

A Guide to Quick-start OpManager

Here are some quick steps to get started with the discovery and monitoring using OpManager. Before that, a quicker note on what OpManager can monitor. Just about anything on your network. It is enough if the device is reachable by OpManager.

The discovered devices are categorized as Servers, Routers, Switches, Firewalls, Printers, UPS, Wireless APs, and Desktops.

What do you want to do?

The series of tasks you might want to perform to get started could be in the following order...

1. Discover networks
2. Discover a single device
3. Find a device
4. Map the devices
5. Monitor memory, cpu, and disk
6. Set thresholds
7. Configure Email Alert
8. When in Trouble...

Discover Networks

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.



The screenshot shows the OpManager Admin interface. At the top, there are navigation tabs: Maps, Alarms, Admin (selected), Reports, and Support. Below the tabs, the breadcrumb path is 'Admin > Discover Network'. The main content area is titled 'Add New Network' and contains two input fields: 'Network IP' with the value '192.168.5.0' and 'Netmask' with the value '255.255.255.0'. Below these fields is an 'Add Network' button. Below the form is a table titled 'Discovered Networks (13)'. The table has five columns: 'Network', 'Netmask', 'Manage/UnManage', 'Re-discover Now', and 'Discovery Status'. The table contains three rows of discovered networks.

<input type="checkbox"/>	Network	Netmask	Manage/UnManage	Re-discover Now	Discovery Status
<input type="checkbox"/>	119.119.119.0	255.255.255.0	✓	▶	✓
<input type="checkbox"/>	192.168.110.0	255.255.255.0	✓	▶	⚠
<input type="checkbox"/>	192.168.111.0	255.255.255.0	✓	▶	⚠

Discover Devices

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.

The screenshot shows the 'Admin > Add Device' page. At the top, there are navigation tabs: Maps, Alarms, Admin (selected), Reports, and Support. Below the navigation is a breadcrumb 'Admin > Add Device'. The main content area is titled 'Add Device' and contains the following form fields:

- Device name / IP Address: 192.168.5.25
- Netmask: 255.255.255.0
- SNMP Port: 161
- Community String: *****

An 'Add Device' button is located at the bottom of the form.

Find the Device

Type the device name in the search field on the left. You will find the device pronto! Here is the screenshot showing you the search field.

The screenshot shows the 'Home' navigation tab selected. On the left, there is a 'Device Search' section with a text input field containing 'buddy' and a 'Search' button. On the right, there is a 'Dashboard' section with an 'Infrastructure Snapshot' table:

Infrastructure Snapshot	
✘ Servers	✔ Routers
✔ Printers	✘ Desktops
✔ Wireless	✔ DomainController

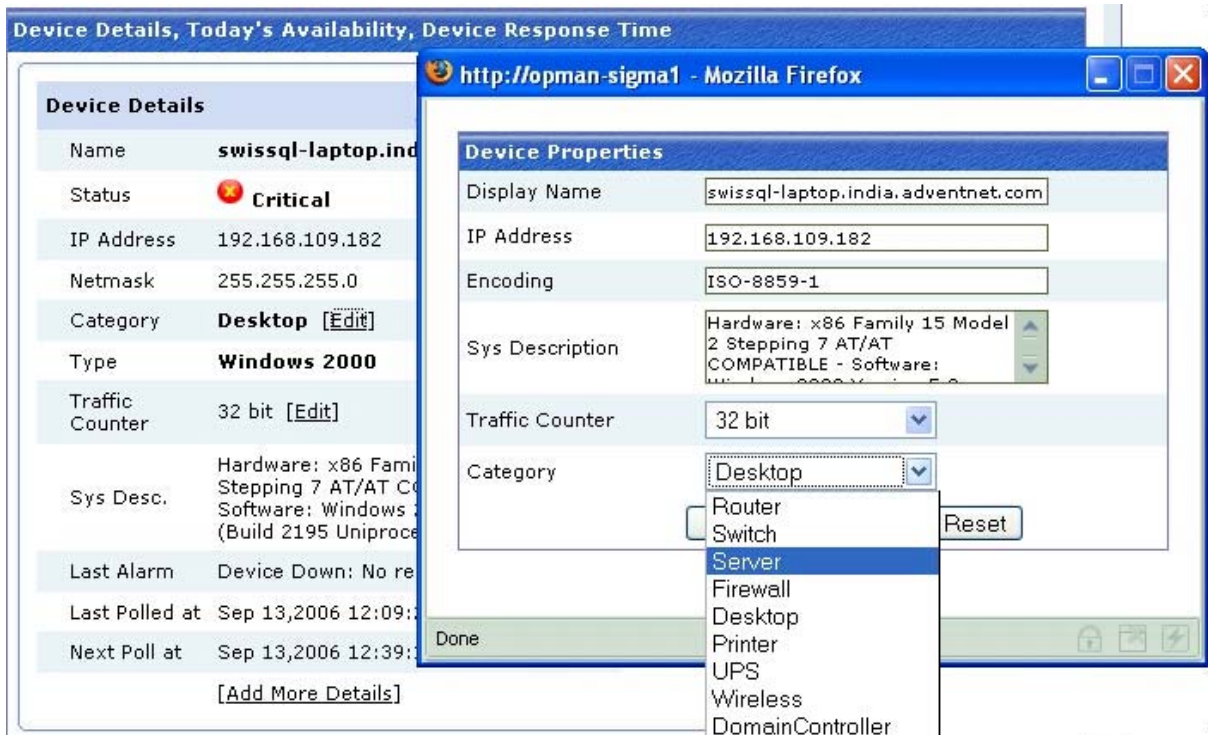
Map the Devices

OpManager automatically 'maps' the discovered devices into few broad categories like Servers, Routers, Switches, Desktops etc.

Don't worry if any of the discovered devices are not classified correctly. Here are the steps to change them:

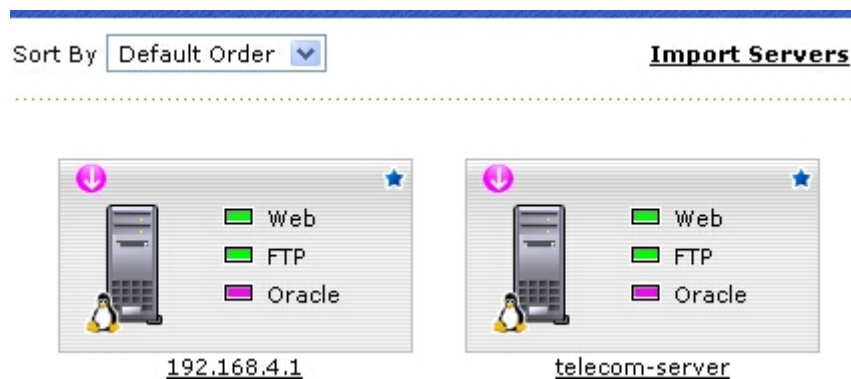
To change category of a single device,

1. Go to the device snapshot page
2. Click Edit icon against the Category field
3. Select the correct category from the corresponding combo-box and save changes



To bulk-import devices from desktops to servers,

1. Go to the Servers map
2. Click Import Servers link on top right corner
3. Move the required devices to the Servers category and save changes.



Monitor CPU, Memory, Disk

The monitors for CPU, Memory, and Disk Utilization are automatically associated for SNMP-enabled devices. These monitors are SNMP-based. You will see the dial graphs for these three resources in the device snapshot page.



Wait! Don't panic if you are not seeing the dial yet. You may not see the dials if SNMP is not enabled in the device. All you need to do is to enable SNMP on the device and rediscover the device, or simply associate a [non-SNMP monitor](#).

Do you see the dial graphs appear for some devices while few dont?

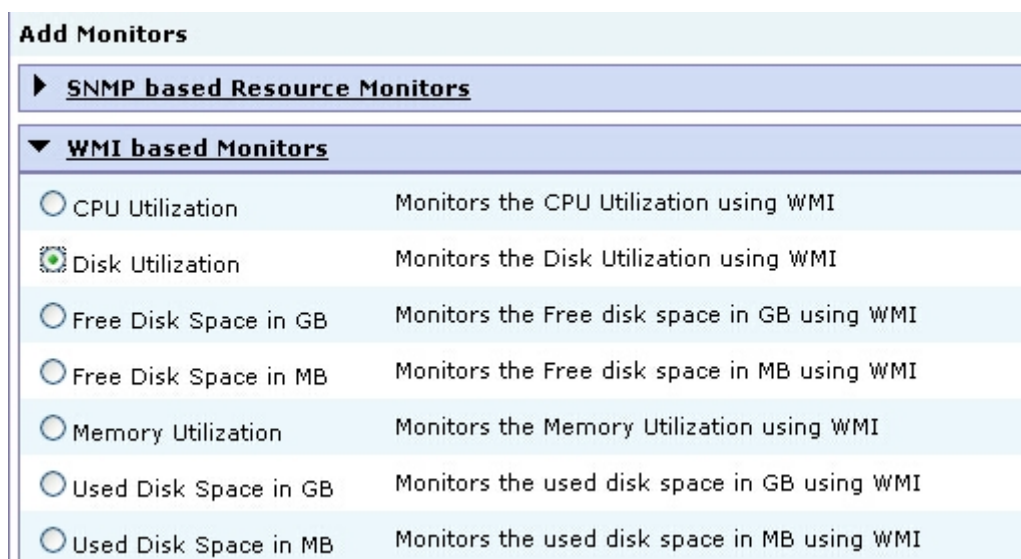
- Check if the device is SNMP-enabled. A blue star is shown on the device icon in the map.
- Click the device to see the device snapshot page. The 'sysDescr' here will show the system description if the device responds to SNMP requests
- Scroll down to the Resource Monitors section and click the Edit icon against the Monitor name.
- Click the Test Monitor link. When you click this link, OpManager queries the device for the data. If it responds, you should be able to see the dial.

If the Test Monitor does not respond, check the [troubleshooting steps](#).

Read on if you want to configure non-SNMP-based monitoring or skip and move to the [next section](#).

WMI / Telnet Monitoring

If your devices are not SNMP-enabled, you can associate WMI-based monitors for all the Windows machines, and Telnet-based monitors for Linux /Solaris machines.



The steps are:

- Go to Admin-->Quick Configuration Wizard.
- Select the option ' Specify a common Username and Password for Windows / Linux / Solaris devices'.
- Select the device type as either Windows, Linux or Solaris.
- If you have selected Windows, configure the domain name, domain admin user name and the password to connect to the remote windows devices. For instance, if the domain name is BigDom and the user name is administrator, in the User name field, configure BigDom\administrator.

Assign password details to several devices

Select a device type Windows Linux Solaris

User name

Password

- If you have selected Linux or Solaris, configure the common username and password with which you can log into these devices.
- After configuring the device passwords, go back to the Quick Configuration Wizard.
- From here, select the option 'Add a new monitor to several devices (Eg. Traffic monitor,Service monitor)' .
- Select Resource Monitors from the monitors list.
- Select WMI based Monitors for non-SNMP windows devices, and select Telnet/SSH based monitors for Linux devices.
- Select the required monitor and associate it to the required devices.

Note: You can effect these configurations for individual devices too. Click the Passwords link on the right in the device snapshot page to configure the password. Scroll down to the 'Resource Monitors' section and associate the required monitor.

Password details for presales-server.india.adventnet.com

SNMP Port

Read Community

Write Community

Login Details

User Name

Password

Command Prompt

Login Prompt

Password Prompt

Connection Protocol

Set Thresholds

You can configure thresholds for the following performance monitors:

1. Resource Monitors, Service Monitors, Traffic Monitors, Custom Monitors, Application Monitors, URL Monitors

The steps to configure are,

- Select the required monitor from Admin-->Monitors tab.
- Select 'Enable Threshold' checkbox and configure the monitor threshold.
- Again, you can configure thresholds for individual devices by editing the resource monitor from the device snapshot page.

Monitor Properties

Monitor Name	: CPUUtilization	<input type="button" value="Test Monitor..."/>
Display Name	: CPU Utilization	
Polling Interval (mins)	: <input type="text" value="15"/>	
Units	: Percentage	


Threshold Settings (optional)

<input checked="" type="checkbox"/>	Enable Threshold
Threshold allow you to set safe limit for the data collected for graphs. OpManager can be configured to send notifications if the limit is violated.	
Threshold Limit	: <input type="text" value="65"/> eg. 70 (or) 95 etc
Threshold Check	: Monitored value is <input type="text" value="greater than"/> threshold limit.
Alarm Message	: <input type="text" value="Threshold Violation"/> (This message will be sent as the Alarm)
Severity of the Alarm	: <input type="text" value="Attention"/>
Generate Alarm, only if threshold is violated <input type="text" value="2"/> consecutive times.	
<hr/>	
Clear Alarm Generation	
Threshold Check	: Monitored value is <input type="text" value="lesser than"/> threshold limit.
Rearm Value	: <input type="text" value="55"/>

2. Device Response Time and Packet Loss Percentage:


- Select the device for which you want to configure the thresholds.
- Click Edit icon in the 'Device Response Time' column to configure threshold on response time.
- Click Edit icon in 'Today's Packet Loss' column to configure threshold on packet loss percentage.



Device Details, Today's Availability, Device Response Time

Device Details	
Name	presales-server.india.adventnet.com
Status	 Clear
IP Address	192.168.4.12
Netmask	255.255.255.0
Category	Server [Edit]
Type	Linux
Sys Desc.	Linux presales-server 2.2.14-5.0 #1 Tue Mar 7 21:07:39 EST 2000 i686
Last Alarm	
Last Polled at	Jul 26,2006 03:11:19 PM
Next Poll at	Jul 26,2006 03:16:19 PM
[Add More Details]	


Today's Availability

7 ^b 30 ^b




 Downtime (0.0%) - 0 Mins 0 Secs
 Uptime (100.0%) - 15 Hrs 12 Mins

Device Response Time

[Click Edit Icon](#)  7 ^b 30 ^b

1 ms

Today's Packet Loss

 7 ^b 30 ^b

0 %

Configure an Email Alert

You will need to configure the mail server settings, configure a notification profile, and associate it to the devices. This will notify you of specific faults through email.

1. Configure Mail Server Settings
 - Select Admin -->Mail Server Settings
 - Configure the Mail server name and port number
 - Configure the email id to which an email alert must be sent when a fault occurs
 - Click OK to save the settings.
2. Configure the Email Alert Profile
 - Select Admin --> Notification Profiles
 - Click Email Alerts link on the right
 - Type the profile name, to and from email address.
 - Select the variables that must appear in the mail subject and message from the corresponding list box.
 - Save the profile.

Profile Name

Mail Composition

To Email Address
(ex: admin@yourdomain.com,operator@yourdomain.com)

From Email Address
(ex: admin@yourdomain.com)

Mail Format Plain Text HTML Both

Mail Subject

Subject

Select Subject Variables
 Message of the alarm
 Source of the alarm
 Category of the alarm

Mail Message

Message

Select Message Variables
 Message of the alarm
 Source of the alarm
 Category of the alarm
 Severity of the alarm
 Time when alarm was generated

3. Associate the Alert Profile to devices

- Click 'Associate to devices' link on the right in the Notification Profiles page
- Select the configured email alert profile and click Next
- Select the criteria for which you would like to receive an email alert. Click Next.

Select all

when the Device misses poll(s)

When an **interface or switch port is down**

when any [selected...] **Service is down**

Select all Services

<input type="checkbox"/> NNTP	<input type="checkbox"/> LDAP	<input type="checkbox"/> Finger	<input type="checkbox"/> HTTPS	<input type="checkbox"/> Oracle	<input type="checkbox"/> IMAP	<input type="checkbox"/> MSSQL	<input type="checkbox"/> Telnet
<input type="checkbox"/> WebLogic	<input type="checkbox"/> DNS	<input type="checkbox"/> FTP	<input type="checkbox"/> Web	<input type="checkbox"/> Echo	<input type="checkbox"/> POP	<input type="checkbox"/> SMTP	<input type="checkbox"/> Exchange
<input type="checkbox"/> MySQL							

when any [selected...] **Windows Service is down**

when a **SNMP trap is received** from the device

when any assigned **Threshold rule** is violated.

when any [selected...] **Event Log Rules** generates alarm

notify when the **alarm is cleared**

- Assign it to the required category, or manually group the devices for which you wish to be notified. For instance, if you want to be notified of threshold violation for all Servers, select Server category from the combo-box.

Email alert is now configured for all the chosen devices. You will receive an email when a fault with the marked criteria is met.

When in Trouble...

All you need to do is,

1. Select Support tab
2. Click Request Support and submit your query.

Our techies will contact you!!!