitor database engine

Table 20-4 Operations Manager Incoming Ports (continued)

Port Number	Usage
9002	Used by the Broker to listen to both the IP telephony server and the device fault server
9009	Default port number used by the IP telephony server for receiving traps from the device fault server

Configuring Service Quality Event Settings

Note Service Quality events are displayed on the Service Quality Alerts display. See Monitoring Service Quality Alerts, page 4-1.

Use this procedure to configure:

- The MOS level that triggers a CriticalServiceQualityIssue event.

  Service Monitor sends a trap when MOS falls below the threshold configured on Service Monitor. You can configure an event setting on Operations Manager that specifies a lower MOS threshold than the one configured on Service Monitor. When Operations Manager receives a trap with MOS less than or equal to the event setting, Operations Manager generates a CriticalServiceQualityIssue event. When Operations Manager receives a trap with MOS greater than the event setting, Operations Manager generates a ServiceQualityIssue event.

- The number of traps and the number of minutes after which to trigger a MultipleServiceQualityIssue event.

Note For Operations Manager to process traps from a Service Monitor, you must add the Service Monitor to Operations Manager *and* you must use Service Monitor to configure Operations Manager as a trap receiver. To add Service Monitors to Operations Manager, see Adding a Service Monitor Link from Operations Manager, page 21-3.

Step 1 Select **Administration >Service Quality Settings > Event Settings**. The Service Quality Event Settings page appears.

Step 2 Enter values in the following fields:

- **Mark the Service Quality Issue event critical when MOS drops below**—Enter the MOS score that should trigger a ServiceQualityIssue event to critical. The default is 3.5. (The range of MOS values is .1 to 4.9.)

  Note Ensure that you set this MOS score lower than the MOS threshold that is set in Service Monitor.

- **Generate a Multiple Service Quality Issues event when more than `[a]` Service Quality Issue events occur in `[b]` minutes**. Enter the number of:
  - [a]—Service Quality Issue events.
  - [b]—Minutes in which the specified number of Service Quality Issue events must occur for Operations Manager to generate a Multiple Service Quality Issues event.

Note By default, Operations Manager clears service quality events after 8 hours. After events are cleared, you can continue to view them in service quality event history for the next 31 days. See Getting Started with Service Quality History Reports, page 12-14.

Step 3 Click **Save**.

Related Topics

- Accessing Service Monitor Servers, page 21-2
- Adding a Service Monitor Link from Operations Manager, page 21-3

Generating and Understanding the System Status Report

To access a System Status report, select **Administration > System Status**. The System Status report opens.

The System Status report represents data immediately and may include data from the server startup or the last 24 hours. Conditions for Synthetic Test are currently displayed. Any failed tests will receive the following error:

```
The test cannot run because the CPU has been busy. The test will run when the CPU becomes
available.
```

To navigate through the System Status report, use the following:

- Go to field—Select a section of the report from the list. At the end of any section, you can click a Back to Top link.
- Summary—Select a section of the report by clicking any of the following links:
  - Failed Processes—If this message is displayed:

    ```
    (Unable to contact SNMP Service. Please check if Windows SNMP Service is installed
    and running.)
    ```

    see Using SNMP to Monitor Operations Manager, page 20-31 for more information.
  - Inventory
  - Data Purging
  - Diagnostics: Synthetic Tests

Note A failed synthetic test indicates that the test did not run, because at the time of execution the systems CPU utilization was greater than 80 percent.

  - Diagnostics: Phone Status Tests
  - Diagnostics: Node-to-Node Tests
  - Notifications
  - System Limits

Note You can also select a section of the report by clicking a View Details link in the summary.

The System Status report contains the following sections:

- **Failed Processes**—Names of processes that failed.
- **Inventory**—Displays the name, last execution time, status, and next scheduled time for the following types of data collection:
  - Discovery—Identifies new devices and adds them to the DCR. (Optional. Can be scheduled or run as needed.)
  - DCR Domain Status—Adds devices to the DCR from other CiscoWorks servers if Operations Manager is configured to synchronize devices and credentials (rather than working in standalone mode).
  - Device Selection—Adds devices to those that Operations Manager monitors either automatically—as they are added to the DCR— or when a user manually selects them from the DCR. Status: Automatic or Manual.
  - Device Inventory Collection—Probes devices that Operations Manager monitors to update device components and their status; does not discover devices.
  - Phone Inventory Collection—Discovers and collects information about all IP phones in the network by checking all switches and Cisco Unified Communications Managers monitored by Operations Manager; does not discover devices.
- **Data Purging**—Start time, end time, and status for most recent database purging task.
- **Diagnostics: Synthetic Tests**—Tests that failed: Test Name, Test Type, Source (IP address or DNS name), Target (IP address or DNS name), Failure Time, Reason.
- **Diagnostics: Phone Status Tests**—Tests that failed: Test Name, Source Router, Extension, MAC Address, IP Address Failure Time, Reason.
- **Diagnostics: Node-to-Node Tests**—Tests that failed: Test Name, Test Type, Endpoints, Failure Time, Reason.
- **Notifications**—Device Event Description, Event ID, Destination(s), Failure Time, Reason.
- **System Limits**—Current value, Limit value, and Limited By (License or System Resources) for the following parameters:
  - Devices—Current: Number of devices in Operations Manager monitored inventory. Limit: Number of devices allowed by license.
  - Phones—Current: Number of phones in Operations Manager monitored inventory. Limit: Number of phones allowed by license.
  - Cisco Unified Service Monitor— Licensed or not licensed.
  - Synthetic Tests.
  - Phone Reachability Tests.
  - Node-to-Node Tests.
  - Devices monitored for performance and capacity.
  - Devices monitored for SRST.

Setting System-Wide Parameters Using System Preferences

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

Step 2 Enter data described in the following table.

GUI Element	Description/Action
Trap Forwarding Parameters table	(Optional) Enter up to three recipients for pass-through traps: • Trap Server *n* (where *n* is a number from 1 to 3)—Enter an IP address or DNS name. • Port—Enter a port number on which the host can receive traps. **Note** By default, Operations Manager does not forward pass-through traps. For more information see: • Processed and Pass-Through Traps, page C-1. • Configuring SNMP Trap Receiving and Forwarding, page 20-4.
CiscoWorks Servers table	(Optional) For each CiscoWorks server (RME, Campus, and CiscoView), do the following: • Protocol—Select http (or https if SSL is enabled on the server). • Server—Enter the IP address or DNS name. • Port—Enter the port number used to start CiscoWorks on the server; the port number is usually 1741 when the protocol is http and 443 when the protocol https. **Note** Operations Manager can use this information to launch these CiscoWorks products.
SNMP Trap Community field	Enter a read community string.
Trap Receiving Port field	Enter a port to change the port on which Operations Manager listens for SNMP traps. The default is 162. For more information, see Configuring SNMP Trap Receiving and Forwarding, page 20-4. **Note** For a list of ports that are already in use, see Ports and Protocols that Operations Manager Uses, page 20-6.
SMTP Server field	Enter a fully qualified SMTP server name for Operations Manager to use when sending e-mail notifications. For more information, see Using Notifications, page 15-1. **Note** See Ensuring that E-Mail Notifications Are Not Blocked, page 20-11.
Purging Scheduler	Select the time of day to start purging the Alert History database: • Hour—From 0 to 23 • Minute—From 0 to 50 in 10-minute intervals The default is 00:00. Purging maintains 31 days of data in the database. **Note** Review the information in Scheduling Operations Manager Tasks, page 20-3 to ensure that daily purging does not conflict with the other scheduled jobs listed there.

Step 3 Click **Apply**.

Ensuring that E-Mail Notifications Are Not Blocked

If you have an antivirus application on the default SMTP server, verify that a port-blocking rule does not stop notification e-mail from being sent. Some antivirus applications use port-blocking to block mass-mailing worms. Delete the port-blocking rule if necessary.

For more information about notification e-mail, see Configuring Notifications, page 15-7.

Viewing Purge Scheduler Status

You can check the status of the Operations Manager data purge job from the Job Browser each day after the job runs.

Note You can also check the status of daily purging on the System Status report; see Generating and Understanding the System Status Report, page 20-8.

Step 1 Launch the CiscoWorks home page by clicking the **CiscoWorks** link in the upper right-hand corner of the Operations Manager home page.

Step 2 From the CiscoWorks home page, select **Common Services > Server > Admin > Job Browser**. The Job Browser page appears, displaying a table of scheduled jobs.

Step 3 Look for the Operations Manager:DataPurge job in the Type column and check for information in the Status column.

Note If you delete the Operations Manager:DataPurge job using the Job Browser, purging will not resume until you restart the daemon manager, reboot the server, or reconfigure the daily purging schedule.

Using Logging to Enable and Disable Debugging

Operations Manager writes application log files for all major functional modules. By default, Operations Manager writes only error and fatal messages to these log files. You cannot disable logging. However, you can:

- Collect more data when needed by increasing the logging level
- Return to the default logging level as the norm

Note The GSU module level logging is now available in Administration > Logging in Operations Manager 2.1 SP1. The log files are available under CSCOpx\log\gpf. For information on how to download this release, go to Cisco.com.

Step 1 Select **Administration > Logging**. The Logging Configuration page is displayed.

Note You cannot disable logging. Operations Manager will always write error and fatal messages to application log files.

Step 2 For each Operations Manager functional module, the Error check box is always selected; you cannot deselect it.

To set all modules to Error, the default logging level:

a. Click the **Default** button. A confirmation page is displayed.

b. Click **OK**.

To change the logging level for individual modules:

a. For each module that you want to change, select one (or deselect all) of the following logging levels:

- Warning—Log error messages and warning messages
- Info—Log error, warning, and informational messages
- Debug—Log error, warning, informational, and debug message

Note Deselecting all check boxes for a module returns it to Error, the default logging level.

b. Review your changes. To cancel your changes, click the **Cancel** button. Otherwise, click the **Apply** button. Clicking the **Apply** button starts immediately resetting the changed logging levels for the Operations Manager functional modules.

Tip You can adjust the number of log files that can exist in Operations Manager by changing the SM_BACKUP_FILE_LIMIT setting. The default is 1,000 files, and there is no parameter for existing file size.

You can start a new log file by using the roll_log utility, which you invoke using the **dmctl** command. Run the following commands:

```
C:\>cd PROGRA~1\CSCOpx\Unified Communications s\smarts\bin
C:\Program Files\CSCOpx\Unified Communications s\smarts\bin> dmctl -s <DM_NAME> exec
roll_log <filename>
```

In the command, C:\Program Files\CSCOpx refers to the path where Operations Manager is installed on the server. If you selected the default directory during installation, it can be entered as “C:\Program Files\CSCOpx” or C:\PROGRA~1\CSCOpx. If you did not select the default directory during installation, replace C:\Program Files with the exact path.

When this command is invoked, an informational message is written to the end of the current log file, the file is renamed, and a new log file is created. Best practice is to create a script that will test the log file size and make a call to dmctl roll_log on a daily basis.

For information about changing the logging level for the system application MIB, see Viewing the System Application MIB Log File, page 20-33.

Accessing and Deleting Log Files

Each Operations Manager module writes log files to its own folder within the <*NMSROOT*>\log\CUOM folder. Table 20-5 lists each Operations Manager module, the name of the folder where the log files are stored, the related log files, and whether the files are automatically saved or deleted (also referred to as rotated).

Note NMSROOT is the folder where Operations Manager is installed on the server. If you selected the default directory during installation, it can be entered as "C:\Program Files\CSCOpx" or C:\PROGRA~1\CSCOpx.

When a log file reaches a preset maximum size, the module backs up the file and starts writing to a new log file. The maximum size for a log file varies by module. The maximum number of backed up log files that a module keeps also varies. When the preset maximum number of backup files stored is reached, Operations Manager starts deleting the old files.

Tip If the log files are not rotated, you should run the log rotation utility, **logrot**, described in the CiscoWorks Common Services documentation on Cisco.com to manage these files.

Note Operations Manager does not automatically reset the DFMServer log file (DFM.log). To maintain good system performance, back up this file when it grows larger than 30 MB. See Maintaining the DFM Log File, page 20-31.

By default, Operations Manager writes error messages only to log files. You can change the logging level and thereby affect the amount of information stored in log files. To do so, see Using Logging to Enable and Disable Debugging, page 20-11.

Table 20-5 Operations Manager Log Files by Module

Function/Module	Folder in <*NMSROOT*>	Log Files	Files Rotated?[1]
Alert and Event History	\log\cuom\FH	FHUI.log FHCollector.log FHServer.log	Yes
Alerts and Events Display	\log\cuom\AAD	AAD.log	Yes
Application and Connectivity Poller	\log\cuom\VHM	Poller.log TISPollerLogger.log	Yes
Detailed Device View	\log\cuom\DDV	DDV.log	Yes
Device Management	\log\cuom\tis	DCRAdapter.log DeviceManagement.log TISServer.log	Yes
Event Processing Adapters	\log\cuom\epa	adapterServer.log dfmEvents.log vhmEvents.log	Yes

Table 20-5 Operations Manager Log Files by Module (continued)

Function/Module	Folder in <*NMSROOT*>	Log Files	Files Rotated?[1]
Event Promulgation Module (EPM)	\log\cuom\EPM	EPM.log	Yes
		EPMDroppedEvents.log	Yes
		EPMServer.log	No
Graphics Utility	\log\cuom\TGU	TGU.log	Yes
		TGU_DataProcessor.log	
Logging	ils	ItemLogService.log	Yes (after size reaches 500 KB).
		MultiProc-Logger.log	
IP Phone Information Facility	\log\ipiu	ipiuapp.log	Yes
IP Phone Information Facility Server	\log	pif.log	No
IP Phone Status	\log\cuom\PR	PhoneEvent.log	No
		PhoneReachability.log	Yes
IP Phone Status Display	\log\cuom\PAD	PAD.log	Yes
IP SLA Library	\log\cuom\IPSLA	STL.log	Yes
IPC Discovery	\log\cuom\discovery	discovery.log	Yes
		NGD1.log	
		NGD2.log	
IPT Health Report	log\cuom\ipthr	ipthr.log	Yes
Inventory Collection Schedule	\log\cuom\Rediscovery	Rediscovery.log	Yes

Table 20-5 Operations Manager Log Files by Module (continued)

Function/Module	Folder in <*NMSROOT*>	Log Files	Files Rotated?[1]
Inventory Collector	\log\cuom\vhm	abstractpoller.log connectivityProgress.log DataStore.log DataStoerGSUJms.log DFMCollector.log InchargeAccess.log InventoryCollector.log InventoryCollector_stdout.log InventoryCollector_stderr.log InvokePoller.log NodesinCluster_MediaServer_colccmpublin.cisco.com.log OnDemand_SnmpResponsivePoller.log OnDemand_VoiceClusterPoller.log Poller.log RisPortAXLSOAPWrapper.log RisPortAXLSOAPWrapperArguments.log SMARTSATTRIBUTECHANGE.log SMARTSEVENTNOTIFY.log Store.log TISPollerLogger.log VHMGSUPoller.log VHMIntegrator.log VHMIntegrator_stdout.log VHMIntegrator_sterr.log VICDFMADD.log VICHTTP.log VICTIS.log VoiceClusterPoller_VoiceCluster_VE-StandAloneCluster.log	Yes
Inventory Interactor	\log\cuom\vhm	CiscoCommunicationsManagerOrClusterGrouping.log Interactor.log	Yes
Inventory Service	\log\cuom\tis	DCRAdapter.log TISServer.log	Yes

Table 20-5 Operations Manager Log Files by Module (continued)

Function/Module	Folder in <*NMSROOT*>	Log Files	Files Rotated?[1]
Node-to-Node Tests Common Utilities	\log\cuom\IPSLA	DAL.log	Yes
		plib.log	
Node-to-Node Tests Data Poller	\log\cuom\IPSLA	WPUSS.log	Yes
		WPU_DataPoller.log	
		WPUDcache.log	
Node-to-Node Tests Device Management	\log\cuom\IPSLA	DMAudit.log	No
		WPUDM.log	Yes
Node-to-Node Tests Management	\log\cuom\IPSLA	SM.log	Yes
		SMAudit.log	No
Notification Services	\log\cuom\nots	nots.log	Yes
		notifications_audit.log	
		notifications_failures.log	
		notifications_success.log	
Personalized Reports	\log\cuom\ipthr	ipthr.log	Yes
PTM Adapter for Data Settings	\log\cuom\cfi	PollingThresholdAdapter.log	Yes
PTM Adapter for Voice Settings	\log\cuom\vhm	VHMPollingThresholdAdapter.log	Yes
Polling and Threshold Manager	\log\cuom\PTM	PTMClient.log	Yes
		PTMDB.log	
		PTMOGS.log	
		PTMPTA.log	
		PTMServer.log	
Purging Scheduler	\log\cuom\DPS	DPS.log	Yes
SRST Monitoring	\log\cuom\srst	srst_audit.log	No
		srst_import_errors.log	No
		srst_test_creation_results.log	No
		srst_import.log	Yes
		srst_ui.log	Yes
		srst_server.log	Yes
Self-Diagnostic Report	\log\cuom\sdr	sdr.log	Yes
Service Impact Reports Server	\log\cuom\sir	Disc_audit.log	No
		sir.log	Yes
Service Level View Server	\log\cuom\topo	Topology_Client.log	Yes
		Topology_Server.log	
Service Quality Alerts Display	\log\cuom\QOVAD	QOVAD.log	Yes
Service Quality Manager	\log\cuom\QoVM	QoVMServer.log	No
Synthetic Testing Server	\log	STServer.log	No

Table 20-5 Operations Manager Log Files by Module (continued)

Function/Module	Folder in <*NMSROOT*>	Log Files	Files Rotated?[1]
Synthetic Testing UI	\log	ct-ui.log	Yes
View Manager	\log\cuom\VGM	vgm.log	Yes
View Severity Manager	\log\cuom\vsm	AlertInfo.log GroupHandler.log UserInfo.log vsmServer.log	Yes

1. For information on how to rotate logs that may require rotation, see Cisco.com for the CiscoWorks Common Services product documentation for information on the logrot utility.

Note The Operations Manager application logging service also maintains log files under the <*NMSROOT*>\log\cuom folder. The configuration files for each module are located in <*NMSROOT*>\log\conf.

Security Considerations

These topics address some important Operations Manager security issues:

- File Ownership and Protection, page 20-17
- SSL, page 20-18
- SNMPv3, page 20-18
- Changing the Password for Operations Manager Databases, page 20-19

File Ownership and Protection

Security for Operations Manager files is based on the same standards used for CiscoWorks.

Caution Do not change the protection of any file or directory to be more restrictive. You may, if you wish, make the protections less restrictive.

All Operations Manager files are installed with owner CASUSER. Only CASUSER can create, delete, or edit the files installed in *NMSROOT*. *NMSROOT* is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as "C:\Program Files\CSCOpx" or C:\PROGRA~1\CSCOpx.

Note File protections are not enforced on FAT partitions.

SSL

Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. It relies upon certificates, public keys, and private keys. You can enable or disable SSL depending on the need to use secure access.

Operations Manager supports SSL between clients and the server.

Enabling SSL Between the Browser and the Server

When you start Operations Manager, the login page always opens in secure mode, providing secure access between the client browser and the Operations Manager server. In secure mode, SSL is used to encrypt the transmission channel between the browser and the server. To use secure mode throughout Operations Manager, enable SSL in Common Services.

Note If you enable SSL on a system with Operations Manager and Service Monitor, SSL is enabled for both applications.

Step 1 Select **CiscoWorks > Common Services > Server > Security > Browser-Server Security Mode Setup**. The Browser-Server Security Mode Setup dialog box appears.

Step 2 Select the Enable check box.

Step 3 Click **Apply**.

Step 4 Log out from Operations Manager, and close all browser sessions.

Step 5 Restart the daemon manager from the command line by entering these commands:

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

Step 6 Restart the browser and use the secure URL to restart Operations Manager:

```
https://<servername>:443
```

Note If you enter http://<*servername*>:1741 in your browser and SSL is enabled, you will be directed to the secure URL.

SNMPv3

Operations Manager supports SNMPv3 (authentication and access control but no data encryption) between server and devices to eliminate leakage of confidential information. This provides packet-level security, integrity protection, and replay protection, but does not encrypt the packets.

Changing the Password for Operations Manager Databases

Before You Begin

The procedure in this topic enables you to change the password for the following Operations Manager databases:

- itemEPM—Event promulgation
- itemFH—Alert History
- itemInv—Inventory
- itemIpiu—IP phone information
- qovr—Cisco Unified Service Monitor

Step 1 At the command prompt on the Operations Manager server, stop the daemon manager by entering the following command:

```
net stop crmdmgmt
```

Step 2 Change directory to *NMSROOT*\conf\itemDb\bin. For example:

```
cd C:\PROGRA~1\CSCOpx\conf\itemDb\bin
```

Note NMSROOT is the folder where Operations Manager is installed on the server. If you selected the default directory during installation, it can be entered as "C:\Program Files\CSCOpx" or C:\PROGRA~1\CSCOpx.

Step 3 Enter ChangeItemDbPasswd.pl, providing a new password as input. For example:

```
ChangeItemDbPasswd.pl newpassword
```

Step 4 Restart the daemon manager by entering the following command:

```
net start crmdmgmt
```

Device Support

When support for new devices becomes available for Operations Manager, Incremental Device Updates (IDUs) will be announced on the planner page for Operations Manager on Cisco.com. Visit the planner page for announcements, downloads, and installation instructions for IDUs as they become available.

When a new IDU becomes available, you can download it from Cisco.com.

For device support information, see *Supported Device Table for* Cisco Unified Operations Manager on Cisco.com at http://www.cisco.com/en/US/products/ps6535/products_device_support_tables_list.html.

Performing System Administration Tasks

You can use CiscoWorks to perform many system administration tasks, including the following:

Launching the CiscoWorks Home Page

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

Configuring Users (ACS and Non-ACS)

The CiscoWorks server provides the mechanism for authenticating and authorizing users for CiscoWorks applications. What users can see and do is determined by their user role. System Administrators can configure user roles from the CiscoWorks home page. Under Common Services, select **Server > Security > Single-Server Management > Local User Setup**. From here you can add, edit, or delete users.

The CiscoWorks server provides two different mechanisms or *modes* for authenticating users for CiscoWorks applications:

- CiscoWorks Local Mode—By default, the CiscoWorks server uses CiscoWorks Local mode, or *non-ACS mode*. In CiscoWorks Local mode, CiscoWorks assigns roles, along with privileges associated with those roles, as described in the Common Services Permission Report. (You can generate a Permission Report from the Common Services home page by selecting **Server > Reports > Permission Report** and clicking **Help**.) For more information, refer to Configuring Users Using CiscoWorks Local Mode, page 20-21.
- CiscoSecure Access Control Server (ACS) Mode—ACS specifies the privileges associated with roles; however, ACS also allows you to perform device-based filtering, so that users only see devices they are authorized to see. Using ACS, which is called *ACS mode*, is supported when ACS is installed on your network and Operations Manager is registered with ACS. For more information, refer to Configuring Users Using ACS Mode, page 20-21.

If Common Services is using ACS mode, Operations Manager must also use ACS mode; otherwise, Operations Manager users will not have any permissions. However, if another instance of Operations Manager is already integrated with ACS, the new Operations Manager will also be integrated with ACS.

Configuring Users Using CiscoWorks Local Mode

Use this procedure to add a user and specify a user role using CiscoWorks Local Mode.

Step 1 Select **Administration > Add Users**. The Common Services Local User Setup window opens.

Step 2 Click the Help button on the Local User Setup window for information on the configuration steps.

Use the CiscoWorks Permission Report to understand how each user role relates to tasks in Operations Manager. From the Common Services home page, select **Server > Reports > Permission Report > Generate Report** and scroll down until you find Cisco Unified Operations Manager.

Configuring Users Using ACS Mode

To use this mode for Operations Manager, Cisco Secure ACS must be installed on your network, and Operations Manager must be registered with ACS.

Step 1 Verify which mode the your server is using. From the Common Services home page, select **Server > Security > AAA Mode Setup** and check which Type radio button is selected: ACS or Non-ACS.

Step 2 Verify whether Operations Manager is registered with ACS (if ACS is selected) by checking the ACS server.

Step 3 To edit ACS roles:

- Refer to the ACS online help (on the ACS server) for information on editing roles.
- Refer to the Common Services online help for information on the implications of ACS on the DCR (specifically, role dependencies).

Note If you edit Operations Manager roles using ACS, your changes will be propagated to all other instances of Operations Manager that are using Common Services servers that are registered with the same ACS server.

Using Operations Manager in ACS Mode

Before performing any tasks that are mentioned here, you must ensure that you have successfully completed configuring Cisco Secure ACS with the Operations Manager server. If you have installed Operations Manager after configuring the CiscoWorks Login Module to ACS mode, then Operations Manager users are not granted any permissions. However, the Operations Manager application is registered to Cisco Secure ACS.

Note The System Identity Setup user that is defined in the CiscoWorks server must be added to the Cisco Secure ACS, and this user must have Network Administrator privileges.

CiscoWorks login modules allow you to add new users using a source of authentication other than the native CiscoWorks server mechanism (that is, the CiscoWorks Local login module). You can use the Cisco Secure ACS services for this purpose.

By default, the CiscoWorks server authentication scheme has five roles in ACS mode. They are listed here from least privileged to most privileged:

Help Desk	User with this role has the privilege to access network status information from the persisted data. User does not have the privilege to contact any device or schedule a job that will reach the network. Example: Launch Service Level View.
Approver	User with this role has the privilege to approve all Operations Manager tasks. User can also perform all the Help Desk tasks. Example: Launch Alerts and Events.
Network Operator	User with this role has the privilege to perform all tasks that involve collecting data from the network. User does not have write access on the network. User can also perform all the Approver tasks. Example: Add a synthetic test.
Network Administrator	User with this role has the privilege to change the network. User can also perform Network Operator tasks. Example: Set the default view for Service Level View.
System Administrator	User with this role has the privilege to perform all CiscoWorks system administration tasks. See the Permission Report from CiscoWorks home page (**Common Services > Server > Reports > Permission Report**). Example: Configure LDAP.

Cisco Secure ACS allows you to edit the privileges for these roles. You can also create custom roles and privileges that help you customize Common Services client applications to best suit your business workflow and needs.

To edit the default CiscoWorks privileges, see Cisco Secure ACS online help. (On Cisco Secure ACS, click **Online Documentation > Shared Profile Components > Command Authorization Sets**.)

Editing CiscoWorks Roles and Privileges in Cisco Secure ACS

If another instance of Operations Manager is registered with the same Cisco Secure ACS, your instance of Operations Manager will inherit those role settings. Furthermore, any changes you make to Operations Manager roles will be propagated to other instances of Operations Manager through Cisco Secure ACS. If you reinstall Operations Manager, your Cisco Secure ACS settings will automatically be applied upon Operations Manager restart.

Step 1 Select **Shared Profile Components >** Operations Manager and click on the Operations Manager roles that you want to edit.

Step 2 Select or deselect any of the Operations Manager tasks that suit your business workflow and needs.

Step 3 Click **Submit**.

Device-Based Filtering

You can configure ACS to restrict access to all Operations Manager displays. You can also configure ACS to restrict access to devices and applications. Device-based and application-based filtering affects:

- Devices—To be able to view information for a device, configure the device, and configure diagnostic tests that involve the device, you must have access to it.
- Phones—To be able to view information for a phone, you must have access to either the switch connected to the phone or to the Cisco Unified Communications Manager to which the phone is registered.

Note ACS does not perform any filtering on VLANs.

Note Device-based filtering is not performed at the Cisco Unified Communications Manager cluster level. All users can see cluster-level alerts and Alert History.

Device-based filtering can only be performed on the following Operations Manager displays:

- **Monitoring Dashboards**—All displays.
- **Diagnostics**—All displays.
- **Device Management**—All displays.

Note If any user starts the inventory collection process, all devices managed by Operations Manager are probed (not just those for which the user has access).

- **Notifications > Notification Criteria**.

  Note If you update device access in ACS, Operations Manager does not update running notifications.

- **Reports**:
  - **Alert and Event History**—All displays.
  - **Service Quality History**—All displays.
- **Administration > Polling and Thresholds**

  Note Only the Polling Parameters Summary and the Thresholds Parameters Summary pages are filtered.

Most Operations Manager tasks are device-centric. The devices listed for you while performing the Operations Manager tasks are based on your role and associated privileges, defined in Cisco Secure ACS.

Note Refer to the Common Services online help for important information on how ACS custom roles affect the DCR and device-based filtering.

Changing ACS Mode to CiscoWorks Local Mode

If your system is configured to use ACS, but you want to change it to CiscoWorks Local mode you must perform the following procedure.

Step 1 Stop the CiscoWorks daemon manager by entering the following command:

```
net stop CRMDmgtd
```

Step 2 Go to Operations Manager install Directory (the default is C:\PROGRA~1\CSCOpx)

Step 3 Cd to bin.

Step 4 Run the following command:

```
perl ResetLoginModule.pl
```

You should see the following message:

```
Changing mode from ACS to CMF.... Please restart the Daemon Manager for changes to take
effect.
```

Step 5 Restart the CiscoWorks daemon manager by entering the following command:

```
net start CRMDmgtd
```

The system should be in non-ACS mode.

Creating Self-Signed Security Certificates Yearly

When you install Operations Manager, Operations Manager creates a self-signed security certificate on the server. Users on some client systems must install the certificate; see Responding to Security Alerts, page 1-24. Self-signed security certificates expire one year from the date of creation.

Create a new self-signed security certificate yearly before the certificate expires. You can also do so after the certificate expires; however, users might not be able to access Operations Manager until you complete this task.

Step 1 Select **Common Services > Server > Admin > Security Management > Create Self Signed Certificates**. The Create Certificates page appears.

Step 2 Enter the values for the fields described in the following table.

Field	Description	Usage Notes
Country Name	Name of your country	Use two-character country code.
State or Province	Name of your state or province	Use two-character state or province code or complete name of state or province.
Locality	Name of your city or town	Use two-character city or town code or complete name of city or town.
Organization Name	Name of your organization	Use complete name or abbreviation for your organization.
Organization Unit Name	Name of department in your organization	Use complete name or abbreviation for your department.

Field	Description	Usage Notes
Host Name	Name of server on which Operations Manager is installed	Use the DNS name of the server. **Note** Use the proper domain name, which should already be displayed in the Host Name field.
Email Address	Your e-mail address	—

Step 3 Click **Submit**. (Alternatively, click **Restore to Default** to clear all fields and re-enter information.)

Backing Up and Restoring Operations Manager Data

There are two options for backup and restore of Operations Manager data:

- Backing Up and Restoring Detailed Device View Configurations Using Operations Manager Utilities, page 20-25
- Backing Up and Restoring Using CiscoWorks, page 20-26

If your Operations Manager 2.0.2 database is over 10 GB it may need to be unloaded and reloaded before an installation/upgrade. For details on the steps to perform, see Handling Sybase Database Issues Before Installation for Operations Manager 2.0.2, page 20-27.

Database backup and restore is supported only on the same version of Operations Manager (which includes the database and user configuration data of all Operations Manager modules).

For additional information on installation or upgrade backup and restore, see the *Installation Guide for Cisco Unified Operations Manager*.

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

The backup utility backs up the states of all components of all types of monitored or partially monitored devices (except for those mentioned below) in the Detailed Device View (DDV). It does not cover suspended devices. Database backup and restore is supported only on the same version of Operations Manager (which includes the database and user configuration data of all Operations Manager modules).

Note Operations Manager does not restore DDV configurations on voice services, system processor, hard disk, virtual memory, and RAM components for Cisco Unified Communications Manager machines. Operations Manager uses RTMT polling, not device MIB polling, to create the above components and therefore does not display the above data in the Operations Manager DDV in 2.1.

Caution Ensure that the daemon processes for this system are up and running to allow for data backup.

The restore utility restores the managed states of non suspended devices in the Detailed Device View.

Step 1 To run the backup utility, open a DOS prompt and enter:

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

Where *default* saves the managed states of *all* monitored and partially monitored devices to the inventoryBackup file. No user input is needed while the script is running.

Caution Backup on a network drive is not supported. Even though the CLI is functional, its use is not recommended due network connectivity issues. As a result, the mapped network drive on the server will not be seen from the user interface for drive selection.

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

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

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

Caution After an Operations Manager 2.1 upgrade, you can run **inventoryRestore** script only after rediscovering all devices from Operations Manager Device Management interface.

Step 2 To run the restore utility, open a DOS prompt and enter:

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

Where *default* restores the data saved in the inventoryBackup.xml file. No user input is needed while the script is running.

If you want to input your own filename enter:

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

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

Backing Up and Restoring Using CiscoWorks

This topic explains how to access the backup applications, such as Back Up Data Now and Schedule Backup. This topic also explains how to locate the online help procedures for restoring data.

When Service Monitor and Operations Manager are installed together, you must use this Common Services database backup procedure. These procedures back up the databases located on the server, including those for Service Monitor, Common Services, and Operations Manager.

Caution Backup on a network drive is not supported. Even though the CLI is functional, its use is not recommended due network connectivity issues. As a result, the mapped network drive on the server will not be seen from the user interface for drive selection.

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

Step 2 Under Common Services, select **Server > Admin > Backup**. The Backup Job page appears.

Step 3 Click the Help button and follow the instructions for backing up and restoring data.

Database files are stored using the backup directory structure described in Table 20-6.

- Format—*/generation_number/suite/directory/filename*
- Example—/1/itemFh/database/itemFh.db

Table 20-6 Operations Manager Backup Directory Structure

Option	Description	Usage Notes
generationNumber	Backup number	For example, 1, 2, and 3, with 3 being the latest database backup.
suite	Application, function, or module	When you perform a backup, data for all suites is backed up. The CiscoWorks server suite is cmf. The Operations Manager application suites are: • dfm—Data collection and analysis for devices in IP infrastructure • itemEpm—Event promulgation • itemFh—Alert history • itemInv—Device inventory • itemIPIU—Phone information • qovr—Service quality • vhm—Data collection and analysis for voice-enabled devices • wpu—Node-to-Node tests.
directory	What is being stored	Each application or suite listed. Directories include database and any suite applications.
filename	File that has been backed up	Files include database (.db), log (.log), version (DbVersion.txt), manifest (.txt), tar (.tar), and data files (datafiles.txt).

Handling Sybase Database Issues Before Installation for Operations Manager 2.0.2

If your Operations Manager 2.0.2 database is over 10 GB it may need to be unloaded and reloaded before the installation/upgrade. There is a Sybase database failure problem where the database can become corrupt, fail to validate, or grows too large (over 10 GB causing the backup procedure to take a long time). If your database shows any of the issues described, use the following procedure to unload and reload the database. You must know your database password to perform this procedure. If you do not know your database password, contact your customer support representative.

Step 1 Stop the daemon manager:

%net stop crmdmgtd

Tip Ensure you wait until all database processes have stopped running. You can check for running dbeng9 or dbsrv9 processes using the process explorer tool.

Step 2 Unload the database:

%dbunload -c "uid=<username>;pwd=<pwd>;dbf=<db name>" <Directory to unload data >

For example:

```
%dbunload -c "uid=itemFhUser;pwd=<pwd>;dbf=itemFh.db" c:\unload
```

Step 3 Remove and save the itemFh.db to another directory.

Step 4 Initialize the new database:

%dbinit -p 4096 itemFh.db

Step 5 Reload the new database:

%dbisqlc -c "uid=<default username;pwd=<default passwd>;dbf=<db name>" reload.sql

For example:

```
%dbisqlc -c "uid=dba;pwd=sql;dbf=itemFh.db" reload.sql
```

Step 6 Delete the *.DAT and *.SQL files newly created, and restart daemon manager.

```
%rm *.dat *.sql
net start crmdmgtd
```

Starting and Stopping Operations Manager Processes

Note You cannot stop or unregister a process if any process that depends on it is running. You must first stop or unregister all dependent processes, and then stop or unregister the process.

Step 1 Log in to Operations Manager as a system administrator.

Step 2 From the Operations Manager home page, click **CiscoWorks** in the upper right-hand corner of the window. The CiscoWorks home page opens.the CiscoWorks home page.

Step 3 Under Common Services, select **Server > Admin > Processes**. The Process Management page appears.

Note If a process is not listed, it has not yet been started.

Step 4 Do one of the following:

- Select check boxes next to processes that are running and click **Stop**.
- Select check boxes next to processes that are stopped and click **Start**.

Table 20-7 provides a complete list of Operations Manager-related CiscoWorks processes.

Table 20-7 Operations Manager-Related CiscoWorks Processes

Name	Description	Dependency
AdapterServer	Event adapter takes events from backend servers.	None
DataPurge	Database and data file purging.	jrm

Table 20-7 Operations Manager-Related CiscoWorks Processes (continued)

Name	Description	Dependency
DfmBroker	DFM Broker maintains a registry about VHM and DFM domain managers. A domain manager registers the following information with the broker when its initialization is complete: • Application name of the domain manager • Hostname where the domain manager is running • TCP port at which the HTTP server is listening When a client needs to connect to the domain manager, it first connects to the broker to determine the hostname and TCP port where that server's HTTP service is listening. It then disconnects from the broker and establishes a connection to the domain manager.	None
DfmServer	Infrastructure device domain manager, a program that provides backend services for Operations Manager. Services include SNMP data retrieval and event analysis. The DfmServer log is *NMSROOT*/Unified Communications s/smarts/logs/DFM.log. For more information, see Maintaining the DFM Log File, page 20-31.	DfmBroker
EPMDbEngine	Event Promulgation Module (EPM) database engine—Repository for the EPM module.	None
EPMDbMonitor	EPM database monitor.	EPMDbEngine
EPMServer	Sends events to notification services.	EPMDbEngine
FHDbEngine	Alert History database engine—Repository for alerts and events.	None
FHDbMonitor	Alert History database monitor.	FHDbEngine
FHPurgeTask	Alert History purge task.	None
FHServer	Alert History server.	FHDbMonitor, FHDbEngine, EPMDbEngine, EPMServer
GPF	Performance and capacity monitoring data collection.	ITMOGSServer, INVDbEngine
GpfPurgeTask	Purges performance polling records.	None
INVDbEngine	Device inventory database engine.	None
INVDbMonitor	Device inventory database monitor.	INVDbEngine
InventoryCollector	Phone inventory collector.	EssMonitor
IPCDiscovery	Physical device discovery.	None.
IPIUDataServer	Provides information about IP phones.	ESS
IPIUDbEngine	Phone inventory database engine.	None
IPIUDbMonitor	Phone inventory database monitor.	IPIUDbEngine
IPSLAPurgeTask	Purges node-to-node test records.	None
IPSLAServer	Node-to-node test server.	INVDbMonitor, InventoryCollector

Table 20-7 Operations Manager-Related CiscoWorks Processes (continued)

Name	Description	Dependency
ITMCTMStartup	Internal communication process.	None
ITMDiagServer	Diagnostics server.	INVDbEngine, ESS
ITMOGSServer	Operations Manager Object Grouping Service server evaluates group membership.	CmfDbEngine, ESS, DCRServer
IVR	Internal process.	None
NOTSServer	Notification server monitors alerts and sends notifications based on subscriptions.	EPMDbEngine, EPMServer, INVDbEngine, ITMOGSServer
PIFServer	Performs phone discovery, CDP neighbor discovery, monitoring, and phone reachability.	PIFDbEngine, ESS
PTMServer	Polling and thresholds server.	ITMOGSServer
QoVMServer	Service Monitor server.	ESS
QOVR	Service Quality alerts process.	QOVRDbMonitor
QOVRDbEngine	Service Monitor database engine.	None
QOVRDbMonitor	Service Monitor database monitor.	QOVRDbEngine
QOVRMultiProcLogger	Service Monitor logging.	None
SDRPurgeTask	Purges Self-Diagnostic Reports.	None
SIRServer	Voice model and rule-based engine for generating Service Impact Reports.	EPMDbEngine, ESS.
SRSTServer	Configures and runs SRST tests.	PIFServer, PMServer, ESS, TISServer
STServer	Periodically runs synthetic tests against Cisco Unified Communications Managers and provides real-time status updates to Operations Manager.	INVDbEngine, ESS
TISServer	Inventory server.	INVDbEngine, EssMonitor
TopoServer	Service level view server.	SIRServer, ITMOGSServer
VHMIntegrator	Integrates voice and infrastructure data.	ESS
VHMServer	Maintains voice data.	DfmBroker
VsmServer	Maintains and evaluates views.	ITMOGSServer

Maintaining Log Files

There are several ways to maintain your log files including:

- Maintaining the DFM Log File, page 20-31
- Maintaining Log Files in CSCOPX/log, page 20-31

Maintaining the DFM Log File

If the DFM.log file grows larger than 30 MB, there is a risk of Operations Manager performance problems. To prevent such problems, you should back up the log file and start a new one.

Step 1 Stop the CiscoWorks daemon manager by entering the following command:

```
net stop CRMDmgtd
```

Step 2 Rename the DFM.log file or copy it to a new location and delete it from the Operations Manager server. You can find the DFM.log file in the *NMSROOT*/Unified Communications s/smarts/logs/ directory.

Note NMSROOT is the folder where Operations Manager is installed on the server. If you selected the default directory during installation, it can be entered as "C:\Program Files\CSCOpx" or C:\PROGRA~1\CSCOpx.

Step 3 Allow 15 minutes to elapse from the time you completed step 1, then restart the CiscoWorks daemon manager by entering the following command:

```
net start CRMDmgtd
```

A new DFM.log file will be created.

Maintaining Log Files in CSCOPX/log

Most process logs (generally files under CSCOPx/log/*.log) are not auto-rotated. Some files may have autorotation. Table 20-5 on page 20-13, "Operations Manager Log Files by Module" includes information on which log files are rotated.

For details on how to maintain log files that are not automatically rotated, see "Configuring Log Files Rotation" in the *User Guide for CiscoWorks Common Services*.

Using SNMP to Monitor Operations Manager

Operations Manager supports the host resources and system application MIBs. This support enables you to monitor Operations Manager using a third-party SNMP management tool, so that you can:

- Consistently monitor multiple platforms—One platform on which Operations Manager resides and one or more on which applications in the IP Telephony Environment Monitor (ITEM) suite reside.
- Access complete hardware and operating system information using the host resources MIB.
- Assess application health using the system application MIB, which provides the following information:
  - Applications that Operations Manager installed.
  - Processes associated with applications and current process status.
  - Processes that ran previously and application exit state.

For MIB implementation details and sample MIB walk, see Appendix I, "Operations Manager Support for SNMP MIBs."

Note You cannot uninstall MIB support; however, you can stop Windows SNMP service and set the startup type to either Manual or Disabled. See Enabling and Disabling Windows SNMP Service, page 20-33.

Configuring Your System for SNMP Queries

To enable SNMP queries, SNMP service must be installed and enabled.

Step 1 Verify that SNMP service is installed and enabled on the server where Operations Manager is installed. See Determining the Status of Windows SNMP Service, page 20-32.

Step 2 If you determined that SNMP service was not installed, install Windows SNMP Service; see Installing and Uninstalling Windows SNMP Service, page 20-32.

Determining the Status of Windows SNMP Service

Windows SNMP service is a Windows component that you can add or remove when you want to. To enable SNMP queries against the MIBs that Operations Manager supports, SNMP service must be installed and enabled. You can verify the status of Windows SNMP service as follows.

Step 1 Open the Windows administrative tool Services window.

Step 2 Verify the following:

- SNMP Service is displayed on the Windows administrative tool Services window; if so, Windows SNMP service is installed.

  Note To install Windows SNMP service, see Installing and Uninstalling Windows SNMP Service, page 20-32.

- SNMP Service startup type is Automatic or Manual; if so, Windows SNMP service is enabled.

  Note To enable Windows SNMP service, see Enabling and Disabling Windows SNMP Service, page 20-33.

Installing and Uninstalling Windows SNMP Service

Windows online help provides instructions for adding and removing Windows components, such as Windows SNMP service. To locate the instructions, try selecting the Index tab in Windows online help and entering a keyword or phrase, such as *installing SNMP service*.

To uninstall Windows SNMP service, follow instructions in Windows help for removing Windows components.

Note When you uninstall Windows SNMP service from the server where Operations Manager is installed, you also remove support for the host resources and system application MIBs. If you want to install support again, see Configuring Your System for SNMP Queries, page 20-32.

Enabling and Disabling Windows SNMP Service

You can enable or disable Windows SNMP service using the Windows administrative tool Services. For instructions to open the Services window, see Windows online help.

Step 1 Locate SNMP Service in the Services window. The status and startup type are displayed.

Note If SNMP Service is not displayed, Windows SNMP service is not installed; see Installing and Uninstalling Windows SNMP Service, page 20-32.

Step 2 Right-click SNMP Service and select Properties. The SNMP Service Properties window opens:

- To disable SNMP service, set Startup Type to Disable and click **OK**.
- To enable SNMP service, set Startup Type to Automatic or Manual and click **OK**.

Note To start SNMP service after you enable it, right-click SNMP Service and select Start.

Configuring Security for SNMP Queries

To improve security, the SNMP set operation is not allowed on any Object ID (OID). You should also edit the credentials for SNMP service to not use a default or well-known community string.

Note You do not need to restart SNMP service to edit credentials for it.

You can edit SNMP service credentials using the Windows administrative tool Services.

Step 1 Locate SNMP Service in the Services window.

Step 2 Right-click SNMP Service and select Properties. The SNMP Service Properties window opens.

Step 3 Select the Security tab.

Step 4 Edit the accepted community names and click **OK**.

Viewing the System Application MIB Log File

The system application MIB log file, SysAppl.log, is located on the server where Operations Manager is installed in *NMSROOT*/log.

Note NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it can be entered as "C:\Program Files\CSCOpx" or C:\PROGRA~1\CSCOpx.

Changing the Hostname on the Operations Manager Server

To change the hostname on the Operations Manager server, you must update several files, reboot the server, and regenerate the self-signed security certificate. Afterward, if you have a licensed copy of Service Monitor, you must update the configuration for it.

Note You will reboot the server twice during this procedure.

Step 1 Change the hostname on the server as follows:

a. Change the hostname at **My Computer > Properties > Computer Name > Change**.

b. Prevent the daemon manager service from restarting after reboot. From Control Panel, or from Start, open Services and change the startup mode to Manual for this service:

- CW2000 Daemon Manager

c. Reboot the server.

Step 2 Change the hostname in the md.properties file (*NMSROOT*\lib\classpath\md.properties).

Note NMSROOT is the directory where you installed Operations Manager. If you selected the default, it can be entered as "C:\Program Files\CSCOpx" or C:\PROGRA~1\CSCOpx.

Step 3 Change the hostname in the following registry entries:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet.
- HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Resource Manager.

Note Look for all instances of the old hostname under these registry entries, and replace them with the new hostname.

Step 4 Change the hostname in these files:

- regdaemon.xml (*NMSROOT*\MDC\etc\regdaemon.xml):
  - Note the old hostname. You will need it to complete Step 5.
  - Enter the new hostname in uppercase.
- web.xml (*NMSROOT*\MDC\tomcat\webapps\classic\WEB-INF\web.xml).

Step 5 Create a file, *NMSROOT*\conf\cmic\changehostname.info, containing the old hostname and new hostname in uppercase in the following format:

```
OLDHOSTNAME:NEWHOSTNAME
```

Note Hostnames in this file are case-sensitive; they must be entered in uppercase, and the new hostname must exactly match the hostname entered in regdaemon.xml.

Step 6 Delete the gatekeeper.ior file from this directory:

NMSROOT\www\classpath

Step 7 Change all occurrences of the old hostname in the following files:

- *NMSROOT*\Unified Communications s\vhmsmarts\local\conf\runcmd_env.sh
- *NMSROOT*\conf\dfm\Broker.info

Step 8 If you do not know the password for the cmf database, reset the password as follows:

a. Open a Command Prompt and go to NMSROOT\bin.

b. Enter the following command:

```
perl dbpasswd.pl dsn=cmf npwd=newpassword
```

where newpassword is the new password.

Note Remember this password. You will need it to complete Step 9.

Step 9 To ensure that devices added before you changed the hostname are properly classified in Device Center, enter the following command:

```
dbisqlc -c "uid=cmfDBA;pwd=dbpassword;eng=cmfEng;dsn=cmf;dbf=NMSROOT\databases\cmf\cmf.db"
-q update PIDM_app_device_map SET app_hostname=`NewhostName' where
app_hostname=`OldhostName'
```

where:

- dbpassword is the Common Services database password.
- NMSROOT is the directory where you installed Operations Manager.
- NewhostName is the new hostname.
- OldhostName is the old hostname.

Step 10 From the Control Panel, or from Start, open Services and change the startup mode to Automatic for this service:

- CW2000 Daemon Manager

Step 11 Reboot the server.

Step 12 Replace the old hostname with the new hostname in the self-signed security certificate and regenerate it by selecting **Common Services > Server > Security > Certificate Setup**.

For more information, click Help.

Step 13 If you have a license for Service Monitor, reconfigure it:

a. Open the Service Monitor home page. (See Launching a Service Monitor, page 21-6.)

b. Click Help and follow the instructions in the topic *Reconfiguring Service Monitor after a Hostname Change*.

Note Service Monitor online help provides detailed instructions for accomplishing the following tasks:

- Change the IP address or hostname in each of the following configuration files:
  - The default configuration file.
  - The specific configuration file for each Cisco 1040 managed by the Service Monitor.
- Copy the updated configuration files from the Service Monitor server to the TFTP server.
- Reset the Cisco 1040s.
- If Service Monitor is configured to send traps to Operations Manager:
  - If Operations Manager is installed on the same server as Service Monitor, set up Service Monitor to send traps to the new hostname or IP address.
  - If Operations Manager is installed on another server, on Operations Manager, delete the Service Monitor and add it again.

Changing the IP Address on the Operations Manager Server

Step 1 Stop the CiscoWorks daemon manager by entering the following command:

```
net stop CRMDmgtd
```

Step 2 Delete the gatekeeper.ior file from this directory:

NMSROOT\www\classpath

Note NMSROOT is the folder where Operations Manager is installed on the server. If you selected the default directory during installation, it can be entered as "C:\Program Files\CSCOpx" or C:\PROGRA~1\CSCOpx.

Step 3 Change the IP address of the Operations Manager server.

Step 4 Allow 15 minutes to elapse from the time you completed step 1, then restart the CiscoWorks daemon manager by entering the following command:

```
net start CRMDmgtd
```

PART 8

Cisco Unified Communications Management Suite

CHAPTER 21

Setting Up Cisco Unified Communications Management Application Links

This section includes the following topics:

Accessing Unified Communications Management Suite Applications from Operations Manager

You can add links to Operations Manager to launch other Cisco Unified Communications Management Suite applications using the UC Management Suite tab. To access Cisco Unified Service Monitor (Service Monitor) diagnostic reports as well as some Cisco Unified Service Statistics Manager (Service Statistics Manager) functions, you must register the application's servers using the UC Management Suite tab. You can run these Cisco Unified Communications Management Suite applications in standalone mode or as coresident applications (having applications run at the same time) on the same server. For guidelines on system requirements, see the *Supported and Interoperable Devices and Software Guide for* Cisco Unified Operations Manager on Cisco.com.

For details on coresidency and hardware and software guidelines, see the *Deployment Best Practices Guide* on Cisco.com.

From the Cisco UC Management Suite tab, you can perform the tasks listed in Table 21-1.

Table 21-1 Operations Manager Cisco Unified Communications Management Suite Tasks

Tasks	Description
Accessing Service Monitor Servers	From Operations Manager, add, edit, or delete a remote Service Monitor, launch the default home page for Service Monitor from inside the Operations Manager interface, and configure Service Monitor.
Accessing Provisioning Manager Servers	From Operations Manager, add, edit, or delete a remote Provisioning Manager and launch the default home page for Provisioning Manager from inside the Operations Manager interface.
Accessing Service Statistics Manager Servers	From Operations Manager, add, edit, or delete a remote Service Statistics Manager and launch the default home page for Service Statistics Manager from inside the Operations Manager interface.

Accessing Service Monitor Servers

The Cisco Unified Communications Management Suite enables you to integrate a Service Monitor with Operations Manager.

Be sure to read Important Notes About Service Monitor, page 21-2 to understand the prerequisites to setting up Service Monitor.

You can perform the following actions on Service Monitor from Operations Manager:

- Adding a Service Monitor Link from Operations Manager, page 21-3
- Editing a Service Monitor from Operations Manager, page 21-4
- Deleting a Service Monitor Link from Operations Manager, page 21-5
- Configuring a Service Monitor, page 21-5
- Launching a Service Monitor, page 21-6

Caution Review the Important Notes About Service Monitor, page 21-2 before you begin adding Service Monitors.

Important Notes About Service Monitor

For Operations Manager to process traps from Service Monitor, you must remember the following:

- Service Monitor is a separately licensed product that is installed when you install Operations Manager; see your Cisco representative to obtain a license.
- You can license Service Monitor on the same server as Operations Manager. You can also obtain standalone versions of Service Monitor to install and license on other servers.
- For Operations Manager to process traps from a Service Monitor, you must add the Service Monitor to Operations Manager *and* you must use Service Monitor to configure Operations Manager as a trap receiver.
- You must configure Service Monitor to send traps to Operations Manager. (See the *User Guide for Cisco Unified Service Monitor*.)

- You must configure Operations Manager to process traps from particular Service Monitors. See Configuring a Service Monitor, page 21-5. Operations Manager discards any traps received from a Service Monitor that has not been added to Operations Manager.

Service Monitor sends MOS violation traps to Operations Manager when MOS falls below a threshold configured on Service Monitor. In response to these traps, Operations Manager generates a warning alert. To enable Operations Manager to generate a critical alert when MOS falls to a more critical level than that defined by Service Monitor, configure a lower MOS threshold on Operations Manager. See Configuring Service Quality Event Settings, page 20-7.

Table 21-2 describes the elements in the Service Monitor window.

Table 21-2 UC Management Suite—Service Monitor Window Elements

Window Element	Action/Description
Check box column	Select to perform a function on a Service Monitor.
IP Address column	Server where Service Monitor is installed. **Note** Operations Manager processes traps from *only* those Service Monitors listed here.
Protocol column	HTTP or HTTPS.
Port column	Port by which Service Monitor is accessed. Cannot be left blank.
Status column	Selection for whether to use this Service Monitor as a cross-launch server. Limit of one cross-launch server active at a time.
Remarks column	User-entered description.
Add button	Click to add a Service Monitor. See Adding a Service Monitor Link from Operations Manager, page 21-3.
Edit button	Click to edit Service Monitor values. See Editing a Service Monitor from Operations Manager, page 21-4
Launch button	Click to open the Service Monitor home page. See Launching a Service Monitor, page 21-6.
Configure button	Click to configure a Service Monitor trap receiver parameters. See Configuring a Service Monitor, page 21-5 and Service Monitor online help for details.
Delete button	Click to delete Service Monitors that you have selected. See Deleting a Service Monitor Link from Operations Manager, page 21-5.

Adding a Service Monitor Link from Operations Manager

Use this procedure to add a link to a local or remotely installed Service Monitor server from Operations Manager.

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

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

Step 3 Enter data in the following fields (see Table 21-2 on page 21-3 for details):

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

Step 4 Click **Add**.

- If you selected cross-launch capabilities for this server a confirmation window displays; click **Yes** or **No**.
- If you selected **Not for cross-launch server**, the Service Monitor page appears displaying the information for the newly added Service Monitor.

Editing a Service Monitor from Operations Manager

Use this procedure to edit a local or remotely installed Service Monitor server from Operations Manager.

Step 1 Select **UC Management Suite > Service Monitor** to add or edit a Service Monitor. The Service Monitor page appears.

Step 2 Click the **Edit** button. The Edit Service Monitor page appears.

Step 3 Enter data in the following fields (see Table 21-2 on page 21-3 for details):

- Protocol
- Port
- Status
- Remarks—Optional

Step 4 Click **Apply**.

- If you selected cross-launch capabilities for this server a confirmation window displays; click **Yes** or **No**.
- If you selected **Not for cross-launch server**, the Service Monitor page appears displaying the updated information.

Deleting a Service Monitor Link from Operations Manager

Use this procedure to delete the link for a locally installed or remotely installed Service Monitor server from Operations Manager.

Note After you delete a Service Monitor link from Operations Manager, Operations Manager discards any traps received from the deleted Service Monitor. Service Monitor continues to function using the configurations made within the Service Monitor product. Since Service Monitor continues to run in the background on Operations Manager, it will continue to use system resources until you suspend Service Monitor's clusters and sensors from **CiscoWorks > Cisco Unified Service Monitor > Configuration > Monitored Phones**.

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

Step 2 Select check boxes for service monitors that you want to delete.

Step 3 Click **Delete**. The Service Monitor page reappears with the updated list of records.

Step 4 To ensure valuable system resources are not used by Service Monitor in the background, select **CiscoWorks > Cisco Unified Service Monitor > Configuration > Monitored Phones**, then select the check box for the cluster or sensor that you want to suspend and click **Suspend**.

Configuring a Service Monitor

Use this procedure to configure which traps Operations Manager will monitor for the selected Service Monitor server.

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

Step 2 Click **Configure**. The Service Monitor Configuration > Trap Receivers page appears.

Note You might be asked to log in.

Step 3 Enter data into the following fields on the Trap Receiver Parameters page:

- SNMP Community String
- Trap Receiver 1 and Port
- Trap Receiver 2 and Port
- Trap Receiver 2 and Port
- Trap Receiver 2 and Port

Step 4 Click **OK**. A confirmation window appears asking you to confirm the setup; click **Yes** or **No**.

For information on using Service Monitor, click **Help** on the Service Monitor home page.

Launching a Service Monitor

Use this procedure to launch the Service Monitor home page for the selected Service Monitor server.

Note You can access the locally installed Service Monitor (if configured) by clicking the Click to Launch Service Monitor button on the Monitoring Dashboard.

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

Step 2 Select a Service Monitor and click **Configure**. The Service Monitor home page appears.

Note You might be asked to log in.

Step 3 Click **Help** on the Service Monitor home page for more information on using Service Monitor.

Accessing Provisioning Manager Servers

You can perform the following actions on Provisioning Manager from Operations Manager:

- Adding a Provisioning Manager Cross-Launch Link from Operations Manager, page 21-6
- Editing Provisioning Manager Servers, page 21-7
- Deleting Provisioning Manager Servers, page 21-8
- Accessing Provisioning Manager Servers, page 21-6

Adding a Provisioning Manager Cross-Launch Link from Operations Manager

Use this procedure to add a cross-launch link to a local or remotely installed Provisioning Manager server from Operations Manager.

Step 1 Select **UC Management Suite > Provisioning Manager** to add a Provisioning Manager. The Provisioning Manager page appears.

Step 2 Click the **Add** button. The Add Provisioning Manager page appears.

Step 3 Enter data in the following fields (see Table 21-3 on page 21-6 for details):

Table 21-3 UC Management Suite—Provisioning Manager Window Elements

Window Element	Action/Description
IP Address column	Server where Provisioning Manager is installed.
Protocol column	HTTP or HTTPS.
Port column	Port by which Provisioning Manager is accessed. Cannot be left blank.

Table 21-3 UC Management Suite—Provisioning Manager Window Elements

Window Element	Action/Description
Status column	Selection for whether to use this Provisioning Manager as a cross-launch server. Limit of one cross-launch server active at a time.
Remarks column	User-entered description. Optional.
Add button	Click to add a Provisioning Manager. See Adding a Provisioning Manager Cross-Launch Link from Operations Manager, page 21-6.
Edit button	Click to edit Provisioning Manager values. See Editing Provisioning Manager Servers, page 21-7
Launch button	Click to open the Provisioning Manager home page. See Accessing Provisioning Manager Servers, page 21-6.
Delete button	Click to delete Provisioning Managers that you have selected. See Deleting Provisioning Manager Servers, page 21-8.

Step 4 Click **Add**.

- If you selected cross-launch capabilities for this server a confirmation window displays; click **Yes** or **No**.
- If you selected **Not for cross-launch server**, the Provisioning Manager page appears displaying the information for the newly added Provisioning Manager.

Editing Provisioning Manager Servers

Use this procedure to edit a local or remotely installed Provisioning Manager server from Operations Manager.

Step 1 Select **UC Management Suite > Provisioning Manager** to add or edit a Provisioning Manager. The Provisioning Manager page appears.

Step 2 Click the **Edit** button. The Edit Provisioning Manager page appears.

Step 3 Enter data in the following fields (see Table 21-3 on page 21-6 for details):

- Protocol
- Port
- Status
- Remarks—Optional

Step 4 Click **Apply**.

- If you selected cross-launch capabilities for this server a confirmation window displays; click **Yes** or **No**.
- If you selected **Not for cross-launch server**, the Provisioning Manager page appears displaying the updated information.

Deleting Provisioning Manager Servers

Use this procedure to delete a locally installed or remotely installed Provisioning Manager server from Operations Manager.

Step 1 Select **UC Management Suite > Provisioning Manager**. The Provisioning Manager page appears.

Step 2 Select check boxes for Provisioning Managers that you want to delete.

Step 3 Click **Delete**. The Provisioning Manager page reappears with the updated list of records.

Launching Provisioning Manager

Use this procedure to launch the Provisioning Manager home page for the selected Provisioning Manager server.

Step 1 Select **UC Management Suite > Provisioning Manager**. The Provisioning Manager page appears.

Step 2 Select a Provisioning Manager and click **Configure**. The Provisioning Manager home page appears.

Note You might be asked to log in.

Step 3 Click **Help** on the Provisioning Manager home page for more information on using Provisioning Manager.

Accessing Service Statistics Manager Servers

You can perform the following actions on Service Statistics Manager from Operations Manager:

- Adding a Service Statistics Manager Link from Operations Manager, page 21-8
- Editing Service Statistics Manager Servers, page 21-9
- Deleting Service Statistics Manager Servers, page 21-10
- Launching Service Statistics Manager Servers, page 21-10

Adding a Service Statistics Manager Link from Operations Manager

Use this procedure to add a link to a local or remotely installed Service Statistics Manager server from Operations Manager.

Step 1 Select **UC Management Suite > Service Statistics Manager** to add or edit a Service Statistics Manager. The Service Statistics Manager page appears.

Step 2 Click the **Add** button. The Add Service Statistics Manager page appears.

Step 3 Enter data in the following fields (see Table 21-4 on page 21-9 for details):

Table 21-4 UC Management Suite—Service Statistics Manager Window Elements

Window Element	Action/Description
IP Address column	Server where Service Statistics Manager is installed.
Protocol column	HTTP or HTTPS.
Port column	Port by which Service Statistics Manager is accessed. Cannot be left blank.
Status column	Selection for whether to use this Service Statistics Manager as a cross-launch server. Limit of one cross-launch server active at a time.
Remarks column	User-entered description. Optional.
Add button	Click to add a Service Statistics Manager. See Adding a Service Statistics Manager Link from Operations Manager, page 21-8.
Edit button	Click to edit Service Statistics Manager values. See Editing Service Statistics Manager Servers, page 21-9
Launch button	Click to open the Service Statistics Manager home page. See Launching Service Statistics Manager Servers, page 21-10.
Delete button	Click to delete Service Statistics Managers that you have selected. See Deleting Service Statistics Manager Servers, page 21-10.

Step 4 Click **Add**.

- If you selected cross-launch capabilities for this server a confirmation window displays; click **Yes** or **No**.
- If you selected **Not for cross-launch server**,, the Service Statistics Manager page appears displaying the information for the newly added Service Statistics Manager.

Editing Service Statistics Manager Servers

Use this procedure to edit a local or remotely installed Service Statistics Manager server link from Operations Manager.

Step 1 Select **UC Management Suite > Service Statistics Manager** to add or edit a Service Statistics Manager. The Service Statistics Manager page appears.

Step 2 Click the **Edit** button. The Edit Service Statistics Manager page appears.

Step 3 Enter data in the following fields (see Table 21-4 on page 21-9 for details):

- Protocol
- Port
- Status
- Remarks—Optional

Step 4 Click **Apply**.

- If you selected cross-launch capabilities for this server a confirmation window displays; click **Yes** or **No**.

- If you selected **Not for cross-launch server**, the Service Statistics Manager page appears displaying the updated information.

Deleting Service Statistics Manager Servers

Use this procedure to delete a locally installed or remotely installed Service Statistics Manager server link from Operations Manager.

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

Step 2 Select check boxes for Service Statistics Managers that you want to delete.

Step 3 Click **Delete**. The Service Statistics Manager page reappears with the updated list of records.

Launching Service Statistics Manager Servers

Use this procedure to launch the Service Statistics Manager home page for the selected Service Statistics Manager.

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

Step 2 Select a Service Statistics Manager and click **Configure**. The Service Statistics Manager home page appears.

Note You might be asked to log in.

Step 3 Click **Help** on the Service Statistics Manager home page for more information on using Service Statistics Manager.

PART 9

Operations Manager Reference

APPENDIX A

Performance Counters Shown in the Detailed Device View

This topic provides definitions for the performance counters shown in the Detailed Device View. This topic also lists the type of polling settings that control whether or not Operations Manager collects the performance counters. For information about enabling and disabling polling, see Editing Polling Parameters, page 19-13. For details on all performance counter Unified Communications s and MIB Unified Communications s that Operations Manager uses, see MIBs Polled and Perfmon Counter Objects Used, page B-1. The following performance counters are displayed in the Detailed Device View:

BRI Channel Status for CCM GW

The set of performance counters in Table A-1 is displayed for each BRI port in the MGCP gateway.

Table A-1 BRI Channel Status for Cisco Unified Communications Manager-Controlled MGCP Gateway

Counters	Description
DS1 name	DS1 name
Channel Status [1]	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved
Channel Status [2]	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved
Channel Status [3]	D channel 0=out-of-service, 1=in-service

BRI Channel Status for IOS GW

The set of performance counters in Table A-2 are displayed for each BRI port in the Cisco IOS gateway registered.

Table A-2 BRI Channel Status for Cisco IOS Gateway

Counters	Description
DS1 Name	DS1 name
B Channel Status [*n*] **Note** Displayed for each of 2 channels with *n* from 0 through 1.	200=idle, 300=unknown, 302=voice, 303=unrestrictedDigital, 304=unrestrictedDigital56, 305=restrictedDigital, 306=audio31, 307=audio7, 308=video, 309=packetSwitched

Cisco Unified Communications Manager

Table A-3 lists performance counters for the Cisco Unified Communications Manager.

Note Polling for these counters is enabled by default and is controlled by Voice Health Settings.

CCM GW Port Usage

Table A-3 Cisco Unified Communications Manager

Counter	Description
Cisco Unified Communications Manager Heartbeat	An incremental count that indicates that Cisco Unified Communications Manager is up and running. If the count does not increase, it indicates that Cisco Unified Communications Manager is down.
Number of Failed Attempts to Allocate Hardware Resources	Number of times this Cisco Unified Communications Manager attempted to allocate a hardware conference resource from those that are registered to this Cisco Unified Communications Manager, when none were available.
Number of Failed Attempts to Allocate Software Resources	Number of times this Cisco Unified Communications Manager attempted to allocate a software conference resource from those that are registered to this Cisco Unified Communications Manager, when none were available.
Number of Times No Transcoder Resources Were Available for Allocation	Number of times that Cisco Unified Communications Manager attempted to allocate a transcoder resource from one of the transcoder devices that is registered to this Cisco Unified Communications Manager, when none were available.
Number of Times No Unicast MOH Resources Were Available for Allocation	Number of times that the Media Resource Manager attempted to allocate a Music On Hold (MOH) resource when none were available.
Number of Times No Multicast MOH Resources were Available for Allocation	Number of times no multicast MOH resources were available for allocation.
Number of Failed Attempts to Allocate an MTP Resource	Number of times that Cisco Unified Communications Manager attempted but failed to allocate an MTP resource from one of the MTP devices that is registered with this Cisco Unified Communications Manager.
Total Number of Calls, via the Location, that Failed Due to Lack of Bandwidth	Total number of calls via the location that failed due to lack of bandwidth.

Table A-3 Cisco Unified Communications Manager (continued)

Counter	Description
Number of Signals Present in the Low-Priority Queue	Number of signals present in the low-priority queue.
Number of Signals Present in the Normal-Priority Queue	Number of signals present in the normal-priority queue.
Number of Signals Present in the High-Priority Queue	Number of signals present in the high-priority queue.
Number of MOH Connections Lost	Number of times that a connection was lost, since the Cisco IP Voice Media Streaming application service started.
Number of MTP Instances Started	Total number of MTP instances that have been started since the Cisco IP Voice Media Streaming application service started.
Number of Simplex Streams Connected to an MTP Device	Total number of simplex streams that have connected to the MOH server since the Cisco IP Voice Media Streaming application service started.

Table A-4 lists performance counters for a Cisco Unified Communications Manager-controlled MGCP gateway.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-4 Cisco Unified Communications Manager-Controlled MGCP Gateway Port Usage

Counters	Description
Number of Active Calls	Number of call legs active.
Total T1 PRI Channels	Number of T1 PRI channels configured on the MGCP gateway.
Active T1 PRI Channels	Number of T1 PRI channels active with voice calls.
Active Nonvoice T1 PRI Channels	Number of T1 PRI channels active with nonvoice calls.
Total E1 PRI Channels	Number of E1 PRI channels configured on the MGCP gateway.
Active E1 PRI Channels	Number of E1 PRI channels active with voice calls.
Active Nonvoice E1 PRI Channels	Number of E1 PRI channels active with nonvoice calls.
Total T1 CAS Channels	Number of T1 CAS channels configured on the MGCP gateway.
Active T1 CAS Channels	Number of T1 CAS channels active with voice calls.
Active Nonvoice T1 CAS Channels	Number of T1 CAS channels active with nonvoice calls.
Total E1 CAS Channels	Number of E1 CAS channels configured on the MGCP gateway.
Active E1 CAS Channels	Number of E1 CAS channels active with voice calls.
Active Nonvoice E1 CAS Channels	Number of E1 CAS channels active with nonvoice calls.
Total FXS Ports	Number of FXS ports configured on the MGCP gateway.
Active FXS Ports	Number of FXS ports active.
Total FXO Ports	Number of FXO ports configured on the MGCP gateway.
Active FXO Ports	Number of FXO ports active.
Total BRI Channels	Number of BRI channels configured on the MGCP gateway.

Table A-4 Cisco Unified Communications Manager-Controlled MGCP Gateway Port Usage (continued)

Counters	Description
Active BRI Channels	Number of BRI channels active with voice calls.
Active Nonvoice BRI Channels	Number of BRI channels active with nonvoice calls.
Total EM Ports	Number of ear and mouth (E&M) ports configured on the Cisco IOS gateway.
Active EM Ports	Number of E&M ports active.
Percentage Active T1 CAS	T1 CAS voice utilization for the MGCP gateway.
Percentage Active E1 CAS	E1 CAS voice utilization for the MGCP gateway.
Percentage Active FXS	FXS port utilization for the MGCP gateway.
Percentage Active FXO	FXO port utilization for the MGCP gateway.
Percentage Active T1 PRI	T1 PRI voice utilization for the MGCP gateway.
Percentage Active E1 PRI	E1 PRI voice utilization for the MGCP gateway.
Percentage Active EM	E&M voice utilization for the MGCP gateway.

CCM Port and CPU Usage

Table A-5 contains port usage and CPU usage for the Cisco Unified Communications Manager.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-5 Port and CPU Usage on the Cisco Unified Communications Manager System

Counters	Description
CPU Usage [0]	Measured CPU utilization for CPU 1.
Number of Active Calls	Number of calls active. This counter shows calls that are fully established and in use. Calls in setup mode or in teardown mode are not reported by this count.
Total PRI Channels	Number of T1/E1 PRI channels that were defined on Cisco Unified Communications Manager.
Active PRI Channels	Number of T1/E1 PRI channels that were active.
Total T1 E1 Channels	Number of defined T1/E1 CAS channels on Cisco Unified Communications Manager.
Active T1 E1 Channels	Number of T1/E1 CAS channels that were active.
Total FXS	Number of defined FXS ports on Cisco Unified Communications Manager platform.
Active FXS	Number of FXS ports that were active.
Total FXO	Number of defined FXO ports on Cisco Unified Communications Manager platform.
Active FXO	Number of FXO ports that were active.
CPU Usage [2]	(Optional) Measured CPU utilization for CPU 2.
CPU Usage [3]	(Optional) Measured CPU utilization for CPU 3.

Table A-5 Port and CPU Usage on the Cisco Unified Communications Manager System (continued)

Counters	Description
CPU Usage [4]	(Optional) Measured CPU utilization for CPU 4.
CPU Usage [5]	(Optional) Measured CPU utilization for CPU 5.
Total CPU Usage	Measured CPU utilization for all CPUs.
Total T1 PRI Channels	Number of T1 PRI channels that were defined on Cisco Unified Communications Manager.
Active T1 PRI Channels	Number of T1 PRI channels that were active.
Total E1 PRI Channels	Number of E1 PRI channels that were defined on Cisco Unified Communications Manager.
Active E1 PRI Channels	Number of E1 PRI channels that were active.
Total BRI Channels	Number of BRI channels that were defined on Cisco Unified Communications Manager.
Active BRI Channels	Number of BRI channels that were active.
Calls Attempted	Number of calls attempted on this Cisco Unified Communications Manager.
Calls Completed	Number of calls completed on this Cisco Unified Communications Manager.
Calls in Progress	Number of calls in progress on this Cisco Unified Communications Manager.
Percentage Active T1 CAS	T1 CAS utilization for Cisco Unified Communications Manager.
Percentage Active FXS	FXS port utilization for Cisco Unified Communications Manager.
Percentage Active FXO	FXO port utilization for Cisco Unified Communications Manager.
Percentage Active T1 PRI	T1 PRI utilization for Cisco Unified Communications Manager.
Percentage Active E1 PRI	E1 PRI utilization for Cisco Unified Communications Manager.
Percentage Active BRI	BRI utilization for Cisco Unified Communications Manager.

IOS GW Port Usage

Table A-6 lists performance counters for a Cisco IOS gateway.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings. For more information, see Notes on Record Type 102, page J-12.

Table A-6 Port Usage on a Cisco IOS Gateway

Counters	Description
Number of Active Calls	Number of call legs active.
Total T1 PRI Channels	Number of T1 PRI channels configured on the Cisco IOS gateway.
Active T1 PRI Channels	Number of T1 PRI channels active with voice calls.
Active Nonvoice T1 PRI Channels	Number of T1 PRI channels active with nonvoice calls.
Total E1 PRI Channels	Number of E1 PRI channels configured on the Cisco IOS gateway.

Table A-6 Port Usage on a Cisco IOS Gateway (continued)

Counters	Description
Active E1 PRI Channels	Number of E1 PRI channels active with voice calls.
Active Nonvoice E1 PRI Channels	Number of E1 PRI channels active with nonvoice calls.
Total T1 CAS Channels	Number of T1 CAS channels configured on the Cisco IOS gateway.
Active T1 CAS Channels	Number of T1 CAS channels active with voice calls.
Active Nonvoice T1 CAS Channels	Number of T1 CAS channels active with nonvoice calls.
Total E1 CAS Channels	Number of E1 CAS channels configured on the Cisco IOS gateway.
Active E1 CAS Channels	Number of E1 CAS channels active with voice calls.
Active Nonvoice E1 CAS Channels	Number of E1 CAS channels active with nonvoice calls.
Total FXS Ports	Number of FXS ports configured on the Cisco IOS gateway.
Active FXS Ports	Number of FXS ports active.
Total FXO Ports	Number of FXO ports configured on the Cisco IOS gateway.
Active FXO Ports	Number of FXO ports active.
Total BRI Channels	Number of BRI channels configured on the Cisco IOS gateway.
Active BRI Channels	Number of BRI channels active with voice calls.
Active Nonvoice BRI Channels	Number of BRI channels active with nonvoice calls.
Total EM Ports	Number of ear and mouth (E&M) ports configured on the Cisco IOS gateway.
Active EM Ports	Number of E&M ports active.
Percentage Active T1 CAS	T1 CAS voice utilization for the Cisco IOS gateway.
Percentage Active E1 CAS	E1 CAS voice utilization for the Cisco IOS gateway.
Percentage Active FXS	FXS port utilization for the Cisco IOS gateway.
Percentage Active FXO	FXO port utilization for the Cisco IOS gateway.
Percentage Active T1 PRI	T1 PRI voice utilization for the Cisco IOS gateway.
Percentage Active E1 PRI	E1 PRI voice utilization for the Cisco IOS gateway.
Percentage Active EM	E&M voice utilization for the Cisco IOS gateway.

CCM – H323 GW Usage

Table A-7 lists performance counters for a H323 gateway registered with Cisco Unified Communications Manager.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-7 Cisco Unified Communications Manager—H323 Gateway Usage

Counters	Description
H323 Gateway Name	Name of the H323 gateway added to Cisco Unified Communications Manager.
Calls Active	Number of calls active through the H323 gateway added to the Cisco Unified Communications Manager.
Calls Attempted	Number of calls attempted through the H323 gateway added to the Cisco Unified Communications Manager.
Calls Completed	Number of calls completed through the H323 gateway added to the Cisco Unified Communications Manager.
Calls in Progress	Number of calls in progress through the H323 gateway added to the Cisco Unified Communications Manager.

CCM Usage

Table A-8 lists performance counters for a Cisco Unified Communications Manager.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-8 Cisco Unified Communications Manager Usage

Counters	Description
MOH Total Multicast Resources	Total MOH multicast resources configured on Cisco Unified Communications Manager.
MOH Multicast Resources Active	Active MOH multicast resources on Cisco Unified Communications Manager.
MOH Multicast Resources Available	Available MOH multicast resources on Cisco Unified Communications Manager.
Percentage MOH Multicast Resources Active	MOH multicast resource utilization on Cisco Unified Communications Manager.
MOH Total Unicast Resources	Total MOH unicast resources configured on Cisco Unified Communications Manager.
MOH Unicast Resources Active	Active MOH unicast resources on Cisco Unified Communications Manager.
MOH Unicast Resources Available	Available MOH unicast resources on Cisco Unified Communications Manager.
Percentage MOH Unicast Resources Active	MOH unicast resource utilization on Cisco Unified Communications Manager.
MTP Total Resources	Total MTP resources configured on Cisco Unified Communications Manager.
MTP Resources Active	Active MTP resources on Cisco Unified Communications Manager.
MTP Resources Available	Available MTP resources on Cisco Unified Communications Manager.
Percentage MTP Resources Active	MTP resource utilization on Cisco Unified Communications Manager.

Table A-8 Cisco Unified Communications Manager Usage (continued)

Counters	Description
Transcoder Total Resources	Total number of transcoder resources on the Cisco Unified Communications Manager.
Transcoder Resources Active	Number of transcoder resources active on the Cisco Unified Communications Manager.
Transcoder Resources Available	Number of transcoder resources available on the Cisco Unified Communications Manager.
Percentage Transcoder Resources Active	Percentage of total transcoder resources on the Cisco Unified Communications Manager active.
Software Conference Total Resources	Total number of software conference resources on the Cisco Unified Communications Manager.
Software Conference Resources Active	Number of software conference resources on the Cisco Unified Communications Manager active.
Percentage Software Conference Resources Active	Percentage of total software conference resources on the Cisco Unified Communications Manager active.
Software Conference Active	Number of active software conferences on the Cisco Unified Communications Manager.
Software Conference Completed	Number of completed software conferences on the Cisco Unified Communications Manager.
Hardware Conference Total Resources	Total number of hardware conference resources on the Cisco Unified Communications Manager.
Hardware Conference Resources Active	Number of hardware conference resources on the Cisco Unified Communications Manager active.
Hardware Conference Resources Available	Number of hardware conference resources on the Cisco Unified Communications Manager available.
Hardware Conference Completed	Number of completed hardware conferences on the Cisco Unified Communications Manager.
Registered Analog Access Gateways	Number of analog access devices registered with the Cisco Unified Communications Manager.
Registered MGCP Gateways	Number of MGCP gateways registered with the Cisco Unified Communications Manager.
Registered Hardware Phones	Number of hardware phones registered with the Cisco Unified Communications Manager.
Registered Other Station Devices	Number of other station devices registered with the Cisco Unified Communications Manager.

CCM – Analog Access GW Usage

Table A-9 lists counters for analog access gateways registered to Cisco Unified Communications Manager.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-9 Cisco Unified Communications Manager—Analog Access Gateway Usage

Counters	Description
Ports Active	Number of ports active on the analog access device registered to Cisco Unified Communications Manager.

CCM – CTI Manager Usage

Table A-10 lists performance counters for CTI Manager usage in Cisco Unified Communications Manager.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings with the exception of Number of Active Links with the Cisco Unified Communications Manager, which is controlled by Voice Health Settings.

Table A-10 Cisco Unified CallManager CTI Manager Usage

Counters	Description
Total CTI Ports	Total number of registered CTI ports on Cisco Unified CallManager.
Number of Active Links with the Cisco Unified CallManager Cisco Unified CallManager Link Active **Note** Cisco Unified CallManager Link Active is displayed only when data for Number of Active Links with the Cisco Unified CallManager is not available.	Number of CTI links active on Cisco Unified CallManager.
CTI Connection Active	Number of CTI connections active on Cisco Unified CallManager.
Devices Open	Number of CTI devices open.
Lines Open	Number of CTI lines open.

CCM – Location Usage

Table A-11 lists counters for location usage in Cisco Unified Communications Manager.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-11 Cisco Unified Communications Manager—Location Usage

Counters	Description
Location Name	Name of the location defined in Cisco Unified Communications Manager.
Bandwidth Maximum	Total bandwidth configured for the location.
Bandwidth Available	Available bandwidth for the location.
Bandwidth utilization	Utilization of the bandwidth for the location.
Calls in Progress	Number of calls in progress.

CCM – Media Streaming Application Usage

Table A-12 lists performance counters for media streaming application usage in Cisco Unified Communications Manager.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-12 Cisco Unified Communications Manager—Media Streaming Application Usage

Counters	Description
Conferences Total	Total conferences on Cisco Unified Communications Manager.
Conferences Active	Active conferences on Cisco Unified Communications Manager.
Percentage Conferences Active	Percentage active conferences on Cisco Unified Communications Manager.
Conference Bridge Streams Total	Total conference streams on Cisco Unified Communications Manager.
Conference Bridge Streams Available	Available conference streams on Cisco Unified Communications Manager.
Conference Bridge Streams Active	Active conference streams on Cisco Unified Communications Manager.
Percentage Conference Bridge Streams Active	Percentage active conference streams on Cisco Unified Communications Manager.
MOH Audio Sources Active	Number of active MOH audio sources on Cisco Unified Communications Manager.
MOH Streams Total	Total number of MOH streams configured on Cisco Unified Communications Manager.
MOH Streams Available	Number of available MOH streams on Cisco Unified Communications Manager.
MOH Streams Active	Number of active MOH streams on Cisco Unified Communications Manager.
Percentage MOH Streams Active	Percentage active MOH streams on Cisco Unified Communications Manager.
MTP Connections Total	Total number of MTP connections on Cisco Unified Communications Manager.
MTP Instances Active	Number of active MTP instances on Cisco Unified Communications Manager.
MTP Streams Total	Total number of MTP streams on Cisco Unified Communications Manager.
MTP Streams Available	Number of available MTP streams on Cisco Unified Communications Manager.
MTP Streams Actives	Number of active MTP streams on Cisco Unified Communications Manager.
Percentage MTP Streams Active	Percentage active MTP streams on Cisco Unified Communications Manager.

CCM – MOH Device Usage

Table A-13 lists counters for a music on hold (MOH) device registered with Cisco Unified Communications Manager.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-13 Cisco Unified Communications Manager—MOH Device Usage

Counters	Description
MOH Device Name	Name of the MOH device.
MOH Highest Active Resources	Highest active resources on the MOH device registered to Cisco Unified Communications Manager.
MOH Total Multicast Resources	Total number of multicast resources on the MOH device.
MOH Multicast Resources Available	Available multicast resources on the MOH device.
MOH Multicast Resources Active	Active multicast resources on the MOH device.
Percentage Multicast Resources Active	Percentage active multicast resources on the MOH device.
MOH Total Unicast Resources	Total number of unicast resources on the MOH device.
MOH Unicast Resources Available	Available unicast resources on the MOH device.
MOH Unicast Resources Active	Active unicast resources on the MOH device.
Percentage Unicast Resources Active	Percentage active unicast resources on the MOH device.

CCM – MTP Usage

Table A-14 lists counters for a media termination point (MTP) registered with Cisco Unified Communications Manager.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-14 Cisco Unified Communications Manager—MTP Usage

Counters	Description
MTP Device Name	Name of the MTP device registered to Cisco Unified Communications Manager.
Resource Total	Total number of resources on the MTP device.
Resources Available	Available resources on the MTP device.
Resources Active	Active resources on the MTP device.
Percentage Resources Active	Percentage active resources on the MTP device.

CCM – Transcoder

Table A-15 lists counters for transcoder devices registered with Cisco Unified Communications Manager.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-15 Cisco Unified Communications Manager—Transcoder

Counter	Description
Transcoder Name	Name of the transcoder.
Transcoder Total Resources	Total number of resources on the transcoder device.
Transcoder Resources Available	Available resources on the transcoder device.
Transcoder Resources Active	Active resources on the transcoder device.
Percentage Transcoder Resources Active	Percentage active resources on the transcoder device.

Cisco Analog Access

Table A-16 lists counters for analog access gateway.

Note Polling for these counters is enabled by default and is controlled by Voice Health Settings.

Table A-16 Cisco Analog Access

Counters	Description
Number of Ports Currently in Use	Number of ports active on the analog access device registered to Cisco Unified Communications Manager.
Number of Ports that Are out of Service	Number of ports out of service. This only applies to Loop Start and Ground Start trunks.
Number of Outbound Calls Attempted when Ports Were Busy	Number of times that a call was attempted through this analog access when no ports were available.

Cisco Unified Communications Manager Attendant Console

Table A-17 lists counters for Cisco Unified Communications Manager Attendant Console.

Note Polling for these counters is enabled by default and is controlled by Voice Health Settings.

Table A-17 Cisco Unified Communications Manager Attendant Console

Counters	Description
Cisco Unified Communications Manager Line Link Status	The line link state. It can be any of the following: 0, 1, 10, or 11.
Attendant Console Heartbeat	An incremental count that indicates whether the Telephony Call Dispatcher (TCD) service is up and running. If the count does not increase, it indicates that the TCD service is down.

Cisco Unified CCE Router Usage

Table A-18 lists performance counters for a Cisco Unified CCE (formerly IPCC) router.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-18 Cisco Unified CCE Router Usage

Counter	Description
IPCC Router Name	Router name.
IPCC Instance Name	Name of IPCC instance.
Agents Logged In	Number of contact center agents currently logged in.
Calls in Progress	Number of calls in progress.
Calls per Second	Number of inbound calls per second.

Cisco Messaging Interface

Table A-19 lists counters for Cisco Messaging Interface.

Note Polling for these counters is enabled by default and is controlled by Voice Health Settings.

Table A-19 Cisco Messaging Interface

Counter	Description
Messaging Heartbeat	An incremental count that indicates whether the Cisco Messaging Interface (CMI) service is up and running. If the count does not increase, it indicates that the CMI service is down.

Cisco SRST Usage

Table A-20 lists counters for Cisco Survivable Remote Site Telephony (SRST) usage information.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-20 Cisco SRST Usage

Counter	Description
Time in SRST Mode	Cumulative number of minutes the SRST device was in SRST mode.

Cisco TFTP Server

Table A-21 lists counters for Cisco TFTP Server.

Note Polling for these counters is enabled by default and is controlled by Voice Health Settings.

Table A-21 Cisco TFTP Server

Counter	Description
TFTP Heartbeat	An incremental count that indicates whether the TFTP server is up and running. If the count does not increase, it indicates that the TFTP server is down.
TFTP Requests Aborted	Number of times a TFTP client-initiated TFTP transfer was aborted.

CME Usage

Table A-22 lists performance counters for a Cisco Unified Communications Manager Express.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-22 Cisco Unified Communications Manager Express

Counters	Description
Number of Active Call Legs	Number of ephone call legs active.
Maximum Ephones	Maximum number of ephones that can be configured on the Cisco Unified Communications Manager Express.
Registered Ephones	Number of ephones registered.
Percentage Ephones Registered	Percentage of ephones that are registered.
Number of Configured Key Ephones	Number of key ephones configured.
Number of Registered Key Ephones	Number of key ephones registered.
Percentage Key Ephones Registered	Percentage of configured key ephones that are registered.
Ephones Seen	Maximum number of sessions configured on the CME.

Consolidated DSP Usage

Table A-23 lists counters for consolidated DSP usage on a Cisco IOS device.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-23 Consolidated DSP Usage

Counters	Description
Total DSP Channels	Total number of DSP channels on the device.
Total Active DSP Channels	Number of active DSP channels on the device.
Total In-Use DSP Channels	Number of DSP channels on the device that are reserved for serving calls.
Percentage Active DSP Channels	Percentage of DSP channels active on the device.

CPU Usage

Table A-24 lists counters for CPU usage on a Cisco IOS device, such as:

- Gateways and gatekeepers
- SRST devices
- Cisco Unity Express
- Cisco Unified Communications Manager Express

Table A-24 CPU Usage

Counters	Description
IOS Device Name	Name of Cisco IOS device.
CPU 1 5 Seconds	Overall CPU-busy percentage for CPU 1 in the last 5-second period; recorded at time stamp.
CPU 1 1 Minute	Overall CPU-busy percentage for CPU 1 in the last 1-minute period; recorded at time stamp.
CPU 1 5 Minutes	Overall CPU-busy percentage for CPU 1 in the last 5-minute period; recorded at time stamp.
CPU 2 5 Seconds	Overall CPU-busy percentage for CPU 2 in the last 5-second period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 2 is not present.
CPU 2 1 Minutes	Overall CPU-busy percentage for CPU 2 in the last 1-minute period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 2 is not present.
CPU 2 5 Minutes	Overall CPU-busy percentage for CPU 2 in the last 5-minute period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 2 is not present.
CPU 3 5 Seconds	Overall CPU-busy percentage for CPU 3 in the last 5-second period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 3 is not present.
CPU 3 1 Minute	Overall CPU-busy percentage for CPU 3 in the last 1-minute period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 3 is not present.
CPU 3 5 Minutes	Overall CPU-busy percentage for CPU 3 in the last 5-minute period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 3 is not present.
CPU 4 5 Seconds	Overall CPU-busy percentage for CPU 4 in the last 5-second period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 4 is not present.
CPU 4 1 Minute	Overall CPU-busy percentage for CPU 4 in the last 1-minute period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 4 is not present.
CPU 4 5 Minutes	Overall CPU-busy percentage for CPU 4 in the last 5-minute period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 4 is not present.
CPU 5 5 Seconds	Overall CPU-busy percentage for CPU 5 in the last 5-second period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 5 is not present.

Table A-24 CPU Usage (continued)

Counters	Description
CPU 5 1 Minutes	Overall CPU-busy percentage for CPU 5 in the last 1-minute period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 5 is not present.
CPU 5 5 Minutes	Overall CPU-busy percentage for CPU 5 in the last 5-minute period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 5 is not present.

CU Usage

Table A-25 lists counters for Cisco Unity.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-25 Cisco Unity Usage

Counter	Description
Total Ports	Total number of ports
Active Ports	Number of ports that are active
Percentage Active Ports	Percentage of total ports that are active
Total Inbound Ports	Total number of inbound ports
Active Inbound Ports	Number of active inbound ports
Percentage Active Inbound Ports	Percentage of total inbound ports that are active
Total Outbound Ports	Total outbound ports
Active Outbound Ports	Number of active outbound ports
Percentage Active Outbound Ports	Percentage of total outbound ports that are active

CU Connection Usage

Counters for Cisco Unity Connection have the same names and definitions as those for Cisco Unity; see Table A-25.

CUE Usage

Table A-26 lists counters for Cisco Unity Express mailbox usage.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-26 Cisco Unity Express Usage

Counters	Description
Licensed Mailboxes	Number of mailboxes that Cisco Unity Express is licensed for.
Orphaned Mailboxes	Number of mailboxes on Cisco Unity Express that are orphaned.
Percentage Orphaned Mailboxes	Percentage of orphaned mailboxes on Cisco Unity Express.

Table A-26 Cisco Unity Express Usage (continued)

Counters	Description
Maximum Sessions	Maximum number of sessions configured on Cisco Unity Express.
Sessions Used	Number of sessions used.
Percentage Sessions Used	Utilization of the sessions.
Licensed Capacity	Minutes of storage that the Cisco Unity Express is licensed for.
Allocated Capacity	Cumulative number of minutes of storage allocated to the mailboxes.
Used Capacity	Cumulative number of minutes of storage used by the mailboxes.
Capacity Used for Messages	Cumulative number of minutes of storage used for storing messages.
Free Capacity	Number of minutes of storage available.
Percentage of Time Used	Utilization of the storage on the Cisco Unity Express system.
Current Number of Messages	Cumulative number of messages stored in the mailboxes.
Current Number of Saved Messages	Cumulative number of saved messages in the mailboxes.
Messages Left	Cumulative number of messages left in the mailboxes since the last reboot of the Cisco Unity Express system.
Messages Retrieved	Cumulative number of messages retrieved in the mailboxes since the last reboot of the Cisco Unity Express system.
Messages Deleted	Cumulative number of messages deleted from the mailboxes since last reboot of the Cisco Unity Express system.
Number of Busy Mailboxes	Number of busy mailboxes.
Number of Mailboxes More than 90 Percent Full	Number of mailboxes that are 90% or more full.

DPA Port and CPU Usage

Table A-27 contains counters for Cisco Digital PBX Adapter (DPA) port usage.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-27 DPA Port and CPU Usage

Counter	Description
Total Voice Mail Ports	Number of voice mail ports on DPA.
Active Voice Mail Ports	Number of voice mail ports that are active.
Total PBX Ports	Number of PBX ports on DPA.
Active PBX Ports	Number of PBX ports that are active.
Unassigned Ports	Number of DPA ports that are not in use.
Percentage Active Voice Mail	Voice mail port utilization for the DPA.
Percentage Active PBX	PBX port utilization for the DPA.
CPU 5 Seconds	Overall CPU-busy percentage in the last 5-second period.

Table A-27 DPA Port and CPU Usage (continued)

Counter	Description
CPU 1 Minute	Overall CPU-busy percentage in the last 1-minute period.
CPU 5 Minutes	Overall CPU-busy percentage in the last 5-minute period.

DSP Usage

Table A-28 contains digital signal processor (DSP) usage information on Cisco IOS gateway.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings. For additional information, see Cisco IOS Gateway Digital Signal Processor Usage—Record Type 109, page J-21.

Table A-28 DSP Usage

Counters	Description
Index	An index assigned to the DSP.
State	1=active, 2=shutdown.
Total Channels	Number of channels on DSP.
Active Channels	Number of channels on DSP that are active.
In-Use Channels	Number of channels reserved for serving calls.

E1 CAS Channel Status for IOS GW

The set of performance counters in Table A-29 is displayed for each E1 CAS port in the Cisco IOS gateway.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-29 E1 CAS Channel Status for Cisco IOS Gateway

Counters	Description
DS1 Name	DS1 name
Channel Status [*n*] **Note** Displayed for each of 31 channels with *n* from 0 through 30.	200=idle, 300=unknown, 301=other, 302=voice, 303=unrestrictedDigital, 304=unrestrictedDigital56, 305=restrictedDigital, 306=audio31, 307=audio7, 308=video, 309=packetSwitched, 310=fax, 312=unknown, 313=analog, 314=digital, 315=v110, 316=v120

E1 PRI Channel Status for CCM GW

The set of performance counters in Table A-30 is displayed for each E1 PRI port in the Cisco Unified Communications Manager-controlled MGCP gateway.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-30 E1 PRI Channel Status for Cisco Unified Communications Manager-Controlled MGCP Gateway

Counters	Description
DS1 Name	DS1 name
Channel Status [*n*] **Note** Displayed for each of 31 channels with *n* from 0 through 30.	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved

E1 PRI Channel Status for IOS GW

The set of performance counters in Table A-31 is displayed for each E1 PRI port in the Cisco IOS gateway.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-31 E1 PRI Channel Status for Cisco IOS Gateway

Counters	Description
DS1 Name	DS1 name
Channel Status [*n*] **Note** Displayed for each of 31 channels with *n* from 0 through 30.	200=idle, 300=unknown, 301=other, 302=voice, 303=unrestrictedDigital, 304=unrestrictedDigital56, 305=restrictedDigital, 306=audio31, 307=audio7, 308=video, 309=packetSwitched, 310=fax, 312=unknown, 313=analog, 314=digital, 315=v110, 316=v120

E1 PRI Usage for CCM GW

The set of performance counters in Table A-32 is displayed for each E1 PRI in the Cisco Unified Communications Manager-controlled MGCP gateway.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-32 E1 PRI Usage for Cisco Unified Communications Manager-Controlled MGCP Gateway

Counters	Description
CCM Name	Cisco Unified Communications Manager that the MGCP gateway is registered with.
DS1 Name	Name of DS1.
Calls Completed	Number of calls completed on this E1 PRI port on the gateway.
Outbound Busy Attempts	Number of outbound busy attempts on this E1 PRI port on the gateway.

FXO Port Usage for CCM GW

The set of performance counters in Table A-33 is displayed for each FXO port in the Cisco Unified Communications Manager-controlled MGCP gateway.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-33 FXO Port Usage for Cisco Unified Communications Manager-Controlled MGCP Gateway

Counters	Description
CCM Name	Cisco Unified Communications Manager that the MGCP gateway is registered with.
FXO Port Name	Name of FXO port.
Calls Completed	Number of calls completed on this FXO port on the gateway.
Outbound Busy Attempts	Number of outbound busy attempts on this FXO port on the gateway.

FXS Port Usage for CCM GW

The set of performance counters in Table A-34 is displayed for each FXS port in the Cisco Unified Communications Manager-controlled MGCP gateway.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-34 FXS Port Usage for Cisco Unified Communications Manager-Controlled MGCP Gateway

Counters	Description
CCM Name	Cisco Unified Communications Manager that the MGCP gateway is registered with.
FXS Port Name	Name of FXS port.
Calls Completed	Number of calls completed on this FXS port on the gateway.
Outbound Busy Attempts	Number of outbound busy attempts on this FXS port on the gateway.

Gatekeeper Zone Statistics

The set of performance counters in Table A-35 is displayed for each gatekeeper zone.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-35 Gatekeeper Zone Statistics

Counters	Description
Zone Name	Name of zone.
Zone Domain	Name of zone domain.
Zone Type	Indicates whether the zone is local or remote.
Total Bandwidth	Total bandwidth in 100 bps configured for local zone, or one of the following: -1=bandwidth limitation not set. *=field is not applicable (when record is for a remote zone).

Table A-35 Gatekeeper Zone Statistics (continued)

Counters	Description
Allocated Bandwidth	Bandwidth in 100 bps allocated to calls for local zone, or asterisk (*) to indicate that the field is not applicable (when record is for a remote zone).
Total Interzone Bandwidth	Total interzone bandwidth in 100 bps configured for local zone, or one of the following: -1=bandwidth limitation not set. *=field is not applicable (when record is for a remote zone).
Allocated Interzone Bandwidth	Bandwidth in 100 bps allocated to calls for the local zone, or asterisk (*) to indicate that the field is not applicable (when record is for a remote zone).
Number of Admission Rejections	Cumulative number of admission rejections for local zone, or asterisk (*) to indicate that the field is not applicable (when record is for a remote zone).
Number of Admission Confirms	Cumulative number of admission confirms for local zone, or asterisk (*) to indicate that the field is not applicable (when record is for a remote zone).
Number of Location Requests	Cumulative number of location requests for remote zone, or asterisk (*) to indicate that the field is not applicable (when record is for a local zone).
Number of Add Lookup Failures	Cumulative number of times the gatekeeper is unable to resolve an address.
Number of Endpoint Timeouts	Cumulative number of times the time to live has expired for an endpoint in this zone.
Number of Other Failures	Cumulative number of call attempts which have failed for reasons other than endpoint timeouts or address lookup failures.
Percentage Allocated Bandwidth	Bandwidth utilization for the local zone.
Percentage Allocated Interzone Bandwidth	Interzone bandwidth utilization for the local zone.

Hardware Conference Bridge

Table A-36 lists counters for a hardware conference bridge registered with Cisco Unified Communications Manager.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-36 Hardware Conference Bridge

Counters	Description
Bridge Name	Name of the hardware conference bridge registered to Unified Communications Manager.
Conferences Completed	Number of conferences completed on this hardware conference bridge.
Conferences Active	Number of conferences active on this hardware conference bridge.
Total Resources	Total number of resources on this hardware conference bridge.
Available Resource	Available resources on this hardware conference bridge.

Table A-36 Hardware Conference Bridge (continued)

Counters	Description
Active Resource	Active resources on this hardware conference bridge.
Percentage Active Resources	Percentage of active resources on this hardware conference bridge.

Memory Usage

Table A-37 lists counters for memory usage; these counters might be displayed for any of the following:

- Cisco Unified Communications Manager Express
- Cisco IOS gateway or gatekeeper
- Cisco Unity Express
- SRST devices
- Cisco IOS gateways and gatekeepers

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-37 Memory Usage

Counters	Description
Processor Used	Amount of memory in bytes.
Processor Free	Amount of memory in bytes.
Processor Largest Free	Amount of memory in bytes.
I/O Used	Amount of memory in bytes.
I/O Free	Amount of memory in bytes.
I/O Largest Free	Amount of memory in bytes.
PCI Used	Amount of memory in bytes.
PCI Free	Amount of memory in bytes.
PCI Largest Free	Amount of memory in bytes.
Fast Used	Amount of memory in bytes.
Fast Free	Amount of memory in bytes.
Fast Largest Free	Amount of memory in bytes.
Multibus Used	Amount of memory in bytes.
Multibus Free	Amount of memory in bytes.
Multibus Largest Free	Amount of memory in bytes.
Percentage Processor Memory Used	Percentage processor memory utilization.
Percentage I/O Memory Used	Percentage I/O memory utilization.

Server Memory Usage

Table A-38 lists counters for memory usage information for a server running one of the following: Cisco Unified Communications Manager, IP Contact Center, Cisco Unity, or Cisco Unity Connection.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-38 Server Memory Usage

Counters	Description
Total Memory in Kilobytes	Total RAM in kilobytes.
Used Memory in Kilobytes	Used RAM in kilobytes.
Free Memory in Bytes	Free RAM in kilobytes.
Percentage Used Memory	Percentage of used memory.
Kilobytes Buffered	Linux buffered memory in kilobytes.
Kilobytes Cached	Linux cached memory in kilobytes.
Kilobytes Shared	Linux shared memory in kilobytes.
Kilobytes Total Swap	Linux total swap memory in kilobytes.
Kilobytes Used Swap	Linux used swap memory in kilobytes.
Kilobytes Free Swap	Linux free swap memory in kilobytes.
Windows Cached Bytes	Windows cached memory in kilobytes.
Windows Commit Limit	Windows total virtual memory in kilobytes.
Windows Committed Bytes	Windows used virtual memory in kilobytes.

SIP Device Usage

Table A-39 lists counters for SIP devices registered with Cisco Unified Communications Manager.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-39 SIP Device Usage

Counters	Description
SIP Device Name	Name of the SIP device.
Calls Active	Number of calls active.
Calls Attempted	Number of calls attempted.
Calls Completed	Number of calls completed.
Calls in Progress	Number of calls in progress.

Software Conference Bridge

Table A-40 lists counters for software conference bridge registered with Cisco Unified Communications Manager.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-39, Part 1 Software Conference Bridge

Counters	Description
Bridge Name	Name of the software conference bridge registered to Unified Communications Manager.
Conferences Completed	Number of conferences completed on this software conference bridge.
Conferences Active	Number of conferences active on this software conference bridge.
Total Resources	Total number of resources on this software conference bridge.
Available Resource	Available resources on this software conference bridge.
Active Resource	Active resources on this software conference bridge.
Percentage Active Resources	Percentage of active resources on this software conference bridge.

T1 CAS Channel Status for CCM GW

The set of performance counters in Table A-40 is displayed for each T1 CAS port in the Cisco Unified Communications Manager-controlled MGCP gateway.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-40 T1 CAS Channel Status for Cisco Unified Communications Manager-Controlled MGCP Gateway

Counters	Description
DS1 Name	DS1 name.
Channel Status [*n*] **Note** Displayed for each of 24 channels with *n* from 0 through 23.	200=idle, 300=unknown, 301=other, 302=voice, 303=unrestrictedDigital, 304=unrestrictedDigital56, 305=restrictedDigital, 306=audio31, 307=audio7, 308=video, 309=packetSwitched, 310=fax, 312=unknown, 313=analog, 314=digital, 315=v110, 316=v120

T1 CAS Channel Status for IOS GW

The set of performance counters in Table A-41 is displayed for each T1 CAS port in the Cisco IOS gateway.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-41 T1 CAS Channel Status for Cisco IOS Gateway

Counters	Description
DS1 Name	DS1 name
Channel Status [*n*] **Note** Displayed for each of 24 channels with *n* from 0 through 23.	200=idle, 300=unknown, 301=other, 302=voice, 303=unrestrictedDigital, 304=unrestrictedDigital56, 305=restrictedDigital, 306=audio31, 307=audio7, 308=video, 309=packetSwitched, 310=fax, 312=unknown, 313=analog, 314=digital, 315=v110, 316=v120

T1 CAS Usage for CCM GW

The set of performance counters in Table A-42 is displayed for each T1 CAS in the Cisco Unified Communications Manager-controlled MGCP gateway.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-42 T1 CAS Usage for Cisco Unified Communications Manager-Controlled MGCP Gateway

Counters	Description
CCM Name	Cisco Unified Communications Manager that the MGCP gateway is registered with
DS1 Name	Name of DS1
Calls Completed	Number of calls completed on this T1 CAS port on the gateway
Outbound Busy Attempts	Number of outbound busy attempts on this T1 CAS port on the gateway

T1 PRI Channel Status for CCM GW

The set of performance counters in Table A-43 is displayed for each T1 PRI port in the Cisco Unified Communications Manager-controlled MGCP gateway.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-43 T1 PRI Channel Status for Cisco Unified Communications Manager-Controlled MGCP Gateway

Counters	Description
DS1 Name	DS1 name
Channel Status [*n*] **Note** Displayed for each of 24 channels with *n* from 0 through 23.	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved

T1 PRI Channel Status for IOS GW

The set of performance counters in Table A-44 is displayed for each T1 PRI port in the Cisco IOS gateway.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-44 T1 PRI Channel Status for Cisco IOS Gateway

Counters	Description
DS1 Name	DS1 name
Channel Status [*n*] **Note** Displayed for each of 24 channels with *n* from 0 through 23.	200=idle, 300=unknown, 301=other, 302=voice, 303=unrestrictedDigital, 304=unrestrictedDigital56, 305=restrictedDigital, 306=audio31, 307=audio7, 308=video, 309=packetSwitched, 310=fax, 312=unknown, 313=analog, 314=digital, 315=v110, 316=v120

T1 PRI Usage for CCM GW

The set of performance counters in Table A-45 is displayed for each T1 PRI in the Cisco Unified Communications Manager-controlled MGCP gateway.

Note Polling for these counters is disabled by default and is controlled by Voice Utilization Settings.

Table A-45 T1 PRI Usage for Cisco Unified Communications Manager-Controlled MGCP Gateway

Counters	Description
CCM Name	Cisco Unified Communications Manager that the MGCP gateway is registered with.
DS1 Name	Name of DS1.
Calls Completed	Number of calls completed on this T1 PRI port on the gateway.
Outbound Busy Attempts	Number of outbound busy attempts on this T1 PRI port on the gateway.

APPENDIX B

MIBs Polled and Perfmon Counter Objects Used

Cisco Unified Operations Manager (Operations Manager) obtains data from MIBs and from Perfmon counter objects:

MIBs that Operations Manager Uses

Operations Manager polls certain MIBs for information that is relevant to fault management. Polling is done based on the polling interval, as described in Configuring Polling and Thresholds, page 19-1. Obtaining MIB information depends on several contingencies—namely, whether a device supports a MIB, has the proper SNMP implementation, is accessible, and so forth.

Operations Manager polls the following MIBs:

- CISCO-CAS-IF-MIB
- CISCO-CDP-MIB
- CISCO-CCM-MIB
- CISCO-CCME-MIB
- CISCO-CONTACT-CENTER-APPS-MIB
- CALISTA-DPA-MIB
- CISCO-DSP-MGMT-MIB
- CISCO-ENVMON-MIB
- CISCO-FLASH-MIB
- CISCO-GATEKEEPER-MIB
- CISCO-ISDN-MIB
- CISCO-LS1010-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-METRO-PHY-MIB
- CISCO-POP-MGMT-MIB
- CISCO-PROCESS-MIB
- CISCO-RHINO-MIB

- CISCO-RTTMON-MIB
- CISCO-SRST-MIB
- CISCO-STACK-MIB
- CISCO-NotificationEvent-MIB
- CISCO-UNITY-MIB
- CISCO-UNITY-EXPRESS-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VOICE-APPS-MIB
- CISCO-VOICE-DIAL-CONTROL-MIB
- CISCO-VOICE-IF-MIB
- CISCO-VTP-MIB
- CPQSIINFO-MIB
- CPQHLTH-MIB
- CPQHOST-MIB
- CPQNIC-MIB
- CPQSM2-MIB
- DIAL-CONTROL-MIB
- ENTITY-MIB
- ENTITY-FRU-CONTROL-MIB
- ETHERLIKE-MIB
- HOST-RESOURCES-MIB (RFC 1514)
- UMSASSETID-MIB
- UMSEVENT-MIB
- UMSLMSENSOR-MIB
- IF-MIB (RFC 1493)
- IF-MIB (RFC 1573)
- ISDN-MIB
- ibmpsgProcessor
- ibmpsgLMSensor
- ibmpsgPower
- ibmpsgLMSensor
- MIB-II (RFC 1213)
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-CPU-MIB
- OLD-CISCO-ENV-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-MEMORY-MIB
- OLD-CISCO-MEMORY-POOL-MIB

- OLD-CISCO-SYSTEM-MIB
- SYS-APPL-MIB
- UMSEVENT-MIB

Perfmon Counter Objects that Operations Manager Uses

Operations Manager uses Perfmon counter objects on Cisco Unified Communications Manager platforms to collect information based on the following polling settings:

- Voice Health Settings—Polling for these settings is enabled by default (see Voice Health Settings—Polling, page 19-19).
- Voice Utilization Settings—Polling for these settings is disabled by default. To collect performance and capacity data—for display on performance graphs—you must enable these settings. See Voice Utilization Settings—Polling, page 19-23. After Voice Utilization Settings polling is enabled, the data that is collected is also stored in files; for more information, see Data Files—Maintenance and Usage, page J-1.

The following are counter objects that Operations Manager uses, with descriptions of each counter:

- Cisco Unity, page B-16
- Memory, page B-16
- Processor, page B-17

Note For information about the MIBs that Operations Manager uses to collect data about Cisco IOS gateways, see MIBs that Operations Manager Uses, page B-1.

Cisco CallManager

This counter object provides data at the Cisco Unified CallManager level.

Table B-1 Cisco Unified CallManager Counter Objects

Counter	Description
Polling for These Counters Is Controlled by Voice Utilization Settings	
CallsActive	Number of streaming connections currently active. CallsActive are calls that actually have a voice path connected.
RegisteredMGCPGateway	Number of registered MGCP gateways.
FXSPortInService	Number of FXS ports currently in service.
FXSPortsActive	Number of FXS ports currently active.
FXOPortsInService	Number of FXO ports currently in service.
FXOPortsActive	Number of FXO ports currently active.
T1SpansInService	Number of T1 CAS spans currently in service.
T1ChannelsActive	Number of T1 CAS voice channels currently active.
PRISpansInService	Number of PRI spans currently in service.
PRIChannelsActive	Number of PRI voice channels currently active.
BRISpansInService	Number of BRI spans currently in service.
BRIChannelsActive	Number of BRI voice channels currently active.
CallsAttempted	Number of calls attempted.
CallsCompleted	Number of calls for which a voice path was established.
CallsInProgress	Number of calls currently in progress (off-hook).
MOHMulticastResourceActive	Number of multicast MOH resources currently in use.
MOHMulticastResourceAvailable	Number of multicast MOH resources currently available.
MOHTotalMulticastResources	Total number of multicast MOH resources.
MOHTotalUnicastResources	Total number of unicast MOH resources.
MOHUnicastResourceActive	Number of unicast MOH resources currently active.
MOHUnicastResourceAvailable	Number of unicast MOH resources currently available.
RegisteredAnalogAccess	Number of registered Cisco Analog Access gateways.
RegisteredHardwarePhones	Number of registered Cisco hardware IP phones.
RegisteredMGCPGateway	Number of registered MGCP gateways.
RegisteredOtherStationDevices	Number of registered station devices other than Cisco hardware IP phones.

Table B-1 Cisco Unified CallManager Counter Objects (continued)

Counter	Description
SWConferenceCompleted	Total number of conferences that used a software conference bridge that was allocated from this Cisco Unified Communications Manager and released.
SWConferenceResourceActive	Total number of conference resources in use on all registered software conference devices.
SWConferenceResourceAvailable	Number of new software-based conferences that can be started at this time.
TranscoderResourceActive	Number of transcoders currently active on all registered transcoder devices.
TranscoderResourceAvailable	Total number of transcoders currently available on all registered transcoder devices.
Counters Supported with Cisco Unified Communications Manager Versions Prior to 4.0	
UnicastHardwareConferenceActiveParticipants	Number of unicast hardware conference resources currently active.
UnicastHardwareConferenceCompleted	Number of completed unicast conferences.
UnicastHardwareConfResourceActive	Number of unicast conference resources currently active.
UnicastHardwareConfResourceAvailable	Number of unicast conference resources currently available.
MediaTermPointsResourceActive	Number of MTP resources currently active.
MediaTermPointsResourceAvailable	Number of MTP resources currently available.
SWConferenceActiveParticipants	Number of active conferences on all registered software conference devices.
Counters Supported with Cisco Unified Communications Manager Versions 4.0 and Later	
HWConferenceActive	Number of active conferences on all hardware conference devices registered with this Cisco Unified Communications Manager.
HWConferenceCompleted	Number of completed (released) conferences that used a hardware conference bridge allocated from this Cisco Unified Communications Manager.
HWConferenceOutOfResources	Number of times this Cisco Unified Communications Manager attempted to allocate a hardware conference resource from those that are registered to this Cisco Unified Communications Manager, when none were available.
HWConferenceResourceActive	Number of conference resources active on all hardware conference devices registered with this Cisco Unified Communications Manager.
HWConferenceResourceAvailable	Number of hardware conference resources currently available.
HWConferenceResourceTotal	Total number of hardware conference resources provided by all registered hardware conference bridge devices.
MTPResourceActive	Number of Media Termination Point resources currently active.
MTPResourceAvailable	Number of MTP resources currently available.
MTPResourceTotal	Total number of MTP resources provided by all registered MTP devices.
SWConferenceActive	Number of active conferences on all registered software conference devices.

Table B-1 Cisco Unified CallManager Counter Objects (continued)

Counter	Description
MediaListResourceExhausted	Number of times this Cisco Unified Communications Manager attempted to allocate a software conference resource from those that are registered to this Cisco Unified Communications Manager, when none were available.
SWConferenceResourceTotal	Number of software conference resources provided by all registered software conference bridge devices.
TranscoderResourceTotal	Total number of transcoder resources provided by all registered transcoder devices.

Cisco CallManager Attendant Console

This counter object provides data for Cisco CallManager Attendant Console.

Table B-2 Cisco CallManager Attendant Console

Counter	Description
CcmLineLinkState	The line state. It can be any of the following: 0, 1, 10, or 11.
HeartBeat	An incremental count that indicates whether the Telephony Call Dispatcher (TCD) service is up and running. If the count does not increase, it indicates that the TCD service is down.

Cisco Messaging Interface

This counter object provides data at the Cisco Messaging Interface level.

Table B-3 Cisco Messaging Interface Counter Object

Counter	Description
HeartBeat	An incremental count that indicates whether the Cisco Messaging Interface (CMI) service is up and running. If the count does not increase, it indicates that the CMI Service is down.

Cisco MGCP Gateway

This counter object provides data at the MGCP gateway level for MGCP gateways registered to the Cisco Unified Communications Manager. There is one set of counters, listed in Table A-2, for each such gateway.

Note Polling for counters in Table B-4 is controlled by Voice Utilization Settings, which are disabled by default; see Voice Utilization Settings—Polling, page 19-23.

Table B-4 Cisco MGCP Gateway Counter Object

Counter	Description
FXSPortsInService	Number of FXS ports currently in service in the gateway
FXSPortsActive	Number of FXS ports currently active in a call in the gateway

Table B-4 Cisco MGCP Gateway Counter Object (continued)

Counter	Description
FXOPortsInService	Number of FXO ports currently in service in the gateway
FXOPortsActive	Number of FXO ports currently active in a call in the gateway
T1SpansInService	Number of T1 CAS spans currently in service in the gateway
T1ChannelsActive	Number of T1 CAS voice channels currently active in a call in the gateway
PRISpansInService	Number of PRI spans currently in service in the gateway
PRIChannelsActive	Number of PRI voice channels currently active in a call in the gateway
BRISpansInService	Number of BRI spans currently in service in the gateway
BRIChannelsActive	Number of BRI voice channels currently active in the gateway

Cisco MGCP T1 CAS Device

This counter object provides channel level data for each T1 CAS trunk on MGCP gateways registered to the Cisco Unified Communications Manager. There is one set of 26 counters, listed in Table A-3, for each T1 CAS trunk.

Note Polling for counters in Table B-5 is controlled by Voice Utilization Settings, which are disabled by default; see Voice Utilization Settings—Polling, page 19-23.

Table B-5 Cisco MGCP T1 CAS Device Counter Object

Counter	Description
Channel 1 Status–Channel 24 Status	Status of the indicated B channel associated with the MGCP T1 CAS device: 0 = Unknown 1 = Out of service 2 = Idle 3 = Busy 4 = Reserved
CallsCompleted	Total number of successful calls made from the MGCP T1CAS device.
OutboundBusyAttempts	Total number of times that a call through the MGCP T1CAS device was attempted when no voice channel was available.

Cisco MGCP PRI Device

This counter object gives channel level data for each T1/E1 PRI trunk on MGCP gateways registered to the Cisco Unified Communications Manager. There is one set of 33 counters, listed in Table A-4, for each PRI trunk. 31 channels will be used for an E1 PRI trunk, while only 24 channels will be used for a T1 PRI trunk.

Note Polling for counters in Table B-6 is controlled by Voice Utilization Settings, which are disabled by default; see Voice Utilization Settings—Polling, page 19-23.

Table B-6 Cisco MGCP PRI Device Counter Object

Counter	Description
Channel 1 Status–Channel 31 Status	Status of the indicated B channel associated with the MGCP PRI device: 0 = Unknown 1 = Out of service 2 = Idle 3 = Busy 4 = Reserved
CallsCompleted	Total number of successful calls made from the MGCP PRI device.
OutboundBusyAttempts	Total number of times a call through the MGCP PRI device was attempted when no voice channel was available.

Cisco MGCP BRI Device

This counter object provides channel level data for each BRI trunk on MGCP gateways registered to the Cisco Unified Communications Manager. There is one set of three counters, listed in Table B-7, for each BRI trunk.

Note Polling for counters in Table B-7 is controlled by Voice Utilization Settings, which are disabled by default; see Voice Utilization Settings—Polling, page 19-23.

Table B-7 Cisco MGCP BRI Device Counter Object

Counter	Description
Channel 1 Status–Channel 2 Status	Status of the indicated B channel associated with the MGCP BRI device: 0 = Unknown 1 = Out of service 2 = Idle 3 = Busy 4 = Reserved
DataLinkInService	Status of the data link.

Cisco MGCP FXO Device

This counter object provides data for each FXO port on MGCP gateways registered to the Cisco Unified Communications Manager. There is one set of two counters, listed in Table B-8, for each FXO device on the registered MGCP gateway.

Note Polling for counters in Table B-8 is controlled by Voice Utilization Settings, which are disabled by default; see Voice Utilization Settings—Polling, page 19-23.

Table B-8 Cisco MGCP FXO Device Counter Object

Counter	Description
CallsCompleted	Number of successful calls made from the MGCP FXO device.
OutboundBusyAttempts	Number of times that a call through the MGCP FXO device was attempted when there was no voice channel available.
PortStatus	Status of the FXO port associated with this MGCP FXO device.

Cisco MGCP FXS Device

This counter object provides data for each FXS port on MGCP gateways registered to the Cisco Unified Communications Manager. There is one set of two counters, listed in Table B-9, for each FXS device on the registered MGCP gateway.

Note Polling for counters in Table B-9 is controlled by Voice Utilization Settings, which are disabled by default; see Voice Utilization Settings—Polling, page 19-23.

Table B-9 Cisco MGCP FXS Device Counter Object

Counter	Description
CallsCompleted	Number of successful calls made from the MGCP FXS device.
OutboundBusyAttempts	Number of times that a call through the MGCP FXS device was attempted when there was no voice channel available.
PortStatus	Status of the FXS port associated with this MGCP FXS device.

Cisco CtiManager

This counter object provides data for application connections, open devices, and lines for Cisco CTIManager. There is one set of four counters, listed in Table B-10.

Note

- This counter object is supported for Cisco Unified Communications Manager versions earlier than 4.0. For Cisco Unified Communications Manager version 4.0 and later, see Cisco CTI Manager, page B-10.
- Polling for counters in Table B-10 is controlled by Voice Utilization Settings, which are disabled by default; see Voice Utilization Settings—Polling, page 19-23.

Table B-10 Cisco CtiManager Counter Object

Counter	Description
NumOfActiveCmLink	Number of connections between Cisco CTIManager and Cisco Unified Communications Managers in the cluster.
NumOfCtiConnection	Number of application connections to Cisco CTIManager.

Table B-10 Cisco CtiManager Counter Object (continued)

Counter	Description
NumOfOpenDevices	Number of devices opened by all applications connected to Cisco CTIManager.
NumOfOpenLines	Number of lines opened by all applications connected to Cisco CTIManager.

Cisco CTI Manager

This counter object provides data for application connections, open devices, and lines for Cisco CTI Manager. There is one set of four counters, listed in Table B-11.

Note

- This counter object is supported for Cisco Unified Communications Manager versions 4.0 and later. For Cisco Unified Communications Manager versions earlier than 4.0, see Cisco CtiManager, page B-9.
- Polling for counters in Table B-11 is controlled by Voice Utilization Settings, which are disabled by default; see Voice Utilization Settings—Polling, page 19-23.

Table B-11 Cisco CTI Manager Counter Object

Counter	Description
CcmLinkActive	Number of connections between Cisco CTI Manager and Cisco Unified Communications Managers in the cluster.
CTIConnectionActive	Number of application connections to Cisco CTI Manager.
DevicesOpen	Number of devices opened by all applications connected to Cisco CTI Manager.
LinesOpen	Number of lines opened by all applications connected to Cisco CTI Manager.

Cisco Analog Access

This counter object provides data for Cisco Analog Access. There is one counter, listed in Table B-12.

Table B-12 Cisco Analog Access Counter Object

Counter	Description
Polling for These Counters Is Controlled by Voice Utilization Settings	
PortsActive	Number of ports currently active. A port is active when a call is in progress on that port. **Note** Although Voice Health Settings also controls polling for this counter, to make this data available for performance graphing, you must enable polling for Voice Utilization Settings.
Polling for These Counters Is Controlled by Voice Health Settings	
OutboundBusyAttempts	Number of times that a call was attempted through this analog access when no ports were available.

Table B-12 Cisco Analog Access Counter Object (continued)

Counter	Description
PortsActive	Number of ports currently active. A port is active when a call is in progress on that port.
PortsOutOfService	Number of ports out of service. This only applies to Loop Start and Ground Start trunks.

Cisco H323

This counter object provides data for Cisco H323 gateways and gatekeepers. There is one set of four counters, listed in Table B-13, for each H323 device.

Note Polling for the counters in Table B-13 is controlled by Voice Utilization Settings, which are disabled by default; see Voice Utilization Settings—Polling, page 19-23.

Table B-13 Cisco H323 Counter Object

Counter	Description
CallsActive	Number of streaming connections currently active. CallsActive are calls that actually have a voice path connected. **Note** This counter is not supported for Cisco Unified Communications Manager versions earlier than 4.0.
CallsAttempted	Number of calls that have been attempted on this device, including both successful and unsuccessful call attempts.
CallsCompleted	Number of calls for which a voice path was established.
CallsInProgress	Number of calls currently in progress; includes all active calls.

Cisco Location

This counter object provides data for Cisco Unified Communications Manager-defined locations. There is one set of two counters, listed in Table B-14, for each location.

Table B-14 Cisco Location Counter Object

Counter	Description
Polling for These Counters Is Controlled by Voice Utilization Settings	
Counters Supported with Cisco Unified Communications Manager Versions Prior to 4.0	
CurrentAvailableBandwidth	Current bandwidth available in a location. A value of zero indicates that no bandwidth is available.
MaxAvailableBandwidth	Maximum bandwidth available in a location. A value of zero indicates that infinite bandwidth is available.
Counters Supported with Cisco Unified Communications Manager Versions 4.0 and Later	
BandwidthAvailable	Current bandwidth available in a location. A value of zero indicates that no bandwidth is available.

Table B-14 Cisco Location Counter Object (continued)

Counter	Description
BandwidthMaximum	Maximum bandwidth available in a location. A value of zero indicates that infinite bandwidth is available.
Counters Supported with Cisco Unified Communications Manager Versions 5.0 and Later	
CallsInProgress	Number of calls currently in progress; includes all active calls.

Cisco Media Streaming Application

Note This counter object is introduced with Cisco Unified Communications Manager version 4.0 and supported with Cisco Unified Communications Manager versions 4.0 and later.

This counter object provides information about registered media termination points (MTPs), music on hold (MOH) servers, conference bridge servers, and annunciators. There is one set of counters, listed in Table B-15, for each Cisco Unified Communications Manager in the Cisco Unified Communications Manager Group associated with the device pool that the annunciator device is configured to use.

Table B-15 Cisco Media Streaming Application Counter Object

Counter	Description
Polling for These Counters Is Controlled by Voice Utilization Settings	
CFBConferencesActive	Number of currently active conferences.
CFBConferencesTotal	Total number of conferences that have been started since the Cisco IP Voice Media Streaming application service started.
CFBStreamsActive	Total number of currently active simplex streams for all conferences.
CFBStreamsAvailable	Number of streams allocated for the conference bridge that are currently available.
CFBStreamsTotal	Total number of simplex streams that have been connected to the conference bridge since the Cisco IP Voice Media Streaming application service started.
MOHAudioSourcesActive	Number of currently active audio sources for this MOH server.
MOHStreamsActive	Total number of currently active simplex streams for all connections.
MOHStreamsAvailable	Number of streams allocated for the MOH device that are currently available.
MOHStreamsTotal	Total number of simplex streams that have connected to the MOH server since the Cisco IP Voice Media Streaming application service started. **Note** Although Voice Health Settings also controls polling for this counter, to make this data available for performance graphing, you must enable polling for Voice Utilization Settings.

Table B-15 Cisco Media Streaming Application Counter Object (continued)

Counter	Description
MTPConnectionsTotal	Total number of MTP instances that have been started since the Cisco IP Voice Media Streaming application service started. **Note** Although Voice Health Settings also controls polling for this counter, to make this data available for performance graphing, you must enable polling for Voice Utilization Settings.
MTPInstancesActive	Number of currently active instances of MTP.
MTPStreamsActive	Total number of currently active simplex streams for all connections.
MTPStreamsAvailable	Number of streams allocated for the MTP device that are currently available.
MTPStreamsTotal	Total number of simplex streams that have been connected to the MTP device since the Cisco IP Voice Media Streaming application service started.
Polling for These Counters Is Controlled by Voice Health Settings	
MTPConnectionsTotal	Total number of MTP instances that have been started since the Cisco IP Voice Media Streaming application service started.
MTPStreamsTotal	Total number of simplex streams that have connected to the MOH server since the Cisco IP Voice Media Streaming application service started.

Cisco MOH Device

This counter object provides data for Cisco MOH servers. There is one set of seven counters, listed in Table B-16, for each MOH server.

Note Polling for the counters in Table B-16 is controlled by Voice Utilization Settings, which are disabled by default; see Voice Utilization Settings—Polling, page 19-23.

Table B-16 Cisco MOH Device Counter Object

Counter	Description
MOHHighestActiveResources	Number of simultaneously active MOH connections for this MOH server; includes both multicast and unicast connections.
MOHMulticastResourceActive	Number of currently active multicast connections to multicast addresses served by this MOH server.
MOHMulticastResourceAvailable	Number of multicast MOH connections to multicast addresses served by this MOH server that are currently available.
MOHTotalMulticastResources	Number of multicast MOH connections allowed to multicast addresses served by this MOH server.
MOHTotalUnicastResources	Number of unicast MOH connections allowed by this MOH server.

Table B-16 Cisco MOH Device Counter Object (continued)

Counter	Description
MOHUnicastResourceActive	Number of active unicast MOH connections to this MOH server.
MOHUnicastResourceAvailable	Number of inactive unicast MOH connections that are still available to be used for this MOH server.

Cisco MTP Device

This counter object provides information about registered Cisco MTP devices. There is one set of three counters, listed in Table B-17, for each MTP device.

Table B-17 Cisco MTP Device Counter Object

Counter	Description
Polling for These Counters Is Controlled by Voice Utilization Settings	
ResourceActive	Number of MTP resources currently active.
ResourceAvailable	Total number of MTP resources currently available.
Counters Supported with Cisco Unified Communications Manager Versions 4.0 and Later	
ResourceTotal	Total number of MTP resources, including those that are active and available.

Cisco HW Conference Bridge Device

This counter object provides information about registered Cisco hardware conference bridge devices. There is one set of six counters, listed in Table B-18, for each hardware conference bridge device.

Table B-18 Cisco HW Conference Bridge Device Counter Object

Counter	Description
Polling for These Counters Is Controlled by Voice Utilization Settings	
HWConferenceCompleted	Total number of conferences that have been allocated and released on this device.
ResourceActive	Number of resources currently active on this device.
ResourceAvailable	Total number of resources currently available on this device.
Counters Supported with Cisco Unified Communications Manager Versions Prior to 4.0	
HWConferenceActiveParticipants	Number of active conferences on all registered hardware conference devices.
Counters Supported with Cisco Unified Communications Manager Versions 4.0 and Later	
HWConferenceActive	Number of active conferences on all registered hardware conference devices.
ResourceTotal	Total number of resources (sum of ResourceAvailable and ResourceActive) on this device.

Cisco Personal Assistant

This counter object provides information about registered Cisco Personal Assistant applications.

Table B-19 Cisco Personal Assistant Counter Object

Counter	Description
Total WorkingSet Memory(MB)	Maximum number of bytes in the working set of this process at any point in time. The working set is the set of memory pages recently used by the threads in the process. If the free memory in the system is above a threshold, the pages are left in the working set of the process even if they are not in use. When the free memory falls below a threshold, pages are trimmed from the working sets. If the pages are needed later, they are soft-faulted back into the working set before they leave the main memory.

Cisco SIP

This counter object provides SIP phone information.

Table B-20 Cisco SIP Counter Object

Counter	Description
Counters Supported with Cisco Unified Communications Manager Versions 5.0 and Later	
CallsActive	Number of active SIP calls. CallsActive are calls that actually have a voice path connected.
CallsAttempted	Number of calls attempted.
CallsCompleted	Number of calls for which a voice path was established.
CallsInProgress	Number of calls currently in progress (off-hook).

Cisco Software Conference Bridge Device

This counter object provides information about registered Cisco software conference bridge devices. There is one set of six counters, listed in Table B-21, for each software conference bridge device.

Table B-21 Cisco Personal Assistant Counter Object

Counter	Description
Polling for These Counters Is Controlled by Voice Utilization Settings	
ResourceActive	Number of resources currently active on this device.
ResourceAvailable	Total number of resources currently available for this software conference device.
SWConferenceCompleted	Total number of conferences that have been allocated and released on this device.
Counters Supported with Cisco Unified Communications Manager Versions Prior to 4.0	
SWConferenceActiveParticipant	Number of software-based conferences currently active on this device.
Counters Supported with Cisco Unified Communications Manager Versions 4.0 and Later	
SWConferenceActive	Number of software-based conferences currently active on this device.
ResourceTotal	Total number of resources on this device (sum of ResourceAvailable and ResourceActive).

Cisco TFTP

This counter object provides information about registered Cisco TFTP servers.

Table B-22 Cisco TFTP Counter Object

Counter	Description
HeartBeat	An incremental count that indicates whether the TFTP server is up and running. If the count does not increase, it indicates that the TFTP server is down.

Cisco Transcode Device

This counter object provides information about registered Cisco transcoding devices. There is one set of three counters, listed in Table B-25, for each transcode device.

Table B-23 Cisco Transcode Device Counter Object

Counter	Description
Polling for These Counters Is Controlled by Voice Utilization Settings	
ResourceActive	Number of resources currently active on this device.
ResourceAvailable	Total number of resources currently available for this device.
Counters Supported with Cisco Unified Communications Manager Versions 4.0 and Later	
ResourceTotal	Total number of resources on this device (sum of ResourceAvailable and ResourceActive).

Cisco Unity

This counter object provides information about registered Cisco Unity applications.

Table B-24 Cisco Unity Counter Object

Counter	Description
Total WorkingSet Memory(MB)	Maximum number of bytes in the working set of this process at any point in time. The working set is the set of memory pages recently used by the threads in the process. If the free memory in the system is above a threshold, the pages are left in the working set of the process even if they are not in use. When the free memory falls below a threshold, pages are trimmed from the working sets. If the pages are needed later, they are soft-faulted back into the working set before they leave the main memory.

Memory

This counter object provides platform memory utilization.

Note Polling for the counters in Table B-26 is controlled by Voice Utilization Settings, which are disabled by default; see Voice Utilization Settings—Polling, page 19-23.

Table B-25 Memory Counter Object

Counter	Description
Counters Supported with Cisco Unified Communications Manager Versions 5.0 and Later	
KBytesBuffered	Amount of memory buffered.
KBytesCached	Amount of memory cached.
KBytesFree	Amount of free memory.
KBytesFreeSwap	Amount of free memory swapped.
KBytesShared	Amount of memory shared.
KBytesTotal	Total memory.
KBytesTotalSwap	Total swapped memory.
KBytesUsed	Amount of memory used.
KBytesUsedSwap	Amount of swapped memory used.
Counters Supported for Cisco IP Contact Center Enterprise, Cisco Unity, and Cisco Unity Connection	
AvailableBytes	Amount of physical memory available to processes running on the system.
CacheBytes	The sum of the, System Cache Resident Bytes, System Driver Resident Bytes, System Code Resident Bytes, and Pool Paged Resident Bytes counters.
CommittedBytes	Amount of committed virtual memory. (Committed memory is physical memory for which space is reserved on the disk paging file in case it needs to be written back to the disk.)
CommitLimit	Amount of virtual memory that can be committed without having to extend the paging file.

Processor

This counter object provides CPU utilization for each processor and total CPU utilization for all processors.

Note Polling for the counters in Table B-26 is controlled by Voice Utilization Settings, which are disabled by default; see Voice Utilization Settings—Polling, page 19-23.

Table B-26 Processor Counter Object

Counter	Description
Processor(*n*)\% Processor Time	CPU utilization of processor *n*
Processor(_Total)\% Processor Time	Total CPU utilization of all processors
Counters Supported with Cisco Unified Communications Manager Versions 5.0 and Later	
CPUTime%	Percentage of CPU time used.
PercentageIdle	Percentage of CPU time idle.
PercentageSystem	Percentage of CPU time used by the system.

Table B-26 Processor Counter Object (continued)

Counter	Description
Percentage User	Percentage of CPU time used by the user.
Counters Supported for Cisco IP Contact Center Enterprise, Cisco Unity, and Cisco Unity Connection	
% Processor Time	Percentage of time that the processor is executing a non-Idle thread.

APPENDIX C

Processed and Pass-Through Traps

For some SNMP traps, Cisco Unified Operations Manager (Operations Manager) either processes them or treats them as pass-through traps.

Traps and how Operations Manager treats them are described in these topics:

Processed SNMP Traps

When Operations Manager receives certain SNMP traps, it analyzes the data found in the following fields of each SNMP trap message, and changes the property value of the object property (if required):

- Enterprise (the sysobjectID of the agent/object)
- Generic Trap Identifier
- Specific Trap Identifier
- Variable-Bindings
- IP address of the SNMP agent

Note Use Notifications to forward *specific* traps to e-mail recipients or host machines. See Chapter 15, "Using Notifications."

Multiple Processed SNMP Traps and the Event Details Displayed for Them

For every specific trap, Operations Manager generates one event (see Processed SNMP Traps and Corresponding Operations Manager Events, page C-2). For subsequent traps with the same specific trap identifier, but different object values, Operations Manager does nothing more until the trap clears. Operations Manager takes about ten minutes to clear an SNMP trap.

As a result, the Event Details display (accessible from the Alerts and Events display) shows the information obtained from the first trap that caused the event. For example, if the first trap contains Extension 101, and subsequent traps contain Extension 102 and Extension 103, Extension 101 continues to be displayed. Operations Manager updates this information only after clearing the trap and receiving the same specific trap from the device.

Processed SNMP Traps and Corresponding Operations Manager Events

This section lists the traps that Operations Manager processes and the event that Operations Manager generates for each trap.

Processed Standard SNMP Traps (RFC 1215)

SNMP Trap	Corresponding Operations Manager Event
Cold Start	RepeatedRestarts
Warm Start	
Link Up	Flapping
Link Down	

Processed CISCO-STACK-MIB Traps

SNMP Trap	Corresponding Operations Manager Event
Module Up	CardDown
Module Down	

Processed CISCO-ISDN-MIB Traps

SNMP Trap	Corresponding Operations Manager Event
demandNbrLayer2Change	OperationallyDown

Processed CISCO-NotificationEvent-MIB Traps

SNMP Trap	Corresponding Operations Manager Event
QoVMOSViolation	ServiceQualityIssue
SMLostContactWithSensor	Cisco1040SensorDown

Processed CPQHLTH-MIB Traps

SNMP Trap	Corresponding Operations Manager Event
cpqHeThermalSystemFanFailed	FanDown
cpqHeThermalSystemFanDegraded	FanDegraded
cpqHeThermalTempFailed	TemperatureSensorDown
cpqHeThermalTempDegraded	TemperatureSensorDegraded

Processed CISCO-UNITY-EXPRESS-MIB Traps

SNMP Trap	Corresponding Operations Manager Event
ciscoUnityExpressApplAlert	CUEApplicationStatusChange
ciscoUnityExpressStorageAlert	CUEStorageIssue
ciscoUnityExpressSecurityAlert	CUESecurityIssue
ciscoUnityExpressCallMgrAlert	CUECCMConnectionLost
ciscoUnityExpressRescExhausted	CUEResourceExhausted
ciscoUnityExpressBackupAlert	CUEBackupFailed
ciscoUnityExpressNTPAlert	CUENTPIssue

Processed CISCO-CCME-MIB Traps

SNMP Trap	Corresponding Operations Manager Event
ccmeEPhoneDeceased	CCMEEphoneDeceased
ccmeEphoneLoginFailed	CCMEEphoneLoginFailed
ccmeEPhoneRegFailed	CCMEEphoneRegistrationFailed
ccmeEphoneUnRegThresholdExceed	CCMEEphoneRegistrationsExceeded
ccmeKeyEphoneRegChangeNotif	CCMEKeyEphoneRegistrationChange
ccmeLivefeedMohFailedNotif	CCMELivefeedMOHFailed
ccmeMaxConferenceNotif	CCMEMaximumConferencesExceeded
ccmeNightServiceChangeNotif	CCMENightServiceChange
ccmeStatusChangeNotif	CCMEStatusChange

Processed CISCO-SRST-MIB Traps

SNMP Trap	Corresponding Operations Manager Event
csrstFailNotif	SRSTRouterFailure

Processed CISCO-CONTACT-CENTER-APPS-MIB Traps

SNMP Trap	Corresponding Operations Manager Event
cccaIcmEvent	IPCCSingleStateNotification/IPCCDualStateNotification

The following are the values (as part of trap varbinds) which Operations Manager receives as part of the trap cccaIcmEvent:

- cccaEventComponentId
- cccaEventState

- cccaEventMessageId
- cccaEventOriginatingProcessName
- cccaEventTimestamp
- cccaEventText

The value cccaEventState is used to identify whether to raise IPCCSingleStateNotification or IPCCDualStateNotification based on the following:

- Raise—A raise state identifies a notification received as a result of a health-impacting condition, such as a process failure. A subsequent clear state notification will follow when the error condition is resolved.
- SingleStateRaise—The single state raise indicates that a health-impacting error has occurred and that a subsequent clear state notification will not be forthcoming. An example of a single state raise condition is an application configuration error that requires the system to be stopped and the problem resolved by an administrator before the affected component will function properly.

For additional information on the supported list of dual state traps, see the Serviceability Best Practices Guide for Unified ICME, Unified ICMN, Unified CCE, and Unified CCH.

Pass-Through and Unidentified Traps

Pass-through traps are traps that Operations Manager does not process. Operations Manager only forwards the trap on to another Manager of Managers application. Pass-through traps are shown in the Alerts and Events display as one of the following:

- InformAlarm
- MinorAlarm
- MajorAlarm

Traps that appear in the Alerts and Events display as unidentified traps are the result of events that are generated from processed traps (see Processed SNMP Traps, page C-1) for devices that are not monitored by Operations Manager.

APPENDIX D

Notification MIB

The CISCO-EPM-NOTIFICATION-MIB specifies the trap message format Cisco Unified Operations Manager (Operations Manager) uses to generate SNMP traps when an alert occurs. The trap includes the attributes of the alert and the events that caused the alert.

This topic includes the following information:

MIB Definition

```
CISCO-EPM-NOTIFICATION-MIB DEFINITIONS ::= BEGIN

 IMPORTS

     MODULE-IDENTITY,
     NOTIFICATION-TYPE,
     Integer32,
     Unsigned32,
     Object-TYPE         FROM SNMPv2-SMI
     MODULE-COMPLIANCE,
     NOTIFICATION-GROUP,
     Object-GROUP        FROM SNMPv2-CONF
     TimeStamp           FROM SNMPv2-TC
     SnmpAdminString     FROM SNMP-FRAMEWORK-MIB
     InetAddressType,
     InetAddress         FROM INET-ADDRESS-MIB
     ciscoMgmt           FROM CISCO-SMI
     ;

 ciscoEpmNotificationMIB MODULE-IDENTITY
     LAST-UPDATED    "200406070000Z"
     ORGANIZATION    "Cisco Systems, Inc."
     CONTACT-INFO    "Cisco Systems
                      Customer Service

                      Postal: 170 W Tasman Drive
                      San Jose, CA 95134

                      Tel: +1 800 553-NETS

                      E-mail: tac@cisco.com"
     DESCRIPTION
     "Notifications directly from hardware and software and processed
     notifications from various management applications can be further
```

```
processed and forwarded by still other management applications to
indicate the status of devices and software (managed Objects).
The status of these managed Objects can be reported by traps.

The CISCO-EPM-NOTIFICATION-MIB contains the trap structure which
carries the identity and status info of the managed object as
analyzed by such an event processor. It is not possible for
receivers of these traps to query the mib Objects.

A unique but optional feature of the application generating the
trap defined in this mib is the ability to contain multiple
partitions in the same system running the application. A
'Partition' is a logical grouping of a set of managed devices.
These devices can belong to only one partition at any given
time. The trap structure will contain information on the exact
partition number and the partition name of the device where it
resides.

The need for trap generation is to enable multiple management
applications in the network to have a consolidated view of the
whole network of Cisco and non-Cisco devices."

REVISION     "200406070000Z"
DESCRIPTION
"Updated the cenAlarmEntry to include new attributes. The new
attributes carries information that adds more value to the already
existing trap structure.

The Management application computes events for a device via
polling snmp mib Objects on the device and/or by listening to
SNMP Traps. Multiple events on a single device roll up into what
is called an Alert - there can be only one alert for a given
device at any given time. The objects contained in the
cenAlarmEntry are the same for both Alert and Event based
notification. The attribute cenAlarmMode added in this revision
of the mib can be used to distinguish between the Alert based and
event based notification.

In case of event based notification, the cenAlertID would contain
the alert id, as computed by the management system, to which the
generated event has been rolled up.

Traps generated from systems that support mutiple Partition, the
cenPartitionNumber and cenPartitionName attributes will carry the
exact partition details of the device for which the trap is
generated.

Through the management application user interface, the user can
customize few attributes of the trap structure. Two attributes
included in this mib revision that allows the user to customize
each trap sent out are cenCustomerIdentification and
cenCustomerRevision.

ciscoEpmNotificationobjectsGroup, ciscoEpmNotificationAlarm, and
ciscoEpmNotificationMIBCompliance have been deprecated in this
revision.

ciscoEpmNotificationAlarmRev1,
ciscoEpmNotificationAlarmGroupRev1,
ciscoEpmNotificationMIBComplianceRev1,
and ciscoEpmNotificationobjectsGroupRev1 have been newly created
in this revision."

REVISION     "200308210000Z"
```

```
    DESCRIPTION
    "Included imports for Integer32, Unsigned32, and
    NOTIFICATION-GROUP."

    REVISION     "200207281420Z"
    DESCRIPTION
    "Initial version of this MIB."
    ::= { ciscoMgmt 311 }

-- MIB Object Definitions

ciscoEpmNotificationMIBNotifs  Object IDENTIFIER
                                ::= { ciscoEpmNotificationMIB 0 }
ciscoEpmNotificationMIBobjects Object IDENTIFIER
                                ::= { ciscoEpmNotificationMIB 1 }
ciscoEpmNotificationMIBConform Object IDENTIFIER
                                ::= { ciscoEpmNotificationMIB 2 }

cenAlarmData                   Object IDENTIFIER
                                ::= { ciscoEpmNotificationMIBobjects 1}

cenAlarmTableMaxLength    Object-TYPE
      SYNTAX              Unsigned32 ( 1..4294967295 )
      MAX-ACCESS          read-write
      STATUS              current
      DESCRIPTION
      "Maximum number of entries permissible in the cenAlarmTable."
      DEFVAL { 1 }
      ::= { cenAlarmData 1 }


cenAlarmTable             Object-TYPE
      SYNTAX              SEQUENCE OF CenAlarmEntry
      MAX-ACCESS          not-accessible
      STATUS              current
      DESCRIPTION
      "A table containing the device identification and
      alarm value. The maximum number of entries permissible
      in this table is defined by cenAlarmTableMaxLength. When
      the number of entries in the table reaches the maximum
      limit, the next entry would replace the oldest existing
      entry in the table."
      ::= { cenAlarmData 2 }

cenAlarmEntry          Object-TYPE
      SYNTAX           CenAlarmEntry
      MAX-ACCESS       not-accessible
      STATUS           current
      DESCRIPTION
      "The information regarding a single device status alarm.
      An entry is created when an alarm is processed."
      INDEX            { cenAlarmIndex }
      ::= { cenAlarmTable 1 }

CenAlarmEntry ::=
        SEQUENCE  {
           cenAlarmIndex                      Unsigned32,
           cenAlarmVersion                    SnmpAdminString,
           cenAlarmTimestamp                  TimeStamp,
           cenAlarmUpdatedTimestamp           TimeStamp,
           cenAlarmInstanceID                 SnmpAdminString,
           cenAlarmStatus                     Integer32,
           cenAlarmStatusDefinition           SnmpAdminString,
           cenAlarmType                       INTEGER,
```

```
            cenAlarmCategory                    Integer32,
            cenAlarmCategoryDefinition          SnmpAdminString,
            cenAlarmServerAddressType           InetAddressType,
            cenAlarmServerAddress               InetAddress,
            cenAlarmManagedObjectClass          SnmpAdminString,
            cenAlarmManagedObjectAddressType    InetAddressType,
            cenAlarmManagedObjectAddress        InetAddress,
            cenAlarmDescription                 OCTET STRING,
            cenAlarmSeverity                    Integer32,
            cenAlarmSeverityDefinition          SnmpAdminString,
            cenAlarmTriageValue                 Integer32,
            cenEventIDList                      OCTET STRING,
            cenUserMessage1                     SnmpAdminString,
            cenUserMessage2                     SnmpAdminString,
            cenUserMessage3                     SnmpAdminString,
            cenAlarmMode                        INTEGER,
            cenPartitionNumber                  Unsigned32,
            cenPartitionName                    SnmpAdminString,
            cenCustomerIdentification           SnmpAdminString,
            cenCustomerRevision                 SnmpAdminString,
            cenAlertID                          SnmpAdminString
          }

-- Alarm attributes

cenAlarmIndex      Object-TYPE
      SYNTAX       Unsigned32 (1..4294967295)
      MAX-ACCESS   not-accessible
      STATUS       current
      DESCRIPTION
      "A monotonically increasing integer for the sole
      purpose of indexing the attributes in
      ciscoEpmNotificationMIBObjects. When the maximum value is
      reached, this value wraps back to 1."
      ::= { cenAlarmEntry 1 }

cenAlarmVersion      Object-TYPE
        SYNTAX       SnmpAdminString (SIZE(1..16))
        MAX-ACCESS   read-only
        STATUS       current
        DESCRIPTION
        "The release version of this MIB. The version string will
        be of the form <major version>.<minorversion>."
        ::= { cenAlarmEntry 2 }

cenAlarmTimestamp      Object-TYPE
        SYNTAX         TimeStamp
        MAX-ACCESS     read-only
        STATUS         current
        DESCRIPTION
        "The time when the alarm was raised."
        ::= { cenAlarmEntry 3 }

cenAlarmUpdatedTimestamp      Object-TYPE
        SYNTAX                TimeStamp
        MAX-ACCESS            read-only
        STATUS                current
        DESCRIPTION
        "Alarms persist over time and can have their field(s)
        change values. The last time a field(s) changed, this
        alarm is updated. The updated time denotes this time.
        Each alarm is identified by the unique alarm instance
        id, cenAlarmInstanceID."
        ::= { cenAlarmEntry 4 }
```

```
cenAlarmInstanceID      Object-TYPE
        SYNTAX          SnmpAdminString (SIZE(1..20))
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
        "The Unique Alarm Instance ID."
        ::= { cenAlarmEntry 5 }

cenAlarmStatus          Object-TYPE
        SYNTAX          Integer32 (1..250)
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
        "The alarm status indicates the status of the alarm
        in integer value."
        ::= { cenAlarmEntry 6 }

cenAlarmStatusDefinition      Object-TYPE
        SYNTAX                SnmpAdminString (SIZE(1..255))
        MAX-ACCESS            read-only
        STATUS                current
        DESCRIPTION
        "The short description of the status of the alarm.
        The string is formatted in
        '<integer>,<alarmStatus description>' tuples. The <integer>
        value is the same value that the 'cenAlarmStatus'
        attribute holds. <alarmStatus description> contains one line
        description of the alarm status generated."
        ::= { cenAlarmEntry 7 }

cenAlarmType            Object-TYPE
        SYNTAX          INTEGER  {
              unknown(1),
              direct(2),
              indirect(3),
              mixed(4)
        }
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
        "unknown:  When the value for this attribute could not be
                   determined.
         direct:   Denotes an alarm generated by a set of events where
                   all events are reported by an observation(s) of a
                   managed Object.
         indirect: Denotes an alarm generated by a set of events where
                   all events were deduced or inferred by the status of
                   managed Objects as determined by the network
                   management system.
         mixed:    Denotes an alarm generated by a set of events which
                   were either direct or indirect."
        ::= { cenAlarmEntry 8 }

cenAlarmCategory        Object-TYPE
        SYNTAX          Integer32 (1..250)
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
        "The category of the alarm generated represented in
        integer value."
        ::= { cenAlarmEntry 9 }

cenAlarmCategoryDefinition    Object-TYPE
```

```
        SYNTAX                SnmpAdminString (SIZE(1..255))
        MAX-ACCESS            read-only
        STATUS                current
        DESCRIPTION
        "The short description of the category of the alarm
        generated. The String is formatted in
        '<integer>,<alarmCategory description>' tuples. The <integer>
        value is the same value that the 'cenAlarmCategory'
        attribute holds. <alarmCategory description> contains one
        line description of the alarm category generated."
        ::= { cenAlarmEntry 10 }

cenAlarmServerAddressType   Object-TYPE
        SYNTAX              InetAddressType
        MAX-ACCESS          read-only
        STATUS              current
        DESCRIPTION
        "The type of Internet address by which the server
        is reachable. The Server is the server
        that is generating this trap."
        ::= { cenAlarmEntry 11 }

cenAlarmServerAddress       Object-TYPE
        SYNTAX              InetAddress
        MAX-ACCESS          read-only
        STATUS              current
        DESCRIPTION
        "The IP Address or the DNS name of the Management
        Server that raised this alarm to be notified."
        ::= { cenAlarmEntry 12 }

cenAlarmManagedObjectClass    Object-TYPE
        SYNTAX                SnmpAdminString (SIZE(1..255))
        MAX-ACCESS            read-only
        STATUS                current
        DESCRIPTION
        "The class of the managed object for which this
        alarm was  generated. For example, Router, Switch,
        GateKeeper and VoicePort."
        ::= { cenAlarmEntry  13 }

cenAlarmManagedObjectAddressType   Object-TYPE
        SYNTAX                     InetAddressType
        MAX-ACCESS                 read-only
        STATUS                     current
        DESCRIPTION
        "The type of Internet address by which the managed
        object is reachable."
        ::= { cenAlarmEntry 14 }

cenAlarmManagedObjectAddress       Object-TYPE
        SYNTAX                     InetAddress
        MAX-ACCESS                 read-only
        STATUS                     current
        DESCRIPTION
        "The IP Address or the DNS name of the Managed Object."
        ::= { cenAlarmEntry 15 }

cenAlarmDescription          Object-TYPE
        SYNTAX               OCTET STRING (SIZE(1..1024))
        MAX-ACCESS           read-only
        STATUS               current
        DESCRIPTION
        "A detailed description of the alarm."
```

```
        ::= { cenAlarmEntry 16 }

cenAlarmSeverity        Object-TYPE
        SYNTAX          Integer32  (0..100)
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
        "The alarm severity indicates the severity of the alarm
        in integer value."
        ::= { cenAlarmEntry 17 }

cenAlarmSeverityDefinition      Object-TYPE
        SYNTAX                  SnmpAdminString (SIZE(1..255))
        MAX-ACCESS              read-only
        STATUS                  current
        DESCRIPTION
        "The short description of the severity of the alarm
        generated. The String is formatted in
        '<integer>,<alarmSeverity  description>' tuples. The <integer>
        value is the same value that the 'cenAlarmSeverity '
        attribute holds. <alarmSeverity description> contains one line
        description of the alarm severity generated."
        ::= { cenAlarmEntry 18 }

cenAlarmTriageValue     Object-TYPE
        SYNTAX          Integer32(0..100)
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
        "The triage value of an alarm is a hierarchical weighting value
        (applied by the application, and more importantly customizable
        by the end  user) to allow an artificial form of evaluating
        impact, interest, or other user-determined functions between
        alarms. The value is a positive number or zero where zero
        denotes an undetermined or uncomputable value."
        ::= { cenAlarmEntry 19 }

cenEventIDList          Object-TYPE
        SYNTAX          OCTET STRING (SIZE(1..1024))
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
        "Comma separated list of the Unique Event identifiers
        that led to the generation of this Alarm."
        ::= { cenAlarmEntry 20 }

cenUserMessage1         Object-TYPE
        SYNTAX          SnmpAdminString (SIZE(1..255))
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
        "User input message. This value can be configured."
        ::= { cenAlarmEntry 21 }

cenUserMessage2         Object-TYPE
        SYNTAX          SnmpAdminString (SIZE(1..255))
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
        "User input message. This value can be configured."
        ::= { cenAlarmEntry 22 }

cenUserMessage3         Object-TYPE
        SYNTAX          SnmpAdminString (SIZE(1..255))
```

```
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
        "User input message. This value can be configured."
        ::= { cenAlarmEntry 23 }

cenAlarmMode            Object-TYPE
        SYNTAX          INTEGER  {
              unknown(1),
              alert(2),
              event(3)
        }
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
        "unknown:  When the value for this attribute could not be
                   determined.
         alert:    Denotes an alarm generated by a set of events where
                   all events are reported by polling of managed
                   Objects and/or listening to SNMP notifications.
         event:    Denotes an event generated by polling of managed
                   ojects and/or listening to SNMP notifications."
        ::= { cenAlarmEntry 24 }

cenPartitionNumber      Object-TYPE
        SYNTAX          Unsigned32(0..100)
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
        "In traps generated by the management application that support
        multiple partitions, the attribute will carry the integer
        value assigned to identify the logical group where the managed
        device resides."
        ::= { cenAlarmEntry 25 }

cenPartitionName        Object-TYPE
        SYNTAX          SnmpAdminString (SIZE(1..255))
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
        "In traps generated by the management application that support
        multiple partitions, the attribute will carry the name
        assigned to identify the logical group where the managed
        device resides."
        ::= { cenAlarmEntry 26 }

cenCustomerIdentification      Object-TYPE
        SYNTAX                 SnmpAdminString (SIZE(1..255))
        MAX-ACCESS             read-only
        STATUS                 current
        DESCRIPTION
        "User input message. The attribute takes in a free format
        text. This attribute can be used by advanced management
        applications to sort responses from the fault management
        server."
        ::= { cenAlarmEntry 27 }

cenCustomerRevision     Object-TYPE
        SYNTAX          SnmpAdminString (SIZE(1..255))
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
        "User input message. The attribute takes in a free format
        text. This attribute can be used by advanced management
```

```
        applications to sort responses from the fault management
        server."
        ::= { cenAlarmEntry 28 }

 cenAlertID     Object-TYPE
        SYNTAX          SnmpAdminString (SIZE(1..20))
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
        "In event based notification, this attribute will contain the
        alert id to which the generated event has been rolled up
        to. In alert based notification, the cenAlarmInstanceId and
        cenAlertID would be identical."
        ::= { cenAlarmEntry 29 }

ciscoEpmNotificationAlarm    NOTIFICATION-TYPE
       ObjectS  {
                   cenAlarmVersion,
                   cenAlarmTimestamp,
                   cenAlarmUpdatedTimestamp,
                   cenAlarmInstanceID,
                   cenAlarmStatus,
                   cenAlarmStatusDefinition,
                   cenAlarmType,
                   cenAlarmCategory,
                   cenAlarmCategoryDefinition,
                   cenAlarmServerAddressType,
                   cenAlarmServerAddress,
                   cenAlarmManagedObjectClass,
                   cenAlarmManagedObjectAddressType,
                   cenAlarmManagedObjectAddress,
                   cenAlarmDescription,
                   cenAlarmSeverity,
                   cenAlarmSeverityDefinition,
                   cenAlarmTriageValue,
                   cenEventIDList,
                   cenUserMessage1,
                   cenUserMessage2,
                   cenUserMessage3
       }
       STATUS           deprecated
       DESCRIPTION
       "Notification of the status of the managed object as
       generated by the  management server.

       New attributes are added to the ciscoEpmNotificationAlarmRev1.
       Hence this notification is deprecated."
       ::= { ciscoEpmNotificationMIBNotifs 1 }

 ciscoEpmNotificationAlarmRev1    NOTIFICATION-TYPE
        OBJECTS  {
                    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
        }
        STATUS           current
        DESCRIPTION
        "Notification of the status of the managed object as
        generated by the  management server."
        ::= { ciscoEpmNotificationMIBNotifs 2 }


-- Conformance information

ciscoEpmNotificationMIBCompliances Object IDENTIFIER
                          ::= { ciscoEpmNotificationMIBConform 1 }
ciscoEpmNotificationMIBGroups Object IDENTIFIER
                          ::= { ciscoEpmNotificationMIBConform 2 }
-- Compliance

ciscoEpmNotificationMIBCompliance MODULE-COMPLIANCE
        STATUS deprecated
        DESCRIPTION
        "The compliance statement for entities which
        implement the CISCO-EPM-NOTIFICATION-MIB.


        New attributes are included in
        ciscoEpmNotificationMIBComplianceRev1. Hence this object is
        deprecated."
        MODULE -- this module
        MANDATORY-GROUPS {
            ciscoEpmNotificationObjectsGroup,
            ciscoEpmNotificationAlarmGroup
        }

        GROUP       ciscoEpmAlarmConfigGroup
        DESCRIPTION
        "This group is optional."

       OBJECT         cenAlarmTableMaxLength
         MIN-ACCESS read-only
         DESCRIPTION
         "Write access is not required."

         OBJECTcenAlarmVersion
         MIN-ACCESS accessible-for-notify
         DESCRIPTION
             "Read access is not required."

         OBJECT  cenAlarmTimestamp
         MIN-ACCESS accessible-for-notify
         DESCRIPTION
```

```
    "Read access is not required."

OBJECT  cenAlarmUpdatedTimestamp
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT  cenAlarmInstanceID
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT  cenAlarmStatus
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT  cenAlarmStatusDefinition
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT  cenAlarmType
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT  cenAlarmCategory
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT  cenAlarmCategoryDefinition
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT  cenAlarmServerAddressType
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT  cenAlarmServerAddress
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT  cenAlarmManagedObjectClass
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT  cenAlarmManagedObjectAddressType
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT  cenAlarmManagedObjectAddress
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT  cenAlarmDescription
MIN-ACCESS accessible-for-notify
```

```
        DESCRIPTION
            "Read access is not required."

        OBJECT  cenAlarmSeverity
        MIN-ACCESS accessible-for-notify
        DESCRIPTION
            "Read access is not required."

        OBJECT  cenAlarmSeverityDefinition
        MIN-ACCESS accessible-for-notify
        DESCRIPTION
            "Read access is not required."

        OBJECT  cenAlarmTriageValue
        MIN-ACCESS accessible-for-notify
        DESCRIPTION
            "Read access is not required."

        OBJECT  cenEventIDList
        MIN-ACCESS accessible-for-notify
        DESCRIPTION
            "Read access is not required."

        OBJECT  cenUserMessage1
        MIN-ACCESS accessible-for-notify
        DESCRIPTION
            "Read access is not required."

        OBJECT     cenUserMessage2
        MIN-ACCESS accessible-for-notify
        DESCRIPTION
            "Read access is not required."

        OBJECT     cenUserMessage3
        MIN-ACCESS accessible-for-notify
        DESCRIPTION
            "Read access is not required."
        ::= { ciscoEpmNotificationMIBCompliances  1 }

ciscoEpmNotificationMIBComplianceRev1 MODULE-COMPLIANCE
        STATUS current
        DESCRIPTION
        "The compliance statement for entities which
        implement the CISCO-EPM-NOTIFICATION-MIB."
        MODULE -- this module
        MANDATORY-GROUPS {
            ciscoEpmNotificationObjectsGroupRev1,
            ciscoEpmNotificationAlarmGroupRev1
        }

        GROUP       ciscoEpmAlarmConfigGroup
        DESCRIPTION
        "This group is optional."

        OBJECT     cenAlarmTableMaxLength
        MIN-ACCESS read-only
        DESCRIPTION
        "Write access is not required."

        OBJECT     cenAlarmVersion
        MIN-ACCESS accessible-for-notify
        DESCRIPTION
            "Read access is not required."
```

```
OBJECT     cenAlarmTimestamp
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenAlarmUpdatedTimestamp
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenAlarmInstanceID
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenAlarmStatus
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenAlarmStatusDefinition
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenAlarmType
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenAlarmCategory
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenAlarmCategoryDefinition
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenAlarmServerAddressType
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenAlarmServerAddress
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenAlarmManagedObjectClass
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenAlarmManagedObjectAddressType
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenAlarmManagedObjectAddress
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."
```

```
OBJECT     cenAlarmDescription
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenAlarmSeverity
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenAlarmSeverityDefinition
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenAlarmTriageValue
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenEventIDList
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenUserMessage1
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenUserMessage2
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenUserMessage3
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenAlarmMode
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenPartitionNumber
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenPartitionName
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenCustomerIdentification
MIN-ACCESS accessible-for-notify
DESCRIPTION
    "Read access is not required."

OBJECT     cenCustomerRevision
MIN-ACCESS accessible-for-notify
DESCRIPTION
```

```
            "Read access is not required."

        OBJECT     cenAlertID
        MIN-ACCESS accessible-for-notify
        DESCRIPTION
            "Read access is not required."

        ::= { ciscoEpmNotificationMIBCompliance  2 }

-- Units of Conformance

ciscoEpmNotificationAlarmGroup NOTIFICATION-GROUP
    NOTIFICATIONS {
        ciscoEpmNotificationAlarm
    }
    STATUS      deprecated
    DESCRIPTION
    "The collection of notifications used to indicate managed
    object status.

    ciscoEpmNotificationAlarmGroupRev1 is defined. Hence this
    object is deprecated."
    ::= { ciscoEpmNotificationMIBGroups 1 }

ciscoEpmNotificationObjectsGroup    Object-GROUP
    ObjectS {
                    cenAlarmVersion,
                    cenAlarmTimestamp,
                    cenAlarmUpdatedTimestamp,
                    cenAlarmInstanceID,
                    cenAlarmStatus,
                    cenAlarmStatusDefinition,
                    cenAlarmType,
                    cenAlarmCategory,
                    cenAlarmCategoryDefinition,
                    cenAlarmServerAddressType,
                    cenAlarmServerAddress,
                    cenAlarmManagedObjectClass,
                    cenAlarmManagedObjectAddressType,
                    cenAlarmManagedObjectAddress,
                    cenAlarmDescription,
                    cenAlarmSeverity,
                    cenAlarmSeverityDefinition,
                    cenAlarmTriageValue,
                    cenEventIDList,
                    cenUserMessage1,
                    cenUserMessage2,
                    cenUserMessage3
    }
    STATUS      deprecated
    DESCRIPTION
    "Trap reflecting the alarm.

    New attributes are added to the new notification
    ciscoEpmNotificationObjectsGroupRev1. Hence
    this object is deprecated."
    ::= { ciscoEpmNotificationMIBGroups   2 }

ciscoEpmAlarmConfigGroup    Object-GROUP
    ObjectS { cenAlarmTableMaxLength }
    STATUS      current
    DESCRIPTION
    "A collection of Objects providing information
    about the total number of cenAlarmTable entries
```

```
    maintained."
    ::= { ciscoEpmNotificationMIBGroups   3 }

ciscoEpmNotificationAlarmGroupRev1 NOTIFICATION-GROUP
    NOTIFICATIONS {
        ciscoEpmNotificationAlarmRev1
    }
    STATUS      current
    DESCRIPTION
    "The collection of notifications used to indicate managed Object
    status."
    ::= { ciscoEpmNotificationMIBGroups 4 }

ciscoEpmNotificationObjectsGroupRev1    Object-GROUP
    ObjectS {
                    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
    }
    STATUS      current
    DESCRIPTION
    "Notification reflecting the alarm."
    ::= { ciscoEpmNotificationMIBGroups   5 }

END
```

cenAlarmEntry Object-Type—Definitions for Selected Attributes

Table D-1 explains the values for attributes related to alert status, category, and severity. You might find it useful to consult this information when you look at a generated trap.

Table D-1 CenAlarmEntry—Alert Status, Category, and Severity

Sequence Numbers	Attributes	Values
(6)	cenAlarmStatus	Number—From 1 to 3.
(7)	cenAlarmStatusDefinition	String—Includes number (cenAlarmStatus) and description: 1-Acknowledged 2-Active 3-Cleared **Note** Alert status changes from state to state: state is Active; if user acknowledges alert, state is Acknowledged; ultimately, state is Cleared. For more information about alerts, see Chapter 3, "Monitoring Alerts and Events."
(9)	cenAlarmCategory	Number—From 0 to 9.
(10)	cenAlarmCategoryDefinition	String—Includes number (cenAlarmCategory) and description: 0-Unknown 1-Application 2-Environment 3-Interface 4-Reachability 5-Connectivity 6-Utilization 7-System Hardware 8-Security 9-Other
(17)	cenAlarmSeverity	Number—From 1 to 3.
(18)	cenAlarmSeverityDefinition	String—Includes number (cenAlarmSeverity) and description: 1-Informational 2-Warning 3-Critical

cenUserMessage1 Object-Type—Attribute with Partition Information

Operations Manager stores the partition number and alias for the identified device in the cenUserMessage1 Object-type. The partition number and alias are separated by a colon; for example, Partition 1: Enterprise1. This information is no longer relevant.

CHAPTER E

Events Processed

This section covers the following topics:

Event Information

Operations Manager is now configured as a Cisco Communications Manager remote syslog receiver for Cisco CallManager (or referred to in later releases, Unified Communications Manager), Call Detail Records (CDR), Disaster Recovery Framework (DRF), and AONS Management Console (AMC) services.

Table E-1 lists all possible events you might see on a Monitoring Dashboard, along with the following:

- Description—A summary of the event, including typical causes (if known).
- Trigger—How Cisco Unified Operations Manager (Operations Manager) learns of the event: from normal polling, from RTMT, syslog that was received, a threshold that was exceeded, a diagnostic test result, a trap that was received, or an event received from Windows Event Manager. For a list of thresholds and events that they trigger, see Table 19-15.
- Severity—The severity that Operations Manager assigns to the event: critical, warning, or informational.
- Device Type—The devices, as classified in Operations Manager, on which the event can occur.
- Clear Interval—The interval at which the event is cleared from the Alert Detail View by Operations Manager. Some syslog-based events have a predetermined clear interval. Upon reaching the expiry of the clear interval, Operations Manager moves the events from active to cleared. (For more information, see Responding to Events Using the Alert Details Page, page 3-31.)
- Event Code—The code used by Notifications to track changes to default Operations Manager event names using the Notification event customization feature. (For more information, see Customizing Events, page 15-23.)

Some events are no longer available for monitoring and have been obsoleted. See Obsolete Events, page E-33 for a list. If you use any of these obsoleted events, refer to the equivalent events that can be used instead of the obsoleted ones.

Events listed in Table E-1 are displayed on:

- The Alert Details page—Shows the majority of events generated. Event names correspond to those displayed in the Description column of the Alert Details page.
- The Phone Activities display—Shows information about the IP phones in your network that have become disconnected from the switch, are no longer registered to a Cisco Unified Communications Manager, or have gone into SRST mode. The following events cause activity to be displayed on the Phone Activities display:
  - SRSTEntered
  - SRSTSuspected
- The Service Quality Alerts display—Shows events generated as a result of traps received from Service Monitor. The following events cause activity to be displayed on the Service Quality Alerts display:
  - CriticalServiceQualityIssue
  - MultipleServiceQualityIssue
  - ServiceQualityIssue

Note The Cisco1040SensorDown event is also generated as a result of traps received from Service Monitor. However, Cisco1040SensorDown appears under Unidentified Trap.

Supported Events

Table E-1 lists the events supported by Operations Manager.

Table E-1 Events that Operations Manager Supports

Event	Description, Cause, Severity and Event Code
AvailableInboxLicenseLow	**Description**: Number of available inbox licenses are fewer than the threshold. **Trigger**: Fell below Unity Inbox License Threshold. **Severity**: Critical. **Device Type**: Media Server. **Event Code**: 2103.
AvailableLicenseLow	**Description**: The number of available Unity licenses are fewer than the threshold. **Trigger**: Fell below Unity License Threshold. **Severity**: Critical. **Device Type**: Media Server. **Event Code**: 2104.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
AverageLatency_ThresholdExceeded	**Description**: The average latency for a node-to-node UDP Jitter for VoIP test exceeds the threshold set for the test. **Trigger**: Node-to-node test. **Severity**: Warning. **Device Type**: Router or Switch. **Event Code**: 4004.
Authentication Failed	**Description**: Occurs when there is authentication failure in a login attempt. **Trigger**: Polling. **Severity**: Warning. **Device Type**: Unified Communications Manager version 6.x or later. **Clear Interval:** Time-based auto clear in Event Promulgation Module (EPM) after 30 minutes. **Event Code**: 7006.
BackupActivated	**Description**: Backup port or interface has come online, indicating that the port or interface it backs up has gone down. **Trigger**: Polling. **Severity**: Warning. **Device Type**: Host, Hub, Router, Optical Switch, or Switch. **Event Code**: 1000.
CCMEDown	**Description**: The Cisco Unified Communications Manager Express application is down. This could be due to some problem in the application or device. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Router. **Event Code**: 2038. For Cisco Unified Communications Manager, see CallManagerDown.
CCMEEphoneDeceased	**Description**: The state of an ephone registered to Cisco Unified Communications Manager Express changed to deceased. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Warning. **Device Type**: Router or VoiceGateway. **Event Code**: 2076.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
CCMEEphoneLoginFailed	**Description**: An ephone login to Cisco Unified Communications Manager Express was rejected or failed. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Warning. **Device Type**: Router or VoiceGateway. **Event Code:** 2078.
CCMEEphoneRegistrationFailed	**Description**: An ephone attempted to register with Cisco Unified Communications Manager Express and failed. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Warning. **Device Type**: Router or VoiceGateway. **Event Code**: 2077.
CCMEEphoneUnregistrationsExceeded	**Description**: The number of ephones registered to Cisco Unified Communications Manager Express was exceeded. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Critical. **Device Type**: Router or VoiceGateway. **Event Code**: 2075.
CCMEKeyEphoneRegistrationChange	**Description**: Registration status changed for a key IP ephone with respect to Cisco Unified Communications Manager Express. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Warning. **Device Type**: Router or VoiceGateway. **Event Code**: 2080.
CCMELivefeedMOHFailed	**Description**: Music on hold (MOH) live feed failed on Cisco Unified Communications Manager Express. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Warning. **Device Type**: Router or VoiceGateway. **Event Code**: 2074.
CCMEMaximumConferencesExceeded	**Description**: Maximum number of simultaneous three-party conferences supported was exceeded on Cisco Unified Communications Manager Express. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Warning. **Device Type**: Router or VoiceGateway. **Event Code**: 2073.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
CCMENightServiceChange	**Description**: Night service status changed on an ephone registered to Cisco Unified Communications Manager Express. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Critical. **Device Type**: Router or VoiceGateway. **Event Code**: 2079.
CCMEStatusChange	**Description**: Cisco Unified Communications Manager Express enabled state has changed. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Warning. **Device Type**: Router or VoiceGateway. **Event Code**: 2072.
CCMHttpServiceDown	**Description**: HTTP service cannot be used to communicate to all Cisco Unified Communications Managers in the cluster. This might be due to the following: • The web service for all Cisco Unified Communications Managers in the cluster is down. • The credentials (username, password) for at least one of the running web services were not found or are incorrect. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Cisco Unified Communications Manager or cluster. **Event Code**: 2009.
CDR Agent Send File Failed Supports Unified Communications Manager version 5.x or later in Syslog/RTMT.	**Description**: The CDR Agent cannot send CDR files from a Communications Manager node to the CDR Repository node within the Communications Manager cluster. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Communications Manager. **Clear Interval:** Time-based auto clear in EPM after 60 minutes. **Event Code**: 7010.
CDR File Delivery Failed Supports Unified Communications Manager version 5.x or later in Syslog/RTMT.	**Description**: The FTP delivery of CDR files to the outside billing server failed. **Trigger**: Polling. **Severity**: Warning. **Device Type**: Communications Manager. **Clear Interval:** Time-based auto clear in EPM after 60 minutes. **Event Code**: 7011.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
CDR High Water Mark Exceeded Supports Unified Communications Manager version 5.1.3 or later in Syslog/RTMT.	**Description**: The High Water Mark for CDR files has been reached and some successfully delivered CDR files have been deleted. **Trigger**: Polling. **Severity**: Warning. **Device Type**: Communications Manager. **Clear Interval:** Time-based auto clear after 30 minutes. **Event Code**: 7014.
CDR Maximum Disk Space Exceeded Supports Unified Communications Manager version 5.x or later in Syslog/RTMT.	**Description**: The CDR files disk usage has exceeded the maximum disk allocation. Some undelivered files have been deleted. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Communications Manager. **Clear Interval:** Time-based auto clear in EPM after 60 minutes. **Event Code**: 7008.
Cisco1040SensorDown	**Description**: A Cisco 1040 has stopped responding to keepalives from Service Monitor. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Critical. **Device Type**: Unidentified Trap (because Operations Manager does not monitor Cisco 1040.) **Event Code**: 8004. This event appears on the Alert Details page and can be generated only when you have a licensed copy of Service Monitor.
Cisco DRF Failure Supported for CCM 5.x and later.	**Description**: The DRF backup or restore process has encountered errors. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Communications Manager. **Clear Interval:** Time-based auto clear in EPM after 4 days. **Event Code**: 7007.
Code Red	**Description:** Cisco Unified Communications Manager has entered Code Red state (call-throttling mode) due to unacceptably high delay in handling incoming calls. **Trigger**: Syslog. **Severity**: Critical. **Device Type**: Cisco Unified Communications Manager or cluster. **Clear Interval:** Time-based auto clear in Event Promulgation Module (EPM) after 4 days. **Event Code:** 2048.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
Code Yellow	**Description**: Cisco Unified Communications Manager has entered Code Yellow state (call-throttling mode) due to an unacceptably high delay in handling incoming calls. **Trigger**: Syslog. **Severity**: Critical. **Device Type**: Cisco Unified Communications Manager or cluster. **Event Code**: 2049.
Code Yellow	**Description**: Cisco Unified Communications Manager call-throttling terminates when the delay in handling incoming calls falls below the exit latency. **Trigger**: Syslog. **Severity**: Informational. **Device Type**: Cisco Unified Communications Manager or cluster. **Event Code**: 2049.
ComponentDown	**Description**: A component within IPCC is down. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Media Server. **Event Code**: 2039.
Core Dump File Found Supports Unified Communications Manager version 5.1.3 or later in Syslog/RTMT.	**Description**: This indicates that a core dump file has been found in the system. **Trigger**: RTMT. **Severity**: Critical. **Device Type**: Cisco Unified Communications Manager or cluster. **Clear Interval:** Time-based auto clear in EPM after 4 days. **Event Code**: 7009.
CPALoginFailureThresholdExceeded	**Description**: The number of failed Cisco Personal Assistant logins that exceeded the limit. **Trigger**: Exceeded the CPA Login Failure threshold. **Severity**: Critical. **Device Type**: Media Server. **Event Code**: 2086.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
CPATransferFailedThresholdExceeded	**Description**: Number of times that Cisco Personal Assistant tried and failed to transfer a call. **Trigger**: Exceeded the CPA Transfer Failed threshold. **Severity**: Critical. **Device Type**: Media Server. **Event Code**: 2087.
CPAVoicemailThresholdExceeded	**Description**: The number of times callers tried to access voice mail but failed, or the number of voicemail login failures that exceeded the limit. **Trigger**: Exceeded the CPA Voice Mail threshold. **Severity**: Critical. **Device Type**: Media Server. **Event Code**: 2088.
CPUPegging	**Description**: The percentage of CPU load on a server is over the configured percentage for the configured period of time. **Trigger**: RTMT. **Severity**: Critical. **Device Type**: Communications Manager or cluster. **Event Code**: 1013. 2126.
cpuUtilizationExceeded	**Description**: CPU utilization of the voice service or the system exceeded the limit. **Trigger**: Exceeded the CPU Utilization threshold. **Severity**: Warning. **Device Type**: Media Server. **Event Code**: 2085.  **Note** Events are removed for CCM only. You may need to manually clear these CCM events after your upgrade is complete.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
CriticalServiceQualityIssue	**Description:** Operations Manager has received a MOS violation trap from Service Monitor and MOS has fallen below the value set on the Event Settings page. See Configuring Service Quality Event Settings, page 20-7. **Trigger:** Event settings. See Configuring Service Quality Event Settings, page 20-7. **Severity:** Critical. **Device Type**: Service Quality events pertain to the call destination, which might be a device (Voice Gateway) or a phone. **Event Code:** 8002. **Note** This event is shown on the Service Quality Alert Details display. (See Using the Service Quality Alerts Display, page 4-3.) This event can be generated only when you have a licensed copy of Service Monitor.
CTILinkDown	**Description**: An active link between CTI Manager and Cisco Unified Communications Manager is down. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Media Server. **Event Code**: 2096.
CUEApplicationStatusChange	**Description**: An application on Cisco Unity Express has come online or gone offline. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Warning. **Device Type**: Router. **Event Code**: 2063.
CUEBackupFailed	**Description**: Cisco Unity Express backup failed. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Critical. **Device Type**: Router. **Event Code**: 2068.
CUECCMConnectionLost	**Description**: Cisco Unity Express has lost connection with Cisco Unified Communications Manager. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Critical. **Device Type**: Router. **Event Code**: 2066.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
CUENTPIssue	**Description**: Cisco Unity Express is affected by a problem with NTP. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Warning. **Device Type**: Router. **Event Code**: 2069.
CUEResourceExhausted	**Description**: A Cisco Unity Express resource has been exhausted. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Critical. **Device Type**: Router. **Event Code**: 2067.
CUESecurityIssue	**Description**: Cisco Unity Express is affected by a problem with security. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Warning. **Device Type**: Router. **Event Code**: 2064.
CUEStorageIssue	**Description**: Cisco Unity Express is affected by a problem with storage. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Warning. **Device Type**: Router. **Event Code**: 2065.
DataPhysicalDiskDown	**Description**: Drive down on Cisco Unified Communications Manager. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Media Server. **Event Code**: 2060.
DB Replication Failure Supports Unified Communications Manager version 5.1.3 or later in RTMT polling. For Unified Communications Manager version 5.0 to 5.1.2 the event name is IDS Replication Failure. Version 4.x is no longer supported.	**Description**: A subscriber in a Cisco Unified Communications Manager cluster experienced a failure while replicating the data to the publisher database. This event needs to be manually cleared to delete it. **Trigger**: RTMT. **Severity**: Critical. **Device Type**: Media Server. **Clear Interval:** Time-based auto clear after 4 days. **Event Code**: 2091.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
D Channel Out of Service	**Description**: The connection to the voice gateway is out of service. **Trigger**: Syslog. **Severity**: Critical. **Device Type**: Voice Gateway. **Clear Interval:** Time-based auto clear after 4 days. **Event Code**: 7021.
DPAPortCallManager LinkDown	**Description**: No connectivity between the DPA port and Cisco Unified Communications Manager. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Voice Mail Gateway. **Event Code**: 2013.
DPAPortTelephonyLinkDown	**Description**: No connectivity between the DPA port and Octel voice mail. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Voice Mail Gateway. **Event Code**: 2014.
Duplicate	**Description**: Same IP address is configured on multiple managed systems. **Trigger**: Polling (often during rediscovery). **Severity**: Critical. **Device Type**: Host, Hub, Router, Optical Switch, or Switch. **Event Code**: 1001.
ExcessiveFragmentation	**Description**: System memory is highly fragmented. **Trigger**: Exceeded Memory Fragmentation Threshold. **Severity**: Critical. **Device Type**: Host, Router, Switch, or Optical Switch. **Event Code**: 1003.
ExpertAdvisorSystemDown	**Description:** This alarm is generated when any of the subsystems of Expert Advisor is down. **Trigger:** Polling. **Severity:** Critical. **Device Type:** Media Server. **Event Code:** 2112.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
FanDegraded	**Description**: Fan condition is Degraded. **Trigger**: Polling, or processed trap (see Processed SNMP Traps, page C-1). **Severity**: Warning. **Device Type**: Media Server or Voice Gateway. **Event Code**: 2015.
FanDown	**Description**: Fan condition is Down. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Critical. **Device Type**: Media Server or Voice Gateway. **Event Code**: 2016.
Flapping	**Description**: Port or interface is repeatedly alternating between Up and Down states over a short period of time. Operations Manager issues this event by monitoring the number of link downs received within the link window for a particular network adapter (using the Link threshold and Link Window parameters). **Trigger**: Exceeded Link Trap Threshold for Link Trap Window; or processed trap (see Processed SNMP Traps, page C-1). **Severity**: Critical. **Device Type**: Host, Hub, Router, Optical Switch, or Switch. **Event Code**: 1004.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
HighAnalogPortUtilization	**Description**: Percentage utilization of an analog port has exceeded a threshold. **Trigger**: Exceeded one of these thresholds: • Cisco Unified Communications Manager Analog Port Utilization. – FXS Port Utilization Threshold. – FXO Port Utilization Threshold. • MGCP Gateway Analog Port Utilization. – FXS Port Utilization Threshold. – FXO Port Utilization Threshold. • H323 Gateway Analog Port Utilization. – FXS Port Utilization Threshold. – FXO Port Utilization Threshold. – EM Port Utilization Threshold. **Note** You must enable polling for Voice Utilization Settings to monitor this event. **Severity**: Critical. **Device Type**: Media Server or Voice Gateway. **Event Code**: 4100.
HighBackplaneUtilization	**Description**: Utilization of the backplane's bandwidth exceeds the backplane utilization threshold. **Trigger**: Exceeded Backplane Utilization Threshold. **Severity**: Critical. **Device Type**: Host, Router, Switch, or Optical Switch. **Event Code**: 1005.
HighBroadcastRate	**Description**: Input packet broadcast percentage exceeds the Broadcast threshold. The input packet broadcast percentage calculates the percentage of total capacity that was used to receive broadcast packets. **Trigger**: Exceeded Broadcast Threshold. **Severity**: Critical. **Device Type**: Host, Router, Switch, or Optical Switch. **Event Code**: 1006.
HighBufferMissRate	**Description**: Rate of buffer misses exceeds the Memory Buffer Miss Threshold. **Trigger**: Exceeded Memory Buffer Miss Threshold. **Severity**: Critical. **Device Type**: Host, Router, Switch or Optical Switch. **Event Code**: 1007.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
HighBufferUtilization	**Description**: Number of buffers used exceeds the Memory Buffer Utilization Threshold. **Trigger**: Exceeded Memory Buffer Utilization Threshold. **Severity**: Critical. **Device Type**: Host, Router, Switch, or Optical Switch. **Event Code**: 1008.
HighCollisionRate	**Description**: Rate of collisions exceeds the Collision Threshold. **Trigger**: Exceeded Collision Threshold. **Severity**: Critical. **Device Type**: Host, Hub, Router, Switch, or Optical Switch. **Event Code**: 1009.
HighDigitalPortUtilization	**Description**: Percentage utilization of a digital port has exceeded a threshold. **Trigger**: Exceeded one of these thresholds: • Cisco Unified Communications Manager Digital Port Utilization – BRI Channel Utilization Threshold. – T1 PRI Channel Utilization Threshold. – E1 PRI Channel Utilization Threshold. – T1 CAS Channel Utilization Threshold. • MGCP Gateway Digital Port Utilization. – BRI Channel Utilization Threshold. – T1 PRI Channel Utilization Threshold. – E1 PRI Channel Utilization Threshold. – T1 CAS Channel Utilization Threshold. • H323 Gateway Digital Port Utilization. – BRI Channel Utilization Threshold. – T1 PRI Channel Utilization Threshold. – E1 PRI Channel Utilization Threshold. – T1 CAS Channel Utilization Threshold. – E1 CAS Channel Utilization Threshold. **Note** You must enable polling for Voice Utilization Settings to monitor this event. **Severity**: Critical. **Device Type**: Media Server or Voice Gateway. **Event Code**: 4101.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
HighDiscardRate	**Description**: A HighDiscardRate event occurs when: • The input packet queued rate is greater than the minimum packet rate, and the input packet discard percentage is greater than the Discard Threshold. The input packet queued rate is the rate of packets received without error. The input packet discard percentage is calculated by dividing the rate of input packets discarded by the rate of packets received. • The output packet queued rate is greater than the minimum packet rate, and the output packet discard percentage is greater than the Discard Threshold. The output packet queued rate is the rate of packets sent without error. The output packet discard percentage is calculated by dividing the rate of output packets discarded by the rate of packets sent. **Trigger**: Exceeded Discard Threshold. **Severity**: Critical. **Device Type**: Host, Hub, Router, Switch, or Optical Switch. **Event Code**: 1010.
HighErrorRate	**Description**: A HighErrorRate event occurs for input or output packets when both of the following thresholds are exceeded: • Error Threshold—Percentage of packets in error. • Error Traffic Threshold—Percentage of bandwidth in use. **Trigger**: Exceeded Error Threshold and equaled or exceeded Error Traffic Threshold. **Severity**: Critical. **Device Type**: Host, Hub, Router, Switch, or Optical Switch. **Event Code**: 1011.
HighPortUtilization	**Description**: Percentage of port utilization exceeds a threshold. **Note** You must enable polling for Voice Utilization Settings to monitor this event. **Trigger**: Exceeded one of these thresholds: • Voice Mail Gateway Port Utilization. – Voice Mail Port Utilization Threshold. – PBX Port Utilization Threshold. **Severity**: Critical. **Device Type**: Media Server or Voice Mail Gateway. **Event Code**: 4102.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
HighResourceUtilization	**Description**: A hardware resource threshold has been exceeded. **Trigger**: Exceeded one of these thresholds: • Cisco Unified Communications Manager Resource Utilization – MOH Multicast Resources Active Threshold. – MOH Unicast Resources Active Threshold. – MTP Resources Active Threshold. – Transcoder Resources Active Threshold. – Hardware Conference Resources Active Threshold. – Software Conference Resources Active Threshold. – Conferences Active Threshold. – Conference Streams Active Threshold. – MOH Streams Active Threshold. – MTP Streams Active Threshold. – Location Bandwidth Available Threshold. • H323 Gateway Resource Utilization. – DSP Utilization Threshold. • Gatekeeper Resource Utilization. – Total Bandwidth Utilization for Local Zone Threshold. – Interzone Bandwidth Utilization for Local Zone Threshold. • Cisco Unified Communications Manager Express Utilization. – Registered IP Phones Threshold. – Registered Key IP Phones Threshold. • Cisco Unity Express Utilization. – Capacity Utilization Threshold. – Session Utilization Threshold. – Orphaned Mailboxes Threshold. **Note** You must enable polling for Voice Utilization Settings to monitor this event. **Severity**: Critical. **Device Type**: Cisco Unified Communications Manager or cluster, Gatekeeper, Media Server, Router, or Voice Gateway. **Event Code**: 4103.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
HighUtilization	**Description**: Current utilization exceeds the utilization threshold configured for this network adapter or processor. **Trigger**: Exceeded one of these thresholds: • Utilization Threshold. • Processor Utilization Threshold. **Severity**: Critical. **Device Type**: Host, Media Server, Router, Switch, Optical Switch, or Voice gateway. **Event Code**: 1013.
ICT Call Throttling	**Description**: Cisco Unified Communications Manager has resumed normal state and starts accepting calls for the indicated H323 device. **Trigger**: Syslog. **Severity**: Informational. **Device Type**: Communications Manager or cluster.
ICT Call Throttling	**Description**: Cisco Unified Communications Manager has detected a route loop over H323 trunk. As a result, it has temporarily stopped accepting calls for the indicated H323 device. **Trigger**: Syslog. **Severity**: Informational. **Device Type**: Communications Manager or cluster.
IdeAtaDiskDown	**Description**: IDE/ATA drive down on Cisco Unified Communications Manager. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Media Server. **Event Code**: 2062.
IDS Replication Failure Supports Unified Communications Manager version 5.0 to 5.1.2 or later in Syslog/RTMT.	**Description**: A subscriber in a Cisco Unified Communications Manager cluster experienced a failure while replicating the data to the publisher database. This event needs to be manually cleared to delete it. **Trigger**: RTMT. **Severity**: Critical. **Device Type**: Media Server. **Clear Interval:** Time-based auto clear after 4 days. **Event Code**: 2091.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
InformAlarm	**Description**: An informational pass-through trap was generated. **Trigger**: Pass-through trap. See Pass-Through and Unidentified Traps, page C-4. **Severity**: Informational. **Event Code**: 1014.
InsufficientFreeHardDisk	**Description**: Free disk space is low. **Trigger**: Exceeded Free Hard Disk Threshold. **Severity**: Critical. **Device Type**: Media Server. **Event Code**: 2020. See also InsufficientFreeMemory, InsufficientFreePhysicalMemory, InsufficientFreeVirtualMemory. **Note** Events are removed for Unified Communications Manager only. You may need to manually clear these CCM events after your upgrade is complete.
InsufficientFreeMemory	**Description**: System is running out of memory resources. Also reported if there has been a failure to allocate a buffer due to lack of memory. **Trigger**: Exceeded Free Memory Threshold. **Severity**: Critical. **Device Type**: Host, Media Server, Router, Switch, or Optical Switch. **Event Code**: 1015. See also InsufficientFreeHardDisk, InsufficientFreePhysicalMemory, InsufficientFreeVirtualMemory. **Note** Events are removed for CCM only. You may need to manually clear these CCM events after your upgrade is complete.
InsufficientFreePhysicalMemory	**Description**: System is running out of physical memory resources. **Trigger**: Exceeded Free Physical Memory Threshold. **Severity**: Critical. **Device Type**: Voice Gateway. **Event Code**: 2021. See also InsufficientFreeHardDisk, InsufficientFreeMemory, InsufficientFreeVirtualMemory. **Note** Events are removed for CCM only. You may need to manually clear these CCM events after your upgrade is complete.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
InsufficientFreeVirtualMemory	**Description**: System is running out of virtual memory resources. **Trigger**: Exceeded Free Virtual Memory Threshold. **Severity**: Critical. **Event Code**: 2022. **Device Type**: Media Server. See also InsufficientFreeHardDisk, InsufficientFreeMemory, InsufficientFreePhysicalMemory. **Note** Events are removed for CCM only. You may need to manually clear these CCM events after your upgrade is complete.
InterfaceOperationallyDown	**Description**: Interface is nonoperational. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Digital Voice Gateway, Media Server, or Voice Gateway. **Event Code**: 2023. See also OperationallyDown, page E-24.
IPCCDualStateNotification	**Description**: The Unified Contact Center sent a notification with a value of cccaEventState in the trap details. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Warning. **Device Type**: Media Server. **Event Code**: 2070.
IPCCSingleStateNotification	**Description:** The Unified Contact Center sent a notification with a value of singleStateRaise for ccaEventState in the trap details. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Warning. **Device Type**: Media Server. **Event Code**: 2070.
JitterDS_ThresholdExceeded	**Description**: Jitter exceeds the node-to-node test threshold. **Trigger**: Node-to-node test. **Severity**: Warning. **Device Type**: Router or Switch. **Event Code**: 4008. For more information, see Using Node-To-Node Tests, page 11-1.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
JitterSD_ThresholdExceeded	**Description**: Jitter exceeds the node-to-node test threshold. **Trigger**: Node-to-node test. **Severity**: Warning. **Device Type**: Router or Switch. **Event Code**: 4007. For more information, see Using Node-To-Node Tests, page 11-1.
LocationBWOutOfResources	**Description**: A call through a Cisco Unified Communications Manager location failed due to lack of bandwidth. **Trigger**: Exceeded Location Out of Resources Threshold. **Severity**: Critical. **Device Type**: Media Server. **Event Code**: 2094.
LogPartitionHighWatermarkExceeded Supports Unified Communications Manager version 5.x or later in Syslog/RTMT.	**Description**: The percentage of used disk space in the log partition has exceeded the configured high-water mark. **Trigger**: Exceeded high-water mark threshold. **Severity**: Informational. **Device Type**: Communications Manager. **Event Code**: 2132.
LogPartitionLowWatermarkExceeded Supports Unified Communications Manager version 5.x or later in Syslog/RTMT.	**Description**: Free disk space is low. The percentage of used disk space in the log partition has exceeded the configured low water mark. There are no files to be purged under such a situation. **Trigger**: Exceeded free hard disk threshold. **Severity**: Informational. **Device Type**: Media Server. **Event Code**: 2131. See also LogPartitionHighWatermarkExceeded, LogPartitionLowWatermarkExceeded, and LowInactivePartitionAvailableDiskSpace.
LostContactWithCluster	**Description**: Voice gateway, voice gatekeeper, voice port, or voice interface lost registration with a Cisco Unified Communications Manager cluster. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Voice Gateway (voice port, voice interface), Voice Mail Gateway (voice port), Digital Voice Gateway, Gatekeeper. **Event Code**: 2035.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
LowActivePartitionAvailableDiskSpace Supports Unified Communications Manager version 5.x or later.	**Description**: The percentage of available disk space on the active partition is lower than the configured value. **Trigger**: Threshold. **Severity**: Critical. **Device Type**: Communications Manager.
LowAvailableDiskSpace Supports Unified Communications Manager version 4.x or later.	**Description**: The percentage of available disk space on the active partition is lower than the configured value. **Trigger**: Threshold. **Severity**: Critical. **Device Type**: Communications Manager.
LowAvailableVirtualMemory	**Description**: The percentage of available virtual memory is lower than the configured value. **Trigger**: Threshold. **Severity**: Critical. **Device Type**: Communications Manager. **Event Code**: 2022.
LowInactivePartitionAvailableDiskSpace Supports Unified Communications Manager version 5.x or later.	**Description**: The percentage of available disk space of the inactive partition is lower than the configured value. **Trigger**: Threshold. **Severity**: Critical. **Device Type**: Communications Manager. **Event Code**: 2020.
LowSwapPartitionAvailableDiskSpace Supports Unified Communications Manager version 5.x or later.	**Description**: The percentage of available disk space of the swap partition is lower than the configured value. **Trigger**: Threshold. **Severity**: Critical. **Device Type**: Communications Manager. **Event Code**: 2121.
MajorAlarm	**Description**: Critical pass-through trap was generated. **Trigger**: Pass-through trap. See Pass-Through and Unidentified Traps, page C-4. **Severity**: Informational. **Event Code**: 1016.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
Media List Exhausted Supports Unified Communications Manager version 5.1.3 or later in Syslog/RTMT.	**Description**: All available media resources defined in media list are busy. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Media Server. **Clear Interval:** Time-based auto clear after 60 minutes. **Event Code:** 2056, 4103, 2052, 2053, 2057 and pass-through trap.
MeetingPlaceSwAlarm	**Description**: This alarm is generated when the Meeting Place device reports any software alarm. **Trigger**: Trap-Based Event. **Severity**: Warning. **Device Type**: Media Server. **Event Code**: 2113.
MinorAlarm	**Description**: Significant pass-through trap was generated. **Trigger**: Pass-through trap. See Pass-Through and Unidentified Traps, page C-4. **Severity**: Informational. **Event Code**: 1017.
MultipleServiceQualityIssue	**Description:** Operations Manager has generated a user-defined number of Service Quality Issue events in a user-defined number of minutes. **Trigger:** Event settings. See Configuring Service Quality Event Settings, page 20-7. **Severity:** Critical. **Device Type:** Service Quality events pertain to the call destination, which might be a device (Voice Gateway) or a phone. **Event Code:** 8003. **Note** When this event occurs, Multiple Service Quality Issues is displayed in the status bar on the Service Quality Alert Details display. (See Using the Service Quality Alerts Display, page 4-3.) This event can be generated only when you have a licensed copy of Service Monitor.
MWIOnTimeExceeded	**Description**: MWIOnTime value exceeded the threshold. **Trigger**: Exceeded MWI on time threshold. **Severity**: Warning. **Device Type**: Media Server. **Event Code**: 2024.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
NicDown	**Description**: Network interface card down on an IPCC. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Media Server. **Event Code**: 2040.
NodeToNodeTestFailed	**Description**: A node-to-node test failed. **Trigger**: Node-to-node tests **Severity**: Warning. **Device Type**: Router or Switch. **Event Code**: 4000.
Number Of Registered Phones Dropped Supports Unified Communications Manager version 5.1.3 or later in Syslog/RTMT.	**Description**: The number of registered phones in the cluster dropped more than the configured percentage between consecutive polls. **Trigger**: Threshold. **Severity**: Warning. **Device Type**: Phone. **Clear Interval:** Time-based auto clear after 60 minutes. **Event Code**: 7016.
Number Of Registered Gateways Decreased[1] Supports Unified Communications Manager version 5.1.3 or later in Syslog/RTMT.	**Description**: The number of registered gateways decreases between consecutive RTMT polls. **Trigger**: Polling. **Severity**: Warning. **Device Type**: Voice Gateway. **Clear Interval:** Time-based auto clear after 60 minutes. **Event Code**:
Number Of Registered Gateways Increased[1] Supports Unified Communications Manager version 5.1.3 or later in Syslog/RTMT.	**Description**: The number of registered gateways increases between consecutive RTMT polls. **Trigger**: Polling. **Severity**: Informational. **Device Type**: Voice Gateway. **Clear Interval:** Time-based auto clear after 60 minutes. **Event Code**:

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
Number Of Registered MediaDevices Decreased[1] Supports Unified Communications Manager version 5.1.3 or later in Syslog/RTMT.	**Description:** A registered media device count decreases between consecutive RTMT polls. **Trigger**: Polling. **Severity**: Informational. **Device Type**: Cluster. **Clear Interval:** Time-based auto clear after 60 minutes. **Event Code**: 7018.
Number Of Registered MediaDevices Increased[1] Supports Unified Communications Manager version 5.1.3 or later in Syslog/RTMT.	**Description**: A registered media device count increases between consecutive RTMT polls. **Trigger**: Polling. **Severity**: Informational. **Device Type**: Cluster. **Clear Interval:** Time-based auto clear after 60 minutes. **Event Code**: 7017.
OperationallyDown	**Description**: Interface—Card or network adapter's operational state is not normal. System Hardware—Disk's operational state is not normal. **Trigger**: Polling, or processed trap (see Processed SNMP Traps, page C-1). **Note** For interfaces, Operations Manager will only generate an OperationallyDown clear event if the card is reinserted into the same slot, and if the module index is the same before and after the card is reinserted. **Severity**: Critical. **Device Type**: Host, Hub, Router, Switch, or Optical Switch. **Event Code**: 1018. See also CardDown, InterfaceOperationallyDown, and VoiceCardDown.
OutofRange	**Description**: Device temperature or voltage is outside the normal operating range. When an OutofRange event is generated, you will normally also see fan, power supply, or temperature events. **Trigger**: Exceeded one of these thresholds: • Relative temperature threshold. • Relative voltage threshold. **Severity**: Critical. **Device Type**: Host, Router, Switch, or Optical Switch. **Event Code**: 1019.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
PacketLossDS_ThresholdExceeded	**Description**: Packet loss exceeds the node-to-node test threshold. **Trigger**: Node-to-node test. **Severity**: Warning. **Device Type**: Router or Switch. **Event Code**: 4006. For more information, see Using Node-To-Node Tests, page 11-1.
PacketLossSD_ThresholdExceeded	**Description**: Packet loss exceeds the node-to-node test threshold. **Trigger**: Node-to-node test. **Severity**: Warning. **Device Type**: Router or Switch. **Event Code**: 4005. For more information, see Using Node-To-Node Tests, page 11-1.
PhoneReachabilityTestFailed	**Description**: Operations Manager cannot reach an IP phone. The IP phone has not responded to three or more successive pings from Operations Manager or the IP SLA device. **Trigger**: Polling. **Severity**: Critical. **Device Type**: IP Phone. **Event Code**: 9002.
PhoneUnregistered	**Description**: The selected phone-based notification group's phones unregistered count is less than the Unified Communications Manager/Unified Communications Manager Express-based event threshold for the same Unified CM Express. **Trigger**: Polling (Notification). **Severity**: Warning. **Device Type**: IP Phone. **Event Code**: N/A
PhonesUnregisteredThresholdBased	**Description**: The selected phone-based notification group's phones unregistered count is more than the Unified Communications Manager/Unified Communications Manager Express-based event threshold for the same Unified CM Express. **Trigger**: Polling (Notification). **Severity**: Warning. **Device Type**: Unified Communications Manager/Unified Communications Manager Express. **Event Code**: N/A

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
PimDown	**Description**: IPCC Peripheral Interface Manager (PIM) down. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Media Server. **Event Code**: 2041.
PowerSupplyDegraded	**Description**: Power supply state is Degraded. **Trigger**: Polling. **Severity**: Warning. **Device Type**: Media Server or Voice Gateway. **Event Code**: 2026.
PowerSupplyDown	**Description**: Power supply state is Down. **Trigger**: Trap and polling. **Severity**: Critical. **Device Type**: Media Server or Voice Gateway. **Event Code**: 2027.
QualityDroppedBelowThreshold	**Description**: Quality has fallen below the node-to-node test threshold. **Trigger**: Node-to-node test. **Severity**: Warning. **Device Type**: Router or Switch. **Event Code**: 4009. For more information, see Using Node-To-Node Tests, page 11-1.
RegistrationResponseTime_Threshold Exceeded	**Description**: Registration response time exceeds the node-to-node test threshold. **Trigger**: Node-to-node test. **Severity**: Warning. **Device Type**: Router or Switch. **Event Code**: 4003. For more information, see Using Node-To-Node Tests, page 11-1.
RepeatedRestarts	**Description**: System repeatedly restarts over a short period of time. Operations Manager issues this event by monitoring the number of system cold and warm starts received within the restart window (using the Restart threshold and the RestartWindow parameters). **Trigger**: Exceeded Restart Trap Threshold for Restart Trap Window; or processed trap (see Processed SNMP Traps, page C-1). **Severity**: Critical. **Device Type**: Host, Hub, Router, Switch, or Optical Switch. **Event Code**: 1020.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
Resumed	**Description**: Operations Manager resumes monitoring for a device or component that had previously been suspended from monitoring. **Trigger**: User clicks Resume on the Detailed Device View for a device or component that was previously suspended from monitoring. Additionally, a user applies changes. **Severity**: Critical. **Device Type**: Any. **Event Code**: 1024. For more information, see Suspending/Resuming Devices, page 3-26, Suspending/Resuming a Device Component, page 3-27, and Applying Changes, page 19-60.
RingBackResponseTime_Threshold Exceeded	**Description**: Ring-back response time exceeds the node-to-node test threshold. **Trigger**: Node-to-node test. **Severity**: Warning. **Device Type**: Router or Switch. **Event Code**: 4002. For more information, see Using Node-To-Node Tests, page 11-1.
RoundTripResponseTime_Threshold Exceeded	**Description**: Round trip response time fallen below the node-to-node test threshold. **Trigger**: Node-to-node test. **Severity**: Warning. **Device Type**: Router or Switch. **Event Code**: 4001. For more information, see Using Node-To-Node Tests, page 11-1.
Route List Exhausted Supports Unified Communications Manager version 5.1.3 or later in Syslog/RTMT.	**Description**: This indicates that all available channels defined in route list are busy. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Voice Gateway. **Clear Interval:** Time-based auto clear after 60 minutes. **Event Code:** 4104, 4106, and 4107.
RTMT Data Missing	**Description**: This indicates that RTMT poll-based data is missing. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Unified Communications Manager. **Event Code:**

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
SCSIControllerDown	**Description**: SCSI controller is down on a Compaq system. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Media Server. **Event Code**: 2101.
SCSIDriveDown	**Description**: SCSI drive down on Cisco Unified Communications Manager. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Media Server. **Event Code**: 2061.
SDL Link Out Of Service	**Description**: This event indicates that the local Cisco Unified Communications Manager has lost communication with the remote Communications Manager. **Trigger**: Syslog. **Severity**: Warning. **Device Type**: Communications Manager. **Clear Interval:** Time-based auto clear in EPM after 4 days. **Event Code**: 7002.
ServiceDown	**Description**: Service can run but is not running due to some problem in the service or device. **Trigger**: Polling. **Severity**: Critical (dependent on service). **Device Type**: Media Server. **Event Code**: 2007. **Note** Events are removed for CCM only. You may need to manually clear these CCM events after your upgrade is complete.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
ServiceQualityIssue	**Description:** Operations Manager has received a MOS violation trap from Service Monitor. This indicates that MOS has dropped below a threshold that is set in Service Monitor. **Trigger:** Processed trap (see Processed SNMP Traps, page C-1). **Severity:** Critical. **Device Type**: Service Quality events pertain to the call destination, which might be a device (Voice Gateway) or a phone. **Event Code:** 8001. **Note** This event is shown on the Service Quality Alert Details display. (See Using the Service Quality Alerts Display, page 4-3.) This event can be generated only when you have a licensed copy of Service Monitor.
SOAPNotReachable	**Description:** Device experienced Simple Object Access Protocol (SOAP) connectivity failure while polling. SOAP attributes will not be polled. **Trigger:** Cisco Unified Communications Manager device experienced SOAP communication failure with the management application. Unified Communications Manager may be overloaded or the web service may be down. Rediscover the device in Cisco Unified Operations Manager. **Severity:** Critical. **Device Type:** Media Server. **Event Code:** 2109.
SRSTEntered	**Description**: An IP telephony router is functioning in Survivable Remote Site Telephony (SRST) mode, performing call management for phones in place of the central Cisco Unified Communications Manager. The event is generated when a WAN link is down, preventing IP phone TCP keepalive messages from reaching the Cisco Unified Communications Manager. **Trigger**: Polling (See also Table 18-1 on page 18-3). **Severity**: Critical. **Device Type**: Router, Switch, or Optical Switch. **Event Code**: 9000. **Note** This event triggers activity on the Phone Activities monitoring dashboard.
SRSTRouterFailure	**Description**: A catastrophic failure occurred on an SRST router. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Warning. **Device Type**: Router or VoiceGateway. **Event Code**: 2071.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
SRSTSuspected	**Description**: IP Phone Information Facility reports that all phones associated with the SRST router are unregistered, but the WAN link between phones and the central Cisco Unified Communications Manager is up. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Router, Switch, or Optical Switch. **Event Code**: 9001. **Note** This event triggers activity on the Phone Activities monitoring dashboard.
StateNotNormal	**Description**: A fan, power supply, temperature sensor, or voltage sensor is not acting normally. When an OutofRange event is generated, you will also see a fan, power supply, or temperature event. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Host, Hub, Router, Switch, or Optical Switch. **Event Code**: 1021.
Suspended	**Description**: Operations Manager suspends monitoring of a device or component. **Trigger**: User clicks Suspend on the Detailed Device View for a device or component. **Severity**: Critical. **Device Type**: Any. **Event Code**: 1023. For more information, see Suspending/Resuming Devices, page 3-26 and Suspending/Resuming a Device Component, page 3-27.
SyntheticTestFailed	**Description**: Individual synthetic test failed on an application. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Media Server. **Event Code**: 2011.
SyntheticTestThresholdExceeded	**Description**: Individual synthetic test execution threshold value is exceeded. **Trigger**: Polling. **Severity**: Warning. **Device Type**: Media Server. **Event Code**: 9003.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
SystemVersionMismatched Supports Unified Communications Manager version 6.0.x in Syslog/RTMT.	**Description**: This alert occurs when there is mismatch in system version. **Trigger**: Polling. **Severity**: Informational. **Device Type**: Unified Communications Manager.
TemperatureHigh	**Description**: Operating temperature exceeds the threshold. **Trigger**: Exceeded Relative Temperature Threshold. **Severity**: Critical. **Device Type**: Media Server, Router, or Switch. **Event Code**: 2029. See also OutofRange, page E-24.
TemperatureSensorDegraded	**Description**: Temperature sensor reports abnormal temperature measurements and reports its condition as Degraded. **Trigger**: Polling, or processed trap (see Processed SNMP Traps, page C-1). **Severity**: Warning. **Device Type**: Media Server or Voice Gateway. **Event Code**: 2030.
TemperatureSensorDown	**Description**: Temperature sensor reports abnormal temperature measurements and reports its condition as Failed. **Trigger**: Processed trap (see Processed SNMP Traps, page C-1). **Severity**: Critical. **Device Type**: Media Server or Voice Gateway. **Event Code**: 2031.
Thread Counter Update Stopped Supports Unified Communications Manager version 5.1.3 or later in Syslog/RTMT.	**Description**: Total number of processes and/or threads exceeded the defined threshold. Usually this indicates system resource leaking. **Trigger**: Exceeded defined threshold. **Severity**: Informational. **Device Type**: Communications Manager. **Clear Interval:** Time-based auto clear in EPM after 4 days. **Event Code**: 7023.
TotalTimeUsedThresholdExceeded	**Description**: Total time used in minutes for greetings and messages in all mailboxes exceeds Total Time Used Threshold. **Trigger**: Exceeded Total Time Used Threshold. **Severity**: Critical. **Device Type**: Media Server. **Event Code**: 2047.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
UMRCommunicationError	**Description**: Cisco Unity Message Repository (UMR) cannot communicate with the Partner Mail Server to deliver messages. Messages will be held in the temporary store until the mail server is0 available. **Trigger**: WMI event. **Severity**: Critical. **Device Type**: Media Server. **Event Code**: 2106.
Unknown Publisher	**Description**: The publisher in the cluster is unknown. This is a poll-based event. **Trigger**: RTMT. **Severity**: Critical. **Device Type**: Unified Communications Manager.
UnityFailOverOrRestart	**Description**: One of the following: • In standalone Cisco Unity configuration—Indicates Cisco Unity system has rebooted/restarted. • In Cisco Unity failover configuration—A failover between the primary and secondary Cisco Unity servers occurred. **Note** UnityFailOverOrRestart is automatically cleared after 30 minutes. Clearing of this event does not indicate that failback has occurred. When failback does occur from secondary to primary, you will see the UnityFailOverOrRestart event on the primary Cisco Unity server. **Trigger**: WMI event. **Severity**: Critical. **Device Type**: MediaServer. **Event Code**: 2105.

Table E-1 Events that Operations Manager Supports (continued)

Event	Description, Cause, Severity and Event Code
Unresponsive	**Description**: Device does not respond to ICMP or SNMP requests. Probable causes are: • On a system: ICMP ping requests and SNMP queries to the device timeout received no response. • On an SNMP Agent: Device ICMP ping requests are successful, but SNMP requests time out with no response. **Note** A system might also be reported as unresponsive if the only link (for example, an interface) to the system goes down. Operations Manager performs root cause analysis for any unresponsive events. If Operations Manager receives a device unresponsive, it will clear any interface unresponsive events from that device until the device is recognized as up/responsive. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Host, Hub, Router, Switch, Optical Switch, Media Server, Phone Access Switch, Voice Mail Gateway, or Voice Gateway. **Event Code**: 1022.
VoicePortOperationallyDown	**Description**: Voice port's operational state is not normal. **Trigger**: Polling. **Severity**: Critical. **Device Type**: Voice Gateway. **Event Code**: 2037. **Note** This event only applies to switch ports, not voice gateway ports.

1. This event is not available out of the box. To activate this pair of events, perform the following steps: a. Open the NMSROOT\conf\seg\sysLogConfig.xml file. b. Uncomment the Syslog by removing the lines marked. c. Restart the SEGServer process.

Obsolete Events

Table E-2 contains a list of events removed from the Monitoring Dashboard on Operations Manager 2.1 release. Also listed are equivalent event, if available, that can be used in place of the obsolete events.

Note Some of the obsolete events may not be removed from the Alerts and Events display immediately after upgrade. It may take up to an hour for these events to be removed. If any of these events are displayed after this timeframe, you must manually clear them. Events that may need to be manually removed appear in the footnote in Table E-2.

Table E-2 Operations Manager Obsoleted Events and Replacement Events

Obsolete Event	Event Replacement Option
ActivePortThresholdExceeded	Consider using FXS/FXO PortsInService/Active counter from Cisco Communications Manager or Cisco MGCP Gateways objects.
ApplicationDown	
CallManagerDown	For Cisco Unified Communications Manager Express, see CCMEDown.
CCMCDRFilesBackupFailed Supports Unified Communications Manager version 5.x or later in Syslog/RTMT.	No replacement event; event is replaced by Real Time Monitor and syslog receiver.
CCMHttpServiceInaccessible	
CCMLineLinkDown	Replaced by syslog event.
CiscoCCMAttendantConsoleHeartBeatExceeded	No replacement event; event is replaced by Real Time Monitor and syslog receiver.
CiscoMessagingInterfaceHeartBeatExceeded	No replacement event; event is replaced by Real Time Monitor and syslog receiver.
CiscoTftpHeartBeatExceeded	No replacement event; event is replaced by Real Time Monitor and syslog receiver.
CiscoTranscoderAvailResourceLow	See HighResourceUtilization.[1]
CodeYellowStateEntered	
CodeRedStateEntered	
ConnectionToDistributorFailed	
cpuUtilizationExceeded[1]	Removed for Unified Communications Manager only. Other devices are supported. This event should be manually cleared after upgrade. Consider using CPUPegging or CallProcessingNodeCPUPegging.
CTIDeviceNotRegistered	None.
DB Replication Failure	No longer supports Cisco Unified Communications Manager version 4.x. Supports Unified Communications Manager version 5.1.3 or later in RTMT polling. For Unified Communications Manager version 5.0 to 5.1.2 the event name is IDS Replication Failure.
ExceededMaximumUptime	Use CiscoWorks LAN Management Solution (LMS) for data network monitoring.
ExcessiveDAFaults	HP MIB incorrectly reported fault on certain MCS platforms.
ExcessiveTFTPRequestsAborted	None.
HardwareConferenceOutOfResources	MediaListResourceExhausted syslog message replaces out-of-resource messages for all media types.
HeartBeatThresholdExceeded	No replacement event; event is replaced by RTMT (Real Time Monitor) and syslog receiver.
HighCapacityUtilization	
HighPriorityQueueFull	CodeYellow is used to reliably report call processing health.

Table E-2 Operations Manager Obsoleted Events and Replacement Events (continued)

Obsolete Event	Event Replacement Option
HighQueueDropRate	
HighRouteGroupUtilization	None.
HighRouteListUtilization	None.
InsufficientFreeHardDisk[1]	Replaced only for Unified Communications Manager. Other devices still support this. This event should be manually cleared after upgrade. Consider using LogPartitionHighWatermarkExceeded, LogPartitionLowWatermarkExceeded, and LowActivePartitionAvailableDiskSpace.
InsufficientFreeMemory[1]	Replaced only for Unified Communications Manager. Other devices still support this. This event should be manually cleared after upgrade. Consider using LowAvailableVirtualMemory.
InsufficientFreePhysicalMemory[1]	Replaced only for Unified Communications Manager. Other devices still support this. This event should be manually cleared after upgrade.
InsufficientFreeVirtualMemory[1]	Replaced only for Unified Communications Manager. Other devices still support this. This event should be manually cleared after upgrade.
LowPriorityQueueFull	None.
MOHConnectionLost	None.
MOHOutOfResource	MediaListResourceExhausted syslog message replaces out-of-resource messages for all media types.
MTPOutOfResource	MediaListResourceExhausted syslog message replaces out-of-resource messages for all media types.
NormalPriorityQueueFull	None.
OutboundBusyAttemptsThresholdExceeded	Consider using OutboundBusyAttempt from counter in Cisco MGCP FXS/FXO device object or Cisco MGCP Gateways object.
PortsOutOfServiceThresholdExceeded	Consider using Port Status under Cisco FXS/FXO Gateway devices counter.
RouteGroupExhausted	None.
RouteGroupFailed	Check Route List Exhausted (generated using syslog) for route list status.
RouteListFailed	Check Route List Exhausted (generated using syslog) for route list status.
ServicePartiallyRunning	None.
ServiceRestarted	Replaced by Real-Time Monitoring Threshold (RTMT).
SoftwareConferenceOutOfResources	MediaListResourceExhausted syslog message replaces out-of-resource messages for all media types.

Table E-2 Operations Manager Obsoleted Events and Replacement Events (continued)

Obsolete Event	Event Replacement Option
SYSLOGNotificationsEvent	This generic event was based on Syslog SNMP Traps and is now replaced by the more specific syslog message-based events.
TooManyUnityPortsActive	See HighPortUtilization.[2]
TooManyInboundPortsActive	See HighPortUtilization.[1]
TooManyOutboundPortsActive	See HighPortUtilization.[1]
TranscoderOutOfResources	MediaListResourceExhausted syslog message replaces out-of-resource messages for all media types.
TranscoderOutOfResources	MediaListResourceExhausted syslog message replaces out-of-resource messages for all media types.
UnityPortHung	None.

1. If these events appear on the Alerts and Events display page, you should manually remove them. These events are removed only for CCM.
2. To view the equivalent HighPortUtilization and HighResourceUtilization events, enable performance polling.

Related Topics

- Events Processed, page E-1

APPENDIX F

Working with Voice Application Systems and Software

The following topics describe hardware-specific and version-specific tasks and behavior:

Note See Cisco Unified Communications Manager Compatibility Matrix on Cisco.com for complete up-to-date information about Cisco Unified Communications Manager versions and support.

Configuring Voice Application Systems and Software for Use with Operations Manager

Table F-1 lists tasks that you must perform before Cisco Unified Operations Manager (Operations Manager) can successfully monitor Cisco voice application software.

Table F-1 Configuration Tasks by Application Software Version and System

If you have the following voice application software…	On the following voice application systems…	You must perform the following tasks
Any voice application software that Operations Manager supports	Media Server	Setting a Media Server's SNMP Services Community String Rights, page F-2
Cisco Unified Communications Manager 3.3 and later	Media Server	Changing the Cisco Unified Communications Manager Cluster Name, page F-2
Cisco Unified Communications Manager 4.x and later	Media Server	Configuring Syslog Receiver on Cisco Unified Communications Manager, page F-3

Table F-1 Configuration Tasks by Application Software Version and System (continued)

If you have the following voice application software…	On the following voice application systems…	You must perform the following tasks
Cisco Unified Communications Manager Express	Router	Set **CCMEEnabled** on the router to true. Set **snmp get** for 1.3.6.1.4.1.9.9.439.1.1.1.0 to return 1.
SRST Router	Router	Enable the SRST service on this router. Set **snmp get** for 1.3.6.1.4.1.9.9.441.1.2.1.0 to return 1.

Changing the Cisco Unified Communications Manager Cluster Name

Note You must use this procedure only if you are running a media server with Cisco Unified Communications Manager 3.3 or later.

Operations Manager cannot manage two clusters with the same name. If you are managing multiple Cisco Unified Communications Manager clusters, you must change the default cluster name. Cisco Unified Communications Manager starting with 3.3 use the default cluster name *StandAloneCluster*.

Note For detailed instructions on configuring Cisco Unified Communications Manager, see the Cisco Unified Communications Manager documentation.

Step 1 Open the Cisco Unified Communications Manager Administration page.

Step 2 From the menu bar, select **System**, and choose Enterprise Parameters. The Enterprise Configuration page appears.

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

Step 4 Click **Update**.

Setting a Media Server's SNMP Services Community String Rights

Note Use this procedure on media servers running voice application software.

Operations Manager cannot monitor supported voice applications running on a media server if community string rights for SNMP services are set to *none*. The SNMP queries will not succeed unless the rights for the community string are changed to *read-only*, *read-write*, or *read-create*.

Step 1 On the media server system, select **Start > Settings > Control Panel > Administrative Tools > Services**. The Services window opens.

Step 2 Double-click **SNMP Service**. The SNMP Services Properties window opens.

Step 3 Select the **Security** tab.

Step 4 Select **Community String** and click **Edit**.

Step 5 Change the rights from NONE to READ ONLY.

Note Operations Manager requires read-only rights. You are not required to set the rights to read-write or read-create.

Configuring Syslog Receiver on Cisco Unified Communications Manager

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

For additional details on what syslog events map to Unified Communications Manager releases, see Table E-1 on page E-2.

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

Step 2 Select **Alarm > Configuration**.

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

Select the correct alarm configuration elements for your particular machine:

- For Unified Communications Manager 4.x, select **Cisco CallManager**.
- For Unified Communications Manager 5.x, select **Server > Service:**
  - Cisco AMC Service.
  - Cisco CDR Agent.
  - Cisco CDR Repository Manager.
  - Cisco CallManager.
  - Cisco Database Layer Monitoring.
  - Cisco DRF Client.
  - Cisco DRF Master.
- For Unified Communications Manager 6.x & 7.0, select:
  - **Service Group > CM Services**, then **Service > Cisco CallManager.**
  - **Service Group > CDR Service**, then **Cisco CDR Agent** and **Cisco CDR Repository Manager.**
  - **Service Group > Database and Admin Services**, then **Cisco Database Layer Monitoring.**
  - **Service Group > Performance and Monitoring Services**, then **Cisco AMC Service.**

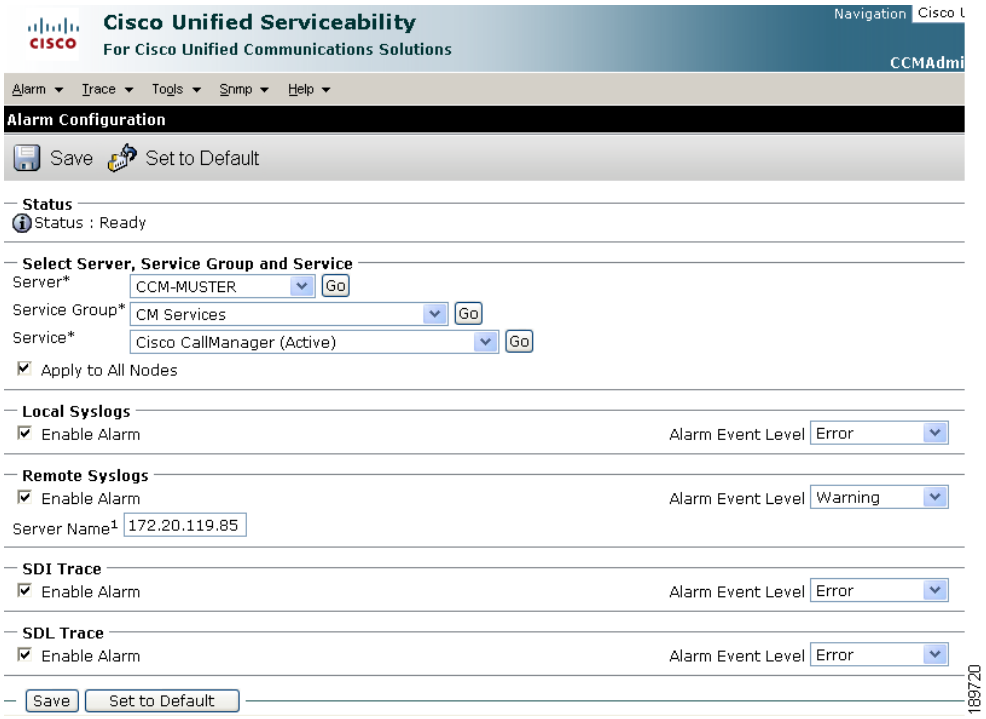
– **Service Group > Backup and Restore**, then **Cisco DRF Client and Cisco DRF Master.**

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

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

Step 4 Check **Apply to all nodes**. (See Figure F-1 on page F-4 for an example of a serviceability page. The serviceability web page may differ depending on the device version you are configuring.)

Figure F-1 Cisco Unified Serviceability Page for Version 6.0



Step 5 Click **Save**.

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

Configuring RTMT on Cisco Unified Communications Manager (Optional)

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

Note This impacts Unified Communications Manager performance and Operations Manager.

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

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

Step 2 To change polling rates:

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

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

Setting HTTP Credentials on Cisco Unified Communications Manager

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

APPENDIX G

Polling—SNMP and ICMP

The topics in this appendix describe the SNMP versions that Cisco Unified Operations Manager (Operations Manager) supports. They also describe how the ICMP and SNMP polling processes that Operations Manager uses work.

The following topics are covered:

SNMP Versions that Operations Manager Supports

Operations Manager supports SNMP version 1 (SNMPv1), SNMPv2, and SNMPv3 (authNoPriv only) traps for polling and receiving. Operations Manager forwards traps as SNMPv1 traps.

SNMP and ICMP Polling

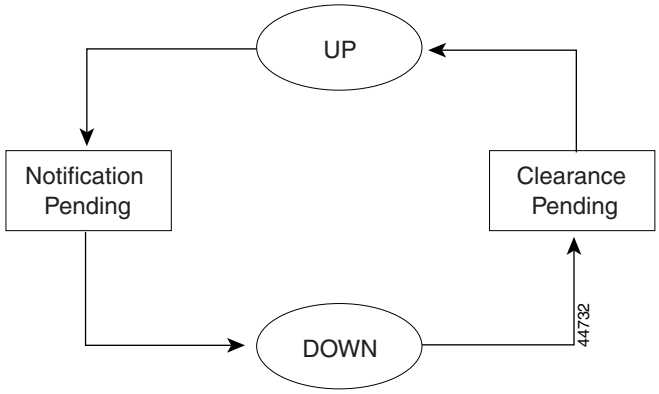
Operations Manager uses both of the following polling processes:

ICMP Polling

Operations Manager uses a high-performance, asynchronous ICMP poller. The ICMP poller performs at a consistent rate that is independent of poll response times. Operations Manager achieves this using two asynchronous threads: one that sends polls and one that receives polls. Because the send and receive threads operate asynchronously, slow response times or excessive timeouts do not affect the polling rate.

Figure G-1 shows the four possible states of an element as determined by its response to an ICMP poll.

Figure G-1 Four Possible States of an Element During a Polling Cycle



The four states are Up, Notification Pending, Down, and Clearance Pending.

An element stays in the Up state until it fails to respond to an ICMP poll. When the element fails to respond, it moves to the Notification Pending state until Operations Manager can determine whether it is up or down. If the minimum stabilization period expires or the maximum failure retry count is exceeded before a successful ICMP poll occurs, the element moves to the Down state. Operations Manager does not poll the element again until the next scheduled polling cycle.

An element stays in the Down state until it responds to an ICMP poll. When the element responds, it moves to the Clearance Pending state. If the maximum success retry count is exceeded or the minimum clear pending time expires, the element returns to the Up state.

IP addresses that are unresponsive to ICMP polls are added to a "do not poll" list. The SNMP poller checks this list before sending an SNMP request. For more information, see SNMP Polling, page G-2.

SNMP Polling

Operations Manager uses an SNMP poller that is synchronous and multithreaded. By default, the SNMP poller uses 10 synchronous polling threads. The SNMP poller supports the following SNMP versions:

- SNMP V1
- SNMP V2C
- SNMP V3 (Authentication and access control, but no data encryption)

SNMP poller uses high-capacity 64-bit counters for data analysis. This capability is critical for performance analysis of high-speed data links where 32-bit counters may wrap between polls.

Operations Manager can support polling for devices with multiple IP addresses because the SNMP poller supports multiple IP addresses for each SNMP agent. The SNMP poller automatically switches to an alternate IP address during failures, ensuring the integrity of Operations Manager analysis during outages.

How the SNMP Poller Works

The SNMP poller's MIB variable poll list is driven by a just-in-time polling algorithm. As a result, only those MIB variables needed for analysis are polled. For example, if a port monitored for performance data is disabled or goes down, the Operations Manager domain manager revokes the SNMP poller's

request to monitor performance data for that port, and the SNMP poller automatically removes the relevant MIB variables from the poll list. If the port is re-enabled or comes back up, the variables are automatically put back onto the MIB poll list.

Consolidating Requests to Optimize Polling

Issuing a single SNMP GET request that requests 10 variables is more efficient than issuing 10 GET requests that each request a single variable. The SNMP poller consolidates as many attributes as possible into a single SNMP GET request. Polling consolidation is not restricted to variables from the same SNMP table. It continually adapts to changes in the MIB variable poll list.

If the SNMP poller encounters recoverable errors during a GET request, it suspends polling of the affected variable and continues to poll the other variables. For example, a MIB variable might become unavailable due to a configuration change. This capability enables the SNMP poller to operate efficiently during unexpected changes to a device's configuration.

Coordinating ICMP and SNMP Polling

Synchronous polling has one drawback: attempting to poll a device that is down reduces polling throughput. This happens because the poller must wait for the initial poll and the subsequent retry polls to time out before polling the next SNMP agent. The problem is exacerbated by the large timeout and retry values that are often required to handle agents that are slow to respond.

The Operations Manager domain manager eliminates this problem by linking its SNMP and ICMP pollers. Operations Manager avoids sending SNMP requests to agent addresses that are known to be unreachable. (The ICMP poller is asynchronous and does not slow down, even in the event of a total network outage.)

IP addresses that are unresponsive to ICMP polls are added to a "do not poll" list. The SNMP poller checks this list before sending an SNMP request. If the SNMP agent address is on the "do not poll" list, the request is not sent. If the SNMP agent has multiple IP addresses, each address is checked against the list. If an alternate address does not appear on the list, the request is sent to that address. If all addresses for an agent are on the list, the agent is deemed unreachable, and all SNMP requests to that agent are temporarily suspended.

As soon as an agent's IP address becomes responsive, the address is removed from the list, and SNMP polling resumes. The net effect is that Operations Manager can support large SNMP timeout and retry values without suffering from polling slow-downs during network outages.

How Operations Manager Calculates ICMP Polling Intervals

Operations Manager calculates ICMP polling intervals for a system (for example, a switch or router) as an offset of the reachability setting's polling interval for a system. System reachability is monitored using a combination of ICMP (Ping) requests for IP status and SNMP requests for interface, port, and card status. If a device does not respond to an ICMP poll, it is placed on a "do not poll" list.

Operations Manager calculates ICMP polling intervals as an offset of the reachability setting's polling interval for a system. The following is an example of a calculation based on the default value of 240 seconds.

1. Operations Manager calculates the offset using this formula:

```
offset = 60;
If (offset > pollingInterval * 0.5) {
offset = pollingInterval * 0.5;
}
```

2. Operations Manager calculates the ICIM polling interval using this formula:

   icimPollingInterval = *pollingInterval* - *offset*

Thus, the default polling intervals are as follows:

- ICMP polling interval is 3 minutes.
- SNMP polling interval is 4 minutes.

APPENDIX H

How Operations Manager Calculates Repeated Restarts and Flapping

Operations Manager uses similar calculations to diagnose both repeated restarts and flapping. Operations Manager considers a system to be restarting repeatedly when it performs too many cold or warm starts over a short period of time. Table H-1 lists the elements, traps, and user-defineable parameters that Operations Manager uses to calculate repeated restarts.

Table H-1 Elements, Traps, and Parameters Used to Calculate Repeated Restarts

Elements	SNMP Traps	Threshold Category	Parameter	Parameter Definition
Hosts Hubs Routers Switches	Cold Start Warm Start	Reachability Settings	Restart trap threshold	Minimum number of SNMP traps required in a user-defined period of time to trigger an event.
			Restart trap window	User-defined period within which minimum number of traps must be received to trigger an event.

Operations Manager considers a network adapter to be flapping when it fluctuates between the Up and Down states too often over a short period of time. Table H-2 lists the elements, traps, and user-defineable parameters Operations Manager uses to diagnose flapping.

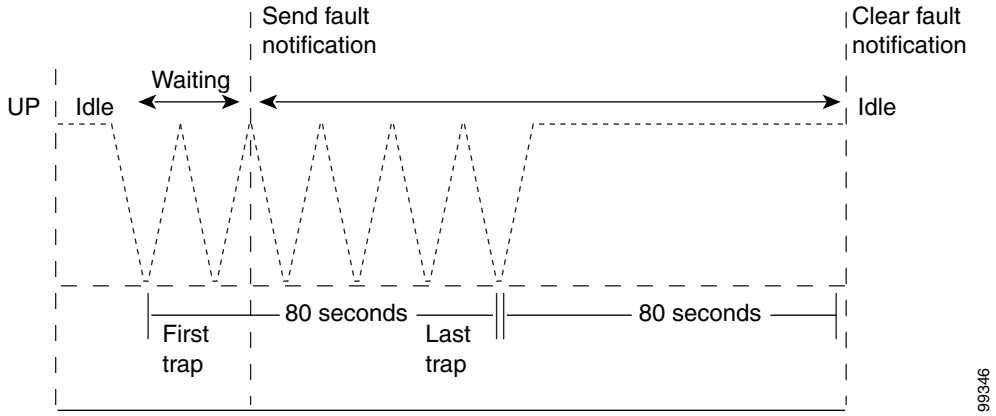
Table H-2 Elements, Traps, and Parameters Used to Calculate Flapping

Elements	SNMP Traps	Threshold Category	Parameter	Parameter Definition
Network adapters (See Interface Groups, Access Port Groups, and Trunk Port Groups in Data Settings—Threshold Categories, page 19-36.)	Link Up Link Down	Interface/port flapping settings	Link trap threshold	Minimum number of SNMP traps required in a user-defined period of time to trigger an event.
			Link trap window	User-defined period within which minimum number of traps must be received to trigger an event.

After Operations Manager generates a Repeated Restarts event or a Flapping event, Operations Manager computes the *stable time* (the amount of time that must elapse without further traps before Operations Manager declares the element stable again). The stable time is at least as long as the time the element was at fault, and at least as long as the trap window; however, it can be no longer than one hour.

Figure H-1 illustrates how a system is diagnosed as performing repeated restarts, or how a network adapter is diagnosed as flapping.

Figure H-1 Diagnosing Repeated System Restarts or Flapping Network Adapters



In Figure H-1, the trap window (Restart trap window or Link trap window parameter) has a value of 30 seconds, and the trap threshold (Restart trap threshold or Link trap threshold parameter) has a value of 2. Operations Manager performs the following actions:

1. As soon as Operations Manager receives a Link Down Trap from a physical port or interface (or a Warm Start/Cold Start Trap from a system), Operations Manager begins counting.
2. When Operations Manager receives 2 or more traps within 30 seconds, it considers the network adapter or system to be at fault and Operations Manager generates a Repeated Restarts event or a Flapping event. The minimum traps parameter (set by the Link trap threshold or Restart trap threshold parameter) determines the number of traps Operations Manager must receive (2) within the trap window (30 seconds, set by the Link trap window or restart trap window parameter) before it considers an element at fault.
3. Operations Manager continues to receive traps for 80 seconds after the initial trap, resulting in a stable time of 80 seconds.

   The stable time is the amount of time that Operations Manager waits before it clears the Repeated Restarts event or Flapping event.

CHAPTER

Operations Manager Support for SNMP MIBs

Cisco Unified Operations Manager (Operations Manager) supports the host resources MIB and implements the system application MIBs using SNMP v2. Operations Manager supplies an SNMP subagent. You can use simple SNMP queries to monitor the health of the system.

For information about configuring your system to use SNMP to manage Operations Manager, see Using SNMP to Monitor Operations Manager, page 20-31. The following topics provide implementation details for the MIBs that Operations Manager supports:

- Host Resource MIB Implementation, page I-1
- System Application MIB Implementation, page I-1

Host Resource MIB Implementation

Operations Manager uses the Windows operating system implementation of the host resources MIB. Support for the host resources MIB, defined in RFC 1514, enables you to monitor the server where Operations Manager is installed, providing details for:

- Hardware such as processors, storage, and memory.
- Software such as operating system and running processes.

For more information about the host resources MIB, you can browse MIB information at the following URL:

http://www.cisco.com/cgi-bin/Support/Mibbrowser/mibinfo.pl?tab=4

System Application MIB Implementation

The system application MIB, defined in RFC 2287, provides applications installed, processes running for an application, and past run information. You can use the information in the system application MIB to determine the overall health of Operations Manager and drill down to the actual processes running for the application.

For more information about the system application MIB, you can browse MIB information at the following URL:

http://www.cisco.com/cgi-bin/Support/Mibbrowser/mibinfo.pl?tab=4

For an example of the data stored in this MIB, see the Sample MIB Walk for System Application MIB, page I-7.

System Application Resource MIB Tables

This section describes MIB tables that contain the following information:

Installed Packages

Table I-1 stores information for installed packages for Operations Manager.

Table I-1 sysApplInstallPkgTable

MIB Row Entry	Description from the MIB	Usage
sysApplInstallPkgIndex	Part of the index for this table. An integer used only for indexing purposes. Generally monotonically increasing from 1 as new applications are installed.	Running number for each application registered with the SNMP subagent.
sysApplInstallPkgManufacturer	The manufacturer of the software application package.	Cisco Systems, Inc.
sysApplInstallPkgProductName	The name assigned to the software application package by the manufacturer.	Name provided when the application was registered with the SNMP subagent. **Note** Use this name to select an application to watch.
sysApplInstallPkgVersion	The version number assigned to the application package by the manufacturer of the software.	Version number such as 2.0.4, where 2 is the major version, 0 is the minor version, and 4 is the patch version or incremental device update (IDU) number.
sysApplInstallPkgSerialNumber	The serial number of the software assigned by the manufacturer.	"n/a"
sysApplInstallPkgDate	The date and time this software application was installed on the host.	—
sysApplInstallPkgLocation	The complete pathname where the application package is installed.	*NMSROOT*—Directory where Operations Manager is installed. If you selected the default directory during installation, it is C:\Program~1\CSCOpx.

Installed Elements

For each entry in the installed packages table, Table I-1, there can be many entries in the installed element table, Table I-2. The number of installed elements for a package corresponds to the number of processes being monitored for that package.

Table I-2 lists the contents of sysApplInstallElmtTable.

Table I-2 sysApplInstallElmtTable

MIB Row Entry	Description from the MIB	Usage
sysApplInstallPkgIndex	Part of the index for this table. This value identifies the installed software package for the application of which this process is a part.	Value from sysApplInstallPkgTable, Table I-1.
sysApplInstallElmtIndex	Unique number across the applications.	Running number.
sysApplInstallElmtName	The name assigned to the software element package by the manufacturer.	Process name used in the CiscoWorks daemon manager (not a file or executable name as specified in RFC 2287).
sysApplInstallElmtType	The type of element that is part of the installed application.	Default application(5).
sysApplInstallElmtDate	The date and time that this component was installed on the system.	**Note** All dates and times are formatted using SNMPv2 textual conventions.
sysApplInstallElmtPath	Install location for this application.	*NMSROOT*—Directory where Operations Manager is installed. If you selected the default directory during installation, it is C:\Program~1\CSCOpx.
sysApplInstallInstallElmt SizeHigh	The installed file size in 2^{32} byte blocks.	Default 0 (not implemented).
sysApplInstallInstallElmt SizeLow	The installed file size in 2^{32} byte blocks.	Default 0 (not implemented).
sysApplInstallElmtRole	An operator-assigned value used in the determination of application status.	Value used in determining application status: • required(3)—Process that must run for the application to be considered running. • unknown(5)—Optional process.
sysApplInstallElmtModifyDate	The date and time that this element was last modified.	**Note** All dates and times are formatted using SNMPv2 textual conventions.
sysApplInstallCurSizeHigh	The current file size in 2^{32} byte blocks.	Default 0 (not implemented).
sysApplInstallCurSizeLow	The current file size in 2^{32} byte blocks.	Default 0 (not implemented).

Package Status Information

Table I-3 supplies current application status for Operations Manager.

Table I-3 sysApplRunTable

MIB Row Entry	Description from the MIB	Usage
sysApplInstallPkgIndex	Part of the index for this table. This value identifies the installed software package for the application of which this process is a part.	Value from sysApplInstallPkgTable, Table I-1.
sysApplRunIndex	Part of the index for this table. An arbitrary integer used only for indexing purposes. Generally, monotonically increasing from 1 as new applications are started on the host, it uniquely identifies application invocations.	Running number.
sysApplRunStarted	The date and time that the application was started.	**Note** All dates and times are formatted using SNMPv2 textual conventions.
sysApplRunCurrentState	The current state of the running application instance. The possible values are running(1), runnable(2) but waiting for a resource such as CPU, waiting(3) for an event, exiting(4), or other(5).	This value is the measure of application health: • running(1)—All required processes are running. • other(5)–One or more required processes are not running. When all required processes stop or the CiscoWorks daemon manager stops, this entry moves to the sysApplPastRun table.

Element Status Information

Table I-4 provides current status for processes that belong to each application that is currently running.

Table I-4 sysApplElmtRunTable

MIB Row Entry	Description from the MIB	Usage
sysApplElmtRunInstallPkg	Part of the index for this table. This value identifies the installed software package for the application of which this process is a part.	Value from sysApplInstallPkgTable, Table I-1.
sysApplElmtRunInvocID	Part of the index for this table. This value identifies the invocation of an application of which this process is a part.	Default 0. **Note** Operations Manager processes run independently and are not invoked by any other process.
sysApplElmtRunIndex	Part of the index for this table. A unique value for each process running on the host.	Process ID in the operating system.

Table I-4 sysApplElmtRunTable (continued)

MIB Row Entry	Description from the MIB	Usage
sysApplElmtRunInstallID	Part of the index for this table. The value of this object is the same value as sysApplInstallElmtIndex for the application element of which this entry represents a running instance.	Value from sysApplInstallElmtTable, Table I-2.
sysApplElmtRunTimeStarted	The time the process was started.	—
sysApplElmtRunState	The current state of the running process. The possible values are running(1), runnable(2) but waiting for a resource such as CPU, waiting(3) for an event, exiting(4), or other(5).	If all processes are running successfully, value is running(1). **Note** If the process terminates, the process entry moves to the sysElmtPastRun table.
sysApplElmtRunName	The full path and filename of the process.	—
sysApplElmtRunParameters	The starting parameters for the process.	—
sysApplElmtRunCPU	Hundredths of a second of the total system CPU resources consumed by this process.	Obtained from the operating system.
sysApplElmtRunMemory	The total amount of real system memory, measured in kilobytes, currently allocated to this process.	Obtained from the operating system.
sysApplElmtRunNumFiles	The number of regular files that the process currently has open.	Default 0 (not implemented).
sysApplElmtRunUser	The process owner's login name.	Either casuser or SYSTEM.

Status of Packages when They Ran Previously

Table I-5 contains the status of applications when they ran previously.

Table I-5 sysApplPastRunTable

MIB Row Entry	Description from the MIB
sysApplInstallPkgIndex	Value from sysApplInstallPkgTable, Table I-1.
sysApplPastRunIndex	Part of the index for this table. An arbitrary integer used only for indexing purposes. Generally monotonically increasing from 1 as new applications are started on the host, it uniquely identifies application invocations.
sysApplPastRunStarted	The date and time that the application started. **Note** All dates and times are formatted using SNMPv2 textual conventions.
sysApplPastExitState	The state of the application instance when it was terminated.
sysApplPastRunEnded	The date and time the application instance was determined to be no longer running. **Note** All dates and times are formatted using SNMPv2 textual conventions.

Status of Elements when They Ran Previously

Table I-6 contains the status of processes when they ran previously.

Table I-6 sysApplElmtPastRunTable

MIB Row Entry	Description from the MIB
sysApplElmtPastRunInvocID	Part of the index for this table. Identifies the invocation of an application of which this process is a part.
sysApplElmtPastRunIndex	Part of the index for this table. A unique value for each process running on the host.
sysApplElmtPastRunInstallID	Part of the index for this table. The value of this object is the same value as the sysApplInstallElmtIndex for the application element of which this entry represents a running instance.
sysApplElmtPastRunTime Started	The time the process was started.
sysApplElmtPastRunTime Ended	The time the process was ended.
sysApplElmtPastRunName	The full path and filename of the process.
sysApplElmtPastRunParameters	The starting parameters for the process.
sysApplElmtPastRunCPU	The last known number of hundredths of a second of the total system CPU resources consumed by this process.
sysApplElmtPastRunMemory	The last known total amount of real system memory, measured in kilobytes, allocated to this process before it terminated.
sysApplElmtPastRunNumFiles	The number of regular files that the process currently has open.
sysApplElmtPastRunUser	The process owner's login name.

Scalar Variables

These variables are used to control MIB table size. You cannot update them.

Table I-7 Scalars

MIB Row Entry	Description from the MIB	Default Value
sysApplPastRunMaxRows	Maximum number of entries allowed in the sysApplPastRun table.	2000
sysApplPastRunTableRemItems	Counter for entries removed from the sysApplPastRun table after the maximum number (sysApplPastRunMaxRows) of entries are exceeded.	20 entries
sysApplPastRunTblTimeLimit	Maximum time that an entry in the sysApplPastRun table can exist before being removed.	86400 seconds (1 day)
sysApplElemPastRunMaxRows	Maximum number of entries allowed in the sysApplElmtPastRuntable.	2000 entries
sysApplElemPastRunTableRemItems	Counter for entries removed from the sysApplElmtPastRun table after the maximum number (sysApplElemPastRunMaxRows) of entries are exceeded.	20 entries

Table I-7 Scalars (continued)

MIB Row Entry	Description from the MIB	Default Value
SysApplElemPastRunTblTimeLimit	Maximum time that an entry in the sysApplElmtPastRunTable can exist before being removed.	86400 seconds (1 day)
sysApplAgentPollInterval	Minimum interval at which polling to obtain the status of the managed resources occurs.	60 seconds

Process Map

The sysApplMapTable contains one entry for each process currently running on the system. Table I-8 provides the index mapping from a process identifier to the invoked application, installed element, and installed application package.

Table I-8 sysApplMapTable

MIB Row Entry	Description from the MIB
sysApplElmtRunIndex	Process identification number.
sysApplElmtRunInvocID	Invoked application (sysApplRunIndex).
sysApplMapInstallElmtIndex	Installed element (sysApplInstallElmtIndex).
sysApplMapInstallPkgIndex	Installed application package (sysApplInstallPkgIndex).

Sample MIB Walk for System Application MIB

This example shows abridged output from a MIB walk of the SYSAPPL-MIB on a system where Operations Manager and Service Monitor are installed.

```
***** SNMP QUERY STARTED *****
1: sysApplInstallPkgManufacturer.1 (octet string) Copyright (c) 2004 by Cisco Systems,
Inc.[43.6F.70.79.72.69.67.68.74.20.28.63.29.20.32.30.30.34.20.62.79.20.43.69.73.63.6F.20.5
3.79.73.74.65.6D.73.2C.20.49.6E.63.2E (hex)]
2: sysApplInstallPkgManufacturer.2 (octet string) Copyright (c) 2004 by Cisco Systems,
Inc.[43.6F.70.79.72.69.67.68.74.20.28.63.29.20.32.30.30.34.20.62.79.20.43.69.73.63.6F.20.5
3.79.73.74.65.6D.73.2C.20.49.6E.63.2E (hex)]
3: sysApplInstallPkgProductName.1 (octet string) Cisco Unified Service Monitor
[43.69.73.63.6F.20.55.6E.69.66.69.65.64.20.53.65.72.76.69.63.65.20.4D.6F.6E.69.74.6F.72
(hex)]
4: sysApplInstallPkgProductName.2 (octet string) Cisco Unified Operations Manager and
Service Monitor
[43.69.73.63.6F.20.55.6E.69.66.69.65.64.20.4F.70.65.72.61.74.69.6F.6E.73.20.4D.61.6E.61.67
.65.72.20.61.6E.64.20.53.65.72.76.69.63.65.20.4D.6F.6E.69.74.6F.72 (hex)]
5: sysApplInstallPkgVersion.1 (octet string) 2.0.0 [32.2E.30.2E.30 (hex)]
6: sysApplInstallPkgVersion.2 (octet string) 2.0.0 [32.2E.30.2E.30 (hex)]
7: sysApplInstallPkgSerialNumber.1 (octet string) n/a [6E.2F.61 (hex)]
8: sysApplInstallPkgSerialNumber.2 (octet string) n/a [6E.2F.61 (hex)]
9: sysApplInstallPkgDate.1 (octet string) 2006-10-12,15:36:45 [07.D6.0A.0C.0F.24.2D (hex)]
10: sysApplInstallPkgDate.2 (octet string) 2006-10-12,15:36:45 [07.D6.0A.0C.0F.24.2D
(hex)]
11: sysApplInstallPkgLocation.1 (octet string) C:\PROGRA~1\CSCOpx
[43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78 (hex)]
12: sysApplInstallPkgLocation.2 (octet string) C:\PROGRA~1\CSCOpx
[43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78 (hex)]
13: sysApplInstallElmtName.1.1 (octet string) QOVR [51.4F.56.52 (hex)]
```

```
14: sysApplInstallElmtName.1.2 (octet string) QOVRDbEngine
[51.4F.56.52.44.62.45.6E.67.69.6E.65 (hex)]
15: sysApplInstallElmtName.1.3 (octet string) QOVRDbMonitor
[51.4F.56.52.44.62.4D.6F.6E.69.74.6F.72 (hex)]
16: sysApplInstallElmtName.1.4 (octet string) Apache [41.70.61.63.68.65 (hex)]
17: sysApplInstallElmtName.1.5 (octet string) CmfDbEngine
[43.6D.66.44.62.45.6E.67.69.6E.65 (hex)]
18: sysApplInstallElmtName.1.6 (octet string) JRunProxyServer
[4A.52.75.6E.50.72.6F.78.79.53.65.72.76.65.72 (hex)]
19: sysApplInstallElmtName.1.7 (octet string) Tomcat [54.6F.6D.63.61.74 (hex)]
20: sysApplInstallElmtName.1.8 (octet string) Web Server [57.65.62.53.65.72.76.65.72
(hex)]
21: sysApplInstallElmtName.2.9 (octet string) AdapterServer
[41.64.61.70.74.65.72.53.65.72.76.65.72 (hex)]
22: sysApplInstallElmtName.2.10 (octet string) Apache [41.70.61.63.68.65 (hex)]
23: sysApplInstallElmtName.2.11 (octet string) CmfDbEngine
[43.6D.66.44.62.45.6E.67.69.6E.65 (hex)]
24: sysApplInstallElmtName.2.12 (octet string) DCRServer [44.43.52.53.65.72.76.65.72
(hex)]
25: sysApplInstallElmtName.2.13 (octet string) DfmBroker [44.66.6D.42.72.6F.6B.65.72
(hex)]
26: sysApplInstallElmtName.2.14 (octet string) DfmServer [44.66.6D.53.65.72.76.65.72
(hex)]
27: sysApplInstallElmtName.2.15 (octet string) EDS [45.44.53 (hex)]
28: sysApplInstallElmtName.2.16 (octet string) EPMDbEngine
[45.50.4D.44.62.45.6E.67.69.6E.65 (hex)]
29: sysApplInstallElmtName.2.17 (octet string) EPMServer [45.50.4D.53.65.72.76.65.72
(hex)]
30: sysApplInstallElmtName.2.18 (octet string) ESS [45.53.53 (hex)]
31: sysApplInstallElmtName.2.19 (octet string) FHDbEngine [46.48.44.62.45.6E.67.69.6E.65
(hex)]
32: sysApplInstallElmtName.2.20 (octet string) FHServer [46.48.53.65.72.76.65.72 (hex)]
33: sysApplInstallElmtName.2.21 (octet string) GPF [47.50.46 (hex)]
34: sysApplInstallElmtName.2.22 (octet string) INVDbEngine
[49.4E.56.44.62.45.6E.67.69.6E.65 (hex)]
35: sysApplInstallElmtName.2.23 (octet string) IVR [49.56.52 (hex)]
36: sysApplInstallElmtName.2.24 (octet string) IPIUDbEngine
[49.50.49.55.44.62.45.6E.67.69.6E.65 (hex)]
37: sysApplInstallElmtName.2.25 (octet string) IPSLAServer
[49.50.53.4C.41.53.65.72.76.65.72 (hex)]
38: sysApplInstallElmtName.2.26 (octet string) ITMDiagServer
[49.54.4D.44.69.61.67.53.65.72.76.65.72 (hex)]
39: sysApplInstallElmtName.2.27 (octet string) Interactor [49.6E.74.65.72.61.63.74.6F.72
(hex)]
40: sysApplInstallElmtName.2.28 (octet string) InventoryCollector
[49.6E.76.65.6E.74.6F.72.79.43.6F.6C.6C.65.63.74.6F.72 (hex)]
41: sysApplInstallElmtName.2.29 (octet string) IPIUDataServer
[49.50.49.55.44.61.74.61.53.65.72.76.65.72 (hex)]
42: sysApplInstallElmtName.2.30 (octet string) ITMOGSServer
[49.54.4D.4F.47.53.53.65.72.76.65.72 (hex)]
43: sysApplInstallElmtName.2.31 (octet string) jrm [6A.72.6D (hex)]
44: sysApplInstallElmtName.2.32 (octet string) LicenseServer
[4C.69.63.65.6E.73.65.53.65.72.76.65.72 (hex)]
45: sysApplInstallElmtName.2.33 (octet string) NOTSServer [4E.4F.54.53.53.65.72.76.65.72
(hex)]
46: sysApplInstallElmtName.2.34 (octet string) PTMServer [50.54.4D.53.65.72.76.65.72
(hex)]
47: sysApplInstallElmtName.2.35 (octet string) PIFServer [50.49.46.53.65.72.76.65.72
(hex)]
48: sysApplInstallElmtName.2.36 (octet string) QoVMServer [51.6F.56.4D.53.65.72.76.65.72
(hex)]
49: sysApplInstallElmtName.2.37 (octet string) SRSTServer [53.52.53.54.53.65.72.76.65.72
(hex)]
```

```
50: sysApplInstallElmtName.2.38 (octet string) SIRServer [53.49.52.53.65.72.76.65.72
(hex)]
51: sysApplInstallElmtName.2.39 (octet string) STServer [53.54.53.65.72.76.65.72 (hex)]
52: sysApplInstallElmtName.2.40 (octet string) Tomcat [54.6F.6D.63.61.74 (hex)]
53: sysApplInstallElmtName.2.41 (octet string) TISServer [54.49.53.53.65.72.76.65.72
(hex)]
54: sysApplInstallElmtName.2.42 (octet string) TopoServer [54.6F.70.6F.53.65.72.76.65.72
(hex)]
55: sysApplInstallElmtName.2.43 (octet string) VsmServer [56.73.6D.53.65.72.76.65.72
(hex)]
56: sysApplInstallElmtName.2.44 (octet string) VHMIntegrator
[56.48.4D.49.6E.74.65.67.72.61.74.6F.72 (hex)]
57: sysApplInstallElmtName.2.45 (octet string) VHMServer [56.48.4D.53.65.72.76.65.72
(hex)]
58: sysApplInstallElmtName.2.46 (octet string) ITMCTMStartup
[49.54.4D.43.54.4D.53.74.61.72.74.75.70 (hex)]
59: sysApplInstallElmtName.2.47 (octet string) IPSLAPurgeTask
[49.50.53.4C.41.50.75.72.67.65.54.61.73.6B (hex)]
60: sysApplInstallElmtName.2.48 (octet string) GpfPurgeTask
[47.70.66.50.75.72.67.65.54.61.73.6B (hex)]
61: sysApplInstallElmtName.2.49 (octet string) FHPurgeTask
[46.48.50.75.72.67.65.54.61.73.6B (hex)]
62: sysApplInstallElmtType.1.1 (integer) application(5)
63: sysApplInstallElmtType.1.2 (integer) application(5)

111: sysApplInstallElmtDate.1.1 (octet string) 2006-10-12,15:36:45 [07.D6.0A.0C.0F.24.2D
(hex)]
112: sysApplInstallElmtDate.1.2 (octet string) 2006-10-12,15:36:45 [07.D6.0A.0C.0F.24.2D
(hex)]

160: sysApplInstallElmtPath.1.1 (octet string) C:\PROGRA~1\CSCOpx
[43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78 (hex)]

209: sysApplInstallElmtSizeHigh.1.1 (integer) 0

258: sysApplInstallElmtSizeLow.1.1 (integer) 0

307: sysApplInstallElmtRole.1.1 (integer) required(3)

356: sysApplInstallElmtModifyDate.1.1 (octet string) 2006-10-12,15:36:45
[07.D6.0A.0C.0F.24.2D (hex)]

405: sysApplInstallElmtCurSizeHigh.1.1 (integer) 0

454: sysApplInstallElmtCurSizeLow.1.1 (integer) 0

503: sysApplRunStarted.1.2 (octet string) 2006-10-18,17:13:24 [07.D6.0A.12.11.0D.18 (hex)]

505: sysApplRunCurrentState.1.2 (integer) running(1)

507: sysApplElmtRunInstallID.0.0.888 (integer) 0

563: sysApplElmtRunTimeStarted.0.0.888 (octet string) 2006-10-18,17:15:35
[07.D6.0A.12.11.0F.23 (hex)]

619: sysApplElmtRunState.0.0.888 (integer) running(1)

675: sysApplElmtRunName.0.0.888 (octet string)
C:\PROGRA~1\CSCOpx\lib\vbroker\bin\osagent.exe
[43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78.5C.6C.69.62.5C.76.62.72.6F.6B.65.72
.5C.62.69.6E.5C.6F.73.61.67.65.6E.74.2E.65.78.65 (hex)]

731: sysApplElmtRunParameters.0.0.888 (octet string) -p 42342 [2D.70.20.34.32.33.34.32
(hex)]
```

```
787: sysApplElmtRunCPU.0.0.888 (timeticks) 0 days 00h:04m:27s.39th (26739)

843: sysApplElmtRunMemory.0.0.888 (integer) 676

899: sysApplElmtRunNumFiles.0.0.888 (integer) 0

955: sysApplElmtRunUser.0.0.888 (octet string) SYSTEM [53.59.53.54.45.4D (hex)]

1000: sysApplElmtRunUser.2.0.9220 (octet string) casuser [63.61.73.75.73.65.72 (hex)]

1011: sysApplElmtPastRunInstallID.2.0.6180 (integer) 44
1012: sysApplElmtPastRunTimeStarted.2.0.6180 (octet string) 2006-10-18,17:16:27
[07.D6.0A.12.11.10.1B (hex)]
1013: sysApplElmtPastRunTimeEnded.2.0.6180 (octet string) 2006-11-5,12:45:49
[07.D6.0B.05.0C.2D.31 (hex)]
1014: sysApplElmtPastRunName.2.0.6180 (octet string) C:\PROGRA~1\CSCOpx\bin\cwjava.exe
[43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78.5C.62.69.6E.5C.63.77.6A.61.76.61.2E
.65.78.65 (hex)]
1015: sysApplElmtPastRunParameters.2.0.6180 (octet string)
-Dcom.smarts.conf.clientConnect=C:\PROGRA~1\CSCOpx\objects\smarts\conf\clientConnect.conf
-Djava.security.policy=C:\PROGRA~1\CSCOpx\lib\jre2\lib\security\java.policy -Xmx128m
-cw:jre
C:\PROGRA~1\CSCOpx\lib\jre  -cw:xrs  -cp:pmf conf\vhm\vhm.classpath
[2D.44.63.6F.6D.2E.73.6D.61.72.74.73.2E.63.6F.6E.66.2E.63.6C.69.65.6E.74.43.6F.6E.6E.65.63
.74.3D.43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78.5C.6F.62.6A.65.63.74.73.5C.73
.6D.61.72.74.73.5C.63.6F.6E.66.5C.63.6C.69.65.6E.74.43.6F.6E.6E.65.63.74.2E.63.6F.6E.66.20
.20.2D.44.6A.61.76.61.2E.73.65.63.75.72.69.74.79.2E.70.6F.6C.69.63.79.3D.43.3A.5C.50.52.4F
.47.52.41.7E.31.5C.43.53.43.4F.70.78.5C.6C.69.62.5C.6A.72.65.32.5C.6C.69.62.5C.73.65.63.75
.72.69.74.79.5C.6A.61.76.61.2E.70.6F.6C.69.63.79.20.2D.58.6D.78.31.32.38.6D.20.20.2D.63.77
.3A.6A.72.65.20.43.3A.5C.50.52.4F.47.52.41.7E.31.5C.43.53.43.4F.70.78.5C.6C.69.62.5C.6A.72
.65.20.20.2D.63.77.3A.78.72.73.20.20.2D.63.70.3A.70.6D.66.20.63.6F.6E.66.5C.76.68.6D.5C.76
.68.6D.2E.63.6C.61.73.73.70.61.74.68.20.20 (hex)]
1016: sysApplElmtPastRunCPU.2.0.6180 (timeticks) 0 days 00h:01m:52s.06th (11206)
1017: sysApplElmtPastRunMemory.2.0.6180 (integer) 970216
1018: sysApplElmtPastRunNumFiles.2.0.6180 (integer) 0
1019: sysApplElmtPastRunUser.2.0.6180 (octet string) SYSTEM [53.59.53.54.45.4D (hex)]
1020: sysApplPastRunMaxRows.0 (integer) 2000
1021: sysApplPastRunTableRemItems.0 (integer) 20
1022: sysApplPastRunTblTimeLimit.0 (integer) 86400
1023: sysApplElemPastRunMaxRows.0 (integer) 2000
1024: sysApplElemPastRunTableRemItems.0 (integer) 20
1025: sysApplElemPastRunTblTimeLimit.0 (integer) 86400
1026: sysApplAgentPollInterval.0 (integer) 60
1027: sysApplMap.2.888.0.0 (integer) 0

1082: sysApplMap.2.15056.0.28 (integer) 2
***** SNMP QUERY FINISHED *****
```

CHAPTER J

Data File Formats

Cisco Unified Operations Manager (Operations Manager) writes data files for performance polling and node-to-node tests. This topic includes the following:

Data Files—Maintenance and Usage

Table J-1 provides information about data files that Operations Manager generates for node-to-node test and performance polling.

Table J-1 Performance Polling and Node-to-Node Data Files

Data File	Node-to-Node Tests	Performance Polling
Storage Location	*NMSROOT*\data\N2NTests*testname*	*NMSROOT*\data\gsu_#GSUDATA#_
Filenames	• *YYYYMMDD*.csv—One data file is written per day; named with year, month, and day; for example: `20060203.csv` • IPSLATestInfo.log—Contains all the configuration information for the node-to-node-test.	• *<device_name>[$<port or card name>]_YYYYMMDD*.csv—One data file is written per day per device: – <device_name> is the name or IP address of the device. – <port or card name> is optional; it is the name of a T1/E1 port or FXS card on a switch in the Cisco Catalyst 6000 family. A filename that includes not only a device name but a port or card name contains data on individual MGCP gateways within a switch in the Cisco Catalyst 6000 family.

Table J-1 Performance Polling and Node-to-Node Data Files (continued)

Data File	Node-to-Node Tests	Performance Polling
Retention period	30 days	3 days
	Operations Manager daily purging deletes files that are older than the retention period. **Note** If you want to retain node-to-node test or performance polling data files beyond the retention period, you should back them up or move them to another folder or server.	
Record format	Fixed 38-field format. The 38th field is reserved and contains the test name. For detailed record formats, see Node-to-Node Test Record Formats, page J-59.	Fixed 38-field format. The 38th field is reserved and contains an asterisk (*). For detailed record formats, see Performance Polling Record Formats, page J-2.

Performance Polling Record Formats

There is one record for each type of data collected. The record types are summarized in Table J-2. Device types and the record types for each are summarized in Table J-3.

Table J-2 Performance Polling Record Types

Type	Reference	Record Count
100	Cisco Unified Communications Manager Port Usage and CPU Usage—Record Type 100, page J-6	One per Cisco Unified Communications Manager
101	Cisco Unified Communications Manager-Controlled Gateway Port Usage—Record Type 101, page J-8	One per Cisco Unified Communications Manager-registered Media Gateway Control Protocol (MGCP) gateway
102	Cisco IOS Gateway Port Usage—Record Type 102, page J-10	One per Cisco IOS gateway
103	Channelized T1 DS0 Channel Status for Cisco Unified Communications Manager-Controlled Gateways—Record Type 103, page J-13	One per T1 CAS in Cisco Unified Communications Manager gateway
104	Reserved for future use	Not applicable
105	Cisco Digital PBX Adapter Port and CPU Usage—Record Type 105, page J-15	One per DPA
106	Cisco IOS Device CPU Usage—Record Type 107, page J-17	One per zone defined in gatekeeper
107	Cisco IOS Device CPU Usage—Record Type 107, page J-17	One per device
108	Cisco Device Memory Usage—Record Type 108, page J-19	One per Cisco IOS gateway or gatekeeper
109	Cisco IOS Gateway Digital Signal Processor Usage—Record Type 109, page J-21	One per DSP channel in Cisco IOS gateway
110	T1 PRI DS0 Channel Status for Cisco Unified Communications Manager-Controlled Gateways—Record Type 110, page J-22	One per T1 PRI in Cisco Unified Communications Manager-registered MGCP gateway
111	E1 PRI DS0 Channel Status for Cisco Unified Communications Manager-Controlled Gateways—Record Type 111, page J-24	One per E1 PRI in Cisco Unified Communications Manager-registered MGCP gateway
112	Channelized T1 CAS DS0 Channel Status for Cisco IOS Gateways—Record Type 112, page J-27	One per T1 CAS in Cisco IOS gateway

Table J-2 Performance Polling Record Types (continued)

Type	Reference	Record Count
113	Channelized E1 CAS DS0 Channel Status for Cisco IOS Gateways—Record Type 113, page J-28	One per E1 CAS in Cisco IOS gateway
114	T1 PRI DS0 Channel Status for Cisco IOS Gateways—Record Type 114, page J-29	One per T1 PRI in Cisco IOS gateway
115	E1 PRI DS0 Channel Status for Cisco IOS Gateways—Record Type 115, page J-31	One per E1 PRI in Cisco IOS gateway
116	BRI Channel Status for Cisco Unified Communications Manager-Controlled Gateways—Record Type 116, page J-33	One per BRI port in Cisco Unified Communications Manager-registered MGCP gateway
117	BRI Channel Status for Cisco IOS Gateways—Record Type 117, page J-34	One per BRI port in Cisco IOS gateway
118	Cisco Unity Express Mailbox Usage—Record Type 118, page J-34	One per Cisco Unity Express
119	Cisco Unified Communications Manager Express Ephone and Key Ephone Usage—Record Type 119, page J-36	One per Cisco Unified Communications Manager Express
120	Cisco Survivable Remote Site Telephony Usage—Record Type 120, page J-37	One per SRST device
121	Cisco Unity Port Usage—Record Type 121, page J-37	One per Cisco Unity
122	Consolidated DSP Usage for Cisco IOS Devices—Record Type 122, page J-38	One per Cisco IOS gateway
123	Cisco Unified Communications Manager Usage 2—Record Type 123, page J-39	One per Cisco Unified Communications Manager
124	FXS Port Usage for Cisco Unified Communications Manager-Controlled Gateways—Record Type 124, page J-41	One per FXS port in a Cisco Unified Communications Manager-registered MGCP gateway
125	FXO Port Usage for Cisco Unified Communications Manager-Controlled Gateways—Record Type 125, page J-42	One per FXO port in a Cisco Unified Communications Manager-registered MGCP gateway
126	Cisco Unified Communications Manager CTI Manager Usage—Record Type 126, page J-43	One per Cisco Unified Communications Manager
127	Cisco Unified Communications Manager Analog Access Gateway Usage—Record Type 127, page J-43	One per analog access gateway registered with a Cisco Unified Communications Manager
128	Cisco Unified Communications Manager H323 Gateway Usage—Record Type 128, page J-44	One per H323 gateway added to Cisco Unified Communications Manager
129	Cisco Unified Communications Manager Location Usage—Record Type 129, page J-45	One per location in Cisco Unified Communications Manager
130	Cisco Unified Communications Manager Media Streaming Application Usage—Record Type 130, page J-46	One per Cisco Unified Communications Manager
131	Cisco Unified Communications Manager MOH Usage—Record Type 131, page J-47	One per MOH device registered with Cisco Unified Communications Manager
132	Cisco Unified Communications Manager MTP Usage—Record Type 132, page J-48	One per MTP device registered with Cisco Unified Communications Manager

Table J-2 Performance Polling Record Types (continued)

Type	Reference	Record Count
133	Cisco Unified Communications Manager Hardware Conference Bridge Usage—Record Type 133, page J-49	One per hardware conference bridge registered with Cisco Unified Communications Manager
134	Cisco Unified Communications Manager Software Conference Bridge Usage—Record Type 134, page J-50	One per software conference bridge registered with Cisco Unified Communications Manager
135	Cisco Unified Communications Manager Transcoder—Record Type 135, page J-50	One per transcoder registered with Cisco Unified Communications Manager
136	T1 PRI Usage for Cisco Unified Communications Manager-Controlled Gateways—Record Type 136, page J-51	One per T1 PRI in a Cisco Unified Communications Manager-registered MGCP gateway
137	E1 PRI Usage for Cisco Unified Communications Manager-Controlled Gateways—Record Type 137, page J-52	One per E1 PRI in a Cisco Unified Communications Manager-registered MGCP gateway
138	T1 CAS Usage for Cisco Unified Communications Manager-Controlled Gateways—Record Type 138, page J-52	One per T1 CAS in a Cisco Unified Communications Manager-registered MGCP gateway
139	Reserved for future use	Not applicable
140	Cisco Unity Connection Usage—Record Type 140, page J-53	One per Cisco Unity Connection
141	Cisco IP Contact Center Usage—Record Type 141, page J-54	One per router configured in IP Contact Center
142	Cisco Unified Communications Manager SIP Device Usage—Record Type 142, page J-55	One per SIP device in Cisco Unified Communications Manager
143	Server Memory Usage—Record Type 143, page J-55	One per Cisco Unified Communications Manager, IP Contact Center, Cisco Unity, or Cisco Unity Connection
144	Server CPU Usage—Record Type 144, page J-56	One per IP Contact Center, Cisco Unity, or Cisco Unity Connection
145	Reserved	Not applicable
146	Reserved	Not applicable
149	Cisco IOS Gateway Total Utilization—Record Type 149, page J-57	One per IOS gateway
9*nnn*	Error Records—Record Type 9nnn, page J-58	One per each related record type for a device when there has been a polling or data collector error.

Table J-3 lists device types and record types that will be written for each device type.

Table J-3 Performance Polling Record Types for Each Device Type

Device Types	Record Number	Record Descriptions
Cisco Unified Communications Manager Express Gatekeepers H323 Gateways SRST Devices	102	• Cisco IOS Gateway Port Usage
	106	• Cisco IOS Gatekeeper Zone Usage
	107	• Cisco IOS Gateway or Gatekeeper CPU Usage
	108	• Cisco IOS Gateway or Gatekeeper Memory Usage
	109	• Cisco IOS Gateway Digital Signal Processor (DSP) Usage
	112	• Channelized T1 CAS DS0 Channel Status for Cisco IOS Gateways
	113	• Channelized E1 CAS DS0 Channel Status for Cisco IOS Gateways
	114	• T1 PRI DS0 Channel Status for Cisco IOS Gateway
	115	• E1 PRI DS0 Channel Status for Cisco IOS Gateways
	117	• BRI Channel Status for Cisco IOS Gateways
	119	• Cisco Unified Communications Manager Express Usage
	120	• Cisco Survivable Remote Site Telephony Usage
	122	• Consolidated DSP Usage
Cisco IP Contact Center	141	• Cisco IP Contact Center Usage
	143	• Server Memory Usage
	144	• Server CPU Usage
Cisco Unified Communications Manager	100	• Cisco Unified Communications Manager Port Usage
	123	• Cisco Unified Communications Manager Usage 2
	126	• Cisco Unified Communications Manager CTI Manager Usage
	127	• Cisco Unified Communications Manager Analog Access Gateway Usage
	128	• Cisco Unified Communications Manager H323 Gateway Usage
	129	• Cisco Unified Communications Manager Location Usage
	130	• Cisco Unified Communications Manager Media Streaming Application Usage
	131	
	132	• Cisco Unified Communications Manager MOH Usage
	133	• Cisco Unified Communications Manager MTP Usage
	134	• Cisco Unified Communications Manager Hardware Conference Bridge Usage
	135	
	142	• Cisco Unified Communications Manager Software Conference Bridge Usage
	143	• Cisco Unified Communications Manager Transcoder Usage
		• Cisco Unified Communications Manager SIP Device Usage
		• Server Memory Usage

Table J-3 Performance Polling Record Types for Each Device Type (continued)

Device Types	Record Number	Record Descriptions
Cisco Unity	121	• Cisco Unity Usage
	143	• Server Memory Usage
	144	• Server CPU Usage
Cisco Unity Connection	140	• Cisco Unity Connection Usage
	143	• Server Memory Usage
	144	• Server CPU Usage
Cisco Unity Express	118	Cisco Unity Express Mailbox Usage
Gateways (MGCP gateways registered to Cisco Unified Communications Manager)	101	• Cisco Unified Communications Manager-Controlled Gateway Port Usage
	103	• Channelized T1 DS0 Channel Status for Cisco Unified Communications Manager-Controlled Gateways
	110	• T1 PRI DS0 Channel Status for Cisco Unified Communications Manager-Controlled Gateways
	111	
	116	• E1 PRI DS0 Channel Status for Cisco Unified Communications Manager-Controlled Gateways
	124	
	125	• BRI Channel Status for Cisco Unified Communications Manager-Controlled Gateways
	136	• FXS Port Usage for Cisco Unified Communications Manager-Controlled Gateways
	137	
	138	• FXO Port Usage for Cisco Unified Communications Manager-Controlled Gateways
		• T1 PRI Usage for Cisco Unified Communications Manager-Controlled Gateways
		• E1 PRI Usage for Cisco Unified Communications Manager-Controlled Gateways
		• T1 CAS Usage for Cisco Unified Communications Manager-Controlled Gateways
Voice Mail Gateways	105	Cisco Digital PBX Adapter Port and CPU Usage

Cisco Unified Communications Manager Port Usage and CPU Usage—Record Type 100

This record contains the port usage and CPU usage for a Cisco Unified Communications Manager. Cisco Unified Communications Manager supports the following ports:

- T1 PRI
- T1 CAS
- E1 PRI
- BRI
- FXO

- FXS

Table J-4 Format of Record Type 100

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 100	100
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco Unified Communications Manager name	Text	Mandatory: name of the Cisco Unified Communications Manager	Example: CCM3
5	CPU 1 usage	Number	Measured percentage. CPU percentage utilization for CPU 1 at time stamp.	≥ 0 and ≤ 100
6	Active calls	Number	Number of calls active at time stamp. This counter shows calls that are fully established and in use. Calls in setup mode or in teardown mode are not reported by this count	≥ 0
7	Total PRIs	Number	Number of PRI channels (T1/E1 PRI) configured on Cisco Unified Communications Manager platform	≥ 0
8	Active PRIs	Number	Number of PRI channels (T1/E1 PRI) active at time stamp	≥ 0 and ≤ total PRIs
9	Total T1 CAS	Number	Number of T1 CAS channels configured on Cisco Unified Communications Manager platform	≥ 0
10	Active T1 CAS	Number	Number of T1 CAS channels active at time stamp	≥ 0 and ≤ total T1/E1
11	Total FXS	Number	Number of FXS ports configured on Cisco Unified Communications Manager platform	≥ 0
12	Active FXS	Number	Number of FXS ports active at time stamp	≥ 0 and ≤ total FXS
13	Total FXO	Number	Number of FXO ports configured on Cisco Unified Communications Manager platform	≥ 0
14	Active FXO	Number	Number of FXO ports active at time stamp	≥ 0 and ≤ total FXO
15	CPU 2 usage	Number	Measured percentage. CPU percentage utilization at time stamp for CPU 2, or an asterisk (*) appears indicating that CPU 2 is not present	≥ 0 and ≤ 100 or *
16	CPU 3 usage	Number	Measured percentage. CPU percentage utilization at time stamp for CPU 3, or an asterisk (*) appears indicating that CPU 3 is not present	≥ 0 and ≤ 100 or *
17	CPU 4 usage	Number	Measured number. CPU percentage utilization at time stamp for CPU 4, or an asterisk (*) appears indicating that CPU 4 is not present	≥ 0 and ≤ 100 or *
18	CPU 5 usage	Number	Measured percentage. CPU percentage utilization at time stamp for CPU 5, or an asterisk (*) appears indicating that CPU 5 is not present	≥ 0 and ≤ 100 or *
19	Total CPU usage	Number	Measured percentage CPU utilization at time stamp for all CPUs	≥ 0

Table J-4 Format of Record Type 100 (continued)

Field Number	Field ID	Content	Description	Value
20	Total T1 PRI	Number	Number of T1 PRI channels configured on Cisco Unified Communications Manager platform	≥ 0
21	Active T1 PRI	Number	Number of T1 PRI channels that were active at time stamp	≥ 0 and ≤ total T1 PRIs
22	Total E1 PRI	Number	Number of E1 PRI channels configured on Cisco Unified Communications Manager platform	≥ 0
23	Active E1 PRI	Number	Number of E1 PRI channels active at time stamp	≥ 0 and ≤ total E1 PRIs
24	Total BRI	Number	Number of BRI channels configured on Cisco Unified Communications Manager platform	≥ 0
25	Active BRI	Number	Number of BRI channels active at time stamp	≥ 0 and ≤ total BRIs
26	Calls attempted	Number	Number of calls attempted on this Cisco Unified Communications Manager	≥ 0
27	Calls complete	Number	Number of calls completed on this Cisco Unified Communications Manager	≥ 0
28	Calls in progress	Number	Number of calls in progress on this Cisco Unified Communications Manager	≥ 0
29	Percentage active T1 CAS	Number	T1 CAS utilization at time stamp for this Cisco Unified Communications Manager	≥ 0 and ≤ 100
30	Percentage FXS	Number	FXS port utilization at time stamp for this Cisco Unified Communications Manager	≥ 0 and ≤ 100
31	Percentage FXO	Number	FXO port utilization at time stamp for this Cisco Unified Communications Manager	≥ 0 and ≤ 100
32	Percentage active T1 PRI	Number	T1 PRI utilization at time stamp for this Cisco Unified Communications Manager	≥ 0 and ≤ 100
33	Percentage active E1 PRI	Number	E1 PRI utilization at time stamp for this Cisco Unified Communications Manager	≥ 0 and ≤ 100
34	Percentage active BRI	Number	BRI utilization at time stamp for this Cisco Unified Communications Manager	≥ 0 and ≤ 100
35	None	Null indicator	Not used	*
Note Fields 36 and 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco Unified Communications Manager-Controlled Gateway Port Usage—Record Type 101

This record contains the port usage for a Cisco Unified Communications Manager-controlled MGCP gateway. MGCP gateways support the following ports:

- T1 PRI
- T1 CAS

- E1 PRI
- BRI
- FXS
- FXO

Table J-5 Format of Record Type 101

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 101	101
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Gateway name	Text	Mandatory: name of subject gateway	Example: sanjose-5720
5	Active calls	Null indicator	Not used. Cisco Unified Communications Manager does not currently provide this information.	*
6	Total PRI	Number	Number of PRI channels (T1/E1 PRI) configured on the gateway	≥ 0
7	Active PRI	Number	Number of PRI channels (T1/E1 PRI) active at time stamp	≥ 0 and ≤ total PRIs
8	Total T1 CAS	Number	Number of T1 CAS channels configured on the gateway	≥ 0
9	Active T1 CAS	Number	Number of T1 CAS channels active at time stamp	≥ 0 and ≤ total T1 CAS
10	Total E1 CAS	Null indicator	Not used. Cisco Unified Communications Manager does not currently support E1 CAS.	*
11	Active E1 CAS	Null indicator	Not used. Cisco Unified Communications Manager does not currently support E1 CAS.	*
12	Total FXS	Number	Number of FXS ports configured on the gateway.	≥ 0
13	Active FXS	Number	Number of FXS ports active at time stamp.	≥ 0 and ≤ total FXS
14	Total FXO	Number	Number of FXO ports configured on the gateway.	≥ 0
15	Active FXO	Number	Number of FXO ports active at time stamp.	≥ 0 and ≤ total FXO
16	Cisco Unified Communications Manager Name	Text	Data for the subject gateway was collected from this Cisco Unified Communications Manager.	Example: CCM3
17	Total T1 PRI	Number	Number of T1 PRI channels configured on the gateway.	≥ 0
18	Active T1 PRI	Number	Number of T1 PRI channels active at time stamp.	≥ 0 and ≤ total T1 PRI
19	Total E1 PRI	Number	Number of E1 PRI channels configured on the gateway.	≥ 0
20	Active E1 PRI	Number	Number of E1 PRI channels active at time stamp.	≥ 0 and ≤ total E1 PRI

Table J-5 Format of Record Type 101 (continued)

Field Number	Field ID	Content	Description	Value
21	Total BRI	Number	Number of BRI channels configured on the MGCP gateway.	≥ 0
22	Active BRI	Number	Number of BRI channels active at time stamp.	≥ 0 and ≤ total BRIs
23	Active T1 CAS	Number	T1 CAS utilization at time stamp for the Cisco Unified Communications Manager-controlled gateway	≥ 0 and ≤ 100
24	Percentage active FXS	Number	FXS port utilization at time stamp for the Cisco Unified Communications Manager-controlled gateway	≥ 0 and ≤ 100
25	Percentage active FXO	Number	FXO port utilization at time stamp for the Cisco Unified Communications Manager-controlled gateway	≥ 0 and ≤ 100
26	Percentage active T1 PRI	Number	T1 PRI utilization at time stamp for the Cisco Unified Communications Manager-controlled gateway	≥ 0 and ≤ 100
27	Percentage active E1 PRI	Number	E1 PRI utilization at time stamp for the Cisco Unified Communications Manager-controlled gateway	≥ 0 and ≤ 100
28	Percentage active BRI	Number	BRI utilization at time stamp for the Cisco Unified Communications Manager-controlled gateway	≥ 0 and ≤ 100
29	None	Null indicator	Not used	*
Note Fields 30 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco IOS Gateway Port Usage—Record Type 102

This record contains the port usage for Cisco IOS gateways. Cisco IOS gateways support the following ports:

- T1/E1 PRI
- T1/E1 CAS
- FXO
- FXS
- E&M
- BRI

For additional information, see Notes on Record Type 102, page J-12.

Table J-6 Format of Record Type 102

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 102	102
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco IOS gateway name	Text	Mandatory: name of subject Cisco IOS gateway	Example: gw1@cisco.com
5	Active call legs[1]	Number	Number of call legs active at time stamp	≥ 0
6	Total T1 PRI[1]	Number	Number of T1 PRI channels configured on Cisco IOS gateway	≥ 0
7	Active voice T1 PRI[1]	Number	Number of T1 PRI channels active with voice calls at time stamp	≥ 0 and ≤ total T1 PRI
8	Total T1 CAS[1]	Number	Number of T1 CAS channels configured on Cisco IOS gateway	≥ 0
9	Active voice T1 CAS	Number	Number of T1 CAS channels active with voice calls at time stamp	≥ 0 and ≤ total T1 CAS
10	Total E1 CAS[1]	Number	Number of E1 CAS channels configured on Cisco IOS gateway	≥ 0
11	Active voice E1 CAS	Number	Number of E1 CAS channels active with voice calls at time stamp	≥ 0 and ≤ total E1 CAS
12	Total FXS	Number	Number of FXS ports configured on Cisco IOS gateway	≥ 0
13	Active FXS	Number	Number of FXS ports active at time stamp	≥ 0 and ≤ total FXS
14	Total FXO	Number	Number of FXO ports configured on Cisco IOS gateway	≥ 0
15	Active FXO	Number	Number of FXO ports active at time stamp	≥ 0 and ≤ total FXO
16	Total BRI	Number	Number of BRI channels active with voice calls at time stamp	≥ 0
17	Active voice BRI[1]	Number	Number of BRI channels active with voice calls at time stamp	≥ 0 and ≤ total BRI
18	Total E&M	Number	Number of E&M ports configured on Cisco IOS gateway	≥ 0
19	Active E&M	Number	Number of E&M ports active at time stamp	≥ 0 and ≤ total E&M
20	Total E1 PRI[1]	Number	Number of E1 PRI channels configured on Cisco IOS gateway	≥ 0
21	Active voice E1 PRI[1]	Number	Number of E1 PRI channels active with voice calls at time stamp	≥ 0 and ≤ total E1 PRI
22	Active nonvoice E1 PRI[1]	Number	Number of E1 PRI channels active with nonvoice calls at time stamp	≥ 0 and ≤ total E1 PRI
23	Active nonvoice T1 PRI[1]	Number	Number of T1 PRI channels active with nonvoice calls at time stamp	≥ 0 and ≤ total T1 PRI

Table J-6 Format of Record Type 102 (continued)

Field Number	Field ID	Content	Description	Value
24	Active nonvoice T1 CAS	Number	Number of T1 CAS channels active with nonvoice calls at time stamp	≥ 0 and ≤ total T1 CAS
25	Active nonvoice E1 CAS	Number	Number of E1 CAS channels active with nonvoice calls at time stamp	≥ 0 and ≤ total E1 PCAS
26	Active nonvoice BRI [1]	Number	Number of BRI channels active with nonvoice calls at time stamp	≥ 0 and ≤ total BRI
27	Percentage active Voice T1 PRI	Number	T1 PRI voice utilization at time stamp for the Cisco IOS gateway	≥ 0 and ≤ 100
28	Percentage active voice E1 PRI	Number	E1 PRI voice utilization at time stamp for the Cisco IOS gateway	≥ 0 and ≤ 100
29	Percentage active voice T1 CAS	Number	T1 CAS voice utilization at time stamp for the Cisco IOS gateway	≥ 0 and ≤ 100
30	Percentage active voice E1 CAS	Number	E1 CAS voice utilization at time stamp for the Cisco IOS gateway	≥ 0 and ≤ 100
31	Percentage active FXS	Number	FXS port utilization at time stamp for the Cisco IOS gateway	≥ 0 and ≤ 100
32	Percentage active FXO	Number	FXO port utilization at time stamp for the Cisco IOS gateway	≥ 0 and ≤ 100
33	Percentage active voice BRI	Number	BRI voice utilization at time stamp for the Cisco IOS gateway	≥ 0 and ≤ 100
34	Percentage active E&M	Number	E&M port utilization at time stamp for the Cisco IOS gateway	≥ 0 and ≤ 100
35	None	Null indicator	Not used	*
Note	Fields 36 through 37 are not used and contain the null indicator "*".			
38	None	Null indicator	Reserved	*

1. For information relevant to this field, see Notes on Record Type 102, page J-12.

Notes on Record Type 102

These notes explain some apparent discrepancies you might notice when you analyze the data in record type 102.

Table J-7 Record Type 102 Notes

Note	Affected Field Numbers	Circumstances
Total number of T1/E1 PRI channels differ by type of device.	6 and 20	For supported Cisco Universal Gateways: Total number of T1/E1 PRI channels = Total B channels + 1 D channel per T1/E1 PRI port For supported devices other than Cisco Universal Gateways: Total number of T1/E1 PRI channels = Total B channels
Total number of T1/E1 CAS channels differ by type of device.	8 and 10	For supported Cisco Universal Gateways, the total T1/E1 CAS channels equal the number of CAS channels configured on the device. For devices other than Cisco Universal Gateways: Total T1 CAS channels = 24 per port Total E1 CAS channels = 31 per port
There can be a discrepancy between active call legs and either of the following: • Active T1/E1 PRI channels • Active BRI channels	5, 7, 17, 21, 22, 23, and 26	Sometimes BRI or PRI channels are active but the number of active call legs does not include them.
There can be a discrepancy between active call legs and active T1/E1 CAS channels.	9 and 11	Sometimes CAS channels are active but the number of active call legs does not include them.

Channelized T1 DS0 Channel Status for Cisco Unified Communications Manager-Controlled Gateways—Record Type 103

This record contains the trunk status for each channelized T1. There can be multiple records for a device with one record per T1 CAS port in the Cisco Unified Communications Manager-controlled MGCP gateway.

Table J-8 Format of Record Type 103

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 103	103
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Gateway name	Text	Mandatory: name of subject gateway	Example: sanjose-5720
5	DS1 name	Text	Mandatory: name of subject DS1	Example: T1-DS1

Table J-8 Format of Record Type 103 (continued)

Field Number	Field ID	Content	Description	Value
6	Channel 1 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
7	Channel 2 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
8	Channel 3 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
9	Channel 4 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
10	Channel 5 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
11	Channel 6 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
12	Channel 7 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
13	Channel 8 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
14	Channel 9 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
15	Channel 10 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
16	Channel 11 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
17	Channel 12 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
18	Channel 13 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
19	Channel 14 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
20	Channel 15 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
21	Channel 16 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
22	Channel 17 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
23	Channel 18 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
24	Channel 19 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
25	Channel 20 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4

Table J-8 Format of Record Type 103 (continued)

Field Number	Field ID	Content	Description	Value
26	Channel 21 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
27	Channel 22 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
28	Channel 23 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
29	Channel 24 status	Number	0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
30	None	Null indicator	Not used	*
Note Fields 31 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Record Type 104—Not Used

Note Record Type 104 is reserved for future use.

Cisco Digital PBX Adapter Port and CPU Usage—Record Type 105

This record contains Cisco Digital PBX Adapter (DPA) port usage: number of voice mail and PBX ports, their usage, and number of unassigned ports. The record also contains CPU usage; DPA supports a single CPU.

Table J-9 Format of Record Type 105

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 105	105
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	DPA name	Text	Mandatory: name of subject Cisco DPA	Example: sanjose-5720
5	Measured 5-second CPU utilization	Number	Overall CPU-busy percentage in the last 5-second period; recorded at time stamp	≥ 0 and ≤ 100
6	Measured 1-minute CPU utilization	Number	Overall CPU-busy percentage in the last 1-minute period; recorded at time stamp	≥ 0 and ≤ 100
7	Measured 5-minute CPU utilization	Number	Overall CPU-busy percentage in the last 5-minute period; recorded at time stamp	≥ 0 and ≤ 100
8	Total voice mail ports	Number	Number of voice mail ports on DPA	≥ 0

Table J-9 Format of Record Type 105 (continued)

Field Number	Field ID	Content	Description	Value
9	Total active voice mail ports	Number	Number of voice mail ports active at time stamp	≥ 0 and ≤ total voice mail ports
10	Total PBX ports	Number	Number of PBX ports on DPA	≥ 0
11	Total active PBX ports	Number	Number of PBX ports active at time stamp	≥ 0 and ≤ total PBX ports
12	Unassigned ports	Number	Number of DPA ports not in use	≥ 0
13	Percentage active voice mail Ports	Number	Voice mail port utilization at time stamp for the DPA	≥ 0 and ≤ 100
14	Percentage active PBX ports	Number	PBX port utilization at time stamp for the DPA	≥ 0 and ≤ 100
15	None	Null indicator	Not used	*
Note Fields 16 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco IOS Gatekeeper Zone Usage—Record Type 106

This record contains gatekeeper zone information including bandwidth, error, and usage. A gatekeeper can have multiple records, with one record per zone configured in the gatekeeper.

Table J-10 Format of Record Type 106

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 106	106
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Gatekeeper name	Text	Mandatory: name of subject gatekeeper	Example: gw1@cisco.com
5	Zone name	Text	Mandatory: name of subject zone	Example: 127.in-addr.arpa
6	Zone domain	Text	Mandatory: name of subject zone domain	Example: cisco.com
7	Total bandwidth	Number	Total bandwidth in 100 bps configured for local zone, or one of the following: -1=bandwidth limitation not set. *=field is not applicable (when record is for a remote zone).	≥ 0 , or -1, or *
8	Allocated bandwidth	Number	Bandwidth in 100 bps allocated to calls at time stamp for local zone, or asterisk (*) to indicate that the field is not applicable (when record is for a remote zone).	≥ 0 and ≤ total bandwidth, or *

Table J-10 Format of Record Type 106 (continued)

Field Number	Field ID	Content	Description	Value
9	Total inter-zone bandwidth	Number	Total interzone bandwidth in 100 bps configured for local zone, or one of the following: -1=bandwidth limitation not set. *=field is not applicable (when record is for a remote zone).	≥ 0 and ≤ total bandwidth, or -1, or *
10	Allocated inter-zone bandwidth	Number	Bandwidth in 100 bps allocated to calls for the local zone, or asterisk (*) to indicate that the field is not applicable (when record is for a remote zone)	≥ 0 and ≤ total interzone bandwidth, or *
11	arjs	Number	Cumulative number of admission rejections for local zone, or asterisk (*) to indicate that the field is not applicable (when record is for a remote zone)	≥ 0
12	acfs	Number	Cumulative number of admission confirms for local zone, or asterisk (*) to indicate that the field is not applicable (when record is for a remote zone)	≥ 0 or *
13	lrqs	Number	Cumulative number of location requests for remote zone, or asterisk (*) to indicate that the field is not applicable (when record is for a local zone)	≥ 0 or *
14	Address lookup failures	Number	Cumulative number of times the gatekeeper is unable to resolve an address	≥ 0
15	End-point timeouts	Number	Cumulative number of times the time to live has expired for an endpoint in this zone	≥ 0
16	Other failures	Number	Cumulative number of call attempts which have failed for reasons other than endpoint timeouts or address lookup failures	≥ 0
17	Zone type	Text	Mandatory: indicates whether the zone is local or remote	local or remote
18	Bandwidth utilization	Number	Bandwidth utilization at time stamp for the local zone	≥ 0 and ≤ 100
19	Interzone bandwidth utilization	Number	Interzone bandwidth utilization at time stamp for the local zone	≥ 0 and ≤ 100
20	None	Null indicator	Not used.	*
Note Fields 21 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco IOS Device CPU Usage—Record Type 107

This record contains the CPU utilization data for Cisco IOS devices of the following device types:

- Gateways and gatekeepers
- SRST devices
- Cisco Unity Express
- Cisco Unified Communications Manager Express

The record allows for a maximum of five CPUs.

Table J-11 Format of Record Type 107

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 107.	107
2	Date	yyyymmdd	Mandatory: calendar date.	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time.	Example: 230000
4	Cisco IOS device name	Text	Mandatory: name of subject Cisco IOS device.	Example: gw1@cisco.com
5	CPU 1 measured 5-second utilization	Number	Overall CPU-busy percentage for CPU 1 in the last 5-second period; recorded at time stamp.	≥ 0 and ≤ 100
6	CPU 1 measured 1-minute utilization	Number	Overall CPU-busy percentage for CPU 1 in the last 1-minute period; recorded at time stamp.	≥ 0 and ≤ 100
7	CPU 1 measured 5-minute utilization	Number	Overall CPU-busy percentage for CPU 1 in the last 5-minute period; recorded at time stamp.	≥ 0 and ≤ 100
8	CPU 2 measured 5-second utilization	Number	Overall CPU-busy percentage for CPU 2 in the last 5-second period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 2 is not present.	≥ 0 and ≤ 100
9	CPU 2 measured 1-minute utilization	Number	Overall CPU-busy percentage for CPU 2 in the last 1-minute period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 2 is not present.	≥ 0 and ≤ 100
10	CPU 2 measured 5-minute utilization	Number	Overall CPU-busy percentage for CPU 2 in the last 5-minute period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 2 is not present.	≥ 0 and ≤ 100
11	CPU 3 measured 5-second utilization	Number	Overall CPU-busy percentage for CPU 3 in the last 5-second period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 3 is not present.	≥ 0 and ≤ 100
12	CPU 3 measured 1-minute utilization	Number	Overall CPU-busy percentage for CPU 3 in the last 1-minute period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 3 is not present.	≥ 0 and ≤ 100
13	CPU 3 measured 5-minute utilization	Number	Overall CPU-busy percentage for CPU 3 in the last 5-minute period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 3 is not present.	≥ 0 and ≤ 100

Table J-11 Format of Record Type 107 (continued)

Field Number	Field ID	Content	Description	Value
14	CPU 4 measured 5-second utilization	Number	Overall CPU-busy percentage for CPU 4 in the last 5-second period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 4 is not present.	≥ 0 and ≤ 100
15	CPU 4 measured 1-minute utilization	Number	Overall CPU-busy percentage for CPU 4 in the last 1-minute period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 4 is not present.	≥ 0 and ≤ 100
16	CPU 4 measured 5-minute utilization	Number	Overall CPU-busy percentage for CPU 4 in the last 5-minute period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 4 is not present.	≥ 0 and ≤ 100
17	CPU 5 measured 5-second utilization	Number	Overall CPU-busy percentage for CPU 5 in the last 5-second period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 5 is not present.	≥ 0 and ≤ 100
18	CPU 5 measured 1-minute utilization	Number	Overall CPU-busy percentage for CPU 5 in the last 1-minute period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 5 is not present.	≥ 0 and ≤ 100
19	CPU 5 measured 5-minute utilization	Number	Overall CPU-busy percentage for CPU 5 in the last 5-minute period; recorded at time stamp. Asterisk (*) in this field indicates that CPU 5 is not present.	≥ 0 and ≤ 100
20	None	Null indicator	Not used.	*
Note Fields 21 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco Device Memory Usage—Record Type 108

This record contains the memory usage information for any of the following:

- Cisco Unified Communications Manager Express
- Cisco IOS gateway or gatekeeper
- Cisco Unity Express
- SRST devices
- Cisco IOS gateways and gatekeepe11rs.

The record includes memory usage in bytes for each of the following types of memory:

- Processor
- I/O
- PCI

- Fast
- Multibus

Table J-12 Format of Record Type 108

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 108	108
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco IOS device name	Text	Mandatory: name of subject device	Example: gw1@cisco.com
5	Processor used memory	Number	Amount of memory in bytes	≥ 0
6	Processor free memory	Number	Amount of memory in bytes	≥ 0
7	Processor largest free	Number	Amount of memory in bytes	≥ 0
8	I/O used memory	Number	Amount of memory in bytes, or asterisk (*) to indicate that I/O memory is not present	≥ 0 or *
9	I/O free memory	Number	Amount of memory in bytes, or asterisk (*) to indicate that I/O memory is not present	≥ 0 or *
10	I/O largest free	Number	Amount of memory in bytes, or asterisk (*) to indicate that I/O memory is not present	≥ 0 or *
11	PCI used memory	Number	Amount of memory in bytes, or asterisk (*) to indicate that PCI memory is not present	≥ 0or *
12	PCI free memory	Number	Amount of memory in bytes, or asterisk (*) to indicate that PCI memory is not present	≥ 0 or *
13	PCI largest free	Number	Amount of memory in bytes, or asterisk (*) to indicate that PCI memory is not present	≥ 0 or *
14	Fast used memory	Number	Amount of memory in bytes, or asterisk (*) to indicate that fast memory is not present	≥ 0 or *
15	Fast free memory	Number	Amount of memory in bytes, or asterisk (*) to indicate that fast memory is not present	≥ 0 or *
16	Fast largest free	Number	Amount of memory in bytes, or asterisk (*) to indicate that fast memory is not present	≥ 0 or *
17	Multibus used memory	Number	Amount of memory in bytes, or asterisk (*) to indicate that multibus memory is not present	≥ 0 or *
18	Multibus free memory	Number	Amount of memory in bytes, or asterisk (*) to indicate that multibus memory is not present	≥ 0 or *
19	Multibus largest free	Number	Amount of memory in bytes, or asterisk (*) to indicate that multibus memory is not present	≥ 0 or *
20	Processor memory utilization	Number	Percentage processor memory utilization	≥ 0 and ≤ 100

Table J-12 Format of Record Type 108 (continued)

Field Number	Field ID	Content	Description	Value
21	I/O memory utilization	Number	Percentage I/O memory utilization	≥ 0 and ≤ 100
22	None	Null indicator	Not used	*
Note Fields 23 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco IOS Gateway Digital Signal Processor Usage—Record Type 109

This record contains the digital signal processor (DSP) usage information on Cisco IOS gateways. A device can have multiple records, with one record per DSP.

Note Operations Manager does not write record type 109 for the following devices:

- Cisco 1700 Series Access Routers
- Cisco MC3810 Multiservice Access Concentrators
- Cisco Series 7500 Routers
- VG200 Voice Gateway

Table J-13 Format of Record Type 109

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 109	109
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco IOS gateway name	Text	Mandatory: name of subject Cisco IOS gateway	Example: gw1@cisco.com
5	Entity index	Number	An index assigned to the DSP	≥ 0
6	State	Number	1=active, 2=shutdown	1 or 2
7	Total channels	Number	Number of channels on DSP	≥ 0
8	Active channels	Number	Number of channels on DSP that are active at time stamp	≥ 0 and ≤ total DSP channels
9	In use channels	Number	Number of channels reserved for serving calls	≥ 0 and ≤ total DSP channels
10	None	Null indicator	Not used	*
Note Fields 11 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

T1 PRI DS0 Channel Status for Cisco Unified Communications Manager-Controlled Gateways—Record Type 110

This record contains the trunk status for each T1 channel configured for ISDN PRI. A device can have multiple records, with one record per T1 PRI port in the Cisco Unified Communications Manager-controlled MGCP gateway.

Table J-14 Format of Record Type 110

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 110	110
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Gateway name	Text	Mandatory: name of subject gateway	Example: sanjose-5720
5	DS1 name	Text	Mandatory: name of subject DS1	Example: T1-DS1
6	Channel 1 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
7	Channel 2 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
8	Channel 3 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
9	Channel 4 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
10	Channel 5 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
11	Channel 6 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
12	Channel 7 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
13	Channel 8 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
14	Channel 9 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4

Table J-14 Format of Record Type 110 (continued)

Field Number	Field ID	Content	Description	Value
15	Channel 10 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
16	Channel 11 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
17	Channel 12 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
18	Channel 13 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
19	Channel 14 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
20	Channel 15 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
21	Channel 16 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
22	Channel 17 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
23	Channel 18 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
24	Channel 19 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
25	Channel 20 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
26	Channel 21 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
27	Channel 22 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
28	Channel 23 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4

Table J-14 Format of Record Type 110 (continued)

Field Number	Field ID	Content	Description	Value
29	Channel 24 status	Number	D channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
30	None	Null indicator	Not used	*
Note Fields 31 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

E1 PRI DS0 Channel Status for Cisco Unified Communications Manager-Controlled Gateways—Record Type 111

This record contains the trunk status for each E1 channel configured for ISDN PRI. There can be multiple records for a device with one record per E1 port in the Cisco Unified Communications Manager-controlled MGCP gateway.

Table J-15 Format of Record Type 111

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 111	111
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Gateway name	Text	Mandatory: name of subject gateway	Example: sanjose-5720
5	DS1 name	Text	Mandatory: name of subject DS1	Example: E1-PRI-D1
6	Channel 1 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
7	Channel 2 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
8	Channel 3 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
9	Channel 4 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
10	Channel 5 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4

Table J-15 Format of Record Type 111 (continued)

Field Number	Field ID	Content	Description	Value
11	Channel 6 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
12	Channel 7 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
13	Channel 8 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
14	Channel 9 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
15	Channel 10 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
16	Channel 11 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
17	Channel 12 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
18	Channel 13 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
19	Channel 14 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
20	Channel 15 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
21	Channel 16 status	Number	D channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
22	Channel 17 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
23	Channel 18 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
24	Channel 19 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4

Table J-15 Format of Record Type 111 (continued)

Field Number	Field ID	Content	Description	Value
25	Channel 20 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
26	Channel 21 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
27	Channel 22 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
28	Channel 23 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
29	Channel 24 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
30	Channel 25 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
31	Channel 26 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
32	Channel 27 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
33	Channel 28 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
34	Channel 29 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
35	Channel 30 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
36	Channel 31 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
37	None	Null indicator	Not used	*
38	None	Null indicator	Not used	*

Channelized T1 CAS DS0 Channel Status for Cisco IOS Gateways—Record Type 112

This record contains the trunk status for each channelized T1. A device can have multiple records, with one record per T1 CAS port in the Cisco IOS gateway.

Note Operations Manager writes record type 112 for supported Cisco Universal Gateways only.

Table J-16 Format of Record Type 112

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 112	112
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco IOS gateway name	Text	Mandatory: name of subject Cisco IOS gateway	Example: gw1@cisco.com
5	DS1 name	Text	Mandatory: name of subject DS1	Example: E1-CAS-D1
6	Channel 1 status	Number	200=idle, 300=unknown, 301=other, 302=voice, 303=unrestrictedDigital, 304=unrestrictedDigital56, 305=restrictedDigital, 306=audio31, 307=audio7, 308=video, 309=packetSwitched, 310=fax, 312=unknown, 313=analog, 314=digital, 315=v110, 316=v120	200, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 312, 313, 314, 315, or 316
7	Channel 2 status	Number	See field number 6	See field number 6
8	Channel 3 status	Number	See field number 6	See field number 6
9	Channel 4 status	Number	See field number 6	See field number 6
10	Channel 5 status	Number	See field number 6	See field number 6
11	Channel 6 status	Number	See field number 6	See field number 6
12	Channel 7 status	Number	See field number 6	See field number 6
13	Channel 8 status	Number	See field number 6	See field number 6
14	Channel 9 status	Number	See field number 6	See field number 6
15	Channel 10 status	Number	See field number 6	See field number 6
16	Channel 11 status	Number	See field number 6	See field number 6
17	Channel 12 status	Number	See field number 6	See field number 6
18	Channel 13 status	Number	See field number 6	See field number 6
19	Channel 14 status	Number	See field number 6	See field number 6
20	Channel 15 status	Number	See field number 6	See field number 6
21	Channel 16 status	Number	See field number 6	See field number 6
22	Channel 17 status	Number	See field number 6	See field number 6
23	Channel 18 status	Number	See field number 6	See field number 6

Table J-16 Format of Record Type 112 (continued)

Field Number	Field ID	Content	Description	Value
24	Channel 19 status	Number	See field number 6	See field number 6
25	Channel 20 status	Number	See field number 6	See field number 6
26	Channel 21 status	Number	See field number 6	See field number 6
27	Channel 22 status	Number	See field number 6	See field number 6
28	Channel 23 status	Number	See field number 6	See field number 6
29	Channel 24 status	Number	See field number 6	See field number 6
30	None	Null indicator	Not used	*
Note	Fields 31 through 37 are not used and contain the null indicator "*".			
38	None	Null indicator	Reserved	*

Channelized E1 CAS DS0 Channel Status for Cisco IOS Gateways—Record Type 113

This record contains the trunk status for each channelized E1. A device can have multiple records, with one record per E1 CAS port in the Cisco IOS gateway.

Note Operations Manager writes record type 113 for supported Cisco Universal Access Gateways only.

Table J-17 Format of Record Type 113

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 113	113
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco IOS gateway name	Text	Mandatory: name of subject Cisco IOS gateway	Example: gw1@cisco.com
5	DS1 name	Text	Mandatory: name of subject DS1	Example: E1-CAS-D1
6	Channel 1 status	Number	200=idle, 300=unknown, 301=other, 302=voice, 303=unrestrictedDigital, 304=unrestrictedDigital56, 305=restrictedDigital, 306=audio31, 307=audio7, 308=video, 309=packetSwitched, 310=fax, 312=unknown, 313=analog, 314=digital, 315=v110, 316=v120	200, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 312, 313, 314, 315, or 316
7	Channel 2 status	Number	See field number 6	See field number 6
8	Channel 3 status	Number	See field number 6	See field number 6
9	Channel 4 status	Number	See field number 6	See field number 6

Table J-17 Format of Record Type 113 (continued)

Field Number	Field ID	Content	Description	Value
10	Channel 5 status	Number	See field number 6	See field number 6
11	Channel 6 status	Number	See field number 6	See field number 6
12	Channel 7 status	Number	See field number 6	See field number 6
13	Channel 8 status	Number	See field number 6	See field number 6
14	Channel 9 status	Number	See field number 6	See field number 6
15	Channel 10 status	Number	See field number 6	See field number 6
16	Channel 11 status	Number	See field number 6	See field number 6
17	Channel 12 status	Number	See field number 6	See field number 6
18	Channel 13 status	Number	See field number 6	See field number 6
19	Channel 14 status	Number	See field number 6	See field number 6
20	Channel 15 status	Number	See field number 6	See field number 6
21	Channel 16 status	Number	See field number 6	See field number 6
22	Channel 17 status	Number	See field number 6	See field number 6
23	Channel 18 status	Number	See field number 6	See field number 6
24	Channel 19 status	Number	See field number 6	See field number 6
25	Channel 20 status	Number	See field number 6	See field number 6
26	Channel 21 status	Number	See field number 6	See field number 6
27	Channel 22 status	Number	See field number 6	See field number 6
28	Channel 23 status	Number	See field number 6	See field number 6
29	Channel 24 status	Number	See field number 6	See field number 6
30	Channel 25 status	Number	See field number 6	See field number 6
31	Channel 26 status	Number	See field number 6	See field number 6
32	Channel 27 status	Number	See field number 6	See field number 6
33	Channel 28 status	Number	See field number 6	See field number 6
34	Channel 29 status	Number	See field number 6	See field number 6
35	Channel 30 status	Number	See field number 6	See field number 6
36	Channel 31 status	Number	See field number 6	See field number 6
37	None	Null indicator	Not used	*
38	None	Null indicator	Not used	*

T1 PRI DS0 Channel Status for Cisco IOS Gateways—Record Type 114

This record contains the trunk status for each T1 channel configured for ISDN PRI. A device can have multiple records, with one record per T1 PRI port in the Cisco IOS gateway.

Table J-18 Format of Record Type 114

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 114	114
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco IOS gateway name	Text	Mandatory: name of subject Cisco IOS gateway	Example: gw1@cisco.com
5	DS1 name	Text	Mandatory: name of subject DS1	Example: E1-PRI-D1
6	Channel 1 status	Number	B channel 200=idle, 300=unknown, 301=other, 302=voice, 303=unrestrictedDigital, 304=unrestrictedDigital56, 305=restrictedDigital, 306=audio31, 307=audio7, 308=video, 309=packetSwitched, 310=fax, 312=unknown, 313=analog, 314=digital, 315=v110, 316=v120	200, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 312, 313, 314, 315, or 316
7	Channel 2 status	Number	B channel See field number 6	See field number 6
8	Channel 3 status	Number	B channel See field number 6	See field number 6
9	Channel 4 status	Number	B channel See field number 6	See field number 6
10	Channel 5 status	Number	B channel See field number 6	See field number 6
11	Channel 6 status	Number	B channel See field number 6	See field number 6
12	Channel 7 status	Number	B channel See field number 6	See field number 6
13	Channel 8 status	Number	B channel See field number 6	See field number 6
14	Channel 9 status	Number	B channel See field number 6	See field number 6
15	Channel 10 status	Number	B channel See field number 6	See field number 6
16	Channel 11 status	Number	B channel See field number 6	See field number 6
17	Channel 12 status	Number	B channel See field number 6	See field number 6
18	Channel 13 status	Number	B channel See field number 6	See field number 6
19	Channel 14 status	Number	B channel See field number 6	See field number 6
20	Channel 15 status	Number	B channel See field number 6	See field number 6

Table J-18 Format of Record Type 114 (continued)

Field Number	Field ID	Content	Description	Value
21	Channel 16 status	Number	B channel See field number 6	See field number 6
22	Channel 17 status	Number	B channel See field number 6	See field number 6
23	Channel 18 status	Number	B channel See field number 6	See field number 6
24	Channel 19 status	Number	B channel See field number 6	See field number 6
25	Channel 20 status	Number	B channel See field number 6	See field number 6
26	Channel 21 status	Number	B channel See field number 6	See field number 6
27	Channel 22 status	Number	B channel See field number 6	See field number 6
28	Channel 23 status	Number	B channel See field number 6	See field number 6
29	Channel 24 status	Number	D channel **Note** D channel status is available for Cisco Universal Gateways only. See field number 6	See field number 6
30	None	Null indicator	Not used	*
Note Fields 31 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

E1 PRI DS0 Channel Status for Cisco IOS Gateways—Record Type 115

This record contains the trunk status for each E1 channel configured for ISDN PRI. A device can have multiple records, with one record per E1 PRI port in the Cisco IOS gateway.

Table J-19 Format of Record Type 115

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 115	115
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco IOS gateway name	Text	Mandatory: name of subject Cisco IOS gateway	Example: gw1@cisco.com
5	DS1 name	Text	Mandatory: name of subject DS1	Example: E1-PRI-D1

Table J-19 Format of Record Type 115 (continued)

Field Number	Field ID	Content	Description	Value
6	Channel 1 status	Number	B channel 200=idle, 300=unknown, 301=other, 302=voice, 303=unrestrictedDigital, 304=unrestrictedDigital56, 305=restrictedDigital, 306=audio31, 307=audio7, 308=video, 309=packetSwitched, 310=fax, 312=unknown, 313=analog, 314=digital, 315=v110, 316=v120	200, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 312, 313, 314, 315, or 316
7	Channel 2 status	Number	B channel See field number 6	See field number 6
8	Channel 3 status	Number	B channel See field number 6	See field number 6
9	Channel 4 status	Number	B channel See field number 6	See field number 6
10	Channel 5 status	Number	B channel See field number 6	See field number 6
11	Channel 6 status	Number	B channel See field number 6	See field number 6
12	Channel 7 status	Number	B channel See field number 6	See field number 6
13	Channel 8 status	Number	B channel See field number 6	See field number 6
14	Channel 9 status	Number	B channel See field number 6	See field number 6
15	Channel 10 status	Number	B channel See field number 6	See field number 6
16	Channel 11 status	Number	B channel See field number 6	See field number 6
17	Channel 12 status	Number	B channel See field number 6	See field number 6
18	Channel 13 status	Number	B channel See field number 6	See field number 6
19	Channel 14 status	Number	B channel See field number 6	See field number 6
20	Channel 15 status	Number	B channel See field number 6	See field number 6
21	Channel 16 status	Number	D channel **Note** D channel status is available for Cisco Universal Gateways only. See field number 6	See field number 6
22	Channel 17 status	Number	B channel See field number 6	See field number 6

Table J-19 Format of Record Type 115 (continued)

Field Number	Field ID	Content	Description	Value
23	Channel 18 status	Number	B channel See field number 6	See field number 6
24	Channel 19 status	Number	B channel See field number 6	See field number 6
25	Channel 20 status	Number	B channel See field number 6	See field number 6
26	Channel 21 status	Number	B channel See field number 6	See field number 6
27	Channel 22 status	Number	B channel See field number 6	See field number 6
28	Channel 23 status	Number	B channel See field number 6	See field number 6
29	Channel 24 status	Number	B channel See field number 6	See field number 6
30	None	Null indicator	Not used	*
Note Fields 31 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

BRI Channel Status for Cisco Unified Communications Manager-Controlled Gateways—Record Type 116

This record contains the channel status for each BRI configured on a Cisco Unified Communications Manager-controlled gateway. A device can have multiple records, with one record per BRI port in the Cisco Unified Communications Manager-controlled gateway.

Table J-20 Format of Record Type 116

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 116	116
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Gateway name	Text	Mandatory: name of subject gateway	Example: sanjose-5720
5	DS1 name	Text	Mandatory: name of subject DS1	Example: BRI-DS1
6	Channel 1 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4

Table J-20 Format of Record Type 116 (continued)

Field Number	Field ID	Content	Description	Value
7	Channel 2 status	Number	B channel 0=unknown, 1=out-of-service, 2=idle, 3=busy, 4=reserved	≥ 0 and ≤ 4
8	Channel 3 status	Number	D channel 0=out-of-service, 1=in-service	0 or 1
9	None	Null indicator	Not used	*
Note Fields 10 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

BRI Channel Status for Cisco IOS Gateways—Record Type 117

This record contains the channel status for each BRI configured on a Cisco IOS gateway. A device can have multiple records, with one record per BRI port in the Cisco IOS Gateway.

Table J-21 Format of Record Type 117

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 117	117
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco IOS gateway name	Text	Mandatory: name of subject gateway	Example: gw1@cisco.com
5	DS1 name	Text	Mandatory: name of subject DS1	Example: BRI-DS1
6	B channel 1 status	Number	200=idle, 300=unknown, 302=voice, 303=unrestrictedDigital, 304=unrestrictedDigital56, 305=restrictedDigital, 306=audio31, 307=audio7, 308=video, 309=packetSwitched	200, 300, 302, 303, 304, 305, 306, 307, 308, 309
7	B channel 2 status	Number	200=idle, 300=unknown, 302=voice, 303=unrestrictedDigital, 304=unrestrictedDigital56, 305=restrictedDigital, 306=audio31, 307=audio7, 308=video, 309=packetSwitched	200, 300, 302, 303, 304, 305, 306, 307, 308, 309
8	None	Null indicator	Not used	*
Note Fields 9 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco Unity Express Mailbox Usage—Record Type 118

This record contains Cisco Unity Express mailbox usage.

Table J-22 Format of Record Type 118

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 118	118
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco Unity Express name	Text	Mandatory: name of subject Cisco Unity Express	ASCII characters
5	None	Null indicator	Not used	*
6	Total memory	Null indicator	Not used—Reserved for total RAM (Kb)	*
7	Available memory	Null indicator	Not used—Reserved for a available RAM (Kb)	*
8	Memory utilization	Null indicator	Not used—Reserved for percentage RAM utilization	*
9	Licensed mailboxes	Number	Maximum number of mailboxes permitted by license	≥ 0
10	Orphaned mailboxes	Number	Number of mailboxes orphaned at time stamp	≥ 0 and ≤ licensed mailboxes
11	Percentage orphaned mailboxes	Number	Percentage of licensed mailboxes that are orphaned at time stamp	≥ 0 and ≤ 100
12	Maximum sessions	Number	Maximum number of sessions configured on Cisco Unity Express	≥ 0
13	Used sessions	Number	Number of sessions in use at time stamp	≥ 0 and ≤ maximum sessions
14	Session utilization	Number	Percentage of maximum sessions in use at time stamp	≥ 0 and ≤ 100
15	Licensed capacity	Number	Number of minutes of storage permitted by license	≥ 0
16	Allocated capacity	Number	Cumulative number of minutes of storage allocated to mailboxes	≥ 0 and ≤ allocated capacity
17	Used capacity	Number	Cumulative number of minutes of storage used by mailboxes	≥ 0 and ≤ allocated capacity
18	Capacity used for messages	Number	Cumulative number of minutes of storage used for storing messages	≥ 0 and ≤ allocated capacity
19	Free capacity	Number	Number of minutes of storage available	≥ 0 and ≤ licensed capacity
20	Capacity utilization	Number	Percentage of storage in use at time stamp	≥ 0 and ≤ 100
21	Current messages	Number	Cumulative number of messages stored in mailboxes at time stamp	≥ 0
22	Current saved messages	Number	Cumulative number of saved messages in mailboxes at time stamp	≥ 0
23	Total messages left since last boot	Number	Cumulative number of messages left in mailboxes since last reboot of Cisco Unity Express	≥ 0

Table J-22 Format of Record Type 118 (continued)

Field Number	Field ID	Content	Description	Value
24	Total messages retrieved since last boot	Number	Cumulative number of messages retrieved in mailboxes since last reboot of Cisco Unity Express	≥ 0
25	Total messages deleted since last boot	Number	Cumulative number of messages deleted from mailboxes since last reboot of Cisco Unity Express	≥ 0
26	Busy mailboxes	Number	Number of busy mailboxes	≥ 0
27	Mailboxes above 90% full	Number	Number of mailboxes that are 90% or more full	≥ 0
28	None	Null indicator	Not used	*
Note Fields 29 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco Unified Communications Manager Express Ephone and Key Ephone Usage—Record Type 119

This record contains Cisco Unified Communications Manager Express ephone and key ephone usage information.

Table J-23 Format of Record Type 119

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 119	119
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco Unified Communications Manager Express name	Text	Mandatory: name of subject Cisco Unified Communications Manager Express	
5	Ephone active call legs	Number	Number of ephone call legs active at time stamp	≥ 0
6	Maximum ephones	Number	Maximum number of ephones that can be configured on the Cisco Unified Communications Manager Express	≥ 0
7	Ephones registered	Number	Number of ephones registered at time stamp	≥ 0 and ≤ maximum ephones
8	Percentage ephones registered	Number	Percentage of ephones that are registered	≥ 0 and ≤ 100
9	Key ephones configured	Number	Number of key ephones configured	≥ 0

Table J-23 Format of Record Type 119 (continued)

Field Number	Field ID	Content	Description	Value
10	Key ephones registered	Number	Number of key ephones registered	≥ 0 and ≤ key ephones configured
11	Percentage key ephones registered	Number	Percentage of configured key ephones that are registered	≥ 0 and ≤ 100
12	Ephones seen	Number	Maximum number of sessions configured on the CUE	≥ 0
13	None	Null indicator	Not used	*
Note Fields 14 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco Survivable Remote Site Telephony Usage—Record Type 120

This record contains Cisco Survivable Remote Site Telephony (SRST) usage information.

Table J-24 Format of Record Type 120

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 120	120
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	SRST name	Text	Mandatory: name of subject SRST device	ASCII characters
5	Minutes in SRST mode	Number	Cumulative number of minutes the SRST device was in SRST mode	≥ 0
6	None	Null indicator	Not used	*
Note Fields 7 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco Unity Port Usage—Record Type 121

This record contains Cisco Unity usage information.

Table J-25 Format of Record Type 121

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 121	121
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco Unity name	Text	Mandatory: name of subject Cisco Unity	ASCII characters

Table J-25 Format of Record Type 121 (continued)

Field Number	Field ID	Content	Description	Value
5	Total ports	Number	Total number of ports	≥ 0
6	Active ports	Number	Number of ports active at time stamp	≥ 0 and ≤ total ports
7	Port utilization	Number	Percentage of total ports active at time stamp	≥ 0 and ≤ 100
8	Total inbound ports	Number	Total number of inbound ports	≥ 0
9	Active inbound ports	Number	Number of active inbound ports at time stamp	≥ 0 and ≤ total inbound ports
10	Inbound port utilization	Number	Percentage of total inbound ports active at time stamp	≥ 0 and ≤ 100
11	Total outbound ports	Number	Total outbound ports	≥ 0
12	Active outbound ports	Number	Number of active outbound ports at time stamp	≥ 0 and ≤ total outbound ports
13	Outbound port utilization	Number	Percentage of total outbound ports active at time stamp	≥ 0 and ≤ 100
14	None	Null indicator	Not used	*
Note	Fields 15 through 37 are not used and contain the null indicator "*".			
38	None	Null indicator	Reserved	*

Consolidated DSP Usage for Cisco IOS Devices—Record Type 122

This record contains consolidated DSP usage information for Cisco IOS devices. There is one record per Cisco 1OS device.

Table J-26 Format of Record Type 122

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 122	122
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco IOS gateway name	Text	Mandatory: name of subject device	ASCII characters
5	Total DSP channels	Number	Total number of DSP channels on the device	≥ 0
6	Total active DSP channels	Number	Number of active DSP channels on the device at time stamp	≥ 0 and ≤ total DSP channels
7	Total DSP channels in use	Number	Number of DSP channels on the device that are reserved for serving calls	≥ 0 and ≤ total DSP channels
8	DSP channel utilization	Number	Percentage of DSP channels active on the device at time stamp	≥ 0 and ≤ 100
9	None	Null indicator	Not used	*

Table J-26 Format of Record Type 122 (continued)

Field Number	Field ID	Content	Description	Value
Note Fields 10 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco Unified Communications Manager Usage 2—Record Type 123

This record contains Cisco Unified Communications Manager resource utilization for software conference bridge, hardware conference bridge, MTP, MOH, and transcoder.

Table J-27 Format of Record Type 123

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 123	123
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco Unified Communications Manager name	Text	Mandatory: name of subject Cisco Unified Communications Manager	Example: CCM
5	Total MOH multicast resources	Number	Total number of MOH multicast resources configured on the Cisco Unified Communications Manager	≥ 0
6	Active MOH multicast resources	Number	Number of MOH multicast resources active on the Cisco Unified Communications Manager at time stamp	≥ 0 and ≤ total MOH multicast resources
7	Available MOH multicast resources	Number	Number of MOH multicast resources on the Cisco Unified Communications Manager available at time stamp	≥ 0 and ≤ total MOH multicast resources
8	MOH multicast resource utilization	Number	Percentage of total MOH multicast resources on the Cisco Unified Communications Manager active at time stamp	≥ 0 and ≤ 100
9	Total MOH unicast resources	Number	Total number of MOH unicast resources configured on the Cisco Unified Communications Manager	≥ 0
10	Active MOH unicast resources	Number	Number of MOH unicast resources active at time stamp	≥ 0 and ≤ total MOH unicast resources
11	Available MOH unicast resources	Number	Number of MOH unicast resources on the Cisco Unified Communications Manager available at time stamp	≥ 0 and ≤ total MOH unicast resources
12	MOH unicast resource utilization	Number	Percentage of total MOH unicast resources on the Cisco Unified Communications Manager active at time stamp	≥ 0 and ≤ 100

Table J-27 Format of Record Type 123 (continued)

Field Number	Field ID	Content	Description	Value
13	Total MTP resources	Number	Total number of MTP resources configured on the Cisco Unified Communications Manager	≥ 0
14	Active MTP resources	Number	Number of MTP resources active on the Cisco Unified Communications Manager at time stamp	≥ 0 and ≤ total MTP resources
15	Available MTP resources	Number	Number of MTP resources available on the Cisco Unified Communications Manager at time stamp	≥ 0 and ≤ total MTP resources
16	MTP resource utilization	Number	Percentage of total MOH resources active on the Cisco Unified Communications Manager at time stamp	≥ 0 and ≤ 100
17	Total transcoder resources	Number	Total number of transcoder resources on the Cisco Unified Communications Manager	≥ 0
18	Active transcoder resources	Number	Number of transcoder resources active on the Cisco Unified Communications Manager at time stamp	≥ 0 and ≤ total transcoder resources
19	Available transcoder resources	Number	Number of transcoder resources available on the Cisco Unified Communications Manager at time stamp	≥ 0 and ≤ total transcoder resources
20	Transcoder resource utilization	Number	Percentage of total transcoder resources on the Cisco Unified Communications Manager active at time stamp	≥ 0 and ≤ 100
21	Total software conference resources	Number	Total number of software conference resources on the Cisco Unified Communications Manager	≥ 0
22	Active software conference resources	Number	Number of software conference resources on the Cisco Unified Communications Manager active at time stamp	≥ 0 and ≤ total software conference resources
23	Available software conference resources	Number	Number of software conference resources on the Cisco Unified Communications Manager available at time stamp	≥ 0 and ≤ total software conference resources
24	Software conference resource utilization	Number	Percentage of total software conference resources on the Cisco Unified Communications Manager active at time stamp	≥ 0 and ≤ 100
25	Active software conferences	Number	Number of active software conferences on the Cisco Unified Communications Manager at time stamp	≥ 0
26	Completed software conferences	Number	Number of completed software conferences on the Cisco Unified Communications Manager	≥ 0
27	Total hardware conference resources	Number	Total number of hardware conference resources on the Cisco Unified Communications Manager	≥ 0

Table J-27 Format of Record Type 123 (continued)

Field Number	Field ID	Content	Description	Value
28	Active hardware conference resources	Number	Number of hardware conference resources on the Cisco Unified Communications Manager active at time stamp	≥ 0 and ≤ total hardware conference resources
29	Available hardware conference resources	Number	Number of hardware conference resources on the Cisco Unified Communications Manager available at time stamp	≥ 0 and ≤ total hardware conference resources
30	Hardware conference resource utilization	Number	Percentage of total hardware conference resources on the Cisco Unified Communications Manager active at time stamp	≥ 0 and ≤ 100
31	Active hardware conferences	Number	Number of hardware conferences on the Cisco Unified Communications Manager active at time stamp	≥ 0
32	Completed hardware conferences	Number	Number of completed hardware conferences on the Cisco Unified Communications Manager at time stamp	≥ 0
33	Registered analog access	Number	Number of analog access devices registered with the Cisco Unified Communications Manager at time stamp	≥ 0
34	Registered MGCP gateways	Number	Number of MGCP gateways registered with the Cisco Unified Communications Manager at time stamp	≥ 0
35	Registered hardware phones	Number	Number of hardware phones registered with the Cisco Unified Communications Manager at time stamp	≥ 0
36	Registered other station devices	Number	Number of other station devices registered with the Cisco Unified Communications Manager at time stamp	≥ 0
37	None	Null indicator	Not used	*
38	None	Null indicator	Reserved	*

FXS Port Usage for Cisco Unified Communications Manager-Controlled Gateways—Record Type 124

This record contains usage statistics for each FXS port on MGCP gateway registered with Cisco Unified Communications Manager.

Table J-28 Format of Record Type 124

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 124	124
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201

Table J-28 Format of Record Type 124 (continued)

Field Number	Field ID	Content	Description	Value
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Gateway name	Text	Mandatory: name of subject MGCP gateway registered with Cisco Unified Communications Manager	ASCII characters
5	FXS port name	Text	Mandatory: name of FXS port	ASCII characters
6	Calls completed	Number	Number of calls completed on this FXS port on the gateway	≥ 0
7	Outbound busy attempts	Number	Number of outbound busy attempts on this FXS port on the gateway	≥ 0
8	Port status	Number	Represents the status of the FXS port associated with this MGCP FXS device	≥ 0
9	None	Null indicator	Not used	*
Note Fields 10 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

FXO Port Usage for Cisco Unified Communications Manager-Controlled Gateways—Record Type 125

This record contains usage statistics for each FXO port on MGCP gateways registered with Cisco Unified Communications Manager.

Table J-29 Format of Record Type 125

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 125	125
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Gateway name	Text	Mandatory: name of subject MGCP gateway registered to Cisco Unified Communications Manager	ASCII characters
5	FXO port name	Text	Mandatory: name of FXO port	ASCII characters
6	Calls completed	Number	Number of calls completed on this FXO port on the gateway	≥ 0
7	Outbound busy attempts	Number	Number of outbound busy attempts on this FXO port on the gateway	≥ 0
8	Port status	Number	Represents the status of the FXO port associated with this MGCP FXO device	≥ 0
9	None	Null indicator	Not used	*

Table J-29 Format of Record Type 125 (continued)

Field Number	Field ID	Content	Description	Value
Note Fields 9 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco Unified Communications Manager CTI Manager Usage—Record Type 126

This record contains usage statistics for CTI Manager in Cisco Unified Communications Manager.

Table J-30 Format of Record Type 126

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 126	126
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco Unified Communications Manager name	Text	Mandatory: name of subject Cisco Unified Communications Manager	Example: CCM3
5	Total registered CTI ports	Number	Total number of CTI ports registered with the Cisco Unified Communications Manager	≥ 0
6	CTI link active	Number	Number of CTI links active on the Cisco Unified Communications Manager	≥ 0
7	CTI connection active	Number	Number of CTI connections active on the Cisco Unified Communications Manager	≥ 0
8	Devices open	Number	Number of CTI devices open	≥ 0
9	Lines open	Number	Number of CTI lines open	≥ 0
10	None	Null indicator	Not used	*
Note Fields 11 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco Unified Communications Manager Analog Access Gateway Usage—Record Type 127

This record contains usage statistics for each analog access gateway registered with Cisco Unified Communications Manager.

Table J-31 Format of Record Type 127

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 127	127
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco Unified Communications Manager name	Text	Mandatory: name of subject Cisco Unified Communications Manager	Example: CCM3
5	Analog access device name	Text	Mandatory: name of analog access device registered with Cisco Unified Communications Manager	ASCII characters
6	Ports active	Number	Number of ports active on this analog access device	≥ 0
7	None	Null indicator	Not used	*
Note Fields 8 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco Unified Communications Manager H323 Gateway Usage—Record Type 128

This record contains usage statistics for each H323 gateway registered with Cisco Unified Communications Manager.

Table J-32 Format of Record Type 128

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 128	128
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco Unified Communications Manager name	Text	Mandatory: name of subject Cisco Unified Communications Manager	Example: CCM3
5	H323 gateway name	Text	Mandatory: name of H323 gateway that is registered with Cisco Unified Communications Manager	ASCII characters
6	Calls active	Number	Number of calls active through the H323 gateway at time stamp	≥ 0
7	Calls attempted	Number	Number of calls attempted through the H323 gateway	≥ 0
8	Calls completed	Number	Number of calls completed through the H323 gateway	≥ 0

Table J-32 Format of Record Type 128 (continued)

Field Number	Field ID	Content	Description	Value
9	Calls in progress	Number	Number of calls in progress through the H323 gateway at time stamp	≥ 0
10	None	Null indicator	Not used	*
Note Fields 11 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco Unified Communications Manager Location Usage—Record Type 129

This record contains bandwidth usage statistics for each Cisco Unified Communications Manager location.

Table J-33 Format of Record Type 129

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 129	129
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco Unified Communications Manager name	Text	Mandatory: name of subject Cisco Unified Communications Manager	Example: CCM3
5	Location name	Text	Mandatory: name of the location defined in Cisco Unified Communications Manager	ASCII characters
6	Maximum bandwidth	Number	Total bandwidth (kbps) configured for the location	≥ 0
7	Available bandwidth	Number	Bandwidth available for the location at time stamp	≥ 0
8	Available bandwidth	Percentage	Percentage of maximum bandwidth available at time stamp	≥ 0 and ≤ 100
9	Calls in progress	Number	Number of calls in progress through the H323 gateway added to the Cisco Unified Communications Manager	≥ 0
10	None.	Null indicator	Not used	*
Note Fields 10 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco Unified Communications Manager Media Streaming Application Usage—Record Type 130

This record contains usage statistics for media streaming applications in Cisco Unified Communications Manager.

Table J-34 Format of Record Type 130

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 130	130
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco Unified Communications Manager name	Text	Mandatory: name of subject Cisco Unified Communications Manager	Example: CCM3
5	Total conferences	Number	Total number of conferences	≥ 0
6	Active conferences	Number	Number of conferences active on the Cisco Unified Communications Manager at time stamp	≥ 0
7	Percentage conferences active	Number	Percentage of total conferences active on the Cisco Unified Communications Manager at time stamp	≥ 0 and ≤ 100
8	Total conference streams	Number	Total number of conference streams on the Cisco Unified Communications Manager	≥ 0
9	Conference streams available	Number	Number of conference streams available on the Cisco Unified Communications Manager at time stamp	≥ 0
10	Conference streams active	Number	Number of conference streams active on the Cisco Unified Communications Manager at time stamp	≥ 0
11	Percentage conference streams active	Number	Percentage of conference streams active on the Cisco Unified Communications Manager at time stamp	≥ 0 and ≤ 100
12	Active MOH audio sources	Number	Number of MOH audio sources active on the Cisco Unified Communications Manager at time stamp	≥ 0
13	Total MOH streams	Number	Total number of MOH streams configured on the Cisco Unified Communications Manager	≥ 0
14	Available MOH streams	Number	Number of MOH streams available on the Cisco Unified Communications Manager at time stamp	≥ 0
15	Active MOH streams	Number	Number of MOH streams active on the Cisco Unified Communications Manager at time stamp	≥ 0
16	Percentage MOH streams active	Number	Percentage of total MOH streams on the Cisco Unified Communications Manager active at time stamp	≥ 0 and ≤ 100

Table J-34 Format of Record Type 130 (continued)

Field Number	Field ID	Content	Description	Value
17	Total MTP connections	Number	Total number of MTP connections on the Cisco Unified Communications Manager	≥ 0
18	Active MTP instances	Number	Number of MTP instances active on the Cisco Unified Communications Manager at time stamp	≥ 0
19	Total MTP streams	Number	Total number of MTP streams on the Cisco Unified Communications Manager	≥ 0
20	Available MTP streams	Number	Number of MTP streams available on the Cisco Unified Communications Manager at time stamp	≥ 0
21	Active MTP streams	Number	Number of MTP streams active on the Cisco Unified Communications Manager at time stamp	≥ 0
22	Percentage active MTP streamS	Number	Percentage of total MTP streams on the Cisco Unified Communications Manager active at time stamp	≥ 0 and ≤ 100
23	None	Null indicator	Not used	*
Note Fields 24 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco Unified Communications Manager MOH Usage—Record Type 131

This record contains usage statistics for each music on hold (MOH) device registered with Cisco Unified Communications Manager.

Table J-35 Format of Record Type 131

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 131	131
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco Unified Communications Manager name	Text	Mandatory: name of subject Cisco Unified Communications Manager	Example: CCM3
5	MOH device name	Text	Mandatory: name of the MOH device registered to the Cisco Unified Communications Manager	ASCII characters
6	Highest active resources	Number	Highest active resources on the MOH device	≥ 0
7	Total multicast resources	Number	Total number of multicast resources on the MOH device	≥ 0
8	Available multicast resources	Number	Number of multicast resources on the MOH device available at time stamp	≥ 0

Table J-35 Format of Record Type 131 (continued)

Field Number	Field ID	Content	Description	Value
9	Active multicast resource	Number	Number of multicast resources on the MOH device active at time stamp	≥ 0
10	Percentage active multicast resources	Number	Percentage of total multicast resources on the MOH device active at time stamp	≥ 0 and ≤ 100
11	Total unicast resources	Number	Total number of unicast resources on the MOH device	≥ 0
12	Available unicast resources	Number	Number of unicast resources available on the MOH device at time stamp	≥ 0
13	Active unicast resource	Number	Number of unicast resources on the MOH device active at time stamp	≥ 0
14	Percentage active unicast resources	Number	Percentage of total unicast resources on the MOH device active at time stamp	≥ 0 and ≤ 100
15	None	Null indicator	Not used	*
Note Fields 16 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco Unified Communications Manager MTP Usage—Record Type 132

This record contains usage statistics for each media termination point (MTP) registered with Cisco Unified Communications Manager.

Table J-36 Format of Record Type 132

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 132	132
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco Unified Communications Manager name	Text	Mandatory: name of subject Cisco Unified Communications Manager	Example: CCM3
5	MTP device name	Text	Mandatory: name of MTP device registered to the Cisco Unified Communications Manager	ASCII characters
6	Total resources	Number	Total number of resources on the MTP device	≥ 0
7	Available resource	Number	Number of resources available on the MTP device at time stamp	≥ 0
8	Active resources	Number	Number of resources active on the MTP device at time stamp	≥ 0
9	Percentage active resources	Number	Percentage of total resources active on the MTP device at time stamp	≥ 0 and ≤ 100

Table J-36 Format of Record Type 132 (continued)

Field Number	Field ID	Content	Description	Value
10	None	Null indicator	Not used	*
Note	Fields 11 through 37 are not used and contain the null indicator "*".			
38	None	Null indicator	Reserved	*

Cisco Unified Communications Manager Hardware Conference Bridge Usage—Record Type 133

This record contains usage statistics for each Hardware Conference Bridge registered with Cisco Unified Communications Manager.

Table J-37 Format of Record Type 133

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 133	133
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco Unified Communications Manager name	Text	Mandatory: name of subject Cisco Unified Communications Manager	Example: CCM3
5	Hardware conference bridge name	Text	Mandatory: name of hardware conference bridge	ASCII characters
6	Completed conferences	Number	Number of conferences completed on this hardware conference bridge	≥ 0
7	Active conferences	Number	Number of conferences active on this hardware conference bridge at time stamp	≥ 0
8	Total resources	Number	Total number of resources on this hardware conference bridge	≥ 0
9	Available resource	Number	Number of resources available on this hardware conference bridge at time stamp	≥ 0
10	Active resources	Number	Number of resources active on this hardware conference bridge at time stamp	≥ 0
11	Percentage active resources	Number	Percentage of total resources active on this hardware conference bridge at time stamp	≥ 0 and ≤ 100
12	None	Null indicator	Not used	*
Note	Fields 13 through 37 are not used and contain the null indicator "*".			
38	None	Null indicator	Reserved	*

Cisco Unified Communications Manager Software Conference Bridge Usage—Record Type 134

This record contains usage statistics for each software conference bridge registered with Cisco Unified Communications Manager.

Table J-38 Format of Record Type 134

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 134	134
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco Unified Communications Manager name	Text	Mandatory: name of subject Cisco Unified Communications Manager	Example: CCM3
5	Software conference bridge name	Text	Mandatory: name of software conference bridge registered to the Cisco Unified Communications Manager	ASCII characters
6	Conferences completed	Number	Number of completed conferences on this software conference bridge	≥ 0
7	Active conferences	Number	Number of conferences active on this software conference bridge at time stamp	≥ 0
8	Total resources	Number	Total number of resources on this software conference bridge	≥ 0
9	Available resource	Number	Number of resources available on this software conference bridge at time stamp	≥ 0
10	Active resources	Number	Number of resources active on this software conference bridge at time stamp	≥ 0
11	Percentage active resources	Number	Percentage of resources active on this software conference bridge at time stamp	≥ 0 and ≤ 100
12	None	Null indicator	Not used	*
Note Fields 13 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco Unified Communications Manager Transcoder—Record Type 135

This record contains usage statistics for each transcoder device registered with Cisco Unified Communications Manager.

Table J-39 Format of Record Type 135

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 135	135
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco Unified Communications Manager name	Text	Mandatory: name of subject Cisco Unified Communications Manager	Example: CCM3
5	Transcoder device name	Text	Mandatory: name of transcoder device registered to this Cisco Unified Communications Manager	ASCII characters
6	Total resources	Number	Total number of resources on the transcoder device	≥ 0
7	Available resource	Number	Number of resources available on the transcoder device at time stamp	≥ 0
8	Active resources	Number	Number of resources active on the transcoder device at time stamp	≥ 0
9	Percentage active resources	Number	Percentage active on the transcoder device at time stamp	≥ 0 and ≤ 100
10	None	Null indicator	Not used	*
Note Fields 11 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

T1 PRI Usage for Cisco Unified Communications Manager-Controlled Gateways—Record Type 136

This record contains usage statistics for each T1 PRI port on MGCP gateways registered with Cisco Unified Communications Manager.

Table J-40 Format of Record Type 136

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 136	136
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Gateway name	Text	Mandatory: name of subject MGCP gateway registered with Cisco Unified Communications Manager	ASCII characters
5	DS1 name	Text	Mandatory: name of the T1 PRI port	ASCII characters
6	Completed calls	Number	Number of calls completed on this T1 PRI port on the gateway	≥ 0

Table J-40 Format of Record Type 136 (continued)

Field Number	Field ID	Content	Description	Value
7	Outbound busy attempts	Number	Number of outbound busy attempts on this T1 PRI port on the gateway	≥ 0
8	None	Null indicator	Not used	*
Note Fields 9 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

E1 PRI Usage for Cisco Unified Communications Manager-Controlled Gateways—Record Type 137

This record contains usage statistics for each E1 PRI port on MGCP gateways registered with Cisco Unified Communications Manager.

Table J-41 Format of Record Type 137

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 137	137
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Gateway name	Text	Mandatory: name of subject MGCP gateway registered with Cisco Unified Communications Manager	ASCII characters
5	DS1 name	Text	Mandatory: name of E1 PRI port	ASCII characters
6	Calls completed	Number	Number of calls completed on this E1 PRI port on the gateway	≥ 0
7	Outbound busy attempts	Number	Number of outbound busy attempts on this E1 PRI port on the gateway	≥ 0
8	None	Null indicator	Not used	*
Note Fields 9 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

T1 CAS Usage for Cisco Unified Communications Manager-Controlled Gateways—Record Type 138

This record contains usage statistics for each T1 CAS port on MGCP gateways registered with Cisco Unified Communications Manager.

Table J-42 Format of Record Type 138

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 138	138
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Gateway name	Text	Mandatory: name of subject gateway	ASCII characters
5	DS1 name	Text	Mandatory: name of the T1 CAS port	ASCII characters
6	Calls completed	Number	Number of calls completed on this T1 CAS port on the gateway	≥ 0
7	Outbound busy attempts	Number	Number of outbound busy attempts on this T1 CAS port on the gateway	≥ 0
8	None	Null indicator	Not used	*
Note Fields 9 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Record Type 139—Not Used

Note Record Type 139 is reserved for future use.

Cisco Unity Connection Usage—Record Type 140

This record contains Cisco Unity Connection usage information.

Table J-43 Format of Record Type 140

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 140	140
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco Unity Connection name	Text	Mandatory: name of the subject Cisco Unity Connection	ASCII characters
5	Total ports	Number	Total number of ports on the system with Cisco Unity Connection	≥ 0
6	Active ports	Number	Active number of ports on the system with Cisco Unity Connection	≥ 0 and ≤ total inbound ports
7	Port utilization	Number	Percentage port utilization on the system with Cisco Unity Connection	≥ 0 and ≤ 100

Table J-43 Format of Record Type 140 (continued)

Field Number	Field ID	Content	Description	Value
8	Total inbound ports	Number	Total number of inbound ports on the system with Cisco Unity Connection	≥ 0 and ≤ total inbound ports
9	Active inbound ports	Number	Active number of inbound ports on the system with Cisco Unity Connection	≥ 0 and ≤ total inbound ports
10	Inbound port utilization	Number	Percentage inbound port utilization on the system with Cisco Unity Connection	≥ 0 and ≤ 100
11	Total inbound ports	Number	Total number of outbound ports on the system with Cisco Unity Connection	≥ 0
12	Active inbound ports	Number	Active number of outbound ports on the system with Cisco Unity Connection	≥ 0 and ≤ total inbound ports
13	Inbound port utilization	Number	Percentage outbound port utilization on the system with Cisco Unity Connection	≥ 0 and ≤ 100
14	None	Null indicator	Not used	*
Note Fields 15 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco IP Contact Center Usage—Record Type 141

This record contains Cisco IP Contact Center usage information.

Table J-44 Format of Record Type 141

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 141	141
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	IP Contact Center name	Text	Mandatory: name of IP Contact Center host	ASCII characters
5	Instance name	Text	Mandatory: name of instance	ASCII characters
6	Router name	Text	Mandatory: name of router component	ASCII characters
7	Agents logged on	Number	number of contact center agents currently logged on	≥ 0
8	Calls in process	Number	Number of calls in progress	≥ 0
9	Calls per second	Number	Number of inbound calls per second	≥ 0
10	None	Null indicator	Not used	*
Note Fields 11 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Cisco Unified Communications Manager SIP Device Usage—Record Type 142

This record contains usage information for SIP devices in Cisco Unified Communications Manager.

Table 10-45 Format of Record Type 142

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 142	142
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Cisco Unified Communications Manager name	Text	Mandatory: name of Cisco Unified Communications Manager	ASCII characters
5	SIP device name	Text	Mandatory: name of SIP device	ASCII characters
6	Calls active	Number	number of calls active	≥ 0
7	Calls attempted	Number	Number of calls attempted	≥ 0
8	Calls completed	Number	Number of calls completed	≥ 0
9	Calls in progress	Number	Number of calls in progress	≥ 0
10	None	Null indicator	Not used	*
Note Fields 11 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Server Memory Usage—Record Type 143

This record contains memory usage information for a server running one of the following: Cisco Unified Communications Manager, IP Contact Center, Cisco Unity, or Cisco Unity Connection.

Table J-46 Format of Record Type 143

Field Number	Field ID	Content	Description	Value
1	Record ID	143	Mandatory: record type 143	143
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Device name	Text	Mandatory: name of the Cisco Unified Communications Manager, IP Contact Center, Cisco Unity, or Cisco Unity Connection	ASCII characters
5	Total memory	Number	Total RAM in kilobytes	≥ 0
6	Used memory	Number	Used RAM in kilobytes	≥ 0
7	Free memory	Number	Free RAM in kilobytes	≥ 0
8	Memory Utilization	Number	Percentage of used memory	≥ 0 and ≤ 100

Table J-46 Format of Record Type 143 (continued)

Field Number	Field ID	Content	Description	Value
9	Linux kilobytes buffered	Number	Linux buffered memory in kilobytes	≥ 0
10	Linux kilobytes cached	Number	Linux cached memory in kilobytes	≥ 0
11	Linux kilobytes shared	Number	Linux shared memory in kilobytes	≥ 0
12	Linux kilobytes total swap	Number	Linux total swap memory in kilobytes	≥ 0
13	Linux kilobytes used swap	Number	Linux used swap memory in kilobytes	≥ 0
14	Linux kilobytes free swap	Number	Linux free swap memory in kilobytes	≥ 0
15	Window cached bytes	Number	Window cached memory in kilobytes	≥ 0
16	Window commit limit	Number	Window total virtual memory in kilobytes	≥ 0
17	Window committed bytes	Number	Window used virtual memory in kilobytes	≥ 0
18	None	Null indicator	Not used	*
Note	Fields 19 through 37 are not used and contain the null indicator "*".			
38	None	Null indicator	Reserved	*

Server CPU Usage—Record Type 144

This record contains CPU usage information for a server running one of the following: Cisco IP Contact Center, Cisco Unity, or Cisco Unity Connection.

Table J-47

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Mandatory: record type 144	144
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	Device name	Text	Mandatory: name of the Cisco IP Contact Center, Cisco Unity, or Cisco Unity Connection	ASCII characters
5	Total CPU usage	Number	Measured CPU percentage utilization for all CPUs at time stamp	≥ 0 and ≤ 100
6	CPU 1 usage	Number	Measured CPU percentage utilization for CPU 1 at time stamp	≥ 0 and ≤ 100

Table J-47

Field Number	Field ID	Content	Description	Value
7	CPU 2 usage	Number	Optional: Measured CPU percentage utilization for CPU 2 at time stamp	≥ 0 and ≤ 100
8	CPU 3 usage	Number	Optional: Measured CPU percentage utilization for CPU 3 at time stamp	≥ 0 and ≤ 100
9	CPU 4 usage	Number	Optional: Measured CPU percentage utilization for CPU 4 at time stamp	≥ 0 and ≤ 100
10	CPU 5 usage	Number	Optional: Measured CPU percentage utilization for CPU 5 at time stamp	≥ 0 and ≤ 100
11	None	Null indicator	Not used	*
Note Fields 12 through 37 are not used and contain the null indicator "*".				
38	None	Null indicator	Reserved	*

Record Type 145—Not Used.

Record type 145 is not in use and is reserved.

Record Type 146—Not Used.

Record type 146 is not in use and is reserved.

Record Type 147—Not Used.

Record type 147 is not in use and is reserved.

Record Type 148—Not Used

Record type 148 is not in use and is reserved.

Cisco IOS Gateway Total Utilization—Record Type 149

This is an addition to record 102. This record has the total utilization for Cisco IOS gateways. Cisco IOS gateways support T1/E1 PRI, T1/E1 CAS, FXO, FXS, E&M and BRI ports.

Table J-48 Format of Record Type 149

Field Number	Field ID	Content	Description	Value
1	Record ID	149	Mandatory: record type 149	149
2	Date	yyyymmdd	Mandatory: calendar date	Example: 20070201

Table J-48 Format of Record Type 149 (continued)

Field Number	Field ID	Content	Description	Value
3	Time stamp	hhmmss	Mandatory: wall clock time	Example: 230000
4	IOS gateway name	Text	Mandatory: name of subject IOS gateway	Example: CiscoDallasMetro
5	Percentage active total BRI	Number	Percentage BRI voice utilization for the H323 gateway at time stamp	≥ 0 and ≤ 100
6	Percentage active total T1 CAS	Number	Percentage T1 CAS voice utilization for the H323 gateway at time stamp RI voice utilization for the route list at time stamp	≥ 0 and ≤ 100
7	Percentage active voice total T1 PRI	Number	Percentage T1 PRI voice utilization for the H323 gateway at time stamp	≥ 0 and ≤ 100
8	Percentage active voice E1 CAS	Number	Percentage E1 CAS voice utilization for the H323 gateway list at time stamp	≥ 0 and ≤ 100
9	Percentage active voice E1 PRI	Number	Percentage E1 PRI voice utilization for the H323 gateway list at time stamp	≥ 0 and ≤ 100
10-37	None	Null indicator	Not used. Entry must be an asterisk (*)	
38	Study name	Text	Reserved: name of the study that generated this record.	Entry must be an asterisk (*)

Error Records—Record Type 9*nnn*

When an error occurs while polling or collecting data on a device, Operations Manager writes error records for the device. When these errors occur during performance polling, Operations Manager writes one for each record type that is related to the device type, prefixing the record type with 9; Table J-48 provides an example.

Device Type	Record Types	Error Record Types
Cisco Unity	121	9121
	143	9143
	144	9144

When polling or data collection errors occur during node-to-node testing, Operations Manager writes a single error record for the test type.

Table J-49 Format of Record Type 9nnn

Field Number	Field ID	Content	Description	Value
1	Record ID	9nnn	Mandatory: 9 precedes the record type that is related to the device or node-to-node test on which the polling or data collection error occurred.	Example: 9200 is an error for record type 200.
2	Date	yyyymmdd	Calendar date	Example: 20070201.
3	Time stamp	hhmmss	Wall clock time	Example: 230000.
4	Device	Text	Device IP address or name	Example: cluster1.cisco.com.
5	Error message	Text	Error message	Example: Cannot collect data from the device. No active HTTP server.
6	Error number	Text	Error number, if provided; see error message for meaning.	Example: 2
Fields 12 through 38 are not used and contain the null indicator "*".				

Node-to-Node Test Record Formats

For more information, see Data Files—Maintenance and Usage, page J-1 and Error Records—Record Type 9nnn, page J-58.

The following are the formats for each node-to-node test record type:

- Echo—Record Type 200, page J-59
- Ping Path Echo—Record Type 201, page J-60
- Record Type 202—Not Used, page J-62
- Ping Path Echo—Record Type 204, page J-62
- Jitter MOS, ICPIF, and Processed Data—Record Type 205, page J-63

Echo—Record Type 200

This record format captures end-to-end statistics for the following types of tests:

- ICMP Echo
- UDP Echo
- Gatekeeper Registration Delay

Table J-50 Format of Record Type 200

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Record type 200	200
2	Date	yyyymmdd	Calendar date	Example: 20070201
3	Time stamp	hhmmss	Wall clock time	Example: 230000
4	Completion time	Number	Round-trip time (RTT), in milliseconds	Between 0 and 4294967295
5	Completion status	Number	The allowed numbers are: • 1—OK • 2—disconnected • 3—overThreshold • 4—timeout • 5—busy • 6—notConnected • 7—dropped • 8—sequenceError • 9—verifyError • 10—applicationSpecific • 11—dnsServerTimeout • 12—tcpConnectTimeout • 13—httpTransactionTimeout • 14—dnsQueryError • 15—httpError • 16—error	Between 1 and 16
6	Application-specific completion status	Number	(Optional) An application-specific status that is valid only when completion status is set to applicationSpecific (10).	Between 1001 and 2147483647
7	Status description	Number	(Optional) The description for the completion status when completion status is set to applicationSpecific (10). Default value is blank.	ASCII characters
8	None	Null indicator	Not used	*
Note Fields 9 through 37 are not used and contain the null indicator "*".				
38	Test name	Text	Name of the node-to-node test	Sjc-VGtest

Ping Path Echo—Record Type 201

This record format captures hop-by-hop statistics for Ping Path Echo tests. The tests record information from source to destination.

Table J-51 Format of Record Type 201

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Record type 201	201
2	Date	yyyymmdd	Calendar date	Example: 20070201
3	Time stamp	hhmmss	Wall clock time	Example: 230000
4	Completion time	Number	Round-trip time (RTT), in milliseconds	Between 0 and 4294967295
5	Hop ID	Number	Unique ID chosen by the study and given to a hop on this path.	Maximum value is 30
6	Hop address	String	IP Address of the hop	ASCII characters
7	Completion status	Number	The allowed numbers are: • 1—OK • 2—disconnected • 3—overThreshold • 4—timeout • 5—busy • 6—notConnected • 7—dropped • 8—sequenceError • 9—verifyError • 10—applicationSpecific • 11—dnsServerTimeout • 12—tcpConnectTimeout • 13—httpTransactionTimeout • 14—dnsQueryError • 15—httpError • 16—error	Between 1 and 16
8	Application-specific completion status	Number	(Optional) Application-specific status that is valid only when completion status is set to applicationSpecific (10).	Between 1001 and 2147483647
9	Status description	Text	(Optional) Description for the completion status when completion status is set to applicationSpecific (10). Default value is blank.	ASCII characters
10	None	Null indicator	Not used	*
Note Fields 11 through 37 are not used and contain the null indicator "*".				
38	Test name	Text	Name of the node-to-node test	Sjc-VGtest

Record Type 202—Not Used

Record type 202 is not in use and is reserved.

Ping Path Echo—Record Type 204

This record format captures end-to-end statistics for Ping Path Echo tests. The tests are from the source to the destination.

Table J-52 Format of Record Type 204

Field Number	Field ID	Content	Description	Value
1	Record ID	nnn	Record type 204	204
2	Date	yyyymmdd	Calendar date	Example: 20070201
3	Time stamp	hhmmss	Wall clock time	Example: 230000
4	Completion time	Number	The round-trip time (RTT) in milliseconds	Between 0 and 4294967295
5	Hop ID	Number	Unique ID given to a hop on this path chosen by the study. For this record, the hop ID is always 1.	1
6	Hop address	String	Mandatory: IP address of the destination	ASCII characters
7	Completion status	Number	The allowed numbers are: • 1—OK • 2—disconnected • 3—overThreshold • 4—timeout • 5—busy • 6—notConnected • 7—dropped • 8—sequenceError • 9—verifyError • 10—applicationSpecific • 11—dnsServerTimeout • 12—tcpConnectTimeout • 13—httpTransactionTimeout • 14—dnsQueryError • 15—httpError • 16—error	Between 1 and 16
8	Application-specific completion status	Number	(Optional) The application-specific status that is valid only when Completion Status is set to applicationSpecific (10).	Between 1001 and 2147483647

Table J-52 Format of Record Type 204 (continued)

Field Number	Field ID	Content	Description	Value
9	Status description	Text	(Optional) This is the description for the completion status when Completion Status is set to applicationSpecific (10). Default value is blank.	ASCII characters
10	None	Null indicator	Not used	*
Note Fields 10 through 37 are not used and contain the null indicator "*".				
38	Test name	Text	Name of the node-to-node test	Sjc-VGtest

Jitter MOS, ICPIF, and Processed Data—Record Type 205

This record format stores MOS and ICPIF values and processed jitter statistics values.

Table J-53 Format of Record Type 205

Field Number	Field ID	Content	Description	Value
1	Record ID	205	Mandatory: record type 205	205
2	Date	yyyymmdd	Calendar date	Example: 20070201
3	Time stamp	hhmmss	Wall clock time	Example: 230000
4	ICPIF	Number	Mandatory: Icpif Value	Example
5	Node-to-node quality	Number	Mandatory: MOS value	Example: 3.6
6	Source to destination packet loss	Number	Mandatory: number of packets	Any positive integer[1]
7	Destination to source packet loss	Number	Mandatory: number of packets	Any positive integer[1]
8	Source to destination jitter	Number	Mandatory: milliseconds	≥ 0 and ≤ 100
9	Destination to source jitter	Number	Mandatory: milliseconds	≥ 0 and ≤ 100
10	Average latency	Number	Mandatory: milliseconds	≥ 0 and ≤ 100
11	None	Null indicator	Not used	*
Note Fields 12 through 37 are not used and contain the null indicator "*".				
38	Test name	Text	Name of the node-to-node test	Sjc-VGtest

1. Positive integers must be 32 bit.

INDEX

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z