OpManager - Network Monitoring Software

ManageEngine OpManager is a comprehensive network monitoring software that provides network administrators with an integrated console for managing routers, firewalls, servers, switches, and printers. OpManager offers extensive fault management and performance management functionalities. It provides handy but powerful Customizable Dashboards and CCTV views that display the immediate status of your devices, at-a-glance reports, business views etc. OpManager also provides a lot of out-of-the-box graphs and reports, which give a wealth of information to network administrators about the health of their networks, servers and applications.

Quick Links:

- OpManager v12 - Read-Me
- Service Pack Download
- Steps to apply Service Pack
- OpManager v11 - Help
- Frequently Asked Questions (FAQs)

OpManager - System Requirements

The system requirements mentioned below are minimum requirements for the specified number of devices. The sizing requirements may vary based on the load.

Hardware requirements

OpManager Standard/ Professional Edition

No. of Devices	Processor	Memory	Hard Disk
1 to 250	Intel Xeon 2.0 Ghz 4 cores/ 4 threads	4 GB	20 GB minimum
251 to 500	Intel Xeon 2.5 Ghz 4 cores/ 8 threads	8 GB	20 GB minimum
501 to 1000	Intel Xeon 2.5 Ghz 4 cores/ 8 threads or higher	16 GB	40 GB minimum

OpManager Plus (or) OpManager Standard/ Professional Edition with Add-ons

OpManager Enterprise Edition

OpManager Enterprise Edition with add-ons

Note:

- CPU recommendation for deployments use the PassMark score. To learn more, click here.
- We strongly recommend assigning a dedicated machine for OpManager.
- For 1000 devices, 5000 monitors and 5000 interfaces with default monitoring interval and default database retention, OpManager utilizes about 1 GB/day of disk space. The number may vary based on the entities monitored in your environment & other factors like events generated, Syslogs, Traps etc.

Software Requirements

The following table lists the recommended software requirements for an OpManager installation.

Software	Evaluation	Production
Windows OS	Windows 10/8/7 (or) Windows Server 2019/ 2016/ 2012 R2/ 2012/ 2008	Windows Server 2019/ 2016/ 2012 R2/ 2012/ 2008
Linux OS	Ubuntu / Suse / Red Hat Enterprise Linux (upto version 8) / Fedora / CentOS / Mandriva (Mandrake Linux)	Red Hat/ 64 bit Linux flavors
Browsers	Chrome/ Firefox/ Edge/ IE11 Do not use OpManager Enterprise Edition in Internet Explorer. This will cause IE11 to work as IE7 which is not supported.	Chrome (preferred)/ Firefox/ Edge/ IE11

User Privilege: Local administrator privileges required for OpManager installation.

Port Requirements

The following table summarizes the ports and protocols that OpManager uses for communication.

Ports used by the application
Ports used for monitoring
Ports used by add-ons

Database Requirements

The following table lists the basic requirements for your OpManager database server.

PostgreSQL

- Comes bundled with the product.
- In case of failover, please use MS SQL.

Microsoft SQL

1. Supported versions:

SQL 2017 | SQL 2016 | SQL 2014 | SQL 2012 | SQL 2008

2. Important Notices:

1. For production use 64 bit versions of SQL
2. Recovery mode should be set to SIMPLE.
3. SQL and OpManager should be in the same LAN. Currently WAN based SQL installations are not supported.

3. Collation:

- English with collation setting (SQL_Latin1_General_CP1_CI_AS)
- Norwegian with collation setting (Danish_Norwegian_CI_AS)
- Simplified Chinese with collation setting (Chinese_PRC_CI_AS)

- Japanese with collation setting (Japanese_CI_AS)
- German with collation setting (German_PhoneBook_CI_AS)

4. Authentication:

Mixed mode (MSSQL and Windows Authentication).

5. BCP:

The "**bcp.exe**" and "**bcp.rll**" must be available in the OpManager bin directory.

The BCP utility provided with Microsoft SQL Server is a command line utility that allows you to import and export large amounts of data in and out of SQL server databases quickly. The **bcp.exe** and **bcp.rll** will be available in the MSSQL installation directory. If MSSQL is in a remote machine, copy **bcp.exe** and **bcp.rll** files and paste them in the <\OpManager\bin> directory.

The SQL server version compliant with the SQL Native Client must be installed in the same Server.

List of Ports to be opened in Firewall

For device discovery

- If your device only supports WMI, you will need to keep the ports 135 and 445 open.
- If TCP is supported by your device, open the ports 5000 - 6000.

For data collection and monitoring of devices

Open the below ports in the firewall to ensure uninterrupted monitoring of your devices.

- SNMP-161(UDP) - Bidirectional
- SNMP Traps- 162(UDP)- Unidirectional (From monitored device to OpManager server)
- Telnet- 23(TCP)- Bidirectional
- SSH- 22(TCP)- Bidirectional
- ICMP- Used to check the availability status and to add a device. - Bidirectional
- Default syslog port 514(UDP)- Unidirectional (From monitored device to OpManager server)

Note: OpManager uses ICMP for its initial discovery of devices. If your device does not support ICMP, discovering it via 'Discovery Profile' is not possible. You will only be able to discover the device through 'Add Device' or 'CSV file' options.

Ports used by Applications Manager plugin

The following are the ports used by Applications Manager plugin:

- HTTP - 9090
- HTTPS - 8443

General Information

The ManageEngine directory (By default: C:\Program Files\ManageEngine\OpManager) and the database directory should be excluded from the antivirus program.

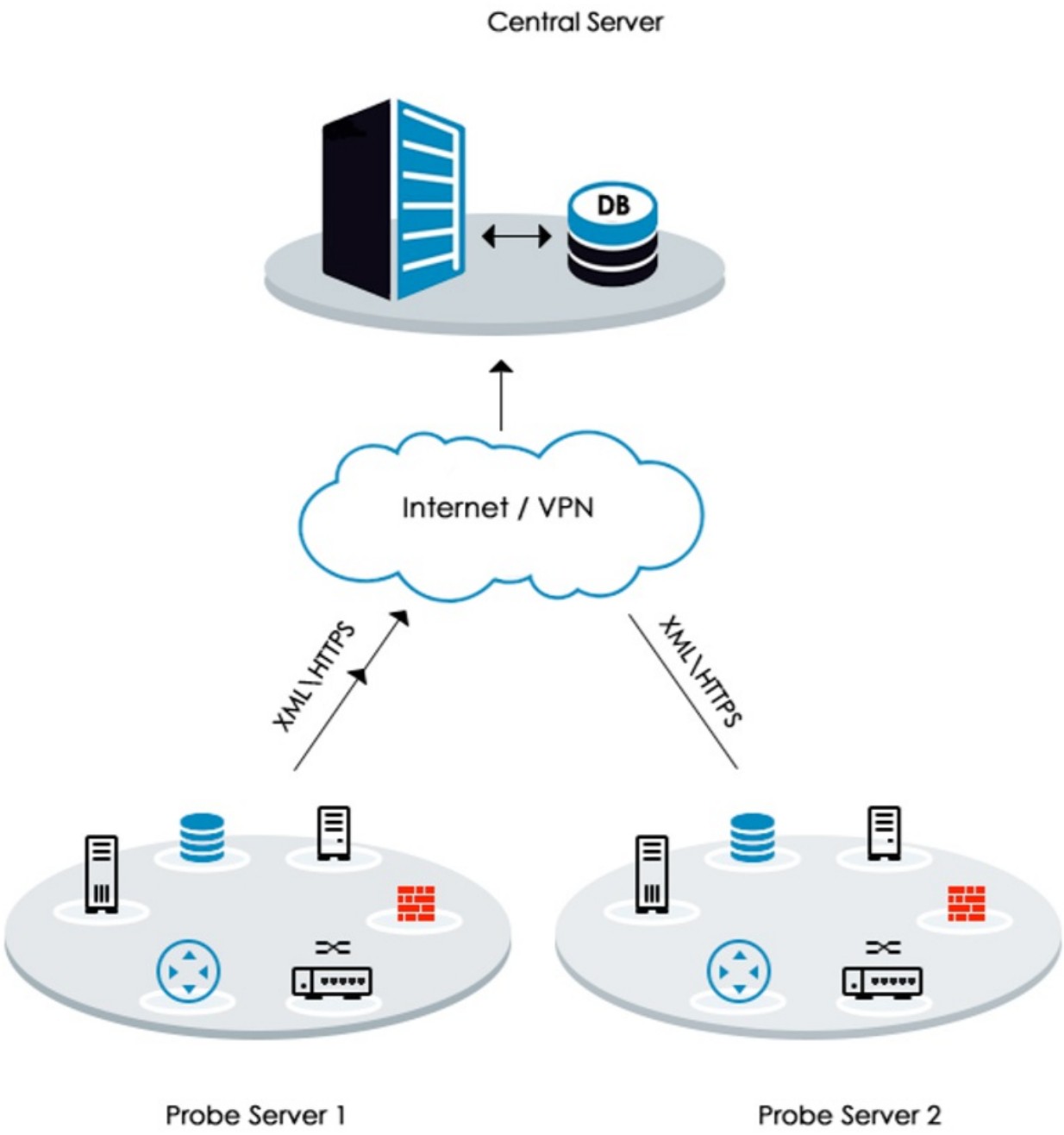
OpManager Enterprise Installation

OpManager Enterprise Edition can be deployed in the following cases:

Case 1: When geographically distributed networks need to be monitored from one location.

Case 2: When the number of devices that need to be monitored is more than 1K devices.

ManageEngine recommends the installation of a Central server and a Probe to effectively achieve a distributed network monitoring environment.



Central Server: Central periodically collects health, performance and fault data across all Probes and consolidates the information in one location.

Probe Server: The Probe periodically polls the devices in the local network and updates data to the central server. It has to be installed at the Remote Location.

Note: If OpManager is run with MSSQL as the backend database, then the MSSQL database must be configured before proceeding with the following installation.

Installing OpManager Enterprise Edition on Windows

OpManager Central Server

Step 1: Download the OpManager Central.exe from this link: Download Central Server | ManageEngine OpManager

Run the exe as 'administrator'

Step 2: Click 'Next' to proceed with installation.

Step 3: Click 'Yes' to the OpManager License agreement

Step 4: Choose the destination folder for OpManager installation and click 'Next' to proceed

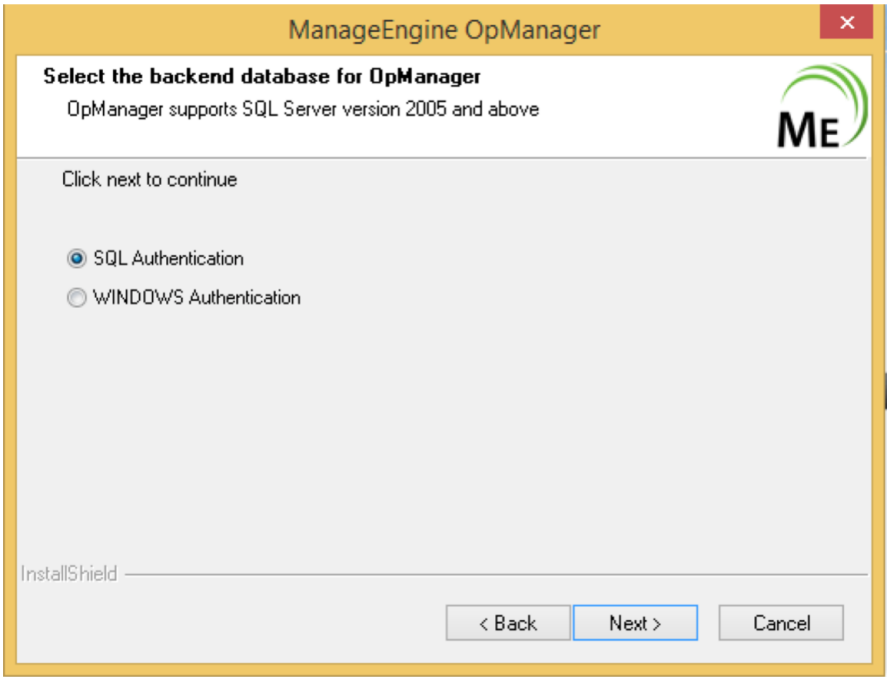
Step 5: If you want to change the default web server port for OpManager installation enter the new port number (OpManager Central uses 80 as the default web server port) and click 'Next' to proceed.

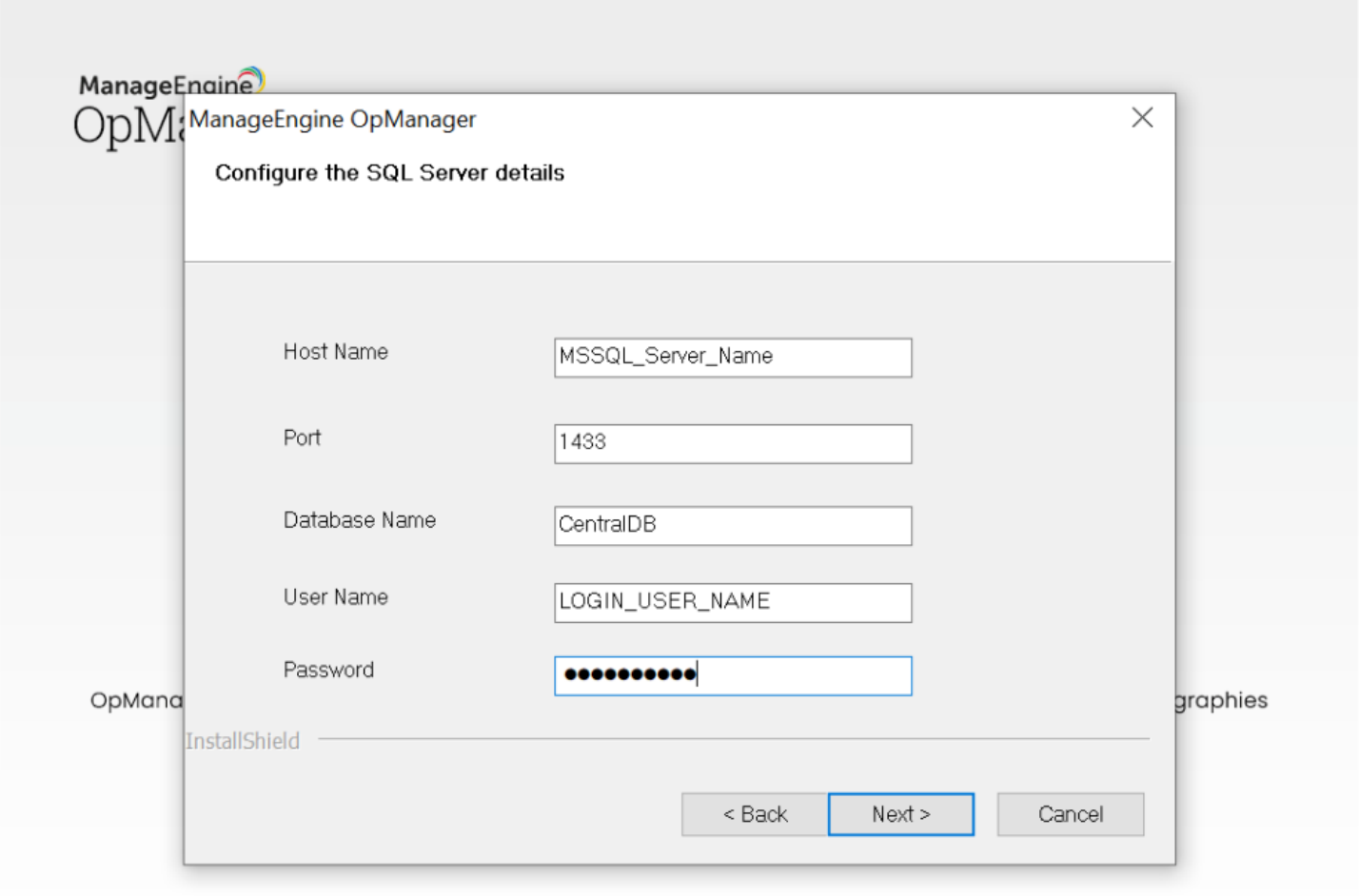
Step 6: Register your OpManager license with required details to get technical support and click 'Next' to proceed.

Step 7: Select 'Standalone' or 'Primary' server . If you are installing failover, select standby server. First configure standalone or primary for failover installation. Click 'Next' to proceed.

Step 8: If you select PGSQL, please proceed with Step 12. **(or)** If you select 'MSSQL' database (recommended for production). Click 'Next' to proceed

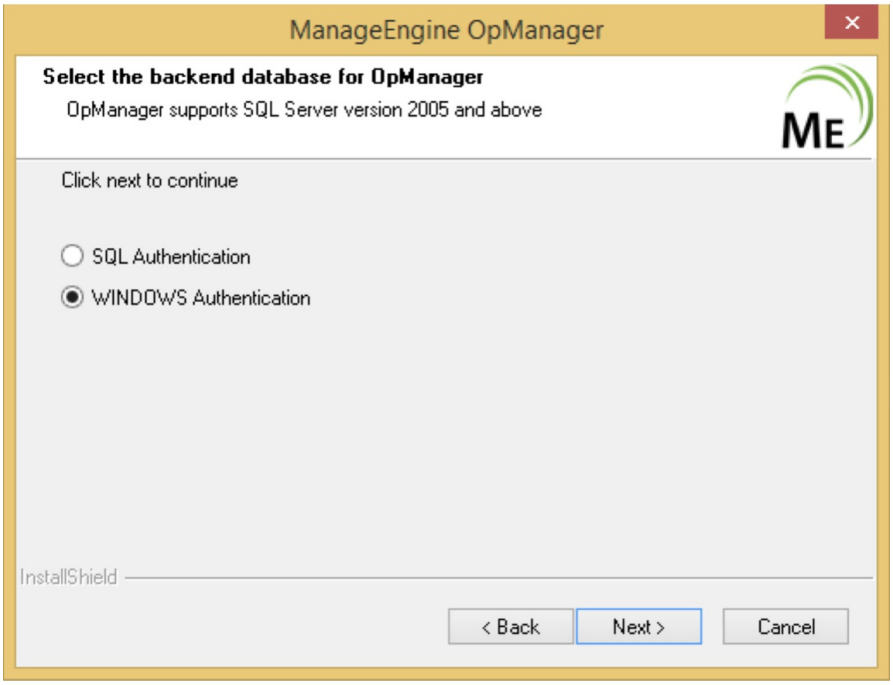
Step 9: If you select SQL Authentication, provide MSSQL details like Host Name, Port, Database Name. Use the SQL Server Authentication credentials (Username and Password) created earlier. Click 'Next' to proceed

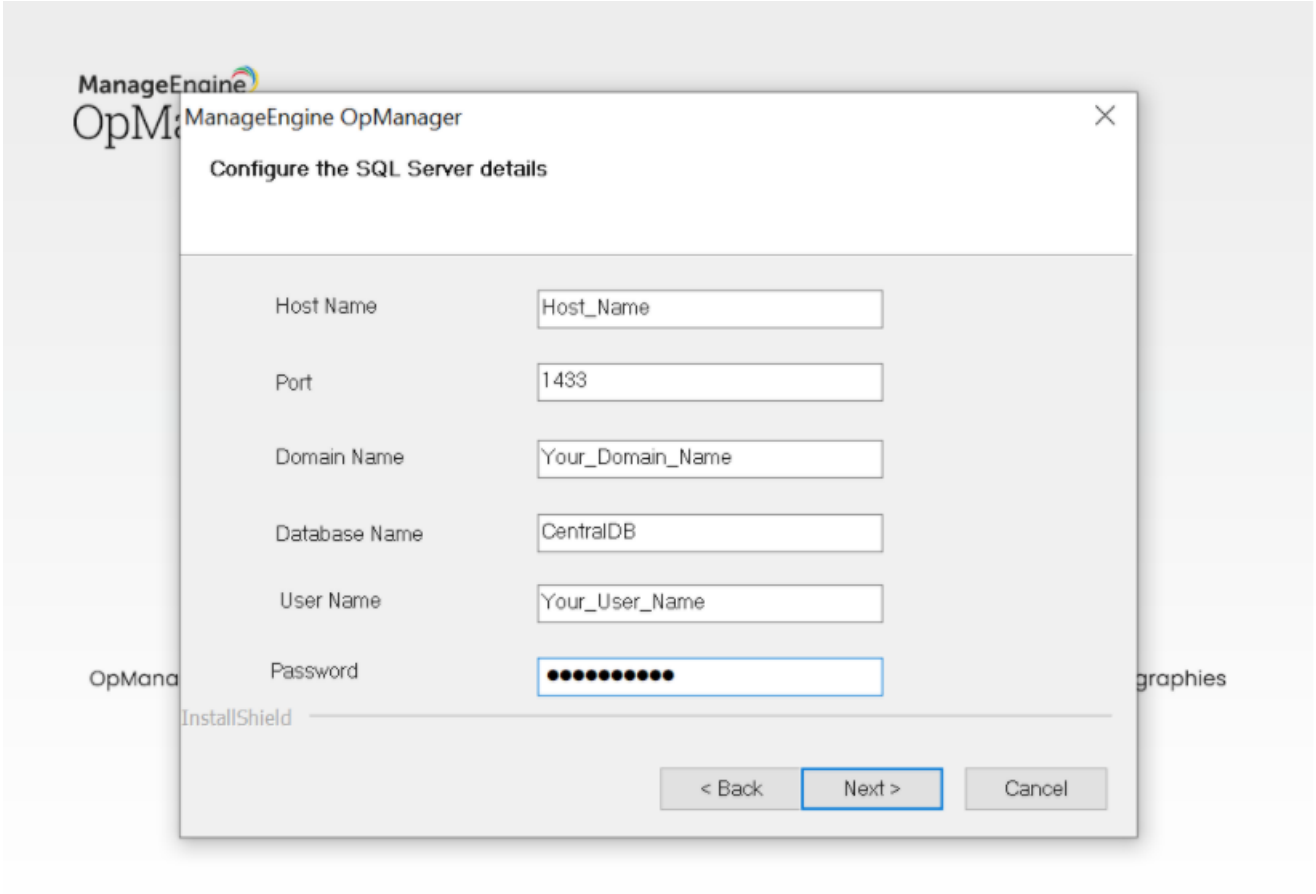




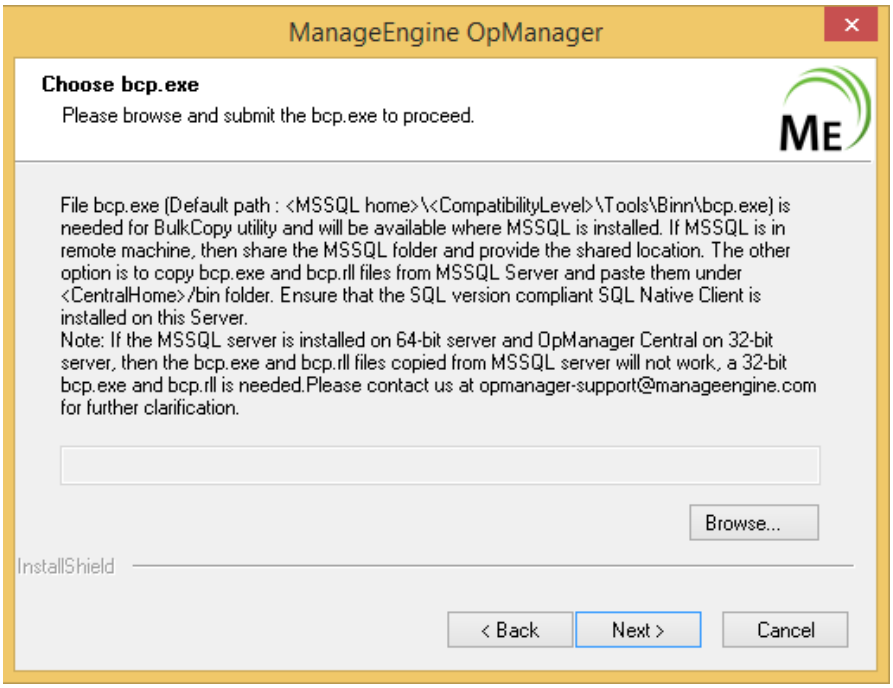
(or)

If you select WINDOWS Authentication, provide MSSQL details like Host Name, Port, Domain Name, Database Name, Username and Password. Click 'Next' to proceed.



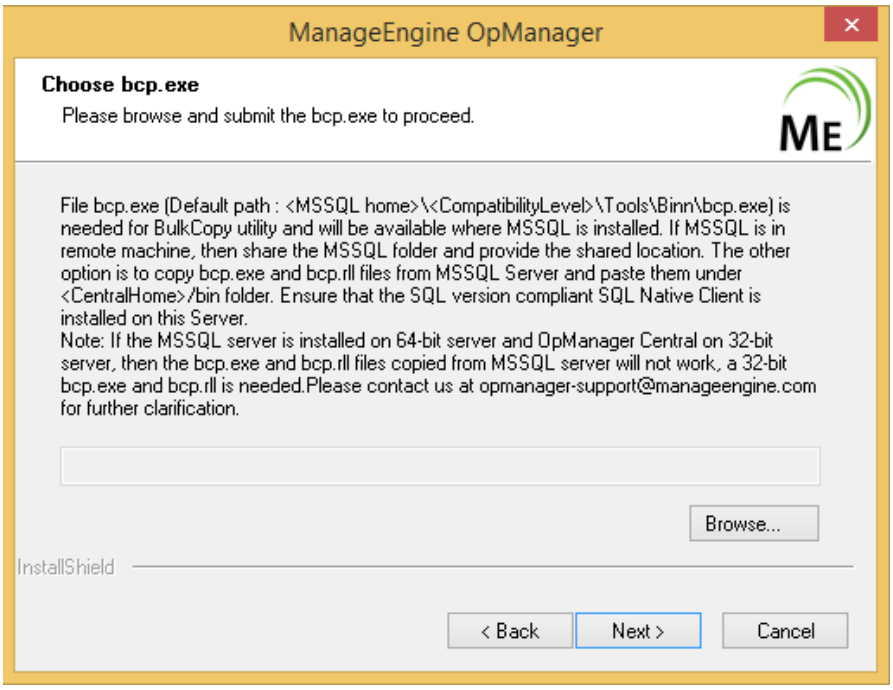


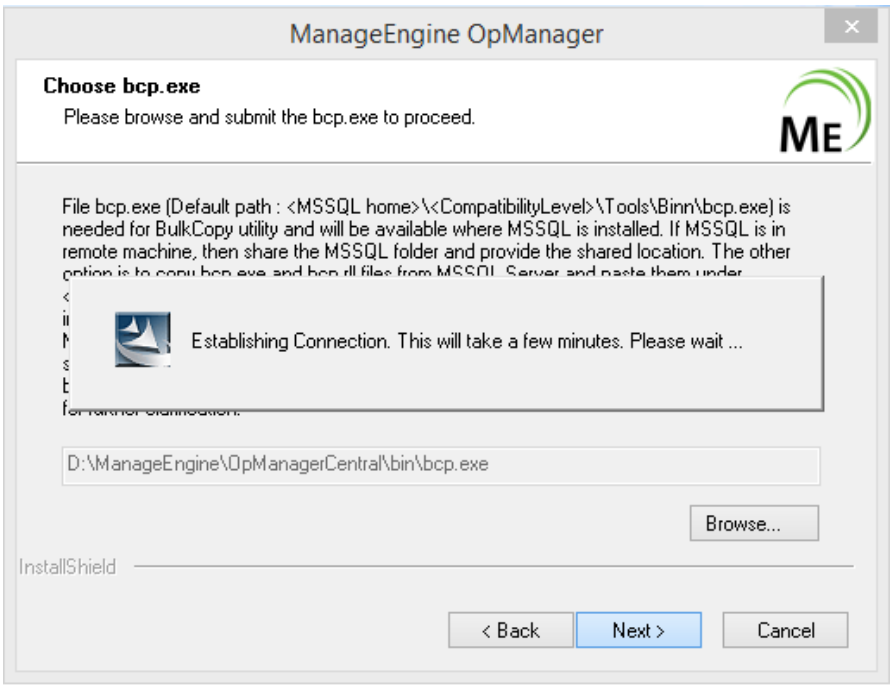
Step 10: Search for 'bcp.exe' and 'bcp.rll' in the MSSQL installation directory and copy these files under \OpManagerCentral\bin directory. Click 'Next' to proceed.



Note: The SQL server version compliant with the SQL Native Client must be installed in the same Server.

Step 11: Click on browse and select \OpManager\bin\bcp.exe. Click 'Next' to proceed





Step 12: Click 'Finish' to complete OpManager Central Server installation.

OpManager Probe Server

Step 1: Download the OpManager Probe.exe from the below link: Download Probe Server | ManageEngine OpManager

Run the exe as 'administrator'

Step 2: Click 'Next' to proceed with installation

Step 3: Click 'Yes' to the OpManager License agreement

Step 4: Choose the destination folder for OpManager Probe installation and click 'Next' to proceed

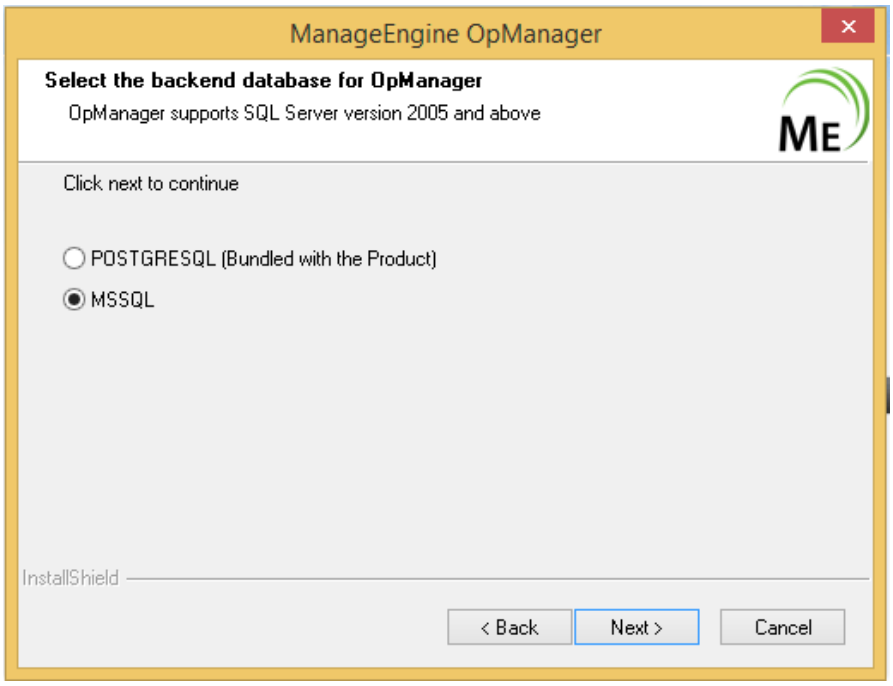
Step 5: If you want to change the default web server, netflow ports for OpManager probe installation enter the new port numbers (OpManager uses 80 as the default web server port and 9996 as the default Netflow port) and click 'Next' to proceed.

Step 6: Enter the details of the proxy server (if the probe is installed behind a proxy server) and click 'Next' to proceed

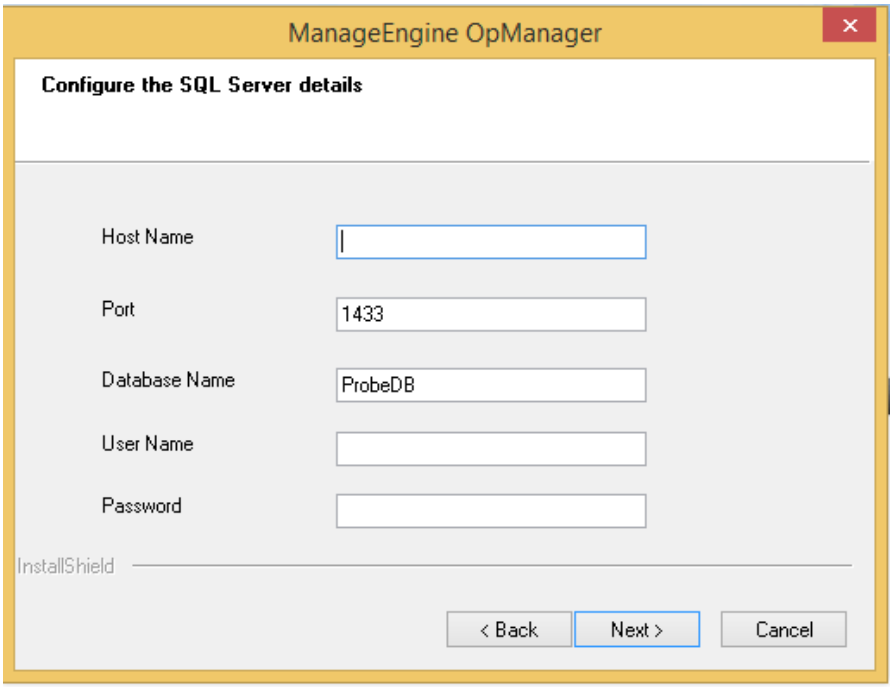
Step 7: Register your OpManager license with required details to get technical support and click 'Next' to proceed.

Step 8: Select 'Standalone' or 'Primary' server. If you are installing Failover, select standby server. First configure standalone or primary for Failover installation. Click 'Next' to proceed.

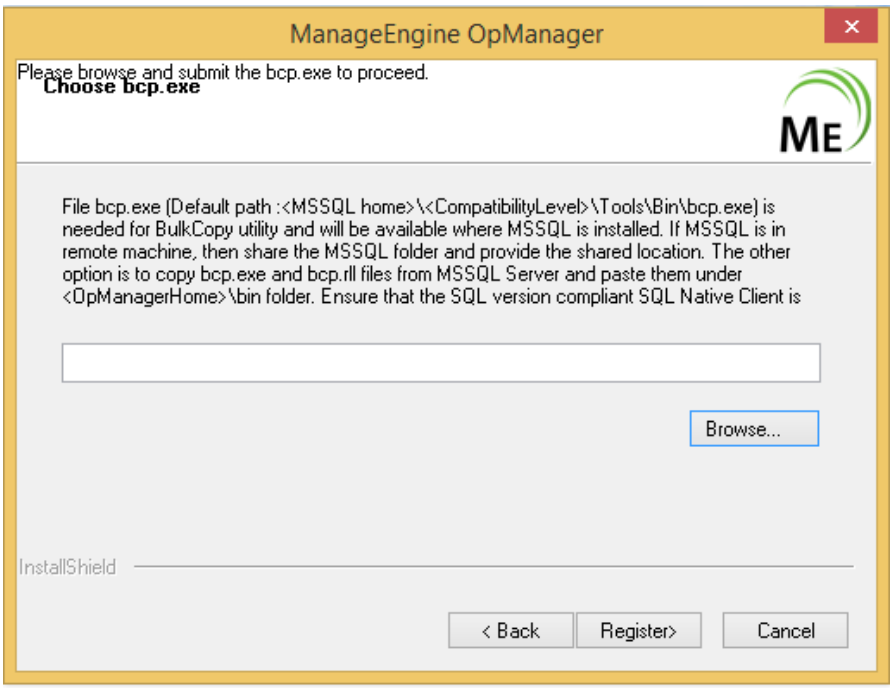
Step 9: If you select PGSQL, please proceed with Step 14. (or) If you select 'MSSQL' database (recommended for production). Click 'Next' to proceed



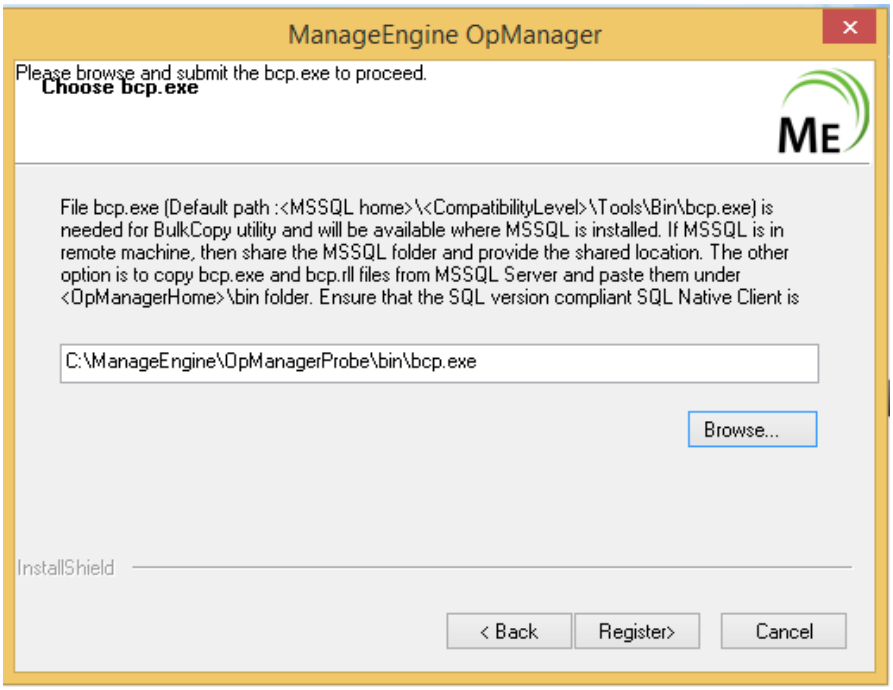
Step 10: Provide MSSQL details like host name, port, database name. Use the credentials (username and password) that was created earlier while configuring SQL. Click 'Next' to proceed



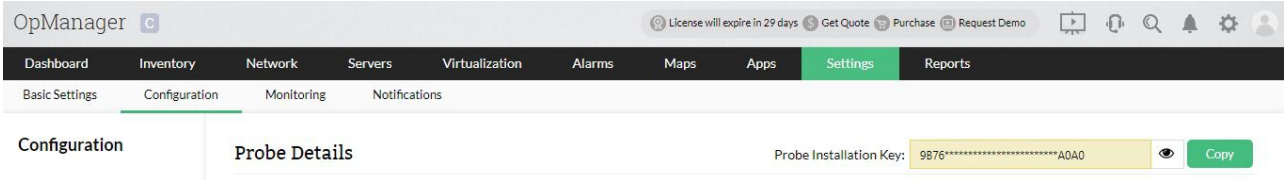
Step 11: Search for bcp.exe and bcp.rll in the MSSQL installation directory. Copy these files under \OpManagerCentral\bin directory. Click 'Next' to proceed



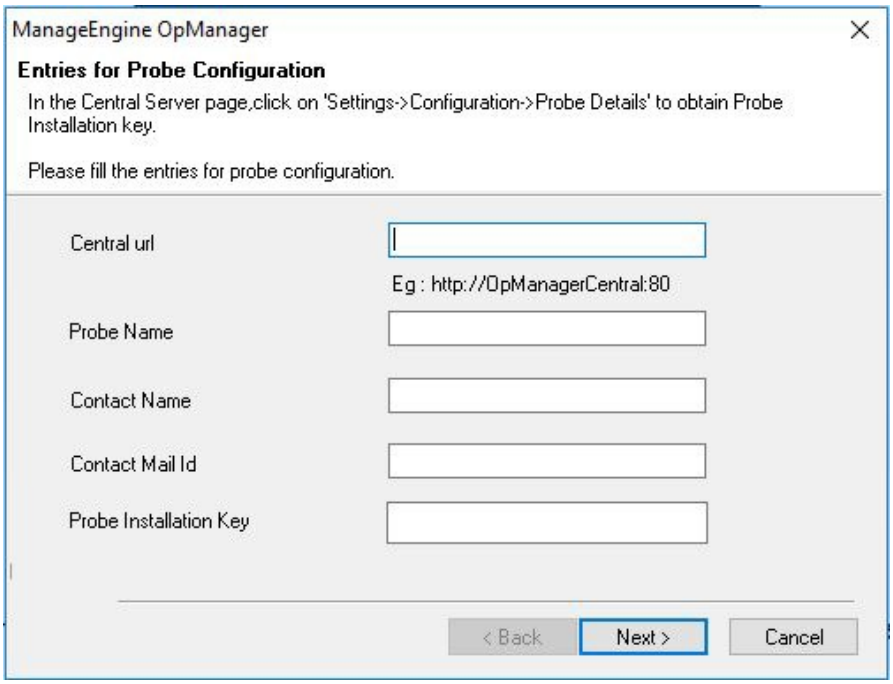
Step 12: Click on browse and select \OpManager\bin\bcp.exe. Click 'Next' to proceed

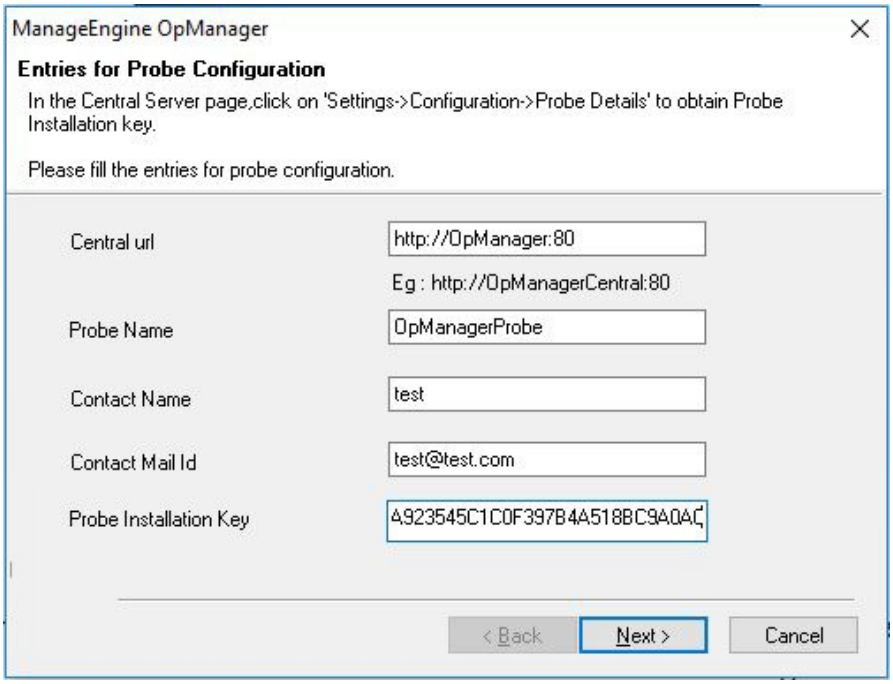


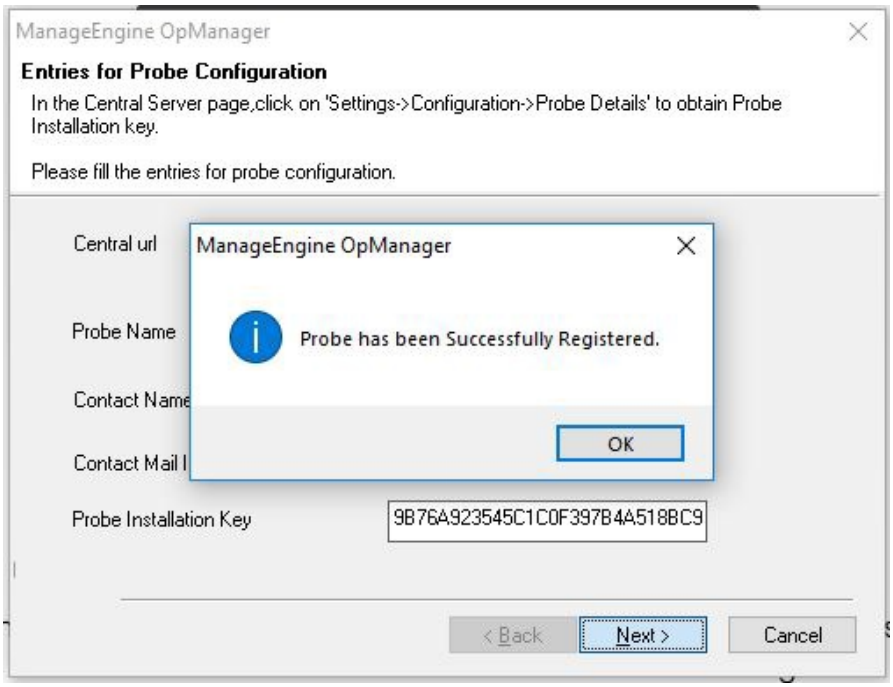
Step 13: Provide OpManager Central server details like central server URL, Probe Name, Contact Name and Contact Mail ID. Enter the Probe installation key. You can find the Probe Installation key in the Central Server page under Settings->Configuration->Probe Details.



Click 'Register' to proceed.


ManageEngine OpManager
Entries for Probe Configuration
In the Central Server page,click on 'Settings->Configuration->Probe Details' to obtain Probe Installation key.
Please fill the entries for probe configuration.
Central url
Eg : http://OpManagerCentral:80
Probe Name
Contact Name
Contact Mail Id
Probe Installation Key
< Back
Next >
Cancel


ManageEngine OpManager
Entries for Probe Configuration
In the Central Server page,click on 'Settings->Configuration->Probe Details' to obtain Probe Installation key.
Please fill the entries for probe configuration.
Central url
http://OpManager:80
Eg : http://OpManagerCentral:80
Probe Name
OpManagerProbe
Contact Name
test
Contact Mail Id
test@test.com
Probe Installation Key
4923545C1C0F397B4A518BC9A0AC
< Back
Next >
Cancel


ManageEngine OpManager
Entries for Probe Configuration
In the Central Server page,click on 'Settings->Configuration->Probe Details' to obtain Probe Installation key.
Please fill the entries for probe configuration.
Central url
Probe Name
Contact Name
Contact Mail I
Probe Installation Key
9B76A923545C1C0F397B4A518BC9
< Back
Next >
Cancel
ManageEngine OpManager
Probe has been Successfully Registered.
OK

Step 14: Click 'Finish' to complete OpManager Probe installation.

Installing OpManager Enterprise Edition on Linux

Prerequisites

1. Sometimes, you might encounter errors such as database connection not getting established or the server not starting up. To workaround these issues, comment the IPv6 related entries in the /etc/hosts file.
2. Check if the DNS resolves properly to the IP Address on the system in which OpManager is installed. Add an entry to /etc/host file with ipaddress and host name if there is trouble starting OpManager.

Central Server

Step 1: Download **ManageEngine_OpManager_Central_64bit.bin** for Linux.

Step 2: Login as root user.

Step 3: Assign the executable permission to the downloaded file using the following command: **chmod a+x ManageEngine_OpManager_Central_64bit.bin**

Step 4: Execute **./ManageEngine_OpManager_Central_64bit.bin** with administator privileges **(sudo).** This will display the installation wizard.

Step 5: Click 'Next' to begin the installation process. Go through the license agreement and proceed to the next step.

Step 6: In the subsequent steps of the wizard, select the OpManagerCentral language, the directory to install OpManagerCentral, and the port number to run OpManagerCentral Web Server. Proceed to the next step.

Step 7: Verify the installation details and click 'Next'.

Step 8: Click 'Finish' to complete the installation process.

Note: It is recommended to install OpManagerCentral in the opt folder. By default, OpManagerCentral is installed in the **/opt/ManageEngine/OpManagerCentral** directory.

Probe Server

Step 1: Download **ManageEngine_OpManager_Probe_64bit.bin** for Linux.

Step 2: Login as root user.

Step 3: Assign the executable permission to the downloaded file using the following command: **chmod a+x ManageEngine_OpManager_Probe_64bit.bin**

Step 4; Execute **./ManageEngine_OpManager_Probe_64bit.bin** with administator privileges **(sudo).** This will display the installation wizard.

Step 5: Click 'Next' to begin the installation process. Go through the license agreement and proceed to the next step.

Step 6: In the subsequent steps of the wizard, select the OpManagerProbe language, the directory to install OpManagerProbe, and the port number to run the OpManagerProbe Web Server. Proceed to the next step.

Step 7: Please enter the Central URL, Probe Name, Probe Installation Key, Username, Email ID and proceed to register the Probe.

Step 8: Verify the installation details and click 'Next'.

Step 9: Click 'Finish' to complete the installation process.

Note: It is recommended to install OpManagerProbe in the opt folder. By default, OpManagerProbe is installed in the **/opt/ManageEngine/OpManagerProbe** directory.

Installing OpManager Enterprise Edition on Linux using Console mode/ Silent mode

Prerequisites

To begin with, make sure you have downloaded the binary for Central and Probe for Linux OS.

Click here to download the binary files for OpManager Central and Probe (Linux OS).

Central Server

Step 1: Execute ManageEngine_OpManager_Central_64bit.bin with administrator privileges (sudo) and **-i console** option.

```
root@opm-u14-64-1:/opt/Naveen/Central# sudo ./ManageEngine_OpManager_Central_64bit.bin -i console
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...

===============================================================================
ManageEngine OpManager Central                  (created with InstallAnywhere)
-------------------------------------------------------------------------------

Preparing CONSOLE Mode Installation...
```

Step 2: Go through the license agreement and enter 'Y' to proceed. You can register for technical support by providing the required details. (Name, E-mail ID, Phone, Company Name)

Step 3: Select the location.

Step 4: Choose the installation directory

```
===============================================================================
Choose Install Directory
------------------------

Space recommended on drive : 10GB

  Default Install Folder: /opt/ManageEngine/OpManagerCentral

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
      : /opt/Naveen/Central

INSTALL FOLDER IS: /opt/Naveen/Central
   IS THIS CORRECT? (Y/N): Y



===============================================================================
```

Step 5: Configure the Webserver Port

```
===============================================================================
Webserver port
--------------

OpManager occupies port 8060 to run the web server. If you want to run it on a
 different port, specify the same here.

Enter the Web Server Port Number (Default: 8060):
```

Step 6: Verify the installation details and press 'Enter' to complete the installation

```
===============================================================================
Pre-Installation Summary
------------------------

Please review the following before continuing:

Product Name:
    ManageEngine OpManager Central

Install Folder:
    /opt/Naveen/Central/OpManagerCentral

Disk Space Information (for Installation Target):
    Required:  554.83 MegaBytes
    Available: 12,170.45 MegaBytes

PRESS <ENTER> TO CONTINUE:



===============================================================================
Installing...
-------------

 [==================|==================|==================|==================]
 [------------------|------------------|------------------|------------------]



===============================================================================
Installation Completed
----------------------

Congratulations! ManageEngine OpManager Central has been successfully
installed to:

/opt/Naveen/Central/OpManagerCentral

Readme file is available at /opt/Naveen/Central/OpManagerCentral/README.html

Technical support : http://support.opmanager.com

root@opm-u14-64-1:/opt/Naveen/Central#
```

Probe Server

Step 1: Execute ManageEngine_OpManager_Probe_64bit.bin with security privileges (sudo) and **-i console** option.

```
root@opm-u14-64-1:/opt/Naveen/Probe# sudo ./ManageEngine_OpManager_Probe_64bit.bin -i console
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...

===============================================================================
ManageEngine OpManager Probe                    (created with InstallAnywhere)
-------------------------------------------------------------------------------

Preparing CONSOLE Mode Installation...
```

Step 2: Go through the license agreement and enter 'Y' to proceed. You can register for technical support by providing the required details. (Name, E-mail ID, Phone, Company Name)

```
DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N): Y



===============================================================================
ManageEngine OpManager Probe
----------------------------


Do you want to register for technical support?(Y/N) (Default: Y): Y




===============================================================================
Registration for Technical support
----------------------------------

Name: OpManager Support


Phone Number: +1-888-720-9500


Email-Id: opmanager-support@manageengine.com


Company Name: Zoho Corporation
```

Step 3: Select the location.

```
  237- United Arab Emirates
  238- United Kingdom
  239- US Virgin Islands
  240- United States
  241- United States Minor Outlying Islands
  242- Uruguay
  243- Uzbekistan
  244- Vanuatu
  245- Venezuela
  246- Vietnam
  247- Wallis and Futuna
  248- Western Sahara
  249- Yemen
  250- Zambia
  251- Zimbabwe

Select Country to continue: 105

 Choose options

 Our Privacy Policy :  https://www.manageengine.com/privacy.html


  ->1- Next
    2- Skip
    3- Cancel
    4- Back

Select option to continue: 1
```

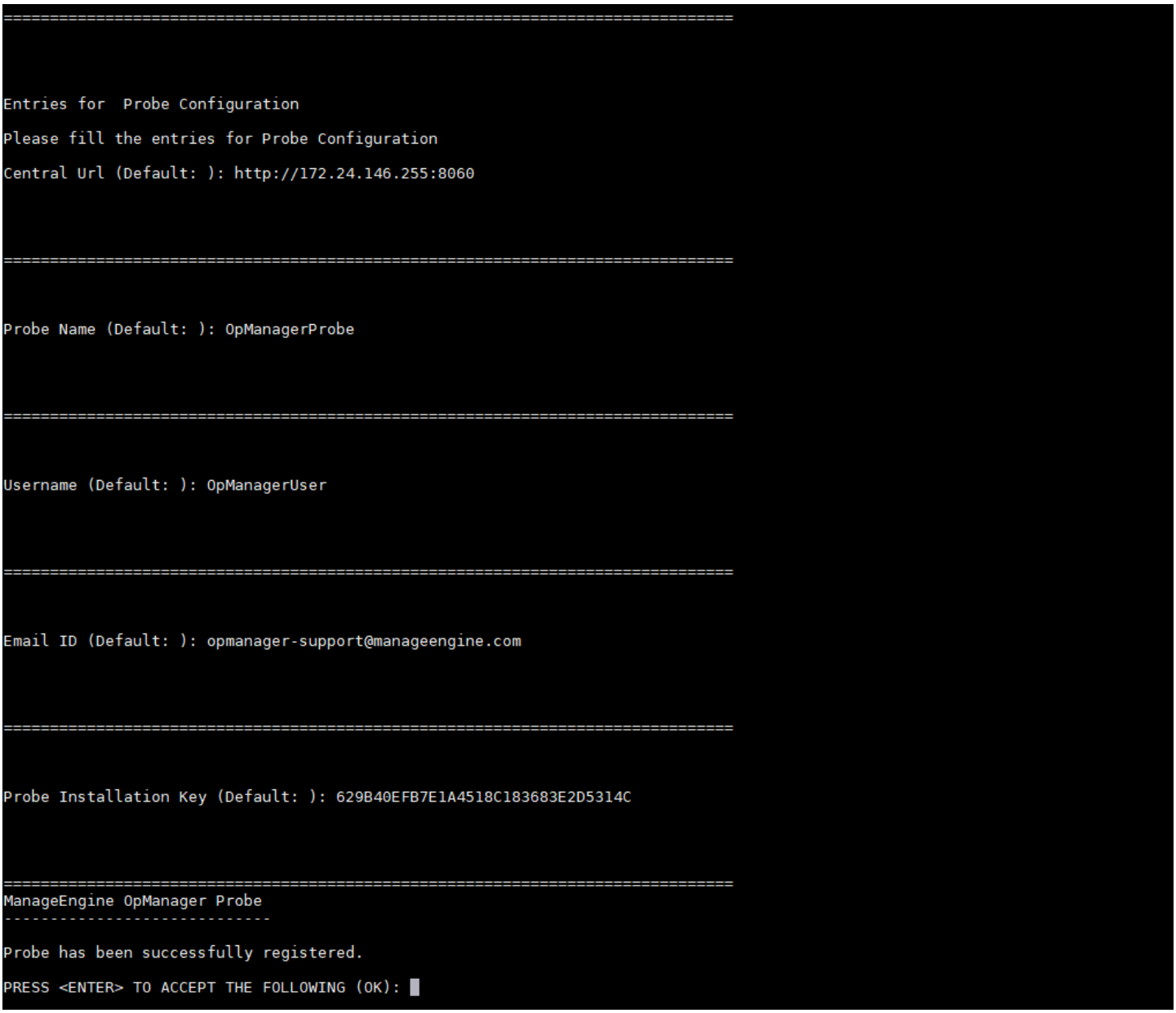
Step 4: Choose the installation directory and configure the Webserver Port.

```
===============================================================================
Choose Install Directory
------------------------

Space recommended on drive : 10GB

  Default Install Folder: /opt/ManageEngine/OpManagerProbe

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
      : /opt/Naveen/Probe

INSTALL FOLDER IS: /opt/Naveen/Probe
   IS THIS CORRECT? (Y/N): Y



===============================================================================




===============================================================================
Webserver port
--------------


Enter the Web Server port number (Default: 8060): 8080



===============================================================================
```

Step 5: Verify the installation details and the installation status.

```
===============================================================================
Pre-Installation Summary
------------------------

Please review the following before continuing:

Product Name:
    ManageEngine OpManager Probe

Install Folder:
    /opt/Naveen/Probe/OpManagerProbe

Disk Space Information (for Installation Target):
    Required:  555.01 MegaBytes
    Available: 10,731.68 MegaBytes

PRESS <ENTER> TO CONTINUE:



===============================================================================
Ready To Install
----------------

InstallAnywhere is now ready to install ManageEngine OpManager Probe onto your
system at the following location:

 /opt/Naveen/Probe/OpManagerProbe

PRESS <ENTER> TO INSTALL:



===============================================================================
Installing...
-------------

 [==================|==================|==================|==================]
 [------------------|------------------|------------------|------------------]



===============================================================================
```

Step 6: Configure the Probe details and press 'Enter' to complete the installation.



Starting OpManager Enterprise Edition on Linux

- Go to **/OpManager/bin** folder
- Execute: **sh run.sh**
- To run OpManager server in the background, execute: **nohup sh run.sh&**

MSSQL Server Configuration for OpManager

If you choose to use MSSQL as the backend database for OpManager, we recommend that you create a seperate account for OpManager in your MSSQL database server. This ensures proper functionality. However, if you wish to proceed with your existing server account credentials, you may skip this configuration procedure and proceed directly with the installation.

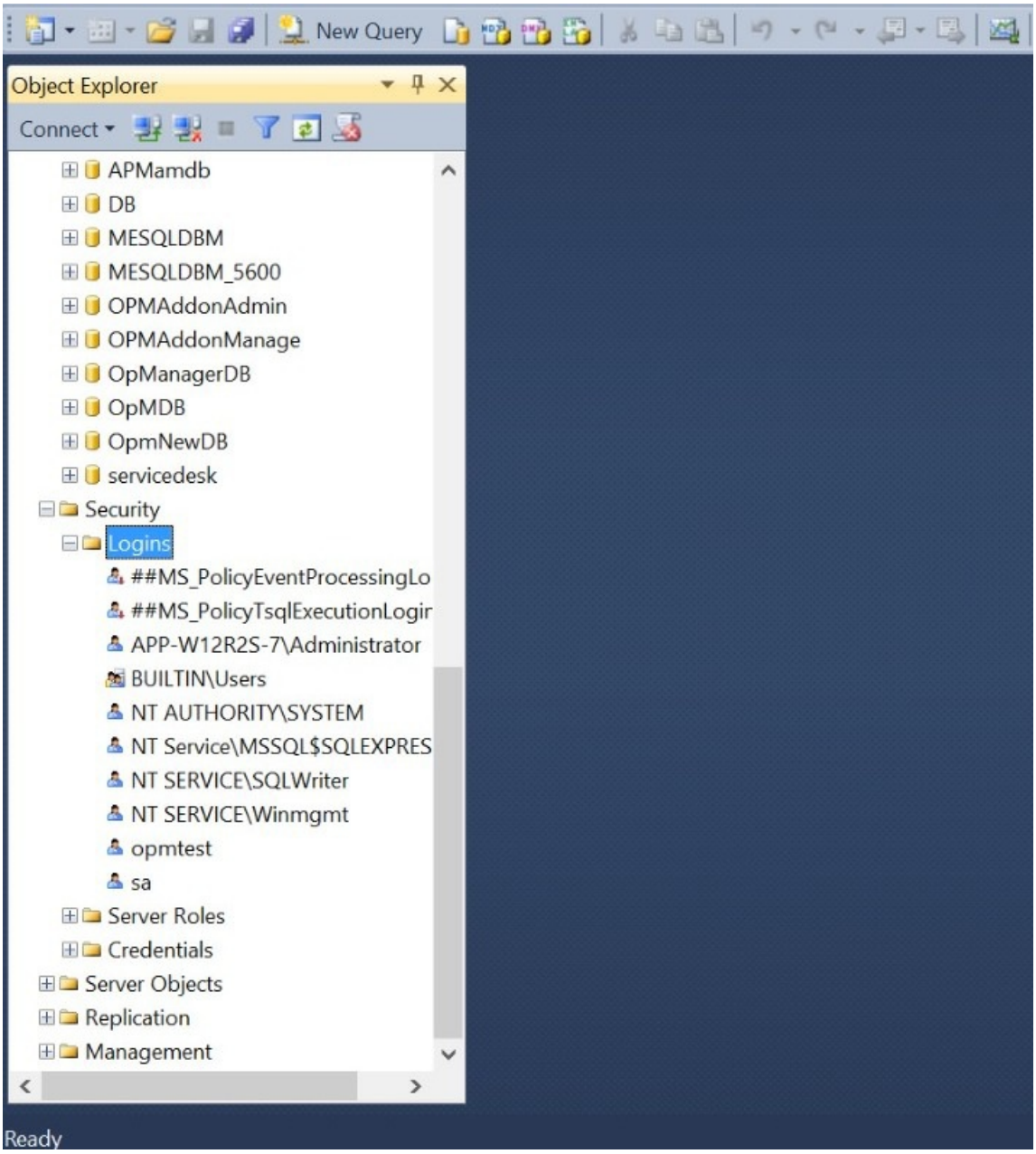
Supported Versions: SQL 2017 | SQL 2016 | SQL 2014 | SQL 2012 | SQL 2008

Note: It is highly recommended that you use MSSQL database for production. This also provides failover/high availability.

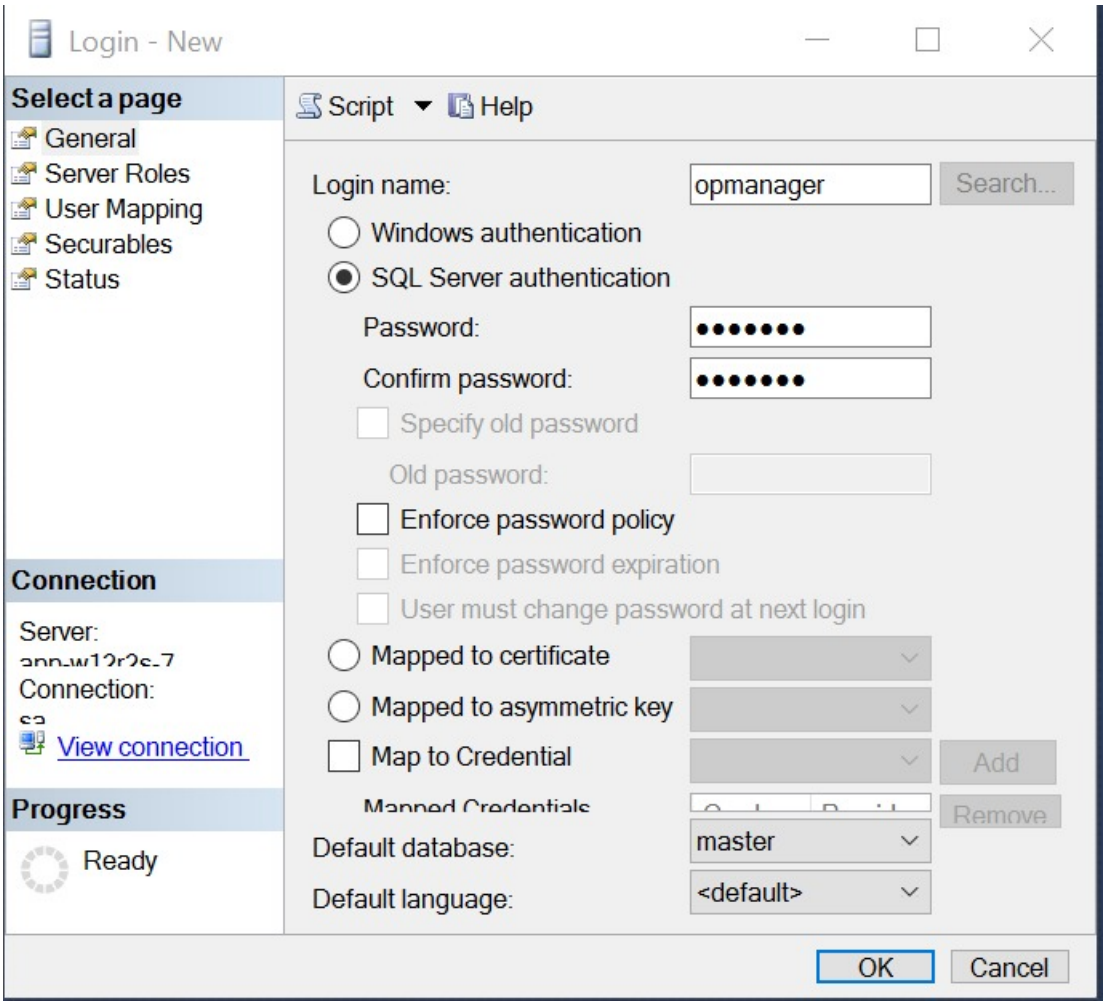
Steps to configure MSSQL

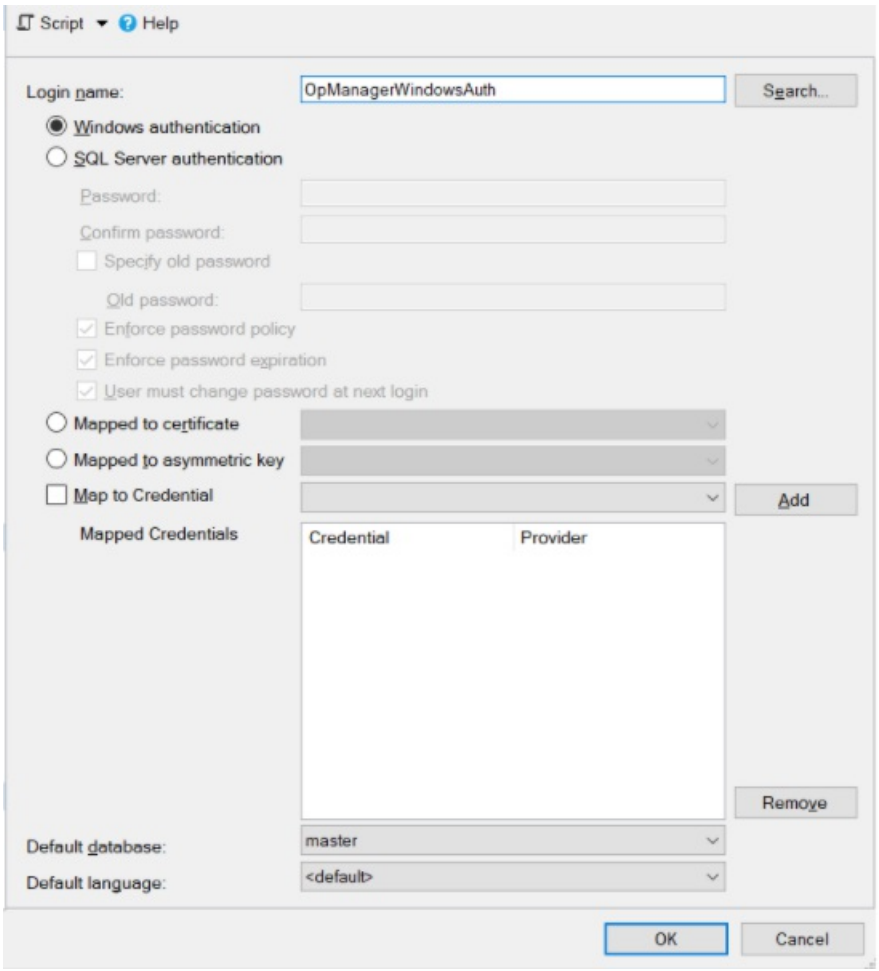
Step 1: To ensure proper communication between the MSSQL database server and OpManager, a new account has to be created with the below mentioned steps.

- Open SQL Management Studio and login using your Server Account (sa)/ Windows credentials.
- Right click on Logins
- Select New Login

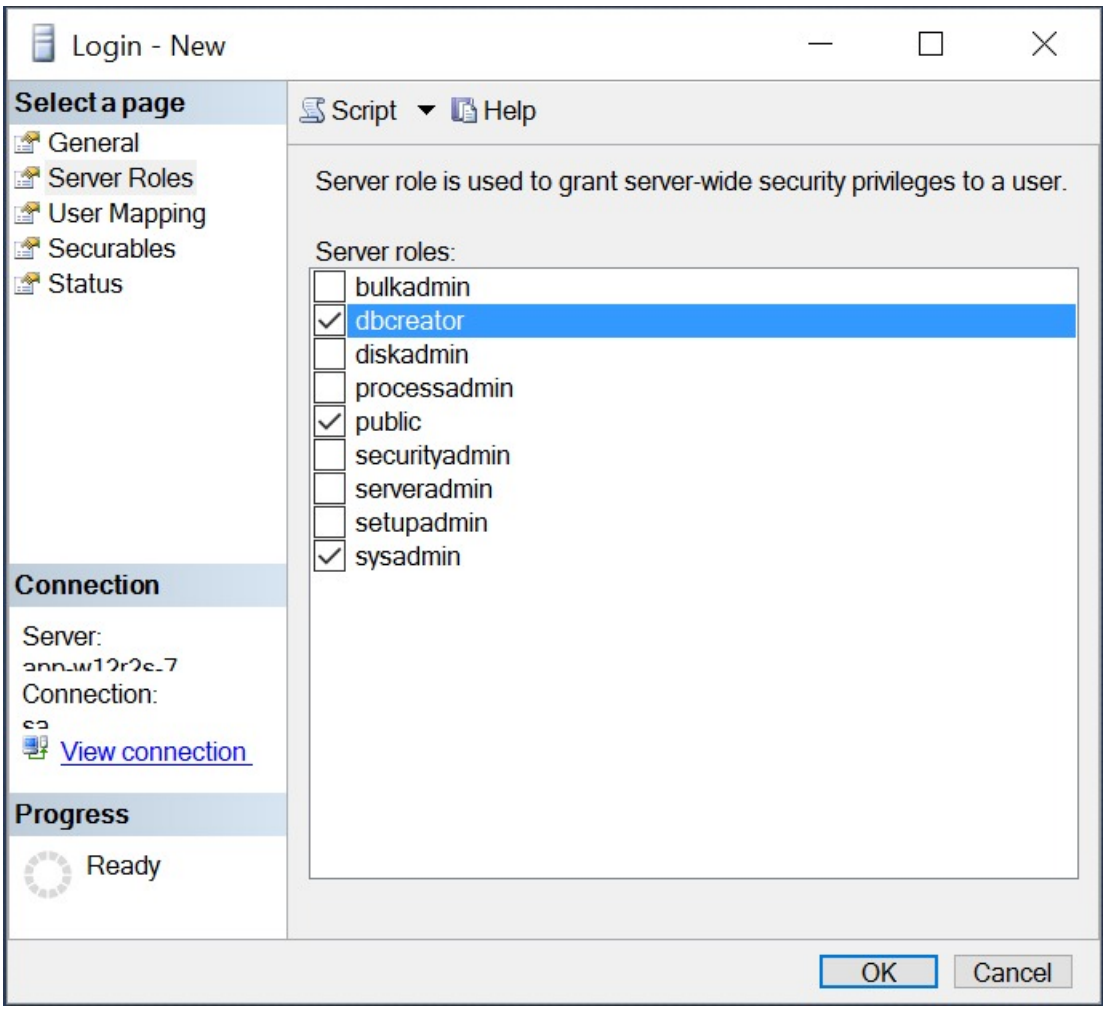


Step 2: Select Authentication type. For Windows authentication, select and login using your Windows login credentials. For SQL Server Authentication, enter the password. Then proceed with Step 3.

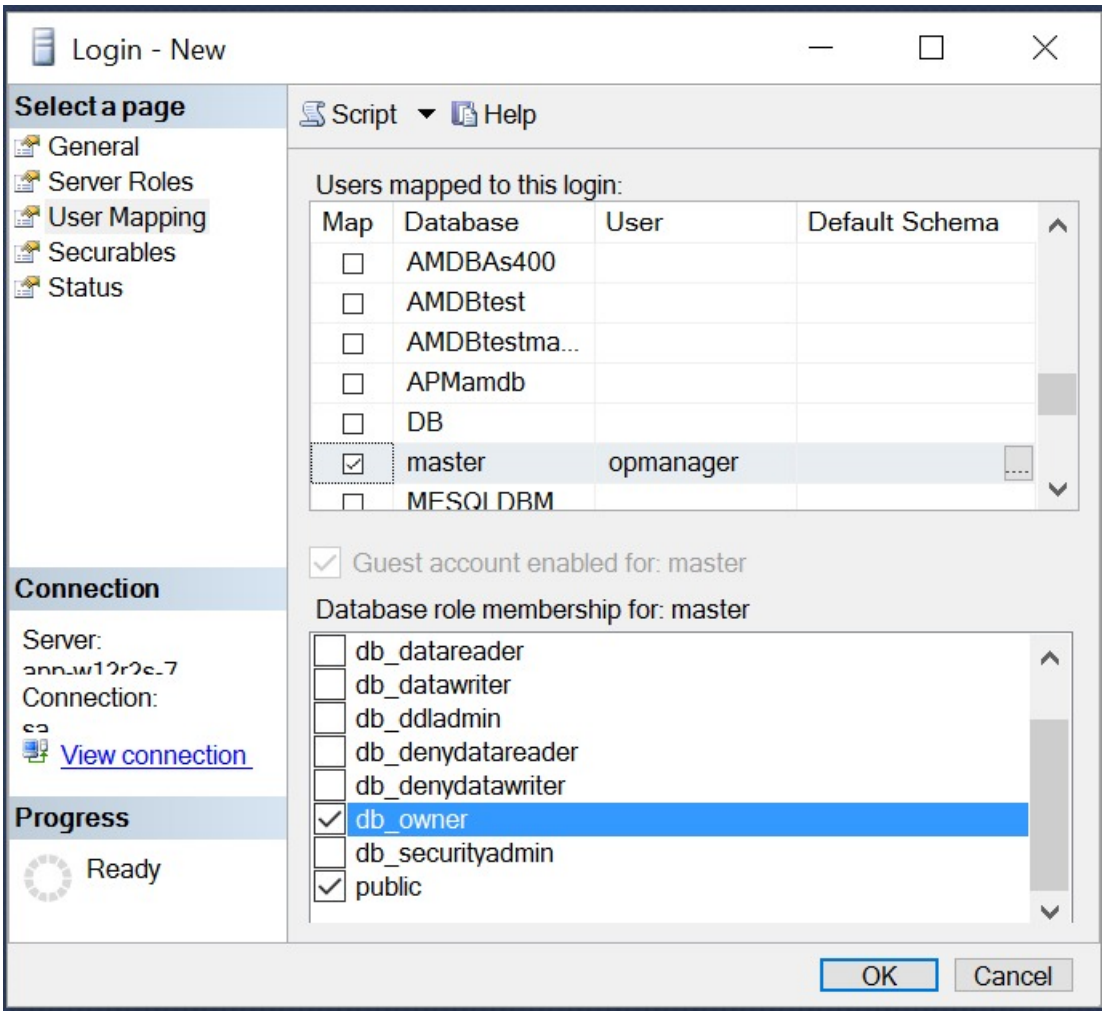




Step 3: Click on Server Role. Select Server Roles "dbcreator", "public" and "sysadmin"



Step 4: Click on User Mapping. Map this login to "master" with database role ownership as "db_owner" and "public". Click OK.



Scalability recommendations

Interface count

We recommend monitoring up to 10000 interfaces in a single installation. If the count exceeds 10000, it will be efficient to increase the monitoring interval of those interfaces. Adding more interfaces will directly impact the overall performance of the product.

Note:

1. Interfaces that have no data collection for the last 30 days will be automatically unmanaged and marked as 'Idle Interfaces' under the interfaces Inventory page.
2. You can avoid the addition of unnecessary interfaces by choosing appropriate criteria and conditions in the interface Discovery page.

VLAN count

To avoid any hindrance in the performance of the product, OpManager limits the count of VLANs discovered to a maximum of 3000. New VLANs will not be allowed to be discovered in OpManager post the specified limit.

Trap processing limit

To avoid any performance degradation in OpManager, the number of traps to be processed per hour is limited to a maximum of 50,000. If this threshold is breached, OpManager stops processing traps for a temporary period.

Recommendations for Availability and Performance monitors

Based on the monitor type/protocol being used with the performance monitor, these are the maximum advisable number of monitors for a single installation:

Protocol/Monitor type	Max Number of Monitors Per Installation
Device Availability Monitoring	1000
SNMP	5000
WMI (including Application Monitors)	4000
CLI	2500
VMware	10000
HyperV	5000
Xen	5000

Overall, the maximum number of monitors per installation is 20000.

Note: Adding more monitors than the numbers suggested above will directly impact the performance of OpManager. If it is required to add more monitor than this, then the polling interval of that monitor must be increased accordingly in order to balance the load on the OpManager server.

For more information on the same, please feel free to contact our support team at opmanager-support@manageengine.com.

OpManager Enterprise Edition - A guide to migration and backup

Learn how to migrate your database, about backup & restore, and the steps to enable HTTPS in OpManager version 12300 and above.

When should you migrate?

- When hardware, server OS, or SQL requirements have been changed.
- When you need new servers for space and better performance.
- If you need to migrate products to a dedicated server.
- When adding a new database or new server type.

Migrating Central and Probe from one server to another server

For PostgreSQL

Steps to migrate Central from one server to another:

1. Stop OpManagerCentral service. Execute '***OpManagerService.bat -r***' under the OpManagerCentral/bin directory to remove the OpManagerCentral service in the existing machine.
2. Take a compressed backup of the entire OpManagerCentral folder.
3. Extract the folder to the new system where Central is about to be installed.
4. Open command prompt with administrator privileges in the machine where the Central needs to be installed.
5. Go to the OpManagerCentral/bin directory in the new machine and execute ***'initPgsql.bat'*** to give access permission for the database from the new server.
6. In the same command prompt, execute ***'OpManagerService.bat -i'*** to add OpManagerCentral as a service.
7. Start OpManagerCentral from Windows services in the new machine.
8. To update Central details for the new machine:
   a. If the new system's IP address or host name differs from that of the existing machine, go to ***"OpManagerProbe/conf/OpManager"*** directory, locate **"NOCServerDetail.xml**  **?** file and update the ***"NOCServerName"*** attribute value with the new server name.
   2. If the IP address and host name of the new machine is the same as that of the existing machine, the ***'NOCServerName'*** need not be updated.
9. From version 12.4.042, update the Central Details in the Central Details page under Settings-->Configuration.
10. Restart all the probes.
11. To clean up the existing machine, uninstall OpManagerCentral.

Steps to migrate Probe from one server to another:

1. Stop OpManagerProbe service. Execute ***'OpManagerService.bat -r'*** under the OpManagerProbe/bin directory to remove the OpManagerProbe service in the existing machine.
2. Take a compressed backup of the entire OpManagerProbe folder.
3. Extract the folder to the new system where the probe is about to be installed.
4. Open command prompt with administrator privileges in the machine where Probe needs to be installed.
5. Go to the OpManagerProbe/bin directory in the new machine and execute ***'initPgsql.bat'*** to give access permission for the database from the new server.
6. In the same command prompt, execute ***'OpManagerService.bat -i'*** to add OpManagerProbe as a service.
7. Start OpManagerProbe from Windows services in the new machine
8. To update probe details for the new machine:
    1. If the new system's IP address or host name differs from that of the existing machine, go to **Settings** --> **Configuration** --> **Probe Details.** Click on the probe name to modify the probe and update NAT Name detail for the probe which has been moved.
    2. If the IP address and host name of the new machine is the same as that of the existing machine, the **NAT name** need not be updated.
9. To clean up the existing machine, uninstall OpManagerProbe.

For MSSQL:

Case 1: To move only the installation without moving the database.

Case 2: To move both the database and the installed machine.

Case 1: To move only the installation without moving the database

In Central:

1. Stop OpManagerCentral Service. Execute ***'OpManagerService.bat -r'*** under the ***OpManagerCentral/bin*** directory to remove the OpManagerCentral service in the existing machine.
2. Take a compressed backup of the entire OpManagerCentral folder.
3. Extract the folder to the new system where the Central is about to be installed.
4. If you want to use the same database, continue without any changes. Please ensure that the database server is reachable in the new machine.
5. To update Central details for the new machine:
    1. If the new system's IP address or host name differs from that of the existing machine, go to ***"OpManagerProbe/conf/OpManager"*** directory, locate ***"NOCServerDetail.xml"*** file and update the ***"NOCServerName"*** attribute value with the new server name.
    2. If the IP address and host name of the new machine is the same as that of the existing machine, the ***'NOCServerName'*** need not be updated.
6. Restart all the probes.
7. To clean up the existing machine, uninstall OpManagerCentral.

In Probe:

1. Stop OpManagerProbe Service. Execute ***'OpManagerService.bat -r'*** under the ***OpManagerProbe/bin*** directory to remove the OpManagerProbe service in the existing machine.
2. Take a compressed backup of the entire OpManagerProbe folder.
3. Extract the folder to the new system where the Probe is about to be installed.
4. If you want to use the same database, continue without any changes. Please ensure that the database server is reachable in the new machine.
5. To update probe details for the new machine:

1. If the new system's IP address or host name differs from that of the existing machine, go to **Settings** --> **Configuration** --> **Probe Details.** Click on the probe name to modify the probe and update NAT Name detail for the probe which has been moved.
2. If the IP address and host name of the new machine is the same as that of the existing machine, the **NAT name** need not be updated.

5. Start OpManagerProbe from Windows services in the new machine.
7. To clean up the existing machine, uninstall OpManagerProbe.

Case 2: To move both the database and the installed machine

It is not recommended to move the database from one Server Studio to another. Contact opmanager-support@manageengine.com for further assistance.

Data Backup and Restoration

Moving installation from one server to another using backup and restore

Steps to migrate Central : (from version 124042 and above)

1. Stop the OpManagerCentral service and take a backup using the steps given in this page.
2. Stop all the probes to avoid loss of data.
3. Do a new, clean installation of Central in the required server.
4. Follow the steps given in this page to restore the data.
5. Start OpManagerCentral.
5. To update Central details for the new machine:
7. If the new system's IP address or host name differs from that of the existing machine, go to ***Settings--> Configuration --> Central*** in each probe and update the new Central system's IP address or host name.
3. If the IP address and host name of the new machine is the same as that of the existing machine, the host name of the Central server need not be updated in the Probes.
9. To clean up the existing machine, uninstall OpManagerCentral.

Steps to migrate Central : (till version 124041)

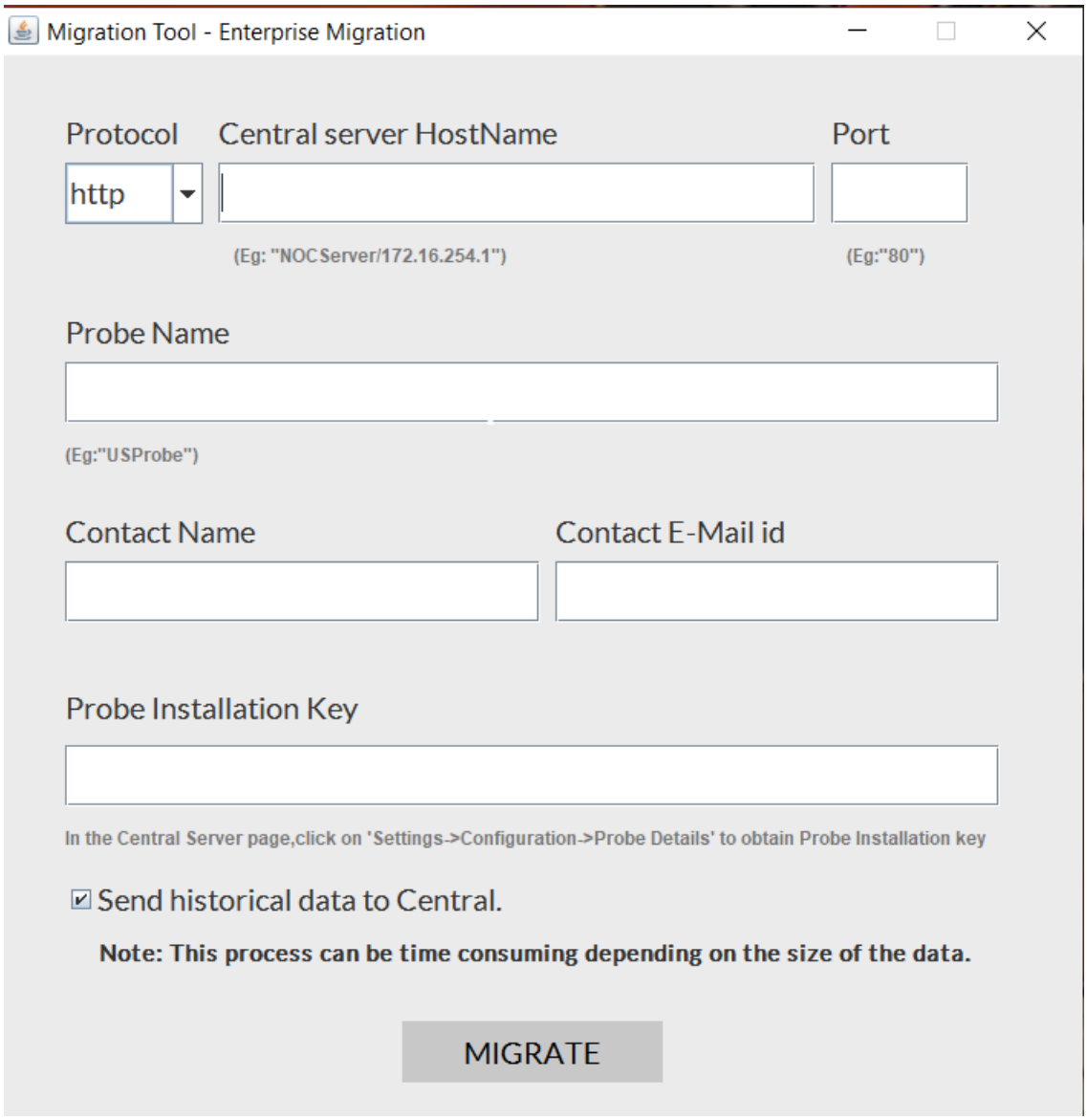
1. Stop the OpManagerCentral service and take a backup using the steps given in this page.
2. Stop all the probes to avoid loss of data.
3. Do a new, clean installation of Central in the required server.
4. Follow the steps given in this page to restore the data.
5. Start OpManagerCentral.
5. To update Central details for the new machine:
7. If the new system's IP address or host name differs from that of the existing machine, go to ***OpManagerProbe/conf/OpManager*** directory and locate **"NOCServerDetail.xml"** file and update ***NOCServerName*** attribute value with new server name. in each probe and update the new Central system's IP address or host name.
3. If the IP address and host name of the new machine is the same as that of the existing machine, the **"NOCServerName"** need not be updated.
9. Restart all the probes.
0. To clean up the existing machine, uninstall OpManagerCentral.

Steps to migrate Probe:

1. Stop the OpManagerProbe service and take a backup using the steps given in this page.
2. Do a new, clean installation of the probe in the required server.
3. After the probe is installed successfully, start the service and check if the probe is communicating properly with the central.
4. Stop the newly installed probe.
5. Follow the steps given in this page to restore the data.
5. Start the OpManagerProbe.

7. In Central, go to **'Probe Details'** page and verify that the status of the old probe is displayed as **"Running"** and the status of new probe is displayed as **"Server Down"**.
8. Delete the new probe (*Do not delete the old probe*).
9. To update probe details for the new machine:
    1. If the new system's IP address or host name differs from that of the existing machine, go to**&#65533; Settings&#65533;** -->**&#65533; Configuration&#65533;** -->**&#65533; Probe Details**. Click on the probe name to modify the probe and update NAT Name detail for the probe which has been moved.
    2. If the IP address and host name of the new machine is the same as that of the existing machine, the NAT name need not be updated.
10. To clean up the existing machine, uninstall OpManagerProbe.

Migrating from OpManager Standard/Professional to OpManager Enterprise Edition



If you are upgrading to OpManager Enterprise Edition for reasons concerning scalability or remote network monitoring or both, you can migrate from OpManager Standard/Professional without having to start afresh. This means all the configuration and historical data in the existing OpManager installation can be safely ported to the enterprise edition during the migration.

Upon migration, the existing OpManager installation (Standard/Professional Edition) will function as a Probe server. The Central server has to be installed in a new machine.

To migrate to OpManager Enterprise Edition, follow the steps given below:(**For OpManager version 124181 and above**)

Step 1: Installing OpManager Central

Install the version of OpManagerCentral corresponding to the version of OpManager Standard/Professional Edition in a new machine.

1. OpManagerCentral can be downloaded from this link.
2. In the ***List of Products*** field, select **OpManager.**
3. In the ***Product Version*** field, enter the version corresponding to the existing OpManager Standard/Professional Edition and click on Submit.
4. In the new page, click on the required version (124181 and above) from the list.
5. Click on the required **OpManager_Central_64bit** file to download.

Step 2: Database Backup

Backup the existing OpManager Standard/Professional Edition database. To backup the database, follow the steps in this page.

Step 3: Migration

Migrating to OpManager Enterprise Edition can be done in two ways:

1. **User Interface** - Migrating with a step by step wizard
2. **Console Mode** - Migrating with Command Prompt. Console mode is chosen as default migration method if the UI is not supported.

1. Migration using User Interface:

- Go to the bin folder under OpManager installation directory.
  - **Windows OS:** Run the MigrateToEnterprise.bat file as administrator.
  - **Linux OS:** Run the **MigrateToEnterprise.sh** file as root user.
- The Migration Tool wizard appears.
- In the wizard, enter the corresponding **< *Central Server Name* >, < *Protocol* >, < *Port* >** and the **< *Probe Installation Key* >**.
- Enter the required **< *Probe Name* >, < *Contact Name* >** and **< *Contact E-mail id* >**.
- Click on **MIGRATE.**

2. Migration using Console mode:

- Go to the bin folder under OpManager installation directory.
  - **Windows OS:** Run the MigrateToEnterprise.bat file using ***-c*** as parameter.
  - **Linux OS:**  Run the MigrateToEnterprise.ssh file using ***-c*** as parameter.
- Enter the details in the below order.
  < *Central Protocol* >
  < *Central Name* >
  < *Central Port* >
  < *Probe Name* >
  < *Contact Name* >
  < *Email* >
  < *Probe Installation Key* >.

Historical data from probe servers can be sent to the Central server based on user preferences. However, the historical data will still be available in probe server.

The migration process is complete. Now the OpManager installation functions as a probe server and synchronizes data with the Central server.

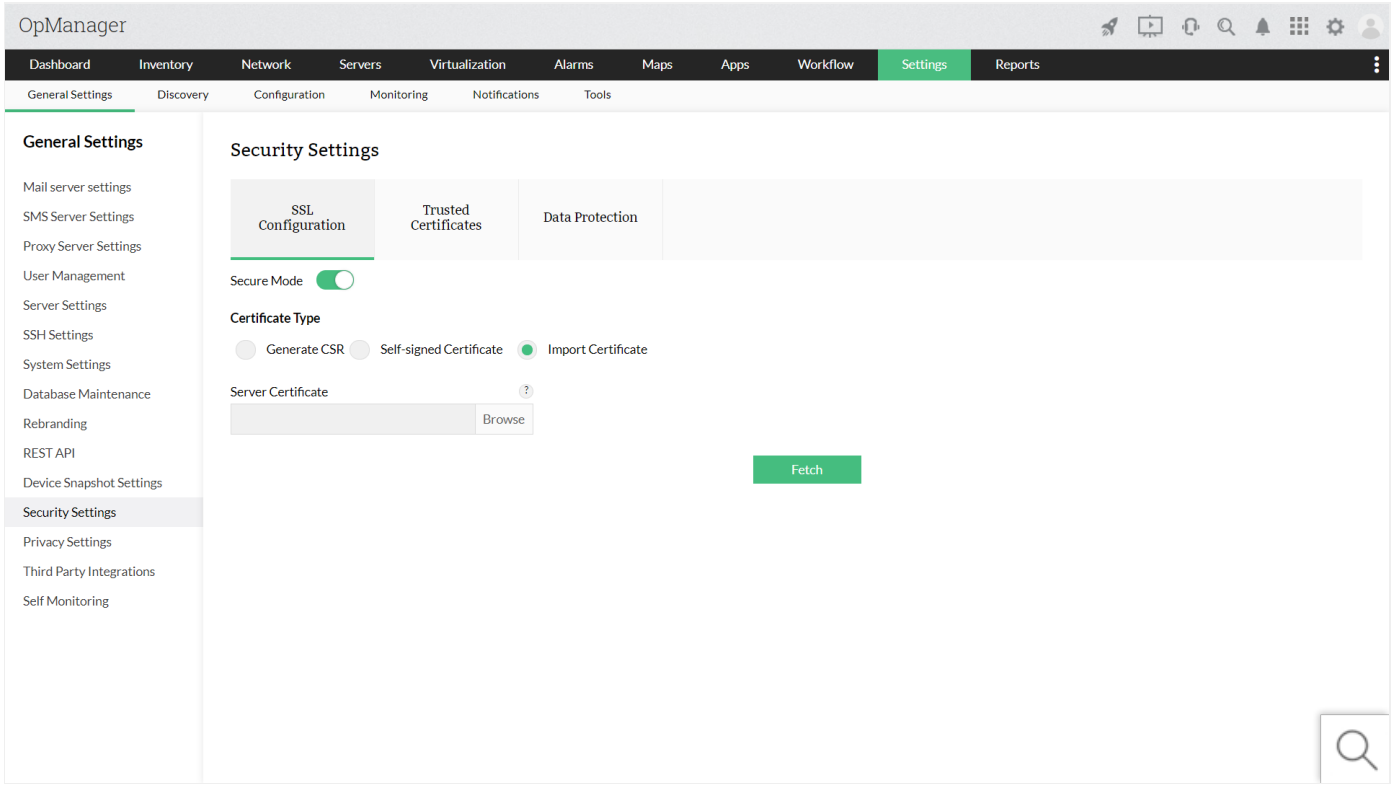
*** Points to note:**

- The OpManager Central version (to be downloaded) has to match with the existing OpManager version (Standard/Professional Edition) for successful migration.
- The OpManager version can be found by clicking on the User icon on the top right hand side of the existing OpManager installation.
- The Probe Installation Key can be found under **OpManagerCentral > Settings > Configuration > Probe Details.**
- **Historical data** - The past performance data collected by OpManager. Historical data is used for populating graphs, charts and generating reports.

Steps to Migrate OpManager Version 11600 LEE edition to Enterprise Edition

Contact opmanager-support@manageengine.com to migrate OpManager version 11600 LEE to OpManager Enterprise.

Enabling HTTPS in Central and Probe



Steps to enable HTTPS in OpManager : (for versions from 123181 till 124041)

1. In both, probe and Central, navigate to **Settings** --> General**&#65533;** **Settings** --> **Security Settings** --> **SSL Configuration** --> **Enable Secure Mode**.
2. For more details on configuring HTTPS, refer this page.
3. Restart Central service.
4. For all Probes edit **InitImpl&#65533;** attribute in**&#65533;** OpManagerProbe/conf/CommunicationInfo.xml**&#65533;** from com.me.opmanager.extranet.remote.communication.http.probe.HTTPProbeCommInit to com.me.opmanager.extranet.remote.communication.http.probe.HTTPProbeCommInit
5. Restart all the Probes.

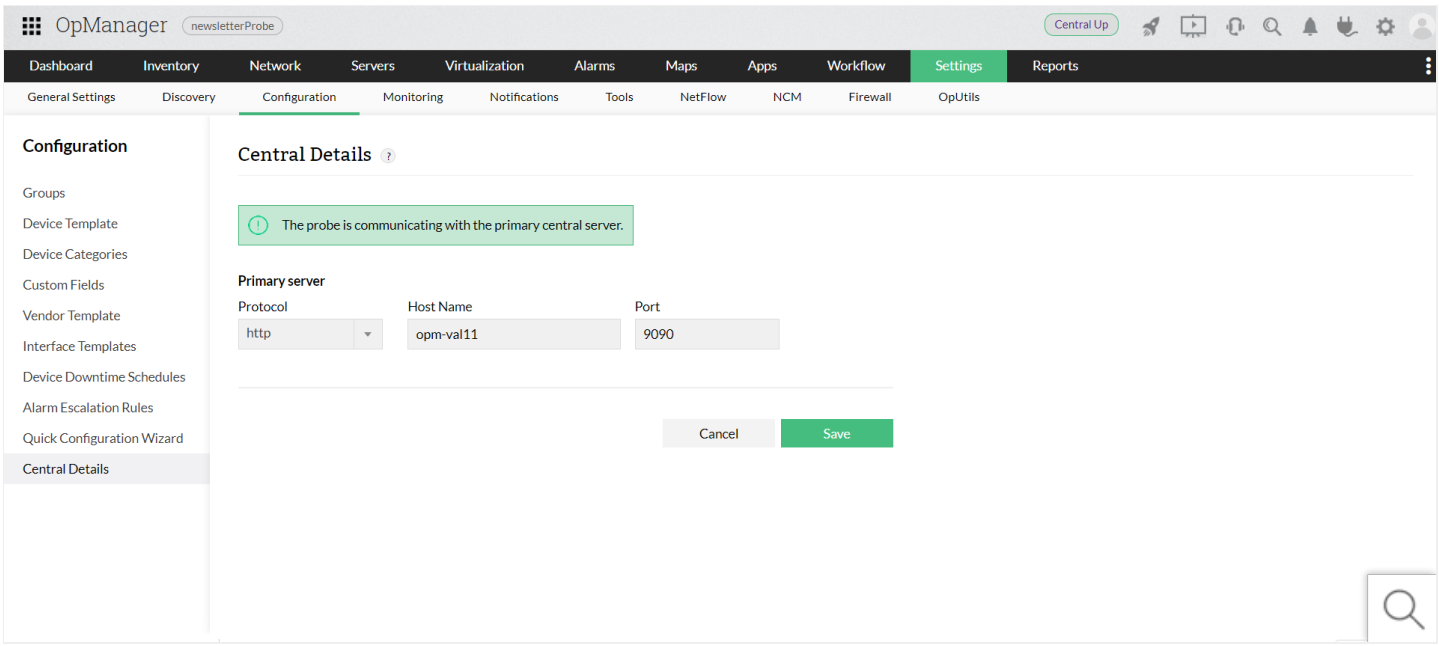
5. In Central, go to **Settings --> COnfiguration --> Probe Details --> Edit Each Probe** --> set **NAT Protocol** as **HTTPS**.

Steps to enable HTTPS in OpManager : (for version 124042 and above)

1. In both, probe and Central, navigate to **Settings** --> General **Settings** --> **Security Settings** --> **SSL Configuration** --> **Enable Secure Mode**.
2. For more details on configuring HTTPS, refer this page.
3. Restart Central service.
4. Then for each of the Probe, navigate to **Settings --> Configuration --> Central Details --> Protocol --> HTTPS**.

Changing Ports in Central & Probe

Prev Next



In Central : (till version 124041)

- Open Command prompt with administrator privileges and go to the ***OpManagerCentral/bin*** directory and execute ***ChangeWebServerPort.bat*** (eg : Change*WebServerPort.bat 443*).
- Restart OpManagerCental.
- For all probes go to **"OpManagerProbe/conf/OpManager"** directory and locate **"NOCServerDetail.xml"** file and update the ***"NOCServerPort"*** attribute value.
- Restart OpManagerCentral and then all Probes.

In Probe : (till version 124041)

- Open Command prompt with administrator privileges and go to the ***OpManagerProbe/bin*** directory and execute ***ChangeWebServerPort.bat*** (eg : *ChangeWebServerPort.bat 443*).
- Restart the Probe
- In Central, go to **Settings** --> **Configuration** --> **Probe Details** --> **Edit each Probe** -->**Update** new port in **NAT Port.**

In Central : (from version 124042 and above)

- Open Command prompt with administrator privileges and go to the ***OpManagerCentral/bin*** directory and execute ***ChangeWebServerPort.bat*** (eg : Change*WebServerPort.bat 443*).
- Restart OpManagerCental.
- Then open each Probe and navigate to**&#65533;** **Settings --> Configuration --> Central Details&#65533;** and specify the updated port number of the Central system.
  &#65533;

In Probe : (from version 124042 and above)

- Open Command prompt with administrator privileges and go to the ***OpManagerProbe/bin*** directory and execute ***ChangeWebServerPort.bat*** (eg : *ChangeWebServerPort.bat 443*).
- Restart the Probe
- In Central, go to **Settings** --> **Configuration** --> **Probe Details** and edit each Probe for which the port is changed.**&#65533;**
- Update it in **NAT Port.**

&#65533;

Starting OpManager

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.

- Starting OpManager on Windows
- Starting OpManager on Linux
- Connecting the Web Client

On Windows Machines

If you have chosen to install OpManager as Windows service, you will be prompted to start the service after successful installation. The Web Client is invoked automatically on installing as a Service. Enter the log-on details. The default user name and password is 'admin' and 'admin' respectively.

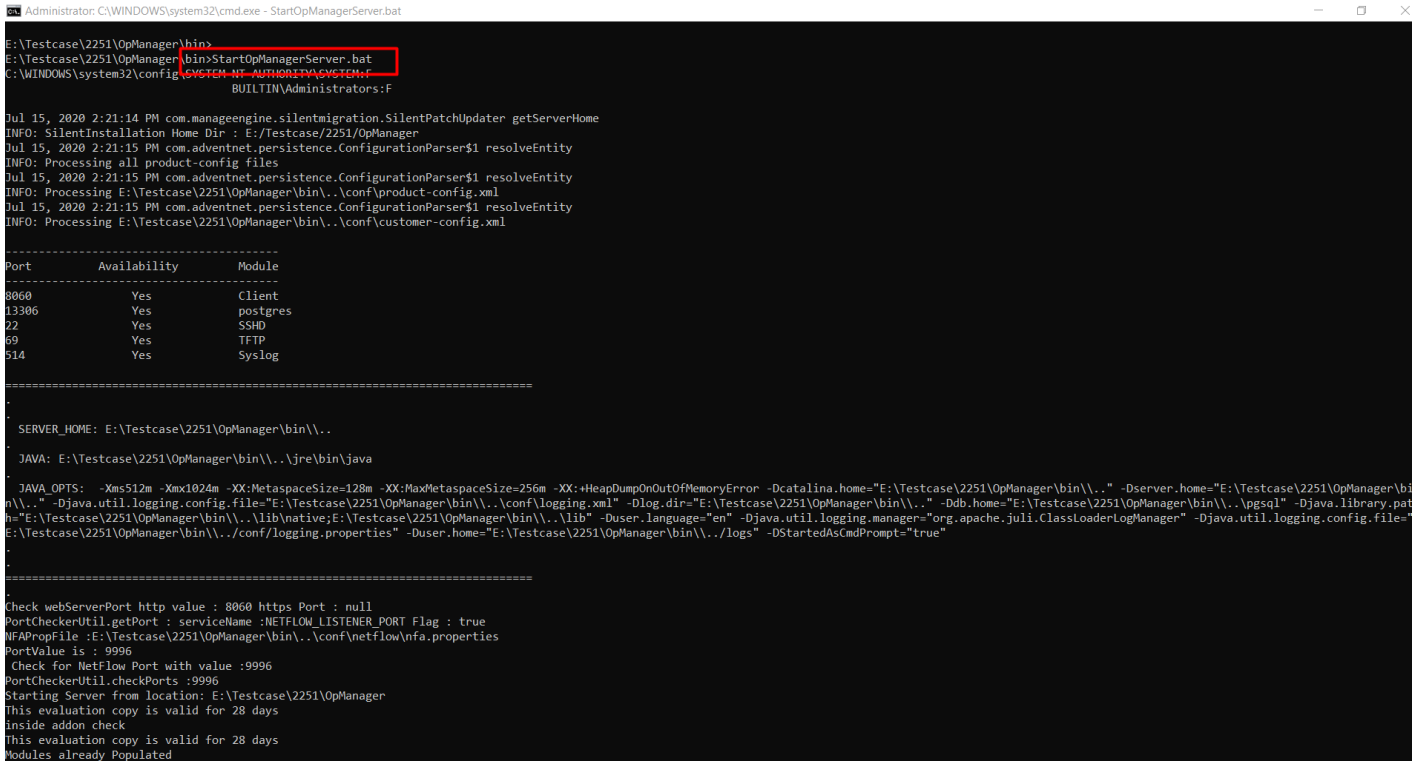
To later start OpManager as a Windows Service, follow the steps below:

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**.

Alternatively, you can choose to start OpManager as a Windows Service using **Command Prompt**:

1. Type "**cmd**" in the search bar and **run Command Prompt**. (Ensure that you are logged in as administrator)
2. Enter the **path** where OpManager is installed in your hard drive and access the **bin directory**.
3. Execute **StartOpManagerServer.bat** or **run.bat** files to start OpManager.
4. To stop OpManager, execute **StopOpManagerServer.bat.**



On Windows machines, an icon is 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.

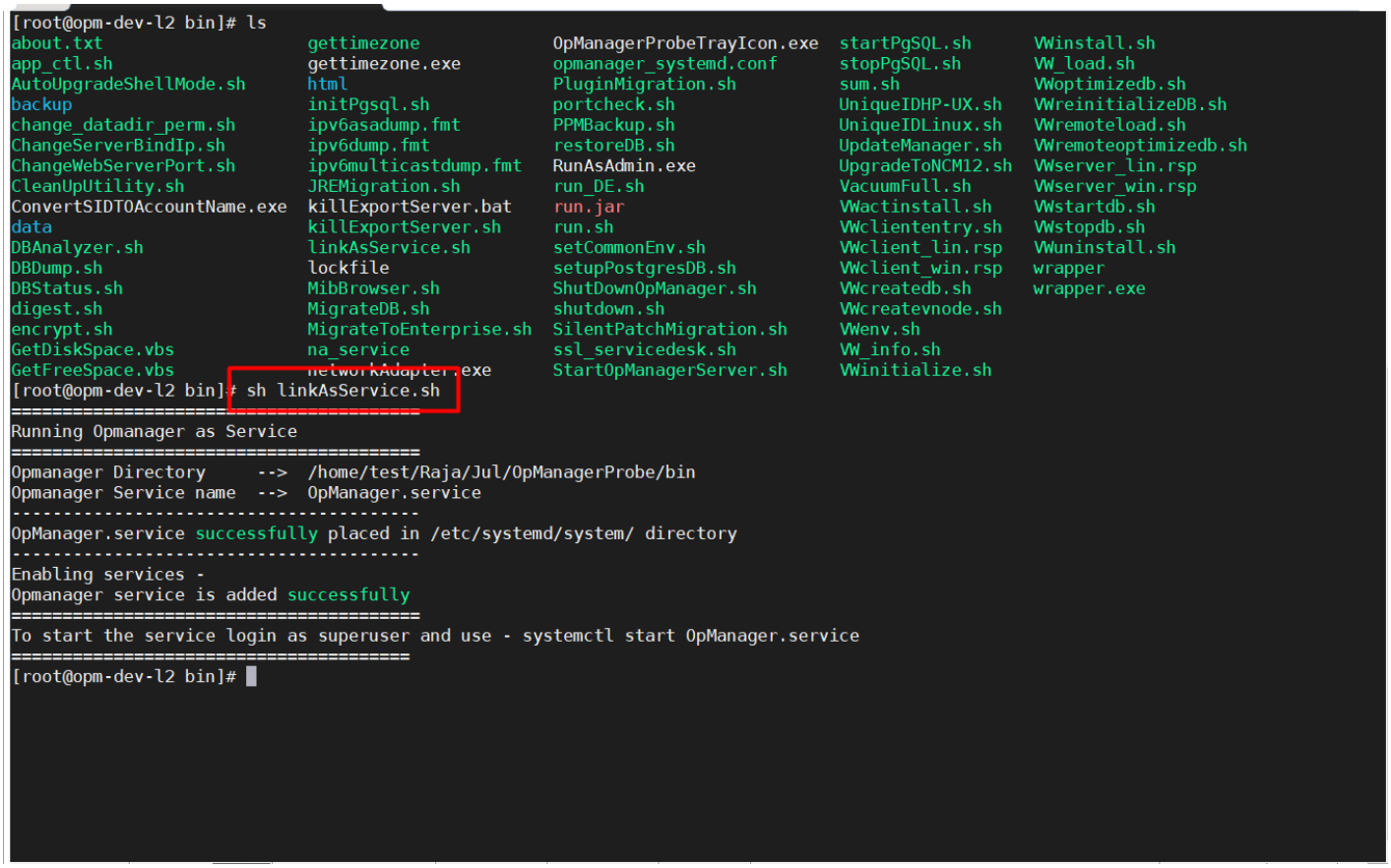
On Linux Machines

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

To stop OpManager running on a linux machine, execute the ShutDownOpManager.sh file present in the <OpManager Home>/bin directory.

Alternatively, you can choose to start OpManager as a service:

1. Open **Terminal** and log in as '**root**' user.
2. Access the **path** where OpManager is installed.
3. Execute the **linkAsService.sh** file present in the *<OpManager Home>/bin* directory by using the **sh linkAsService.sh** command.



4. Start OpManager by executing **systemctl start OpManager.service** or **/etc/init.d/OpManager.service start** files, depending on your OS version.

```
change_datadir_perm.sh        ipv6asadump.fmt          PPMBackup.sh               UniqueIDLinux.sh    VWremoteload.sh
ChangeServerBindIp.sh         ipv6dump.fmt             restoreDB.sh               UpdateManager.sh    VWremoteoptimizedb.sh
ChangeWebServerPort.sh        ipv6multicastdump.fmt    RunAsAdmin.exe             UpgradeToNCM12.sh   VWserver_lin.rsp
CleanUpUtility.sh             JREMigration.sh          run_DE.sh                  VacuumFull.sh       VWserver_win.rsp
ConvertSIDTOAccountName.exe   killExportServer.bat     run.jar                    VWactinstall.sh     VWstartdb.sh
data                          killExportServer.sh      run.sh                     VWcliententry.sh    VWstopdb.sh
DBAnalyzer.sh                 linkAsService.sh         setCommonEnv.sh            VWclient_lin.rsp    VWuninstall.sh
DBDump.sh                     lockfile                 setupPostgresDB.sh         VWclient_win.rsp    wrapper
DBStatus.sh                   MibBrowser.sh            ShutDownOpManager.sh       VWcreatedb.sh       wrapper.exe
digest.sh                     MigrateDB.sh             shutdown.sh                VWcreatevnode.sh
encrypt.sh                    MigrateToEnterprise.sh   SilentPatchMigration.sh    VWenv.sh
GetDiskSpace.vbs              na_service               ssl_servicedesk.sh         VW_info.sh
GetFreeSpace.vbs              networkAdapter.exe       StartOpManagerServer.sh    VWinitialize.sh
[root@opm-dev-l2 bin]# sh linkAsService.sh
=======================================
Running Opmanager as Service
=======================================
Opmanager Directory     -->  /home/test/Raja/Jul/OpManagerProbe/bin
Opmanager Service name  -->  OpManager.service
---------------------------------------
OpManager.service successfully placed in /etc/systemd/system/ directory
---------------------------------------
Enabling services -
Opmanager service is added successfully
=======================================
To start the service login as superuser and use - systemctl start OpManager.service
=======================================
[root@opm-dev-l2 bin]# systemctl start OpManager.service
[root@opm-dev-l2 bin]#
[root@opm-dev-l2 bin]# systemctl status OpManager.service
● OpManager.service - OpManager As Service
   Loaded: loaded (/etc/systemd/system/OpManager.service; enabled; vendor preset: disabled)
   Active: active (exited) since Fri 2020-07-10 17:18:42 IST; 4 days ago
 Main PID: 799 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/OpManager.service
           ├─915 ./wrapper ../conf/wrapper.conf wrapper.pidfile=.//OpManager.pid wrapper.daemonize=TRUE
           └─921 /home/test/abdul/6092769/OpManager/jre/bin/java -Dcatalina.home=.. -Dserver.home=.. -Dserver.stats=1000 -Djava.uti...

Jul 10 17:18:38 opm-dev-l2 systemd[1]: Starting OpManager As Service...
Jul 10 17:18:42 opm-dev-l2 systemd[1]: Started OpManager As Service.
[root@opm-dev-l2 bin]#
```

5. Check the status of OpManager by executing the **systemctl status OpManager.service** or **/etc/init.d/OpManager.service status** files.

```
---------------------------------------
OpManager.service successfully placed in /etc/systemd/system/ directory
---------------------------------------
Enabling services -
Opmanager service is added successfully
=======================================
To start the service login as superuser and use - systemctl start OpManager.service
=======================================
[root@opm-dev-l2 bin]# systemctl start OpManager.service
[root@opm-dev-l2 bin]#
[root@opm-dev-l2 bin]# systemctl status OpManager.service
● OpManager.service - OpManager As Service
   Loaded: loaded (/etc/systemd/system/OpManager.service; enabled; vendor preset: disabled)
   Active: active (exited) since Fri 2020-07-10 17:18:42 IST; 4 days ago
 Main PID: 799 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/OpManager.service
           ├─915 ./wrapper ../conf/wrapper.conf wrapper.pidfile=.//OpManager.pid wrapper.daemonize=TRUE
           └─921 /home/test/abdul/6092769/OpManager/jre/bin/java -Dcatalina.home=.. -Dserver.home=.. -Dserver.stats=1000 -Djava.uti...

Jul 10 17:18:38 opm-dev-l2 systemd[1]: Starting OpManager As Service...
Jul 10 17:18:42 opm-dev-l2 systemd[1]: Started OpManager As Service.
[root@opm-dev-l2 bin]#
[root@opm-dev-l2 bin]#
[root@opm-dev-l2 bin]#
[root@opm-dev-l2 bin]# systemctl stop OpManager.service
[root@opm-dev-l2 bin]#
[root@opm-dev-l2 bin]#
[root@opm-dev-l2 bin]# systemctl status OpManager.service
● OpManager.service - OpManager As Service
   Loaded: loaded (/etc/systemd/system/OpManager.service; enabled; vendor preset: disabled)
   Active: inactive (dead) since Wed 2020-07-15 14:38:42 IST; 9s ago
  Process: 14926 ExecStop=/home/test/Raja/Jul/OpManagerProbe/bin/na_service stop (code=exited, status=0/SUCCESS)
 Main PID: 799 (code=exited, status=0/SUCCESS)

Jul 10 17:18:38 opm-dev-l2 systemd[1]: Starting OpManager As Service...
Jul 10 17:18:42 opm-dev-l2 systemd[1]: Started OpManager As Service.
Jul 15 14:38:39 opm-dev-l2 systemd[1]: Stopping OpManager As Service...
Jul 15 14:38:39 opm-dev-l2 na_service[14926]: Stopping ManageEngine OpManager...
Jul 15 14:38:39 opm-dev-l2 na_service[14926]: ManageEngine OpManager was not running.
Jul 15 14:38:42 opm-dev-l2 systemd[1]: Stopped OpManager As Service.
[root@opm-dev-l2 bin]#
```

5. Stop OpManager by executing the **systemctl stop OpManager.service** or the **/etc/init.d/OpManager.service stop** commands.

Connecting the Web Client

1. Open a JavaScript-enabled Web browser such as Internet Explorer or Mozilla Firefox.
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.

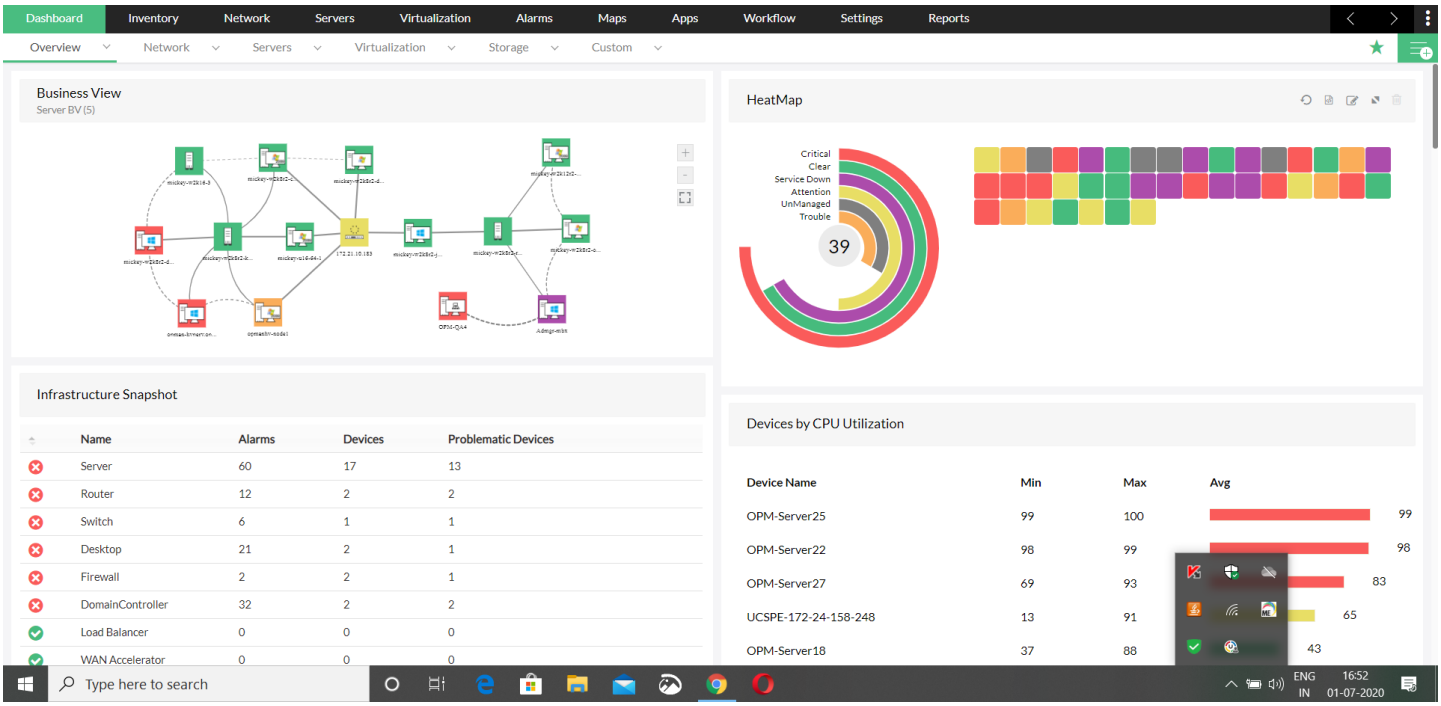
   [Note: If you have enabled SSL, connect as **https**://<**host_name**>:<**port_number**> in the address bar and press Enter.]
3. Type the **User Name** and **Password** and click **Login**. The default user name and password are 'admin' and 'admin' respectively.

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

Start > Programs > ManageEngine OpManager > OpManager Web Client.

[OR]

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



From OpManager build 7010 onwards we provide SSL support for the webclient. Click here to enable SSL.

Registering OpManager

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

1. Click on the profile icon (Next to the Settings icon on the top bar).

2. Click on the **Register** tab.
3. Click **Browse** and choose the license file from the location it is saved.
4. Click the **Register** button to apply the license file and close.

Should you encounter any errors when applying the license, contact Support with the license error code.

Changing Web Server port in OpManager

You will be prompted to change Web Server port during installation. You can also 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. Open Command Prompt as Administrator, and navigate to ***<OpManager Home>/bin*** directory. Then, execute the following command:
   In Windows,
   ChangeWebServerPort <new_port_number>

   In Linux,
   sh ChangeWebServerPort.sh <new_port_number>

   Here, **new_port_number** is the one where you want to run the Web server now.
3. Start the OpManager server.

Configuring System Settings

Date and Time Format Settings:

Select the required format for the date and time to be displayed in the OpManager web client. Report generated time will be based on the selection of date and time format for exported reports.

Default Authentication:

Authentication mechanism to authorize access to OpManager. It can either be local or domain specific authentication. Authentication type chosen here will be displayed in the login page and will set as the default authentication mode for OpManager.

Send Benchmark Statistics:

Data collected from the OpManager community is presented to the user for bench marking their performance.

Send Usage Statistics:

We collect benchmark and statistical data about quality, stability, and usability of the product from every installation with an intent to enhance the product quality. The collected data will be used as a whole during the analysis and we will not share this data with others. This feature is enabled by default. If you do not want your data to be collected, you can disable it any time.

Alert Notification:

When an alarm/alert is triggered, a notification pops up at the bottom right corner of the client. This option can be used to show/hide the notification from popping up on your screen.

Printer Alarm:

This option allows you to view/hide the alarm notifications generated by printers.

Rack & 3D Floor View: Modification required

Enable or disable viewing the Rack & 3D Floor View in Maps.

Alert when interface bandwidth exceeds its speed:

To keep your interface bandwidth in check, enable this option. When the bandwidth of an interface exceeds its configured speed, an alert will be raised.

Add/Remove Disclaimer Text in exported PDF/XLSX:

Enable this option to add a disclaimer in all your exported reports.

Add/Remove widgets in default dashboard:

To add/remove widgets on your default dashboard, enable this option.

Help Card details:

You can view the in-product How-to and FAQs present by enabling this option.

DB Query:

Enabling the DB Query option allows you to execute all read-only queries in the Submit Query window (Eg: select * from). To get to the Submit query window, 'Enable' the DB Query option, click on the support icon and select DB query in the support window, or alternatively press Alt+Q.

Product promotions:

Enable this option to receive in-product promotions and training announcements that includes helpful webinars and product training sessions.

Product Assistance Notification:

Click here to enable/disable the helpful information that appears in the product to guide you to operate the product better.

Allow dashboard creation for operator:

If Enabled, operator user will get access to create their own custom dashboard.

Displayed Modules:

You can choose to view modules forStorage Monitoring, Flow Analysis, Log Analysis, Config Management, IP Management by selecting their respective checkboxes. This adds a more complete IT Operations Management experience.

Displayed Add-on Modules:

Add-on Module for Applications Monitoring can be viewed by enabling this option.

Real Time Chart Rendering Mode:

Toggle between SVG and Image option to view the real-time charts.

Send Device and Monitor statistics:

Enable this option to allow OpManager to send anonymous data from the devices and the monitors associated with it. This information will help in enhancing the Device Templates module.

Auto Sync Device Templates:

Enable this option to sync new Device Templates automatically and update existing Device Templates by verifying with the OpManager Shared Device Template repository. A device template is a set of predefined properties such as device type, vendor, monitors and the monitoring interval for a device. It lets you automatically classify and associate monitors across multiple devices.

Remote Desktop/Terminal:

Enabling this option will allow users to connect to the device's terminal from the device snapshot page. Additionally, it will also provide access to Remote Desktop Protocol (RDP) port from OpManager.

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 monitoring 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, Active Directory, Exchange Servers, Web servers, Mail servers, CRM Applications, etc.
- **Host Resources:** CPU, Memory, and Disk Utilization of critical devices.
- Critical Desktops and Workstations.
- **Virtual machines:**  VMware, ESX/ESXi servers, HyperV, Xen servers and related guest virtual machines.

Monitoring Interval for a Device Category

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

To do so, follow the steps given below:

1. Under **Settings** > **Configuration** > **Quick Configuration Wizard** > click **Monitoring Intervals**.
2. To enable monitoring for a category, select the check box under **Enable** column for the infrastructure you want to monitor and enter the monitoring interval in minutes. To disable monitoring a specific category, uncheck the respective check box.
3. 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 then enter '1' in the adjacent box.

Types of Credentials supported by OpManager

Monitoring Credentials (SNMPv1/v2,SNMPv3,Telnet,SSH, WMI, VMWare, Citrix, UCS, Nutanix)

- 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.

SNMP v1/SNMPv2: SNMPv1 /v2 are community based security models. They use access mechanisms known as 'Read community' (for Read access) and 'Write community' (for Write access). The following are the parameters that are essential for a SNMP v1/v2 credential:

- Provide a name for the Credential name and description. Configure the correct Read and Write community, SNMP Port, SNMP Timeout (in seconds) and SNMP Retries.
- **Note:** SNMP Write Community is optional and is used if you don't have read access. But it is mandatory for the OpManager plugins.

SNMP v3: SNMPv3 is a user based security model. It provides secure access to the devices by a combination authenticating and encrypting packets over the network. The security features provided in SNMPv3 are Message integrity, Authentication and Encryption. If you select SNMPv3 as the credential type, then configure the following parameters.

1. **Name:** Credential name
2. **Description**: A brief description about the credential.
3. **User Name**: The user (principal) on behalf of whom the message is being exchanged.
4. **Context Name**: An SNMP context name or "context" in short, is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context. An SNMP entity potentially has access to many contexts. In other words, if a management information has been defined under certain context by an SNMPv3 entity, then any management application can access that information by giving that context name. The "context name" is an octet string, which has at least one management information.
5. **Authentication**: Select any of the authentication protocols either MD5 or SHA and enter the password. MD5 and SHA are processes which are used for generating authentication/privacy keys in SNMPv3 applications.
6. **Encryption**: Select any of the encryption protocols between DES, AES-128, AES-192 or AES-256 and enter the password. Note: Only after configuring Authentication it is possible to configure Encryption.
7. **SNMP Port**: SNMP port number.
8. **SNMP Timeout**:SNMP timeout in seconds.
9. **SNMP Retries**: SNMP retries.

Note:

- Ensure that the snmpEngineBoots and snmpEngineTime parameters specified in the device are in-sync with those specified in the SNMP agent. If not, the device discovery in OpManager will fail.
- Make sure that the context name given in OpManager is mapped properly to the agent credential

How to check if the snmpEngineBoots and snmpEngineTime values specified in the device are in-sync with those in the SNMP Agent ?

You can use the **Wireshark** tool to check if the snmpEngineBoots and snmpEngineTime parameters specified in the device and the SNMP Agent are in-sync with one another.

Download wireshark from here and query for the SNMP OID from the MIB browser. If the SNMP response message is a report with OID 1.3.6.1.6.3.15.1.1.2, then it means that the boot time and boot count are not synchronized.

WMI: WMI is a windows based credential used for authentication of devices that run on Windows operating system. If you select WMI as the protocol, configure the Domain Name, the User Name, and the Password. Example:- *TestDomain\TestUser.* Also enter the credential name and description.

Note:

- The amount of information that can be monitored using the WMI credential depends on the whether the credential supplied to OpManager has full admin privilige or not.
- If the credential does not have full admin privilige, certain operations like Folder monitoring (for restricted folders) cannot be done. Hence it is recommended (though not mandatory) to use WMI credentials that has full admin priviliges for monitoring using OpManager.
- If your network has a threshold limit on the number of incorrect login attempts, supplying an incorrect WMI credential might lock out the device in the Active Directory if the number of incorrect attempts cross the threshold limit.
- Incorrect credentials will also affect the OpManager performance. Hence it is always advisable to schedule Test Credentials to ensure that the credentials supplied are correct and up-to-date.

Telnet/SSH:

These are authentication credentials for CLI based server monitoring.

- **Telnet:** Ensure you configure the correct login prompt, command prompt, and password prompt besides user name, password, port number, timeout (in seconds) and click Save to access the device.
- **SSH:** Configuring the SSH protocol is similar to Telnet. Follow the steps mentioned in Telnet to add a SSH credential.
- **SSH Key Authentication:** This is a feature available for the SSH protocol. Choose SSH and select the SSH Key Authentication option. Ensure you configure the user name and choose the SSH Key using the Browse button. Enter the correct command prompt besides the port number and timeout (in seconds) to access the device. To know more, click here.

A **Password prompt / Login prompt** is the symbol in the CLI response which is used to decide the end of the response. The most commonly used password / login prompts are #, $.

Ensure that the correct password prompt and Login prompt is provided while defining the Telnet / SSH credential in OpManager since an incorrect Login / Password prompt will lead to failure of device discovery

VMware:Provide the VSphere client username and password. Enter the VMware web service port number and timeout interval for the connection between the Host and OpManager server.

Also, ensure that the credentials provided are those of the VCenter under which the required hosts / VM's are present

Citrix: Provide the Username and Password of the Host. Enter the web service port number and timeout interval for the connection between the Host and OpManager server.

UCS: Provide the UCS Manager Username and Password. Enter the Port, Protocol and Timeout interval for the connection between the UCS and OpManager Server.

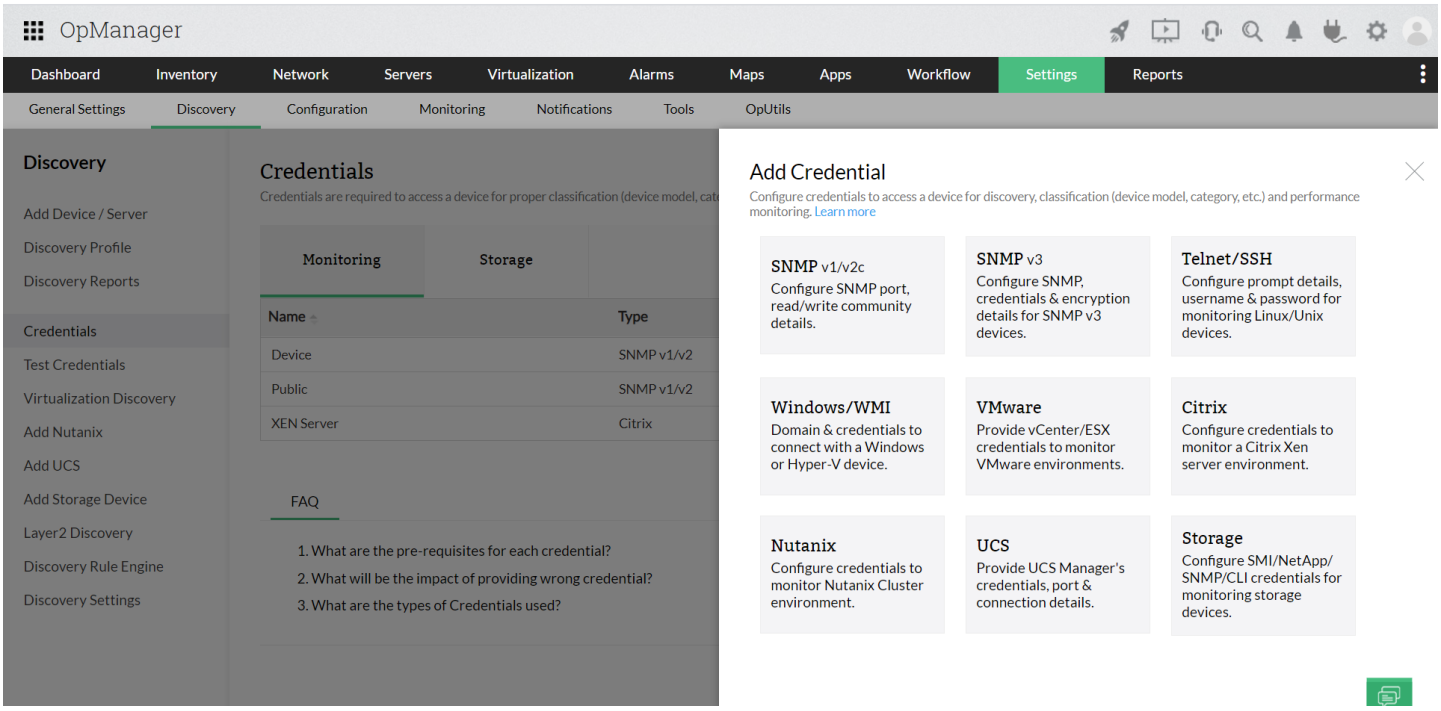
Nutanix: Provide the username and password of the Prism API element, the protocol being used (HTTP/HTTPS), the timeout value for the connection and the port in which the Prism element is running.

Backup Credentials (Telnet, SSH, SNMPv1, SNMPv2c, SNMPv3)

- These credentials are used for discovering devices into OpManager plugins like the Network Configuration Manager module.
- The Network Configuration module uses these credentials for taking Router/Switch config backup, and to perform complaince check and config change management periodically.

Storage Credentials (SNMPv1/v2, v3, CLI, SMI, NetAppAPI) :

- These credentials are used for discovering devices into the OpStore module.
- This module enables storage monitoring of Disk, LUN, RAID etc. The Storage credentials helps you to monitor the storage devices like Storage Arrays, Fabric Switches, Tape Libraries, Tape Drives, Host servers and Host Bus Adapters cards from all leading vendors in the industry.



To learn how to add storage credentials in OpManager, click here.

SNMPv1 / v2:

Credential Pre-requisites:

The following are the pre-requisites for the various types of credentials supported in OpManager

SNMPv1 / v2:

- SNMP read credential is mandatory
- **Ports**: The default port used for SNMP is 161. Make sure that this port is not blocked by your firewall

SNMP v3:

- Make sure the SNMP v3 authentication details received from your vendor has been implemented properly in the device
- Make sure the context name given in OpManager is mapped properly to the credential
- EngineID should be unique for all the SNMP v3 devices in an environment
- **Ports**: The default port used for SNMP v3 is 161. Make sure that this port is not blocked by your firewall

- Make sure the engine boot time and engine boot count is updated properly in the SNMP agent

WMI:

- Required credentials: Domain/User name, password
- Make sure the Windows Management Instrumentation service & RPC service is running in the remote device for WMI monitoring

Telnet/SSH:

- For Telnet/SSH, ensure you configure the correct login prompt, command prompt, and password prompt besides the user name, password, port number and timeout (in seconds) to access the device.
- The default port used for Telnet is 23 and SSH is 22. Ensure that the port is not blocked by your firewall.
- For SSH Key Authentication, ensure you configure the user name and choose the SSH Key using the Browse button, and correct command prompt besides the port number and timeout (in seconds) to access the device.
- The default port used for SSH Key Authentication is 22. Ensure that the port is not blocked by your firewall.

UCS:

- Make sure the UCS Manager Username and Password having remote authentication is configured.
- Enter the Port, Protocol and Timeout interval for the connection between the UCS and OpManager Server

VMWare:

- The default HTTPS port used for VMWare is 443. Ensure that this port is not blocked by your firewall
- Provide the VSphere Username and Password of the VCenter under which the hosts and VMs which need to be discovered are present.
- Auto VM discovery feature is used to automatically update any changes in the vCenter environment (such as addition of new VMs to a vCenter) to OpManager.
- For monitoring VMware related devices, it is enough if a credential has 'Read only' privilege.
- Certain functions like VM On & VM Off require admin privilege. Hence ensure that the credentials supplied has admin privileges.

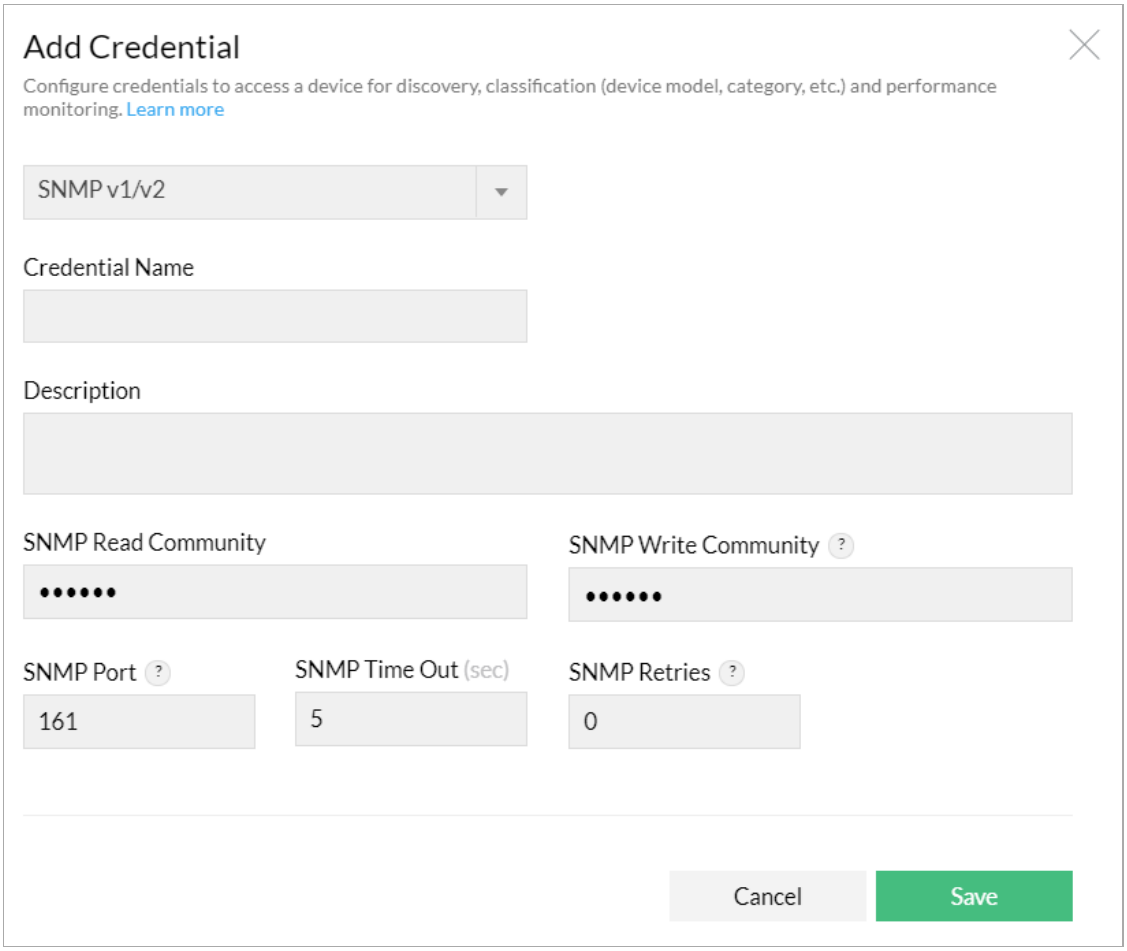
Nutanix:

- The default HTTPS port used for Nutanix is 9440, and the default timeout is 20 seconds. If necessary, please change these values according to your requirement.
- Provide the username and password of the Prism element of the cluster under which the hosts and VMs to be discovered are present.

Add Credentials

OpManager accesses the remote devices using the protocols SNMP, CLI, WMI or VMWare API. 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 **Settings** > **Discovery** > **Credentials**
2. Click **Add Credential**
3. Select the required credential category & credential type.
4. Click **here** to know the **prerequisites** of each credential
5. Configure the following parameters and click **Save** to add the credentials:



Discovering Networks Using OpManager

OpManager uses ICMP/Nmap to discover the devices in a network. You can either discover a specific range of devices or the entire network.

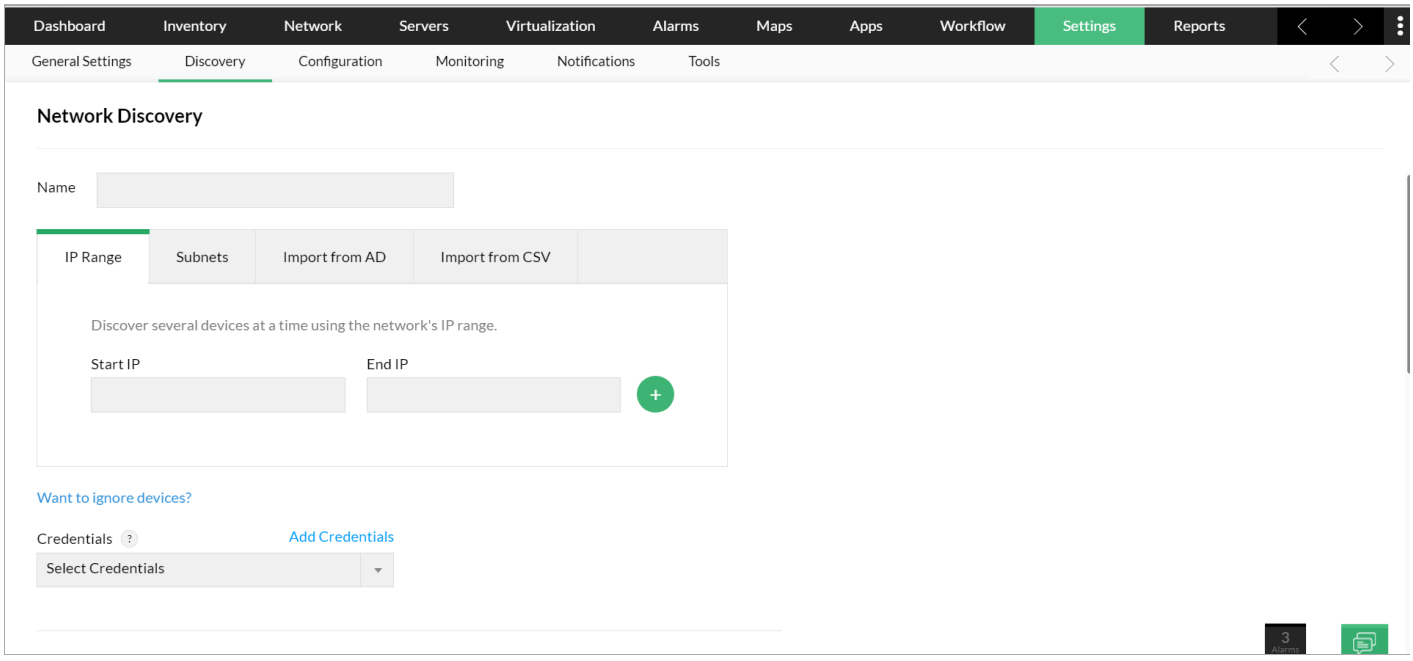
1. Discovering devices from an IP Range
2. Discovering individual devices
3. Discovering a complete network
4. Discovering devices by CSV import
5. Import devices from Active Directory
6. Rediscover the existing devices
7. Discovering Interfaces
8. Scheduled discovery

Discover devices in an IP range

To discover a selected range of devices,

For OpManager versions 125174 and above:

1. Go to **Settings** -> **Network Discovery** -> **New Discovery**.
2. Select the **IP Range** option.
3. Enter the start and end IP of the required range.
   Start IP: Specify the IP address of the device in the range from where OpManager should start the discovery process. End IP: Specify the IP address till which the devices are to be discovered.
4. Select the required Credentials
5. Click on **Discover** and OpManager will direct you to the **'Discovered Devices'** page.
6. **Approve** or **Ignore** the discovered devices by clicking on the respective options. The approved devices will be added to the OpManager inventory and moniotored. The ignored devices will be removed from the queue of discovered devices and restricted from future addition.

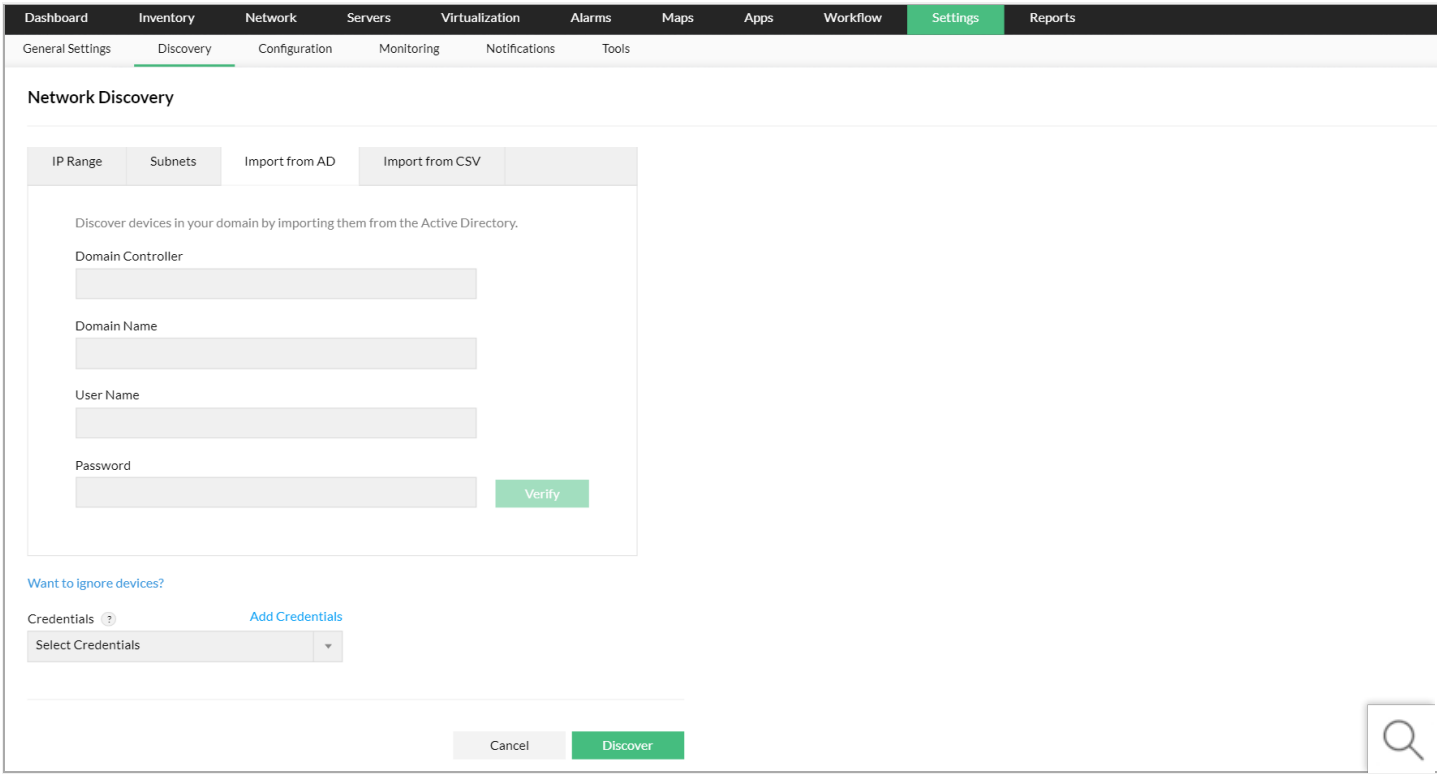


For OpManager versions below 125174

Import devices from Active Directory

Discover devices in your domain by importing them from the Active Directory.

1. Go to **Settings** -> **Network Discovery** -> **New Discovery**.
2. Select the **Import from AD** option.
3. Enter domain controller name, domain name, user name and password.
4. Click on **Verify** to initiate the discovery process and OpManager will direct you to the **'Discovered Devices'** page.
5. **Approve** or **Ignore** the discovered devices by clicking on the respective options. The approved devices will be added to the OpManager inventory and moniotored. The ignored devices will be removed from the queue of discovered devices and restricted from future addition.



Discover interfaces

Interface discovery can be performed in different ways.

During the initial discovery of devices

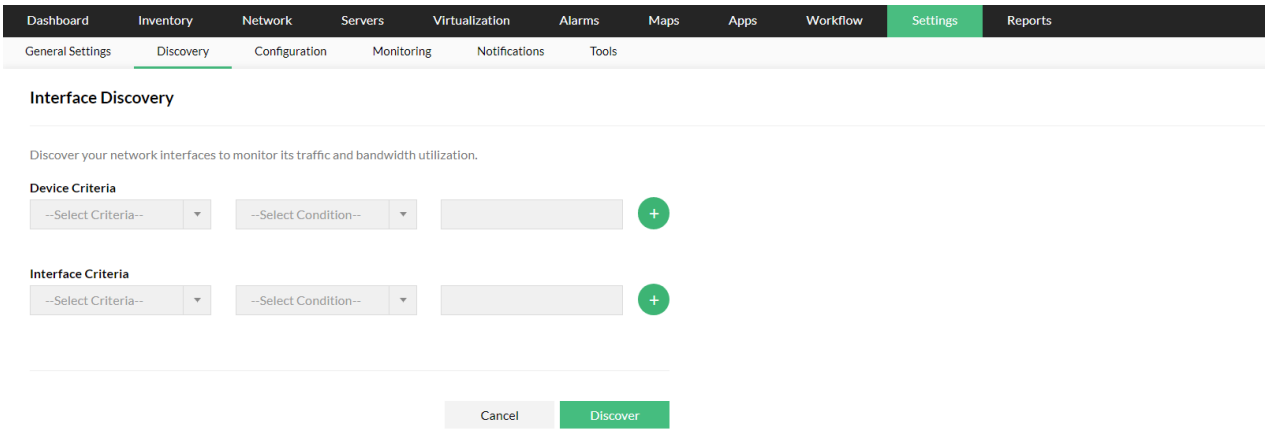
By default, automatic discovery of devices will be disabled in OpManager. To enable it, go to **Settings -> Discovery -> Discovery Settings** and enable the **Interface Discovery** option. OpManager will now automatically discover the interfaces associated with the discovered devices (when discovery is performed from 'Add Device' page). During bulk device discovery, the required interfaces can be selected and discovered from the Discovery-Interface page.

From the Device Snapshot page

1. Go to the device snapshot page of the discovered device.
2. In the Interface tab, click on the **Discover Interfaces** option.
3. The interfaces associated with your device will be discovered and added in OpManager.

From the Interface Discovery page (only for OpManager versions 125174 and above):

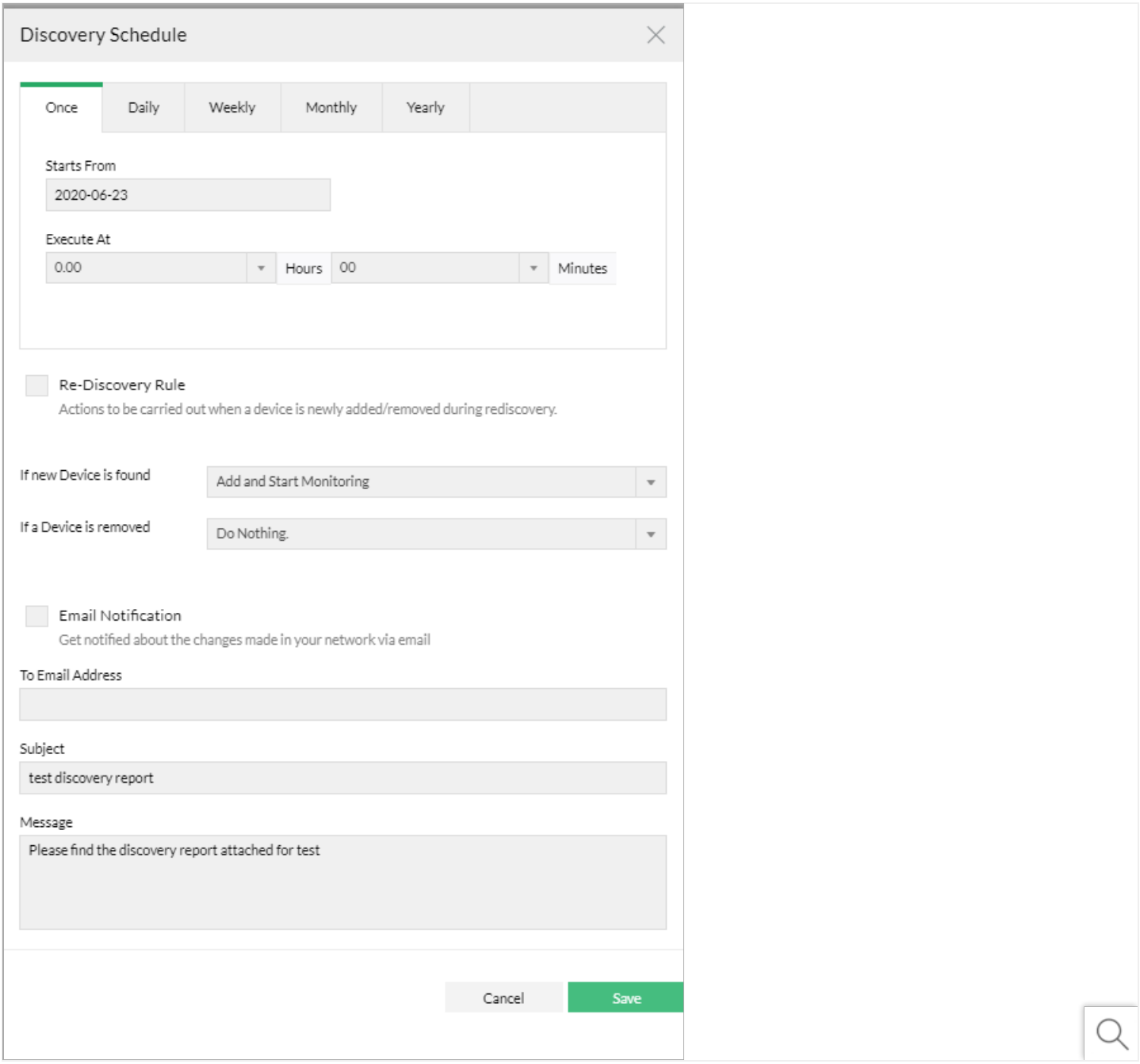
1. Go to **Settings -> Discovery -> Interface Discovery**
2. Define a condition and criteria for interfaces to be discovered.
3. Click on the **Discover** option to start discovering interfaces that matches the specified criteria.



Schedule Discovery

You can schedule device discovery in OpManager at specific intervals by specifying the IP range. The created schedule can be saved as a profile and reports can be generated. To schedule a profile,

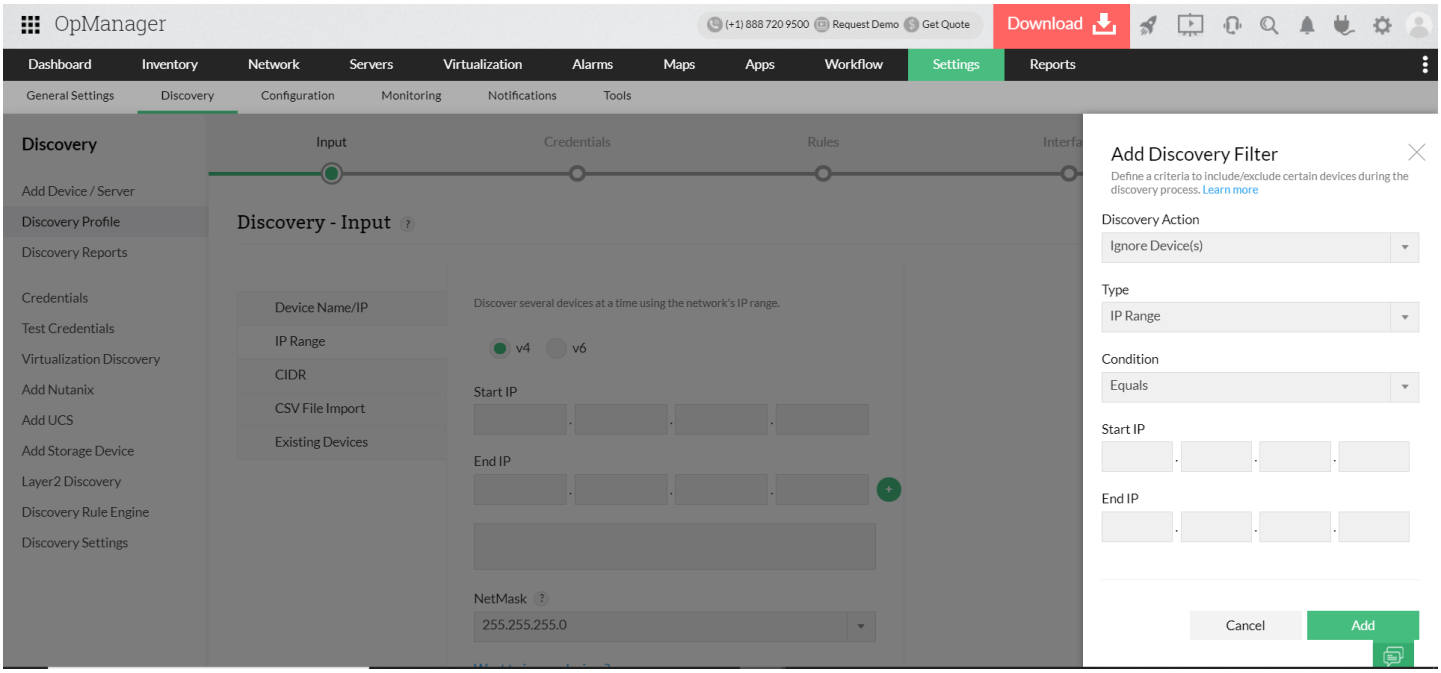
1. Click on the 'clock' icon displayed under **Actions** column of the respective Discovery Profile.
2. In the Discovery Schedule page, define the frequency at which you would like to re-run the discovery schedule and save the profile.


Discovery Schedule
Once
Daily
Weekly
Monthly
Yearly
Starts From
2020-06-23
Execute At
0.00
Hours
00
Minutes
Re-Discovery Rule
Actions to be carried out when a device is newly added/removed during rediscovery.
If new Device is found
Add and Start Monitoring
If a Device is removed
Do Nothing.
Email Notification
Get notified about the changes made in your network via email
To Email Address
Subject
test discovery report
Message
Please find the discovery report attached for test
Cancel
Save

Discovery Filter in OpManager

You can choose to add or ignore any single device or a set of devices before configuring device discovery schedule in OpManager.

- Open OpManager and click on **Settings -> Discovery -> Discovery Profile.**
- Click on the **Add Discovery Filter** at the top right corner.
- Choose either **Ignore/Add Device(s).**
- Specify the criteria - IP Range/ IP Address/ Category/ Device Type/Device Name.
- Enter the Value or IP address as per the 'Type' you selected.
- Finally click on **Add** and proceed with scheduling discovery.
- OpManager will add/ignore the devices as per the filter specifications.



Add Device Failure Message

Is an error stopping you from adding new devices to OpManager? Here is a list of error messages and the corresponding reasons on why a particular error is triggered and solutions on how to resolve them.

Device not reachable

Cause

When the device you are trying to add is not pingable, this error is displayed. It is triggered when you are attempting to add a device using its device name.

Solution

OpManager searches for the device using its device name and pings the device. If the device name is not found, this error is displayed. This can be fixed by avoiding typos in the device name.

> **Note:** When adding the device using its IP address, the device gets added even though it is not pingable. But its status is classified as "Device not monitored". OpManager periodically pings this device and when it is available, it is added and classified accordingly

Device already exists in OpManager

Cause

This error is caused by one of the following reasons

- Same display name is used for devices with different IP addresses.
- The IP address and display name of the new device is same as an existing device.

Solution

When using the same display name for multiple devices with different IP address, make sure to disable Unique System Display Name (Discovery > Discovery Settings > Unique System Display Name)

Make sure devices with the same IP does not exist in OpManager.

Network IP not allowed

Cause

This error is displayed when the network IP and device IP are the same.

Solution

Network IP turns out invalid when the IP that is standard to a network (.0) is configured for a device. Check for typos and make sure the correct value is entered.

Ensure the Device IP doesn't match the Network IP when it is fetched automatically.

Cannot add device. This edition of OpManager does not support adding more than {n} devices

Cause

Your device has run out of licenced devices that can be monitored. Here, {n} indicates the number of device that has exceeded the licencing limit.

Solution

Delete/Unmanage unwanted devices to make room for the new ones or purchase a licence that can accommodate a larger number of devices.

Add Device Failed - Device Name : Problem in adding the device, please contact support with support information file

Cause

This error is exclusive to SNMP devices. This error is triggered even though the device you are attempting to add is pingable. The reason this is happening is because the Sysname turns up empty when trying to fetch the device details.

Solution

Sysname is a mandatory field, make sure this field is populated before attempting to add the device. To verify the status of the Sysname, query the SNMP device to check if the SysName (.1.3.6.1.2.1.1.5) returns a value.

Device Discovery Error: 'Unable to contact IP driver. General failure'

This alert message is generated when OpManager server fails to contact the monitored device during its periodic availability status poll. This error generally appears in a VM environment where the Virtual devices are running any Windows OS and when they are unable to reach outside the network due to any of the following causes.

- Hyper V **&#65533;** WinSock issue
- VM duplicate Security Identifier issue
- TCP/IP issues

Hyper V **&#65533;** WinSock issue

Cause:

This error occurs in your VM when there is a possibility of WinSock and WinSock2 setting being corrupted.

Solution:

You could try to point to the following registry paths:

- HKLM\SYSTEM\CurrentControlSet\Services\WinSock
- HKLM\SYSTEM\CurrentControlSet\Services\WinSock2

i. Backup the above registry.
i. Go to another server (running the same OS configuration), go to the above registry paths, export the registry and copy them to your current server.
i. Double click on the reg files to register, reboot the system to see how it works.

Source

VM duplicate Security Identifier issue

Cause:

This issue is caused by a duplicate Security Identifier (SID) in a Windows 2008 or Windows 2012 virtual machine, when the either of them are deployed from a template or a cloned virtual machine. And the guest customization option is not selected while deploying the virtual machine.

Solution:

To resolve the issue, you need to run the **sysprep** tool to generate a new security identifier for the virtual machine. To do this,

i. Open a console to the affected Windows virtual machine.
i. Open a command prompt in elevated mode. Right-click a shortcut to the Windows Command Processor and select the **Run as administrator** option.
i. Change the path to C:\Windows\System32\sysprep.
v. Run the sysprep command.
v. When the sysprep wizard appears, check the generalize check box, leave all other setting at the default values.
i. Reboot the virtual machine to apply the changes.

Source

TCP/IP issues

Cause:

When you are unable to ping the loopback address/local setup, there are chances of your TCP/IP stack being corrupted.

Solution:

Turn off User Account Control (UAC) and login with the domain admin account. Follow the below steps to reset TCP/IP to its original state:

i. On the Start screen, type CMD. In the search results, right-click Command Prompt, and then select Run as administrator.
i. At the command prompt, enter the command given below and then press Enter.

netsh int ip reset resetlog.txt

i. Restart the computer.

When you run the reset command, it overwrites the following registry keys, both of which are used by TCP/IP:

- SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
- SYSTEM\CurrentControlSet\Services\DHCP\Parameters

Source

Adding devices using SSH Key based authentication in OpManager

A SSH key is an access credential used in SSH protocol. It provides the same functionality as the user name & password except that it is much more reliable and cant be easily cracked.

OpManager supports SSH key based authentication. To use a SSH key, you must first generate it. Use the following steps to generate a SSH key credential and discover devices using OpManager:

Generating SSH Key(Windows)

Generating SSH Key(Linux)

Generating SSH key (Windows)

Generating the keys

- Install putty on your windows machine
- Once the installation is done, go to the directory in which putty was installed and open the puttygen.bat file
- Click Generate. (It will generate public & Private key.
- Create a folder under windows user directory named SSH Key. Save the Public key and private key under that folder. (Do not close the puttygen window). Copy the public key displayed in PuttyGen window
- Open the private key file and save it as key.txt.This will be used by OpManager to access the Linux system (Note: do not modify anything in it).

Adding the public key in the Linux Machine

- Find the authorized_keys file in the file /etc/ssh/sshd_config

```
AuthorizedKeysFile      /etc/ssh/%u/authorized_keys
```

- Paste the public key copied previously in the authorized_keys file.

```
[root@ My_OPM_device  root]# echo ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDLiGgmD2f8K16QXA/B55u3j9AHkHmEqcUoaiJcoNgtmJxfefIQC7Ngcv2
ZWJS1HzrGH+VTLn0h+Kcgfaklof6+shaGRYZ9m3YjaYf+8I6hL/1nE+sWGzAsQmlwsh/CLjW7aVks/JguqxNRIz34G
sTGaCb5ebbAeFGv01FF3I9jzF0paUssj2ffiBZ8ucDSSBOpDXXwxoW9PzZgPLhOXlA+e2ONlBrJcUIP9pwMMlVEYgs
HSDVictqasdUY/O+jjrB+BeshIqpHx2tsD4ikbu0YmezvX40vvSFlQNHw+f4MM8IcbPZHThXbEMm3pVC1OxPFR5Gw
XWgopn8Jf0gGmKmv test@ My_device_1 >>authorized_keys
```

Key Verification:

You can check if the SSH key has been generated and assigned correctly by opening the putty.exe, entering the machine name and then from the left side panel selecting SSH -> Auth -> Load the Private key and opening the connection. This should log in with the key file. A successful login is an indication that the device has been added correctly using the SSH key.

Generating SSH Key(Linux)

Generating the keys

Generate key using the command ssh-keygen

```
[test@ My_device_1 .ssh]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/test/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/test/.ssh/id_rsa.
Your public key has been saved in /home/test/.ssh/id_rsa.pub.
The key fingerprint is:
56:d7:16:bc:33:cf:90:a2:4e:08:8d:f5:0a:ec:b4:d1 My_device_1
The key's randomart image is:
+--[ RSA 2048]----+
|          .. |
|       .   ... |
|    . = .. . oo |
|     B E.....*  |
|    o =So . . * |
|     o.o o    o|
|       o      |
|        .     |
|              |
+-----------------+
```

This step will generate two keys - a public key and a private key.

The public key can be shared with other devices while the private key must be kept confidential as it will be used for authorization purpose.

```
[test@ My_device_1 .ssh]$ ls -l
total 8
-rw------- 1 test test 1679 2018-07-31 14:08 id_rsa
-rw-r--r-- 1 test test  396 2018-07-31 14:08 id_rsa.pub
```

Adding the Public Key in the Linux

Find the authorized_keys file in the file /etc/ssh/sshd_config

```
AuthorizedKeysFile      /etc/ssh/%u/authorized_keys
```

Paste the public key copied previously in the authorized_keys file.

```
[root@ My_OPM_device  root]# echo ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDLiGgmD2f8K16QXA/B55u3j9AHkHmEqcUoaiJcoNgtmJxfefIQC7Ngcv2
ZWJS1HzrGH+VTLn0h+KcgfaklOf6+shaGRYZ9m3YjaYf+8I6hL/1nE+sWGzAsQmlwsh/CLjW7aVks/JguqxNRIz34G
sTGaCb5ebbAeFGv01FF3I9jzF0paUssj2ffiBZ8ucDSSBOpDXXwxoW9PzZgPLhOXlA+e2ONlBrJcUIP9pwMMlVEYgs
HSDVictqasdUY/O+jjrB+BeshIqpHx2tsD4ikbu0YmezvX40vvSFlQNHw+f4MM8IcbPZHThXbEMm3pVC1OxPFR5Gw
XWgopn8Jf0gGmKmv test@ My_device_1 >>authorized_keys
```

Key Verification

Now login with the private key.

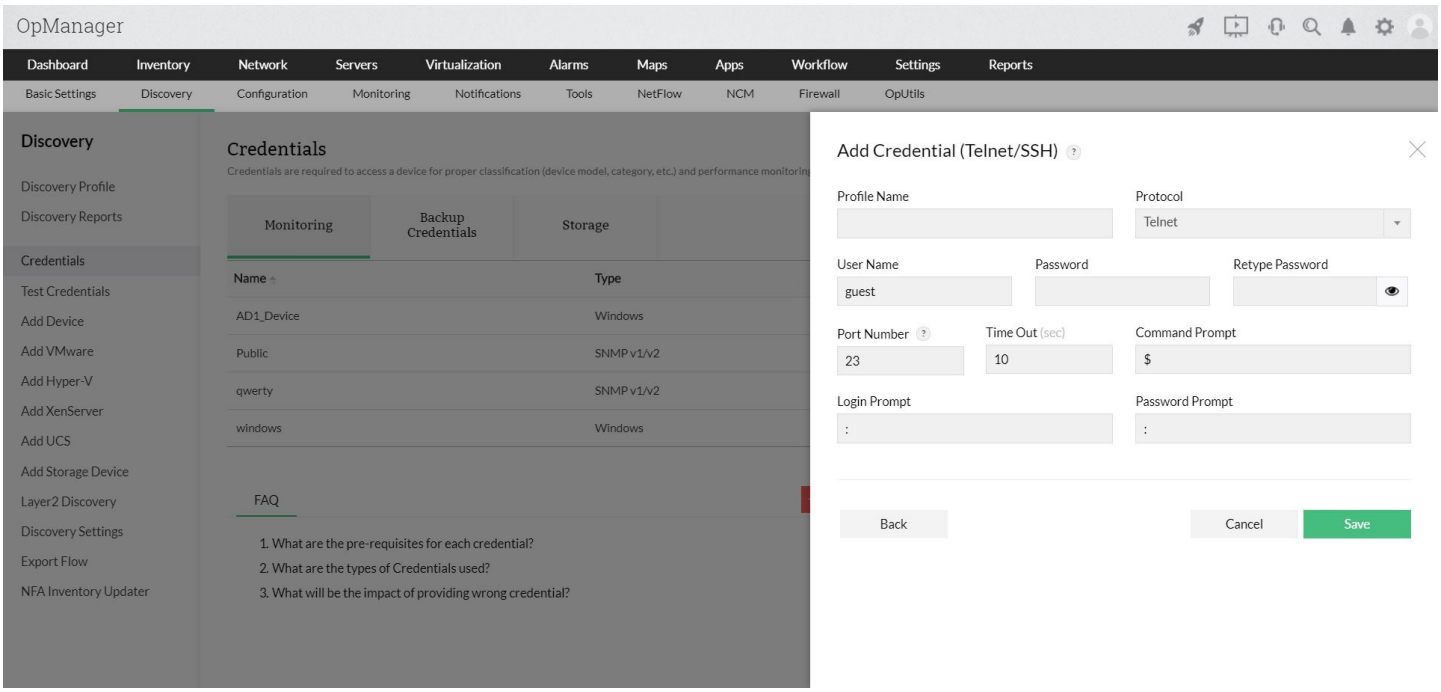
```
[test@My_device_1.ssh]$ ssh -i id_rsa root@172.21.151.96
Last login: Tue Jul 31 03:58:30 2018 from My_device_1.mynetwork.com
[root@OPM-C6-32-AIO ~]#
```

If the key used is right, you should be able to login successfully without the system prompting you for a password.

Adding devices into OpManager using SSH credentials:

- In the OpManager server, go to **Settings -> Discovery -> Device Credentials.**
- Click on **Add Credentials** and select **Telnet/SSH.**
- Name the credential and check the **SSH Key Authentication** check box.
- Provide the user name and upload the **private_key.txt** saved in the previous step and save the credential.

You can now add/discover Linux devices using this credential.



Discovery Rule Engine

Discovery Rule Engine helps you automate the activities such as adding monitors to a device or adding a device to a business view that you carryout after adding the devices to OpManager. This helps you start monitoring the devices straightaway as soon as you add them and avoid repetitive manual effort.

How does Discovery Rule Engine Work?

The Discovery Rule Engine is condition/criteria based. During discovery, devices that satisfy the condition/criteria are associated with the actions specified in the Discovery Rule Engine.

Steps to add a Discovery Rule Engine

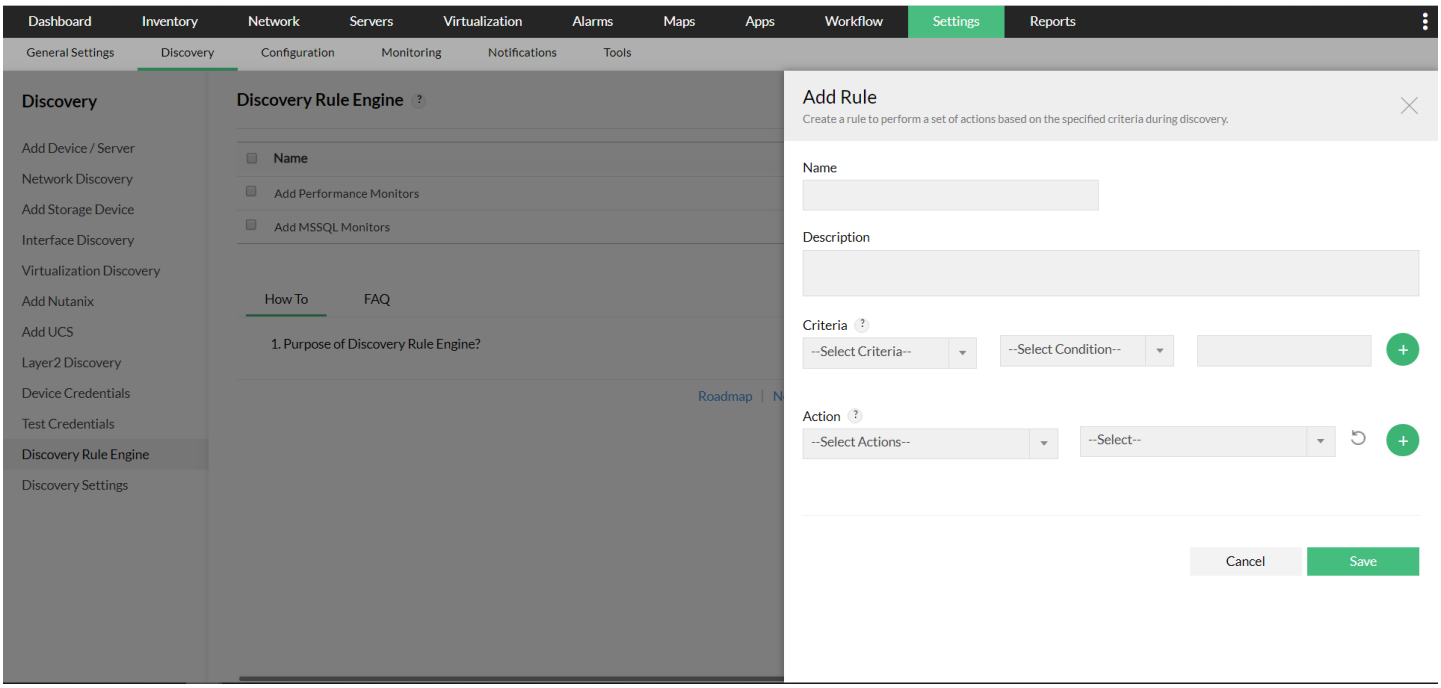
1. Go to **Settings** -> **Discovery** -> **Discovery Rule Engine** and click on **Add rule** on the top right.
2. Enter a **Name** and **Description** for the Discovery Rule Engine.
3. **Criteria** refers to the parameter of the device which must be checked for applying the rule (Such as DNS Name / Category / Type...). Define the Criteria and select the Condition.
   Eg. Select Service Name as the Criteria and equals as the Condition, and enter the POP3Svc (POP3Svc is a MSExchange service. This is to verify whether the discovered device is an exchange server or not.)
4. If required you can define multiple criteria, but have to select either AND or OR option.
   AND: Executes the action when all the defined criteria are satisfied.
   OR: Executes the actions when any one of the defined criteria is satisfied.
5. Define the **Actions**. An **Action** refers to the process to be performed on a device if it satisfies the specified criteria.
   The following are the list of possible actions that can be performed by a Discovery rule Engine:

   - Associate a Process Monitor with the device
   - Associate a Service Monitor with the device
   - Associate a Windows NT Service Monitor with the device
   - Associate a File / Folder / Script Monitor with the device
   - Add the device to a Business View
   - Associate a URL Monitor with the device
   - Associate an Event Log Rule to the device
   - Associate MSSQL Monitors with the device
   - Associate Notification Profiles with the device

6. Select the required action. You can add additional actions by clicking on the **Add (+)**.
   Following are the list of actions that be performed on the created Discovery Rule.

   - Edit
   - Copy As
   - Enable/Disable
   - Delete

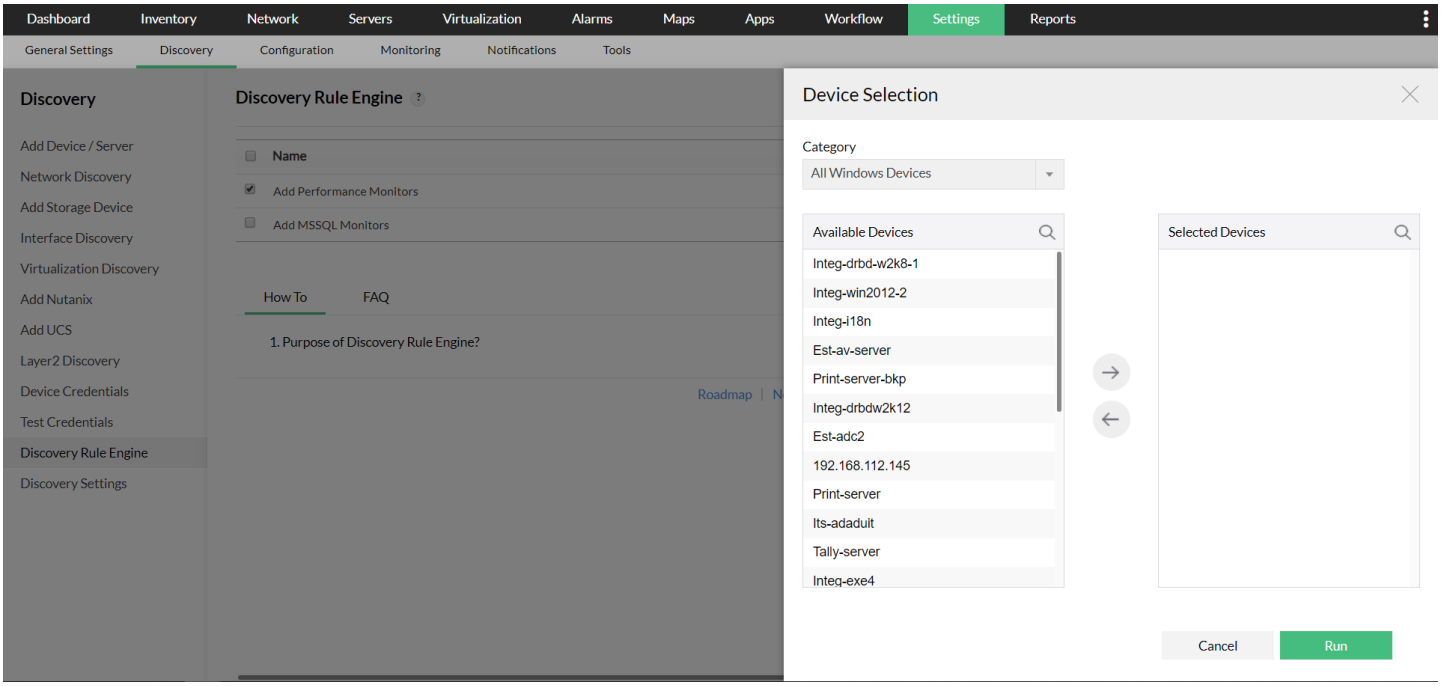
7. Click on **Save**.



Re-running a Discovery Rule Engine

To re-run a rule on demand,

1. Select the rule that you want to re-run.
2. Click on the **Re-run** button.
3. Select the devices on which you want to execute the rule.
4. Click **Run.**



Discovering devices using Layer2 maps

How to draw Layer 2 maps?

OpManager allows you to discover Layer2 devices that are connected to your network and draws a visual representation of the same. This includes a detailed map of all the nodes, interconnected layers and port-to-port connectivity in addition to the interfaces.

To start discovering your layer2 devices, go to **Settings** > **Discovery** > **Layer2 Discovery**. This process can also be initiated from **Maps** > **Layer 2 Maps** > **Create New**.

Enter a name in the **Layer2 Map Name** section and proceed to type the IPv4 of your seed device in the **Router IPv4 Address** section.

> **Configure a seed device :** A seed device is the core router or L3 switch in your network. The device must have SNMP-enabled so that OpManager is able to query the device and draw the links automatically. The seed device should have "ipForwarding" set to 1 for the OID - .1.3.6.1.2.1.4.1.0 and must have two or more interfaces. (identified by querying the OID - 1.3.6.1.2.1.4.20.1.1)

The seed router will be connected to a vast number of devices. If you wish to restrict your Layer2 Map to a certain IP range, enter their Start IP and End IP and press the ⊕ icon. You can specify multiple such entries.

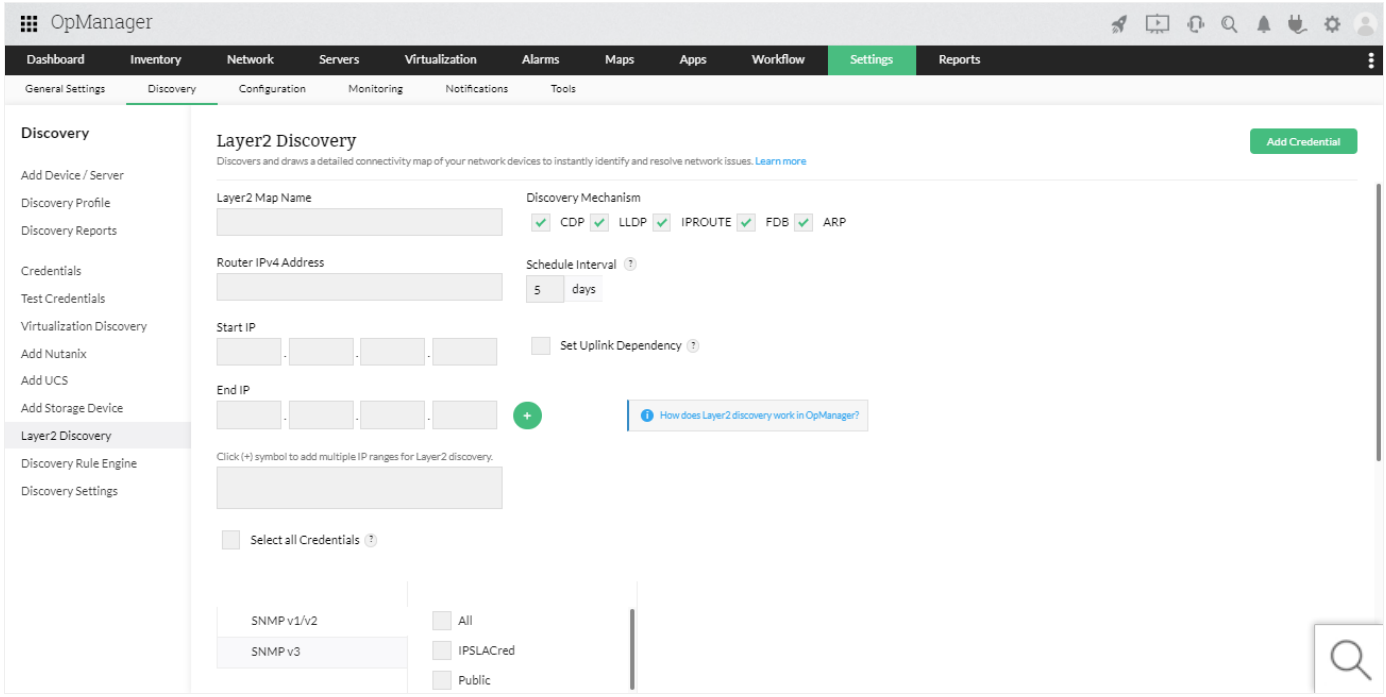
Discovery Mechanism:
OpManager supports multiple discovery protocols. Choose one (or more) that is implemented in your seed router/L3 switch. This will drastically reduce the time taken to discover the devices.

Schedule interval:
As changes happen to the networks frequently, OpManager allows you to configure an interval (in days) to re-draw the map. For instance, if a change happens once in a week, you can configure OpManager to re-draw the map every seven days.

Set Uplink Dependency:
This option helps in avoiding multiple device-down alerts when the parent device is down. Besides the layer2 discovery window, Uplink Dependency can also be set from the Quick Configuration Wizard.

> **Note:** Uplink Dependency happens only during **Device Import** and not during Layer2 Map discovery.

Credentials:
Choose the SNMP credentials required for the seed router to identify the devices. You can add new credentials from the **Add Credentials** button.



To learn how to customize your layer 2 Map, click here.

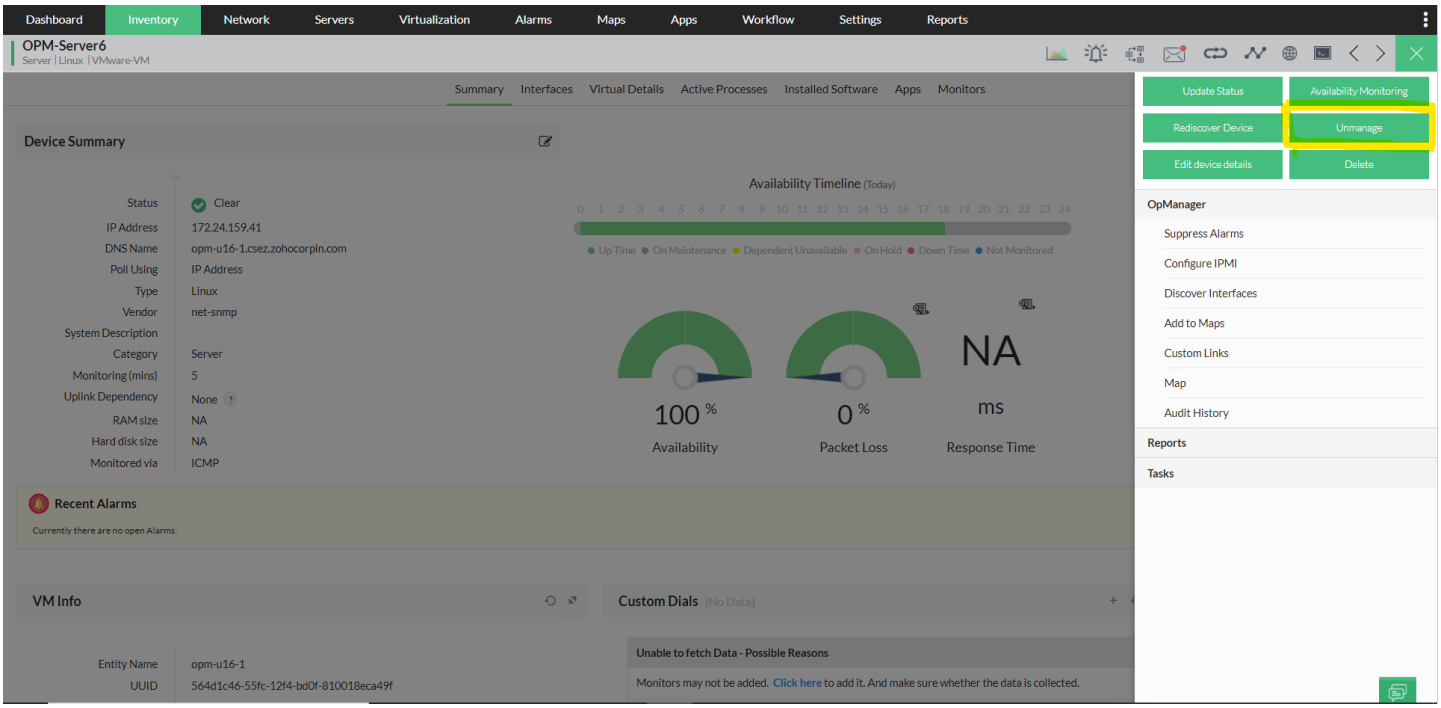
Managing and Unmanaging a Device

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 managed device:

- Go to **Inventory > Devices > Device snapshot** page
- Click the **Menu** icon and select **Unmanage**.

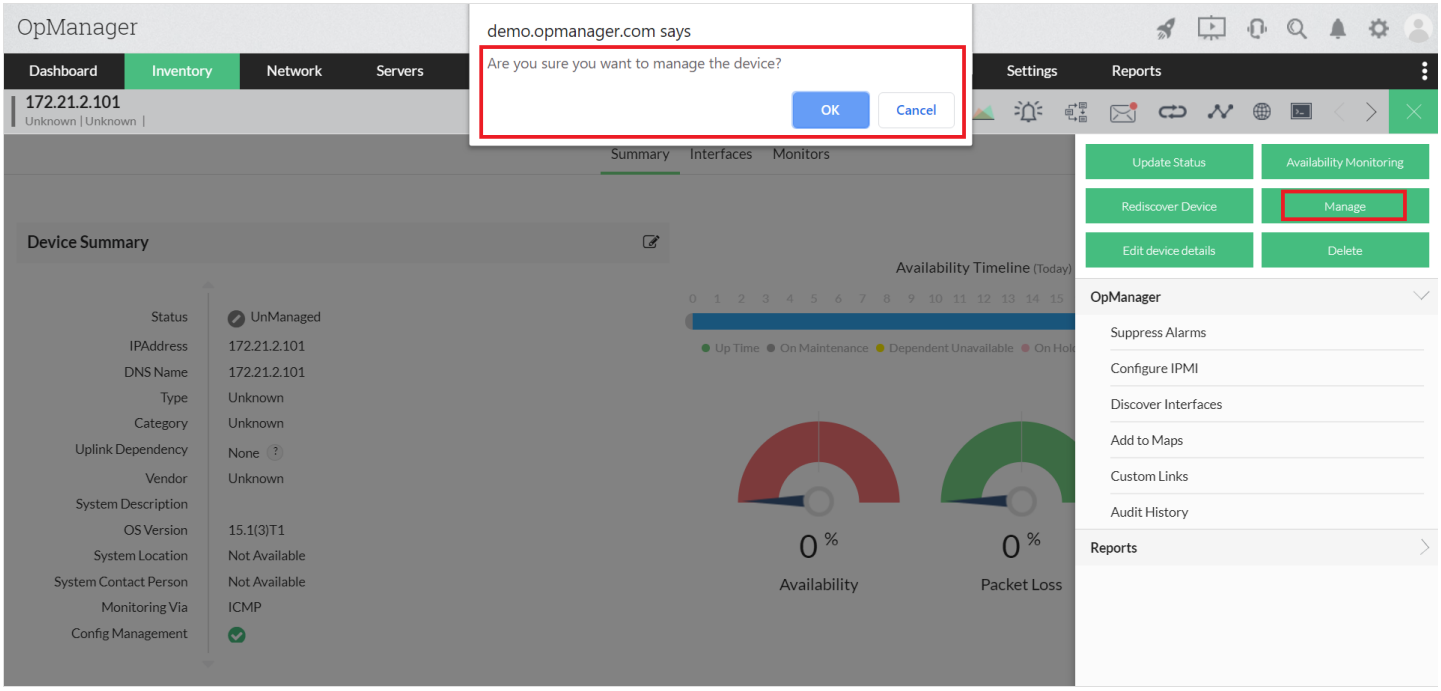
This stops the status polling and data collection for the device and changes the device status icon to grey.



To start managing an unmanaged device:

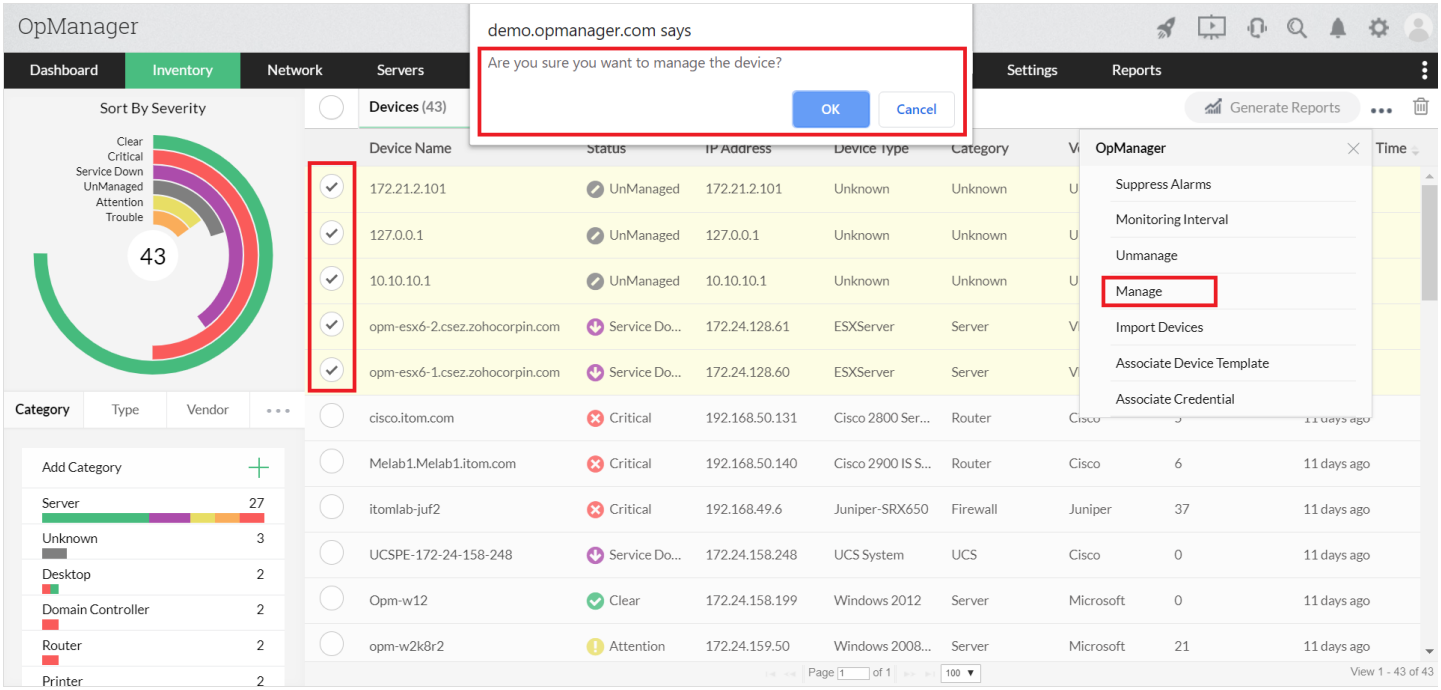
- Go to **Inventory > Devices > Device snapshot** page
- Click the **Menu** icon and select **Manage**.

This resumes the status polling and data collection for the device. The status icon shows the current status of the device.

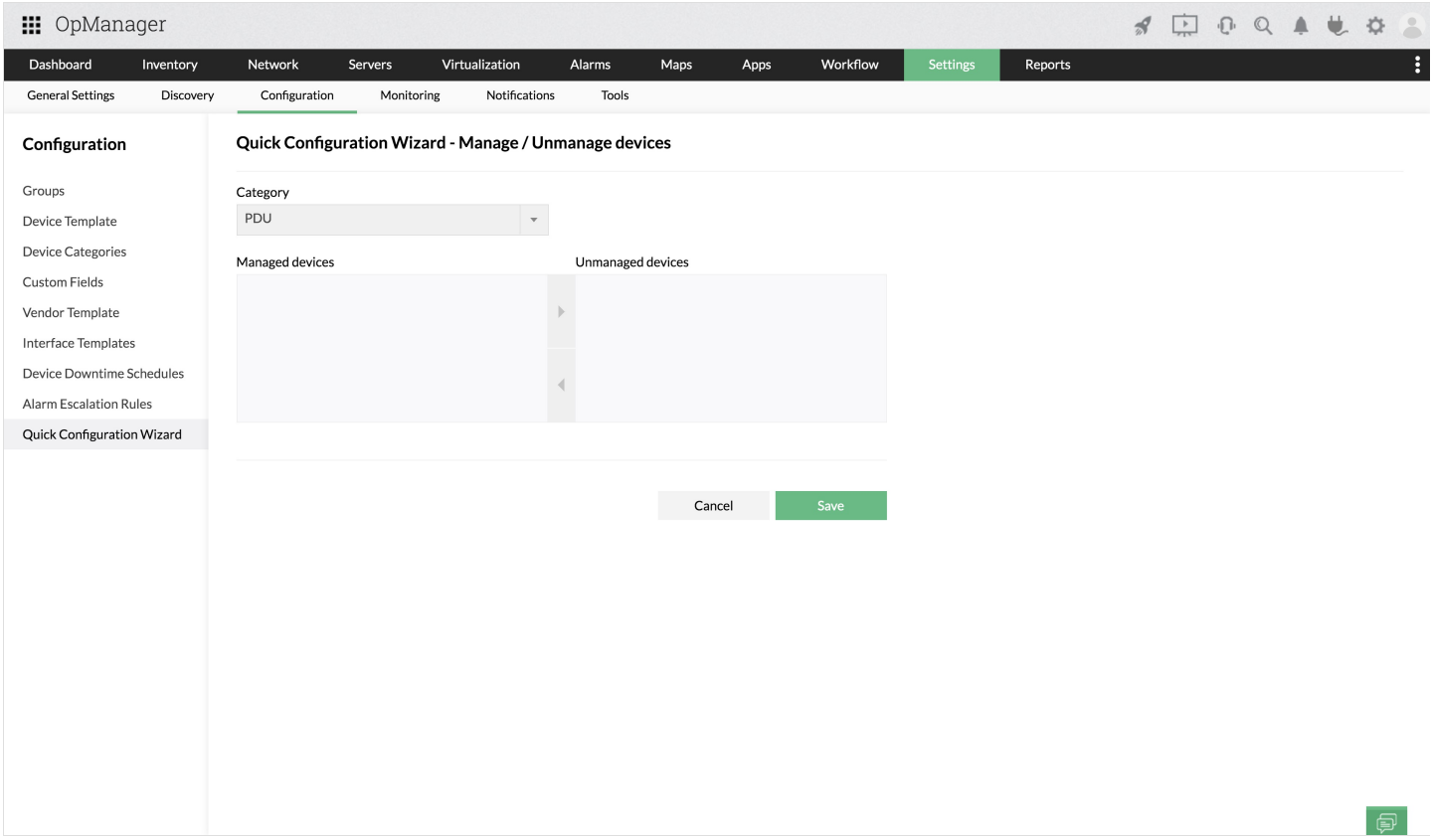


To Manage or Unmanage devices in bulk:

- Go to **Inventory.**
- Select the devices you wish to manage/unmanage.
- Click on the **menu** at the top right and select **manage/unmanage** devices.



You can also use the **Quick Configuration Wizard (Settings ? Configuration ? Quick Configuration Wizard ? Manage/Unmanage devices)** to manage or unmanage devices in bulk.


OpManager
Dashboard
Inventory
Network
Servers
Virtualization
Alarms
Maps
Apps
Workflow
Settings
Reports
General Settings
Discovery
Configuration
Monitoring
Notifications
Tools
Configuration
Groups
Device Template
Device Categories
Custom Fields
Vendor Template
Interface Templates
Device Downtime Schedules
Alarm Escalation Rules
Quick Configuration Wizard
Quick Configuration Wizard - Manage / Unmanage devices
Category
PDU
Managed devices
Unmanaged devices
Cancel
Save

Configuring Custom Fields for Devices or Interfaces

Configure additional properties of a device/interface by adding Custom Fields. This makes device management easy.

1. Go to **Settings ? Configuration ? Custom Fields**. A list of pre-populated fields are shown.
2. Choose between Device Fields or Interface Fields, click **Add Field** button on the top right corner and configure the following values.
    1. **Field Name:** Configure the name of the additional
    2. **Field Type:** Select the property type (text, numeric and date)
    3. **Field Length:** Set the length of the field.
    4. **Description :** Add a meaningful description for the field.
    5. Click **Save**

You can also import custom field properties from a CSV file. To do this, go to **Settings** ? **Configuration** ? **Custom Fields** ? **Import Values** button. Click **Browse** button and choose the CSV file containing the Custom Field properties for device or interface.

The properties added is applied to all the devices or interfaces. To view the Custom Fields, go to the respective Device or Interface snapshot page and check the **Custom Field** section.

> In Enterprise edition, the **'Add Field'** action can only be performed from the Central server. You cannot add new custom fields from the Probe servers.

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:

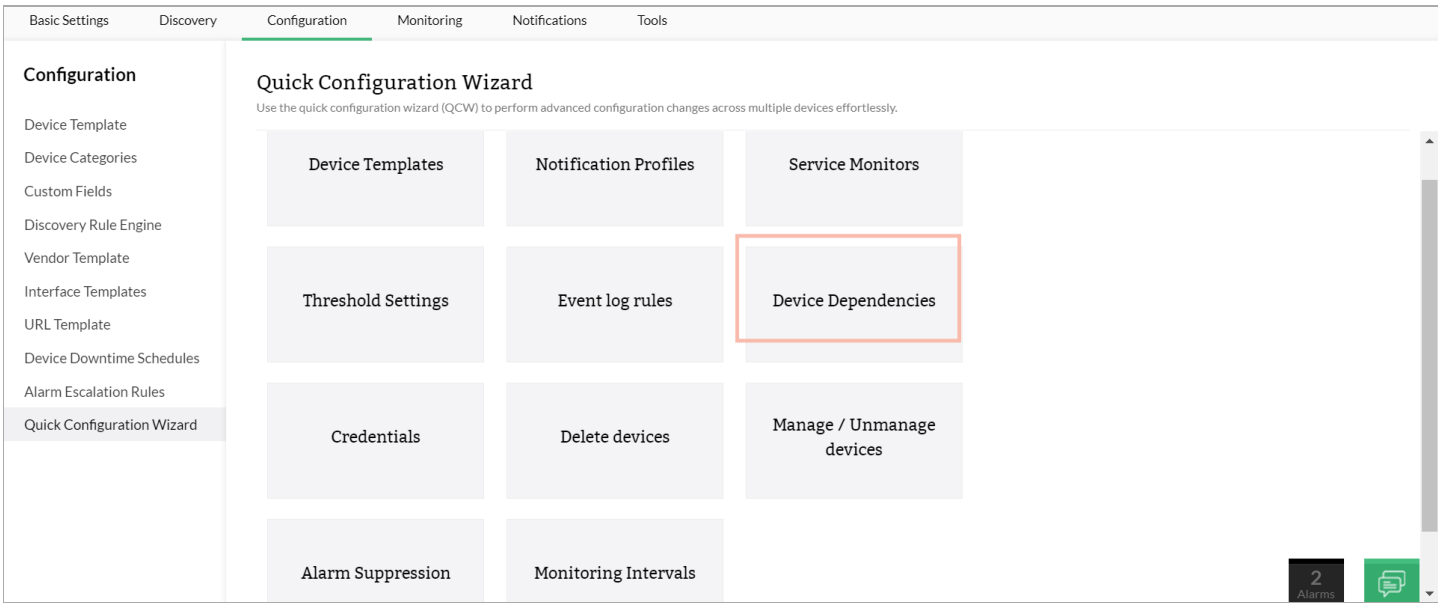
- Select **Settings** ? **Configuration** ? **Quick Configuration Wizard**.
- Select **Configure Device Dependencies** and click **Next**.
- Select a category from **Filter by category** to list the devices managed under a specified category. Select a device from **Select parent device** and click **Next**.

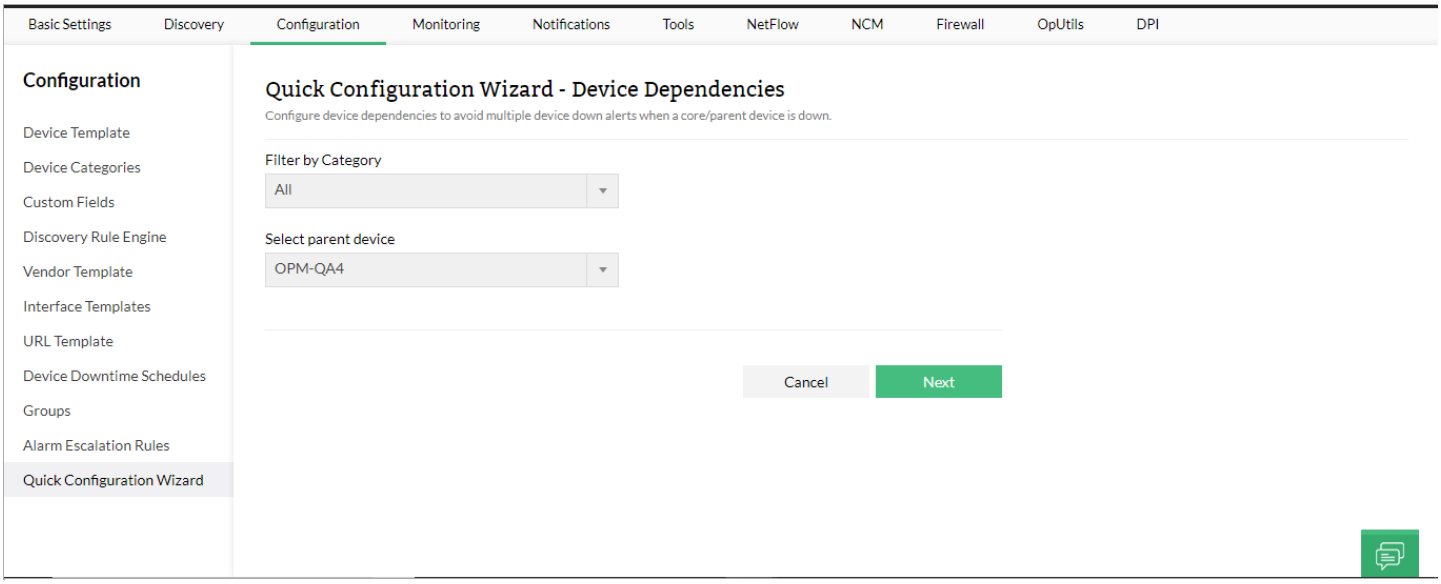
Select Device Dependencies in individual devices

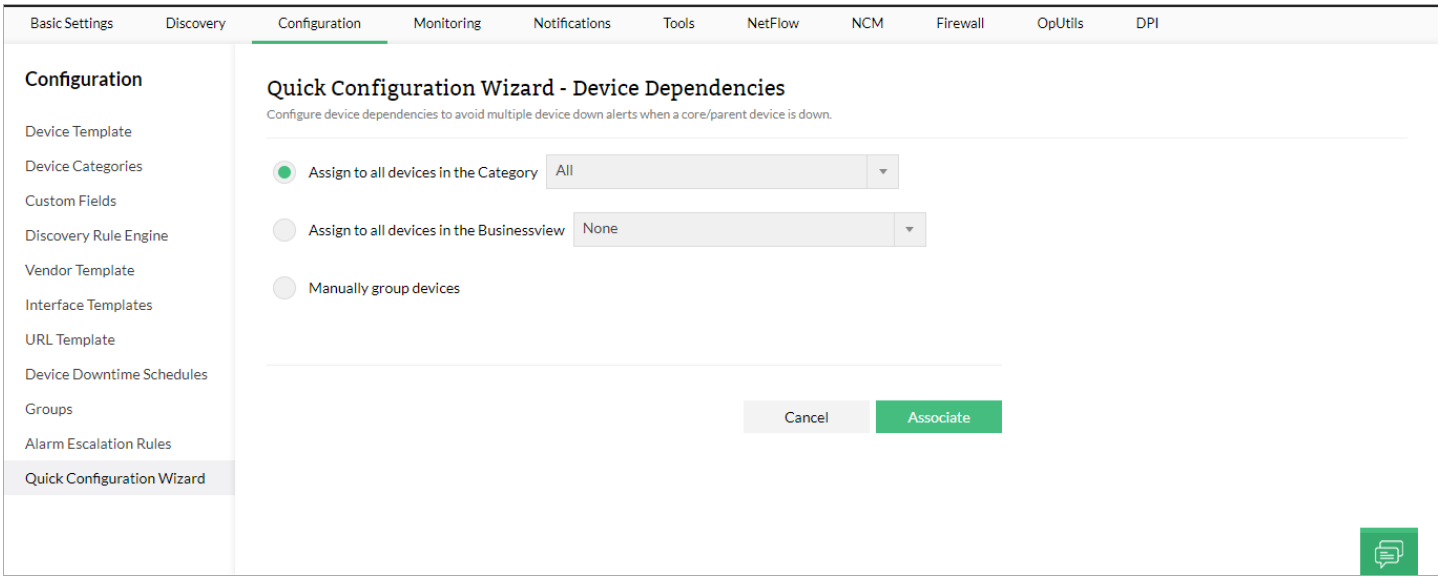
You can also configure dependencies for a single device from the device snapshot page. Here are the steps:

1. Go to the device snapshot page.
2. From the device details, click the link against the property **Dependency**.
3. Select the device on which it is dependent.

OpManager stops monitoring the devices if the dependent device is down. Configuring dependencies prevents false alarms.




Basic Settings
Discovery
Configuration
Monitoring
Notifications
Tools
NetFlow
NCM
Firewall
OpUtils
DPI
Configuration
Device Template
Device Categories
Custom Fields
Discovery Rule Engine
Vendor Template
Interface Templates
URL Template
Device Downtime Schedules
Groups
Alarm Escalation Rules
Quick Configuration Wizard
Quick Configuration Wizard - Device Dependencies
Configure device dependencies to avoid multiple device down alerts when a core/parent device is down.
Filter by Category
All
Select parent device
OPM-QA4
Cancel
Next


Basic Settings
Discovery
Configuration
Monitoring
Notifications
Tools
NetFlow
NCM
Firewall
OpUtils
DPI
Configuration
Device Template
Device Categories
Custom Fields
Discovery Rule Engine
Vendor Template
Interface Templates
URL Template
Device Downtime Schedules
Groups
Alarm Escalation Rules
Quick Configuration Wizard
Quick Configuration Wizard - Device Dependencies
Configure device dependencies to avoid multiple device down alerts when a core/parent device is down.
Assign to all devices in the Category
All
Assign to all devices in the Businessview
None
Manually group devices
Cancel
Associate

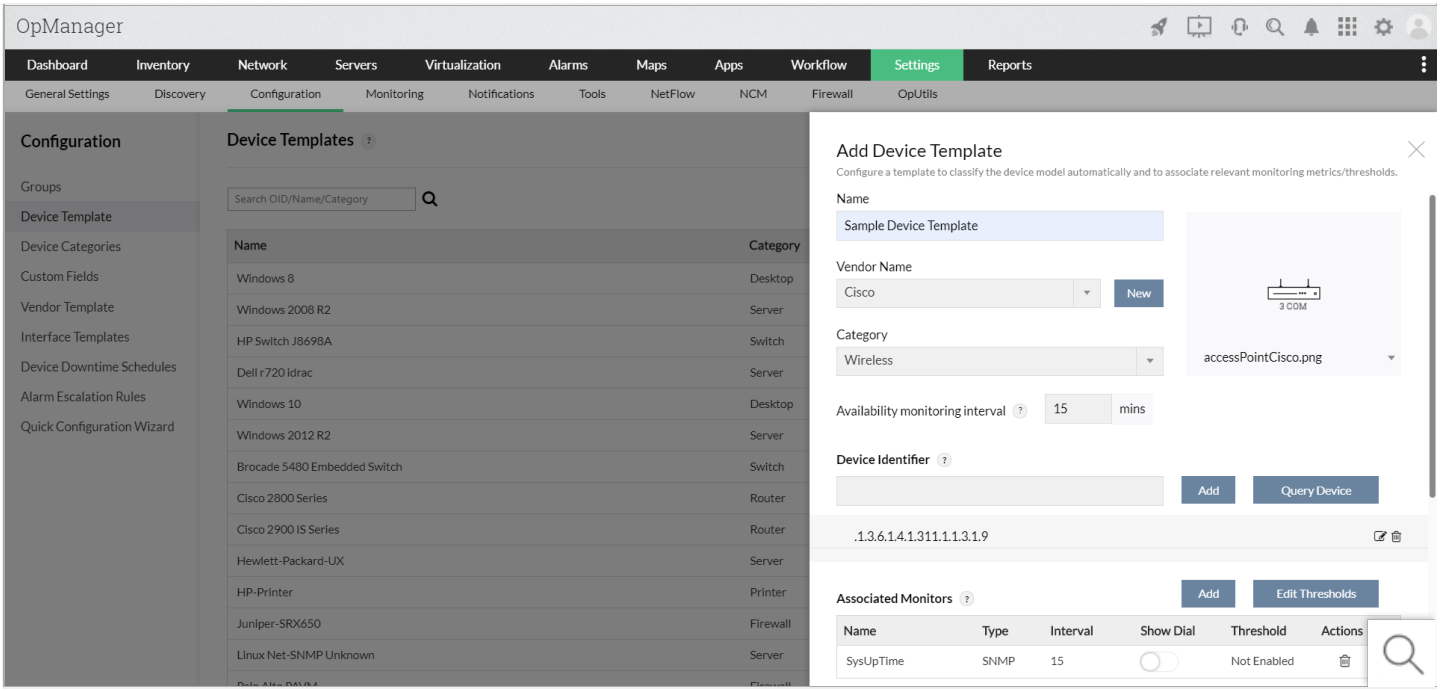
Configuring Device Templates

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.

OpManager comes with over 9000 device templates which carry the initial configurations to classify the devices into the pre-defined categories, and to associate monitors to them. The device templates enables you to effect a configuration once and is applied to several devices at a time whenever there is a change.

The templates carry the information required to classify the devices and to associate relevant monitors. You can define your own templates and modify the existing ones.

Creating/Modifying Device Templates



1. Go to **Settings ? Configuration ? Device Templates.**
2. Device Templates can also be **Imported** from ManageEngine Support / Community Forums / from a different instance of OpManager. Click here to learn how.
3. To define a template for a new device type, click **Add Template** and proceed with the steps given below.
4. To modify an existing template, click any existing **Template name**and configure/modify the following properties:

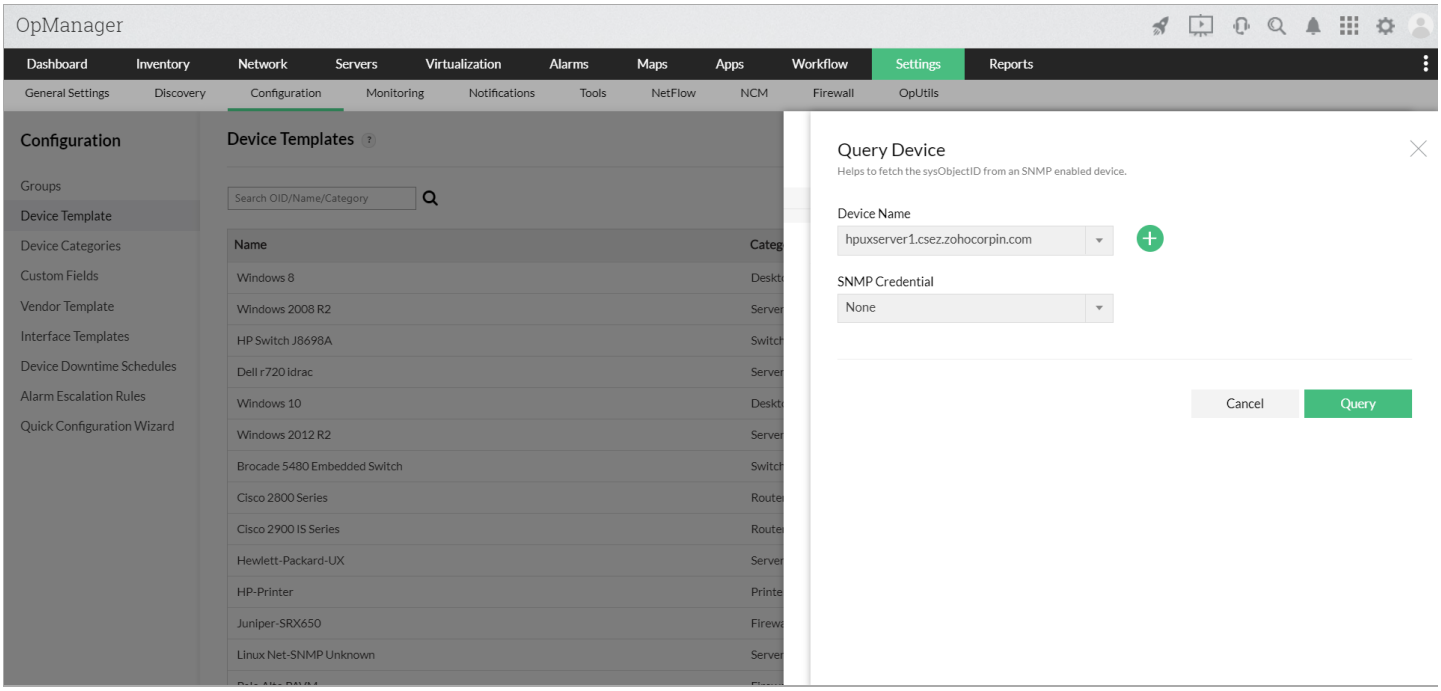
    - **Device Template**: Specify the device type.
    - **Vendor Name**: Select the vendor. Click **New** to add a new vendor, and **Save**.
    - **Category**: Select the category for the device type. On discovery, the devices are automatically placed in the select Category map.
    - **Monitoring Interval**: Configure the interval at which the device needs monitoring.
    - **Device Image**: Select the image for this device type.
    - **Device Identifier** : Type the sysOID and click **Add** (or) Click **Query Device** for OpManager to query the device for the OID.
    - **Associated Monitors**: Click on **Add** to add monitors. You can choose to add an existing monitor or create a new SNMP monitor.
    - **Edit Thresholds**: Click this option to edit thresholds of the Associated Monitors.
    - Click the **Save** button to save all the changes.

5. Device Templates are automatically associated to devices upon Discovery, however, it can also be done manually. To learn how to

manually associate a Device Template to a new device, click here.

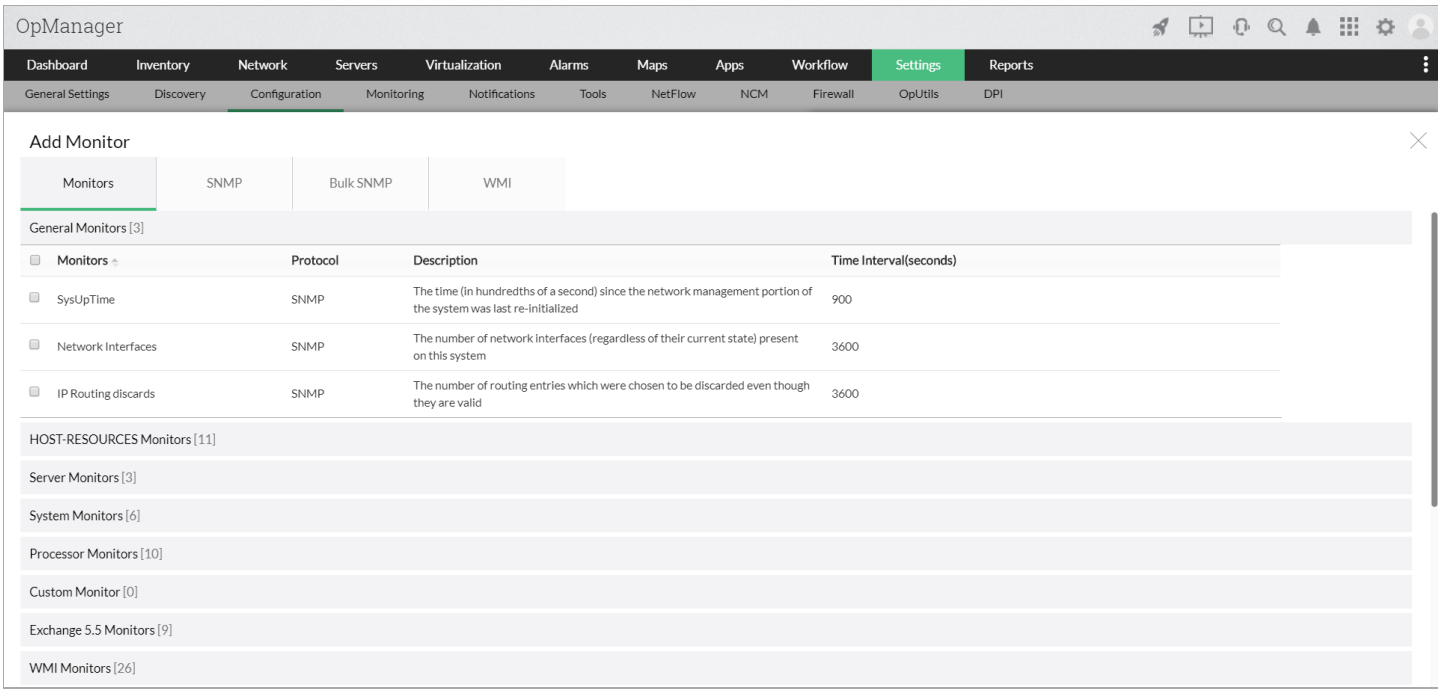
Device Identifier:

Device identifier is used to pin point an SNMP device by observing its sysOID. OpManager uses this feature to map the device to its respective device template. If you do not have the sysOID, you can also obtain it by querying an SNMP device of your network using **Query Device**. To further assist you with in \-depth device template classification, **Additional SysOIDs** can be employed. This is done by editing the existing sysOID and adding special criteria. Click here to learn more.



Associating Monitors:

Choose and add Monitors to the Device Template. These Monitors will automatically be associated to the devices upon discovery. You can choose from existing Monitors or create new ones.



- **Monitors:** Choose a monitor from an existing list.
- **SNMP:** Add SNMP monitors by selecting the Device name, SNMP OID and Functional Expression.

- **Bulk SNMP:** Choose to add SNMP monitors in bulk.
- **WMI:** Add WMI monitors by choosing Device Name, Credentials and specifying Monitoring Interval.

Device Classification:

The classified devices are placed under different categories for easy management. For proper device classification, make sure you have installed and started SNMP in all the network devices before starting OpManager service.

The default category includes:

- Servers
- Routers
- Desktops
- Switches
- Firewalls
- DomainControllers
- Load Balancer
- WAN Accelerator
- Wireless
- UPS
- PDU
- Printers
- Unknown
- Storage
- URLs
- WAN RTT Monitors
- VoIP Monitors

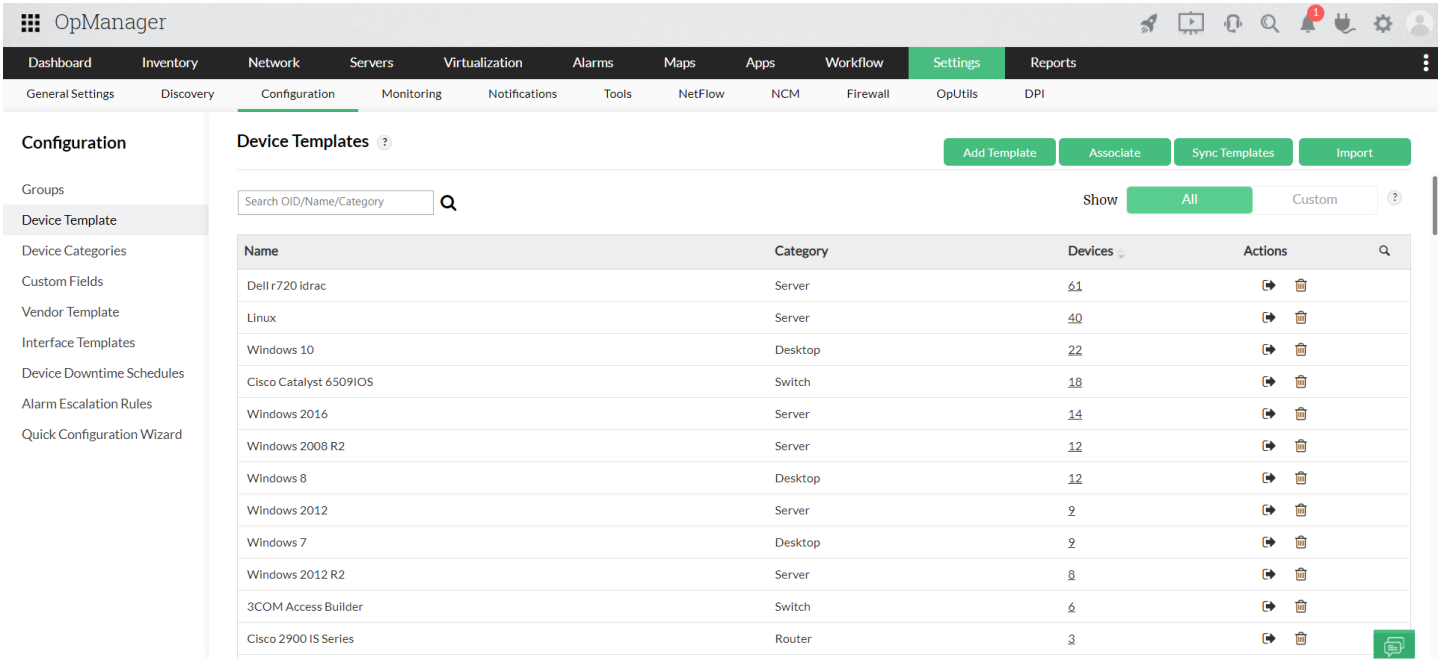
You can also add your own infrastructure views. For example, if you want to group a set of sensors, it will be absurd to classify them under servers or desktops. In such cases, the custom infrastructure allows you to create more defined groups by adding additional custom views.

This initial classification may not be accurate if -

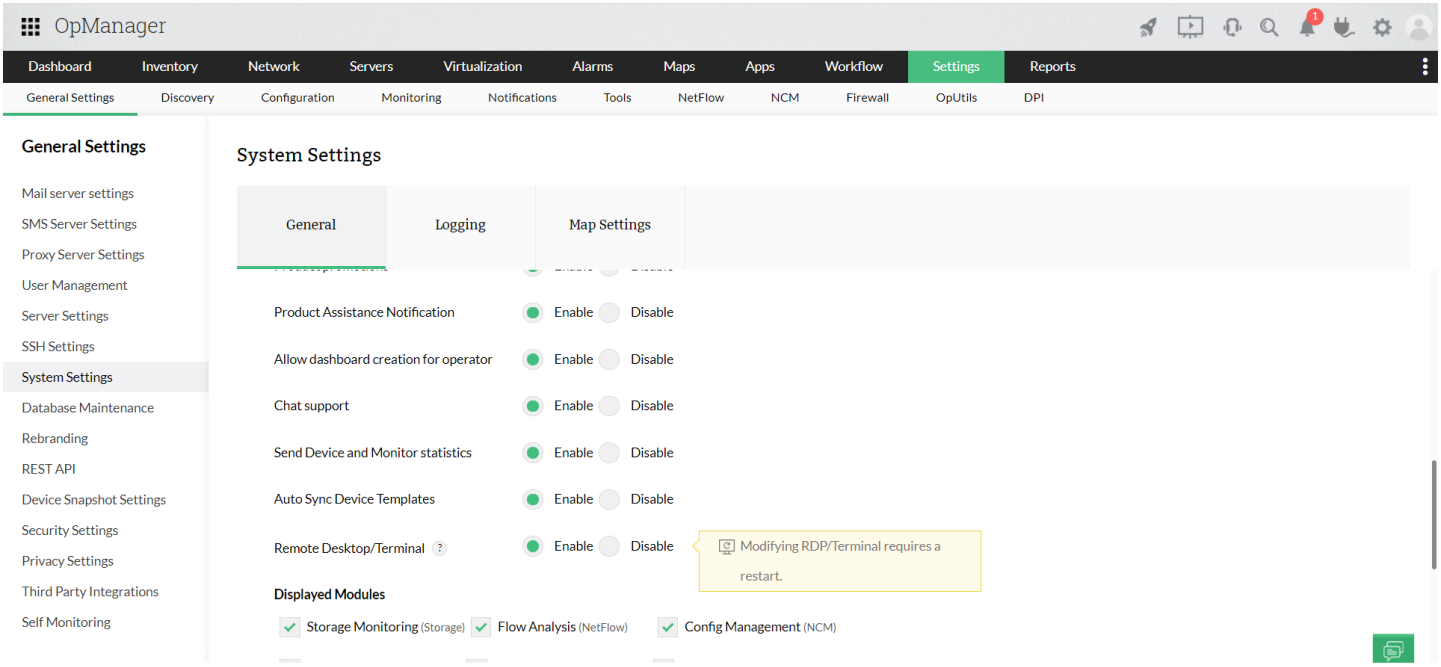
- The network devices do not support SNMP.
- Some devices have their SNMP settings different from those specified in the Credential Settings.

Sync new device templates

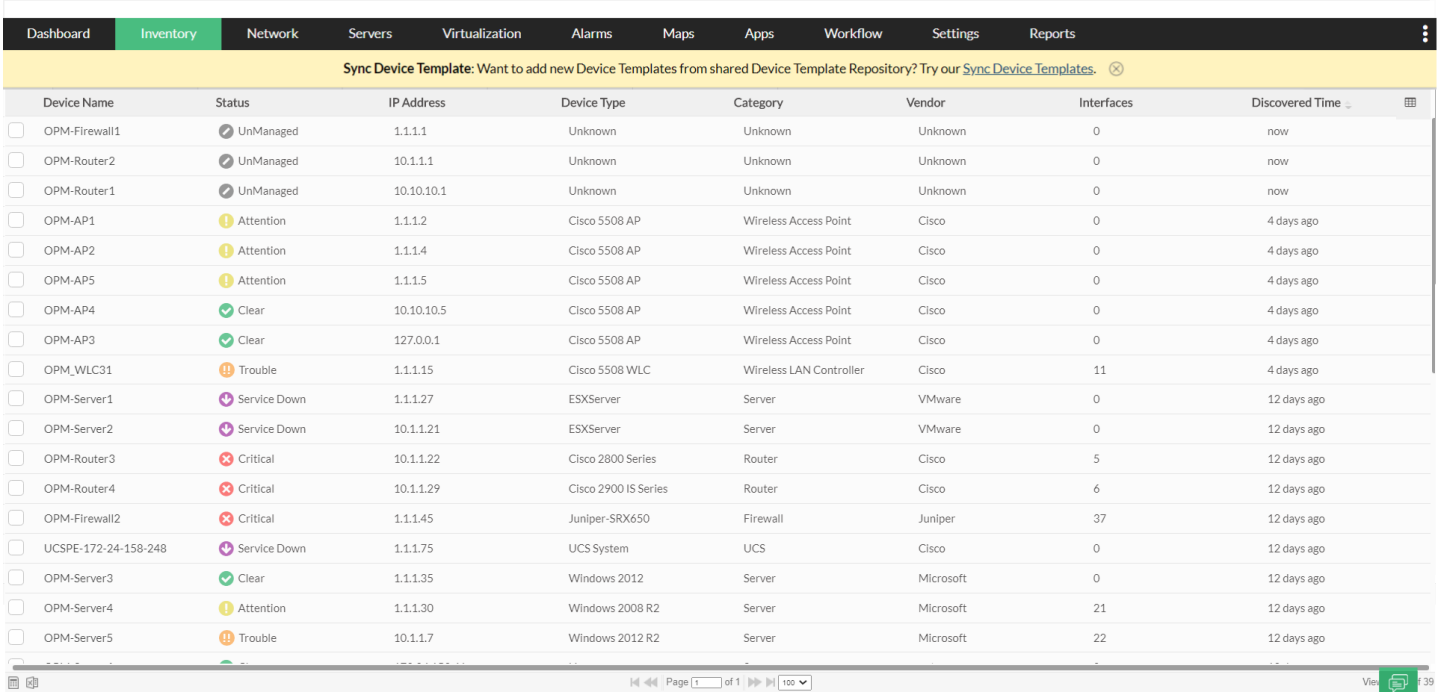
You can access the sync option by visiting Settings -> Configuration -> Device Templates -> Sync Templates.



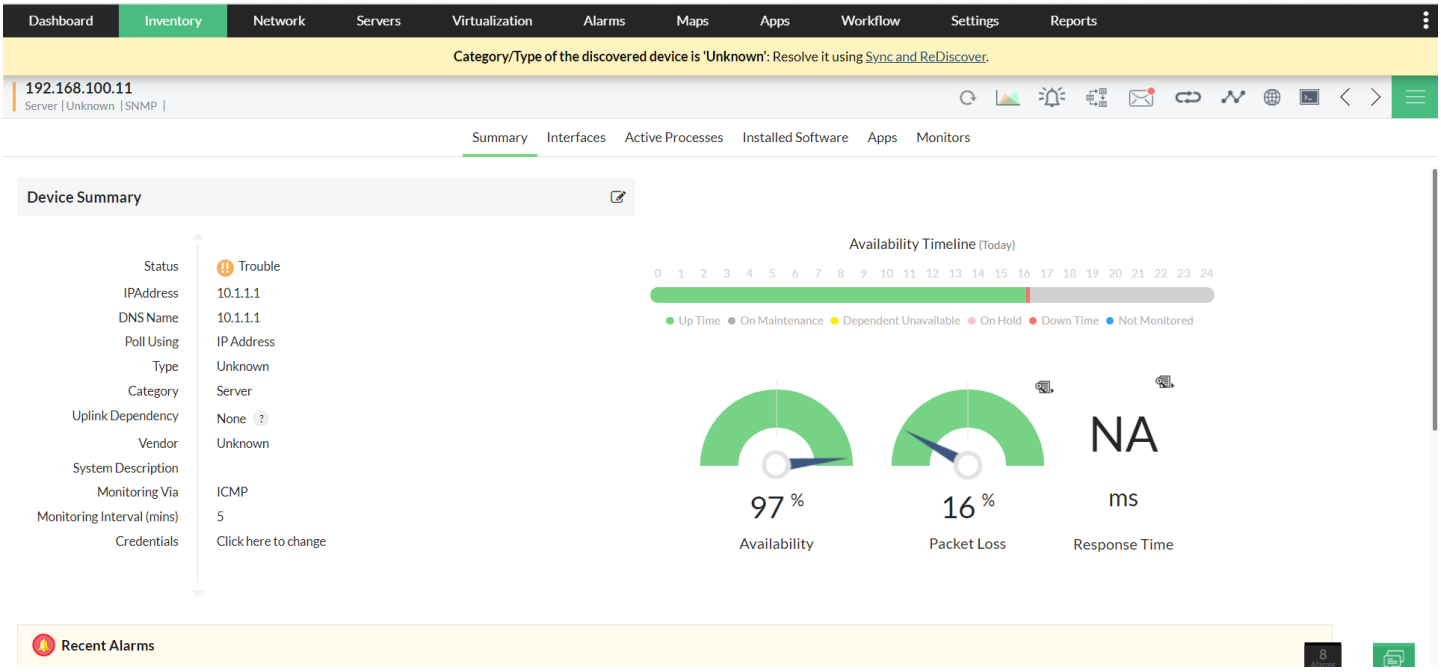
This will fetch and sync all new device templates from the shared repository of OpManager. You can also enable auto sync option. This enables you to discover new deivce templates at constant intervals.



You can enable auto sync by visiting Settings -> System Settings. But if the auto sync fails to for about three consecutive times due to connection issues, it will get disabled internally. However, on the product UI it would still appear as 'enabled'. To actually re-enable it you have to restart the service once again.



Auto sync will also be available in the inventory page. And when you drill down to the device snapshot page, you can see the 'sync and rediscover' option which allows you to rediscover the device which was perviously unavailable without the device template.



Configuring Interface Templates

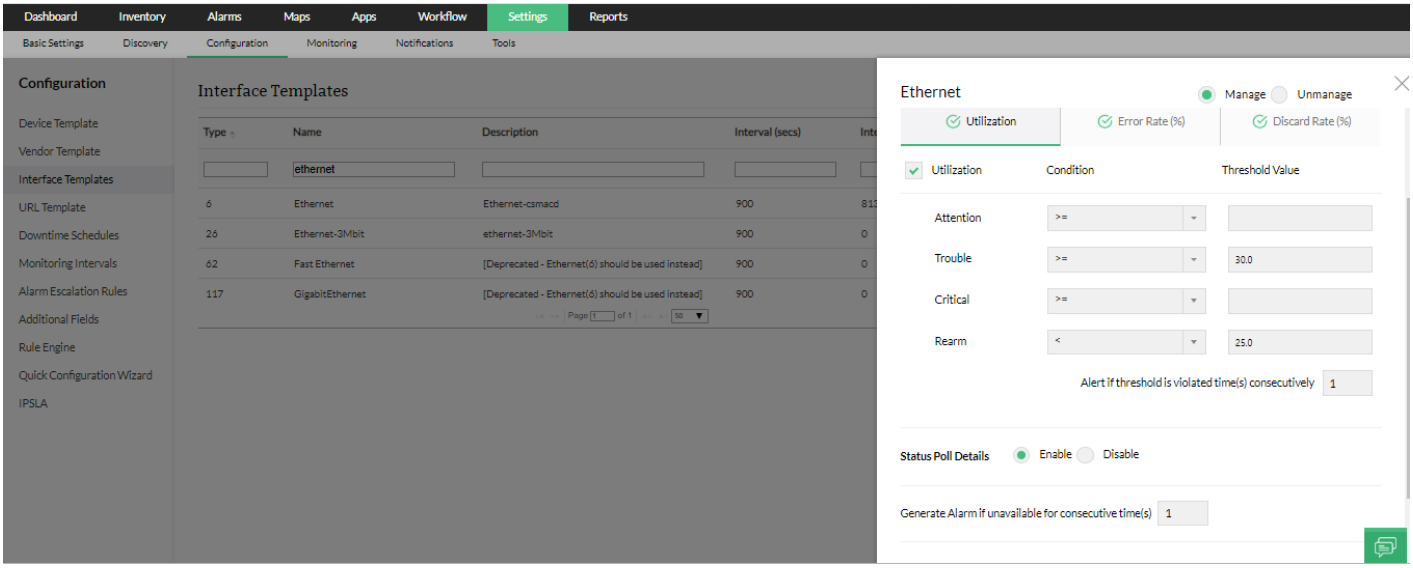
During initial discovery, OpManager categorizes the device interfaces into corresponding interface types with the help of predefined templates that are bundled with the product. OpManager comes with 292 interface templates which carry the initial configurations to classify these interfaces and associate monitors to them. Any changes made in the interface template will directly reflect on all the corresponding interfaces of the same type across all the devices in one go.

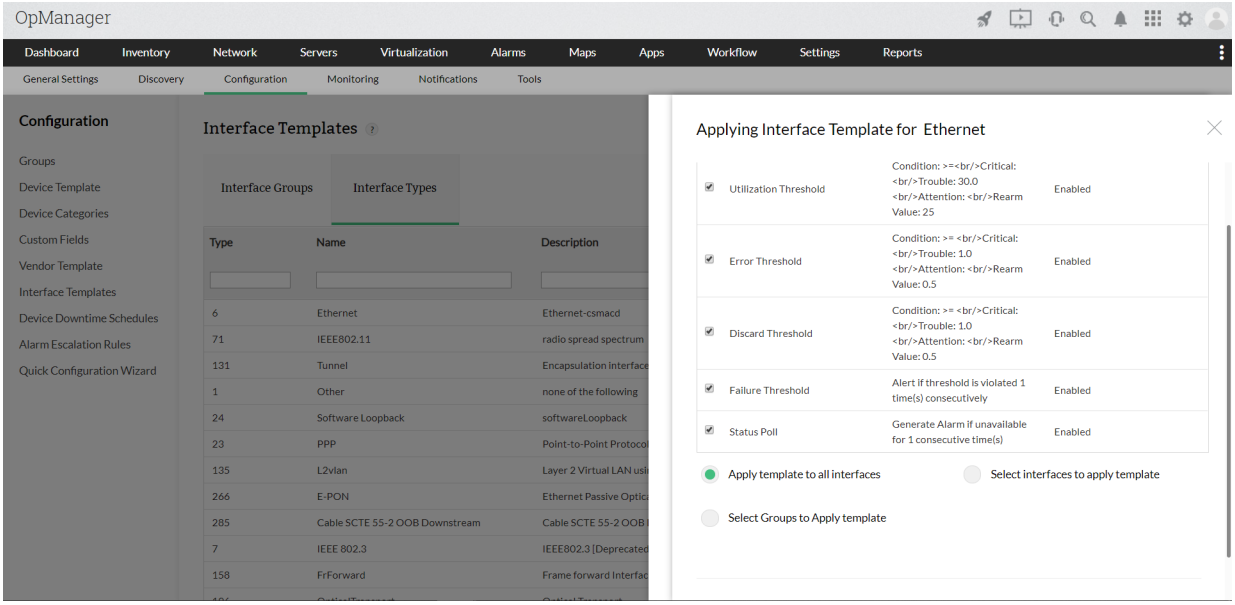
OpManager also allows the users to define multiple severity thresholds for interface templates, thereby generating alerts when the threshold values are violated.

Modifying Interface Templates

1. Go to **Settings** > **Configuration** > **Interface Templates**
2. Under **Interface Types**, search for the template you wish to edit and click on it. Don't forget to use the All/Common toggle at the top right to list all type of interfaces.
3. Configure/Modify the following properties:

- **Manage/UnManage**: Specify whether the interfaces belonging to the template must be managed or unmanaged.
- **Monitoring interval**: Select the interval at which this interface type must be polled to fetch monitoring data & availablity status.
- **Configure Thresholds:** The threshold values for Utilization, Error Rate and Discard Rate can be specified under the corresponding tabs. OpManager also allows you to configure **multiple severity thresholds** for the same. Enter the threshold values for Attention, trouble, discard and rearm. If the threshold values are violated, corresponding alarms will be raised. You can also configure thresholds for Interface groups.
  Note: To stop monitoring the Utilization / Error Rate / Discard Rate, uncheck the checkbox in the corresponding tabs.
- **Status poll** : Poll the interface for its availability using **SNMP** (ifAdminStatus & ifOperStatus).





NOTE: Selecting ***Apply template to all interfaces***, ***Select interfaces to apply template*** or ***Select Groups to apply template*** option will completely override the existing interface configurations.

Categorization into Default Maps

Devices are categorized into the following default maps in OpManager: The classification is done using SNMP and NMAP.

- Servers
- Routers
- Desktops
- Switches
- Firewalls
- DomainControllers
- Load Balancer
- WAN Accelerator
- Wireless
- UPS
- Printers
- PDU
- Virtual Device
- UCS
- Unknown
- Storage
- URLs
- WAN RTT Monitors
- VoIP Monitors

The discovered devices are classified into the above categories based on response to SNMP requests sent by OpManager to the devices. The devices that are not SNMP enabled, and the device types which are not included in the template are incorrectly classified under desktops. You can also add your own infrastructure maps to group your devices according to categories, or create business views to logically group devices, for instance, based on geography.

Adding new Infrastructure Views

You can create more defined groups by adding more custom views. For instance, you might want to group all your Environment Sensors or IP Phones into separate infrastructure views.

Steps to add a new Infrastructure View:

- Go to **Inventory ? Sort By Category ? Add Category.**
- Specify the category **Name**.
- Select the category whose properties needs to be inherited for this category.
- Click **Add**.

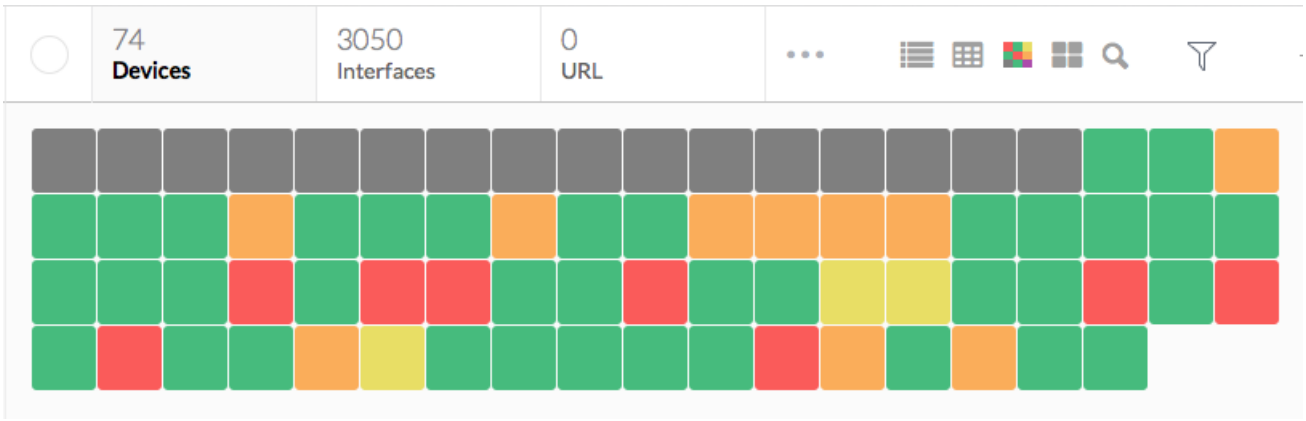
After you create new infrastructure views, you can create device templates for devices of this category. This allows you to define monitors specific to the category and automatically applies the configurations defined in the template to the devices as soon as they are discovered.

Different Types of Views

Heat Map View

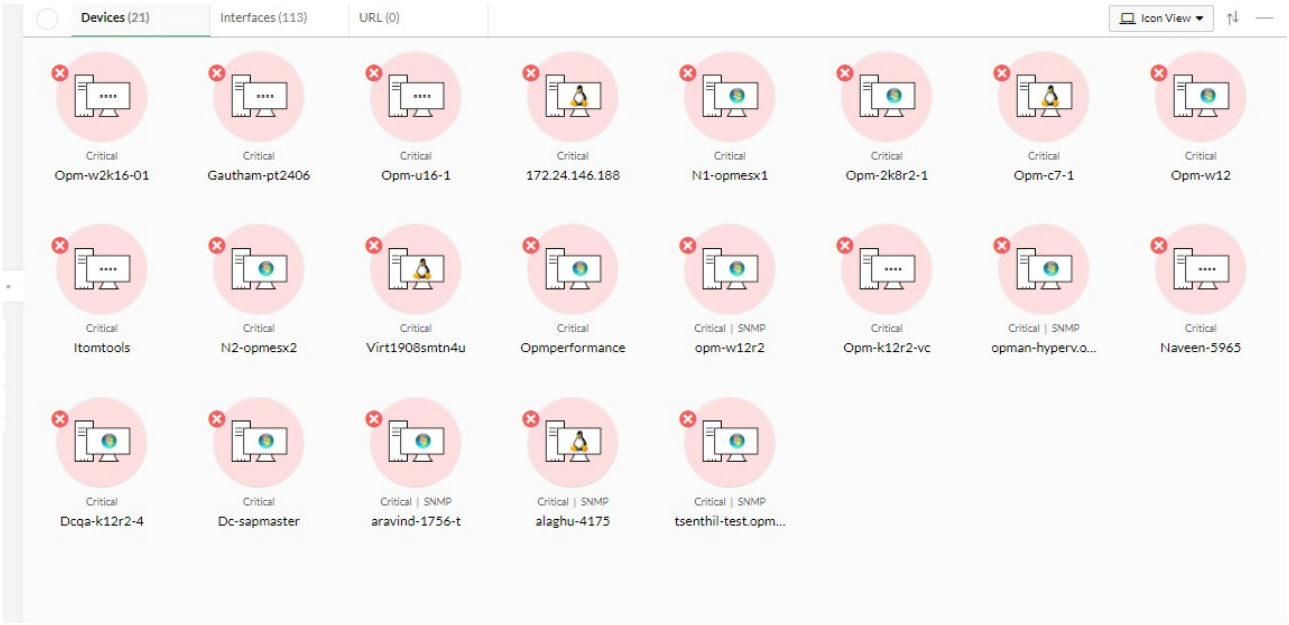
It helps you to visualize your entire network health in real-time from a single page. It uses color codes to communicate the severity of the monitored devices. HeatMap view can be accessed from the Inventory > All Devices, Server, Router, Server, Desktop&#65533; etc.

&#65533;



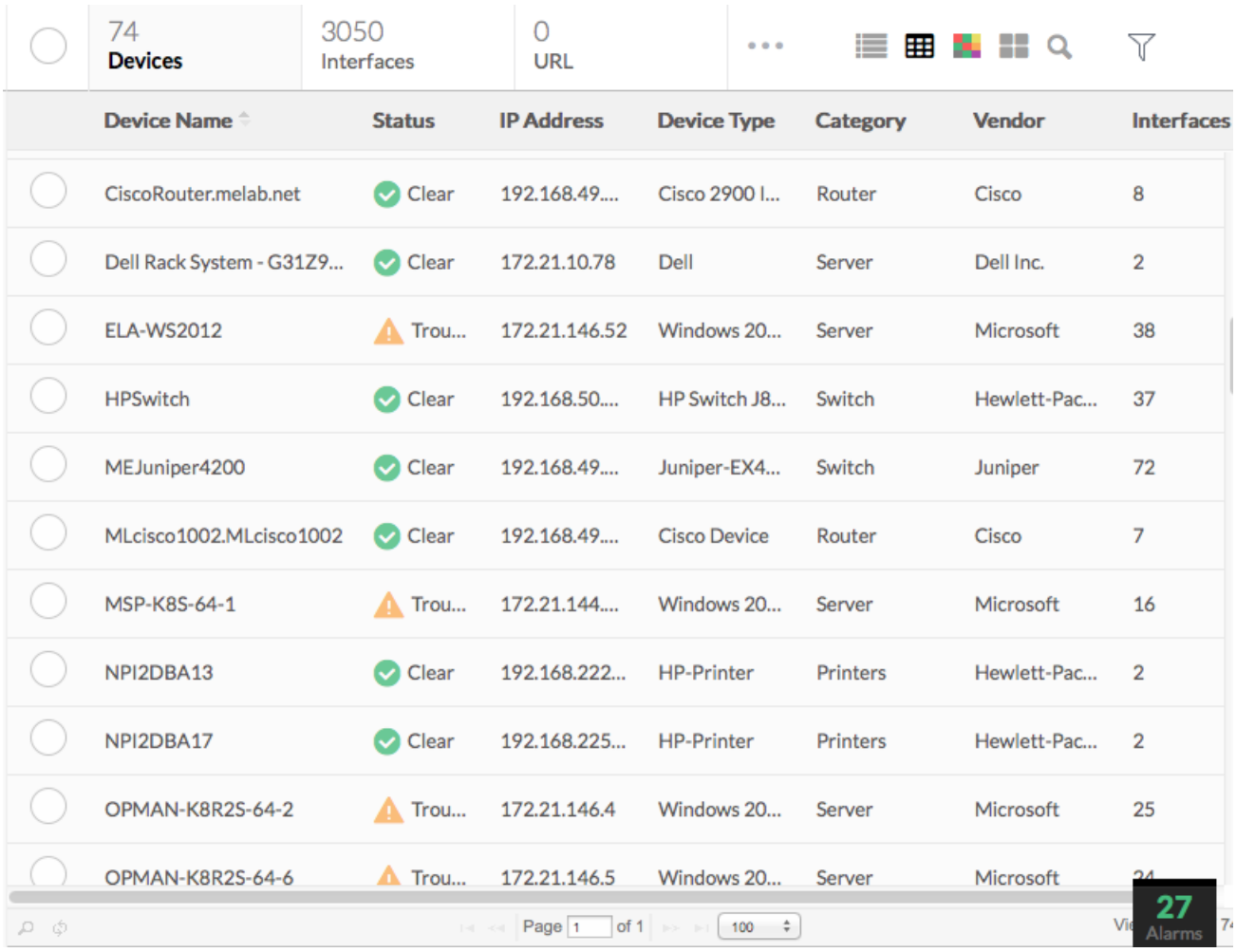
&#65533;

Icon View



&#65533;

List View


74
Devices
3050
Interfaces
0
URL
Device Name
Status
IP Address
Device Type
Category
Vendor
Interfaces
CiscoRouter.melab.net
Clear
192.168.49....
Cisco 2900 I...
Router
Cisco
8
Dell Rack System - G31Z9...
Clear
172.21.10.78
Dell
Server
Dell Inc.
2
ELA-WS2012
Trou...
172.21.146.52
Windows 20...
Server
Microsoft
38
HPSwitch
Clear
192.168.50....
HP Switch J8...
Switch
Hewlett-Pac...
37
MEJuniper4200
Clear
192.168.49....
Juniper-EX4...
Switch
Juniper
72
MLcisco1002.MLcisco1002
Clear
192.168.49....
Cisco Device
Router
Cisco
7
MSP-K8S-64-1
Trou...
172.21.144....
Windows 20...
Server
Microsoft
16
NPI2DBA13
Clear
192.168.222...
HP-Printer
Printers
Hewlett-Pac...
2
NPI2DBA17
Clear
192.168.225...
HP-Printer
Printers
Hewlett-Pac...
2
OPMAN-K8R2S-64-2
Trou...
172.21.146.4
Windows 20...
Server
Microsoft
25
OPMAN-K8R2S-64-6
Trou...
172.21.146.5
Windows 20...
Server
Microsoft
Page 1 of 1
100
27
Alarms

What is a group?

The Group feature in OpManager helps the admin group devices or interfaces together for organized network management and to push bulk configurations easily throughout the product. Groups and subgroups can be used as a filter in Reports, Widget, Notification Profile, URL Templates, Downtime schedule, Alarm suppression, Device template, Interface template, Test credentials and Workflow. Groups are useful to view the average availability distribution of all the members in a group, automatically add members to a group on discovery and to configure threshold for a group of interfaces irrespective of the interface type. Admin users will have complete access to groups whereas, operator users will have only Read-Only access to groups.

What is Grouping?

What is a subgroup?

OpManager allows you to create subgroups within a group. Subgroups make bulk configuration and filtering of devices much more easier. You can create multiple subgroups and associate it with a parent group.

For eg:

Consider two device groups - "Routers of model A" and "Routers of model B" in an organization. They can be collectively grouped under a parent group called "Routers".
Similarly two device groups - "Central Servers" and "Production servers" can be created and placed under a parent group called "Servers".

The two parent groups - "Routers" and "Servers" can be placed under a group "Network devices in India", which now becomes the parent group.

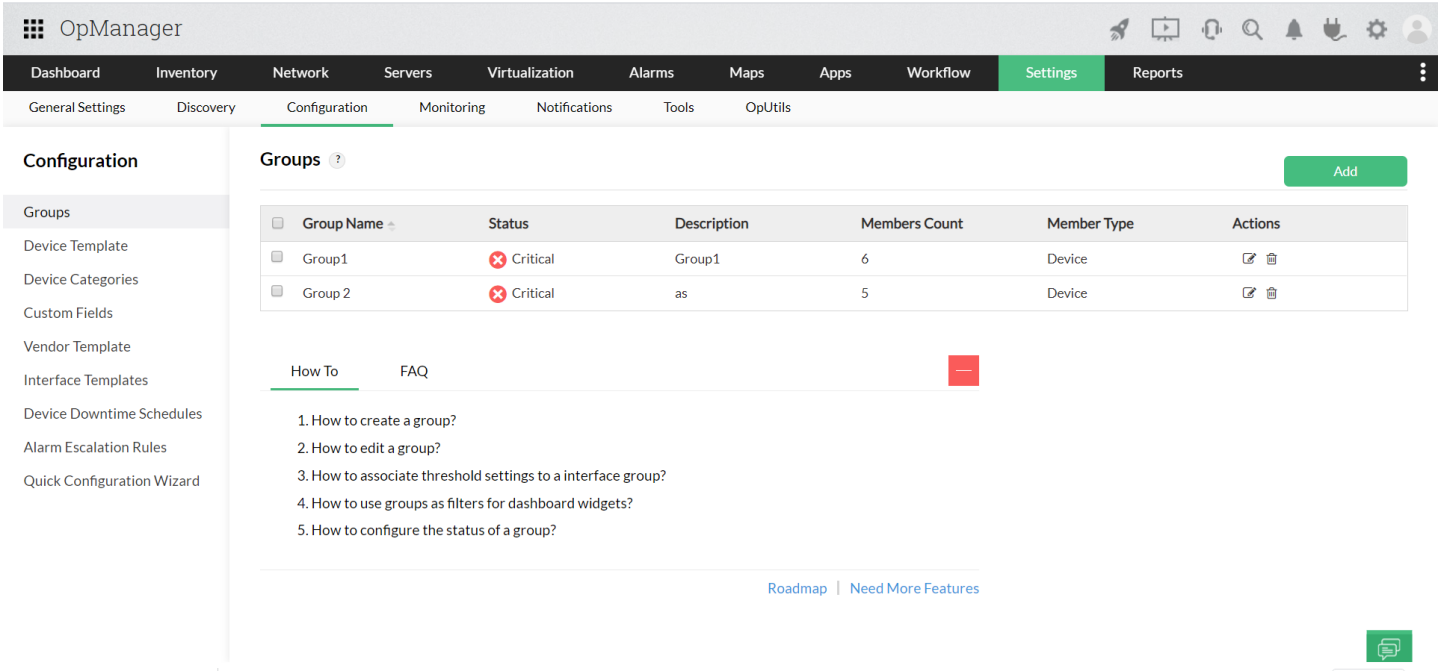
In Reports/Widgets, when "Network devices in India" group is selected, OpManager provides a detailed report of all the devices under the subgroups present under the parent group -&#65533; "Network devices in India".

Similarly the subgroup feature can be used in any module where grouping is supported.

How to create a group?

Steps to create a group

- Click on **Settings** → **Configuration** → **Groups** and click on the "**Add**" button or go to **Inventory** → **Groups** → **Add Group**.
- Provide a suitable **group name** and **description** and click on **Next**.
- Select the type of **elements** you want to add to this group.
- Select the **method to group** the elements. You can group elements either 'Manually' or by 'Criteria'.
- If you selected the '**Manually**' option - Select the group members from the available list and click on 'Next'.
- If you selected the '**By criteria**' option - Select any one of the property available from the dropdown box, select a condition and provide a suitable value resolving the property and condition and click on&#65533; '**+**' icon.
- Add multiple criteria if needed, along with the logical operation&#65533; you need to perform based on the criteria. Click on **Next**.
- From the available members listed, **select the members** you want the group's health to depend on. If no members are chosen, then the health status of the group will depend on&#65533; all the available members by default.



How to edit a group?

- Click on **Settings** → **Configuration** → **Groups** and click on the '**Edit**' icon under '**Actions**'. You can also edit Groups from **Inventory** → **Groups** → and click on the '**Edit**' icon under '**Actions**'
- Edit the description if needed and click on '**Next**'.
- The group type and method of creation of the group cannot be edited.
- If the '**Manually**' option was selected - Edit the group members from the available list and click on 'Next'.
- If the '**By criteria**' option was selected - The existing criteria can be deleted and new criteria can be added if required. Click on 'Next'.
- From the available members listed, edit the members you want the group's health to depend on.

How to create a group based on custom fields?

Groups can be created based on custom fields. Create a group with '**By Criteria**' method and select the '**custom fields**' properties from the drop down box. Select the suitable condition required and provide a custom field value associated to devices/interfaces.

How to associate threshold settings to an interface group?

Interface Groups :

- Click on **Settings** → **Configuration** → **Interface Templates**. Under the Interface groups tab, click on a group name and **configure the threshold settings**. Click on '**Save and Apply**'.
- The configured threshold values will be applied to all interfaces in a group irrespective of type.

Interface Types :

- Click on **Settings** → **Configuration** → **Interface Templates**. Under interface types, click on a interface type name and configure the threshold values. Click on '**Save and Apply**'.
- In the new tab displayed, click on "**Select groups to apply**" option and click on '**Save**'.
- The threshold will be applied only to interfaces of the selected type.

How to configure status of a group?

While creating a group, you can configure the health status of the group. The health status of the group will depend on the members

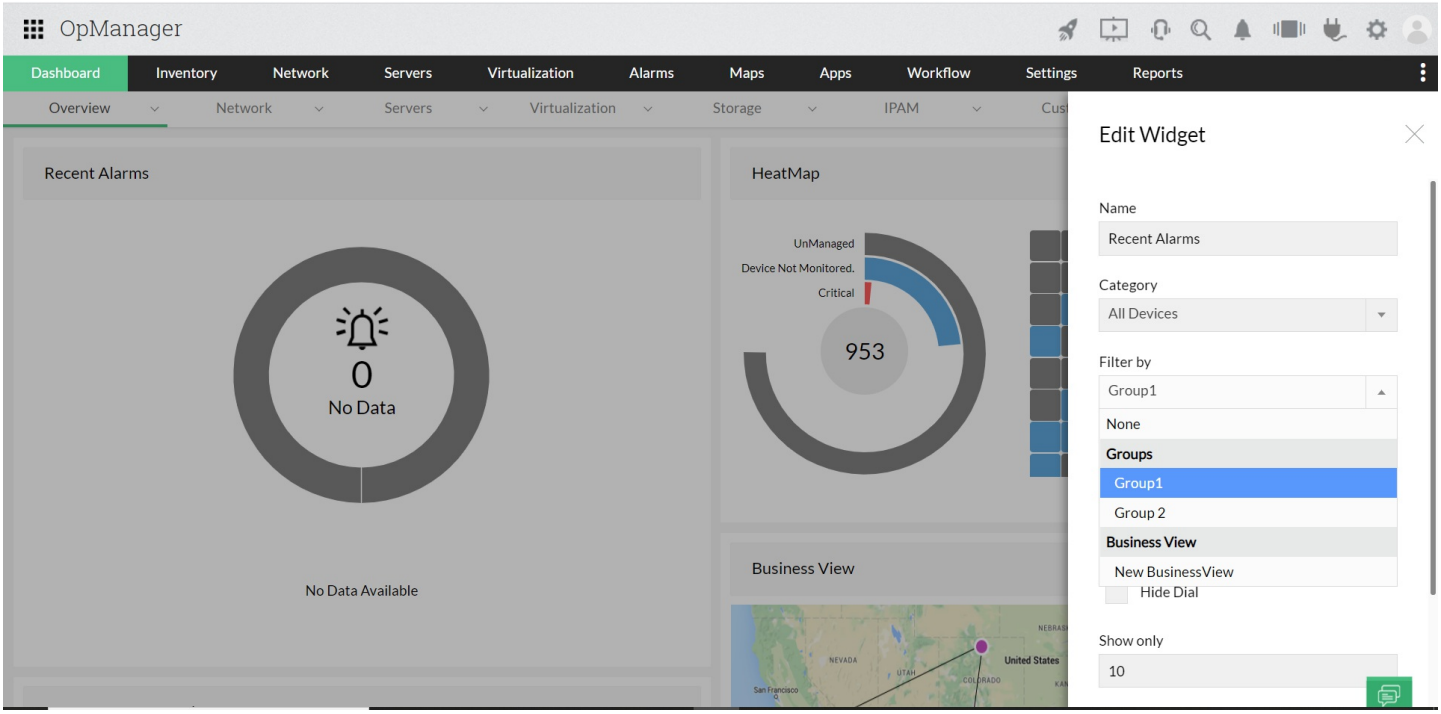
selected. If no member is selected, by default the health status will depend on all available group members.

How to use groups as filters for dashboard widgets?

Groups can also be used as a filter in the dashboard. You can customize the widgets to display only specific data or devices based on your requirement using Groups.

Steps to use Groups in dashboard:

- In the **Dashboard**, click on the '**Edit**' icon in any widget.
- In the 'Edit' widget menu, select groups under the **'filter by**' drop menu and click on **'Save'**.

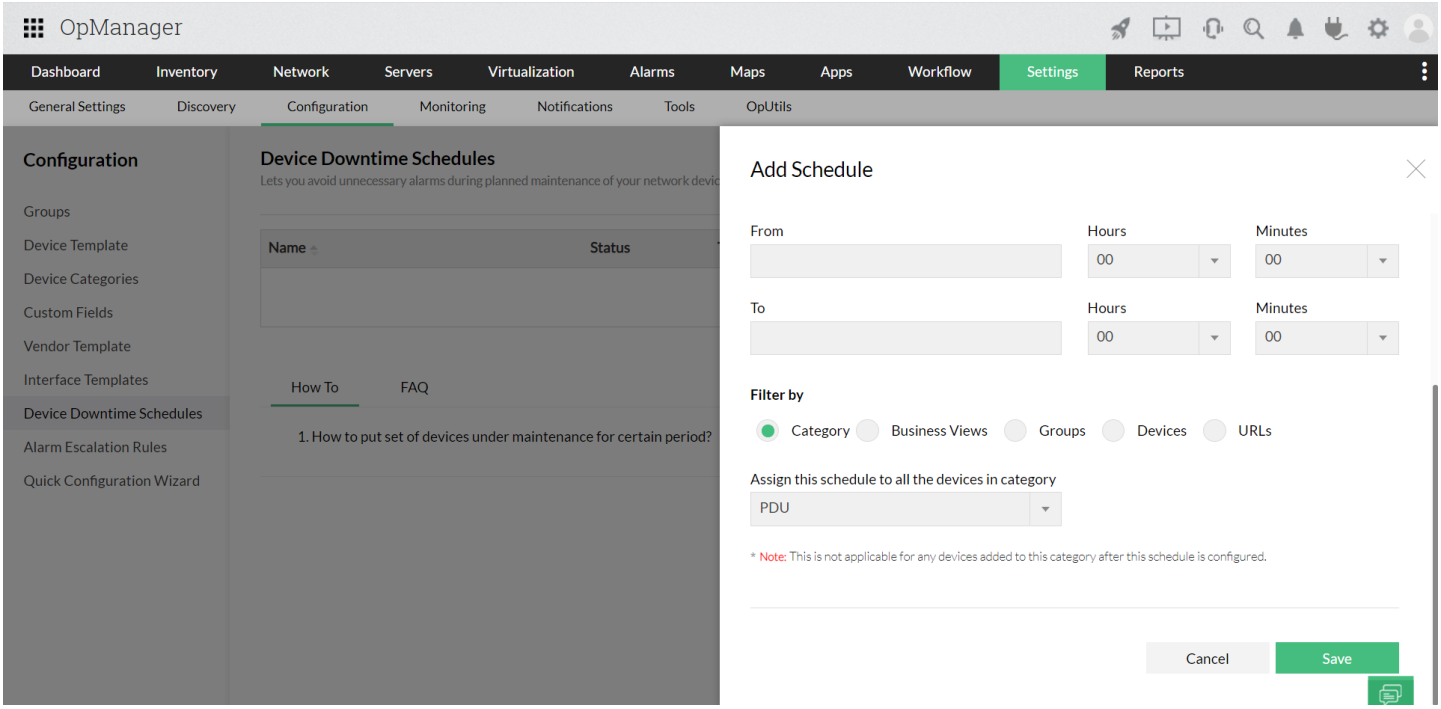


You can also view the availability data in the 'all groups' widget in the dashboard of OpManager.

How to create device downtime schedules for groups?

IT admins can now configure device downtime schedule for 'Groups' to prevent OpManager from polling those devices during maintenance for availability.

- Visit **Settings -> Configuration -> Device Downtime Schedules.**
- Click on 'Add Schedule'.
- Choose filter by 'Groups' after filling the relevant fields.


OpManager
Dashboard
Inventory
Network
Servers
Virtualization
Alarms
Maps
Apps
Workflow
Settings
Reports
General Settings
Discovery
Configuration
Monitoring
Notifications
Tools
OpUtils
Configuration
Groups
Device Template
Device Categories
Custom Fields
Vendor Template
Interface Templates
Device Downtime Schedules
Alarm Escalation Rules
Quick Configuration Wizard
Device Downtime Schedules
Lets you avoid unnecessary alarms during planned maintenance of your network devic
Name
Status
How To
FAQ
1. How to put set of devices under maintenance for certain period?
Add Schedule
From
Hours
Minutes
00
00
To
Hours
Minutes
00
00
Filter by
Category
Business Views
Groups
Devices
URLs
Assign this schedule to all the devices in category
PDU
* Note: This is not applicable for any devices added to this category after this schedule is configured.
Cancel
Save

AD Authentication

Identity and Access Management is an important part of network and data security for any organization. It helps you ensure compliance with policies, password management and acts as a means to administer access control to users.

The AD Authentication feature in OpManager helps you with just this. It allows you to authenticate users from within OpManager without using an external third party identity management tool. It allows you to grant / revoke access & security restrictions to users and also allows you to provide role based access control for accessing OpManager within your organization.

You can make Active Directory's password policy work for you if you have a Windows domain. Users login to OpManager using their domain login name and password. This will greatly minimize the risk of making others using your password to access the OpManager Web interface, thereby not just improving the security but also making it easier for users to login/create accounts. You can define a scope for users (AD groups, remote offices or all users), thereby restricting their access based on their roles.

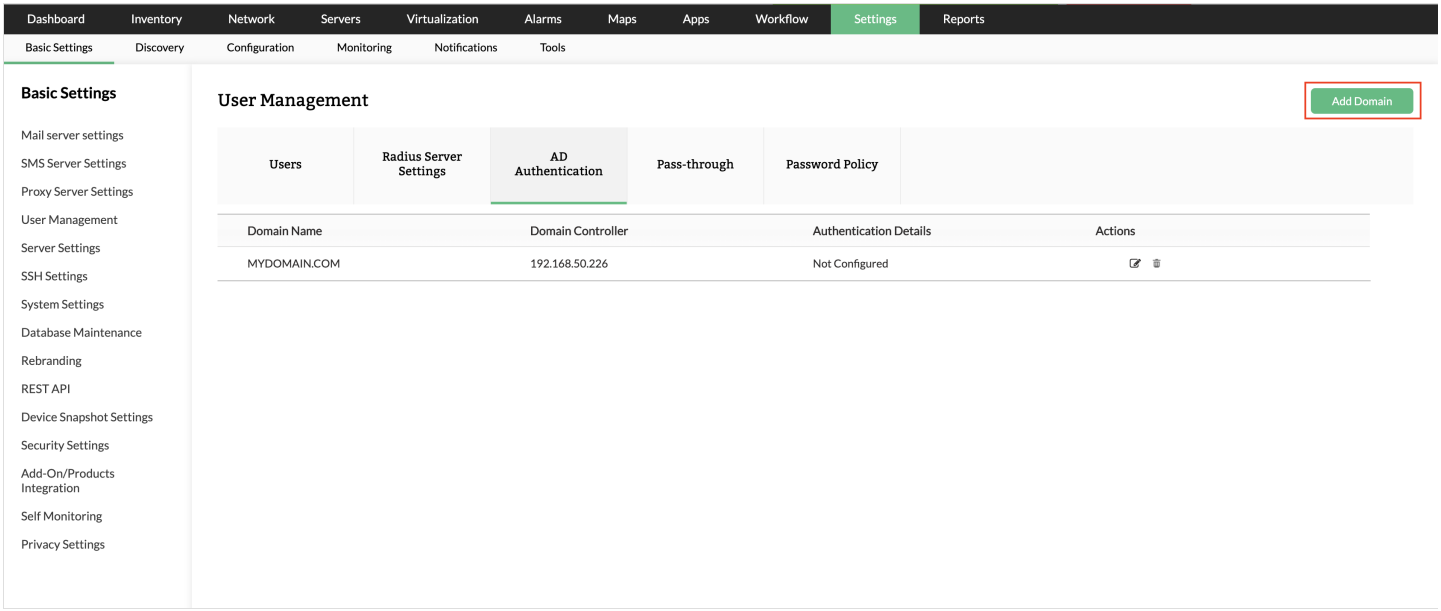
With the increase in software applications, each with their own authentication and password complexity levels, this feature also saves you the trouble of having to remember way too many passwords.

Add an AD Domain

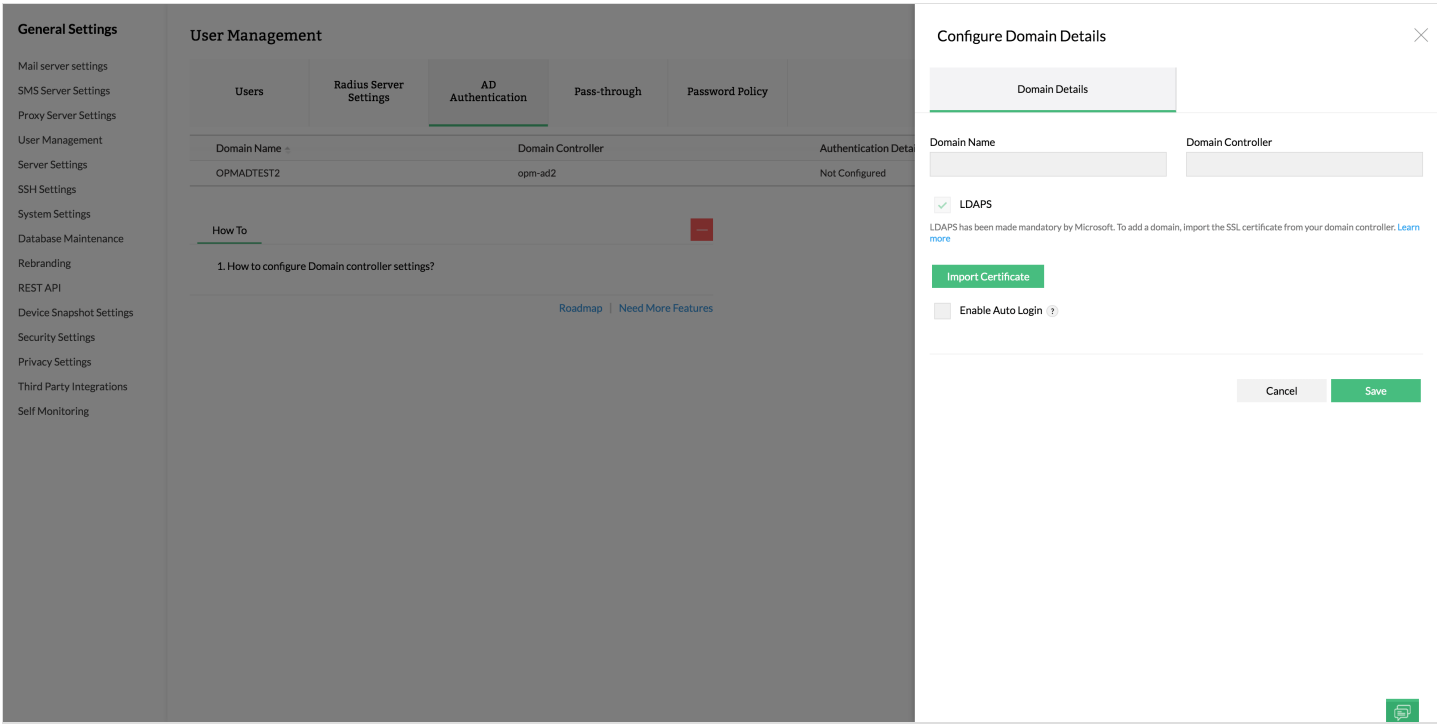
You can create Domains in OpManager and users manually in OpManager with the AD Authentication and User Management features.

To add a domain:

1. Go to **Settings** ? **General Settings** ? **User Management** ? **AD Authentication** ? **Add Domain**.



2. Enter the **Domain Name** and the **Domain Controller name** in the respective fields.



3. If you are on builds **125111 and above,** you can see that LDAPS authentication is mandatory when you add a new domain, to ensure secure communication with the domain controllers. Simply click on the **'Import Certificate'** button and select your domain controller's certificate to add it to OpManager.

To know more on how to export a certificate from your domain controller, check out these articles:

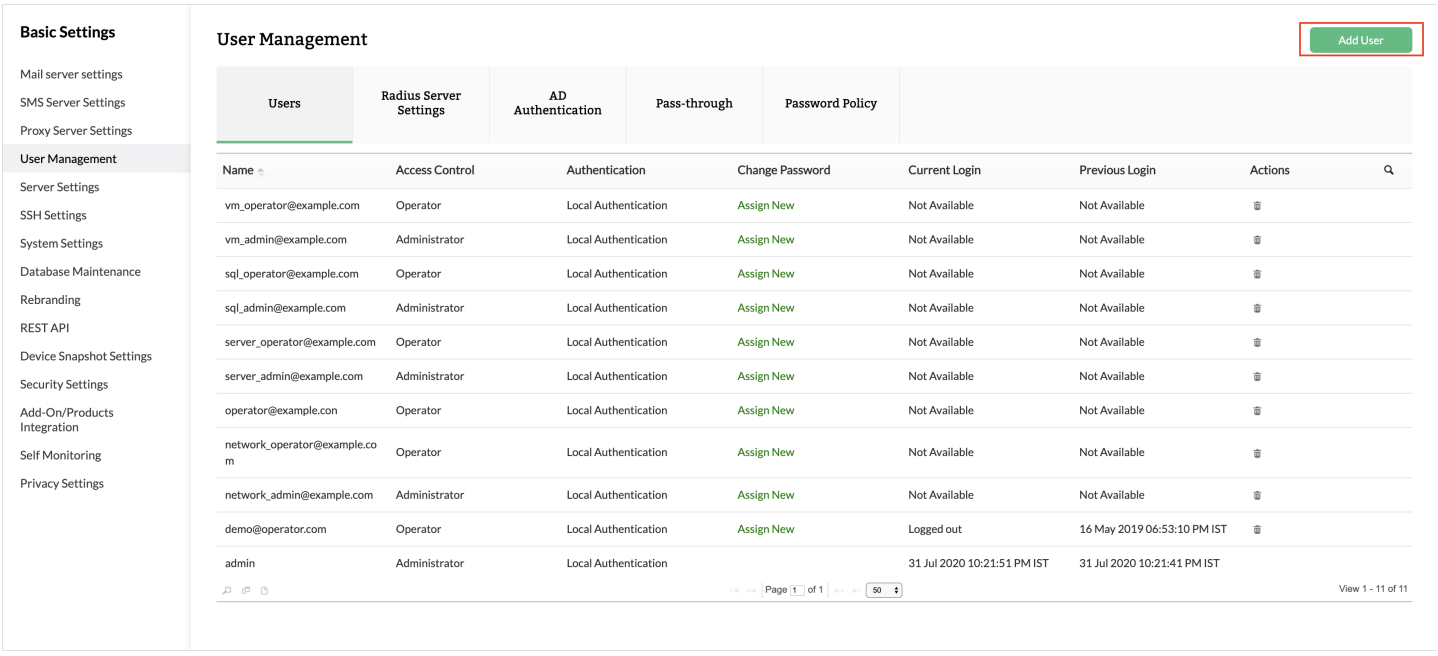
1. Exporting the LDAPS Certificate and Importing for use with AD DS
2. LDAP over SSL (LDAPS) Certificate

Note: When you upgrade from a lower version of OpManager to 125111 or above, LDAPS is mandatory only for the domains that you will be adding after the upgrade. For domains that are already present in OpManager, it is optional. You can just click on the **'Edit'** button to import certificates for your existing domains.

4. **Auto Login*** is disabled by default.

5. **Save** the Settings.

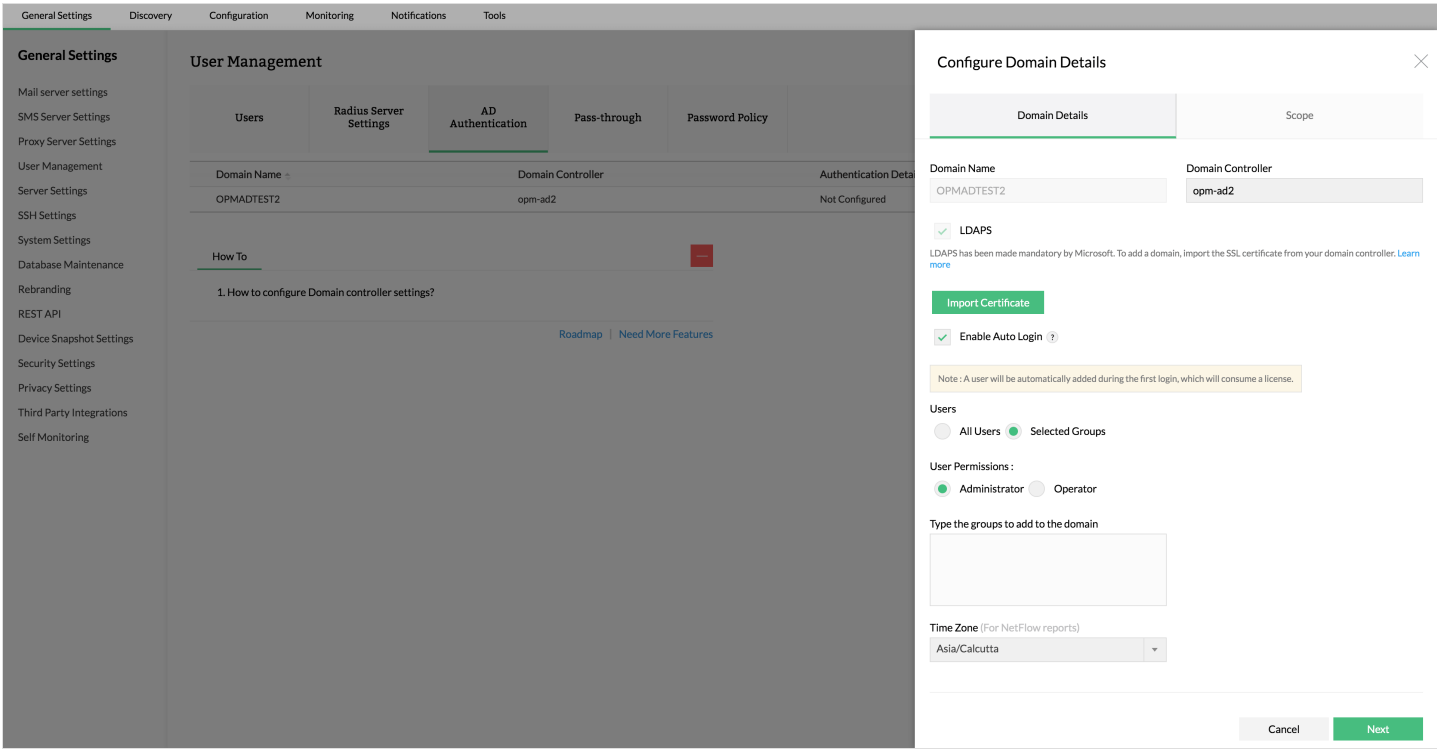
6. Once the domain is added, you can manually add users in the **Users** tab.



Configure Auto-login

The auto-login feature allows you to add all/individual users or selected AD groups to any domain, and assign user permissions to them.

1. Select **Add/Edit** under **Actions** for the domain you want to configure.



2. Select the **Enable Auto Login** check box.
By enabling auto-login, the scope defined for the selected domain will be auto-assigned to users logging-in for the first time. If **Auto-login** is not enabled, then the users must be added manually.

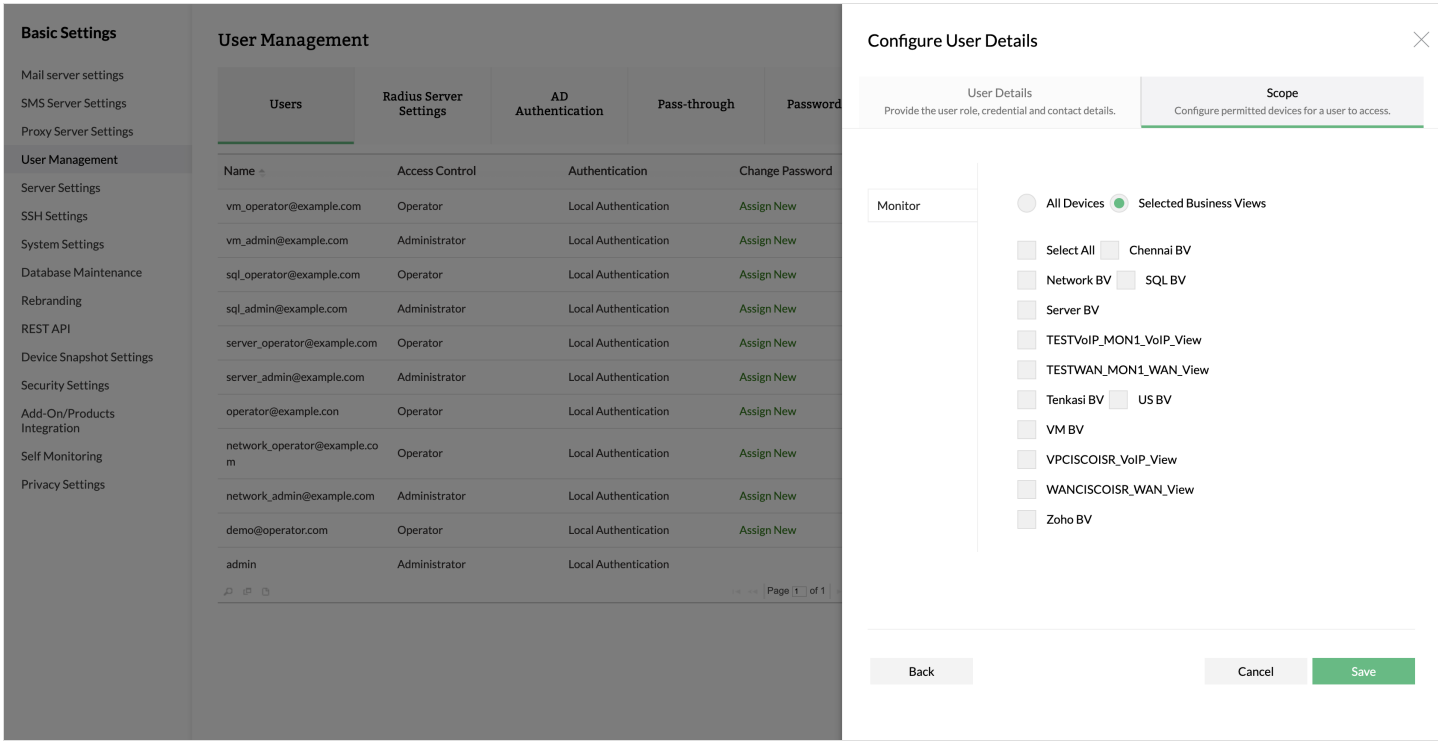
3. **Configuring Auto-login for**

- **All users**
  To enable **Auto-login** for all users, select **All Users** under **Users**. The auto login will be enabled to all the users logging into that domain.
- **Selected AD groups**
  To enable **Auto-login** for selected AD groups, select **Selected groups** under **Users** and type the names of the AD groups. The auto login will be enabled to the AD groups you specify.

4. Once you enable **Auto-login**, select the **Users** and **User Permissions** for the domain, edit the **Time zone** if required, and click **Next**.

5. To configure **Scope**,

Monitor - You can provide this user access to either **All Devices**, or only **Selected Business Views**. If **All Devices** is selected, the user will have access to all the devices in OpManager module. If **Selected Business Views** is selected, you can give the access to all business views with "Select All" option and business views without title with Untitled option.



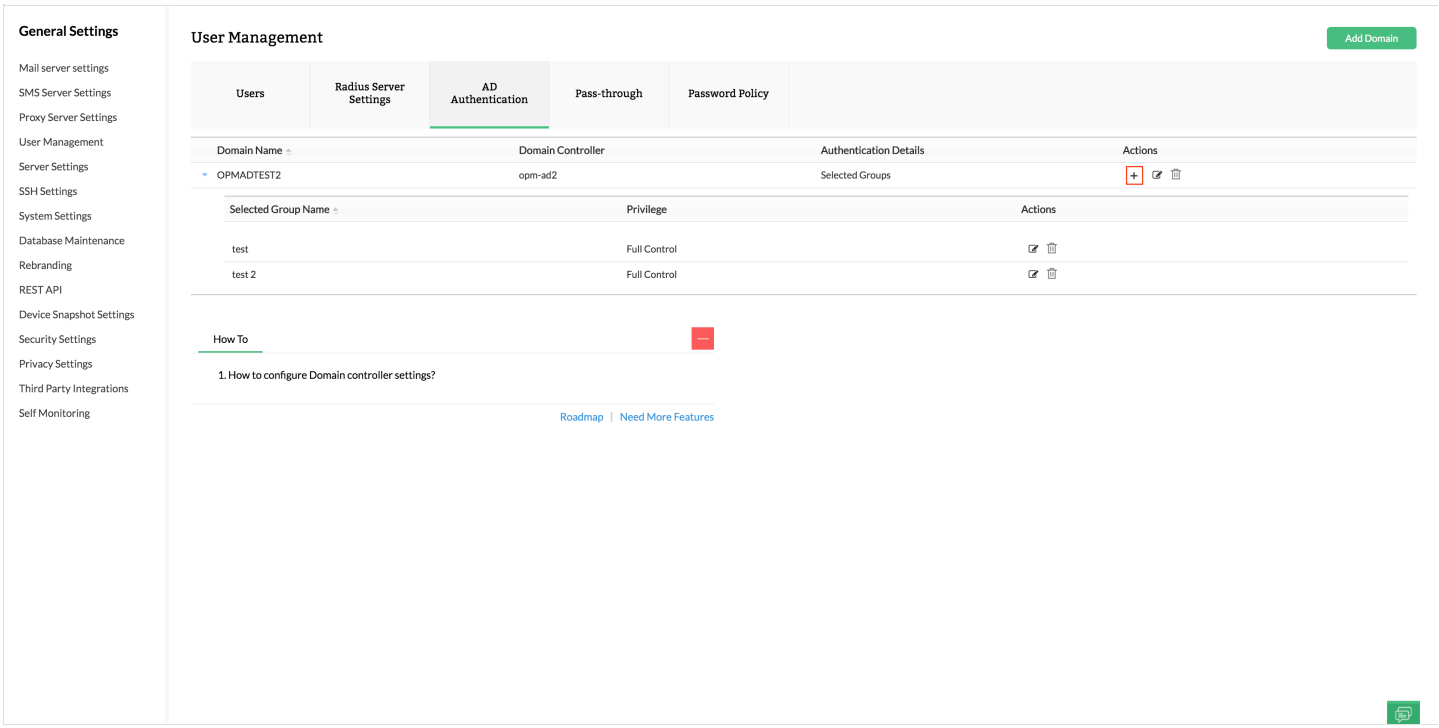
6. **Save** the settings.

Edit Domain Settings

Once you create a domain and assign users, you can edit the configurations as required any time. You can add or delete AD users/groups, edit the user permissions, and also edit the scope settings.

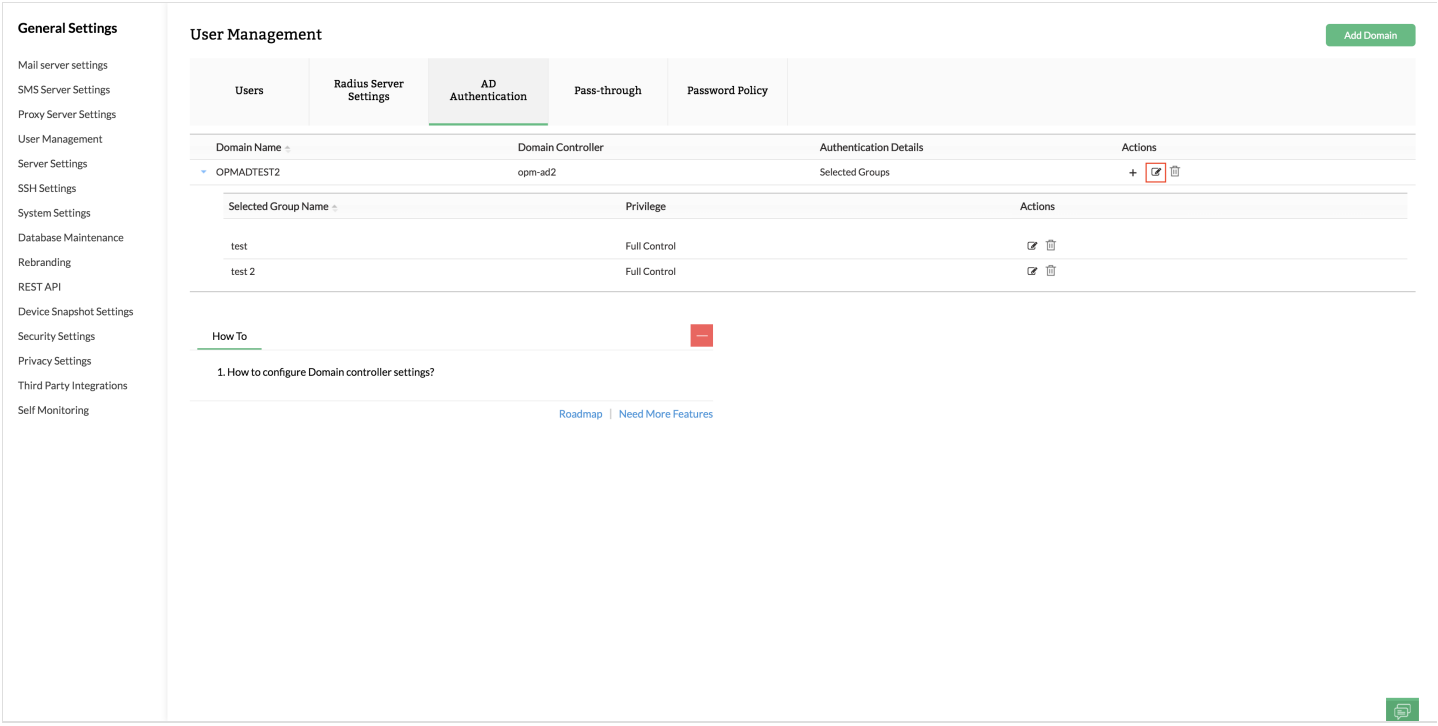
To add AD groups:

Click on the **'Plus'** icon next to the domain of your choice to add new AD groups to it.



To edit timezone:

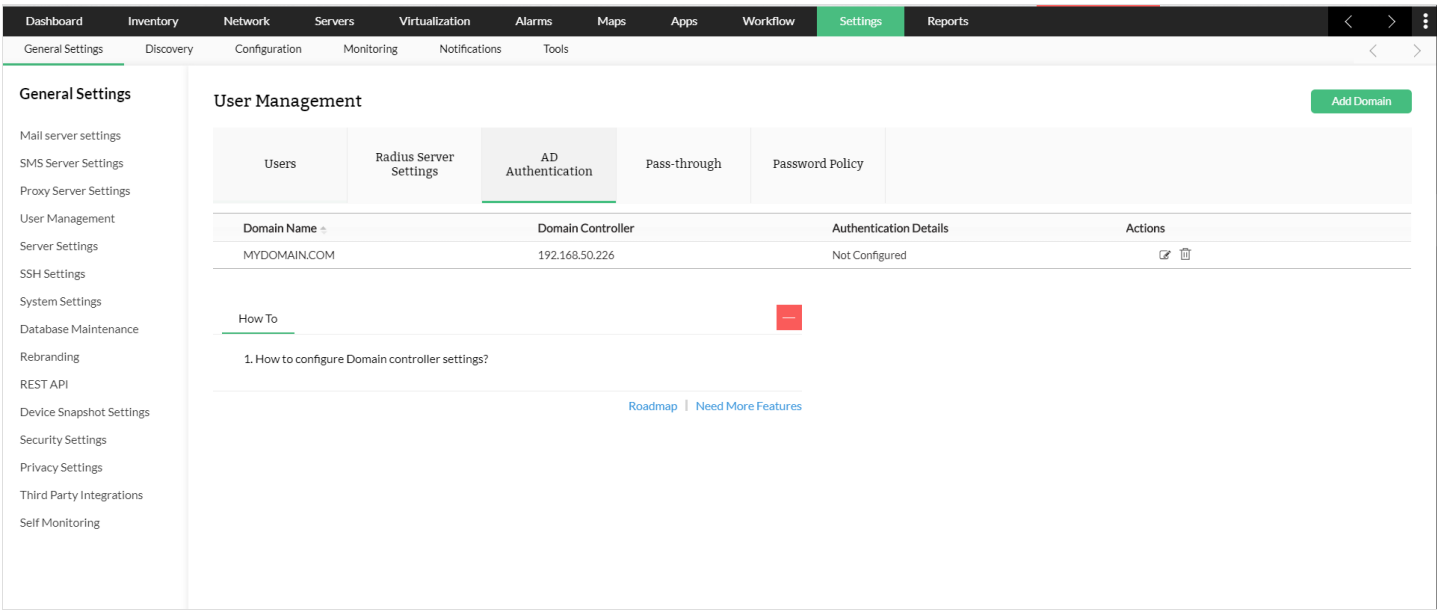
Select **Edit** under **Actions** for the domain you want to edit, change the timezone as per your requirement, and click **'Save'.**



To Edit/Delete AD groups:

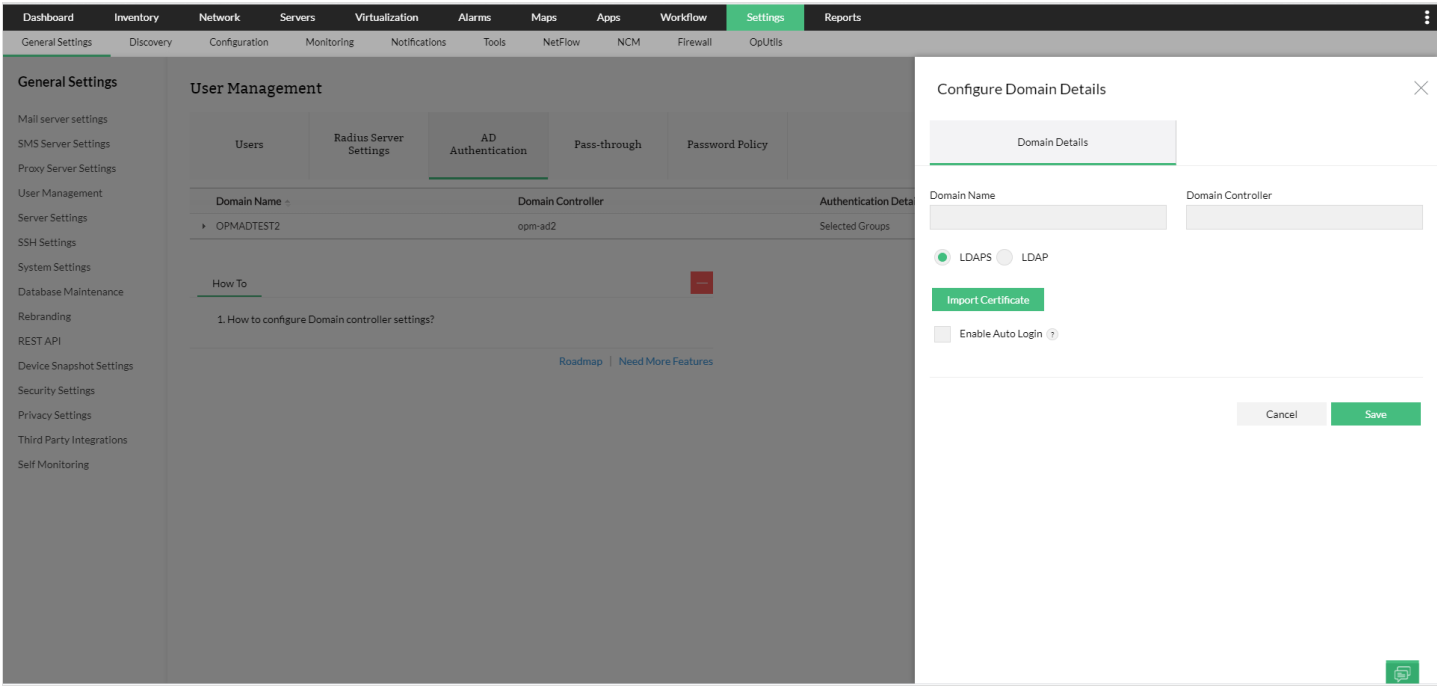
1. Click on the arrow mark next to the name of your domain to display all AD groups under it.

2. Click on the **'Edit'** icon next to the group you wish to edit, select the **Users** and **User Permissions** for the domain, and click **Next**.



3. To edit a particular user/group in a domain, select **Edit** under **Actions** for the domain you want to edit.

4. **User Permissions** for the AD groups can be edited by selecting either **Read Only** (Operator User) or **Full Control** (Administrator User).



5. To configure **Scope**,

Monitor - You can provide this user access to either **All Devices**, or only **Selected Business Views**. If **All Devices** is selected, the user will have access to all the devices of NetFlow, NCM, and Firewall. If **Selected Business Views** is selected, you can give the access to all business views with Select All option and business views without title with Untitled option.

6. **Save** the settings.

7. To delete a group, just click on the **'Delete'** icon next to it.

For AD Authentication, we support on-premise AD with LDAP query access to the domain controller in the network.

Create New Users

You can create users in OpManager and provide required privileges to them. The option to create users is available only for the **admin** login account or those accounts which have 'Full Control' privilege.

Administrator User: Administrator Users have unrestricted access to perform read/ write operations in OpManager. They add/remove devices, troubleshoot issues, change configurations and more without any limitations i.e they have complete access.

Operator User: Operator Users have read-only/ restricted access in OpManager. They can be granted further access by the Administrator User.

Steps to add a user:

1. Go to **Settings** → **General Settings** → **User Management** → **Users** → **Add.**
2. Select user role in **Role** as **Administrator** or **Operator** from the drop down list
3. Select **User Type** from the drop down list

    - Local Authentication
    - Radius Authentication
    - AD Authentication

Add a local user

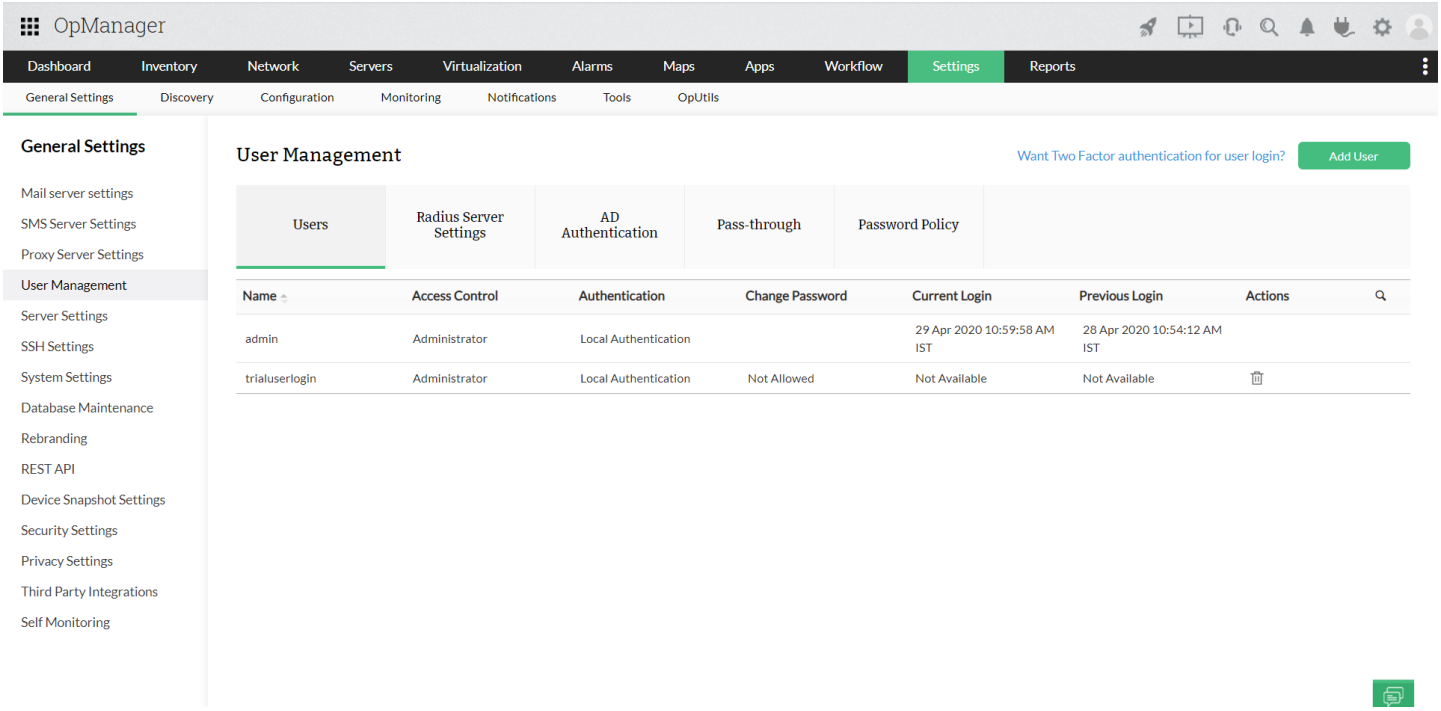
1. **User Details**:

    - Email ID - Email ID for the user
    - Phone Number: Enter the user's phone number
    - Mobile Number: Enter the user's mobile number
    - Password: Create a password for the above user
    - Re-type Password: Retype the password for confirmation
    - Time Zone: Enter the Time zone of the user's location

Note: This Email ID will be used in password recovery when the user clicks the Forgot Password option in the login page.

2. **Scope**:
   Monitor - You can provide this user an access to either **All Devices,** or only **Selected Business Views**. If **All Devices** is selected, the user will have access to all the devices of NetFlow, NCM, and Firewall. If **Selected Business Views** is selected, you can give the access to all business views with Select All option and business views without title with **Untitled** option
3. Click **Add User** to add the user according to the scope specified here

Logout and try logging in as the new user and check the privileges.



Add a Radius user

1. **User Details**:
    - User Name - Name of the Radius user to be added
    - Email ID - &#65533; Email ID&#65533; for the Radius user
    - Phone Number: Enter the user's phone number
    - Mobile Number: Enter the user's mobile number
    - Time Zone: Enter the Time zone of the user's location
2. **Scope**:
   Monitor&#65533; - You can provide this user an access to either&#65533; **All Devices,**&#65533; or only&#65533; **Selected**&#65533; **Business Views**. If&#65533; **All Devices**&#65533; is selected, the user will have access to all the devices of NetFlow, NCM, and Firewall. If&#65533; **Selected Business Views**&#65533; is selected, you can give the access to all business views with Select All option and business views without title with **Untitled** option
3. Click&#65533; **Add User**&#65533; to add the user according to the scope specified here

Logout and try logging in as the new user and check the privileges.

Add an&#65533; AD user

1. **User Details**:
    - User Name - Name of the AD user to be added
    - Email ID - &#65533; Email ID&#65533; for the AD user
    - Phone Number: Enter the user's phone number
    - Mobile Number: Enter the user's mobile number
    - Domain Name -&#65533; Select the desired AD domain from the list of available domains or Click **Add Domain** to add a new domain
    - Time Zone: Enter the Time zone of the user's location
2. **Scope**:
   Monitor&#65533; - You can provide this user an access to either&#65533; **All Devices,**&#65533; or only&#65533; **Selected**&#65533; **Business Views**. If **All Devices** is selected, the user will have access to all the devices of NetFlow, NCM, and Firewall. If **Selected Business Views** is selected, you can

give the access to all business views with Select All option and business views without title with **Untitled**&#65533; option

3. Click&#65533; **Add User**&#65533; to add the user according to the scope specified here

Logout and try logging in as the new user and check the privileges.

Changing User Passwords

You can change the password for the users. Either the admin user or an user with full control privilege only can change the passwords.

1. Go to **Settings ? Basic Settings ? User Management**.

2. Click on the name of the user whose password you want changed. The Configure User Details tab will pop-up, where you can change the following.

1. **Password Details:**

   Password- A new password for the above user

   Re-type Password- Retype the password for confirmation

2. **Contact Details:**

   Phone number: The user's phone number

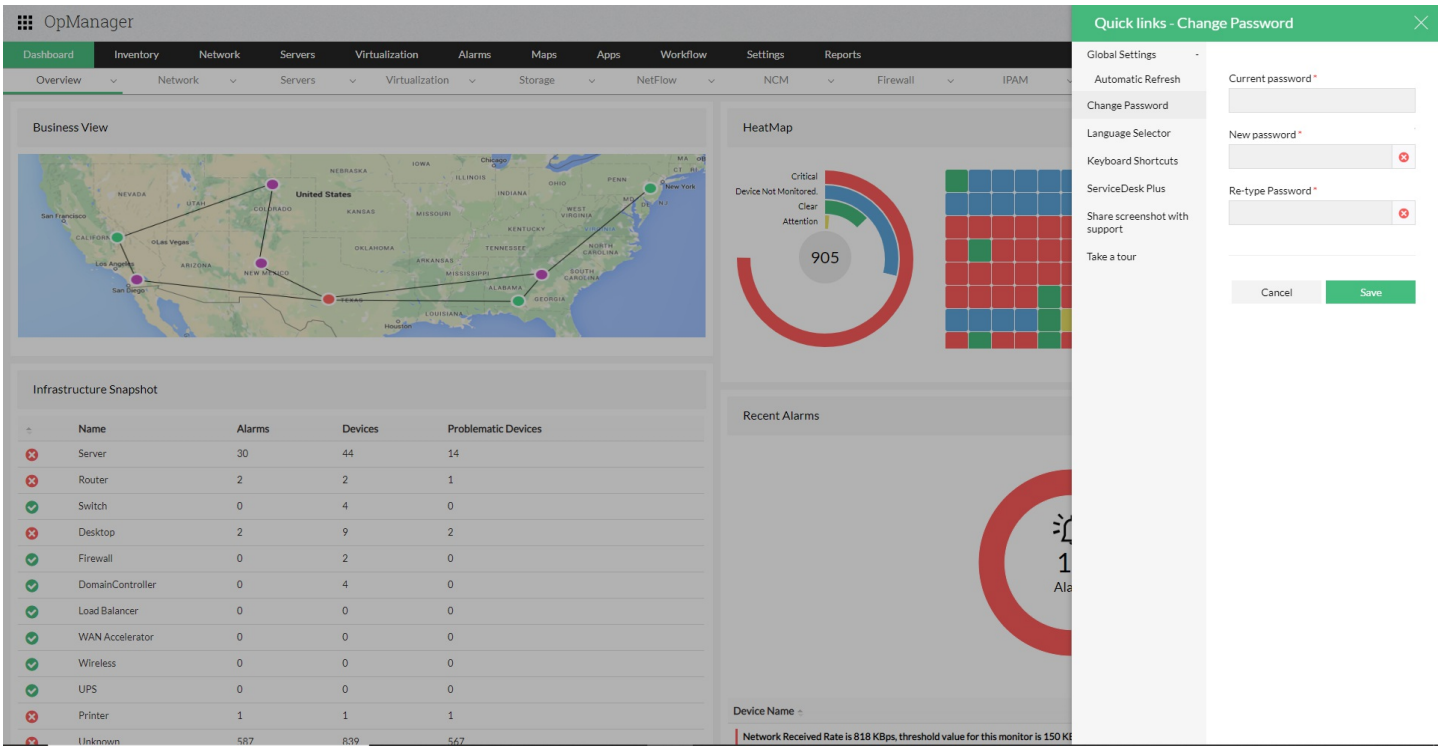
   Mobile number: The user's mobile number

3. **Access Details:**

For users with only partial permission, the business views assigned to that user is displayed. Remove selection for the view if you want to remove the views from the user's purview. For users with full control, this option is not displayed.

(or)

Click on the **'Settings'** icon in the **top band** and go to the **'Change Password'** tab.



(or)

In **User Management**, the administrator user can also assign new passwords by clicking "**Assign New**" under **Change Password** in the **Users** section.

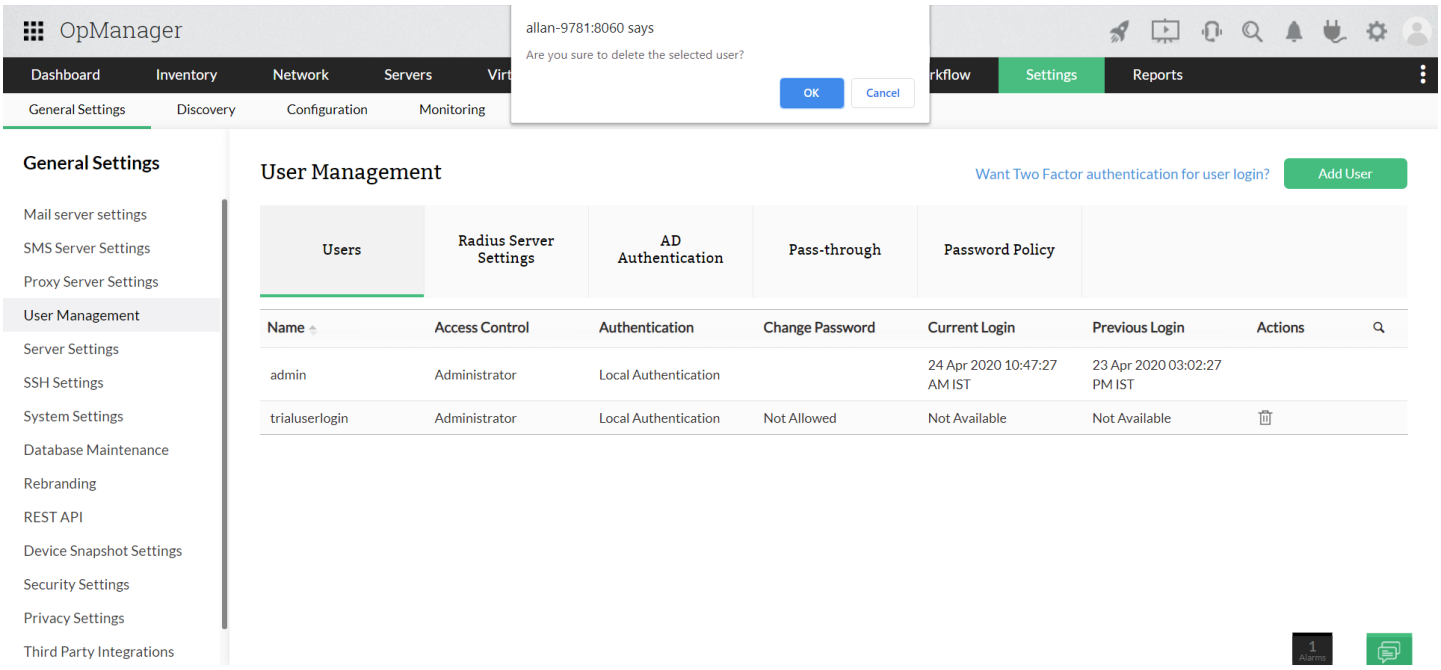
(or)

You can change the password on the login page itself by clicking 'forgot password' option.

Remove Users

In OpManager, it is possible to add and remove users using an admin account or with an account having permission to do so. Follow the steps given below to remove users from OpManager.

1. Go to **Settings** > **User Management**
2. Click the Delete icon against the user name whose account you want to delete.
3. A confirmation dialog pops up. Click **OK**. The user account is deleted.



Pass-through Authentication

Pass-through authentication (Single Sign-on) provides the ability to authenticate yourself automatically in OpManager using your currently logged in windows system username and password. You would not need to manually enter your windows credential to log-in to OpManager webclient.

Prerequisites:

- ### Configuring Active Directory authentication

  Active directory authentication must have been configured in OpManager for the domain you want enable Pass-through Authentication. Click here to know how to add a domain under Active Directory authentication in OpManager.

- ### Creating necessary user accounts in OpManager

  User accounts to whom you want to enable pass-through must have been already available in OpManager. Click here to know how you can add new users.

  Note: Pass-through authentication will work only for the active directory users already been added to OpManager. If you do not want to manually create user account for all the users in your domain, enable auto-login for the domain (Admin ? User Manager ? Windows Domains). Once auto-login is enabled, you have to manually enter username and password of your account only during the first login and an user account in OpManager will be created automatically. From there on, you can simply work without manually entering.

- ### Creating Computer Account:

  A computer account must be created in the Domain Controller for accessing the NETLOGON service in a domain by OpManager. Click here to know how you can create a new computer account.

  Note: After version 124085, new computer accounts can be created from the Passthrough configuration window itself, if the **OpManager service is running under a user who has administrative privileges.** Also, if the OpManager server has been started from Command Prompt, make sure it is being **run as a administrator.**

- ### Configuring OpManager as a trusted site in your browser(s):

  OpManager webserver must be added as a trusted site in all browsers you are going to use to access the OpManager webclient, to prevent the browsers from opening unnecessary popups for providing your credentials.

  To configure trusted sites, follow these steps:

  - For Internet Explorer (applicable to Chrome as well):

    Open **Control Panel ? Network and Internet ? Internet Options ? Security ? Local Intranet ? Sites ? Advanced**. Enter OpManager server URL, click **Add**.

  - For Firefox:

    In URL box enter **about:config**. Click the button "I'll be careful. I promise", if warning page is displayed. In the resulting page, search for **ntlm**. Double click the option **network.automatic-ntlm-auth.trusted-uris**. Enter OpManager server URL in the text box and click OK. (Multiple site entries can be entered separated by comma.)

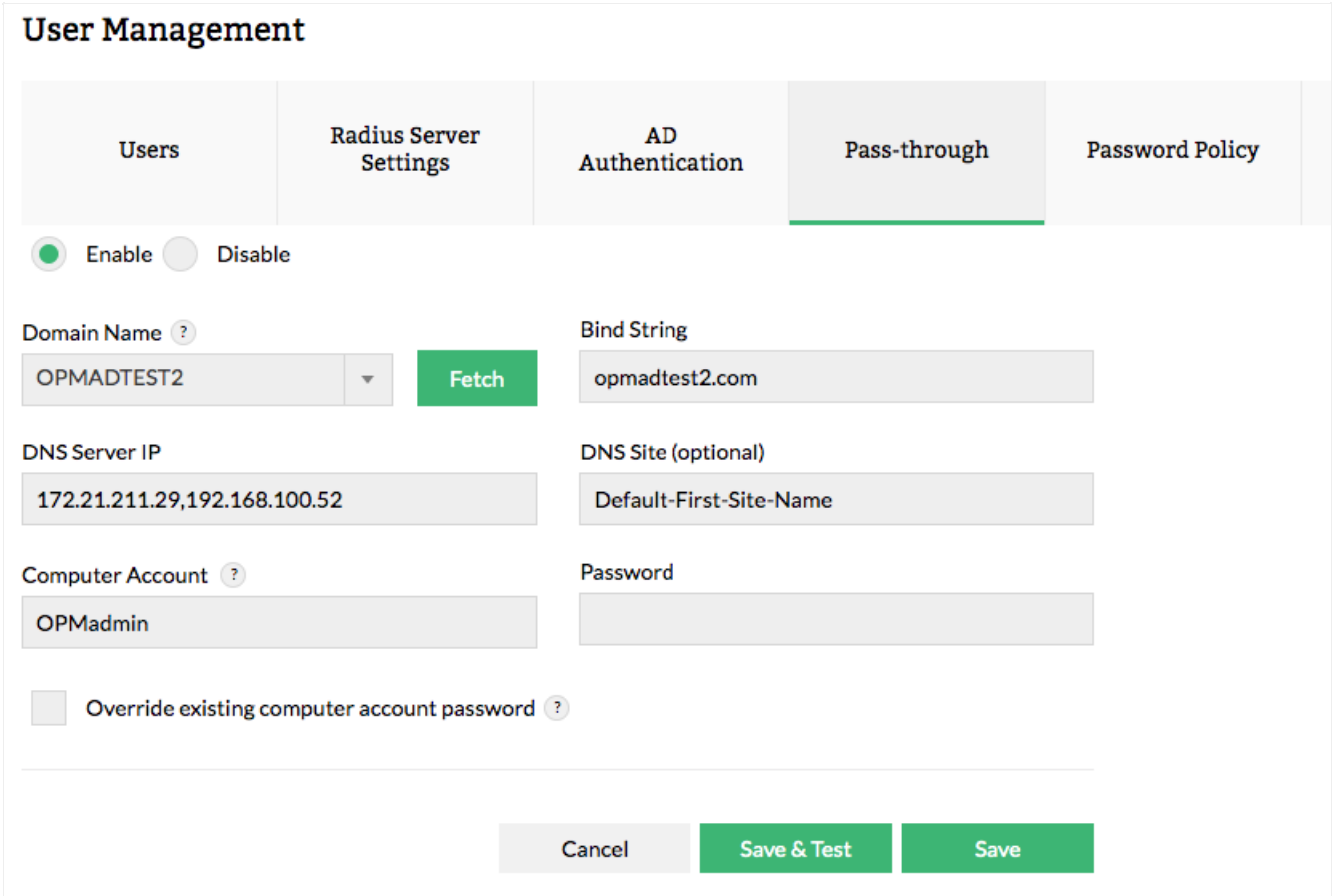
Configuring Passthrough Authentication in OpManager:

After all the prerequisites have been ensured, follow the steps below to auto-configure Passthrough Authentication in OpManager:

- Go to **Settings > User management > 'Pass-through'** tab.
- Click on the **'Enable'** button, and select the required domain from the dropdown list.
- Click on **'Fetch'** to get all the necessary credentials from the domain controller such as Bind string, DNS server IPs and DNS site.

> **Note:** If there are any issues in fetching the necessary details, or if you're in a version of OpManager **earlier than 124085,** you will have to configure these settings manually.

- Also, enter the Computer account and password of the Domain Controller (computer account name **must be less than or equal to 15 characters**). If you provide the wrong credentials, an error message will be displayed which indicates whether the account name or the password is wrong, or if the account doesn't exist.
- After version 124085, if the OpManager service runs under a user who has administrator privileges, an account will be created with the provided account name even if it doesn't exist already.
- Also, if you want to update your password, just select the **'Override existing computer account password'** checkbox, and the existing password for the computer account will be overridden with the value that you have provided in the 'Password' field.
- To verify if the provided details are right, click on **'Save & Test'.** If all the details are provided correctly, a success message will be displayed on your screen. If not, a message displaying the possible errors in the parameters passed will be displayed. Rectify those errors and then click **'Save'.**
- Else if you are confident with the credentials that you provided, you can directly click **'Save'.**



Configuring Passthrough Authentication manually

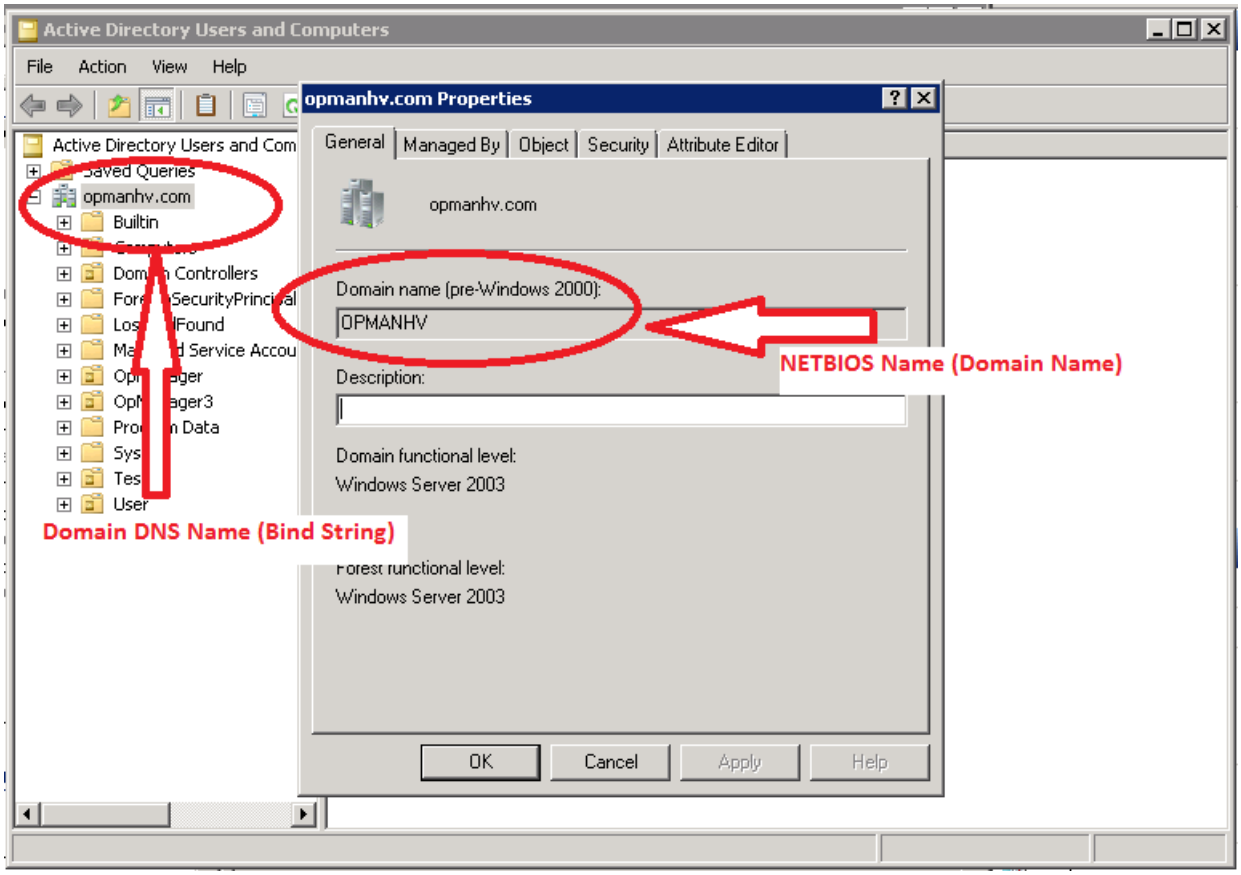
To manually configure Passthrough authentication, you'll need the following details:

1. **Domain Name:** NETBIOS name of your domain. Example: OPMANHV (How can I find it?)
2. **Bind String:** DNS Name of your domain. Example: opmanhv.com (How can I find it?)

3. **DNS Server IP:** Primary IP Address of the DNS Server. (Separated by commas if there are multiple DNS server IPs) (How can I find it?)
4. **DNS Site:** Site under which the Domain Controller is listed. (How can I find it?)
5. **Computer Account:** Account name of the computer account created.
   Example: mytestacc$@OPMANHV.COM
   (For versions of OpManager before 124085, it is mandatory to append *$@domain_dns_name* with the account name.)
   Note that the computer account name must be **less than or equal to 15 characters.**
6. **Password:** Password of the computer account

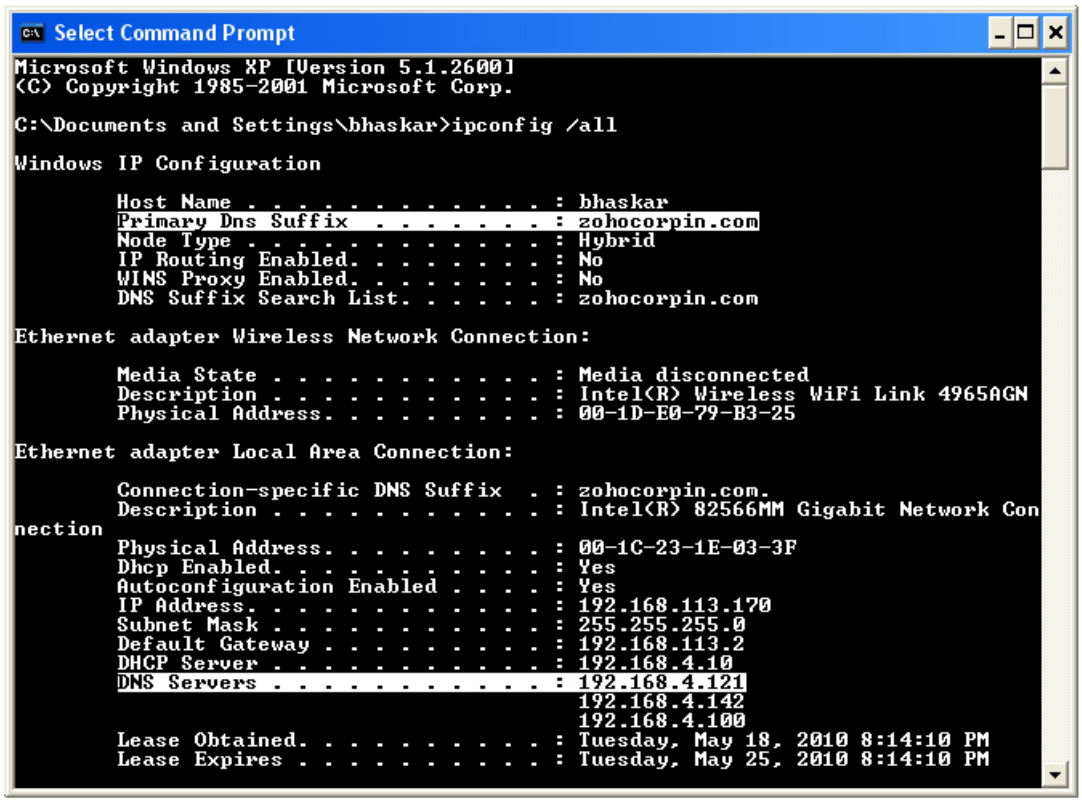
1 & 2 - Getting Domain DNS Name and NETBIOS Name:

In the Domain Controller device, open **Start ? Administrative Tools ? Active Directory Users and Computers.**



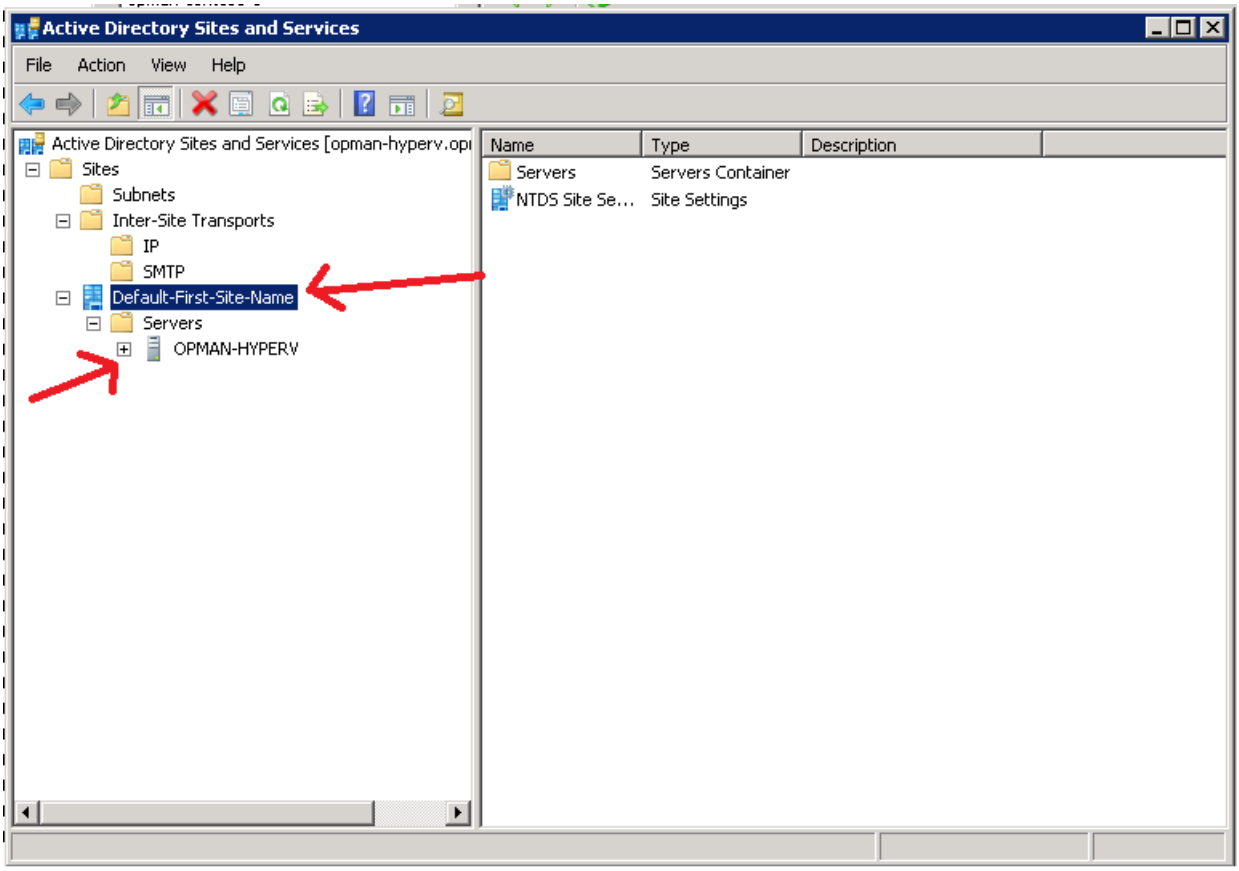
3 - Getting DNS Server IP:

Open Command Prompt in OpManager server. Run the command "ipconfig /all". The first IP Address mentioned in the DNS Servers field is the primary DNS Server IP Address.



4 - Getting DNS Site:

In Domain Controller device, open **Start ? Administrative Tools ? Active Directory Sites and Services.** The Site under which your Domain Controller device name listed is your site name. You can leave the DNS Site field empty in Pass-through configuration form in OpManager, if there is only one site present in your Domain Controller.



Creating a new computer account:

To create a new computer account, follow the steps below:

- Run the script NewComputerAccount.vbs present under OpManager_Home\conf\OpManager\application\scripts to create a new computer account.

  cscript NewComputerAccount.vbs *account_name* /p *password* /d *domain_name*

- To reset the password for an existing computer account, run the script SetComputerPass.vbs present under OpManager_Home\conf\OpManager\application\scripts to create a new computer account.

  cscript SetComputerPass.vbs *account_name* /p *password* /d *domain_name*

- Ensure that the password you give is compliant to the password policy for that domain. Do not use the New Computer Account option present in AD native client which will not allow you to choose password. If you face problem running this script from OpManager server, copy the script to the domain controller machine itself and try running it.

Note: The length of the computer account name must be **less than or equal to 15 characters.**

Design Limitation:

- Pass-through authentication can be enabled for only one domain, preferably the domain in which OpManager server resides. If pass-through has been configured for a domain other than the one in which OpManager server resides, ensure the other domain will provide logged in user information to a website from different domain.

Disable Pass-through Authentication:

In OpManager webclient, click on Settings ? Basic Settings ? User Management ? Pass-through. Use the radio buttons to Enable/ Disable Passthrough Authentication.

Log File:

If you face any issue with Pass-through Authentication, contact support with a ZIP file of the logs present under **OpManager_Home\logs** folder.

Monitoring Resources Using CLI

OpManager monitors the system resources using SNMP by default. But if needed, you can also add monitors based on CLI, and both these types of monitors will work in tandem. All the Unix Servers templates have the resource monitors preconfigured. All you need to do is to select the CLI monitors and associate them to the required devices.

Prerequisites

For monitoring the Unix servers, make sure either Telnet or SSH is enabled on them.

Steps to configure Telnet/SSH Monitoring:

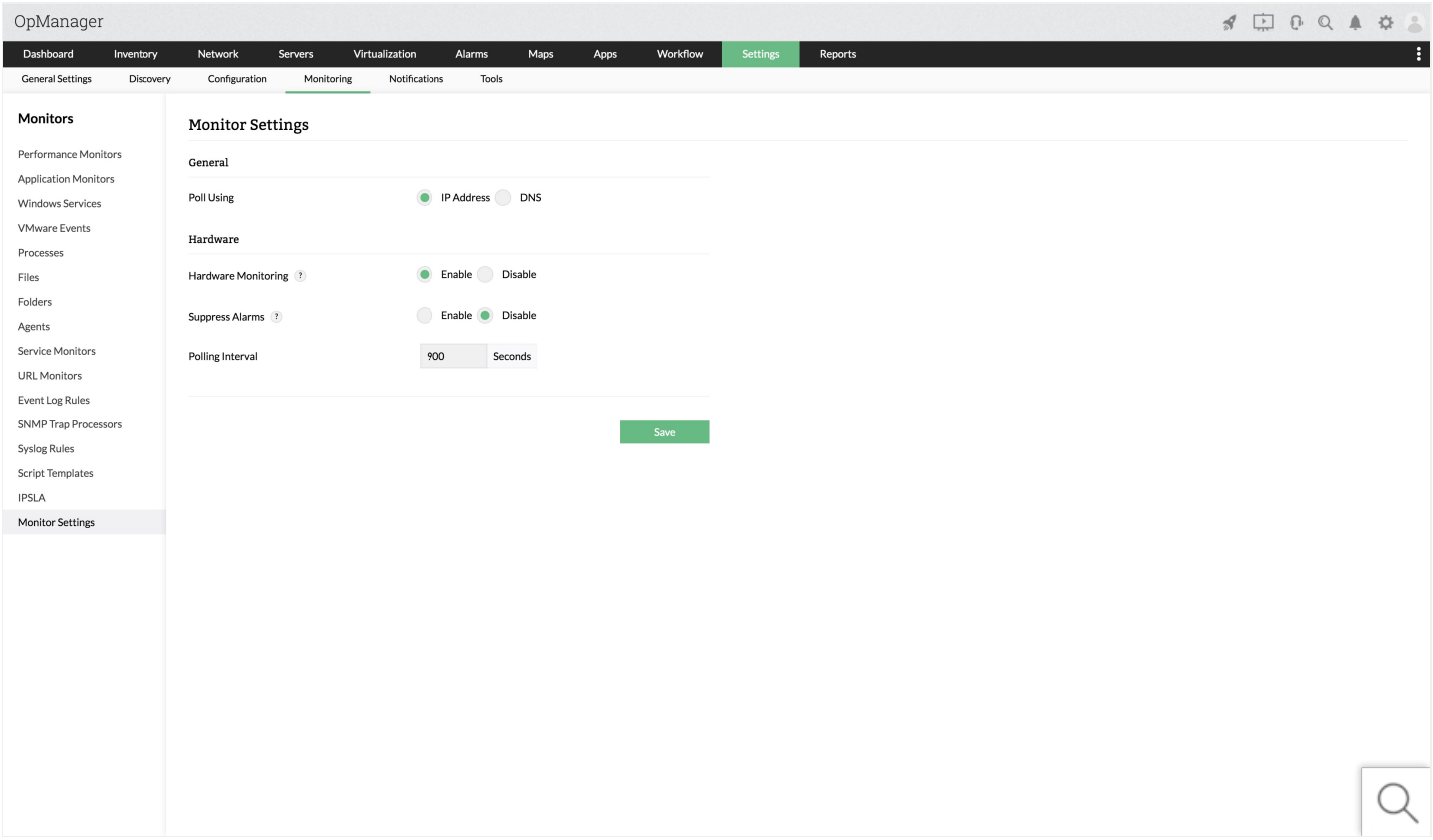
1. Go to the snapshot page of any device you wish to monitor.
2. Click the **Actions** button.
3. Now, from the list of resource monitors, select the CPU, Memory, and Disk Utilization monitors which has the protocol name as CLI against the monitor name.
4. Once done, click **Add**. The monitors are added to the device under the Monitors column.

IP/DNS polling

Most network monitoring solutions use IP addresses to poll the devices and fetch performance data, but some network admins might want to poll their devices using DNS names of the devices. OpManager allows you to select whether you want to poll your devices using the IP address of the device or the DNS name. This setting can be controlled throughout OpManager or can also be configured for individual devices.

1. Global setting for polling mode

Go to **Settings ? Monitoring ? Monitor settings,** and select which mode you want to use to poll the devices in your network. Once you're done, click **'Save'.**

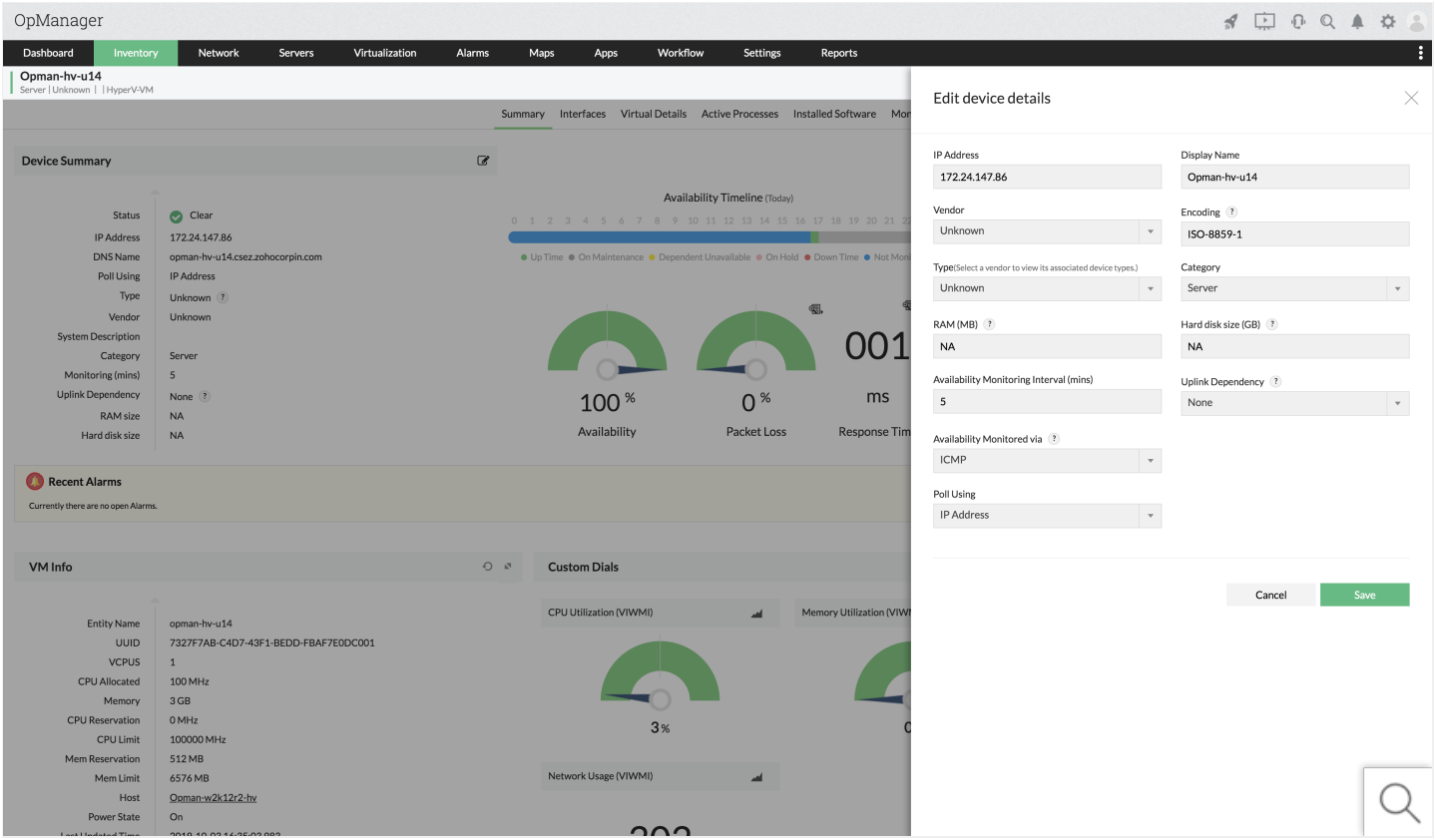


Note: Changes in the global setting apply only for devices that will be discovered in the future. The polling method of devices already discovered will not be affected in any way.

2. Device-specific configuration

You can also configure this setting individually for any device. To configure it:

- Go to Inventory and click on the device you want to change this setting for.
- Click on the three-line menu and click **'Edit device details'.** You can also click on the Edit button in the device summary.
- Under **'Poll using',** select the mode that you wish to use to poll that device and click **'Save'.**



Note: The device-specific value always overrides the global value provided in Settings ? Monitoring ? Monitor settings.

Example: Consider you have 50 devices added into OpManager. If you have selected **IP address** as the global setting, but you've chosen DNS name for only 5 devices by changing it from the respective device snapshot pages, **only these 5 devices will be polled using DNS** and the rest of the devices will be polled using IP address.

Adding More Monitors

Following are the monitors associated by default for the different device categories:

- **Servers**: CPU, Memory, Disk Utilization
- **Routers**: CPU, Memory, Buffer Hits/Misses, Temperature
- **Switches**: CPU, Memory, BackPlane Utilization
- **Firewalls**: CPU, Memory, and Connection Count.

Similarly, other categories also have few resources monitoring triggered by default. Besides the ones automatically associated, you can monitor more parameters. Here are the steps to configure more monitors:

1. Go to **Settings** > **Configuration** > **Device Templates**
2. From the list of templates, select the template for the device type to which you want to associate more monitors. Use the search bar to locate your device template quickly.
3. In the device template, from the **Monitors** column, click the **Add** button.
4. All the predefined monitors are listed. Select the required monitors from here and click **OK**
5. To save this setup, press **Save** or press **Save and Associate** to directly associate the selected monitor to the devices mapped to the Device Template. Press **Copy** to copy the Device Template.

Adding Custom Monitors

In addition to OpManager's default monitors, you can also create your own monitors for the SNMP-enabled devices in your network. The SNMP variable for which you intend configuring a monitor can return either a numeric or a string output when queried.

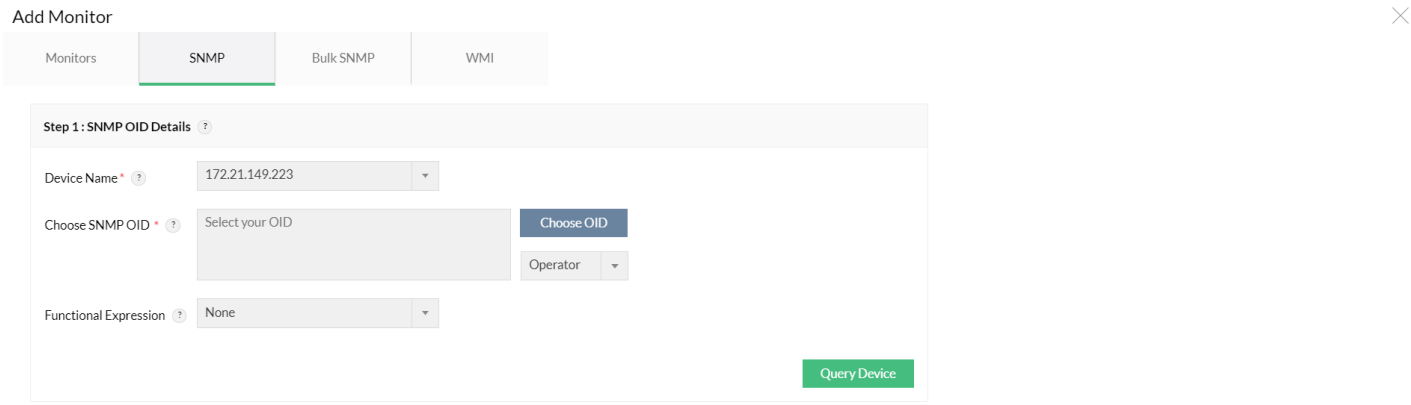
To add a custom monitor for a resource of a particular device type, the device template must be modified. The new monitor should be defined in the device template so that the monitor is associated for all devices of that type. Here are the steps.

1. Go to **Settings** > **Configuration** > **Device Templates**.
2. Click on the template in which you want to add a new monitor.
3. Example > Linux. Scroll down the template and click **Add** under Monitors column.
4. Click on the **SNMP** at the top of this page.
5. Configure the SNMP OID, Monitor Name, Display Name etc and click **OK**
6. Click **Save** to save the changes to the Device Template or press **Save and Associate** to directly associate them to the devices or press **Copy** to copy the Device Template.

Add SNMP Monitor

OpManager allows you to create custom SNMP monitors to get performance metrics based on vendor specific OIDs provided in the MIB.

Go to **Settings ? Monitoring ? Performance Monitors ? Add** (or) **Inventory ? Device Snapshot Page ? Monitors ? Performance Monitors ? Actions ? Add monitor.**



Step 1: SNMP OID Details

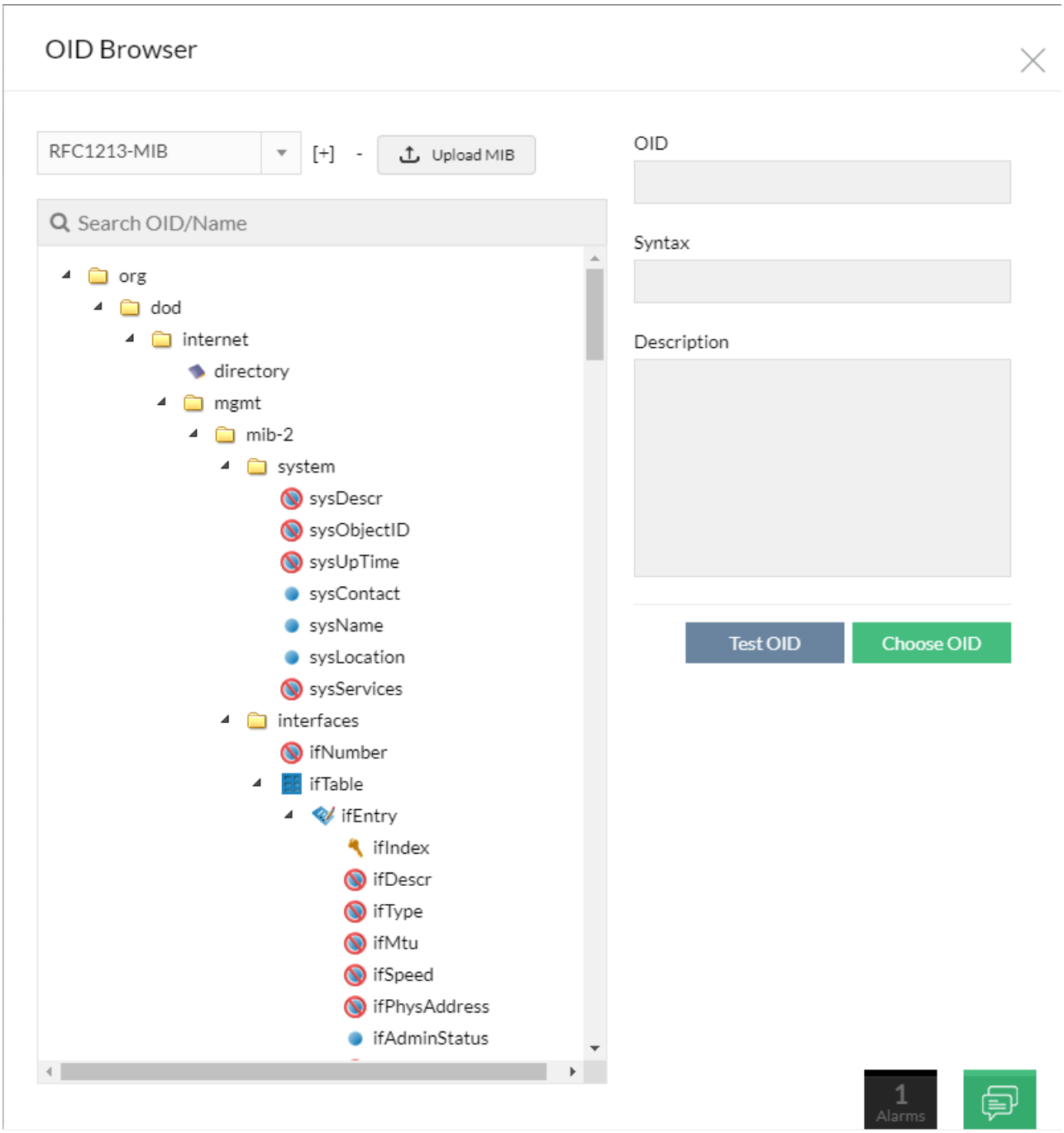
To add an SNMP monitor, you need to first provide the OID based on which OpManager will fetch data related to the required metric from a device.

1. Choose SNMP OID:

You can either enter the OID for which you want to add a monitor/ select an OID from the OID browser.

OID Browser

To access the OID browser, click **Choose OID**.



Step 1: Select MIB

In the drop-down menu provided on the top-left corner of the OID browser, you can select the MIB file from which you want to select the SNMP OID. You can find a list of default/ supported MIBs included in this drop-down.

If you do not find a suitable MIB, you can also upload a MIB provided by your vendor using the **UploadMIB** option.

I) Click **Upload MIB**.

ii) **Browse** and **Upload** a vendor provided MIB file.

Note: Please upload MIBs with RFC2578 MIB Standard to avoid parsing errors.

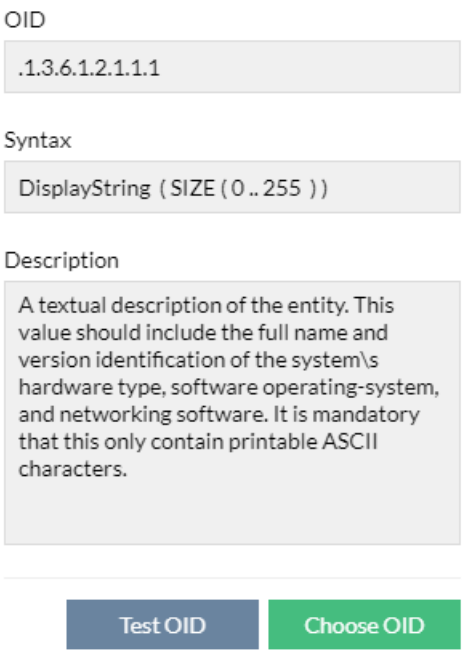
Step 2: Select OID

Search OID/Name: The OID browser in OpManager allows you to search the MIB for OIDs using the object identifier/name (.1.3.6.1.2.1.1.3/ sysUpTime). You can also browse and select the required OID directly from the MIB tree.

Step 3: Test OID

Once you have selected an OID from the MIB tree, you will be able to view the OID, its Syntax and its Description. You can now test

the OID to check if the output is desirable by clicking **TestOID**. This option allows you to review an OID's output, even before adding it to the expression.



Step 4: Now, click **Choose OID**. This will insert the selected OID into the **Choose SNMP OID** field.

2. Performing operations on OIDs using expressions:

The **Choose SNMP OID** field is not limited to just containing the OID. It also provides options for the user to construct OID expressions that perform simple mathematical operations on the output values of the OID. You can also construct expressions by combining OIDs.

Example: (.1.3.6.1.2.1.1.3.0)/8640000

Restrictions on OID expressions:

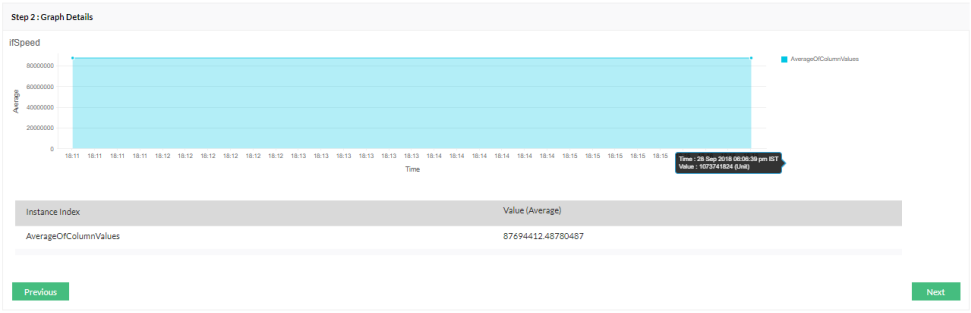
1. If more than one Multiple Instance OID is present in the expression, then it should be of the same parent node.
2. Monitor involving both Scalar and Multiple OIDs are not supported.
3. Monitor involving both String and Numeric OIDs are not supported.
4. You cannot use string monitors to create expressions.
5. You cannot add Table OIDs as a Monitor.

3. Functional Expression

Functional Expressions allow you to set a predefined format on the display parameters of an output value.

E.g. In the case of adding an SNMP monitor to fetch the **CPU temperature** value, you can use a functional expression to convert **Celsius to Fahrenheit**.

It also supports aggregate methods that allow you to perform operations which combine multiple values to give a single output. **E.g. AverageOfColumnValues**, **SumOfColumnValues**, etc.



4. Device Name

This option helps you test the OID against a device. The template will not get associated to the selected device.

5. Vendor Name

Use the drop-down menu to select a vendor to which you want to associate the template (or) Enter a new vendor name (Click New -> Enter a new Vendor Name -> Click Add).

Now, click **Query Device**.

Step 2: Graph Details

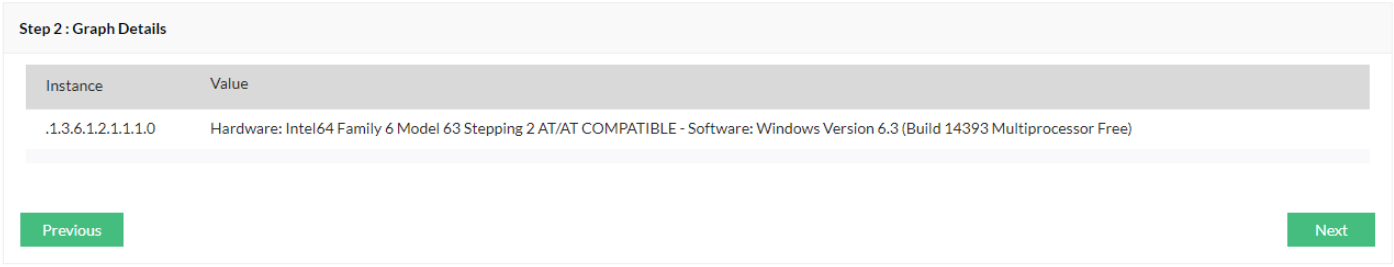
Object identifiers (OIDs) have both a type and a value. It is on this basis that they are classified into **Scalar Objects** and **Tabular Objects**. A **scalar object** is a managed object that always has a **single instance**, whereas, **tabular objects** have **multiple instances**. In both these cases, the output can either be a string or a numerical value.

Graph Details

i) Scalar Objects:

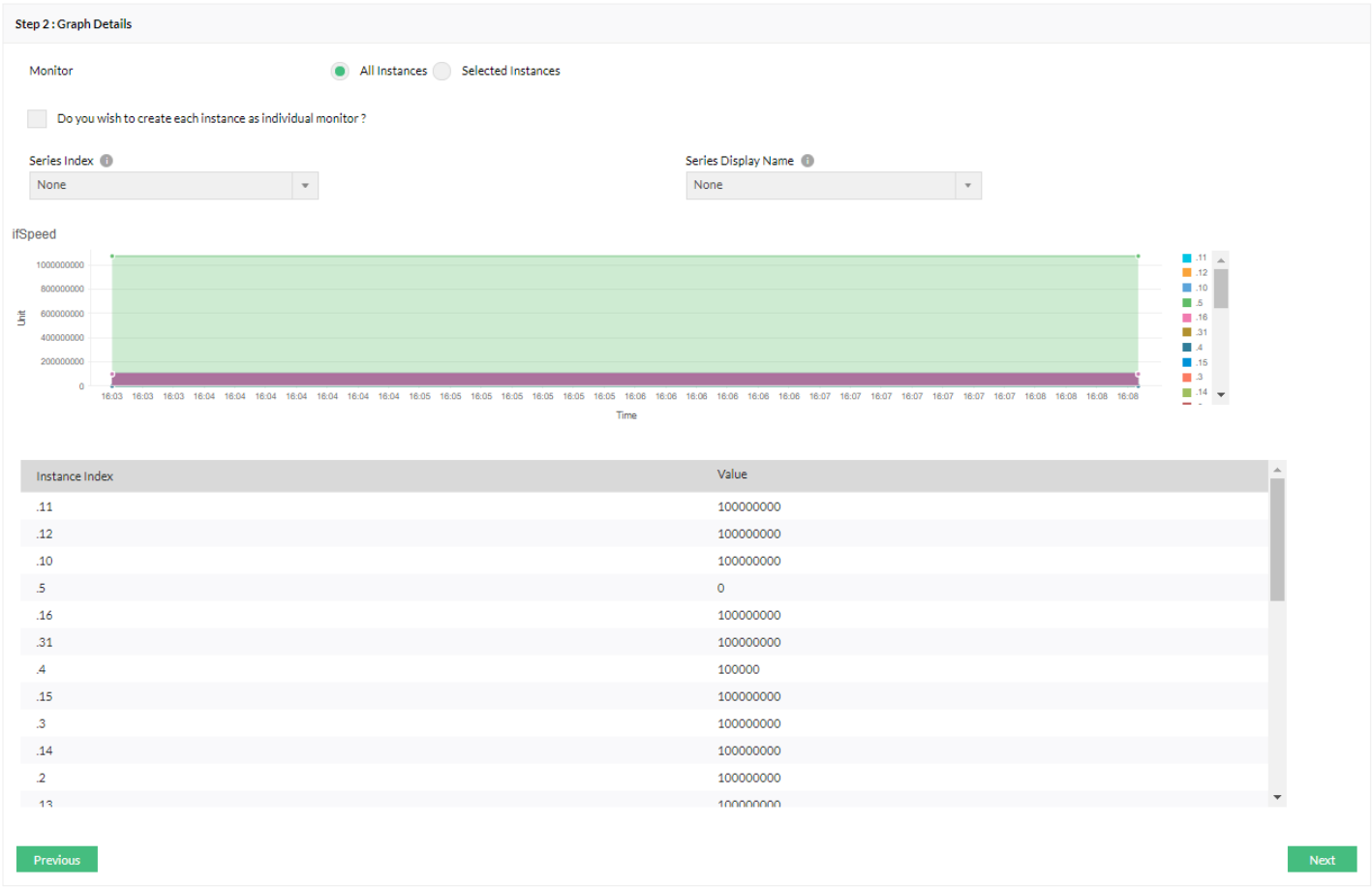
1. Scalar objects with a numerical output will display a table containing the instance and the value along with a graph.

2. Scalar objects with a string output will only display the instance and the value.

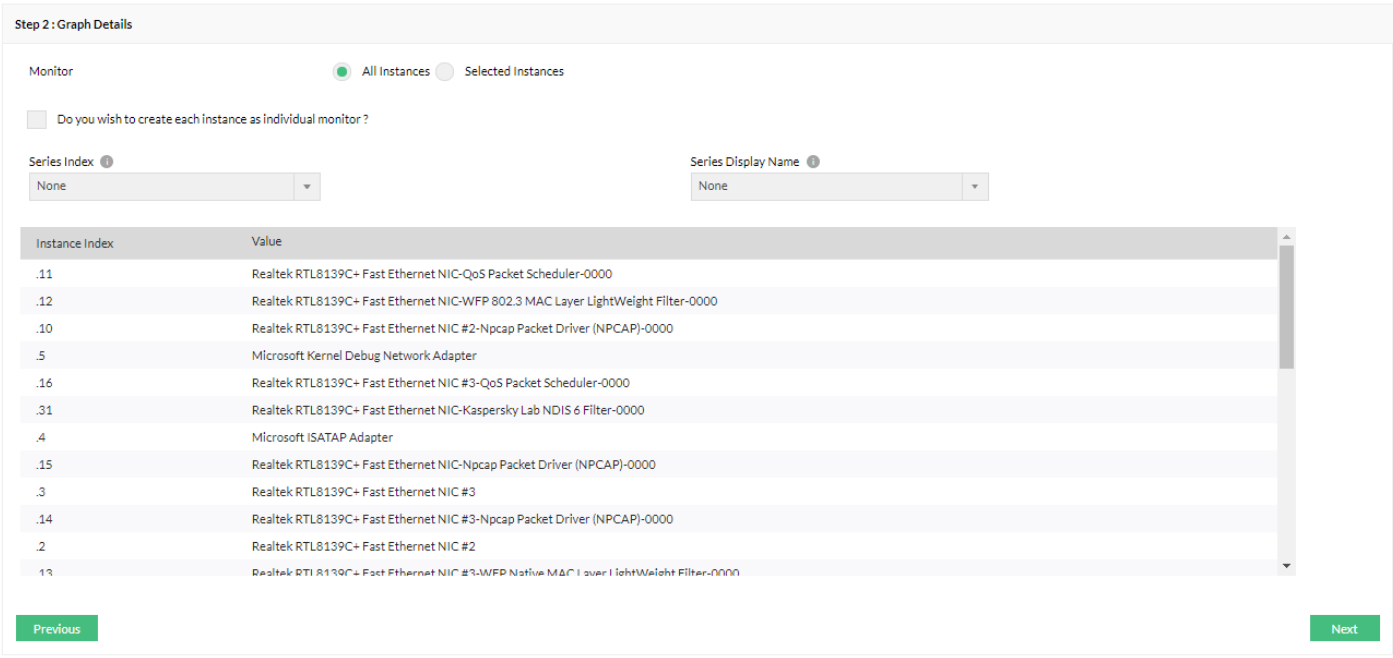


ii) Tabular Objects:

1. Tabular objects with a numerical output will display a table containing the instance and the value along with a graph.

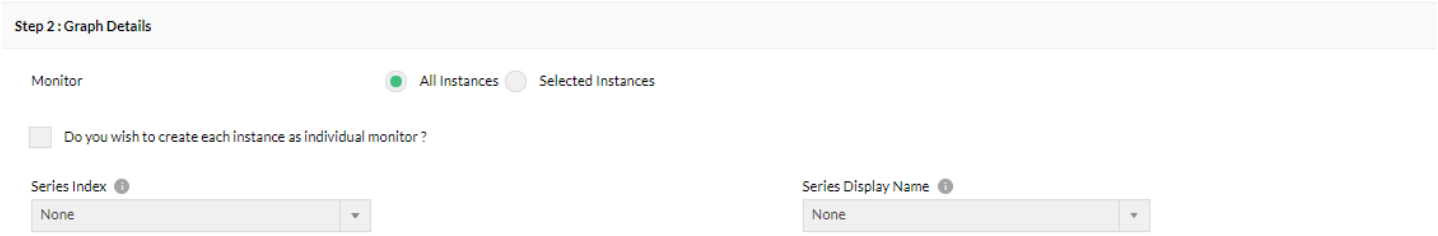


2. Tabular objects with a string output will only display the instance and the value.



Monitor Instances

OpManager provides the option of selecting specific instances that you want to monitor from a tabular object.



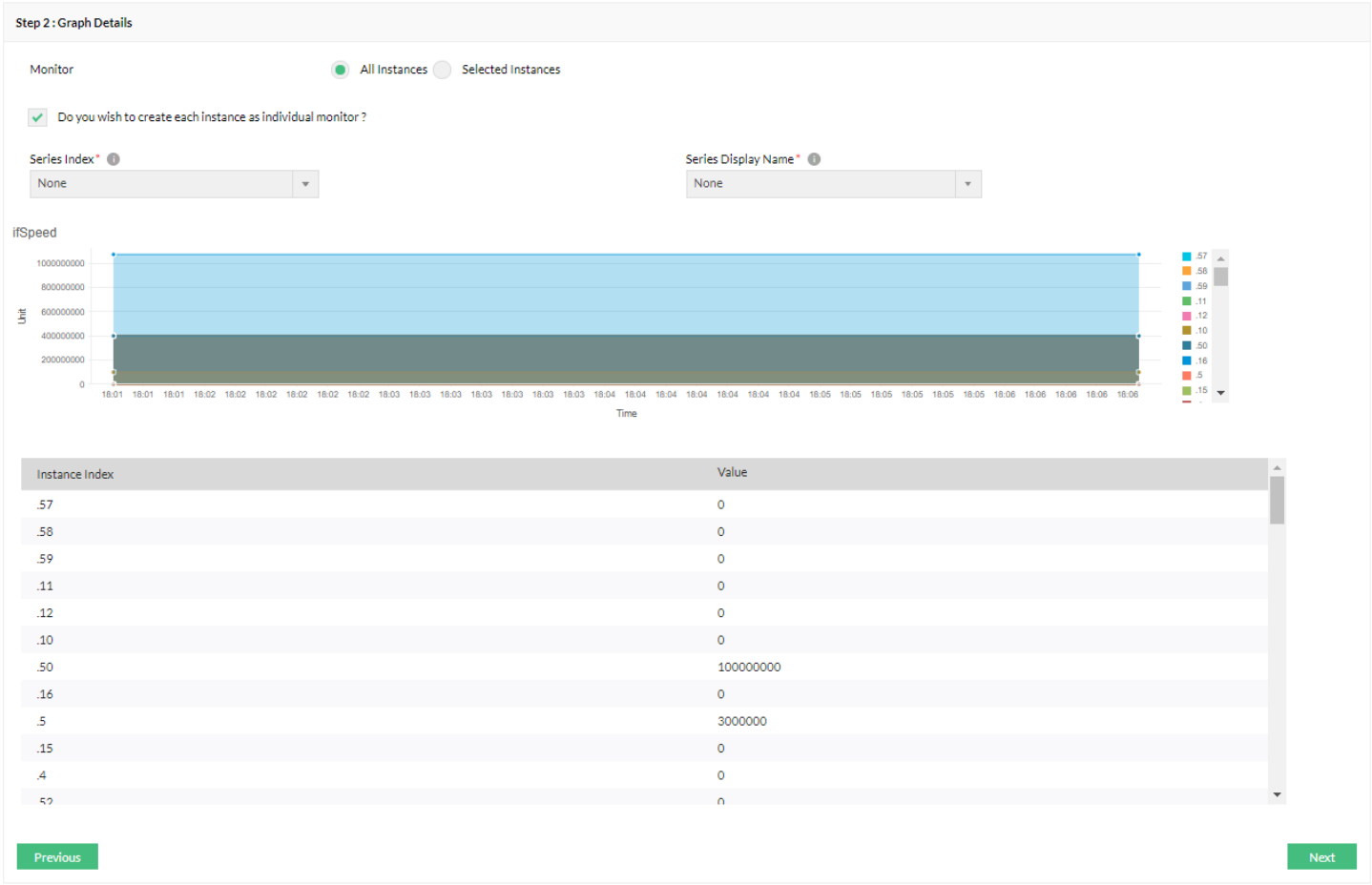
All Instances: A single SNMP monitor that monitors multiple instances will be created.

Selected Instances: You can select desired instances from the available list and add it as separate templates/ monitors. The Series Index and Series Display OID columns are mandatory.

Do you wish to create each instance as an individual monitor?

This checkbox creates a separate SNMP monitor for each instance.

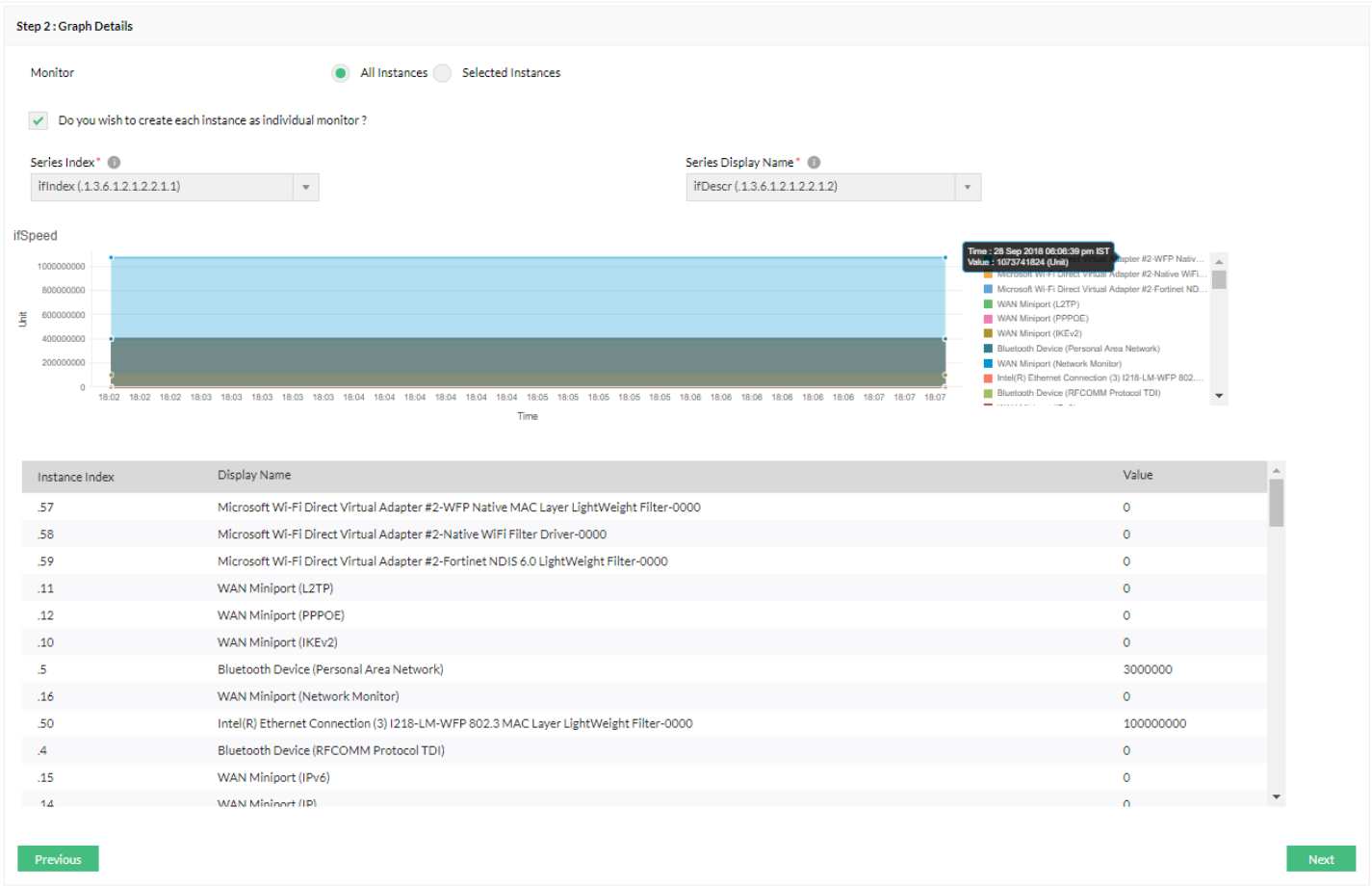
If you choose to select this option, it is mandatory that you provide inputs to the **Series Index** and the **Series Display Name** fields.



Series Index & Series Display Name

Series Index: An index is used to refer to a particular instance of a tabular object. A tabular object can have one or more instances and is identified by its index value. To identify a specific columnar variable, the index of the row has to be appended to its OID.

Series Display Name: This corresponds to the description/ name/ label that should be associated to an instance.



Note: The **Series Index** and the **Series Display Name** drop-down menu will automatically list all the OIDs under the same parent. If the index or description OIDs are not listed, you can type in the required OID.

Click **Next**.

Step 3: Monitor Details

1. Monitor Name: Enter your preferred monitor name. The default name will be the OID name.

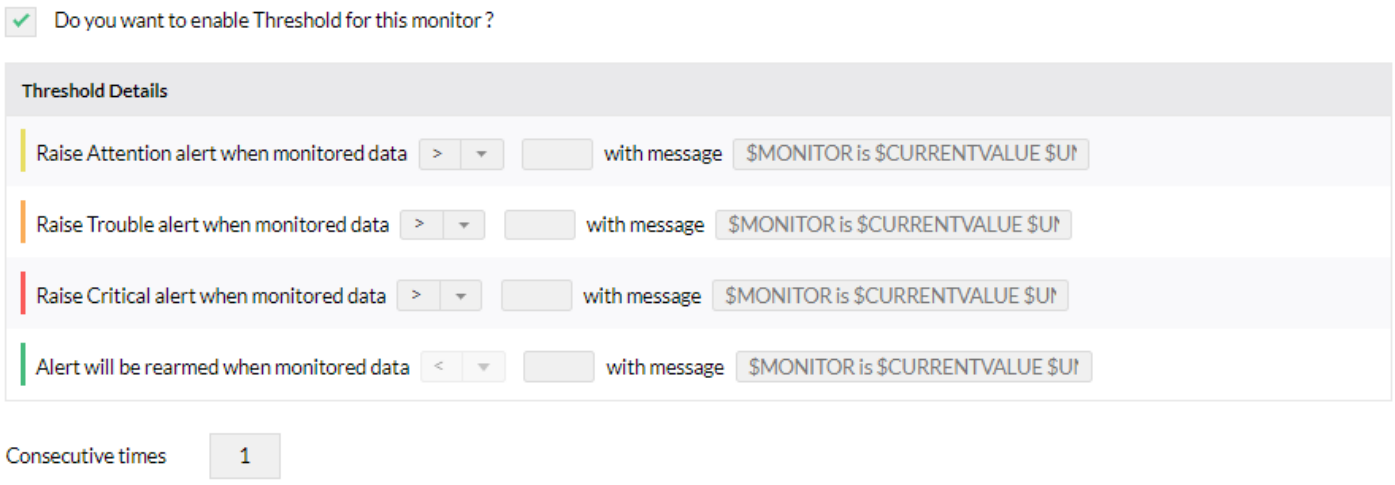
2. Interval (Mins): This value specifies the time interval in which you want to re-run the monitor to fetch the corresponding values.

3. Units: Specify the unit for the monitored resource.

4. Data Type: Select between 'Integer' and 'Decimal' depending on the data type required.

5. Do you want to enable Threshold for this monitor?

You can check this option to set thresholds on the alerts that will be generated based on this monitor.



Select the condition **[>,=, <, or !=]** for **attention, trouble & critical alert** thresholds, and enter the value. An alert is raised if the monitored value is greater than, equal to, not equal to, or lesser than (which ever is selected) the specified threshold value.

Rearm Value

Enter the **Rearm Value**. A rearm value helps determine if the condition of a monitor has returned to normal after a threshold violation alert.

Example: Let us assume that the attention alert threshold for a memory monitor is configured as, "Raise Attention alert when the monitored data is > 75" and the monitored memory value of that device exceeds this value, say 80. An alert will be raised.

In the next poll, if the monitored memory value is 72. Another alert will be generated, stating that the device is in a normal condition.

Now, if in the next poll, the monitored value climbs to 80. A threshold violation alert will again be generated which becomes troublesome to manage.

A **rearm value** helps avoid this hassle by confirming that a device has returned to normal, only if the monitored value matches the rearm value.

Note: The rearm value must be lesser/ greater than the threshold value, based on monitor requirements and the configured threshold condition.

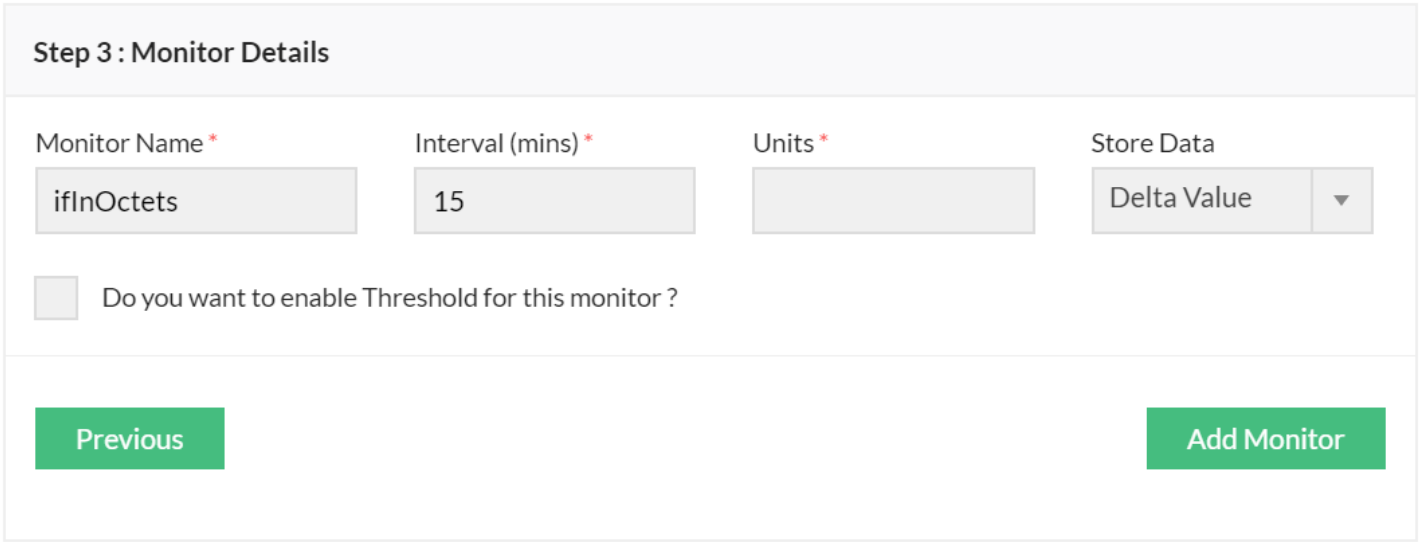
In the **Consecutive Times** field, enter the value of how many consecutive times the thresholds (Attention, Trouble and Critical) can be violated for an alert to be generated.

5. Click **Add Monitor.**

Note: If the custom SNMP monitor is created from the Settings page, it will be created as a template. Whereas, if the monitor is created from the Device Snapshot page, it will automatically be associated to that device.

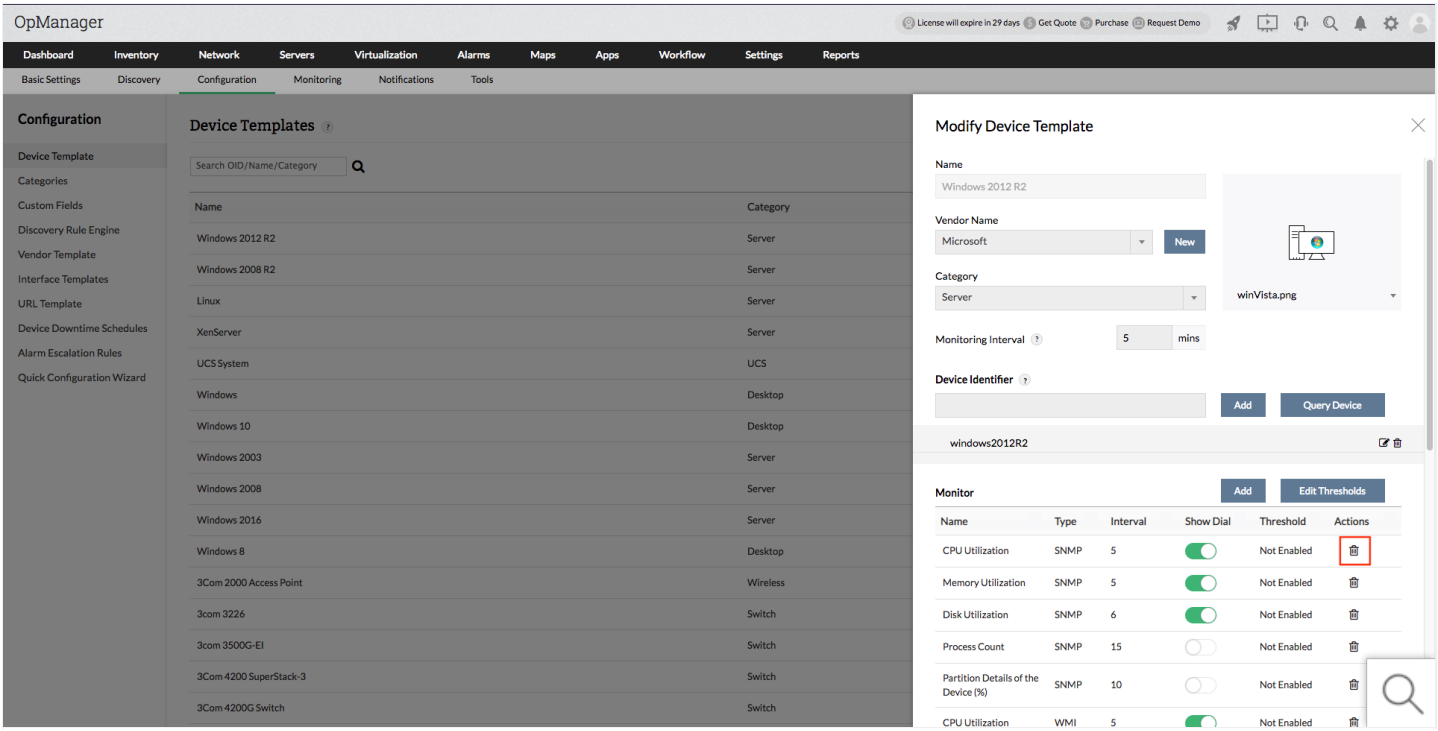
Counter Type OIDs

If you select **Counter type OIDs**, you can store data based on the delta value or the absolute value. By default, OpManager stores data using the delta value. However, you can use the **Store Data** drop-down to select your preference.



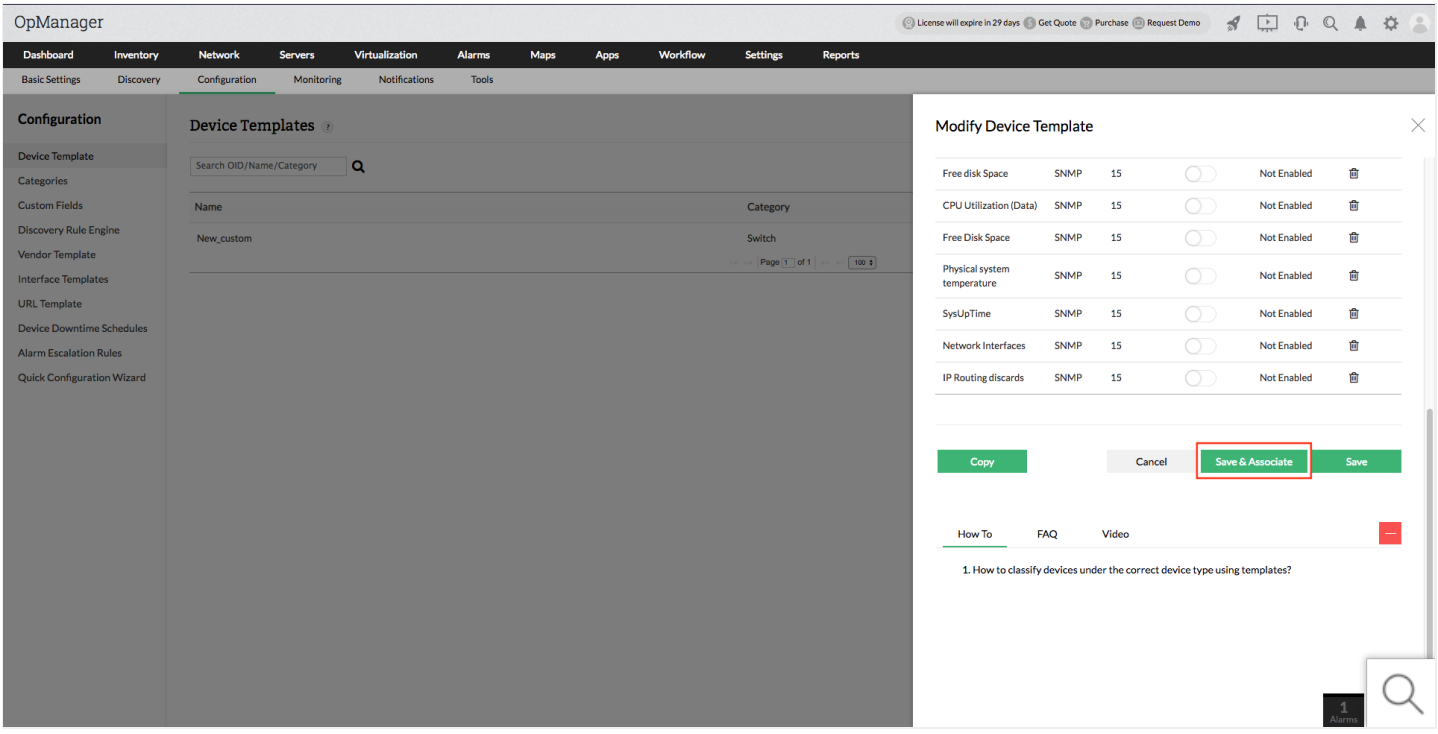
Deleting performance monitors

1. Deleting a monitor from Device Template page:



- Go to **Settings ? Configuration ? Device template.**
- Navigate to the template of your choice, and click to edit it. You can find the list of monitors associated under **'Monitors'** tab.
- Click on the bin icon next to the monitor you wish to delete and click **'Save'**.

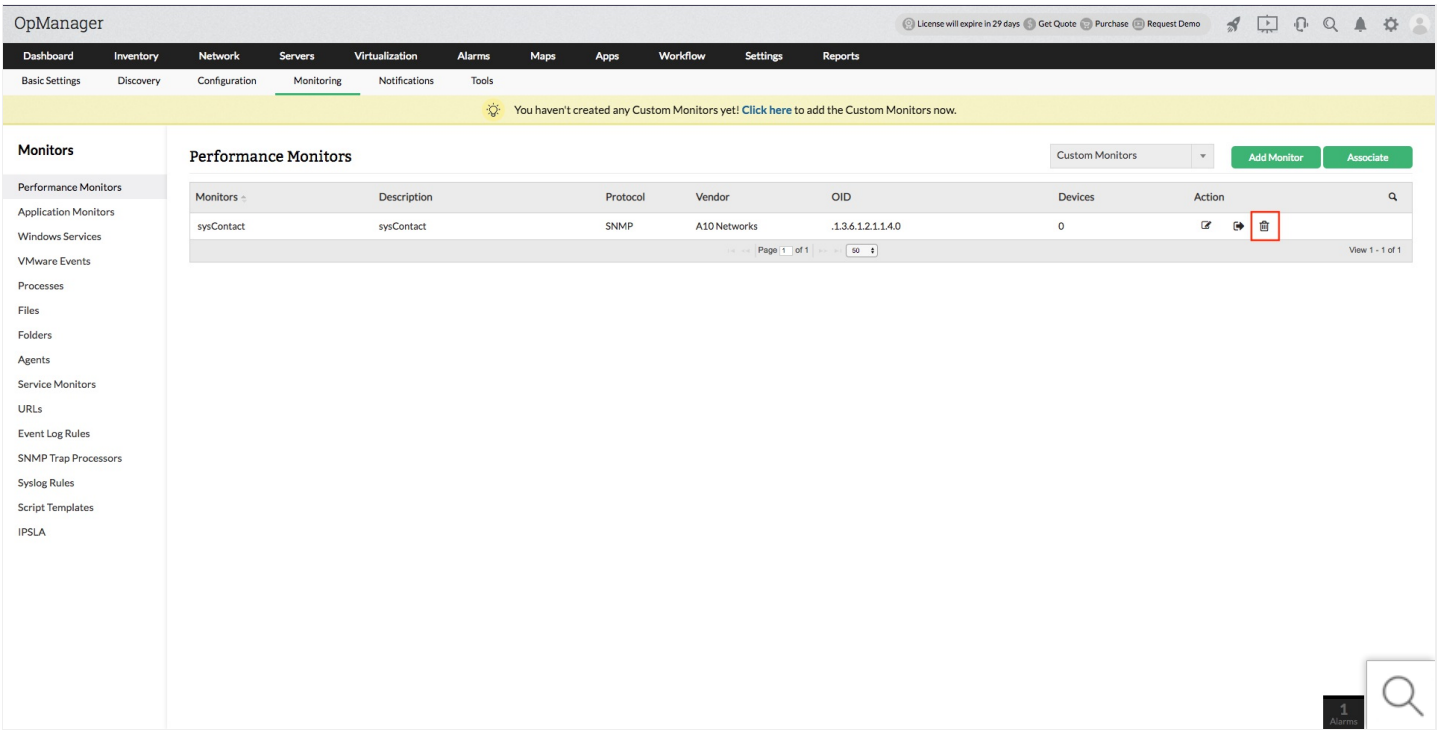
Deleting a monitor from this page is reflected instantly and the devices that will be associated with that template in the future, but it still remains in all the devices that have been already associated with that template. To apply the changes to all these devices, click on **'Save and Associate'** button in the Edit device template page.



2. Deleting a monitor from Performance monitors page:

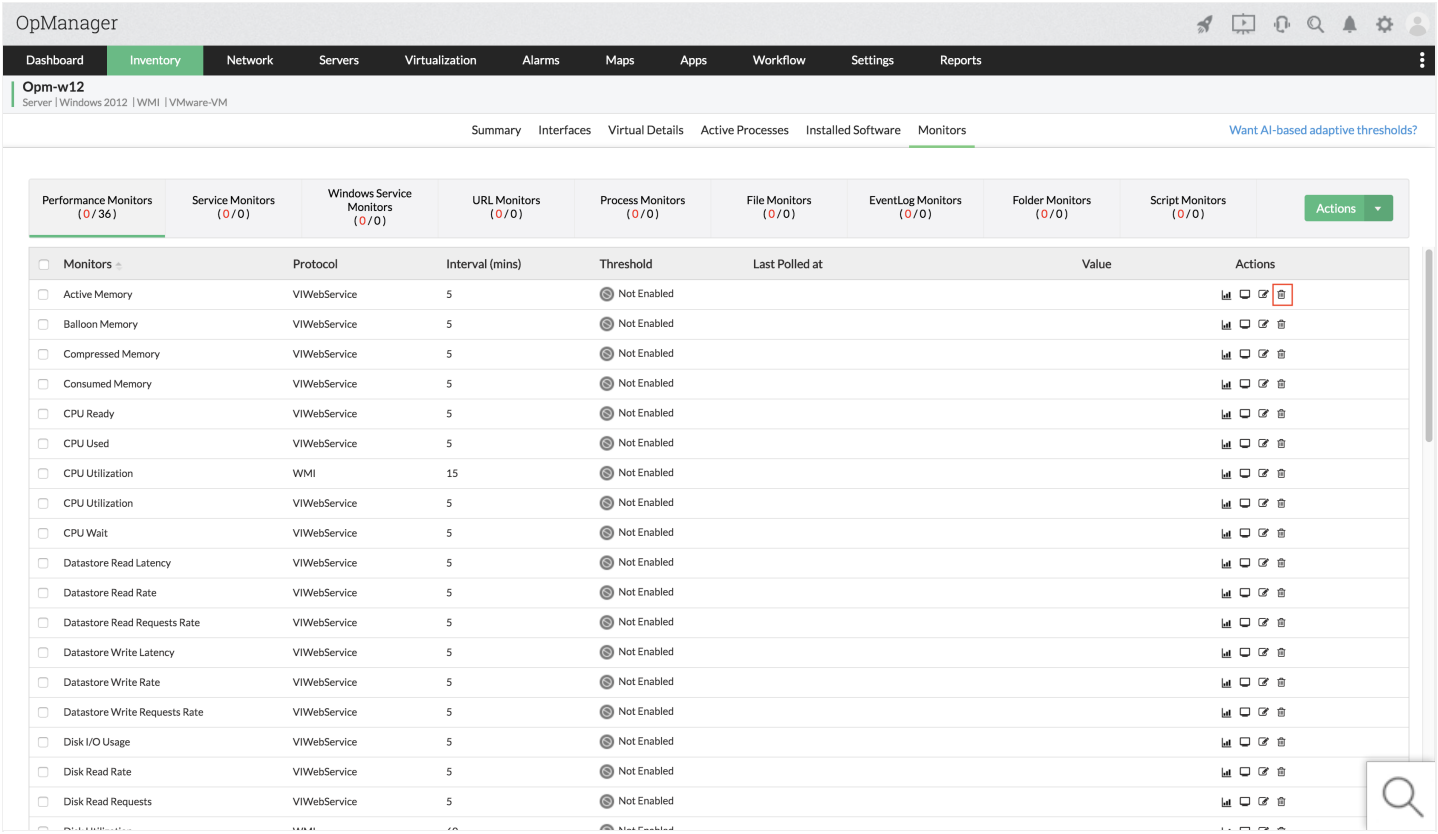
Only custom monitors created by the users can be deleted from this page.

- Go to **Settings ? Monitoring ? Performance monitors** and switch to **'Custom monitors'** section from the dropdown menu.
- Scroll to the custom monitor you wish to delete, & click on the bin icon next to it.



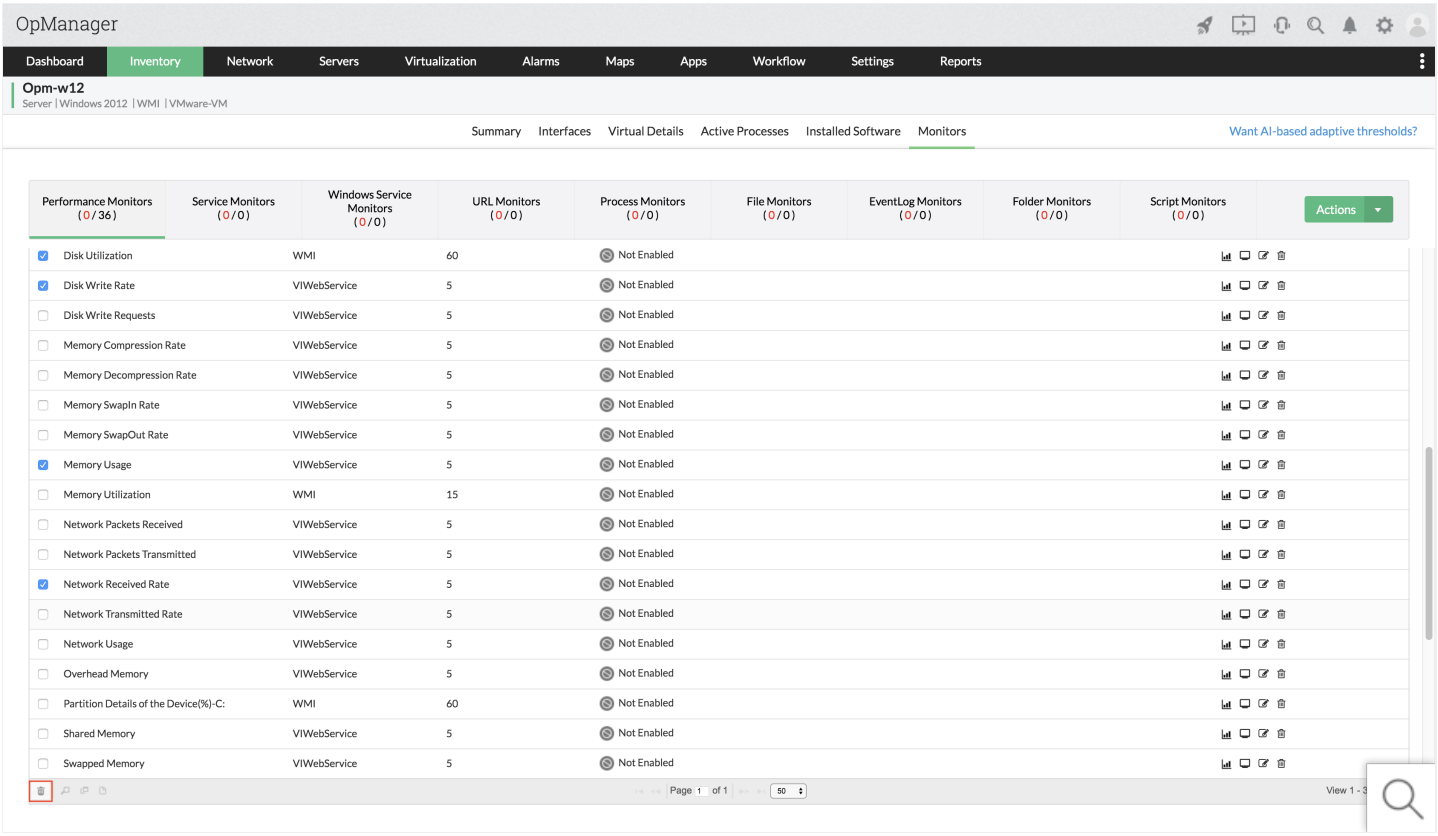
Deleting a custom monitor from here **removes it permanently from OpManager**, and from any device/device template that has this monitor configured already.

3. Deleting a monitor from the device snapshot page:



- Navigate to the device you want to delete the monitor for in the Inventory page, and click on it to view the snapshot page.
- Click on the **'Monitors'** tab.
- Click the bin icon next to any monitor to delete it.

Removing it from the device snapshot page will only de-associate that monitor from the particular device and **will not affect other devices or the device template** in any way. You can also **bulk delete** multiple monitors by selecting them and clicking the bin icon (**Delete selected row**) below the monitors list.



OpManager Performance Monitors

A list of all the performance monitors used in OpManager along with the vendor details, description, protocol and category can be found in this list:

Vendor	Monitors	Description	Protocol	Category
3Com	CPU Temperature	Monitors the CPU temperature	SNMP	Switch / Wireless
3Com	CPU Utilization	Monitors the CPU utilization	SNMP	Switch / Wireless
A10 Networks	Active Connections	Monitors the count of current connections.	SNMP	Load Balancer/WAN Accelerator
A10 Networks	CPU Utilization	Monitors the average CPU usage in last 5 seconds.	SNMP	Load Balancer/WAN Accelerator
A10 Networks	Disk Utilization	Monitors the usage of the disk in MB.	SNMP	Load Balancer/WAN Accelerator
A10 Networks	Fan Status	Monitors the fan status: 0: Failed, 4: OK-fixed/high, 5: OK-low/med, 6: OK-med/med, 7: OK-med/high, -2: not ready, 1: unknown.	SNMP	Load Balancer/WAN Accelerator
A10 Networks	Free disk Space	Monitors the Free space of the disk in MB.	SNMP	Load Balancer/WAN Accelerator
A10 Networks	Lower Power Supply Status	Monitors the lower power supply status. Power supply status : off(0),on(1),unknown(-1).	SNMP	Load Balancer/WAN Accelerator
A10 Networks	Memory Utilization	Monitors the memory utilization(%).	SNMP	Load Balancer/WAN Accelerator
A10 Networks	Server Count	The total count of axServer entries in the table.	SNMP	Load Balancer/WAN Accelerator
A10 Networks	System Temperature	Monitors the physical system temperature in Celsius.	SNMP	Load Balancer/WAN Accelerator
A10 Networks	Upper Power Supply Status	Monitors the Upper power supply status. Power Supply status: off(0),on(1),unknown(-1).	SNMP	Load Balancer/WAN Accelerator
Alcatel	Chassis Temperature	Maximum one-minute chassis temperature over the last hour (percent)	SNMP	Switch / Router

Alcatel	CMM CPU Temperature	Maximum one-minute CMM CPU temperature over the last hour (percent)	SNMP	Switch / Router
Alcatel	Device CPU Utilization	Maximum one-minute device-level CPU utilization over the last hour (percent)	SNMP	Switch / Router
Alcatel	Device Memory Utilization	Maximum one-minute device-level memory utilization over the last hour (percent)	SNMP	Switch / Router
Alcatel	Module CPU Utilization	Maximum one-minute module-level CPU utilization over the last hour (percent)	SNMP	Switch / Router
Alcatel	Moduler Memory Utilization	Maximum one-minute module-level memory utilization over the last hour (percent)	SNMP	Switch / Router
Amaranten	Amaranten-Connections	Monitors the Connections of Amaranten Firewall	SNMP	Firewall
Amaranten	CPU Utilization	Monitors the CPU of Amaranten Firewall	SNMP	Firewall
Amaranten	Memory Utilization	Monitors the Memory of Amaranten Firewall	SNMP	Firewall
American Power Conversion Corp.	Number of PDU Outlets	Monitors the OID will return the number of outlets contained in the device.	SNMP	UPS / PDU
American Power Conversion Corp.	PDU Bank Load	Monitors the OID will return the phase/bank load measured in tenths of Amps.	SNMP	UPS / PDU
American Power Conversion Corp.	PDU Phase Load	Monitors the current draw, in tenths of Amps, of the load on the Rack PDU phase being queried	SNMP	UPS / PDU
American Power Conversion Corp.	PDU Phase Load status	Monitors the present load status of the Rack PDU phase being queried { lowLoad (1) , normal (2) , nearOverload (3) , overload (4) }	SNMP	UPS / PDU
American Power Conversion Corp.	PDU Phases	Monitors the OID will return the number of phases supported by the device.	SNMP	UPS / PDU
American Power Conversion Corp.	PDU Power Load	Monitors the load power, in hundredths of kiloWatts, consumed on the Rack PDU phase being queried	SNMP	UPS / PDU
American Power Conversion Corp.	PDU Voltage	Monitors the Voltage, in Volts, of the Rack PDU phase being queried	SNMP	UPS / PDU

American Power Conversion Corp.	UPS Charge	Monitors UPS Charge	SNMP	UPS
American Power Conversion Corp.	UPS Input Line Voltage	The current utility line voltage in VAC	SNMP	UPS
American Power Conversion Corp.	UPS Load	Monitors UPS Load	SNMP	UPS
American Power Conversion Corp.	UPS Output Current	The current in ampres drawn by the load on the UPS	SNMP	UPS
American Power Conversion Corp.	UPS Output Voltage	The output voltage of the UPS system in VAC	SNMP	UPS
APC	CPU Utilization	CPU Utilization	SNMP	UPS
APC	Total Active Sessions	Total Active Sessions	SNMP	UPS
Array	Connection	Monitors the Connections of Array-APV LoadBalancer	SNMP	Load Balancer
Array	CPU Utilization	Monitors the CPU of Array-APV LoadBalancer	SNMP	Load Balancer
Array	Memory Utilization	Monitors the Memory of Array-APV LoadBalancer	SNMP	Load Balancer
Autelan	CPU Utilization	Monitors the CPU of Autelan-AS3200 Switch	SNMP	Switch
Autelan	Memory Utilization	Monitors the Memory of Autelan-AS3200 Switch	SNMP	Switch
Barracuda	Bounced Mail Queues	Monitors the Bounced mail queues	SNMP	Networking Device
Barracuda	Buffer Memory	Monitors the system Buffer Momory Utilization	SNMP	Networking Device
Barracuda	CPU Utilization	Monitors the system 15 minutes cpu Load	SNMP	Networking Device
Barracuda	CPU Utilization (Last 1 min)	Monitors the system last 1 minute cpu load	SNMP	Networking Device
Barracuda	CPU Utilization (Last 5 min)	Monitors the system last 5 minutes cpu Load	SNMP	Networking Device
Barracuda	InBound Mail Queues	Monitors the InBound mail queues	SNMP	Networking Device

Barracuda	Mail Input	Monitors the system Mail Input counts	SNMP	Networking Device
Barracuda	Mail Output	Monitors the systems Mail output counts	SNMP	Networking Device
Barracuda	Memory Utilization	Monitors the system MemoryUtilization	SNMP	Networking Device
Barracuda	OutBound Mail Queues	Monitors the OutBound Mail queues	SNMP	Networking Device
Barracuda	Used Disk Space	Monitors the systems used disk space	SNMP	Networking Device
Blue Coat Systems, Inc.	Client HTTP Errors	Monitors the number of HTTP errors caused by client connections.	SNMP	WAN Accelerator
Blue Coat Systems, Inc.	Client HTTP Hit(s)	Monitors the number of HTTP hits that the proxy clients have produced.	SNMP	WAN Accelerator
Blue Coat Systems, Inc.	Client HTTP In Traffic	Monitors the number of kilobits recieved from the clients by the proxy.	SNMP	WAN Accelerator
Blue Coat Systems, Inc.	Client HTTP Out Traffic	Monitors the number of kilobits delivered to clients from the proxy.	SNMP	WAN Accelerator
Blue Coat Systems, Inc.	Client HTTP Request(s)	Monitors the number of HTTP requests recieved from clients.	SNMP	WAN Accelerator
Blue Coat Systems, Inc.	CPU Utilization	Monitors the CPU of Bluecoat Switches	SNMP	WAN Accelerator
Blue Coat Systems, Inc.	CPU Utilization	Monitors the Percent of resource in use.	SNMP	WAN Accelerator
Blue Coat Systems, Inc.	Disk Utilization	Monitors the Percent of resource in use. When the resource is disk, it is the amount of disk used by the cache subsytem.	SNMP	WAN Accelerator
Blue Coat Systems, Inc.	Memory Utilization	Monitors the Memory of Bluecoat Switches	SNMP	WAN Accelerator
Blue Coat Systems, Inc.	Memory Utilization	Monitors the MemoryUtilization.	SNMP	WAN Accelerator
Blue Coat Systems, Inc.	Objects In Cache	Monitors the number of objects currently held by the proxy.	SNMP	WAN Accelerator
Blue Coat Systems, Inc.	Server HTTP Errors	Monitors the number of HTTP errors while fetching objects.	SNMP	WAN Accelerator
Blue Coat Systems, Inc.	Server HTTP In Traffic	Monitors the number of Kbs recieved by the proxy from remote servers.	SNMP	WAN Accelerator
Blue Coat Systems, Inc.	Server HTTP Out Traffic	Monitors the number of kbs transmitted by the proxy to remote servers.	SNMP	WAN Accelerator
Blue Coat Systems, Inc.	Server HTTP Requests	Monitors the number of Http requests that the proxy has issued.	SNMP	WAN Accelerator

Check Point Software Technologies Ltd	FW Dropped Packets	Monitors the number of dropped packets	SNMP	Firewall
Check Point Software Technologies Ltd	FW Logged Packets	Monitors the number of logged packets	SNMP	Firewall
Check Point Software Technologies Ltd	FW Rejected Packets	Monitors the number of rejected packets	SNMP	Firewall
Cisco	Aborted Interface In Packets	Monitors the aborted interfaces in packets	SNMP	Networking Device
Cisco	Active Session Count	Active Session Count	SNMP	Firewall
Cisco	Associated Mobile Stations	Monitors the number of Mobile Stations currently associated with the WLAN.	SNMP	Wireless
Cisco	Associated Mobile User(s)	Monitors associated Mobile User(s) for Cisco devices	SNMP	Wireless
Cisco	Backplane Utilization	Monitors the Backplane Utilization	SNMP	Switch
Cisco	BGP PEER STATE	idle2, connect3, active4, opensent5, openconfirm6, established	SNMP	Router
Cisco	Big Buffer Hits	Monitors the Total big buffer hits	SNMP	Router
Cisco	Big Buffer Misses	Monitors the Total big buffer misses	SNMP	Router
Cisco	Buffer Create Failures	Monitors the buffer create failures	SNMP	Router
Cisco	Buffer Failures	Monitors the Buffer Failures	SNMP	Router
Cisco	CardOperstatus	1 : not-specified2 : up3 : down4 : standby	SNMP	Switch
Cisco	Chassis Input Power	Monitors the Chassis Input Power	UCS	UCS
Cisco	Chassis Output Power	Monitors the Chassis Output Power	UCS	UCS
Cisco	Cisco Memory Utilization	Monitors the Memory Utilization	SNMP	Networking Device
Cisco	Cisco Temperature	Monitors temperature at the testpoint maintained by the environmental monitor	SNMP	Networking Device
Cisco	CPU Usage (1 min avg)	Monitors the one-minute moving average of the CPU busy percentage	SNMP	Networking Device
Cisco	CPU Usage (5 mins avg)	Monitors the five-minute moving average of the CPU busy percentage	SNMP	Networking Device
Cisco	CPU Usage (5 secs avg)	Monitors the CPU busy percentage in the last 5 seconds	SNMP	Networking Device
Cisco	CPU Utilization	Monitors the average utilization of CPU on the active supervisor.	SNMP	Switch

Cisco	CPU Utilization	Monitors the device CPU Utilization.	SNMP	Networking Device
Cisco	CPU Utilization(WLC)	Monitors the Current CPU Load of the switch (Cisco WLC device) in percentage.	SNMP	Wireless
Cisco	devCellularstatus	Custom Monitor	SNMP	Wireless
Cisco	devClientCount	Custom Monitor	SNMP	Wireless
Cisco	devContactedat	Custom Monitor	SNMP	Wireless
Cisco	devLanIP	Custom Monitor	SNMP	Wireless
Cisco	devMac	Custom Monitor	SNMP	Wireless
Cisco	devMeshstatus	Custom Monitor	SNMP	Wireless
Cisco	devName	Custom Monitor	SNMP	Wireless
Cisco	devNetworkname	Custom Monitor	SNMP	Wireless
Cisco	devProductcode	Custom Monitor	SNMP	Wireless
Cisco	devProductdescription	Custom Monitor	SNMP	Wireless
Cisco	devpublicIP	Custom Monitor	SNMP	Wireless
Cisco	devSerial	Custom Monitor	SNMP	Wireless
Cisco	devStatu	Custom Monitor	SNMP	Wireless
Cisco	devSubnet	Custom Monitor	SNMP	Wireless
Cisco	Disk Utilization	Monitors the disk I/O utilization.	SNMP	Firewall
Cisco	Fabric Interconnect CPU Utilization	Monitors the Fabric Interconnect CPU Utilization	UCS	UCS
Cisco	Fabric Interconnect FanCtrlrInlet1	Monitors the Fabric Interconnect FanCtrlrInlet1	UCS	UCS
Cisco	Fabric Interconnect FanCtrlrInlet2	Monitors the Fabric Interconnect FanCtrlrInlet2	UCS	UCS
Cisco	Fabric Interconnect FanCtrlrInlet3	Monitors the Fabric Interconnect FanCtrlrInlet3	UCS	UCS
Cisco	Fabric Interconnect FanCtrlrInlet4	Monitors the Fabric Interconnect FanCtrlrInlet4	UCS	UCS
Cisco	Fabric Interconnect MainBoardOutlet1	Monitors the Fabric Interconnect MainBoardOutlet1	UCS	UCS
Cisco	Fabric Interconnect MainBoardOutlet2	Monitors the Fabric Interconnect MainBoardOutlet2	UCS	UCS
Cisco	Fabric Interconnect MemAvailable	Monitors the Fabric Interconnect Memory Available	UCS	UCS
Cisco	Fabric Interconnect MemCached	Monitors the Fabric Interconnect MemCached	UCS	UCS
Cisco	Fabric Interconnect PsuCtrlrInlet1	Monitors the Fabric Interconnect PsuCtrlrInlet1	UCS	UCS

Cisco	Fabric Interconnect PsuCtrlrInlet2	Monitors the Fabric Interconnect PsuCtrlrInlet2	UCS	UCS
Cisco	Fan Speed	Monitors the Fan Speed	UCS	UCS
Cisco	FanModule Exhaust Temperature	Monitors the FanModule Exhaust Temperature	UCS	UCS
Cisco	Firewall CPU Utilization	Monitors the CPU utilization of the Firewall	SNMP	Firewall
Cisco	Free 1550K Buffers	Monitors the number of free 1550K blocks	SNMP	Networking Device
Cisco	Free 256K Buffers	Monitors the number of free 256K blocks	SNMP	Networking Device
Cisco	Free 4K Buffers	Monitors the number of free 4K blocks	SNMP	Networking Device
Cisco	Free 80K Buffers	Monitors the number of free 80K blocks	SNMP	Networking Device
Cisco	Free Memory	Monitors the number of bytes from the memory pool that are currently unused	SNMP	Networking Device
Cisco	Ignored Interface In Packets	Monitors the ignored interfaces in packets	SNMP	Networking Device
Cisco	Input Packet Drops	Monitors the input packets drops after the input queue was full	SNMP	Networking Device
Cisco	Interface Collisions	Monitors the interface collisions	SNMP	Networking Device
Cisco	Interface In CRC Errors	Monitors the number of input packets which had cyclic redundancy checksum errors	SNMP	Networking Device
Cisco	Interface In Giants	Monitors the number of input packets larger than the physical media permitted	SNMP	Networking Device
Cisco	Interface In Runts	Monitors the interface in runts	SNMP	Networking Device
Cisco	Interface Input Bits	Monitors the five-minute exponentially decayed moving average of input bits per second	SNMP	Networking Device
Cisco	Interface Output Bits	Monitors the five-minute exponentially decayed moving average of output bits per second	SNMP	Networking Device
Cisco	Interface Reset Count	Monitors the number of times the interface has internally reset	SNMP	Networking Device
Cisco	Interface Restart Count	Monitors the number of times the interface needed to be completely restarted	SNMP	Networking Device
Cisco	Ironport Temperature	Monitors the Temperature in degrees Celsius.	SNMP	Firewall

Cisco	Largest Free Memory	Monitors the largest number of contiguous bytes from the memory pool that are currently unused	SNMP	Networking Device
Cisco	MailTransfer Threads	Monitors the number of threads that perform some task related to transferring mail.	SNMP	Firewall
Cisco	Medium Buffer Hits	Monitors the Total medium buffer hits	SNMP	Router
Cisco	Medium Buffer Misses	Monitors the Total medium buffer misses	SNMP	Router
Cisco	Memory Utilization	Monitors the average utilization of memory on the active supervisor.	SNMP	Switch
Cisco	Memory Utilization	Monitors the device memory utilization.	SNMP	Firewall
Cisco	Memory Utilization	Monitors the device Memory Utilization	SNMP	Switch
Cisco	Memory Utilization(WLC)	Monitors the current Memory Utilization of the Cisco WLC device.	SNMP	Wireless
Cisco	Modems in Use	Custom Monitor	SNMP	Router
Cisco	Motherboard Consumed Power	Monitors the Monitors the Motherboard Consumed Power	UCS	UCS
Cisco	Motherboard Input Current	Monitors the Motherboard Input Current	UCS	UCS
Cisco	Motherboard Input Voltage	Monitors the Motherboard Input Voltage	UCS	UCS
Cisco	OpenFilesOrSockets	Monitors the number of open files or sockets.	SNMP	Firewall
Cisco	OSPF IF State	down2, loopback3, waiting4, pointToPoint5, designatedRouter6, backupDesignatedRouter7, otherDesignatedRouter	SNMP	Router
Cisco	Output Packet Drops	Monitors the output packets drop	SNMP	Router
Cisco	Outstanding DNS Requests	Monitors the number of DNS requests that have been sent but for which no reply has been received.	SNMP	Firewall
Cisco	Pending DNS Requests	Monitors the number of DNS requests waiting to be sent.	SNMP	Firewall
Cisco	PSUs Input Voltage	Monitors the PSUs Input Voltage	UCS	UCS
Cisco	PSUs Internal Temperature	Monitors the PSUs Internal Temperature	UCS	UCS
Cisco	PSUs Output Current	Monitors the PSUs Output Current	UCS	UCS
Cisco	PSUs Output Power	Monitors the PSUs Output Power	UCS	UCS
Cisco	PSUs Output12v	Monitors the PSUs Output12v	UCS	UCS
Cisco	PSUs Output3v3	Monitors the PSUs Output3v3	UCS	UCS
Cisco	Router Memory Utilization	Monitors the Memory utilization of the router	SNMP	Router

Cisco	Small Buffer Hits	Monitors the Total small buffer hits	SNMP	Networking Device
Cisco	Small Buffer Misses	Monitors the Total small buffer misses	SNMP	Router
Cisco	Switch CPU Utilization(5 mins avg)	Monitors the five-minute moving average of the CPU busy percentage	SNMP	Switch
Cisco	Switch Memory Utilization	Monitors the Memory utilization of the switch	SNMP	Networking Device
Cisco	sysUpTimeAtLastChassisChange	"Time in seconds/100 from the last coldstart to the last change in the chassis configuration. This value will be updatedwhenever the chassis experiences a changein the count, type, or slot position ofa card in cardTable."	SNMP	Switch
Cisco	Temperature(WLC)	Monitors the current Internal Temperature of the unit in Centigrade(Cisco WLC).	SNMP	Wireless
Cisco	Total Huge Buffer Hits	Monitors the huge buffer hits	SNMP	Router
Cisco	Total Huge Buffer Misses	Monitors the total huge buffer misses	SNMP	Router
Cisco	Total Large Buffer Hits	Monitors the Total large buffer hits	SNMP	Router
Cisco	Total Large Buffer Misses	Monitors the total large buffer misses	SNMP	Router
Cisco	Tunnel In-Drop Packets	VPN Tunnel In-Drop Packets	SNMP	Firewall
Cisco	Tunnel In-Octet	VPN Tunnel In-Octet	SNMP	Firewall
Cisco	Tunnel In-Packets	VPN Tunnel In-Packets	SNMP	Firewall
Cisco	Tunnel Out-Drop Packets	VPN Tunnel Out-Drop Packets	SNMP	Firewall
Cisco	Tunnel Out-Octet	VPN Tunnel Out-Octet	SNMP	Firewall
Cisco	Tunnel Out-Packets	VPN Tunnel Out-Packets	SNMP	Firewall
Cisco	Used Memory	Monitors the number of bytes from the memory pool that are currently in use	SNMP	Networking Device
Citrix Systems, Inc.	Active Server Connection(s)	Monitors the number of connections currently serving requests.	SNMP	Load Balancer
Citrix Systems, Inc.	Client Connection(s) in ClosingState	Monitors the number of client connections in NetScaler in closing states.	SNMP	Load Balancer
Citrix Systems, Inc.	Client Connection(s) in OpeningState	Monitors the number of client connections in NetScaler in opening states.	SNMP	Load Balancer
Citrix Systems, Inc.	CPU Utilization	Monitors the CPU utilization percentage.	SNMP	Load Balancer
Citrix Systems, Inc.	CPU Utilization	Average physical cpu usage	XenService	Server
Citrix Systems, Inc.	CPU Utilization	Average of VM VCPUs Utilization	XenService	Server

Citrix Systems, Inc.	Current Client Connection(s)	Monitors the number of client connections in NetScaler.	SNMP	Load Balancer
Citrix Systems, Inc.	Current Server Connection(s)	Monitors the number of server connections in NetScaler.	SNMP	Load Balancer
Citrix Systems, Inc.	Disk I/O Usage	Virtual Disk I/O Usage of VM	XenService	Server
Citrix Systems, Inc.	Disk Utilization	Monitors the Percentage of the disk space used.	SNMP	Load Balancer
Citrix Systems, Inc.	Domain0 Average Load	Load for Domain0 in XenServer	XenService	Server
Citrix Systems, Inc.	Established Client Connection(s)	Monitors the number of client connections in NetScaler in established state.	SNMP	Load Balancer
Citrix Systems, Inc.	Established Server Connection(s)	Monitors the number of server connections in NetScaler in established state.	SNMP	Load Balancer
Citrix Systems, Inc.	Http Total Gets	Monitors the number of HTTP GET requests received.	SNMP	Load Balancer
Citrix Systems, Inc.	Http Total Others(non-GET/POST)	Monitors the number of non-GET/POST HTTP methods received.	SNMP	Load Balancer
Citrix Systems, Inc.	Http Total Posts	Monitors the number of HTTP POST requests received.	SNMP	Load Balancer
Citrix Systems, Inc.	Memory Allocation By XAPI	Memory allocation done by the xapi daemon	XenService	Server
Citrix Systems, Inc.	Memory Utilization	Monitors the Memory utilization percentage.	SNMP	Load Balancer
Citrix Systems, Inc.	Memory Utilization	Memory Utilization of host	XenService	Server
Citrix Systems, Inc.	Memory Utilization	Memory Utilization of VM	XenService	Server
Citrix Systems, Inc.	Network Received Rate	Bytes per second received on all physical interfaces	XenService	Server
Citrix Systems, Inc.	Network Transmitted Rate	Bytes per second sent on all physical interfaces	XenService	Server
Citrix Systems, Inc.	Network Usage	Network Usage of host	XenService	Server
Citrix Systems, Inc.	Network Usage	Network I/O Usage by XenServer VM	XenService	Server
Citrix Systems, Inc.	scPolicy Url Hits	This counter gives the number of times netscaler matched an incoming request with a Configured sureconnect policy.	SNMP	Load Balancer
Citrix Systems, Inc.	scSession Requests	This counter gives the number of requests which came in a SureConnect session.	SNMP	Load Balancer

Citrix Systems, Inc.	SSL CardsUP	Monitors the number of ssl cards UP. If number of cards UP is lower than a threshold, a failover will be initiated.	SNMP	Load Balancer
Citrix Systems, Inc.	SSL session(s)	Monitors the number of SSL sessions.	SNMP	Load Balancer
Citrix Systems, Inc.	TCP Total ClientConnection Opened	Monitors the total number of opened client connections.	SNMP	Load Balancer
Citrix Systems, Inc.	TCP TotalSyn	Monitors the number of SYN packets received.	SNMP	Load Balancer
Citrix Systems, Inc.	TCPSurgeQueueLength	Monitors the number of connections in surge queue.	SNMP	Load Balancer
Citrix Systems, Inc.	Total Hit(s)	Monitors the total hits for the policy.	SNMP	Load Balancer
Citrix Systems, Inc.	Total Policy Hits	Monitors the Total policy hits count.	SNMP	Load Balancer
Citrix Systems, Inc.	TTFB between Netscaler to server	Monitors the average TTFB between the netscaler and the server.	SNMP	Load Balancer
Citrix Systems, Inc.	VCPUs Concurrency Hazard	Fraction of time that some VCPUs are running and some are runnable	XenService	Server
Citrix Systems, Inc.	VCPUs Full Contention	Fraction of time that all VCPUs are runnable (i.e., waiting for CPU)	XenService	Server
Citrix Systems, Inc.	VCPUs Full Run	Fraction of time that all VCPUs are running	XenService	Server
Citrix Systems, Inc.	VCPUs Idle	Fraction of time that all VCPUs are blocked or offline	XenService	Server
Citrix Systems, Inc.	VCPUs Partial Contention	Fraction of time that some VCPUs are runnable and some are blocked	XenService	Server
Citrix Systems, Inc.	VCPUs Partial Run	Fraction of time that some VCPUs are running, and some are blocked	XenService	Server
Citrix Systems, Inc.	VServer Current ClientConnections	Monitors the number of current client connections.	SNMP	Load Balancer
Citrix Systems, Inc.	VServer Current OutOfService(s)	Monitors the current number of services which are bound to this vserver and are in the state 'outOfService'.	SNMP	Load Balancer
Citrix Systems, Inc.	VServer Current ServerConnections	Monitors the number of current connections to the real servers behind the vserver.	SNMP	Load Balancer
Citrix Systems, Inc.	VServer Current ServicesDown	Monitors the current number of services which are bound to this vserver and are in the state 'down'.	SNMP	Load Balancer
Citrix Systems, Inc.	VServer Current ServicesUp	Monitors the current number of services which are bound to this vserver and are in the state 'up'.	SNMP	Load Balancer

Citrix Systems, Inc.	VServer Total Hits	Monitors the Total vserver hits.	SNMP	Load Balancer
Citrix Systems, Inc.	VServer Total RequestBytes	Monitors the total number of request bytes received on this service/vserver.	SNMP	Load Balancer
Citrix Systems, Inc.	VServer Total Requests	Monitors the total number of requests received on this service/vserver(This is applicable for HTTP/SSL servicetype).	SNMP	Load Balancer
Citrix Systems, Inc.	VServer Total ResponseBytes	Monitors the number of response bytes received on this service/vserver.	SNMP	Load Balancer
MGE	UPS Charge	Monitors UPS Charge	SNMP	UPS
Citrix Systems, Inc.	VServer TotalResponses	Monitors the number of responses received on this service/vserver(This is applicable for HTTP/SSL servicetype).	SNMP	Load Balancer
Citrix Systems, Inc.	XAPI Memory Usage	XenAPI Memory Utilization	XenService	Server
Compaq	CpqHe Server Temperature	Monitors the server temprature	SNMP	Server
Compaq	CPU Utilization	Monitors the CPU Utilization	SNMP	Server
Compaq	CPU Utilization (30 Min Avg)	Monitors the CPU Utilization	SNMP	Server
Compaq	CPU Utilization (5 Min Avg)	Monitors the CPU Utilization	SNMP	Server
Compaq	CPU Utilization (Hr. Avg)	Monitors the CPU Utilization	SNMP	Server
Compaq	Deferred Transmission	Monitors the interfaces deffered transmission	SNMP	Server
Compaq	Excessive Collisions	Monitors the interface excessive collisions	SNMP	Server
Compaq	File System Usage Percentage	Monitors the percetage space used in File System	SNMP	Server
Compaq	File System Usage Size	Monitors the space used by file system	SNMP	Server
Compaq	Free Physical Memory	Monitors the free physical memory	SNMP	Server
Compaq	Free Virtual Memory	Monitors the free virtual memory	SNMP	Server
Compaq	Input Voltage	Monitors the input voltage of power supply	SNMP	Server
Compaq	Interface Rx Errors	Monitors the interface receive errors	SNMP	Server
Compaq	Interface Rx Traffic	Monitors the interface received traffic	SNMP	Server
Compaq	Interface Tx Errors	Monitors the interface transmit error	SNMP	Server
Compaq	Interface Tx Traffic	Interface Transmit Traffic	SNMP	Server
Compaq	Internal MAC Transmit Errors	Monitors the internal MAC transmit errors	SNMP	Server
Compaq	Late Collisions	Monitors the interface Late Collisions	SNMP	Server
Compaq	Multiple Collision Packets	Multiple Collision Frames	SNMP	Server
Compaq	Power Capacity	Monitors the utilized power in Watts	SNMP	Server
Compaq	SCSI Corrected Read Errors	Monitors the SCSI corrected read errors	SNMP	Server

Compaq	SCSI Drive Spin Up Time	Monitors the SCSI drive spin up time	SNMP	Server
Compaq	SCSI Hard Read Errors	Monitors the SCSI hard read errors	SNMP	Server
Compaq	SCSI Hard Write Errors	Monitors the hard write errors	SNMP	Server
Compaq	SCSI High Read Sectors	Monitors the SCSI high speed sector	SNMP	Server
Compaq	SCSI High Write Sectors	Monitors the SCSI high write sectors	SNMP	Server
Compaq	SCSI Low Read Sectors	Monitors the SCSI low read sector	SNMP	Server
Compaq	SCSI Low Write Sectors	Monitors the SCSI low write sectors	SNMP	Server
Compaq	SCSI Recovered Read Errors	Monitors the SCSI recovered read errors	SNMP	Server
Compaq	SCSI Recovered Write Errors	Monitors the SCSI recovered write errors	SNMP	Server
Compaq	SCSI Seek Errors	Monitors the SCSI seek errors	SNMP	Server
Compaq	SCSI Service Time	Monitors the SCSI service time	SNMP	Server
Compaq	SCSI Timeout Errors	Monitors the SCSI timeout errors	SNMP	Server
Compaq	SCSI Trap Packets	Monitors the number of SCSI trap packets	SNMP	Server
Compaq	SCSI Used Reallocation Sectors	Monitors the SCSI used reallocation sectors	SNMP	Server
Compaq	Single Collision Packets	Single Collision packets	SNMP	Server
Compaq	SNMP Trap Log Size	Monitors the SNMP trap log size	SNMP	Server
Compaq	Traffic Trap Count	Monitors the number of trap count in traffic	SNMP	Server
Cyberoam	CPU Utilization	Monitors the cpu usage.	SNMP	Firewall
Cyberoam	Disk Utilization	Monitors the used disk percentage.	SNMP	Firewall
Cyberoam	FTP Hits	Monitors the count of Ftp Hits.	SNMP	Firewall
Cyberoam	HTTP Hits	Monitors the count of Http Hits.	SNMP	Firewall
Cyberoam	IMAP Hits	Monitors the count of imapHits.	SNMP	Firewall
Cyberoam	Live Users	Monitors the count of Live Users.	SNMP	Firewall
Cyberoam	Memory Utilization	Monitors the Momory utilization.	SNMP	Firewall
Cyberoam	POP3 Hits	Monitors the count of pop3Hits.	SNMP	Firewall
Cyberoam	SMTP Hits	Monitors the count of Smtp Hit.	SNMP	Firewall
DCN	CPU Utilization	CPU Utilization for DCN	SNMP	Switch
DCN	Memory Utilization	Memory Utilization for DCN	SNMP	Switch
Dell Inc.	Alert	Custom Monitor	SNMP	Networking Device
Dell Inc.	CPU Utilization	CPU Utilization for DELL Inc	SNMP	Switch
Dell Inc.	CPU Utilization	Monitors the CPU of DELL_Force10_S25N switch	SNMP	Switch

Dell Inc.	Memory Utilization	Monitors the Memory of DELL_Force10_S25N switch	SNMP	Switch
Dell Inc.	Memory Utilization	Memory Utilization for Dell Inc	SNMP	Switch
DPtech	Connections	Monitors the Connections of DPtech Firewall	SNMP	Firewall
DPtech	CPU Utilization	CPU Utilization for DPtech	SNMP	Firewall
DPtech	CPU Utilization	Monitor the CPU Utilization for DPtech devices	SNMP	Firewall / Router
DPtech	Memory Utilization	Memory Utilization for DPtech	SNMP	Firewall
DPtech	Memory Utilization	Monitors the Memory of DPTECH Switches	SNMP	Firewall
DPtech	Memory Utilization	Monitor the Memory Utilization for DPtech devices	SNMP	Firewall / Router
Eaton	Online	Custom Monitor	SNMP	UPS
Eaton	UPS Battery Current	Battery Current as reported by the UPS metering. Current is positive when discharging, negative when recharging the battery.	SNMP	UPS
Eaton	UPS Charge	Battery percent charge.	SNMP	UPS
Eaton	UPS Input Line Voltage	The measured input voltage from the UPS meters in volts.	SNMP	UPS
Eaton	UPS Input Source	The present external source of input power.	SNMP	UPS
Eaton	UPS Load	Powerware UPS Load	SNMP	UPS
Eaton	UPS Output Current	The measured UPS output current in amps.	SNMP	UPS
Eaton	UPS Output Voltage	The measured output voltage from the UPS metering in volts.	SNMP	UPS
Eaton	UPS Time Remaining	Battery run time in seconds before UPS turns off due to low battery.	SNMP	UPS
Emerson	LiebertUPS Charge	Monitors UPS Charge	SNMP	UPS
Emerson	LiebertUPS Load	Monitors UPS Load	SNMP	UPS
Extreme	Extreme CPU Utilization	Monitors the CPU Utilization for Extreme Devices	SNMP	Switch
Extreme	Extreme Temperature	Monitors the Temperature for Extreme Devices	SNMP	Switch
Extreme	XOS CPU Utilization	Monitors the XOS CPU Utilization for Extreme Devices	SNMP	Switch
Extreme	XOS Memory Utilization	Monitors the XOS Memory Utilization for Extreme Devices	SNMP	Switch
F5 Networks, Inc.	Active Client Connection(s)	Monitors F5 LoadBalancer Client Active Connections.	SNMP	Load Balancer

F5 Networks, Inc.	Active connections(server-PoolMember)	Monitors the current connections from server-side to the pool member.	SNMP	Load Balancer
F5 Networks, Inc.	Active connections(ServerToSystem)	Monitors the current connections from server-side to the system.	SNMP	Load Balancer
F5 Networks, Inc.	ActiveClientConnections	Monitors the ActiveClientConnections of F5-BIG-IP-1600 LoadBalancer	SNMP	Load Balancer
F5 Networks, Inc.	ClusterMember State	Monitors the state indicating whether the specified member is enabled or not {false(0), true(1)}.	SNMP	Load Balancer
F5 Networks, Inc.	CPU FanSpeed	Monitors the fan speed (in RPM) of the indexed CPU on the system., This is only supported for the platform where the sensor data is available.	SNMP	Load Balancer
F5 Networks, Inc.	CPU Temperature	Monitors the temperature of the indexed CPU on the system. This is only supported for the platform where the sensor data is available.	SNMP	Load Balancer
F5 Networks, Inc.	CPU Utilization	Monitors the CPU of F5-BIG-IP-1600 LoadBalancer	SNMP	Load Balancer
F5 Networks, Inc.	CPU Utilization	Monitors the CPU of F5 LoadBalancer	SNMP	Load Balancer
F5 Networks, Inc.	CPU Utilization	Monitors F5 LoadBalancer CPUUtilization.	SNMP	Load Balancer
F5 Networks, Inc.	Dropped Packet(s)	Monitors the total dropped packets.	SNMP	Load Balancer
F5 Networks, Inc.	Global TM PoolMember State	Monitors the state indicating whether the specified pool member is enabled or not {disable(0), enable(1)}.	SNMP	Load Balancer
F5 Networks, Inc.	Global TM VirtualServer Status	Monitors the activity status of the specified virtual server, as specified by the user {none(0), enabled(1), disabled(2), disabledbyparent(3)}.	SNMP	Load Balancer
F5 Networks, Inc.	HTTP Request(s)	Monitors the total number of HTTP requests to the LoadBalancer system.	SNMP	Load Balancer
F5 Networks, Inc.	Incoming Packet Error(s)	Monitors the total incoming packet errors for the system.	SNMP	Load Balancer
F5 Networks, Inc.	Local TM PoolMember state	Monitors the activity status of the specified pool, as specified by the user{none(0), enabled(1), disabled(2), disabledbyparent(3)}.	SNMP	Load Balancer
F5 Networks, Inc.	Memory Utilization	Monitors the Memory of F5-BIG-IP-1600 LoadBalancer	SNMP	Load Balancer
F5 Networks, Inc.	Memory Utilization	Monitors the Memory of F5 LoadBalancer	SNMP	Load Balancer
F5 Networks, Inc.	Memory Utilization	Monitors F5 LoadBalancer MemoryUtilization.	SNMP	Load Balancer

F5 Networks, Inc.	Outgoing Packet Error(s)	Monitors the total outgoing packet errors for the system.	SNMP	Load Balancer
FiberHome	CPU Utilization	Monitors the CPU of FiberHome-EPON-5516 Switch	SNMP	Switch
FiberHome	CPU Utilization	Monitors the CPU of FiberHome-S2200ME-PAF Switch	SNMP	Switch
FiberHome	Memory Utilization	Monitors the Memory of FiberHome-EPON-5516 Switch	SNMP	Switch
FiberHome	Memory Utilization	Monitors the Memory of FiberHome-S2200ME-PAF Switch	SNMP	Switch
Fortigate	Connections	Monitors the Connections of Fortigate Firewall 200B	SNMP	Firewall
Fortigate	Connections	Monitors the Connections of Fortigate devices	SNMP	Router
Fortigate	CPU Utilization	Monitors the CPU of Fortigate Firewall 200B	SNMP	Firewall
Fortigate	CPU Utilization	Monitors the CPU of Fortigate devices	SNMP	Router
Fortigate	Memory Utilization	Monitors the Memory of Fortigate Firewall 200B	SNMP	Firewall
Fortigate	Memory Utilization	Monitors the Memory of Fortigate devices	SNMP	Router
Fortinet, Inc.	Active Session Count	Active Session Count	SNMP	Router
Fortinet, Inc.	CPU Utilization	Monitors the CPU utilization	SNMP	Firewall
Fortinet, Inc.	Memory Utilization	Monitors the Memory Utilization	SNMP	Firewall
Foundry Networks, Inc.	CPU Utilization	The statistics collection of utilization of the CPU in the device	SNMP	Switch
Foundry Networks, Inc.	Foundry Temperature	Temperature of the chassis. Each unit is 0.5 degrees Celcius. Only management module built with temperature sensor hardware is applicable. For those non-applicable management module, it returns no-such-name	SNMP	Switch
Foundry Networks, Inc.	PowerSupply	The power supply operation status	SNMP	Switch
Foundry Networks, Inc.	QosProfileCalculatedBandwidth	Qos Profile Calculated Bandwidth	SNMP	Switch
Foundry Networks, Inc.	QosProfileRequestedBandwidth	Qos Profile Requested Bandwidth	SNMP	Switch

Foundry Networks, Inc.	ViolatorPortNumber	The port number of the switch or router that received a violator packet. It is included in the locked address violation trap	SNMP	Switch
H3C	CPU Utilization	Monitors the CPU of H3C-S10508 Switch	SNMP	Switch
H3C	CPU Utilization	Monitor the CPU Utilization for H3C devices	SNMP	Switch
H3C	CPU Utilization	Monitors the CPU of H3C-S2108-E0004 switch	SNMP	Switch
H3C	CPU Utilization	Monitors the CPU of H3C-S3610-PWR-EI Switch	SNMP	Switch
H3C	CPU Utilization	Monitors the CPU of H3C-S5120-52SC-HI Switch	SNMP	Switch
H3C	CPU Utilization	CPU Utilization for H3C	SNMP	Switch
H3C	CPU Utilization	CPU Utilization for H3C	SNMP	Switch
H3C	CPU Utilization	Monitor the CPU Utilization for H3C devices	SNMP	Switch
H3C	CPU Utilization	Monitors the CPU of H3C-S5800-32C Switch	SNMP	Switch
H3C	CPU Utilization	Monitor the CPU Utilization for H3C devices	SNMP	Switch
H3C	CPU Utilization	Monitor the CPU Utilization for H3C devices	SNMP	Switch
H3C	CPU Utilization	Monitor the CPU Utilization for H3C devices	SNMP	Switch
H3C	CPU Utilization	Monitors the CPU of H3C-S7506E-S Switches	SNMP	Switch
H3C	CPU Utilization	Monitor the CPU Utilization for H3C devices	SNMP	Switch
H3C	CPU Utilization	Monitors the CPU of H3C-S9505E Switch	SNMP	Switch
H3C	CPU Utilization	Monitor the CPU Utilization for H3C devices	SNMP	Switch
H3C	CPU Utilization	Monitor the CPU Utilization for H3C devices	SNMP	Switch
H3C	CPU Utilization	CPU Utilization for H3C	SNMP	Firewall
H3C	CPU Utilization	Monitors the CPU of H3C-WX3008 Switches	SNMP	Switch
H3C	CPU Utilization	Monitors the CPU of H3C Devices	SNMP	Networking Device
H3C	CPU Utilization	Monitor the CPU Utilization for H3C devices	SNMP	Switch
H3C	CPU Utilization	Monitor the CPU Utilization for H3C devices	SNMP	Switch

H3C	CPU Utilization	Monitor the CPU Utilization for H3C devices	SNMP	Router
H3C	CPU Utilization	Monitor the CPU Utilization for H3C devices	SNMP	Networking Device
H3C	CPU Utilization	Monitor the CPU Utilization for H3C devices	SNMP	Switch
H3C	CPU Utilization	Monitor the CPU Utilization for H3C devices	SNMP	Switch
H3C	CPU Utilization	Monitor the CPU Utilization for H3C devices	SNMP	Switch
H3C	CPU Utilization	Monitor the CPU Utilization for H3C devices	SNMP	Switch
H3C	CPU Utilization	Monitor the CPU Utilization for H3C devices	SNMP	Switch
H3C	CPU Utilization	Monitor the CPU Utilization for H3C devices	SNMP	Router / Firewall
H3C	Memory Utilization	Monitors the Memory of H3C-S10508 Switch	SNMP	Switch
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Switch
H3C	Memory Utilization	Monitors the Memory of H3C-S3610-PWR-EI Switch	SNMP	Switch
H3C	Memory Utilization	Monitors the Memory of H3C-S5120-52SC-HI Switch	SNMP	Switch
H3C	Memory Utilization	Memory Utilization for H3C	SNMP	Switch
H3C	Memory Utilization	Memory Utilization for H3C	SNMP	Switch
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Switch
H3C	Memory Utilization	Monitors the Memory of H3C-S5800-32C Switch	SNMP	Switch
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Switch
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Switch
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Switch
H3C	Memory Utilization	Monitors the Memory of H3C-S7506E-S Switches	SNMP	Switch
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Switch

H3C	Memory Utilization	Monitors the Memory of H3C-S9505E Switch	SNMP	Switch
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Switch
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Switch
H3C	Memory Utilization	Memory Utilization for H3C	SNMP	Firewall
H3C	Memory Utilization	Monitors the Memory of H3C-WX3008 Switches	SNMP	Switch
H3C	Memory Utilization	Monitors the Memory of H3C Devices	SNMP	Networking Device
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Switch
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Switch
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Router
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Networking Device
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Switch
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Switch
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Switch
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Switch
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Switch
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Switch
H3C	Memory Utilization	Monitor the Memory Utilization of H3C devices	SNMP	Switch
H3C	Memory Utilization	Monitor the Memory Utilization for H3C devices	SNMP	Router / Firewall
Hewlett-Packard	Associated Mobile User(s)	Monitors associated Mobile User(s) for HP devices	SNMP	Wireless
Hewlett-Packard	CPU Utilization	Monitors the CPU Utilization for HP ProCurve Devices	SNMP	Switch
Hewlett-Packard	Memory Utilization	Monitors the Memory Utilization for HP ProCurve Devices	SNMP	Switch
Hillstone	ActiveClientConnections	Monitors the ActiveClientConnections of Hillstone-SG-6000-G5150 Firewall	SNMP	Firewall

Hillstone	CPU Utilization	Monitors the CPU of Hillstone-SG-6000-G5150 Firewall	SNMP	Firewall
Hillstone	Memory Utilization	Monitors the Memory of Hillstone-SG-6000-G5150 Firewall	SNMP	Firewall
Huawei	CPU Utilization	Monitors the CPU of Eudemon1000E Firewall	SNMP	Firewall
Huawei	CPU Utilization	Monitors the CPU of Huawei-Symantec-USG9310 Router	SNMP	Router
Huawei	CPU Utilization	Monitors the CPU of Huawei-AR1220 Routers	SNMP	Router
Huawei	CPU Utilization	Monitors the CPU of Huawei-AR2240 Routers	SNMP	Router
Huawei	CPU Utilization	Monitors the CPU of Huawei Devices	SNMP	Switch
Huawei	CPU Utilization	Monitors the CPU of Huawei-epon-MA5600T Switch	SNMP	Switch
Huawei	CPU Utilization	Monitors the CPU of Huawei-epon-olt Switch	SNMP	Switch
Huawei	CPU Utilization	CPU Utilization for Huawei	SNMP	Firewall
Huawei	CPU Utilization	Monitors the CPU of Huawei NE20E Router	SNMP	Router
Huawei	CPU Utilization	Monitors the CPU of Huawei-NE40-4 Router	SNMP	Router
Huawei	CPU Utilization	Monitors the CPU of Huawei-Quidway-Router-R2621 Router	SNMP	Router
Huawei	CPU Utilization	CPU Utilization for Huawei	SNMP	Switch
Huawei	CPU Utilization	CPU Utilization for Huawei	SNMP	Switch
Huawei	CPU Utilization	Monitors the CPU of Huawei devices	SNMP	Switch
Huawei	CPU Utilization	Monitor the CPU Utilization for Huawei devices	SNMP	Switch
Huawei	CPU Utilization	Monitors the CPU of Huawei S3352 Switches	SNMP	Switch
Huawei	CPU Utilization	CPU Utilization for Huawei	SNMP	Switch
Huawei	CPU Utilization	CPU Utilization for Huawei	SNMP	Switch
Huawei	CPU Utilization	CPU Utilization for Huawei	SNMP	Switch
Huawei	CPU Utilization	Monitors the CPU of Huawei-S7703 switch	SNMP	Switch
Huawei	CPU Utilization	CPU Utilization for Huawei	SNMP	Switch
Huawei	CPU Utilization	Monitor the CPU Utilization for Huawei devices	SNMP	Switch / Router
Huawei	CPU Utilization	Monitors the CPU of Huawei S9303 Switches	SNMP	Switch

Huawei	CPU Utilization	Monitors the CPU of Huawei S9312 Switches	SNMP	Switch
Huawei	CPU Utilization	Monitors the CPU of Huawei USG9520 Switches	SNMP	Switch
Huawei	CPU Utilization	Monitors the CPU of Huawei_AR3260 Switch	SNMP	Router
Huawei	CPU Utilization	Monitors the CPU of Huawei devices	SNMP	Router
Huawei	CPU Utilization	Monitor the CPU Utilization for Huawei devices	SNMP	Switch / Router
Huawei	CPU Utilization	Monitor the CPU Utilization for Huawei devices	SNMP	Switch / Router
Huawei	Memory Utilization	Monitors the Memory of Eudemon1000E Firewall	SNMP	Firewall
Huawei	Memory Utilization	Monitors the Memory of Huawei-Symantec-USG9310 Router	SNMP	Router
Huawei	Memory Utilization	Monitors the Memory of Huawei-AR1220 Routers	SNMP	Router
Huawei	Memory Utilization	Monitors the Memory of Huawei-AR2240 Routers	SNMP	Router
Huawei	Memory Utilization	Monitors the Memory of Huawei-epon-MA5600T Switch	SNMP	Switch
Huawei	Memory Utilization	Monitors the Memory of Huawei-epon-olt Switch	SNMP	Switch
Huawei	Memory Utilization	Memory Utilization for Huawei	SNMP	Firewall
Huawei	Memory Utilization	Monitors the Memory of Huawei devices	SNMP	Switch
Huawei	Memory Utilization	Monitors the Memory of Huawei NE20E Router	SNMP	Router
Huawei	Memory Utilization	Monitors the Memory of Huawei-NE40-4 Router	SNMP	Router
Huawei	Memory Utilization	Memory Utilization for Huawei	SNMP	Router
Huawei	Memory Utilization	Monitors the Memory of Huawei-Quidway-Router-R2621 Router	SNMP	Router
Huawei	Memory Utilization	Memory Utilization for Huawei	SNMP	Switch
Huawei	Memory Utilization	Monitors the Memory of Huawei devices	SNMP	Switch
Huawei	Memory Utilization	Monitor the Memory Utilization for Huawei devices	SNMP	Switch
Huawei	Memory Utilization	Monitors the Memory of Huawei S3352 Switches	SNMP	Switch
Huawei	Memory Utilization	Memory Utilization for Huawei	SNMP	Switch
Huawei	Memory Utilization	Memory Utilization for Huawei	SNMP	Switch

Huawei	Memory Utilization	Monitors the Memory of Huawei-S7703 switch	SNMP	Switch
Huawei	Memory Utilization	Memory Utilization for Huawei	SNMP	Switch
Huawei	Memory Utilization	Monitors the Memory of Huawei-S8505 Switch	SNMP	Switch
Huawei	Memory Utilization	Monitor the Memory Utilization for Huawei devices	SNMP	Switch
Huawei	Memory Utilization	Monitors the Memory of Huawei S9303 Switches	SNMP	Switch
Huawei	Memory Utilization	Monitors the Memory of Huawei S9312 Switches	SNMP	Switch
Huawei	Memory Utilization	Monitors the Memory of Huawei-USG9300 Router	SNMP	Router
Huawei	Memory Utilization	Monitors the Memory of Huawei USG9520 Switches	SNMP	Switch
Huawei	Memory Utilization	Monitors the Memory of Huawei_AR3260 Switch	SNMP	Router
Huawei	Memory Utilization	Monitors the Memory of Huawei devices	SNMP	Router
Huawei	Memory Utilization	Monitors the Memory of Huawei_SRG1220 Routers	SNMP	Router
Huawei	Memory Utilization	Monitor the Memory Utilization for Huawei devices	SNMP	Switch
Huawei	Memory Utilization	Monitor the Memory Utilization for Huawei devices	SNMP	Switch / Router
IBM	IBM Interface Rx Traffic	Monitors the total number of octets received on the interface	SNMP	Server
IBM	IBM Interface Tx Traffic	Monitors the total number of octets transmitted out of the interface	SNMP	Server
IBM	IBM InterfaceRx Utilization	Monitors the utilization of the interface based on the incoming traffic	SNMP	Server
IBM	IBM InterfaceTx Utilization	Monitors the utilization of the interface based on the outgoing traffic	SNMP	Server
IBM	iBMPSGPhysicalMemoryDataWidth	Monitoring the data width used in this Physical Memory	SNMP	Server
IBM	iBMPSGPhysicalMemoryTotalWidth	Monitoring the total width used in this Physical Memory	SNMP	Server
IBM	IBMPSGProcessorCurrentClockSpeed	Current clock speed of this Processor	SNMP	Server
IBM	IBMPSGTachometerCurrentReading	Monitors the fan speed	SNMP	Server
IBM	IBMPSGTemperatureSensorCurrentReading	Monitors the Current Reading of this Temperature Sensor	SNMP	Server
IBM	IBMPSGVoltageSensorCurrentReading	Monitors the Current Reading of this Voltage Sensor	SNMP	Server

IBM	Total Memory Width Utilization	Monitoring the total used width utilization of this Physical Memory	SNMP	Server
Juniper	Active Session Count	Description	SNMP	Firewall
Juniper	Average delay	Average round-trip time (in milliseconds) between two measurement points.	SNMP	Switch / Router
Juniper	Buffer Utilization	Operating Buffer Utilization	SNMP	Switch / Firewall
Juniper	Component operating status	Operational status of a router hardware component	SNMP	Switch / Router
Juniper	Component operating temperature	Operational temperature of a hardware component, in Celsius	SNMP	Networking Device
Juniper	CPU load	Average utilization over the past minute of a CPU.	SNMP	Networking Device
Juniper	CPU Utilization	Monitors the CPU of Firewall	SNMP	Firewall
Juniper	CPU Utilization	Monitors the CPU of Juniper-EX Switch	SNMP	Switch
Juniper	CPU Utilization	Monitors the CPU of Juniper-SRX650 Firewall	SNMP	Firewall
Juniper	CPU Utilization(Last 1 min)	Monitors the Last one minute CPU utilization in percentage.	SNMP	Firewall
Juniper	CPU Utilization(Last 15 min)	Monitors the Last fifteen minutes CPU utilization in percentage.	SNMP	Firewall
Juniper	CPU Utilization(Last 5 min)	Monitors the Last five minutes CPU utilization in percentage.	SNMP	Firewall
Juniper	DRAM size	DRAM size	SNMP	Networking Device
Juniper	FRU state	Operational status of each field-replaceable unit (FRU)	SNMP	Switch / Router
Juniper	Juniper Connections	Monitors the Connections of Firewall	SNMP	Firewall
Juniper	Juniper Temperature	Temperature Measurement	SNMP	Swich / Router
Juniper	Label Switched Path state	Operational state of an MPLS label-switched path	SNMP	Router
Juniper	LSP utilization	Utilization of the MPLS label-switched path	SNMP	Switch / Router
Juniper	Memory Utilization	Monitors the Memory of Juniper-EX Switch	SNMP	Switch
Juniper	Memory Utilization	Monitors the Memory of Juniper Switches	SNMP	Switch
Juniper	Memory Utilization	Monitors the Memory of Juniper-SRX650 Firewall	SNMP	Firewall
Juniper	Memory utilization	Utilization of memory on the Routing Engine and FPC.	SNMP	Swich / Router

Juniper	Memory Utilization	Monitors the Memory Utilization	SNMP	Switch / Firewall
Juniper	Memory Utilization	Monitors the Memory of Firewall	SNMP	Firewall
Juniper	Outbound Counters	Number of bytes belonging to the specified forwarding class that were transmitted on the specified virtual circuit	SNMP	Switch / Router
Juniper	Outbound Counters for non-ATM	Number of transmitted bytes or packets per interface per forwarding class	SNMP	Router
Juniper	Output queue size	Size, in packets, of each output queue per forwarding class, per interface	SNMP	Switch / Router
Juniper	Rate of tail dropped packets	Rate of tail-dropped packets per output queue, per forwarding class, per interface	SNMP	Router
Juniper	Redundancy switchover	Total number of redundancy switchovers reported by this entity	SNMP	Swich / Router
Juniper	Rss Session FailureCount	Monitors the rss session failure count.	SNMP	Firewall
Juniper	RSS SessionCount	Monitor the allocate rss session number	SNMP	Firewall
KYLAND	CPU Utilization	CPU Utilization for KYLAND	SNMP	Switch
KYLAND	Memory Utilization	Memory Utilization for KYLAND	SNMP	Switch
leadsec	CPU Utilization	Monitors the CPU of leadsec Firewall	SNMP	Firewall
leadsec	Memory Utilization	Monitors the Memory of leadsec Firewall	SNMP	Firewall
MAIPU	CPU Utilization	CPU Utilization for MAIPU	SNMP	Swich / Router
MAIPU	CPU Utilization	Monitors the CPU of MAIPU S4126E Switch	SNMP	Switch
MAIPU	CPU Utilization	Monitors the CPU of MAIPU S4128E Switch	SNMP	Switch
MAIPU	Memory Utilization	Memory Utilization for MAIPU	SNMP	Swich / Router
MAIPU	Memory Utilization	Monitors the Memory of MAIPU S4126E Switch	SNMP	Switch
MAIPU	Memory Utilization	Monitors the Memory of MAIPU S4128E Switch	SNMP	Switch
MAIPU	Temperature	Monitors the Temperature of MAIPU Router	SNMP	Router
MGE	Battery Installed	Battery Installed	SNMP	UPS
MGE	Battery sys Shutdown	Battery sys Shutdown Duration	SNMP	UPS
MGE	UPS Load	Monitors UPS Load	SNMP	UPS
Microsoft	Bytes Received	Number of bytes the server has received from the network. This property indicates how busy the server is	WMI	Server

Microsoft	Bytes Total	Number of bytes the server has sent to and received from the network, an overall indication of how busy the server is	WMI	Server
Microsoft	Bytes Transmitted	Number of bytes the server has received from the network. This property indicates how busy the server is	WMI	Server
Microsoft	Cache Hit Ratio	Monitors the cache hit ratio	SNMP	Server
Microsoft	ContextSwitches	Rate of switches from one thread to another. Thread switches can occur either inside of a single process or across processes	WMI	Server
Microsoft	CPU Idle Time	Monitors the CPU Idle (MilliSecond) of HyperV Host using WMI	VIWMI	Server
Microsoft	CPU Ready	Monitors the CPU Ready (MilliSecond) of HyperV Guest using WMI	VIWMI	Server
Microsoft	CPU Usage MHz per core	Monitors the CPU Usage MHz per core of HyperV Guest using WMI	VIWMI	Server
Microsoft	CPU Used	Monitors the CPU Used (MilliSecond) of HyperV Guest using WMI	VIWMI	Server
Microsoft	CPU Used Time	Monitors the CPU Used (MilliSecond) of HyperV Host using WMI	VIWMI	Server
Microsoft	CPU Utilization	Monitors the Overall CPU Utilization of HyperV Host using WMI	VIWMI	Server
Microsoft	CPU Utilization	Monitors the CPU Utilization of HyperV Guest using WMI	VIWMI	Server
Microsoft	CPU Utilization	Monitors the CPU Utilization using WMI	WMI	Server / Desktop
Microsoft	CPU Utilization Per Core	Monitors the CPU Utilization per Core of HyperV Host using WMI	VIWMI	Server
Microsoft	CPU Wait	Monitors the CPU Wait (MilliSecond) of HyperV Guest using WMI	VIWMI	Server
Microsoft	Data Space of DB	Monitors the total data size in Database	SNMP	Server
Microsoft	Data Transaction LogSpace	Monitors the data transaction logspace	SNMP	Server
Microsoft	Delivered Outbound Messages	Monitors the delivered outbound messages	SNMP	Server
Microsoft	Disk I/O Usage	Monitors Disk I/O Usage of HyperV Host using WMI	VIWMI	Server
Microsoft	Disk Queue Length	Number of requests outstanding on the disk	WMI	Server
Microsoft	Disk Read Latency	Monitors Disk Read Latency of HyperV Host using WMI	VIWMI	Server

Microsoft	Disk Read Requests	Monitors Disk Read Requests of HyperV Host using WMI	VIWMI	Server
Microsoft	Disk Read Requests	Monitors Disk Read Requests of HyperV Guest using WMI	VIWMI	Server
Microsoft	Disk Read Speed	Monitors Disk Read Speed of HyperV Host using WMI	VIWMI	Server
Microsoft	Disk Read Speed	Monitors Disk Read Speed of HyperV Guest using WMI	VIWMI	Server
Microsoft	Disk Reads	Rate of read operations on the disk per Second	WMI	Server / Desktop
Microsoft	Disk Space Usage	Monitors Disk Space Usage Latency of HyperV Host using WMI	VIWMI	Server
Microsoft	Disk Utilization	Monitors the Disk Utilization using WMI	WMI	Server / Desktop
Microsoft	Disk Write Latency	Monitors Disk Write Latency of HyperV Host using WMI	VIWMI	Server
Microsoft	Disk Write Requests	Monitors Disk Write Requests of HyperV Host using WMI	VIWMI	Server
Microsoft	Disk Write Requests	Monitors Disk Write Requests of HyperV Guest using WMI	VIWMI	Server
Microsoft	Disk Write Speed	Monitors Disk Write Speed of HyperV Host using WMI	VIWMI	Server
Microsoft	Disk Write Speed	Monitors Disk Write Speed of HyperV Guest using WMI	VIWMI	Server
Microsoft	Disk Writes	Rate of write operations on the disk	WMI	Server / Desktop
Microsoft	File Read Bytes	Overall rate at which bytes are read to satisfy file system read requests to all devices on the computer, including read requests from the file system cache	WMI	Server / Desktop
Microsoft	File Read Operations	Combined rate of file system read requests to all devices on the computer, including requests to read from the file system cache	WMI	Server / Desktop
Microsoft	File Write Bytes	Overall rate at which bytes are written to satisfy file system write requests to all devices on the computer, including write requests to the file system cache	WMI	Server / Desktop
Microsoft	File Write Operations	Combined rate of the file system write requests to all devices on the computer, including requests to write to data in the file system cache	WMI	Server / Desktop
Microsoft	Free Disk Space in GB	Monitors the Free disk space in GB using WMI	WMI	Server / Desktop

Microsoft	Free Disk Space in MB	Monitors the Free disk space in MB using WMI	WMI	Server / Desktop
Microsoft	Free Physical Memory	Physical memory currently unused and available, in Mega Bytes	WMI	Server / Desktop
Microsoft	Idle Time	Percentage of time during the sample interval that the processor was idle. Not applicable for Windows XP and Windows 2000 devices.	WMI	Server / Desktop
Microsoft	Inbound Connection Rate	Monitors the inbound connection rate	SNMP	Server
Microsoft	IO Batch Writes	Monitors the IO batch writes	SNMP	Server
Microsoft	IO Outstanding Reads	Monitors the IO outstanding reads	SNMP	Server
Microsoft	IO Outstanding Writes	Monitors the IO outstanding writes	SNMP	Server
Microsoft	IO Page Reads	Monitors the IO page reads	SNMP	Server
Microsoft	Memory Active	Monitors Memory Active in KB of HyperV Host using WMI	VIWMI	Server
Microsoft	Memory Consumed	Monitors Memory Consumed in KB of HyperV Guest using WMI	VIWMI	Server
Microsoft	Memory Overhead	Monitors Memory OverHead in KB of HyperV Guest using WMI	VIWMI	Server
Microsoft	Memory Used	Monitors Memory Used in KB of HyperV Host using WMI	VIWMI	Server
Microsoft	Memory Utilization	Monitors Memory Usage of HyperV Host using WMI	VIWMI	Server
Microsoft	Memory Utilization	Monitors Memory Usage of HyperV Guest using WMI	VIWMI	Server
Microsoft	Memory Utilization	Monitors the Memory Utilization using WMI	WMI	Server / Desktop
Microsoft	Network Packets Received	Monitors Network Packets Received of HyperV Host using WMI	VIWMI	Server
Microsoft	Network Packets Received	Monitors Network Packets Received of HyperV Guest using WMI	VIWMI	Server
Microsoft	Network Packets Transmitted	Monitors Network Packets Transmitted of HyperV Host using WMI	VIWMI	Server
Microsoft	Network Packets Transmitted	Monitors Network Packets Transmitted of HyperV Guest using WMI	VIWMI	Server
Microsoft	Network Received Speed	Monitors Network Received Speed of HyperV Host using WMI	VIWMI	Server
Microsoft	Network Received Speed	Monitors Network Received Speed of HyperV Guest using WMI	VIWMI	Server
Microsoft	Network Transmitted Speed	Monitors Network Transmitted Speed of HyperV Host using WMI	VIWMI	Server
Microsoft	Network Transmitted Speed	Monitors Network Transmitted Speed of HyperV Guest using WMI	VIWMI	Server

Microsoft	Network Usage	Monitors Network Usage of HyperV Host using WMI	VIWMI	Server
Microsoft	Network Usage	Monitors Network Usage of HyperV Guest using WMI	VIWMI	Server
Microsoft	Non-delivery Reports (Total Inbound)	Monitors the total inbound non-delivery report	SNMP	Server
Microsoft	Non-delivery Reports (Total Outbound)	Monitors the total outbound non-delivery report	SNMP	Server
Microsoft	Outbound Connection Rate	Monitors the outbound connection rate	SNMP	Server
Microsoft	Page Faults	Overall rate at which faulted pages are handled by the processor	WMI	Server / Desktop
Microsoft	Page Reads	Number of times the disk was read to resolve hard page faults	WMI	Server / Desktop
Microsoft	Page Writes	Overall rate at which faulted pages are handled by the processor	WMI	Server / Desktop
Microsoft	Pages Per Second	Number of pages read from or written to the disk to resolve hard page faults	WMI	Server / Desktop
Microsoft	Partition Details of the Device(%)	Monitoring the usage in each partition of the Device using WMI.	WMI	Server / Desktop
Microsoft	Privileged Time	Percentage of non-idle processor time spent in privileged mode	WMI	Server / Desktop
Microsoft	Processor Queue Length	Number of threads in the processor queue	WMI	Server / Desktop
Microsoft	Processor Time	Percentage of time that the processor is executing a non-idle thread	WMI	Server / Desktop
Microsoft	Total Active Locks	Monitors the total active locks	SNMP	Server
Microsoft	Total Blocking Locks	Monitors the total blocking locks	SNMP	Server
Microsoft	Total IO Transactions	Monitors the total IO transactions	SNMP	Server
Microsoft	Total Messages Received (from internet)	Monitors the total messages received from internet	SNMP	Server
Microsoft	Total Msgs (awaiting final delivery)	Monitors the total awaiting messages for delivery	SNMP	Server
Microsoft	Total Msgs Queued for delivery (to internet)	Monitors the to total messages queued for delivery to internet	SNMP	Server
Microsoft	Total Open User Connections	Monitors the total open user connections	SNMP	Server
Microsoft	Total Size of DB	Monitors the total database size	SNMP	Server
Microsoft	Total Size of the Msgs (awaiting final delivery)	Monitors the total size of the awaiting messages for delivery	SNMP	Server
Microsoft	Unused Space of DB	Monitors the unused space in database	SNMP	Server
Microsoft	Used Disk Space in GB	Monitors the used disk space in GB using WMI	WMI	Server / Desktop

Microsoft	Used Disk Space in MB	Monitors the used disk space in MB using WMI	WMI	Server / Desktop
Microsoft	Used LogSpace	Monitors the used logspace	SNMP	Server
Microsoft	User Time	Percentage of non-idle processor time spent in user mode	WMI	Server / Desktop
NetApp, Inc.	Active Disk Count	Monitors the number of disks which are currently active, including parity disks.	SNMP	Storage
NetApp, Inc.	Active snapvault destinations.	Monitors the number of active snapvault destinations	SNMP	Storage
NetApp, Inc.	Active snapvault sources	Monitors the number of active snapvault sources.	SNMP	Storage
NetApp, Inc.	Aggregate Available	Monitors the aggregate available in bytes	SNMP	Storage
NetApp, Inc.	Aggregate State	Monitors the current state of the aggregates	SNMP	Storage
NetApp, Inc.	Aggregate Used	Monitors the aggregate used in bytes	SNMP	Storage
NetApp, Inc.	Aggregate Used Percentage	Monitors the aggregate used percentage	SNMP	Storage
NetApp, Inc.	Battery Status	Monitors the indication of the current status of the NVRAM batteries. { ok (1) , partiallyDischarged (2) , fullyDischarged (3) , notPresent (4) , nearEndOfLife (5) , atEndOfLife (6) , unknown (7) , overCharged (8) , fullyCharged (9) }	SNMP	Storage
NetApp, Inc.	Cache Age	Age in minutes of the oldest read-only blocks in the buffer cache.	SNMP	Storage
NetApp, Inc.	CPU Utilization	Monitors the percent of time that the CPU has been doing useful work since the last time a client requested the cpuBusyTimePerCent.	SNMP	Storage
NetApp, Inc.	Disk Read Bytes	Monitors the total number of bytes read from disk since the last boot.	SNMP	Storage
NetApp, Inc.	Disk State	Monitors the current state of the disks	SNMP	Storage
NetApp, Inc.	Disk Write Bytes	Monitors the total number of bytes written to disk since the last boot.	SNMP	Storage
NetApp, Inc.	Failed Disk count	Monitors the number of disks which are currently broken.	SNMP	Storage
NetApp, Inc.	Fan Status	Monitors the Count of the number of chassis fans which are not operating within the recommended RPM range.	SNMP	Storage
NetApp, Inc.	FCP Operations	Monitors the total number of FCP ops handled since the last boot	SNMP	Storage
NetApp, Inc.	FCP Read Bytes	Monitors the total number of bytes read via fcp since the last boot.	SNMP	Storage

NetApp, Inc.	FCP Write Bytes	Monitors the total number of bytes written via fcp since the last boot.	SNMP	Storage
NetApp, Inc.	Global Status	Monitors the overall status of the appliance.{ other (1) , unknown (2) , ok (3) , nonCritical (4) , critical (5) , nonRecoverable (6) }	SNMP	Storage
NetApp, Inc.	ISCSI Operations	Monitors the total number of iSCSI ops handled since the last boot	SNMP	Storage
NetApp, Inc.	ISCSI Read Bytes	Monitors the total number of bytes read via iscsi since the last boot.	SNMP	Storage
NetApp, Inc.	ISCSI Write Bytes	Monitors the total number of bytes written via iscsi since the last boot.	SNMP	Storage
NetApp, Inc.	LUN State	Monitors the current state of the lun's	SNMP	Storage
NetApp, Inc.	NetApp Temperature	Monitors the indication of whether the hardware is currently operating outside of its recommended temperature range. { no (1) , yes (2) }.	SNMP	Storage
NetApp, Inc.	Power Supply Status	Monitors Count of the number of power supplies which are in degraded mode. { no (1) , yes (2) }	SNMP	Storage
NetApp, Inc.	qrV Files Used	Monitors the current number of files used for this qrVEntry.	SNMP	Storage
NetApp, Inc.	qrVEntry Used bytes	Monitors the current number of KBytes used for this qrVEntry.	SNMP	Storage
NetApp, Inc.	Quota State Status	Monitors whether quotas are ON, OFF or initializing. quotaStateOff {(1) , quotaStateOn (2) , quotaStateInit (3) }	SNMP	Storage
NetApp, Inc.	Snapvault Status	Monitors the current transfer status of the snapvault relationship.	SNMP	Storage
NetApp, Inc.	Snapvault Total Primary Failures	Monitors the total number of failed snapvault transfers on the snapvault primary. Persistent across reboot.	SNMP	Storage
NetApp, Inc.	Snapvault Total Primary Successes	Monitors the total number of successful snapvault transfers from the snapvault primary. Persistent across reboot.	SNMP	Storage
NetApp, Inc.	Snapvault Total Secondary Failures	Monitors total number of failed snapvault transfers on the snapvault secondary. Persistent across reboot.	SNMP	Storage
NetApp, Inc.	Snapvault Total Secondary Successes	Monitors the total number of successful snapvault transfers from the snapvault secondary. Persistent across reboot.	SNMP	Storage
NetApp, Inc.	Total DiskCount	Monitors the total number of disks on the system.	SNMP	Storage
NetApp, Inc.	Volume Available	Monitors the volume available in bytes	SNMP	Storage

NetApp, Inc.	volume available bytes	monitors the total disk space in kbytes that is free for use on the referenced file system.	SNMP	Storage
NetApp, Inc.	Volume State	Monitors the current state of the volumes	SNMP	Storage
NetApp, Inc.	Volume Used	Monitors the volume used in bytes	SNMP	Storage
NetApp, Inc.	Volume Used Percentage	Monitors the volume used percentage	SNMP	Storage
NetScreen Technologies, Inc.	Active Session Count	Active Session Count Desc	SNMP	Firewall
NetScreen Technologies, Inc.	CPU Utilization	Monitors the CPU utilization	SNMP	Firewall
NetScreen Technologies, Inc.	Memory Utilization	Monitors the Memory Utilization	SNMP	Firewall
Novell	Cache maximum size	Cache maximum size in Kbytes, this is hard limit parameter	SNMP	Server
Novell	Contact failures	The number of failures since the last time an attempt to contact the peer eDirectory Server was successful	SNMP	Server
Novell	Cumulative failures	Cumulative failures in contacting the peer eDirectory Server since the creation of this entry	SNMP	Server
Novell	Cumulative successes	Cumulative successes in contacting the peer eDirectory Server since the creation of this entry	SNMP	Server
Novell	Database Size	Current size of the eDirectory Database	SNMP	Server
Novell	Dynamic Cache Memory	Dynamic Cache Adjust percentage	SNMP	Server
Novell	Entries in cache	Number of Entries in cache	SNMP	Server
Novell	Entry hits	Number of Entry hits	SNMP	Server
Novell	Entry misses	Number of Entries examined to determine misses	SNMP	Server
Novell	Fetched replication updates	Number of replication updates fetched or received from eDirectory Servers	SNMP	Server
Novell	Incoming traffic	Incoming traffic on the interface	SNMP	Server
Novell	Operations forwarded	Number of operations forwarded by this eDirectory Server to other eDirectory Servers	SNMP	Server
Novell	Outgoing traffic	Outgoing traffic on the interface	SNMP	Server
Novell	Received add Entry requests	Number of addEntry requests received	SNMP	Server
Novell	Received read requests	Number of read requests received	SNMP	Server

Novell	Rejected bind requests	Number of bind requests that have been rejected due to inappropriate authentication or invalid credentials	SNMP	Server
Novell	Sent replication updates	Number of replication updates sent to or taken by eDirectory Servers	SNMP	Server
Novell	Unauthenticated requests received	Number of unauthenticated/anonymous bind requests received	SNMP	Server
Nsfocus	CPU Utilization	Monitors the CPU of Nsfocus Firewall	SNMP	Firewall
Nsfocus	Memory Utilization	Monitors the Memory of Nsfocus Firewall	SNMP	Firewall
OpZoon	CPU Utilization	Monitors the CPU of OpZoon Switch	SNMP	Switch
OpZoon	CPU Utilization	Monitors the CPU of OpZoon PE-3810 Router	SNMP	Switch
OpZoon	CPU Utilization	Monitors the CPU of OpZoon Switch	SNMP	Switch
OpZoon	Memory Utilization	Monitors the Memory of OpZoon Switch	SNMP	Switch
OpZoon	Memory Utilization	Monitors the Memory of OpZoon PE-3810 Router	SNMP	Switch
OpZoon	Memory Utilization	Monitors the Memory of OpZoon Switch	SNMP	Switch
Oracle	DataFile DiskReads	Monitors the number of disk reads in data file	SNMP	Server
Oracle	DataFile DiskWrites	Monitors the number of disk writes in data file	SNMP	Server
Oracle	DataFileSize Allocated	Monitors the allocated data file size	SNMP	Server
Oracle	Library CacheGets	Monitors the number of request for Library CacheGets	SNMP	Server
Oracle	Library CacheInvalidations	Monitors the number of CacheInvalidations	SNMP	Server
Oracle	Library CacheReloads	Monitors the number of reloads	SNMP	Server
Oracle	Number of UserCommits	Monitors the number of commits	SNMP	Server
Oracle	OraDbSysUserRollbacks	Monitors the number of rollbacks	SNMP	Server
Oracle	TableScan Blocks	Monitors the number of blocks	SNMP	Server
Oracle	Tablespace Allocated	Monitors the total table space allocated	SNMP	Server
Oracle	Tablespace Largest Available	Monitors the largest available tablespace	SNMP	Server
Oracle	Tablespace Used	Monitors the total tablespace used	SNMP	Server
Radware	CPU Utilization	CPU Utilization for Radware	SNMP	Switch
Radware	Memory Utilization	Monitors the Memory of Radware AD-508 Switches	SNMP	Switch
Radware	Memory Utilization	Monitors the Memory of Radware DP-502 Switches	SNMP	Switch

Research In Motion	Average Response Time	Monitors the average response time (in milliseconds) for operations for users on this mail server in the last 10 minutes. Applies to BlackBerry Enterprise Server for Lotus Domino only.	SNMP	Server
Research In Motion	Failed Connections	Monitors the number of failed connection attempts to this mail server in the last 10 minutes. Applies to BlackBerry Enterprise Server for Lotus Domino only.	SNMP	Server
Research In Motion	MDS Connection Failure	Monitors the number of failed connections initiated by MDS to another address/service.	SNMP	Server
Research In Motion	MDS Connection Success	Monitors the number of successful connections initiated by MDS to another address/service.	SNMP	Server
Research In Motion	MDS Push Connections	Monitors the number of push server connections.	SNMP	Server
Research In Motion	Messages received per min	Monitors the total number of messages delivered to handhelds per min.	SNMP	Server
Research In Motion	Messages sent per min	Monitors the total number of messages sent from handhelds per min.	SNMP	Server
Research In Motion	Total License Configured	Monitors the total number of licenses installed on the server.	SNMP	Server
Research In Motion	Total License Used	Monitors the total number of licenses in use currently.	SNMP	Server
Research In Motion	Total messages pending	Monitors the total number of messages delivered to handhelds per min.	SNMP	Server
Research In Motion	Total messages received	Monitors the total number of messages delivered to handhelds.	SNMP	Server
Research In Motion	Total messages sent	Monitors the total number of messages sent from handhelds.	SNMP	Server
Research In Motion	Total Users	Monitors the number of users who are homed on this mail server. Applies to BlackBerry Enterprise Server for Lotus Domino only.	SNMP	Server
Riverbed Technology, Inc.	Active Connection(s)	Monitors the current number of active (optimized) connections.	SNMP	WAN Accelerator
Riverbed Technology, Inc.	BW aggregate in LAN	Monitors the total optimized bytes across all application ports, in the WAN to LAN direction since the last restart of service, as measured on the LAN side.	SNMP	WAN Accelerator

Riverbed Technology, Inc.	BW aggregate in WAN	Monitors the total optimized bytes across all application ports, in the WAN to LAN direction since the last restart of service, as measured on the WAN side.	SNMP	WAN Accelerator
Riverbed Technology, Inc.	BW aggregate out LAN	Monitors the total optimized bytes across all application ports, in the LAN to WAN direction since the last restart of service, as measured on the LAN side.	SNMP	WAN Accelerator
Riverbed Technology, Inc.	BW aggregate out WAN	Monitors the total optimized bytes across all application ports, in the LAN to WAN direction since the last restart of service, as measured on the WAN side.	SNMP	WAN Accelerator
Riverbed Technology, Inc.	BW Passthrough In	Monitors the Passthrough bytes in WAN to LAN direction.	SNMP	WAN Accelerator
Riverbed Technology, Inc.	BW Passthrough Out	Monitors the Passthrough bytes in LAN to WAN direction.	SNMP	WAN Accelerator
Riverbed Technology, Inc.	BW Passthrough total	Monitors the total passthrough bytes.	SNMP	WAN Accelerator
Riverbed Technology, Inc.	CPU Usage(5 mins avg)	Monitors the Five-minute CPU load in hundreths.	SNMP	WAN Accelerator
Riverbed Technology, Inc.	CPU Utilization	Monitors the percentage CPU utilization, aggregated across all CPUs, rolling average over the past minute.	SNMP	WAN Accelerator
Riverbed Technology, Inc.	dsCostPerSegment	Monitors the Cost per segment expressed in microseconds.	SNMP	WAN Accelerator
Riverbed Technology, Inc.	dsHits Total	Monitors the total number of datastore hits since last restart of service.	SNMP	WAN Accelerator
Riverbed Technology, Inc.	dsMiss Total	Monitors the total number of datastore misses since last restart of service.	SNMP	WAN Accelerator
Riverbed Technology, Inc.	Established Connection(s)	Monitors the current number of established (optimized) connections.	SNMP	WAN Accelerator
Riverbed Technology, Inc.	Half Closed Connection(s)	Monitors the Current total number of half-closed (optimized) connections.	SNMP	WAN Accelerator
Riverbed Technology, Inc.	Half Opened Connection(s)	Monitors the current total number of half-opened (optimized) connections.	SNMP	WAN Accelerator

Riverbed Technology, Inc.	Optimization Service Status	Monitors the Current status of the optimization service.	SNMP	WAN Accelerator
Riverbed Technology, Inc.	Optimized Connection(s)	Monitors the current total number of optimized connections.	SNMP	WAN Accelerator
Riverbed Technology, Inc.	Pass-Through Connection(s)	Monitors the current total number of pass-through connections.	SNMP	WAN Accelerator
Riverbed Technology, Inc.	Steelhead Temperature	Monitors the temperature of the system(C).	SNMP	WAN Accelerator
Riverbed Technology, Inc.	System Health Status	Monitors the current health of the system. The value is one amongst Healthy, Admission Control, Degraded, Critical.	SNMP	WAN Accelerator
Riverbed Technology, Inc.	Total Connection(s)	Monitors the total number of connections.	SNMP	WAN Accelerator
RuiJie	CPU Utilization	CPU Utilization for RuiJie	SNMP	Switch
RuiJie	Memory Utilization	Memory Utilization for RuiJie	SNMP	Switch
SecGate	CPU Utilization	Monitors the CPU of SecGate Firewall	SNMP	Firewall
SecGate	Memory Utilization	Monitors the Memory of SecGate Firewall	SNMP	Firewall
SOCOMEC UPS	Battery Capacity	Estimate of the battery charge remaining expressed as a percent of full charge.	SNMP	UPS
SOCOMEC UPS	Battery Capacity	Estimate of the battery charge remaining expressed in percent	SNMP	UPS
SOCOMEC UPS	Battery Capacity	Estimate of the battery charge remaining expressed in percent	SNMP	UPS
SOCOMEC UPS	Battery Capacity	Estimate of the battery charge remaining expressed in percent	SNMP	UPS
SOCOMEC UPS	Battery Negative Voltage	Battery negative voltage in volts	SNMP	UPS
SOCOMEC UPS	Battery Positive Voltage	Battery positive voltage in volts	SNMP	UPS
SOCOMEC UPS	Battery Voltage	Battery Voltage in volts.	SNMP	UPS
SOCOMEC UPS	Battery Voltage	Battery Voltage in volts	SNMP	UPS
SOCOMEC UPS	Battery Voltage	Battery Voltage in volts	SNMP	UPS
SOCOMEC UPS	Output Load Phase 1	Monitor UPS Output Load Phase 1 expressed in percent	SNMP	UPS

SOCOMEC UPS	Output Load Phase 2	Monitor UPS Output Load Phase 2 expressed in percent	SNMP	UPS
SOCOMEC UPS	Output Load Phase 3	Monitor UPS Output Load Phase 3 expressed in percent	SNMP	UPS
SOCOMEC UPS	Output Load Rate Phase 1	Monitor UPS Output Load Phase 1 expressed in percent	SNMP	UPS
SOCOMEC UPS	Output Load Rate Phase 1	Monitor UPS Output Load Phase 1 expressed in percent	SNMP	UPS
SOCOMEC UPS	Output Load Rate Phase 2	Monitor UPS Output Load Phase 2 expressed in percent	SNMP	UPS
SOCOMEC UPS	Output Load Rate Phase 3	Monitor UPS Output Load Phase 3 expressed in percent	SNMP	UPS
SOCOMEC UPS	UPS Output Load Rate	UPS Output Load Rate in %.	SNMP	UPS
Symbol	UPS Battery current	Custom Monitor	SNMP	UPS
Tainet	CPU Utilization	Monitors the CPU of Tainet_Venus_2816 Switch	SNMP	Switch
Tainet	Memory Utilization	Monitors the Memory of Tainet_Venus_2816 Switch	SNMP	Switch
Topsec	CPU Utilization	Monitors the CPU of TopSec Firewall	SNMP	Firewall
Topsec	Memory Utilization	Monitors the Memory of TopSec Firewall	SNMP	Firewall
Topsec	VPN-Connections	Monitors the VPN-Connections of TopSec Firewall	SNMP	Firewall
Trango	SU Count	SU Count	SNMP	Wireless
TrippLite	UPS Charge	Monitors UPS Charge	SNMP	UPS
TrippLite	UPS Load	Monitors UPS Load	SNMP	UPS
VENUS	Connections	Monitors the Connections of VENUS-VSOS-V2.6 Firewall	SNMP	Firewall
VENUS	Connections	Monitors the Connections of VENUS_FW Firewall	SNMP	Firewall
VENUS	CPU Utilization	Monitors the CPU of VENUS-VSOS-V2.6 Firewall	SNMP	Firewall
VENUS	CPU Utilization	Monitors the CPU of VENUS_FW Firewall	SNMP	Firewall
VENUS	Memory Utilization	Monitors the Memory of VENUS-VSOS-V2.6 Firewall	SNMP	Firewall
VENUS	Memory Utilization	Monitors the Memory of VENUS_FW Firewall	SNMP	Firewall
Vmware	Active Memory	Amount of guest physical memory actively used.	VIWebService	Server
Vmware	Balloon Memory	Amount of guest physical memory that is currently reclaimed from the VM through ballooning.	VIWebService	Server

Vmware	Compressed Memory	Amount of memory compressed by ESX for VM	VIWebService	Server
Vmware	Consumed Memory	Amount of memory consumed by a virtual machine,	VIWebService	Server
Vmware	CPU Idle Time	Total time that the CPU spent in an idle state	VIWebService	Server
Vmware	CPU Ready	Time that the virtual machine was ready, but could not get scheduled to run on the physical CPU	VIWebService	Server
Vmware	CPU Usage	Sum of the actively used CPU of all powered on virtual machines on a host.	VIWebService	Server
Vmware	CPU Used	Total CPU usage By HostSystem	VIWebService	Server
Vmware	CPU Used	Time accounted to the virtual machine	VIWebService	Server
Vmware	CPU Utilization	Actively used CPU of the host, as a percentage of the total available CPU	VIWebService	Server
Vmware	CPU Utilization	Actively used VCPU, as percentage of total available CPU. This is the host view of the CPU usage	VIWebService	Server
Vmware	CPU Wait	CPU time spent in wait state	VIWebService	Server
Vmware	Datastore Free Space	VMware Datastore Freespace Monitor	VIWebService	Server
Vmware	Datastore Read IOPs	Average number of read commands issued per second to the datastore during the collection interval.	VIWebService	Server
Vmware	Datastore Read Latency	Average amount of time for a read operation from the datastore	VIWebService	Server
Vmware	Datastore Read Latency	Average amount of time for a read operation from the datastore	VIWebService	Server
Vmware	Datastore Read Rate	Rate of reading data from the datastore	VIWebService	Server
Vmware	Datastore Read Requests	Average number of read commands issued per second to the datastore during the collection interval.	VIWebService	Server
Vmware	Datastore Read Requests Rate	Average number of read commands issued per second to the datastore	VIWebService	Server
Vmware	Datastore Read Speed	Rate of reading data from the datastore.	VIWebService	Server
Vmware	Datastore Throughput Usage	The current bandwidth usage for the datastore or LUN.	VIWebService	Server
Vmware	Datastore Write IOPs	Average number of write commands issued per second to the datastore during the collection interval	VIWebService	Server
Vmware	Datastore Write Latency	Average amount of time for a write operation to the datastore	VIWebService	Server
Vmware	Datastore Write Latency	Average amount of time for a write operation to the datastore	VIWebService	Server

Vmware	Datastore Write Rate	Rate of reading data to the datastore	VIWebService	Server
Vmware	Datastore Write Requests	Average number of write commands issued per second to the datastore during the collection interval.	VIWebService	Server
Vmware	Datastore Write Requests Rate	Average number of write commands issued per second to the datastore	VIWebService	Server
Vmware	Datastore Write Speed	Rate of reading data to the datastore.	VIWebService	Server
Vmware	Disk Bus Resets	Number of SCSI-bus reset commands issued during the collection interval.	VIWebService	Server
Vmware	Disk I/O Usage	Aggregated diskI/O rate for HostSystem over VMs	VIWebService	Server
Vmware	Disk I/O Usage	Aggregated disk I/O rate	VIWebService	Server
Vmware	Disk Max Total Latency	Highest latency value across all disks used by the host.	VIWebService	Server
Vmware	Disk Read Rate	Rate at which data is read from each disk on the vm	VIWebService	Server
Vmware	Disk Read Requests	Number of times data was read from each disk on the vm	VIWebService	Server
Vmware	Disk Read Speed	Rate at which data is Read from each LUN on the host	VIWebService	Server
Vmware	Disk Reads	Number of times data was read from each LUN on the host.	VIWebService	Server
Vmware	Disk Write Rate	Rate at which data is written to each disk on the vm	VIWebService	Server
Vmware	Disk Write Requests	Number of times data written to each disk on the vm	VIWebService	Server
Vmware	Disk Write Speed	Rate at which data is written to each LUN on the host	VIWebService	Server
Vmware	Disk Writes	Number of times data written to each LUN on the host	VIWebService	Server
Vmware	Dropped Received Packets	Number of received packets dropped during the collection interval.	VIWebService	Server
Vmware	Dropped Transmitted Packets	Number of transmitted packets dropped during the collection interval.	VIWebService	Server
Vmware	Memory Active	Sum of all active metrics for all powered-on virtual machines plus vSphere services	VIWebService	Server
Vmware	Memory Compression Rate	Rate of memory compression for the VM	VIWebService	Server
Vmware	Memory Consumed	Amount of machine memory used on the host	VIWebService	Server
Vmware	Memory Decompression Rate	Rate of memory decompression for the virtual machine	VIWebService	Server

Vmware	Memory Granted	Amount of Granted to Entities by HostSystem	VIWebService	Server
Vmware	Memory Overhead	Total of all overhead metrics for powered-on virtual machines, the overhead of running vSphere services on the host.	VIWebService	Server
Vmware	Memory SwapIn Rate	Rate at which memory is swapped from disk into active memory	VIWebService	Server
Vmware	Memory SwapOut Rate	Rate at which memory is being swapped from active memory to disk	VIWebService	Server
Vmware	Memory Usage	Percentage of available machine memory Used	VIWebService	Server
Vmware	Memory Usage	Amount of machine memory used by the VMkernel to run the VM	VIWebService	Server
Vmware	Network Packets Received	The number of packets received by each vNIC on the VM	VIWebService	Server
Vmware	Network Packets Transmitted	Number of packets transmitted by each vNIC on the virtual machine	VIWebService	Server
Vmware	Network Received Packets	Number of packets Received during the collection interval.	VIWebService	Server
Vmware	Network Received Rate	The rate at which data is received across each physical NIC instance on the host.	VIWebService	Server
Vmware	Network Received Rate	The rate at which data is received across the VMs vNIC	VIWebService	Server
Vmware	Network Transmitted Packets	Number of packets Transmitted during the collection interval.	VIWebService	Server
Vmware	Network Transmitted Rate	The rate at which data is transmitted across each physical NIC instance on the host.	VIWebService	Server
Vmware	Network Transmitted Rate	The rate at which data is transmitted across the VMs vNIC	VIWebService	Server
Vmware	Network Usage	Sum of data transmitted and received across all physical NIC instances connected to the host.	VIWebService	Server
Vmware	Network Usage	Sum of data transmitted and received across all vNIC instances connected to the VM	VIWebService	Server
Vmware	Overhead Memory	Amount of machine memory used by the VMkernel to run the VM	VIWebService	Server
Vmware	Shared Memory	Sum of all shared metrics for all powered-on virtual machines, plus amount for vSphere services on the host.	VIWebService	Server

Vmware	Shared Memory	Amount of guest physical memory shared with other VMs	VIWebService	Server
Vmware	Swapped Memory	Current amount of guest physical memory swappedout to the VMs swap file by the VMkernel.	VIWebService	Server
Vmware	Swapped Used Memory	Amount of memory that is used by swap. Sum of memory swapped of all powered on VMs and vSphere services on the host.	VIWebService	Server
Vmware	Total Disk Latency	Average amount of time taken to process a SCSI command issued from/by the Guest OS to the VM	VIWebService	Server
Vmware	Total Disk Read Latency	Average amount of time takento process a SCSI read command issued from GuestOS to the VM	VIWebService	Server
Vmware	Total Disk Write Latency	Average amount of time taken to process a SCSI read command issued by GuestOS to the VM	VIWebService	Server
YAMAHA	NVR500_CPU Utilization (1 Min)	Custom Monitor	SNMP	Switch
YAMAHA	NVR500_CPU Utilization (5 Min)	Custom Monitor	SNMP	Switch
YAMAHA	NVR500_CPU Utilization (5 Sec)	Custom Monitor	SNMP	Switch
YAMAHA	NVR500_Memory Utilization	Custom Monitor	SNMP	Switch
YAMAHA	RTX1200_CPU Utlization (1 Min)	Custom Monitor	SNMP	Router
YAMAHA	RTX1200_CPU Utlization (5 Min)	Custom Monitor	SNMP	Router
YAMAHA	RTX1200_CPU Utlization (5 Sec)	Custom Monitor	SNMP	Router
YAMAHA	RTX1200_Inbox Temperature	Custom Monitor	SNMP	Router
YAMAHA	RTX1200_Memory Utlization	Custom Monitor	SNMP	Router
YAMAHA	RTX810_CPU Utilization (1 Min)	Custom Monitor	SNMP	Router
YAMAHA	RTX810_CPU Utilization (5 Min)	Custom Monitor	SNMP	Router
YAMAHA	RTX810_CPU Utilization (5 Sec)	Custom Monitor	SNMP	Router
YAMAHA	RTX810_Memory Utlization	Custom Monitor	SNMP	Router
ZhongXing	CPU Utilization	CPU Utilization for ZhongXing	SNMP	Switch
ZhongXing	CPU Utilization	CPU Utilization for ZhongXing	SNMP	Switch
ZhongXing	CPU Utilization	CPU Utilization for ZhongXing	SNMP	Switch
ZhongXing	CPU Utilization	CPU Utilization for ZhongXing	SNMP	Switch
ZhongXing	Memory Utilization	Memory Utilization for ZhongXing	SNMP	Switch
ZhongXing	Memory Utilization	Memory Utilization for ZhongXing	SNMP	Switch
ZhongXing	Memory Utilization	Memory Utilization for ZhongXing	SNMP	Switch
ZhongXing	Memory Utilization	Memory Utilization for ZhongXing	SNMP	Switch
ZTE	CPU Utilization	Monitors the CPU of ZTE-2850-26TM Switch	SNMP	Switch

ZTE	CPU Utilization	CPU Utilization for ZTE	SNMP	Switch
ZTE	CPU Utilization	Monitors the CPU of ZTE-ZXPON-EPON-ONU Switch	SNMP	Switch
ZTE	CPU Utilization	Monitors the CPU of ZTE-ZXR10-2826E Switch	SNMP	Switch
ZTE	CPU Utilization	Monitors the CPU of ZTE-ZXR10-2826S-LE Switch	SNMP	Switch
ZTE	Memory Utilization	Monitors the Memory of ZTE-2850-26TM Switch	SNMP	Switch
ZTE	Memory Utilization	Monitors the Memory of ZTE-ZXPON-C220 Switch	SNMP	Switch
ZTE	Memory Utilization	Monitors the Memory of ZTE-ZXR10-2826E Switch	SNMP	Switch
ZTE	Memory Utilization	Monitors the Memory of ZTE-ZXR10-2826S-LE Switch	SNMP	Switch
ZTE	Memory Utilization	Memory Utilization for ZTE	SNMP	Switch

Adding WMI-based Custom Monitors

In addition to OpManager's default monitors, you can also create your own monitors for the WMI-enabled devices in your network.

1. Go to Device Snapshot page on which you wish to add a custom WMI monitor.
2. Click **Monitors ? Performance Monitors ? Actions ? Add monitor.**
3. Select the required WMI class, and OpManager will list the performance counters available under that class.
4. Along with the counter, you can also select the instance of the counter that you wish to monitor.
5. Once you've selected the counters and the instances, click **Add** to add the monitor to the device.

Device-specific Monitors

The monitoring configuration may need alteration for specific devices. Doing a bulk-configuration using the device templates, applies the same set of configurations for the devices of the same type. In order to change the configuration for specific devices, here are the steps:

1. Go to the device snapshot page.
2. Click on **Monitors** > **Performance Monitors**
3. Click the **Edit** icon against the monitor name. The Edit Monitor page is displayed.
4. Change the values for the required parameters and and click **Save**.

The changes to the monitor are effected only for that device.

Configuring thresholds for performance monitors

Configuring thresholds enable OpManager to proactively monitor the resources and the services running on the servers and network devices, and raise alerts before they go down or reach the critical condition. OpManager offers multiple threshold levels namely:

- Attention threshold - low severity
- Trouble threshold - medium severity
- Critical threshold - high severity
- Rearm - to rearm the alert after it has been triggered

You can configure multiple thresholds for the monitors that are associated to a single device, and even configure them from a device template in order to apply across multiple devices.

Configure threshold limits for performance monitors in an individual device

1. Go to the device snapshot page.
2. Click **Monitors** ? **Performance Monitors** ? click on the edit icon corresponding to the monitor for which you want to configure threshold limits. **Edit Monitor** page opens.
3. Ensure that the monitoring **Interval** is configured.
4. Specify the unit for the monitored resource in terms of percentage, MB, KB etc (based on how the parameter is measured).
5. Select the condition [>,=, <, or !=] for Warning Threshold, Trouble Threshold & Error Threshold, and enter the value. Alert is raised if the monitored value is greater than, equal to, not equal to, or lesser than (which ever is selected) the threshold value.

   Also, for = operator, you can provide multiple values using pipe '|' as the separator. Note that this is applicable only for thresholds configured from **Device Snapshot ? Monitors.**
6. Enter the **Rearm Value**. Rearm is the value that determines when the monitor is reverted back to 'Normal' status.

   > **Example:** The Warning threshold condition for a memory monitor is selected as greater than [>] and the threshold value is configured as 75. If the value of the monitor oscillates between 72, 80 and 73 for three successive polls, an alert is not raised for the poll with value '80' but the admin might still wish to receive an alert for it.
   >
   > To avoid this, you can set the Rearm value at a considerably wide interval (say 70 in this situation) to make sure the status returns to 'Normal' only when the value goes below this threshold.

   Note that if you set the thresholds' conditions using **'>'** criteria, then the rearm value can only be set using **'<='** and vice versa.
7. In the **Consecutive Times** field enter the value of how many consecutive times the thresholds (Attention, Trouble and Critical) can be violated to generate the alert.
8. Click on **Save.**

Configure threshold limits for multiple devices of same type using Device Template

1. Go to **Settings** ? **Configuration** ? **Device Templates** and select the template in which you want to configure the threshold.
2. Under **Monitors** column, all the monitors that are currently associated with the devices are listed. If you want add or remove required monitors. Click on **Edit Thresholds** button. Edit Thresholds page opens.
3. Configure the Attention, Trouble, Critical Threshold and the Rearm Value and click on **OK**
4. Click on **OK.**

Configure from the Performance Monitors page:

1. Go to **Settings ? Performance monitors** and click the **'Edit'** icon next to the monitor of your choice.

2. Change the threshold values as required and click **'Save'.**
3. Once it's done, click the **'Associate'** button next to the monitor to associate it to the necessary devices.

Monitoring TCP Services

OpManager provides out-of-the-box support for the following services: Web, HTTPS, FTP, IMAP, LDAP, Telnet , MySQL, MS-Exchange, SMTP, POP3, WebLogic, Finger, Echo, DNS, and NTTP. By default, during discovery, OpManager scans the devices for the services: DNS, MSSQL, MySQL, Oracle, SMTP, Web. You can also select other services in the list. When they are found running on their default ports, OpManager starts monitoring the services.

Scanning Services 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:

- Go to **Settings** > **Monitoring** > **Service Monitors** > Select the service and check "**Scan during discovery**"

OpManager allows you to change the settings for monitoring these services as per your network needs. You can configure new services that are not available in the list. OpManager can manage services running on standard TCP ports.

Note:

- The list contains the service names and the corresponding port numbers. To edit the settings of any of the available services, click on the service name.
- If you do not find the service you want to manage in the list, you can add the service by clicking **Add Service. (**Adding a New Service**)**.

Viewing Service Status and Response Time

Go to the **Device Snapshot** page > **Monitors** > **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.

Configuring Alerts

By default OpManager raises an alarm if a service is down. If required you can configure OpManager to raise an alarm if the service is unavailable for an N number of times consecutively.

- Go to the **Device Snapshot** page > **Monitors** > **Service Monitors** > Click the edit icon against the service on which you wish to cofigure the threshold or to modify the consecutive time.

Note: Threshold alert will be raised based on the response time of the service.

Monitoring TCP Services on a Device

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

1. Go to **Inventory** > Click on the Device for which you wish to add a service.
2. Click **Monitors** > **Service Monitors** > **Add Monitor** at the top of the page
3. Select the services to be discovered from the list and click **Add Monitor**.
4. If you wish to associate the monitor to existing devices, click on **Save & Associate**. This option will prompt you to select the required devices to which the monitor must be associated
   Select the required devices and click on Save.
5. If you wish to only add the monitor (and not associate it to any of the existing devices), click on **Save**.

You can also associate existing service monitors to devices.

1. Go to **Inventory** > Click on the Device for which you wish to associate a service monitor.
2. Click **Monitors** > **Service Monitors** > **Associate Monitor** at the top of the page
3. Select the services to be discovered from the list and click **Associate**.

Adding New TCP Service Monitors

You can add new TCP services for monitoring.

1. Go to **Settings** > **Monitoring** > **Service Monitors >** Click **Add.**
2. Specify the name of the TCP service that you want to monitor.
3. Specify the TCP Port number that has to be checked for service availability
4. Specify the timeout interval in seconds for the port-check request.
5. Specify the consecutive time to generate an alarm if the service unavailable for N number of times
6. Select an option for **Scan during Discovery**. This will scan network devices for the monitored service during the discovery process and will automatically associate the monitor to the device if the specified service is available.
7. If you wish to associate the monitor to existing devices, click on **Save & Associate**. This option will prompt you to select the required devices to which the monitor must be associated
   Select the required devices and click on Save.
8. If you wish to only add the monitor (and not associate it to any of the existing devices), click on **Save**.

Associating the Service to Devices

1. Go to **Settings > Monitoring > Service Monitors > Associate**
2. Select the required TCP service from the **Service Monitors** drop-down.
3. Select the devices on which you want to monitor the service from the column on the left and move them to the right.
4. Click **Associate.**

Dissociate Devices

1. Go to **Settings > Monitoring > Service Monitors > Associate** option.
2. Select the monitor from the **Service Monitors** drop-down menu.
3. Select the devices on which you do not want to monitor the service from the column on the right and move them to the left.
4. Click **Associate**.

You can also associate/dissociate service monitors to devices from the **Quick Configuration Wizard**. Go to **Settings > Configuration > Quick Configuration Wizard > Service Monitors** and associate/dissociate services to devices as mentioned above.

Monitoring Windows Services

Certain applications in Windows machine run in the background as services. OpManager discovers and monitors the status of such services using WMI monitoring. OpManager generates alarms whenever they fail.


Monitoring Windows Services

Prerequisites

To monitor Windows services, OpManager should be installed in a Windows machine. 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. So, make sure you configure a WMI credential so that you can apply this to the windows devices.

Add Windows Services to a Device

To monitor a Windows service with OpManager's Windows service monitoring feature, follow the steps given below:

1. Go to the **Inventory** and click on the device to which you want to add a Windows Service monitor.
2. Confirm if the correct WMI credential is associated to the device. Else, configure the credential details in the device.
3. Click **Monitors ? Windows Service Monitors**. This option will be available only for devices being monitored using WMI.
4. Click **Actions** on the top-right corner and the click **'Add Monitor'**.
5. Select the necessary Windows services and click on 'Add' to add those monitors to the device.

Note: The polling interval cannot be set at single monitor level. This value is same as the polling interval of the device.

Associate Windows Service Monitors to several devices

1. Go to **Settings ? Monitoring ? Windows Services.**
2. Click **Associate** next to the monitor you wish to associate to your devices.
3. In the following window, select all the devices you want to add the monitor to, move them to the 'Selected Devices' column on the right and click **'Save'.**
4. You can also do the same action from **Settings ? Configuration ? Quick Configuration Wizard ? Service Monitors** and selecting the 'Associate a Windows Service' icon.

Configuring Alerts

By default OpManager raises an alarm if a Windows service is down. If required you can configure OpManager to raise an alarm if the service unavailable for a N number of times consecutively.

1. Go to the device snapshot page.
2. **Monitors ? Windows Service Monitors,** click on the Edit icon corresponding to the Windows service for which you want to configure the alert.
3. Modify the count entered for '**Generate alarm if unavailable for _ consecutive times**'. For example if you enter the value as 2, OpManager will raise alarm only if the service is unavailable for 2 consecutive polls.
4. You also have to option to either **restart the service** (automatically restart a service when the service is down) or **restart the server** (automatically restart the server when a service is down). Select the check box and the appropriate radio button.
5. Click **Save**.

Adding New Windows Service Monitors

In addition to the Windows service monitoring performance monitors supported by OpManager out-of-the-box, you can add monitors for other windows services too.

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

Adding Windows Service Monitors

1. Go to **Settings** > **Monitoring ? Windows Services**.
2. Click **Add** and select the device from the drop-down.
3. Type the domain administrator user name and password for the device (not required for the localhost) in the respective fields and click **Next**.
4. A list of all the Windows Services available on that machine is displayed. From this select the services that you want be monitored on the device.
5. Configure the consecutive time for alert.
6. Based on whether you want to **restart the service** (automatically restart a service when the service is down) or **restart the server** (automatically restart the server when a service is down), select the corresponding option.
7. Click **Save & Asssociate**. You can choose the devices to which you want to associate this new Windows Service monitor.
8. Select the devices and click **'Save'.** If you just wish to save the monitor and not associate it to any devices for now, you can just leave the devices unselected and click 'Save'.

Associating Windows Services to Devices

1. Go to **Settings ? Monitoring ? Windows Services ? Associate** option.
2. Select the monitor from the **Windows Service Monitors** drop-down menu.
3. Select the devices to which you would like to associate this monitor and click on the right arrow to move these devices into the **Devices on which the service is monitored** column.
4. To **dissociate devices**, select the devices in which you would not like to monitor the services and click on the left arrow. This will move these devices to the **Devices on which the service is not monitored**column.
5. Click **Associate**.

Dissociate Devices

1. Go to **Settings ? Monitoring ? Windows Services ? Associate** option.
2. Select the monitor from the **Windows Service Monitors** drop-down menu.
3. Select the devices in which you would not like to monitor the services from the right-pane and click on the left arrow. This will move these devices to the **Devices on which the service is not monitored** column.
4. Click **Associate**.

You can also associate/dissociate service monitors to devices from the **Quick Configuration Wizard**. Go to **Settings ? Configuration ? Quick Configuration Wizard ? Service Monitors** and associate/dissociate services to devices as mentioned above.

Monitoring Processes on Windows/Unix Servers & Desktops

OpManager provides out-of-the-box support for monitoring the availability of all the processes running on a Windows or Unix system. Windows systems use WMI and Unix systems use CLI to monitor the processes that are running on a system. We also support SNMP in the Server/ Desktop and Domain Controller categories.

Here are the steps for configuring a Process Monitor:

1. Go to the device snapshot page.
2. Ensure that you have associated the SNMP/WMI/CLI Credentials to the device.
3. Click **Monitors ? Process Monitors**.
4. Click **Add Monitor,** select the required Process Monitors and click **Add** at the bottom of the page to get these monitors associated to the device.

Note: The polling interval cannot be set at single monitor level. This value is same as the polling interval of the device.

Configure Thresholds for Process Monitors

You can set resource thresholds for the Process Monitor. Once a resource (CPU/memory) utilization by a process exceeds the configured threshold, an alert is triggered.

1. Click the Edit icon against the process name.
2. Configure the threshold values for CPU and Memory resources.
3. Configure the number of times you would like to allow threshold violation before being notified. For instance, if you configure the value as 3, OpManager will notify you if the resource threshold is violated 3 consecutive times.
4. Configure the number of the process instances, exceeding which you would like to be notified. For instance, if you would like to be notified if the number of Apache.exe instances on the monitored device exceeds 3, configure the value here as 3 and save the changes.

Alerts are fired based on the above settings.

You can also view active processes on a device and process diagnostics against a system resource. We currently support active processes for SNMP/WMI/CLI protocols.

Viewing Active Processes

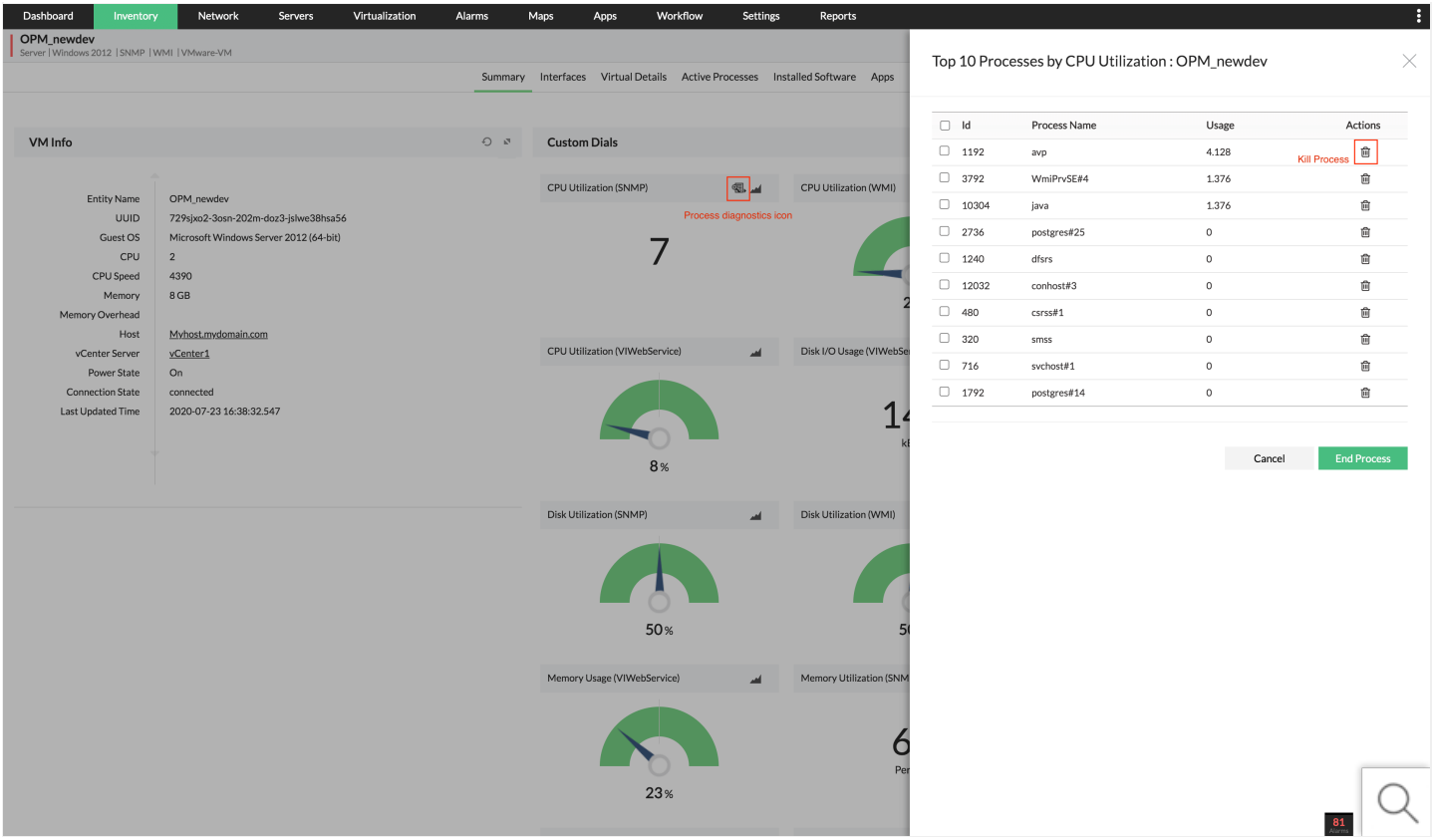
OpManager provides you the information on the processes that are currently running on the managed device. For this, OpManager uses the protocol of the default credential of that device (SNMP / WMI / CLI).

To view the details, navigate to the Snapshot page of the device from the Inventory, and you can view all the processes that are currently running on the device from the **Active Processes** tab.

Note:

- When multiple types of credential profiles are associated, OpManager follows this priority to fetch the active processes: **WMI > CLI > SNMP**
- **Example 1:** If a device has both SNMP and WMI credentials associated to it, OpManager will first try to fetch the active processes via WMI. If that fails, then the processes will be fetched via SNMP.
- **Example 2:** If a device has bot SNMP and CLI credentials associated, OpManager will first try to fetch the processes via CLI and then via SNMP.

Also, if you have enabled Custom Dials for your devices, you can view the top 10 processes of a device by clicking on the **Process Diagnostics** icon on the top-right corner of the dial. From there, you can choose to end processes that are consuming a lot of resources by simply clicking on the **Kill Process (bin)** icon. (Top 10 processes available only for CPU utilization and memory utilization dials)



Adding New Process Template

Process templates helps you to select the processes that are running on a device, convert each of them into individual templates and apply all of them across multiple devices. To add a new process template,

1. Go to **Settings ? Monitoring ? Processes** and click **'Add'.**
2. **Device Name**: Select the device which runs the process(es) that needs to be converted into template(s).
3. **Protocol**: Select the relevant protocol to access the device.
4. Select the relevent credential from the drop-down by clicking on the **Credential** radio button or Click **Associated username password** to associate the accociated credential.
5. Click **Next**. All the processes that are currently running on the device are listed along with their ID, Path and Arguments.
6. Select the required process(es).
7. Click **Save** button at the bottom of the page.

The selected processes are now added and available as templates under Settings ? Monitors ? Processes.

Associating Process Template to Multiple Devices

To associate a process template across multiple devices, follow the steps given below:

1. Go to **Settings ? Monitoring ? Processes**
2. Click **Associate**.
3. Select the process template to be associated to multiple devices
4. From the listed devices, select and move the required devices to box seen on the right.
5. Click **Associate**

The selected process template is applied across multiple devices.

Associating Script Monitoring Templates

Script Monitoring templates help you create custom scripts to monitor custom parameters .

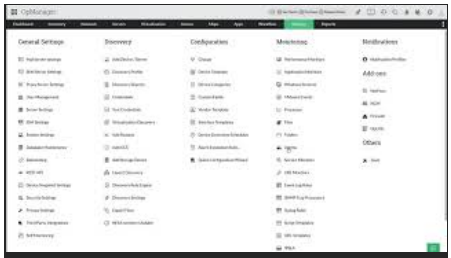
Follow the steps given below to add script templates

1. Go to **Settings ? Monitoring ? Script Templates.**
2. Click **Associate**
3. This will open a page to associate multiple devices to a specific template.
4. Select the required script from the drop-down.
5. Select the devices from left-side box and move it to the right box
6. Click **Associate**

You have successfully associated script template to multiple devices.

Log File Monitoring

Every application prints status messages, error messages, and other critical information in its log. It is very tedious to skim through all these bulky log files to understand application performance. To manage such mission critical applications in real time, monitoring their log files is necessary. OpManager offers agent-based log file monitoring for real-time fault and performance management.



Log File Monitoring

How does log file monitoring work?

The log file monitoring agent installed in the end machine, monitors the log files continuously for the required string (It may even be a regex). Once that string is printed, it immediately notifies the OpManager server, which in-turn raises an alarm based on the polling interval specified for that file monitor.

Steps to add a log file monitor

Prerequisites:

- Ensure that device in which you are about to install the agent **has already been added in OpManager.**
- Download and install the log file monitoring agent in the device(s). You can do it in two ways:
  - **From the OpManager UI:** You can go to **Settings ? Monitoring ? Agents** and click on 'Download agent' to download the file monitoring agent.
  - In case of multiple devices, you can remotely push the downloaded agent through your AD service, and OpManager agent will get automatically installed on all selected devices.

1. Go to **Settings ? Monitoring ? Files ? Add a New Template**.
2. Enter a template name, and a path to the file.
3. Set the polling interval, so that the alarms can be raised.
4. Under File Contains row, enter the string to be searched. OpManager supports regular expressions as well. **Note:** All the special characters should be preceded by a backslash.
5. Select 'Match Case' check box, if you want the search to be case-sensitive.
6. Enter the number of consecutive times of the log print for which you want to raise the alarm.
7. Save the template and associate it to a device.
8. Now map the agent to the device that you have added in OpManager (prerequisite).
   1. Go to **Settings ? Monitoring ? Agents.** You can find the agent installed device listed.
   2. Select the respective device in the Mapped Device column.
   3. Click **'Confirm'** to map the device.

You can also add a log file monitor from a particular device's snapshot page.

1. Go to the **Device's Snapshot Page ? Monitors ? File Monitor ? Add New Monitor.**
2. Follow the same steps as provided above to add the file monitor.
3. There is an additional option available here which allows you to test the file path to ensure that the file is available.

You have successfully created a log file monitor.

Note:

1. If the file monitoring interval is modified, the match string appeared in the current polling span (old monitoring interval) will be ignored and hence the alert will not be generated. The alert will be raised as usual based on the new monitoring interval from next poll.

For example:

- Consider the file monitoring interval is 5 mins, starting at 10.00 AM.
- Search string appears in the monitored log file at 10.02 AM (which will be raised as an alert at 10.05 AM).
- File monitoring interval is modified as 10 mins at 10.03 AM.

In the above case, the agent will **ignore the search string which appeared at 10.02 AM.** It starts monitoring the log file afresh from 10.03 AM based on the new monitoring interval (10 mins).

2. Once a log file monitor is added and the agent is mapped to a device, a pointer will be set at the very end of that log file. OpManager will only monitor strings that are input after this point, and ignores all instances of the same string that were present before the monitor was mapped to the device.

Adding File Monitoring Template

You can now track changes on critical system and user files and be notified if a specific change occurs.

E.g. If you want to get notified about an increase in a file's size, you can configure an appropriate file monitoring template with a file size monitor and apply the same to devices in which you want the files monitored.

Using file monitoring, you can monitor the following parameters on Windows/ WMI based devices:

- **File Content:** Presence of a word/string or in a log file (Supports RegEx too)
- **File size**: Monitor increase or decrease in the size of the file
- **Presence of a file:** Check the availability of a file in the specified directory (to check if it has been moved, renamed, or deleted)
- **File age:** Keep track of the age of a file and take actions based on its age
- **File modification:** Get notified if a file has been modified

Steps to configure a file monitoring template

1. Go to **Settings ? Monitoring ? Files.**
2. Click **New Template**. Add New Template page opens.
3. Configure the following fields:
    - **Template Name**: Configure a name for the template.
    - **File Path**: Specify the path in which OpManager should locate the file.
    - **Polling Interval**: Configure the interval at which OpManager should monitor the file.
    - **Description**: Provide a brief, meaningful description for the template.
4. If you wish to associate the monitor to existing devices, click on **Save & Associate**. This option will prompt you to select the required devices to which the monitor must be associated. Select the required devices and click on **Save**.
5. If you wish to only add the monitor (and not associate it to any of the existing devices), click on **Save**.

Configuring Alerts for File Monitors

Configure the monitoring criteria based on which you want to be notified:

1. **File Contains:** To monitor if a word/string is being printed in a log file, you have to install OpManager's log file monitoring agent in the end server/device where the application is running. Once you install the agent, it looks for the specified string in the said log file. If the word/string is printed in the log file, OpManager raises an alert. If required, you can configure the agent to match the case when searching for the word/string, and also to notify the admin if the alert is raised for a certain number of times.

   Click here to know more on this type of monitor and the prerequisites to be satisfied for log file monitoring.
2. **File Existence:** OpManager looks for the file in the specified path and alerts based on the conditions specified. You can configure to be notified if the file does not exist in the path specified, or be notified if the file exists, or you can choose not to monitor. Also, you can choose the severity that you would like to assign to this alert. The notification can be triggered if the alert condition is met for a predefined number of times. That is, OpManager alerts you if a particular file exists/ is unavailable in a path during two consecutive polls.
3. **File Size:** Configure OpManager to alert you if the file size goes over, or comes below a specified size. Select the relevant threshold for alerting. You can configure the size in terms of bytes, KB, MB, or GB, and you can also choose the severity that you would like to assign to this alert. The alert can be triggered if the threshold is violated a specified number of times.
4. **File Age:** Similarly, you can configure OpManager to alert you based on the age of the file. For instance, you can be notified if a file is over 20 days old.
5. **File Modification:** When a file is modified, the date on which the file is modified is updated. You can configure OpManager to notify you whenever there is a change in the date modified. This option helps you keep track of any changes done in critical files.

Configuring alarms - available variables for alarm messages

You can customise your alarm message generated when a provided criteria is violated, by using these alarm variables in the Alarm Message Format field:

1. **$MONITOR** - Displays the name of the monitor. Can be used with all criteria types.
2. **$CURRENTVALUE -** Displays the latest polled value of the provided trigger criteria (File Contains/Age/Size). Can be used with **all criteria types EXCEPT File Existence and File Modification.**

   > **Note:** The variable $CURRENTVALUE works differently for File Contains and File Age/Size. For File Contains criteria type the provided search string is returned, whereas it returns the latest polled value for File Age/File Size criteria types.

3. **$THRESHOLDVALUE -** Displays the threshold value of the provided trigger criteria. Can be used with **File Size and File Age** criteria types.
4. **$UNITS -** Displays the units of the trigger criteria. Can be used for **File size and File Age** criteria types.
   - **Available units in File Size:** bytes, KB, MB, GB
   - **Available units in File Age:** minutes, hours, days
5. **$MODIFIEDTIME -** Displays the latest Modified Time value of the file in the provided file path. Can be used with **File Modification** criteria type.

Sample messages for each criteria type using alarm variables

Criteria type	Supported alarm variables	Sample alarm message with variables	Generated alarm message
File contains	**$MONITOR -** Monitor name **$CURRENTVALUE -** Search string	File monitor **$MONITOR** contains the string **$CURRENTVALUE**	File monitor **FileMonitor1** contains the string **test**
File Existence	**$MONITOR -** Monitor name	File monitor **$MONITOR** exists (OR) File monitor **$MONITOR** does not exist any more	File monitor **FileMonitor2** exists (OR) File monitor **FileMonitor2** does not exist any more
File Size	**$MONITOR -** Monitor name **$THRESHOLDVALUE -** Minimum size of file required to trigger the alarm (in bytes/KB/MB/GB) **$CURRENTVALUE -** Current size of the file in the path (in bytes/KB/MB/GB) **$UNITS -** Units provided for the threshold value (bytes/KB/MB/GB)	File size of the monitor **$MONITOR** is $CURRENTVALUE, violating the threshold of **$THRESHOLDVALUE $UNITS**	File size of the monitor **FileMonitor3** is **2,** violating the threshold of **1 GB**

File Age	**$MONITOR -** Monitor name **$THRESHOLDVALUE -** Minimum size of file required to trigger the alarm (in seconds/minutes/hours) **$CURRENTVALUE -** Current size of the file in the path (in seconds/minutes/hours) **$UNITS -**Units provided for the threshold value (seconds/minutes/hours)	File age of the monitor **$MONITOR** is **$CURRENTVALUE,** violating the threshold of **$THRESHOLDVALUE $UNITS**	File age of the monitor **FileMonitor4** is **95**, violating the threshold of **90 mins**
File Modification	**$MONITOR -** Monitor name **$MODIFIEDTIME -** Latest value for Modified Time of the value (MM/DD/YYYY HH:MM:SS AM/PM)	File monitor **$MONITOR** got modified at **$MODIFIEDTIME**	File monitor **FileMonitor5** got modified at **8/13/2017 1:12:35 AM**

Associating the File monitor to devices

Having created a template with the alert criteria, you can now associate the template to the devices.

1. Go to **Settings ? Monitoring ? Files.**
2. Click **Associate.**
3. Select the required template from the drop-down.
4. Select the devices for which you want to apply this template and click on the right arrow to move them to the 'Selected devices' list.
5. Click **Associate** button at the bottom of the tab to associate the template to all the selected devices.

The monitor is now added to the device and OpManager raises alerts based on the alert conditions provided by the user.

Adding Folder Monitoring Template

Besides monitoring files on the systems, you can also monitor the folders.You can track changes in folders based on the folder size, the number of files in a folder etc. Again, like file monitors, you can be notified if a specific change occurs. For instance, you might want to be notified if the folder size increases beyond a defined limit, if some files in a folder are missing etc. Configure meaningful templates in OpManager and apply them to devices on which you want the folders monitored. Monitor the following parameters on folders:

- Folder size: Watch for an increase or decrease in the file size
- Existence of a file: Check the availability of a file in the specified directory (may have been moved, renamed, or deleted)
- Folder Modification: Keep track of any file changes (add/remove/rename) in a folder.
- File Name: Watch files in a folder by their name.
- File Size/Age: Check the last modified file or all files in a folder for file size and age.
- File count: Keep track of the number of files within a folder.

Steps to configure a file monitoring template

1. Go to **Settings ? Monitoring ? Folders.**
2. Click **New Template**. Add New Template window opens.
3. **Template Name**: Configure a name for the template.
4. **Folder Path**: Specify the path in which OpManager should locate the file. You can either provide the local directory (C:) or UNC share path (\servername\shareddirectory).
5. **Polling Interval**: Configure the interval at which OpManager should monitor the file.
6. **Description**: Provide a brief, meaningful description for the template.
7. If you wish to associate the monitor to existing devices, click on Save & Associate. This option will prompt you to select the required devices to which the monitor must be associated
   Select the required devices and click on Save.
8. If you wish to only add the monitor (and not associate it to any of the existing devices), click on Save.
   .

Configuring Thresholds for Folder Monitors

Configure the monitoring criteria for Folder/File monitoring conditions based on which you want to be notified:

1. **Folder Existence:** OpManager looks for the folder in the specified path and alerts based on the conditions specified. You can configure to be notified if the folder does not exist in the path specified, or be notified if the folder exists , or you can choose not to monitor.
2. **Folder Size:** Configure OpManager to alert you if the folder size goes over, or comes below a specified size. Select the relevant threshold for alerting. You can configure the size in terms of bytes, KB, MB, or GB. Configure the rearm accordingly to reset the alarm.
3. **Folder Modification:** Select Alert if modified check box to receive alerts when files/sub-folders are added/deleted/renamed in the specified folder.
4. **File Filter:** By default all the files in the specified folder are monitored. Deselect All files check box and enter the file name or extension (*.pdf,*.txt) of the files alone you want to monitor. You can enter multiple values separated by comma, but no blank space is allowed. You can enter the filename in the following formats:
   - Full file name with extension ﷺstdout.doc,stdlog.txt﷽
   - File name with wild characters ﷺout﷽ or ﷺstd*﷽. Files containing the same prefix or suffix name with same/different extension will be monitored
   - File name in date format ﷺ2011062200001.txt﷽. Enter the file name in a static format $YYYY$MM$DD*.txt or $YYYY

DDMM*.txt

5. **File Name Contains:** OpManager looks for the files in the specified folder and alerts based on the conditions specified. You can configure to be notified if the folder does not contain any file in the specified name , or be notified if the folder contains files in the specified name, or you can choose not to monitor.
6. **File Size/Age:** OpManager looks either last modified file or all files for file size and age. If the threshold condition for either file size or file age is violated, an alarm is raised. Configure the relevant threshold and rearm conditions.
7. **File Count:** You can monitor the number of files specified in the File Filter and be alerted if the count changes, or of it violates a count threshold. Configure the rearm accordingly to reset the alarm.

Configuring Alerts for Folder Monitors

Configure the following alerting options:

1. **Severity:** Choose the severity that you would like to assign to this alert.
2. **Consecutive Times:** Specify how many time the threshold can be violated to generate the alert
3. **Alarm Message Format:** Configure the alarm message. You can include the alarm variables by appending $ to the variable name.

Associating the Folder monitor to devices

Having created a template with the alert criteria, you can now associate the template to the devices.

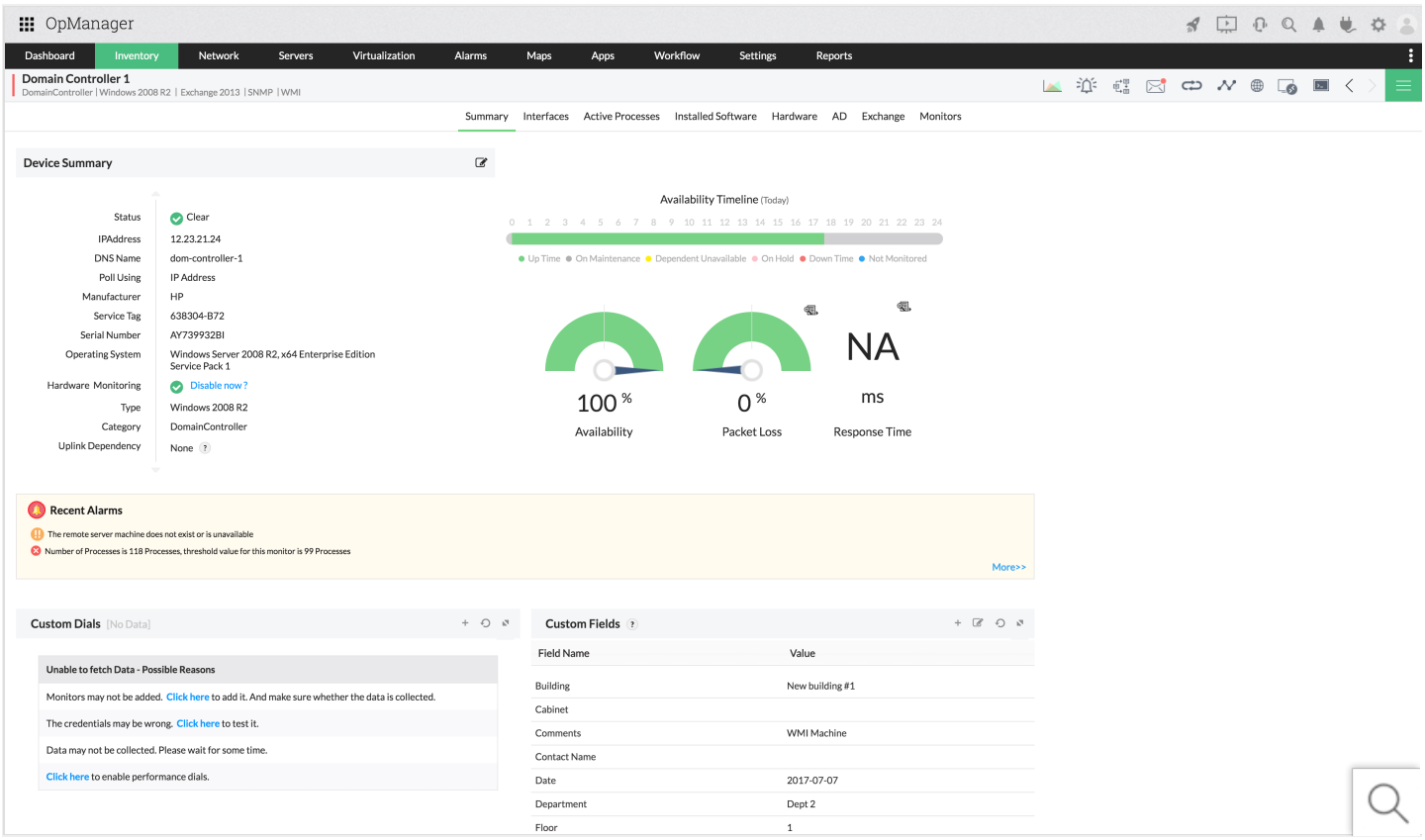
1. Go to **Settings ? Monitoring ? Folders.**
2. Click **Associate**
3. Selecte the required Template from the drop-down
4. Select the devices for which you want to apply this template and move them to the right.
5. Click on **Associate** button at the bottom of the column to associate the template to all the selected devices.

The monitor is added to the device and OpManager alerts based on the alert conditions configured.

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 the dial graphs for Availability, Packet Loss and Response Time. In addition to this, there are also provisions to monitor CPU, Disc and Memory 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.

Exchange Server Monitoring

You can monitor critical MSExchange (2000/2003/2010/2013/2016/2019) Services and parameters using OpManager's exchange monitoring feature. 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 Attendant
- 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

Configuring Exchange Parameters and Services Monitoring

1. Go to the snapshot page of a device that has Exchange running.
2. Click **Monitors** > **Performance Monitors** > **Add Exchange Monitor**
3. Select the Exchange Server version. The monitors of all the Exchange parameters and services are displayed.
4. From this list, select the required Monitors and Click **Add** to associate it to the Server.

These monitors are associated to the device. Ensure to associate the correct WMI credential to the device. OpManager uses these credentials to connect to the device using WMI.

Monitoring MSSQL Parameters

MSSQL Services and Parameters can be monitored using WMI. OpManager detects the SQL servers by itself and MSSQL related resource metrics are added automatically.

Here are the steps to manually associate the MSSQL monitors to a device :

1. Go to the snapshot page of a device that has MSSQL running.
2. Click on **Monitors** > **Performance Monitors** > **Add MSSQL Monitor**
3. The monitors of all the MSSQL parameters are displayed.
4. From this list, select the required MSSQL Monitors and click **Add** to associate it to the Server.

These monitors are associated to the device. Ensure to associate the correct WMI credential to the device. OpManager uses these credentials to connect to the device using WMI.

Monitoring Windows Event Logs

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.

You can view the list of all events monitored by OpManager, Go to **Settings** > **Monitoring** > **Event Log Rules**

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. Go to the device snapshot page.
2. Click **Monitors** > **EventLog Monitors** > **Add Monitor**.
3. Select the event logs to be monitored in the device.
4. Click **Associate** to add the selected monitors to the device.

Note: The **Monitoring Interval** checkbox must be enabled. If disabled, all the event log monitors associated with the device will be disabled and they will not work although they are associated to the device.

Creating an Event Log Monitor

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

1. Go to **Settings** > **Monitoring** > **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 **Add New Rule** under any one of the categories to add a rule.
   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.

    1. Select the Log File Name.
    2. Type a unique **Rule Name**.
    3. Enter the **Event ID** to be monitored. This is the unique identifier for the event logs.
    4. Enter the event **Source**. This is the name of the software that logs the event.
    5. 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.
    6. Type the **User** name to filter the event log based on the user who has logged on when the event occurred.
    7. 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.
    8. **Description Match Text :** Enter the string to be compared with the log message. This will filter the events that contains this string in the log message.
    9. **Generate Alarm if event is raised :** By default OpManager raises an alarm if the event occurs. However, you can configure the no. of consecutive times the event can occur within the specified no. of seconds, to raise an alarm.
    10. Choose a **severity** for the alarm generated in OpManager for this event.
3. Click **OK** to save the event log rule.

Monitoring Custom Event Logs

You can monitor event logs under a custom category too. Some applications log the events in a new category other than the default System/Applications/Security category. You can now configure rules in OpManager to parse the events in such custom categories and trigger corresponding alerts in OpManager. Here are the steps:

1. Go to **Settings** > **Monitoring** > **Event Log Rules**
2. Click **Add Custom Event log**
3. Select a device from the drop-down on which you can query for the event categories.
4. Provide the WMI details **User Name** and **Password** of the device.
5. **List logs that were created in last** Configure the time to list the logs and Click **Query Device**
6. The custom logs in the selected device are listed. Select a log from **Discovered Log Files** and click **OK**

You can now associate the rules (default or custom event logs) to the required devices.

Associating URL Monitors to Desktop, Servers and Domain Controllers

You can add URL monitors to Desktop/Servers/Domain Controllers to check the availability of local URLs.

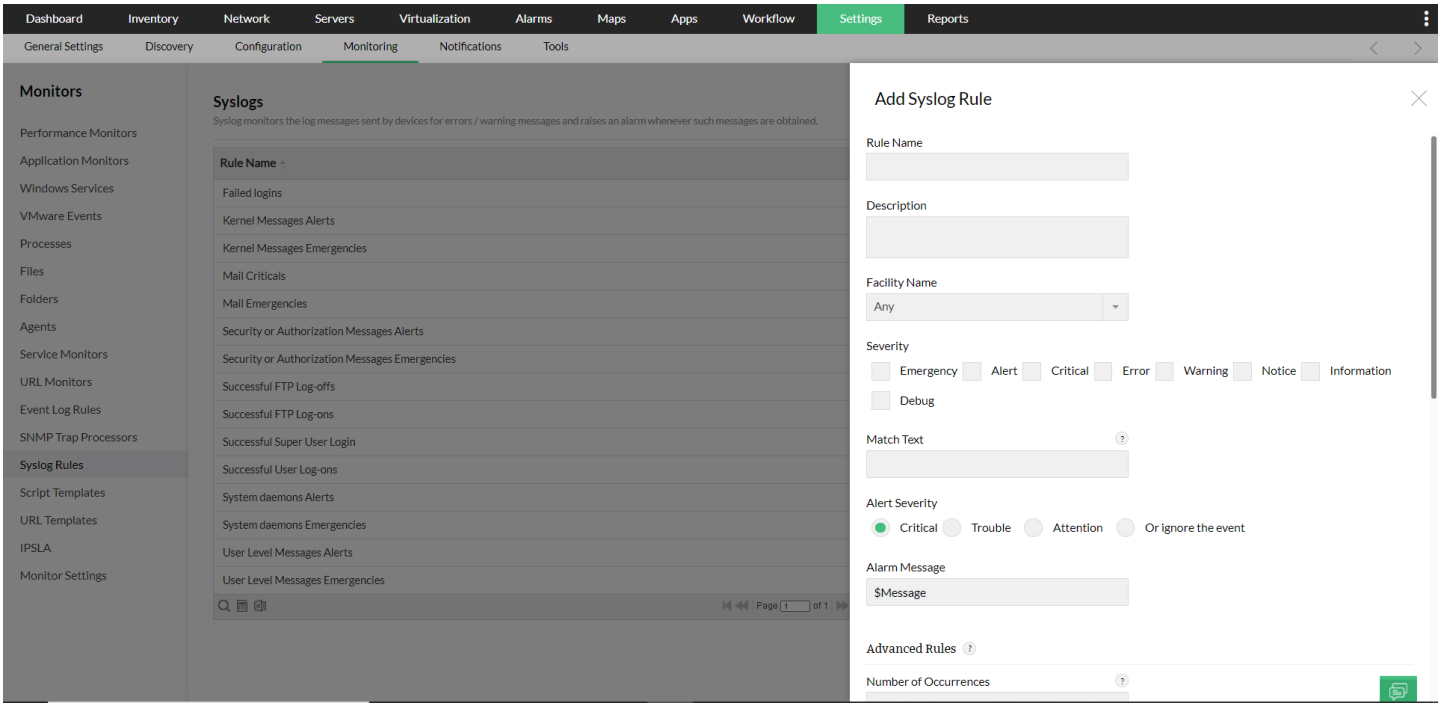
1. Go to the device snapshot page.
2. Click **Monitors ? URL Monitors**.
3. Click the **Actions** button and select **'Add monitor'.**
4. Configure all the values for the URL Monitor and Click **'Save'**.

The configured URL is monitored for availability. You can configure to receive an e-mail or SMS when the URL monitored in a device goes down. For this, you can create a notification profile for the 'URL is down' criteria and associate it to the devices.

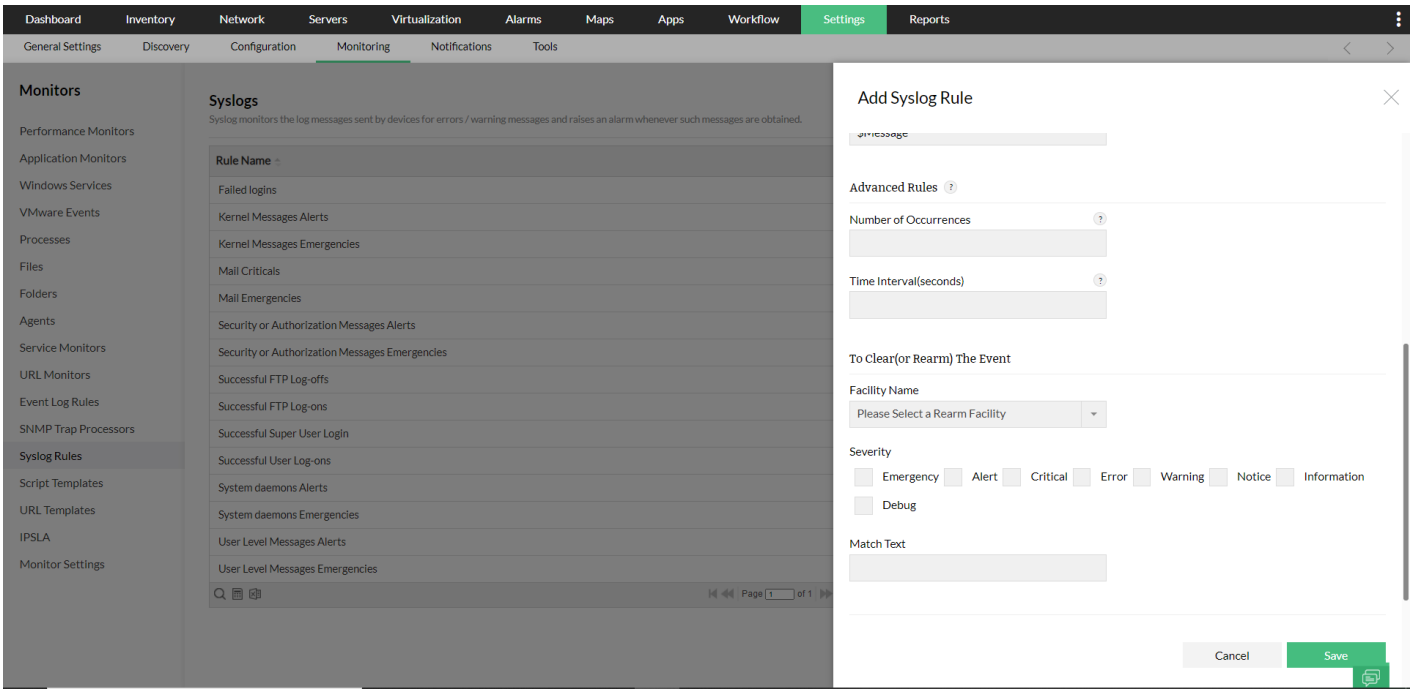
Adding Syslog Rules

Syslog is a client/server protocol that sends event notification messages to the syslog receiver. These event notification messages (usually called as syslog messages) help in identifying the authorized and unauthorized activities like installing software, accessing files, illegal logins etc. that take place in the network. In OpManager Syslog rules helps in notifying you if some particular syslog messages such as kernel messages, system daemons, user level messages etc. are sent by the devices.

Apart from the pre-defined syslog rules you can also add any number of syslog rules. Here are the steps to add a syslog rule:



1. Go to **Settings ? Monitoring ? Syslogs.**
2. Click on **Add New**. Add Syslog Rules page opens.
3. Enter a unique **Rule Name**.
4. Enter a brief **Description** about the rule.
5. Select a **Facility**. Facility refers to the application or the OS that generates the syslog message. By default "Any" is selected.
6. Select the required **Severity**.
7. **Match Text** : Enter the text that needs to be verified for matching. Note: Regex is supported for this field.
8. Select the **Alarm Severity**.
9. Enter the **Alarm Message**.



). Click the **Advanced** button to configure advanced (threshold) rules. This is optional.

1. **Number of Occurrences**: Enter the count of the number of consecutive times OpManager can receive syslog message from a device before raising an alert.
2. **Time Interval (seconds)**: Enter the time interval that should be considered for calculating the number of occurrences.

To clear or rearm the event:

3. Select the **Facility Name**.
4. Select the **Severity**.
5. Enter the **Matching Text**.
6. Click **Save.**

Configuring Syslog Ports

OpManager receives the syslog packets via the default syslog port 514. However, if required you can configure additional ports in OpManager to receive the syslog packets. To configure additional ports, follow the steps given below:

1. Go to **Settings ? Monitoring ? Syslog Rules.**
2. Click on the **Syslog Port**.
3. Enter the port number(s) separated by a comma.
4. Click **Save.**

Monitoring Syslog Packets

Syslog viewer allows you to ensure whether OpManager receives the syslog packets sent by the devices. Here are the steps to view the list of the devices that send the syslog packets:

1. From **Settings** tab, click **Tools ? Syslog Viewer.**
2. Click on the **Start** button to start listening to the Syslog packets.

The syslog packets sent by the devices to OpManager are listed. You can also filter the syslog packets by device and port.

Filtering Syslog packets

- Enter the device's IP address in the **Source** field.

  (OR)
- Enter the **port** number via which OpManager receives the syslog packets.

Viewing Syslog Flow Rate

To view the flow rate of the syslog packets,

1. Go to **Settings ? Monitoring ? Syslog Rules** and click on **'Flow Rate'**
2. Click on the **Flow Rate** tab to view the Syslog flow rate.

The flow rate of the Syslog packets are displayed in **packets/sec.**

Hardware Health Monitoring

Monitor the hardware health of key device parameters such as temperature, voltage, power, fan speed, status of processors, disk arrays, etc. of VMware, HP, Dell, Cisco, Nexus & Checkpoint Firewall systems and get alerted if they violate pre-defined thresholds.

- To enable hardware monitoring, go to **Settings ? Monitoring ? Monitor Settings ? Hardware**. Select 'Enable' next to the Hardware Monitoring field and click 'Save'.
- You can also enable hardware monitoring for individual devices from their Device Snapshot page by clicking on the Enable option for **Hardware Monitoring** under the **Summary** tab.

Before you start monitoring the hardware of your network device(s), ensure that it satisfies OpManager's prerequisites for hardware monitoring.

Collecting Hardware Health Data:

OpManager uses SNMP to monitor and collect the hardware health status of servers, routers & switches. In-case of VMware, the vSphere API is used to collect sensor data. The hardware health monitors are associated automatically whenever you add a device with proper SNMP credential. If you encounter any problem associating the hardware health monitors, then check for the correct SNMP credentials or contact our support team.

Reporting of Hardware Health:

OpManager provides historical reports on the status of hardware health which can be scheduled based on user needs.

Suppress Hardware alarms at device level:

OpManager allows you to suppress hardware alarms for individual devices. Just go to the Hardware tab in the device snapshot page of the corresponding device, and click on **Suppress Hardware Alarms** to turn off the hardware alarms for that particular device.

Customize the hardware health monitoring interval at device level:

You can customize the hardware health monitoring interval for each device from the corresponding device snapshot page. To change the hardware monitoring interval for a particular device, go to the Hardware tab in the device snapshot page and edit the value for the **Interval** option.

Prerequisites for Hardware Monitoring

It is essential to monitor the hardware components of various critical devices in your network to ensure continuous service availability and network uptime. OpManager, the advanced hardware monitor solution, supports monitoring the hardware status of the servers and network devices in your environment from vendors such as Cisco, Juniper, HP and Dell. It monitors various important hardware parameters such as voltage, temperature, power, fan speed, processors, etc., via SNMP for your network and server devices and via vSphere for VMware ESX/ ESXi hosts. OpManager offers in-depth server and hardware monitor functionality for your network.

Prerequisites for HP/Dell Servers:

HP:

If Hardware Sensor Monitors are not displayed, then please make sure that these tools are installed on that server:

- HP Insight Server Agents
- HP Insight Foundation Agents
- HP Insight Storage Agents

Dell:

If Hardware Sensor Monitors are not displayed, then please make sure that **Dell OpenManage** has been installed on that server.

Where are the hardware tabs?

If you find the hardware tabs missing, follow the below steps:

1. If the device is a VMware ESX/ESXi host:

OpManager uses the methods **hardwareStatusInfo** and **numericSensorInfo** from VMware API to poll the hardware status and stats of devices in the VMware environment. To make sure hardware monitoring works properly, check whether sensor information are available on MOB by using the following MOB link:

- **In case of ESX discovery:**
  - **For numericSensorInfo:**

    ```
    https://<<hostname/IPAddress>>/mob/?moid=ha-host&doPath=runtime.healthSystemRuntime.systemHealthInfo.numericSensorInfo
    ```

  - **For hardwareStatusInfo (cpuStatusInfo / memoryStatusInfo / storageStatusInfo):**

    ```
    https://<<hostname/IPAddress>>/mob/?moid=ha-host&doPath=runtime.healthSystemRuntime.hardwareStatusInfo
    ```

- **In case of vCenter discovery:**

  ```
  https://<<vcentrename/IPAdress>>/mob/?
  ```

  After logging into the MOB, navigate to the paths given below and check if values are being populated for both the methods:

  - **For numericSensorInfo:** content ? rootFolder ? childEntity ? hostFolder ? childEntity [select appropriate host] ? host ? runtime ? healthSystemRuntime ? systemHealthInfo ? numericSensorInfo
  - **For hardwareStatusInfo:** content ? rootFolder ? childEntity ? hostFolder ? childEntity [select appropriate host] ? host ?

runtime ? healthSystemRuntime ? hardwareStatusInfo ? cpuStatusInfo (or) memoryStatusInfo (or) storageStatusInfo

Note that OpManager raises alerts based on the colour value available (alerts are raised if the colour is anything other than "green").

If the sensors are not available, install **VMware tools** on that host.

2. If the device is HP/Dell/Cisco/Juniper:

Query the below OIDs and check if it responds for all the OIDs if it responds then rediscover the device. If it is not responding, then OpManager won't show the tabs.

- **HP:**

OID	Parameter
.1.3.6.1.4.1.232.11.2.2.1.0	Operating System
.1.3.6.1.4.1.232.11.2.2.2.0	OS Version
.1.3.6.1.4.1.232.2.2.4.2.0	Model
.1.3.6.1.4.1.232.2.2.2.6.0	Service tag
.1.3.6.1.4.1.232.2.2.2.1.0	Serial number

- **Dell:**

OID	Parameter
.1.3.6.1.4.1.674.10892.1.300.10.1.8.1	Manufacturer
.1.3.6.1.4.1.674.10892.1.300.10.1.9.1	Model
.1.3.6.1.4.1.674.10892.1.300.10.1.11.1	Service Tag
.1.3.6.1.4.1.674.10892.1.400.10.1.6.1	Operating System
.1.3.6.1.4.1.674.10892.1.400.10.1.7.1	OS Version

- **Cisco:**

OID	Parameter
.1.3.6.1.2.1.47.1.1.1.1.13.1	Hardware Model
.1.3.6.1.2.1.47.1.1.1.1.11.1	Serial Number

- **Juniper:**

OID	Parameter
.1.3.6.1.4.1.2636.3.1.2.0	Model
.1.3.6.1.4.1.2636.3.1.3.0	Serial Number

3. Check whether Hardware monitoring is enabled under **Settings ? Monitoring ? Monitor Settings ? Hardware.**

4. Check if Hardware monitoring is enabled for the individual devices in the **Device snapshot ? Hardware** tab.

5. Suppress Hardware Alarms:

a. Check if the hardware alarms for the respective devices have been suppressed in OpManager.
b. To suppress all the Hardware Alarms for all devices: Go to **Settings ? Monitoring ? Monitor Settings ? Hardware** tab and click on **Suppress Alarms** under Hardware section.
c. You can also go to the Hardware tab in the Device Snapshot page and suppress the hardware alarm for a particular device.

6. Check if Hardware status is not updated:

For OpManager to monitor the hardware of your devices, check if the following OIDs are responding properly.

- **For Cisco devices:**

  Supported MIBs: Cisco-envmon-mib | ENTITY-MIB MIB
  (All Cisco devices that use these MIBs can be monitored using OpManager)

  .1.3.6.1.2.1.47.1.1.1.1.13.1 - HW_MODEL
  .1.3.6.1.2.1.47.1.1.1.1.11.1 - HW Serial num

Metric type	OID of corresponding metric name	OID of corresponding metric status	OID of corresponding metric value
Temperature	.1.3.6.1.4.1.9.9.13.1.3.1.2 (TemperatureStatusDescr)	.1.3.6.1.4.1.9.9.13.1.3.1.3 (TemperatureStatusValue)	.1.3.6.1.4.1.9.9.13.1.3.1.6 (TemperatureState)
Voltage	.1.3.6.1.4.1.9.9.13.1.2.1.2 (VoltageStatusDescr)	.1.3.6.1.4.1.9.9.13.1.2.1.3 (VoltageStatusValue)	.1.3.6.1.4.1.9.9.13.1.2.1.7 (VoltageState)
Fan	.1.3.6.1.4.1.9.9.13.1.4.1.2 (FanStatusDescr)	.1.3.6.1.4.1.9.9.13.1.4.1.3 (FanState)	NA
Power	.1.3.6.1.4.1.9.9.13.1.5.1.2 (SupplyStatusDescr)	.1.3.6.1.4.1.9.9.13.1.5.1.3 (SupplyState)	NA

- **For Cisco Nexus devices:**

  Supported MIB: CISCO-ENTITY-FRU-CONTROL-MIB
  (All Cisco Nexus devices that use this MIB can be monitored using OpManager)

Metric type	OID
Power	.1.3.6.1.4.1.9.9.117.1.1.2.1.1 {FRUPowerAdminStatus)
	.1.3.6.1.4.1.9.9.117.1.1.2.1.2 (FRUPowerOperStatus)
	.1.3.6.1.4.1.9.9.117.1.1.2.1.3 (FRUCurrent)
Fan	.1.3.6.1.4.1.9.9.117.1.4.1.1.1 (FanTrayOperStatus)

- **For Checkpoint devices:**

  Supported MIBs: CHECKPOINT-MIB
  (All Checkpoint devices that use these MIBs can be monitored using OpManager)

Metric type	OID of corresponding metric name	OID of corresponding metric status	OID of corresponding metric value
Voltage	.1.3.6.1.4.1.2620.1.6.7.8.3.1.2 (voltageSensorName)	1.3.6.1.4.1.2620.1.6.7.8.3.1.6 (voltageSensorStatus)	.1.3.6.1.4.1.2620.1.6.7.8.3.1.3 (voltageSensorValue)
Fan	.1.3.6.1.4.1.2620.1.6.7.8.2.1.2 (fanSpeedSensorName)	1.3.6.1.4.1.2620.1.6.7.8.2.1.6 (fanSpeedSensorStatus)	1.3.6.1.4.1.2620.1.6.7.8.2.1.3 (fanSpeedSensorValue)
Temperature	.1.3.6.1.4.1.2620.1.6.7.8.1.1.2 (tempertureSensorName)	.1.3.6.1.4.1.2620.1.6.7.8.1.1.6 (tempertureSensorStatus)	1.3.6.1.4.1.2620.1.6.7.8.1.1.3 (tempertureSensorValue)

- **For HP servers:**

  Supported MIBs: CPQHOST-Mib | CPQHLTH-Mib | CPQSINFO-Mib
  (All HP servers that use these MIBs can be monitored using OpManager)

Metric type	OID of corresponding metric name	OID of corresponding metric status	OID of corresponding metric value
Temperature	.1.3.6.1.4.1.232.6.2.6.8.1.8 (TemperatureHwLocation) **(or)** .1.3.6.1.4.1.232.6.2.6.8.1.3 (TemperatureLocale)	.1.3.6.1.4.1.232.6.2.6.8.1.6	.1.3.6.1.4.1.232.6.2.6.8.1.4
Fan	.1.3.6.1.4.1.232.6.2.6.7.1.11 (FanHwLocation) **(or)** .1.3.6.1.4.1.232.6.2.6.7.1.3 (FanLocale)	.1.3.6.1.4.1.232.6.2.6.7.1.9 (FanCondition)	.1.3.6.1.4.1.232.6.2.6.7.1.12 (FanCurrentSpeed)
Processors	.1.3.6.1.4.1.232.1.2.2.1.1.3 (CpuName)	.1.3.6.1.4.1.232.1.2.2.1.1.6 CpuStatus)	.1.3.6.1.4.1.232.1.2.2.1.1.4 (CpuSpeed)
Power	.1.3.6.1.4.1.232.6.2.9.3.1.11 (PowerSupplySerialNumber)	.1.3.6.1.4.1.232.6.2.9.3.1.4 (PowerSupplyCondition)	.1.3.6.1.4.1.232.6.2.9.3.1.8 (PowerSupplyCapacityMaximum)
Partition details	.1.3.6.1.4.1.232.11.2.4.1.1.2 (FileSysDesc)	.1.3.6.1.4.1.232.11.2.4.1.1.8 (FileSysStatus)	.1.3.6.1.4.1.232.11.2.4.1.1.5 FileSysPercentSpaceUsed)
Memory	.1.3.6.1.4.1.232.6.2.14.12.1.3 (BoardCpuNum)	.1.3.6.1.4.1.232.6.2.14.12.1.11 (BoardCondition)	.1.3.6.1.4.1.232.6.2.14.12.1.9 (BoardOsMemSize)

- **For Dell servers:**

  Supported MIBs: DELL-RAC-Mib | StorageManagement-MIB.mib | MIB-Dell-10892.mib
  (All Dell servers that use these MIBs can be monitored using OpManager)

Metric type	OID of corresponding metric name	OID of corresponding metric status	OID of corresponding metric value
Temperature	.1.3.6.1.4.1.674.10892.1.700.20.1.8 (ProbeLocationName)	.1.3.6.1.4.1.674.10892.1.700.20.1.5 (ProbeStatus)	.1.3.6.1.4.1.674.10892.1.700.20.1.6 (ProbeReading)
Fan	.1.3.6.1.4.1.674.10892.1.700.12.1.8 (DeviceLocationName)	.1.3.6.1.4.1.674.10892.1.700.12.1.5 (DeviceStatus)	.1.3.6.1.4.1.674.10892.1.700.12.1.6 (DeviceReading)

Processors	.1.3.6.1.4.1.674.10892.1.1100.30.1.23 (DeviceBrandName)	.1.3.6.1.4.1.674.10892.1.1100.30.1.5 (DeviceStatus)	.1.3.6.1.4.1.674.10892.1.1100.30.1.11 (DeviceMaximumSpeed)
Power	.1.3.6.1.4.1.674.10892.1.600.60.1.6 (EntityName)	.1.3.6.1.4.1.674.10892.1.600.60.1.5 (Status)	.1.3.6.1.4.1.674.10892.1.600.60.1.9 (PeakWatts)
Voltage	.1.3.6.1.4.1.674.10892.1.600.20.1.8 (ProbeLocationName)	.1.3.6.1.4.1.674.10892.1.600.20.1.5 (ProbeStatus)	.1.3.6.1.4.1.674.10892.1.600.20.1.6 (ProbeReading)
Disk Array Data	.1.3.6.1.4.1.674.10893.1.20.130.4.1.2 (arrayDiskName)	.1.3.6.1.4.1.674.10893.1.20.130.4.1.4 (arrayDiskStatus)	.1.3.6.1.4.1.674.10893.1.20.130.4.1.17 (arrayDiskUsedSpaceInMB)
Battery	.1.3.6.1.4.1.674.10892.1.600.50.1.7 (LocationName)	.1.3.6.1.4.1.674.10892.1.600.50.1.5 (Status)	.1.3.6.1.4.1.674.10892.1.600.50.1.4 (StateSettings)

- **For Juniper devices:**

  Supported MIB: JUNIPER-MIB
  (All Juniper devices that use these MIBs can be monitored using OpManager)

  - For Juniper devices, performing a walk on the OID 1.3.6.1.4.1.2636.3.1.15.1.6 gives us a list of all hardware components or 'Field-Replaceable Units' (FRUs) present in the Juniper device(s). OpManager primarily monitors Power, Temperature and Fan speed, and these are the responses for the corresponding FRU types:

    Temperature - 6 | Power - 7 | Fan - 13

  - The instances that respond with these values are noted, and the suffix for the instance can be used to obtain data for that FRU.

    For example, consider an SNMP walk being performed on a Juniper device, on the FruType OID (1.3.6.1.4.1.2636.3.1.15.1.6) and it returns the following response:

    1.3.6.1.4.1.2636.3.1.15.1.6.**A** ? 13
    1.3.6.1.4.1.2636.3.1.15.1.6.**B** ? 6
    1.3.6.1.4.1.2636.3.1.15.1.6.**C** ? 7
    1.3.6.1.4.1.2636.3.1.15.1.6.**D** ? 2
    1.3.6.1.4.1.2636.3.1.15.1.6.**E** ? 6

    Note: The values of A, B, C, D, E can be anywhere from **one to four octets, i.e, they can have the value of 'z', 'z.y', 'z.y.x' or 'z.y.x.w'.**

  - Now we take the instances that returned **6 (or) 7 (or) 13** as the response, and we note down their instance IDs. Here, **A, B, C and E** are the instances that provided the required responses. Therefore, these are the instances that OpManager should be able to query to perform hardware monitoring on that device.

  - Now that we know the instance IDs, we can use them to check if we can query the required parameters from that instance. OpManager queries the name, status and value of each instance. So, if you want to perform hardware monitoring on the gives Juniper device, the following OIDs must respond when queried:

Response for FruType	Metric Type	Instance ID	OID of corresponding metric identifier (OperatingDescr)	OID of corresponding metric status (OperatingState)	OID of corresponding metric value (OperatingTemp)
6	Temperature	B	.1.3.6.1.4.1.2636.3.1.13.1.5.**B**	.1.3.6.1.4.1.2636.3.1.13.1.6.**B**	.1.3.6.1.4.1.2636.3.1.13.1.7.**B**
6	Temperature	E	.1.3.6.1.4.1.2636.3.1.13.1.5.**E**	.1.3.6.1.4.1.2636.3.1.13.1.6.**E**	.1.3.6.1.4.1.2636.3.1.13.1.7.**E**
7	Power	C	.1.3.6.1.4.1.2636.3.1.13.1.5.**C**	.1.3.6.1.4.1.2636.3.1.13.1.6.**C**	NA
13	Fan	A	.1.3.6.1.4.1.2636.3.1.13.1.5.**A**	.1.3.6.1.4.1.2636.3.1.13.1.6.**A**	NA

Note:

The following are the Hardware sensor status responses for devices from various supported vendors (N/A for VMware Hosts):

HP: 1 - Unknown | 2 - Clear | 3 - Trouble | 4 - Critical

Dell: 1 - Unknown | 2 - Unknown | 3 - Clear | 4 - Trouble | 5 - Critical | 6 - Service Down

Cisco: 1 - Clear | 2 - Trouble | 3 - Critical | 4 - Service Down | 5 - Unknown | 6 - Unknown

Cisco Nexus: 2 - Clear | 3 - Critical | 4 - Trouble (Any other response is considered as 'Unknown')

Checkpoint: 1 - Clear | 2 - Trouble | 3 - Critical | 4 - Service Down | 5 - Unknown | 6 - Unknown

Juniper: 1 - Unknown | 2 - Clear | 3 - Clear | 4 - Clear | 5 - Clear | 6 - Critical | 7 - Attention

7. Check if SNMP is installed:

It is mandatory that SNMP is enabled in the corresponding devices, since OpManager primarily uses SNMP to query device status and metrics. To install SNMP agent in a Linux device, follow this steps.

VoIP Monitoring with OpManager

OpManager allows you to manage your VoIP links effectively using the VoIP monitoring add-on. It combines the functionalities of fault and performance management with the Quality of Service monitoring through Cisco's IPSLA technology to give you a comprehensive view of your VoIP connections. Click on the links below to know more on this topic:

- Adding a new VoIP monitor
- Configuring VoIP monitor template
- Viewing top 10 call paths

Learn more about VoIP monitoring in OpManager.

VMware monitoring with OpManager

OpManager provides intensive, agentless virtual device monitoring to enable effortless performance management of your VMware devices. With proactive VMware monitoring and extensive reporting, make sure that your virtual devices are constantly running at peak performance. Also, set thresholds for critical parameters in your network and get notified when they cross the set values.

Click on any of these topics to browse through the help documents:

HyperV Monitoring

OpManager provides support to monitor the HyperV servers in your network, and also its hosts. OpManager provides a dedicated snapshot page to comprehensively monitor your HyperV server stats such as Health, Inventory, Performance and other critical metrics.

Click on any of these links to navigate to the help document:

- About Hyper-V Monitoring
- Discovering Hyper-V Server
- Configuring Thresholds for Hyper-V Host and VMs
- Managing Hyper-V Alerts
- Notifying Hyper-V Alerts

WAN monitoring with OpManager

WAN links are an important part of any corporate network, and it's really important that they are constantly monitored for any changes in performance such as improper connectivity or outage issues. Using OpManager, you can manage and monitor your WAN links and detect issues before they even affect your network. Also, visualize the entirety of your WAN network, and keep an eye on critical performance metrics to ensure peak performance.

- Adding a new WAN monitor
- Configuring WAN monitor template
- Viewing WAN Monitor alerts

Monitoring CIS-hardened devices

A CIS-hardened device goes a long way in improving overall security in your network. CIS hardening corresponds to tightening of security in the software component, based on the benchmarks provided by CIS (Center for Internet Security). It can mean anything from disabling unused ports and services to restricting visitor access to a system.

Monitoring CIS-enabled devices require special permissions to be provided to the network monitoring software. Please follow the steps below to enable monitoring of CIS-hardened devices in OpManager:

1. Monitoring availability via ICMP

To monitor device availability via ICMP, we first have to enable access for ICMP v4 protocols in our firewall. Below are the steps to enable ICMP in the monitored device:

1. From the monitored device, open **Command Prompt in Administrator mode.**
2. If you want to enable firewall access for OpManager server, please execute the command below, replacing <OpManager_IP> with OpManager server's IP.

```
netsh advfirewall firewall add rule name="OPM_ICMP_RULE" dir=in action=allow enable=yes protocol=ICMPv4
remoteip=<OpManager_IP>
```

2. Monitoring via SNMP

To monitor your devices through SNMP, we just have to configure SNMP service on all your network devices. Know more here on how to enable and configure SNMP in your network devices.

3. Monitoring via WMI

3.1 To enable WMI traffic, DCOM, WMI, callback sink and outgoing connections in Firewall.

To monitor hardened devices using WMI, a few connections/protocols have to be enabled for OpManager to be able to reach the device, the foremost of which would be to allow OpManager's traffic (both inward and outward) through your firewall. By default, WMI settings in Windows Firewall settings are configured to enable only WMI connections, rather than allowing other DCOM applications too. We must add an exception in the firewall for WMI, that allows the remote device to receive remote connection requests and asynchronous callbacks to Unsecapp.exe. To enable the necessary connections in your firewall, execute the below commands one by one in the monitored device, depending on your requirements.

1. To establish a firewall exception for DCOM port 135, use the following command:

    Firewall access for OpManager server:

```
netsh advfirewall firewall add rule dir=in name="OPM_DCOM_CIS"
program=%systemroot%\system32\svchost.exe service=rpcss action=allow protocol=TCP localport=135
remoteip=<OpManager_server_IP>
```

2. To establish a firewall exception for the WMI service, use the following command:

   Firewall access for OpManager server:

   ```
   netsh advfirewall firewall add rule dir=in name ="OPM_WMI_CIS"
   program=%systemroot%\system32\svchost.exe service=winmgmt action = allow protocol=TCP localport=any
   remoteip=<OpManager_server_IP>
   ```

3. To establish a firewall exception for the sink that receives callbacks from a remote computer, use the following command:

   Firewall access for OpManager server:

   ```
   netsh advfirewall firewall add rule dir=in name ="OPM_UnsecApp_CIS"
   program=%systemroot%\system32\wbem\unsecapp.exe action=allow remoteip=<OpManager_server_IP>
   ```

4. To establish a firewall exception for outgoing connections to a remote computer that the local computer is communicating with asynchronously, use the following command:

   Firewall access for OpManager server:

   ```
   netsh advfirewall firewall add rule dir=out name ="OPM_WMI_OUT_CIS"
   program=%systemroot%\system32\svchost.exe service=winmgmt action=allow protocol=TCP localport=any
   remoteip=<OpManager_server_IP>
   ```

3.2 Allow remote WMI access with restricted permissions:

You can configure a regular Windows user to access WMI information by adding the necessary user account to the Distributed COM Users and the Performance Monitor Users group using lusrmgr.msc, and then configuring the DCOM security settings to allow the groups to access the system remotely (using dcomcnfg).

Note: These configurations are required to be performed in the User profiles of the client devices that are to be monitored.

Configuring Distributed COM Users in Local user and Groups Setting:

To begin with, we are adding the DCOM user group in our local user settings.

1. Click Start ? Run, type **lusrmgr.msc** and click OK.
2. In the Users folder, right-click the user to bring up the menu, and select **Properties**.
3. Click over to the **Members of** tab, and click **Add**.
4. Under 'Enter the object names to select', type **'Distributed COM Users'** (without quotes), click **Check Names**, then click **OK**.
5. Click **Add**.
6. Repeat steps 3-5 for the **Performance Monitor Users** group and **Event Log Readers** group.

Configuring the DCOM Security Settings to allow the groups to access the system remotely:

Next, we're providing basic access permissions to the user groups (Distributed COM Users and Performance Monitor Users) to be able to gain control of the device remotely.

7. Click **Start ? Run**, type **dcomcnfg** and click OK.
8. Drill down into the **Component Services tree** until you get to My Computer. Right-click '**My Computer'** to bring up the menu, and click **Properties**.

9. Click the COM Security tab, then click **Edit Limits** under the **Launch and Activation Permissions** section.
10. Click Add.
11. Under 'Enter the object names to select', type **'Distributed COM Users'** (without quotes), click **Check Names**, then click **OK**.
12. Click **Add**.
13. Repeat steps 9-12 for the **Performance Monitor Users** group.
14. Check **Allow** for each of the permissions (Local Launch, Remote Launch, Local Activation, Remote Activation) for each of these groups, and click **OK**.

Setting the WMI Control security settings to be applied to all namespaces:

Finally, access is provided for all classes under all namespaces for both the user groups, in order to enable OpManager to fetch those data using WMI.

15. Click **Start ? Run**, type **wmimgmt.msc** and click OK.
16. Right-click WMI Control (Local) to bring up the menu, and click **Properties**.
17. Click over to the Security tab, then click **Root**, and click the **Security** button.
18. Click **Add**.
19. Under 'Enter the object names to select', type **'Distributed COM Users'** (without quotes), click **Check Names**, then click **OK**.
20. Make sure the Distributed COM Users group is selected, and click **Advanced**.
21. Highlight the row with **Distributed COM Users** in it and click **Edit**.
22. From the '**Applies to**' drop-down list, select **'This namespace and subnamespaces'**.
23. Under the 'Allow' column, check **Execute Methods, Enable Account** and **Remote Enable**, and then click **OK**.
24. Repeat steps 17-23 for the **Performance Monitor Users** group.
25. Click **OK** to close all windows.

3.3 Set permissions to Service Control Manager Security for Windows Service Monitoring:

If you wish to monitor whether Windows Service monitors are up/down, you need to grant permission to SCManager. The access to the Windows services is controlled by the Security Descriptor of Service Control Manager, which by default is restricted for hardened OS. The below mentioned steps will grant remote access to Service Control Manager in user level, to get the list of services on a server.

Retrieve the user SID of the User Account

- From the monitored device, open Command Prompt in Administrator mode.
- Run the below command to retrieve the user SID. Replace UserName with the user name for the User account.

```
wmic useraccount where name="UserName" get name,sid
```

Example:

```
wmic useraccount where name="administrator" get name,sid
```

- Note down the SID. (Ex. S-1-0-10-200000-30000000000-4000000000-500)

Retrieve the current SDDL for the SC Manager

- Run the below command which will save the current SDDL for the SC Manager to the CurrentSDDL.txt.

```
sc sdshow scmanager > CurrentSDDL.txt
```

- Edit the CurrentSDDL.txt and copy the entire content.
- The SDDL will be look like below:

```
D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)(A;;CC;;;AC)S:
(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)
```

Update the SDDL:

- Frame new SDDL snippet for above SID

```
(A;;CCLCRPWPRC;;;<SID of User>)
```

Ex.

```
(A;;CCLCRPWPRC;;;S-1-0-10-200000-30000000000-4000000000-500)
```

- Now place this snippet in before "S:" of original SDDL.
- Updated SDDL will be like this:

```
D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)(A;;CC;;;AC)
(A;;CCLCRPWPRC;;;S-1-0-10-200000-30000000000-4000000000-500)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)
```

Finally Execute the below command with Updated SDDL:

```
sc sdset scmanager D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)
(A;;CC;;;AC)(A;;CCLCRPWPRC;;;S-1-0-10-200000-30000000000-4000000000-500)S:(AU;FA;KA;;;WD)
(AU;OIIOFA;GA;;;WD)
```

This will grant the following permissions to the user:
CC - To Get Service's current configuration
LC - To Get Service's current status
RP - To Read Properties/Start the Service
WP - To Write Properties/Stop the Service
RC - To Read the Security Descriptor.

Monitoring VMware servers

OpManager monitors your VMware servers for availability and performance using native APIs. The advantage of using native APIs is that it does not require any agent to be installed on your servers. Moreover, it enhances the usability and offers in-depth monitoring capabilities to troubleshoot your Virtual Infrastructure.

Some of the highlights of monitoring VMware Servers with OpManager:

- Supports ESX/ESXi from 4.0.
- Monitors effective utilization of critical resources like CPU, Memory, Network and Disk
- Supports monitoring of hardware health such as temperature, voltage, power, fan speed, status of processors etc. via VMware API.
- Out-of-the-box 70 plus reports on Host and VMs
- Automatically maps the VMotioned VMs to the corresponding Hosts

Apart from monitoring the Hosts, VMs & DataStores, OpManager's VMware monitoring functionalities also encompass monitoring the Key Performance Indicators (KPIs) of guest OSs. Similar to that of any Windows or Linux server, OpManager monitors the applications, Windows & TCP services, processes running on the VMs using WMI/SNMP/CLI.

Pre-requisites for monitoring VMware ESX/ESXi Servers

- VCenter's vSphere / ESX client User Name and Password: As OpManager uses native APIs to monitor the VMware servers, it requires the username and password of the VCenter / Host server to poll the performance data. Provide the correct username and password when discovering the Host / VCenter.
- VMware Tools (optional): We recommend that you install VMware tools on the VMs. In general, VMware tools improve the performance of the Virtual Machine. Moreover, they offer IP address of the VMs, which helps OpManager to automatically discover them. Click here to know the procedures for installing VMware tools.
- If VMware Tools are not installed, OpManager discovers it using the VM's name. You can assign the IP address manually for such VMs in the host's snapshot page and monitor the VMs.

Discovering VMware ESX / ESXi servers in OpManager

To discover the host and the VMs, you just need to provide the IP Address/DNS Name and the vSphere credentials of the vCenter/ Host.

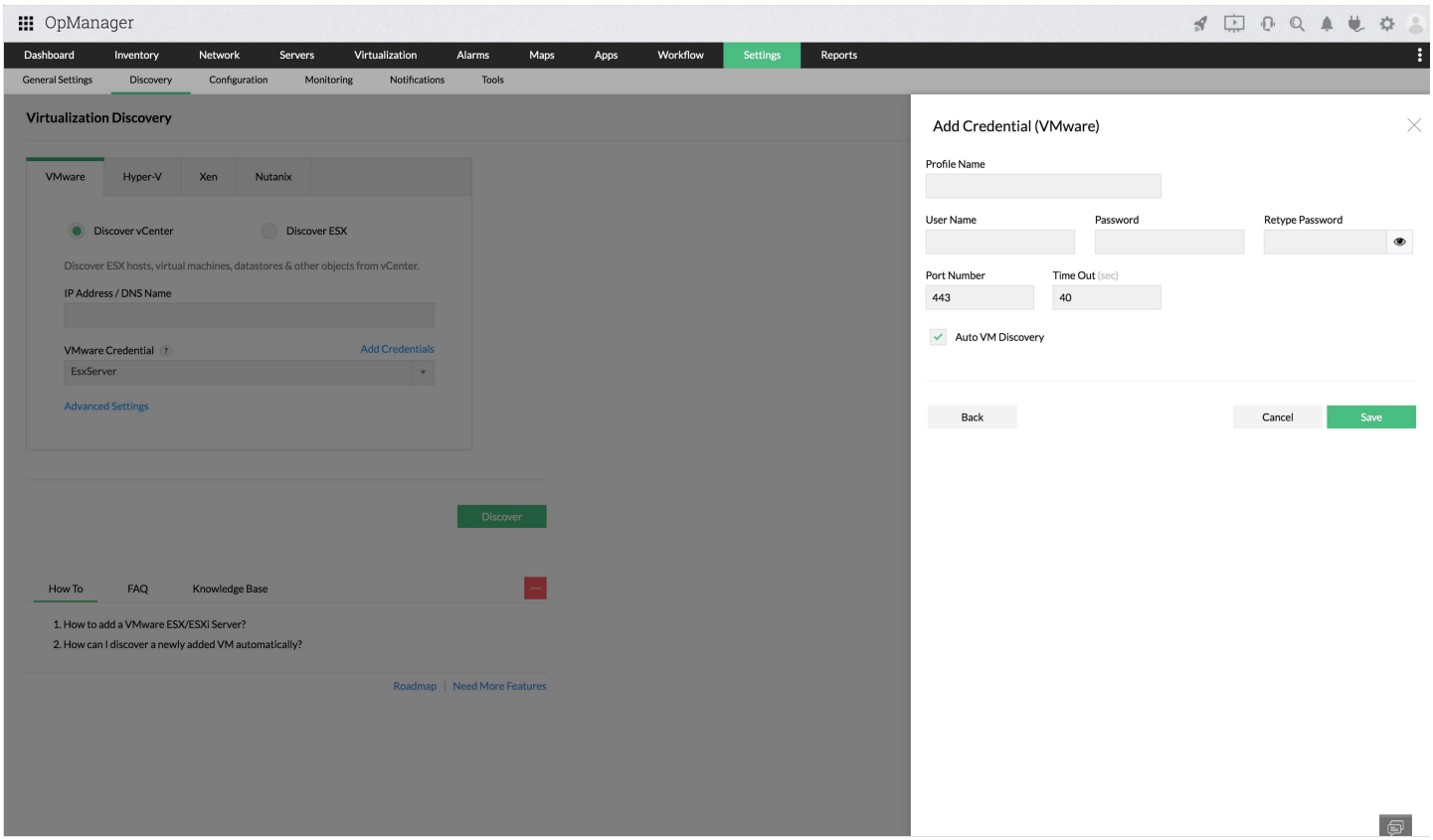
Note that the vSphere user must have access to all hosts and VMs (at least Read access) in order to monitor the devices without any issues. In case a user wants to execute actions like powering on/off VMs, please make sure that user has sufficient privileges for those actions (providing Administrator privileges works in most situations).

Discover vCenter: Use discover vCenter with the vCenter's VMware credentials, to discover all the hosts, VMs and datastores managed by that particular vCenter.

Discover ESX: Use discover ESX with the ESX's VMware credentials, to discover the host along with its datastore and VMs.

Configuring VMware credentials

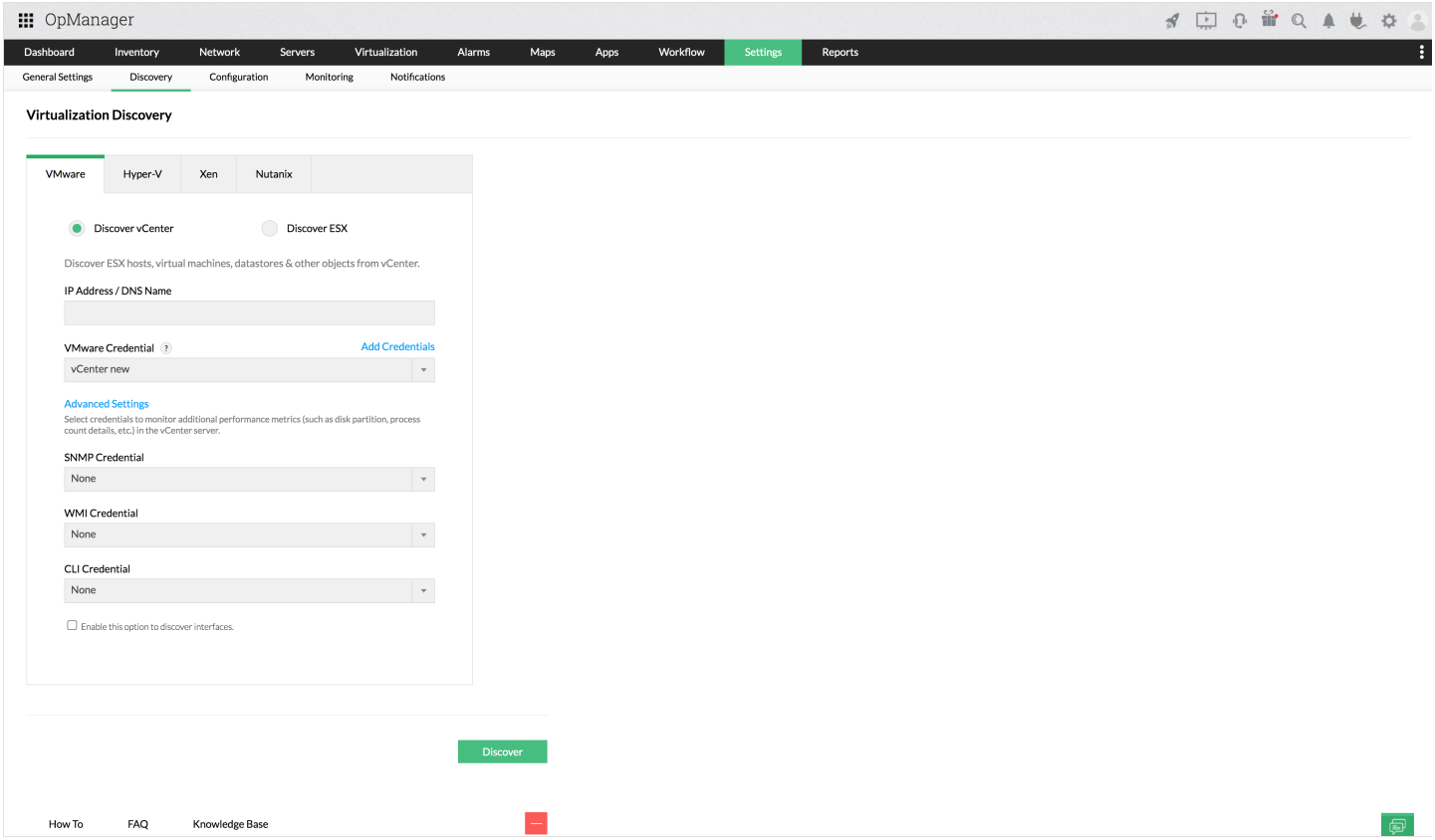
Before proceeding, ensure that you have configured the VMware credentials for the vCenter/ ESX host and the SNMP and WMI credentials for the VMs in the credential library.



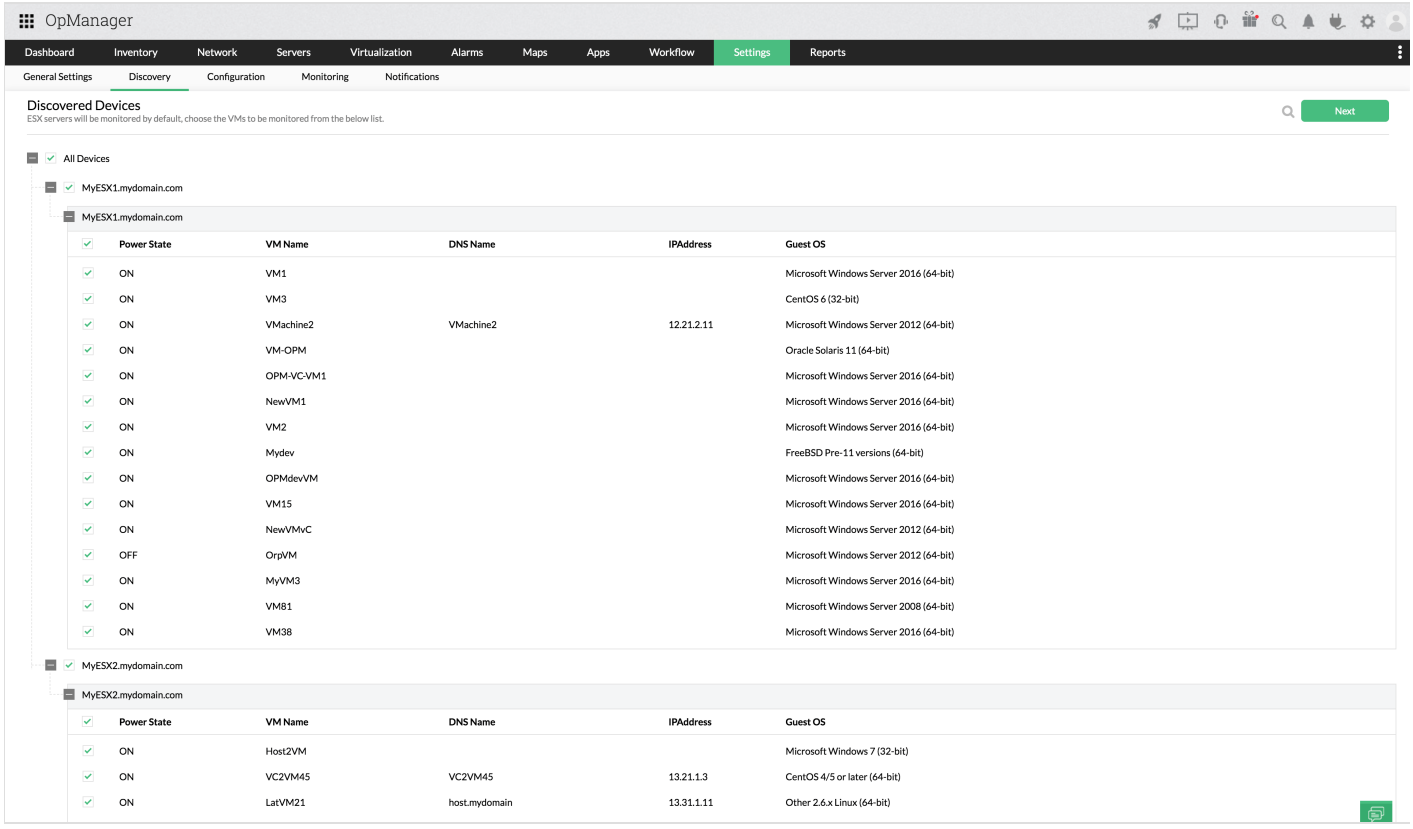
1. Go to **Settings ? Discovery ? Credentials ? Add Credentials** (or) **Settings ? Discovery ? Virtualization Discovery ? Add Credential**.
2. Select VMware as the **Credential type** and enter the vCenter/ Host's vSphere login Username and Password.
3. Enter the HTTPS (VMware web service's) **port number** and **timeout** interval for the connection between the vCenter/ Host and the OpManager server.
4. Select the **Auto VM Discovery** option to automatically discover any new VMs that are henceforth created in the vCenter.
5. Click Save to add the credential.

Similarly, add the vCenter's SNMP/WMI/CLI credentials to monitor additional performance metrics such as disk partition, process count details, etc., in vCenter servers. Select the Credential Type as WMI for Windows, CLI for Linux and SNMP for other non-Windows OS.

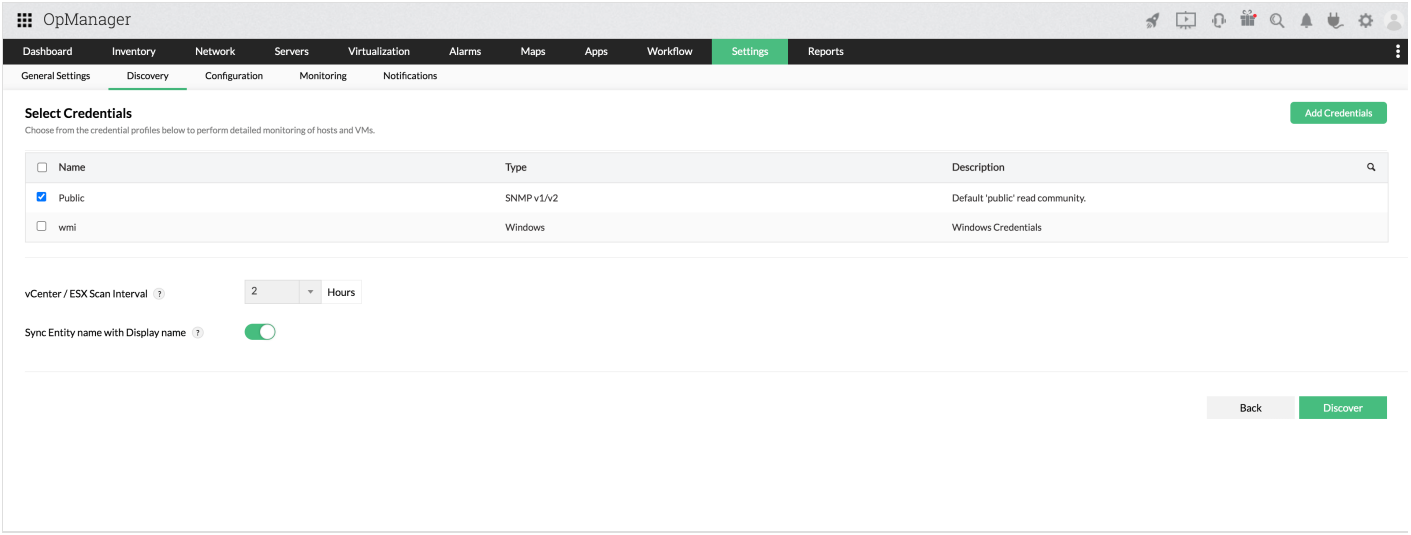
Discovering vCenter/Host



1. Go to **Settings ? Discovery ? Virtualization discovery ? VMware.**
2. If you wish to add and monitor VMs and their corresponding ESX hosts in a vCenter, select **vCenter Discovery.** Or, if you wish to monitor only a particular ESX host, select **ESX Discovery.**
3. Enter the **vCenter server's DNS Name/ IP Address.**
4. Select the appropriate vCenter's VMware credentials and other dependant SNMP/WMI/CLI credentials.
5. Click **Next** to list all the hosts and VMs in a particular vCenter.



6. By default, all hosts will be added to OpManager. However, you can select the VMs that you want to discover.
7. Click **Next** to select the VM's SNMP/WMI/CLI credentials for in-depth monitoring. You can also select multiple credentials.



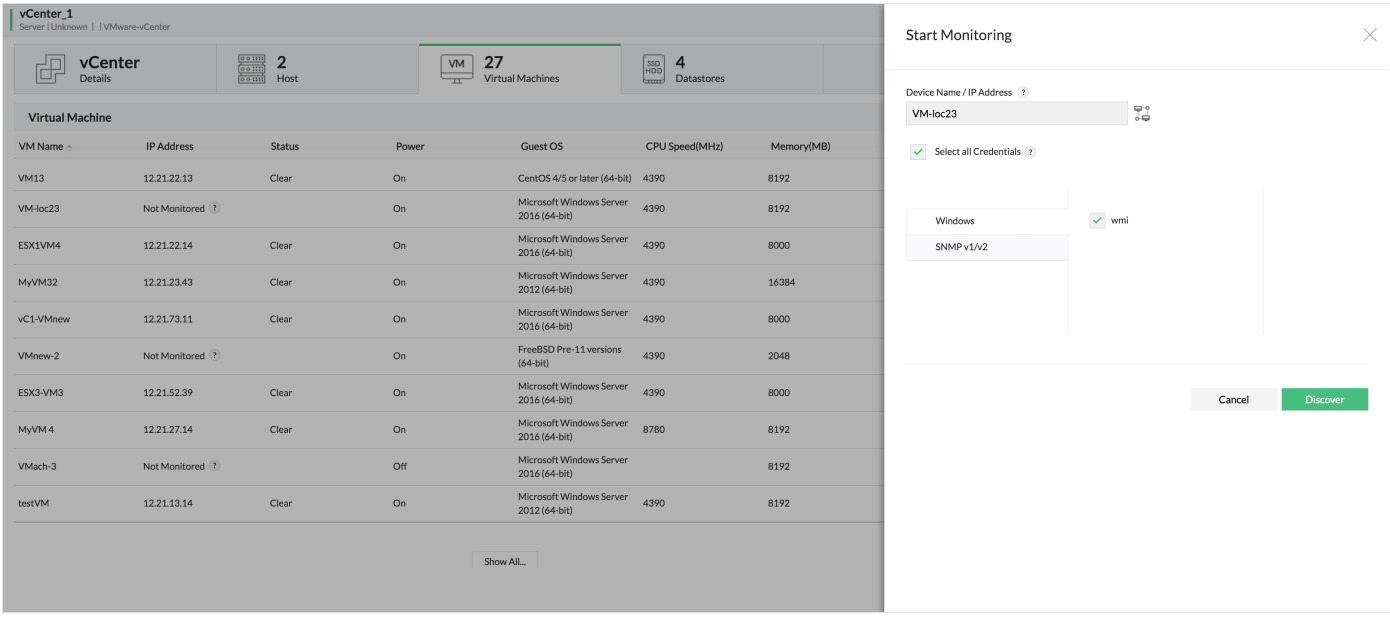
3. You can choose the time interval in which want any changes in the vCenter environment should be automatically updated in OpManager by choosing a value for **Scan vCenter/ ESX Interval (hrs).** This will automatically rediscover any changes in the vCenter environment.
3. Also, you can choose whether to sync the display name of the virtual device (the name that will be displayed in OpManager) with the entity name by enabling the **"Sync entity name with display name"** button. Once you're done, click **'Discover'** to start the discovery process.

If any of the VMs are already discovered or added, OpManager automatically maps them as virtual devices.

Configuring VM IP Address

OpManager, with the help of the installed VMware Tools, identifies the IP address of the VM and maps it to the host. If VMware Tools are not installed, OpManager discovers it using the VM's entity name. You can assign the IP address manually for such VMs in the host's snapshot page.
If VM's are not discovered/ mapped to its vCenter/Host because of an unassigned IP address, you can assign an IP address in the vSphere environment. OpManager will automatically map that VM to its vCenter/Host. (or) You can manually assign an IP address to a VM by following the simple steps below.

- Go to the **vCenter/Host's snapshot page ? Virtual Machines** tab.



- Click the start monitoring button in the **Monitoring** column for devices that are not monitored.
- This will open **IP Mapping**. Enter the **VM's IP address/ DNS name** and the corresponding credentials to rediscover and map the VM to its vCenter/Host.

You can now choose to monitor only the required VMs on a Host. If you wish to stop monitoring a VM, you can do so by clicking on the Stop monitor button of the corresponding VM under Virtual Details tab in the vCenter/Hosts snapshot page. Select the relevant icon to stop monitoring the required VMs on the host. OpManager maintains this configuration when a HA, VMotion, or rediscovery happens.

To learn more about VMware monitoring, click here.

Monitoring VMware ESX servers

All the discovered hosts, VMs and datastores are mapped in the '**VMware**' section in the **Virtualization** menu . Click on **Virtualization** to access the dashboard page, which provides a quick glance of your critical resources such as CPU, Memory, Network & Disk that are under pressure. Though ideal resource utilization is the key benefit we get from virtualization, it can lead to other problems because it is shared among the servers. Even if a single system has a resource crunch, it hugely affects the performance of the other systems running on the same host. Quickly identifying and fixing the resource utilization problems is therefore vital for a business to run smooth.

OpManager's VMware monitoring feature shows the top hosts and VMs by resource utilization and the recent alarms raised. Click on the host / VM / Datastore name to see its snapshot page. The Virtualization Dashboard page refreshes automatically every 5 minutes to reflect the latest collected statistics.

Listed below are a few of the various types of top resource utilization widgets that can help you to quickly identify any over utilized resource. These widgets give a quick glance on systems which are the top consumers of CPU, Memory, Network, Disk I/O and Disk Space and much more.

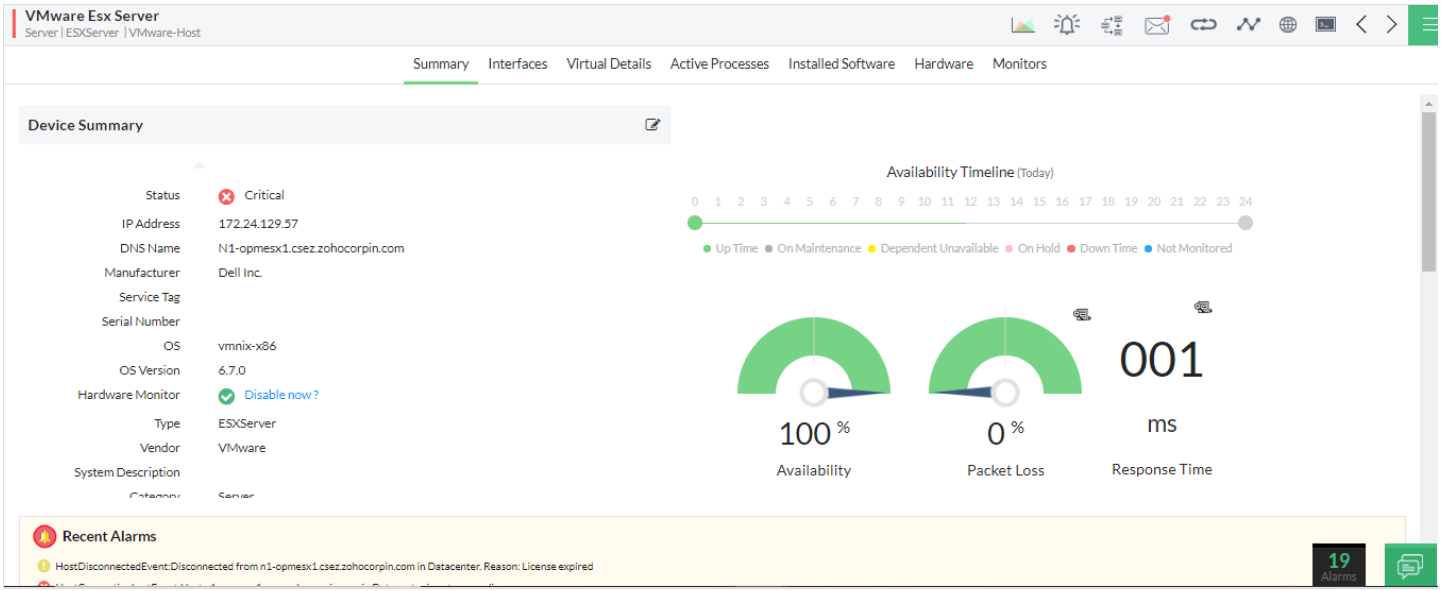
Top VMs	Top Hosts
1. Top CPU Consumers 2. Top CPU Ready Consumers 3. Top Memory Consumers 4. Top Swap Memory Consumers 5. Top Disk I/O Consumers 6. Top Network Consumers	1. Top CPU Consumers 2. Top Memory Consumers 3. Top Swap Memory Consumers 4. Top Network Consumers 5. Top Disk I/O Consumers 6. Top Disk Space Consumers

Snapshot page of a ESX Server Host

Snapshot page of a host provides a summary of the current statistics, recent alarms, configuration details such as hardware status, VMs inventory, resource allocation for each VM, Network Adapters, HBA list and Datastores.

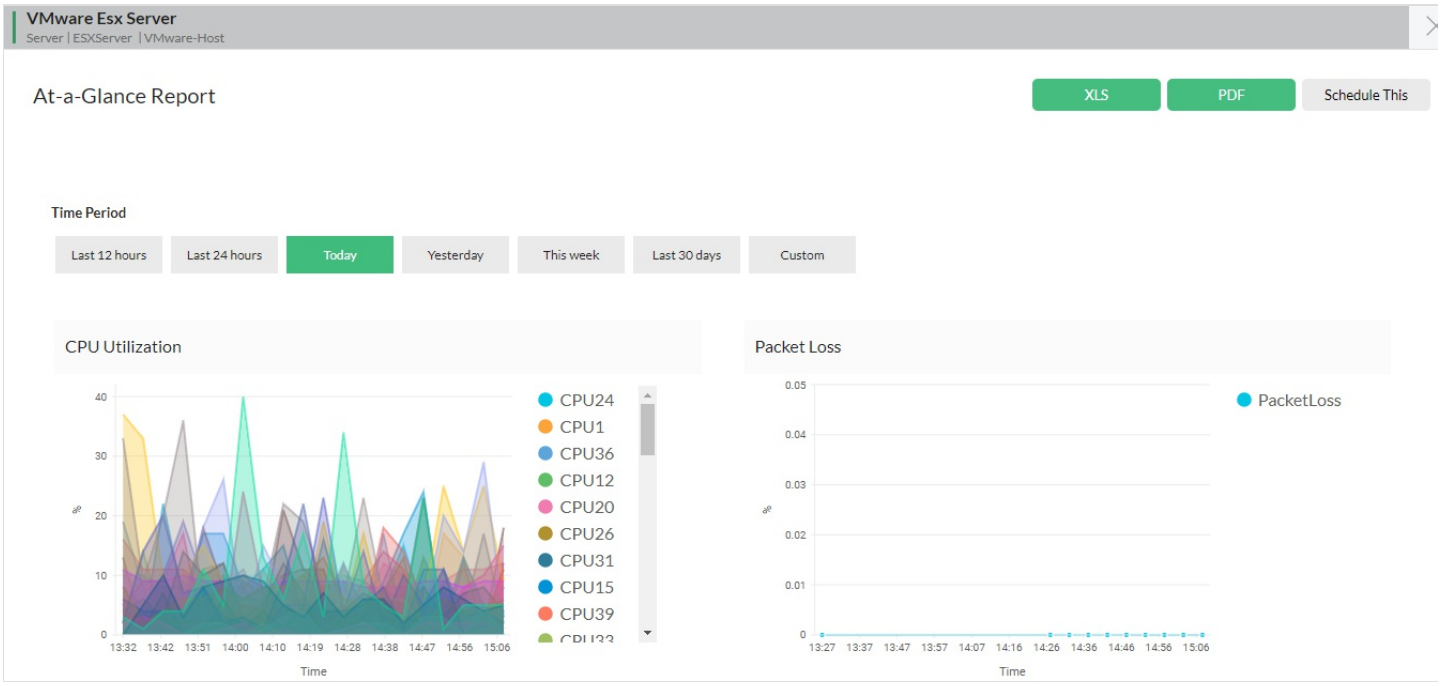
Host Details and Performance Charts

In this section you can find the Host details like IP Address, Vendor of Host, CPU Cores etc. on the left side. The right side gives a quick glance on performance data like CPU Utilization, Memory Utilization, Disk I/O Usage etc., collected during the last poll. These values are collected periodically at a pre-defined interval (in minutes). These data help you determine the current performance of the Host.

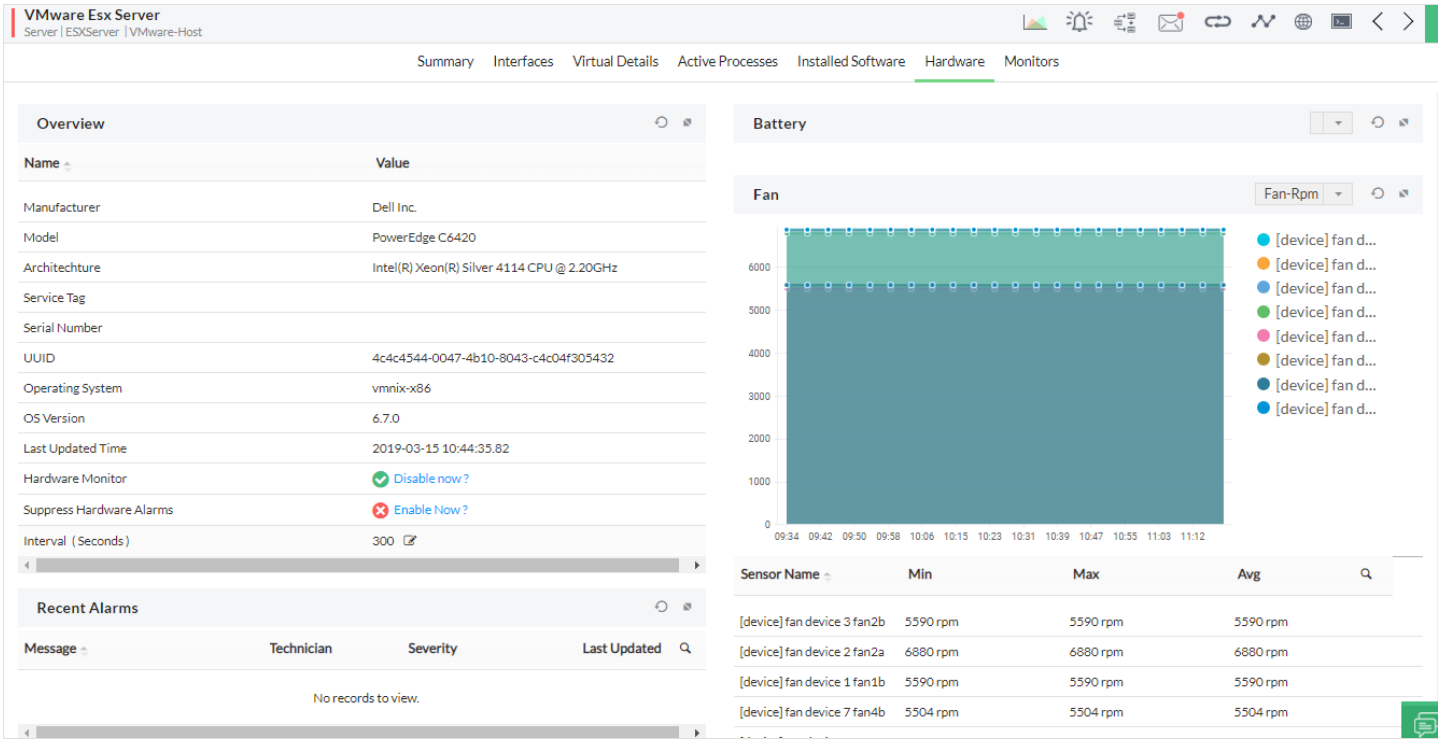


Host Health At-a-Glance

This section provides the current day's performance chart of the host by default. You can view the reports of last 12 hours / 24 hours / 7 days or even a custom date range. You can export the report as XLS / PDF or even schedule it to be delivered via email.



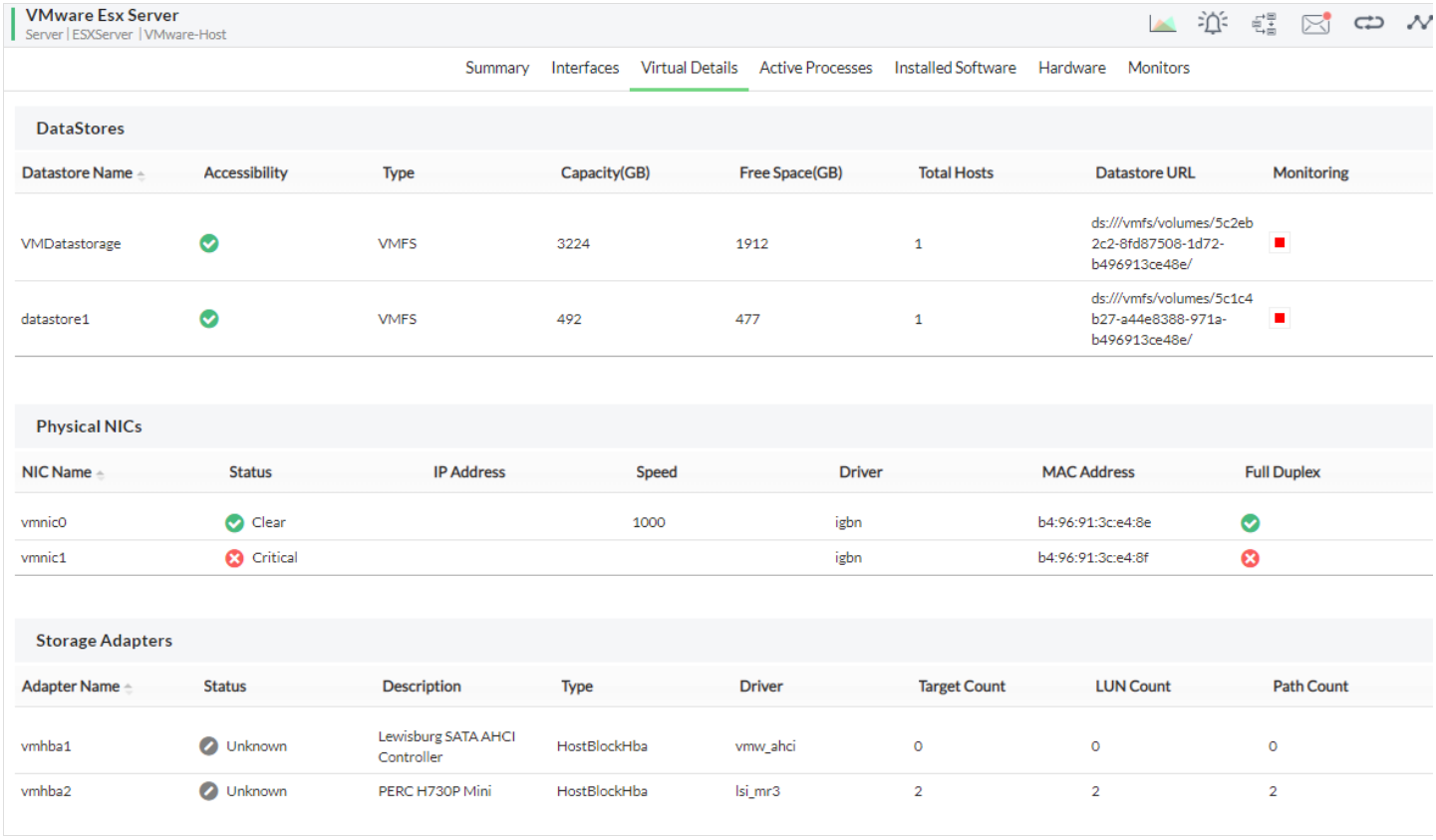
Hardware details



- You can view a host device's hardware stats such as sensor information, battery, memory , power, processor etc under the **hardware** tab in the device snapshot page.
- The hardware tab also shows the basic hardware and software information of the host such as manufacturer, OS version, model, alarms etc.

VM List & Resource Allocation Details

This section lists all the VMs on the Host, resources allotted to each VM, network adapters, storage adapters and datastore details. Any change in the inventory, gets updated automatically. You can also find the monitors that are enabled on the Host and notification profiles associated to it. Click on the respective tab to view its details.



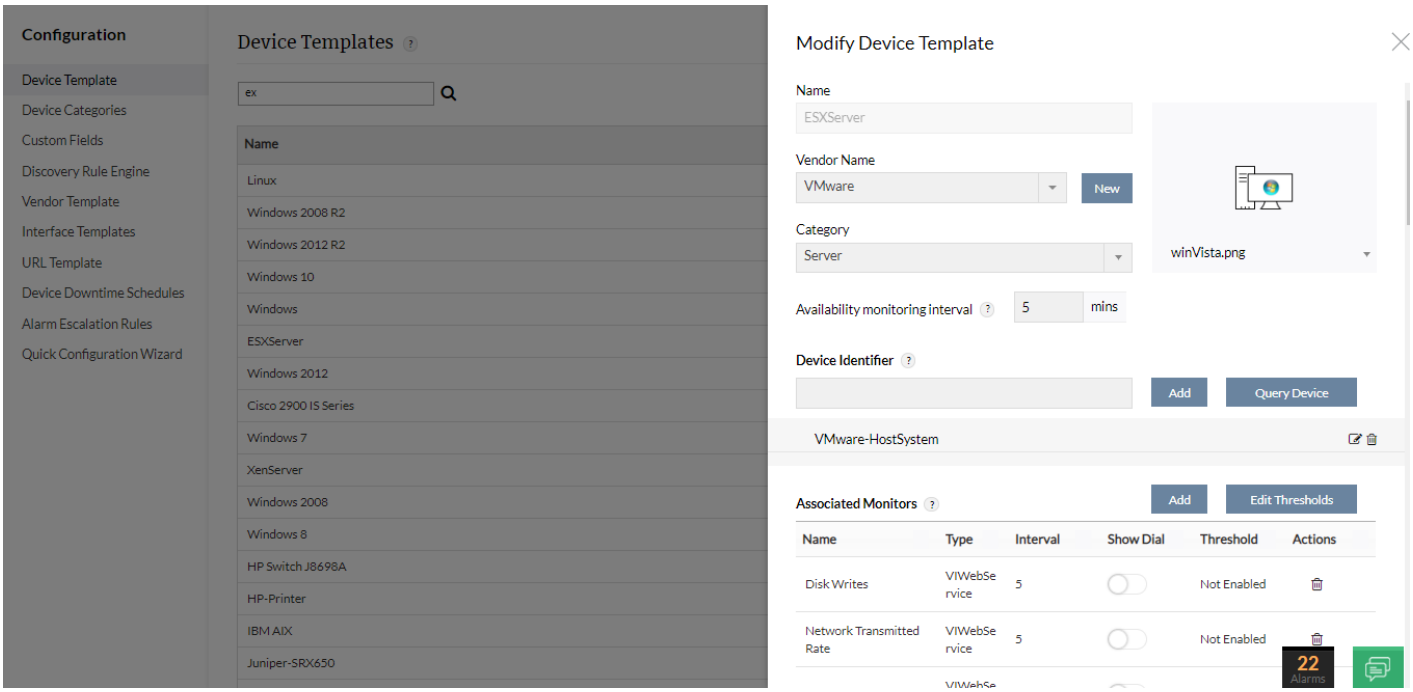
Click on the VM name to see its snapshot page. The snapshot page of the VM is similar to that of any Windows or Linux Server's snapshot page. It also displays the VMs virtual details.

Configuring Thresholds for VMware ESX and VMs

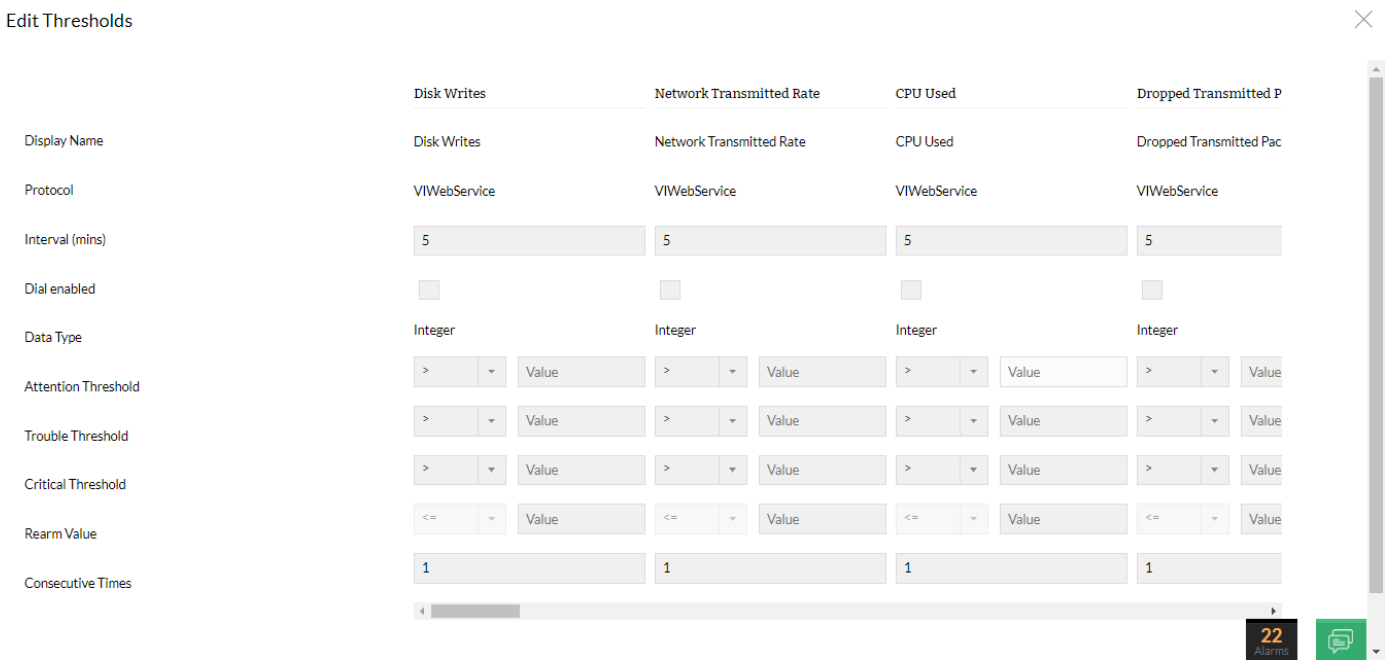
OpManager out-of-the-box offers monitoring templates for ESX hosts and VMs. The templates help you configure thresholds for multiple ESX hosts and VMs at one shot. For each performance metric you can configure Warning Threshold as well as Error Threshold, and receive proactive alerts if they are violated.

To configure the threshold value and apply the template

1. Go to **Settings ? Configuration ? Device Templates.**
2. You can find the **ESX Server** and **VMware Virtual Machine** templates for the hosts and VMs respectively. Click on the required template.



3. Click on the monitor name to enable or disable the threshold, and to modify Warning Threshold, Error Threshold and Rearm Values.



4. Click **OK**.

5. Click on **Save** to save the device template. Click on **Save & Associate** to save the device template and apply the changes to the devices associated to the template.
5. Click **Associate** for the devices to inherit the configurations in the template. Or, click **Associate & Overwrite** for the devices to remove the old and add the new configurations in the template.

Note: To edit the threshold values of a single ESX host, go its snapshot page and click the Monitors tab under Inventory Details. Click on the Edit icon of a monitor to edit its threshold values.

Managing VMware Alerts

OpManager fetches events from each VCenter / ESX Host, similar to SNMP traps. Currently we support important events, and this list is updated every release. Apart from these events, OpManager also monitors threshold for critical performance indicators and raises alerts.

To change the pre-set threshold values for each performance monitor, go to the monitors section under the snapshot page of the host / VM / Datastore.

To view the complete list of VMware monitors,

- Go to the **Monitors** tab in the VMware host's snapshot page.
- Under the **Performance Monitors** tab, click on the + sign. This will display a list of all performance monitors available in OpManager.
- To view the list of Performance monitors for VMware hosts alone, scroll down to the **VMware-Host Monitors** section.
- To view the list of Performance monitors for VMs, scroll down to the **VMware- VM Monitors** section.
- To view the list of Performance monitors for Datastore, scroll down to the **VMWare - Datastore Monitors** section.
- You can also view and add the performance monitors for hosts / vms by clicking on '**Add Monitors**' under their corresponding Device Templates.

Table 1: List of few Threshold Monitors for critical performance indicators related to host, datastore & VM's supported by OpManager

S.No.	Threshold Monitors	Virtual Device Type	Resource	Severity
1.	Host connection Status	Host	General	=2 (notresponding) - Critical =1 (disconnected) - Warning
2.	Host Data Received (avg)	Host	Network	>1000000 KBps - Critical >800000 KBps - Warning
3.	Host Data Transmission (avg)	Host	Network	>1000000 KBps - Critical >800000 KBps - Warning
4.	Host Network Usage (avg)	Host	Network	>4000000 KBps - Critical >3600000 KBps - Warning
5.	Host CPU Utilization (avg)	Host	CPU	> 90% - Critical > 85% - Warning
6.	Host Memory Utilization (avg)	Host	Memory	> 90% - Critical > 85% - Warning
7.	Host Disk Read Latency	Host	Disk	> 50ms - Critical > 45ms - Warning
8.	Host Disk Write Latency	Host	Disk	> 50ms - Critical > 45ms - Warning
9.	Datastore Freespace	Host	Network	< 5GB - Critical < 10GB - Warning
10.	VirtualMachine Data Received (avg)	VM	Network	>125000 KBps - Critical >100000 KBps - Warning
11	VirtualMachine Data Transmitted (avg)	VM	Network	>125000 KBps - Critical >100000 KBps - Warning

12.	VirtualMachine Network Usage (avg)	VM	Network	>250000 KBps - Critical >200000 KBps - Warning
13.	VirtualMachine CPU Usage (avg)	VM	CPU	> 90% - Critical > 85% - Warning
14.	VirtualMachine Memory Usage (avg)	VM	Memory	> 90% - Critical > 85% - Warning

Table 2: Few of the VCenter / ESX hosts' Events supported by OpManager

S.No.	Events	Virtual Device Type	Severity
1.	VmFailedToPowerOffEvent	VM	Major (Cleared on event 2 or 3)
2.	VmPoweredOffEvent	VM	Clear
3.	VmPowerOffOnIsolationEvent	VM	Clear
4.	VmFailedToPowerOnEvent	VM	Major (Cleared on event 5)
5.	VmPoweredOnEvent	VM	Clear
6.	VmFailedToSuspendEvent	VM	Major (Cleared on event 7)
7.	VmSuspendedEvent	VM	Clear
8.	VmFailedToRebootGuestEvent	VM	Major (Cleared on event 9)
9.	VmGuestRebootEvent	VM	Clear
10.	VmFailoverFailed	VM	Critical (Cleared on event 11)
11	VmPrimaryFailoverEvent	VM	Clear
12.	VmUpgradeFailedEvent	VM	Major (Cleared on event 13)
13.	VmUpgradeCompleteEvent	VM	Clear
14.	VmDisconnectedEvent	VM	Warning (Cleared on event 15)
15.	VmConnectedEvent	VM	Clear
16.	VmDiskFailedEvent	VM	Major
17.	VmRelocatedEvent	VM	Clear
18.	VmRelocateFailedEvent	VM	Critical (Cleared on event 17)

You can view the complete list of ESX host / VCenter Events that are supported by OpManager, under **Settings -> Monitors -> VMware Events.**

Note: OpManager only triggers alarms based on VMware events, and they have to be manually cleared once the issue/notification has been taken care of.

Notifying VMware Alerts

Notification profiles help you to notify when any alert is raised for virtual devices. The notification can be a sound alert/ email alert/ running a script etc. You can associate any of the notification profiles that is already created for the VCenter / ESX host. To associate a notification profile to a virtual device,

1. Go to the snapshot page of the host.
2. Click on **Notification** icon present at the top.
3. If no profiles are associated. Then click on 'Associate' to view the list of notification profiles already created.
4. Select the notification profile that you want to associate and click **Associate**.

You can create a notification profile specifically for receiving alerts on events related to Virtual devices using the following steps :

- Go to **Settings -> Notifications -> Add Profile.**
- Select the required mode of notification (email / sms / web console etc) and fill in the required fields. Click here to know more about setting up notification profiles generally.
- Click on next.
- Scroll down to the section that says "**When any Virtual Devices has a problem**". Click on it and select the situations for which you wish to get alerted.
- You can get alerted either for General Alarms (like VM Power on / off, VM Failover failed, Host disconnect failed etc) or for virtual device related performance issues (such as threshold violations) .
- Click on Next and continue the steps followed to setup a notification profile (click here to view the complete list of steps required for setting up notification profile.)

Monitoring Hyper-V Host and VMs

OpManager aids in comprehensive Hyper-V monitoring via WMI. It provides separate dashboard for Hosts and VMs, to have a quick view on its performance. It also offers a dedicated Snapshot page for the Hyper-V host, which provides comprehensive data such as Health, Inventory, Performance Reports, etc.

Some highlights of monitoring Hyper-V servers with OpManager:

- Monitors effective utilization of critical resources like CPU, Memory, Network and Disk
- Out-of-the-box offers 50 reports on Host and VMs
- Automatically maps the migrated VMs to the corresponding Hosts

Apart from monitoring the Hosts and VMs, OpManager also monitors the Key Performance Indicators (KPIs) of guest OSs. Similar to that of any Windows or Linux server, OpManager monitors the applications, Windows & TCP services, processes running on the VMs using WMI/SNMP.

Discovering Hyper-V Servers in OpManager

To discover the Hyper-V host and VMs, you just need to provide the IP address and WMI credentials of Hyper-V host. The VMs are automatically discovered along with the host.

Steps to discover the Hyper-V host and VMs:

Before proceeding to discover the host and VMs, ensure that you have configured the credentials for both the host and VMs in the credential library. To discover the host and VMs:

1. Go to **Settings** ? **Discovery** ? **Add Device**.
2. Enter the **Host Name / IP Address.**
3. Enter the correct **Netmask** and select the appropriate **credentials**.
4. Click **OK** button to add the host.

If any of the VMs are already discovered or added, OpManager automatically maps them as Virtual Device.

Note: If the device has been added successfully, but not displayed under the 'Virtualization' tab. Search for that device. Upon finding the particular device, Go to its snapshot page and look for the device type. If it is mentioned as 'unknown', wrong credentials might have been provided or it is not reachable during discovery. Provide the correct credentials and click on 'Rediscover Now' present under three-line menu at the top right corner in the snapshot page, to discover it as an Hyper-V host.

To learn more about Hyper-V monitoring, click here.

Configuring Thresholds for Hyper-V Host and VMs

OpManager out-of-the-box offers monitoring templates for Hyper-V hosts and VMs. The templates help you configure thresholds for multiple hosts and VMs at one shot. The process is similar to that of configuring threshold to monitors available for Windows/Linux servers.

To configure the threshold value and apply the template

1. Go to **Settings ? Configuration ? Device templates.**
2. You can find the **HyperV Server** and **HyperV Virtual Machine** templates for the hosts and VMs respectively. Click on the required template.
3. Click on **Edit Thresholds** button to configure the threshold and rearm value for the required monitors.
4. Click **OK**.
5. Click **Associate** for the devices to inherit the configurations in the template. While associating the template, click on **Apply & Overwrite** for the devices to remove the old and add the new configurations in the template.

Note: To edit the threshold values of a single host, go its snapshot page and click the Monitors tab under Inventory Details. Click on the Edit icon of a monitor to edit its threshold values.

Managing Hyper-V Alerts

OpManager monitors Hyper-V host and VM similar to that of any Windows server. Upon clicking the monitors tab in the host snapshot page, the monitors listed for a Windows server is listed here. You can add the required monitors and configure thresholds. If the threshold is violated, OpManager raises an alarm.

Notifying Hyper-V Alerts

Notification profiles help you to notify when any alert is raised for virtual devices. The notification can be a sound alert/ email alert/ running a script etc. You can associate any of the notification profiles that is already created for the Hyper-V host.

Click here to know how to create a new notification profile.

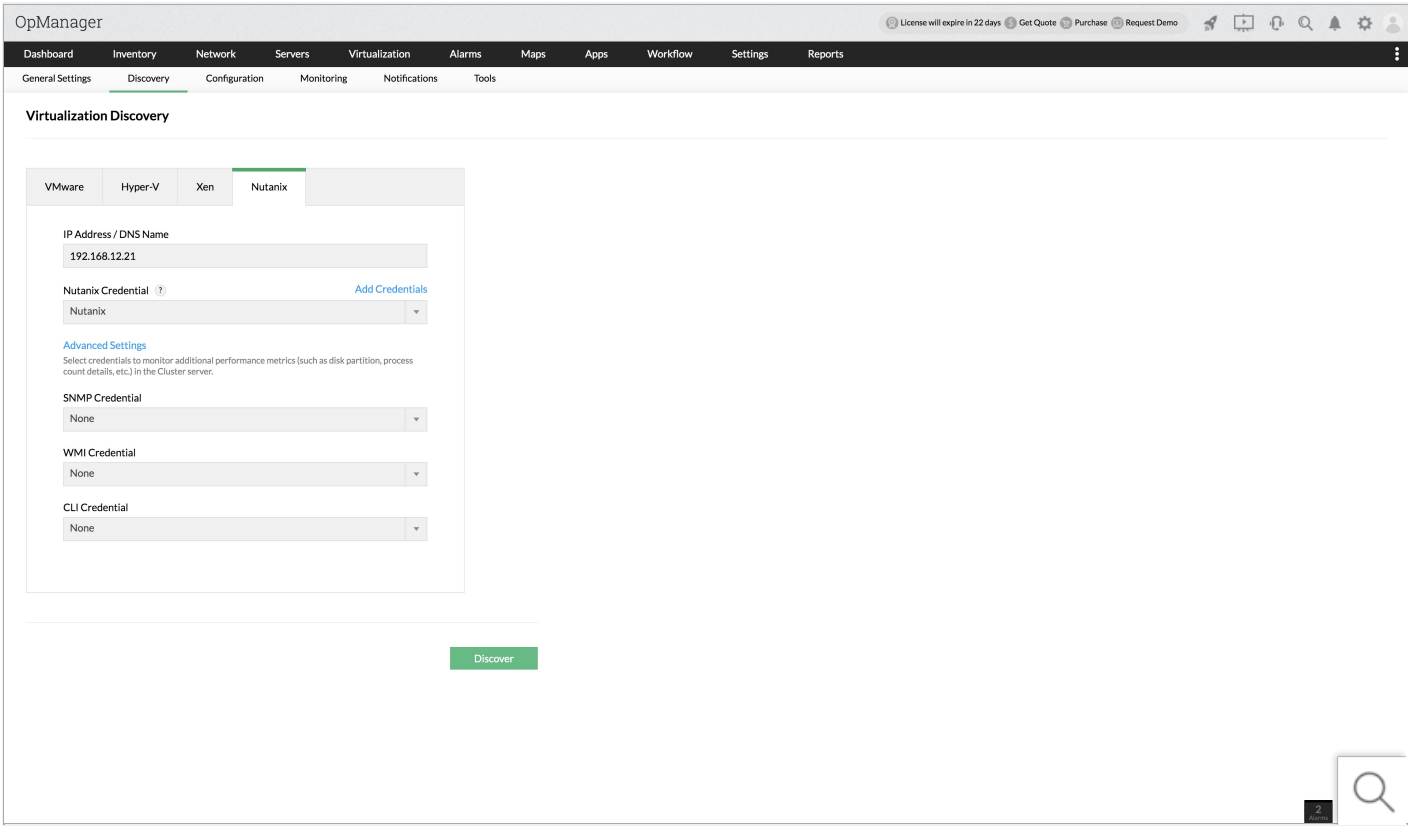
Discovering Nutanix clusters in OpManager

Nutanix is a vendor of distributed computing and storage virtualization solutions, specialising in an area called 'Hyperconverged Infrastructure'. Basically, the idea is to provide an all-inclusive virtual environment, including the storage component of the VM itself. This is to enable data requests to be handled inside the VM itself instead of being sent to an external storage, and so the latency for data retrieval and access reduces to a negligible level.

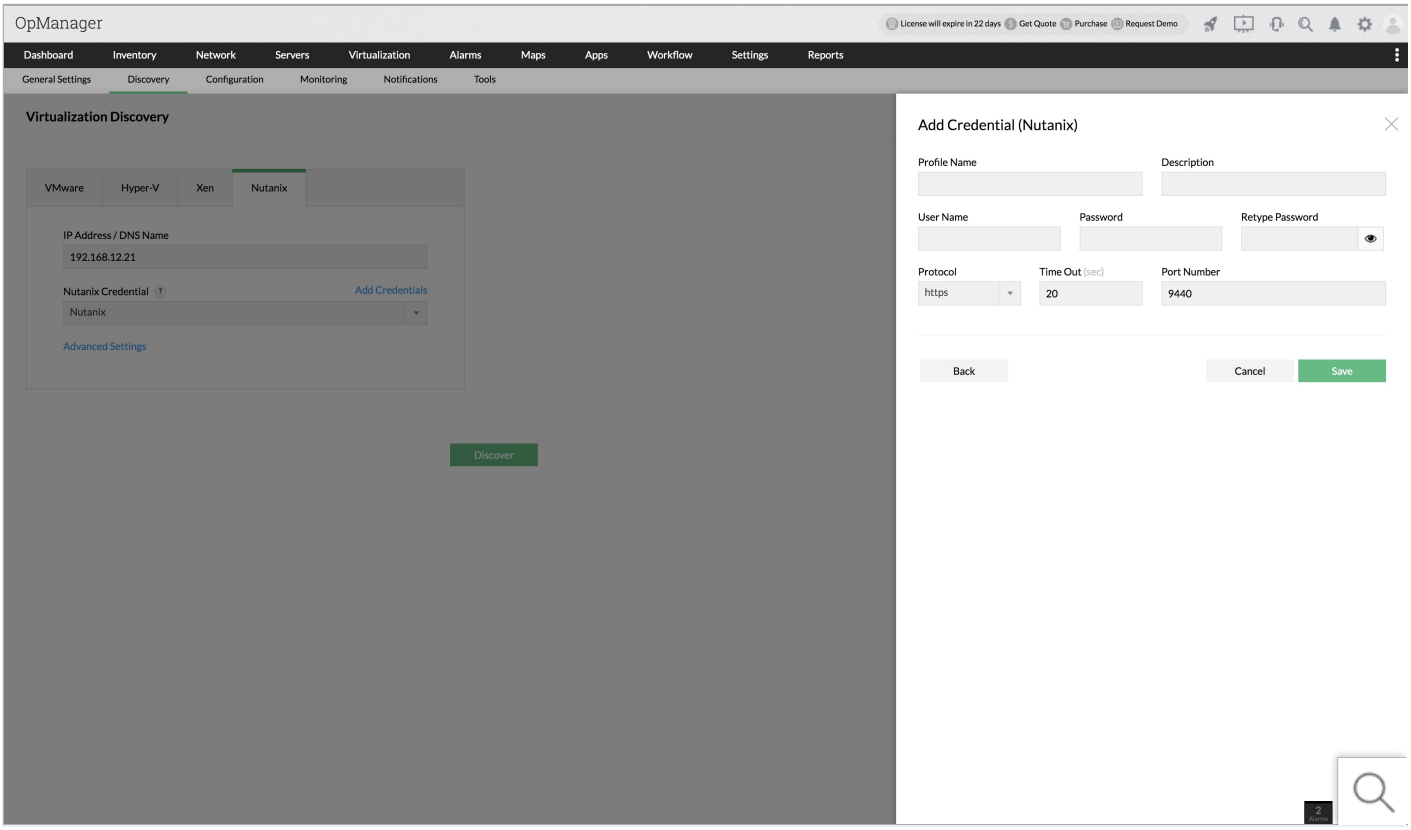
OpManager makes use of the **Prism API** framework to fetch performance metrics from the devices in the Nutanix environment.

Discovering your Nutanix cluster into OpManager

1. Go to Settings ? Discovery ? Add Nutanix. You can also go to Settings ? Virtualization discovery and select the Nutanix tab.
2. Enter the IP address. The IP address of the Nutanix cluster is to be provided here.



3. In the credentials field, select the credentials of the cluster. If you haven't already added it, you can click on 'Add Credentials' and create a credential profile right away. Click on 'Add Credentials', select 'Nutanix' and provide the following details:
    1. Profile name (mandatory): A name for the credential profile
    2. Description: A short description for the credential profile
    3. Username (mandatory): The username of the Prism element used to manage the Nutanix environment.
    4. Password (mandatory): Password of the Prism element.
    5. Protocol (mandatory): Select http/https, based on your requirement.
    6. Time out (mandatory): The time out threshold for the connection. The default value is **20 seconds.**
    7. Port number (mandatory): The port number on which the Prism element is running. The default value is **9440.**



4. Once you have provided all these details, click **'Save'** to create the credential profile.
5. If you want to monitor your cluster OS more intensively for other performance metrics, just click on **'Advanced settings'** and select the necessary credential profiles (either of these - SNMP, WMI or CLI).
6. Once you've provided all these basic details, click on **'Discover'** to start discovering the elements in your Nutanix network.
7. In the next window, all the Hosts and the VMs under that cluster are listed. You can simply choose which elements you want to be monitored by checking them. Once done, click **'Next'.**
8. If you want to perform in-depth monitoring of your Hosts/VMs based on other protocol (SNMP / WMI / CLI), you can select which credentials you want to use for the same in the following **'Select Credentials'** window.
9. You can also choose whether or not you want to auto-discover new VMs under this cluster by enabling or disabling the **'Discover new VMs automatically'** option. Once you're done, click **'Discover'.**
10. The Nutanix discovery is now initiated, and OpManager adds all the selected elements using the chosen credentials. You can view the progress of the discovery in the discovery progress bar in the bottom-right corner of the window.
11. Once discovered, click on **Virtualization** and go the Nutanix tab to view all the clusters, hosts and VMs that have been discovered into OpManager.

Introduction to Storage Monitoring

OpManager helps you to efficiently monitor and manage all your storage devices with the storage monitoring add-on. Now, monitor your RAID and Tape Libraries, get forecasts on usage of storage space and manage your FC switches proactively with OpManager.

Some of the key features in the storage monitoring add-on are:

- Monitor your storage devices such as **RAIDs and Tape Libraries**
- Manage **FC (Fiber Channel) switches** in your Storage Area Network
- Get notified of issues in real-time with instant mobile and email notification.
- Know the overall picture of your network storage through extensive reports.

Note: Before you proceed with the installation, make sure you check out the prerequisites of the installation.

Supported devices for storage monitoring

Below is the list of supported vendors and the respective devices for storage monitoring in OpManager.
If you couldn't find a device, send us a request here so that we can extend support to your storage device.

- Dell EMC storage devices
- HP storage devices
- IBM storage devices
- Infinidat storage devices
- NetApp storage devices
- Hitachi storage devices
- Huawei storage devices
- InforTrend storage devices
- Promise storage devices
- Storage devices from other vendors

Prerequisites to add storage devices

The list of storage devices that are monitored by OpManager and their respective supported models, features supported and prerequisites for monitoring are listed below.

SAN Switches	Storage Arrays	Tape Libraries
• Brocade Silkworm Series • McData Sphereon series • EMC Connectrix • Cisco MDS series • QLogic SANbox • HP Switches	• IBM ESS • HP MSA • HP EVA • EMC CLARiiON • Infortrend • NetApp • Hitachi Lightning • Hitachi Thunder • Huawei Storage • IBM DS4000 / FastT • StorageTek / LSI Logic • SUN StorEdge • Areca RAID • EMC Centera • IBM Spectrum Virtualize	• HP ESL / HP EML • DELL • IBM 3584 / TS 3310 / TS 3500 • Overland Neo • ADIC Scalar • StorageTek • Qualstar • Quantum • Tandberg • SUN StorEdge

Monitoring Brocade switches & directors

OpManager provides monitoring and management of Brocade silkworm switches and directors.

Models Supported

- Brocade SilkWorm switches
  - SilkWorm 4100
  - SilkWorm 4102
- All the rebranded models or OEM models are supported.

Features Supported

- Inventory information for switch & switch ports
- Switch ports monitoring
- Reports:
  - Switch zoning configuration report
  - Availability reports for switch & switch ports

- Performance reports for switch Ports
    - Bandwidth Utilization
    - Errors
    - Rx Traffic
    - Rx Utilization
    - Tx Traffic
    - Tx Utilization
- Switch summary reports

- Real time graphs for trouble shooting
- SNMP trap based alarms
- Launch of telnet/applet brocade client for configuration

Prerequisites for Monitoring

- Ensure SNMP agent is running in the Brocade silkworm switch/director.
- By default, OpManager uses SNMP port 161 and read community 'public' for discovery. If your settings are different , please provide the same in the OpManager web-client while adding Switch.
- Ensure that the IP of the server running OpManager is included in the the **SNMP access list**of the Brocade Switch.
    - The following command can be used to know the snmp community & access list configurations in brocade silkworm switches.
      Run the command**&#65533;** **agtcfgdefault** via CLI**&#65533;** console of the switch.
      Details: Refer the "Brocade Fabric OS Reference Manual"
- Register OpManager server IP address as a trap destination for the Brocade Silkworm Switch.
    - Use **agtcfgset** command in the Brocade Fabric OS command line interface to specify the Trap Recipient.

Note: For more details refer the Brocade Fabric OS Reference Manual

Note:&#65533; In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try re-adding the device.

Monitoring McData switches / directors

OpManager provides monitoring and management of McData switches and directors like Sphereon / Intrepid etc.

Models Supported

- &#65533; Sphereon 4500 Fabric Switch
- &#65533; Sphereon 3216 Fabric Switch
- &#65533; Sphereon 3232 Fabric Switch
- &#65533; ES-3016 switch
- &#65533; ES-3032 switch
- &#65533; ES-1000 switch

- • Intrepid 6064 Director
- • Intrepid 6140 Director
- • ED-6064 director
- • ED-5000 director

Features Supported

- Complete inventory information for switch & switch ports
- Switch ports monitoring
- Reports:
  - Availability reports for switch & switch ports
  - Performance reports for switch Ports
    - Errors
    - Rx Traffic
    - Rx Throughput
    - Tx Traffic
    - TxThroughput
    - Total Throughput
  - Switch Port summary reports
- Real time graphs for trouble shooting
- SNMP trap based alarms
- Launch of Telnet/web client for configuration

Prerequisites for Monitoring

- Ensure SNMP agent is running in the McData switch / director. McData Switch SNMP information can be checked in the McData Switch's Web-based• interface -> Configure (option)• -> SNMP• (option).
- By Default, OpManager uses SNMP port 161 and read community 'public' for discovery. If your settings are different , please provide the same in the OpManager web-client while adding Switch.
- Register OpManager server IP address as trap destination.
- For details refer Configure SNMP section in the **McData Switch Product Manager** user manual.

Note: In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try readding the device.

Monitoring EMC switches / directors

OpManager provides monitoring and management of EMC switches and directors.

Models Supported

- EMC Connectrix switches
- EMC Connectrix directors

Features Supported

- Inventory information of switch & switch ports
- Switch ports monitoring
- Reports:
  - Availability reports for switch & switch ports
  - Performance reports for switch Ports
    - Errors
    - Rx Traffic
    - Rx Throughput
    - Tx Traffic
    - Tx Throughput
    - Total Throughput
  - Switch Port summary reports
- Real time graphs for trouble shooting
- SNMP trap based alarms
- Launch of Telnet/Applet EMC client for configuration

Prerequisites for Monitoring

- Ensure SNMP agent is running in the EMC Switch / director.
- By default, OpManager uses SNMP port 161 and read community 'public' for discovery. If your settings are different, please provide the same in the OpManager web-client while adding Switch.
- Register OpManager server IP address as a trap destination for the EMC Switch.

Note: In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try re-adding the device.

Monitoring Cisco MDS switches / directors

OpManager provides monitoring and management of Cisco MDS 9000 Series SAN Switches.

Models Supported

- Cisco MDS 9000 Series Switches such as Cisco MDS9216i
- Cisco SN 5428-K9 Storage Router

Features Supported

- Inventory information of switch & switch ports
- Cisco VSAN information
- Switch ports monitoring
- Reports:

- Availability reports for switch & switch ports
- Performance reports for switch Ports
    - Bandwidth Utilization
    - Port Frame Error Rate
    - Port In Drop Rate
    - Port Out Drop Rate
    - Rx Utilization
    - Rx Throughput
    - Tx Utilization
    - Rx Throughput
    - Total Throughput
- Switch Port summary reports

- Real time graphs for trouble shooting
- SNMP trap based alarms
- Remote launch of CLI to facilitate device configuration

Prerequisites for Monitoring

- OpManager by default uses 'public' snmp community for discovery. This community should have read access right. In case your read community is different , please provide the same in the OpManager web-client while adding Switch.. You can check the community names (and their access rights) configured in your MDS switch by issuing the command "**show snmp community**" via telnet to switch
    - To set the access rights for a community in your cisco switch , you need to do the following ,
        - Go to config mode , by typing the command ,
            - **config t**
        - Set the snmp community by typing the command,
            - **snmp-server community <community> <rw | ro>**
                - For example, to set read-only access right to "public" community you can type ,
                    - snmp-server community public ro

- Register OpManager server IP address as a trap destination for the Cisco Switch.
    - Check if the server running OpManager is registered as a trap destination in the switch by issuing the command "**show snmp host**" via telnet to switch. This should have an entry with OpManager server IP and port 162
    - If entry is not available, use **snmp-server host <host_address>traps** command to specify Trap Recipient.

Note: For more details check Cisco MDS 9000 Family Command Reference Guide.

Note: In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try re-adding the device.

Monitoring QLogic switches

OpManager provides monitoring and management of QLogic SANbox switches.

Models Supported

- SANbox2-64
- SANbox 5600
- SANbox 5200
- SANbox 3050
- SANbox Express 1400

Features Supported

- Inventory information of switch & switch ports
- Switch ports monitoring
- Reports:
  - Availability reports for switch & switch ports
  - Performance reports for switch Ports
    - Errors
    - Tx Traffic
    - Rx Traffic
    - Tx Throughput
    - Rx Throughput
    - Total Throughput
  - Switch port summary reports
- Real time graphs for trouble shooting
- SNMP trap based alarms
- Launch of telnet / QLogic client for configuration

Prerequisites for Monitoring

- Ensure SNMP agent is running in the QLogic SANbox Switch. To view the SNMP settings, use the QLogic Switch telnet command "**show setup snmp**". For any changes use "**set setup snmp**". (Refer "QLogic Switch Management User's Guide" for details.)
- OpManager by default, uses snmp port 161 and read community 'public' for discovery. If your settings are different , please provide the same in the OpManager web-client while adding Switch.
- Register OpManager server IP address as a snmp trap destination for the QLogic Switch.

Note: In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try readding the device.

Monitoring HP switches / directors

OpManager provides monitoring and management of HP Storageworks switches and directors.

Models Supported

- HP storageworks switches
- HP storageworks directors

Features Supported

- Inventory information for switch & switch ports
- Switch ports monitoring
- Reports:
  - Switch zoning configuration report
  - Availability reports for switch & switch ports
  - Performance reports for switch Ports
    - Errors
    - Rx Traffic
    - Rx Throughput
    - Tx Traffic
    - Tx Throughput
    - Total Throughput
  - Switch Port summary reports
- Real time graphs for trouble shooting
- SNMP trap based alarms
- Launch of telnet/applet HP client for configuration

Prerequisites for Monitoring

- Ensure SNMP agent is running in the HP storageworks switch / director.
- By default, OpManager uses snmp port 161 and read community 'public' for discovery. If your settings are different , please provide the same in the OpManager web-client while adding Switch.
- Register OpManager server IP address as a trap destination for the HP StorageWorks Switch.

Note: In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try readding the device.

Monitoring IBM ESS Shark Storage Systems

OpManager provides monitoring and management of IBM ESS Shark series storage systems.

Models Supported

- DS6000 Series
- DS8000 Series
- ESS 2105-800

- ESS 2105-750
- ESS 2105-F20

Features Supported

- Inventory information of physical components
  - Array Controllers, Array controller Ports
  - Disk Drives
- Logical configuration details
  - Storage Pools
  - Storage Volumes
  - Intercocnnects Info
- Monitoring
  - Array system status
  - Array controller status
  - Disk drive status, Storage Pools Status, Storage Volumes status
- Reports:
  - Availability reports for storage system, RAID controller & RAID controller ports

Prerequisites for Monitoring

- OpManager uses the IBM Common Information Model (CIM) Agent for ESS to monitor the IBM ESS Shark Array
- The IBM ESS CIM agent can be installed on any server that is pingable from the server where OpManager is installed.
- IBM CIM agent install requires **esscli** utility is already installed in the server
- Install the necessary software from the OEM website.
- Disable DigestAuthentication by setting **DigestAuthentication** flag to false in **cimom.properties** file
  Note : Default directory is C:\Program Files\IBM\cimagent
- Start the ESS Provider service **CIM Object Manager - DS Open API** from the Windows services menu
- Ensure that, OpManager installed host and the Storage system has a Fibre Channel Connectivity.

Note: In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try re-adding the device.

Monitoring HP Modular Storage Arrays

OpManager provides monitoring and management of HP Modular Storage Arrays.

Models Supported

- HP MSA 1000
- HP MSA 1500

Features Supported

- Inventory information of physical components ,
  - Array Controllers, Array controller Ports
  - Disk Drives
- Logical configuration details
  - Storage Pools
  - Storage Volumes
  - Intercocnnects Info
- Monitoring
  - Array system status
  - Array controller status
  - Disk drive status, Storage Pools Status, Storage Volumes status
- Reports:
  - Availability reports for storage system, RAID controller & RAID controller ports

Prerequisites for Monitoring HP MSA Array

- OpManager uses the HP SMI-S MSA Provider based on SNIA standard to monitor the HP MSA
- The MSA provider can be installed on any server running Microsoft Windows 2000 or Windows 2003 Server.
- This server must have a path through the SAN to the MSA devices that will be managed.
- Also the server must be reachable from the server where OpManager is installed.
- Install the necessary software from the OEM website.
- Ensure that MSA firmware version is compatible with the installed SMI-S provider (latest download corresponds to SMI v1.0.3).
- Start the MSA Provider service **hp StorageWorks SMI-S CIMOM** from the Windows services menu.

Note: In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try readding the device.

Monitoring HP StorageWorks Enterprise Virtual Array

OpManager provides monitoring and management of HP StorageWorks Enterprise Virtual Array.

Models Supported

- HP StorageWorks EVA 3000,4000,5000,6000,8000

Features Supported

- Inventory information of physical components
  - Raid Controllers

    - Raid Controller Ports
    - Disk Drives
- Logical configuration details
    - Storage Volume
    - Storage Pool
    - Interconnects Info
- Monitoring
    - Disk Drive status
    - Raid Controller status
    - Raid Controller Port status
- Reports:
    - **Performance reports** for HP EVA arrays (via **evaperfutil**utility)
        - Array Statistics
            - Total Host Req/s, Total Host MB/s
        - Array Controller Statistics
            - CPU %, Data %
        - Virtual Disks
            - Read Hit MB/s, Read Hit Latency(ms), Read Hit Req/s, Read Miss Req/s, Read Miss MB/s, Read Miss Latency, Write Req/s, Write MB/s, Write Latency(ms), Flush MB/s, Mirror MB/s,
        - Host Port Statistics
            - Read Req/s, Read MB/s, Read Latency(ms), Write Req/s, Write MB/s, Write Latency (ms), Av. Queue Depth
        - Physical Disks
            - Disk Queue Depth, Drive Latency(ms), Read Req/s, Read MB/s, Read Latency (ms), Write Req/s, Write MB/s, Write Latency(ms)
        - Physical Disk Groups
            - Total Read Req/s, Total Read MB/s, Average Read Latency(ms), Total Write Req/s, Total Write MB/s, Average Write of Latency(ms), Total Flush Bytes, Total Mirror Bytes, Total Prefetch Bytes
    - Availability reports for Raid Controller & Raid Controller ports
- Threshold monitoring for Disk Drive Temperature , Power Supply status

Prerequisites for Monitoring HP StorageWorks EVA

OpManager monitors HP EVA based on the Command View EVA(CV EVA) version installed in the your environment.

A) SSSU Installation Instructions

OpManager uses SSSU (Storage System Scripting Utility) available as part of HP StorageWorks Windows Kit for Enterprise Virtual Array installation.

- This needs to be installed in the server where OpManager is installed and running
- Ensure that "SSSU.exe" is included in the **PATH** environment variable in the server in which OpManager is installed. (You can check this by executing SSSU.exe in a command prompt which will print the version) .

Note: In case your current SSSU version is higher (say 5.0) , you need to download SSSU.exe (Version 4.0) and include it in the %PATH%. For this you may follow the steps below,

1. Open the HP software download URL, HP Software Download Page
2. Click on "HP StorageWorks Command View EVA V4.0 Media Kit". This will open a page which lists the supported Operating Systems
3. Click on the operating system corresponding to the server running OpManager (Example: Windows 2003)
4. Click on the "Download" button corresponding to the "HP StorageWorks Storage System Scripting Utility (SSSU) v4.0". This will download SSSU.exe

Steps to add the HP EVA into OpManager (using SSSU)

- After including SSSU utility in the %PATH% environment variable, restart OpManager (shutdown & start). This is required for the Environment PATH settings to take effect.
- In the OpManager browser client go to Admin tab --> Manage Storage Devices option.
- In the "IP Address" field enter the Management_Appliance_IP_address (The IP address of the HP Management Appliance that is managing the HP EVA array)
- Choose Device Type as Raid
- Choose Vendor as HP
- Choose Model as "EVA(Below 6.0)"
- Provide the Administrator Username, Password and the Community String
- Click on Add Device.

B) EVA SMI Provider Installation Instructions

- OpManager uses the HP SMI-S EVA Provider (SNIA standard) to monitor the HP EVA (Command View EVA version 6.0.2 and above) The HP SMI-S EVA Provider is integrated with Command View EVA.
- Install the necessary software from the OEM website.
- Ensure that EVA firmware version is compatible with the installed SMI-S provider
- Check the SMI service say like, **HP StorageWorks SMI-S CIMOM** or **HP StorageWorks CIM Object Manager** is listed in Windows Services of the Command View EVA Host.
- Now start the service

Steps to add HP EVA into OpManager (using SMI-S)

- Ensure that SMI provider is properly started and is listed in Windows Services Panel
- Restart OpManager (shutdown & start). This is required for the Environment PATH settings to take effect.

- In the OpManager client go to Admin Tab -->Manage Storage Devices
- Provide IP Address of the host in which SMI-S Provider is running
- Choose Device Type, Vendor and Model as RAID, HP and EVA(Above 6.0) respectively
- In Username field enter the EVA Provider username
- In the Password field enter the EVA Provider password
- Provide the Port number at which the CIM Agent is running(5989 or 5988)
- Choose whether the SSL should be Enabled(https) or Disabled(http)
- Provied the name space (by default root/eva)
- Change the Timeout if needed.
- Click on Add Device

Note: If the Ping option is disabled for the device, then please uncheck 'Ping the given IP' field.
Note: In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try readding the device.

C) evaperf Installation Instructions

For Performance monitoring, **evaperf** utility needs to be installed in the server running OpManager.

Ensure that, the evaperf utility installed host and the CommandView EVA running host are connected via Fibre Channel.

1. Include evaperf in the PATH environment variable
2. Ensure that the installed EvaPerf utility is compatible with EVA firmware version.
3. Ensure that **evapdcs** (EVA Performance Data Collection Service) is installed along with evaperf by executing the command "**evapdcs -v**"
    - If it prints "evapdcs is currently installed" , you may check its startup status in the Windows "Services" menu . This service is registered with the name "HP EVA Performance Data Collector". (If the status is "disabled", it indicates that it is in an improper state and you will need to restart the host server once and then check the above again)
    - In case the above command prints "evapdcs not installed" , install evapdcs via the following command **evapdcs -i -m**
4. The server running OpManager needs to be registered to the Command View EVA server via , **"evaperf fnh [hostname] [username] [password]"**
   hostname - CVE host name , username - CVE username , password - CVE password
5. OpManager uses EVA name (known as friendly name in EVA terminology) to issue evaperf commands. For this the EVA name - WWN mapping needs to be registered via **"evaperf fn"** command
6. If the EVA is password protected, the EVA password needs to be registered for the respective EVA WWN via **"evaperf spw array_WWN array_Password"** command
7. You can check if evaperf is able to fetch valid data by entering the following command in the OpManager/ directory ,
    - **evaperf all -sz <EVA Name> -csv -nots** (This will automatically start evapdcs service, if it is not started already) . This should print all the EVA performance statistics (for Array, VDisk , Disk etc).
    - The sample output should look similar to the one given below : CPU %,Data %,Ctlr,Serial,Node
      82,81,A,V8398ADVBP2003,5065-1FD1-5021-8781
      94,99,B,V8398ADVHV200D,5060-1FF1-5031-8582

Note: Installation details for evaperf are available in the HP StorageWorks Command View EVA installation guide.

Monitoring EMC CLARiiON Networked Storage System

OpManager provides monitoring and management of EMC CLARiiON Networked Storage Systems.

Models Supported

- CX Series like CX3-20, CX3-40, CX3-80, CX300, CX500, CX700 & CX800
- FC Series like FC4700

Features Supported

- Inventory information of physical components ,
  - Storage Processor (SP)
  - SP Ports
  - Disk Drives
- Logical configuration details
  - LUNs
  - RaidGroups
  - Host-Port mapping
  - InterConnects Info
- Monitoring
  - SP status
  - SP Port status
  - Free space of Disk Drives / Raid Groups /LUNs
- Reports:
  - Performance
    - Storage Processors
      - Utilization, Total Bandwidth, Total throughput, Read Bandwidth, Read Size, Read throughput, Write Bandwidth, Write Size, Write throughput, Dirty Pages, Flush Ratio, Mbs Flushed,&#65533; Idle Flush On, High Water Flush On, Low water Flush Off, Write Cache Flushes
    - Disk Drives
      - Total Bandwidth, Total throughput, Read Bandwidth, Read Size, Read throughput, Write Bandwidth, Write Size, Write throughput, Disk Service Time
    - LUNs
      - Read Bandwidth, Read Size, Read throughput, Write Bandwidth, Write Size, Write throughput, Read Cache Hits, Read Cache Hit Ratio, Write Cache Hits, Write Cache Hit Ratio, Forced Flushes.
  - Availability reports for SP & SP ports
- SNMP trap based alarms

Prerequisites for Monitoring EMC CLARiiON

- **NaviCLI** should be installed in the server in which OpManager is installed.
- Include the directory containing NaviCLI.exe in the **PATH** environment variable. (This is normally C:\Program Files\EMC\Navisphere CLI\ ).
- Ensure that OpManager is restarted (shutdown & started) after including NaviCLI in the path.&#65533; This is required for the latest path changes to take effect for OpManager.
- Now open a command prompt to execute the navicli command to check for the proper response from EMC CLARiiON RAID.
    - Command: **navicli -h <array name> getall**
- For Performance monitoring, please ensure that setStats flag is enabled. You can enable the same using NaviCLI command
    - Command : **NaviCLI -h <array-ip> setstats -on**

Note: In case the device is not discovered, then the probable reasons for non-discovery are displayed in the client. Please go through the instructions and try re-adding the device.

&#65533;

Monitoring Infortrend EonStor Storage System

OpManager provides monitoring and management of Infortrend EonStor Storage System.

Models Supported

EonStor storage systems such as,

- A16F-G2422
- A24F-R2224
- A24F-G2224
- A16F-R2221
- A16F-G2221
- A16F-R/S1211
- A12F-G2221
- A08F-G2221
- A16U-G2421
- A12U-G2421
- A08U-G2421
- A08U-C2412
- A08U-C2411
- U12U-G4020
- F16F-R/S2021
- F12F-G2A2
- FF-R/S2021-4/6
- S16F-R1430
- S16F-G1430

- All the rebranded models or OEM models are supported.

Features Supported

- Inventory information of physical components ,
  - RAID Controllers
  - RAID Controller&#65533; Ports
  - Channels
  - Disk Drives
- Logical configuration details
  - LUNs
  - Raid Partitions
  - Logical Volumes
  - Logical Drives
- Monitoring
  - RAID Controller status
  - RAID Controller port status
  - Fan, Power supply, UPS, &#65533; Battery, Temperature Sensor, Voltage status, Door status, Speaker status
- Reports:
  - Performance
    - CurrentQueuedIOCount,CurrentLunNumber,CurrentAccessDelayTime
    - CurrentTagCount,CurrentIOTimeOut,CurrentDriveCheckPeriod
    - CurrentSAFTEPollingPeriod,CurrentAutoDetectPeriod
  - Availability reports for storage system, RAID Controller & RAID Controller ports

Prerequisites for Monitoring

- Ensure SNMP agent is running.
- Register OpManager server IP address as trap destination

Note :&#65533; In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try re-adding the device.

&#65533;

Monitoring NetApp Primary Storage series

OpManager provides monitoring and management of NetApp Primary Storage series System.

Models Supported

- FAS series like ,
  - FAS200
  - FAS250

- FAS270
- FAS270c
- FAS3000
- FAS 920
- FAS920c
- FAS940
- FAS940c
- FAS960
- FAS960c
- FAS980
- FAS980c
- FAS3000
- FAS3020

- F-500, F-600 & F-700 series like ,
  - F825c
  - F825
  - F210
  - F230
  - F520
  - F630
  - F720
  - F740
  - F760

- C Series like ,
  - C1200
  - C2100
  - C6200

Features Supported

- Discovers and displays NetApp Raid information including status parameters such as Global Status, Fan / Power supply status
- Monitors Volume usage including snapshots
- Monitors cluster status information when deployed in cluster configuration
- Receives SNMP Traps covering over 75 system and threshhold alerts
- Performance graphs
  - NFS/CIFS Ops/sec
  - NetRx/Tx Throughput
  - Disk Read Writes / sec , Tape Read Writes / sec
  - CacheAge

Prerequisites for Monitoring

- Ensure SNMP agent is running.
- Register OpManager server IP address as trap destination

Note:&#65533; In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try re-adding the device.

&#65533;

Monitoring Hitachi HDS Lightning 9900V&#65533; series storage systems

OpManager provides monitoring and management of HDS Lightning 9900V series storage System.

Models Supported

- Hitachi HDS Lightning 9900V series storage systems such as HDS Lightning 9970V & HDS Lightning 9880V&#65533;
- NSC55

Features Supported

- Inventory information of physical components
  - Disk Controllers,&#65533; Disk Units,&#65533; Disk Processor
  - Port Details
- Logical configuration details
  - LUNs
  - LUN Host Mapping
- Monitoring
  - Disk Controller status
  - Disk Unit status
  - Port Status
- Reports:
  - Availability reports
  - Capacity Summary
- Monitoring and alarm generation for faulty conditions (via SNMP traps)

Prerequisites for Monitoring

- Ensure SNMP agent is running.
- Register OpManager server IP address as trap destination

Note :&#65533; In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try re-adding the device.

Monitoring Hitachi HDS Thunder 9500V series storage systems

OpManager provides monitoring and management of HDS Thunder 9500V series storage system.

Models Supported

- Hitachi HDS Thunder 9500V series storage systems such as HDS Thunder 9570V & HDS Thunder 9585V
- Hitachi HDS TagmaStore

Features Supported

- Inventory information of physical components ,
  - RAID Controller
  - RAID Controller Ports
- Logical configuration details
  - LUNs
  - LUN Host Mapping
  - Interconnects Info
- Monitoring
  - RAID Controller status
  - RAID Controller Port status
- Reports:
  - Performance
    - LUNs
      - ReadCommandNumber,ReadHitNumber, ReadHitRate
      - WriteCommandNumber,WriteHitNumber,WriteHitRate
  - Availability reports for RAID, RAID Controller & RAID Controller ports
- Monitoring and alarm generation for faulty conditions (via SNMP traps)
  - Controller blockade
  - Drive blockade
  - Internal FCAL Loop failure
  - NAS server / path failures.
  - Battery/Fan alarms.
  - Other alarms defined in MIB

Prerequisites for Monitoring

- Ensure SNMP agent is running.

- Register OpManager server IP address as trap destination
- Refer the **SNMP Agent Support Function** user guide of **Hitachi Freedom Series Thunder 9500 V Series** for agent installation and configuration detail.

Note:&#65533; In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try re-adding the device.

&#65533;

Monitoring Huawei Storage Systems

OpManager supports monitoring and management of Huawei OceanStor storage devices

Models Supported

- Huawei OceanStor V3/V5 Series.
- Huawei OceanStor Dorado V3/V6 Series.

Pre-Requisites:

- Select 'Enable Performance Monitor' checkbox under Settings in the Huawei Storage UI to monitor the performance of Huawei storage devices with OpManager

&#65533;

Monitoring IBM FastT, DS4000 Storage Systems

OpManager provides monitoring and management of IBM FastT / DS4000 series storage systems

Models Supported

- IBM FastT series
- IBM DS4000 series

Features Supported

- Inventory information of physical components
  - RAID,&#65533; RAID Controller,&#65533; RAID Controller Ports
  - Disk Drives
  - Tray/Enclosure Component Health Information
- Logical configuration details
  - VolumeGroups
  - Volumes
  - VolumeLUN Mappings
  - Host Groups
  - Interconnects Info
- Monitoring
  - RAID status

- RAID&#65533; Port status
- Status of Volume Groups, Volumes & Disk Drives

- Reports:
  - Performance reports for DS4000 / IBM FastT Storage arrays
    - Includes reports for Controllers, Volumes and Array for the following stats (via SMcli utility),
      - Total IO Count
      - Read Percentage
      - Cache Hit Percentage
      - Current Data Transfer Rate
      - Maximum Data Transfer Rate
      - Current IO Count
      - Maximum IO Count
  - Availability reports for storage system, RAID controller & RAID controller ports
- Alarms
  - SNMP trap based alarms
  - Status alerts for Disk Drives, Volume Groups & Volumes

Prerequisites for Monitoring

- OpManager uses command line utility (**SMcli.exe**) available as part of IBM FastT / DS4000 Storage Manager installation
- Ensure that SMcli is installed in the server in which OpManager is installed.
  - Include the directory containing SMcli.exe in the **PATH**environment variable.
    - By default for Windows Servers this is *C:\Program Files\IBMFastT\client*
    - By default for UNIX Servers this is */opt/IBMFastT/client/*
- Ensure that OpManager is restarted (shutdown & started) after including SMcli in the path
- Register OpManager server IP address as snmp trap destination.
- Ensure that&#65533; the OpManager installed server and the Storage system are connected via Fibre Channel.

Note:&#65533; In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try readding the device.

&#65533;

Monitoring StorageTek Storage Systems

OpManager provides monitoring and management of StorageTek B-series & D-series storage systems.

Models Supported

- D Series
- B Series

- Flexline 200 series
- Flexline 300 series

Features Supported

- Inventory information of physical components ,
  - RAID,&#65533; RAID Controller,&#65533; RAID Controller Ports
  - Disk Drives
  - Tray/Enclosure Component Health Information
- Logical configuration details
  - VolumeGroups
  - Volumes
  - VolumeLUN Mappings
  - Host Groups
  - Intercocnnects Info
- Monitoring
  - RAID status
  - RAID&#65533; Port status
  - Status of Volume Groups, Volumes & Disk Drives
- Reports:
  - Performance reports for StorageTek /LSI Storage arrays
    - Includes reports for Controllers, Volumes and Array for the following stats (via SMcli utility),
      - Total IO Count
      - Read Percentage
      - Cache Hit Percentage
      - Current Data Transfer Rate
      - Maximum Data Transfer Rate
      - Current IO Count
      - Maximum IO Count
  - Availability reports for storage system, RAID controller & RAID controller ports
- Alarms
  - SNMP trap based alarms
  - Status alerts for Disk Drives, Volume Groups & Volumes

Prerequisites for Monitoring

- OpManager uses command line utility (**SMcli.exe**) available as part of SANtricity Storage Manager Client installation
- Ensure that SMcli is installed in the server in which OpManager is installed.

- Include the directory containing SMcli.exe in the **PATH**environment variable.
    - By default for Windows Servers this is *C:\Program Files\SM8\client*
    - By default for UNIX Servers this is */opt/SM8/client/*

- Ensure that OpManager is restarted (shutdown & started) after including SMcli in the path
- Register OpManager server IP address as SNMP trap destination.
- Ensure that, OpManager installed host and the Storage system has a Fibre Channel Connectivity.

Monitoring SUNStorEdge Systems

OpManager provides monitoring and management of SUN StorEdge systems.

Models Supported

- SUN StorEdge 6920
- SUN StorEdge6120

Features Supported

- Inventory information of physical components ,
    - Disk Drives
    - Storage Volumes, Storage Pools
    - Ports info
- DSP information
    - Disk Drives
    - Volumes
    - Domains
    - SCSI info
    - Ports info
- Monitoring
    - Drive status
    - Storage pool status, Storage volume status
    - Domain status
    - Port status
- Reports:
    - Performance reports for StorageTek /LSI Storage arrays
        - Includes reports for Controllers, Volumes and Array for the following stats (via SMcli utility),
            - Total IO Count
            - Read Percentage

        - Cache Hit Percentage
        - Current Data Transfer Rate
        - Maximum Data Transfer Rate
        - Current IO Count
        - Maximum IO Count
    - Availability reports for storage system, RAID controller & RAID controller ports
- Alarms
    - SNMP trap based alarms
    - Status alerts for Disk Drives, Volume Groups & Volumes

Prerequisites for Monitoring

- OpManager uses command line utility (**SMcli.exe**) available as part of SANtricity Storage Manager Client installation
- Ensure that SMcli is installed in the server in which OpManager is installed.
    - Include the directory containing SMcli.exe in the **PATH**environment variable.
        - By default for Windows Servers this is *C:\Program Files\SM8\client*
        - By default for UNIX Servers this is */opt/SM8/client/*
- Ensure that OpManager is restarted (shutdown & started) after including SMcli in the path
- Register OpManager server IP address as SNMP trap destination.
- Ensure that, OpManager installed host and the Storage system has a Fibre Channel Connectivity.

Note : In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try readding the device.

Monitoring Areca ARC Storage System

OpManager provides monitoring and management of Areca ARC Storage System

Models Supported

- ARC Series like ARC-5010, ARC-6010, ARC-6020.

Features Supported

- Inventory information of physical components ,
    - RAID Controller
    - Disk Drives
- Logical configuration details
    - Raid Set

    - Volume Set
- Monitoring
    - Disk Drive state
    - Raid Set state
    - Volume Set state
    - Power Supply state
    - Disk Drive temperature
- Reports:
    - Availability reports for RAID Controller.
- SNMP trap based alarms

Prerequisites for Monitoring Areca ARC

- Ensure SNMP agent is running.
- Register OpManager server IP address as trap destination.

Note:&#65533; In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try readding the device.

&#65533;

Monitoring EMC Centera Storage System

OpManager provides monitoring and management of EMC Centera Storage Systems.

Features Supported

- Inventory information of physical components ,
    - Centera Clusters
    - Centera Nodes (Access & storage)
    - Centera Internal Switches
- Logical configuration details
    - CenteraClusterPools
    - CenteraProfiles
- Monitoring
    - Centera HeartBeat
    - Cluster status
    - Node status
    - Free space of Clusters / Nodes
- Reports:

    - Availability reports for Cluster
- SNMP trap based alarms

Prerequisites for Monitoring EMC Centera

- OpManager uses CLI interface to monitor EMC Centera
- Ensure that CenteraCLI software is installed in the server in which OpManager is installed (By default this is C:\Program Files\EMC\Centera\2_4\SystemOperator\lib)
- Copy the following jars to {OpManager Install Dir/classes/ directory.
    - C:\Program Files\EMC\Centera\2_4\SystemOperator\lib\CenteraViewer.jar
    - C:\Program Files\EMC\Centera\2_4\SystemOperator_jvm\lib\jsse.jar
- Ensure that OpManager is restarted (shutdown & started) after copying these JAR files.

Note:&#65533; In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try re-adding the device.

Monitoring IBM Spectrum Virtualize

Models Supported

OpManager supports the following models:

All IBM devices with IBM Spectrum Virtualize can be monitored by adding them in this template. For Eg: IBM SVC/ Storwise, IBM FS9100, 9150, 9110.

Pre-requisite

The default port must be 7443.&#65533;

Monitoring HP EML and ESL Tapelibraries in SAN / NAS networks

OpManager provides monitoring and management of HP EML and ESL Tapelibraries.

Models Supported

- HP EML E-Series
- HP ESL E-Series

Features Supported

- Inventory information
    - Tape library
    - Tape Drive status
    - Chassis Info
    - Fibre Channel ports
    - Storage Media details
    - Media Access Device
- Monitoring

- Tape library status
- Tape drive status
- Drive port status
- Changer device status

- Reports:
  - Availability reports for Tape library

Prerequisites for monitoring HP EML / ESL Tapelibrary

- OpManager uses the HP **SMI-S TL** Provider to monitor the HP Tape Libraries
- The TL provider can be installed on any server running Microsoft Windows 2000 / Windows 2003 / Windows XP / Windows Professional.
- This server must have a path through the SAN to the TL devices that will be managed.
- Also the TL Provider installed server must be pingable from the server where OpManager is installed.
- Install the necessary software from the OEM website.
- Start the TL Provider service **hp StorageWorks SMI-S CIMServer** from the Windows services menus

Note: In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try re-adding the device.

Monitoring Dell PV - PowerVault tape libraries

OpManager provides monitoring and management of Dell PV series tape libraries like DELL PV 132T & Dell PV 136T

Models supported

- DELL PV132T
- DELL PV136T

Features Supported

- Inventory information of physical components ,
  - Tape Drives
- Logical configuration details
  - Movers
- Monitoring
  - Tape library status
  - Tape drive status
  - Mover status
- Reports:

    - Availability reports for Tape library .
- Monitoring and alarm generation for faulty conditions (via SNMP traps)
    - Tape library state
    - Door state
    - MailBox state
    - Error notification
    - Shutdown notification
    - Service Action Code (SAC) notification

Prerequisites for Monitoring

- In the RemoteManagementUnit (RMU) ensure that the SNMP agent is running.
- Register OpManager server IP address as trap destination
- Check if the community name is configured as public
- To ensure this check the value of Public Name under Configuration tab-->SNMP Configuration area. **Note:** If a different community is used, it needs to be specified when you add the device via OpManager
- Details are available in ADIC Scalar 100 User's Guide (Dell PV 136T is essentially a rebranded version of ADIC scalar 100 tape library)

Note : In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try readding the device.

Monitoring IBM 3584 / TS 3500 tape libraries

OpManager provides monitoring and management of IBM 3584 / TS 3500 Tape Libraries.

Models Supported

- IBM 3584
- TS 3500
- IBM ULT3582

Features Supported

- Inventory information of physical components
    - Chassis details
    - Changer Device details
    - Library Fibre Channel Port details
    - Library SCSI Controllerdetails
    - Storage Media details
    - Media Access Device
- Monitoring

    - Tape Library status
    - SCSI Controller status
    - Changer Device status
    - Media Access Device status
- Reports:
    - Availability reports for Tape library , Media Access Device
- Monitoring and alarm generation for faulty conditions (via SNMP traps)

Prerequisites for monitoring IBM 3584 / TS 3500 Tapelibrary

- Ensure that the SNMP agent is enabled in the tape library before adding the device via OpManager web-client .
  The details are available in the "IBM 3584 Planning & Operator Guide" in "Chapter 4 Advanced Operating Proceedures --> Selecting the Network Settings".
- Register OpManager server IP address as trap destination.

Note :&#65533; In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try readding the device.

&#65533;

Monitoring Overland Neo series tape libraries

OpManager provides monitoring and management of Overland Neo series tape libraries like Overland Neo 2000, Overland Neo 4000.

Models Supported

- Overland Neo series tape libraries like&#65533;
    - Overland Neo 2000
    - Overland Neo 4000

Features Supported

- Inventory information of physical components ,
    - Tape Drives
- Logical configuration details
    - Library Modules (Master module / Slave module)
- Monitoring
    - Tape library status
    - Tape drive status
    - Library Module status
- Reports:
    - Availability reports for Tape library.

- Monitoring and alarm generation for faulty conditions (via SNMP traps)
    - Tape library state
    - Door state
    - Mail Slot state
    - Power supply state
    - Tape drive state
    - Tape drive cleaning state
    - Library Module state

Prerequisites for monitoring Overland Neo series

- Ensure that the SNMP agent is running.
- Register OpManager server IP address as trap destination

Note:&#65533; In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try re-adding the device.

&#65533;

Monitoring ADIC Scalar i2000 & 100 tape libraries

OpManager provides monitoring and management of ADIC Scalar i2000 & Scalar 100 tape libraries

&#65533;

Features Supported For ADIC Scalar i2000

- Complete inventory information of physical components
    - Tape Library
    - Tape Drives
- Monitoring
    - Tape library status
    - Tape drive status
- Reports:
    - Availability reports for Tape library
- Monitoring and alarm generation for faulty conditions (via SNMP traps)
    - Sensor state change (Voltage, Temperature, Cooling)
    - Tape library state change
    - Tape drive added/removed
    - Media mounted /unmounted

Features Supported For ADIC Scalar 100

- Complete inventory information of physical components ,
  - Tape Library
  - Tape Drives
- Logical configuration details
  - Library partitions
  - Movers
- Monitoring
  - Tape library status
  - Tape drive status
  - Mover status
- Reports:
  - Availability reports for Tape library
- Monitoring and alarm generation for faulty conditions (via SNMP traps)
  - Tape library state
  - Door state
  - MailBox state
  - Error notification
  - Shutdown notification
  - Service Action Code (SAC) notification

Prerequisites for Monitoring ADIC Scalar 100

- In the RemoteManagementUnit (RMU) ensure that the SNMP agent is running.
- Register OpManager server IP address as trap destination.
- Check if the snmp community name configured as public.
- To ensure this check the value of Public Name under Configuration tab->SNMP Configuration area.
  Note: If a different community is used, it needs to be specified when you add the device via OpManager.
- Details are available in ADIC Scalar 100 User's Guide.

Prerequisites for Monitoring ADIC Scalar i2000

- Ensure that the SNMP agent is running.
- Register OpManager server IP address as trap destination.
- Details are available in ADIC Scalar i2000 User's Guide.

Note: In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try re-adding the device.

Monitoring StorageTek L-series tape libraries

OpManager provides monitoring and management of STK - StorageTek L-series tape libraries like L20 , L40 & L80.

Models Supported

- L20
- L40
- L80

Features Supported

- Complete Inventory information
  - Tape library
  - Tape Drives
- Monitoring
  - Tape library status
  - Tape drive status
- Reports:
  - Availability reports for Tape library .
  - Performance reports
    - Get fails/Retries
    - Label fails/Retries
    - Num of cartidge moves
    - Num of door opens , IPLs , Mounts
    - Put fails/ retries
    - Target fails/retries
- Alarm generation for faulty conditions (via SNMP traps)
  - Tape library state
  - Tape drive state
  - CAP state
  - PTP state

Prerequisites for Monitoring

- Ensure that the SNMP agent is running.
- Register OpManager server IP address as trap destination.

Note:&#xFFFD; In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try readding the device.

&#xFFFD;

Monitoring QualStar TLS, QLS & RLS series tape libraries

OpManager provides monitoring and management of QualStar TLS, QLS & RLS series tape libraries like TLS-1210, QLS-SDX-220 & RLS 4445.

Models Supported

- Qualstar TLS series tape libraries like TLS-1210 & TLS-1220
- Qualstar QLS series tape libraries like QLS-SDX-220 , QLS-4G-236
- Qualstar RLS series tape libraries like RLS-4221 & RLS-4445

Features Supported

- Inventory information of physical components
  - Tape Drive
  - Fibre Channel details
  - Library SCSI details
  - Cartidge details
- Logical configuration details
  - LUN information for library SCSI
- Monitoring
  - Tape library status
  - Tape drive status
- Reports:
  - Availability reports for Tape library
  - Tape Library status report
    - No of door opens
    - No of cartidge moves
    - No of picks
    - No of times placed
    - No of grips
- Monitoring and alarm generation for faulty conditions (via SNMP traps)
  - Door Open
  - Unit Fault
  - Inventory Violation
  - Needs Maintenance

Prerequisites for Monitoring

- Ensure that the SNMP agent is running.
- Register OpManager server IP address as trap destination.

- Refer the Q-Link (Qualstar's Remote Library Management software) user manual section "SNMP" under the chapter "Q-Link Remote Library Manager" for details.

Note: In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try readding the device.

Monitoring Quantum - ATL tape libraries

OpManager provides monitoring and management of Quantum - ATL tape libraries - PX, P, M and DX series.

Models Supported

- P series
  - P7000
  - P4000
  - P3000
  - P2000
  - P1000
- PX series
  - PX502
  - PX506
  - PX510
  - PX720
- M Series
  - M1500
  - M1800
  - M2500
- DX Series
  - DX3000
  - DX5000
  - DX100
  - DX30

Features Supported

- Tape library Inventory information
- Tape library status Monitoring
- Reports:
  - Availability reports for Tape library.
- Monitoring and alarm generation for faulty conditions (via SNMP traps)

- Tape library state
- Tape library availability state

Prerequisites for Monitoring

- Ensure that the SNMP agent is running
- Register OpManager server IP address as trap destination
- Has the SNMP community name configured as"public" ?(If a different community is used , it needs to be specified when you add the device via OpManager.)

Note: In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try re-adding the device.

Monitoring Tandberg tape libraries

OpManager provides monitoring and management of Tandberg M series tape libraries.

Models Supported

- M Series
  - M1500
  - M2500

Features Supported

- Tape library Inventory information
- Tape library status Monitoring
- Reports:
  - Availability reports for Tape library .
- Monitoring and alarm generation for faulty conditions (via SNMP traps)
  - Tape library state
  - Tape library availability state

Prerequisites for Monitoring

- Ensure that the SNMP agent is running
- Register OpManager server IP address as trap destination
- Has the SNMP community name configured as"public" ?(If a different community is used , it needs to be specified when you add the device via OpManager.)

Note: In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try re-adding the device.

Monitoring SUN StorEdge tape libraries

OpManager provides monitoring and management of SUN StorEdge L-series tape libraries.

Models Supported

- L Series
  - 140
  - 400
  - 1000
  - 1800

Features Supported

- Tape library Inventory information
- Tape library status Monitoring
- Reports:
  - Availability reports for Tape library .
- Monitoring and alarm generation for faulty conditions (via SNMP traps)
  - Tape library state
  - Tape library availability state

Prerequisites for Monitoring

- Ensure that the SNMP agent is running
- Register OpManager server IP address as trap destination.
- Have the snmp community name configured as"public"? (If a different community is used , it needs to be specified when you add the device via OpManager.)

Note : In case the device is not discovered, then the probable reasons for non discovery are displayed in the client. Please go through the instructions and try readding the device.

Discovering storage devices

The topics covered under this section are:

- Prerequisites For Device Discovery
- Adding A Device
- Adding Device Details

Prerequisites for Device discovery

The list of storage devices that are monitored by OpManager and their respective supported models, features supported and prerequisites for monitoring are listed below.

SAN Switches	Storage Arrays	Tape Libraries
• Brocade Silkworm Series • McData Sphereon series • EMC Connectrix • Cisco MDS series • QLogic SANbox • HP Switches	• IBM ESS • HP MSA • HP EVA • EMC CLARiiON • Infortrend • NetApp • Hitachi Lightning • Hitachi Thunder • Huawei Storage • IBM DS4000 / FastT • StorageTek / LSI Logic • SUN StorEdge • Areca RAID • EMC Centera	• HP ESL / HP EML • DELL • IBM 3584 / TS 3310 / TS 3500 • Overland Neo • ADIC Scalar • StorageTek • Qualstar • Quantum • Tandberg • SUN StorEdge

Adding a device

After the initial discovery, you can use **'Add Storage Device'** option under **Settings** → **Discovery** to add a new device.

Note: Only Admin users can add devices.

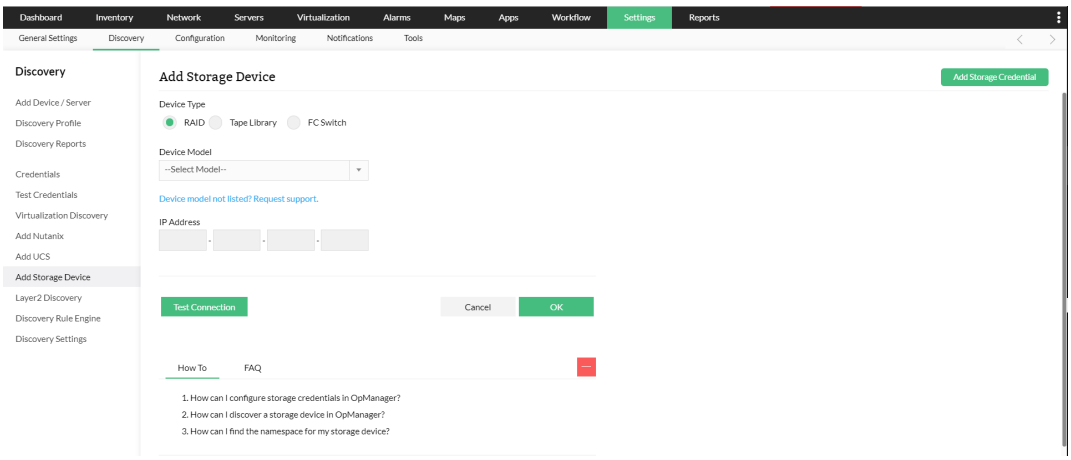
Steps for adding a Device :

- Click the 'Settings' tab in the OpManager client.
- Select 'Discovery' tab and click on 'Add Storage Device'.
- Enter the IP address of the new device.
- Choose the Device Type whether it is a RAID array, FC Switch or a Tape Library.

- Choose the Device model of the storage device.
- Depending on the Device model selected, enter the credential as SNMP/SMI/CLI/NetAppAPI/Storage API.

> **Note:** If you want to add a new credential, click the **'Add Storage Credential'** button on the top right corner and provide the necessary details.

- You can test the device right away from the same window by clicking the 'Test Connection' button.
- Click 'Add Device' button to add it.



Adding Device details

Clicking on any device name in the Inventory tab takes you to the device snapshot page. There you can view all the operational stats of the device in a single pane and also its basic details such as IP Address, Device vendor and model, Firmware version, and so on.

To edit the device details

1. Go to the **Inventory** tab, click on 'Storage' and then click on the device whose details you want to edit.
2. In the device snapshot page that is opened, click on the **three-line menu button** on the top-right corner of the screen and select **'Edit Device Details'.**
3. Here, you can change the details of the device namely **IP Address, Display name** and the **monitoring interval**.

> **Note:** Only Admin users can add and edit device details.

Fault Monitoring And Escalation

The traps and other notifications from the devices are received by the software and are converted into events and alarms. Depending of the criticality of the fault condition, each event and alarm is assigned a severity ranging from critical to clear. Each severity is given a specific color for easy visual identification.

OpManager actively monitors the faulty events and reports or escalates the faults to the user, administrator, or any other person via email or SMS.

Alarms are widely classified into two types : **Device status-based** alarms and **threshold-based** alarms.

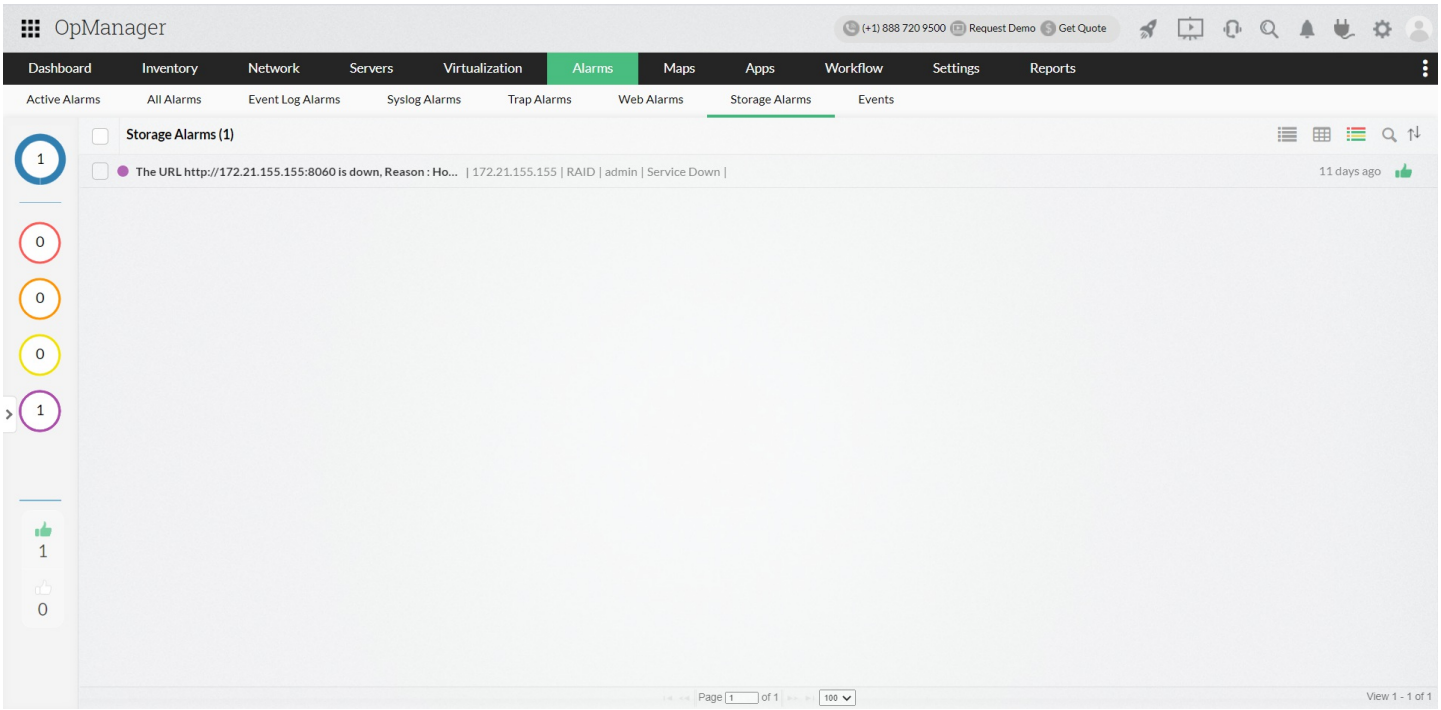
The topics covered under this section are :

- Viewing Alarms
- Viewing Alarm Details
- Alarm Operations
- Escalate Unattended Alarms

Viewing alarms

You can view all the alarms in a single console under '**Alarms**' tab. Here, the alarms related to storage can be found by clicking '**Filter → Storage Alarms**' from the 'Sort by category' pane.

This tab displays all the alarms with their source, status, date & time, and message. It displays a maximum of 500 alarms in a page, and you can use the navigation buttons on the bottom of the page to view the other alarms. Each column heading is a link, which when clicked, sorts the alarms based on that column.



You can go to the alarm details page with a single click. To see the details of the device that caused an alarm, click on the source link of the alarm. To see the details of the alarm, click the message of the alarm.

Just above the table on the top right corner there are options to acknowledge, clear, or delete alarms. To do any of these operations, select the specific alarms, and clicking on the corresponding link.

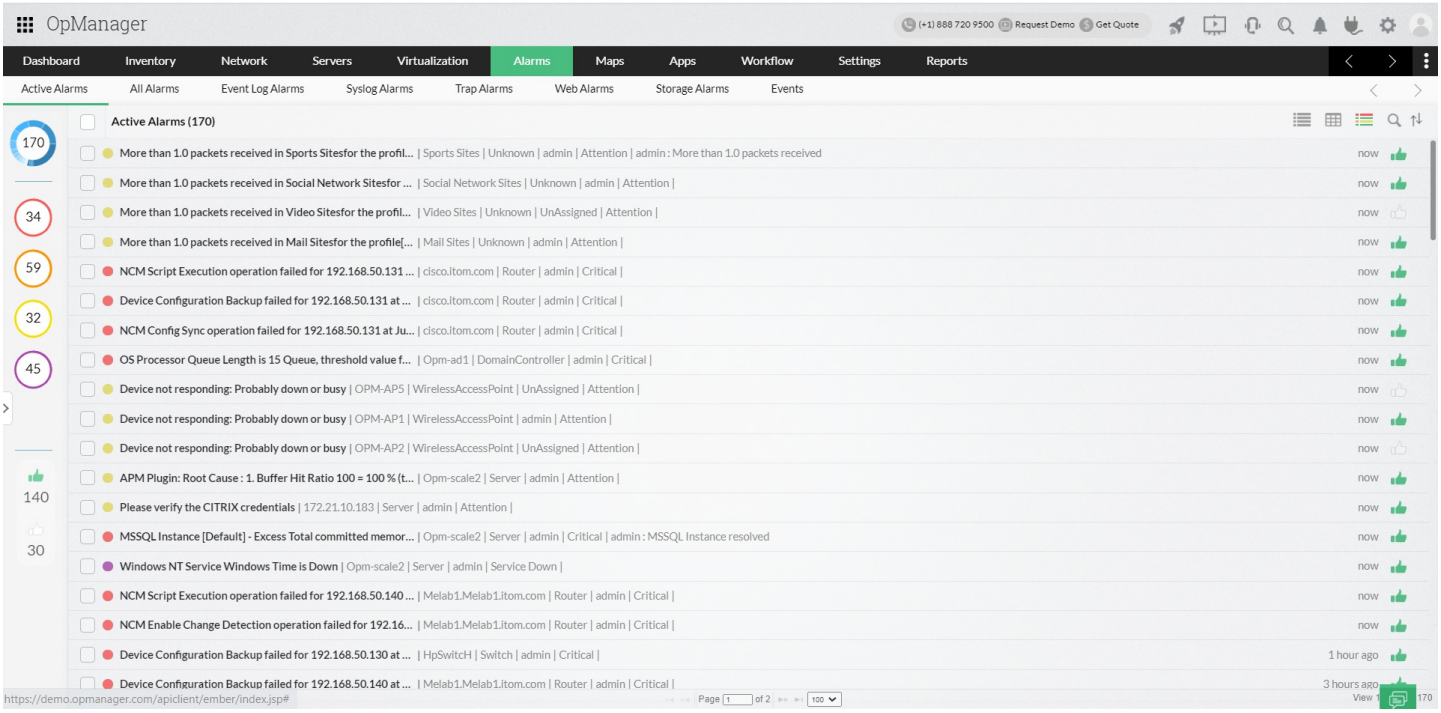
You can even view the alarms depending on the criteria like Severity, Category or alarms generated between a specific time

period.&#65533; For this, you can just click on the relevant heading on the alarms pane, and the alarms will be sorted based on that criteria.

If needed, you can export the same to HTML, PDF, Excel sheet and CSV formats.

Viewing alarm details

Clicking on the message link in an alarm brings you to the alarm details page.



Alarm details page shows :

- Message - The warning message in the specified alarm.
- Status - The status of that alarm (Attention, Trouble, Critical or Clear).
- Date & Time - The date and time at which the alarm was triggered.
- To see details of the device that caused the alarm, click on the source link.

Just above the table there are options to acknowledge, clear, delete, and annotate alarms.

- To take ownership of the alarm, click 'Acknowledge'. You can also revert the acknowledgement by using the 'Unacknowledge' button.
- To add comments to the alarm, click 'Add note' (The plus icon).
- To ping and test the concerned device manually, click 'Ping' (The sync icon).
- To perform a traceroute on the device, click 'Trace Route'.
- To clear the alarm, click on 'Clear' (The tick icon).
- To delete the icon, click on 'Delete' (The trashcan icon).

Alarm Operations

Acknowledging Alarms :

OpManager provides an option for the users to pick and own alarms that they work on. This helps in avoiding multiple users working on a single alarm.

Alarms can be acknowledged in two ways.

1. In the 'Alarms' tab, select the checkbox before the specific alarm and click ‘Acknowledge’. This option is available only for Admin users.
2. In the alarm details page, click ‘Acknowledge’.

By doing one of the two actions above, the user becomes the owner of the particular alarm.

To unacknowledge an alarm, click ‘Unacknowledge’ in the specific alarm details page. The alarm ownership gets removed.

Annotating Alarms :

In case of a user wants to add more details on a particular alarm, he can annotate the same in the alarm. This will be useful for later reference.

To annotate an alarm, click ‘**Add note**’ link in the specific alarm details page and add the content in the text-box. The annotation will get added in the alarm notes table.

Clearing alarms :

After fixing the fault condition in the device, the particular alarm can be cleared by the user, so that its status becomes clear.

To clear an alarm, click ‘**Clear**’ link in the specific alarm details page. The severity of the alarm will change to clear.

Deleting alarms :

After fixing the fault condition in the device, the particular alarm can be deleted by the user, if he feels that the record need not be maintained.

To delete an alarm, click ‘**Delete**’ link in the specific alarm details page. The alarm and its related events will get deleted permanently.

Escalate unattended alarms

When some alarms are not attended for a particular time-period, it needs to be escalated to the administrator or the IT manager (based on need). For example, you get a critical alarm for a tape library and the fault condition is not resolved within 6 hours, it might cause a major problem in the operation of the storage infrastructure. Such alarms can be escalated and quick action can be taken to avoid any major problem.

To add an alarm escalation rule :

- From web client go to Settings → Configuration → Alarm Escalation rules.
- Click on 'Add Rule'.
- Enter a name for the new rule.
- Provide all the details for the escalation rule.
- Finally provide the contact details of the people that have to be notified. You can provide either.
- Enter the time duration in which the above rule has to be checked.
- Click ‘Add Rule’.

The rule gets added in the table in the page. You can disable the rule by clicking on the green icon inside the modify rule window.

To modify an alarm escalation rule :

- Click the name link of the rule that needs to be modified.

- The configured values are shown in the form below.
- You can edit the required values and click ‘Save’.

To delete an alarm escalation rule :

- Click the trash-can icon against the particular rule, in the escalation rules table.

Storage reports

OpManager helps you get crucial insights on the performance of your network storage using intuitive reports. Reports help you with both real-time monitoring and historical stat analysis of your network.

Some of the storage reports available are:

- **Storage Summary reports:** Know the overall status of yor network's storage devices with this report.
- **RAID Capacity Utilisation:** Know how much your RAID disks have been utilised, with Max, Min and Avg values for each storage.
- **RAID IOPS:** View the number of Input/Output Operations per second (IOPS) for your RAID disks.
- **RAID Latency:** Know the latency in your network storage so that you can understand the overall accessibility of your disks. These reports are very useful to find performance bottlenecks.
- **Disk IOPS:** Know the IOPS stats for your storage disks.
- **RAID Forecast by utilisation:** Know when your storage might reach 80%, 90% and 100% of its capacity with this report.
  It predicts the storage space availability using the current usage rate and usage growth rate, helping you to avoid any kind of data loss due to delay in disk addition.
- **RAID Reads/Sec:** Rate of read operations on the RAID storage per second with Max, min and Avg values
- **RAID Writes/Sec:** Rate of write operations on the RAID storage per second with Max, min and Avg values
- **RAID Controller IOPS:** Number of input/output operations per second on your RAID controller
- **RAID Controller Reads/sec:** Number of read operations per second on your RAID controller
- **RAID Controller Writes/sec:** Number of write operations per second on your RAID controller
- **Disk Reads/sec:** Number of read operations per second on individual disks in your storage
- **Disk Writes/sec:** Number of write operations per second on individual disks in your storage
- **Growth trend:** Detailed stats on growth trend in your storage including utilization, growth rate percentage, growth rate per day and average future utilization

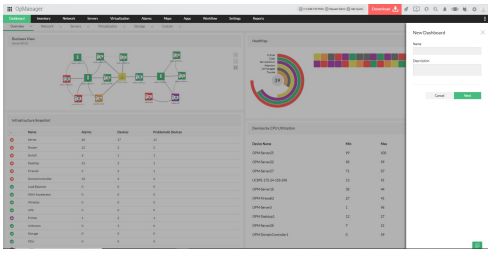
More reports for storage monitoring are available under **Reports ? Storage Reports.**

Create Custom Dashboards

The dashboard customization feature in OpManager helps you to create your own dashboard and view desired performance metrics and reports at a glance. Now, a user can create and share dashboards with other users.

> **Note**: For an operator to create custom dashboards, admin user has to first enable the 'Create dashboard for Operator' option.
> To enable this feature go to **Settings ? System settings.** Under **General,** select **Enable** the **Allow dashboard creation for operator.**

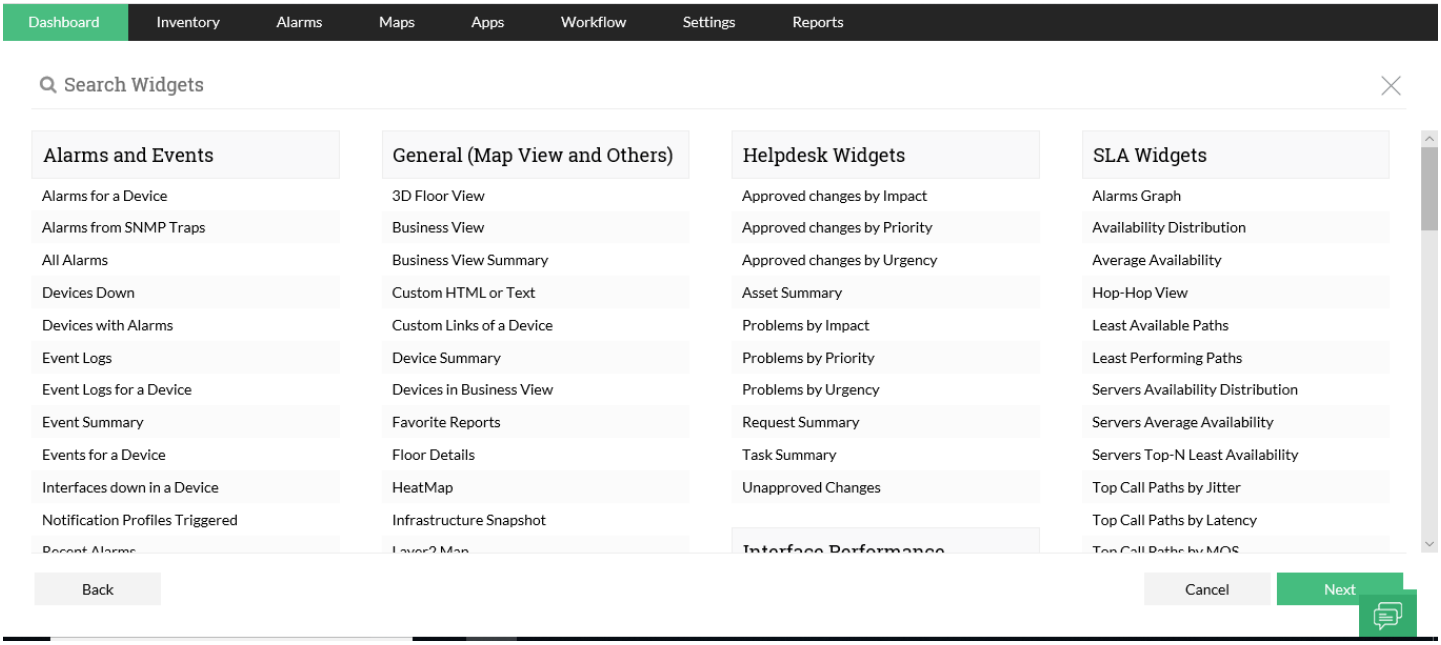
1. Click on **Dashboard.** In the top right corner of the screen, click on the icon with + symbol. Create **New Dashboard** page opens [screen shots given below].



2. **Name**: Enter a unique name for the dashboard.

3. **Description**: Enter a description about the dashboard.

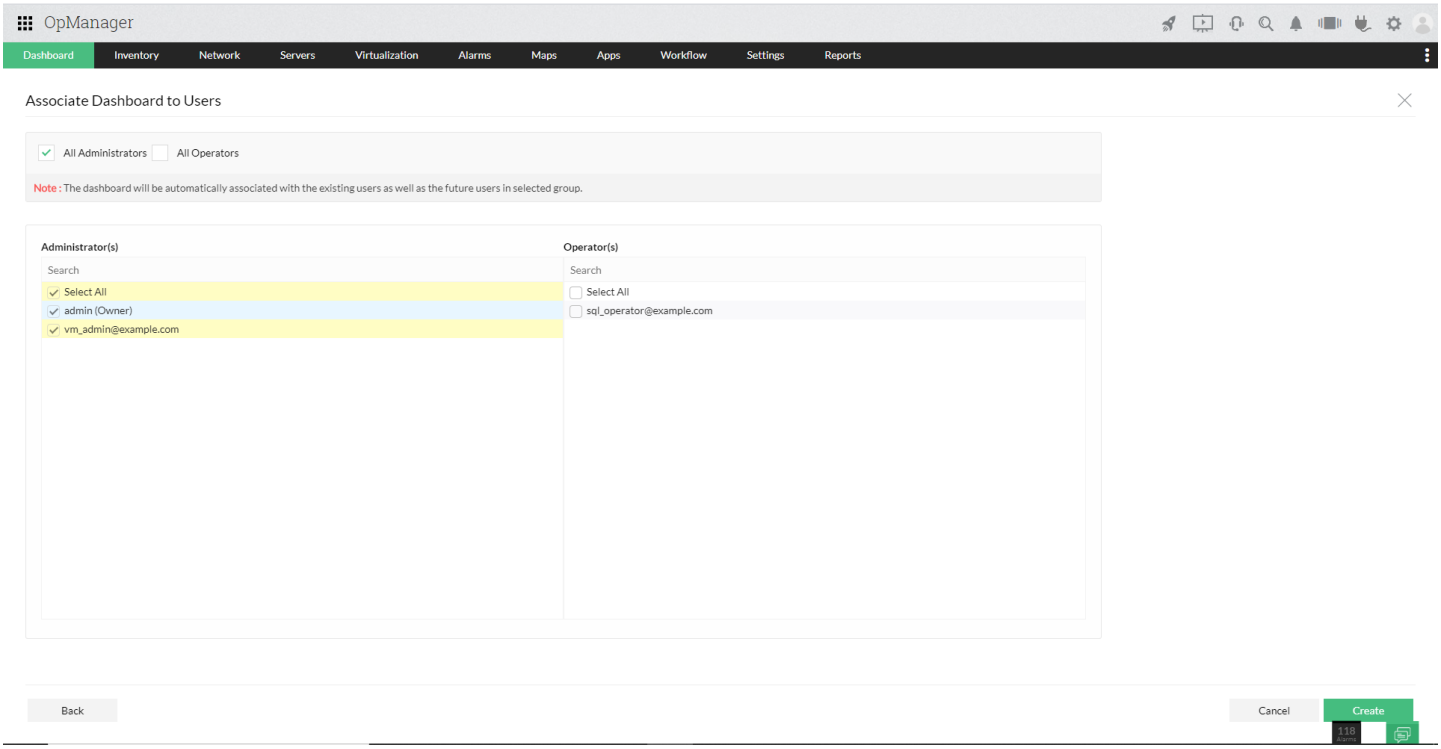
4. Click **Next**.



5. Select Widget(s) from the list of widget categories. You could use the search bar to find the widget.

6. Click **Next**.

7. Select the user(s) whom you wish to share the dashboard with (Refer to the table below for privilege-based actions on custom dashboards).



8. You can associate the dashboards with either of the following

- All admins and/or all operators **(or)**
- You can manually select individual users.

Note: When you select all admins, all operators or both, the dashboard will be associated with existing users as well as future users in the selected group.

9. After selected users to be associated, click on **create**. A new dashboard is created and listed on the **My Dashboard** page.

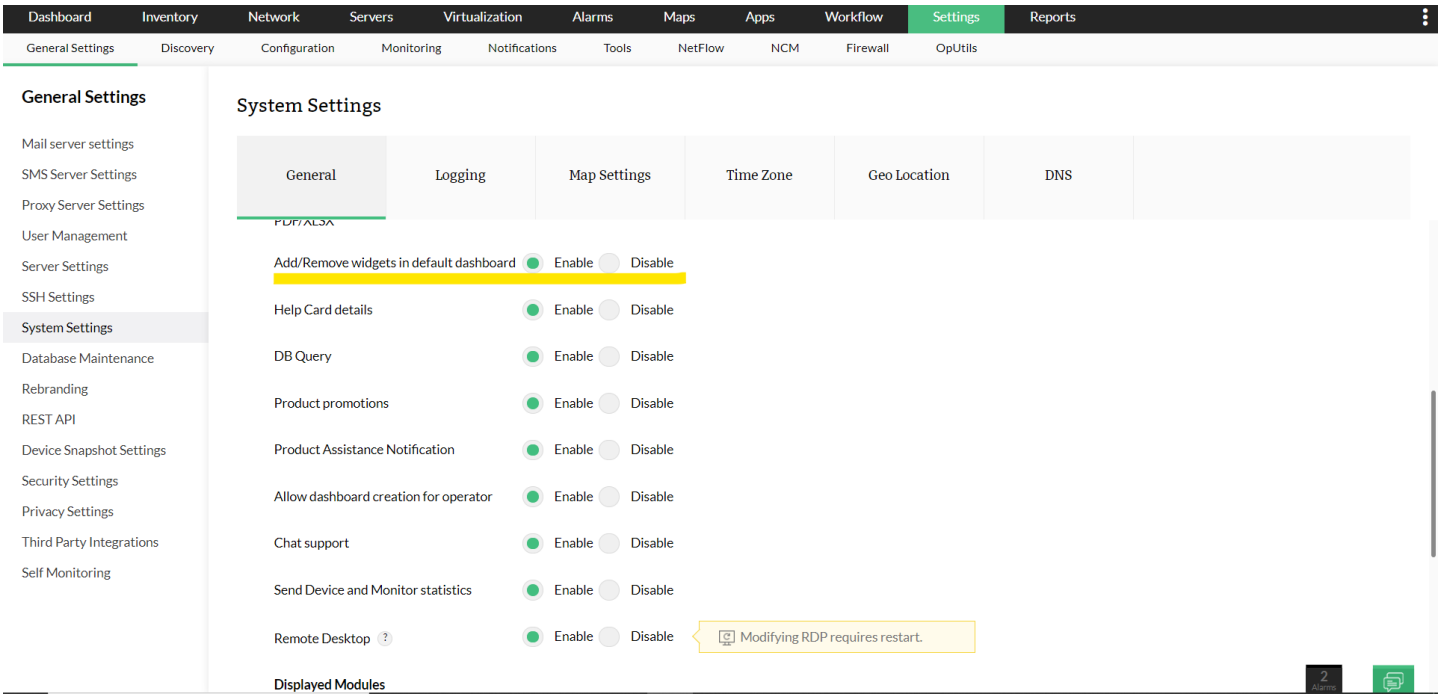
Privilege-based actions allowed for admins/operators on custom dashboards

The role-based sharing/editing actions that can be performed by the admin/operator on custom dashboards have been tabulated below.

Action	Admin	Operator
Create dashboard	Available	Available
Dashboard association authority	Can associate with all users.	Can associate with other operators only
Edit/Modify Widget	On dashboards of all users.	On dashboards created by self
Delete widget / Delete Dashboard	Can delete self-created and associated dashboards	Can delete self-created dashboards
View dashboard	All	Only Self-created and associated dashboards

To Add/Remove Widgets from Default Dashboard:

1. Go to Settings > General Settings > System Settings.
2. Enable the Add/Remove Widgets from Default Dashboard option.



Delete Dashboard

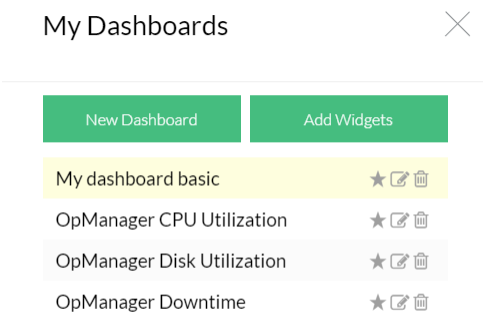
To delete a dashboard, follow the steps given below:

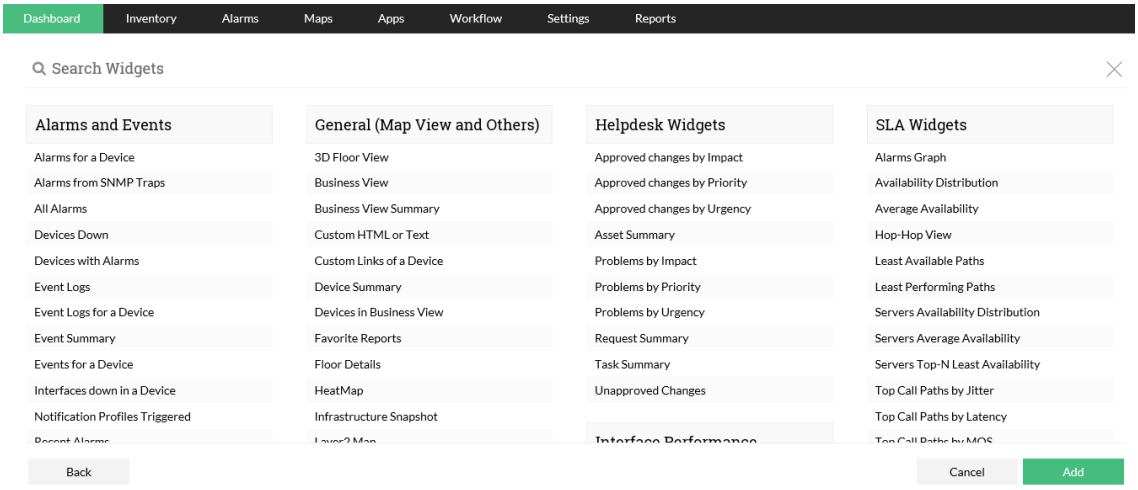
1. Go to **Dashboard** > **My Dashboard** page
2. Click **Delete** icon of the **Dashboard** that you want to delete. A confirmation window pops-up.
3. Click **OK** to confirm deleting.

Adding New Widgets

To add a new widget to a dashboard follow the steps given below:

1. Click on**&#65533;** **Dashboard.** Click on the green colored icon at the top right of the menu bar. Select the dashboard you want to add widgets to from from**&#65533;** **My Dashboards.** If you want to know the steps to create a new custom dashboard, click here
2. Click on**&#65533;** **Add Widgets&#65533;** seen at the bottom**&#65533;** of the page.
3. Select the Widget(s) that you want to add to the dashboard.
4. Click**&#65533;** **Add&#65533;** button to add the selected widget(s) to the dashboard.

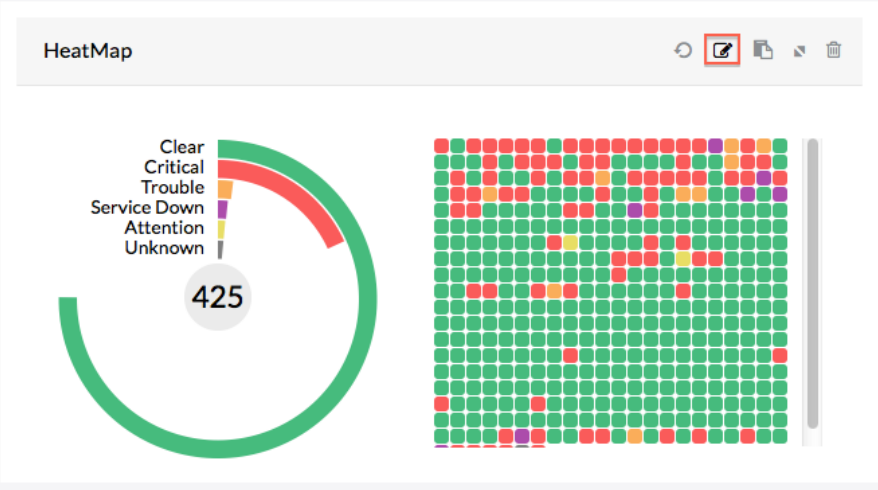


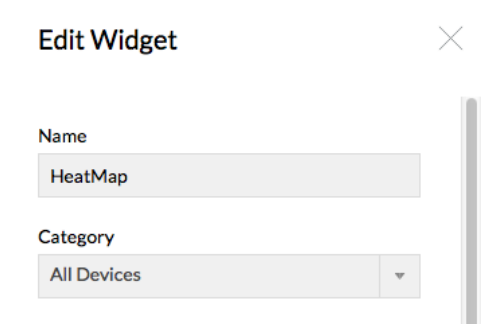


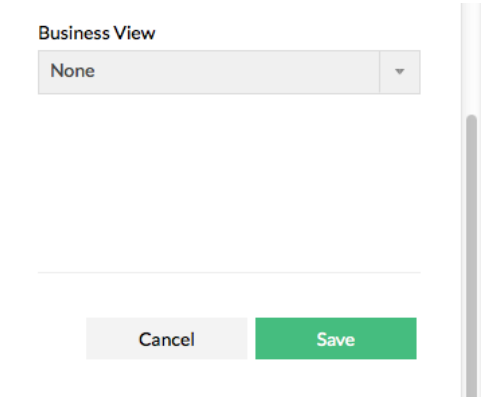
Editing Widgets

To modify the existing widgets go through the steps given below:

1. Click on the**&#65533;** **Edit&#65533;** against the widget on which you wish to modify the fields.
2. Modify the required fields.
3. Click **Save&#65533;** to effect the changes.





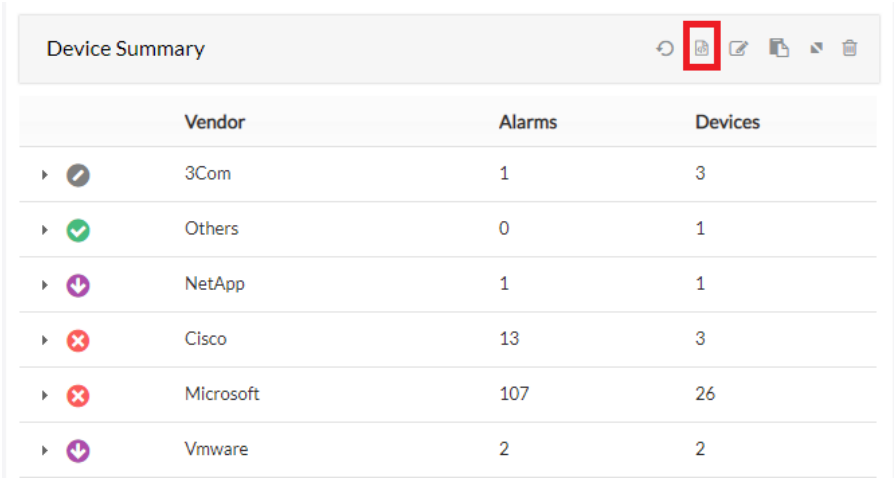


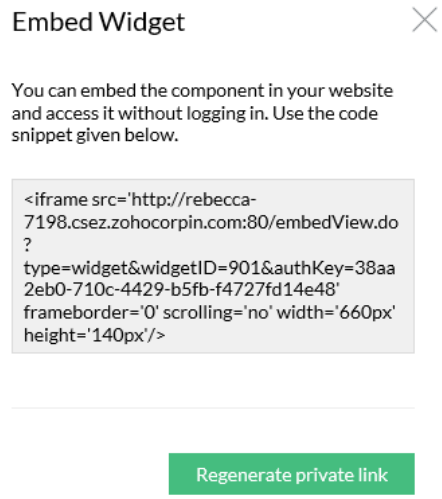
Embedding widgets

The embed widget feature lets you embed a dashboard widget with its realtime data on any webpage. To embed a widget into your webpage, simply copy and paste the code snippet into the HTML of the website where you want it to be displayed.

The following are the steps to obtain the code snippet to embed a widget:

1. Click on the embed widget icon in the top right of the widget.
2. Copy the code snippet.
3. Paste the code snippet into the HTML of the webpage.



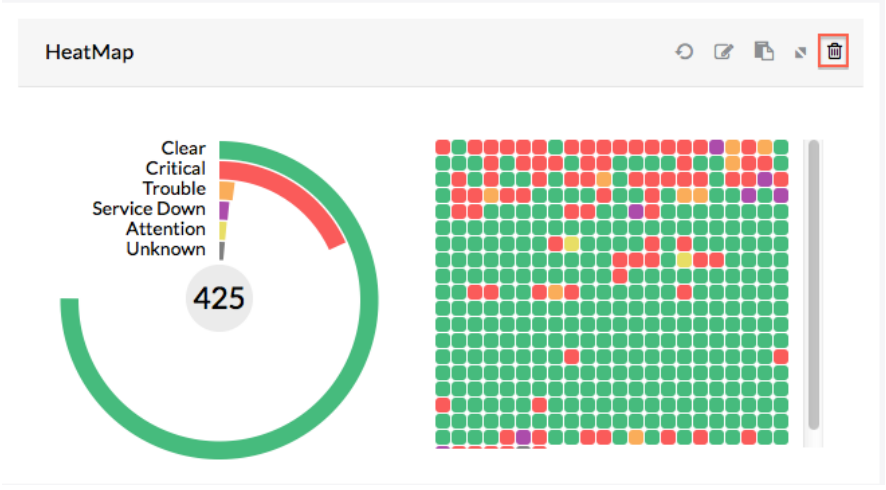


Note: The regenerate private link option generates a new authentication key for a widget. If you click on this option, the previously generated code snippet for the widget will no longer be valid.

Deleting widgets

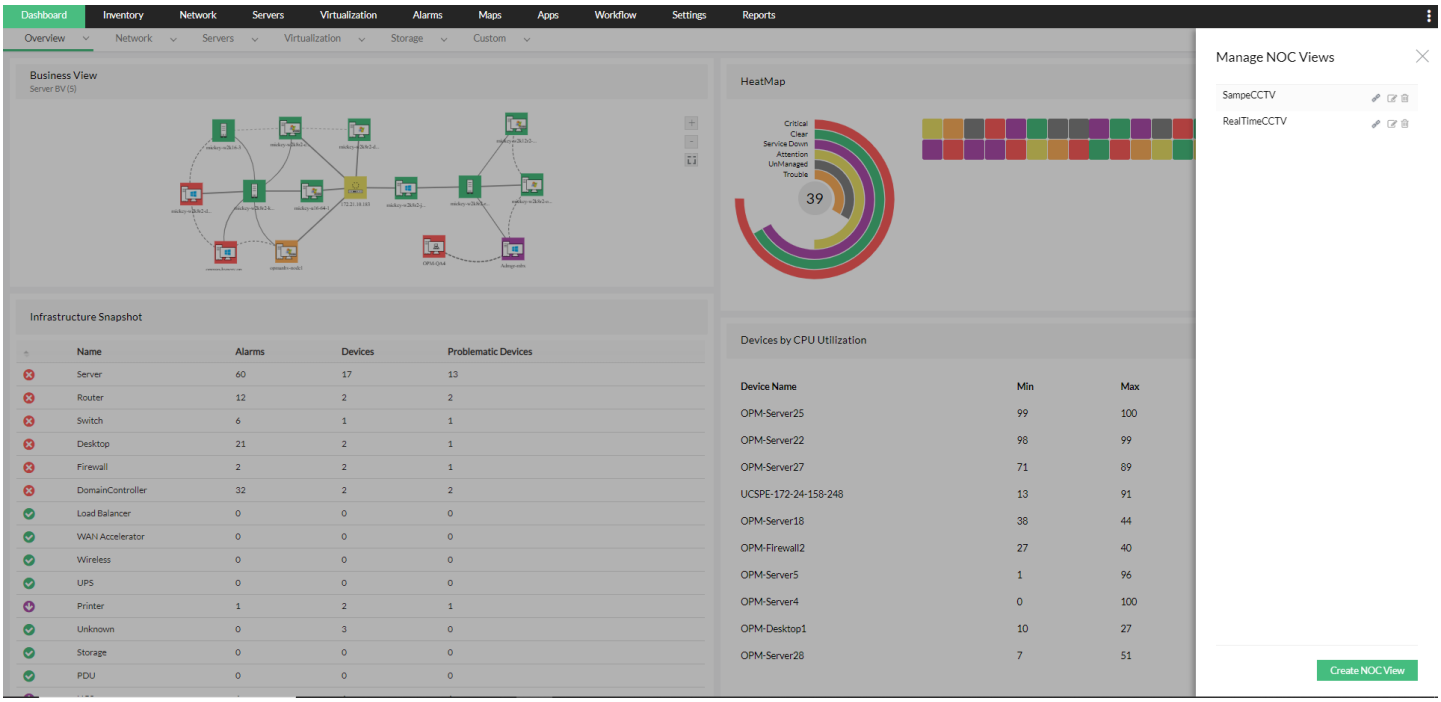
To delete a widget go through the steps given below:

1. Click on **Delete** icon available on the widget box. A confirmation window pops up.
2. Click **OK** to confirm deleting the widget.

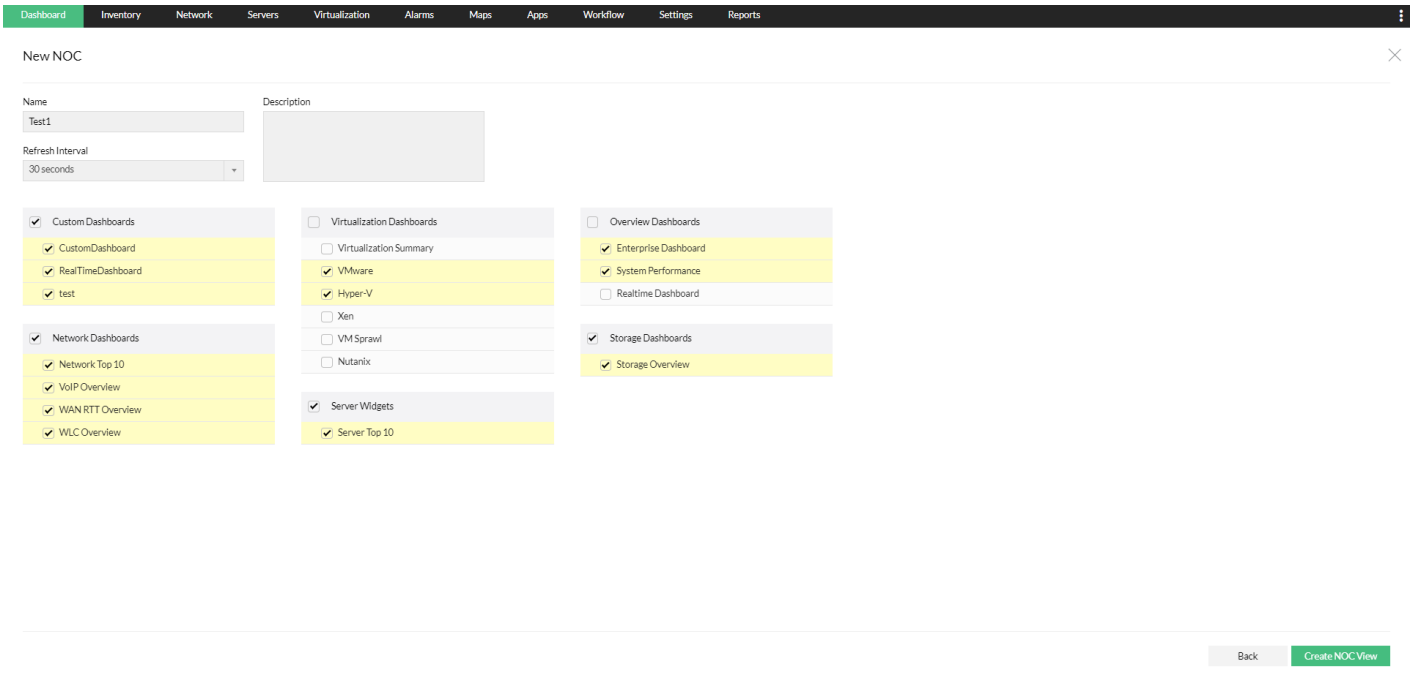


Adding New NOC View/CCTV

NOC View or CCTV helps you view only the required dashboards repeatedly at required intervals. To add a new NOC view follow the steps given below:

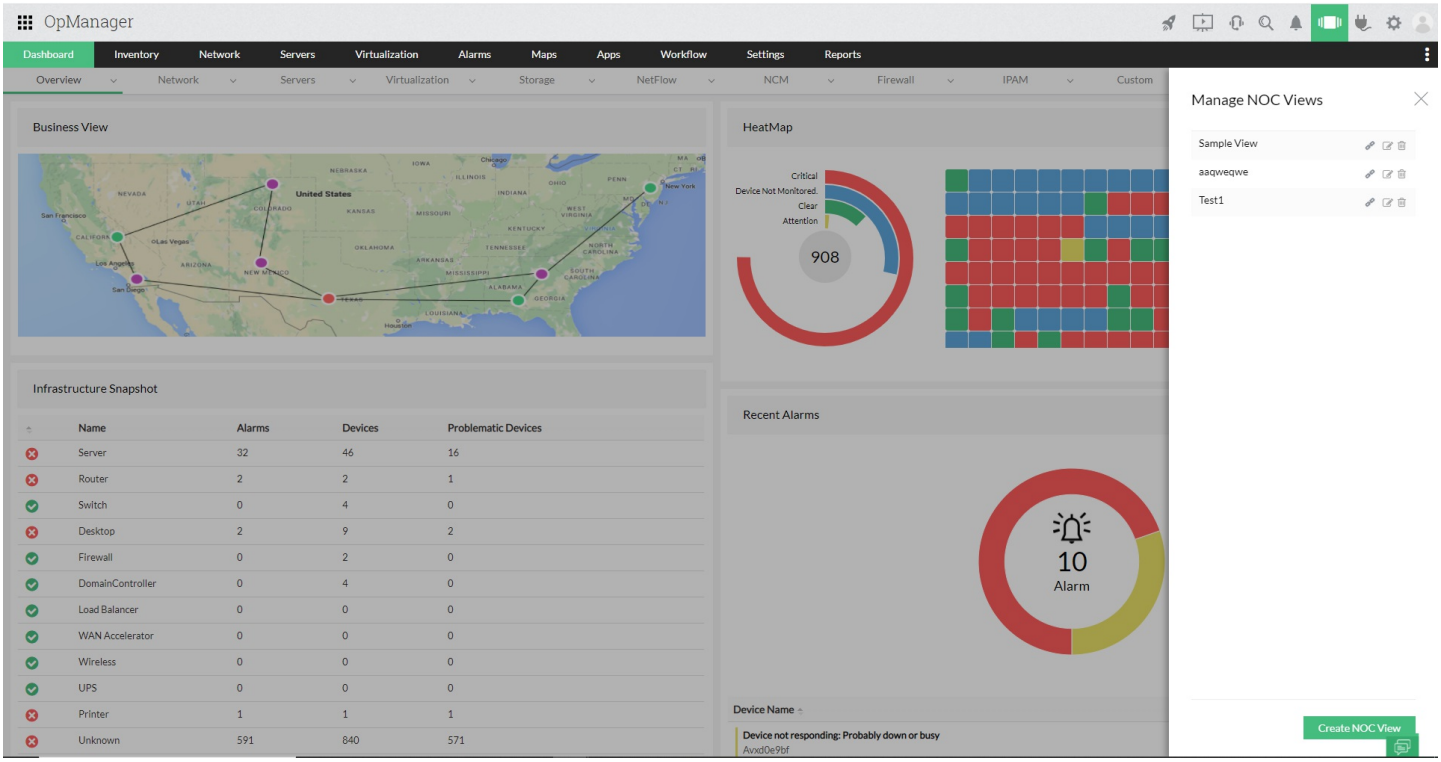


1. Go to **Dashboard** page and click NOC views**.**
2. Click **Create NOC View**. New NOC page opens.
3. **Name**: Enter a unique NOC name.
4. **Refresh Interval**: Select the interval required to switch over to the next dashboard.
5. **Description**: Enter a brief description about this NOC view.
6. Select the desired dashboards that you want to include in this NOC view.
7. Click **Create NOC View.**
8. A new NOC view has been added.



Viewing NOC

To view a NOC view, go to **Dashboard** page > **NOC Views** > Click on the name of the NOC that you want to view. That particular NOC view opens in a new window.



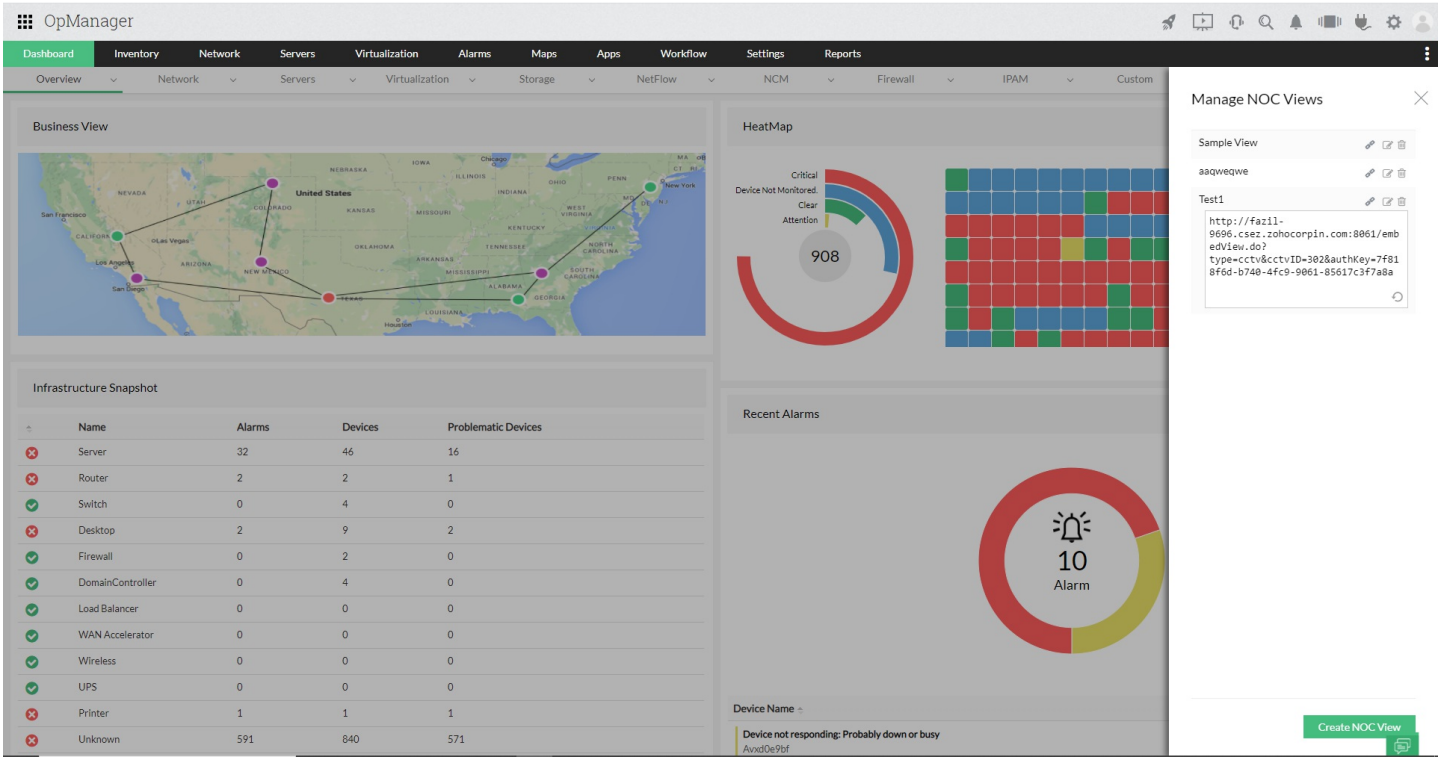
Editing NOC

To edit a NOC view follow the steps given below:

1. Go to **Dashboard** > **NOC Views** on the top right > Click on the edit icon against the NOC name that you want to edit.
2. Make the necessary changes.
3. Click **Edit NOC View** to effect the changes.

Embedding a NOC view

To embed a NOC view link, follow the steps below.



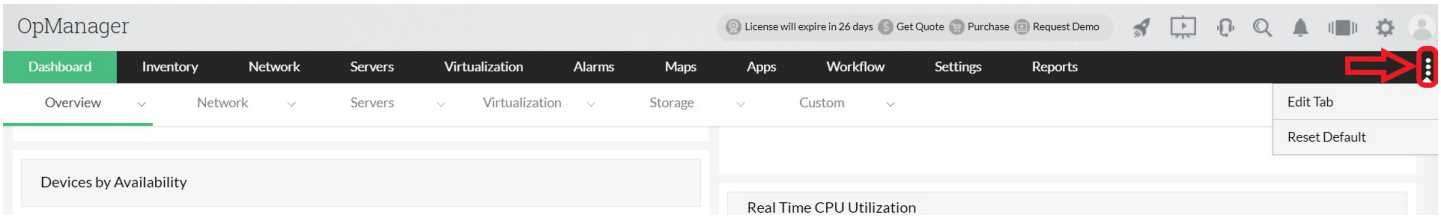
1. Go to the **Dashboard** page and click **NOC** Views on the top right.
2. Click the **Embed icon** present next to the **NOC Name**. The **Embed link** will be displayed.
3. Click the link to copy it to your clipboard. The **NOC Embed link** is ready to be shared.
4. Click the **Regenerative Private link** icon present towards the bottom of the **Embed link box** to generate a new embed link. This will **deactivate** the embedded link generated previously.

Note:

- The NOC embed URL allows a viewer to modify or customize it as per his/her requirements. However, the change will not be saved on the server. If any new user accesses the same NOC view using the embed link, he/she will be loaded with the default version.

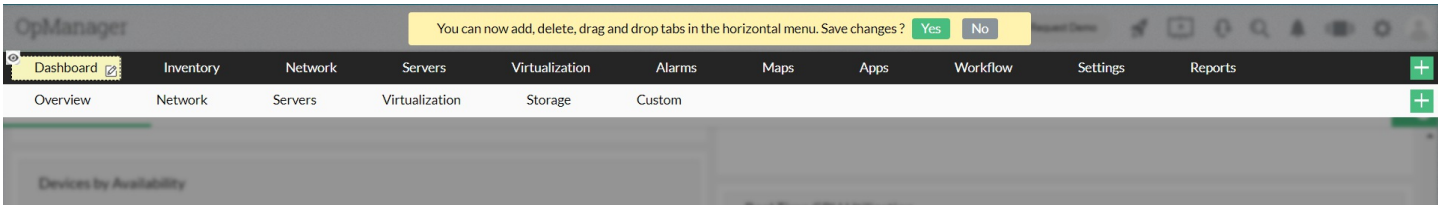
Menu Tab Customization

By default, OpManager comes with features arranged into menus and submenus based on their functionality. You can now fully customize the default menu layout using the **Menu Tab customization** option in a matter of minutes. Click on the three dots at the top right corner to access the Menu Tab Customization options and start customizing your menu as per your preferences.



1. Drag and drop menu / submenu tabs

The menu and submenu buttons can be rearranged. To do this, click the **Edit** button on the right corner and dragging the menu / submenu that you want to rearrange to its desired location. Click **Yes** to save the changes.

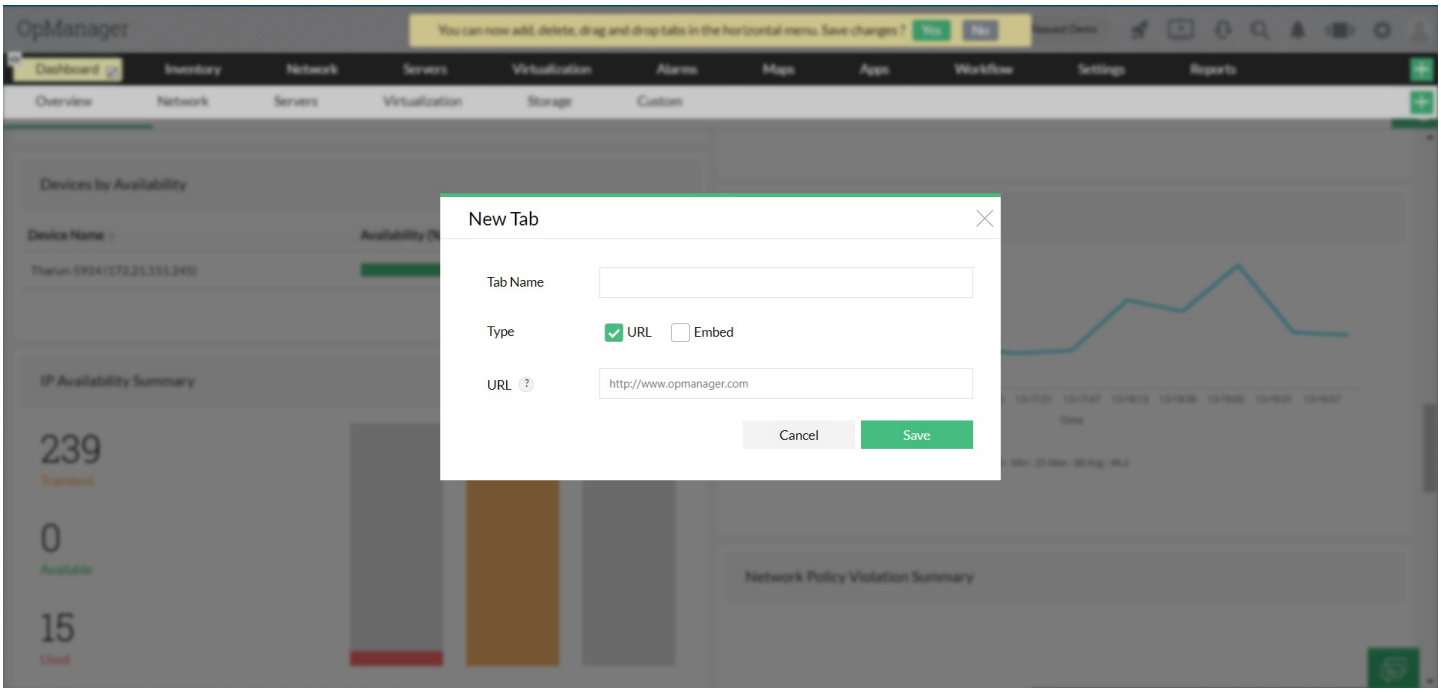


2. Add a menu / submenu tabs (with URL / Embed URL in it)

To create an additional menu / submenu, click the **Edit** option and select the **Plus** icon. You can now create a new menu/sub menu from one of the two types.

- URL - Enter an URL of your choice. Choosing this option will open the entered URL in a new browser tab.
- Embed - Add an URL of your preference. Choosing this option will open the specified URL in an embedded view within the product.

> **Note**: The page will not be displayed if the embedded page has an X-Frame-Options header that is set to restrict embedding in the frame.



3. Hide default menu / submenu tabs

The default menu / submenu that is present and cannot be deleted. However, they can be hidden.

To hide the default menu/sub menu, choose **Edit** and select the **Visibility icon** (eye shaped) that is present in the top left corner of all the default menu/sub menu tabs. when you click on it, the tab becomes faded out. (which means this tab is hidden) Click **Yes** to confirm the changes.

Click the eye icon on the faded out tab to make it visible again.

> **Note**: Only default tabs can be hidden.

4. Delete custom menu / submenu tabs

To delete a menu / submenu that was created by you, click the edit option and click on the red cross on the top right corner of the tab. This will delete the respective tab. Press **Yes** to save progress.

The default menu / submenu cannot be deleted. However, they can be hidden by clicking on the eye icon present at the top left corner of the tabs.

5. Rename the menu / submenu tabs

To rename the menu / submenu tabs, click on **Edit** and select the **Pencil** icon on the tab whose name has to be changed. Enter the new name and click the save button.

6. Reset Default menu / submenu tabs

Choose **Reset Default** to restore default settings of all the menu / submenu. This will erase all the custom tabs created by that particular user.

Press **Yes** to confirm reverting to default settings.

7. Customize user-specific menu / submenu with that user login

The changes made in the menu/submenu are mapped to the particular user who has made them. The next time this particular user logs in, all their saved preferences will be loaded.

> **Note**: Admin user cannot set a defined menu / submenu for any user.

Client Settings

Change Password

- To change the Login Password, click **Client Settings** icon > **Change Password**
- Provide the **Current Password**
- Provide the **New Password**
- Provide the new password again in **Re-type password**
- Click **Save**

Change Language

OpManager is available in English, Spanish, Chinese Simplified, Japanese, French, German, Korean and Italian languages. The following are the steps to change OpManager from one language to other supported language.

- To change the OpManager language, click **Client Settings** icon > **Language Selector**
- Select your preferred language

Keyboard Shortcuts for Quick Navigation

Click **Client Settings** icon > **Keyboard Shortcuts**

ALT + C	Clear Alarm
ALT + H	Home Dashboard
ALT + S	Server Dashboard
ALT + N	Network Dashboard
ALT + SHIFT + I	IPAM Dashboard
ALT + I	Inventory
ALT + W	Workflow
ALT + M	Maps
ALT + V	Virtualization
ALT + L	Group Chat
ALT + SHIFT + A	About
ALT + Q	Submit Query
CTRL + ALT + 1	View Logs
ALT + SHIFT + S	Screenshot feedback

ServiceDesk Plus Integration

ServiceDesk Plus software can be integrated with OpManager using this shortcut

- To integrate ServiceDesk Plus with OpManager, click **Client Settings** icon > **ServiceDesk Plus**
- Configure all the required parameters
- Click **Save**

To send a screenshot feedback to OpManager support

- To send a screenshot feedback to OpManager support, click **Client Settings** icon > **Screenshot Feedback**
- Alternatively, you can use the keyboard shortcut **Alt + SHIFT + S**
- Screenshot of the selected portion of the screen will be taken and a text box will appear on top to add the feedback. Enter the feedback
- Click **Submit**

To sign out as current user from OpManager client

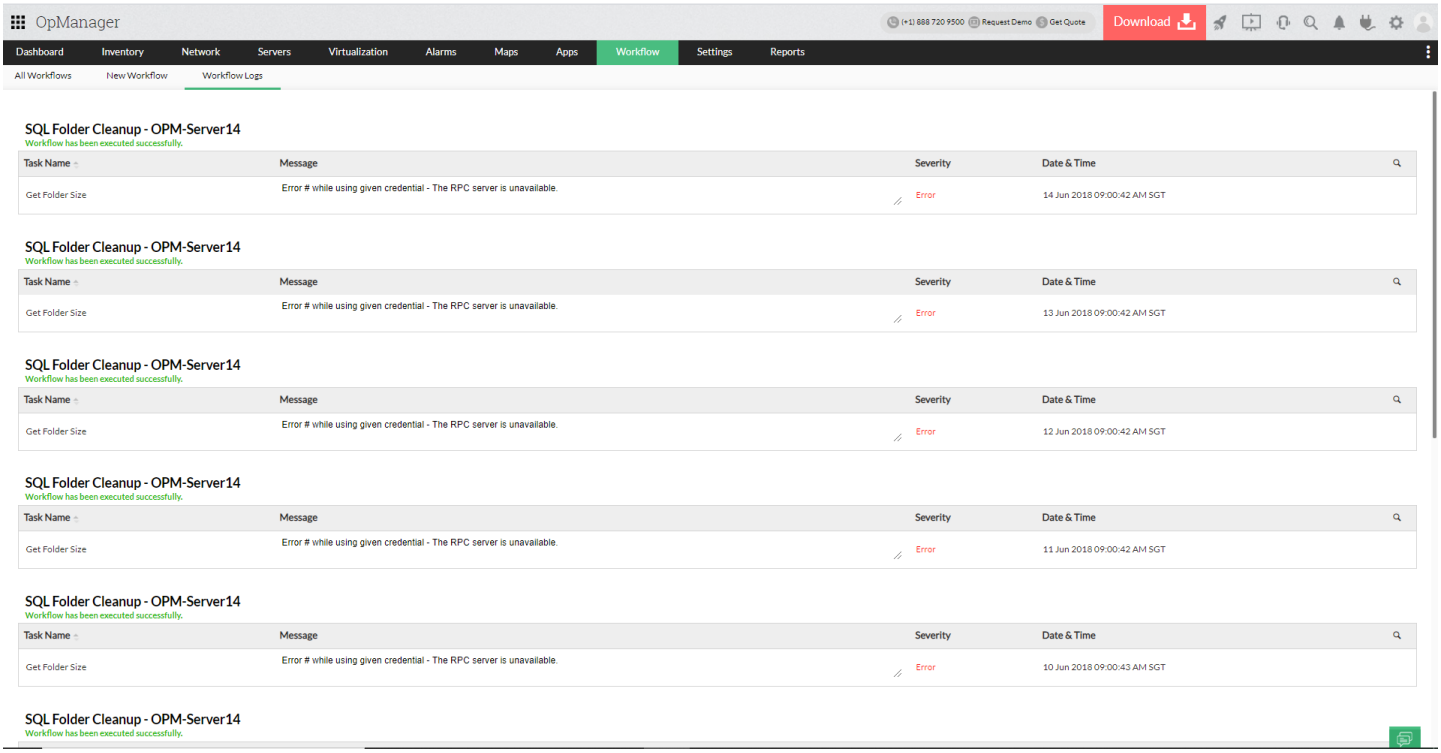
- To sign out as current user from OpManager client, click **Client Settings** icon > **Sign Out**

Workflow Execution Logs

Workflow Logs provide the ouput of the executed workflows. It provides the result as well the data of each task that had been included in the workflow.

To view Workflow logs

- Click on **Workflows** from the left pane and select **Workflow Logs**. Workflow output for each of the associated device is listed along with the executed date & time and numnber of tasks.



Severity

Each task once executed is logged with its severity for understanding its execution status. Following are the severities in Workflow:

- **Info**: Notifies a task has been executed successfully.
- **Error**: Notifies a task has been failed.
- **Warning**: Notifies that a task cannot be performed. Eg.: A delete file action cannot be performed when the directory does not have the specified file. In such cases, the delete file actions is marked as warning

Workflow Tasks

Tasks are nothing but checks and actions that help you automate IT actions that are repetitive.

Checks:
Checks are if-else condition based. If the condition is passed/satisfied, the workflow executes the set of actions associated on the success part, executes the other set of actions associated on the failure part. Example: Consider that you have created a workflow with Test a Service, Send Mail, and Start a Service tasks. Send Mail is associated on the success part of Test a Service, and Start a Service is associated on the part. If the service is running, workflow executes Send Mail task to notify the admin that the service is running, else executes Start a Service task to start the service.

Actions:
An action just performs the said activity. Tasks such as start a service, delete file, reboot system are action tasks. If an action task is executed successfully, workflow executes the next successive task. If an action task fails, action task associated on the failure part is executed. Example: Consider that you have created a workflow with 2 action tasks - Start Process and List All Process. List All Process is associated to the success part of the Start Process task. When the workflow is executed, in case if the Start Process task fails, workflow looks for the task associated on the failure section. If no task is found, the workflow executes the task in the success section i.e., List All Process.

Conditions and Actions available in Workflow

Device	
Checks	**Description**
DNS Lookup	Executes a DNS lookup command on the end device.
Ping Device	Sends ICMP packets to the end device.
Trace Route	Executes a trace route command on the end device.
Actions	
Add a Time Delay	Adds a delay to the execution of an action
Reboot System	
Reboots the system	
Shut Down System	Shuts down the system
Windows Service	
Check	
Test a Service	Tests whether a service is running or not.
Actions	
Get Active Services	Provides a list of service that are currently running.
Pause a Service	Pauses a service.
Restart Service	Restarts a service.
Resume a Service	Resumes a service.
Start a Service	Starts a service.
Stop a Service	Stops a service.

Process	
Check	**&#65533;**
Test a Process	Test whether a process is running or not.
Actions	**&#65533;**
List All Processes	Lists all the processes that currently running.
Processes by Disk Read	Lists processes by Disk Read.
Processes by Disk Write	Lists processes by Disk Write.
Processes by Memory Usage	Lists processes by Memory usage.
Processes by CPU Usage	Lists processes by CPU usage.
Start Process	Starts a process.
Stop Process	Stops a process.
&#65533;	**&#65533;**
HTTP & FTP	
Check	**&#65533;**
Check URL	Test the availability of a URL.
Actions	**&#65533;**
FTP Delete File	Deletes a file via FTP.
FTP Move File	Moves a file within the same remote device via FTP.
FTP Rename File	Renames a files via FTP.
FTP Upload File	Writes the given content in a file (.txt) and uploads it to the remote device via FTP.
HTTP Post Data/Result	Posts the output received upon querying an URL, in the workflow logs.
&#65533;	**&#65533;**
File	
Checks	**&#65533;**
Check File	Checks the availability of a file.
Get File Size	Gets the size of a file.
Actions	**&#65533;**
Compress Files	Files are compressed with Windows Compression.
Compress Older Files	Files which are not used for a long time are compressed with Windows Compression. You can configure the age of the files.
Copy File	Copies file to another directory within the same device.
Delete File	Deletes a file.
Delete Older Files	Deletes the files which are not used for a long time. Also deletes older files in sub folders. You can configure the age of the files.
Move File	Moves the files to another directory within the same device.

Move Older Files	Moves the files which are not used for a long time to another directory within the same device. You can configure the age of the files.
Rename File	Renames a file.
Uncompress File	Uncompresses a file.
&#65533;	**&#65533;**
Folder	
Checks	**&#65533;**
Check Drive Free Space	Checks for free space available in a drive.
Get Folder Size	Gets the size of a folder.
Actions	**&#65533;**
Compress Folder	Compresses a folder.
Copy Folder	Copies the folder to another local directory.
Create Folder	Creates a folder.
Delete Folder	Deletes a folder.
List Files	List the files available in a folder.
Move Folder	Moves a folder to another location.
Rename Folder	Renames a folder.
Uncompress Folder	Uncompresses a folder.
&#65533;	**&#65533;**
VMware	
Actions	**&#65533;**
Power Off VM	Turns off the power to a VM.
Power On VM	Turns on the power to a VM.
Reboot Guest OS	Restarts a VM.
Refresh Datastore	Refreshes the datastore.
Reset VM	Resets a VM abruptly.
Shut Down Guest OS	Shuts down a VM.
Stand by Guest OS	Puts a VM in the Stand By mode.
Suspend VM	Suspends a VM.
Take snapshot	Takes a snapshot of the current state of the VM server.
&#65533;	**&#65533;**
OpManager	
Check	**&#65533;**
Check Device Status	Checks the availability status of a device.
Actions	**&#65533;**
Acknowledge Alarm	Acknowledges an alarm.
Add Alarm Note	Adds a note to an alarm.

Clear Alarm	Clears an alarm.
Delete Alarm	Deletes an alarm.
Exit Maintenance	Moves the device under maintenance mode to normal.
Generate Alarm	Generates an alarm in OpManager.
Place on Maintenance	Puts the device on maintenance mode.
Rediscover Device	Rediscovers a device and automatically updates all device related details.
Unacknowledge Alarm	Unacknowledges an alarm.
****	****
External Actions	
Actions	****
Execute Another Workflow	Executes another workflow as an action.
Execute Linux Script	Executes a script on the end Linux devices.
Execute Windows Script	Executes a script from the installed server on OpManager.
Log a Ticket (Remedy)	Creates a ticket in BMC Remedy.
Log a Ticket (SDP/ServiceNow)	Creates a ticket in ManageEngine ServiceDesk Plus/ ServiceNow respectively.
Send Email	Sends a notification via Email. Ensure that you have configured Mail server settings.
Send Popup Message	Sends a notification via a pop-up on the end device. At present Workgroup devices alone are supported.
Send SMS	Sends a notification via SMS. Ensure that you have configured SMS server settings.
Send Slack Message	Sends a notification in Slack as per the given condition.
****	****
NCM Actions	
Actions	****
Backup	Takes backup of device configuration files
Execute Command	Executes a command on the end device
Execute Template	Executes a template created in NCM Plug-in on the end device
Get Last N Changes	Fetches the last N configuration changes made

****

DNS Lookup:

DNS Lookup executes a DNS lookup command on the end device and provides its status.

Parameter	**Description**
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select devices icon to select the device. If no device is selected, it will be executed on the device selected in the Info tab.

****

Ping Device:

Sends ICMP packets to test whether the device is responding.

Parameter	Description
Name	Display name for the task
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Number of requests	Number of ping requests you want to send.
Packet Size	Size of the ping packets.
Timeout	Timeout interval for the ping requests.
Retries	Number of retries for the ping operation.

Trace Route:

Executes a trace route command on the end device.

Parameter	Description
Name	Display name for the task
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device.

Add a Time Delay:
Adds a delay to the execution of the subsequent operation.

Parameter	Description
Name	Display name for the task.
Duration	Time delay to carry out the subsequent task. You can configure time delay in hours, minutes, and seconds. Select the required one from the dropdown menu.

Reboot System:
Reboots a remote Windows machine.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device.

Shut Down System:

Logs off, shuts down, reboots or powers off a remote Windows device forcefully.

Parameter	Description

Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select devices icon to select the device. You can also log off by selecting the Log Off action from the dropdown.
Options	Select the action (Log off, Shut down, Reboot or Power off) that you want to carryout on the remote device.

Test a Service

Tests whether a service is running or not.

Parameter	**Description**
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select devices icon to select the device. Supported Variable: ${Alarm.ServiceName} - Select this option if you want to retrieve the service name from the alarm entity. If the workflow is triggered from the service down alarm, then this variable is replaced by the servicename from the alarm entity during runtime. Note: If multiple services down alarm is triggered, this task will be executed for all those services.
Service Name	Name of the service that you want to task whether it is running or not. Use the dropdown menu to select the service. If the service is not listed, use the discover icon to discover the services running the device.

Get Active Services

Provides the list of active services running in the device.

Parameter	**Description**
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select devices icon to select the device.

Pause/Restart/Resume/Start/Stop a Service

Pauses/Restarts/Resumes/Starts/Stops a service.

Parameter	**Description**
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select devices icon to select the device.

Service Name	Name of the service that you want to pause/restart/resume/start/stop. Use the dropdown menu to select the service. If the service is not listed, use the discover icon to discover the services running the device. Supported Variable: ${Alarm.ServiceName} - Select this option if you want to retrieve the service name from the alarm entity. If the workflow is triggered from the service down alarm, then this variable is replaced by the servicename from the alarm entity during runtime. Note: If multiple services down alarm is triggered, this task will be executed for all those services.

Test a Process

Tests whether a process is running or not.

Parameter	**Description**
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select devices icon to select the device.
Process Name	Name of the process that you want to test. Either you can enter the process name right away (Eg.:mysqld-nt.exe) or you can use the select icon to select the process from the remote devices.
Path	This field is optional. If you want to match the path also, then check the checkbox near path field and specify the full executable path with process name. Otherwise leave this field empty. Eg.: C:Program FilesMySQLMySQL Server 5.0binmysqld-nt.exe
Arguments	This field is also optional. If you want to match the arguments, then check the checkbox near arguments field and specify the arguments. Otherwise leave this field empty. Eg.: --defaults-file="my.ini"

List All Processes/Processes by Disk Read/Processes by Disk Write/Processes by Memory Usage/Processes by CPU Usage

Provides the list of active services, processes by disk read/disk write/Memory usage/CPU usage.

Parameter	**Description**
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select devices icon to select the device.

Start Process

Starts a process.

Parameter	**Description**
Name	Display name for the task.

Destination Device	Device on which the task has to be executed. Click on the select devices icon to select the device.
Start Directory	The directory from where you want to execute the process.
Process Command	Command to start the process.

Stop Process

Stops a process running on a device.

Parameter	**Description**
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select devices icon to select the device.
Process Name	Name of the process that you want to test. Either you can enter the process name right away (Eg.:mysqld-nt.exe) or you can use the select icon to select the process from the remote devices.
Path	This field is optional. If you want to match the path while terminating the process, then check the checkbox near path field and specify the full executable path with process name. Otherwise leave this field empty. Ex: C:Program FilesMySQLMySQL Server 5.0binmysqld-nt.exe Note: If the checkbox is unchecked and multiple instance of process is running with the same name, all the processes will be terminated.
Arguments	This field is also optional. If you want to match the arguments when terminating the process, select the checkbox near arguments field and specify the arguments. Otherwise leave this field empty. Ex: --defaults-file="my.ini" Note: If the checkbox is unchecked and multiple instance of process is running with the same name, all the processes will be terminated.

Check URL

Check whether the URL for its availability.

Parameter	**Description**
Name	Display name for the task.
URL Address	Address of the HTTP URL that has to be queried. Supported Variables : ${Alarm.URLAddress} - will retrieve the URLAddress from the alarm entity, if workflow is triggered through alarm. Otherwise nothing will happen.
Form Method: Get or Post	OpManager tests the URL via Get or Post method. Select the appropriate condition.
Search and Match Content	The content specified here is verified for its presence in the web page.

Timeout	Timeout interval for the URL. Default value is 25 seconds. Click on check now button to verify the URL.
URL Authorization Details	Provide the username and password for URLs that require authentication.
Check Now	Checks whether the URL is accessible with the entered details.

FTP Delete File

Deletes a file via FTP.

Parameter	Description
Name	Display name for the task.
FTP Server	Name of the FTP Server. You can enter the ftp server name directly or use '${DeviceName}' variable. '${DeviceName} will be replaced with the name device selected in the Info tab, during the workflow execution.
FTP Username	Username of the FTP server.
FTP Password	Password to connect to the FTP server.
File Name	Name of the file to be deleted. Enter the file name with the path.

FTP Move File

Move a file to another directory within the same system via FTP.

Parameter	Description
Name	Display name for the task.
FTP Server	Name of the FTP Server. You can enter the ftp server name directly or use '${DeviceName}' variable. '${DeviceName} will be replaced with the name device selected in the Info tab, during the workflow execution.
FTP Username	Username of the FTP server.
FTP Password	Password to connect to the FTP server.
File Name	Name of the file to be moved. Enter the file name with the path.
Destination Folder	Destination folder where the file to has to be moved. Enter the path.

FTP Rename File

Renames a file via FTP.

Parameter	Description
Name	Display name for the task.
FTP Server	Name of the FTP Server. You can enter the ftp server name directly or use '${DeviceName}' variable. '${DeviceName} will be replaced with the name device selected in the Info tab, during the workflow execution.
FTP Username	Username of the FTP server.
FTP Password	Password to connect to the FTP server.

Source File	Name of the file to be renamed. Enter the file name with the path. Eg.:/root/OpManager/backup/Backup_DB.zip
New Name	New name for the file. Eg.: Backup_DB_Old.zip

FTP Upload File

Writes the given content in a file (.txt) and uploads it to the remote device via FTP.

Parameter	**Description**
Name	Display name for the task.
FTP Server	Name of the FTP Server. You can enter the ftp server name directly or use '${DeviceName}' variable. '${DeviceName} will be replaced with the name device selected in the Info tab, during the workflow execution.
FTP Username	Username of the FTP server.
FTP Password	Password to connect to the FTP server.
Directory	Directory where the file has to be uploaded.
Content	Content/value that has to be uploaded

HTTP Post Data/Result

Posts the output received upon querying an URL, in the workflow logs.

Parameter	**Description**
Name	Display name for the task.
URL Address	Address of the HTTP URL that has to be queried. Supported Variables : ${Alarm.URLAddress} - will retrieve the URLAddress from the alarm entity, if workflow is triggered through alarm. Otherwise nothing will happen.
Form Method: Get or Post	OpManager tests the URL via Get or Post method. Select the appropriate condition.
Search and Match Content	The content specified here is verified for its presence in the web page.
Timeout	Timeout interval for the URL. Default value is 25 seconds. Click on check now button to verify the URL.
URL Authorization Details	Provide the username and password for URLs that require authentication.
Check Now	Checks whether the URL is accessible with the entered details.
Post Data	The content specified here will be displayed in the execution logs. Supported Variables : ${URLAddress} - will replace the address specified in the URL Address field. ${Result} - will replace the response obtained from the URL Address.

Check File

Checks the existence of a file in the specified path.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
File Name	Name of the file that has to be checked for its existence. Specify the file name with its path.

Get File Size

Checks the file for its size and execute tasks accordingly.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
File Name	Name of the file that has to checked for its size. Specify the file name with its path.
File Size	The size of the file is compared with the value specified here. According to the condition (greater or lesser than) selected the actions are executed.

Compress File/Delete File

Compresses a file with Windows Compression/Deletes a file.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
File Name	Name of the file that has to be compressed/deleted. Specify the file name with its path.

Compress Older Files/Delete Older Files

Compresses older files with Windows Compression/deletes older files.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Folder Name	Folder that contains the old files. Specify the folder path. Note: Delete older files option, deletes the older files in the sub folders also.
Files Older Than	Files older than the specified number of months/days/hours are compressed/deleted.

Copy File/Move File

Copies/moves a file from one folder to another within the same computer.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
File Name	Name of the file that has to be copied/moved to another folder. Specify the file name with its path.You can use the wild card character * (eg.: stderr*.txt) to do the action on all the files. You can also enter multiple files separated by a comma.
Destination Folder	Name of the folder where the file has to be pasted/moved. Specify the folder path.

Move Older Files

Moves files that match the age specified to another folder.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Source Folder	Folder that contains the old files. Specify the folder path.
Destination Folder	Folder to which the old files have to be moved to.
Files Older Than	Files older than the specified number of months/days/hours are moved.

Rename File

Renames a file.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Source File Name	Specify the source file name to be renamed Eg.: C:Program FilesOpManagerbackupBackup_DB.zip
New Name	New name for the file. Eg.: Backup_DB_Old.zip

Uncompress File

Uncompresses a file that had been compressed with Windows Compression.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
File Name	Name of the file that has to be uncompressed. Specify the file name with its path. You can use the wild card character * (eg.: stderr*.txt) to do the action on all the files. You can also enter multiple files separated by a comma.

Check Drive Free Space

Checks the free space available in a drive.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Drive Name	Name of the drive that has to checked for free space.
Drive Size	The size of the drive is compared with the value (GB/MB/KB) specified here. According to the condition (greater or lesser than) selected the actions are executed.

Check Folder Exists

Checks the existence of a folder in the specified path.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
File Name	Name of the folder that has to be checked for its existence. Specify the folder path.

Get Folder Size

Checks the free space available in a drive.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Folder Name	Name of the folder that has to checked for its size.

Folder Size	The size of the drive is compared with the value (GB/MB/KB) specified here. According to the condition (greater or lesser than) selected the actions are executed.

Compress /Uncompress/Delete Folder

Compresses/uncompresses/deletes a folder.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Folder Name	Folder that has to be compressed/uncompressed/deleted. Specify the folder path.

Create Folder

Creates a folder in the computer.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Folder Name	Name of the folder that has to be created. Specify the folder name with its path.

Copy Folder/Move Folder

Copies/moves a folder to another folder within the same computer.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Folder Name	Name of the folder that has to be copied/moved to another folder. Specify the file name with its path.
Destination Folder	Name of the destination folder where the source folder has to be pasted/moved. Specify the folder path.

List Files

List the files available in a folder.

Parameter	Description
Name	Display name for the task.

Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Folder Name	Name of the folder whose files has to be listed. Specify the folder path.

Rename Folder

Renames a folder.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Source Folder	Specify the source folder name to be renamed Eg.: C:OpManagerlogs
New Name	New name for the folder. Eg.: logs_old

Add Alarm Note

Adds note to an alarm.

Parameter	Description
Name	Display name for the task.
Note	Note that has to be added to the alarm. Supported Variables : ${Result} - will be replaced with the previously executed task's result.

Generate Alarm

Generates an alarm in OpManager.

Parameter	Description
Name	Display name for the task.
Source	Note that has to be added to the alarm. Supported Variables : ${Result} - will be replaced with the previously executed task's result.
Severity	Select the severity of the alarm.
Message	Message that you want to display in the alarm.
Alarm Code	Unique string used to trigger the event. Eg:-Threshold-DOWN

Entity	Uniquely identifies the failure object within the source.Events will be correlated into alarms according to the entity field. Multiple events with the same entity will be grouped as a single alarm.
Event Type	Description of the event type

Execute Linux Script

Execute script on remote Linux machines and retrieves the output. Depending on the input, this script will either execute from OpManager server or from remote machine. Its success/failure is decided based on its exit code. If the script returns with the exit code 0, then it is consider as success, any other value is consider as failure.

Eg.: For shell script,
exit(0) -- Success
exit(1) -- Failure
exit(-2) -- Failure

Parameter	**Description**
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Command Line	Specify the command used to execute the script. Eg.: sh ${FileName} ${DeviceName} arg1 Here, ${FileName} variable is a must to execute the script. OpManager will replace this variable during runtime. Supported Variables : ${DeviceName} - will replace the executing devicename during runtime. ${UserName} - will replace the device username if already given for this device. ${Password} - will replace the device password if already given for this device.
Script Body	The actual script that has to be executed.
Advanced	Click on Advanced button to configure the following fields.
Execute from Remote Machine	If this option is checked, the script is pushed to remote machine and will be executed. Otherwise it will be executed from OpManager server.
Working Directory	Specify the directory from where you want to execute the script. Supported Variables : ${UserHomeDir} - will replace the user's home directory during runtime. ${TempDir} - will replace device temp directory during runtime. Eg: /tmp
Response Timeout	Time to wait for the script to complete its execution. The default value given here is 60 seconds.

Execute Windows Script

Script execution is done by the OpManager server on the destination Windows machines and retrieves the output. Its success/failure is decided based on its exit code.

If the script returns with&#65533; the exit code 0, it is consider as success, any other value is consider as a failure.

Eg.: for VBscript:
WScript.Quit(0) -- Success
WScript.Quit(1) -- Failure
WScript.Quit(-2) -- Failure

&#65533;

Parameter	**Description**
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Command Line	Specify the command used to execute the script. Eg. : cscript ${FileName}.vbs ${DeviceName} ${UserName} ${Password} arg1 Here, ${FileName} variable is must to execute the script.&#65533; OpManager will replace this variable during runtime. Supported Variables : ${DeviceName} - will replace the executing devicename druing runtime. ${UserName} -&#65533; &#65533; will replace the device username if already given for this device. ${Password} - will replace the device password if already given for this device.
Script Body	The actual script that has to be executed.
Advanced	Click on Advanced button to configure the following fields.
Working Directory	Specify the directory from where you want to execute the script. Supported Variables : ${UserHomeDir}&#65533; - will replace the user's home directory during runtime. ${TempDir} - will replace OpManager temporary directory during runtime. &#65533;
Response Timeout	Timeout interval for the response from the device for the script execution status.

&#65533;

Log a Ticket (Remedy)

Logs a ticket in BMC Remedy.

Parameter	**Description**
Name	Display name for the ticket.
From Email ID	Email ID of the sender.
Service Desk Mail ID	Email ID of BMC Remedy service desk.
Impact	Select the impact level of the ticket.
Urgency	Select the severity of the ticket.
Summary	Add summary for quick understanding of the issue reported.
Description	Describe the issue.

&#65533;

Log a Ticket (SDP)

Logs a ticket in ManageEngine ServiceDesk Plus. Ensure that ServiceDesk Plus is integrated with OpManager.

Parameter	Description
Name	Display name for the ticket.
Category	Select the appropriate category for the ticket.
Sub Category	Select the appropriate sub category.
Item	Select the appropriate item.
Priority	Select the priority level of the ticket.
Group	Select the group.
Technician	Select the technician to whom you want to assign the ticket.
Title	Subject of the ticket. You can use variables.
Description	Describe the issue. You can use variables.

Send Mail

Sends a mail to the email IDs specified. This is useful to notify the result/completion of a task in the workflow.

Parameter	Description
Name	Display name for the task.
From Email ID	Email ID of the sender.
To Mail ID	Email ID of of the recipients.
Mail Format	Email can be sent in plain text or html or in both the formats. Select the required format.
Subject	Subject of the email. You can use variables.
Message	Content of the email. You can use variables.

Send Popup Message

Opens a popup window with the given message on remote computers.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Message	Message that has to be displayed in the popup.

Send SMS

Sends SMS notifications to the mobile number specified. This is useful to notify the result/completion of a task in the workflow.

Parameter	Description
Name	Display name for the task.

Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Message	Message that has to be sent as an SMS. Message should not exceed 160 characters.

Send Slack Message

Parameter	**Description**
Name	Display name for the task.
Destination	The message can be sent to a single member or to a specific channel.
Channel	Select the specific channel for which you want to share the message.
Message Title	A suitable title for the message can be given.
Message Description	Enter the entire message in the description box.

Variables:
Variables are used to append dynamic values in a field of a task. Following are the variables:

${DeviceName} - Name of the device to which workflow has to be associated. Can be used in all fields

${WorkflowName} - Name of the Workflow that is to triggered. Can be used in all fields.

${Result} - Result of previous task.

${Alarm.ServiceName} - Name of the service for which an alarm is raised.

${URLAddress} - URL address

${Alarm.URLAddress} - URL address for which an alarm is raised.

${UserName} - Username of the device.

${Password} - Password of the device.

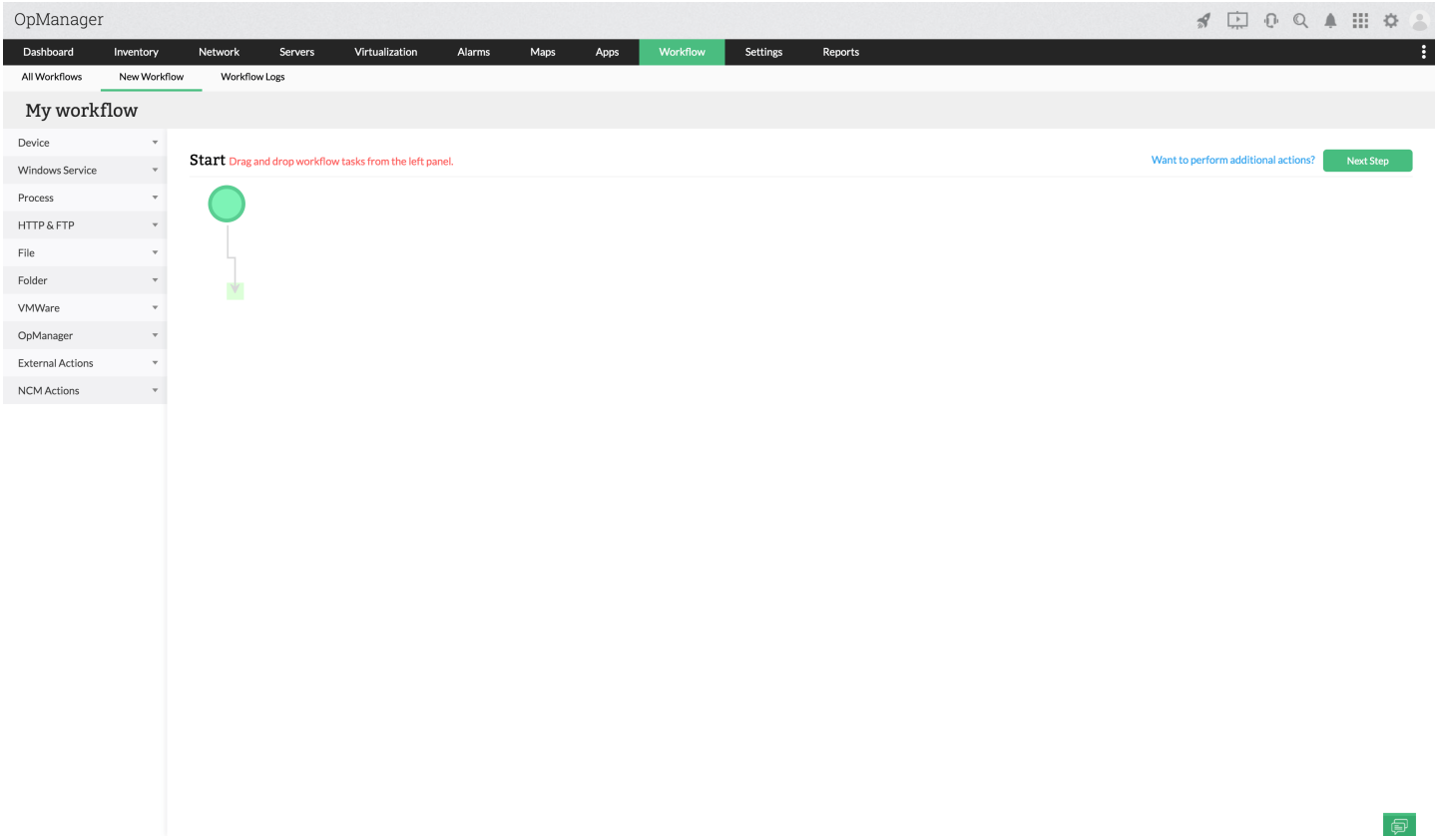
${Device.DisplayName} - Display name of the device for which an alarm is raised.

${Alarm.ProcessName} - Name of the process for which an alarm is raised.

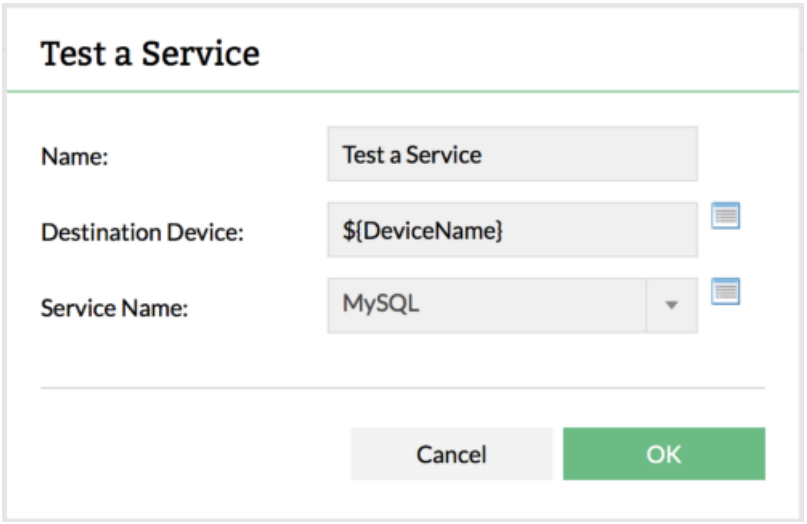
$message - Alarm message will be displayed

Using Variables

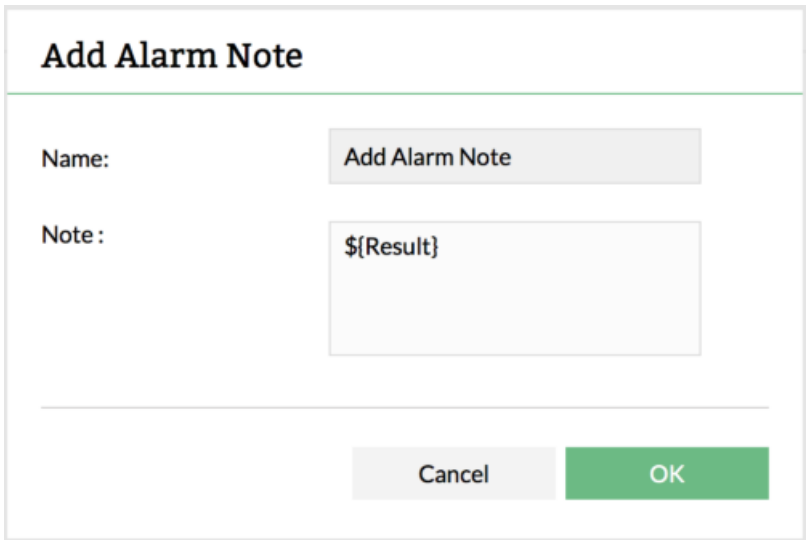
Variables can be better understood with an example. Following is the workflow that has to be triggered as an action whenever a service down alarm is raised.



Task 1: 'Test a service' task is created to test the service that is down. When the workflow is triggered, the variable ${Alarm.ServiceName`} is replaced with the name of the service that has gone down. ${DeviceName} is replaced with the name of device



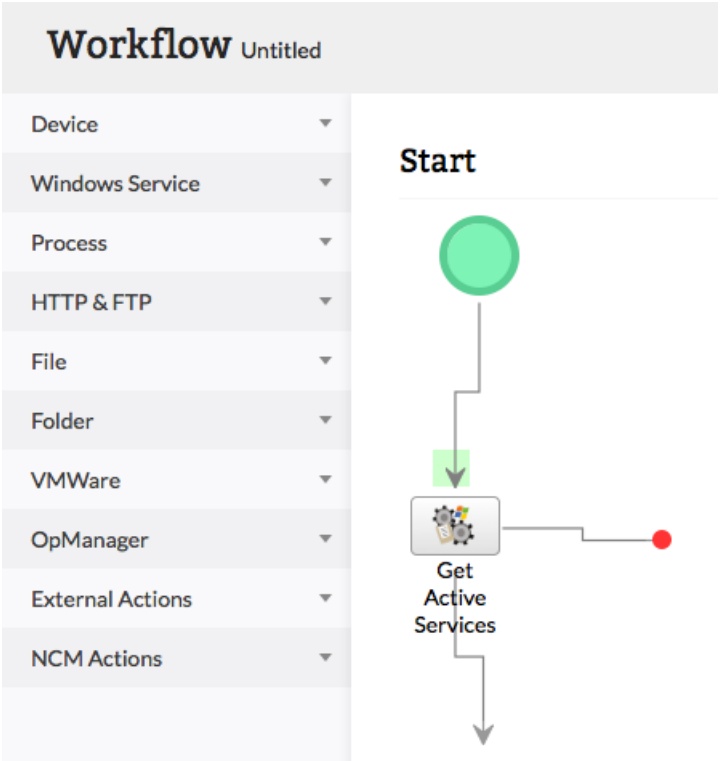
Task 2: The result of previous task (service up or down) is added as notes to the alarm using ${Result} variable.


Add Alarm Note
Name:
Add Alarm Note
Note :
${Result}
Cancel
OK

Adding a Workflow

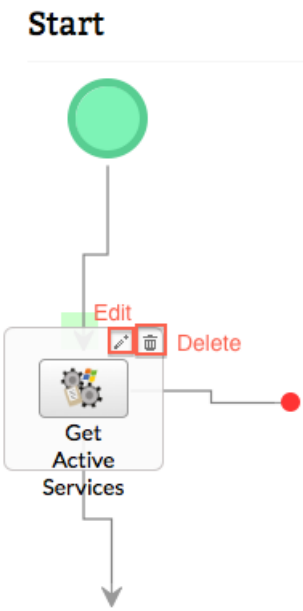
To add a workflow, follow the steps given below:

1. Click on **Workflow** and select **New Workflow**.
2. Drag and drop the required conditions and actions from the left panel to editor panel.





1. Enter a **Name** for the condition and actions.
2. To edit or delete a condition or action, click on it and select edit or delete icon.





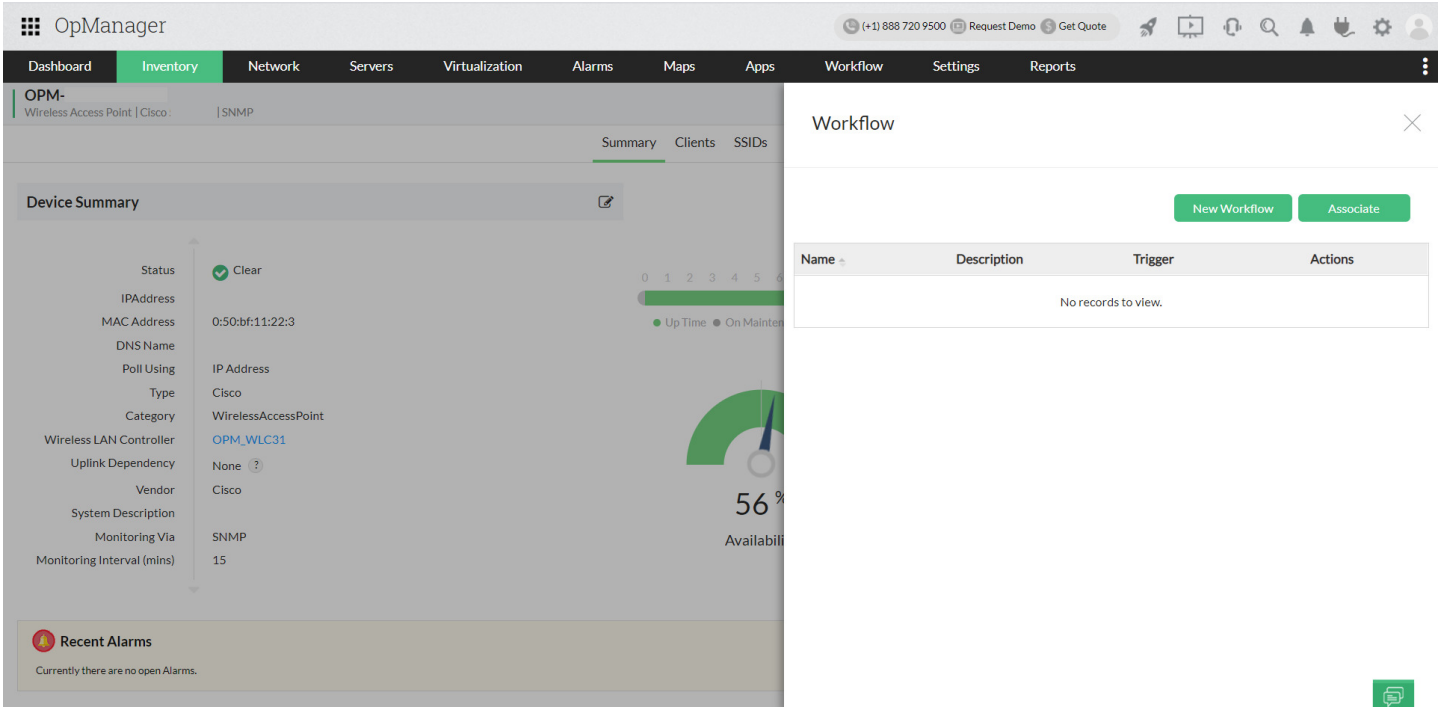
1. Click **Trigger**&#65533; at the top of the page.&#65533;
2. Associate the workflow to the devices.
    a. Click on the&#65533; **Devices** tab.
    b. Select the devices in Available Devices column and move to Selected devices column. Use the search box to search the devices.
    c. Click **Next**
3. Configure the alarm trigger to trigger a workflow when an alarm is raised or configure a schedule trigger&#65533; if you want to schedule this workflow for periodical execution.
    a. Click on the&#65533; **Trigger** tab.
    b. **Alarm Trigger:** Click on the&#65533; **Alarm Trigger**&#65533; option.&#65533; Select the required criteria. Executes this workflow on the associated devices, if any of the criteria is satisfied.
    c. **Schedule Trigger:**&#65533; Click on the&#65533; **Schedule Trigger** option to schedule the workflow action.&#65533; Configure the date and time i.e. you can choose to execute the workflow either once, daily, weekly, monthly or yearly at a specified day/time, based on your preference.
    d. Click **Next**
4. Configure the delayed and recurring triggerring of worflow
    a. Enter a&#65533; **Name**,&#65533; **Description**, and&#65533; **Tags**&#65533; for the workflow.&#65533; &#65533;
    b. Define Time: Select either&#65533; **Apply this profile**&#65533; all time or&#65533; **Apply this profile during the below mentioned time window**. Selecting the latter keeps the Workflow active only during the specified days and hours.
    c. Delayed Trigger: If you want the workflow to be triggered at a delay, enter the delay time (in minutes). If you don't want to trigger the workflow if the alarm has been acknowledged in the mean time, you can select the 'Do not trigger if alarm is acknowledged' check box.
    d. Recurring Trigger: This option helps you trigger the workflow at regular intervals, till the alarm is cleared. Enter the trigger interval and number of triggers. If you don't want to trigger the workflow repeatedly if the alarm has been acknowledged, you can select the 'Do not trigger if alarm is acknowledged' check box.
    e. Click **Save**&#65533;

The workflow has been successfully added. It will be executed on the associated devices at the scheduled time or when any of the criteria selected is satisfied. You can check the output of the workflow in the Workflow Logs.

How to trigger workflow from device snapshot page?

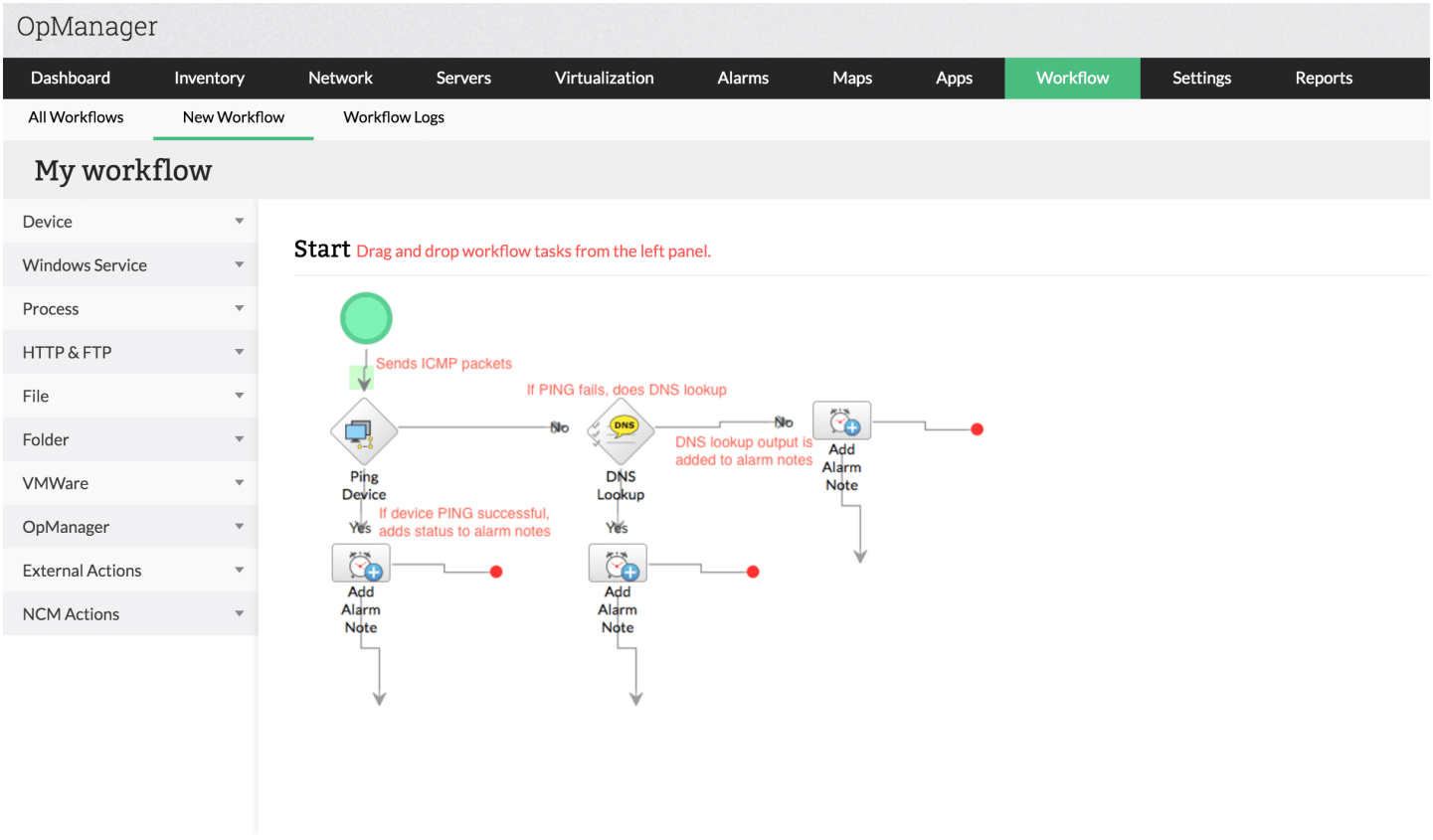
- Navigate to **Inventory** --> **Devices**.
- Click on a particular device, to open its corresponding snapshot page.
- On the top right tab having a list of icons click the workflow icon.
- Click on **New Workflow**. (This will take you to the Workflow page in OpManager)
- You can design your own workflow here.

&#65533;



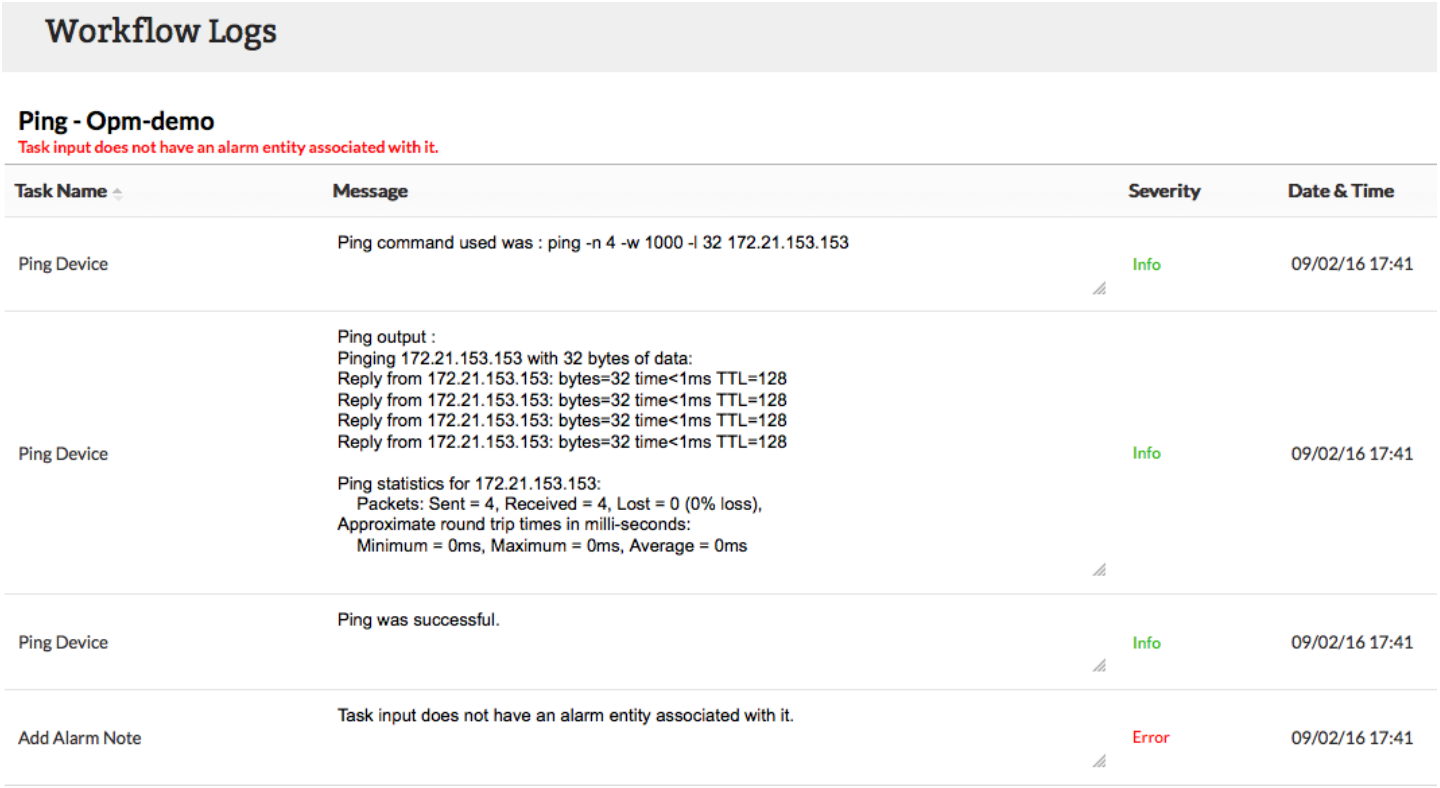
Sample Workflow

Following is a sample workflow which helps gets executed automatically when a device down alarm is raised. This workflow sends ping request, if passed does DNS Lookup and adds the output as notes to the alarm.



Workflow Execution Logs for the sample workflow:

Click on **Workflows** from the left pane and select **Workflow Logs**



Editing a Workflow:

To edit a workflows, follow the steps given below:

1. Click on **Workflows** from the left pane and click on the respective workflow name to edit. 
2. The workflow panel opens. Click **Trigger** button on top to perform the changes you want to do and click **Next**.
3. Modify the name, description, tags, associated devices, schedule, and alarm trigger options if required.
4. Click **Save**



How can I trigger an action in case of any issues in the network?

To trigger an action in case of any/ selective network issues, all you have to do is to create a workflow action with alarm triggers. You can refer the steps above to add a new workflow and select all/ specific triggers as per your requirements.

Executing Workflows

Before executing a workflow, ensure that you have associated the workflow to the devices. To execute a worklow

1. Click on **Workflows** from the left pane. All the created workflows are listed.
2. Click against the Execute icon on the respective workflow.
3. There is also an option to execute the workflow from the device page. Go to Device page > Workflow > click against the execute icon on the respective workflow.

How can I run a powershell script using Execute Windows Script task in Workflow?

1. Go to **Workflow > New Workflow > External Actions > Execute Windows Script.**
2. Drag and drop the **Execute Windows Script** action into the workspace. In the pop-up, configure the **Name**, **Destination Device** and **Command Line**.
3. In **Script Body**, enter the powershell script shown below:

```
Set objShell = CreateObject("Wscript.Shell")
objShell.Run("powershell.exe -noexit c:\scripts\test.ps1")
```

4. Click **OK.**

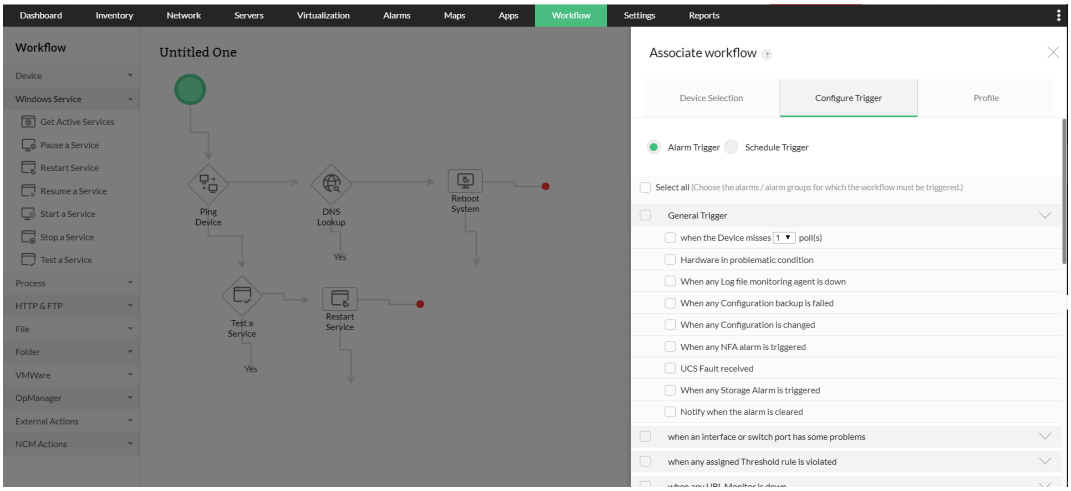
Triggers in Workflow

A Trigger initiates an action in a workflow based on the pre-configured criteria. There are two types of triggers

1. Alarm Trigger
2. Scheduled Trigger

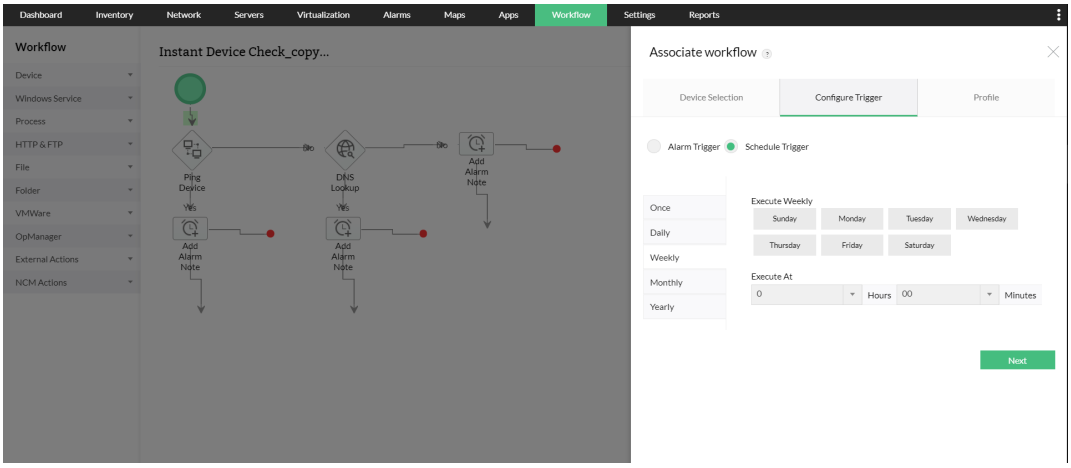
Alarm Trigger

An alarm trigger performs a workflow action when an alarm is generated based on the specified criteria. This alarm will trigger a workflow action. Eg. Let us assume that a General Trigger has been configured to perform a workflow action when a device misses 3 polls. A workflow action will be triggered, when an alarm is generated because the selected remote device missed 3 polls.



Scheduled Trigger

A scheduled trigger will perform a workflow action at the specified time irrespective of any other criteria.



Define Time & Delay/Recurring Trigger in Workflow

Define Time: Select one of the following options

- **Apply this profile all the time**- This activates a workflow action for the selected trigger at any time.
- **Apply the profile for the selected time window**- You can specify a time-window during which period, the workflow will be executed based on the configured trigger. For instance, if you set the values as From 09:30 To 18:30, and select the days from Monday through Friday, the workflow will only be activated during the specified interval i.e. Within the mentioned timeframe.

Delayed Trigger: If you want to perform a delayed workflow action, after an alarm is triggered, enter the delay time in **Trigger after (in minutes)**. If you don't want to trigger a workflow action if the alarm has been acknowledged in the meantime, you can select

the **'Do not trigger if alarm is acknowledged'** checkbox.

Recurring Trigger: This option helps you re-trigger the workflow action at regular intervals, till the alarm is cleared. Enter the **Trigger interval** and **Restrict the number of triggers**, if you want to restrict the number of times the trigger recurs.

For instance, if you set the trigger interval as 10 mins and restrict the number of triggers to 5 times, the workflow action will be triggered every 10 mins, for 5 times or till the alarm is cleared (whichever is the earliest).

If the number of times to trigger the workflow action is not specified, then the workflow action will be re-triggered indefinitely, till the alarm is cleared. If you do not want to trigger a workflow action in case an alarm has been acknowledged, you can select the **'Do not trigger if alarm is acknowledged'** checkbox.

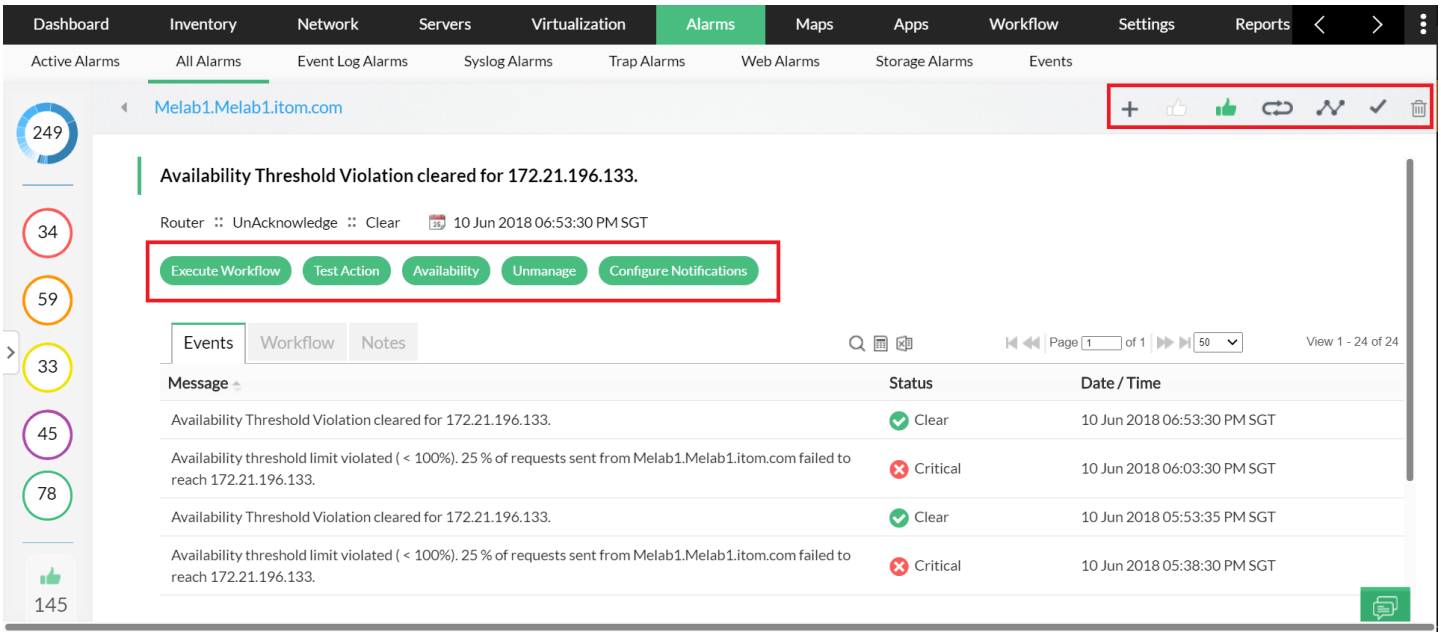
Alert Actions

You can perform the following alert actions:

Acknowledge: This option is useful for the operators to pick up the problem and work on it. When you select an alarm and click on Acknowledge button on top the alarms list, the administrator/operator's name is populated in the technician's field.

Note: Alarms that are acknowledged can be excluded from being escalated by configuring accordingly the alarm escalation rule.

- **Unacknowledge**: The assigned technician is removed and the alarm is back in the unassigned list.
- **Clear**: You can click this to clear an alarm manually.
- **Delete**: You can delete an alarm.
- **View History**: Click on the alarm message to view the alarm details and event history.
- **Add Notes**: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. In the Alarm history page, click the **Add Notes** option.
- **Execute Workflow**: You can execute a workflow to troubleshoot an alarm. Click on **Execute Workflow** in the Alarm Details page, and select the workflow. The workflow will be executed and the output will be added in the notes.
- **Test Actions**: You can notify this alarm via any of the notification profiles created by you. Click on **Test Actions** in the Alarm Details page, and select the desired notification profile.
- **View Availability**: You can view the availability history of the faulty device. Click on **More** link in Alarm Details page and select **Availability**.
- **Ping**: You can ping the faulty device by clicking on the **Ping** icon from the top of the Alarm Details page.
- **Trace Route:** You can trace route the faulty device by clicking on the **Trace Route** icon from the top of the Alarm Details page.
- **Unmanage:** Alarms created for devices that are under maintenance can be can be avoided by moving the device to unmanaged state.
- Click Actions> Select **Unmanage** from Alarm Details page.
- **Configure Notifications**: You can configure a notification profile to the faulty devices. Click Actions> **Configure Notifications** from Alarm Details page.
- **Edit thresholds:** You can configure the threshold values for the criticality levels. If a device fails to meet the threshold conditions then an alarm will be raised.
- **Test monitor:** You can use the test monitor to check whether the monitor is fetching data.



Notification Profile

When a fault is detected in your network, an event occurs and multiple events correlate to trigger an alarm. You can configure OpManager to notify the network administrator or perform automatic actions based on the alarm raised for a device using the notification profiles.

Profile Types

The different types of notification profiles available are:

- Email
- Email based SMS
- SMS
- Run a System Command
- Run a Program
- Log a Ticket
- Web Alarm
- SysLog Profile
- Trap Profile

These notification profiles can be associated to different devices for different fault criteria.

Other Configurations of Notification Profiles

Time Window: Select one of the following options:

- **Apply this profile all the time- This notifies alerts occurring for the selected criteria at any time.**
- **Apply the profile for the selected time window**- You can specify the required time- window here. For instance, if you set the values as From 09:30 To 18:30, and select the days from Monday through Friday, alerts triggered during the specified interval and selected days only will be notified.

Delayed Trigger: If you want the notification profile to be triggered by a delay, enter the delay time in Trigger after (in minutes). If you don't want to trigger the notification profile if the alarm has been acknowledged in the meantime, you can select the 'Do not trigger if alarm is acknowledged' checkbox.

Recurring Trigger: This option helps you re-trigger the notification profile at regular intervals, till the alarm is cleared. Enter the Trigger interval and Restrict the number of triggers to. For instance, if you set trigger interval as 10 mins and restrict the number of triggers as 5 times, an alert will be notified every 10 mins, for 5 times or till alarm is cleared(Whichever is earliest). If the number of triggers is set as empty, then alert will be notified for given interval, till the alarm is cleared. If you don't want to trigger the notification profile repeatedly if the alarm has been acknowledged, you can select the 'Do not trigger if alarm is acknowledged' checkbox.

Enable/ Disable a Notification Profile

In case you want to temporarily disable a notification profile, you can follow the simple steps listed below.

1. Go to **Settings -> Notifications -> Notification Profiles**. Here, you will find a list of all the notification profiles available.
2. Find the profile that you wish to disable and click on  under '**Status**'. This will prompt a confirmation message.
3. If you still wish to proceed, click '**OK**'.

Now, you have successfully disabled a notification profile. If you wish to re-enable a notification profile, you simply enable it by

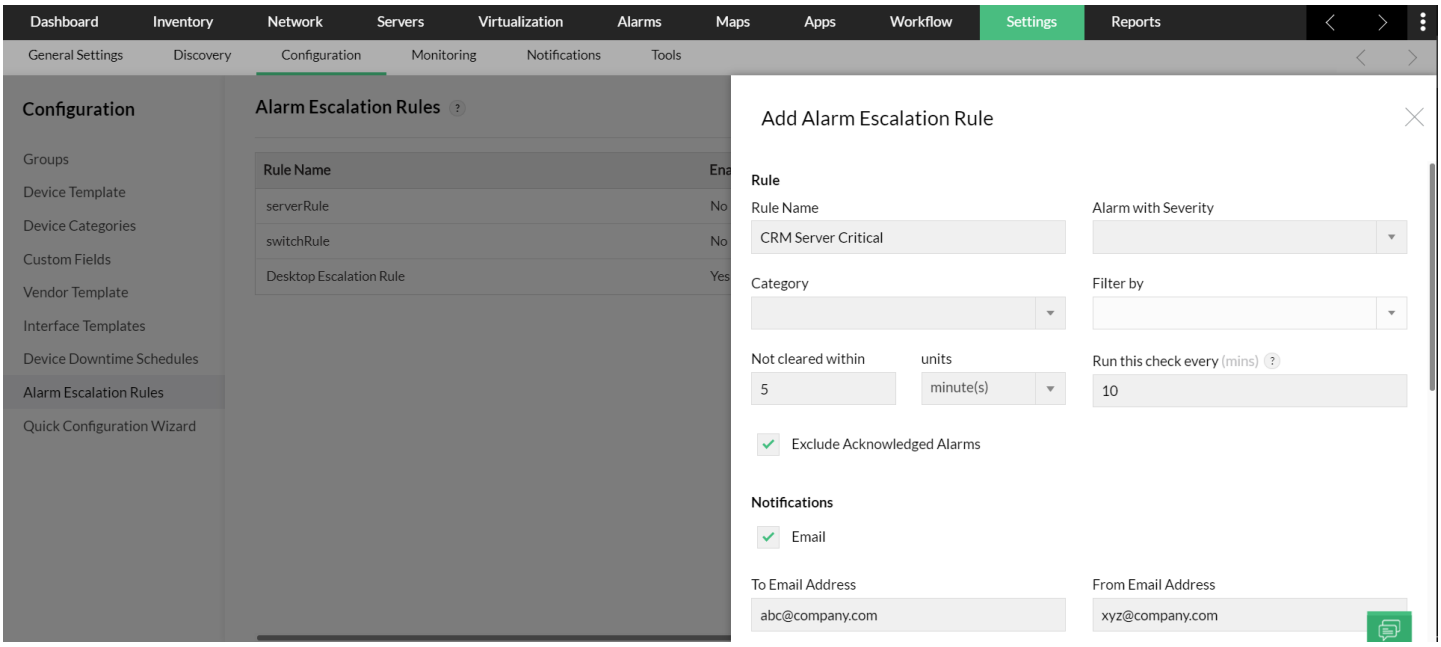
clicking on the slider again.

Escalating Alarms

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. However, you have an option to exclude the alarms that are acknowledged from being escalated.

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

1. Click **Settings ? Configuration ? Alarm Escalation Rules**.
2. Click **Add Rule** to create a rule.
3. Assign a name to the rule in the **Rule Name** field.
4. Select the **Severity** and **Category** of the alarm.
5. Select the **Business View** in order to associate the rule only to the alarms of the devices of the selected business view. If not select None to associate the rule to the alarms of all the devices.
6. Then configure the the interval (**Not Cleared Within**) in either hours or minutes to wait for the alarm to get cleared.
7. In the **Run this check every** box, set the interval in minutes to execute this rule.
8. You can exclude the acknowledged alarms from being escalated by selecting **Exclude Acknowledged Alarms** option.
9. Type the values for the fields under **Notifications** > **Email** to send an e-mail if the alarm is not cleared within the specified interval.
10. Configure the **To Email Address**, **From Email Address**, the **Subject** and the **Message** of the escalation mail.
11. Type the values for the fields under **Notifications** > **SMS** to send a SMS if the alarm is not cleared within the specified interval.
12. Configure the **Mobile Number** and **Message** of the escalation SMS.
13. Click **Save**.



If you configure a new alarm escalation rule, by default it will be enabled. To disable an alarm escalation rule click on Edit icon, deselect the **Enable this rule** option and click on **Ok**.

Alarm escalation rule can be deleted by clicking the Delete icon in the Actions column of the particular rule.

Managing Faults in Network

There can various types of faults in a network. With the network health depending on various resources like the system resources, services, network connectivity etc, getting to the root of the problem is simplified when the monitoring solution raises meaningful alarms. OpManager helps you identify the fault quickly with its detailed alarms indicating the resource that is poorly performing in the device . The different types of OpManager alarms include:

- Status-poll Alarms (device, service, interface, port down alarms).
- Threshold-based alarms for host resources, response times etc proactive monitoring.
- Alarms from SNMP Traps.
- Windows event logs based alarms.
- Syslog based alarms

OpManager monitors the resources for availability and performance and triggers alarms for all the criteria mentioned above. These alarms can also be sent as email or sms alerts from OpManager.

Processing SNMP Traps into Alarms

What is SNMP Trap?

Traps are cryptic messages of a fault that occurs in an SNMP device. SNMP traps are alerts generated by agents on a managed device. These traps generate 5 types of data:

- **Coldstart or Warmstart:** The agent reinitialized its configuration tables.
- **Linkup or Linkdown:** A network interface card (NIC) on the agent either fails or reinitializes.
- **Authentication fails:** This happens when an SNMP agent gets a request from an unrecognized community name.
- **egpNeighborloss:** Agent cannot communicate with its EGP (Exterior Gateway Protocol) peer.
- **Enterprise specific:** Vendor specific error conditions and error codes.

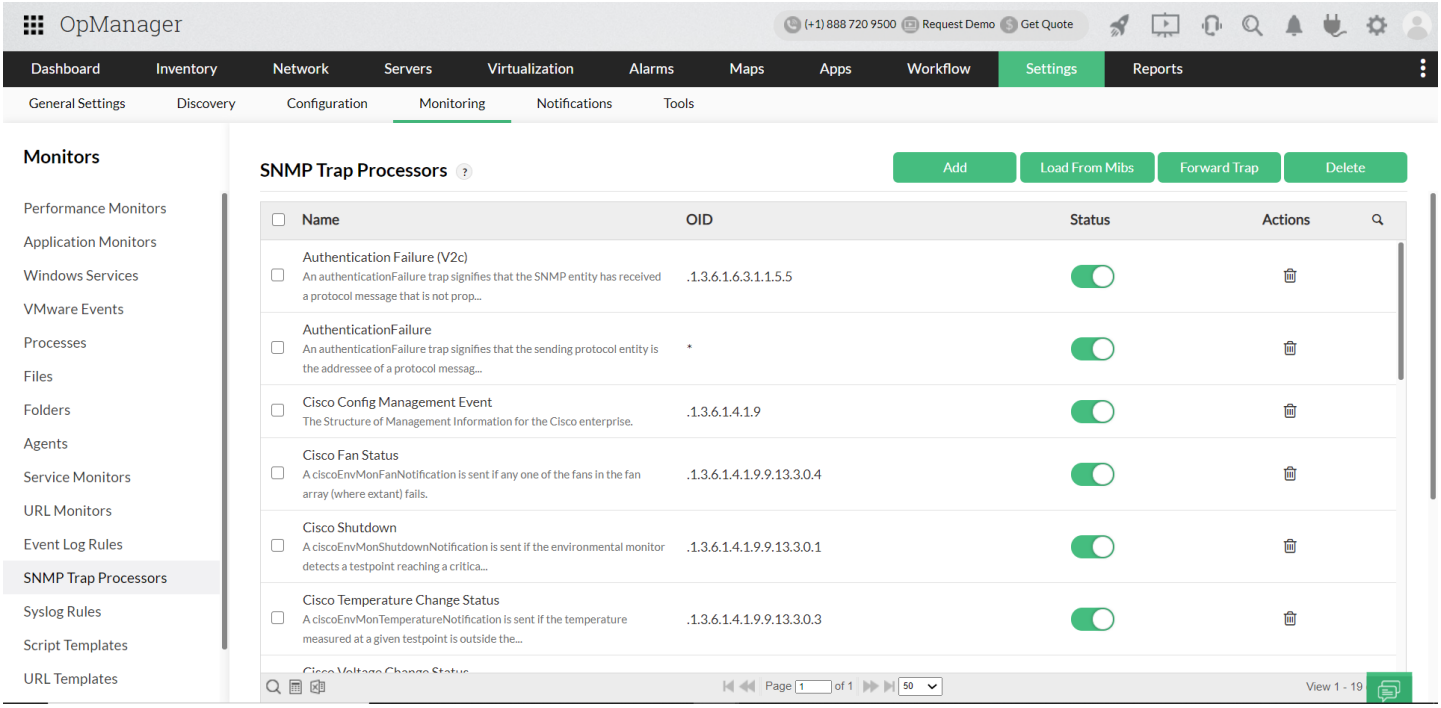
Processing SNMP Traps into Alarms
OpManager enables you to process the traps from the managed devices.

When a trap is received from a managed device, the match criteria in the parser determines whether a specific trap matches the conditions specified in the Trap Processor. Once a matching trap is found, an alert is generated.

Trap Processor converts the cryptic message to human-readable alarm.

Configure OpManager to process the traps that are not processed out-of-the-box and convert them into alarms.

The traps that are not processed are listed under 'Unsolicited Traps'.



Tools

The following actions can be done by clicking the relevant icon:

Edit: Edit the Trap

Enable or disable trap processing: Click to enable/disable trap processing

Delete processor: Delete the Trap Processor

Adding/Modifying Trap Processor

- Go to **Settings** → **Monitoring** → **SNMP Trap Processors**.
- Click **'Add New'** to add a new trap.
- Click the TrapParser name/ Edit icon to modify an existing one.
- Configure/Modify the following properties:
    - **Name:** Configure a name for the new trap processor.
    - **Description:** Describe the trap.
    - **SNMP Trap Version:**Select the version (SNMP V1/V3).
        - **SNMP V1 Properties:**
            - **Generic Type:** Cold Start, Link Up, Enterprise, etc. Select the appropriate type for the OID
            - **Specific Type:** When Generic Type is set to Enterprise a specific trap ID s identified
            - **Trap OID:** For devices with SNMP v2c version, select the trap oid from the MIB using the Select button.
            - **Severity:** Select the Alarm severity.
            - **Failure Component:** This option is useful when you deal with a single trap OID that has multiple failure components. The Varbinds containing more details on the trap will have information on the failed components (entities like CPU, Temperature etc). You can match the entity too by appending the VarBind number in this field to generate separate alarms for the failed components. For instance, $Source_trapName_trap_$v5.
            - **Source:** Append the Varbinds to be matched if required. This option is useful if the trap is forwarded from another source.

- **Message:**&#65533; Select the required message variables
- **Match Criteria:**&#65533; Select the appropriate radio button to either match any one or all the conditions that you specify. Select the variable bindings, the condition, and the string to be matched.
- **Rearm Criteria:**&#65533; Similarly, select the appropriate radio button to match the rearm conditions. Select the variable bindings, the condition, and the string to be matched.

- **SNMP V3 Properties:**
  - **Trap OID:** For devices with SNMP v3&#65533; version, select the trap oid from the MIB using the Select button.
  - **Severity:** Select the Alarm severity.
  - **Failure Component:**&#65533; This option is useful when you deal with a single trap OID that has multiple failure components. The Varbinds containing more details on the trap will have information on the failed components (entities like CPU, Temperature etc). You can match the entity too by appending the VarBind number in this field to generate separate alarms for the failed components. For instance, $Source_trapName_trap_$v5.
  - **Source:** Append the Varbinds to be matched if required. This option is useful if the trap is forwarded from another source.
  - **Message:**&#65533; Select the required message variables.
  - **Match Criteria:** Select the appropriate radio button to either match any one or all the conditions that you specify. Select the variable bindings, the condition, and the string to be matched.
  - **Rearm Criteria:** Similarly, select the appropriate radio button to match the rearm conditions. Select the variable bindings, the condition, and the string to be matched.

- Click **Save** for the configuration to take effect.&#65533;

Loading Trap Parsers from a MIB

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

- Go to **Settings** → **Monitoring** → **SNMP Trap Processors**.&#65533; All the configured processors are listed here.
- Click on **Load Traps From Mibs** at the top of the page.
- 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.
- Select the required trap variable, and click **Add**.
- A Processor for the selected trap is added, and is listed under the **Traps** tab.&#65533;

How to process the Unsolicited Traps?

- Go to **Alarms (ALT+A)** >&#65533; Click on **Unsolicited Traps**.
- Click on Create Trap Processor corresponding to the trap message.
- Type a name for TrapName.
- Make sure that the status is enabled.
- Select the Severity.
- Click on Add.&#65533;

How to configure SNMP Traps in Agent?

Despite configuring the SNMP Trap Processor in opmanager, you might still not see the alarms based on traps. You might need to check the SNMP agent configuration on the monitored devices.

Can I process traps from a device which is not available in OpManager?

No, the device must be available in OpManager for you to be able to process those traps.

How to combine multiple traps and generate them as a single alarm?

If the value for the **Failure Component** field is the same for two or more trap processors, it'll be processed as a single entity. For instance, let us assume **CISCO_SHUTDOWN** and **CISCO_FANSTATUS** as two different trapprocessors. Now, if the **Failure Component** field for both these trap processors contain the value **CISCO**, then these trap processors will be processed as a single entity.

To configure,

- Go to **Settings** → **Monitoring** → **SNMP Trap Processors**
- Select **Add/Edit a trap procesor**
- **Add/Edit** the **Failure Component** field to contain the same value.

Now, OpManager will process these traps as a single entity.

How can I ignore a trap from being processed?

- Go to **Settings** → **Monitoring** → **SNMP Trap Processors**
- Under **Status**, disable the trap processor that you do not wish to be processed.

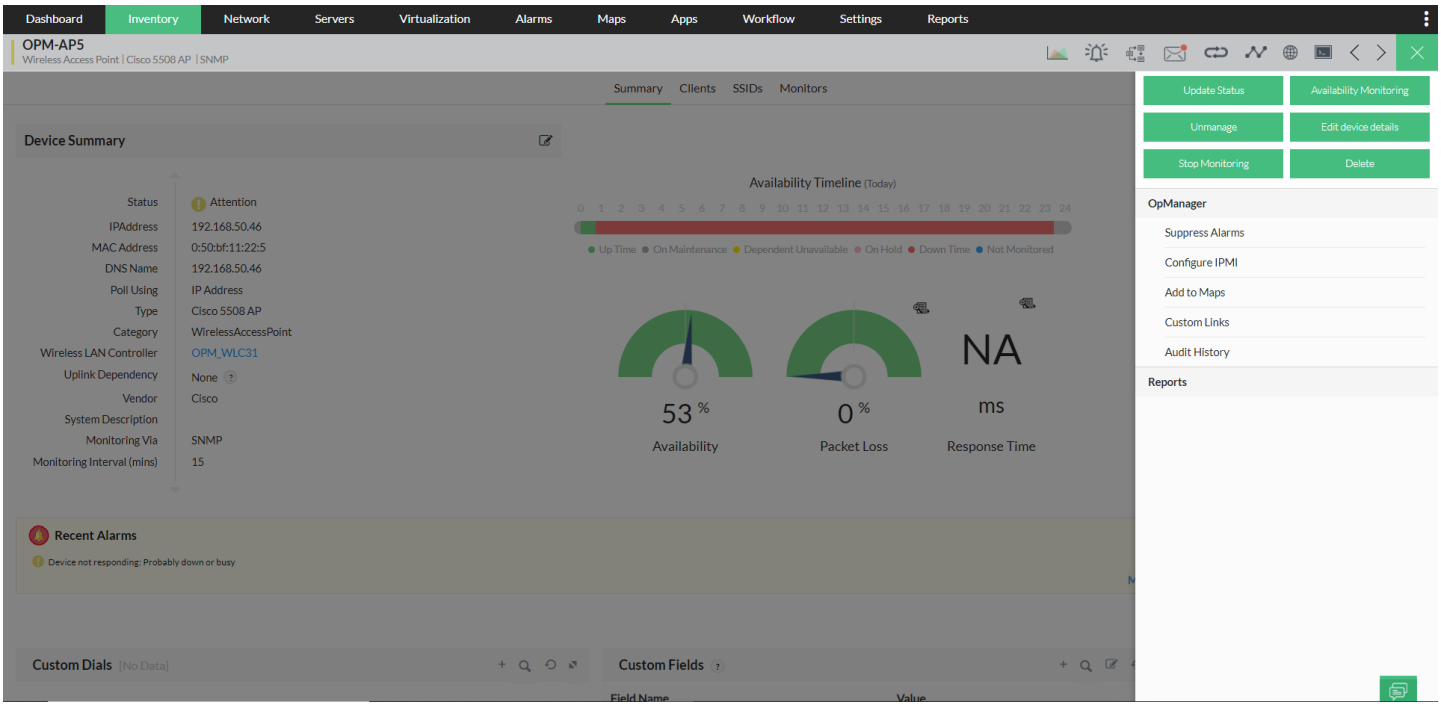
Receiving SNMP Traps in OpManager

OpManager listens for SNMP traps from devices on the default port 162. So, it automatically acts as a trap receiver and based on the trap processors defined in OpManager, the traps are processed and shown as OpManager alarms. When the default port 162 is blocked, the trap port can be switched to a different port.

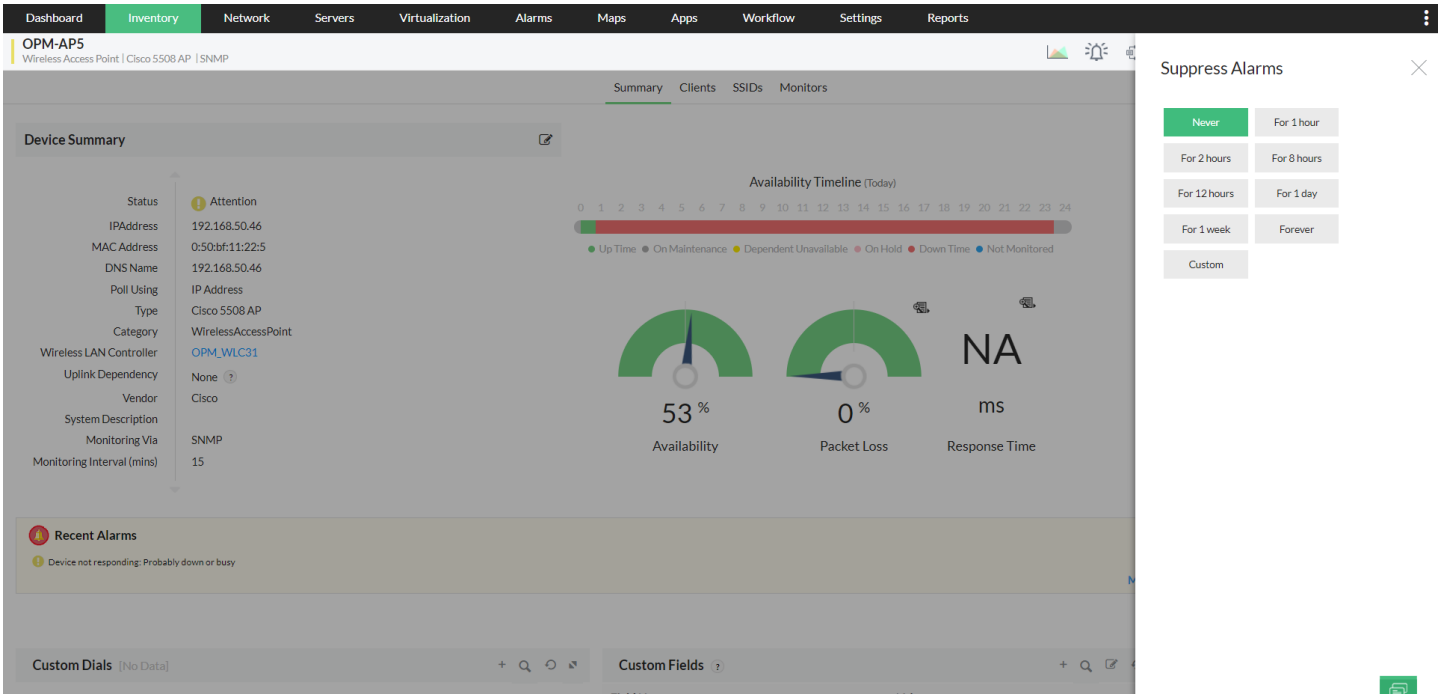
Alarm Suppression

OpManager provides you the option to suppress the alarms of the devices for a pre-defined time interval. This option will be very useful in cases, where the devices are under maintenance or some known issues exist with them.

Configuring Alarm Suppression for a Single Device

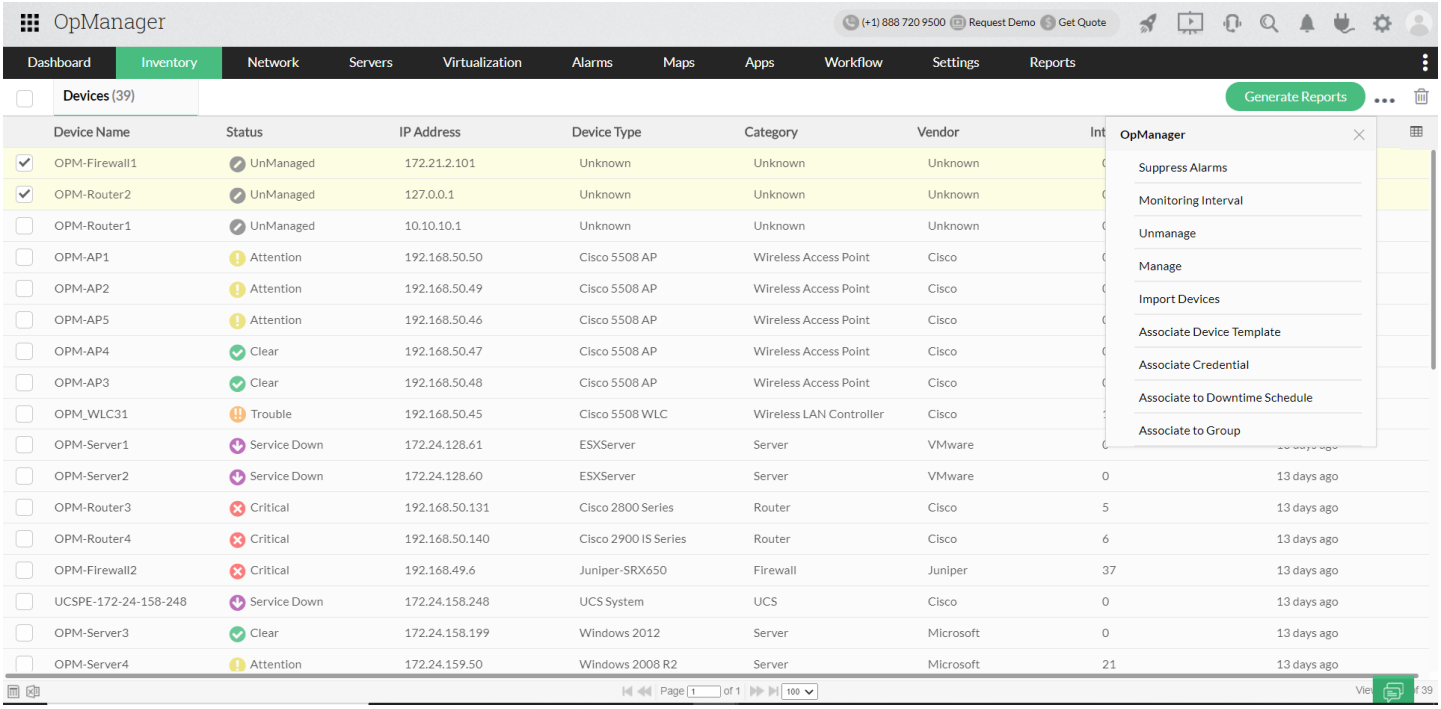


1. Go to the device snapshot page.
2. Click on **Actions** and select **Suppress Alarms**.
3. Select the period for which you want to suppress the alarm.

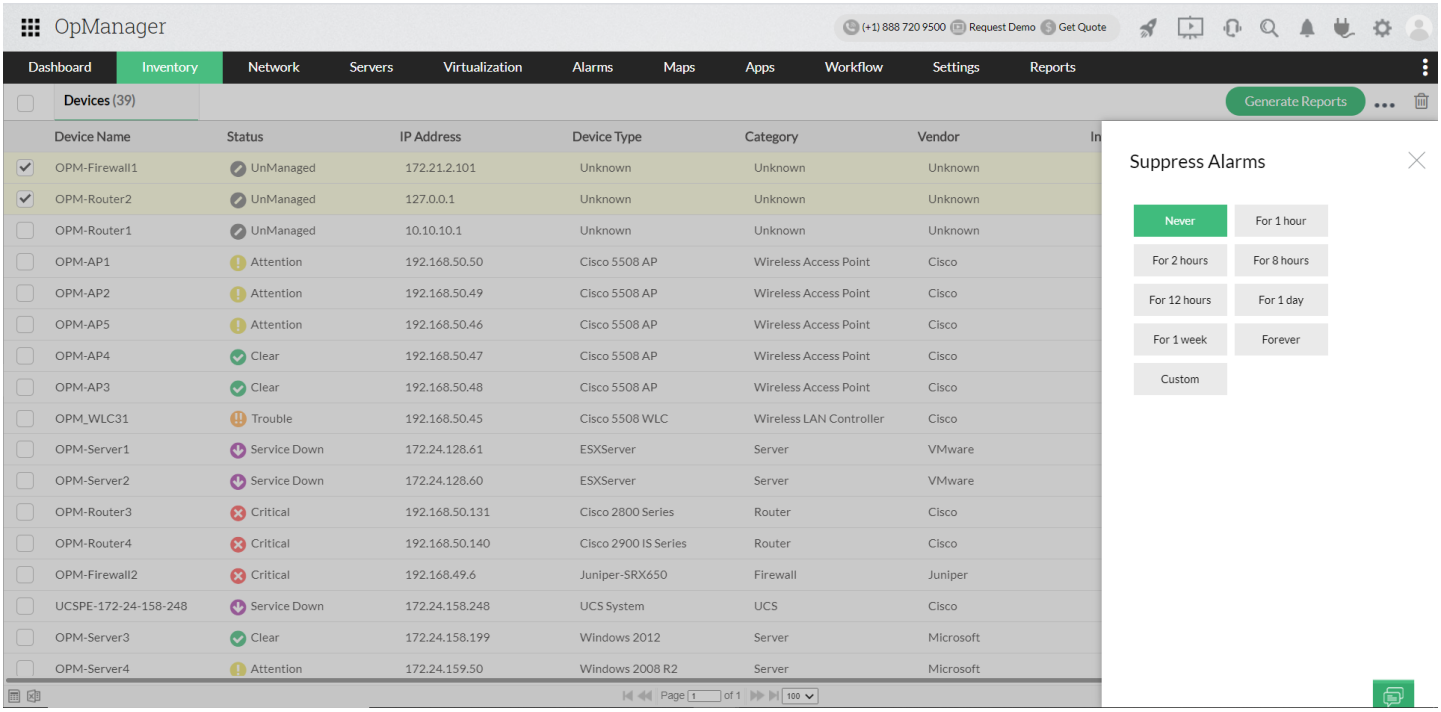


Alarms of this device will be suppressed for the selected period. You can also suppress alarms for devices in a bulk.

To configure the Alarm Suppression in a bulk



1. Go to the **Inventory.**
2. Select the devices for which you want to suppress the alarms.
3. Click options on the top right corner and choose**&#65533;** **Suppress Alarms.**
4. Select the period for which you want to suppress the alarm.



You can also configure alarm suppression in bulk by visiting**&#65533;** **Settings -> Configuration -> Quick Configuration Wizard -> Alarm Suppression**.

Here you can select devices based on -**&#65533;** **Category/ Businsess View/ Groups**. Select the devices from the available devicies and click**&#65533;** **Save**.

Viewing Alerts

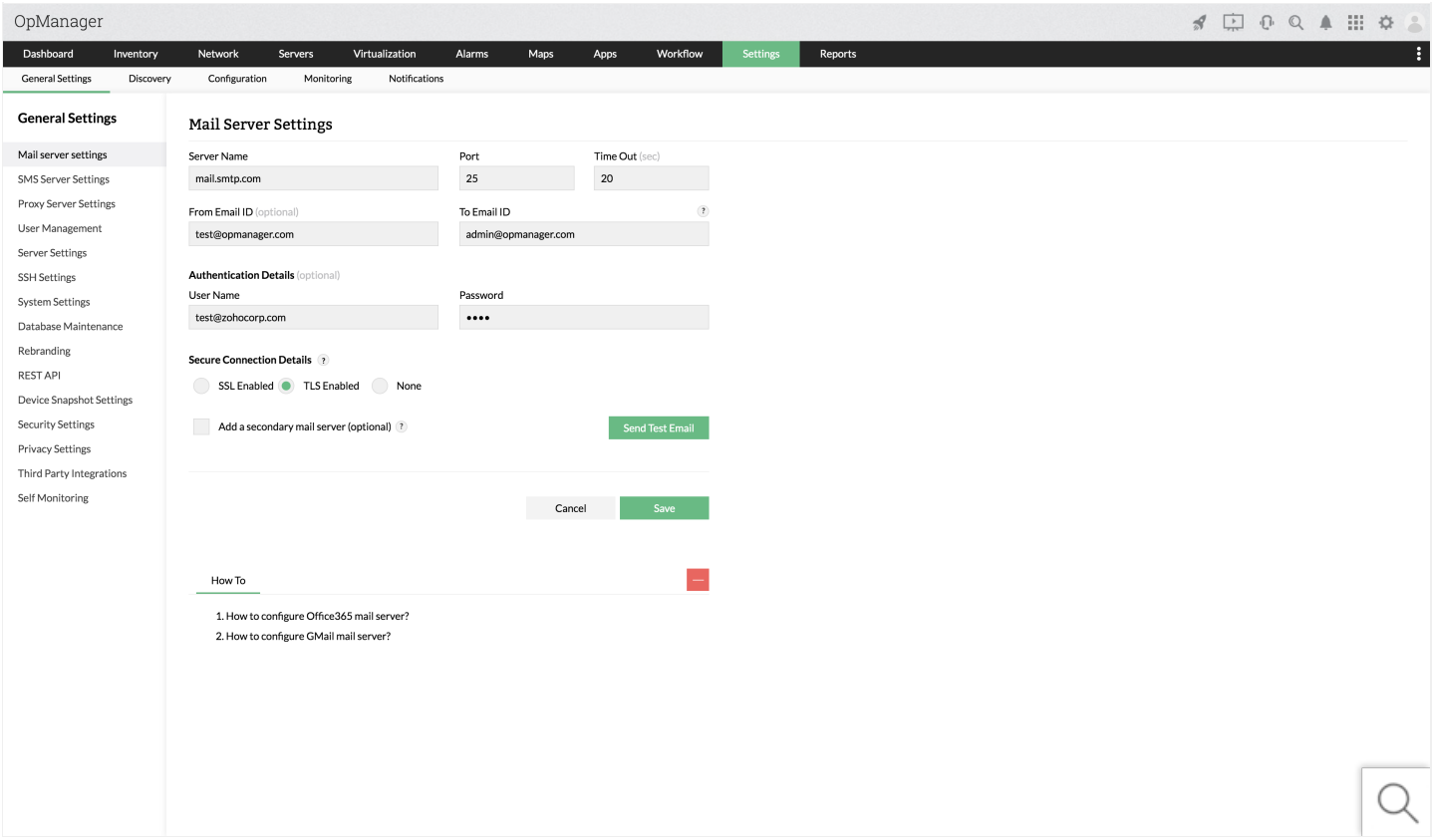
The Alarms tab in OpManager shows all the latest alerts.

From the list box on the top right corner, you can access the following:

- **All Alarms**: A complete list of alarms is displayed here.
- **Active Alarms**: This view lists only the active alarms that are not yet cleared.
- **Unsolicited Traps**: You can view the list of unsolicited traps by navigating to Alarms-> Unsolicited Traps. 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 received from the agent.
- **EventLog Alarms**: This view lists only the alarms that are triggered from Windows event logs as the source.
- **Syslog Alarms**: This view lists only the alarms logged via syslog.
- **Trap Alarms**: This view lists only the alarms logged via traps.
- **Web Alarms:** This view lists web alarms that are triggered via Notification Profiles.
- **Events:** This view lists all logged events from all types of alarms.

Configuring Mail Server Settings

OpManager allows you to configure e-mail alerts to get notified on any fault in your network. The send email feature uses the mail server settings configured here as the default setting for email alerts across OpManager. However, specific requirements can be configured while setting up a profile for each feature, i.e. Notification Profile, Schedule Reports, etc.



To configure the SMTP server settings globally and to provide the secondary mail server settings, follow the steps given below:

1. Go to **Settings** > **Basic Settings**, click **Mail Server Settings**.
2. Enter the SMTP **Server name** and **Port** number.
3. Configure the **From** and **To Email ID** fields.
4. Enter a **Time Out** interval.
5. Configure the **User name** and **Password** details, if the server requires authentication to send e-mail.
6. For SSL authentication, select the **SSL Enabled** check-box, browse and select the SSL certificate and key-in the password.
7. Click **Save**

Verifying Configuration

- To test the settings, enter the **Email ID** and click **Send Test Mail**. This e-mail ID will be considered as the default To Email ID while creating Email and Email based SMS notification profiles.
- If you have a secondary mail server in your network, select **Add a secondary mail server** and provide the details. In case of a failure in the primary mail server, OpManager uses the secondary mail server to send E-mails.

Find more information on configuring Gmail and Office 365.

If you are getting delayed email notifications, click here to troubleshoot.

Configuring Proxy Server Settings

Any business enterprise will have a proxy server to optimize its connectivity to the Internet and to filter access to restricted Web sites. Proxy server acts as an intermediary between the client and the server, thus providing indirect network services to the client and facilitates security/user privacy while accessing the other servers through URL calls. 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. Go to **Settings** > **Basic Settings**, click **Proxy Server Settings**.
2. Select the **Enable Proxy** check-box.
3. 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.
4. For the devices that do no require to go through a proxy, specify the name or the IP Address of the devices as a comma separated list in the **No Proxy** field.
5. Click **Save** to save the details.

SMS server settings

OpManager sends SMS notifications via

- **SMS Gateway**
- **SMPP**

SMS Gateway:

Users can now select from the below list of SMS providers and set them as your default SMS getaway.

- Clickatell
- SMSEagle
- Twilio
- Custom

SMPP:

OpManager also supports SMS notification via SMPP. SMPP stands for Short Message Peer to Peer Protocol. Short Message Peer-to-Peer (SMPP) in the telecommunications industry is an open, industry standard protocol designed to provide a flexible data communication interface for the transfer of short message data between External Short Messaging Entities (ESMEs), Routing Entities (REs) and Message Centres.

Using the SMPP protocol, an SMS application system called the ﷺExternal Short Message Entityﷺ (ESME) may initiate an application layer connection with an SMSC over a TCP/IP connection and may then send short messages and receive short messages to and from the SMSC respectively. It allows fast delivery of SMS messages.

1) **SMPP Server Name:** IP Address or Hostname of the SMPP Server

2) **SMPP Server Port:** Port number of the SMPP Server

3) **User Name:** Specify the username of the SMPP Server

4) **Password:** Specify the password of the SMPP Server

Optional Advanced settings:

5) **Source Address:** Address of Short Message Entity which originated this message.

6) **Source Address's TON:** Denotes Type of Number for the source address.

7) **Source Address's NPI:** Denotes Numbering Plan Indicator for the source address.

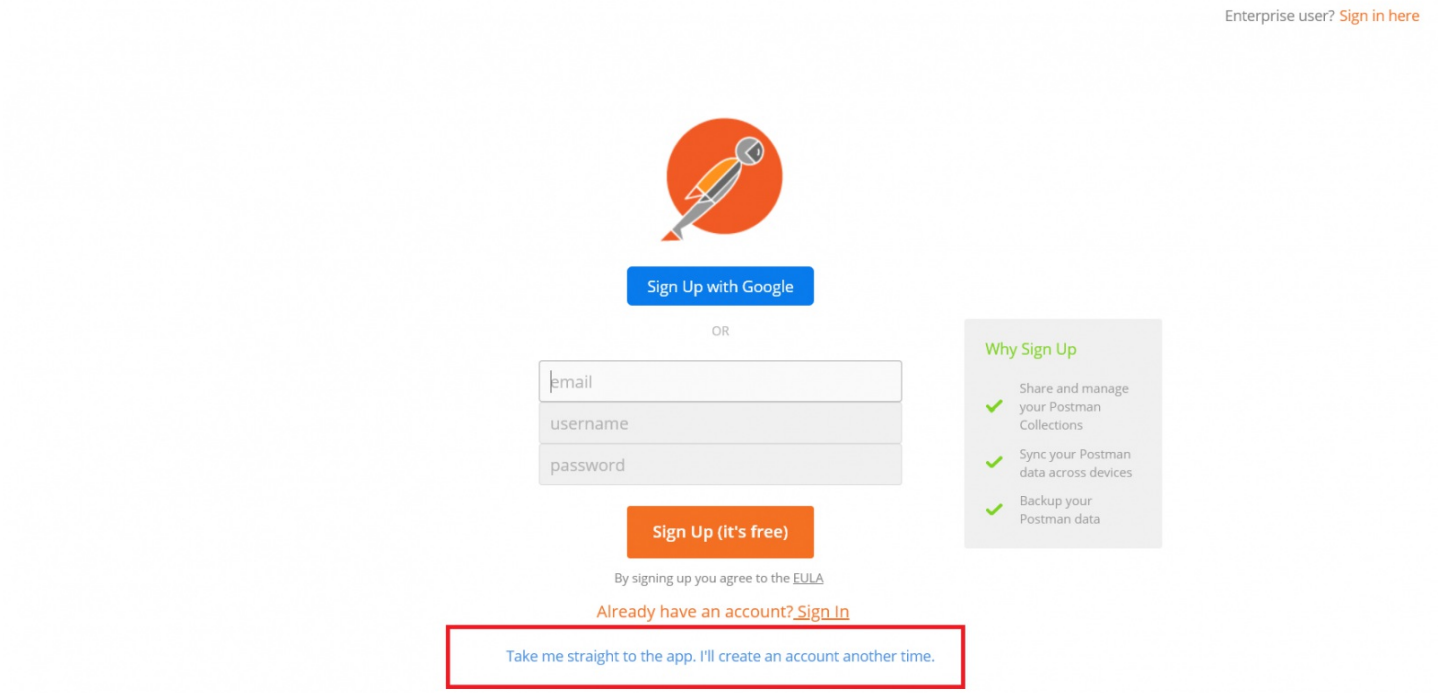
8) **Destination Address's TON:** Denotes Type of Number for the destination address.

9) **Destination Address's NPI:** Denotes Numbering Plan Indicator for Numbering Plan Indicator for the source address.

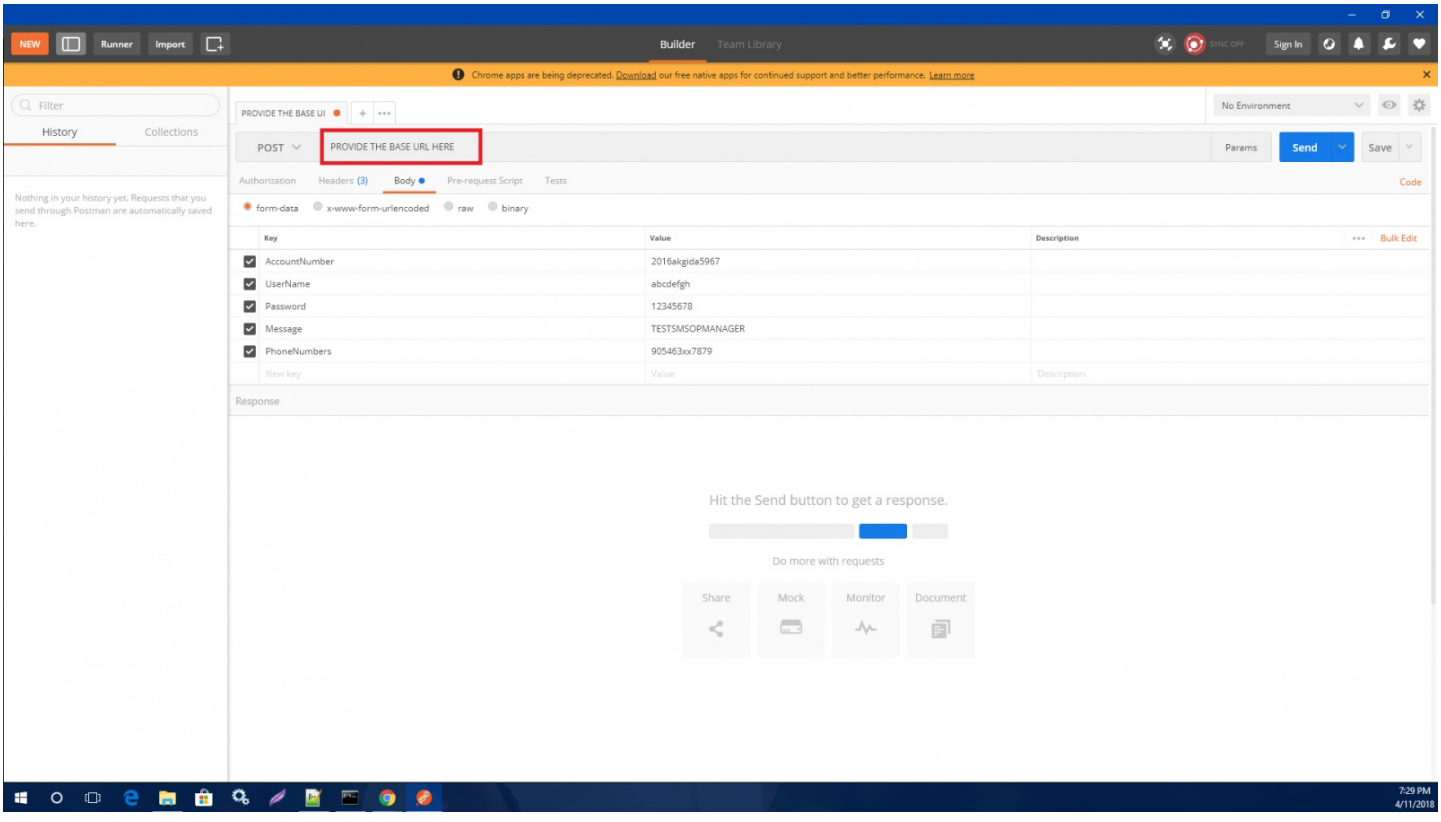
POSTMAN - Third party API tool - An App in chrome

This tool will help you to check whether the API is successful or not. Provide the details which should be used in the SMS server settings and you can cross verify once here before configuring in OpManager.

You can download this from here and either sign in or click "Take me straight to the app".

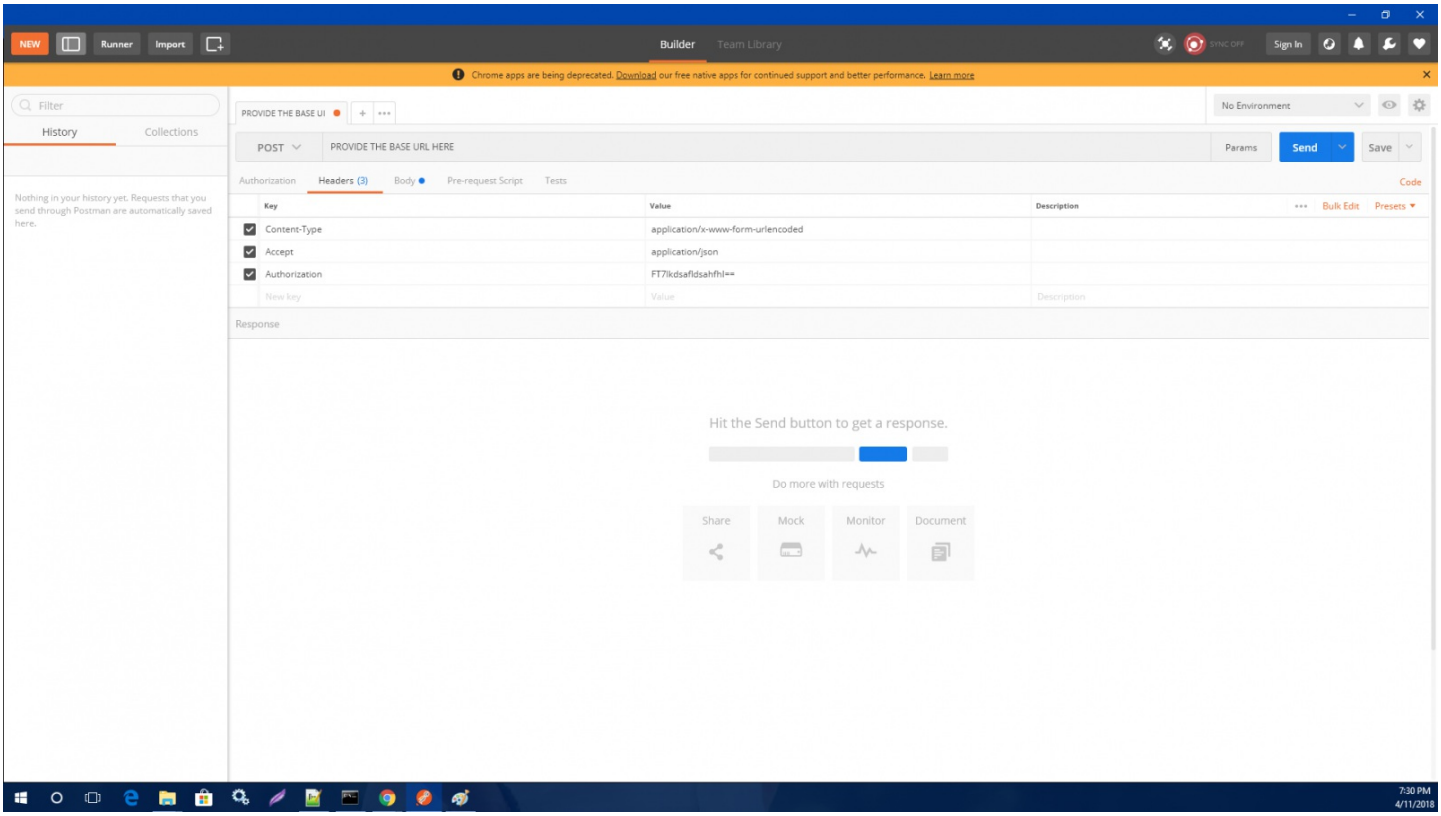


1.Please provide the base URL of the SMS gateway provider and select the API method as POST or GET.



2.Please provide the body with the required "HTTP parameters" you provide in OpManager.

3.Provide the headers under Headers tab which you will use it as "Request Headers" in OpManager.

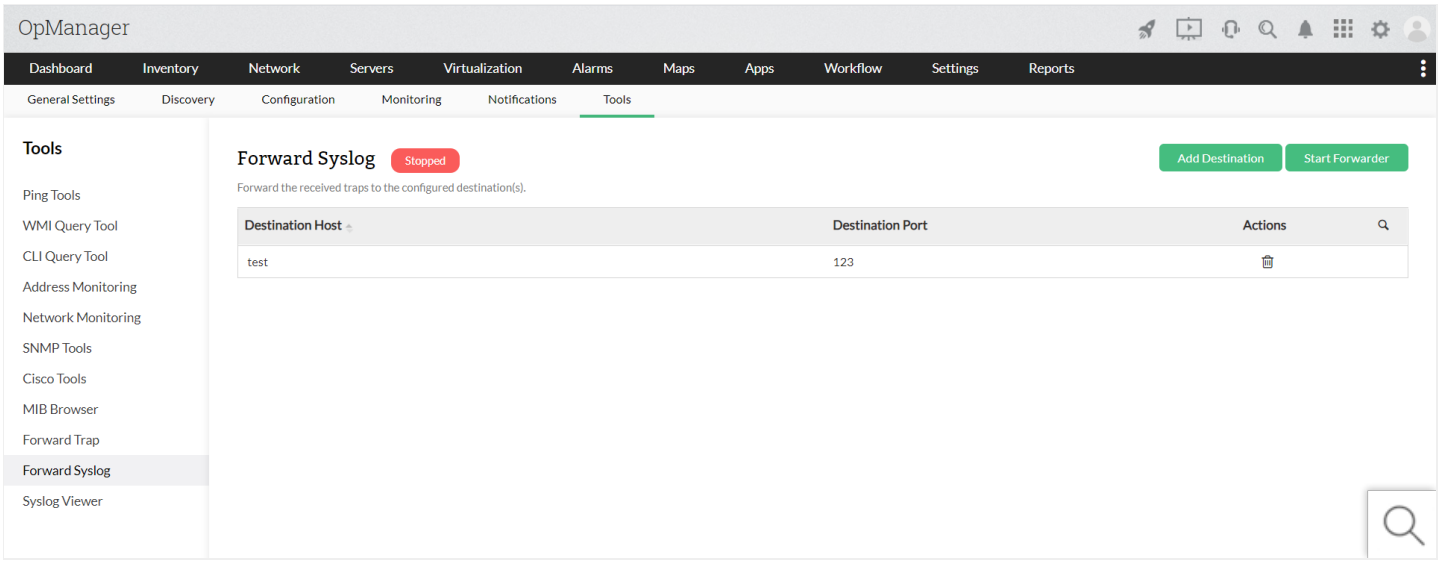


4.Click "Send" and check the status.

Forwarding Syslog

You can forward the syslog received in OpManager to any NMS.

Prev Next



Steps to forward syslog:

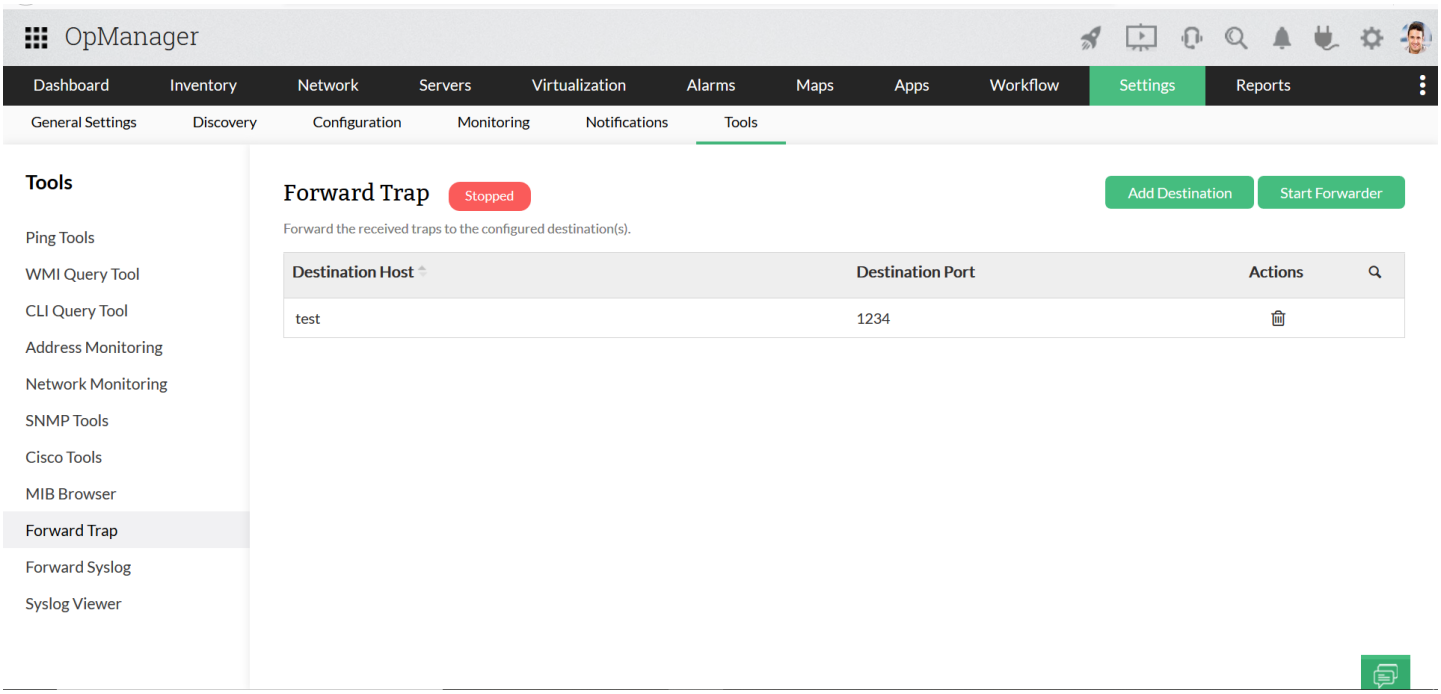
1. Go to **Settings ? Monitoring ? Syslog rules** and click on 'Forward Syslog'.
2. Click on **Add Destination** button.
3. Provide the Name/IP address of the NMS Host to which SysLog has to be forwarded.
4. Provide the SysLog listening port number of the NMS to which SysLog has to be forwarded.
5. Click on **Start Forwarder** to initiate sending of SysLog to the destination NMS. You can also **Stop forwarder** at any desired time.

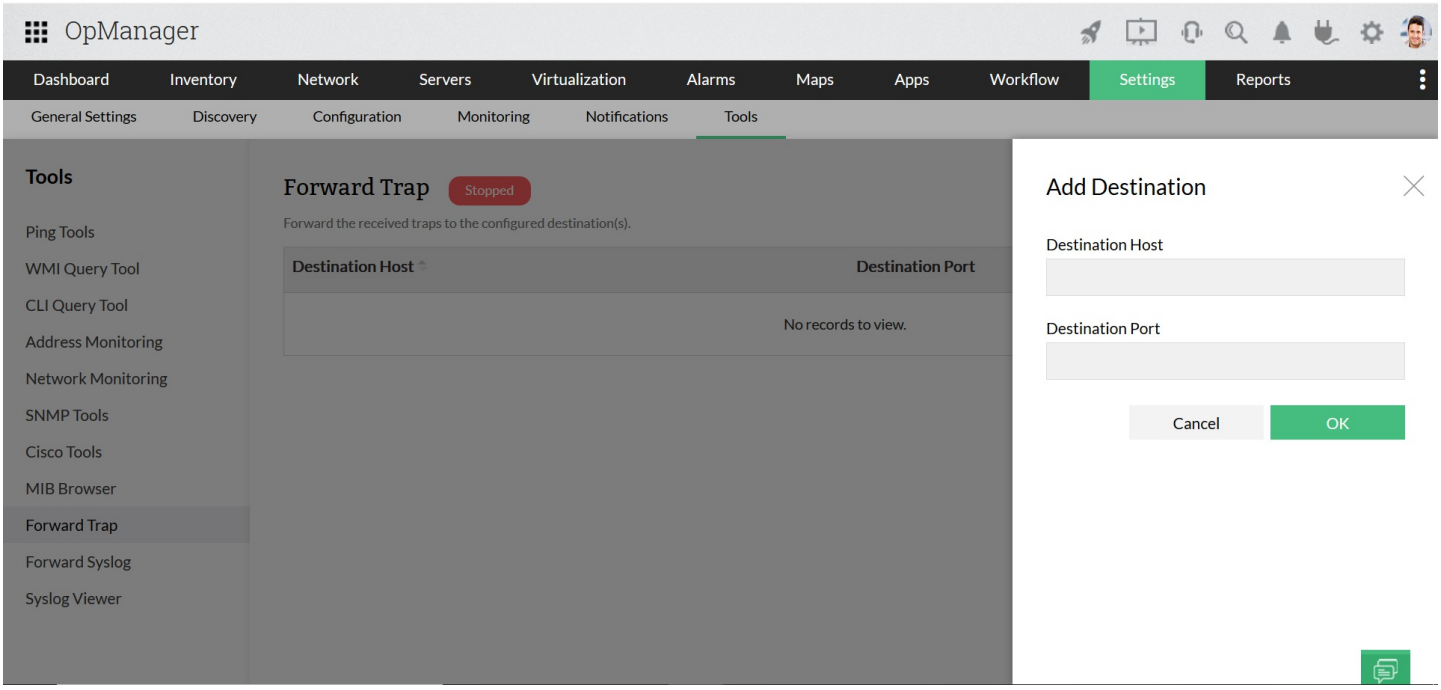
Forwarding Traps

Configure OpManager to notify users over a Trap when there is a specific fault.

Steps to forward Traps:

1. Go to **Settings ? Monitoring ? SNMP Trap Processors ? Forward Trap.**
2. Provide the **Name/IP address** of the host to which notifications has to be sent.
3. Provide the trap listening **port** number of the host to which notifications has to be sent.
4. Click **Save.**





Email Notification Profile

You can configure OpManager to send e-mail to network administrators when 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 has a fault, an e-mail is sent to the technician concerned.

Configuring an Email Alert

To create an email alert profile, follow the steps given below:

1. Go to **Settings** > **Notification Profile**.
2. Click **Add**.
3. Select the Notification type as **Send Email.**
4. Provide the **From, To,** and **CC Email Address** in addition to **Subject** and **Message** (select the required alarm variables which is to be displayed on the email subject and message). Click **Next**.
5. 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'. Additionally notify only when any or all the severity: Critical, Trouble, Attention, Service Down. Click **Next**
6. Select the devices either **By Category** or **By Business View** or **By Devices** and click **Next**.
7. Select the required **Time Window, Delayed Trigger** and **Recurring Trigger** and click **Next**.
8. Give a profile name and Click **Test Action** to test the email profile or **Save** to save the profile.

The profile is associated to the selected devices. A notification is sent every time a threshold is violated for a server.

Note: Primary and secondary SMTP server settings can be provided in the Mail Server Settings page in OpManager. Whenever a new email profile is created, the values of the primary SMTP server and the authentication details are retrieved 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 is used to send the mail automatically.

If your email notifications are delayed, click here to troubleshoot.

OpManager also supports Email based SMS alerts, click here to learn more.

SMS Notification Profile

Configuring SMS Alerts

You can configure OpManager to send SMS to administrators when 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 has a fault, an SMS will be sent to the technician concerned.

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

1. Go to **Settings > Notification profiles**.
2. Click **Add**.
3. Select the Notification type as **SMS**.
4. Choose the gateway and provide the mobile number(s).
5. Provide the **Subject** and **Message** (select the required alarm variables which is to be displayed on the email subject and message). Click **Next**.
6. 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'. Additionally notify only when any or all the severity: Critical, Trouble, Attention, Service Down. Click **Next.**
7. Select the devices either **By Category** or **By Business View** or **By Devices** and click **Next**.
8. Select the required **Time Window**, **Delayed Trigger** and **Recurring Trigger** and click **Next.**
9. Give a profile name and Click **Test Action** to test the SMS profile or **Save** to save the profile.

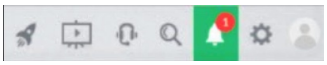
The profile is associated to the selected devices. A notification is sent every time a threshold is violated for a server. To configure SMS server settings, click here.

OpManager also sends Email based SMS alerts, click here to know more.

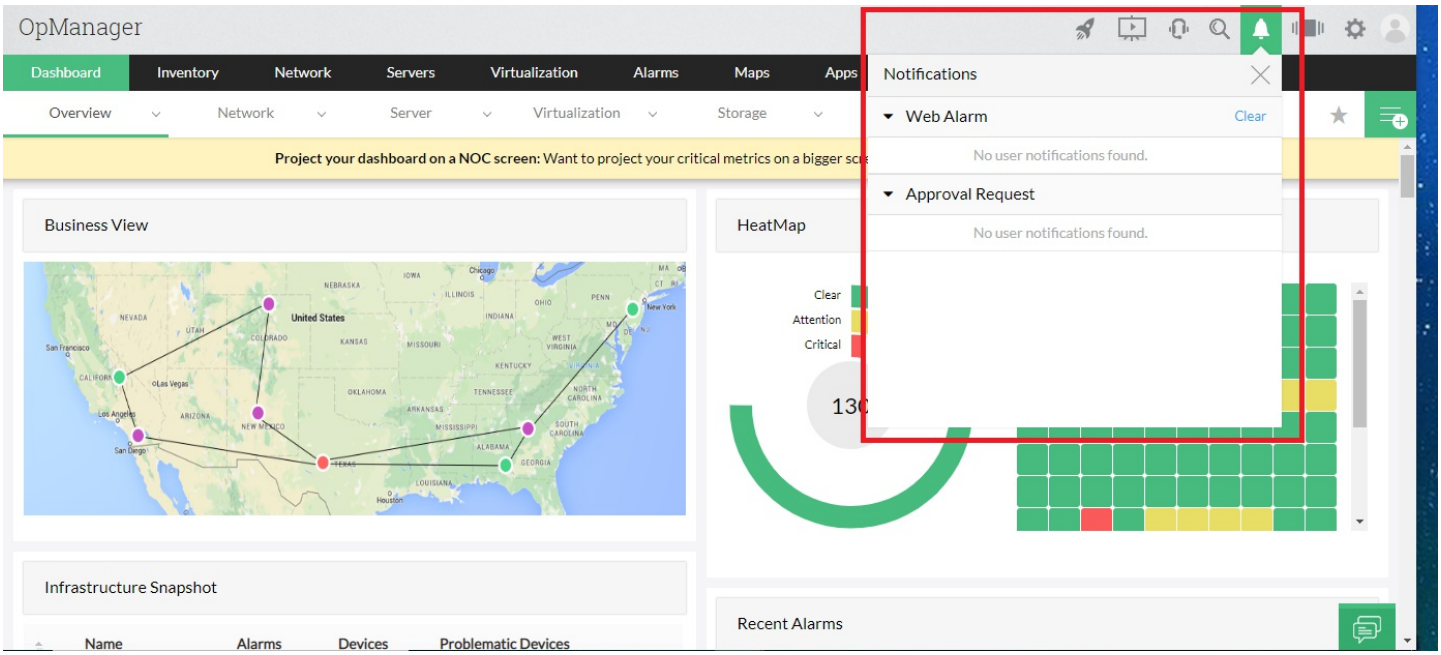
Web Alarm Notification Profile

Configuring Sound Alerts using Web Alarm profile

Web alarm lets you get updates on the alerts raised, as a Push Notification to the bell icon with a short notification sound in the OpManager window.



This can prove essential in your real time network monitoring environment, where you can configure sound alerts only for critical alarms (Device Down/ URL Down). This will allow you respond immediately to troubleshoot business critical issues.



The criteria and schedule based on which you want to be notified, can be configured in the profile.

Configure Web Alarm profile

Go to Notification Profile,**Settings** >**Notification Profile > Add**.

Select**Web Alarm**, to configure the Web Alarm profile.

Web Alarm Properties:

1. **Associate Users:** In this section, you will find a list of all users mapped to OpManager classified as 'Administrators' and 'Operators'. You can either select all users or only specific users, to receive this sound alert.
2. **Associate Sound:** Select a sound file to be played when the Web Alarm profile is triggered. You can also upload and select a personalized soundtrack for the alert.

Criteria: Select the criteria based on which the alert will be generated. You can also select the "Notify me when the alarm is cleared" option to be notified once an alarm is cleared. To know more about the different criteria in OpManager, click here.

Device Selection: Select the devices for which you want the web alarm to be generated. They can be selected based on Category, Business View or Devices.

Schedule: This section allows you to configure the Time Window, Delayed Trigger and Recurring Trigger.

Preview: Provides a summary of the Web Alarm profile that you will be creating. You can name the profile and also test the action

by clicking the Test Action button.

Once the Web Alarm profile has been configured according to your preference, click **Save** to save the profile. Now, the profile will automatically be applied to the selected devices and any alerts will be intimated with the help of a notification sound.

Use-Case:

Eg: Tim is a Network Manager who is also responsible for the health of an enterprise's network infrastructure. He spends his day continuously monitoring the network using OpManager and receives multiple alerts per day. But, he wishes to only get notified of critical events while focusing on his other demanding tasks. Therefore, he configures a Web Alarm profile in OpManager. He no longer needs to keep a constant watch on the webclient. He can simply allow the webclient to run in the background while carrying on with his day-to-day tasks and OpManager will automatically notify him with a sound alert in the case of a critical alarm as per the configured criteria. He can now learn more about the alert from the push notification at the Bell icon and request his peers to handle the issue.

Run Program Notification Profile

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.

Configure a Run Program Profile

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

1. Go to **Settings** > **Notification Profiles**.
2. Click **Add**.
3. Select the Notification type as **Run Program**.
4. In the **Command Name** field, specify the name of the program to be executed with the absolute path. Example C:profilestestprogram.bat.

   Note: These commands will be executed in the OpManager installed server. Please verify the source of the commands before using it here, to prevent any unexpected behaviour or vulnerabilities.

5. If the program requires some arguments, specify the **Program Arguments, Message Variables** and click **Next**.
6. 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'. Additionally notify only when any or all the severity: Critical, Trouble, Attention, Service Down. Click **Next**
7. Select the devices either **By Category** or **By Business View** or **By Devices** and click **Next**.
8. Select the required **Time Window**, **Delayed Trigger** and **Recurring Trigger** and click **Next**.
9. Give a profile name and Click **Test Action** to test the program or **Save** to save the profile.

The profile is associated to the selected devices. The program is executed with the specified arguments whenever a fault matching the selected criteria occurs.

Run System Command Notification Profile

You can configure OpManager to automatically run a system command whenever a fault is detected in the device. For instance, you can configure OpManager to execute a netsend command to send popup messages to users machines whenever a specific type of an alarm is raised for a device.

Configuring a Run System Command Notification Profile

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

1. Go to **Settings** > **Notification Profiles**.
2. Click **Add**.
3. Select the Notification type as **Run System Command.**
4. In the **Command String** field, specify the command name with additional arguments if any.

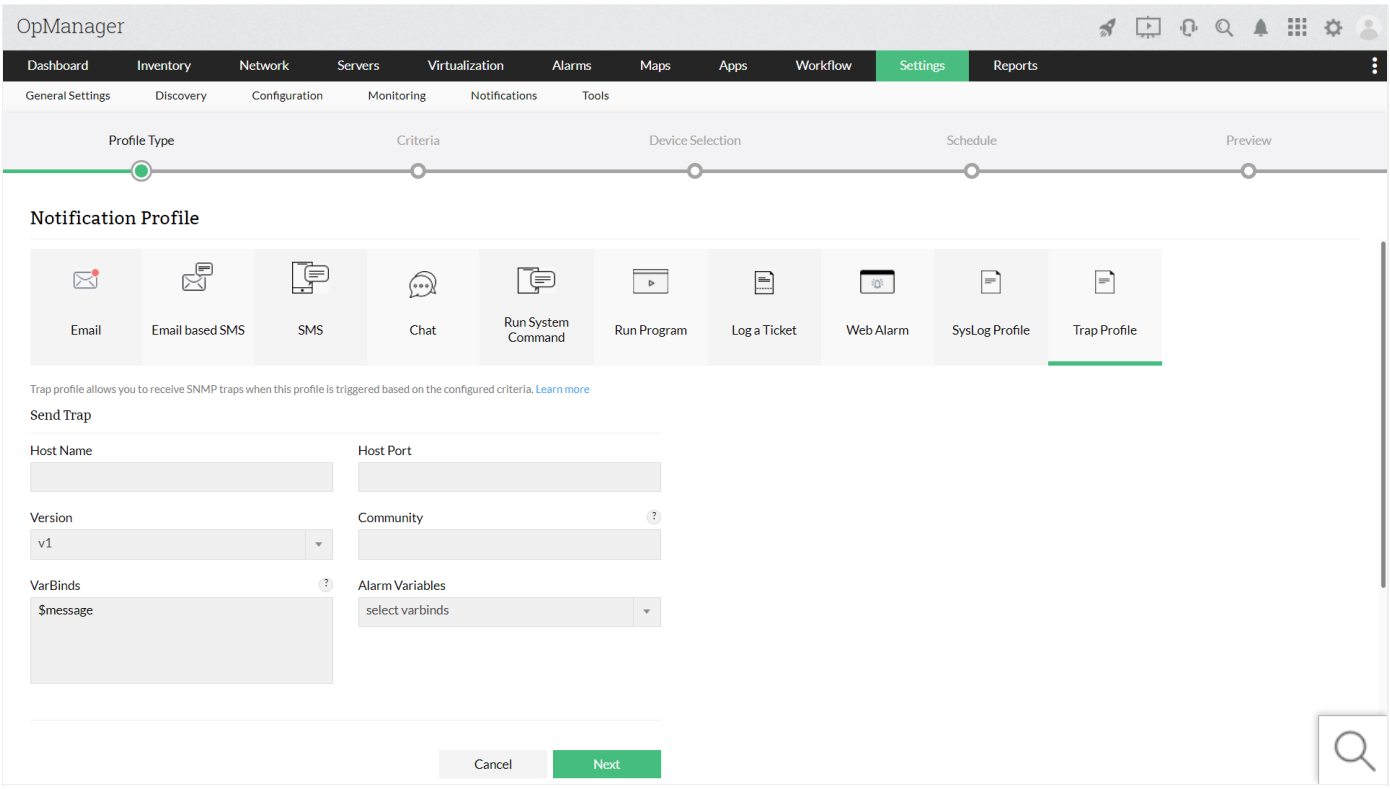
> **Note:** These commands will be executed in the OpManager installed server. Please verify the source of the commands before using it here, to prevent any unexpected behaviour or vulnerabilities.

5. Select the **Error** and **Output** check-boxes to append the output and the error message on executing the command.
6. 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'. Additionally notify only when any or all the severity: Critical, Trouble, Attention, Service Down. Click **Next**
7. Select the devices either **By Category** or **By Business View** or **By Devices** and click **Next**.
8. Select the required **Time Window**, **Delayed Trigger** and **Recurring Trigger** and click **Next**.
9. Give a profile name and Click **Test Action** to test the system command(s) or **Save** to save the profile.

The system command is executed with the specified arguments whenever a fault matching the selected criteria occurs.

Trap Notification Profile

Configure OpManager to notify users over a Trap when there is a specific fault.



Configure a Trap Profile

1. Go to **Settings** > **Notification Profiles**.
2. Click **Add**.
3. Select the Notification type as **Trap Profile.**
4. Provide the **Host Name, Host Port, Version (SNMP version), Community (SNMP read community string)** and **Varbinds** if any. Click **Next**
5. 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'. Additionally notify only when any or all the severity: Critical, Trouble, Attention, Service Down. Click **Next**
6. Select the devices either **By Category** or **By Business View** or **By Devices** and click **Next**.
7. Select the required **Time Window**, **Delayed Trigger** and **Recurring Trigger** and click **Next**.
8. Give a profile name and Click **Test Action** to test the email profile or **Save** to save the profile.

You have successfully configured the notification profile.

SysLog Notification Profile

When any fault occurs you can notify users via SysLog.

Configure a SysLog profile

1. Go to **Settings** > **Notification Profiles**.
2. Click **Add**.
3. Select the Notification type as **Send SysLog.**
4. **Destination Host**: Provide the **Name/IP address** of the host to which notifications has to be sent.
5. **Destination Port**: Provide the SysLog listening **port** number of the host to which notifications has to be sent.
6. **Severity**: You can choose any of SysLog severity events to be processed.
7. Select the **Facility** and required **Message Variables**. Click **Next**
8. 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'. Additionally notify only when any or all the severity: Critical, Trouble, Attention, Service Down. Click **Next**
9. Select the devices either **By Category** or **By Business View** or **By Devices** and click **Next**.
10. Select the required **Time Window**, **Delayed Trigger** and **Recurring Trigger** and click **Next**.
11. Give a profile name and Click **Test Action** to test the email profile or **Save** to save the profile.

You have successfully configured the notification profile.

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. Go to **Settings -> Configuration -> Device Downtime Schedules**.
2. Click on **Add Schedule**.
3. In the **Add Schedule** form, provide the following details:
    - Schedule Name
    - Schedule Description
    - 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.
    - Select the frequency at which the Task has to be scheduled/executed. It can be **Once**, **Every Day**, **Every Week,** and **Every Month**.
    - Specify the start and end time/day of the task in the corresponding fields.
    - If it is a schedule to be executed **every day**, then specify the date from which the task must be scheduled.
    - If it is a monthly schedule, select either the date or the day with the time window for the schedule.
    - You can assign the task to only one of the following options:
        - **Category** (switch, router, server, etc.)
        - **Business view**
        - **Device**
        - **URL Monitors**
4. Click **Save**

The schedule will be executed as configured.

To disable a Device Downtime Schedule

If you wish to disable the device downtime schedule, Go to **Settings > Configuration > Device Downtime Schedules** and set the status as **Disable** for the corresponding device downtime schedule.

To stop the currently running Device Downtime Schedule

- Go to **Settings > Configuration > Device Downtime Schedules** and select the one to be stopped.
- In the **Edit Schedule** page, scroll to the bottom and click on **Save**.
- A message stating 'This schedule is active. Click here to stop the schedule, or update the schedule details after the process is completed' will be displayed. You can stop the schedule or update it by doing so.
- To delete a Device Downtime Schedule, click on the delete icon under **Actions** header of the respective schedule.

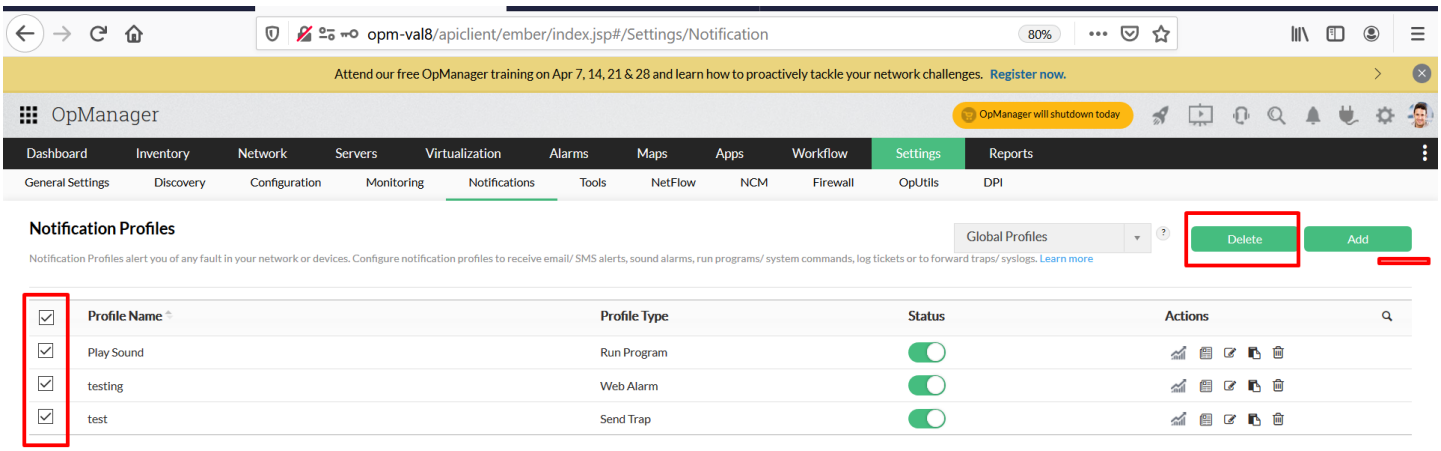
Points to remember:

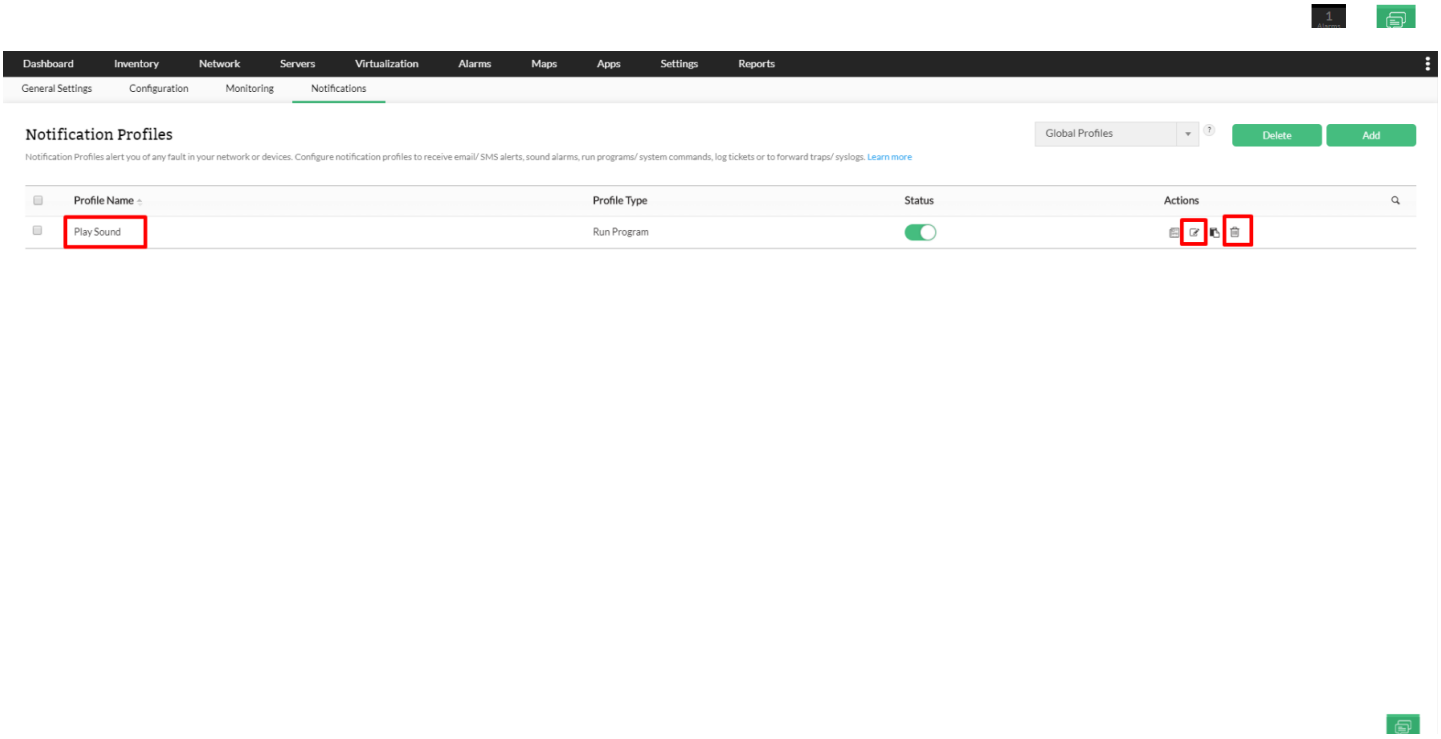
- If a device is added under multiple device downtime schedules, chances are that one of the device downtime schedules under which the device is specified may still be in running state. Hence, the specific device will continue to remain in downtime.
- When the parent device is on maintenance, the child devices will not be monitored and their status will be shown as dependent unavailable
- On Maintenance devices are also considered in the OpManager license count.

Modifying and Deleting Notification Profiles

You can modify or remove an existing notification profile. Here are the steps:

1. Go to **Settings** > **Notification Profiles**.
2. All the configured profiles are listed here.
3. Click the **Delete** icon against the profile's name to delete the profiles.
4. Click on the profile's name or the edit option to modify the profile properties.





The changes made here are applied for all the devices to which the profile is associated.

Note: You can also delete the notification profiles in bulk by selecting the profiles and clicking **Delete**.

Adding a new VoIP monitor

Prerequisites

The source and the destination devices should always be a IP SLA responder enabled Cisco device.

Steps to set up a new VoIP monitor

OpManager performs the UDP jitter operation to proactively monitor the VoIP quality between Cisco devices. The UDP jitter operation simulates continuous VoIP traffic to consistently monitor the voice quality scores between the source and the destination devices. Using OpManager, you can now monitor the voice and video quality of a 'call path'. Call path is the WAN link between the router in your main office and the one in the branch office that you want to monitor.

Step 1: Enable Add (/discover) the router in your LAN to OpManager. And make sure the SNMP read and write community are configured properly, for that router.

Step 2: Enable SLA responder on the destination device you wish to monitor. The steps are detailed below.

1. Open a CLI session on the destination router and enable the EXEC mode as follows:

   Router>enable

2. Start the global configuration mode:

   Router#configure terminal

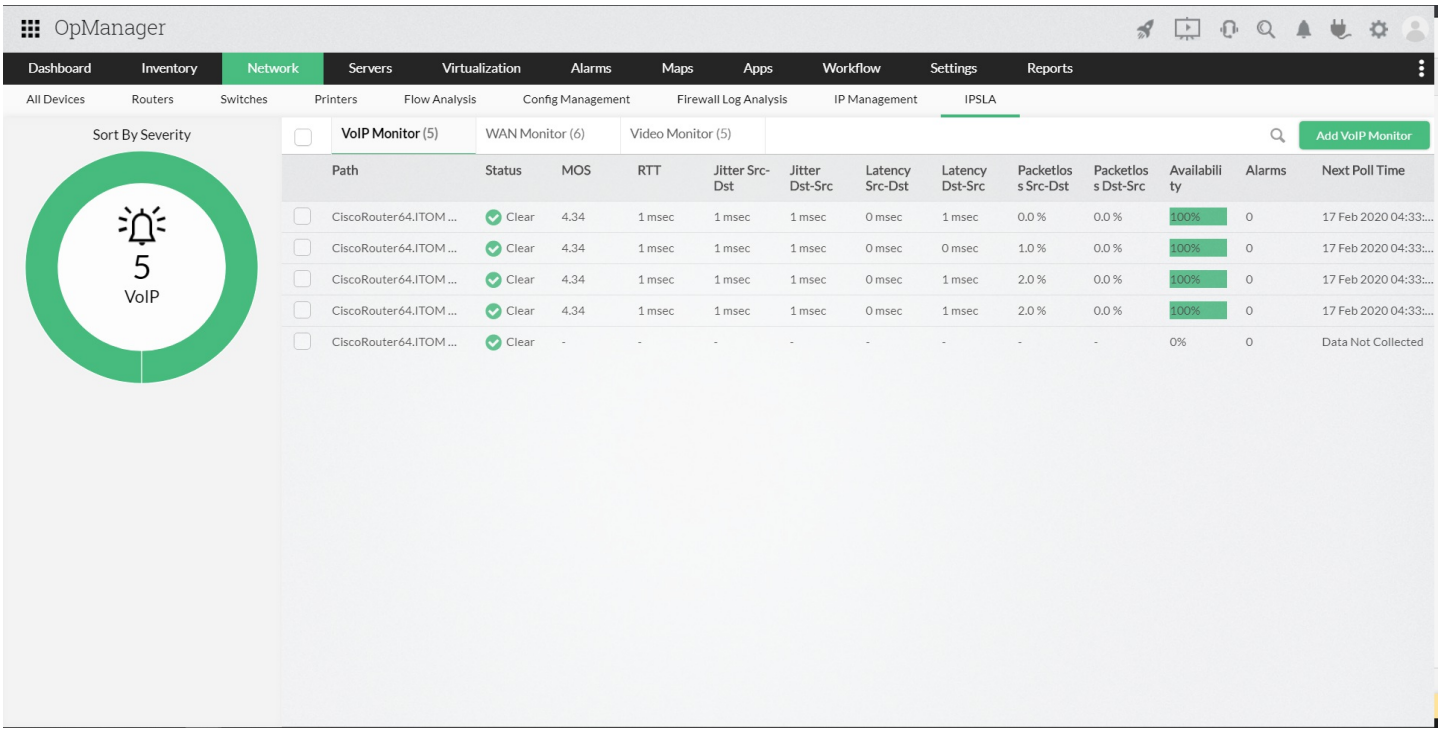
3. Enable the IP SLA responder:

   Router(config)#ip sla responder
   [or]
   Router(config)#ip sla monitor responder
   (Note: Enter any one of the command to enable IP SLA responder as it varies according to the IOS versions.)

4. Repeat the above steps for all the destination routers on which you want to monitor VoIP performance.

Step 3: Creating the VoIP monitor:

1. Go to **Network** ? **IPSLA** ? **VoIP monitor** ? Click on **Add VoIP monitor** at the top right corner
2. Enter a name for the monitor.
3. Select the source router from the list of routers discovered in OpManager, and select the relevant interface.
4. Specify the destination router either by using the 'Search' option to pick from the discovered routers, or use the 'Add' option to specify the IP address of the destination router and submit the details.
5. You will see the summary of the monitor you are about to configure. Now click 'Save' to submit the details to the device. This will take few seconds to configure.



Learn more about VoIP monitoring in OpManager

Configuring call settings and threshold template

Defining Call Settings:

Define a template with the required VoIP settings to be used for monitoring performance. The VoIP template comes with pre-populated default values. Incase you would like to effect some changes to the values before initiating monitoring, make the changes as follows:

1. Click on Settings. Under the Monitoring section, click on IPSLA. Click on the VoIP Call Settings tab.
2. Configure the following parameters:

Source Port - Specify the VoIP UDP port to which VoIP Monitor sends simulated traffic to generate performance metrics. The default port number is set as 16384. You can specify a port in the range of 16384 - 32766.

Simulated VoIP Codec - The VoIP jitter codec decides the type of traffic that VoIP Monitor simulates over your network.

Operation Frequency - The operation frequency is the frequency with which QoS metrics are collected by the IP SLA agent on your network to determine performance.

Operation Timeout - The operation timeout is time to wait for the response from the responder / destination device in msecs.

Type of service - The Type of Service octet allows you to set precedence levels for VoIP traffic of the IP SLA operations.

MOS Advantage Factor - The advantage factor is a measure, on a scale of 0 to 20, of the willingness of your VoIP network users to trade call quality for convenience

Defining Thresholds for the monitored parameters:

You can define a threshold template so that the VoIP performance parameters can be better suit your company SLA's (Service Level Agreements). Alerts are triggered based on the thresholds configured so that you can take corrective actions in time. Here are the steps to define a threshold template:

1. Go to Settings ? Monitoring ? IPSLA ? VoIP Threshold Template.
2. Configure the following parameters:

MOS Threshold : Configure the MOS threshold by specifying the upper and lower MOS range values in the range of 1 to 5.

Jitter Threshold : Configure the jitter threshold in msecs with upper and lower threshold limits. The range is from 0 to 6000 msecs.

Latency Threshold : Specify the delay allowed in msecs again in the range of 0 to 6000.

Packet Loss : Specify the number of packets that can be lost in transit.

Notification Profile : Select the required notification profile(s) in order to notify when the any threshold rule is violated.

Viewing Top 10 Call Paths

With VoIP Monitor you can view the top 10 call paths by MOS, Packet Loss, Jitter and Latency. This provides you to have a quick view and react proactively. To view the top 10 call paths, follow the steps given below:

1. Go to Inventory ? Select IPSLA from three line menu ? Select VoIP and click on **VoIP Monitors**.
2. Click on **Top 10**. The top 10 call paths by MOS, Packet Loss, Jitter and Latency are listed.
3. Click on the required call path view its snapshot page.

Configuring WAN Monitor

Prerequisites

OpManager primarily relies on Cisco's IP-SLA for monitoring the WAN and the prerequisite therefore is that the device should be a Cisco router and must have IPSLA agent enabled on it. Almost all the routers from Cisco are enabled with IP SLA agent and OpManager supports IOS version 12.3 and above. OpManager uses SNMP to query the Cisco routers for the links' performance data. IPSLA familiarity is not a prerequisite. You just need to tell OpManager which links you want to monitor. OpManager provides an intuitive configuration wizard to help you configure all the IPSLA parameters for monitoring the WAN health.

Steps to set up the WAN Monitor

Using OpManager, you can now monitor the availability and latency of a WAN link / path. A WAN link mentioned here is the path between the router in your main office and the one in the branch office that you wish to monitor.

Step 1 : Add (discover) the router in your LAN to OpManager. And make sure the snmp read and write community are configured properly, for that router.

Step 2: Configuring the Router to send traps

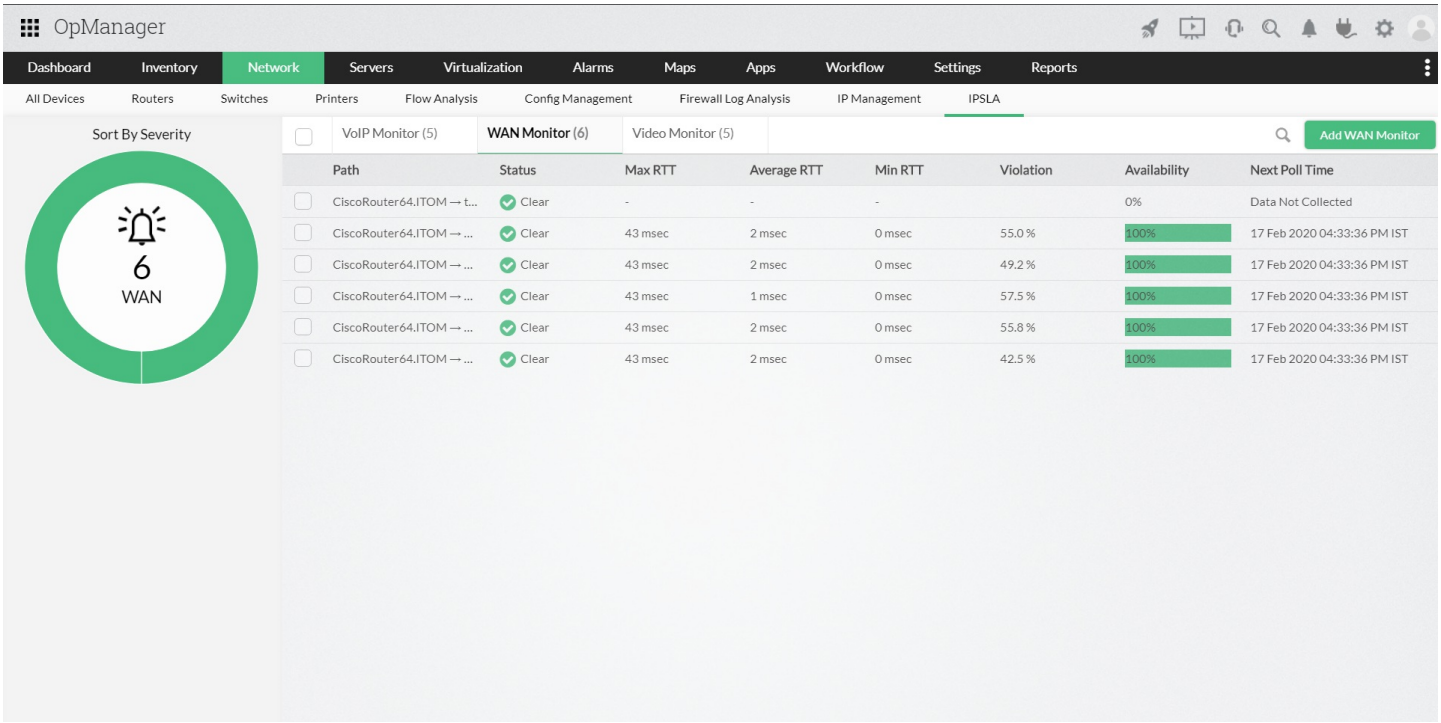
Configure the cisco router to send traps to OpManager. Alerts are shown based on the traps received in OpManager. To configure OpManager server as the SNMP Server receiving traps for the routers, telnet the router and type the following command:

snmp-server host <opmanager server IP> traps <host community string> rtr

For instance, if the OpManager host IP Address is 192.168.18.128, and the community string is private, the command would be:
snmp-server host 192.168.18.128 traps private rtr

Step 3: Creating the WAN Monitor

a. Go to **Network** ? **IPSLA** ? **VoIP Monitor** and click on the **Add new Device** option on the top right corner.
b. Enter a name for the monitor.
c. Select the source router from the list of routers discovered in OpManager and then select the relevant interface of the source router.
d. Specify the destination IP Address either by using the 'Search' option to pick from the discovered routers, or directly enter the IP Address and click 'Add' and submit the details.
e. You will see the summary of the monitor you are about to configure. Now click 'Apply to device' to submit the details to the device. This will take few seconds to configure.
   Refresh the page after few seconds to see the new monitor. The data is collected every hour, from the time you have configured.



To edit any of the configuration details, go to the respective template, make the changes and save the details. When you create a new monitor, the updated values take effect. When the configuration is complete, the router starts collecting the data at the specified frequency i.e. 60 seconds (default value). OpManager updates this statistics (collected data) every hour and the reports are generated after one hour of configuration.

Configuring Test Parameters and Threshold Template for WAN Monitor

Define a template with the required WAN monitoring settings to be used for monitoring performance. The RTT template comes with pre-populated default values. OpManager uses the configured values to simulate traffic. Incase you would like to effect some changes to the values before initiating monitoring, make the changes as follows

Configuring Test Parameters

OpManager uses the default settings specified here,

- **Payload**: The default value is 24 kb. Specify an echo payload value in the range of 0 to 16384.
- **Type of Service**: Specify the Echo TOS in the range of 0 to 255, the default being 30.
- **Operation Frequency**: Specify the interval in the range of 0 to 604800 msecs. The default interval is 60. The operation frequency is the frequency with which QoS metrics are collected by the IP SLA agent on your network to determine performance.
- **Operation Timeout**: Specify the timeout in the range of 0 to 604800000, the default being 60 msecs. Make sure that the timeout interval is lesser than the configured operation frequency so that if the operation is not successful, that is, if there is no response from the device, or in the event of a delay, the request is timed out and the subsequent operation is launched at the configured frequency correctly.

Defining Threshold for Round Trip Time

You can define a threshold template so that you are alerted with the WAN monitor violates a specified value. Here are the steps to define a threshold template:

1. Click on Settings. Click on to IPSLA under Monitoring section. Click on WAN Threshold Template tab.
2. Configure the upper and lower threshold limits for Round Trip time in msecs, the range being 0 to 60000 msecs. You can also choose various notification profiles configured in OpManager to alert you.

Viewing WAN Monitor Alerts

Go to Inventory ? Select IPSLA from three line menu ? Select VoIP (Select any monitor) ? Alarms (present at the end of the page) to view the alerts raised by WAN Monitor.

All the alarms are listed with the Source name, Alarm Message, Status of the Device, Technician, Device category, date and time. Click the alarm message to view the alarm history.

About Reports

Intuitive dashboards and detailed reports helps you determine the performance of your network in very less time. OpManager allows you to export the default reports to other file formats such as exporting to PDF or XLS. You can also schedule the reports to be emailed or published. The default reports available in OpManager include:

- **System**: Provides a complete report on all the system related activities of all the devices. This category of reports include All Events, All Down Events, SNMP Trap Log, Windows Event Log, Performance Monitor Log, Notification Profiles Triggered, Downtime Scheduler Log, Schedule Reports Log, All Alerts and All Down Alerts.
- **Health and Performance**: Gives you a detailed report on the health and performance of all/top N devices.
- **Availability and Response**: Gives you a detailed report on the availability and the response time of all/top N devices
- **Inventory**: Inventory reports are available for servers, desktops, all devices, SNMP-enabled devices and non-SNMP devices.
- **WAN RTT Monitors:** Gives you a detailed report on RTT & threshold of icmp packets and availability statistics of paths.
- **VoIP Monitors:** Gives you a detailed report on various factors related to VoIP packets & traffic.
- **Virtual Servers report :** Gives you detailed reports on your VM's which includes stats like list of all idle VM's, VM's with over-allocated CPU etc.
- **Storage Reports:** Gives you detailed reports on the performance of your storage devices.
- **Forecast reports:** Get forecasts on usage of CPU, memory and disk of all devices in your network, calculated based on history of utilization.
- **Nutanix reports:** Get Inventory and performance reports for Nutanix devices in your network, such as Cluster/Host summary, usage stats about your storage container and disks, and Cluster/Disk Inventory reports.
- **My Favorites:** OpManager provides the option to categorize all your important and frequently viewed reports under My Favorites.
- **Schedule Reports:** OpManager allows you to **schedule a new report** and also to **schedule a generated report**.

Viewing Interface Reports

Interface reports help you to determine the health of the interface by generating detailed reports on In and Out Traffic, In and Out Errors and Discards, Bandwidth & Outage Report, At-a-Glance Report etc. The reports can be exported to PDF format, taken printouts or emailed by clicking the respective icons. To generate the interface reports, follow the steps given below:

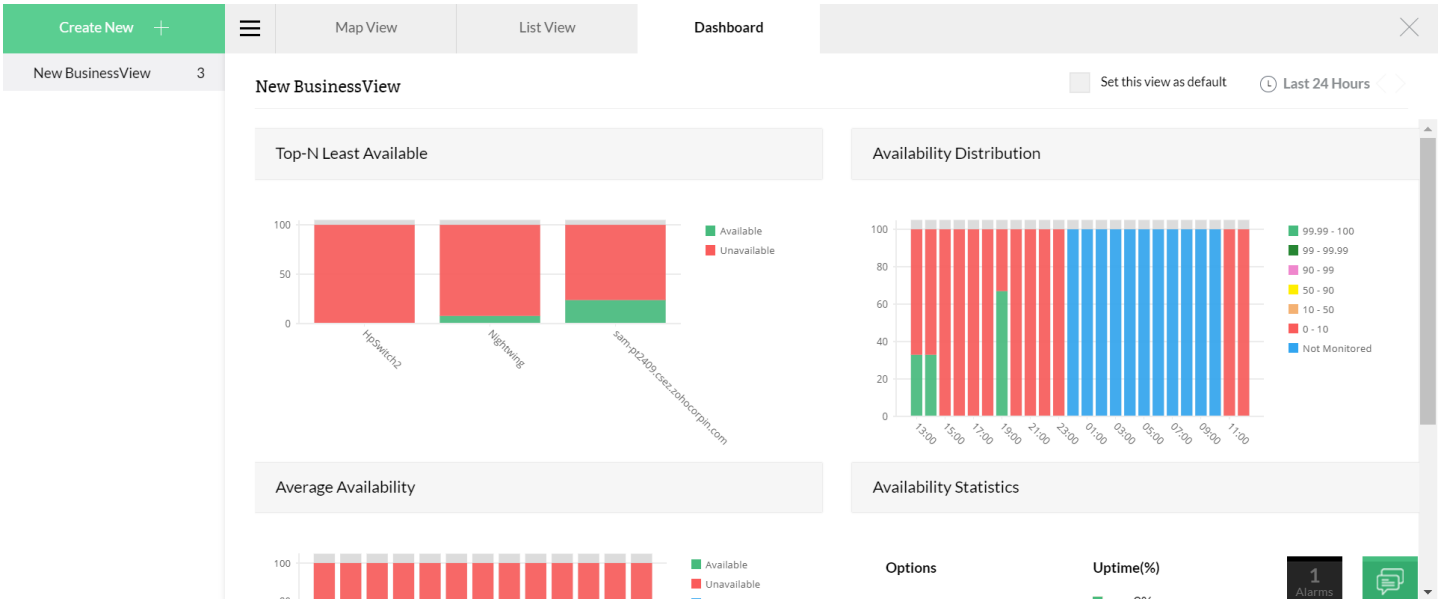
1. Go to the snapshot page of the interface whose health report you want to generate.
2. Go to **Reports** > available on the right pane of the page. All the default reports that can be generated are listed.
3. Click on the preferred time window for which you want to view the report. The default Time Window available in OpManager are follows:

    - Last 12 hours
    - Last 24 hours
    - Today
    - Yesterday
    - This week
    - Last 30 days
    - Custom

Note: The reports can be exported in XLS or PDF format. It can also be scheduled for report generation.

Business View-based Reports

OpManager provides an intuitive Availability Dashboard for your business view. You can track the fault to the root in no time.



To access the business view dashboard, follow the steps below:

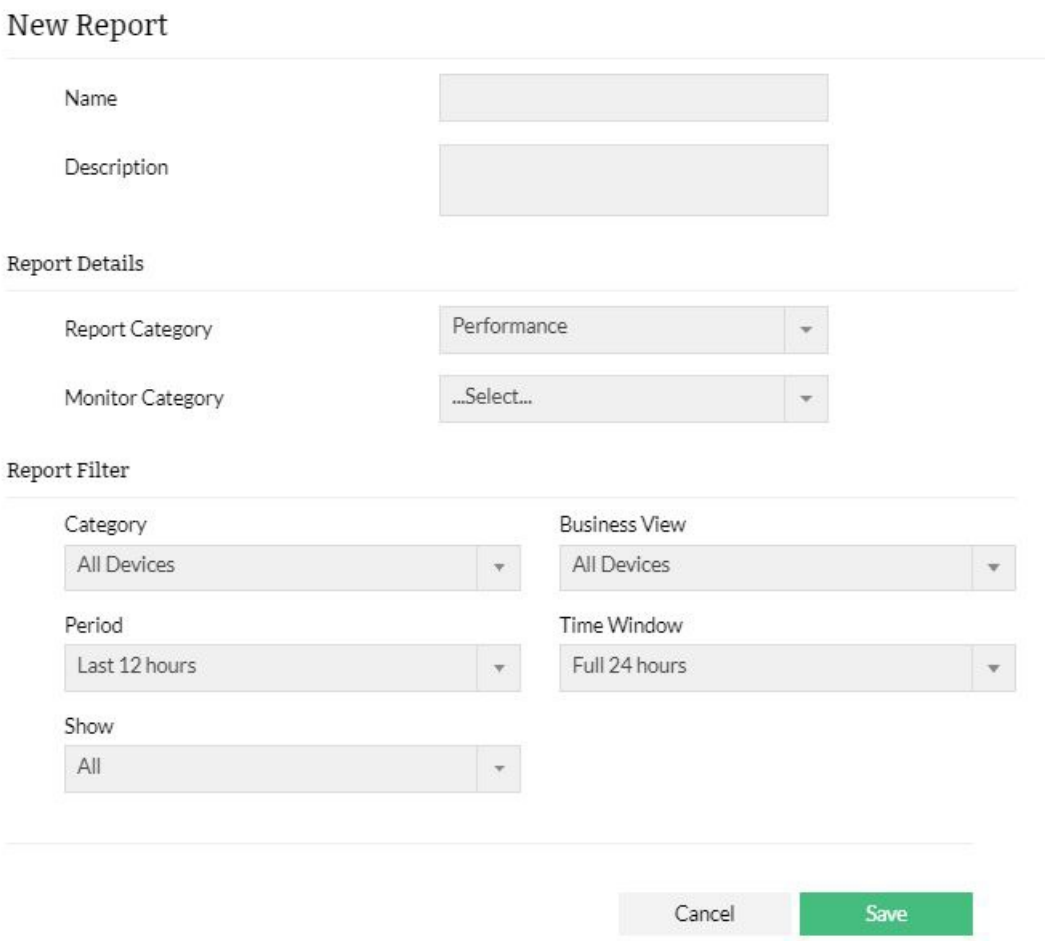
1. Go to the required business view.
2. Click on the **Dashboard** tab. The business view dashboard shows the availability distribution and also the least available devices in that view.
3. Click on the bar indicating a problem to drill down to the actual fault.
4. You can also view the dashboard for various periods like the last 24 hours, or last few days to analyze the trend.

Creating New Reports

Apart from the 100+ available default reports you could also create a new report based on the data that you want. To create a new report follow the steps given below:

1. Go to **Reports,** click on any tab in the page and click **'Create New Report'**.
2. Enter a unique Name and brief **Description**.
3. **Report Category**- You can choose from one of the following categories of reports :

   - **Performance:** A report on the performance of your devices
   - **Availability:** A report on the availability of the devices over a period of time
   - **Response Time & Packet Loss:** A report on the time taken for the device to respond as well as the packet loss for a particular time period..
   - **Inventory:** A report on the available devices in OpManager.



3. **Monitor category:** Select the category of monitors for which you want the report to be generated.
4. Select the specific monitor under the category of monitors for which the report is to be generated.
5. Report filter: You can filter the data that needs to appear in the report based on the following categories:

   - **Category:** The category of devices for which the report is to be generated. You can find more information about Categories in OpManager here.
   - **Business View:** You can choose to display the data for devices under a specific Business View. To learn more about Business Views, click here.
   - **Period:** The day(s) / the hours for which you wish to generate the report data

- **Time Window:** Apart from choosing Time Period i.e, the days of the week, you can also select the hours for which the report has to be generated. This includes:
  - 24-hour report
  - 8:00AM - 8:00PM report
  - Custom hours report - which can be configured with Business Hour Rules
- **Show:** You can select the top N devices for which the data must be displayed in the report.

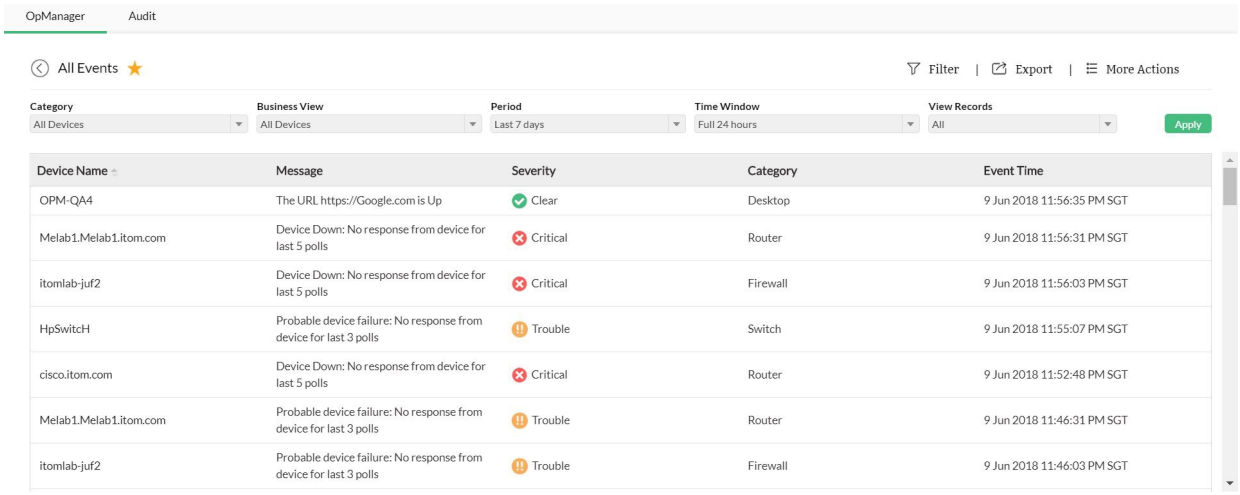
5. Click **Save** to create the new report.
7. After that, a success message will be displayed with an option to Preview the report. It will be displayed as a banner message on the top of the OpManager UI.

The created report gets saved under the appropriate report category. Go to that category and click on the report to generate the report.

Editing Reports

OpManager allows you to edit a generated report in order to refine for some specific parameters, devices or time periods. To edit a generated report follow the steps given below:

1. Go to **Reports > OpManager** > Select the category > Click against the report name that you wish to edit.
2. Click **Filter** button available on the top right of the report page.



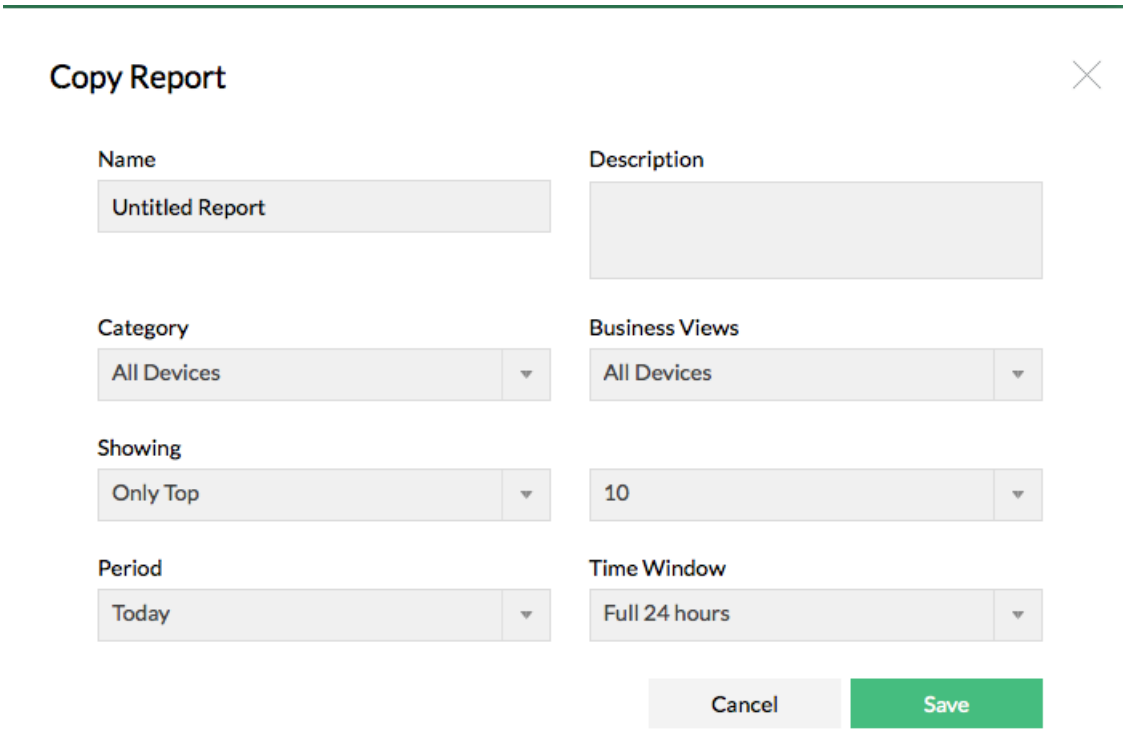
4. Change the required fields. The various fields that can be altered are Category, Business Views, Period, Time Window, Business Hour, Exclude Days, View Records.
5. After modifying the required fields, click on **Apply** to generate the report effecting the changes made.

Copying Reports

OpManager allows you to copy a generated report in order to retain the already configured parameters as template and do some minor changes on them and save as a new report. To copy and save a report follow the steps given below:&#65533;

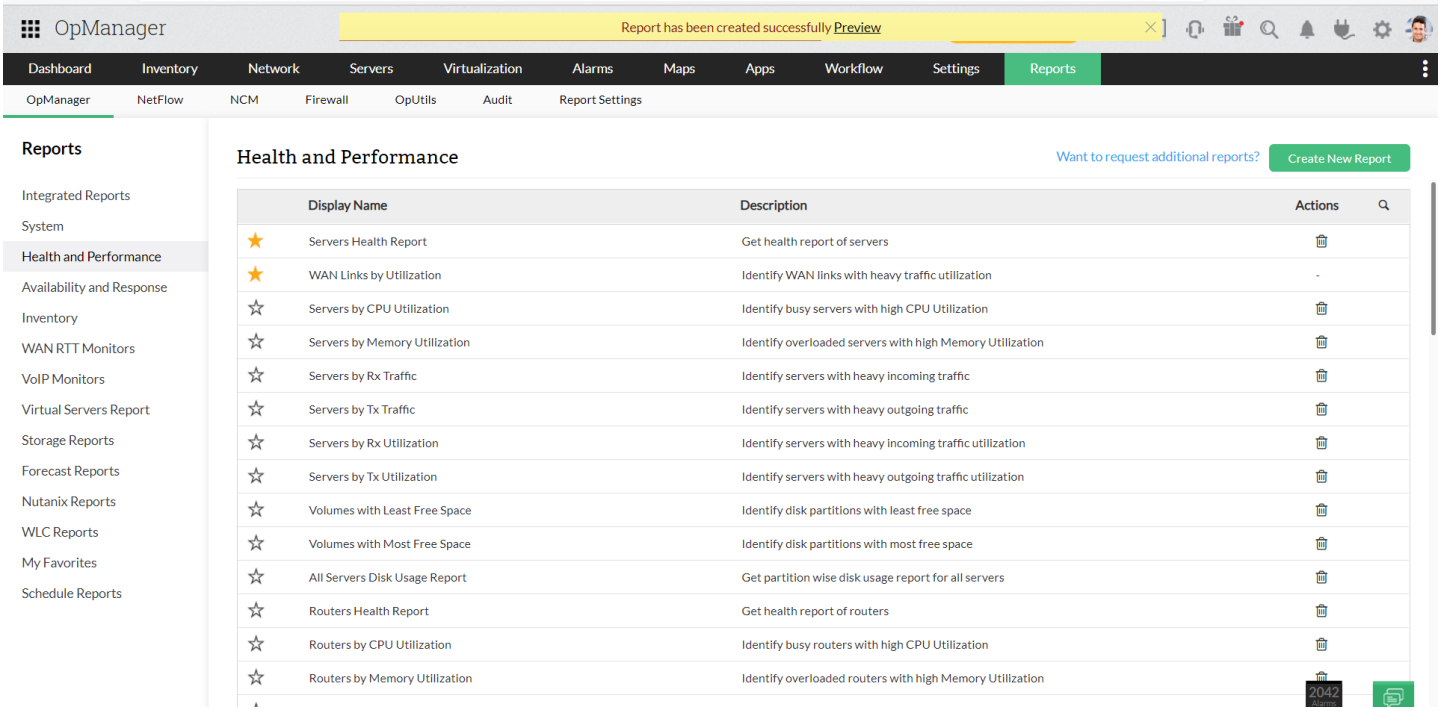
1. Navigate to **Reports -> OpManager.**
2. Choose the report that you want to copy.
3. After choosing the report, click on More Actions&#65533; on the top right corner.&#65533;
4. Click **Copy As** icon available on the top&#65533; of the report that is generated. A small window opens.

&#65533;



&#65533;

2. Enter a unique **Name** and a brief **Description**.
3. Change the required fields. The various fields that can be altered are Category, Period, Business Views, Time Window and Show all or Top N or Bottom N devices.
4. After modifying the required fields, click **Save** button to save the new report.
5. Once the report is generated, it will be notified as a banner message on the top in the OpManager UI (user interface).


OpManager
Report has been created successfully Preview
Dashboard
Inventory
Network
Servers
Virtualization
Alarms
Maps
Apps
Workflow
Settings
Reports
OpManager
NetFlow
NCM
Firewall
OpUtils
Audit
Report Settings
Reports
Integrated Reports
System
Health and Performance
Availability and Response
Inventory
WAN RTT Monitors
VoIP Monitors
Virtual Servers Report
Storage Reports
Forecast Reports
Nutanix Reports
WLC Reports
My Favorites
Schedule Reports
Health and Performance
Want to request additional reports?
Create New Report
Display Name
Description
Actions
Servers Health Report
Get health report of servers
WAN Links by Utilization
Identify WAN links with heavy traffic utilization
Servers by CPU Utilization
Identify busy servers with high CPU Utilization
Servers by Memory Utilization
Identify overloaded servers with high Memory Utilization
Servers by Rx Traffic
Identify servers with heavy incoming traffic
Servers by Tx Traffic
Identify servers with heavy outgoing traffic
Servers by Rx Utilization
Identify servers with heavy incoming traffic utilization
Servers by Tx Utilization
Identify servers with heavy outgoing traffic utilization
Volumes with Least Free Space
Identify disk partitions with least free space
Volumes with Most Free Space
Identify disk partitions with most free space
All Servers Disk Usage Report
Get partition wise disk usage report for all servers
Routers Health Report
Get health report of routers
Routers by CPU Utilization
Identify busy routers with high CPU Utilization
Routers by Memory Utilization
Identify overloaded routers with high Memory Utilization
2042

Scheduling Reports

OpManager allows you schedule a new report,&#65533; schedule a generated report&#65533; and also to view a scheduled report.

Schedule a new report

1. Go to **Reports** → **Schedule Reports**.
2. In the Scheduler Reports Page, click the **Add Schedule** button on the top right.
3. Configure the following details:

   - **Schedule Name**: Configure a name for the schedule.
   - **Choose Report Type**: All the available reports types can be scheduled (select either one and follow the instructions given below followed by&#65533; **Configuring the Time Settings**)

   Scheduling Device Availability reports:

   - If you have chosen to schedule reports for **Device availability reports** and&#65533; configure the following,&#65533; Select either a category of devices, or the required business view, or select specific devices manually for generating the availability reports.
   - Select the **Period** and **Time Window** for which you want to generate the reports.
   - Select the days for which you want to exclude data in report using **Exclude Days** option.

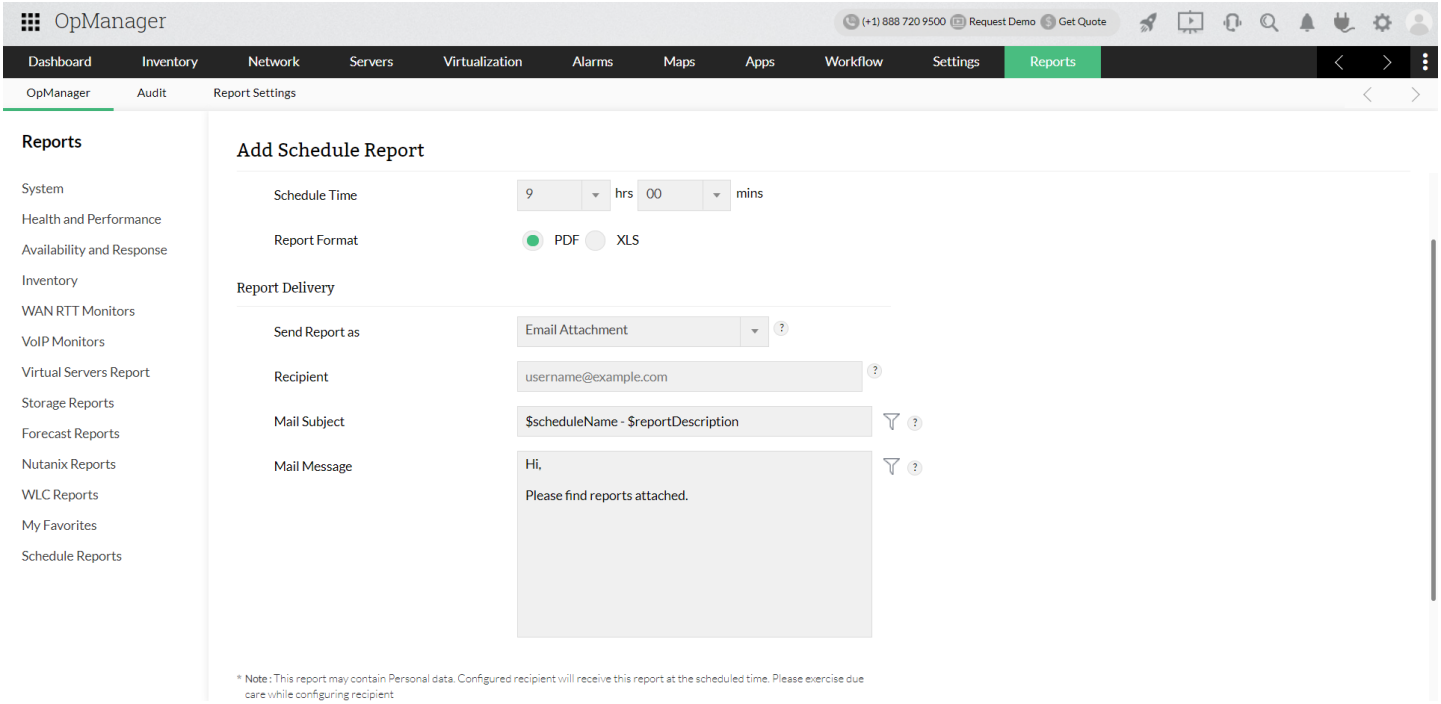
   Scheduling Top N Reports / All Devices reports:

   - If you have selected to schedule the Top N Reports, configure the following details:
   - **Top N Reports**: Select from Top 10/25/50/100/1000 reports.
   - **Period and Time Window**: Choose the Period and Time Window for which you want the report scheduled. In time period, select the days for which you want to exclude data in the report using Exclude Days option.
   - **Select Report(s)**: Select the required resource reports to be scheduled.
   - **Generate Availability Report to all devices in this Business View**: Select the relevant check-box and the business view to generate reports specific to the devices in that business view.

4. Click **Next**
5. **Configuring the Schedule for generating reports:**

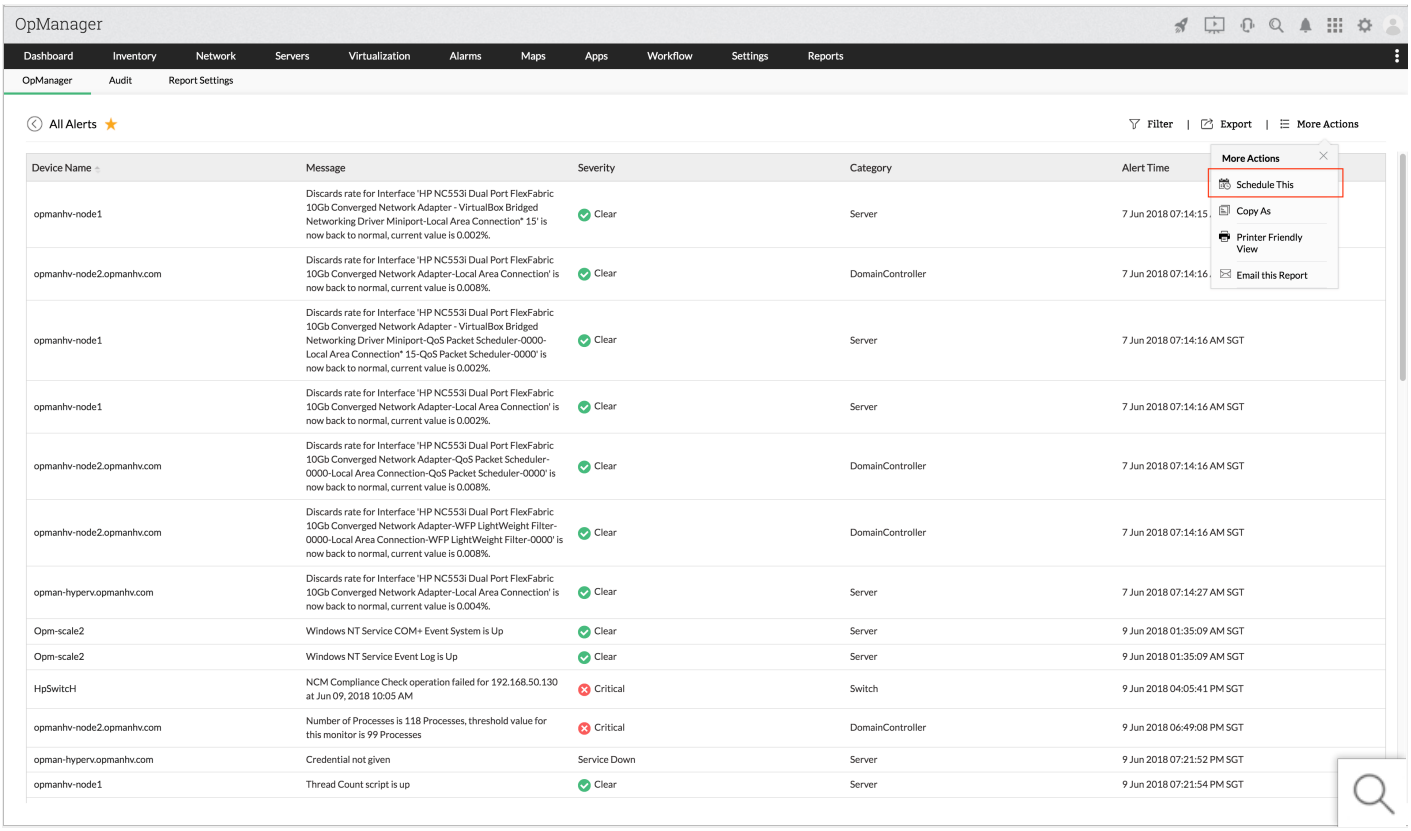
   - **Daily**: Select the time at which the reports must be generated every day
   - **Weekly**: Select the time and also the days on which the reports must be generated
   - **Monthly**: Select the time, day, and the months for which the reports must be generated
   - **Report Format Type**: Select either PDF or XLS to receive the report in the respective formats
   - **Report Delivery**: Select any one of the following options
     - **Send report as attachment to**: Configure the email ids to which the reports are to be sent as attachments [or]
     - **Publish the report and send URL alone to**:&#65533; Configure the url where the reports can be published
     - Add **Mail Subject** and **Mail Message**

6. Verify the details of the configured schedule and hit **Add Schedule** for the schedule to take effect

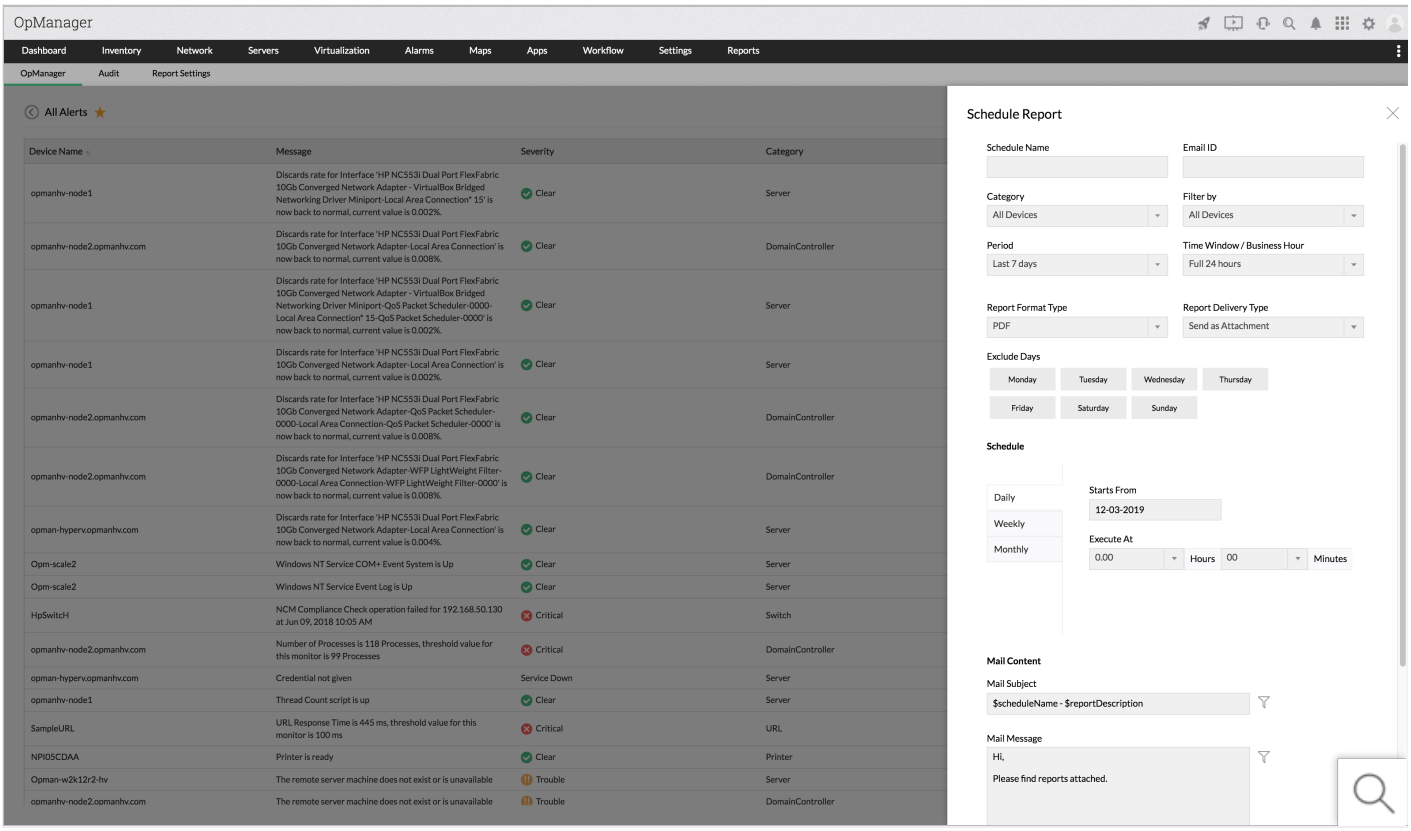


Scheduling a generated report

1. In the report page that is generated, click **Schedule This**icon to schedule the report.



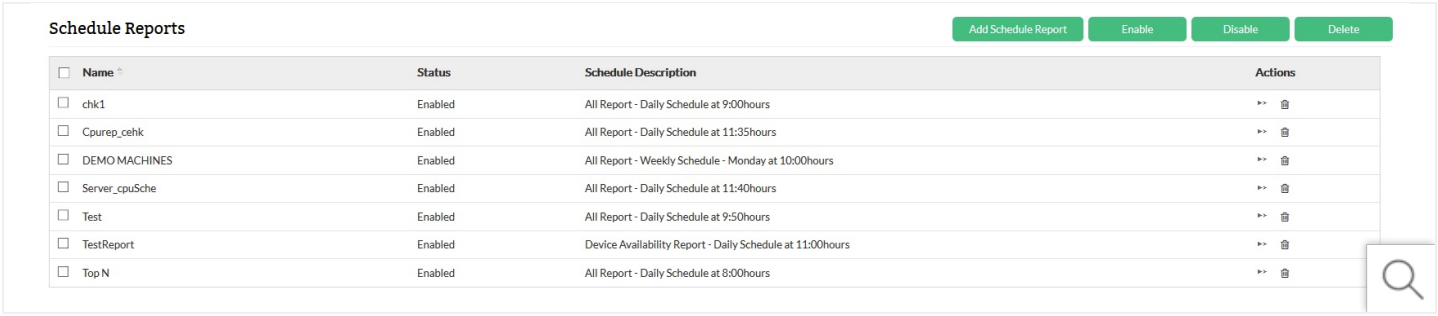
2. Enter the **Schedule Name**
3. Enter the**&#65533; Email ID&#65533;** to which the report has to be delivered
4. Select the **Category** followed by**&#65533; Business View**
5. Select the **Period** and **Time Window**. In time period, you can select the days for which you want to exclude data in the report using **Exclude Days** option
6. Select the **Report Format&#65533;** (PDF or XLS)
7. Select the **Report Delivery Type&#65533;** (Attachment or URL)
8. Configure the Generate Report at Daily, Weekly or Monthly
9. Add the required **Mail Subject** and **Mail Message**



3. Click **Save** to create a schedule for the generated report.

Viewing the Scheduled Report

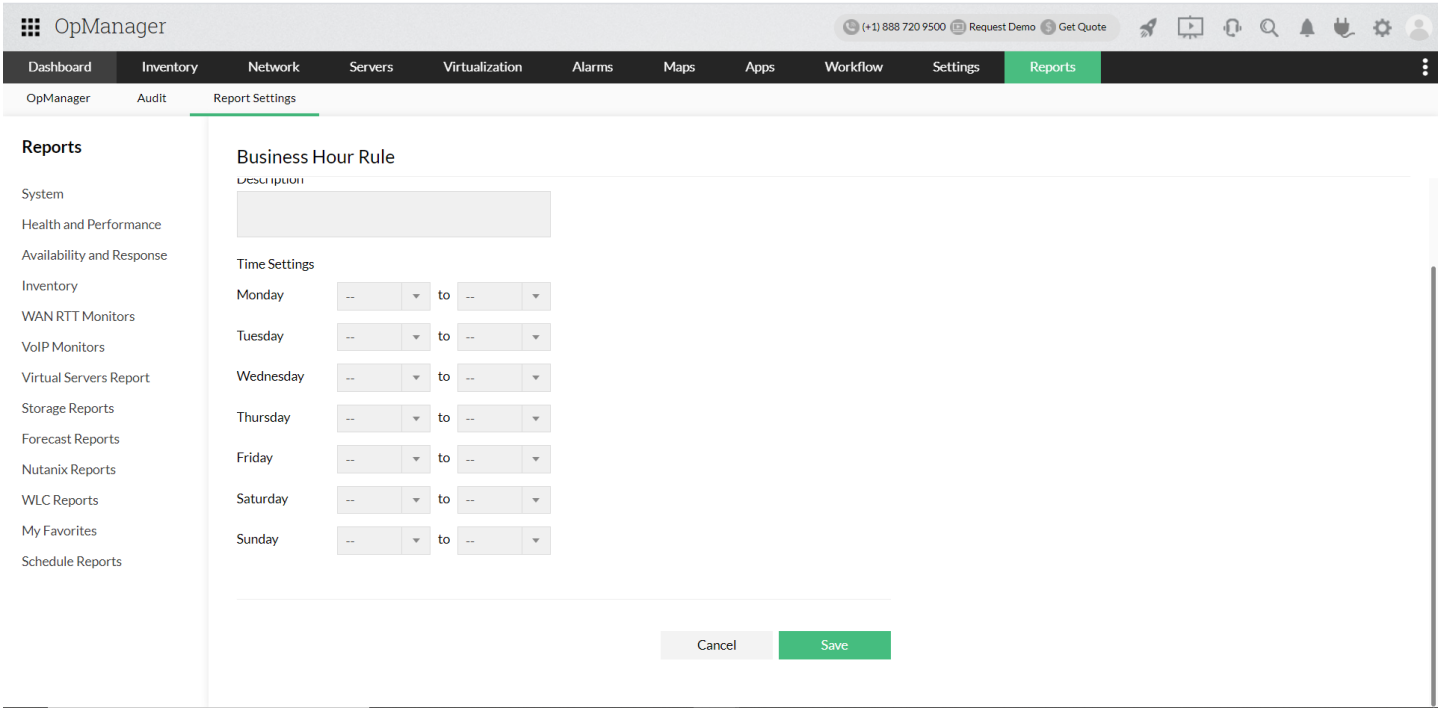
1. Go to Reports → Schedule reports
2. Click against the **View** icon on the required report that you wish to see.
3. The list of generated reports for the selected report will appear.



Configure Business Hour Rules

You can configure the Business Hour Rule in OpManager to filter out and view only the reports generated within the business hours of your organization.

- Navigate to **Reports-> Report Settings-> Business Hour Rules.**
- Click on **Add Rule**.
- Provide a Name and Description.
- Select the time duration from the drop down for each day.
- Click on **Save**.

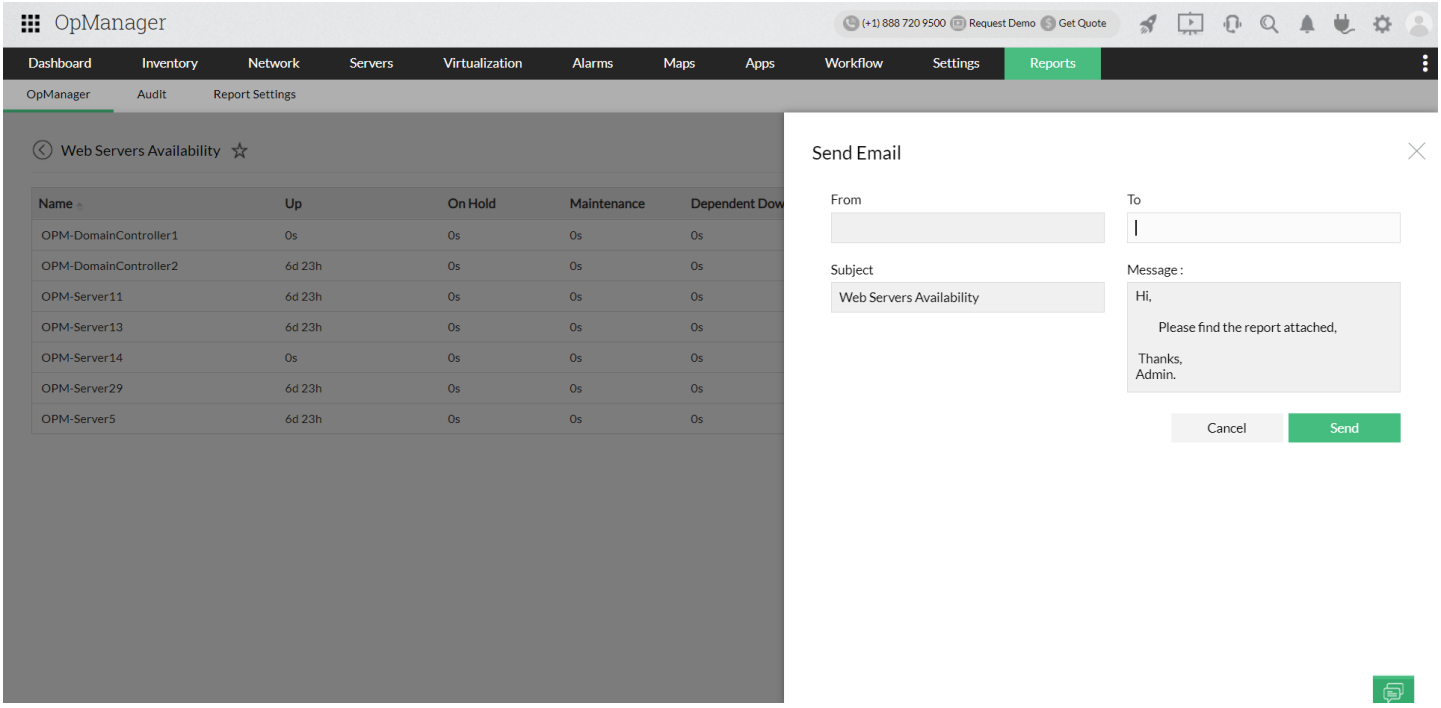


How to disable or enable scheduled reports in bulk

- Navigate to **Reports --> OpManager --> Scheduled Reports**.
- Select the reports that you want to enable/disable by checking the box left adjacent to the Name of the report.
- Click on*Enable/Disable* available on the top to update the list.
- Once updated, a banner message will appear on top as 'Values updated successfully'.

How to email default reports in OpManager

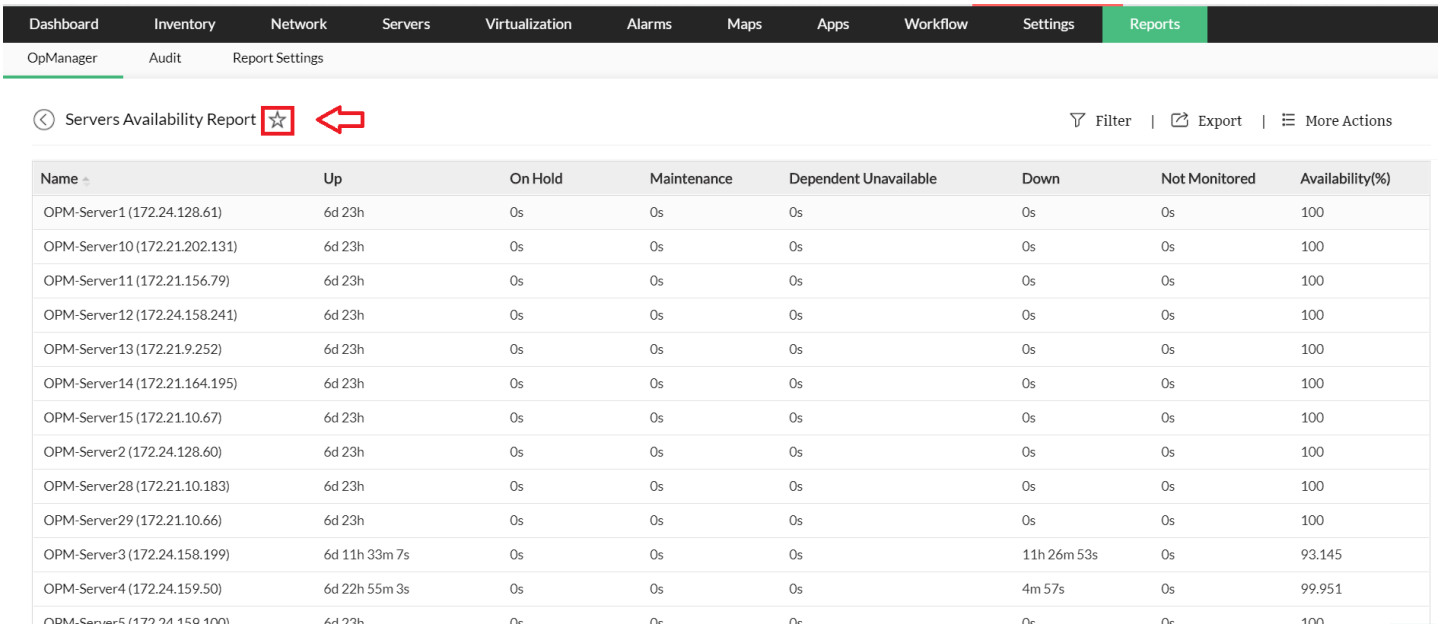
- Navigate to **Reports --> OpManager**.
- Select the particular report from a report category. (For Eg: Availability and Response --> Web Servers Availability)
- Click on *More Actions* on the top right corner.
- And click on *Email this Report*.
- Then enter the *From* and *To* mail IDs along with the *Subject* and *Message.*
- Finally click *Send*.


OpManager
(+1) 888 720 9500
Request Demo
Get Quote
Dashboard
Inventory
Network
Servers
Virtualization
Alarms
Maps
Apps
Workflow
Settings
Reports
OpManager
Audit
Report Settings
Web Servers Availability
Name
Up
On Hold
Maintenance
Dependent Dow
OPM-DomainController1
0s
0s
0s
0s
OPM-DomainController2
6d 23h
0s
0s
0s
OPM-Server11
6d 23h
0s
0s
0s
OPM-Server13
6d 23h
0s
0s
0s
OPM-Server14
0s
0s
0s
0s
OPM-Server29
6d 23h
0s
0s
0s
OPM-Server5
6d 23h
0s
0s
0s
Send Email
From
To
Subject
Web Servers Availability
Message :
Hi,
Please find the report attached,
Thanks,
Admin.
Cancel
Send

Configuring Favorite Reports

With OpManager you can mark the reports that are frequently viewed as Favorite reports. The reports that are marked as favorite reports are listed under My Favorites report category. To mark a report as your favorite one, follow the steps given below:

1. Generate the report that you want to mark as your favorite.
2. Click the **Star** icon (Mark a report as Favorite) at the top of the page to mark a report as Favorite.



Name	Up	On Hold	Maintenance	Dependent Unavailable	Down	Not Monitored	Availability(%)
OPM-Server1 (172.24.128.61)	6d 23h	0s	0s	0s	0s	0s	100
OPM-Server10 (172.21.202.131)	6d 23h	0s	0s	0s	0s	0s	100
OPM-Server11 (172.21.156.79)	6d 23h	0s	0s	0s	0s	0s	100
OPM-Server12 (172.24.158.241)	6d 23h	0s	0s	0s	0s	0s	100
OPM-Server13 (172.21.9.252)	6d 23h	0s	0s	0s	0s	0s	100
OPM-Server14 (172.21.164.195)	6d 23h	0s	0s	0s	0s	0s	100
OPM-Server15 (172.21.10.67)	6d 23h	0s	0s	0s	0s	0s	100
OPM-Server2 (172.24.128.60)	6d 23h	0s	0s	0s	0s	0s	100
OPM-Server28 (172.21.10.183)	6d 23h	0s	0s	0s	0s	0s	100
OPM-Server29 (172.21.10.66)	6d 23h	0s	0s	0s	0s	0s	100
OPM-Server3 (172.24.158.199)	6d 11h 33m 7s	0s	0s	0s	11h 26m 53s	0s	93.145
OPM-Server4 (172.24.159.50)	6d 22h 55m 3s	0s	0s	0s	4m 57s	0s	99.951
OPM-Server5 (172.24.158.100)	6d 23h	0s	0s	0s	0s	0s	100

A message is displayed saying that "This report has been added to your favorite list".

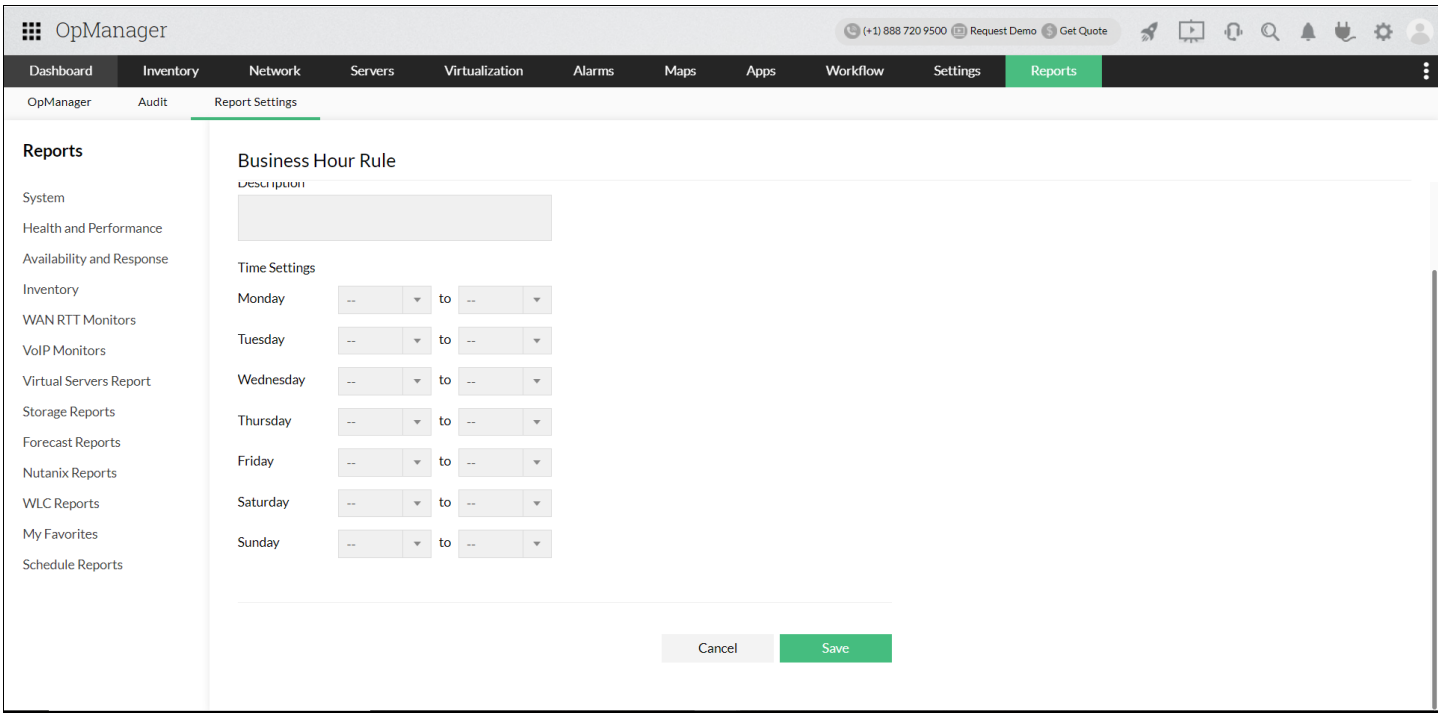
Report Settings

Under Report Settings in OpManager, users can configure the Business Hour Rule. Each organization will have different working hours/ business hours and by defining this rule, users can filter out reports only for the specified business hours.

Also, users can specify a different time window each day as per their needs.

How to configure Business Hour Rule?

- Navigate to **Reports -> Report Settings -> Business Hour Rules**.
- Click on **Add Rule**.
- Provide a Name and Description.
- Select the time duration from the drop down for each day or the particular days which are required.
- Click on **Save**.

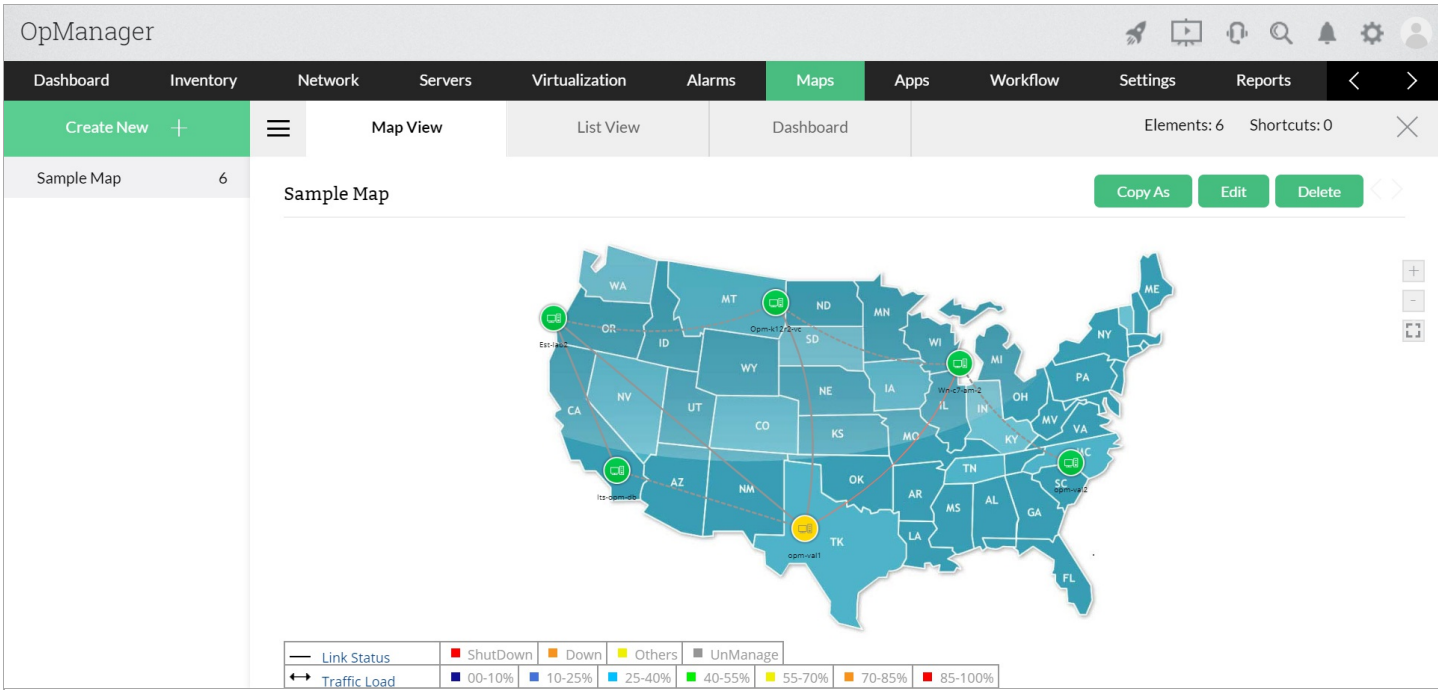


Business Views:

Business views in OpManager provide a graphical representation of devices according to the business service they cater to. This ensures the availability of business critical applications at all times and helps in quicker troubleshooting.The Business View Tab can be accessed both from the Maps and Inventory section of OpManager.

Creating a Business View:

1. Go to **Maps** > **Business Views** > **Create New**. Or go to **Inventory** > **Business Views** > **Add Business View**.
2. Rename the Business view from 'New Business View' on the upper left corner to the desired one.
3. From the list of available devices, you can add devices onto the white board individually, using **Drag and Drop** or add devices in bulk with **Multi select** option.
4. You can customize the view by changing font type, size and color.
5. Choose the required **Background**(Map) from the preloaded images or upload a new background image and select Apply.
6. Drag and drop devices on the Map based on your requirement.
7. **Save** the created view.
8. Select **Exit** to close the view. The created view would be displayed under the Business Views Tab.



Creating Links between devices:

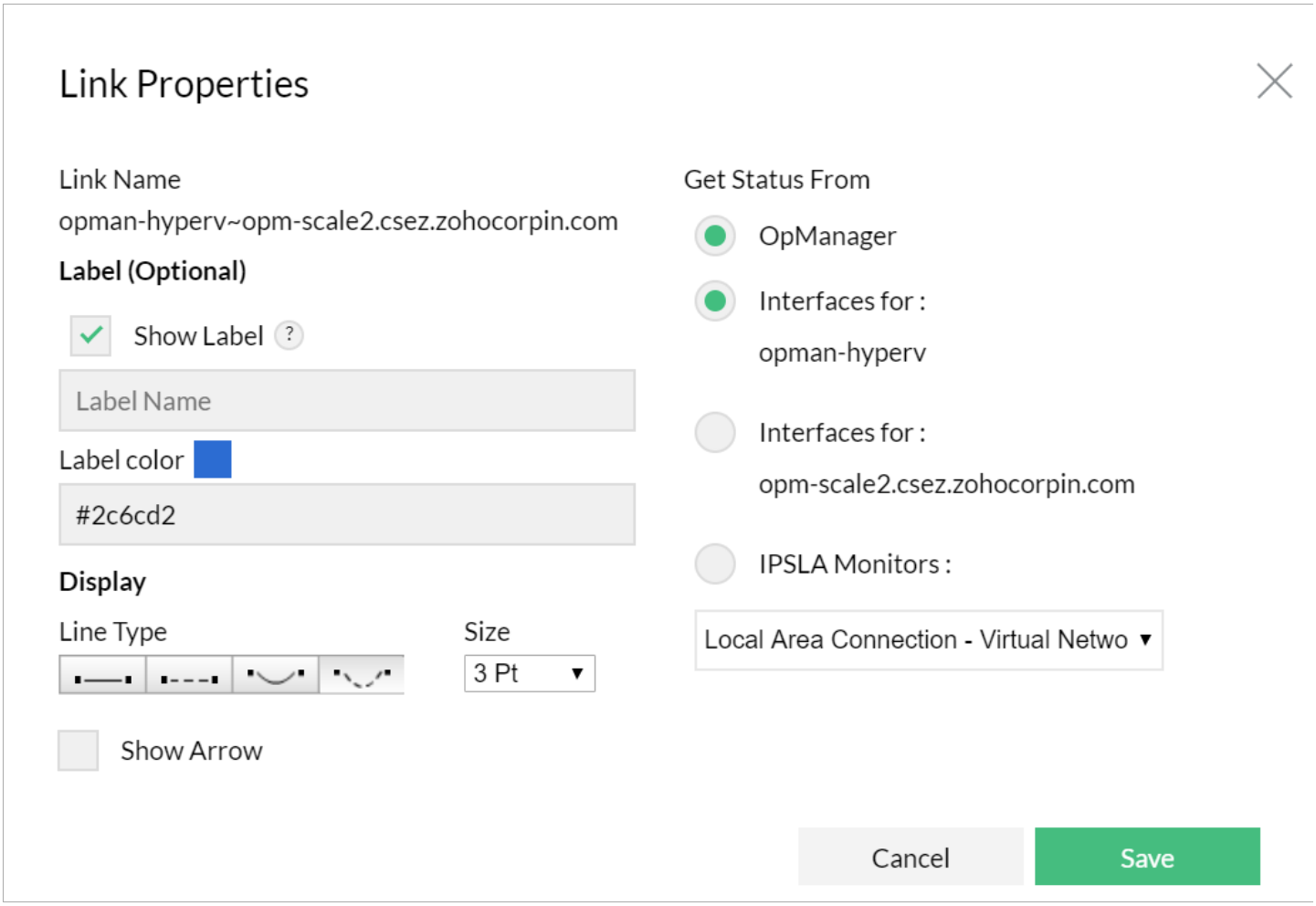
Adding links between devices in business views, helps to represent network diagram on the map. These links can be configured based on user requirements.

To add a link between two devices in a business view,

1. Select the **Add link** button next to the **Background tab**. Drag a link from the source to the destination device and click that device. A link properties dialog pops up.
2. Alternatively you can also drag the link button at the top right corner of the source device icon to create a link to the destination device.
3. Configure a display name for the link.
4. In the **Get Status from** field, select any interface from either the source device or the destination device. The link will inherit the status of the interface that you choose here. For instance, if the source device goes down, and if you have selected an interface from that device, the link also inherits the status of that device.

Note: You can also select to Get Status from either OpManager or NetFlow. If OpManager is selected, status is got through SNMP. If NetFlow is selected, detailed data like Top Source, Destination, QoS etc., can be obtained.

5. Select the line type and size.
5. Deselect the **Show Arrow** check box if you don't want to show the traffic arrows.
7. Click **Apply**.
3. Click **Save** on the left to save the changes.



Modifying Business Views:

1. To make changes to the existing business views, Access the business view from the **Maps** tab.
2. Click the **Edit** icon to modify the view properties.
3. After modifying the properties like adding/removing links, adding more devices to the view, adding shortcuts on the view, changing background etc, click the **Save** button on the left to save the changes.

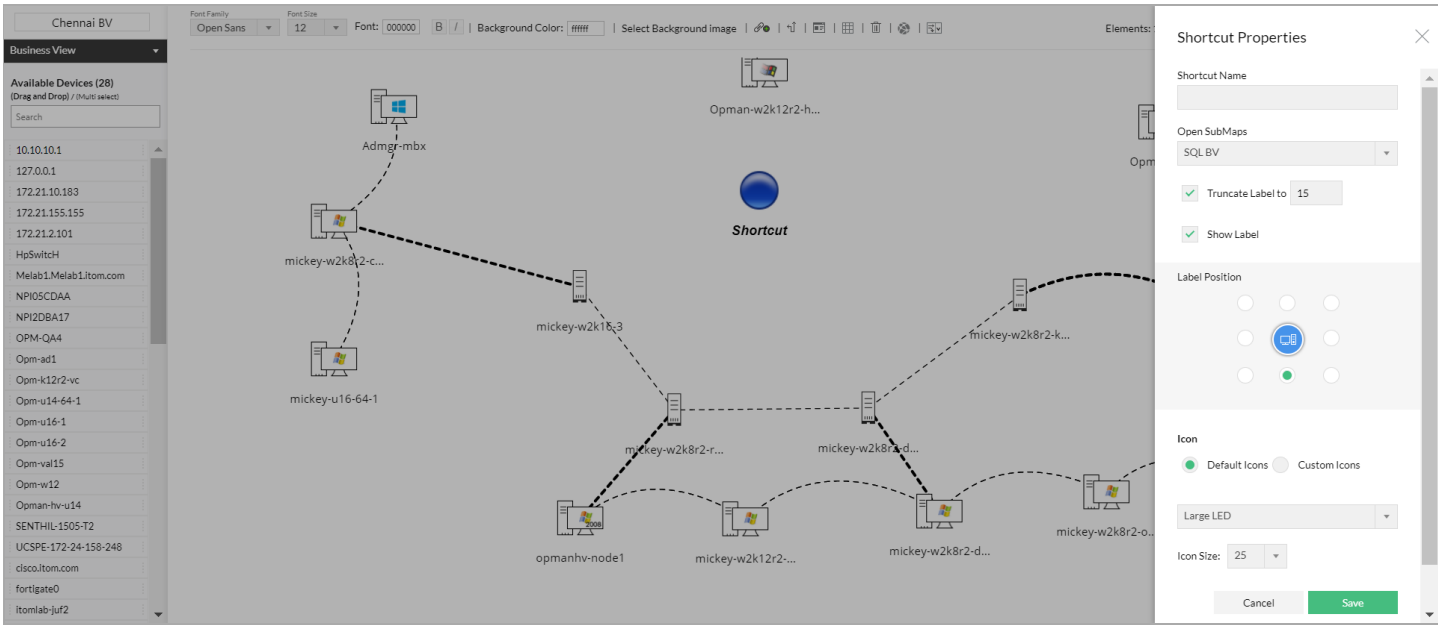
Adding Shortcuts:

You can add shortcut icons to business views that helps to easily navigate to a view from another view when objects are grouped based on their geographical location.

1. Go to the business view and click the Edit option on right-top corner of the view.
2. Click the Add Shortcut button on the left. A shortcut properties dialog pops up.
3. Configure a name for the shortcut in the Shortcut Name field.
4. From the **Open Submap** list-box, select the map which should be opened when you click the shortcut.
5. Select the icon to be used for the shortcut from the Default Icons or select from the Custom Icon combo-box.

5. Click Apply for the shortcut to be added.

Note: You must have created at least two business views to be able to add a shortcut from one view to another.



Traffic Load Legend:

Traffic load legend is a color coded representation of the status of the Link and Traffic load data of the devices in a Business view.

The Traffic load legend colors can be edited. To do this, go to **Settings** > **General Settings** > **System Settings** > **Map Settings**. Hover your cursor on the color that you wish to change and click the edit icon that appears. Choose a color of your preference and click **Save**.

Note: For the Traffic load legend to be displayed, make sure the devices in the Business view are not in unmanaged state. In addition to this, the devices in the Business view should have atleast one active link connection with the availability of traffic.

Google Maps:

OpManager allows you to integrate Google Maps and place the devices on the maps according to the geographic distribution. Please refer to the google licensing terms and pricing plans before you proceed further.

To configure Google maps

1. Download this map file to your desktop.
2. Map filed named GMaps_12300.zip is downloaded.
3. Upload the downloaded map file in OpManager and enter the API key. (In case you do not have the API key, click on the link given above the API box in the client)
4. Accept the terms of service and click on 'Submit'.

Adding Devices on the Google Map

1. You can zoom in/out the map and double-click on the location where you want to place a discovered device.
2. A device list box pops up allowing you to select a device to be placed in that location.
3. Select the device and click on Add.
4. You can also add the devices to the map from the device snapshot page.
5. Go to the device snapshot page and select a device. Click on the green colored menu button.
6. Choose **Add to Maps** option to add the device to the map.
7. Once done, you can switch between the different views such as Road map, Terrain, Satellite, Hybrid (Satellite view with label) and save it accordingly in Maps and its corresponding widgets.

Viewing Device Details from Google Map

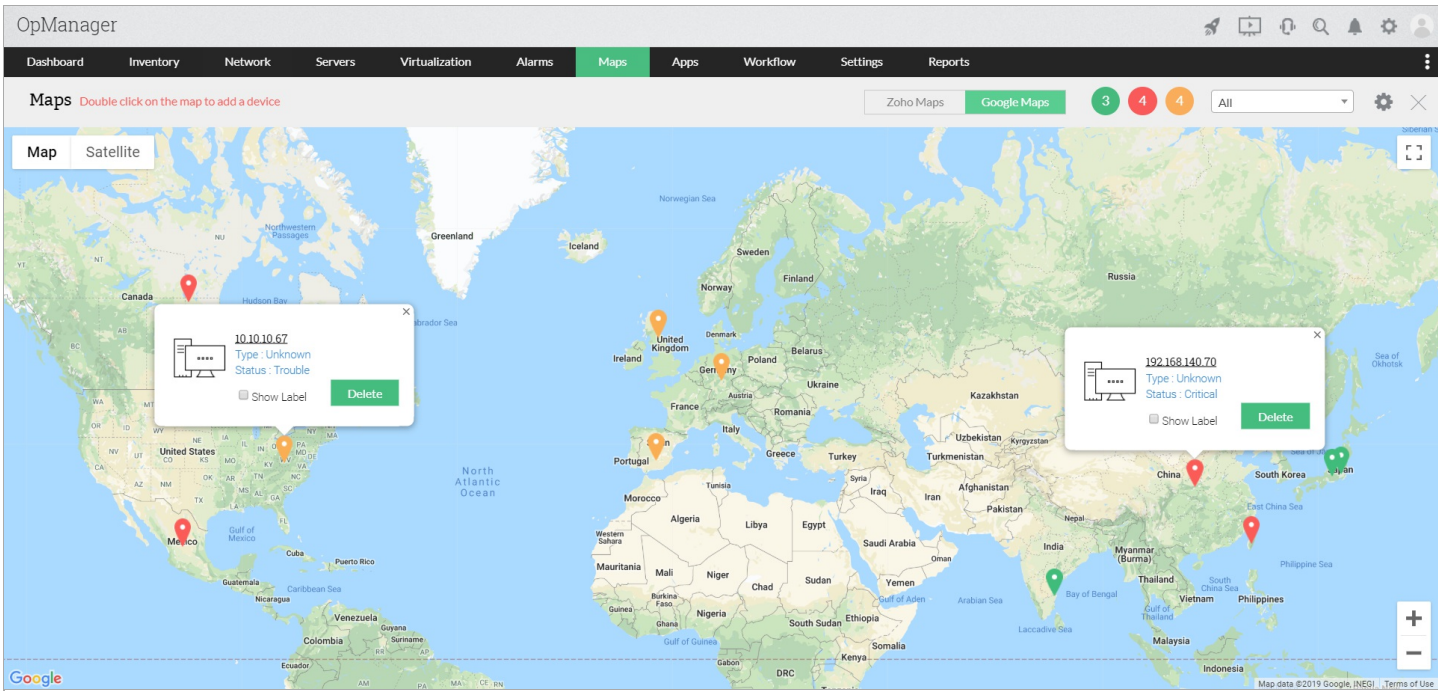
1. Click on the device marker on the Google Map to see the device information popup.
2. Click the device name/IP address on this popup to get into the device snapshot page.
3. The popup also shows the device status.

Import/Export devices

1. **Import:** You can import device to Google maps directly from a CSV file. OpManager will position them on the map as per the latitude and longitude details in the CSV file. However, only the devices that are already discovered in OpManager can be imported.
2. **Export:** You can download the information of the devices that are placed on the Map including their geographic location (latitude and longitude) in XLS format using this option.

Deleting Devices from Google Map

1. Click on the device marker on the Google Map to see a popup.
2. Click the Delete link on this popup to delete the device from the map.


OpManager
Dashboard
Inventory
Network
Servers
Virtualization
Alarms
Maps
Apps
Workflow
Settings
Reports
Maps
Double click on the map to add a device
Zoho Maps
Google Maps
3
4
4
All
Map
Satellite
10.10.10.67
Type : Unknown
Status : Trouble
Show Label
Delete
192.168.140.70
Type : Unknown
Status : Critical
Show Label
Delete
Google
Map data ©2019 Google, INEGI
Terms of Use

Zoho Maps

OpManager uses Zoho Maps as the default map provider for the Maps feature. You can use it to visualize your network by placing the devices on the maps according to their geographic distribution. You can also display the equivalent ground distance in kilometres or miles using Zoho Maps.

Adding Devices on the Zoho Map&#65533;

1. Now, zoom in/out the map and double-click on the location where you want to place a discovered device.
2. A device list box pops up allowing you to select a device to be placed in that location.
3. Select the device and click on Add.
4. Add the required devices on to the map by double-clicking the location.
5. You can also add the devices to the map from the device snapshot page.
6. Go to the device snapshot page.
7. Click on Add to Map link in the page to add the device to the map.

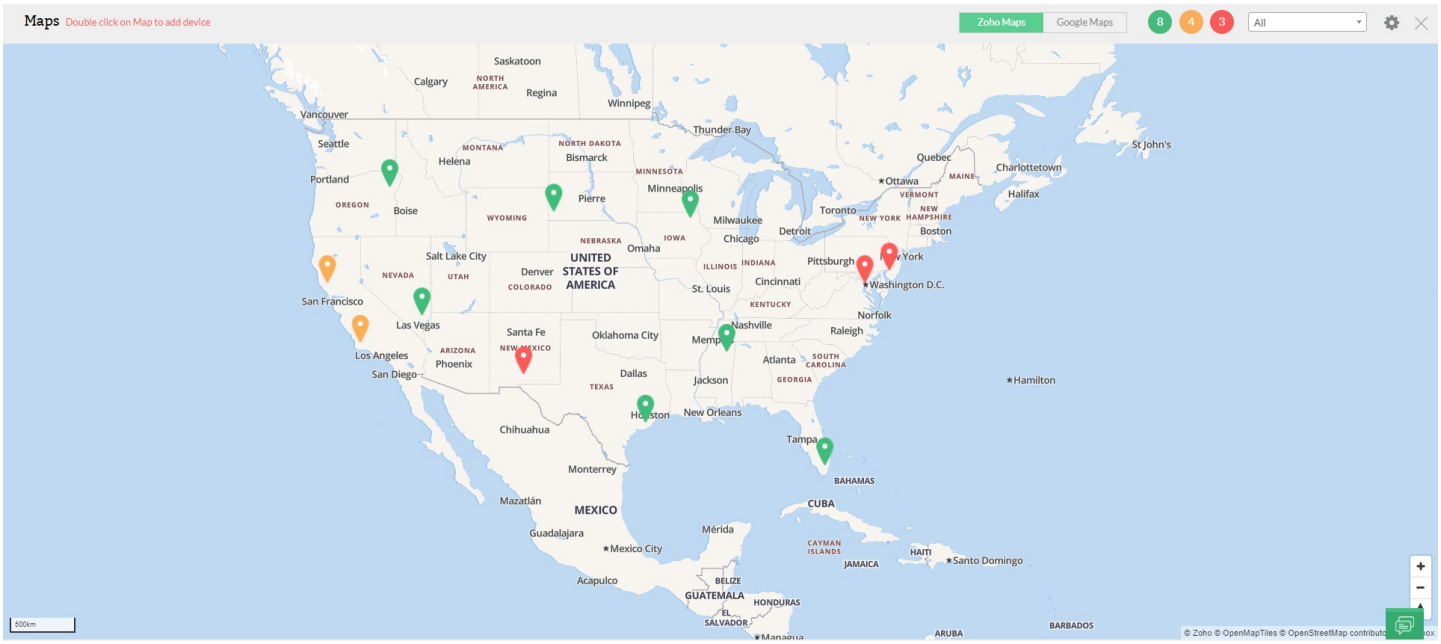
Viewing Device Details from Zoho Map

1. Click on the device marker on the Zoho Map to see a popup.
2. Click the device name/IP&#65533; address on this popup to get into the device snapshot page.
3. The popup also shows the device status.

Deleting Devices from Zoho Map&#65533;

1. Click on the device marker on the Zoho Map to see a popup.
2. Click the Delete link on this popup to delete the device from the map.

&#65533;



Datacenter Visualization

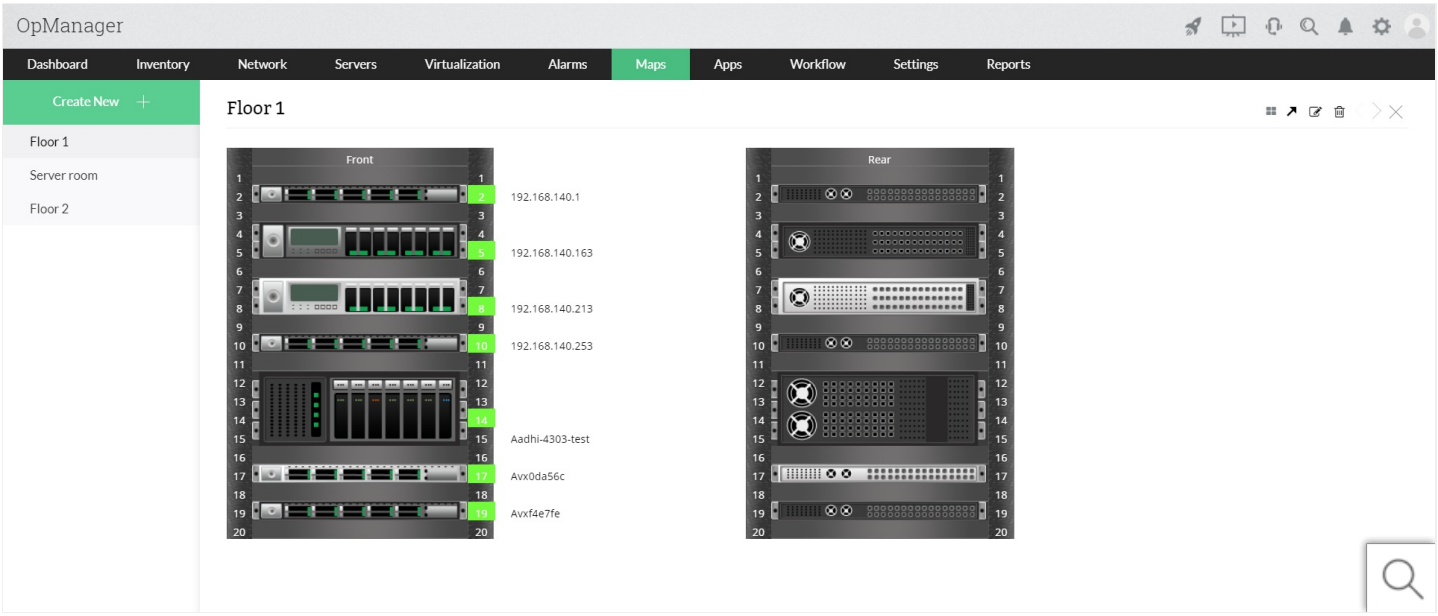
OpManager helps in creating a virtual replication of Datacenter floors and racks to enable 24x7 monitoring. Datacenter visualization is one among the many features of OpManager's data center networking tool.

3D Rack View:

Virtual Racks can be created with OpManager. These racks display the status of the devices present in them.

To create a Rack View,

1. Under Maps, select the Create New option under Rack Views Tab.
2. Drag and Drop the devices onto the Rack.
3. Click Save on the top right corner.
4. The status and availability of the devices can be seen in the rack created.
5. To observe the rear view of your rack in addition to the front view, click **Edit** and select **Rear view**.

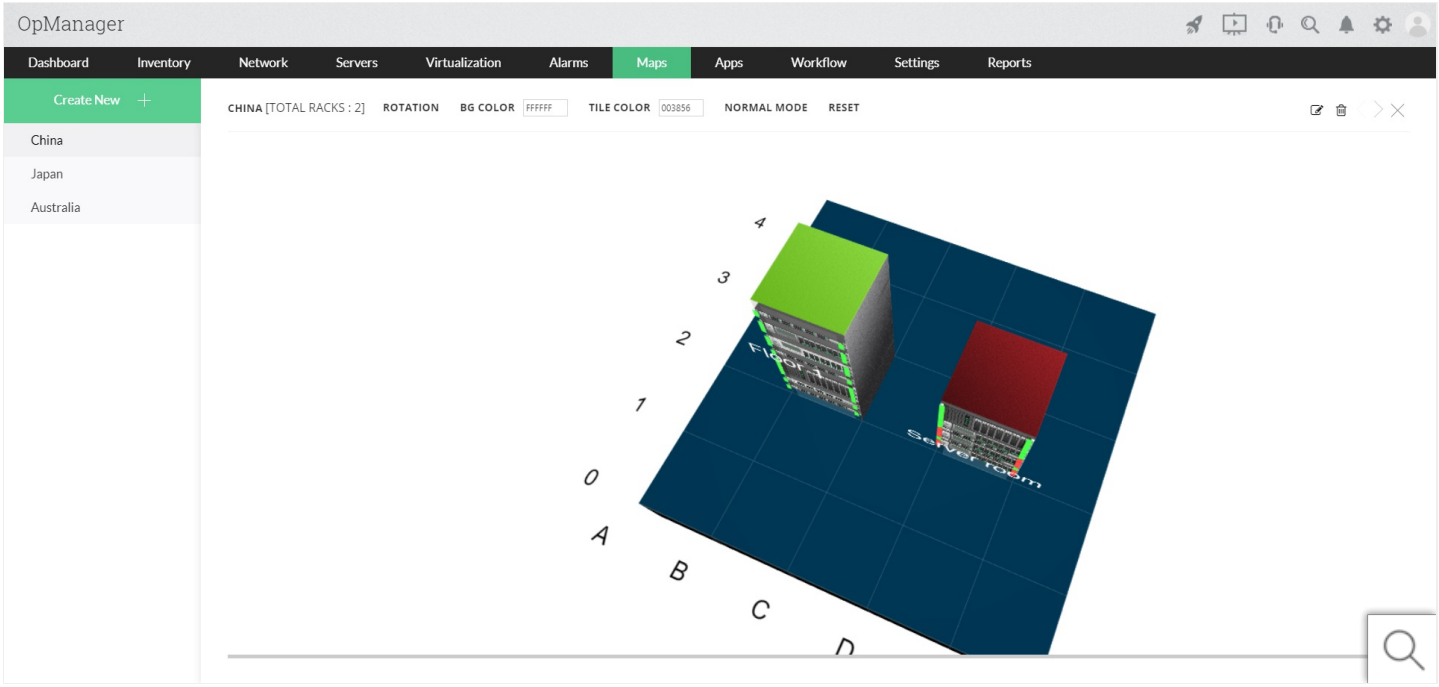


3D Floor View:

Floor views can be created in OpManager. The racks are then loaded onto the floor views to create a virtual replica of the Data center.

To create a Floor View,

1. Under Maps, select the Create New option under Floor Views Tab.
2. Select your floor size .
3. Drag and drop paths, aisles and walls as per your Data center.
4. Populate an existing rack view onto the floor map to create your Data center replica.


OpManager
Dashboard
Inventory
Network
Servers
Virtualization
Alarms
Maps
Apps
Workflow
Settings
Reports
Create New
China
Japan
Australia
CHINA [TOTAL RACKS : 2]
ROTATION
BG COLOR
FFFFFF
TILE COLOR
003856
NORMAL MODE
RESET
4
3
2
1
0
A
B
C
D

Layer 2 Map

Create a Layer2 map:

OpManager renders the logical network topology diagram once you discover the networks and network devices. For a better visualization of the physical network connectivity in real networks and the consequences of a failure of a device, network topology map comes handy.

To create a Layer2 Map, go to **Map** > **Layer 2 Maps** > **Create New**. For detailed instructions click here.

Layer2 Map views:

After discovering your network topology, you can choose to view it in three different views, **Radial Tree** (default view), **Node Link** and **Balloon Tree**. You can switch between the views by clicking on their respective icon present in the top right corner.

Layer2 Map Settings:

Click on the settings icon to explore additional functions.

- **Import Devices:**
  The devices that are discovered in Layer2 maps will not be added to OpManager for monitoring purposes unless they have been imported.

  Click on **Settings** and choose **Import Devices**. A screen containing all the devices that have been identified by the Layer2 Map will be displayed. This list also includes the ones that have already been imported to OpManager.

  From the list, select the devices that are yet to be imported to OpManager and click on **Discover**. Discovery process will commence and a list of all the newly imported devices will be displayed in the device snapshot page.

- **ReDiscover Map:**
  This option is used when you want to rerun Layer2 discovery with-in the same device IP range specified in the discovery window. You can also perform ReDiscovery by clicking on the refresh icon in the **Layer2** section at the **Map** page

- **Save as Business View:**
  The devices that are identified in the Layer2 Map can be saved as a Business view. To do this, click on **Save as Business View**, give the layout a name and press **Save**. The result can be viewed in the Business View section.

- **Export to Visio:**
  Visio is a Microsoft oowned graphic tool exclusively used for drawing network diagrams. The network map discovered in Layer2 Maps can be exported to Visio in an xml file. To know more, click here.

- **Printer Friendly View:**
  You can print a physical copy of your network layout using this option. Click on this button and you will be taken to the Print page. Choose your print preferences and click print. You can also save this layout to your PC as a PDF.

Locating Layer 2 Maps:

OpManager automatically maps L2 devices when Layer 2 discovery is done. The resultant map can be viewed under the Layer 2 tab

of the Maps Section.

Modifying Layer 2 Maps:

OpManager allows you to perform edits on Layer2 Maps that have already been discovered. Click on **Maps** from the horizontal tab and scroll down to the Layer2 Maps section. In the **Actions** column, there is a provision to perform the following:

- **Re-Discovery:**
  Click on the refresh icon to rediscover all the devices within the IP range specified during Layer2 device discovery. This is especially useful when:
  - You have added new devices to your topology.
  - You have updated the device template or interfaces that were connected to existing devices.
  - Made hardware changes to one or many devices.
- **Edit:**
  You can edit the discovery parameters (such as modifying the IP range, editing the seed router, changing the discovery mechanism, set device dependency, change schedule discovery time) of the existing Layer2 Map and rerun the discovery process.