

Quick-start OpManager 7

Here are some quick steps to install and 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. And whats more! You can add your own categories.

What do you want to do?

1. [Intall and Start OpManager](#)
2. [Connect Web Client](#)
3. [Configure Discovery Credentials](#)
4. [Discover networks](#)
5. [Discover a single device](#)
6. [Categorize the device](#)
7. [Monitor memory, cpu, and disk utilization](#)
8. [Set thresholds for proactive monitoring](#)
10. [Configure Email Alert](#)
11. [Advanced Configurations](#)

Install and Start OpManager

Windows installtion

1. [Download](#) the latest version of OpManager.
2. Execute OpManager.exe and follow the instructions in the installation wizard.
3. Click Next to begin the installation process. Go through the license agreement and proceed to the next step.
4. In the subsequent steps of the wizard, select the OpManager Edition (Professional or Free), language, the directory to install OpManager, the Programs folder to add the OpManager shortcuts, and the port number to run OpManager Web Server. Proceed to the next step.
5. If you want to install OpManager as Windows service, select Install OpManager as service option and proceed to the next step.
6. Register for technical support by supplying your contact information such as name, email id etc.
7. Verify the installation details and click Next.
8. Select the database as MySql and click Next.
9. Click Finish to complete the installation process.

OpManager starts as a service and the WebClient is automatically launched.

Connect the Webclient

If OpManager is installed as a service, the WebClient is launched automatically. You can also open a new browser instance and connect to OpManager by typing the hostname and port number in the address bar as follows:

<http://<hostname>:port> number.

Example: The host name is opmanager-host, and the port number as 8060. Connect as:

http://opmanager-host:8060

Configure Discovery Credentials

OpManager accesses the remote devices using the protocols SNMP, CLI, or WMI. The credentials like the password/snmp community, port etc., may differ for different device types. Pre-configuring a set of credentials in OpManager helps applying them to multiple devices at a time, saving a lot of manual effort.

1. Go to Admin → Credential Settings
2. Click New in this screen
3. Configure the following parameters and click Add to add the credentials:

Credential Type: Select the relevant protocol.

Name: Configure a name for the credential and also provide the description.

SNMP Community & Port For SNMP v1 and SNMP v2 protocols, configure the correct Read and Write community, and the SNMP Port.

WMI: If you select WMI as the protocol, configure the Domain Name, the user name, and the password. Example:- TestDomain\TestUser

Telnet/SSH: For Telnet/SSH, make sure you configure the correct login prompt, command prompt, and password prompt besides the user name and password to access the device.

The screenshot displays the 'Credential Library' window with a table of existing credentials and an 'Add Credential' dialog box open over it.

Name
Public v1
Public v2

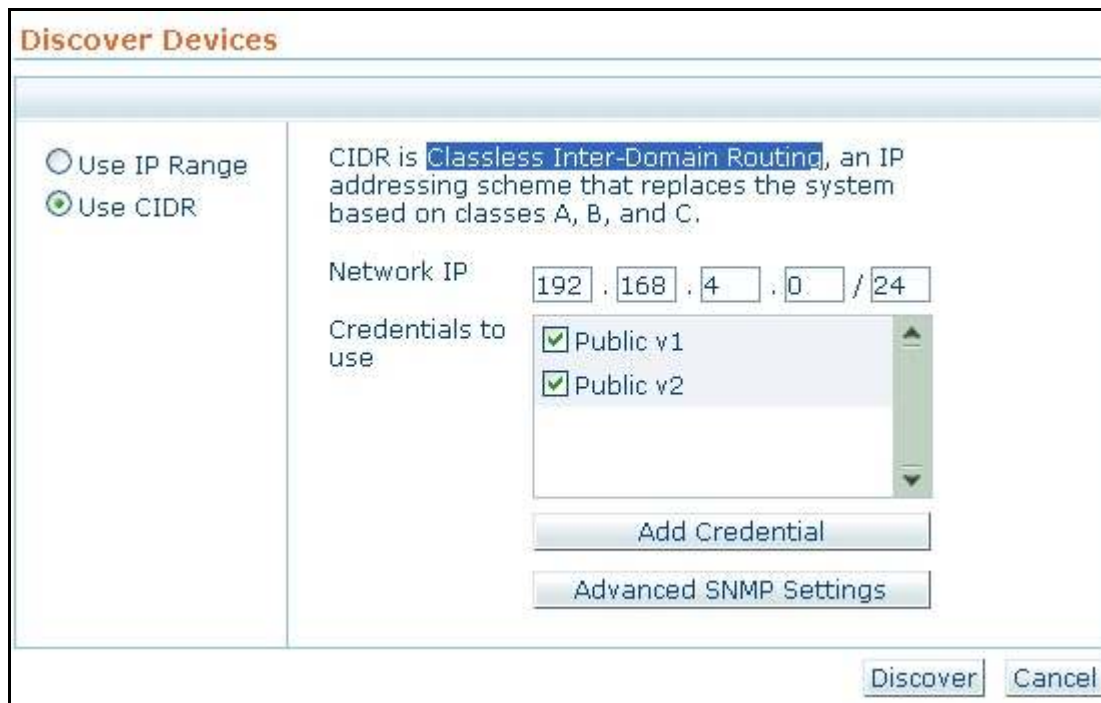
Add Credential	
Credential Type	SNMP v1
Name	
Description	
SNMP Read	public
SNMP Write	public
SNMP Port	161

Delete	
community for	
community for	

At the bottom right of the dialog box are buttons for New and Cancel.

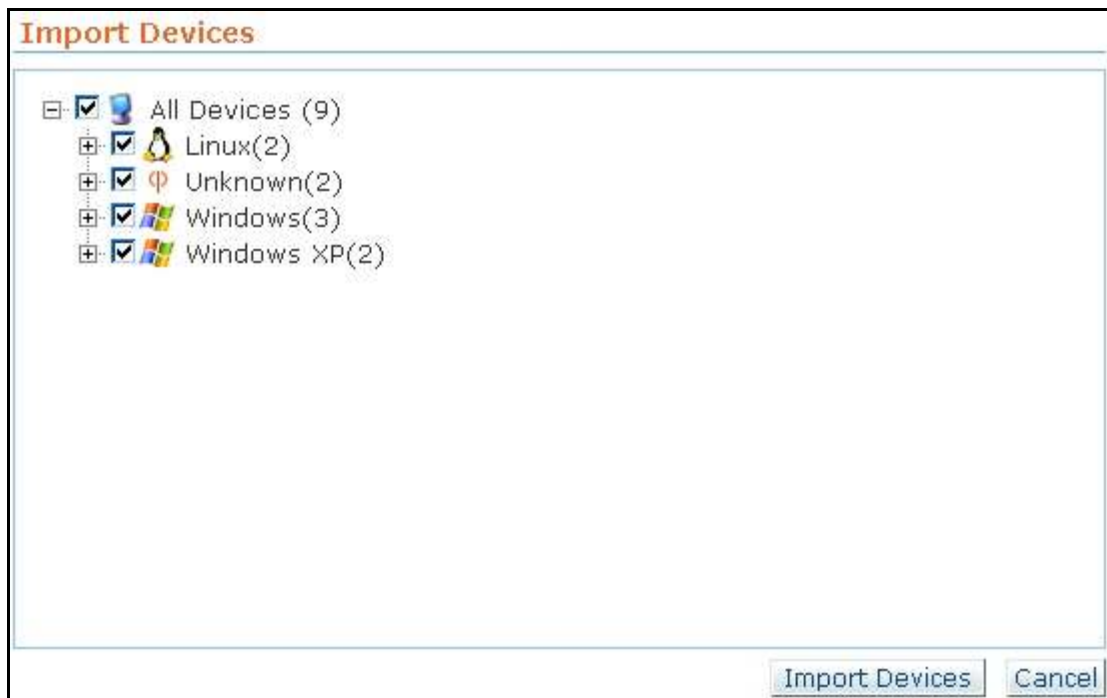
Discover Networks

1. Click the Admin tab.
2. Under Discovery, select Discover Devices.
3. Select Use CIDR (Classless Inter-Domain Routing) option.
3. Type the address of the network to be discovered. Example: 192.168.4.0
4. Click Discover. All the devices will be scanned for discovery and devices responding to OpManager are listed category wise.



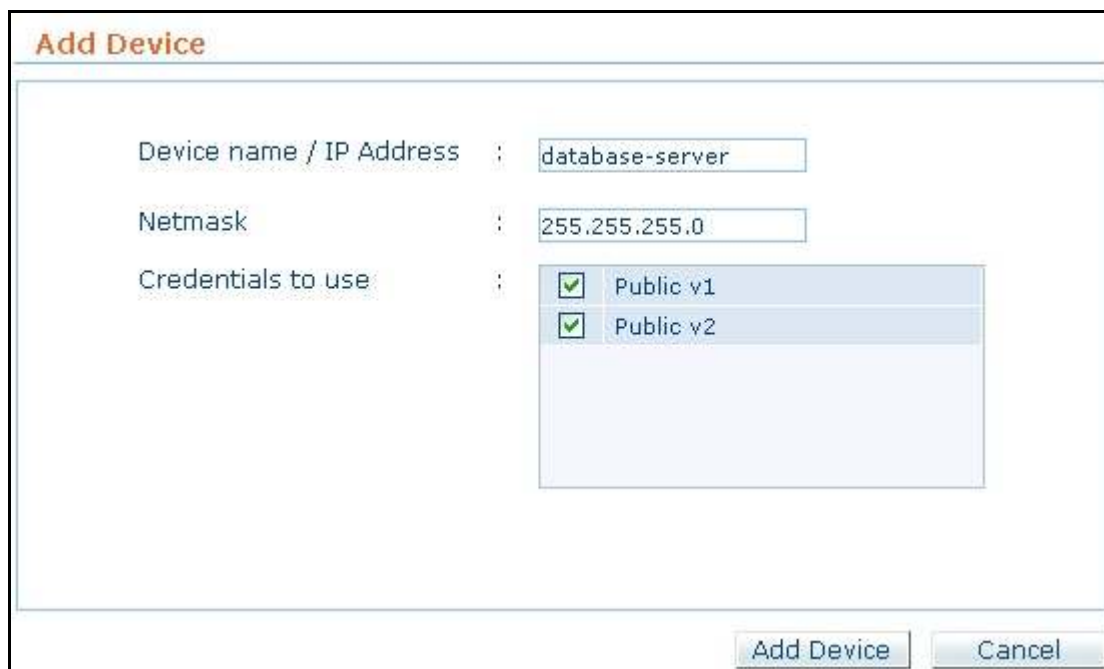
The screenshot shows the 'Discover Devices' dialog box. On the left, there are two radio buttons: 'Use IP Range' and 'Use CIDR'. The 'Use CIDR' option is selected. To the right of these buttons, there is a text box containing the text: 'CIDR is Classless Inter-Domain Routing, an IP addressing scheme that replaces the system based on classes A, B, and C.' Below this text, there is a 'Network IP' field with a text input showing '192 . 168 . 4 . 0 / 24'. Below the network IP field, there is a 'Credentials to use' section with a list box containing two items: 'Public v1' and 'Public v2', both of which are checked. Below the list box, there is an 'Add Credential' button. Below the 'Add Credential' button, there is an 'Advanced SNMP Settings' button. At the bottom right of the dialog box, there are two buttons: 'Discover' and 'Cancel'.

5. Click Import Devices to add all the devices for monitoring.
6. Click Finish once the devices are added.



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. Select the discovery credentials.
5. Click Add Device to start discovery.



Find the Device

Type the device name in the search field on the right. You will find the device pronto! Here is an image showing you the search field.



Import the Devices

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

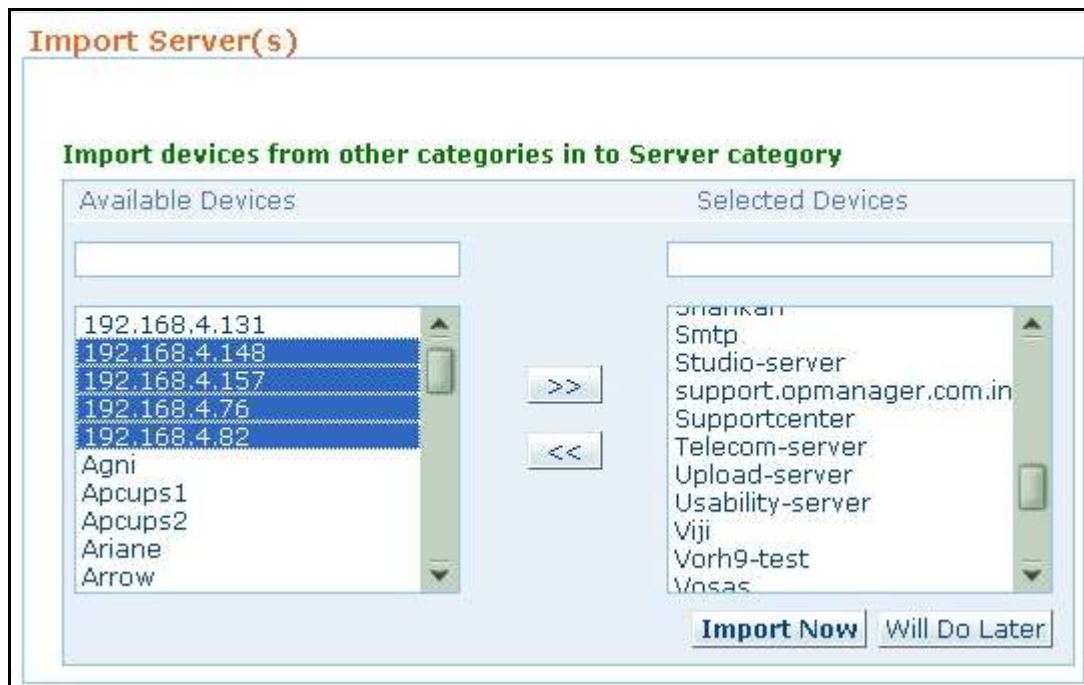
Don't worry if any of the discovered devices are not classified correctly. Here are the steps to change them:

To change category of a single device,

1. Go to the device snapshot page
2. Click the Category field
3. Select the correct category from the corresponding combo-box and wait.
The page refreshes with the category changed.

To bulk-import devices into any infrastructure view,

1. Select Maps tab.
2. Select the required infrastructure map from here, say Servers.
3. Click Import link on the right
4. Select the devices to be imported from the list and move to the right.
5. Click Import Now.



Monitor CPU, Memory, Disk

The monitors for CPU, Memory, and Disk Utilization are automatically associated for the devices based on the device template definitions. For instance, for Linux servers, the default template has SNMP-based monitors associated. So, all Linux servers will have SNMP-based resource monitors associated. You will see the dial graphs for these three resources in the device snapshot page if SNMP is enabled.

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. You have the option of either enabling SNMP, or associating CLI-based monitors. Here are the steps to associate CLI monitors.

1. Go to the device snapshot page.
 2. Click the Passwords link.
 3. Select the 'Apply Global Parameters' and select from the listed credential if you have already configured them.
- [OR]

Specify a new CLI credential for OpManager to authenticate to the device.

Change password

Credential Details

Use this Snmp Credential: None

Login Details

☐ Apply Global Parameters: CLI 2

☒ Use the below credential for the device

User Name: guest3

Password: *****

Command Prompt: \$

Login Prompt: :

Password Prompt: :

Connection Protocol: Telnet

4. Under Monitors → Performance Monitors, click Add Monitor..

5. Select the CLI monitors for the resources.

1. Do you see the dial graphs appear for some devices while few don't?

- 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 Monitors → Performance 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, try the troubleshooting steps provided here:

<http://manageengine.adventnet.com/products/opmanager/troubleshooting-guide.html>

2. If your devices are not SNMP-enabled, you can associate WMI-based monitors for all the Windows machines, and Telnet-based monitors for Linux machines as explained above. Pre-configured credentials come handy here..

Set Thresholds

You can configure thresholds for the following:

Resource Monitors, Service Monitors,Traffic Monitors :

Here are the steps to globally apply a threshold for a resource:

- Go to Admin→ Device Template. Example: Linux.
- Scroll down the template and click Edit Threshold and specify the thresholds for all the resources.
- Click Apply.
- Select the devices for which this change should be applied, and click Apply again.

The template will be modified and change will be carried to all the devices..

You can also configure thresholds for individual devices by clicking the Edit icon against each monitor name. You will find the provision to specify the threshold here.

Device Response Time and Packet Loss Percentage:

- Select the device for which you want to configure the thresholds
- Click Edit icon in the ' Response Time' and 'Today's Packet Loss'column to configure the thresholds.

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. Select Admin -->Mail Server Settings
2. Configure the Mail server name and port number
3. Configure the email id to which a notification must be sent when a fault occurs
4. Click OK to save the settings.
5. Select Admin --> Notification Profiles
6. Click 'Add New' option against Email Profiles.
7. Type the profile name, to and from email address.
8. Select the alarm variables that you want to see in the email and click Save.
9. Click Associate link on the right to associate the profile to devices.
10. Select the Profile and click Next.
- 11.
12. Select the fault criteria for which you need to be notified. For instance, if you want to be notified of threshold violation, select 'Threshold rule is violated'. Click Next
13. Select the devices or the category of devices for which you want to be notified. For instance, if you want to be notified of threshold violation for all Servers, select Server category from the combo-box. Click Next.

The profile will be associated to all the servers. You will be notified when ever a threshold is violated for a server.

Advanced Options

Define Device Templates

Define device templates to setup initial device configurations for existing and new device types.

1. Go to Admin → Device Templates
2. Click 'New Template' to define a template for a new device type. Click the Template name to modify an existing one.
3. Configure/Modify the following properties:

Device Template: Specify the device type.

Vendor Name: Select the vendor. Click **Add New** to add a new vendor, and **Save**.

Category: Select the category for the device type.

Monitoring Interval: Configure the interval at which the device needs monitoring.

Device Image: Select the image for this device type.

System OID: Type the sysOID and click **Add**. Click **Query Device** for OpManager to query the device for the OID.

Select Monitor: Click this option to select the monitors.

Edit Thresholds: Click this option to edit thresholds.

Click **Create** button to create the new device template.

Using Interface Templates

Monitoring requirement differs for different interfaces on a device. OpManager allows you to define configuration templates for interfaces of specific types. For instance, the configurations specified for an Ethernet interface can be applied to interfaces of this type across all devices, saving a lot of time.

1. Go to Admin → Interface Templates
2. Click an Interface Template to modify its properties.

Using the New Map Maker

OpManager 7 comes with an in-built flash-based MapMaker. No more hassles of invoking a separate tool to create business views.

Click the small down arrow in the Maps tab or simply mouse-over. The default maps, with options to add more maps are seen.



Adding New Infrastructure Views:

1. From the pop-up in the Maps tab, click Add Infrastructure View option.
2. Specify the category name and click Add
3. From the listed devices, select and move the required devices to this view
4. Click Import Now option.

Adding Business Views:

1. From the pop-up in the Maps tab, click Add Business View option.
2. Specify the business view properties such as map, the background map, the devices to be grouped into this view etc.
3. Click Apply and place the devices where ever required.

You can perform the usual operations of adding more device, adding links between devices, creating shortcuts, etc using the options provided on the left in the business views.

Contact Support

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