



## Introduction

---

These topics provide an overview of IP Communications Operations Manager (Operations Manager):

- [What Is Operations Manager?, page 1-1](#)
- [Is Operations Manager Ready to Use?, page 1-2](#)
- [How Will I Use Operations Manager for Day-to-Day Operations?, page 1-4](#)
- [How Does Operations Manager Work?, page 1-10](#)
- [Getting Started with Operations Manager, page 1-14](#)
- [Using Displays and Reports, page 1-17](#)
- [Selecting Objects and Groups, page 1-18](#)
- [Understanding Your User Role, page 1-20](#)
- [Responding to Security Alerts, page 1-21](#)
- [Responding to Messages About Device Limits, page 1-21](#)

## What Is Operations Manager?

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 thus is nondisruptive 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.
- **Clickable information in notification messages**—Includes context-sensitive links to more detailed information about service outages.
- **Context-sensitive links to other CiscoWorks tools and Cisco tools**—For managing IP communications implementations.

Operations Manager also does the following:

- **Presents service-quality alerts**—Uses information from CiscoWorks IP Communications Service Monitor 1.0, when it is also deployed, to:
  - Display Mean Opinion Scores (MOSs) associated with poor voice quality between pairs of endpoints (Cisco IP phones, Cisco Unity messaging systems, or voice gateways) involved in a call and other associated details about the voice-quality problem.
  - Enable you to perform a probable path trace between the two endpoints and reports on any outages or problems on intermediate nodes in the path.
- **Highlights current connectivity-related and registration-related outages affecting Cisco 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 IP phone status changes and creates a variety of reports that document move, add, and change operations on Cisco 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).

## 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 and Configuration Guide for IP Communications Operations Manager*.

To use Operations Manager, you must import devices into the Operations Manager inventory as explained in [Importing Devices from the DCR, page 15-9](#).

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

Before Operations Manager can start to monitor your network:

- You need to configure 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 must complete inventory collection.

[Table 1-1](#) lists all the steps you need to complete.

**Table 1-1** *How to Start Monitoring Devices*

	Description	References
<b>Step 1</b>	Add devices to the DCR. You have three options: <ul style="list-style-type: none"> <li>• Use Operations Manager to add devices to the DCR. This is called physical discovery.</li> <li>• Share a master repository with applications on other servers.</li> <li>• Bulk import using a seed file to import devices into the DCR.</li> </ul>	<a href="#">Adding Devices to the DCR From Operations Manager, page 15-4</a> <a href="#">DCR Masters and Slaves, page 15-6</a> See the instructions in the Common Services online help.
<b>Step 2</b>	Configure device selection.	<a href="#">Importing Devices into Operations Manager, page 15-8</a>
<b>Step 3</b>	Allow inventory collection to complete and start to monitor devices.	
<b>Step 4</b>	Verify device import by using the Service Level View.	<a href="#">Verifying Device Import, page 15-14</a>

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.

[Table 1-2](#) 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 1-2** *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, and Service Quality Alerts). There are two default views. You can add more views.	<a href="#">Managing Views, page 6-1</a>
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.	<a href="#">Using Notifications, page 14-1</a>
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.	<a href="#">Configuring Polling and Thresholds, page 17-1</a>

**Table 1-2** 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 <a href="#">Using Performance Graphs, page 7-1</a> . For information on setting polling parameters, see <a href="#">Managing Polling Parameters, page 17-11</a> .
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 CallManagers.	<a href="#">Using Synthetic Tests, page 9-1</a>
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.	<a href="#">Using Node-To-Node Tests, page 10-1</a>
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.	<a href="#">Using Phone Status Testing, page 8-3</a>
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.	<a href="#">Understanding How Operations Manager Monitors SRST, page 18-1</a>
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.	<a href="#">Working with the Device Inventory Collection Schedule, page 15-22</a>
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.)	<a href="#">Working with IP Phone Discovery, page 15-22</a>
Update the Purging Scheduler.	By default, Operations Manager purges the database at midnight. You can edit the schedule.	<a href="#">Setting System-Wide Parameters Using System Preferences, page 19-12</a>
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.	<a href="#">Integrating SNMP Trap Receiving with Other Trap Daemons or NMSs, page 19-5</a>

## 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, and Service Quality Alerts) 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.

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 19-3](#).

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

- [What Are the Monitoring Dashboards?, page 1-5](#)
- [What Are Diagnostics?, page 1-7](#)
- [What Are Reports?, page 1-8](#)
- [What Are Notifications?, page 1-9](#)
- [What Is Device Management?, page 1-9](#)

## 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 1-5](#)
- [What Is the Alerts and Events Display?, page 1-6](#)
- [What Is the Service Quality Alerts Display?, page 1-6](#)
- [What Is the Phone Activities Display?, page 1-6](#)

## 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 CallManager clusters, Cisco CallManager Express, associated gateways, gatekeepers, application servers, and Survivable Remote Site Telephony (SRST) enabled devices, as well as their registration status with Cisco CallManager.

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 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 a fault.

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 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 MIB 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 IP Communications 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 and Deleting Service Monitors, page 19-7](#).

## 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 CallManager, or have gone into SRST mode.

## What Are Diagnostics?

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 1-7
- [What Are Synthetic Tests?](#), page 1-7
- [What Are Node-to-Node Tests?](#), page 1-7

## 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 CallManager.

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 CallManager and Cisco CallManager Express
- Cisco TFTP Server
- Cisco Emergency Responder
- Cisco Conference Connection
- Cisco Unity and Cisco Unity Express

## 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 1-8
- [What Is Service Quality?](#), page 1-8
- [What Are IP Phones and Applications Reports and IP Phone Status Change Reports?](#), page 1-8
- [What Is a Personalized Report?](#), page 1-8

## 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).

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 31 days.

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

## What Is Service Quality?

Service Quality reports enable you to view alerts and events for service quality that occurred during the past 31 days. The available information includes alert status and date, related device and device components, annotations (informational text you entered), and event details.

**Note**

---

Service Quality is useful only if you have purchased a license for CiscoWorks IP Communications Service Monitor (Service Monitor). For more information, see *User Guide for CiscoWorks IP Communications 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 CallManager. 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 only 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. 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 1-3](#) lists all the steps you need to complete.

**Table 1-3**      **How to Start Monitoring Devices**

	Description	References
<b>Step 1</b>	<p>Add devices to the DCR.</p> <p>You have three options:</p> <ul style="list-style-type: none"> <li>• Use Operations Manager to add devices to the DCR. This is called physical discovery</li> <li>• Share a master repository with applications on other servers.</li> <li>• Bulk import using a seed file to import devices into the DCR.</li> </ul>	<p><a href="#">Understanding the Device and Credentials Repository, page 15-3</a></p> <p>See the instructions in the Common Services online help.</p>
<b>Step 2</b>	Configure device selection.	<ul style="list-style-type: none"> <li>• <a href="#">Automatically Importing DCR Devices, page 15-10</a></li> <li>• <a href="#">Manually Importing DCR Devices, page 15-11</a></li> </ul>
<b>Step 3</b>	Allow inventory collection to complete and start to monitor devices.	<a href="#">Performing Inventory Collection, Viewing Details, and Deleting Devices, page 15-16</a>
<b>Step 4</b>	Verify device import by using the Service Level View.	<a href="#">Verifying Device Import, page 15-14</a>

## How Does Operations Manager Work?

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

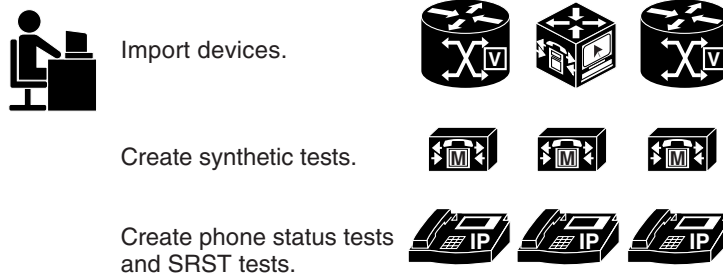
- [Users Perform Device Management and Configuration, page 1-10](#)
- [Operations Manager Performs Ongoing Monitoring, Analysis, and Notification, page 1-12](#)
- [Users Respond to Notifications and Alerts, page 1-14](#)

## Users Perform Device Management and Configuration

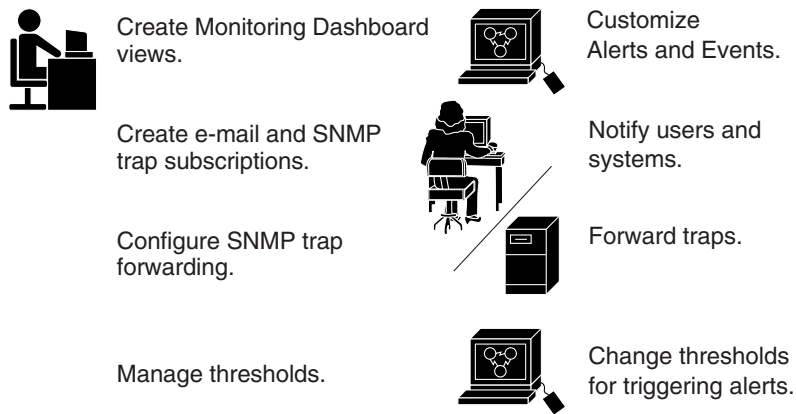
Users supply the information that tells Operations Manager what to monitor. [Figure 1-1](#) shows a user importing devices and phones, and performing optional configuration tasks to optimize Operations Manager.

Figure 1-1 The Role of User Input

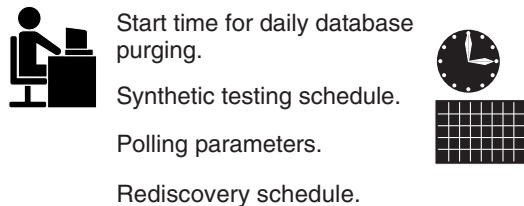
## What to Manage in the IP Telephony Environment



## How to Manage Information for Alerts and Traps



## When to Update Data



141508

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 CallManager) 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:

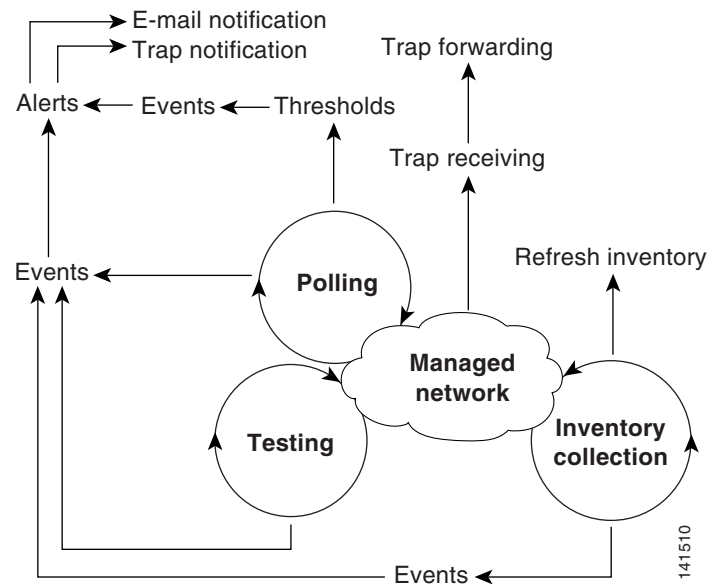
- Create views, enabling users to monitor specific groups of devices on the Monitoring Dashboard displays.
- Create subscriptions to send e-mail and generated SNMP trap notification to users and systems, respectively.
- Determine where to forward traps by configuring the port to which Operations Manager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

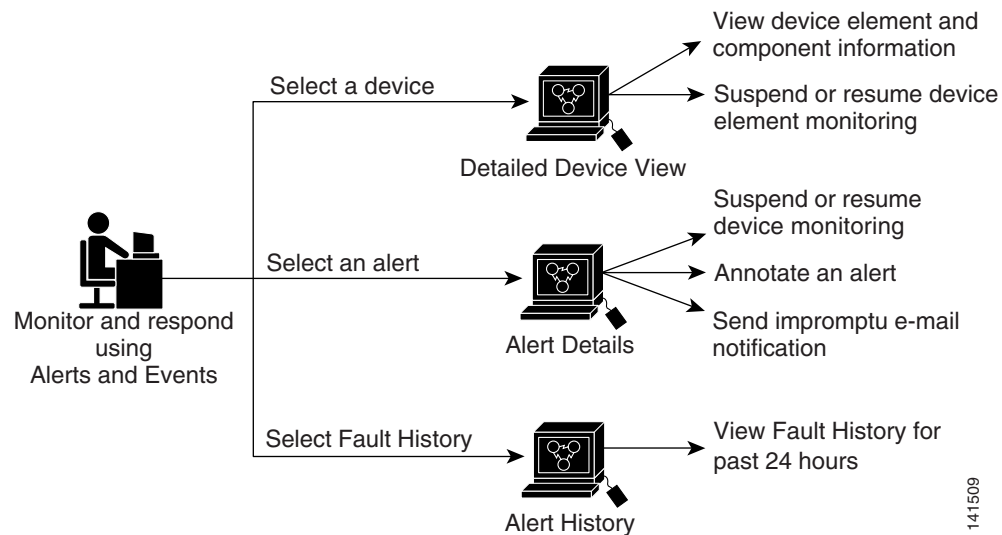
- [MIBs Polled and Perfmon Counter Objects Used, page A-1](#)
- [Processed and Pass-Through Traps, and Unidentified Traps and Events, page B-1](#)
- [Events Processed, page D-1](#)

- [Polling—SNMP and ICMP, page F-1](#)
- [How Operations Manager Calculates Repeated Restarts and Flapping, page G-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 1-15](#)
- [Working with Operations Manager Windows, page 1-15](#)
- [Using Displays and Reports, page 1-17](#)
- [Selecting Objects and Groups, page 1-18](#)
- [Understanding Your User Role, page 1-20](#)
- [Responding to Security Alerts, page 1-21](#)
- [Responding to Messages About Device Limits, page 1-21](#)

## Starting Operations Manager

To start Operations Manager, from the Windows desktop select **Start > Programs > IPC Operations Manager 1.0 and Service Monitor 1.0 > IPC Operations Manager 1.0 and Service Monitor 1.0**.

**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 IP Communications 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 1-15.](#))

## 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 > IP Communications Operations Manager > IP Communications 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 1-15](#)
- [Why do I see the error "The page cannot be displayed"?, page 1-16](#)
- [When I press the Enter key, why doesn't Operations Manager complete the current task?, page 1-16](#)
- [Where is the Help button?, page 1-16](#)

### 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.

## 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.

## Understanding the 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 IP Communications Operations Manager 1.0*. You can view the release notes on Cisco.com.

## Using Displays and Reports

Operations Manager presents information in displays, and you can also generate 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:



- **Sorting**—You can sort a display in the order you prefer by clicking any clickable column heading.
- **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](#).
- **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 2,000 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.

## 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 2,000 records available, all records are sorted, not just those that are displayed. The first 2,000 records are displayed after sorting.

## Viewing Data from Reports with Over 2000 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 1-18](#).

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 1-17](#).

## Exporting Data from a Display or Report

All 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.
- 

## 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.
- 

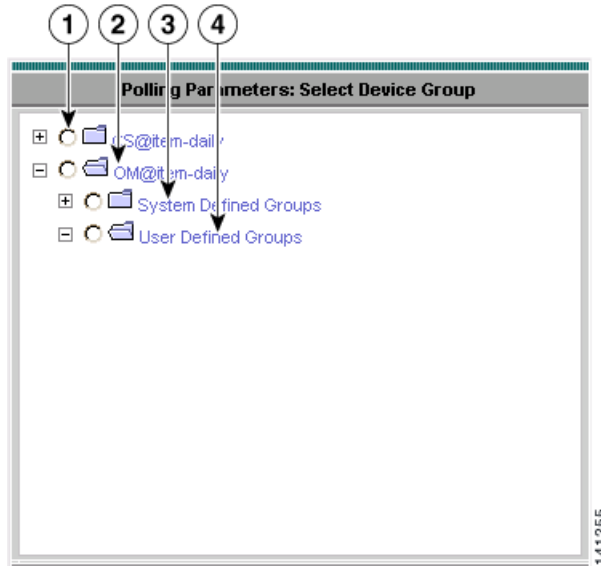
## Selecting Objects and Groups

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.

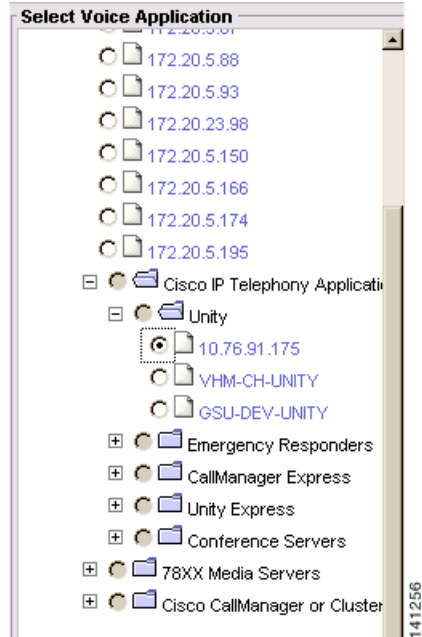
**Figure 1-4** Device Group Selector as Displayed on the Polling Parameters: Select Device Group Page



1	CS@item-daily—Groups that are controlled by Common Services. Subgroups are System Defined Groups and User Defined Groups. These groups are different from the Operations Manager groups.	3	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 <a href="#">Working with System-Defined Groups, page 16-3</a> .
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 Groups, User Defined Groups, and groups you create. (See <a href="#">Understanding Operations Manager Groups, page 16-1</a> .)

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 CiscoWorks Permission Report to determine which tasks are permitted for each user role. From the Common Services home page, 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 19-19
- [Using Operations Manager in ACS Mode](#), page 19-21

## Responding to Security Alerts

The first time that you connect to the IP Communications 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 15-3](#)).
- 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 19-14](#)).
- For information about device-based licensing, see *Installation Guide for IP Communications Operations Manager*.

