



## Table Of Contents

<b>MANAGEENGINE OPMANAGER - NETWORK MONITORING SOFTWARE.....</b>	<b>7</b>
<b>RELEASE NOTES .....</b>	<b>9</b>
<b>GETTING STARTED .....</b>	<b>11</b>
Starting OpManager Server.....	11
Running OpManager as a Windows Service.....	12
Starting the Web Client.....	13
Shutting Down the Server.....	14
Registering OpManager.....	15
Changing the Database to MSSQL .....	16
Data Backup and Restoration.....	17
Changing Web Server Port.....	18
Server Startup: Troubleshooting Tips.....	19
<b>USING SUPPORT PORTAL.....</b>	<b>21</b>
Accessing Customer Support Portal.....	21
Logging a New Support Request.....	22
Browsing the Solutions .....	23
Supported Devices .....	24
<b>WORKING WITH THE CLIENT .....</b>	<b>25</b>
Personalizing Web Client.....	25
Selecting a Skin .....	25
Configuring Client Session Timeout .....	26
Changing Password.....	27
Configuring Discovery.....	28
Configuring Discovery: Overview.....	28
Discovering Multiple Networks.....	29
Deleting a Network.....	29
Discovering a Specific Device .....	30
Deleting a Device.....	30
Rediscovering Managed Networks .....	31

Configuring SNMP Parameters .....	32
Configuring SNMP Discovery .....	32
Modifying SNMP Parameters in Devices.....	33
Classifying Devices.....	34
Classifying Devices: Overview.....	34
Changing the Device Type .....	36
Changing the Device Category.....	37
Identifying Servers in Your Network .....	38
Identifying Laptops in Your Network.....	39
Network Monitoring.....	40
What Should Be Monitored?.....	40
How Frequently Should I Monitor? .....	41
Setting Monitoring Interval for a Device Category .....	42
Setting Monitoring Interval for a Device.....	43
Monitoring Packet Loss in a Network .....	44
Configuring Device Dependencies .....	45
Adding a New Device Type .....	46
Managing Devices .....	47
Device Snapshot.....	47
Configuring Device Management Parameters.....	48
Configuring Authentication Details for Non-SNMP Devices .....	49
Managing and Unmanaging a Device.....	51
Viewing Device Availability Details .....	52
Modifying Monitor Settings of a Device .....	53
Viewing Software Installed in a Device.....	54
Viewing Active Processes in a Device.....	55
Sorting Devices in Maps .....	56
Using Quick Configuration Wizard.....	57
Managing Switches.....	58
Managing and Unmanaging Switch Ports.....	58
Switch Port Mapper.....	59
Enabling and Disabling a Switch Port.....	60
Changing Display Name of Switch Ports .....	61
Viewing STP Port Details.....	62

Managing Routers .....	63
Managing and Unmanaging Router Interfaces .....	63
Changing Display Name of Router Interfaces .....	64
Viewing IP Routing Table.....	65
Viewing IP Address Table.....	66
Managing UPS.....	67
Monitoring Exchange Servers.....	68
Exchange Server Monitoring .....	68
Configuring Exchange Services to be Monitored .....	69
Active Directory Monitoring.....	70
Service Monitoring .....	71
Configuring Services.....	71
Adding a New Service .....	71
Modifying Service Configuration.....	72
Services and Their Default Ports.....	73
Managing Services .....	74
Specifying Services to Be Scanned during Discovery .....	74
Specifying Services to Be Monitored in Devices .....	75
Viewing Service Status and Response Time.....	76
Windows Services Monitoring.....	77
Monitoring Windows Services.....	77
Creating a Windows Service Monitor.....	78
Associating a Windows Service Monitor with a Device .....	79
Windows Event Logs Monitoring .....	80
Event Log Monitors .....	80
Creating an Event Log Monitor .....	81
Monitoring Windows Events in a Device.....	82
Device and Application Monitors .....	83
OpManager Monitors: Overview .....	83
Creating a Custom Monitor.....	84
Associating a Monitor with a Device .....	85
Configuring Threshold for Critical Parameters.....	86
Modifying Monitor Settings .....	87
Testing the Configured Monitors.....	88
Viewing Graphs.....	89

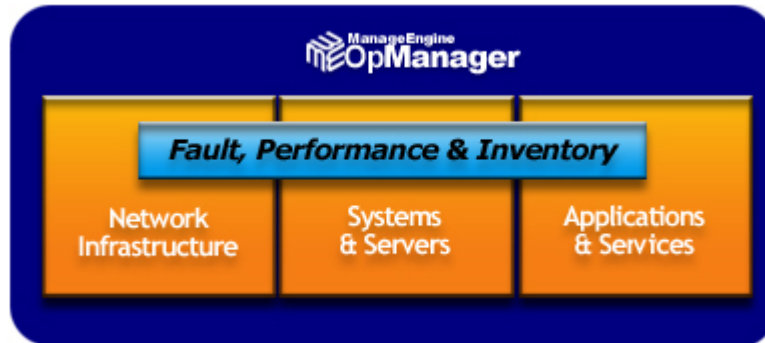
Resource Monitoring.....	90
SNMP-based Monitoring in Windows/Linux/Solaris .....	90
WMI-based Monitoring for Windows.....	91
Telnet and SSH based Monitoring in Unix Devices.....	92
Viewing Asset Details. ....	93
Customizing Snapshot Page .....	94
URL Monitoring.....	95
Configuring URL Monitors.....	95
Managing a URL in a Server .....	96
URL Response Time and Availability .....	97
Trap Processing.....	98
OpManager Trap Processors .....	98
Creating a Trap Processor.....	100
Loading Traps From MIB .....	101
Modifying Trap Processor Settings.....	102
Enabling and Disabling Trap Processors.....	103
Events and Alarms.....	104
Maintaining Events and Alarms .....	104
Viewing Events and Alarms .....	105
Working with Alarms .....	107
Acknowledging an Alarm.....	107
Adding Notes to an Alarm .....	108
Clearing an Alarm Manually .....	109
Deleting an Alarm.....	109
Escalating Alarms when not Cleared .....	110
Configuring Notifications.....	111
Configuring Notifications: Overview.....	111
Creating an E-Mail Notification Profile .....	112
Creating an SMS Notification Profile .....	113
Notification by Running a Program .....	114
Notification by Running a System Command .....	115
Creating a Sound Notification Profile.....	116
Modifying a Notification Profile .....	117
Deleting a Notification Profile.....	118
Associating Notification with Managed Devices .....	119

Configure Maintenance.....	120
Maintaining OpManager Database .....	120
Scheduling Downtime .....	121
Configuring Mail Server Settings .....	122
Configuring Proxy Server Settings.....	123
Managing Users.....	124
Creating a User Account.....	124
Changing the Password of a User .....	125
Setting User Account Limitations .....	126
Deleting a User Account .....	127
OpManager User Permissions.....	128
Reports .....	129
About Reports .....	129
Custom Reports .....	130
Viewing Reports.....	131
Saving and Printing Reports .....	132
MIB Browser .....	133
MIB Browser: Overview .....	133
Invoking MIB Browser.....	134
Loading MIBs .....	135
Getting the Values of SNMP Variables for a Device .....	136
Setting Values to SNMP Variables of a Device .....	137
Setting SNMP Parameters in MIB Browser .....	138
Standalone MIB Browser .....	139
Invoking MIB Browser .....	139
Loading MIBs .....	140
Setting SNMP Parameters in MIB Browser .....	141
Getting the Values of SNMP Variables for a Device .....	142
Setting Values to SNMP Variables of a Device .....	144
Viewing Real-time Graphs for SNMP data .....	145
Business Views.....	146
Starting the Java Client.....	146
Creating a Business View .....	147
Modifying Business View Settings .....	148

Drawing a Link Between Devices .....	149
Adding Shortcut to a Business View .....	150
<b>INTEGRATING WITH MANAGEENGINE PRODUCTS.....</b>	<b>151</b>
ServiceDesk Plus.....	151
Integrating with ServiceDesk Plus .....	151
Configure Servers Settings.....	152
Logging a Trouble Ticket to ServiceDesk Plus .....	153
NetFlow Analyzer.....	154
Integrating with NetFlow Analyzer .....	154
Configure NetFlow Analyzer Settings.....	155
<b>SNMP INSTALLATION GUIDE .....</b>	<b>156</b>
Installing SNMP Agent on Windows Systems .....	156
Installing SNMP Agent on Linux systems .....	158
Installing SNMP Agent on Solaris Systems .....	159
Configuring SNMP Agents.....	160
Configuring SNMP Agents in Cisco Devices .....	164
Configuring SNMP Agent for Lotus Domino Server.....	165
Configuring SNMP Agent in MSSQL Server.....	166
Configuring SNMP Agent in Oracle Server.....	167
<b>TROUBLESHOOTING TIPS.....</b>	<b>168</b>
Server Startup: Troubleshooting Tips .....	168
Client Errors: Troubleshooting Tips .....	170
Discovery: Troubleshooting Tips .....	171
Monitors: Troubleshooting Tips .....	174
Reports: Troubleshooting Tips.....	176
Other Troubleshooting Tips .....	178
<b>APPENDIX.....</b>	<b>179</b>
Third Party Software .....	179
<b>GLOSSARY .....</b>	<b>180</b>

## ManageEngine OpManager - Network Monitoring Software

With the growing need for the network monitoring software in the IT industry, OpManager has been built to satisfy the needs of network administrators by monitoring servers, routers, switches, firewalls, printers and so on, from a single console.



### Network Monitoring Software

ManageEngine OpManager is a comprehensive network monitoring software that provides the network administrators with an integrated console for managing routers, firewalls, servers, switches, and printers. OpManager offers extensive fault management and performance management functionality. It provides a lot of out-of-the-box graphs and reports, which give a wealth of information to the network administrators about the health of their networks, servers and applications.

OpManager's network monitoring functionality includes the following:

**Network Monitoring:** OpManager discovers switches, routers and firewalls in the network during the network discovery automatically and monitors the critical parameters such as the traffic rate, error and discards rate, buffer hits and misses and so on. You can get the availability report of each port and interface. Using the Switch Port Mapper tool, you can get the list of devices connected to each port of the switch. You can also create your own views and draw the diagram to virtually represent your network and get the availability of the interfaces visually.

**Server Monitoring:** OpManager allows you to classify devices as servers and desktops. This facilitates separating critical servers from end-user workstations and allows for more meaningful management. You can manage the [Windows event logs](#) and [Windows services](#).

**Applications and Services Monitoring:** OpManager discovers and actively monitors services and applications running in the servers. Out-of-the-box support is provided for services such as Web, HTTPS, FTP, IMAP, LDAP, Telnet, MySQL, MS-Exchange, SMTP, POP3, WebLogic, etc., and applications such as MSSQL, MS Exchange, Oracle and Lotus. You can also configure OpManager to monitor other critical service or application running in your servers.

**URL Monitoring:** OpManager monitors your Web sites, both [global URLs](#) and [URLs in the servers](#), and promptly notifies you when the host becomes unavailable.



**Fault Management:** OpManager detects faults in the network through periodical status polling and generates color-coded alarms for the faults. OpManager can also be configured to notify the administrator about the fault detected in the network.

**Performance Management:** OpManager measures the performance of the network hardware and software, such as the bandwidth, memory, disk and CPU utilization, and service response time by collecting data at regular intervals. These data are provided in the form of reports and graphs to the administrators. The threshold limits can be configured to pro-actively monitor the critical parameters in the managed devices.

For more details on the new features and fixes in the latest version of OpManager, refer to [Release Notes](#).

## Release Notes

[Release Highlights](#)

[New Features](#)

[Bug Fixes](#)

### Release Highlights

**MSSQL Database Support as 'add-on':** Support for MSSQL database in addition to MySQL. Provision to also migrate existing MySQL data to MSSQL.

**Active Directory Monitoring as 'add-on':** Separate category under Infrastructure Views for DomainControllers with support for monitoring critical Active Directory Services.

*(This release is compatible with ServiceDesk Plus Build No.4104 and higher, and NetFlow Analyzer Build No.4010 or higher).*

### New Features

- Provision to add custom fields to store additional device properties. These custom fields can be used to store information such as the geographical location etc. These fields can be set as subject variables even in the Notification Profiles.
- CPU/Memory diagnostics provided to help determine process-wise resource utilization, listing top 10 processes. Helpful in performance analysis and diagnosis. Based on this, you can even terminate processes from OpManager.
- Scheduling Reports is now possible. You can schedule all the default reports. Provision to automatically email the reports is also available.
- A [Support portal](#) for registered users is provided.
- A 'Request for Support' option is provided under Support tab. This automatically logs a request into OpManager Support and users can upload the Support Information File if required.
- The Java Client is stripped down and is renamed as MapMaker Tool. This will be used only to create business views. You can customize the size and shape of the icons in the business views.
- In the Web Client the Links between devices in business views will be shown more clearly and you can click the link to get to the interface snapshot page.
- The Web Client now has provisions to set thresholds for device response time, service response time, and packet loss. Earlier this was available only in the Java Client.
- Enhanced Traffic graph reports.
- Layer3 Switches discovered as Routers earlier, will now be discovered as Switches.
- Support for Spanish version is provided.
- Separate alarms will be generated for each interface failure, and the alarm will bear the display name configured for the interface.
- DB Manager Utility included. This helps in porting data from MySQL to MSSQL and also for backup and restoration of data.

## Changes

- Alarm Escalation can now be configured in minutes
- Availability percentage is shown with first two decimal values without approximating it to the nearest whole number.
- The dial graph in the device snapshot page is changed for enhanced look and feel.
- Added CPU, Memory Utilization for HP Procurve Switches
- Automatic refresh is included for all static pages.
- The 'Discover Networks' screen has been enhanced to accommodate the Manage/Unmanage and 'Rediscover now' options for the networks.

## Bug Fixes

- There was discrepancy in the bar color between html & pdf in disk utilization reports. This is fixed.
- The network addresses was getting added as a valid device ip address. This is fixed. Also, any ip addresses ending with .0 was not getting added. This is also fixed.
- A device was shown to be down even after clearing the alarm. This is fixed such that the correct status is shown.
- The default email in the URL Monitor configuration screen has been changed to Notification@opmanager.com.
- Sometimes, resource utilization values shown in percentage were shown to be over 100%. This has been fixed.
- Port Check for Multiple Trap Ports is Fixed.
- When any option in Select View/Sort By combo in Maps page is selected with automatic refresh enabled, 'no infrastructure view' page was getting displayed. This has been fixed.
- Support for monitoring Exchange Mail Store and Exchange Public Store folders in different partitions is provided using DomainController.
- New lines were introduced in Notifications after each warm start. That is fixed now.
- The changed Display Name will be shown for the devices and interfaces in **Today's Availability** Page. The changed name is retained even after rediscovery.
- Interfaces were always shown to be 100% available in the availability report page. This is fixed.
- There was an issue of compressed url monitoring. This is fixed.
- Scheduled downtime was not effected properly if two intervals are mentioned. This has been fixed.
- If the CPU Utilization monitor is deleted and re-added for a router, the dial graph was not displayed. This is fixed now.
- Wrong values were shown in the reports for Volumes with Least Space, Volumes with Most Free Space, and All Servers Disk Usage Report if configured from Quick Configuration Wizard. This is fixed and correct values are shown now.

## Getting Started

### Starting OpManager Server

After installation, all the OpManager-related files will be available under the directory that you choose to install OpManager. This is referred to as *OpManager Home* directory.

To start OpManager follow the steps depending on the OS you have on your machine:

- [Windows](#)
- [Linux](#)

#### On Windows Machines

If you have chosen to install OpManager as [Windows service](#), you will be prompted whether to start the service after successful installation. If you choose to start the service, the Web client will be invoked automatically. Enter the log-on details, the default user name and password is 'admin' and 'admin' respectively.

When you open the OpManager Web client for the first time, the discovery wizard will be invoked.

1. Click **Next** to proceed with the steps in the wizard or **Cancel** to quit the wizard.
2. In the first page, enter the values for the SNMP Parameters and click **Next**.
3. In this page, move the services to be scanned in the discovered devices from the **Supported Services** list to **Selected Services** list.
4. Click **Next** to move to the next step.
5. Type the network IP address in the **Network** box and select the subnet mask from the **Netmask** list.
6. Click **Add** to add the network to the list of networks to be discovered.
7. Once you have added all the networks to be discovered, click **Finish**.

This will start discovering all the networks in the list. Click the Maps tab and select the added network IP to view the devices discovered in it.




**Note:** At any point of time, you can go back the wizard using the **Back** button and modify the discovery settings.

#### On Linux Machines

1. Log in as '**root**' user.
2. Execute the **StartOpManagerServer.sh** file present in the *<OpManager Home>/bin* directory.
3. Once the server is started successfully, execute **StartOpManagerClient.sh** to start the client. In the displayed login window, type the **User Name** and **Password** and press Enter. To start the Web client, refer to [Starting the Web client](#).



**Note:** On Windows machines, if you started OpManager using the shortcuts and not as Windows service, an icon  will be displayed on the system tray to manage the application. You can start the client, start the server, and shut down the server using this icon.

## Running OpManager as a Windows Service

To start OpManager as a Windows service, follow the steps given below:

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Under **Administrative Tools**, select **Services**.
3. In the details pane, right-click **ManageEngine OpManager** and click **Start**.

To stop the ManageEngine OpManager service, right-click the **ManageEngine OpManager** service in the Services window and click **Stop**.

## Starting the Web Client

1. Open a JavaScript-enabled Web browser such as Internet Explorer or Netscape Navigator.
2. Type `http://<host_name>:<port_number>` in the address bar and press Enter. Here, `<host_name>` is the name of the machine in which OpManager is running and `<port_number>` is the port that you have chosen to run OpManager Web Server during installation.
3. Type the **User Name** and **Password** and click **Login**. The default user name and password are 'admin' and 'admin' respectively.

Alternatively, if the OpManager server is running on Windows machines, you can start the Web client using

**Start > Programs > ManageEngine OpManager > OpManager Web Client.**

## Shutting Down the Server

- **On Windows machines**

If you have installed OpManager as [Windows service](#), then stop the **ManageEngine OpManager** service in the Windows service list.

Otherwise, right-click the tray icon  and click **Shut Down Server**.

- **On Linux machines**

1. Log in as '**root**' user.
2. Execute the **ShutDownOpManager.sh** file present in the *<OpManager Home>/bin* directory.

Type the **User Name** and **Password** in the Shut Down OpManager window and press Enter.

## Registering OpManager

You can register OpManager by applying the license file that you receive from AdventNet. To apply the license, follow the steps given below:

1. Click **Register** at the top right corner of the client page.
2. Click **Browse** and choose the license file from the location it is saved.
3. Click the **Register** button to apply the license file.

Using the Java client, you can apply the license file by following the steps given below:

1. Select **Register Now** under the Help menu.
2. Click **Browse** and choose the license file from the location it is saved.
3. Click **Next** to view the licensing details.
4. Verify the information displayed and click **Finish** to apply the license file.



## Changing the Database to MSSQL

OpManager uses the MySQL database by default and this is bundled with the application. From Build No. 6000 and higher, support for MSSQL database also is provided.

### Prerequisites

- The Build Number of OpManager must be 6000 or higher.
- MSSQL support is provided as an 'add-on' feature over OpManager. This needs licensing. Write to [licensing@adventnet.com](mailto:licensing@adventnet.com) to procure the add-on license.
- MSSQL database must be installed as this is not bundled with OpManager.

### Steps to choose MSSQL as OpManager's database

1. Ensure you have registered with the add-on license for MSSQL database support.
2. Stop OpManager if it is running.
3. Select Start --> Programs --> ManageEngine OpManager --> DB Manager --> DB Configuration.
4. A DB Configuration window pops up. Select MSSQL option.
5. Configure the following information:
  - DB Host : The name or the IP address of the machine where MSSQL is installed.
  - Port: The port number in which OpManager must connect with the database. Default is 1433.
  - User Name and Password: The user name and password with which OpManager needs to connect to the database.

### Migrating Existing MySQL Data to MSSQL

Following are the steps to port your existing MySQL data to MSSQL in OpManager:

1. Stop OpManager and Upgrade by applying the latest upgrade pack.
2. Start OpManager after upgrade and apply the add-on license.
3. Stop OpManager again and take a backup of the data using BackupDB.bat present under /bin/backup directory .
4. [Change the database to MSSQL](#) using steps mentioned above.
5. Restore the data using RestoreDB.bat present in /bin/backup directory and restart OpManager.

## Data Backup and Restoration

### Backup

To take a backup of the data and configurations in OpManager,

- Go to `<OpManager Home>/bin/backup` directory
- Execute **BackupDB.bat/sh** to start the data backup

Once the backup is over, a directory **backup** is created in `<OpManager Home>`, and the backup file with **.data** extension is placed in this directory. The name of the backup file contains the date and time at which backup is taken. Example:

BackUp\_FEB28\_2005\_15\_51.data

### Restoration

To restore the backed up data,

- Go to `<OpManager Home>/bin/backup` directory
- Execute **RestoreDB.bat/sh** with the backup file name as argument. See example below:

```
C:\<OpManager Home>\bin\backup>RestoreDB.bat  
BackUp_FEB28_2005_15_51.data
```

During restoration, the existing tables are dropped, new tables are created, and the data is restored in all the tables.

**Note:**

- You can schedule backup at required interval using a cron job.
- During restoration, a message 'Unable to create the table STATSDATA\_HOURLY/DAILY/HTML' is printed in the console. This is harmless and the tables are created.

## Changing Web Server Port

You will be prompted to change Web Server port during installation. You can change it after installation.

The script for changing the Web Server port number, **ChangeWebServerPort** (in Windows this will be a *.bat* file and in Linux, *.sh* file) is available under the *<OpManager Home>/bin* directory.

The steps to change the port number are as follows:

1. Stop the OpManager server. If you are running OpManager as Windows service, stop the service.

2. Execute the script as follows:

In Windows,

```
ChangeWebServerPort <old_port_number> <new_port_number>
```

In Linux,

```
sh ChangeWebServerPort.sh <old_port_number> <new_port_number>
```

Here, *old\_port\_number* is the port number you specified during installation and *new\_port\_number* is the one where you want to run the Web server.

3. Start the OpManager server.

## Server Startup: Troubleshooting Tips

- Enter a proper AdventNet license file
- Failed to establish connection with Web server. Gracefully shutting down OpManager
- Port 80 needed by OpManager is used by some other application
- Port 8009 needed by OpManager is used by some other application
- Unable to start MySQL daemon
- MySQL related error messages in Windows machines
- Error while starting OpManager service
- Other server startup problems

### Enter a proper AdventNet license file

If your system date is set to a future or a past date, you will get this error message. Uninstall OpManager, set the system date settings to current date and time, and re-install OpManager.

### Failed to establish connection with Web server. Gracefully shutting down OpManager.

In Linux 8 and 9 versions, you will get this error because the file **libdb-3.2.so** may not exist in your system. This file is made optional while installing Linux Red Hat 8 & 9 versions. This file is required to start the Apache server. The file has been bundled with the product and is present in the `<OpManager Home>/lib/backup` directory. Copy it to the `<OpManager Home>/lib` directory and restart OpManager.

### Port 80 needed by OpManager is used by some other application

1. If you have installed OpManager as Windows service, the server will be started automatically after installation. When you try to start the server again using the shortcuts, you will get this message. So you can directly start the client using Start > Program Files > ManageEngine OpManager 5 menu.
2. If you have not chosen to install OpManager as Windows service, refer to Question 1 under FAQs to change the port. Then restart OpManager.

### Port 8009 needed by OpManager is used by some other application

You get this message since the port 8009 needed by OpManager to run Tomcat server is already occupied. You can either shut down the application running in this port or configure OpManager to use a different port to run Tomcat server.

To stop the Tomcat server, do the following:

1. Set the JAVA\_HOME variable in the **setclasspath.sh** file located at `<OpManager Home>/apache/tomcat/bin` directory as `JAVA_HOME=/usr/java/<jdkversion>`.
2. Execute the script **shutdown.sh** from `<OpManager Home>/apache/tomcat/bin` directory.
3. Then restart OpManager.

To configure OpManager to use a different port to run Tomcat server, you need to do the following:

1. If you have installed OpManager in Windows machine, find and replace all instances of "8009" with a free port number in the *<OpManager Home>/conf/opmanager\_processinfo.xml* file.  
If you are using Linux machine, then replace the port number in the *<OpManager Home>/setEnv.sh* file.
2. Then restart OpManager.

### **Unable to start MySQL daemon (or) any other MySQL related error messages in Windows machines**

You will run into MySQL related errors in Windows machines if MySQL is already installed or another instance of MySQL is running on the same machine.  
The best solution is to uninstall MySQL and install OpManager or install OpManager in a different machine.

Note: Deleting or renaming the My.ini file present in C:\Winnt (C:\Windows in Windows XP) also solves this problem.

### **Error while starting OpManager service**

When you get an error while starting OpManager service, try starting the OpManager server using the shortcut available at Desktop or using the menu, **Start > Programs > ManageEngine OpManager 5 > OpManager 5**.

### **Other Server startup problems**

- You will find problems while starting the server in Windows machines, if environment variables are assigned non-ascii values. Remove the variables containing non-ascii values and restart the server.
- If you choose to install OpManager under a directory named in Japanese and Chinese language, you will find problem while starting the apache service. Choose a directory in English to install OpManager.

## Using Support Portal

### Accessing Customer Support Portal

All registered OpManager users can access the customer support portal. You can log into the support portal with your license email ID as username and password.

For instance, if the email id in the OpManager's license file is john@abcd.com, you can log onto the support portal using the same email ID as username and password.

You can view all the queries you place with our technical support and can also know the status of your queries.

### Steps to Access Support Portal from OpManager

1. Log into OpManager Web Client.
2. Select the Support tab.
3. All your support requests can be accessed from **My Requests Summary** column.
  - Click **Open Requests** to see all your unresolved requests.
  - Click **Closed Requests** to see all the resolved requests.
  - Click **All Requests** to check all the requests you have placed
4. You will be prompted to enter your user name and password. Provide the email ID present the Registered license procured from us. If you have a multiple users license, login option will be available only for the license recipient email ID.

For instance, if the multiple users are **a@abcd.com**, **b@abcd.com**, and **c@abcd.com**, and the license file recipient email id is **a@abcd.com**, login will be possible only with this email ID.

5. Click **New Request** link to log a new request/query.

### Steps to Access Support Portal Directly

1. Connect your browser to <http://support.opmanager.com>.
2. Login with the email ID as user name and password as mentioned in step 4 above.

You can browse through [OpManager Solutions](#) to check if it has resolutions/workarounds to the problems you face when using OpManager.

## Logging a New Support Request

We have been providing email-based support during evaluation and after purchase. Henceforth, you can raise a new support request seeking technical assistance from within OpManager instead of opening a composer to draft a mail. This helps in logging a query quickly without having to switch between applications. Following are the steps to log a new request.

1. Select the Support tab in OpManager.
2. Click Request Support link from **OpManager Support** column.
3. Type the nature of the issue faced with a complete problem-description in the corresponding fields.
4. Attach the Support Information File to help us in faster analysis and provide a quick resolution.
5. Click Finish.

The request will be logged as an email to our technical support who will respond to the query based on priority.

## Browsing the Solutions

The support portal has solutions to few frequently reported issues. This serves as an in-built OpManager knowledge-base. Following are the steps to access the Solutions:

1. Log into the [Customer Support Portal](#).
2. Select the **Solutions** tab
3. Click the relevant topic under Solutions. The topics may contain sub-categories. You can therefore drill down to the sub-categories too.

You can also search for a solution by typing relevant key words in the **Search** field.

Browse through the solutions provided before placing a query. This will help in resolving few common issues yourselves.

Please note that this knowledgebase is being expanded and enhanced and may not contain solutions to all your queries. If you do not find any solution, or if you find it hard to search through the solutions, do not hesitate to [raise a new request](#).



## Supported Devices

OpManager supports discovery of more than 100 device types. The discovered device types are classified into Routers, Switches, Firewalls, Printers, Servers, Desktops, UPS, Wireless etc.

To check the supported device types,

- Select Admin tab.
- Click Device Types under Global Settings.

The device types not included in this list must be created manually, else they are discovered as 'Unknown' device type. You can [create a device type](#) and [group it under one of these categories](#).

## Working with the Client

### Personalizing Web Client

#### Selecting a Skin

OpManager provides few skins which allow you to choose the look-and-feel of your choice. To select and apply the required skin,

1. Click the **Personalize** option on top, in the Web Client
2. In the screen that pops up, select the **Skin Selector** tab
3. From the **Select Skin** combo-box, select the required skin
4. Click **Apply** for the new skin to take effect

When you select the skin, a preview of the skin would be shown adjacent to the combo-box which helps you decide before applying.

## Configuring Client Session Timeout

OpManager provides you options to keep the session alive. To configure the client session timeout,

1. Click the **Personalize** option on top, in the Web Client
2. In the configuration screen that pops up, select the **Automatic Refresh** tab
3. You can either select **Automatically refresh page...** option, and provide the required interval in minutes.

For example, if you provide the refresh interval as 5 minutes, the page refreshes every 5 minutes, and the session does not expire. Moreover, you can view the fresh updates on the page.

Otherwise, you can select the **Do not refresh automatically...** and from the corresponding combo-box select the required interval for the session to expire, or select 'Never Expires' option. This keeps the session alive. But the page is not automatically refreshed. You need to refresh it manually.

## Changing Password

The default user name and password to log in to the client are admin and admin. You can change the password as follows:

1. Click the **Personalize** link on top, in the Web Client
2. In the screen that pops up, click the **Change password** tab
3. Type the existing password in the **Current password** field
4. Type the new password in the **New password** field
5. Re-type the new password in the **Re-type password** field to confirm the change

The new password takes effect now. You can try logging in with the new password.

## Configuring Discovery

### Configuring Discovery: Overview

#### How Does OpManager's Discovery Work?

OpManager automatically discovers all devices in the networks chosen to discover in the Discovery Wizard. It uses the SNMP and ICMP settings provided in the wizard to perform this discovery. To identify the operating system of the non-SNMP devices, OpManager uses the Telnet protocol.

In addition to discovering devices in the selected networks, OpManager also scans for the services on the discovered devices. The services that are selected in the Discovery Wizard will be scanned during discovery. For details about the services managed by OpManager, refer to [Configuring Services: Overview](#).

#### Customizing Discovery

OpManager's discovery can be customized to perform the following:

- [Discover multiple networks/subnets](#)
- [Discover a specific device](#)

To perform the above tasks using Web client, follow the links below:

- [Discovering Multiple Networks](#)
- [Discover a Specific Device](#)

## Discovering Multiple Networks

By default, OpManager discovers the networks chosen in the Discovery wizard. You can expand your management domain by configuring OpManager to discover additional networks or subnets.


To discover multiple networks, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Discovery**, select **Discover Network**.
3. Type the **Network Address** and the **Netmask** of the network to be discovered.
4. Click **Add Network** to start discovery.

### Note:

Before discovering the devices, verify the following:


- More information about the devices can be obtained by performing SNMP-based discovery. To specify the SNMP parameters, in the **Admin Tab**, under **Discovery**, click **SNMP Parameters**.
- To select the services to be monitored for this discovery, click **Services** under **Discovery**.

If you could not locate the service you want to monitor in the list, you can add it using the **Add New Service** option under **Actions**. Refer to [Adding a New Service](#) for details. If you want to change the service port number or timeout value, click  corresponding to the service to be modified. Refer to [Modifying Service Configuration](#) for details.



## Deleting a Network

To delete a discovered network, follow the steps given below:

1. Under the **Admin** tab, click **Discover Network**.
2. Click  corresponding to the network IP to be deleted in the **Discovered Networks** list.
3. Click **OK** to confirm deletion.



**Note:** When a network is deleted, some devices (such as routers) in it may not be deleted if they have multiple IP addresses of different networks.

## Discovering a Specific Device

To manually add a device that is not discovered during initial discovery, follow the steps given below:

1. Click the **Admin** tab.
2. Under Discovery, select **Add Device**.
3. Type either the **IP Address** or the **Device Name** of the device to be discovered.
4. If the device is SNMP-enabled, type the **SNMP Port** number and the **Community String** to fetch the values from the SNMP agent.
5. Click **Add** to start discovery.

If the device is found, it will be added to the corresponding network map.



**Note:** To configure status polling, notifications, and service monitoring for this device, refer to [Configuring Device Management Parameters](#).

## Deleting a Device

OpManager allows you to delete a device, when you do not want to manage it any more.

To delete a device, follow the steps given below:

1. Click the device icon in the map.
2. Click **Delete** under **Actions**.
3. Click **OK** to confirm deletion.

You can also delete multiple devices at a time using Quick Configuration wizard. To do so, follow the steps given below:

1. In the **Admin** tab, under **Tools**, click **Quick Configuration wizard**.
2. Select **Delete Devices** and click **Next**.
3. Select the devices to be deleted from the list and click **Finish**.

## Rediscovering Managed Networks

Rediscovery of managed networks helps to discover all the devices in the networks once again. This helps to discover the devices that were not discovered earlier.

By default, rediscovery of all discovered networks is done every 7 days. To modify this, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Discovery**, click **Rediscovery**.
3. In the **Rediscovery interval** box, type the number of days after which the networks are to be rediscovered.
4. Click **Save** to apply the changes.



**Note:**

During warm-start of OpManager Server, rediscovery does not happen. If you would like rediscovery to happen during warm start, set the value of **REDISCOVERY\_ON\_WARM\_START** to **true** in **seed.file** present in <OpManager Home>/conf directory.



## Configuring SNMP Parameters

### Configuring SNMP Discovery

When you perform an SNMP-based discovery, OpManager collects many valuable information from the discovered devices, such as the active processes, installed software, the traffic and bandwidth utilization details, asset details and so on.

If your network devices are SNMP-enabled, that is, if SNMP is installed and started on the devices in your network, you can facilitate accurate network discovery by specifying the SNMP parameters. This also enables OpManager to fetch the device details and present them as graphs and reports.

To configure SNMP parameters for discovery, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Discovery**, click **SNMP Parameters**.
3. Type the values for the [text fields](#).
4. Click **Update**.

## Modifying SNMP Parameters in Devices

You might need to modify the SNMP settings if the SNMP agent in a device is running in a different port, and/or if community strings are changed for a device.

To modify the SNMP settings for a single device, follow the steps given below:

1. [Open the snapshot page of the device.](#)
2. Under **Configure**, select **Passwords**.
3. Modify the values of the SNMP port and community strings as configured in the agent.
4. Click **OK**.
5. Click **Rediscover Now** under **Actions** to discover the device again with the modified parameters. This enables SNMP data collection for this device.



**Warning:** When a device is re-discovered, the data collected for the device so far such as the availability and response time details will be lost.

Alternatively, you can use the Quick Configuration Wizard to change the community string in many devices or in all devices under a category or in all devices grouped under a business view at a time.

To do so, follow the steps given below:

1. In the **Admin** tab, under **Tools**, click **Quick Configuration wizard**.
2. Select **Configure SNMP Community String** and click **Next**.
3. Enter the community string and click **Next**.
4. Select an option for configuring the community string and click **Next**.
  - If you have selected a category, then the profile will be associated with all the devices in the category automatically.
  - If you choose Select devices manually, the subsequent page will list all the managed devices. Move the devices from the list in the left to the one in the right and click **Finish**.
  - If you have chosen a business view, the profile will be associated with all the devices in the view. This option will be available only if you have created a business view.

## Classifying Devices

### Classifying Devices: Overview

During initial discovery, OpManager categorizes the network devices into servers, printers, switches, routers and firewalls. For proper classification, install and start the SNMP agent on all the managed devices.

By default, OpManager classifies the devices as follows:

- If the device is detected to be of type Sonic, Check Point, Fortigate, Cisco Pix, NetScreen, or VPN 3000 Concentrator, it will be classified as a **Firewall**.
- If the device is detected to be of type Linux, Windows 2003, Solaris, HP-UX, Novell NetWare, AS400, or if it responds to the SysOID of NT Server, NT Domain Controller, or IBM server, it will be classified as a **Server**.
- If the device has more than one interface and if the SNMP variable IpForwarding is set to true or if the device is detected to be of type Cisco 7500, 3200, 3100, or 2500 series, it will be classified as a **Router**.
- If the device responds to the Printer MIB, or if the type is detected to be HP or Canon printer, it will be classified as a **Printer**.
- If the device responds for the OID 17.1.2.0 or 17.2.7.0 or if it is detected to be of type Cisco Catalyst, HP, Extreme, Foundry or 3COM, it will be classified as a **Switch**.
- The device that do not satisfy any of the above conditions will be classified as a **Desktop**.

The classified devices are placed under different maps for easy management.

This initial classification may not be accurate if

- the network devices do not support SNMP.
- some devices have their SNMP settings different from those specified in the Discovery Settings dialog.

Perform the following tasks to ensure that OpManager maintains accurate information about your network:

- [Change the device type for unknown devices or wrongly discovered devices](#)
- [Change the device category](#)
- [Identify the servers in your network](#)
- [Identify the laptops in your network](#)

To perform the above tasks using Web client, follow the links below:

- [Changing the Device Type](#)
- [Changing the Device Category](#)
- [Identifying Servers in Your Network](#)
- [Identifying Laptops in Your Network](#)



**Note:**

1. For devices to get classified properly, you need to have installed and started SNMP in all the network devices before starting OpManager server.
2. By default, workstations that run services are classified as servers. OpManager allows you to have your own list of servers using the Populate Server Map option. For details, refer to [Identifying Servers in Your Network](#).

## Changing the Device Type

If a device is identified as a wrong or unknown device type during initial discovery, OpManager allows you to assign an appropriate device type as per your network needs. This is required when you want to associate the WMI monitors to the Windows devices that are not discovered as Windows device type.

To change the device type of a device, follow the steps given below:

1. [Open the snapshot page of the device.](#)
2. Under **Configure**, select **Device Type**.
3. Select the appropriate type from the **Device Type** list in the displayed window. If the required device type is not found in the list, you can create your own device types. Refer to [Adding a New Device Type](#) for details.
4. Click **Save** to apply the changes.

## Changing the Device Category

- [Manually moving a device under one of the default categories after discovery](#)
- [Automatically moving a device under one of the default categories during discovery](#)

If you find a device classified under a different category, you can easily move it to the proper category. This might be needed when the device is not SNMP-enabled and hence not classified properly.

1. [Open the snapshot page of the device.](#)
2. Under **Configure**, click **Device Properties**.
3. Select the category of the device from the **Category** list and click **Save**.



**Warning:** When a device is moved to a different category, the performance data collected for the device so far will be lost.

Instead of manually moving each device to a appropriate category, if you want to **classify a device type under one of the default categories of OpManager during its discovery**, follow the steps given below:

1. [Create a device type for the device.](#) Ensure that you have given the correct OID for the device type.
2. Edit the **opmanager\_categoryinfo.xml** file under the *<OpManager Home>/conf* folder as follows:

In the appropriate [device category](#), include the [device type](#) added in the previous step in the tag

```
<Check>
<MOPropertyCheck>
<PropertyName>type</PropertyName>
<Condition>contains</Condition>
<Value>device type</Value>
</MOPropertyCheck>
</Check>
```

## Identifying Servers in Your Network

To monitor the servers in your network effectively, you need to ensure that all the servers have been identified correctly and placed on the Servers map. OpManager allows you to select the devices that are to be categorized as Servers.

To select the Servers in your network, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Tools**, click **Quick Configuration Wizard**.
3. Select **Group servers** and click **Next**.
4. If your servers are found in the Desktops list, select them from the **Desktops** list and click >>.
5. If some of the servers are found in the Servers list, select them from the **Servers List** and click <<.
6. Click **Next** to save the settings.



**Note:** Grouping servers in your network will help you set the common monitoring interval, associate a common notification and common monitor to all servers. To set the monitoring interval for devices, refer to [Setting Status Poll Interval for a Device Category](#). To associate a notification profile or a common monitor, you can use the Quick Configuration Wizard.

## Identifying Laptops in Your Network

Laptops will be identified as Desktops during initial discovery. To change the device type to Laptop, follow the steps given below:

1. Select the device from the map.
2. Under **Configure**, select **Device Type**.
3. Select **Laptop** from the **Device Type** list in the displayed window.
4. Click **Save** to apply the changes.



## **Network Monitoring**

### **What Should Be Monitored?**

Active network monitoring is a must to gain accurate and real-time visibility of the health of your network. However frequent monitoring can become a huge strain on your network resources as it generates a lot of traffic on the network, especially in large networks.

We recommend you to monitor only the critical devices on the network. This is a best practice adopted by the network administrators worldwide.

Following are the components of networks that are considered critical:

- WAN Infrastructure: Routers, WAN Switches, Firewall, etc.
- LAN Infrastructure: Switches, Hubs, and Printers.
- Servers, Services, and Applications: Application Servers, Database servers, Web servers, Mail servers, CRM Applications, etc.
- Host Resources: CPU, Memory, and Disk Utilization of critical devices.
- Critical Desktops and Workstations.

## How Frequently Should I Monitor?

The general practice is to monitor critical devices more frequently than non-critical devices.

Given below are the recommended monitoring intervals for small and medium-sized networks (up to 1000 devices):

- Routers and Critical Servers: 5 - 10 minutes
- Switches, Hubs, and Printers: 10 - 20 minutes
- Desktops and Workstations: We recommend you to [turn off monitoring for desktops and workstations](#) to reduce the amount of network traffic generated by OpManager. Alternatively, monitor them less frequently, say for every hour or 30 minutes.

If there are a few critical workstations that you want to monitor, you can [turn on monitoring for those devices individually](#).

Using the Web client, to turn off monitoring for a device category,

## Setting Monitoring Interval for a Device Category

OpManager allows you to set a common monitoring settings for all the devices under a specific category.


To do so, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Global Settings**, click **Monitoring Intervals**.
3. To enable monitoring for a category, select the check box under **Enable** corresponding to the category and type the monitoring interval in minutes, in the adjacent box.

To disable monitoring a specific category, clear the respective check box.

4. Click **Save** to save the settings.

For instance, if you want to monitor servers every minute, ensure that the check box corresponding to **Servers** is selected and type 1 in the adjacent box.

	<p><b>Note:</b></p> <ul style="list-style-type: none"><li>▪ To see the recommended monitoring intervals, refer to <a href="#">How Frequently Should I Monitor?</a></li><li>▪ The settings made here will be applied to all devices under the respective category. To change the settings for an individual device, refer to <a href="#">Setting Monitoring Interval for a Device</a>.</li></ul>
--	---

## Setting Monitoring Interval for a Device

If you want to set a different polling interval for a critical device, follow the steps given below:

1. [Open the snapshot page of the device.](#)
2. Under **Configure**, select **Monitoring**.
3. Make sure that the **Polling enabled** check box is selected and type the interval in minutes, in the adjacent box.
4. Click **Submit** to apply the change.



**Note:** To stop monitoring the device, clear the **Polling Enabled** check box. Even when the monitoring is disabled, you can get the current status of the device by clicking **Update Status** under **Actions** in the Device Snapshot page.

## Monitoring Packet Loss in a Network

Packet loss for a device can be monitored in terms of percentage. By default, only one packet is sent at a time. If a response is received for the packet sent, the packet loss for the device is shown as 0%. If there is no response for the packet sent, the percentage packet loss is shown to be 100%. This information is displayed in the device snapshot page.

It is possible to configure the number of packets to be sent. This is defined in the configuration file called **Ping.properties**. Following are the steps to configure:

1. Open the file **Ping.properties** file from `<OpManager Home>/conf` directory.
2. Change the value of the **Count** parameter (the number of ICMP ECHO requests to be sent for each and every test) to the required number.
3. Save the change and restart the server.

Example entry:

```
#Number of ICMP ECHO requests to be sent for each and every test.  
count=4
```

So, if you configure the count as 4, and if there is response for just 2 packets, the packet loss percentage is said to be 50%.

## Configuring Device Dependencies

The status polling for a device can be controlled based on its dependency on some other device. This prevents the unnecessary status checks made to the dependent nodes.

For instance, many devices will be connected to a switch. If the switch goes down, all the devices connected to it will not be reachable. In this case, it is unnecessary to check the status of the dependent devices.

To configure the dependency for devices, follow the steps given below:

1. In the **Admin** tab, under **Tools**, click **Quick Configuration Wizard**.
2. Select **Configure Dependencies** and click **Next**.
3. Select the category of the device, Router, Switch, Firewall or Server on which the dependency is to be configured. The devices managed under the chosen directory will be listed. Choose a device and click **Next**.
4. Select an option for choosing dependent devices and click **Next**.
  - If you select a category, the dependency will be configured in all the devices in the category automatically.
  - If you choose Select devices manually, the subsequent page will list all the managed devices. Move the devices from the list in the left to the one in the right and click **Finish**.
  - If you choose a business view, the dependency will be configured in all the devices in the view. This option will be available only if you have created a business view.

To configure dependency for a single device, follow the steps given below:


1. [Open the snapshot page of the device](#).
2. Under **Configure**, click **Dependency**.
3. To set the dependency for the selected device on another device, say *switch\_1*, select *switch\_1* from the **Check status only if** list in the **Dependency** section.
4. Click **Submit** to apply the change.

## Adding a New Device Type

OpManager provides support to a number of device types. Refer to Supported Devices for the default device types supported by OpManager. You can also create your own device types and assign them to the discovered devices if they are not found in this list.

To define a new device type, follow the steps given below:


1. Click the **Admin** tab.
2. Under **Global Settings**, select **Device Types**.
3. Select **Add New Device Type**.
4. Type a unique name for the new device type in the **Device Type** box. Entry to this field is mandatory.
5. Specify the **SNMP OID** for this device type. This enables OpManager to automatically assign this device type to the devices discovered with the same OID.



**Note:**

- If you are not sure about the OID, click **Query Device** and type the **Device Name** or **IP Address** of a device to obtain its OID. Type the **Port Number** and **Community String** to perform an SNMP query to this device. Then click **Submit**. The OID of the device will be displayed in the OID box.
- You cannot assign an OID that is already assigned to some other device type. To view the OIDs assigned to each of OpManager's device types, click **Device Types** under **Global Settings**.

5. Click the **Click to Select** link to select an image for this device type. This image will be used in the Network maps, Devices to watch map, and in the Inventory views. Entry to this field is mandatory.
6. Click **Submit**.



**Note:** once this is done, if a device with the above-specified device type is discovered, they will be assigned this device type automatically. To manually assign the new device type to an already discovered device, refer to [Changing the Device Type](#). Further to put move this device under one of the default categories, refer to [Changing the Device Category](#).

## Managing Devices

### Device Snapshot

OpManager's Device Snapshot shows the information about the hardware and software resources of the device.

- **To view the snapshot page of the device**, click the device name link in the map, or type the name of the device in the **Device Search** box and click **Search**.



**Note:** If there are many devices satisfying the specified criteria, the list of devices will be displayed with their IP Address and category. Click the device whose snapshot you want to view.

The descriptions for various sections of Device Snapshot are as follows:

**Device Details:** Displays the system's details such as the IP address, operating system, time stamp of previous and next polls and a description on the system hardware details.

**Today's Availability:** Displays the device availability of the current day in the form of a pie graph. Click **7<sup>d</sup>** or **30<sup>d</sup>** to view the availability report for the past 7 days or 30 days respectively.

**Response Time:** Shows the current response time of the device. Click **7<sup>d</sup>** or **30<sup>d</sup>** to view the response time details for the past 7 days or 30 days respectively.

**CPU Utilization:** Shows the current CPU load of the device. Clicking the graph shows the trend chart of CPU utilization

**Memory Utilization:** Displays the current memory utilization of the device.

**Disk Utilization:** Displays the current disk usage of the device.

**Monitors:** List of different monitors monitored in the device. Expand each monitor section to view the monitor settings.

**Interfaces:** Displays the list of interfaces in the selected device with their status and other details.

Click the interface name link to view its availability and graphs on traffic and bandwidth utilization.

**Actions:** List of actions that can be performed on the device.

**Configure:** List of configurations that can be performed on the device.

**Device Info:** Displays the options to get the device-specific information.

For routers, you will see the graphs for buffer hits, buffer misses, buffer create failures, and CPU and memory usage in KB at the bottom of the snapshot page.



## **Configuring Device Management Parameters**

For a discovered device, OpManager allows you to do the following:

- [Unmanage/manage the device](#)
- [Change the device type](#)
- [Change the device category](#)
- [Configure SNMP parameters](#)
- [Configure monitoring settings](#)
- [Configure device dependencies](#)
- [Configure notifications](#)
- [Configure service monitors](#)
- [Configure resource monitors](#)
- [Configure traffic monitors](#)
- [Configure event log rules](#)
- [Configure URL monitors](#)

All of the above can also be configured for multiple devices or for all devices belonging to a category using Quick Configuration Wizard.

## Configuring Authentication Details for Non-SNMP Devices

To collect the CPU, memory and disk utilization details from the non-SNMP devices, OpManager uses WMI service in Windows machines and Telnet or SSH protocol in Linux machine. You need to provide the authentication details for using these protocols. Further, to monitor Windows event logs and Windows services, OpManager uses WMI.

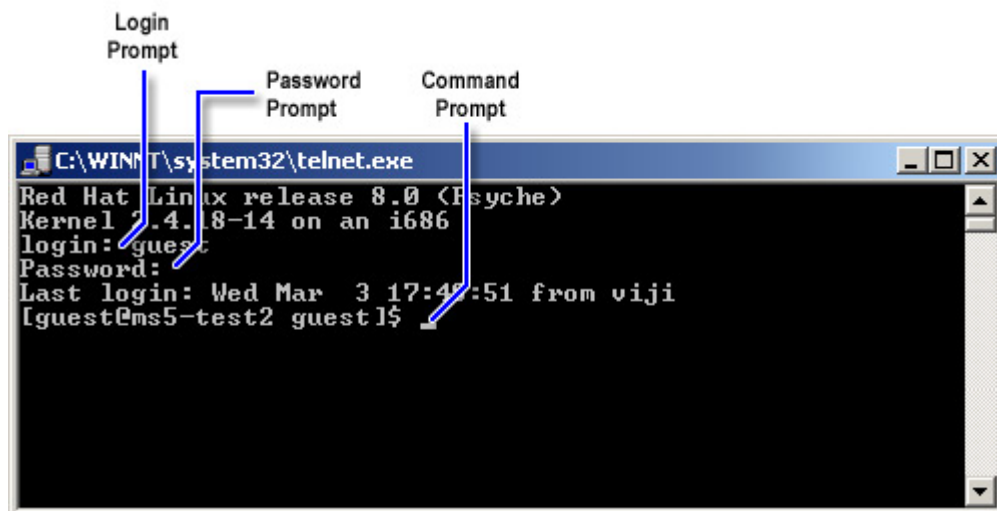
If your network device have common settings for WMI/Telnet/SSH authentication, you can configure the details to many devices at a time using Quick Configuration Wizard.

To do so, follow the steps given below:

1. In the **Admin** tab, under **Tools**, click **Quick Configuration Wizard**.
2. Select **Configure WMI/Telnet/SSH logon details** and click **Next**.
3. Select the **Operating System** of the devices and type the **User name** and **Password** with administrative privilege to connect to the device.
4. Click **Next**.
5. Move the devices from the list in the left to the one in the right to configure the logon details.
6. Click **Finish**.



**Note:** If you have provided the Telnet/SSH logon details, make sure to configure the prompt parameters in each device individually. Refer to image below for details.



If you want to provide the authentication details for each device individually, follow the steps given below:

1. [Open the snapshot page of the device.](#)
2. Click **Passwords** under **Configure**.
3. Enter the **User Name** and **Password** with administrative privilege to connect to the device. This will be taken as WMI authentication detail for Windows devices and Telnet/SSH authentication detail for Linux/Solaris devices.
4. If the operating system of the selected device is Linux or Solaris, enter the characters that appear in the **Login Prompt**, **Password Prompt**, and

**Command Prompt.** Refer to the image above for details. In this image, the Login Prompt is ":", Password Prompt is ":" and Command Prompt is "\$".


5. Select the protocol to collect the information from the device from the **Connection Protocol** list.
6. Click **OK** to save the details.

## Managing and Unmanaging a Device

By default, OpManager manages all the discovered devices. However, there might be some known devices that are under maintenance and hence cannot respond to status polls sent by OpManager. These devices can be set to unmanaged status to avoid unnecessary polling. Once maintenance gets over, they can be set to managed status.

### To unmanage a device

1. [Open the snapshot page of the device.](#)
2. Under **Actions**, select **Unmanage**.

This stops the status polling and data collection for the device and changes the device status icon to gray .

### To start managing an unmanaged device

1. [Open the snapshot page of the device.](#)
2. Under **Actions**, select **Manage**.

This invokes the status polling and data collection for the device. The status icon will show the current status of the device.

To manage or unmanage many devices at a time, you can use Quick Configuration wizard of OpManager. To do so, follow the steps below:

1. In the **Admin** tab, under **Tools**, click **Quick Configuration Wizard**.
2. Select **Manage/Unmanage a group of devices** and click **Next**.
3. To stop managing the devices, move them to the list in the right. To start managing the unmanaged devices, move them to the list in the left.
4. Click **Finish**.

## Viewing Device Availability Details


[Open the snapshot page of the device.](#) The Today's Availability pie graph shows the device availability of the current day.

Click on it to view further details about the availability. The details that are shown in this page are as follows:

- You can see the intervals during which the device was down in the current day.
- You can also see the total down time in hours and minutes, availability percentage, average time taken to repair the failure (MTTR), and the average time between the failures (MTBF).
- You can see the above information for the day before, last 7 days, last 30 days and the current month.

## Modifying Monitor Settings of a Device

You can modify the polling interval and the threshold settings of a monitor associated with a device. To do so, follow the steps given below:

1. [Open the snapshot page of the device.](#)
2. Under **Monitors**, expand the category of the monitor to be modified.
3. Click  corresponding to the monitor to be modified.
4. Edit the **Polling Interval** field and the threshold settings as required and click **OK**.



**Note:** To change the monitor settings globally, refer to [Modifying Monitor Settings](#).

## **Viewing Software Installed in a Device**

At any time, OpManager provides you the information on the processes that are currently running on the managed device. You need to have SNMP agent running in the device to view this information.

To view the details, click the device icon in the map. Under **Device Info**, click **Installed Software**.

## Viewing Active Processes in a Device

At any time, OpManager provides you the information on the processes that are currently running on the managed device. You need to have SNMP agent running in the device to view this information.

To view the details, click the device icon in the map. Under **Device Info**, click **Active Processes**.



## Sorting Devices in Maps

You can sort the devices on maps by the Name, Display Name, Device Type, or the Severity of the device. This helps you locate a resource faster.

To sort the devices in a map, from the **Sort By** combo-box, select the required option based on which you need the sorting to be done.

## Using Quick Configuration Wizard

OpManager's quick configuration wizard helps you to configure monitors, notification profiles, dependency, and so on, for many devices at a time.

To invoke the wizard, in the **Admin** tab under **Tools**, click **Quick Configuration wizard**.

Following are the tasks that you can perform on multiple devices, all devices in a category or devices grouped under a business view using Quick Configuration Wizard:

- [Assign a notification profile](#)
- [Add a monitor](#) (Resource monitor, Traffic monitor, Application Monitor, and so on)
- [Configure dependency](#)
- [Group servers](#)
- [Configure SNMP community string](#)
- [Configure WMI/Telnet/SSH login details](#)
- [Delete devices](#)
- [Manage and unmanage devices](#)
- [Monitor Windows event logs](#)

## Managing Switches

### Managing and Unmanaging Switch Ports

The Switch icon visually shows the ports that are operationally up, down, and not linked to any devices.

You can choose to manage only the ports that are connected to critical devices. In general, mail servers, Web servers, proxy servers, desktops of managers, routers, and switches are considered critical in a network. You can manage only the ports connected to these devices and stop managing other ports. This stops the status polling and data collection for non-critical ports, preventing alarms generated for these non-critical ports.

#### To unmanage a port

To stop managing ports, in the Switch snapshot page, click **Configure Ports** and deselect the check boxes under **Manage** corresponding to the ports to be unmanaged.

Alternatively, to unmanage a port, click the port from the Switch Infrastructure view, and click **Unmanage** under **Actions**.

#### To manage an unmanaged port

To start managing ports, in the Switch snapshot page, click **Configure Ports** and select the check boxes under **Manage** corresponding to the ports to be managed.

Alternatively, to start managing a port, click the port from the Switch Infrastructure view, and click **Manage** under **Actions**.



**Note:** You can also choose to shut down the port that produces unnecessary traffic bringing down the network's performance. To do so, refer to [Enabling and Disabling a Switch Port](#).

## Switch Port Mapper

OpManager shows the connectivity between a switch and other connected devices in the network in Switch Port Mapper. You get the details such as the MAC address, IP Address and DNS names of the devices connected to the switch.

You need to provide the details such as the community string and port number of the switch and if needed, the details of the server or router that may contain the layer 3 details.

To view the switch port mapping details, follow the steps given below:

1. Click the switch icon in the map.
2. In the displayed Snapshot page, click **Switch Port Mapper** under **Device Info**.
3. Click **Show Mapping** in the Switch Port Mapper window to view the mapping details.

## Enabling and Disabling a Switch Port

OpManager allows you to shut down a switch port when it is found to create problems in the network. While unmanaging a port temporarily stops OpManager from managing the port, disabling the port shuts down the port.

To shut down a switch port, click the port in the Switches Infrastructure view. Then click **Disable** under **Actions**.

To restart the port that is down, click the port in the Switches Infrastructure view. Then click **Enable** under **Actions**.



**Note:** Make sure you have provided correct SNMP write community string to shut down and start a port. Refer to [Modifying SNMP Parameters for a Device](#) for details.

## Changing Display Name of Switch Ports

You can give a meaningful name to switch ports for identifying them easily. To change the display name of a switch port, follow the steps given below:

1. [Open the snapshot page of the switch.](#)
2. Click **Configure Ports** under **Configure**.
3. Change the name of the port and click **OK**.

The display name of the port will be used in alarms and notifications and can be viewed in the Switch and Port snapshot pages.

## Viewing STP Port Details

STP information for every port can be viewed in the STP Port details table.

To view this table, follow the steps given below:

1. [Open the snapshot page of the device.](#)
2. Under **Device Info**, click **STP Port Details**.

The details that are displayed in this table are:

Field Name	Description
Port No.	The port number of the port for which this entry contains Spanning Tree Protocol management information
Priority	The value of the priority field which is contained in the first (in network byte order) octet of the (2 octet long) Port ID. The other octet of the Port ID is given by the value of Port No. field.
Port State	The port's current state as defined by application of the Spanning-Tree Protocol. This state controls what action a port takes on reception of a frame. The possible states of a port are: disabled, blocking, listening, learning, forwarding, and broken. This object will have a value, disabled, for ports which are disabled as in the Status field.
Status	The enabled/disabled state of the port.
Path Cost	The contribution of this port to the path cost of paths toward the spanning tree root which include this port.
Designated Cost	The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received bridge PDUs.
Root Cost	The cost of the path to the root as seen from this bridge.
Designated Bridge	The unique bridge identifier of the bridge recorded as the root in the configuration BPDUs transmitted by the designated bridge for the segment to which the port is attached.
Bridge Port	The port identifier of the port on the designated bridge for this port's segment.
Forward Transitions	The number of times this port has changed from the Learning state to the Forwarding state.

## Managing Routers

### Managing and Unmanaging Router Interfaces

During discovery, the interfaces connected to the external networks (the networks that are managed by OpManager) will not be monitored. To start managing them, in the Router snapshot page, click **Configure Interfaces** and select the check boxes under **Manage** corresponding to the interfaces to be managed.

Alternatively, to start managing an interface, click the interface from the Router Infrastructure view, and click **Manage** under **Actions**.

Also, if you do not want to manage certain links, you can stop managing the corresponding interfaces in OpManager. This stops the status polling and data collection to those interfaces.

To stop managing interfaces, in the Router snapshot page, click **Configure Interfaces** and deselect the check boxes under **Manage** corresponding to the interfaces to be unmanaged.

Alternatively, to unmanage an interface, click the interface from the Router Infrastructure view, and click **Unmanage** under **Actions**.



## Changing Display Name of Router Interfaces

You can give a meaningful name to router interfaces to identify them easily. To change the display name of the router interface, follow the steps given below:

1. [Open the snapshot page of the router.](#)
2. Click **Configure Interfaces** under **Configure**.
3. Change the name of the interface and click **OK**.

The display name of the port will be used in alarms and notifications and can be viewed in the Switch and Port snapshot pages.

## Viewing IP Routing Table

OpManager shows the IP Routing table with the information such as the route destination, interface name, IP address of the next hop and the type of routing.

To view the IP Routing table, follow the steps given below:

1. [Open the snapshot page of the router.](#)
2. Under **Device Info**, click **IP Routing Table**.

## Viewing IP Address Table

You can get the details of IP Addresses of the interfaces from the IP Address table.

To view it, follow the steps given below:

1. [Open the snapshot page of the router.](#)
2. Under **Device Info**, click **IP Address Table**.

## Managing UPS

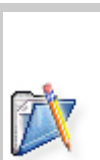
The UPS resources monitored are the UPS Load, Output Voltage, Output Current, Battery Status such as percentage charged, remaining backup time, battery health etc. A dial graph is displayed for the UPS Load.

To monitor the UPS resources,

1. From the UPS snapshot page, click Add Monitor in the Vendor Specific Monitors column.
2. Click **APC** under **Add Monitors**. The resources that can be monitored are listed.
3. Select the required resources to be monitored.
4. Click OK

The selected resources are monitored.

You can add custom monitors to monitor any other UPS resources other than the default ones.



**Note:**

1. The variables of PowerNet-MIB are queried to obtain the device information.
2. APC UPS is monitored by default. To monitor other UPS types, you can configure the UPS type in the configuration file **ups\_monitors.xml** present in <OpManager Home>/conf directory. You must include the required MONITOR element.

## Monitoring Exchange Servers

### Exchange Server Monitoring

You can monitor critical MExchange 2000/2003 Services and parameters using OpManager. Monitoring is done using WMI. Thresholds are pre-configured for critical services. You can also modify or enable thresholds for other services and parameters.

The services monitored are:

- Information Store
- Site Replication Store
- MTA Stacks
- Exchange Management
- SMTP
- POP3
- IMAP4
- System Attendent
- Routing Engine
- Event Service

The Exchange parameters that are monitored can be classified under the following categories:

- Address List Monitors
- POP3 and IMAP Monitors
- Information Store Public Folder Monitors
- Event Service Monitors
- SMTP Monitors
- Information Store Mailbox Monitors
- Message Transfer Agent Monitors
- Directory Service Monitors
- Information Store Monitors

You can configure the monitoring of [Exchange Services and the Parameters](#) for the Windows devices having Exchange Service.

## **Configuring Exchange Services to be Monitored**

The Exchange monitor can be associated to Windows devices. To configure a monitor,

1. Go to the snapshot page of the device running Exchange Service.
2. Click **Add Monitor** option against Application Monitors column in the snapshot page.
3. Click **MSExchange 2000/2003 Monitors (WMI Based)** from the list.
4. Select the required services and parameters and click **Add**.

## Active Directory Monitoring

Active directory monitoring feature takes OpManager a step further in proactive monitoring of Windows environment. The system resources of the Domain Controllers where the Active Directory (AD) database resides, and few critical Active Directory Services are monitored in OpManager.

To make AD monitoring more simple and easily accessible, The Domain Controllers are classified under a separate category under Infrastructure Views. The categorization of the device as a Domain Controller is done automatically if SNMP is enabled. The system resources of the device and the AD services are monitored using WMI.

The snapshot page of the Domain Controller shows a dial graph for AD Store in addition to the dial graphs for CPU, Memory, and Disk Utilization.

The other utilization data displayed in the snapshot page for the Domain Controller are:

- Resource Utilization by LSASS ( Local Security Authority Subsystem Service)
- Resource Utilization by NTFRS (NT File Replication Service)
- Ad Store Utilization
- Performance Counters showing information such as the AD Reads, the AD Replication objects etc

Besides these, following are the AD Services monitors associated by default. :

- Windows Time service : The service synchronizes the time between domain controllers, which prevents time skews from occurring.
- DNS Client Service : This service resolves and caches (Domain Name Server) DNS names.
- File Replication Service : This service maintains file synchronization of file directory contents among multiple servers.
- Intersite Messaging Service : This service is used for mail-based replication between sites. Active Directory includes support for replication between sites by using SMTP over IP transport.
- Kerberos Key Distribution Center Service : This service enables users to log on to the network using the Kerberos version 5 authentication protocol.
- Security Accounts Manager Service : This service signals other services that the Security Accounts Manager subsystem is ready to accept requests.
- Server Service : This service enables the computer to connect to other computers on the network based on the SMB protocol.
- Workstation Service : This service provides network connections and communications.
- Remote Procedure Call (RPC) Service : This service provides the name services for RPC clients.
- Net Logon Service : This service supports pass-through authentication of account logon events for computers in a domain.

You can add more AD Monitors to be monitored by clicking the Add Monitor button.

## Service Monitoring

### Configuring Services

#### Adding a New Service

In addition to out-of-the-box support provided for managing services, OpManager allows adding your own services to be managed on the network devices.

To manage a new service in your network, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Discovery**, select **Services**.
3. Select **Add New Service** under **Actions**.
4. Type the **Service Name**, **Time out** and **Port Number** of the service.
5. Click **Add Service**.




**Note:** To manage the added service in a device, please refer to [Specifying Services to Be Monitored in a Device](#).



## Modifying Service Configuration

You can modify the configuration settings of any service managed using OpManager. This will be required when the service is not running on the default port or if you wish to change the timeout interval. To know about the default ports of services managed by OpManager, refer to [Services and Their Default Ports](#).

To modify the settings, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Discovery**, select **Services**.
3. Click  corresponding to the service to be modified.
4. Modify the settings as required.
5. Click **Save** to apply the changes.

## Services and Their Default Ports

Following table lists the services managed by OpManager and the ports where they run by default:

Service Managed by OpManager	Default Port
DNS	53
Echo	7
Exchange (monitored using SNMP)	-
FTP	21
Finger	79
HTTPS	443
IMAP	143
LDAP	389
MSSQL	1433
MySQL	3306
NNTP	119
Oracle	1521
POP	110
SMTP	25
Telnet	23
Web	80
WebLogic	7001



## Managing Services

### Specifying Services to Be Scanned during Discovery

By default, OpManager scans each device on the network for the services that are chosen during discovery.

To modify this list, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Discovery**, click **Services**.
3. Select the check boxes under **Scan during discovery?**, corresponding to the services to be discovered and clear the selection for the services that are not to be discovered.

	<p><b>Note:</b></p> <ul style="list-style-type: none"><li>▪ The list contains the service names and the corresponding port numbers. To edit the settings of any of the available services, click <b>Edit</b> .</li><li>▪ If you do not find the service you want to manage in the list, you can add the service by clicking <b>Add New Service</b> under <b>Actions</b>. For details, refer to <a href="#">Adding a New Service</a>.</li></ul>
---	---


3. Click **Update** to apply the changes.

These settings will apply to all the subsequent discoveries.

## Specifying Services to Be Monitored in Devices

To select the services to be monitored in a device, follow the steps given below:

1. Click the device in the map.
2. Under **Service Monitors**, click **Add Monitor**.
3. Select the services to be discovered from the list and click **OK**.

	<p><b>Note:</b></p> <ul style="list-style-type: none"><li>▪ The list contains the service names and the corresponding port numbers. To edit the settings of any of the available services, refer to <a href="#">Modifying Service Configuration</a>.</li><li>▪ If you do not find the service you want to manage in this list, you can add the service with the necessary parameters to manage it. For details, refer to <a href="#">Adding a New Service</a>.</li></ul>
---	--

To associate the services to many devices at a time, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Discovery**, select **Services**.
3. Click **Associate to Devices** in the Actions list.
4. Select the service to be monitored from the drop-down list.
5. Select the devices from the list in the left and click >>.
6. Click **Save**.

The service will be scanned in these devices and if found running, OpManager starts managing them. You can also achieve this using the Quick Configuration Wizard tool that can be invoked by clicking **Quick Configuration Wizard** under **Tools** in the **Admin** tab.

## Viewing Service Status and Response Time

Open the snapshot page of the device.

Under **Service Monitors**, you will see the list of services managed in the device, if any, with their status and current response time.

- Click the service name to view the historical report on the response time and the availability chart of the service.
- Click the Availability chart to view the service downtime/uptime chart, summary and historical information.



**Note:**

To view the 7 days or 30 days report, click **7** or **30**.

## Windows Services Monitoring

### Monitoring Windows Services

Certain applications in Windows machine run in the background as services. You can monitor the status of such services using OpManager and configure to generate alarms whenever they fail.



**Note:** To monitor Windows services, OpManager should be installed in a Windows machine.

OpManager can manage the following Windows services out-of-the-box:

- Alerter
- DHCP Server
- DNS Server
- Disk Manager
- Event Log
- FTP
- IAS
- IIS
- Messenger
- MySQL
- Net Logon
- Print Spooler
- RPC
- Telephony
- Telnet

To monitor these services in your Windows devices, refer to [Associating a Windows Service Monitor to a Device](#). If you want to monitor a Windows service that is not in the list, refer to [Creating Windows Service Monitor](#).

## Creating a Windows Service Monitor

In addition to the Windows services monitor supported by OpManager out-of-the-box, you can add your own monitors.

To create a Windows service monitor, follow the steps given below:

1. Under the **Admin** tab, click **Windows Service Monitor**.
2. Under **Actions**, click **Add New Service**.
3. Type the name of the service in the **Service Name** field as it appears in the Services window. Note that this field is case-sensitive.
4. Enter a display name for this service in the **Name** field.
5. If you want to restart the service or the server itself when the service is down, select the check box in the page and then select between the options.
6. Click **Add Service**.

Use the **Associate to Devices** link under **Actions** to associate this service to servers.



**Note:** To monitor Windows services, OpManager should be installed in a Windows machine.

## Associating a Windows Service Monitor with a Device

OpManager uses WMI to monitor the Windows services and hence you need to provide the log on details of a user with administrative privilege to connect to the device. For steps, refer to [Configuring WMI/Telnet/SSH Authentication Details](#) topic.

To monitor a Windows service, follow the steps given below:

1. [Open the snapshot page of the device.](#)
2. Click **Add Monitor** in the **Windows Service Monitors** section. This option will be available only for Windows servers.
3. Select the services to be monitored in the device and click **OK**.



**Note:** To monitor Windows services, OpManager should be installed in a Windows machine.

Alternatively, you can associate a Windows service monitor to many devices at a time using Quick Configuration wizard.

To do so, follow the steps given below:

1. In the **Admin** tab, under **Tools**, click **Quick Configuration wizard**.
2. Select **Add a monitor** and click **Next**.
3. Select **Associate a Windows service** and click **Next**.
4. Choose the service to be monitored and click **Next**. The Windows servers managed in your network will be listed.
5. Move the devices from the list in the left to the one in the right to monitor the selected service in them and click **Finish**.



## Windows Event Logs Monitoring

### Event Log Monitors

The Event Log is a Windows service that logs about program, security, and system events occurring in Windows devices. The events can be related to some application, system or security. You can monitor these events using OpManager and configure to generate alarms when critical events are logged. OpManager uses WMI to fetch the details of these logs and hence you need to provide the log on details of a user with administrative privilege to connect to the Windows machine. For steps, refer to the [Configuring WMI/Telnet/SSH Authentication Details](#) topic.

You can view the list of all events monitored by OpManager, by clicking **Event Log Rules** under the **Admin** tab. To monitor these events in a Windows machine, refer to [Monitoring Windows Events in a Device](#). To add a new monitor, refer to [Creating an Event Log Monitor](#).



**Note:** To monitor Windows event logs, OpManager should be installed in a Windows machine.

## Creating an Event Log Monitor

To create an event log monitor, follow the steps given below:

1. Under the **Admin** tab, click **Event Log Rules**.

In this page, you can see the rules supported by OpManager. They are categorized into Applications, Security, System, DNS Server, File Replication Service, and Directory Service. You can add the event logs that you want to monitor under any of these categories.

2. Click **New Rule** under any one of the categories to add a rule in it.

Entries to all the fields except Rule Name are optional. Event ID is a required field to identify the event but can be left empty in few exceptional cases, such as you want to monitor all events that are of the Event Types, say, error or information. Here the filter will be based on the Event Type.

- Type a unique **Rule Name**.
- Enter the **Event ID** to be monitored. This is the unique identifier for the event logs.
- Enter the event **Source**. This is the name of the software that logs the event.
- Enter the event **Category**. Each event source defines its own categories such as data write error, date read error and so on and will fall under one of these categories.
- Type the **User** name to filter the event log based on the user who has logged on when the event occurred.
- Choose the **Event Types** to filter the event logs based on its type. This will typically be one among Error, Warning, Information, Security audit success and Security audit failure.
- Enter the string to be compared with the log message. This will filter the events that contains this string in the log message.
- Choose a severity for the alarm generated in OpManager for this event.

3. Click **Add Rule** to save the event log rule.



**Note:** To monitor Windows event logs, OpManager should be installed in a Windows machine.

## Monitoring Windows Events in a Device

To monitor Windows events, you need to associate the event log monitors with the device. To do so, follow the steps given below:

1. [Open the snapshot page of the device.](#)



**Note:** Make sure you have provided the WMI authentication details for the device. Refer to [Configuring WMI/Telnet/SSH Authentication Details](#) for steps.

2. Click **Event Log Rules** under **Configure**.
3. Select the event logs to be monitored in the device.
4. Change the **Polling Interval** if necessary. During each poll, the selected event logs are compared with the events logged in the device and for the matching events, alarms will be generated.
5. Click **Save** to save the changes.



**Note:** To monitor Windows event logs, OpManager should be installed in a Windows machine.

Alternatively, you can associate an event log rule with many devices at a time using Quick Configuration wizard.

To do so, follow the steps given below:

1. In the **Admin** tab, under **Tools**, click **Quick Configuration wizard**.
2. Select **Event Log** and click **Next**.
3. Choose the type of log from the list. The rules defined under the selected log type will be listed.
4. Choose a rule and click **Next**. The Windows servers managed in your network will be listed.
5. Move the devices from the list in the left to the one in the right to monitor the selected service in them and click **Finish**.

## Device and Application Monitors

### OpManager Monitors: Overview

OpManager provides a variety of monitors out-of-the-box that helps you know the performance of your network devices. You can also configure your own monitor for any SNMP variable of a managed device. Once a monitor is configured and associated with a device, OpManager collects data and shows them in the form of graphs. To plot the graphs, the SNMP variables must be of numeric data type.

OpManager supports host resources monitors for SNMP and non-SNMP devices. In case of non-SNMP devices, you can configure OpManager to use WMI in Windows machines and Telnet/SSH protocol in Linux/Solaris machines and fetch the performance data. For this, you need to provide the corresponding authentication details. Refer to [Configuring WMI/Telnet/SSH Authentication Details](#) for details.

Following are the monitors supported by OpManager by default:

- **Resource Monitors**
  - *Resource monitors - for SNMP-enabled Windows, Linux and Solaris devices*  
Monitors for CPU, memory, and disk utilization, free and used disk space, and active system processes.
  - *WMI-based monitors - for non-SNMP Windows devices*  
Monitors for CPU, memory, and free and used disk space.
  - *Telnet/SSH-based monitors - for Linux and Solaris devices*  
Monitors for CPU, memory, and free and used disk space.
  - *Cisco monitors*  
Monitors for used memory, free memory, buffer create failures, largest free memory, and CPU usage.
  - *3COM monitors*  
Monitors for CPU temperature and utilization.
- **Traffic Monitors**
  - *Traffic monitors*  
Monitors for interface Tx and Rx traffic, utilization, errors, and discards.
  - *RMON monitors*  
Monitors jabber, oversize, and undersize packets, packets to BC and MC addresses, total number of collisions, total number of octets, number of fragments and drops events statistics.
- **Application Monitors**  
Monitors for MS-Exchange, MSSQL, RDBMS, Oracle, and Lotus applications.
- **Vendor-specific Monitors**  
Monitors for Cisco devices, Dell PowerEdge servers, and Compaq Proliant servers.
- **Custom Monitors**  
Monitors that you create on your own. Refer to [Creating a Custom Monitor](#) for steps to create you own monitor.

## Creating a Custom Monitor

In addition to OpManager's [default monitors](#), you can also create your own monitors for the SNMP-enabled devices in your network.

To create a custom monitor, follow the steps given below:

1. In the **Admin** tab, under **Monitors**, click **Custom Monitors**.
2. Click **Add new custom graphs** under **Actions**.
3. Select the SNMP OID to be monitored by clicking the Select button.
4. Enter a name and display name for the monitor.
5. Type the polling interval and the unit of data collection.
6. Click **Save**.



**Note:** To configure the graph profile to an SNMP-enabled device, refer to [Assigning a Graph Profile to an SNMP-Enabled Device](#).

## Associating a Monitor with a Device

You can associate a monitor to a device that helps in keeping track of the performance of the device and pro-actively managing the device.

To do so, follow the steps given below:

1. In the **Admin** tab, under **Tools**, click **Quick Configuration wizard**.
2. Select **Add a monitor** and click **Next**.
3. Select the type of monitor and click **Next**.
4. Choose the monitor to be associated and click **Next**.
5. Select an option to associate the monitor and click **Next**.
  - If you select a category, then the profile will be associated with all the devices in the category automatically.
  - If you choose Select devices manually, the next page will list all the managed devices. Move the devices from the list in the left to the one in the right and click **Finish**.
  - If you choose a business view, the profile will be associated with all the devices in the view. This option will be available only if you have created at least a business view.

Alternatively, to associate a monitor with a particular device, follow the steps given below:


1. [Open the snapshot page of the device](#).
2. Under **Monitors**, click **Add Monitor** in the category under which you want to add a monitor. You can associate a resource monitor, service monitor, traffic monitor or an application-specific monitor with the device. Refer to the list of [default monitors](#) to know about the monitors available under each category.
3. Click the monitor to associate it with the device. For WMI, Telnet and SSH based monitors, you need to provide the authentication details. Refer to [Configuring WMI/Telnet/SSH Authentication Details](#) for details. All other monitors need SNMP to be configured properly in the device.
4. Click **OK**.

## Configuring Threshold for Critical Parameters

Using OpManager, thresholds can be set so that an alarm is generated when the status of a device crosses a certain limit. This way, OpManager helps monitor the device's health and detect degradation much before the device fails, thereby enabling proactive device management.

To configure a threshold rule, follow the steps given below:

*If you want to configure threshold for a parameter in all the managed devices, under the **Admin** tab, click **Monitors**. Then follow the steps given below.*

*If you want to configure threshold for a parameter in a device alone, [open the snapshot page of the device](#). Under **Monitors**, click **Show All**. Click **Edit**  corresponding to the monitor for which you want to configure threshold. Then follow the steps given below.*

1. Verify whether the monitor is already available in the list. If available, select the profile and click **Edit**. Otherwise, create a new profile.
2. Select the **Enable Threshold** check box.
3. Enter the **Threshold Limit** and select the **Threshold Check** condition.
4. Specify the message and the severity of the alarm to be generated when the threshold rule is violated.
5. Specify the number of times the threshold rule can be violated before generating an alarm. This will be needed for monitors like traffic, CPU utilization and others, where there could be a sudden rise in the value that would come down to normal during the next polling.
6. Enter the **Rearm Value** for generating a Clear alarm.
7. Click **OK** to apply the changes.

## Modifying Monitor Settings

You can modify the settings of OpManager graphs and custom graphs whenever required. You can change the interval in which the data is collected, set a different name to be displayed in graph, and change the text that explains the units for data.

To change the graph settings globally, follow the steps given below:

1. In the **Admin** tab, under **Monitors**, select the category of the monitor to be modified.
2. Select the sub-category of the monitor from the displayed list and click the monitor to be modified.
3. Edit the fields in the page as required.
4. Click **Save**.

**Note:**

- The changes made here will be applied globally. Hence, if a profile assigned to some devices is changed, the changes will have effect on the graphs of all these devices.
- To change the graph settings that affect only a particular device, refer to [Modifying Monitor Settings for a Device](#).



## Testing the Configured Monitors

You can test a configured monitor for a device. This helps you determine the current performance of a system resource. For instance, if you would like to know the current CPU utilization value of a device for which you have already configured a [resource monitor](#), you can follow the steps below:

1. In the [device snapshot](#) page, click the **Edit** icon against the required monitor.
2. In the Monitor Properties screen, click the link **Test Monitor**.  
The current value is displayed.

The **Test Monitor** option is available for Resource Monitors, Traffic Monitors, Application Monitors, Vendor Specific Monitors, etc.

## Viewing Graphs

1. [Open the Device Snapshot page of the device.](#)
2. Click **Show All** in the **Monitors** section.
3. Click on the monitor whose graph you want to view.



**Note:**

- Click on the graph area to get the detailed view.
- By default, the graph is displayed for the current day. Click **7<sup>d</sup>** or **30<sup>d</sup>** to view the graph for the past 7 days or 30 days respectively.
- For a router, the graphs for buffer hits, buffer misses, buffer create failures, and CPU and memory usage in KB are available in the Device Snapshot page.

## Resource Monitoring

### SNMP-based Monitoring in Windows/Linux/Solaris

System resources such as CPU, Memory, etc can be monitored in Windows, Linux, and Solaris devices using SNMP. Steps to configure a resource monitor for a device is explained below:

1. [Go to the device snapshot page.](#)
2. Under **Monitors**, click **Add Monitor** in **Resource Monitors** column.
3. Click **SNMP based Resource Monitors** under **Add Monitors**
4. Click the required resource from the list such as Disk Utilization, and click **OK**
5. Configure the correct Read/Write community for the device:
  - In the device snapshot page, click **Passwords** under **Configure** tab
  - In the configuration screen that pops up, type the correct Read/Write Community

You can also configure and [associate the monitor to a group of devices or to a category](#) of devices.

## WMI-based Monitoring for Windows

System resources such as CPU, Memory, etc can be monitored in Windows devices using WMI. Steps to configure a resource monitor for a device is explained below:

1. [Go to the device snapshot page.](#)
2. Under **Monitors**, click **Add Monitor** in **Resource Monitors** column.
3. Click **WMI based Monitors** under **Add Monitors**
4. Click the required resource from the list such as Disk Utilization, and click **OK**
5. Configure the [user name and password details](#) for the device.

You can also configure and [associate the monitor to a group of devices or to a category](#) of devices.

## Telnet and SSH based Monitoring in Unix Devices


System resources such as CPU, Memory, etc can be monitored in Linux and Solaris devices using Telnet. Steps to configure a resource monitor for a device is explained below:

1. [Go to the device snapshot page](#).
2. Under **Monitors**, click **Add Monitor** in **Resource Monitors** column.
3. Click **Telnet/SSH based monitors for Linux** for linux devices and click **Telnet/SSH based monitors for Solaris** for solaris devices.
4. Click the required resource from the list such as Disk Utilization, and click **OK**
5. Configure the [user name and password details](#) for the device.

You can also configure and [associate the monitor to a group of devices or to a category](#) of devices.


## Viewing Asset Details.

If you have both, OpManager and ServiceDesk Plus running in your network, you can view a detailed asset information of a device, provided the device is discovered in both the applications, and the [ServiceDesk settings are configured](#) in OpManager.

To view the Asset Details, select the device and click **Asset Details** . This will show the detailed asset information from ServiceDesk Plus.

The details about the operating system, the disk size, and the RAM size will not be gathered for non-SNMP devices.

To enter these details manually for such devices, follow the steps given below:

1. Select the device and click **Asset Details** .
2. Enter the values of **Operating System**, **RAM size**, and **Hard Disk**.

The value "Unknown" for Operating System and "Details not available" for RAM Size and Hard Disk fields denotes that the SNMP agent was not running in the device during discovery. You can enter values to this fields manually.

3. Click **Save** to apply the changes.

## Customizing Snapshot Page

The device snapshot page, by default displays the dial graph for the resources Disk Utilization, Memory Utilization, and CPU Utilization. You can customize to show the dial for the required resources.

The steps to configure are,

1. From `<OpManager Home>/conf` directory, open the file **opmanager\_snapshot\_dial.xml** file.
2. Add a new Snapshot DIAL entry for the required CATEGORY like Routers, Switches, Desktops etc.

### Example:

To add Interface Rx Utilization as a new DIAL entry to the Server Category, the entry in the configuration file would be:

```
<DIAL name="InterfaceInUtilization"
  displayName="Interface In Utilization"
  dialType="meter"
  shortKey="Rx Util">
  <PARAM type="windows"
    pollKey="InterfaceInUtilization"/>
  <DEFAULT pollKey="InterfaceInUtilization"/>
</DIAL>
```



### Note:

- Only three dials can be displayed at a time.
- Snapshot dials is displayed only for the resources for which the monitored value is in percentage (unit is %, like CPU Utilization, Interface Tx Utilization, Disk Utilization etc...).

The name of the dial corresponds to the Graph Name as specified in `<OpManager Home>/ conf/opmanager_graphInfo.xml` file. In case you wish to add a custom monitor as the snapshot dial, use the name of the custom monitor.

## URL Monitoring

### Configuring URL Monitors

You can configure OpManager to monitor your Web sites. Many business enterprises require continuous monitoring of their Web sites, as the failure of these sites might have an impact on the business.

You can monitor global URLs, such as [www.yahoo.com](http://www.yahoo.com) and [www.adventnet.com](http://www.adventnet.com) or URLs in a server, such as <http://192.168.4.11/index.html>, <http://web> and so on.

You can perform a content match on these URLs and confirm their availability. Further, for pages that require a form submit, such as user name and password, you can provide these details and verify the availability of the next page.



**Note:** If a proxy server is configured in your network, make sure to provide its details in the Proxy Server Settings page of OpManager. Refer to [Configuring Proxy Server Settings](#) for steps to do this. This is required for monitoring any URL in a proxy-enabled LAN.

To configure a global URL monitor, follow the steps given below:

1. Under the **Admin** tab, click **URL monitor**. In this page you can add, edit, and delete the URL monitors.
2. To add a URL monitor, click **Add URL**.
3. Enter a name to the URL monitor in the **URL Monitor name** field.
4. Type the **URL address** to be monitored.
5. Type the **Polling Interval** and the value of **Timeout** in the respective fields.
6. Enter the **Email ID** to send the alert when this URL goes down, if needed.
7. Type the string to be compared with the contents of the monitored Web page.
8. Select between **Get** and **Post**, the methods for any HTTP/HTTPS-based URLs. This is required because certain URLs cannot be accessed using a Get request.
9. Type the request parameters and their values in the form <parameter name>=<value>, if any, to know the actual availability of the URL. Note that you can enter only one parameter in a line.

This will be required in the pages where you need to log-on and test the availability of the host.

Entries to the fields in the Other Details section and the **Send Alert to** field are optional.

Click **Check Now** to check the availability of the URL based on the given details. You can verify the correctness of the given details using this instant check.

10. Click **Add** to add the URL monitor.



**Note:** Use the **Edit**  and **Delete**  icons in the Configure URL page to edit and delete the URL monitors.



## Managing a URL in a Server

You can monitor a URL hosted in a server. If the same URL is managed on multiple servers for undisturbed availability, you can trace the failure details by monitoring the URL in each server.

1. Enter a name to the URL monitor in the **URL Monitor name** field.
2. Type the **URL address** to be monitored. For example  
http://10.12.10.2/index.html or http://web
3. Type the **polling interval** and the value of **timeout** in the respective fields.
4. Type the string to be compared with the contents of the monitored Web page, in the **Match Content** field.
5. Select between **Get** and **Post**, the methods for any HTTP/HTTPS-based URLs. This is required since certain URLs cannot be accessed using a Get request.
6. Type the request parameters and their values in the form <parameter name>=<value>, if any, to know the actual availability of the URL. Note that you can enter only one parameter in a line.

You can configure to receive an e-mail or SMS when the URL monitored in a server goes down. For this, you need to create an [e-mail/SMS](#) notification profile with the criteria URL is down option selected and [associate it with this server](#).

## **URL Response Time and Availability**

You can get the details about the URL response time and availability in the URL snapshot page.

To view the URL snapshot, click the URL link in the Home page or Maps tab. Then click the URL whose snapshot you want to view.

Click the Availability chart to view the availability history and the URL downtime/uptime chart.

## Trap Processing

### OpManager Trap Processors

OpManager enables you to process the traps from the managed devices. By default, the traps in the list below are processed. When a trap is received from a managed device, OpManager notifies the administrator with an alarm. You can configure the severity and the message of the alarm generated for the traps.



**Note:** Ensure that SNMP agent is running in the managed devices and also the agent is configured to send traps to OpManager Server. Refer to [Configuring SNMP Agents](#) for details.

### Types of traps

OpManager provides out-of-the-box support for the following generic traps and generates alarm with the respective severity as specified in the table below:

Trap Name	Description	Severity
LinkUp	A communication interface has been enabled.	Clear
LinkDown	A communication interface has been disabled.	Critical
AuthenticationFailure	A message that cannot be authenticated has been received.	Trouble
EgpNeighborLoss	An Exterior Gateway Protocol (EGP) neighbor has been lost.	Trouble
ColdStart	The agent is reinitializing. The SNMP data and configuration might have changed.	Attention
WarmStart	The agent is reinitializing without any change in the SNMP data and configuration.	Attention
Cisco Voltage Change Status	The voltage measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the warning, critical, or shutdown stage). Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the Cisco Shutdown trap.	Trouble
Cisco Config Management Event	The Cisco configuration has been changed.	Trouble
Cisco Temperature Change Status	The temperature measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the warning, critical, or shutdown stage). Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the Cisco Shutdown trap.	Trouble

Trap Name	Description	Severity
Redundant Supply Notification	The redundant power supply (where extant) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the Cisco Shutdown trap.	Trouble
Cisco Fan Status	One of the fans in the fan array (where extant) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the Cisco Shutdown trap.	Trouble
Cisco Shutdown	The environmental monitor detects a testpoint reaching a critical state and is about to initiate a shutdown. This notification contains no objects so that it may be encoded and sent in the shortest amount of time possible. Even so, management applications should not rely on receiving such a notification as it may not be sent before the shutdown completes.	Critical

## Creating a Trap Processor

OpManager supports basic SNMP traps out-of-the-box. Operators can add support for traps from any custom SNMP MIB. OpManager can extract useful information that is sent with SNMP traps as variable bindings (SNMP varbinds). So if you have bought devices from different vendors, all you need to do is get access to those vendor-specific MIBs and you can easily have OpManager monitor critical variables on that device.

OpManager compares the received traps with the defined set of trap processors and converts them into meaningful alarms. These alarms can be used to send e-mail or SMS notification. If a managed device sends a trap that has not been defined, you can view them in the [Unsolicited Traps view](#).

To create a trap processor, follow the steps given below:

1. Click **SNMP Trap Processors** under the **Admin** Tab.
2. Click **Add New Trap Processor** under **Actions**.
3. Fill in the values for the text fields in this dialog.
4. Click **Add**.



**Note:** OpManager compares the received traps with the defined set of trap processors in the order they appear in the list.

## Loading Traps From MIB

Trap Processors are defined for few traps by default in OpManager. But for few MIBs, the processor is not configured. Instead of manually defining a processor for the trap variables in such MIBs, OpManager provides an option in the WebClient to load the traps and add a processor immediately.

Following are the steps to load the traps from various MIBs.


1. Under the **Admin** tab, select **SNMP Trap Processors**. All the configured processors are listed here.
2. On the right, select **Load Traps from MIB** under **Actions**
3. From the list of MIBs, select the MIB from which you would like to load the trap variable. The traps in that MIB are listed.
4. Select the required Mib, and click **Add Trap Processor(s)**.

A Processor for the selected trap is added, and is listed under the SNMP Trap Processors.

## **Modifying Trap Processor Settings**

You can change the trap settings and the alarm settings of the trap processors.


To modify a defined trap processor, follow the steps given below:

1. Click **SNMP Trap Processors** under the **Admin** Tab.
2. Select the trap processor to be modified from the list and click  .
3. Make necessary changes to the text fields.
4. Click **Update**.
5. Click **OK**.


## Enabling and Disabling Trap Processors

If you do not want OpManager to listen to a trap that has a processor defined for it, OpManager allows you to disable them temporarily. Later you can enable the trap processor to start listening to the corresponding trap.

### To disable a trap processor

1. Click **SNMP Trap Processors** under the **Admin** Tab.
2. In the list of trap processors, click  corresponding to the trap processor name.
3. Click **OK**.

### To enable a trap processor

Click  corresponding to the disabled trap processor.



## Events and Alarms

### Maintaining Events and Alarms

OpManager allows you to maintain events and alarms for a particular period and delete them automatically.

To configure settings for maintaining events and alarms, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Global Settings**, click **Database Maintenance**.
3. In the **Maintain \_\_\_\_\_ recent Alarms in the database** box, type the number of recent alarms that you want to maintain always. The default value for this option is 10000, that is, at any time, a maximum of 10000 recent alarms can be maintained.
4. In the **Delete Events older than \_\_\_\_\_ days** box, type the number of days for which the events are to be maintained. The default value is 30, that is, events will be deleted after 30 days from the day they were generated.
5. Click **Save** to save the settings.

## Viewing Events and Alarms

OpManager helps you to identify the fault quickly in a device using the Alarms.

Using OpManager you can view,

- [the devices under trouble](#)
- [the list of unsolicited traps](#)
- [the list of all alarms generated](#)
- [the list of alarms that are yet to be cleared](#)
- [the list of alarms generated for a particular device](#)

You can also quickly get the snapshot of alarms from the Alarms Graph in the Home Page. You can see the recently generated 10 alarms in your network here.

### Viewing Devices under Trouble

1. Click the **Alarms** tab.
2. Click **Devices to watch** under the **Alarms** section.

You can view the devices with fault in this map. This map is similar to any other map in OpManager, in the way that you can perform all device-related actions such as viewing and configuring device settings.

### Viewing Unsolicited Traps

1. Click the **Alarms** tab.
2. Click **Unsolicited Traps** under the **Alarms** section.


The unsolicited traps sent by the agents in the managed devices are listed here. These are the traps that are not configured to be processed in OpManager.

If you find any of these traps to be critical, you can configure OpManager to process the traps using the information that are received from the agent. Refer to [Creating a Trap Processor](#) for details.

### Viewing All Alarms

1. Click the **Alarms** tab.
2. Click **All Alarms** under the **Alarms** section.

The list displays the details, namely the device name, device type, severity of the alarm generated, date and time of alarm generation, and a brief description about the fault in the device.

	<p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▪ To sort the list by a column, click the respective column heading.</li> <li>▪ The panel above the list shows the range of alarms that are currently displayed. Use the navigation bar at the right end of the panel to navigate through the list.</li> <li>▪ To view the list of events generated for a particular device, click the alarm message link of the corresponding alarm.</li> <li>▪ OpManager allows you to configure the number of alarms to be maintained. For details, refer to <a href="#">Maintaining Events and Alarms</a>.</li> </ul>
---	--

### **Viewing Active Alarms**

To view only the active alarms that are not yet cleared,

1. Click the **Alarms** tab.
2. Click **Active Alarms** under the **Alarms** section.

The list displays the details, namely the device name, device type, severity of the alarm generated, date and time of alarm generation, and a brief description about the fault in the device.

### **Viewing Alarms Generated for a Device**

1. Click the device icon in the map.
2. Under **Actions**, click **Show Alarms**.

## Working with Alarms


### Acknowledging an Alarm

OpManager provides an option to mark the alarms on which you have worked on. This helps the other operators working on alarms to know the current status.

To acknowledge an alarm, click  in the **Actions** column corresponding to the alarm.




**Note:**

1. This changes the icon to . Click on this to revert the operation and show the alarm as not acknowledged.
2. To acknowledge multiple alarms at a time, select the alarms and click **Acknowledge**.

## **Adding Notes to an Alarm**

You can add notes to the alarms to explain the steps you have followed to correct the fault or to give tips to the operator who is working on the fault.

To add notes, follow the steps given below:

1. Click the **Alarms** tab.
2. Click the message of the alarm to be annotated.
3. Click  **Add Notes**.
4. Type the notes in the displayed window and click **Annotate**.

The notes will be maintained even if the severity of the alarm changes for a device and can be used for future reference.

## Clearing an Alarm Manually

The alarms generated by some traps, such as coldStart and warmStart are not cleared automatically. You need to clear them manually once the device is rebooted successfully.

To clear such alarms, select the alarm and click **Clear**.

## Deleting an Alarm

All generated alarms are displayed in the alarms list until they are manually deleted or until the number of alarms reaches the limit as specified in the OpManager Settings dialog.

To delete the alarms, select the alarm and click **Delete**. Click **Yes** to confirm deletion.

To configure OpManager for deleting alarms automatically when the number of alarms exceeds a limit, refer to [Maintaining Events and Alarms](#).

## Escalating Alarms when not Cleared

The alarms of critical devices should not be left unnoticed for a long time. For instance, the mail-servers, web-servers, backup-servers, switches, and routers are so critical that if their faults are not solved within a specified time, the networking functionality will be brought down. You can configure OpManager to escalate such unnoticed alarms by sending an e-mail to the person concerned.

To configure an alarm escalation rule, follow the steps given below:

1. Click the **Admin** Tab.
2. Under **Global Settings**, click **Alarm Escalation**.
3. Click **Add New Rule** to create a rule.
4. Assign a name to the rule in the **Rule Name** box.
5. Select the **Severity** and **Category** of the alarm. Then type the interval to wait for the alarm to get cleared.
6. Type the values for fields under Escalation Email Details to send an e-mail if the alarm is not cleared within the specified interval.
7. In the **Run this check every** box, set the interval to execute this rule.
8. Click **OK**.

For example, let us assume that you want to escalate the fault to manager@yourCompany.com, if the alarm of Trouble severity and Switch category is not cleared within 1 hour, then do the following:

1. Select Trouble from the first list and Switch from the second list. Then type 1 in the box and select hours from the list next to it.
2. Then click '**this mail id**'. Enter your company's mail-server name, recipient's mail ID (in this case, manager@yourCompany.com), sender's mail ID (in this case, your mail ID), subject and the message to be sent with the mail.
3. Type 2 in the **Run this check every \_\_\_ hours** box.

## Configuring Notifications

### Configuring Notifications: Overview

When a fault is detected in your network, an event is said to occur. OpManager processes this event and generates an alarm. You can configure OpManager to notify the network administrator or perform automatic actions based on the alarm raised for a device. To know about events and alarms, refer to [About OpManager Events and Alarms](#).

OpManager provides options to perform the following notification actions:

- [Send an e-mail](#)
- [Send a message to a cell phone](#)
- [Run a system command](#)
- [Run an external program](#)
- [Log a trouble-ticket to ServiceDesk Plus](#)

OpManager maintains these actions as profiles so that they can be assigned to any number of devices. Once a notification profile is assigned to a device, corresponding action will be performed whenever an alarm is generated for the device.



## Creating an E-Mail Notification Profile

You can configure OpManager to send e-mail to network administrators whenever a fault is detected in the device. You can create separate profiles for each administrator and assign them to devices so that whenever the device is under trouble, depending on the trouble, an e-mail will be sent to the respective person.

To create an e-mail notification profile, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Global Settings**, click **Notification Profiles**.
3. Under **Add New**, click **Email**.
4. Assign a meaningful name to this profile.
5. Type valid To and From Email addresses.
6. Type the name of the SMTP server and the port number. If the SMTP server needs authentication to send e-mail, provide the **User Name** and **Password** details here.



**Note:** Primary and secondary SMTP server settings can be provided in the Mail Server Settings page in OpManager. Whenever a new e-mail profile is created, the values of the primary SMTP server and the authentication details will be considered from the Mail Server settings. Refer to [Configuring Mail Server Settings](#) for steps to enter the details. If the SMTP server is not available while sending e-mail, secondary mail server will be used to send the mail automatically.

7. Type a meaningful **Subject** and **Message** for the mail. Along with the message you type in these fields, if you want to see device-related details in the mail, use the list box beside the subject and message boxes. These variables fetch the details about the fault in the device.
8. Select the options under **Criteria**, if you want to restrict sending the e-mail to particular events, such as when device is down, when a service outage occurs, when threshold is violated and so on.



**Warning:** If you do not select any option under **Criteria**, by default, OpManager will send notification for all alarms generated for the device. For more details about criteria options, refer to Notification Criteria Options.

9. Verify the entries that you have made and click **Submit**.



**Note:** You need to associate the notification profile to a device to trigger the alert for the faults in the device. For steps, refer to [Associating Notification to Managed Devices](#).

## Creating an SMS Notification Profile

You can configure OpManager to send SMS to network administrators whenever a fault is detected in the device. You can create separate profiles for each administrator and assign them to devices so that whenever the device is under trouble, depending on the trouble, SMS will be sent to the respective person.

To create an SMS notification profile, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Global Settings**, click **Notification Profiles**.
3. Under **Add New**, click **SMS**.
4. Assign a meaningful name to this profile.
5. Type valid To and From Email addresses.
6. Type the name of the SMTP server. If the SMTP server needs authentication to send the message, provide the **User Name** and **Password** details here.



**Note:** Primary and secondary SMTP server settings can be provided in the Mail Server Settings page in OpManager. Whenever a new SMS profile is created, the values of the primary SMTP server and the authentication details will be considered from the Mail Server settings. Refer to [Configuring Mail Server Settings](#) for steps to enter the details. If the SMTP server is not available while sending e-mail, secondary mail server will be used to send the mail automatically.

7. Type a meaningful **Message**. Along with the message you type, if you want to see device-related details, use the options in the list box beside the message box. These variables fetch the details about the fault in the device.
8. Select the options under **Criteria**, if you want to restrict sending the message to selected faults, such as when device is down, when a service outage occurs, when threshold is violated and so on.



**Warning:** If you do not select any option under **Criteria**, by default, OpManager sends notification for all alarms generated for the device. For more details about criteria options, refer to Notification Criteria Options.

9. Verify the entries that you have made and click **Submit**.



**Note:** You need to associate the notification profile to a device to trigger the alert for the faults in the device. For steps, refer to [Associating Notification to Managed Devices](#).

## Notification by Running a Program

You can configure OpManager to automatically run a program whenever a fault is detected in the device. For instance, you can configure OpManager to execute a program that corrects the fault or simply produces a sound or that whenever a specific type of an alarm is raised for a device.

To create a profile that executes the specified program, follow the steps given below :

1. Click the **Admin** tab.
2. Under **Global Settings**, click **Notification Profiles**.
3. Click **Run Program** under **Add New**.
4. Type the name of the program and arguments for executing the program, if any.
5. Select the options under **Criteria** for which the program has to be executed.



**Warning:** If you do not select any option under **Criteria**, then by default, OpManager sends notification for all alarms generated for the device.

6. Verify the entries you have made and click **Submit**.



**Note:**

1. You can insert alarm variables to the arguments of the program. For details, refer to [Using Alarms Variables in Notification Profile](#).
2. Make sure to assign the profile to the devices to get notified whenever the devices are under trouble. To assign the notification profile to a device, refer to [Assigning Notification for a Device](#).
3. To create your own sound notification profiles, refer to [Creating Sound Notification Profiles](#).

## Notification by Running a System Command

You can configure OpManager to execute a system command automatically whenever an alarm is raised in the network. For instance, Windows-based command "net send" can be used to notify the administrator based on the alarm raised for a device.

To create a notification profile of this type, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Global Settings**, click **Notification Profiles**.
3. Click **System Command** under **Add New**.
4. Type the command to be executed and select the options for appending the output and the error message on executing the command.
5. Select the options under **Criteria** for which the command has to be executed.



**Warning:** If you do not select any option under **Criteria**, then by default, OpManager sends notification for all alarms generated for the device.

6. Verify the entries you have made and click **Submit**.



**Note:**

1. You can insert alarm variables to the arguments of the program. For details, refer to Using Alarms Variables in Notification Profile.
2. Make sure to assign the profile to the devices to get notified whenever the devices are under trouble. To configure the notification profile to a device, refer to [Assigning Notification for a Device](#).

## Creating a Sound Notification Profile

By default, OpManager provides a sound notification that plays a beep sound when a fault is detected in the associated devices. You can also create profiles to play the sound of your interest.

To create a sound profile, follow the steps given below:

1. Copy the sound file you want to play in the *<OpManager Home>/conf/application/scripts* directory.
2. [Create a Run Program notification profile](#) with the following values to the fields:


**Command Name:** `./jre1.4.1/bin/java`

**Program arguments:** `-classpath ./classes/OpManagerServerClasses.jar  
com.adventnet.me.opmanager.server.alert.AudioNotifier  
./conf/application/scripts/<audio_file_name>`

You need to associate the profile with the device for triggering it during a fault. The sound can be heard in the OpManager server.

## Modifying a Notification Profile

You can modify an existing notification profile as per your requirement. For this, follow the steps given below:


1. Click the **Admin** tab.
2. Under **Global Settings**, click **Notification Profiles**.
3. Click  under **Edit** corresponding to the profile to be modified.
4. Make the required changes and click **Submit**.



**Warning:** When you modify an existing profile that is already assigned to some devices, the changes will have effect on all these devices.

## Deleting a Notification Profile

OpManager allows you to delete the notification profiles if they are not required any more. To delete a profile, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Global Settings**, click **Notification Profiles**.
3. Click  under **Delete** corresponding to the profile to be deleted.
4. Click **OK** to confirm deletion.



**Warning:** When you delete an existing profile that is already assigned to some devices, the link between this profile and the devices will be removed. The corresponding notification actions will not be performed for the devices any more.

## Associating Notification with Managed Devices

You need to associate the notification profiles with devices to trigger the corresponding action whenever these devices are under trouble.

To associate a profile with devices or a category of devices, you can use the Quick Configuration wizard. For doing so, follow the steps given below:

1. In the **Admin** tab, under **Tools**, click **Quick Configuration wizard**.
2. Select **Assign a Notification Profile** and click **Next**.
3. Choose the profile to be associated with devices and click **Next**.
4. Choose an option to associate the profile and click **Next**.
  - If you select a category, then the profile will be associated with all the devices in the category automatically.
  - If you choose Select devices manually, the next page will list all the managed devices. Move the devices from the list in the left to the one in the right and click **Finish**.
  - If you choose a business view, the profile will be associated with all the devices in the view. This option will be available only if you have created at least one business view.

To associate a notification profile with a single device, follow the steps given below:

1. [Open the snapshot page of the device](#).
2. Under **Configure**, select **Notifications**.
3. Select the profiles for this device and click **Submit**.



## Configure Maintenance

### Maintaining OpManager Database

To plot graphs and generate reports, OpManager collects data from the managed devices at regular intervals. By default, OpManager aggregates the performance data into hourly data at the end of each hour. The hourly data thus calculated will be aggregated into daily data at the end of each day. These aggregated data will be used in graphs and reports.

OpManager allows you to maintain the database with the required data. By default, the detailed data will be maintained for 7 days, the hourly data for 30 days and the daily data for 365 days. After the specified period, the database will be cleaned up automatically.

To configure your own settings for database maintenance, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Global Settings**, click **Database Maintenance**.
3. Specify the values for the fields in the **Performance Database** section.
4. Click **OK** to apply the changes.

To know about events and alarms database maintenance, refer to [Maintaining Events and Alarms](#).

## Scheduling Downtime

Maintenance of network devices forms an integral part of network administration. You may want to perform a maintenance of specific device types at specific intervals. If such devices are removed from the network, or rebooted, then you will see alarms indicating that the device, or the applications in the device are unavailable. Since the devices are not available when polled for status during the maintenance period, unnecessary alarms are fired. To prevent the devices from being monitored for status during maintenance, you can schedule a maintenance task for such devices. Following are the steps:


1. From the **Admin** tab, select **Downtime Scheduler** option under **Tools**.
2. Under **Actions** tab on the right, click **New Schedule**.
3. In the **New Downtime Schedule** form, provide the following details:
  - o Schedule Name
  - o Schedule Description
  - o Select the Status as **Enabled**, if you want the Scheduled task to take effect immediately. Else select **Disabled**, so that you can enable it when required.
  - o Select the frequency at which the Task has to be scheduled/executed. It can be **Once, Every Day, Every Week**.
  - o Specify the start and end time/day of the task in the corresponding fields.
  - o Specify the date from which the task must be scheduled.
  - o You can assign the task to only the required devices, or a device category like switches, routers, or to a Business view.
4. Click Save to save the Task configuration.

Once the Scheduler is configured, OpManager stops monitoring the selected devices during the configured time and the configured day, and automatically starts managing the devices after the configured time.

## Configuring Mail Server Settings

OpManager allows you to configure e-mail alerts and SMS alerts to get notified about the fault in your network. By default, OpManager sends the mail to the mail server specified in the e-mail notification profile. To configure the SMTP server settings globally and to provide the secondary mail server settings, follow the steps given below:

1. Under the **Admin** tab, click **Mail Server Settings**.
2. Enter the SMTP **Server name** and **Port** number.
3. Select **Requires Authentication** and enter the **User name** and **Password** details, if the server requires authentication to send e-mail.

	<p><b>Note:</b></p> <ul style="list-style-type: none"><li>▪ To test the settings enter the <b>Email ID</b> and click <b>Send a test message</b>. This e-mail ID will be considered as the default To Email ID while creating Email and SMS notification profiles.</li><li>▪ If you have a secondary mail server in your network, select <b>Add a secondary mail server</b> and provide the details. In case of failure of primary mail server, OpManager uses secondary mail server to send e-mail and SMS.</li></ul>
---	---

4. Click **OK** to update the changes.

## Configuring Proxy Server Settings

Any business enterprise will have a proxy server to optimize its connectivity to Internet and to filter access to restricted Web sites. In OpManager, to monitor URLs over internet, you need to provide the proxy server details of your enterprise.

To enter the details, follow the steps given below:

1. Under the **Admin** tab, click **Proxy Server Settings**.
2. Enter the Proxy server name, port number in which the Web service is running on the proxy server, and the user name and password to connect to the proxy server.
3. Click **Save** to save the details.

## Managing Users

### Creating a User Account

You can create users in OpManager and provide required privileges to them.



**Note:** You need to have [Full Control](#) over OpManager to create a new user. You can create and manage users only from the Web client.

To create a new user, follow the steps given below:


1. Click the **Admin** Tab.
2. Under **Global Settings**, click **Users**.
3. Click **Add Users** under **Actions**.
4. Type the **User Name**.
5. Type the password for authenticating this user in both the text fields.
6. Select a **User Permission**. *Full Control* will allow the user to do all administrative operations. *Read-only* allows the user to view the status, alarms, graphs, and reports of the managed devices.
7. Select the user's access level to the devices. *All Devices* allows the user to view and access all devices that are managed using OpManager. *Only the selected Business Views* will restrict the user access to the selected business views. However, the operations that can be performed on the devices are decided by the selected User Permission.
8. Click **Add User**.

The number of users that can be created depends on the license you have purchased for OpManager. For details, contact your system administrator.

## Changing the Password of a User


You have to be a user having **Full Control** over OpManager to change your password or other user's password.

To change the password of a user, follow the steps given below:

1. Click the **Admin** Tab.
2. Under **Global Settings**, click **Users**.
3. Click  corresponding to the user whose password you want to change.
4. Type the new password in both the Password fields and click **Submit**.

## Setting User Account Limitations

You can create customer-specific user accounts and restrict the views allowed to the customers. You must have administrative privileges to create or edit a user account settings. Log in as a user with Full Control privilege and follow the steps given below to set user account limitation.

1. Select **Users** under the **Admin** Tab.
2. Click  corresponding to the user to limit his privileges.
3. Assign the user with proper **User Permissions**. Refer to [OpManager User Permissions](#) for details.
4. Select an access level. **All Devices** will allow the user to view and access all devices that are managed using OpManager. **Only the selected Business Views** will restrict the user access to the selected business views.

If you have selected **Only the selected Business Views**, then select the business views that can be accessed by the user from the list.

5. Click **Submit**.




**Note:** Business views can be created and edited only from the Java client. To create a business view, refer to the [Creating a Business View](#) topic.

## **Deleting a User Account**

You can delete a user account when it is not needed any more.

To do so, follow the steps given below:

1. Click the **Admin** Tab.
2. Under **Global Settings**, click **Users**.
3. Click  corresponding to the user you want to delete.



## OpManager User Permissions

The OpManager user types and their respective privileges are listed below:

User Permission	Tasks That Can Be Performed
Full Control	<ol style="list-style-type: none"> <li>1. Discover networks and devices</li> <li>2. Manage and unmanage the devices</li> <li>3. Create custom views</li> <li>4. Create notification profiles</li> <li>5. Create monitors</li> <li>6. Modify OpManager settings for database maintenance, alarm escalation and user privileges</li> <li>7. Create device types</li> <li>8. Configure SNMP trap processors</li> <li>9. Configure monitoring intervals for devices</li> <li>10. Create event log rules</li> <li>11. Configure URL monitors</li> <li>12. Modify device settings</li> <li>13. Modify discovery settings</li> </ol> <p>and all operations that a user with Read-only access can perform.</p>
Read-only Access	<ol style="list-style-type: none"> <li>1. View the status, snapshot, graphs and reports of the managed devices</li> <li>2. View, annotate, acknowledge and clear alarms</li> <li>3. View installed software and active processes list of a managed device</li> <li>4. View and modify asset details</li> </ol>

In addition to this, the users can also be restricted to view only the selected devices. Refer to [Setting User Account Limitations](#) for details.

To know about the privileges assigned to you, contact your system administrator.

## Reports

### About Reports

In Web client, in addition to all the reports available in the Java client, you can see All Servers Availability Report, All Interfaces Availability Report and All Devices Availability Report.

#### **Servers**

CPU, memory, disk utilization, interface traffic and utilization, and all servers availability reports are available for servers.

To view the Volumes with Least/Most Free Space reports and All Servers Disk Usage report, you must assign the Free Disk Space and Used Disk Space graph profiles to the managed devices. Refer to [Associating a Monitor to a Device](#) for details.

#### **Routers**

CPU, memory utilization, interface traffic and utilization, and all interfaces availability reports are available for routers.

#### **Switches**

Port traffic, utilization and error reports are available for switches.

#### **Applications**

Response time reports are available for HTTP, SMTP, and MySQL applications.

#### **All Devices**

CPU and memory utilization, interface traffic and utilization reports are available for all devices.

#### **Inventory**

Inventory reports are available for servers, desktops, all devices, SNMP-enabled devices and non-SNMP devices.

## Custom Reports

You can view multiple graphs of a device under a single view and get a printer version of the same using custom reports.

To get a multi-graph report for a device, follow the steps given below:

1. Under the **Reports** tab, select **Custom Report**.
2. Type the **Device Name** or use the **Select Device** link to select a device from the list. Once the device is selected, all the monitors configured in the device will be listed.
3. Select the graphs you want to view and click **Show Report**.

You can export the reports to PDF format by clicking **Export to PDF**. To print the report, click **Printer Friendly View** and then click **Print** from the displayed window.

## Viewing Reports

1. Click the **Admin** Tab. The list of reports for different types of devices with a short description about the reports is displayed.
2. Click the report you want to view.



**Note:**

- By default, reports are displayed for the whole day. You can view the report for a specific period of the day by choosing the period from the **Time Window** list.
- To change the period of report to the day before, last 7 days, last 30 days and so on, use the drop-down list box under **Period**.
- To view the report for any other custom period, use the **Start Time** and **End Time** boxes in the **Custom Period** section.

## **Saving and Printing Reports**

Under the Reports tab, select the report you want to view.

- To save the report in PDF format, click **Export to PDF**.
- To print the report, click **Printer Friendly View** and then click **Print** from the displayed window.

## MIB Browser

### MIB Browser: Overview

The MIB Browser tool is a complete SNMP MIB Browser that enables loading and browsing MIBs and allows you to perform all SNMP-related operations. You can also view and operate on the data available through the SNMP agent running on a managed device.

The features of MIB Browser include the following:

1. Saving the MIB Browser settings.
2. Loading and viewing MIB modules in a MIB tree.
3. Traversing the MIB tree to view the definitions of each node for a particular object defined in the MIB.
4. Performing the basic SNMP operations, such as GET, GETNEXT, GETBULK, and SET.
5. Support for multi-varbind requests. This feature is available only in the Java client.
6. Real-time plotting of SNMP data in a graph. Line graph and bar graph are the two types of graphs that are currently supported. This feature is available only in the Java client.
7. Table-view of SNMP data. This feature is available only in the Java client.
8. Enables loading of MIBs at startup. This feature is available only in the Java client.

### MIB Browser Interface

**Menu bar:** Contains menus with related commands to perform all administrative operations.

**Toolbar:** Contains frequently used administrative commands for easy access.

**MIB Tree:** Shows all the loaded MIBs. You can traverse the tree and view the definition of each node in the tree.

**SNMP Settings:** Displays the SNMP settings of the selected node.

**Result Display Area:** Displays the result of the SNMP operations.

**Object Attributes:** Shows the attributes of the selected node.

## Invoking MIB Browser

MIB Browser can be used to view the values of SNMP variables of a device.

1. Click the **Admin** tab
2. Under **Tools**, click **Mib Browser**

## Loading MIBs

Using OpManager, you can load your own MIB file and query the SNMP values from the devices. For this, you need to put the MIB files in the *<OpManager Home>/mibs* directory.

To load a MIB file, follow the steps given below:

1. Invoke the MIB Browser.
2. Click **Load MIB**.
3. Select the MIB file to be opened from the list.

**Loading MIBs from a compiled file** compiles and loads the MIB file for the first time. While loading the file subsequently, the compiled files will be used for loading the MIB. This saves the time taken for compiling the MIB every time it is loaded.

**Loading MIBs from a database** is used when you have a large number of files to be loaded. In such cases, the MIBs to be loaded will be read from a RDBMS, such as MySQL or Oracle.

If none of these options are selected then the MIB file will be compiled every time it is loaded.

4. Click **Load**.



## Getting the Values of SNMP Variables for a Device

### To retrieve the value of an SNMP variable

1. Invoke the MIB Browser.
2. [Load the MIB file](#) that contains the SNMP variable.
3. Select the SNMP variable from the tree and click **Get**.

### To retrieve the values of consecutive SNMP variables

Select an SNMP variable from the tree and click **Get Next**. This retrieves the value of the variable next to the currently selected one.

If the SNMP version in your network is v2c or v3, you can retrieve the values of a set of consecutive variables next to the currently selected one.

To do so, follow the steps given below:

1. Invoke the MIB Browser.
2. Click **Parameters**.
3. Specify the number of consecutive variables to fetch their values in the **Max-Repetitions** box. By default, this is set as 50.
4. [Load the MIB file](#) that contains the SNMP variable.
5. Select the SNMP variable from the list and click **Get Bulk**.

## **Setting Values to SNMP Variables of a Device**

You can set values only to variables having read-write access.

To set the value for an SNMP variable of a device, follow the steps given below:

1. Invoke the MIB Browser.
2. Select the SNMP variable from the tree.
3. Type the value in the **Set Value** box.
4. Click **Set**.

## Setting SNMP Parameters in MIB Browser

To perform SNMP operations, you have to set the SNMP parameters as per your network requirements.

1. Invoke the MIB Browser.
2. Click **Parameters**.
3. Click the **General Settings** tab.
4. Enter the values for the SNMP parameters.

The descriptions of the SNMP parameters in this tab are given below:

**Snm Version:** Select the SNMP version supported in your network.

**Snm Port:** Refers to the port in which the SNMP agent is running on your device. By default, the value is set as 161.

**Timeout:** Specifies the time interval in seconds to wait for a response to an SNMP query. The default value is 5 seconds.

**Retries:** Refers to the number of times an SNMP request is re-sent if the preceding request times out. By default the value is 0.

5. Click **OK** to save the settings.

## **Standalone MIB Browser**

### **Invoking MIB Browser**

Standalone MIB Browser can also be used to view the values of SNMP variables of a device.

1. Go to <OpManager Home>/bin directory.
2. Execute MibBrowser.bat/sh file to invoke the standalone tool.

## Loading MIBs

MIB Browser allows you to load MIBs in the following three ways:

### Loading MIBs directly

This allows you to load the MIB files directly. Whenever the files are loaded using this option, they are compiled and then loaded.

### Loading MIBs from a compiled file


This is similar to loading MIBs directly for the first time the MIB is loaded. Once the MIB is compiled, two files are created. When the same file is loaded subsequently, these compiled files will be used for loading the MIB. This saves the time taken for compiling the MIB every time it is loaded.

### Loading MIBs from a database

This is useful when you have a large number of files to be loaded. In such cases, the MIBs to be loaded will be read from a RDBMS, such as MySQL or Oracle.

## Setting SNMP Parameters in MIB Browser

To perform SNMP operations, you have to set the SNMP parameters as per your network requirements.

1. Invoke the MIB Browser.
2. Click **Settings**  on the toolbar.
3. Click the **General Settings** tab.
4. Enter the values for the SNMP parameters.

The descriptions of the SNMP parameters in this tab are given below:

**Snmp Version:** Select the SNMP version supported in your network.

**Snmp Port:** Refers to the port in which the SNMP agent is running on your device. By default, the value is set as 161.


**Timeout:** Specifies the time interval in seconds to wait for a response to an SNMP query. The default value is 5 seconds.

**Retries:** Refers to the number of times an SNMP request is re-sent if the preceding request times out. By default the value is 0.

5. Click **OK** to save the settings.


## Getting the Values of SNMP Variables for a Device

### To retrieve the value of an SNMP variable


1. Invoke the MIB Browser.
2. [Load the MIB file](#) that contains the SNMP variable.
3. Select the SNMP variable from the tree and click **Get** .

### To retrieve the values of multiple SNMP variables

You have to select the Multi-Varbind display mode to retrieve the values of multiple SNMP variables.


1. Invoke the MIB Browser.
2. [Load the MIB file](#) that contains the SNMP variable.
3. Click **View**, point to **Display**, and click **Multi-Varbind**.
4. Select the SNMP variable from the tree and click **Add**. Perform this step until you have selected the required SNMP variables.
5. Select the **Multi-Var** check box.
6. Click **Get** . This retrieves the values of all SNMP variables in the list.

### To retrieve the values of consecutive SNMP variables

Select an SNMP variable from the tree and click **Get Next** . This retrieves the value of the variable next to the currently selected one.

If the SNMP version in your network is v2c or v3, you can retrieve the values of a set of consecutive variables next to the currently selected one.

To do so, follow the steps given below:

1. Invoke the MIB Browser.
2. Click **Settings** and then click **General**.
3. Specify the number of consecutive variables to fetch their values in the **Max-Repetitions** box. By default, this is set as 50.
4. [Load the MIB file](#) that contains the SNMP variable.
5. Select the SNMP variable from the list and click **Get Bulk** .

**Note:**



- If you have selected the **Multi-Var** check box, the Get Bulk operation fetches the values for  $x$  variables next to each of the variables in the Multi-Var list, where  $x$  is the number specified in the **Max-Repetitions** box.
- If you want to perform the Get Bulk operation only for selected variables in the list, click **Settings** and then click **General**. Type the number of variables to restrict the Get Bulk operation in the **Non-Repeaters** box. This restricts the Get Bulk operation to the number of variables specified from the top of the list.


For instance, if you have 3 variables in the Multi-Var list and specify 2 for Non-Repeaters, the Get Bulk operation will be performed only for the third variable. For the first two variables in the list, the value of the next variable will be retrieved respectively.



## Setting Values to SNMP Variables of a Device

You can set values only to variables having read-write access.

To set the value for an SNMP variable of a device, follow the steps given below:

1. Invoke the MIB Browser.
2. Select the SNMP variable from the tree.
3. Type the value in the **Set Value** box.
4. Click **Set**  .

## Viewing Real-time Graphs for SNMP data

1. Invoke the MIB Browser.
2. Select the SNMP variable from the tree. The variable must be of an integer or unsigned integer data type. In general, the graph will be plotted for variables of type Counter, Gauge, or Timeticks.
3. On the **View** menu, click **Line Graph** or **Bar Graph**.

### Descriptions of the fields in the Line Graph window:

**Polling Interval:** Specifies the polling interval in seconds. The default value is 5 seconds.

**Average over Interval:** Select this option to plot the average of all values of instances, when there are multiple instances for an SNMP variable.

**Show Absolute Time:** Shows the time in the format 'minutes:seconds' in the X-axis.

**Show Polled Values:** Select this option to view the graph plotted over the period of time as specified in the Max Poll Duration option. The X-axis Scale and Max Poll Duration options will be editable only if this option is selected.

**X-axis Scale:** Specifies the X-axis scale. The minimum and default value of this field is 300 seconds.

**Max Poll Duration:** Specifies the maximum poll duration. The graph will be plotted for the interval specified here.

**Log Polled Values:** Select this option to save the polled values in a text file.

**Log FileName:** Specifies the file name for saving the polled values. By default, the file name is "graph.txt".

**Show Absolute Counters:** By default, the graph plots only the difference between the two counter values. Select this option to plot the absolute value.

**Disable Error Dialog:** Select this option to prevent the error messages that are displayed when a status poll request times out.

### Description of the fields in the Bar Graph window:

**Polling Interval:** Specifies the polling interval in seconds. The default value is 5 seconds.

**Average over Interval:** Select this option to plot the average of all values of instances, when there are multiple instances for an SNMP variable.

**Range:** Specifies the X-axis scale. The minimum and default value of this field is 300 seconds.

**Show Absolute Time:** Shows the time in the format 'minutes:seconds' in the X-axis.

## Business Views

### Starting the Java Client

- **On Windows Machines**

Right-click the tray icon  and click **Start Client**.

If you have installed OpManager as [service](#), click **Start > Programs > ManageEngine OpManager > OpManager Client** to start the client.

- **On Linux**

Log in as '**root**' user. Execute the shell file **StartOpManagerClient.sh** present in the `<OpManager Home>/bin` directory.

In the displayed login window, type the **User Name** and **Password**. The default user name and password is 'admin' and 'admin' respectively.

## Creating a Business View



In addition to Networks views and Infrastructure views, OpManager allows you to create your own views to group the devices of your interest and manage them from one place. This will be required when you want to create a new category for devices other than those available under Infrastructure views, or if you want to manage the devices under each geographical location from one place. This is also helpful if you want to restrict the access to devices to users.

You can also draw links between the devices, rearrange the devices and set a background image. Further you can add shortcut icons to the view that opens another business view. This helps in getting a drill-down view when you group the devices based on geographical location.



**Note:** You can create and modify business views only from the Java client. However, you can view them from the Web client.

To create a business view, follow the steps given below:

1. Click **Add Business View** .
2. Enter the name for the view.
3. Select an icon that appears for this view in the tree and a background image for this business view.
4. Select the devices that are to be grouped under this view.
5. Click **OK**.
6. Drag and position the devices as per the need.
7. Click **Save Business View**  on the toolbar to save the business view settings.



**Note:**

- In business views, you can change the icon used for the devices, as required. Right-click the device and click **Change icon**. Choose the icon from the displayed dialog and click **OK**.
- You can draw links between the nodes to show the connectivity in the map. Refer to [Drawing a Link between Devices](#) for details.
- To add a shortcut icon that opens another business view, refer to [Adding Shortcut to a Business View](#).
- To provide access to the devices in this view alone to a user, refer to [Setting User Account Limitations](#).



## Modifying Business View Settings

You can modify the background, the tree icon, and the devices placed in the view.



**Note:** You can modify the business view settings only from the Java client. Make sure to save the changes after modifying the business views for changes to take effect in the Web client.


To modify the settings, follow the steps given below:

1. Select the business view to be modified and click **Modify Business View** .
2. Do the required changes and click **OK**.
3. Drag and position the devices as per the need.
4. Click **Save Business View**  on the toolbar to save the business view settings.

## Drawing a Link Between Devices

To represent the network diagram in the map, OpManager allows you to draw links between the devices in a business view. You can assign a meaningful name to the link and also configure to change the color of the link to indicate its status.

To draw a link, follow the steps given below:

1. Select the two devices to be linked either by holding the Ctrl key or dragging the mouse over the devices.
2. Click **Add link between devices** .
3. Type a meaningful **Display Name** for this link.
4. Using the (...) browse button beside the **Get status from** field, select an interface of one of the devices, whose status should be shown as the link status.
5. Choose the **Thickness** for the line drawn as the link.
6. Click **OK**.



**Note:** The links can be drawn only in the business views.

## Adding Shortcut to a Business View

You can add shortcut icons to business views that helps you to drill-down the network. This helps you to easily navigate to a view from another view when objects are grouped based on their geographical location.



**Warning:** You need to have created at least two business views to create a shortcut.

To add a shortcut icon, follow the steps given below:

1. Right-click the business view name in the tree and click **Add shortcut**.
2. Type a **Display Name** for the shortcut.
3. Choose an icon to represent the shortcut in the view.
4. Choose a background shape to the icon.
5. Choose the business view to be opened on double-clicking the icon.
6. Click **OK** to save the settings.



**Note:** The background shape chosen for the shortcut icon will be filled with the color of the highest severity status among all the devices in the linked business view.

## **Integrating with ManageEngine Products**

### **ServiceDesk Plus**

#### **Integrating with ServiceDesk Plus**

If you have [ServiceDesk Plus](#) installed in your network, you can automatically log trouble tickets from OpManager for specific network faults. So, besides the provision to email, sms, or notify fault in other forms, you can also track the faults by logging trouble tickets to ServiceDesk Plus. This helps in issue tracking.

For logging the trouble ticket to ServiceDesk Plus correctly, you need to ensure the following:

1. Incoming Mail Settings must be configured properly in ServiceDesk Plus
2. [ServiceDesk Plus Settings](#) must be configured in OpManager
3. [A notificaton profile](#) to log a trouble ticket to ServiceDesk Plus must be configured and associated.



## Configure Servers Settings

Following are the steps to configure the ServiceDesk Plus and OpManager Server settings:

1. Configure [Incoming Mail Settings](#) in ServiceDesk Plus
2. Configure [Mail Server Settings](#) in OpManager
3. OpManager must 'know' where ServiceDesk Plus resides to log the ticket. To configure the ServiceDesk Plus settings details, follow the steps given below
  - Click **Admin** tab, and select **Add-On/Products Settings** and configure the following values:

**Server where ServiceDesk Plus is running:** Name or the IP address of the machine where ServiceDesk Plus is installed and running.

**ServiceDesk Plus server port number :** The port number in which the ServiceDesk Plus application is running. Default port is 8080.

**ServiceDesk Plus login:** The user name with which you will log in into ServiceDesk Plus. Default is **admin**

**ServiceDesk Plus password :** The password to log in into ServiceDesk Plus. Default password for **admin** user is **admin**

**HelpDesk Email Address :** The email address in the mail server to which the email must be sent. This should be the same as configured in the mail-server settings in ServiceDesk Plus. Example: help@servicedeskplus.com

**From Email Address :** The initiator's email address. Example: requestor@company.com

After the settings are configured correctly, you can configure a [notification profile to log a trouble ticket](#).

## Logging a Trouble Ticket to ServiceDesk Plus

Following are the steps to configure a notification profile to log a trouble ticket to ServiceDesk Plus.

1. Ensure that the [servers settings](#) are configured properly.
2. Under Admin tab, click Notification Profiles.
3. On the right, click **Log a Ticket** under **Add New**
4. Configure the following notification profile details
  - Profile Name
  - Choose the appropriate device category from the **Category** combo-box
  - Choose the priority of the issue from the **Priority** combo-box
  - Choose a technician to whom the issue is to be assigned from the **Technician** combo-box
  - Select the alarm variables such as the alarm severity, device display name etc, from the corresponding combo-box under **Ticket Contents**. These details are displayed on the issue title
  - Select the required alarm variables to be included for the alarm description. This will provide accurate fault information to the assigned technician
  - Select the criteria for the trouble ticket to be logged into [ServiceDesk Plus](#).
4. Click **Submit**.

After the profile is created, you can [associate it to the required devices](#).

## NetFlow Analyzer

### Integrating with NetFlow Analyzer

OpManager can seamlessly integrate with the network traffic monitoring tool, Netflow Analyzer, one of the AdventNet ManageEngine suite of products. Netflow Analyzer provides detailed interface traffic reports.

To view the detailed traffic report from Netflow Analyzer, the prerequisites are,


1. Netflow Analyzer must be up and running in your network
2. The interface whose traffic you would like to monitor must be discovered in both, OpManager and Netflow Analyzer.
3. The [NetFlow Analyzer settings](#) must be configured properly in OpManager.

## Configure NetFlow Analyzer Settings

To configure the NetFlow Analyzer Settings in OpManager

1. Click **Admin** tab
2. From Global Settings column, click **Add-On/Products Settings**
3. Click **NetFlow Settings** icon in this screen
4. Type the following NetFlow Analyzer server details:
  - Server Name
  - Port (default is 8080)
  - User Name
  - Password
  - Polling Interval in mins
5. Save the settings.

After configuring the settings, you can follow the steps given below to see the detailed reports:

1. Go to the Routers map
2. Click the required interface icon in the Routers map to see its snapshot page
3. In the Interface Traffic details column, do a mouse-over the  **NetFlow** icon. Select
  - Top Applications
  - Top Sources
  - Top Destinations
  - Top Conversations



**Note:**

You will be prompted to log on with the NetFlow Analyzer's administrator user name and password the first time you view the report.

## SNMP Installation Guide

### Installing SNMP Agent on Windows Systems

(Adapted from Windows help)

- [Installing SNMP Agent on Windows XP/2000/2003](#)
- [Installing SNMP Agent on Windows NT](#)
- [Installing SNMP Agent on Windows 98](#)

You need to know the following information before you install the Simple Network Management Protocol (SNMP) service on your computer:

- Community names in your network.
- Trap destinations for each community.
- IP addresses and computer names for SNMP management hosts.

**To install SNMP on Windows XP, 2000, and 2003, follow the steps given below:**

You must be logged on as an administrator or a member of the Administrators group to complete this procedure. If your computer is connected to a network, network policy settings may also prevent you from completing this procedure.

1. Click **Start**, point to **Settings**, click **Control Panel**, double-click **Add or Remove Programs**, and then click **Add/Remove Windows Components**.
2. In Components, click **Management and Monitoring Tools** (but do not select or clear its check box), and then click **Details**.
3. Select the **Simple Network Management Protocol** check box, and click **OK**.
4. Click **Next**.
5. Insert the respective CD or specify the complete path of the location at which the files stored.
6. SNMP starts automatically after installation.

This completes the installation process. This also implements the Host Resources MIB automatically. To configure SNMP agents respond to SNMP requests, refer to [Configuring SNMP agents](#).

**To install SNMP in Windows NT, follow the steps given below:**

1. Right-click the **Network Neighborhood** icon on the Desktop.
2. Click **Properties**.
3. Click **Services**.
4. Click **Add**. The Select Network Service dialog box appears.
5. In the Network Service list, click **SNMP Service**, and then click **OK**.
6. Insert the respective CD or specify the complete path of the location at which the files stored and click **Continue**.
7. After the necessary files are copied to your computer, the Microsoft SNMP Properties dialog box appears.

This completes the installation process. This also implements the Host Resources MIB automatically. To configure SNMP agents respond to SNMP requests, refer to [Configuring SNMP agents](#).

### **To install SNMP in Windows 98**

Make sure your Windows 98 CD is in the drive. Then follow the steps given below:

1. On the **Network** control panel, click **Add**.
2. Double-click **Service** in the Select Network Component Type dialog box.
3. Click **Have Disk** in the Select Network Service dialog box.
4. Type the path to the "TOOLS\RESKIT\NETADMIN\SNMP" directory on your computer's CD drive in the Install From Disk dialog box and then click **OK**.
5. Select **Microsoft SNMP agent** from the **Models** list in the Select Network Service dialog box and then click **OK**.

This completes the installation process. This also implements the Host Resources MIB automatically. To configure SNMP agents respond to SNMP requests, refer to [Configuring SNMP agents](#).

## Installing SNMP Agent on Linux systems

The installation of new version of SNMP is required only for versions prior to 8.

Download the latest rpm version of SNMP using the following URL:

<http://prdownloads.sourceforge.net/net-snmp/net-snmp-5.1.1-1.rh9.i686.rpm?download>

Download the zip version of SNMP using the following URL:

<http://heanet.dl.sourceforge.net/sourceforge/net-snmp/ucd-snmp-4.2.6.tar.gz>

To **install using the rpm**, follow the steps given below:

1. Login as "root" user.
2. Before installing the new version of net-snmp, you need to remove the earlier versions of net-snmp in your machine. To list the versions of net-snmp installed in your machine, execute the following command:

```
rpm -qa | grep "net-snmp"
```

3. If there are already installed version in your machine, remove them using the command:

```
rpm -e <version of net-snmp listed as the output for previous command> --nodeps
```

4. If there are no previously installed versions in your machine, then execute the following command to install the new version:

```
rpm -i <new downloaded version of SNMP agent> --nodeps
```

To **install using the zip**, follow the steps given below:

Extract the file using following command:

```
tar -zxvf ucd-snmp-4.2.6.tar.gz
```

To install SNMP, follow the steps given below:

1. Login as *root* user.
2. Execute the command to set the path of the C compiler:  
*export PATH=<gcc path>:\$PATH*
3. Execute the following four commands from the directory where you have extracted the ucd-snmp:
  1. *./configure --prefix=<directory\_name> --with-mib-modules="host"*

**directory\_name** is the directory to install SNMP agent. Preferably choose a directory under /root. The directories /usr and /local might contain the files of an older version of SNMP and so do not choose these directories to ensure proper installation.

2. *make*
3. *umask 022*
4. *make install*

This completes the installation process. For configuring SNMP agents to respond to SNMP requests, refer to [Configuring SNMP agents](#).

## Installing SNMP Agent on Solaris Systems

Download the latest version of SNMP using the following URL:

<http://heanet.dl.sourceforge.net/sourceforge/net-snmp/ucd-snmp-4.2.6.tar.gz>

Extract the file using following command:

```
tar -zxvf ucd-snmp-4.2.6.tar.gz
```

To install SNMP, follow the steps given below:

1. Login as *root* user.
2. Execute the command to set the path of the C compiler:  
`export PATH=<gcc path>:$PATH`
3. Execute the following four commands from the directory where you have extracted the ucd-snmp:
  1. `./configure --prefix=<directory_name> --with-mib-modules="host"`

**directory\_name** is the directory to install SNMP agent. Preferably choose a directory under /root. The directories /usr and /local might contain the files of an older version of SNMP and so do not choose these directories to ensure proper installation.

2. `make`
3. `umask 022`
4. `make install`

This completes the installation process. To configure SNMP agents respond to SNMP requests, refer to [Configuring SNMP agents](#).



## Configuring SNMP Agents

- [Configuring SNMP agent in Windows XP/2000,2003](#)
- [Configuring SNMP agent in Windows NT](#)
- [Configuring SNMP agent in Linux versions prior to 8](#)
- [Configuring the Agent in Linux versions 8 and above](#)
- [Configuring SNMP agent in Solaris](#)

### Configuring SNMP Agent in Windows XP, 2000, and 2003 Systems

For details about installing SNMP agents in Windows systems, refer to [Installing SNMP Agent on Windows Systems](#).

To configure SNMP agent in Windows XP and 2000 systems, follow the steps given below:

1. Click **Start**, point to **Settings**, click **Control Panel**.
2. Under Administrative Tools, click **Services**.
3. In the details pane, right-click **SNMP Service** and select **Properties**.
4. In the **Security** tab, select **Send authentication trap** if you want a trap message to be sent whenever authentication fails.
5. Under Accepted community names, click **Add**.
6. Under **Community Rights**, select a permission level for this host to process SNMP requests from the selected community.
7. In **Community Name**, type a case-sensitive community name, and then click **Add**.
8. Specify whether or not to accept SNMP packets from a host:
  - To accept SNMP requests from any host on the network, regardless of identity, click **Accept SNMP packets from any host**.
  - To limit acceptance of SNMP packets, click **Accept SNMP packets from these hosts**, click **Add**, type the appropriate host name, IP or IPX address, and then click **Add** again.
10. Click **Apply** to apply the changes.

To configure SNMP traps, follow the steps given below:

1. Click **Start**, point to **Settings**, click **Control Panel**.
2. Under Administrative Tools, click **Services**.
3. In the details pane, right-click **SNMP Service** and select **Properties**.
4. In the **Traps** tab, under **Community name**, type the case-sensitive community name to which this computer will send trap messages, and then click **Add** to list.
5. Under **Trap destinations**, click **Add**.
6. In the **Host name, IP or IPX address** field, type host name or its IP address of the server (OpManager server) to send the trap, and click **Add**.
7. Repeat steps 5 through 7 until you have added all the communities and trap destinations you want.
8. Click **OK** to apply the changes.

## Configuring SNMP Agent in Windows NT Systems

For details about installing SNMP agents in Windows systems, refer to [Installing SNMP Agent on Windows Systems](#).

To configure SNMP agent in Windows NT systems, follow the steps given below:

1. Click **Start**, point to **Settings**, click **Control Panel**.
2. Under Administrative Tools, click **Services**.
3. In the details pane, right-click **SNMP Service** and select **Properties**.
4. In the **Security** tab, select **Send authentication trap** if you want a trap message to be sent whenever authentication fails.
5. Under **Accepted Community Names**, click **Add**.
6. In the **Community Names** box, type the community name to authenticate the SNMP requests.
7. To move the name to the **Accepted Community Names** list, click **Add**.
8. Repeat steps 6 and 7 for any additional community name.
9. To specify whether to accept SNMP packets from any host or from only specified hosts, click one of two options:
  - **Accept SNMP Packets From Any Host**, if no SNMP packets are to be rejected on the basis of source computer ID.
  - **Only Accept SNMP Packets From These Hosts**, if SNMP packets are to be accepted only from the computers listed. To designate specific hosts, click Add, type the names or addresses of the hosts from which you will accept requests in the IP Host or IPX Address box, and then click Add.
10. Repeat step 11 for any additional hosts.
11. In the **Agent** tab, specify the appropriate information (such as comments about the user, location, and services).
12. Click **OK** to apply the changes.

Further, the SNMP Agent running Windows NT does not respond to Host Resource Data, by default. To include this support, you should have Windows NT Service Pack 6 & above. Verify this and then follow the steps given below:

1. Extract the NTHR-MIB.zip available at <http://bonitas.adventnet.com/opmanager/09Sep2004/NTHR-MIB.zip> into C:\WinNT\system32 folder.
2. Double click on the registry files to import the mibs into Windows registry.
3. Restart your Windows NT box.

To Configure SNMP Traps, follow the steps given below:

1. Click **Start**, point to **Settings**, and then click **Control Panel**. Double-click **Administrative Tools**, and then double-click **Services**.
2. In the details pane, click **SNMP Service**, and then click **Properties**.
3. Click the **Traps** tab.
4. To identify each community to which you want this computer to send traps, type the name in the **Community Name** box. Community names are case sensitive.
5. After typing each name, click **Add** to add the name to the list.

6. To specify hosts for each community you send traps to, after you have added the community and while it is still highlighted, click **Add** under Trap Destination.
7. To move the name or address to the Trap Destination list for the selected community, type the host name in the **IP Host/Address or IPX Address** box, and then click **Add**.
8. Repeat step 10 for any additional hosts.
9. Click **OK** to apply the changes.

### Configuring the Agent in Linux versions prior to 8

For details about installing SNMP agents in Linux systems, refer to [Installing SNMP Agent on Linux Systems](#).

1. Stop the agent if it is running already using the command:  
*/etc/rc.d/init.d/snmpd stop*
2. Make the following changes in */etc/rc.d/init.d/snmpd* file
  - Replace the line  
*daemon /usr/sbin/snmpd \$OPTIONS*  
with  
*daemon /root/ucd\_agent/sbin/snmpd \$OPTIONS*
  - Replace the line  
*killproc /usr/sbin/snmpd*  
with  
*killproc /root/ucd\_agent/sbin/snmpd*

This is to choose the current installed version while starting and stopping the SNMP agent.
3. Start the agent using the command */etc/rc.d/init.d/snmpd start*.

### Configuring the Agent in Linux versions 8 and above

On Linux versions 8 and above, the latest version of SNMP will already be available. You need to just make the following changes in **snmpd.conf** file:

1. Insert the line  
*view allview included .1.3.6*  
next to the line  
*# name incl/excl subtree mask(optional)*
2. Change the line  
*access notConfigGroup "" any noauth exact systemview none none*  
next to the line  
*# group context sec.model sec.level prefix read write notif*  
as  
*access notConfigGroup "" any noauth exact allview none none*
3. Then restart the snmp agent using the following command:  
*/etc/rc.d/init.d/snmpd restart*

## Configuring the Agent in Solaris Systems

For details about installing SNMP agents in Solaris systems, refer to [Installing SNMP Agent on Solaris Systems](#).

1. Stop the agent if it is running already using the following command:

```
/etc/init.d/init.snmpdx stop
```

2. Make the following changes in **/etc/init.d/init.snmpdx** file

- Replace the lines

```
if [ -f /etc/snmp/conf/snmpdx.rsrc -a -x /usr/lib/snmp/snmpdx ]; then  
/usr/lib/snmp/snmpdx -y -c /etc/snmp/conf -d 3 -f 0  
fi
```

with

```
<Installation Directory>/sbin/snmpd
```

- Replace the line

```
/usr/bin/pkill -9 -x -u 0 '(snmpdx|snmpv2d|mibiisa)'
```

with

```
/usr/bin/pkill -9 -x -u 0 '(snmpd)'
```

3. Restart the agent using the following command:

```
/etc/init.d/init.snmpdx start.
```

## Configuring SNMP Agents in Cisco Devices

For configuring SNMP agents in Cisco devices, you need to log into the device and switch to privileged mode.

Use the following set of commands listed below to enable SNMP:

### To enable SNMP:

From the command prompt, run the following commands:

```
#configure terminal
#snmp-server community <community_string> rw/ro (example: snmp-server
community public ro)
#end
#copy running-config startup-config
```

### To enable trap:

Again, from the command prompt, run the following commands:

```
#configure terminal
#snmp-server enable traps snmp authentication
#end
#copy running-config startup-config
```

### To set OpManager as host:

Run the following commands from the command prompt:

```
#configure terminal
#snmp-server host <OpManager server running system's IP> <Trap community string>
snmp (example: snmp-server host 192.168.9.58 public snmp)
#end
#copy running-config startup-config
```

## Configuring SNMP Agent for Lotus Domino Server

The Domino SNMP Agent is configured as a Windows Service and is set up to run automatically. This means that once the Domino SNMP Agent is configured, it is virtually always running, even when Domino is not. If you later upgrade Domino you should stop the LNSNMP and Windows SNMP Services before beginning the upgrade process.

- Stop the LNSNMP and SNMP services. Enter these commands:

```
net stop Insnmp  
net stop snmp
```

- Configure the Lotus Domino SNMP Agent as a service. Enter this command:

```
Insnmp -Sc
```

- Start the SNMP and LNSNMP services. Enter these commands:

```
net start snmp  
net start Insnmp
```

## Configuring SNMP Agent in MSSQL Server

Verify whether SNMP agent is running in the server. If the agent is not installed in the server, refer to Installing SNMP Agent on Windows System and Configuring SNMP agents for installing and configuring SNMP agent.

Then, start the SQLSERVERAGENT service following the steps given below:

### In Windows 2000/XP:

1. Click **Start**, point to **Settings**, and then click **Control Panel**. Double-click **Administrative Tools**, and then double-click **Computer Management**.
2. In the console tree, click **Services and Applications** and then click **Services**.
3. Right-click **SQLSERVERAGENT** and click **Start**.

### In Windows NT:

1. Right-click on the **Network Neighborhood** icon on the Desktop.
2. Click **Properties**.
3. Click **Services**.
4. Right-click **SQLSERVERAGENT** and click **Start**.

## Configuring SNMP Agent in Oracle Server

To collect data from the Oracle servers and to receive traps from them using OpManager, you need to install and configure Oracle Intelligent Agent. The Oracle Intelligent Agent supports SNMP, allowing third-party systems management frameworks to use SNMP to receive SNMP traps directly from the Agent. By configuring the Agent to recognize SNMP requests from the master agent, third-party systems can gather relevant data.

In Windows machines

1. Once you have installed and configured the SNMP agents in your Windows machines, you have to integrate SNMP with Intelligent agent. This requires Oracle Peer SNMP Master Agent and SNMP Encapsulator Agent to be installed in the Oracle server. Note that these agents must be the same version as the Intelligent Agent and installed in the same ORACLE\_HOME.

After the installation completes, the following new NT services will be created: Oracle SNMP Peer Encapsulator Oracle Peer SNMP Master Agent

If you do not install the Intelligent Agent software in the default \$ORACLE\_HOME, the names of all the services will begin with the following: Oracle<home name>

For SNMP master agent to communicate with both the standard SNMP service and the Intelligent Agent, the SNMP services file must be configured properly.

Specify an unused port where the encapsulated agent, Microsoft SNMP Service, should be listening. Microsoft SNMP Service typically uses port 1161. The port is specified in the SERVICES file located in the NT\_HOME\SYSTEM32\DRIVERS\ETC directory.

Make sure that you have the following lines in the file:

```
snmp 1161/udp snmp  
snmp-trap 1162/udp snmp
```

Note: If an entry for SNMP already exists in the file, change the port from 161 (default number) to another available port (1161 in this example).

2. In the same location, check that the HOSTS and LMHOSTS.SAM files contain the mappings of IP addresses to host names for all computers in the SNMP setup. System performance will improve if more computer addresses can be resolved locally. Even if you use DHCP and WINS, adding the IP addresses will speed up the SNMP integration.



## Troubleshooting Tips

### Server Startup: Troubleshooting Tips

- Enter a proper AdventNet license file
- Failed to establish connection with Web server. Gracefully shutting down OpManager
- Port 80 needed by OpManager is used by some other application
- Port 8009 needed by OpManager is used by some other application
- Unable to start MySQL daemon
- MySQL related error messages in Windows machines
- Error while starting OpManager service
- Other server startup problems

#### Enter a proper AdventNet license file

If your system date is set to a future or a past date, you will get this error message. Uninstall OpManager, set the system date settings to current date and time, and re-install OpManager.

#### Failed to establish connection with Web server. Gracefully shutting down OpManager.

In Linux 8 and 9 versions, you will get this error because the file **libdb-3.2.so** may not exist in your system. This file is made optional while installing Linux Red Hat 8 & 9 versions. This file is required to start the Apache server. The file has been bundled with the product and is present in the *<OpManager Home>/lib/backup* directory. Copy it to the *<OpManager Home>/lib* directory and restart OpManager.

#### Port 80 needed by OpManager is used by some other application

1. If you have installed OpManager as Windows service, the server will be started automatically after installation. When you try to start the server again using the shortcuts, you will get this message. So you can directly start the client using Start > Program Files > ManageEngine OpManager 5 menu.
2. If you have not chosen to install OpManager as Windows service, refer to Question 1 under FAQs to change the port. Then restart OpManager.

#### Port 8009 needed by OpManager is used by some other application

You get this message since the port 8009 needed by OpManager to run Tomcat server is already occupied. You can either shut down the application running in this port or configure OpManager to use a different port to run Tomcat server.

To stop the Tomcat server, do the following:

1. Set the JAVA\_HOME variable in the **setclasspath.sh** file located at *<OpManager Home>/apache/tomcat/bin* directory as `JAVA_HOME=/usr/java/<jdkversion>`.
2. Execute the script **shutdown.sh** from *<OpManager Home>/apache/tomcat/bin* directory.
3. Then restart OpManager.

To configure OpManager to use a different port to run Tomcat server, you need to do the following:

1. If you have installed OpManager in Windows machine, find and replace all instances of "8009" with a free port number in the *<OpManager Home>/conf/opmanager\_processinfo.xml* file.  
If you are using Linux machine, then replace the port number in the *<OpManager Home>/setEnv.sh* file.
2. Then restart OpManager.

### **Unable to start MySQL daemon (or) any other MySQL related error messages in Windows machines**

You will run into MySQL related errors in Windows machines if MySQL is already installed or another instance of MySQL is running on the same machine.  
The best solution is to uninstall MySQL and install OpManager or install OpManager in a different machine.

Note: Deleting or renaming the My.ini file present in C:\Winnt (C:\Windows in Windows XP) also solves this problem.

### **Error while starting OpManager service**

When you get an error while starting OpManager service, try starting the OpManager server using the shortcut available at Desktop or using the menu, **Start > Programs > ManageEngine OpManager 5 > OpManager 5**.

### **Other Server startup problems**

- You will find problems while starting the server in Windows machines, if environment variables are assigned non-ascii values. Remove the variables containing non-ascii values and restart the server.
- If you choose to install OpManager under a directory named in Japanese and Chinese language, you will find problem while starting the apache service. Choose a directory in English to install OpManager.

## Client Errors: Troubleshooting Tips

- Error connecting to server
- Connection lost to Server
- The page cannot be displayed
- Please check whether the server is running

### Error connecting to server

- In Linux machines if you have installed OpManager in a directory other than *opt* (recommended during installation), then this error message will be displayed while starting the client. This is because the Apache server will not have 'read' and 'execute' permissions to access the files under OpManager directory. To give the required permissions, perform the following:

Execute the command **chmod -R 755 <OpManager Home>** and then restart the server. The absolute path should be given for OpManager Home directory.

Then execute the command **chmod 755 <directory name>**, for each of the directory in the absolute path including root.

- While trying to open the client with a incorrect Server name, User Name or Password, you will get this error message. So check whether these entries are correct and restart the client.
- When you try to open the client before the server has been started, you will get this error. So wait until the server startup is completed and then open the client. You can ensure the successful server startup in Windows machines by green tray icon and in Linux and Solaris machines by the message "OpManager modules started successfully" displayed in the console.

### Connection lost to Server

If the server is accidentally shut down when the client is running, this message will be displayed. Exit the client, then restart the server and the client.

### The page cannot be displayed (or) Please check whether the server is running

You will get this error message when you try to connect to the server when the server is not running. Verify whether the server is running and try connecting to it.

This might happen when you start the OpManager service with an expired license file. In this case, though the service appears to have got started, the server will not be up. You can verify this and apply the license file by starting the server using the **Start >**

**Program Files > ManageEngine OpManager 5 > OpManager 5** option. You will be prompted to enter the proper license file.

## Discovery: Troubleshooting Tips

- Not able to discover network. While adding a Network IP for discovery, it does nothing
- No Devices are discovered during initial discovery
- SNMP nodes are shown as non-SNMP nodes
- Strange networks appear on my map
- Some of my Routers are discovered as Desktops or Servers
- Some of my Printers are discovered as Desktops or Servers
- Some of my Switches are discovered as Desktops or Servers
- My critical Servers are listed as Desktops
- Devices are identified by IP addresses rather than host names

**Not able to discover network. While adding a Network IP for discovery, it does nothing.**

This happens because, while discovering routers, if interfaces with IPs from undiscovered networks are detected, those networks are added with unmanaged status and the devices under it will not be discovered automatically. You can view such networks in the administrative client. In the Networks map, verify whether you find the network that you want to discovered with an Unmanaged status in this view. If so, right-click on the network icon and select Delete Network. Then discover the network again.

### No Devices are discovered during initial discovery

This happens if ICMP request times out. To solve this, increase the **ICMP\_TIMEOUT** value in the **NATIVE\_PING** tag in **seed.file** located under the `<OpManager Home>/conf` directory. Then restart the OpManager server.

### SNMP nodes are shown as non-SNMP nodes

- If SNMP agent is not running on a device during discovery, then the device will be discovered as non-SNMP node. Refer to [Configuring SNMP Agents](#) for details. You can verify this by the blue star that appears at the top left corner of the device icon for the SNMP-enabled devices. To discover it as an SNMP node, follow the steps given below:
  - Click **Passwords** in the snapshot page of the device.
  - Enter the correct SNMP parameters as configured in the agent.
  - Click **Rediscover Now** under **Actions**.
- If the SNMP agent is running on the router, still you do not see the blue star in the device icon, then check whether SNMP parameters are properly specified during discovery. If not, [re-discover the device with correct SNMP parameters](#).

### Strange networks appear on map

Strange networks will appear on the map when subnet mask is not specified properly. Delete all the strange networks and perform discovery with correct subnet mask.

### Some of my Routers are discovered as Desktops or Servers

- If you could see the blue star in the device icon and the device has not been classified properly, then use the options under **Move To** to move the it to the proper category.
- If SNMP agent is not running on the router, then the category to which it belongs cannot be properly identified and hence will be placed in a different map. You can verify this by the blue star that appears at the top left corner of the device icon for the SNMP-enabled devices. To categorize the device properly, start the SNMP agent in the device. Refer to [Configuring SNMP agents in Cisco Devices](#) for details. Then [re-discover the device with correct SNMP parameters](#).
- If the SNMP agent is running on the router, still you do not see the blue star in the device icon, then check whether SNMP parameters are properly specified during discovery. If not, [re-discover the device with correct SNMP parameters](#).
- If the IP Forwarding parameter of the device is set to false, then router will be discovered as a server or desktop. To set the value of this parameter to true, right-click the device, point at **Tools** and click **MIB Browser**. Expand **RFC1213-MIB**. In the **ip** folder, click **ipForwarding**. Type **1** in the **Set Value** box and click **Set SNMP variable** on the toolbar. Then, [re-discover the device with correct SNMP parameters](#).

### Some of my Printers are discovered as Desktops or Servers

- If SNMP agent is not running on the printer, then the category to which it belongs cannot be properly identified and hence will be placed in a different map. You can verify this by the blue star that appears at the top left corner of the device icon for the SNMP-enabled devices. To categorize the device properly, start the SNMP agent in the device. Then [re-discover the device with correct SNMP parameters](#).
- If the SNMP agent is running on the router, still you do not see the blue star in the device icon, then check whether SNMP parameters are properly specified during discovery. If not, [re-discover the device with correct SNMP parameters](#).

### Some of my Switches are discovered as Desktops or Servers

- If you could see the blue star in the device icon and the device has not been classified properly, then use the options under **Move To** to move the it to the proper category.
- If SNMP agent is not running on the switch, then the category to which it belongs cannot be properly identified and hence will be placed in a different map. You can verify this by the blue star that appears at the top left corner of the device icon for the SNMP-enabled devices. To categorize the device properly, start the SNMP agent in the device. Refer to [Configuring SNMP agents in Cisco Devices](#) for details. Then [re-discover the device with correct SNMP parameters](#).
- If the SNMP agent is running on the router, still you do not see the blue star in the device icon, then check whether SNMP parameters are properly specified during discovery. If not, [re-discover the device with correct SNMP parameters](#).

### My critical Servers are listed as Desktops

If there are no services running on the server during discovery, then it will be categorized as a desktop. Use Servers under Move To for moving the device . For more details, refer to [Identifying Servers in your Network](#).

**Devices are identified by IP addresses rather than host names**

If DNS Server address is not set properly in the machine hosting OpManager, the DNS names of the managed devices cannot be obtained from the DNS server.

The other possible reasons could be:

1. the DNS Server is not reachable
2. the DNS Server is down during discovery
3. the DNS Server does not exist

## Monitors: Troubleshooting Tips

- Snapshot view does not show Interface details
- Snapshot view displays "No Data" for CPU, Memory or Disk utilization
- Junk characters in Snapshot
- Graphs show "No Data Available"

### Snapshot view does not show Interface details

The reason for this could be one of the following:

- The SNMP agent is not running on a device. Start the agent and [re-discover the device with correct SNMP parameters](#).
- If the SNMP agent is running on the device but the interface details are not shown, then check whether SNMP parameters are properly specified during discovery. If not, [re-discover the device with correct SNMP parameters](#).

### Snapshot view displays "No Data" for CPU, Memory or Disk utilization

If Snapshot view shows interface details but the CPU, memory and disk utilization are not shown, then the reason could be the absence of HOST-RESOURCES-MIB in the device. Refer to **SNMP Installation Guide** for details on installing and configuring SNMP agents on managed devices. Then, [re-discover the device with correct SNMP parameters](#).

### Graphs show "No Data Available"

If none of the graphs for a device are displayed, it could be due to one of the following reasons:

- Verify the graph profile has been assigned to the device. If not, assign it to the device. Refer to Assigning a Graph Profile to a Device for details.
- In general, data should be collected to produce graphs. So try the graph after a period of 2 polling intervals.
- Even after 2 polling intervals, if graphs are not shown, it may be due to one of the following reasons:
  1. If the SNMP agent is running on the device and still the graphs are not shown, then verify the following:
    - Check whether SNMP parameters are properly specified during discovery. If not, [re-discover the device with correct SNMP parameters](#).
    - Verify whether HOST-RESOURCES-MIB is enabled in the device. Refer to [Configuring SNMP Agents](#) for configuring the SNMP agent. Then [re-discover the device with correct SNMP parameters](#).
    - Verify whether the agent returns a value for the SNMP OID. Refer to [Getting the values of SNMP Variables](#) for details.
  2. If the SNMP agent is not running on a device, then to view the CPU, memory and disk utilization details, you need to provide the WMI/Telnet/SSH authentication details and configure the respective graph profiles to the device. Refer to Assigning a Graph Profile to a Non-SNMP device for details.



To view all other graphs supported out-of-the-box by OpManager or the custom graphs that you have configured, you need to have SNMP agent running in the managed devices. Refer to the **SNMP Installation Guide** for details about installing and configuring SNMP agent in the managed devices.

Following are the possible reasons for the dial graphs not being displayed:

#### 1. SNMP-based Monitors for Windows/Linux devices

If you have configured SNMP based Resource Monitors, and the graphs are not displayed, ensure the following:

- i. Check if SNMP is enabled in the device. A blue star on the device icon in the map indicates that SNMP is enabled in the device. Configure the right SNMP read/write community.
- ii. If the graph is still not displayed, increase the SNMP timeout interval.
- iii. Try querying the relevant OIDs in the HOST-RESOURCE MIB using the Mib Browser tool.

#### iv. Check if user permission is set for the group.

SNMP based Resource Monitors for Switches

SNMP based Resource Monitors for Routers

SNMP based Resource Monitors for Firewall

SNMP based Resource Monitors for UPS

Telnet/SSH-based Resource Monitors for Linux/Solaris

- i. Check if the username, password, and protocol is selected properly. If not, configure the same.

- ii. Check if the selected protocol is actually enabled in the remote device. If not enable the respective process.

- iii. From the command prompt, try establishing a telnet/ssh session to the remote device, with the same username and password. If you are able to successfully login, there should not be any problem connecting to the device from OpManager using these protocols.

WMI based Resource Monitors in Windows

- i. Check if WMI is enabled in the remote Windows device. WMI is available by default in Windows 2000 and above versions. If the remote device is Windows NT, you need to install WMI separately.

- ii. If WMI is enabled, check if RPC is enabled or not. If it is not, enable this service.

- iii. If the managed device is in the domain, configure the domain administrator username and password to connect to the device using WMI as in 'testdomainuser\test'. If the machine is not in a domain, configure the administrator username and password

- iv. If the managed device is Windows XP + SP2 + auto-upgrade patch, revert the auto-upgrade and try.

- v. Open the required ports in the firewall to enable contact to the device.

### Junk characters in Snapshot

In Chinese or Japanese version of OpManager, if the SNMP agents sends data as Unicode characters, OpManager might not be able to translate it properly and hence display the values as junk.

To display this properly, you need to specify the encode type of your agent in the Device Settings dialog. Double-click the device and click **Monitoring** under **Categories**. Enter the encode type in the **Encoding** Box and click **OK**.



## Reports: Troubleshooting Tips

- [Top N Reports shows No Data Available](#)
- [All Servers Disk Usage Report shows No Data Available](#)
- [Top N Volumes having Low/More Disk Space report shows No Data Available](#)
- [Junk Characters in Interface Reports](#)
- [NA in All Servers Disk Usage Report](#)
- [Applications Reports show No Data Available](#)

### Top N Reports shows No Data Available

To view the CPU utilization, Memory Utilization, Disk Utilization, Interface Traffic, Interface Utilization and Interface Errors reports, you need to have SNMP installed in the managed devices. Reports list only the SNMP-enabled devices.

OpManager requires a minimum of 1 hour to collect data and so please try reports after 1 hour from server startup.

### All Servers Disk Usage Report shows No Data Available

To view the All Server Disk Usage report, you must assign the Free Disk Space and Used Disk Space graphs to the managed devices. Refer to [Assigning a Graph Profile to a Device](#) for details.

Assign both the Used Disk Space and Free Disk Space graphs to the devices, wait for two polling intervals and then view the report again.

### Top N Volumes having Low/More Disk Space report shows No Data Available

To view the partition-wise reports, you must assign the Free Disk Space and Used Disk Space graphs to the managed devices. Refer to [Assigning a Graph Profile to a Device](#) for details.

Assign both the Used Disk Space and Free Disk Space graphs to the devices, wait for two polling intervals and then view the report again.

### Junk characters in Interface Reports

In Chinese or Japanese version of OpManager, if the SNMP agents sends data as Unicode characters, OpManager might not be able to translate it properly and hence display the values as junk.

To display this properly, you need to specify the encode type of your agent in the Device Settings dialog. Double-click the device and click **Monitoring** under **Categories**. Enter the encode type in the **Encoding** Box and click **OK**.

### "NA" in All Servers Disk Usage Report

You will see NA in All Servers Disk Usage report if you have not assigned both the Used Disk Space and Free Disk Space graph profiles to the managed devices.

Assign both the Used Disk Space and Free Disk Space graphs to the devices, wait for two polling intervals and then view the report again.

### **Applications Reports show No Data Available**

The applications reports such as HTTP Servers by Response Time, SMTP Servers by Response Time, and others can produce results only if the application is running in at least one of the managed devices. Otherwise, the report shows No Data Available.

## Other Troubleshooting Tips

- [Error bringing up browser](#)
- [Selected device type is not applied to the device icon](#)

### Error bringing up browser

You will get this error in Linux machines when you try to invoke Help or use the Browse tool when the system has no browser installed in it. Install a browser and set the path in the **.bash\_profile** file and execute it. (The name of the file in certain versions may be **.bash\_rc**).

If a browser is already installed, then check whether the browser path is set properly. If not specify it in the **.bash\_profile** file and execute it.

### Selected device type is not applied to the device icon

Right-click the device and click **Refresh**.

## **Appendix**

### **Third Party Software**

For details about the third-party software bundled with ManageEngine OpManager, refer to *<OpManager Home>/COPYRIGHT* file.

The source file "dori.jasper.view.JRViewer" in the Jasper Reports package has been modified in the current version of OpManager and is available at the *<OpManager Home>/classes* directory. The original source file of "dori.jasper.view.JRViewer" is available at <http://sourceforge.net/projects/jasperreports>.

## Glossary

### A

**Acknowledge:** OpManager provides an option to mark the alarms on which you have worked on. This helps the other operators working on alarms to know the current status.

**Active alarms:** Alarms with severity status other than Clear.

**Alarm:** A visual notification generated for every event. The alarms are color-coded that helps the administrator in understanding about the fault quickly.

**Alarm variables:** The alarm variables are strings preceded by \$ (dollar) symbol that fetches the value from the generated alarm.

**Asset:** A device managed on the network. It can be a switch, router, server, or a workstation.

**Attention:** One of the severity levels used by OpManager. By default, when a device misses one status poll, an event is logged and a corresponding alarm will be generated with this severity. This can also be used for threshold and trap related alarms.

### B

**BPDUs:** All switches in an extended LAN participating in Spanning-Tree Protocol gather information on other switches in the network through an exchange of data messages. These messages are bridge protocol data units (BPDUs). BPDUs contain information about the transmitting switch and its ports, including switch and port Media Access Control (MAC) addresses, switch priority, port priority, and port cost. The Spanning-Tree Protocol uses this information to elect the root switch and root port for the switched network, as well as the root port and designated port for each switched segment.

### C

**Category:** OpManager classifies the discovered devices into five categories: Servers, Switches, Routers, Firewalls, Printers, and Desktops. They can be viewed from the respective maps under Infrastructure view.

**Community String:** The authentication string used to communicate with the SNMP agent running on a device.

**Critical:** One of the severity levels used by OpManager. By default, when a device misses five status polls, an event is logged and a corresponding alarm will be generated with this severity. This can also be used for threshold and trap related alarms.

**Custom graphs:** Graphs that you can configure to be plotted for any device.

### D

**Dependency:** The status polling for a device can be controlled based on its dependency on some other device. This prevents the unnecessary status checks made to the dependent nodes.

**Device Snapshot:** An OpManager feature that shows the real-time details of a device.

**Device status:** The current operational status of the device.

**Device type:** Device type of the device indicates the model of the device. OpManager automatically identifies many common device types during discovery including Cisco 1700 series, 800 series, Catalyst 2950, 3000 Windows XP, 2000, Linux and so on.

**Devices to watch:** Devices that are under various trouble status. They can be viewed from the Devices to Watch map.

**DHCP:** Dynamic Host Configuration Protocol, a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

## E

**Event:** An event is generated whenever a fault is identified in a managed device. The events are color-coded so that the administrator can easily understand the nature of the fault.

**Event history:** List of events generated for a selected device.

## F

**FTP:** The protocol that allows users to copy files between the local system and any system that can be reached on the network.

## H

**Home Page:** The page that will be opened when the application client is started.

## I

**ICMP:** Internet Control Message Protocol. A required maintenance protocol that reports errors and allows simple connectivity.

**IP Routing:** Routing is the act of moving information across an internetwork from a source to a destination. Along the way, at least one intermediate node typically is encountered.

## L

**Local Network:** Network to which the machine hosting OpManager is connected.

## M

**MAC address:** Short for Media Access Control address, a hardware address that uniquely identifies each node of a network.

**Map toolbar:** Toolbar in the map.

**MIB:** Management Information Base. A MIB is a standard set of definitions for exchanging information about hardware and software components. Each MIB contains a group of objects, which specify a structure and format for defining manageable elements.

**MIB Browser:** The MIB Browser tool is a complete SNMP MIB Browser that enables loading and browsing MIBs and allows performing all SNMP-related operations.

**Monitoring:** The process of keeping track the health of all the discovered devices. OpManager monitors each discovered device, service, port and interface periodically. You can also choose to stop monitoring a device.

**Monitors:** OpManager includes many out-of-the-box Monitors to monitor the resources, services, application, traffic details and so on, in the devices in the networks.

## N

**Netmask:** In administering Internet sites, a netmask is a string of 0's and 1's that mask or screen out the network part of an IP address(IP) so that only the host computer part of the address remains. The binary 1's at the beginning of the mask turn the network ID part of the IP address into 0's. The binary 0's that follow allow the host ID to remain. A frequently-used netmask is 255.255.255.0. (255 is the decimal equivalent of a binary string of eight ones.) Used for a Class C subnet (one with up to 255 host computers), the ".0" in the "255.255.255.0" netmask allows the specific host computer address to be visible.

**Network Address:** IP address of the network.

**Network discovery:** The process of discovering all devices in the network.

**Non-SNMP Devices:** Devices that do not support SNMP.

**Notification criteria:** Criteria specifies the faults for which the notification action has to be performed.

**Notification profile:** A profile containing the settings and criteria for notifying the network administrator whenever alarms are generated.

## O

**OID:** Object Identifier. Object identifiers are, basically, strings of numbers. They are allocated in a hierarchical manner, so that, for instance, the authority for "1.2.3" is the only one that can say what "1.2.3.4" means. They are used in a variety of protocols.

**Operator Notes:** Any information that an operator want to add to the alarm generated for a device.

**OpManager's Discovery:** OpManager automatically discovers all devices in the local network using SNMP and ICMP protocols.

## P

**Ping:** Network diagnostic tool used to verify connectivity to the selected device on your network.

**Polling interval:** The time interval between each status checks made by OpManager to find the current status of managed services and devices.

**Profile:** Settings saved under a name to reuse them.

**Protocol:** A set of rules and conventions for sending information over a network. These rules govern the content, format, timing, sequencing, and error control of messages exchanged among network devices.

**Proxy server:** A server between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

## Q

**Quick find:** OpManager feature that helps to quickly locate the devices on the maps.

## R

**Rediscovery:** The process that discovers an already discovered network again to add the missed devices, and to update the configuration settings of all the discovered devices.

**Response time:** The time between the request sent to a particular port and getting a response from it.

## S

**Service Down:** One of the severity levels used by OpManager. When a managed service does not respond to the poll, an event is logged and a Service Down alarm will be generated.

**SMS:** Short Message Service. Using SMS, a short alphanumeric message (160 alphanumeric characters) can be sent to a mobile phone.

**SMTP:** Simple Mail Transfer Protocol. A protocol used to transfer electronic mails between computers.

**SMTP Server:** Name of the server through which the mail has to be routed.

**SNMP:** Simple Network Management Protocol. It is the most common network management protocol that provides a means of exchanging the data between the network devices. It is based on the manager-agent model, and uses MIBs to exchange information between them. Using the SNMP protocol, a manager can query and modify the status and configuration information on each managed device.

**SSH:** Secure SHell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels.

**Status polling:** The automatic status checks made by OpManager on the managed devices periodically.

**STP:** Spanning-Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations.

**Suppress alarms:** Controlling the alarm generation for a device for a specific period.



## T

**Telnet:** A protocol that is widely used to log on to network computers. Telnet also refers to the application that uses the Telnet protocol for users who log on from remote locations.

**Threshold:** A region marking a boundary. OpManager allows you to define thresholds for SNMP variables on a device to monitor the device performance.

**Trace route:** A utility that records the route in which a packet of information traverses when transmitted between your computer and a specified destination computer.

**Trouble:** One of the severity levels used by OpManager. By default, when a device misses three status polls, or when a switch or a router port is operationally down, or when printer has some internal problems, an event is logged and a corresponding alarm will be generated with this severity. This can also be used for threshold and trap related alarms.

## U

**Unmanage:** Unmanaging a device will stop sending status polls to the device and the data collection for the graph profiles assigned to the device.

## W

**WMI:** The WMI (Windows Management Instrumentation) Control is a tool that lets you configure WMI settings on a remote computer or local computer.