ManageEngine 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. ManageEngine 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.

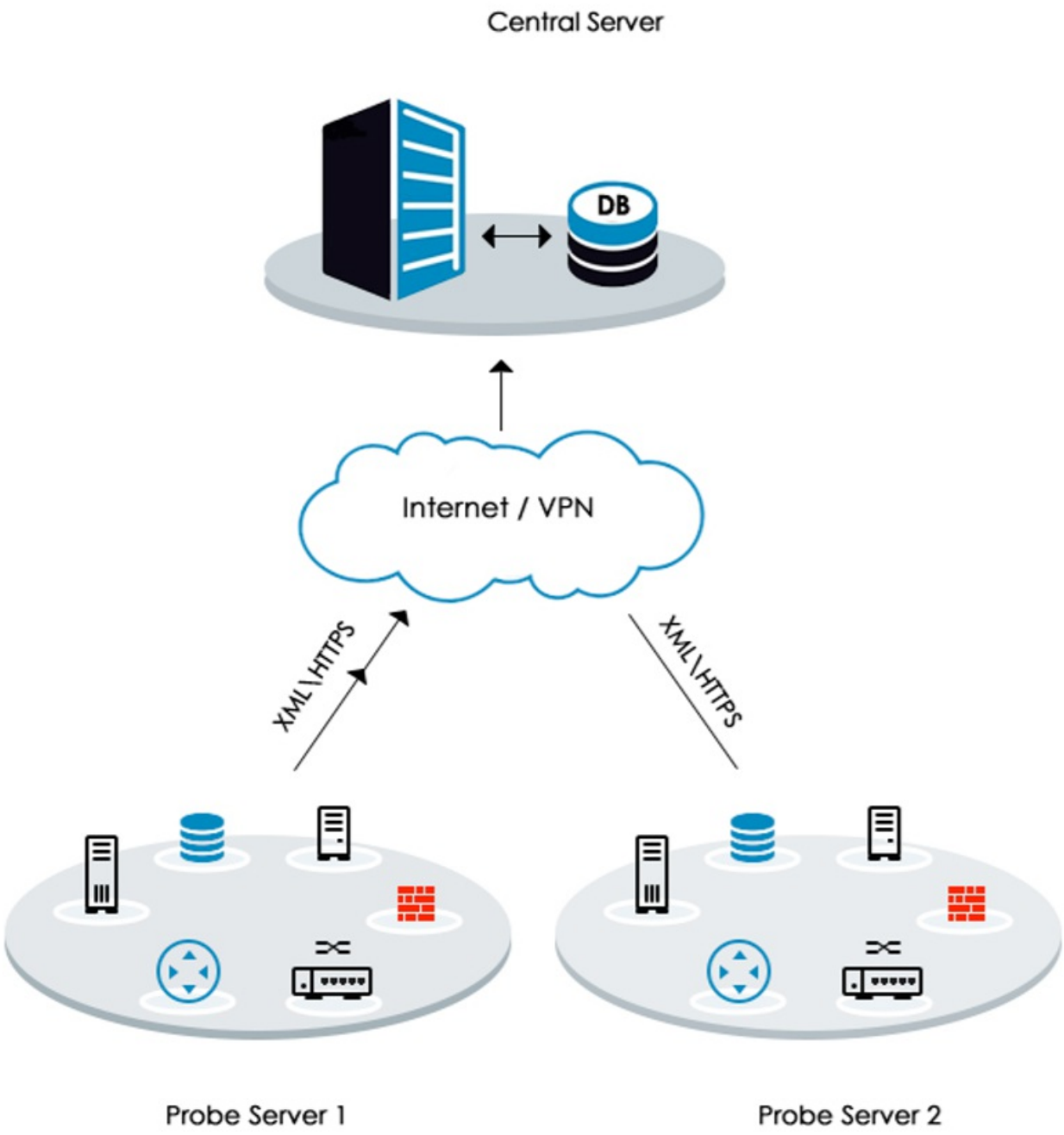
OpManager Enterprise Installation

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

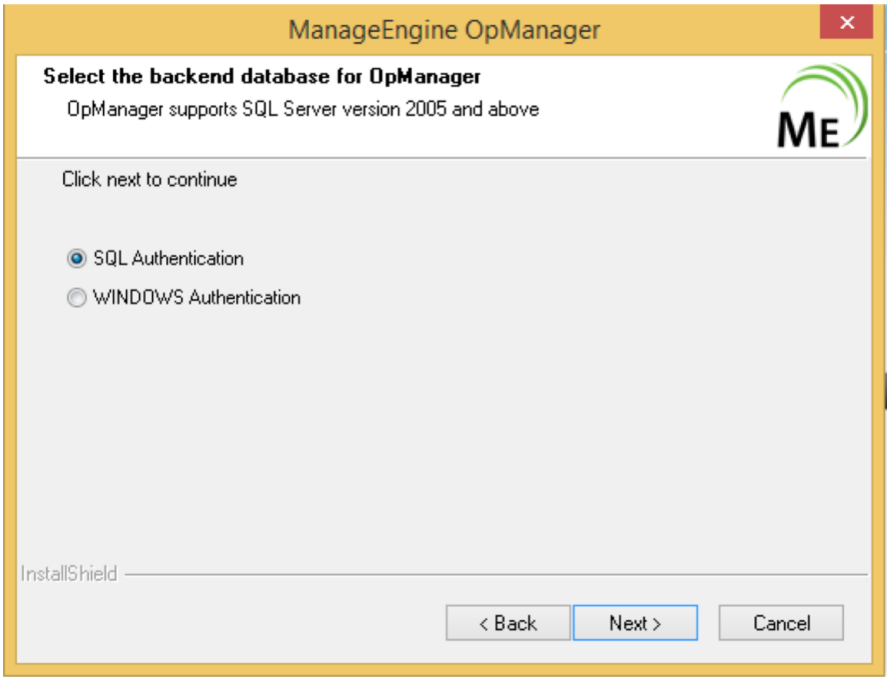
Step 4: Choose the destination folder for OpManager installation and click 'Next' to proceed

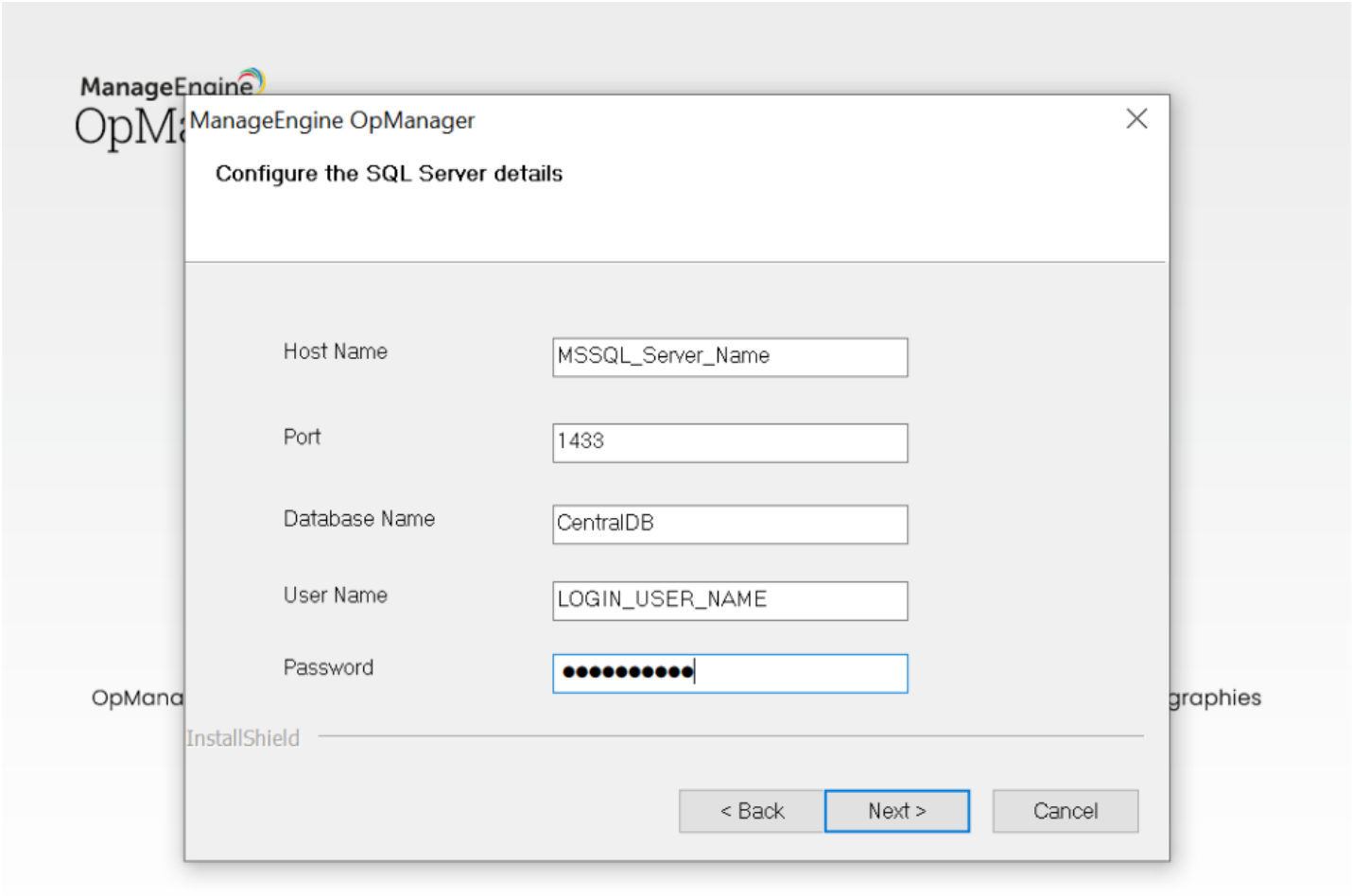
Step 5: If you want to change the default web server port for OpManager installation enter the new port number (OpManager Central uses 8060 as the default web server port) and click 'Next' to proceed.

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

Step 7: If you select PGSQL, please proceed with Step 10. **(or)** If you select 'MSSQL' database (recommended for production). Click 'Next' to proceed

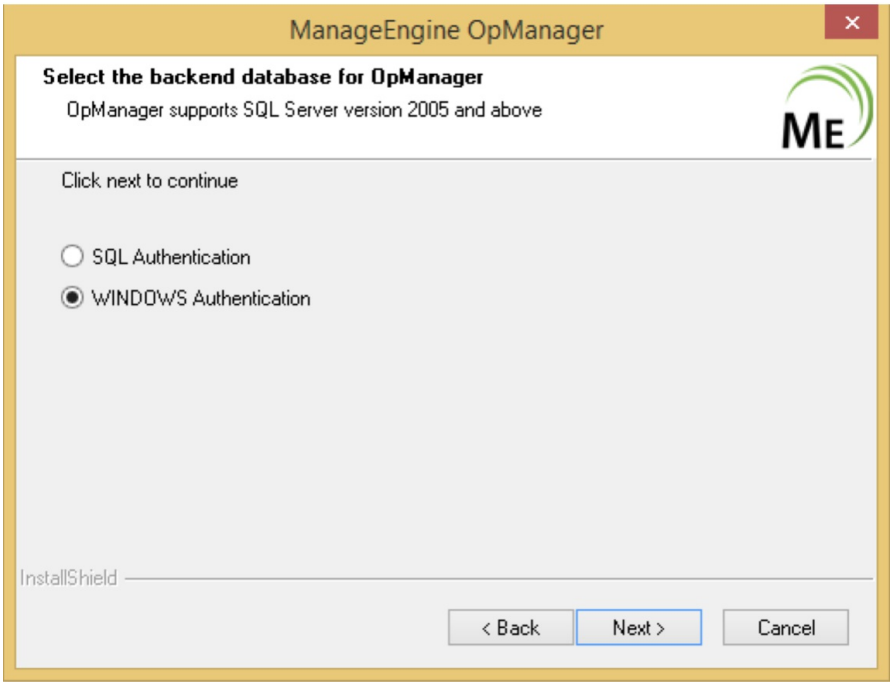
Step 8: If you select SQL Authentication, then provide MSSQL details like Host Name, Port, Database Name. Use the SQL Server Authentication credentials (Username and Password) created earlier. Click 'Next' to proceed

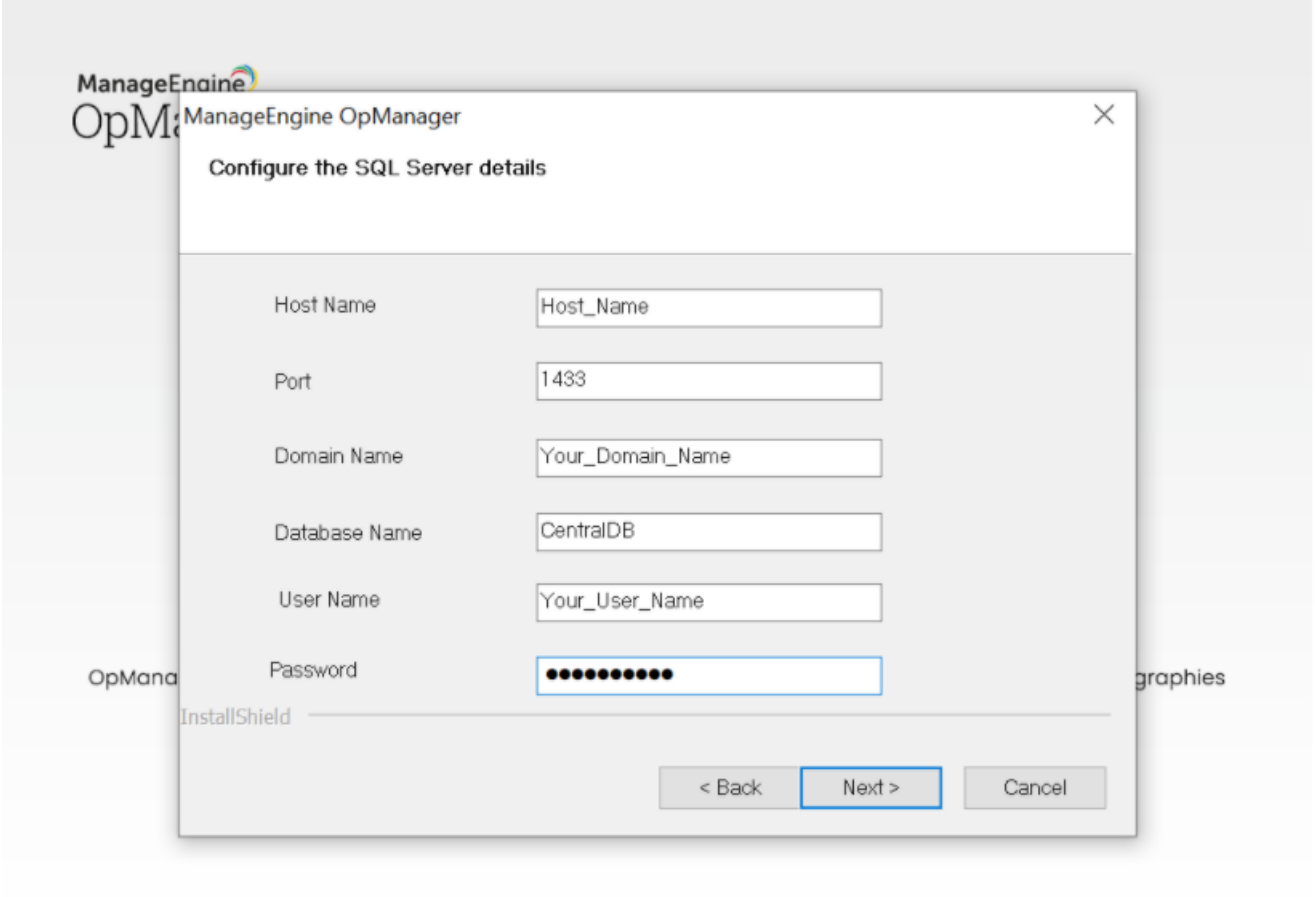




(or)

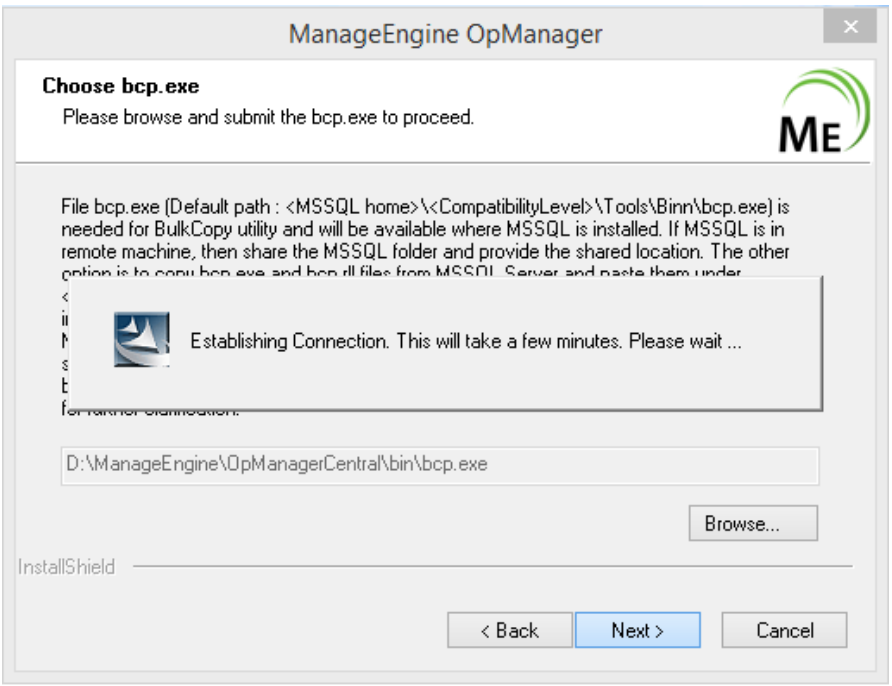
If you select WINDOWS Authentication, then provide MSSQL details like Host Name, Port, Domain Name, Database Name, Username and Password. Click 'Next' to proceed.





Step 9: Search for 'bcp.exe' file click 'Next' to proceed.

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

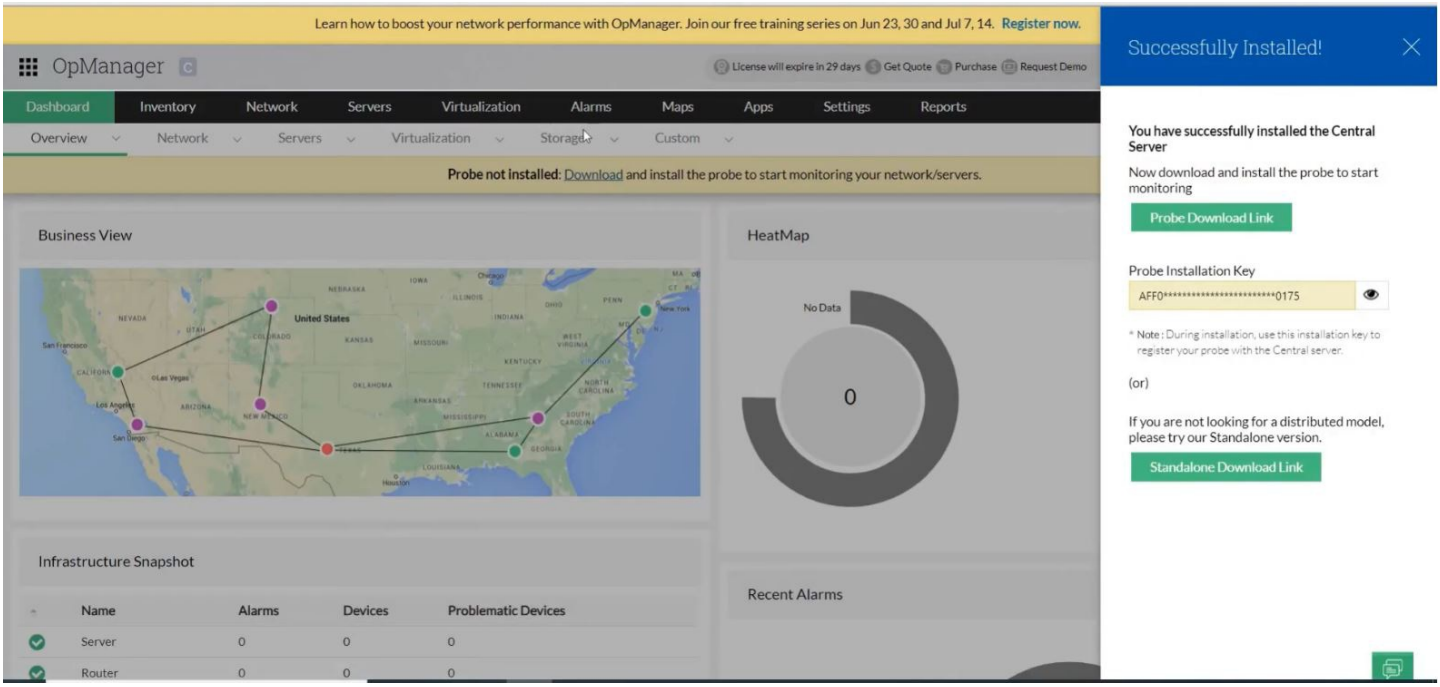


Step 10: Click 'Finish' to complete OpManager Central Server installation.

OpManager Probe Server

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

Run the exe as 'administrator' or Open the installed OpManager Central and click on Probe Link Download to download the appropriate Probe installer.



Step 2: Click 'Next' to proceed with installation

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

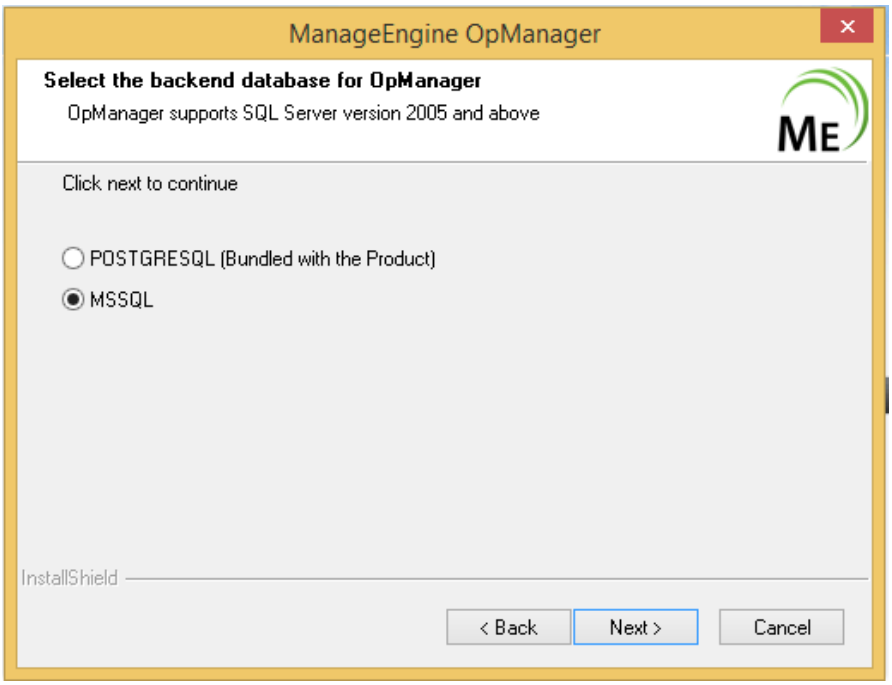
Step 4: Choose the destination folder for OpManager Probe installation and click 'Next' to proceed

Step 5: OpManager uses 8060 as the default web server port, change it as per your preference and click 'Next' to proceed.

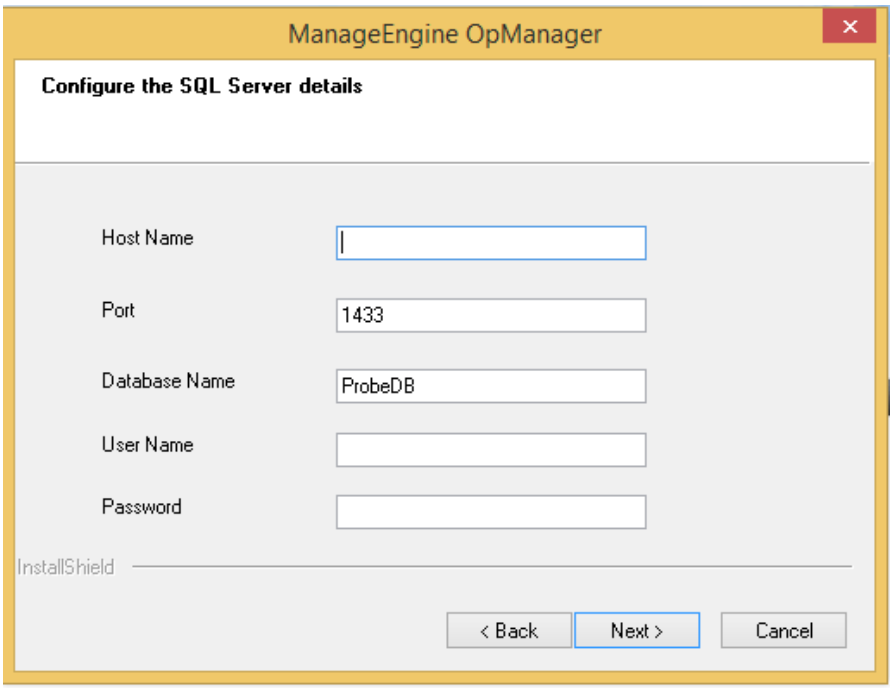
Step 6: Register your OpManager license with required details to get technical support and click 'Next' to proceed.

Step 7: Enter the details of the proxy server (if the probe is installed behind a proxy server) and click 'Next' to proceed

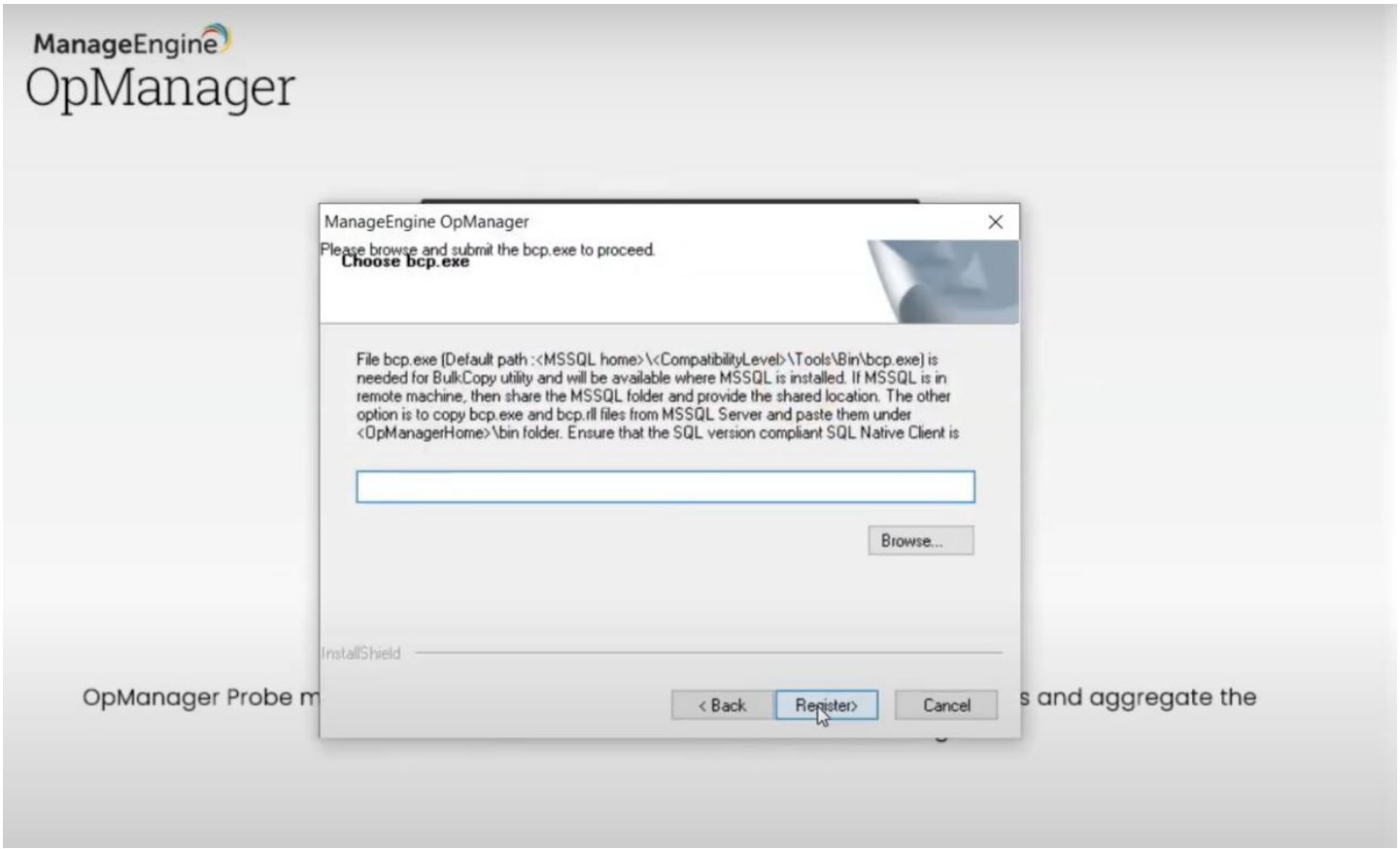
Step 8: If you select PGSQL, please proceed with Step 12. (or) If you select 'MSSQL' database (recommended for production). Click 'Next' to proceed and choose the authentication type - Windows/SQL.



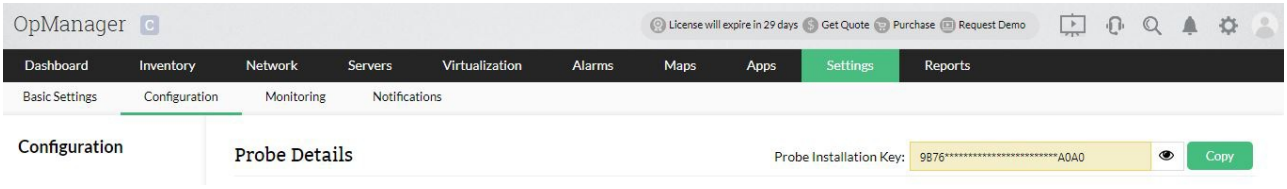
Step 9: Provide MSSQL details like host name, port, database name. Use the credentials (username and password) that was created earlier while configuring SQL. Click 'Next' to proceed

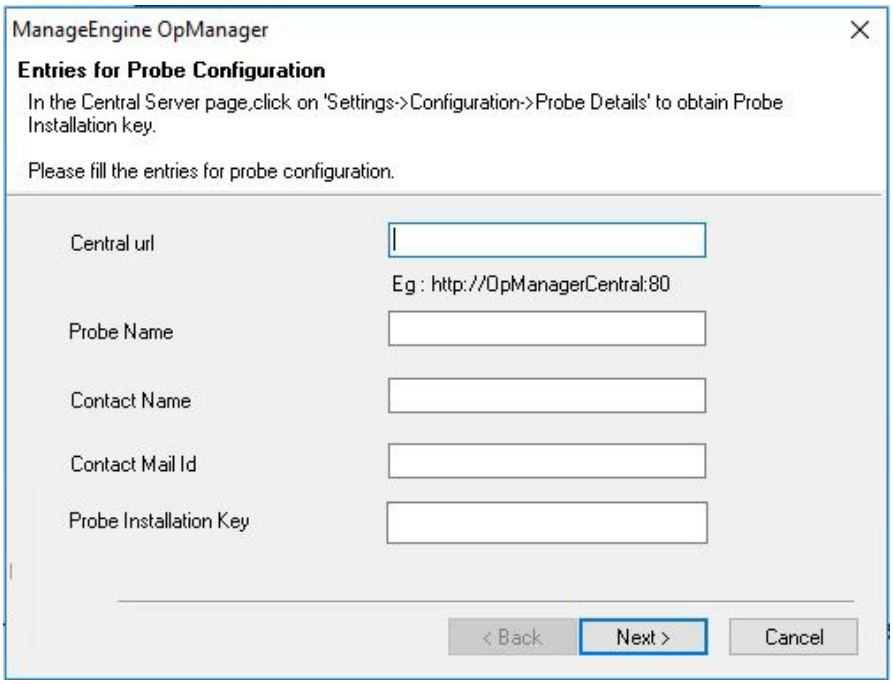


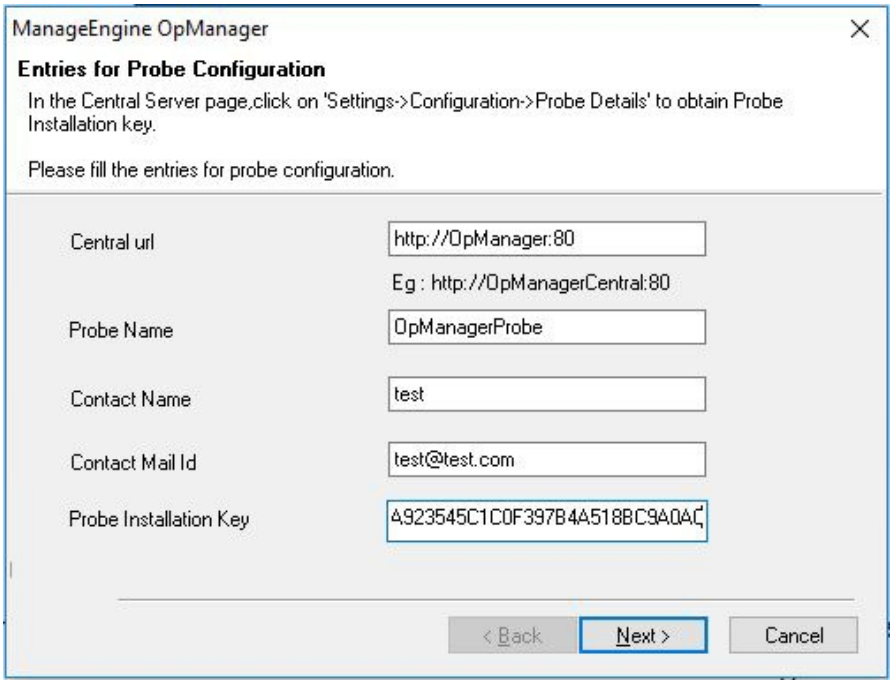
Step 10: Search for bcp.exe file and select it. Click 'Register' to proceed.

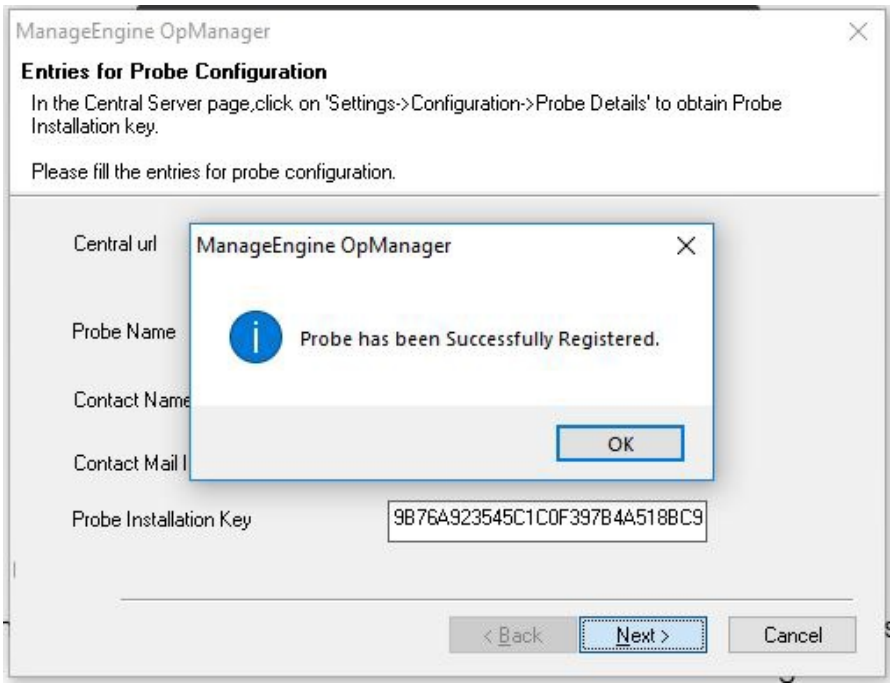


Step 11: Provide OpManager Central server details like central server URL, Probe Name, Contact Name and Contact Mail ID. Enter the Probe installation key. You can find the Probe Installation key in the Central Server page under **Settings->Configuration->Probe Details**.




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 12: 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...
```

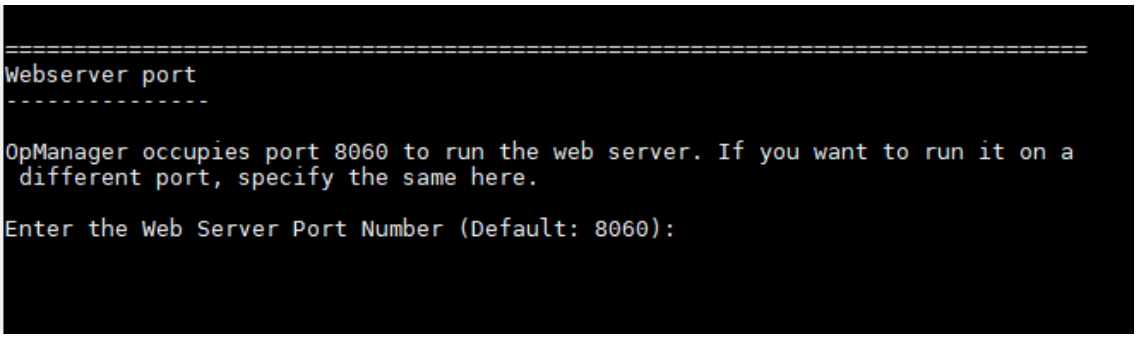
Step 2: Go through the license agreement and enter 'Y' to proceed. You can register for technical support by providing the required details. (Name, E-mail ID, Phone, Company Name)

Step 3: Select the location.

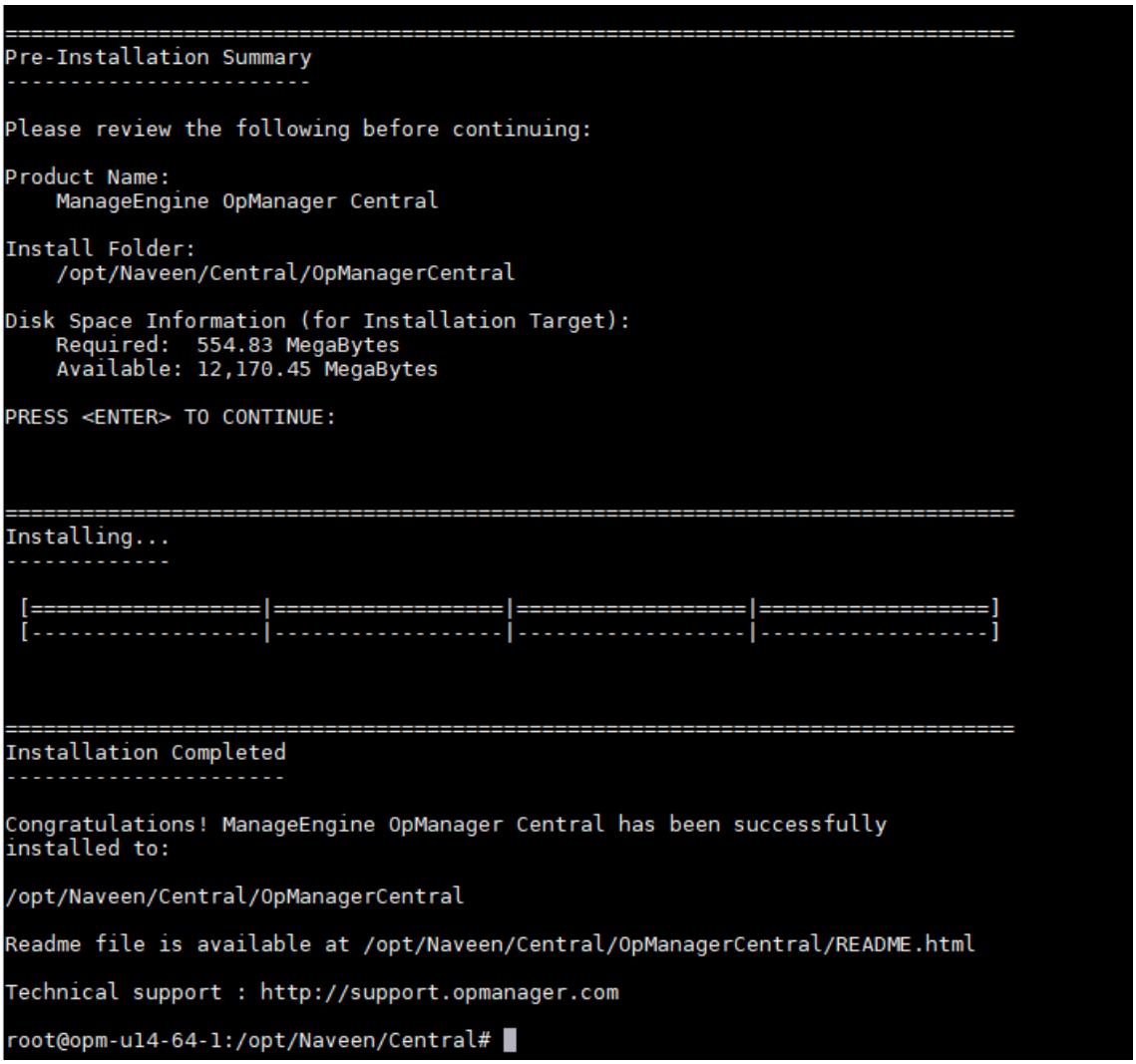
Step 4: Choose the installation directory

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



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



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



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

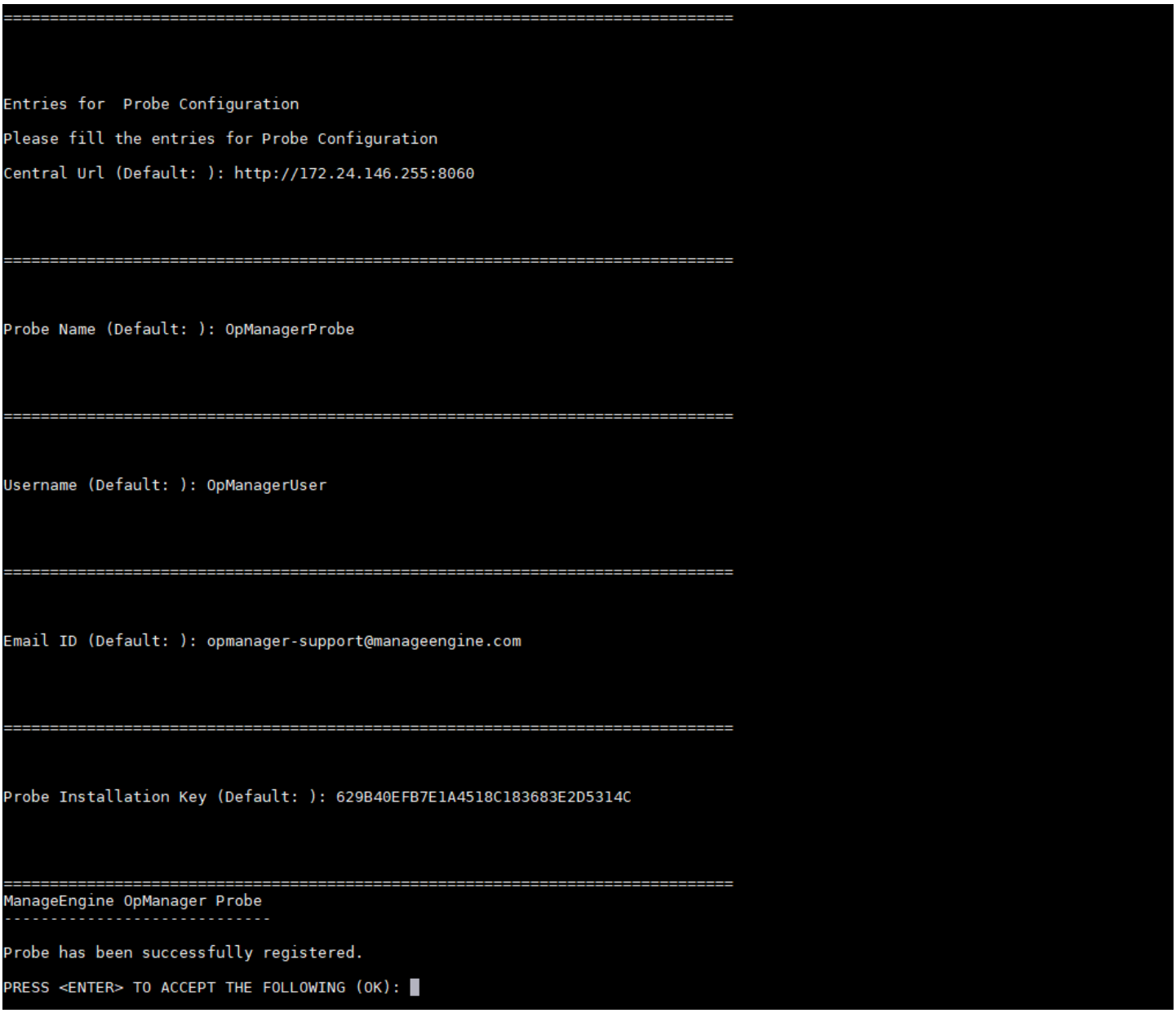


```
===============================================================================
Webserver port
--------------


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.

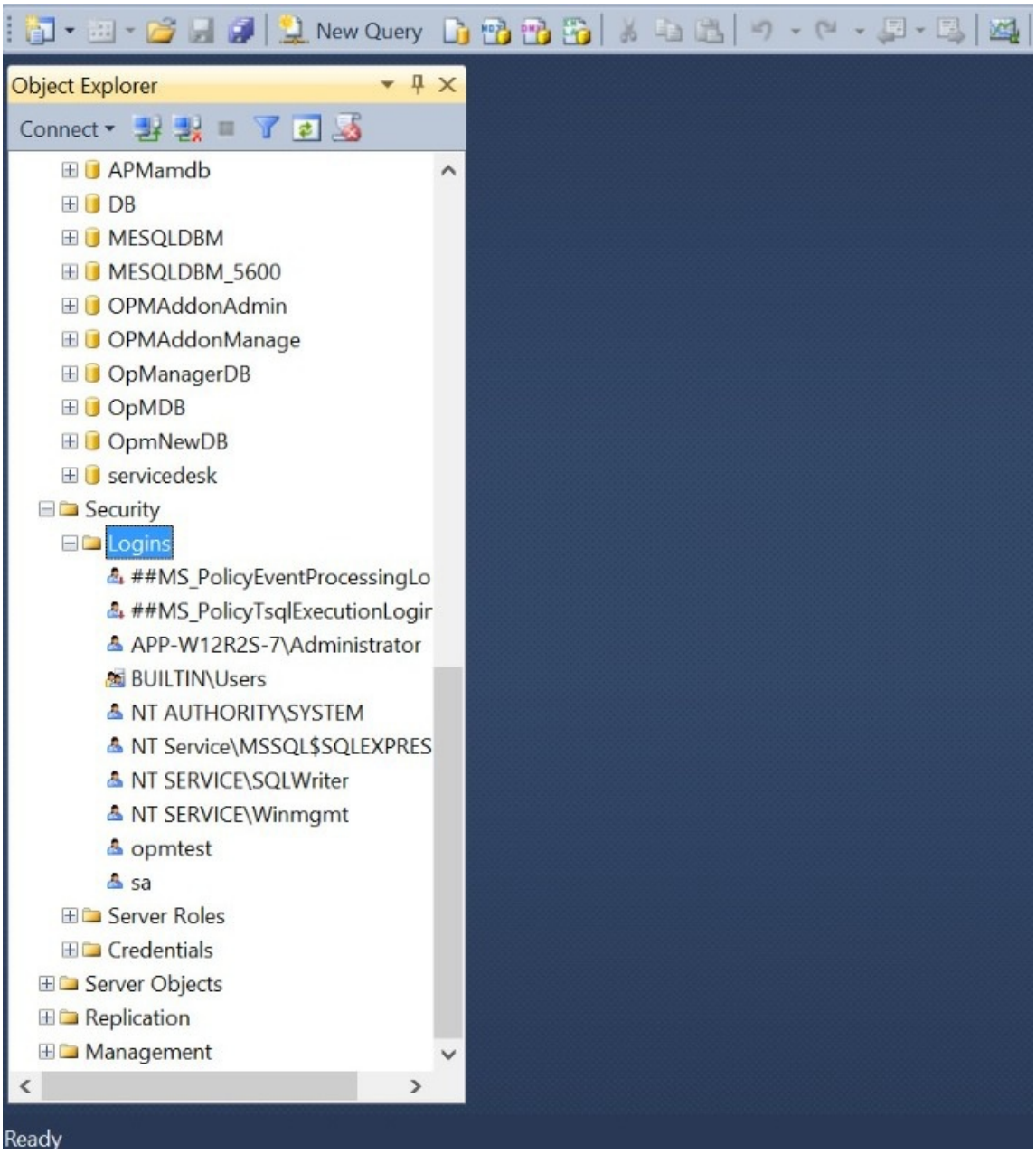
Supported Versions: SQL 2017 | SQL 2016 | SQL 2014 | SQL 2012 | SQL 2008

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

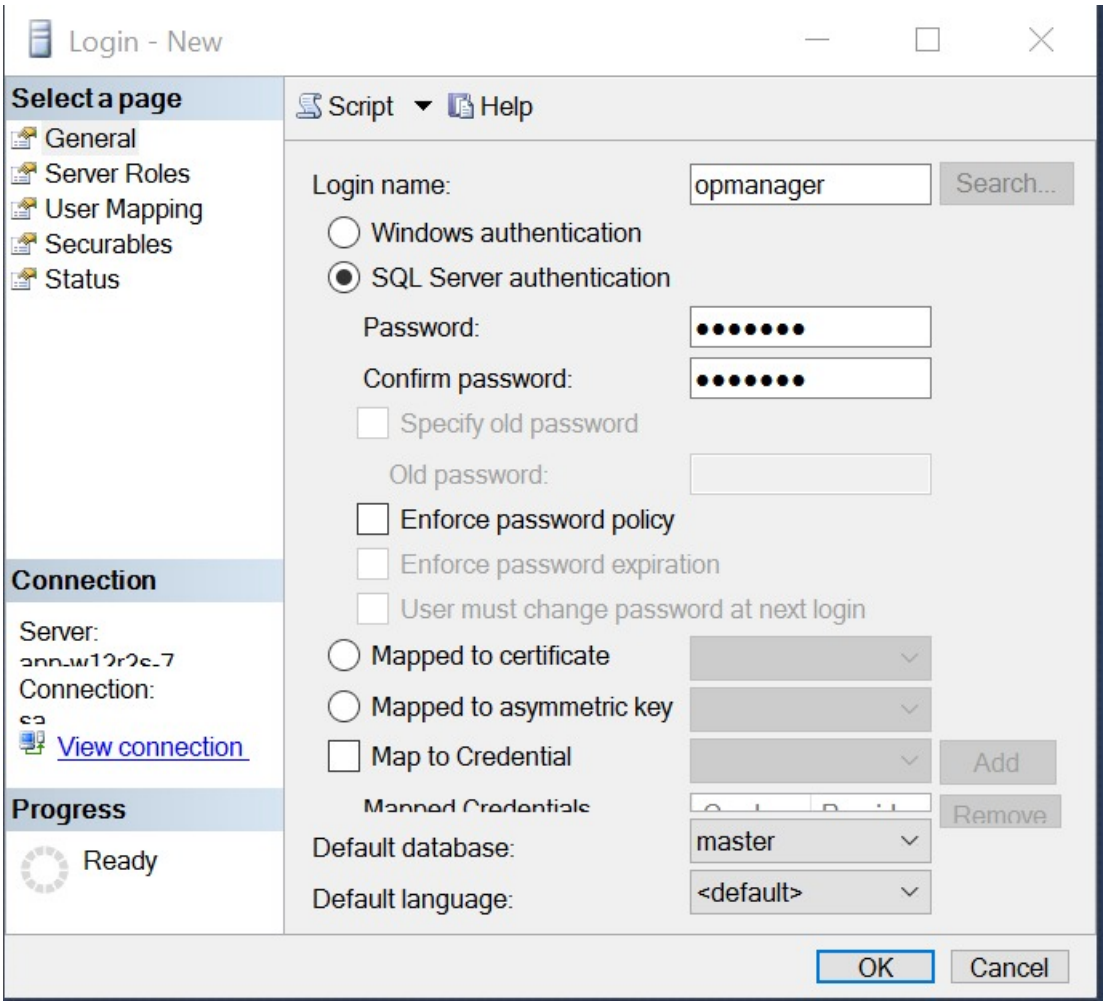
Steps to configure MSSQL

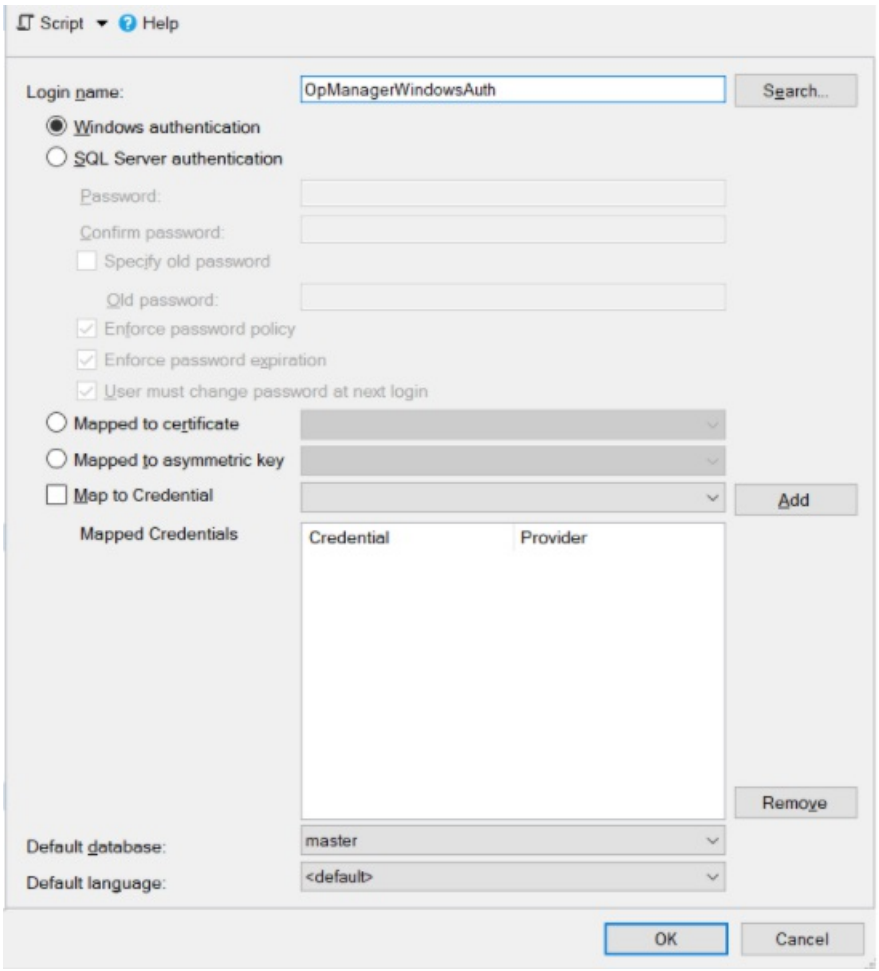
Step 1: To ensure proper communication between the MSSQL database server and OpManager, a new account has to be created with the below mentioned steps.

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

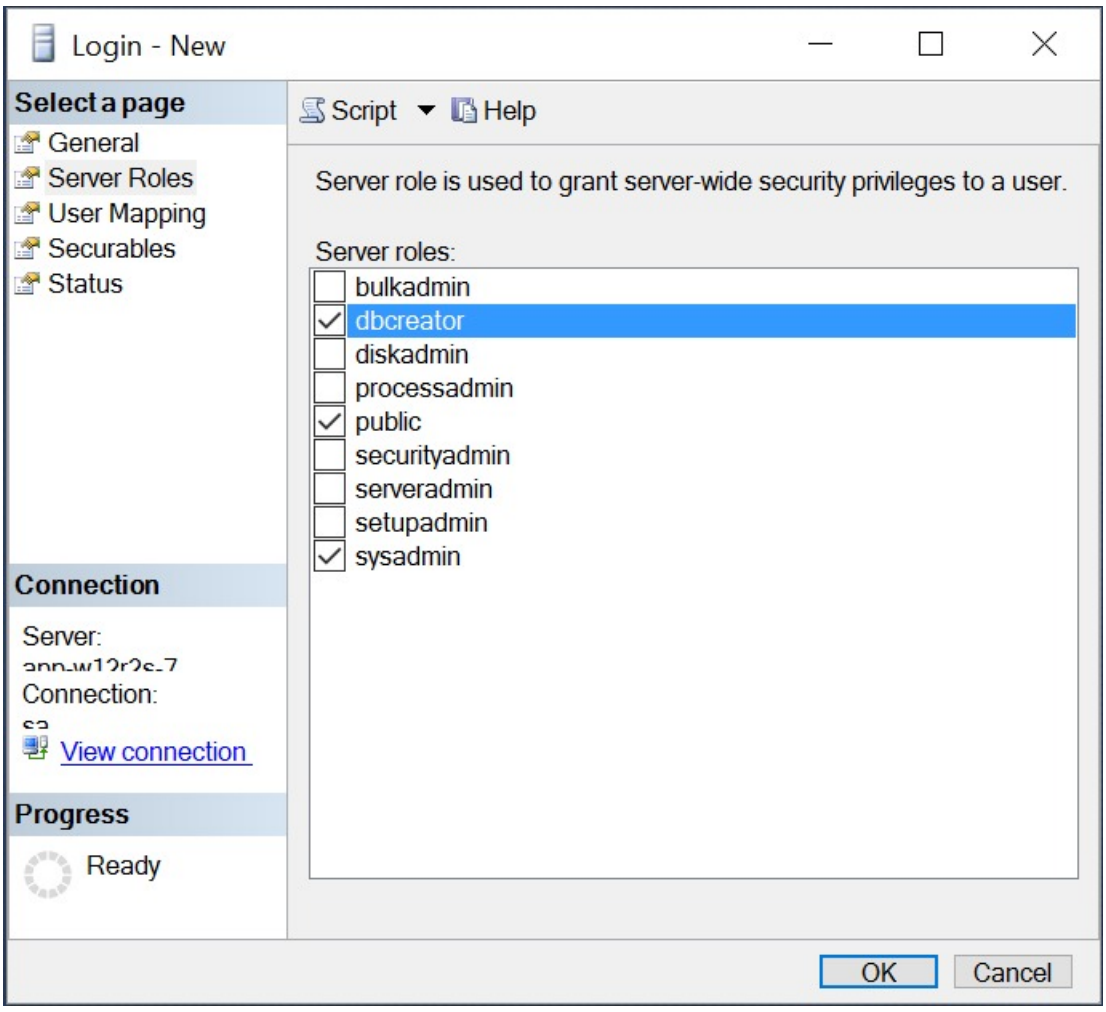


Step 2: Select Authentication type. For Windows authentication, select and login using your Windows login credentials. For SQL Server Authentication, enter the password. Then proceed with Step 3.

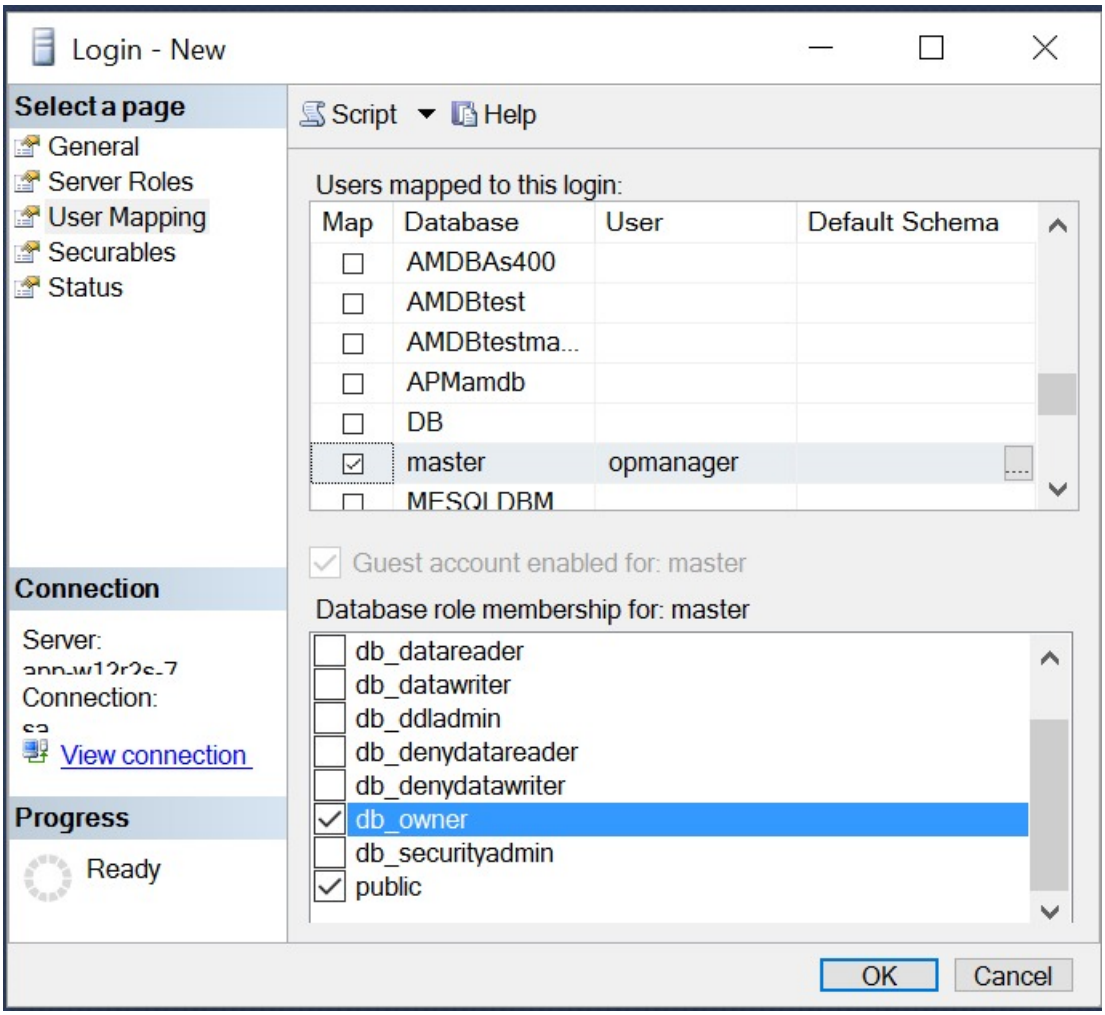




Step 3: Click on Server Role. Select Server Roles "dbcreator", "public" and "sysadmin"



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 including interface monitors.

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. In the same command prompt execute**&#65533;** ***OpManagerService.bat -i&#65533;*** to add OpManagerCentral as a service.
5. If you want to use the same database, continue without any changes. Please ensure that the database server is reachable in the new machine.
6. 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.
7. Restart all the probes.
8. 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. In the same command prompt execute ***OpManagerService.bat -i&#65533;*** to add OpManagerProbe as a service.
5. 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.
7. Start OpManagerProbe from Windows services in the new machine.
8. 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.
6. 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.
8. 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.
6. 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.
8. 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.
10. To clean up the existing machine, uninstall OpManagerCentral.

Steps to migrate Probe:

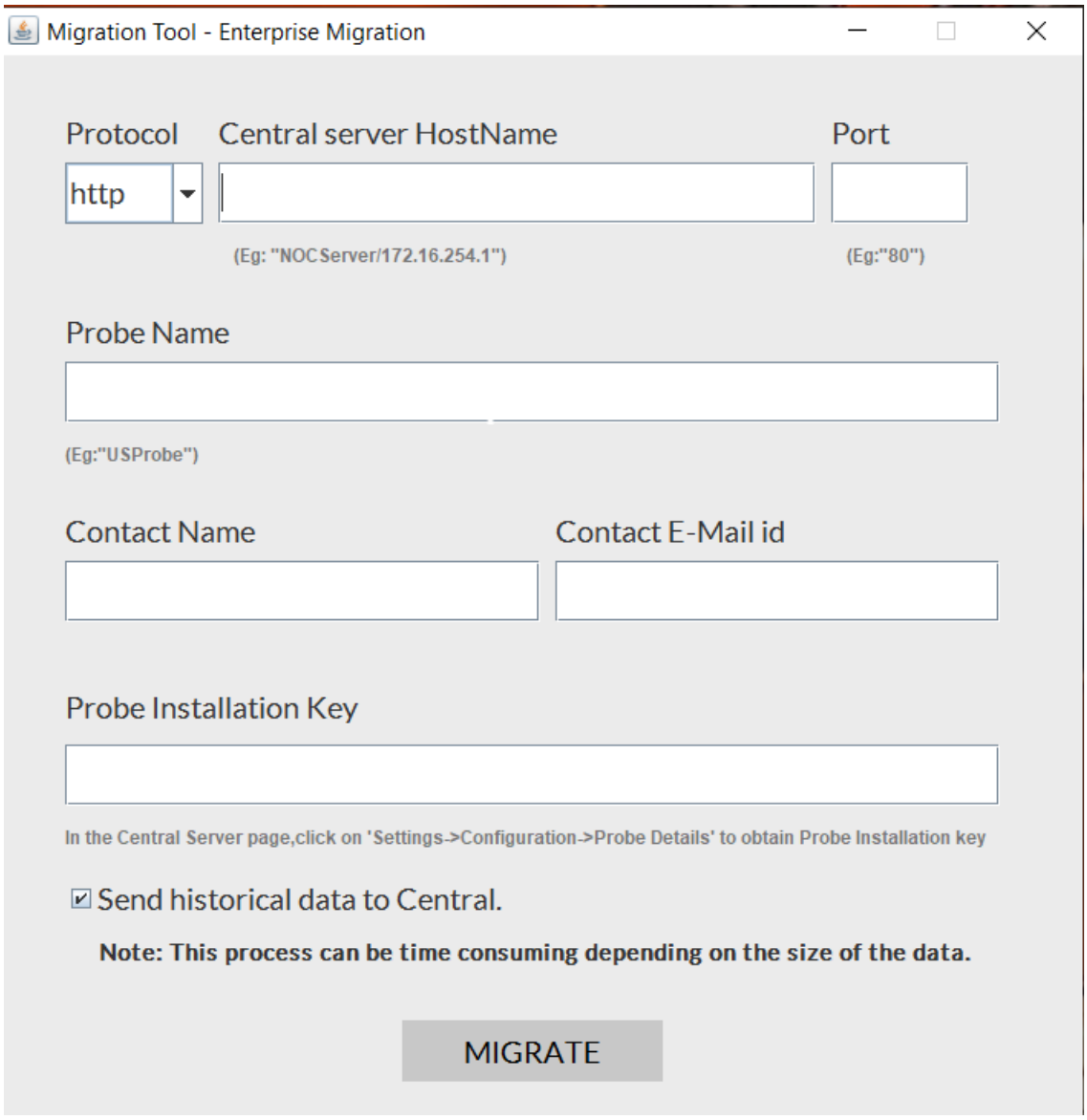
1. Stop the OpManagerProbe service and take a backup using the steps given in this page.
2. Do a new, clean installation of the probe in the required server.
3. After the probe is installed successfully, start the service and check if the probe is communicating properly with the central.
4. Stop the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

). 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.**

(Click on the check box if the historical data in existing OpManager Professional/Essential edition has to be sent to the Central.)

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.

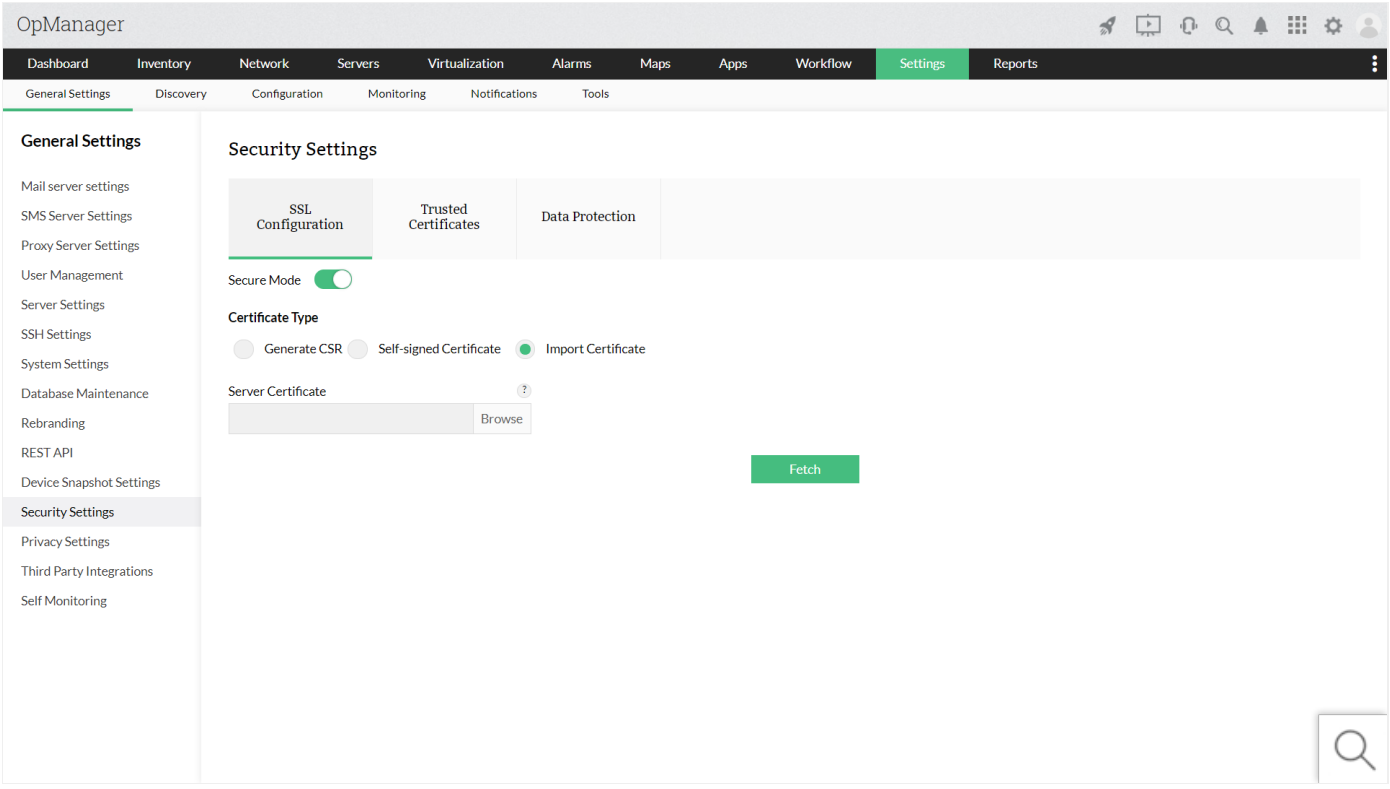
*** Points to note:**

- 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 **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** attribute in OpManagerProbe/conf/CommunicationInfo.xml 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

In Central : (till version 124041)

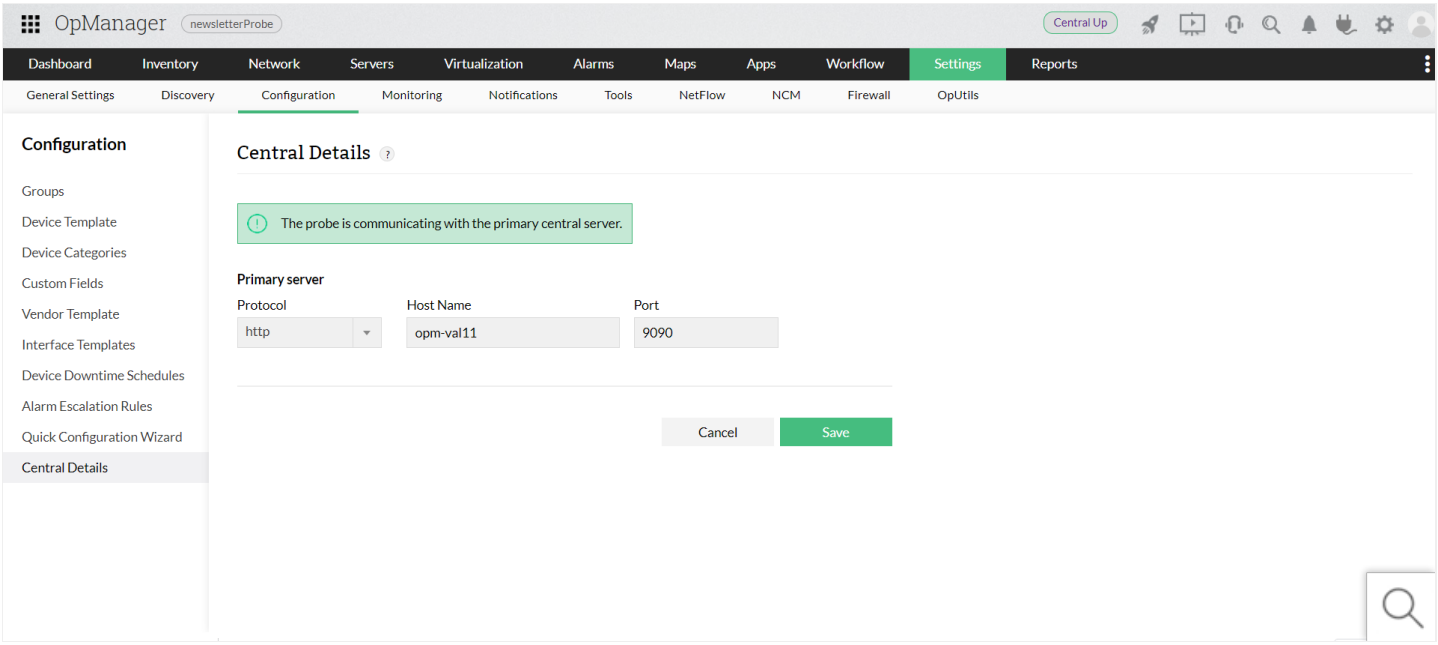
- Open Command prompt with administrator privileges and go to the ***OpManagerCentral/bin*** directory and execute ***ChangeWebServerPort.bat*** (eg : Change*WebServerPort.bat 443*).
- Restart OpManagerCental.
- For all probes go to **"OpManagerProbe/conf/OpManager"** directory and locate **"NOCServerDetail.xml"**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

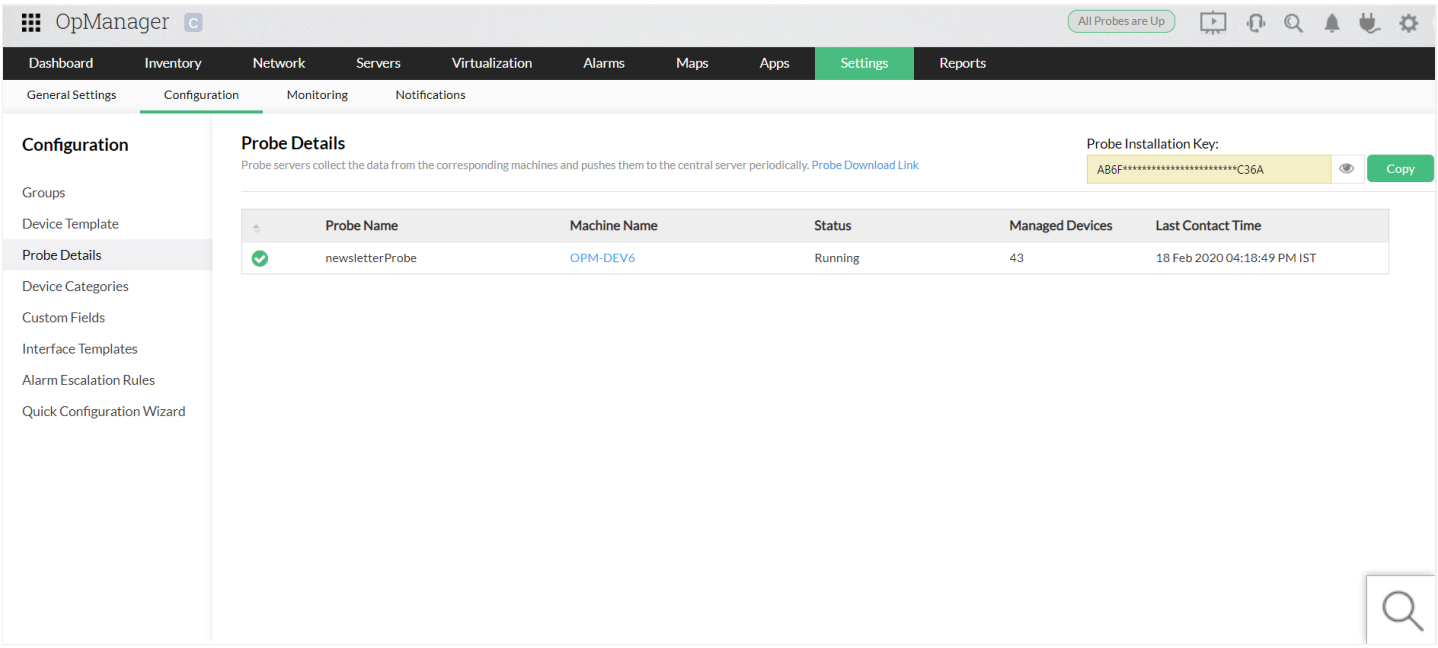
In Central : (from version 124042 and above)

- 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 **Settings --> Configuration --> Central Details** and specify the updated port number of the Central system.



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.
- Update it in **NAT Port.**



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.

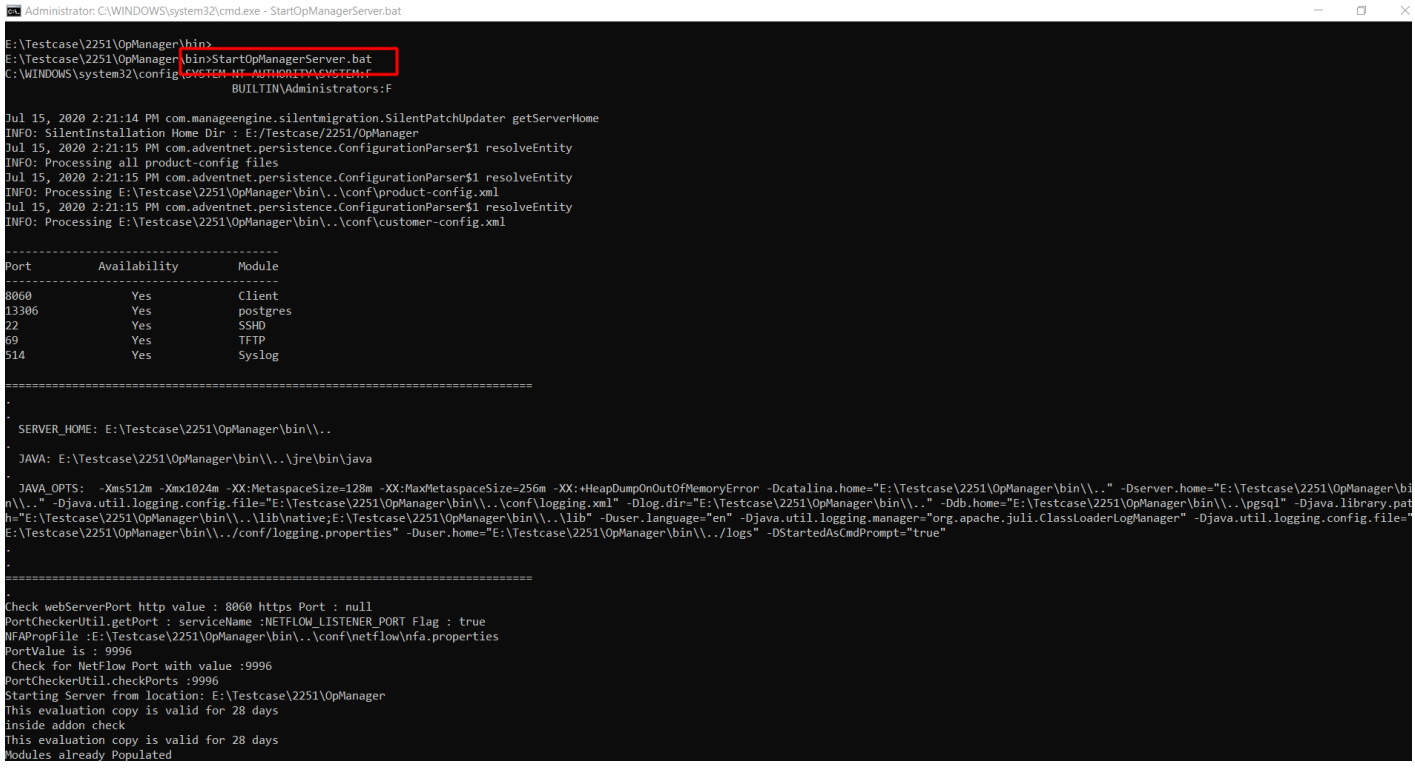
To later start OpManager as a Windows Service, follow the steps below:

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.

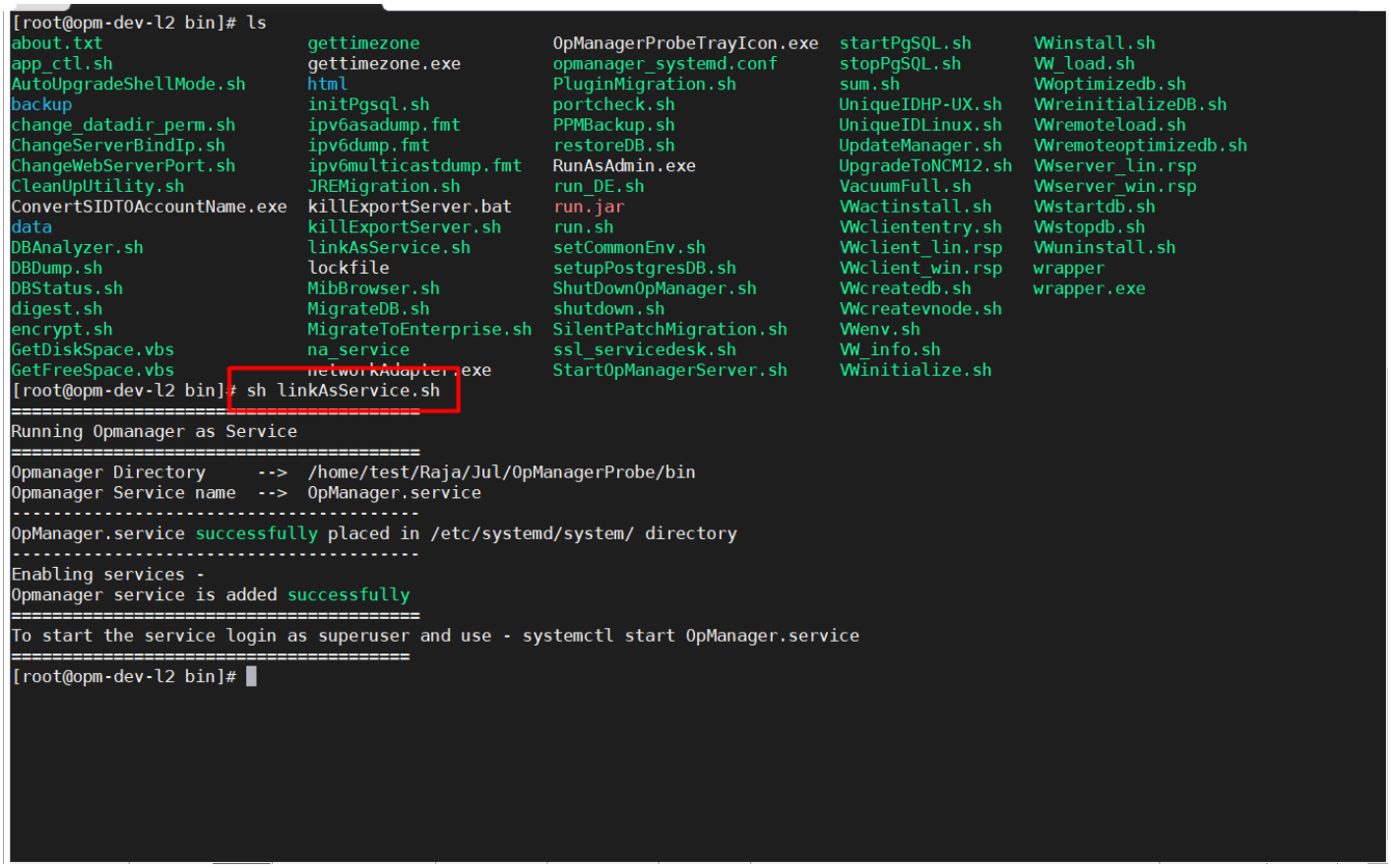
On Linux Machines

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.

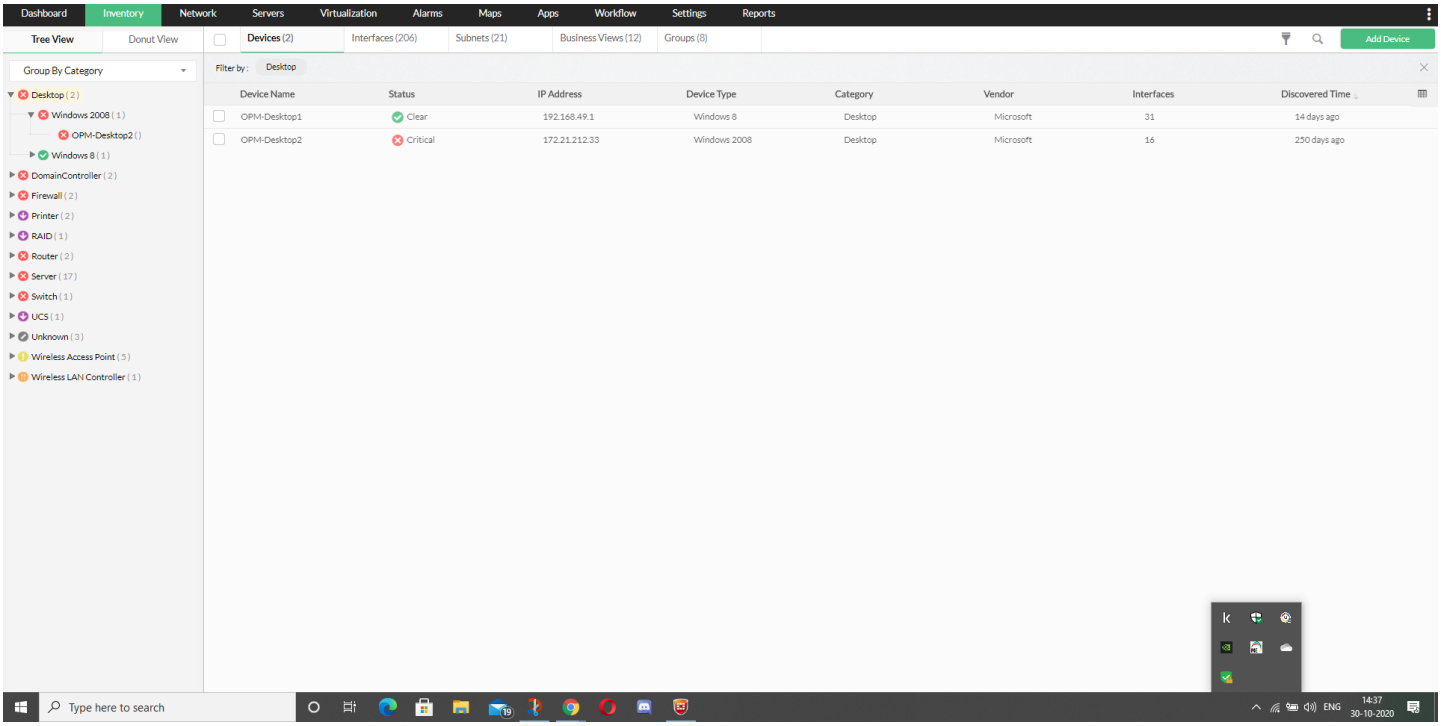
   [Note: If you have enabled SSL, connect as **https**://<**host_name**>:<**port_number**> in the address bar and press Enter.]
3. Type the **User Name** and **Password** and click **Login**. The default user name and password are 'admin' and 'admin' respectively.
4. If the client is not accessible, check if the port is not blocked by Windows Firewall.

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)

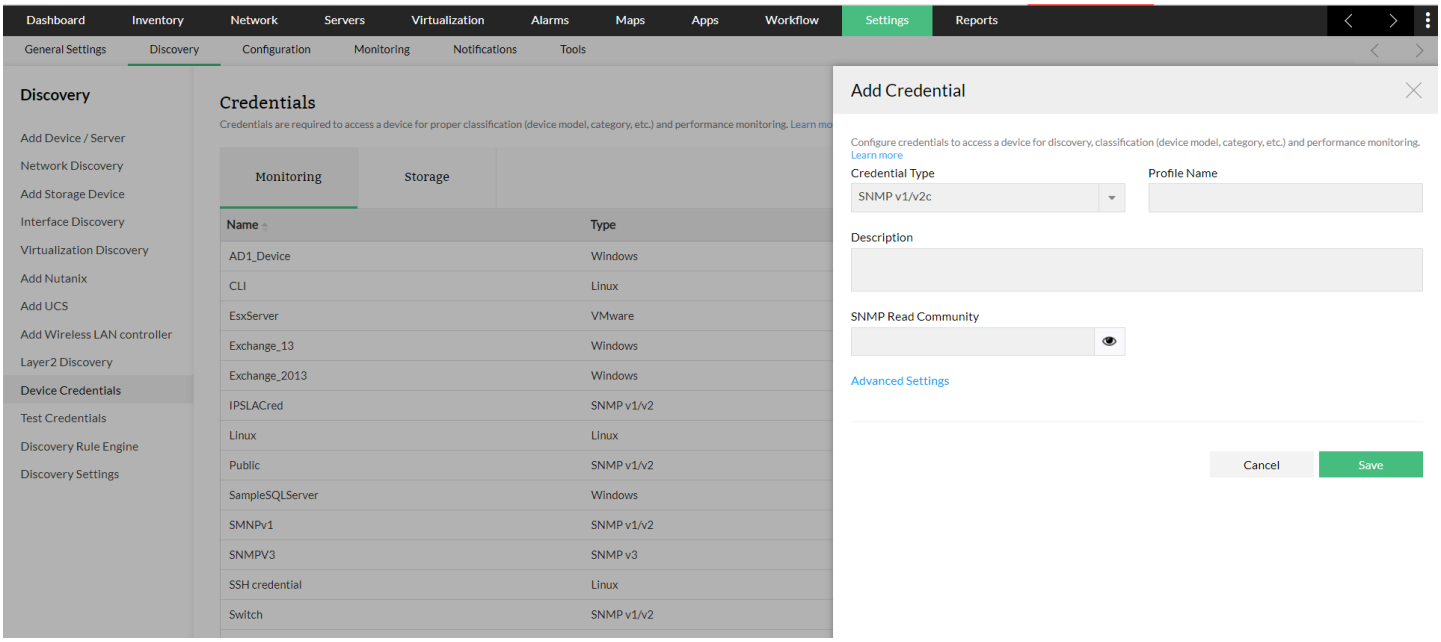
- OpManager accesses the remote devices using the protocols SNMP, CLI, or WMI. The credentials like the password/snmp community, port etc., may differ for different device types. Pre-configuring a set of credentials in OpManager helps applying them to multiple devices at a time, saving a lot of manual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

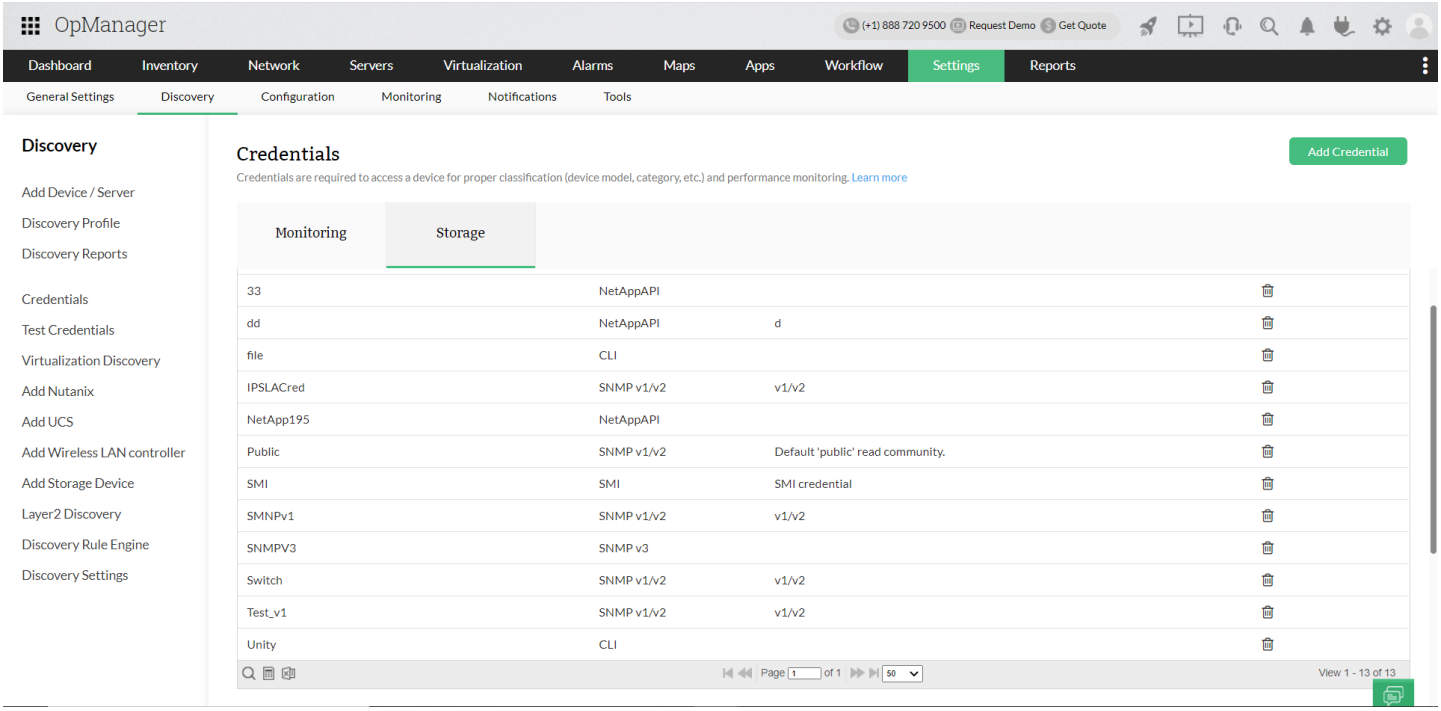
Nutanix: Provide the username and password of the Prism API element, the protocol being used (HTTP/HTTPS), the timeout value for the connection and the port in which the Prism element is running.

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.

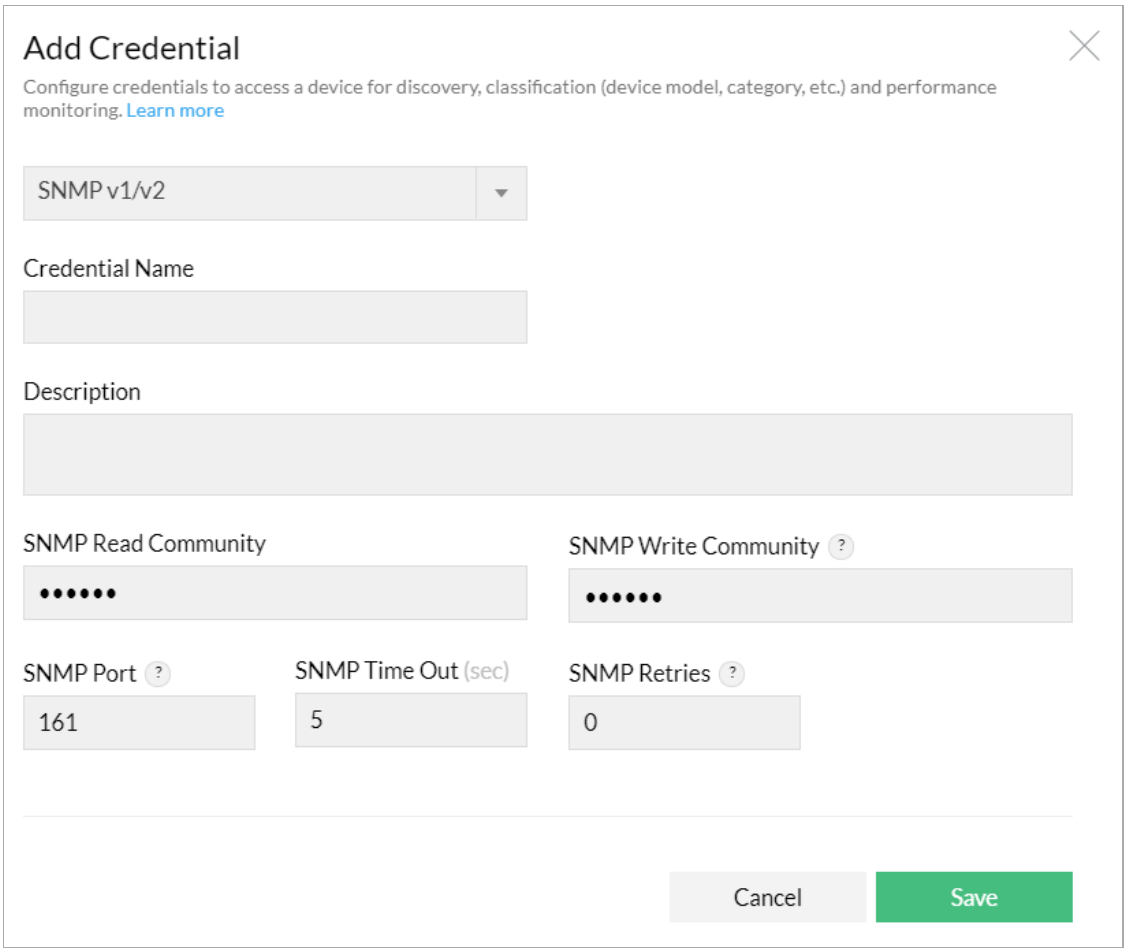
Nutanix:

- 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:


Add Credential
Configure credentials to access a device for discovery, classification (device model, category, etc.) and performance monitoring. Learn more
SNMP v1/v2
Credential Name
Description
SNMP Read Community
SNMP Write Community
SNMP Port
SNMP Time Out (sec)
SNMP Retries
161
5
0
Cancel
Save

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.

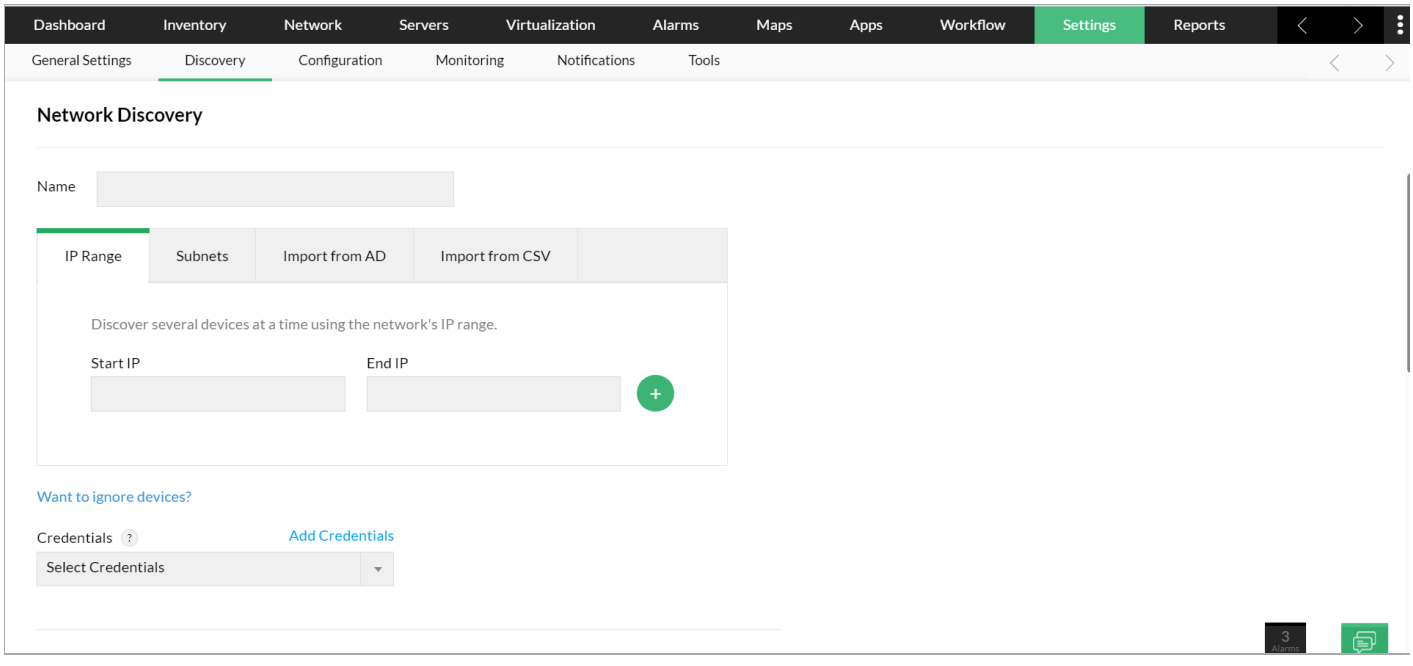
Discover devices in an IP range

To discover a selected range of devices,

For OpManager versions below 125174

For OpManager versions 125174 and above:

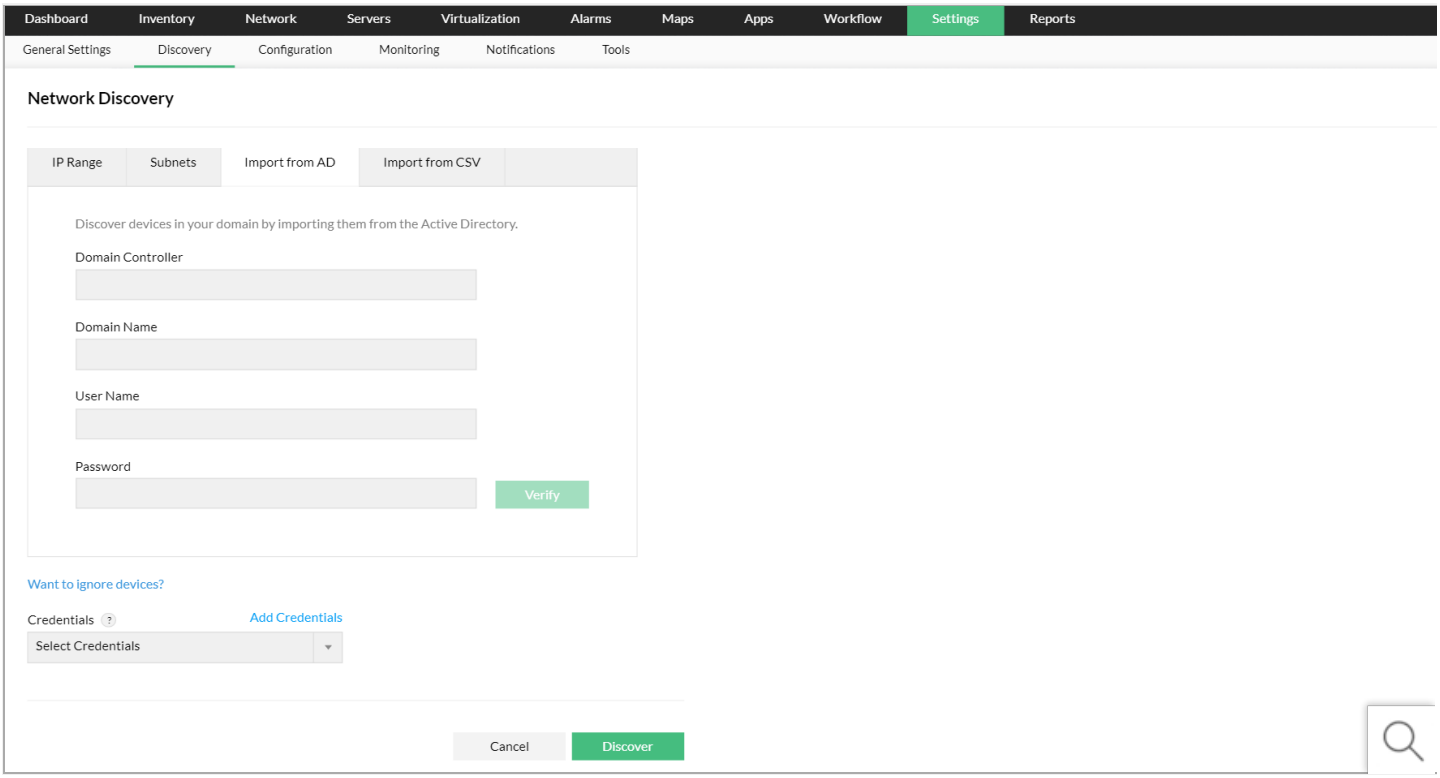
1. Go to **Settings** -> **Network Discovery** -> **New Discovery**.
2. Select the **IP Range** option.
3. Enter the start and end IP of the required range.
   Start IP: Specify the IP address of the device in the range from where OpManager should start the discovery process. End IP: Specify the IP address 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.



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.

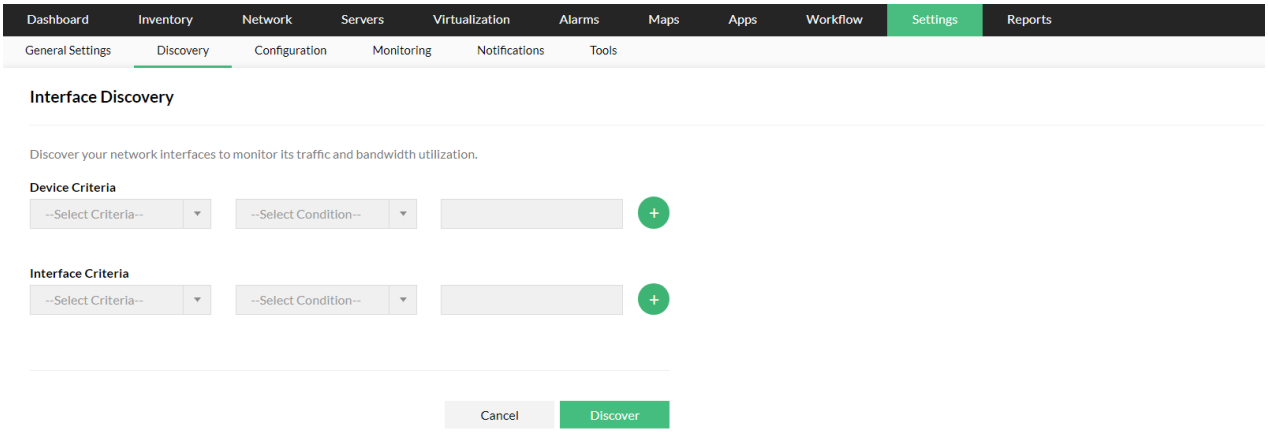
From the Device Snapshot page

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.

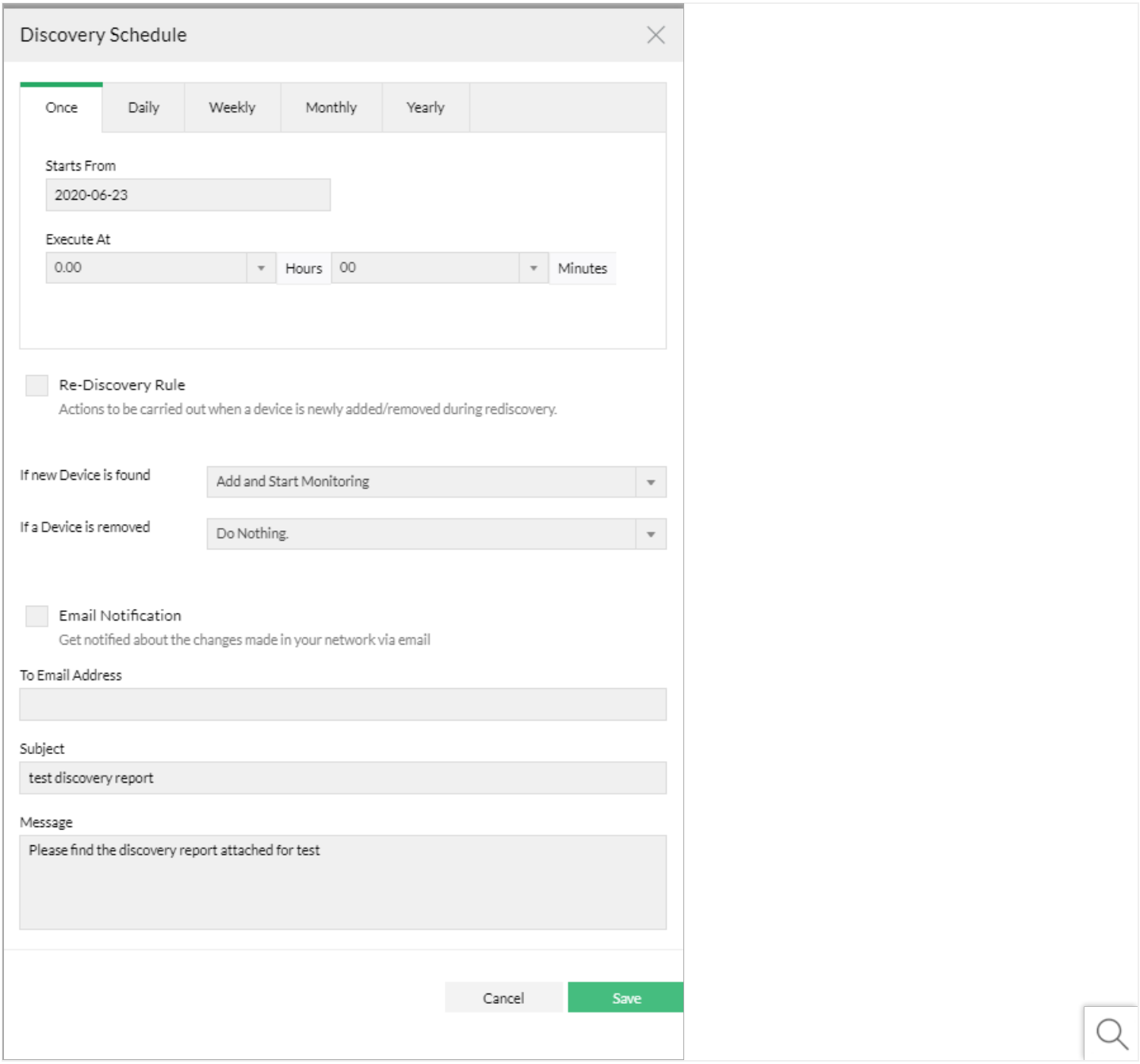


Schedule Discovery

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.

More about Scheduled Discovery


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

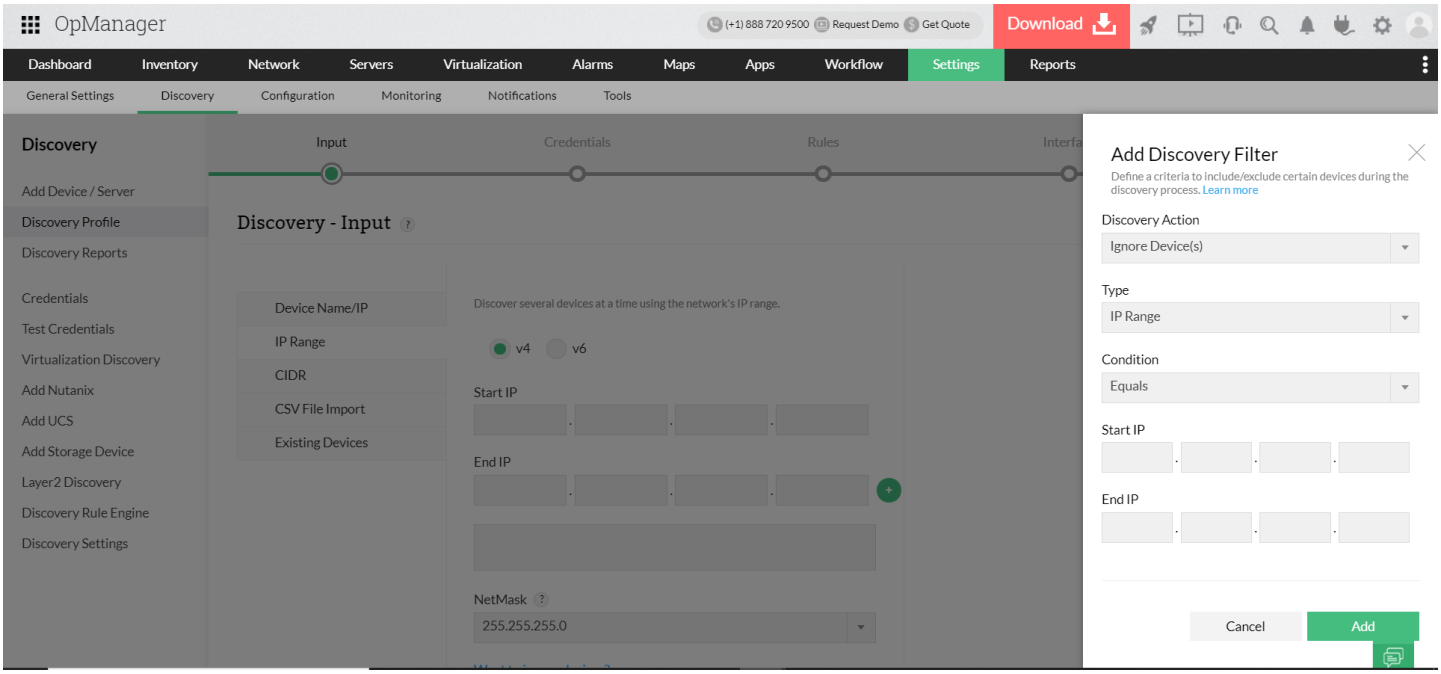
You can choose to add or ignore an individual device or a set of devices before configuring device discovery schedule in OpManager.

For OpManager versions below 125174

- Go to **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.

For OpManager versions 125174 and above

- Go to **Settings -> Discovery -> Network Discovery.**
- Choose the discovery type and click on the **Want to Ignore devices** option.
- Choose either **Ignore/Add Device(s)**, specify a criteria and entwr the value or IP address as per the selected 'Type'.
- Finally click on **Add** and proceed with the discovery process. 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.

Unable to add device. The given IP address already exists as a subnet.

Cause

The IP address of the device to be discovered may be available in OpManager as a subnet address.

Solution

In OpManager, an specific address cannot be used both IP address and Subnet. The required device can only be added if the device IP doesn't exist as a Subnet in OpManager or if the 'DNS Name' of the device is resolved.

Other messages

Device addition might take a longer time than usual. Please check the Inventory after some time.

Cause:

- The device would have responded slowly to the OpManager server's request.
- Due to the large number of interfaces in the device, the time taken for device addition may be longer than usual.

Solution:

Check whether the device is reachable from the OpManager server continuously and without any hindrance. Also ensure that there is no delay in the protocol response chosen for the corresponding credential that is associated with the device(SNMP, WMI, etc). In some cases, the device would have been added in OpManager, but not notified. Please check the Inventory after a few minutes of discovery to make sure the device is added.

Device Discovery has been initiated

The message **'Device Discovery has been initiated'** will be displayed when two or more devices are discovered at the same time (separated by comma) via 'Add Device'. In such cases, the mentioned devices will be added into OpManager without an additional message confirming the completion of the discovery process. These devices will be listed under Inventory once the discovery progress notification shows the completion status.

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.

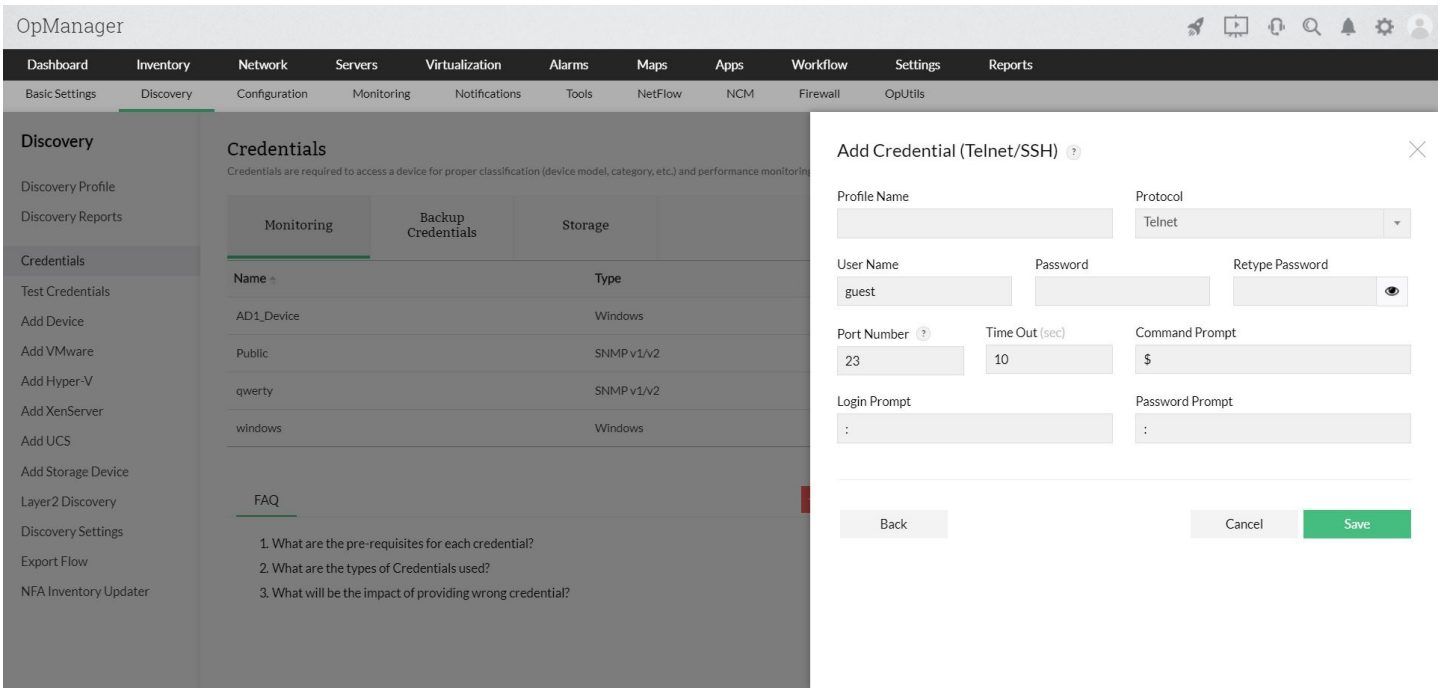
```
[test@My_device_1.ssh]$ ssh -i id_rsa root@172.21.151.96
Last login: Tue Jul 31 03:58:30 2018 from My_device_1.mynetwork.com
[root@OPM-C6-32-AIO ~]#
```

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

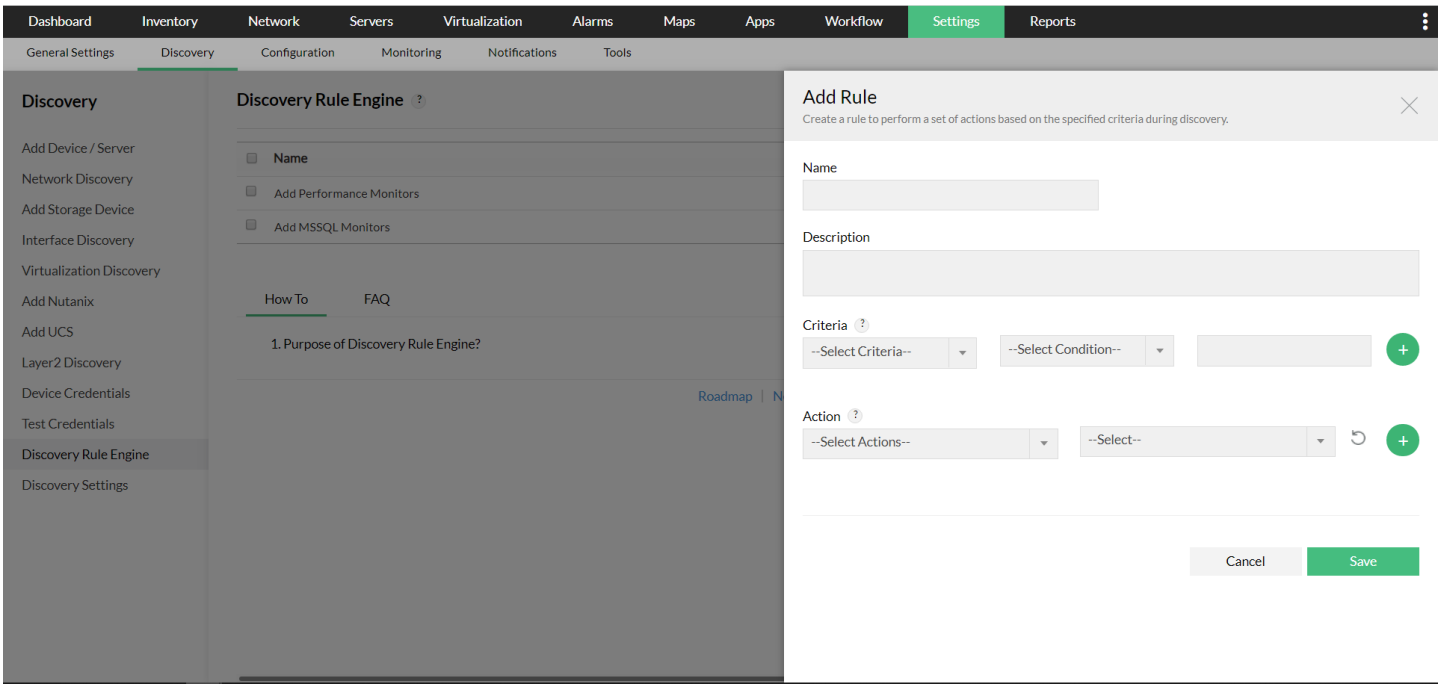
1. Go to **Settings** -> **Discovery** -> **Discovery Rule Engine** and click on **Add rule** on the top right.
2. Enter a **Name** and **Description** for the Discovery Rule Engine.
3. **Criteria** refers to the parameter of the device which must be checked for applying the rule (Such as DNS Name / 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

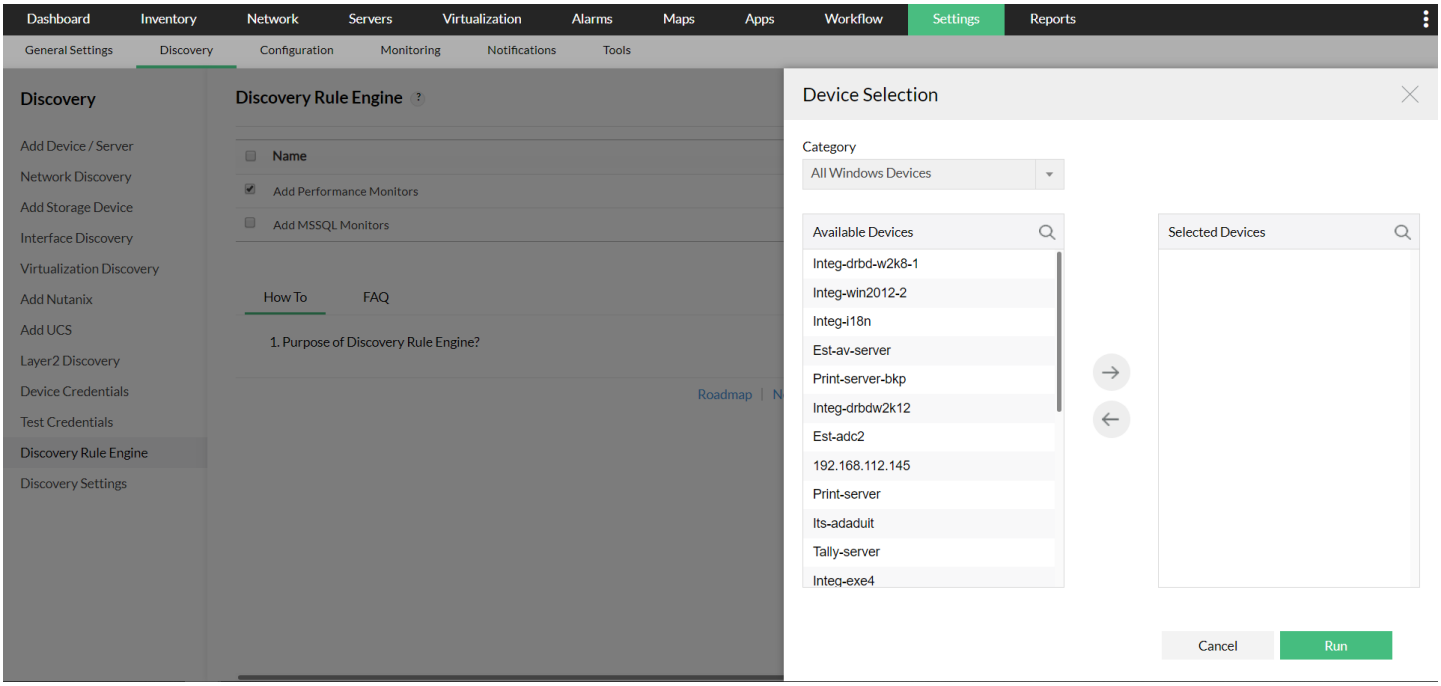
7. Click on **Save**.



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.

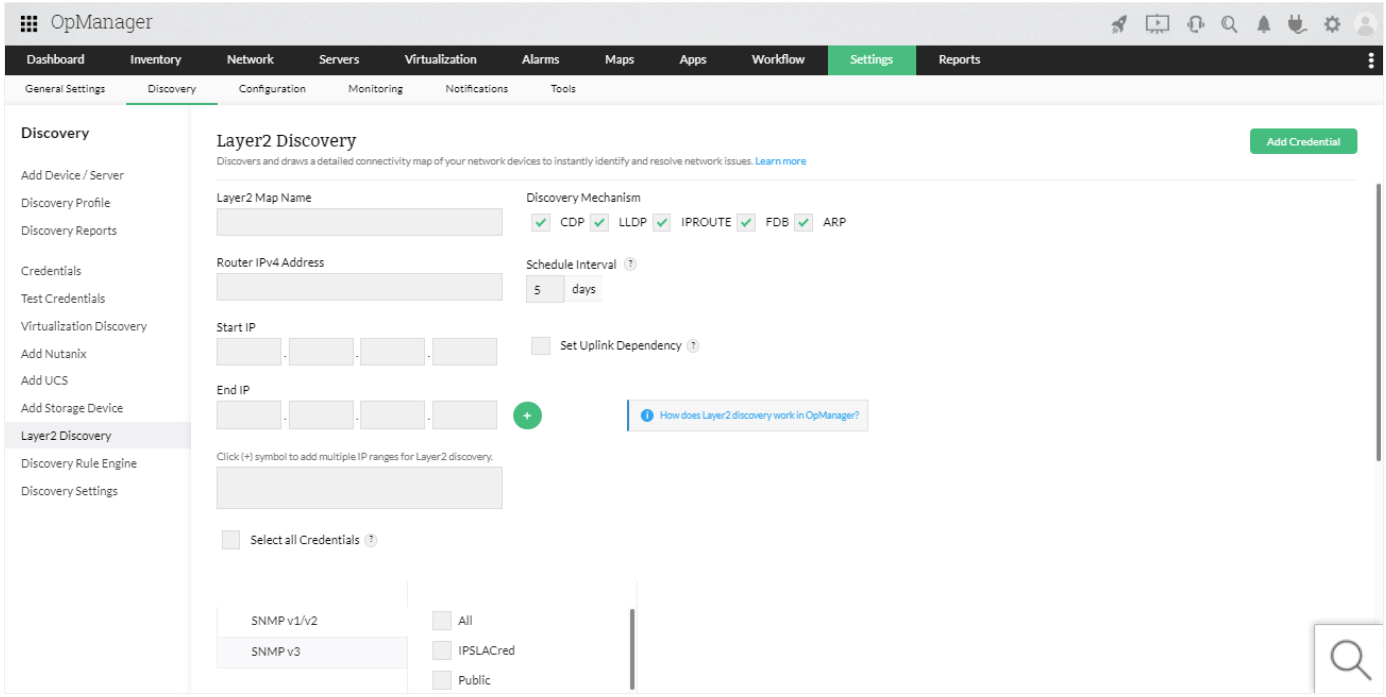
Discovery Mechanism:
OpManager supports multiple discovery protocols. Choose one (or more) that is implemented in your seed router/L3 switch. This will drastically reduce the time taken to discover the devices.

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.

Bulk actions performed from the Inventory page

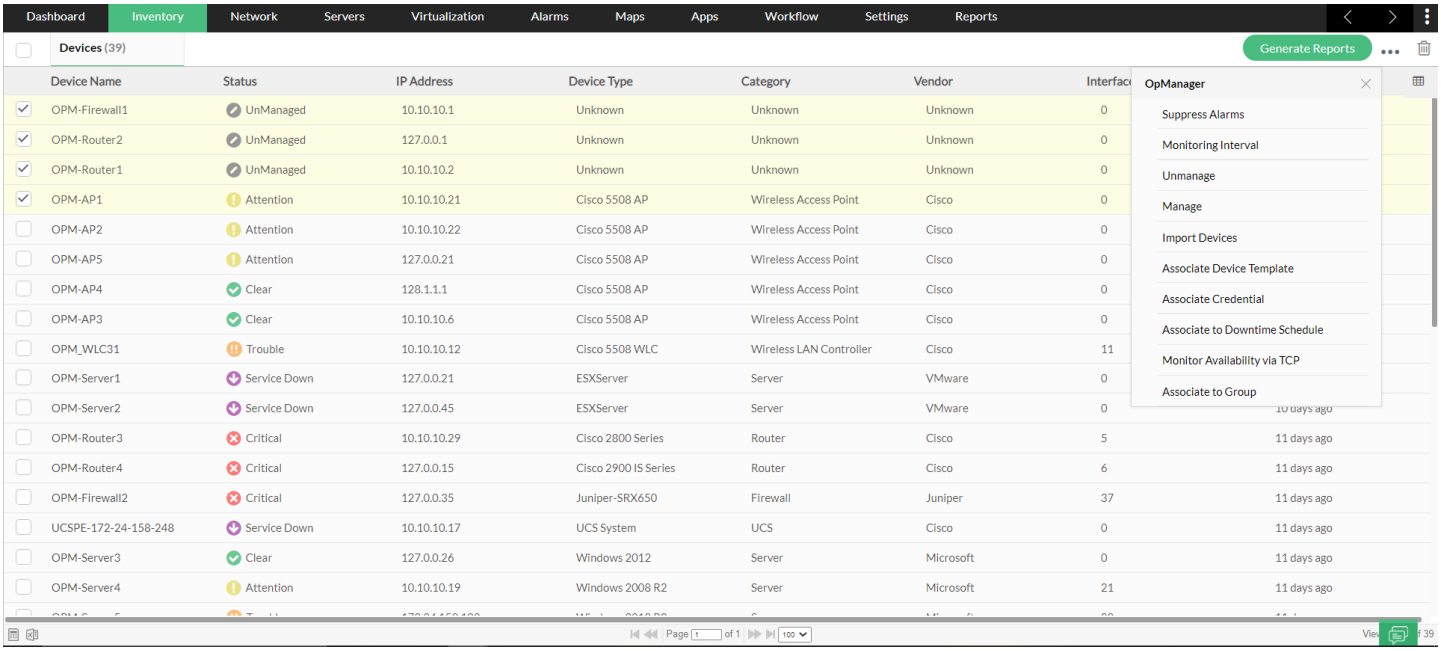
There are various actions that can be accessed from the Inventory page. These functions can be applied to the devices in bulk. Listed below are the various options available in the device inventory page.

Suppress Alarms: You can use this option to suppress the alarms associated with the selected devices. All associated alarms (except Device Availability alarms) will be suppressed for a the specified time period.

Monitoring Interval: Allows you to enable or disable status polling (availability monitoring). You can also configure the monitoring interval from here.

Unmanage/Manage: The selected devices can be manually unmanaged and managed in bulk. For planned maintenance in your network, you can schedule a downtime scheduler

Import Devices: Allows you to change the category of the device (PDU, Server, Wireless, etc) in bulk.



Device Name	Status	IP Address	Device Type	Category	Vendor	Interfac	
OPM-Firewall1	UnManaged	10.10.10.1	Unknown	Unknown	Unknown	0	
OPM-Router2	UnManaged	127.0.0.1	Unknown	Unknown	Unknown	0	
OPM-Router1	UnManaged	10.10.10.2	Unknown	Unknown	Unknown	0	
OPM-AP1	Attention	10.10.10.21	Cisco 5508 AP	Wireless Access Point	Cisco	0	
OPM-AP2	Attention	10.10.10.22	Cisco 5508 AP	Wireless Access Point	Cisco	0	
OPM-AP5	Attention	127.0.0.21	Cisco 5508 AP	Wireless Access Point	Cisco	0	
OPM-AP4	Clear	128.1.1.1	Cisco 5508 AP	Wireless Access Point	Cisco	0	
OPM-AP3	Clear	10.10.10.6	Cisco 5508 AP	Wireless Access Point	Cisco	0	
OPM_WLC31	Trouble	10.10.10.12	Cisco 5508 WLC	Wireless LAN Controller	Cisco	11	
OPM-Server1	Service Down	127.0.0.21	ESXServer	Server	VMware	0	
OPM-Server2	Service Down	127.0.0.45	ESXServer	Server	VMware	0	10 days ago
OPM-Router3	Critical	10.10.10.29	Cisco 2800 Series	Router	Cisco	5	11 days ago
OPM-Router4	Critical	127.0.0.15	Cisco 2900 IS Series	Router	Cisco	6	11 days ago
OPM-Firewall2	Critical	127.0.0.35	Juniper-SRX650	Firewall	Juniper	37	11 days ago
UCSPE-172-24-158-248	Service Down	10.10.10.17	UCS System	UCS	Cisco	0	11 days ago
OPM-Server3	Clear	127.0.0.26	Windows 2012	Server	Microsoft	0	11 days ago
OPM-Server4	Attention	10.10.10.19	Windows 2008 R2	Server	Microsoft	21	11 days ago

Associate Device Template: This is similar to the Associate Template option available in the Edit Device Templates page. You can choose the required devices from OpManager Inventory and associate the 10000+ device templates available in OpManager.

Associate Credentials: You can associate existing credentials for the selected devices and rediscover to enable the proper monitoring of those devices. You can create Test credential profile under Settings -> Discovery menu to generate alarms on credential failure.

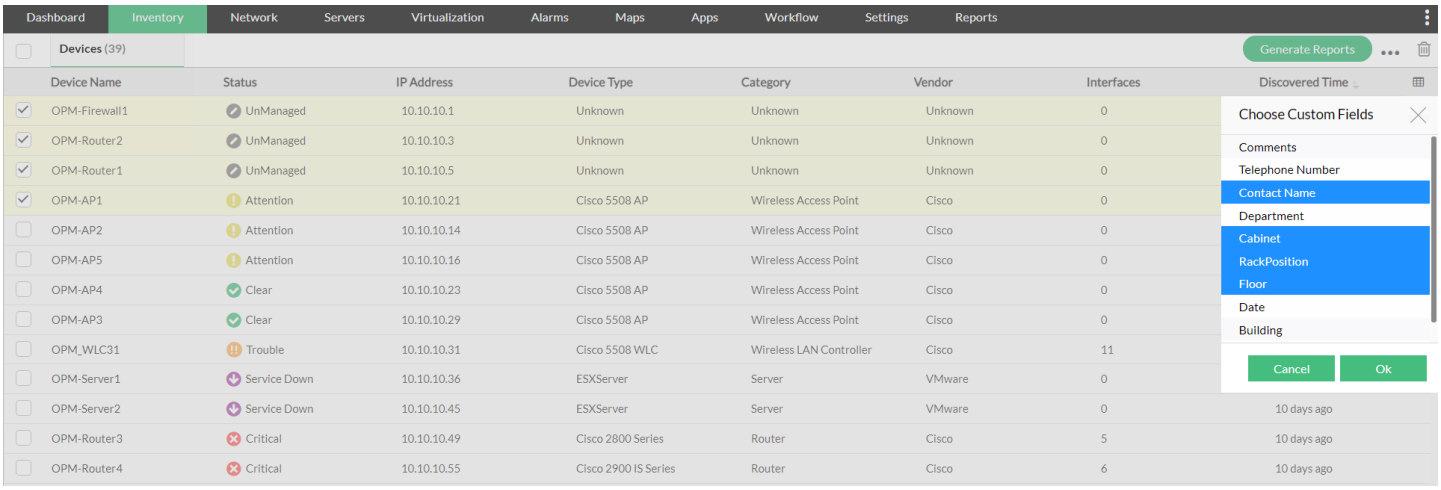
Associate to Downtime Schedule: You can associate the selected devices to an existing or new downtime scheduler. The devices associated to a downtime scheduler will be in unmanaged state (not monitored) for the defined time interval.

Monitor Availability via TCP: You can enable TCP based availability monitoring for the selected devices. TCP based availability monitoring is most suitable for ping disabled environments or networks that solely prefer TCP port based monitoring due to security concerns. OpManager should be able to communicate with the given port to perform availability monitoring.

Associate to Group: The selected devices can be associated with an existing or new group. Only the device based groups will be listed here. If a device group is created with device properties criteria, the devices that match the criteria upon discovery or further update will be automatically associated to the respective group.

Generate Reports: You can generate customized availability reports for of the discovered devices and interfaces in bulk. Learn more.

Custom Fields via Column Chooser: You can associate the available custom fields with all available devices directly from the Inventory page. To add custom fields, select the devices, click on the 'table' icon on the right corner and select the required custom fields. Once done, click on OK to save the changes. You can also export this view as CSV or Excel file by clicking on the export icon available at the bottom of the grid.


Dashboard
Inventory
Network
Servers
Virtualization
Alarms
Maps
Apps
Workflow
Settings
Reports
Devices (39)
Generate Reports
Device Name
Status
IP Address
Device Type
Category
Vendor
Interfaces
Discovered Time
OPM-Firewall1 UnManaged 10.10.10.1 Unknown Unknown Unknown 0
OPM-Router2 UnManaged 10.10.10.3 Unknown Unknown Unknown 0
OPM-Router1 UnManaged 10.10.10.5 Unknown Unknown Unknown 0
OPM-AP1 Attention 10.10.10.21 Cisco 5508 AP Wireless Access Point Cisco 0
OPM-AP2 Attention 10.10.10.14 Cisco 5508 AP Wireless Access Point Cisco 0
OPM-AP5 Attention 10.10.10.16 Cisco 5508 AP Wireless Access Point Cisco 0
OPM-AP4 Clear 10.10.10.23 Cisco 5508 AP Wireless Access Point Cisco 0
OPM-AP3 Clear 10.10.10.29 Cisco 5508 AP Wireless Access Point Cisco 0
OPM_WLC31 Trouble 10.10.10.31 Cisco 5508 WLC Wireless LAN Controller Cisco 11
OPM-Server1 Service Down 10.10.10.36 ESXServer Server VMware 0
OPM-Server2 Service Down 10.10.10.45 ESXServer Server VMware 0 10 days ago
OPM-Router3 Critical 10.10.10.49 Cisco 2800 Series Router Cisco 5 10 days ago
OPM-Router4 Critical 10.10.10.55 Cisco 2900 IS Series Router Cisco 6 10 days ago
Choose Custom Fields
Comments
Telephone Number
Contact Name
Department
Cabinet
RackPosition
Floor
Date
Building
Cancel
Ok

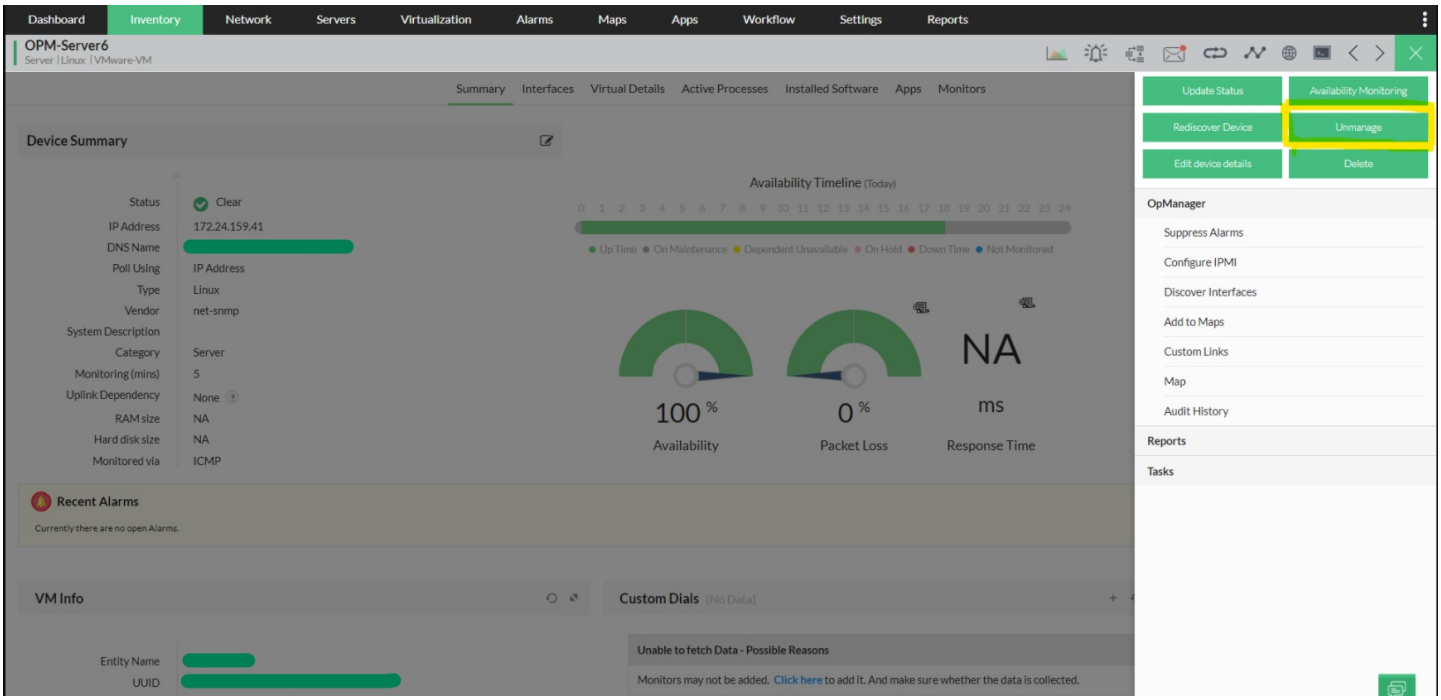
Managing and Unmanaging a Device

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**.

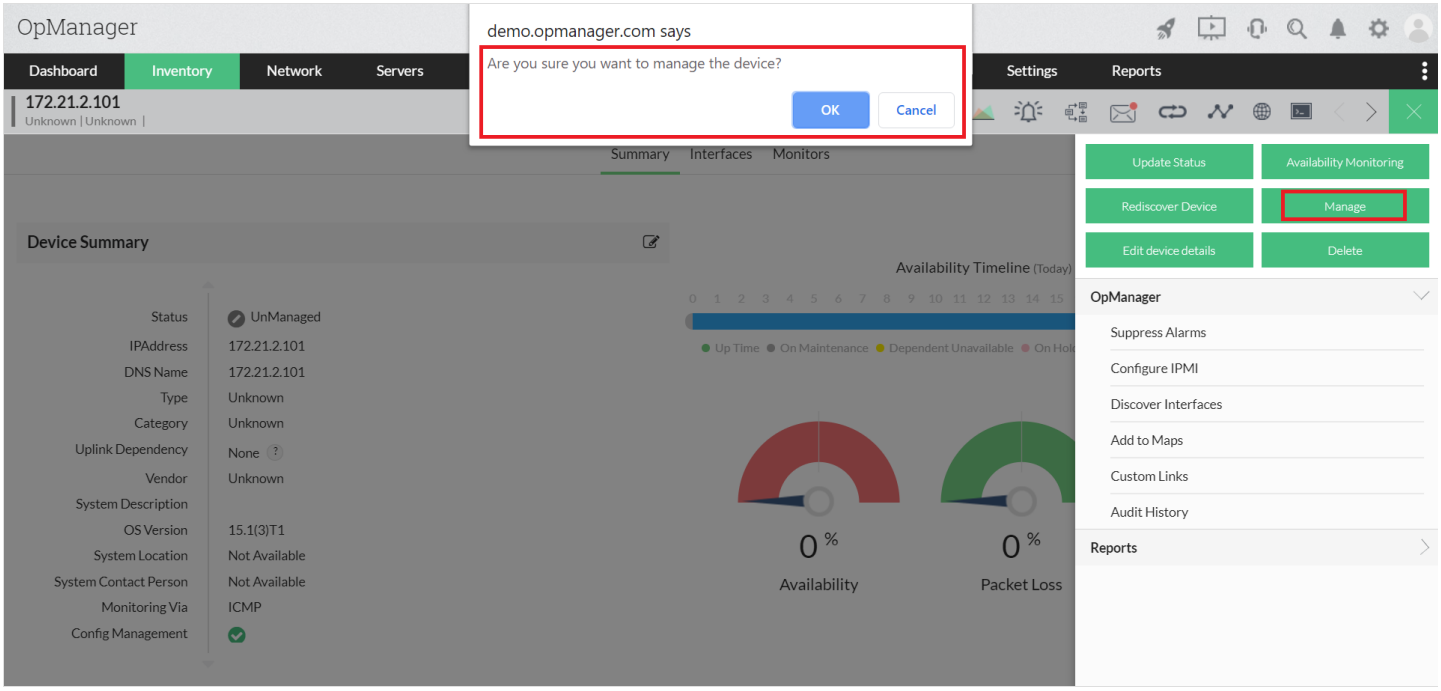
This stops the status polling and data collection for the device and changes the device status icon to grey.



To start managing an unmanaged device:

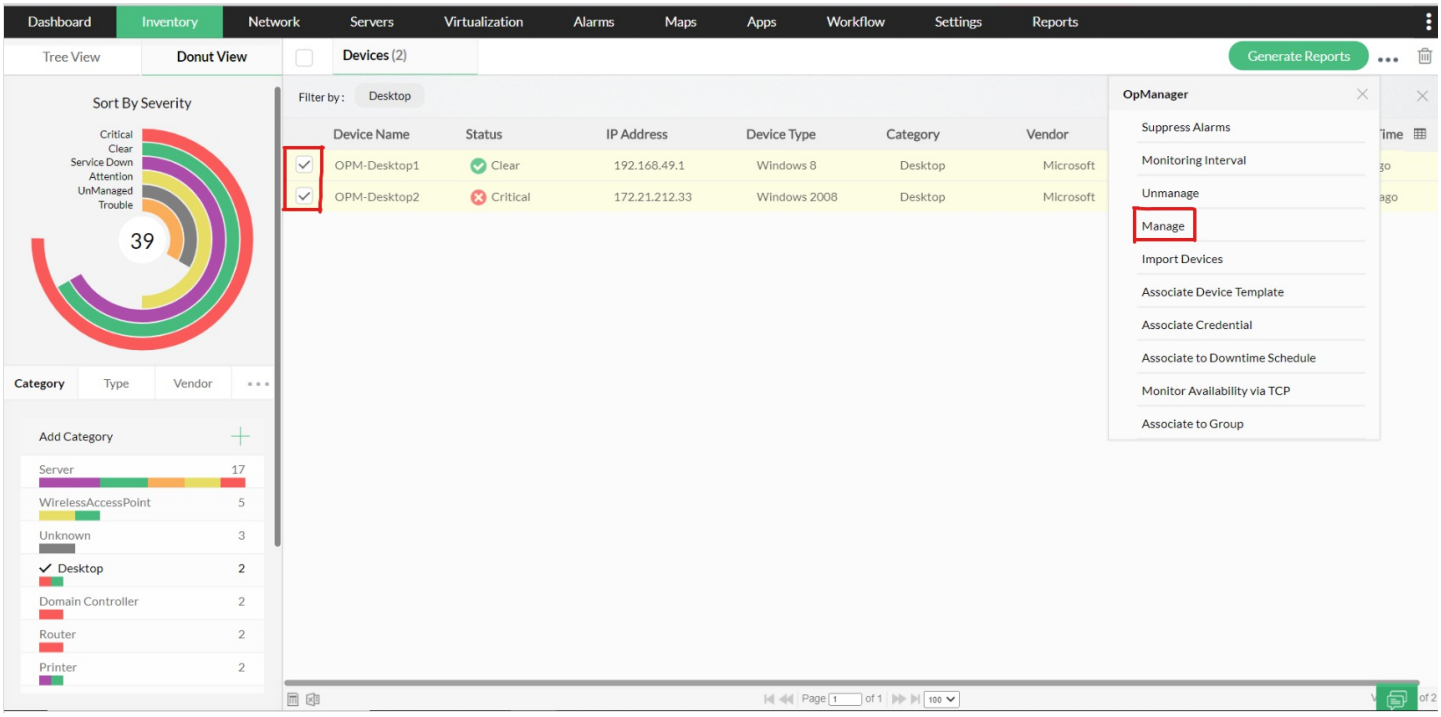
- Go to **Inventory > Devices > Device snapshot** page
- Click the **Menu** icon and select **Manage**.

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

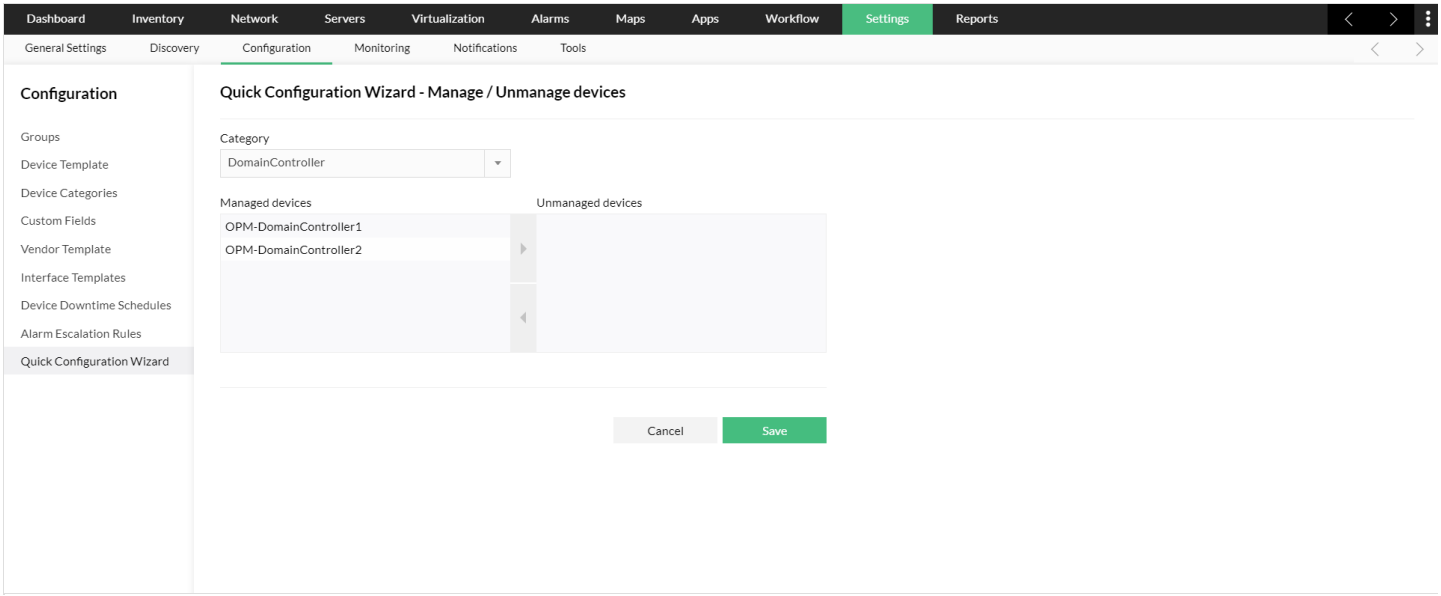


To Manage or Unmanage devices in bulk:

- 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.


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
DomainController
Managed devices
Unmanaged devices
OPM-DomainController1
OPM-DomainController2
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.

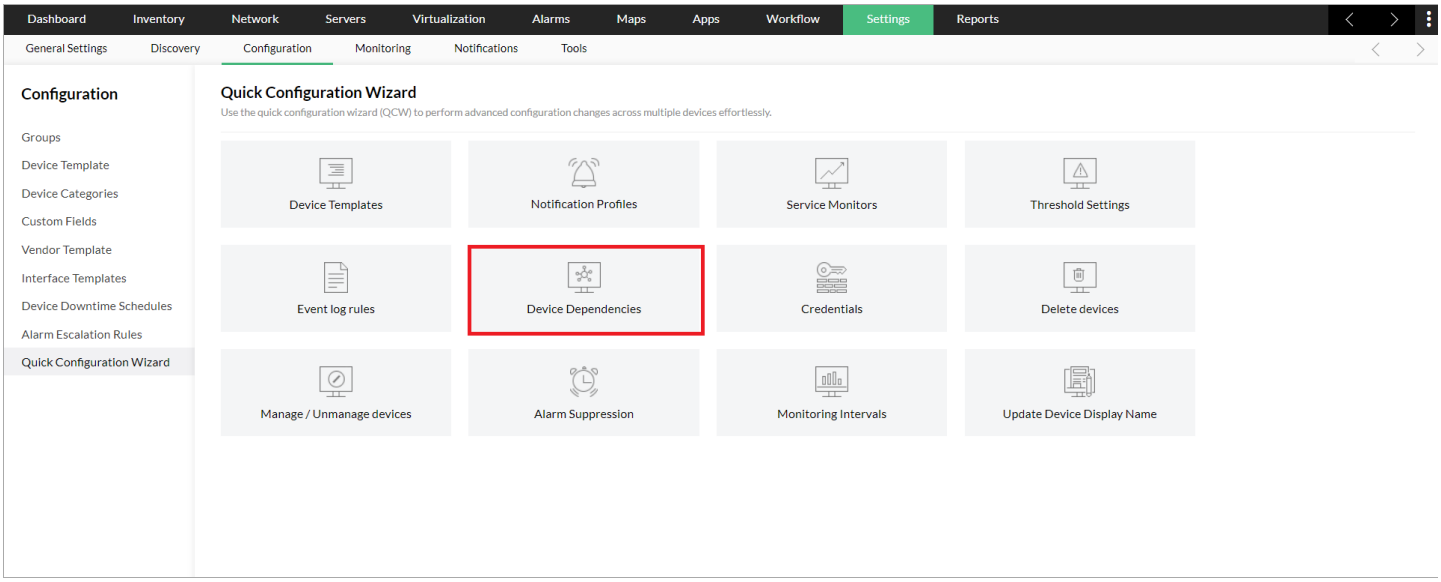
Configuring Device Dependencies

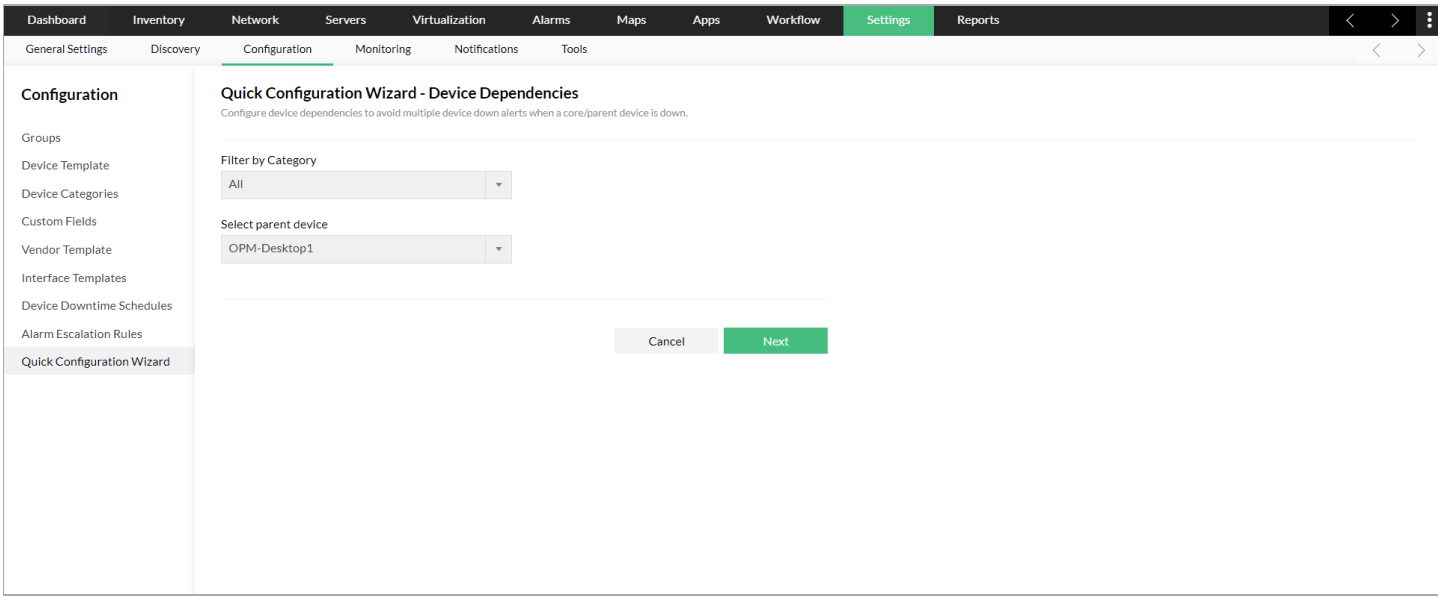
The status polling for a device can be controlled based on its dependency on some other device. This prevents the unnecessary status checks made to the dependent nodes.

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**.



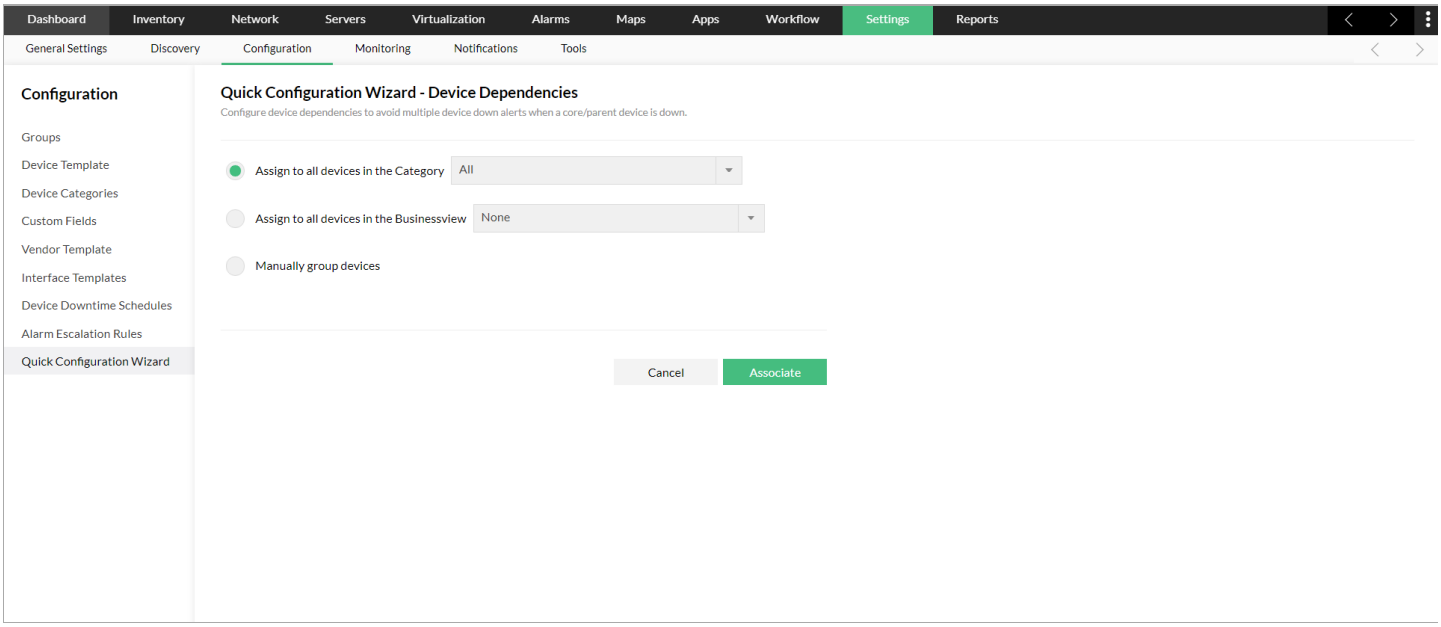


Select Device Dependencies in individual devices

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.



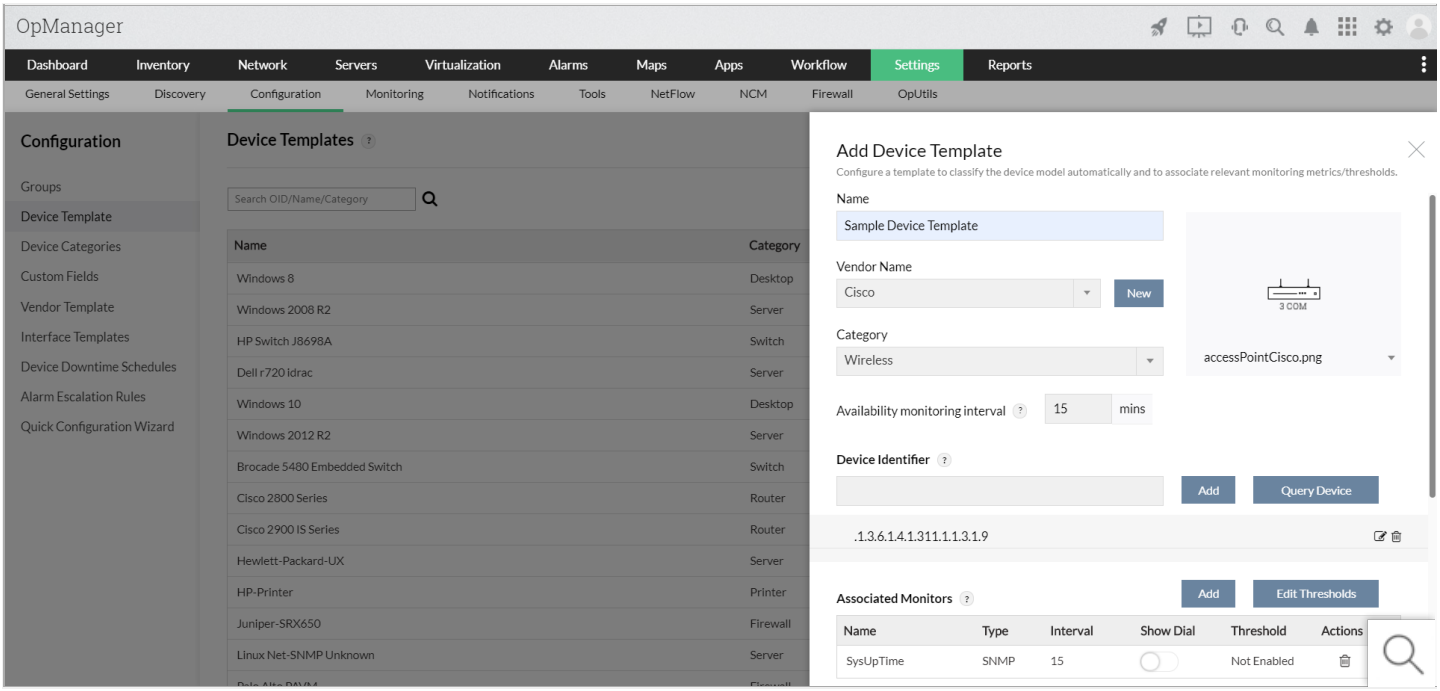
Configuring Device Templates

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:

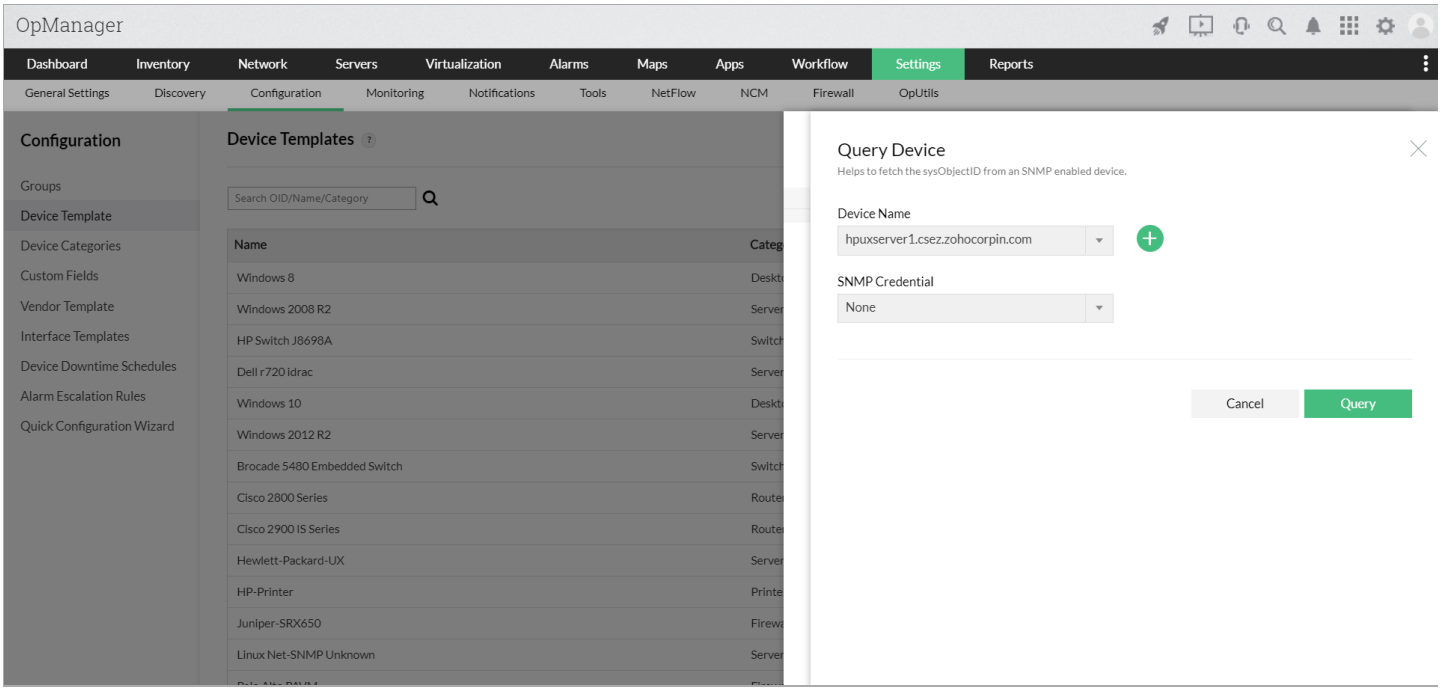
    - **Device Template**: Specify the device type.
    - **Vendor Name**: Select the vendor. Click **New** to add a new vendor, and **Save**.
    - **Category**: Select the category for the device type. On discovery, the devices are automatically placed in the select Category map.
    - **Monitoring Interval**: 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.

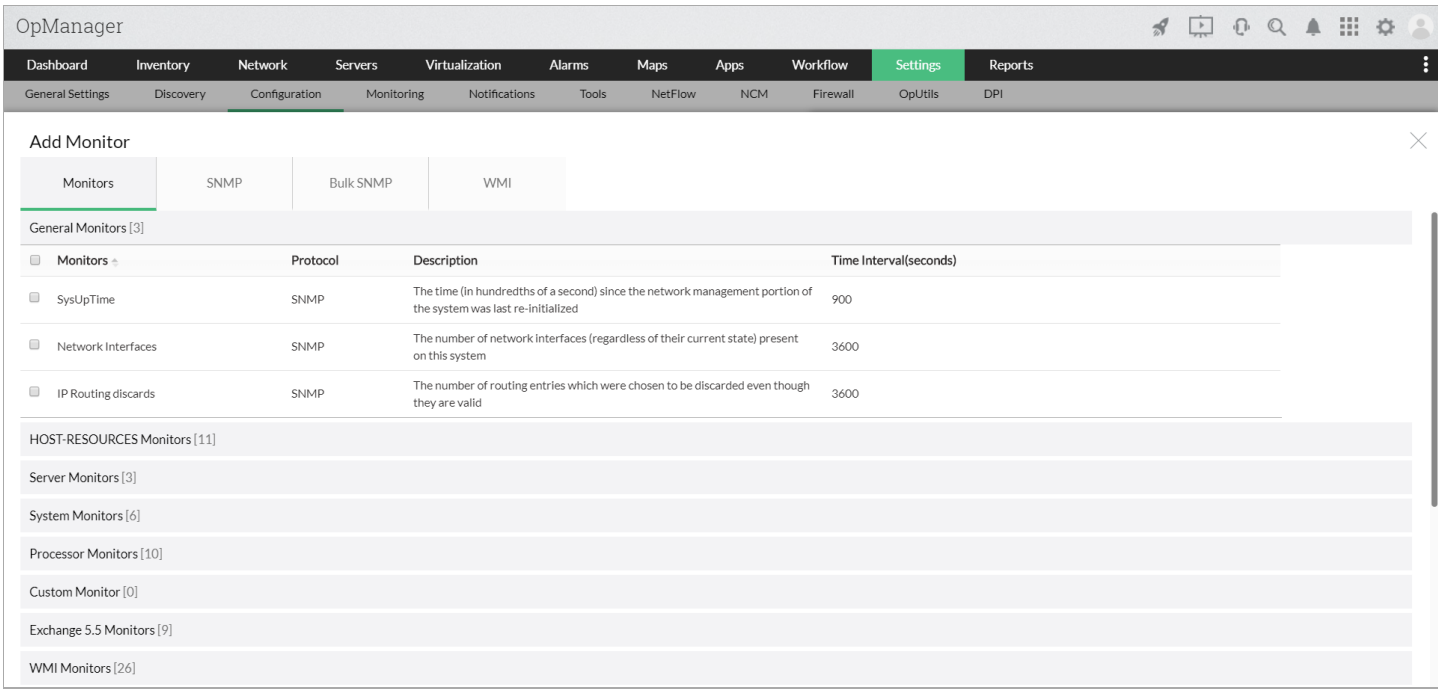
Device Identifier:

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

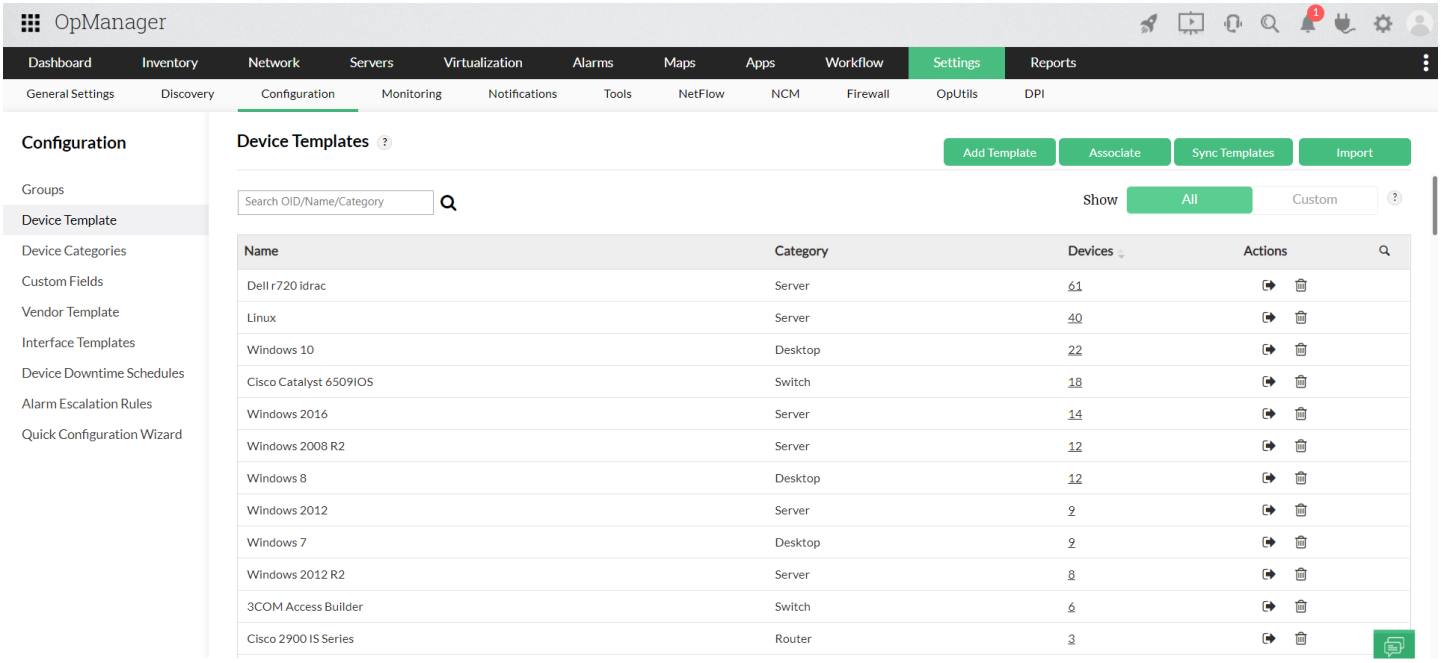
You can also add your own infrastructure views. For example, if you want to group a set of sensors, it will be absurd to classify them under servers or desktops. In such cases, the custom infrastructure allows you to create more defined groups by adding additional custom views.

This initial classification may not be accurate if -

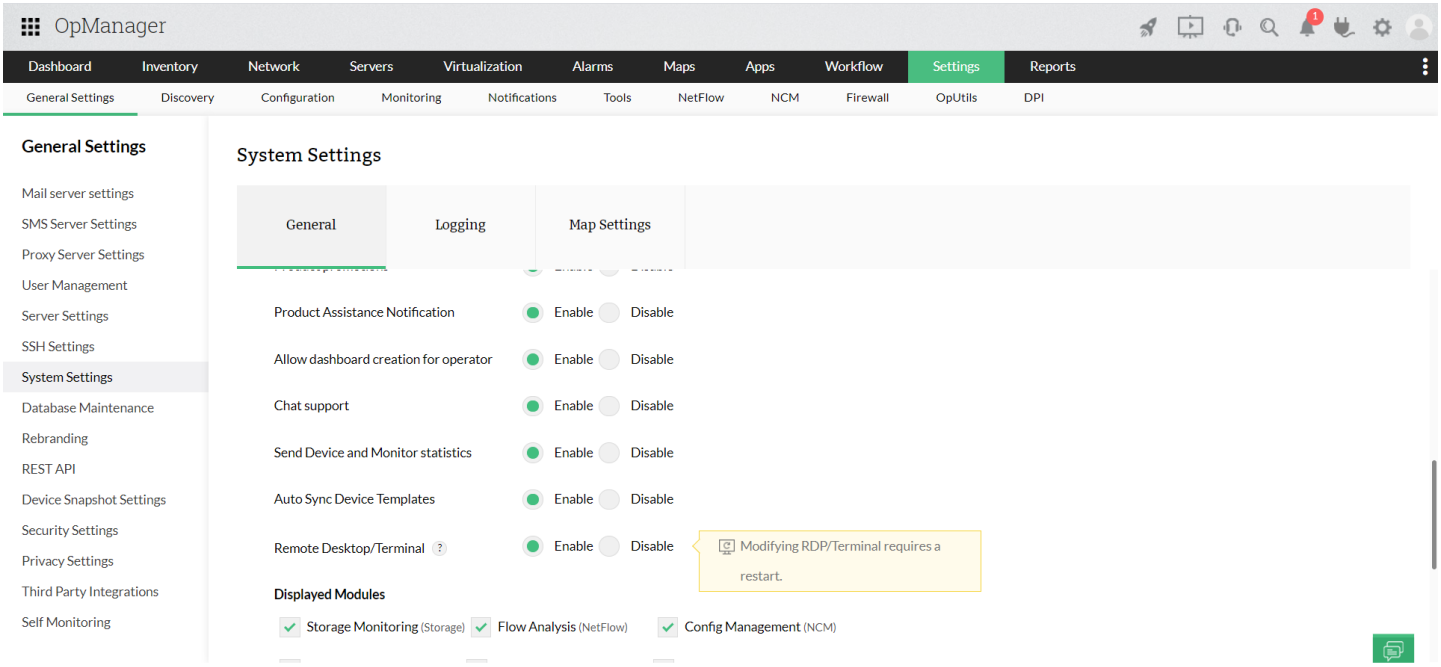
- The network devices do not support SNMP.
- Some devices have their SNMP settings different from those specified in the Credential Settings.

Sync new device templates

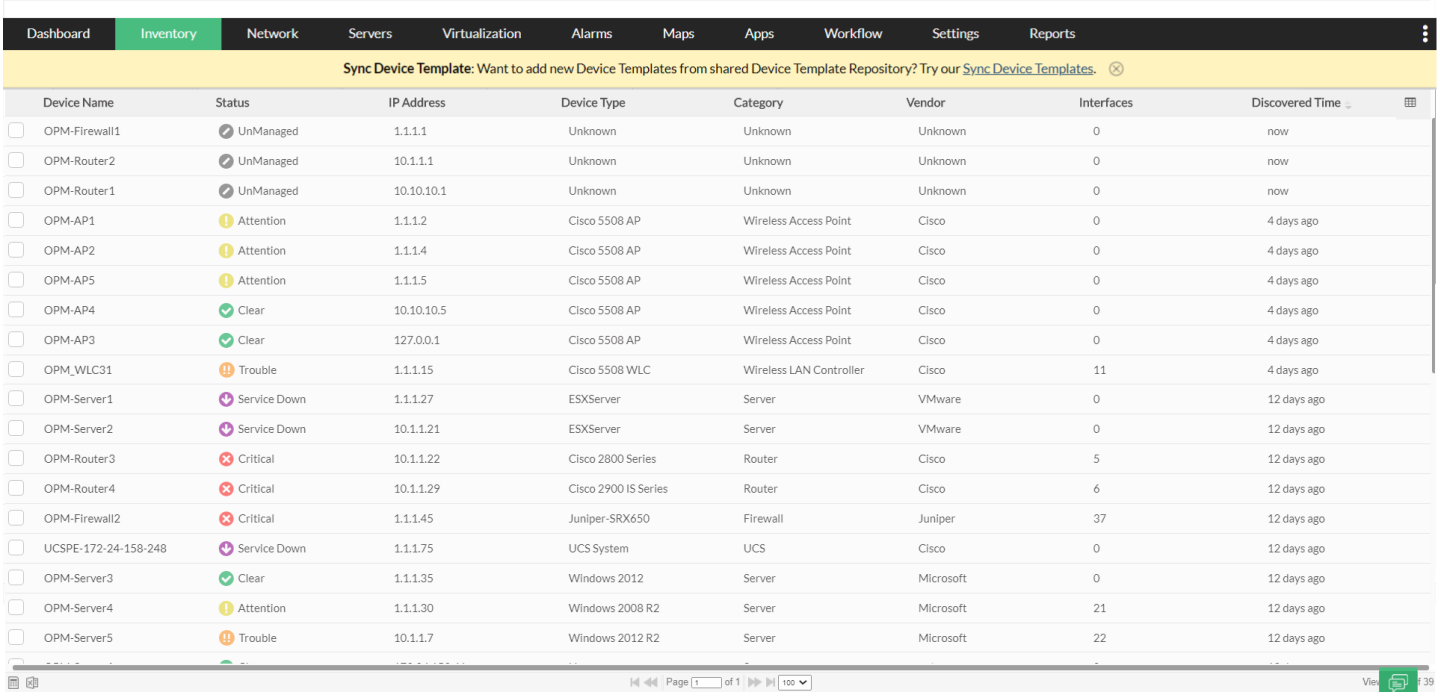
You can access the sync option by visiting Settings -> Configuration -> Device Templates -> Sync Templates.



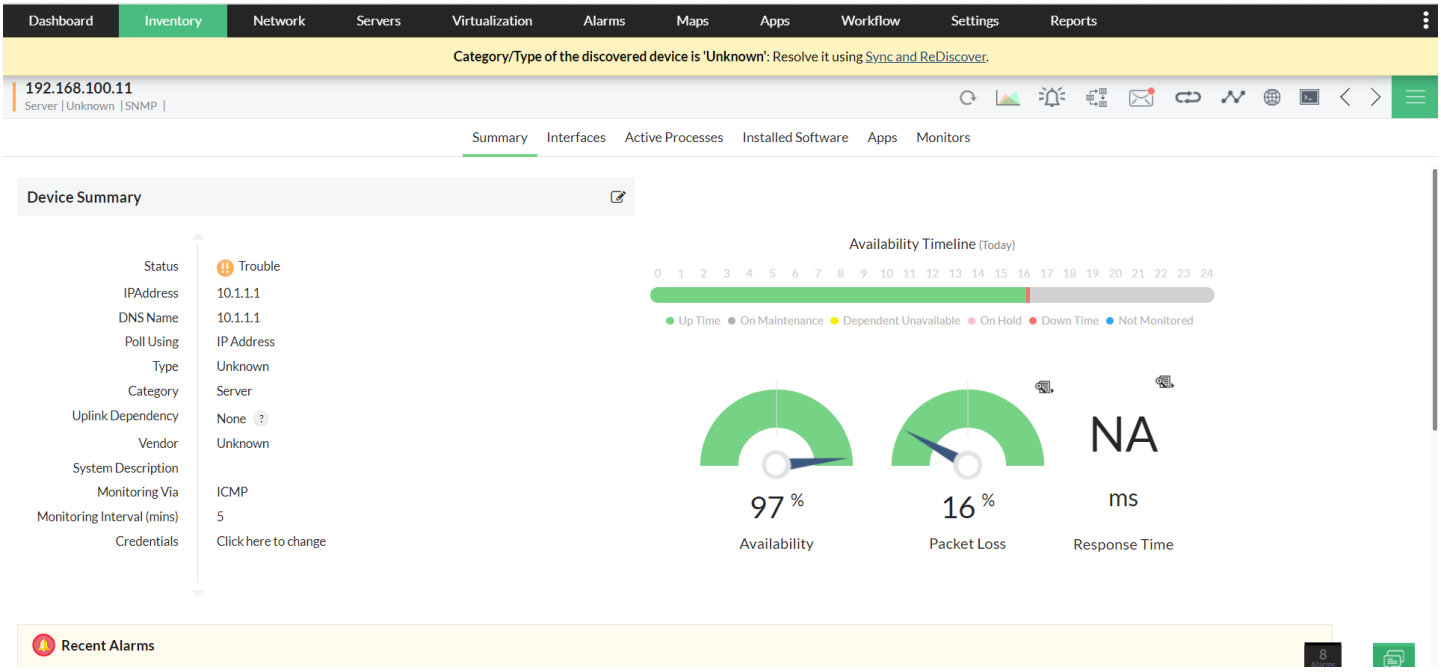
This will fetch and sync all new device templates from the shared repository of OpManager. You can also enable auto sync option. This enables you to discover new deivce templates at constant intervals.



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

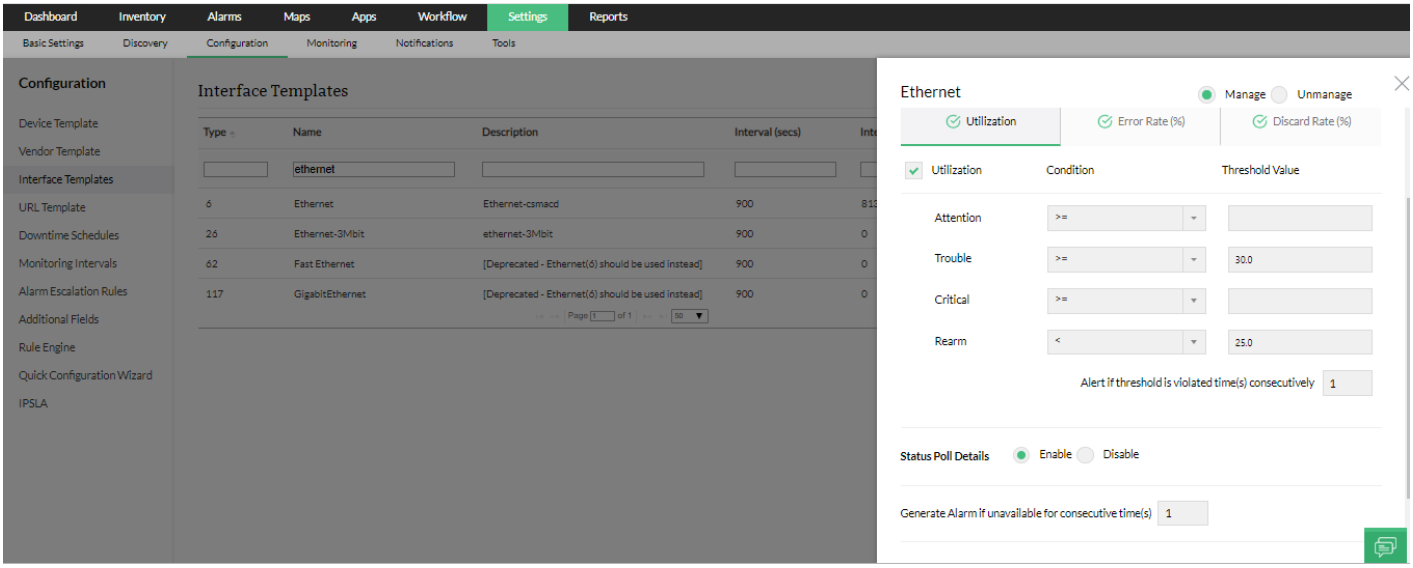
During initial discovery, OpManager categorizes the device interfaces into corresponding interface types with the help of predefined templates that are bundled with the product. OpManager comes with 292 interface templates which carry the initial configurations to classify these interfaces and associate 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.

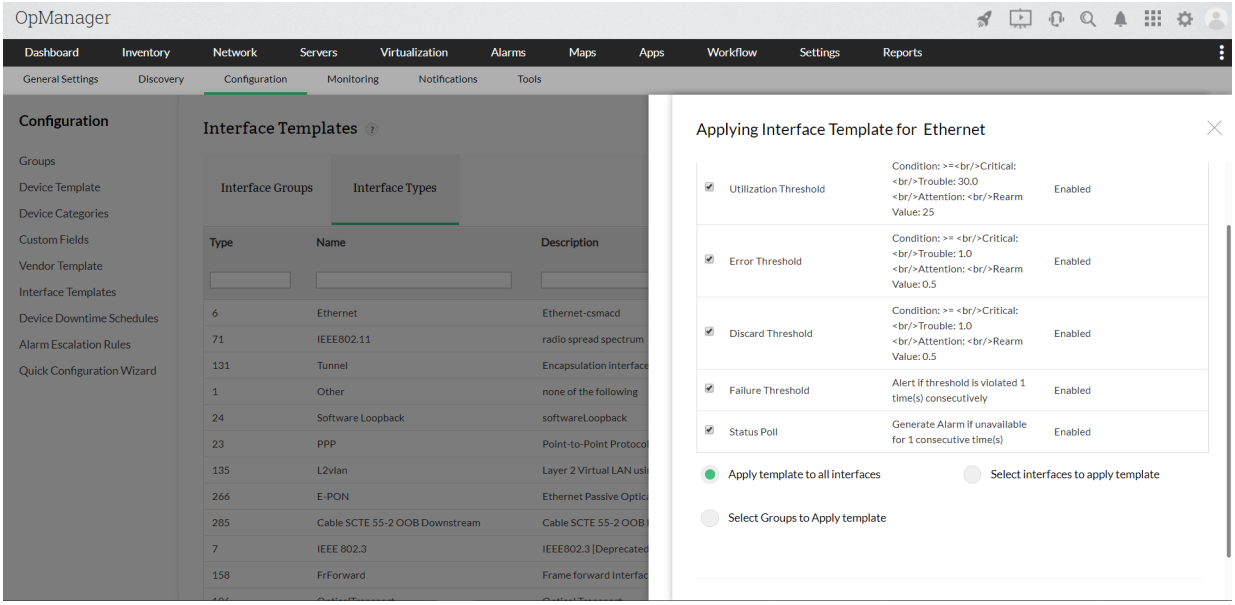
OpManager also allows the users to define multiple severity thresholds for interface templates, thereby generating alerts when the threshold values are violated.

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

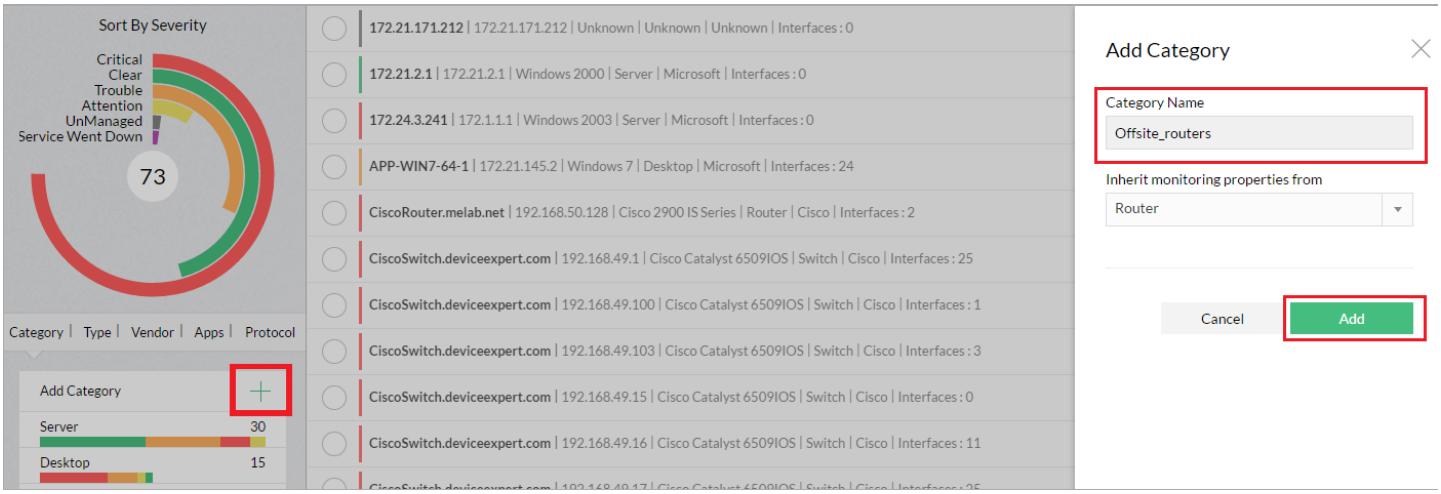
The discovered devices are classified into the above categories based on response to SNMP requests sent by OpManager to the devices. The devices that are not SNMP enabled, and the device types which are not included in the template are incorrectly classified under desktops. You can also add your own 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**.



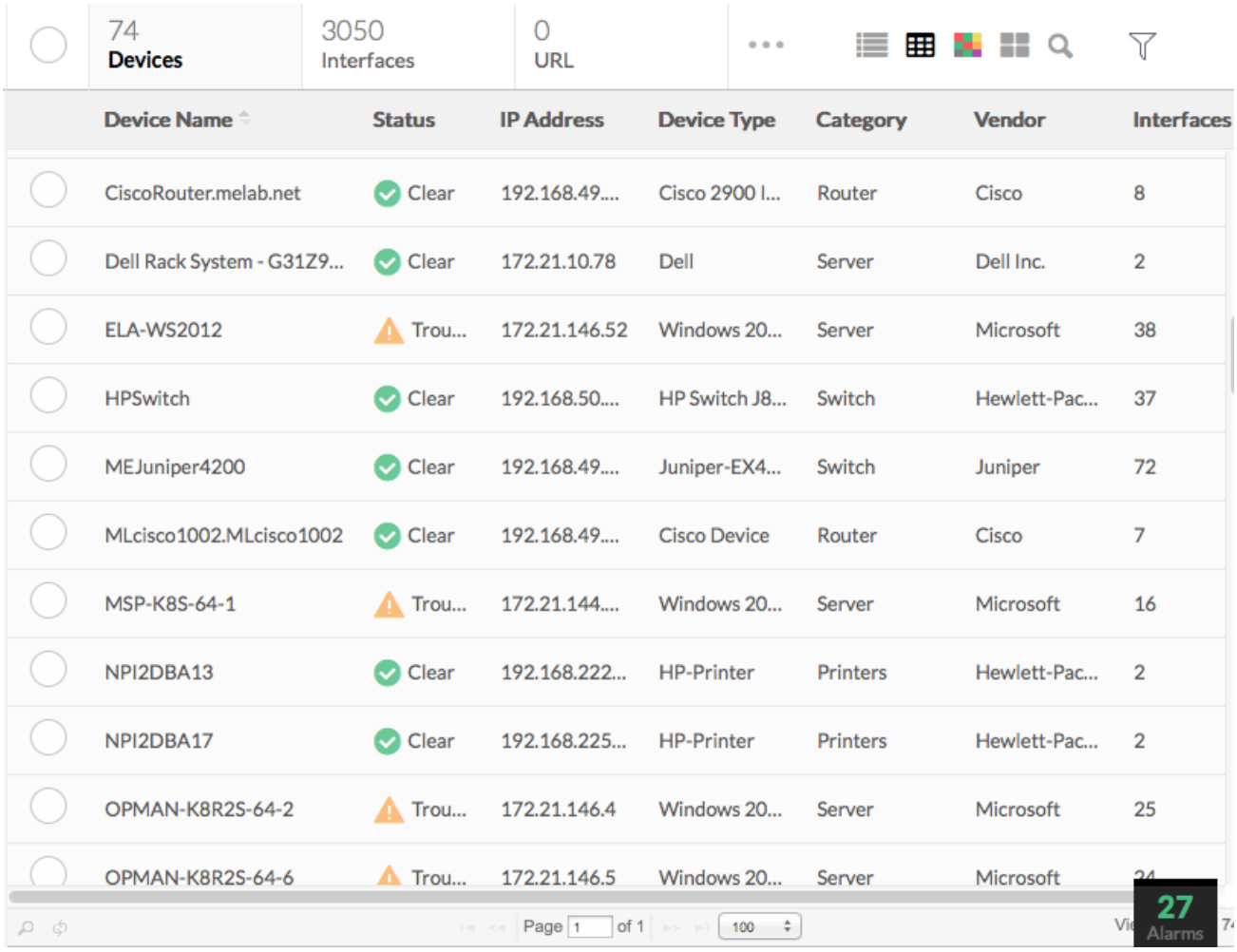
After you create new infrastructure views, you can create device templates for devices of this category. This allows you to define monitors specific to the category and automatically applies the configurations defined in the template to the devices as soon as they are discovered.

Different Types of Views

OpManager helps you visualize your entire network health in real-time with the help of built-in views. This can be accessed from **Network -> All Devices**. There are five different set of views available in OpManager such as List view, Table view, Heat Map view, Icon view and Interface view.

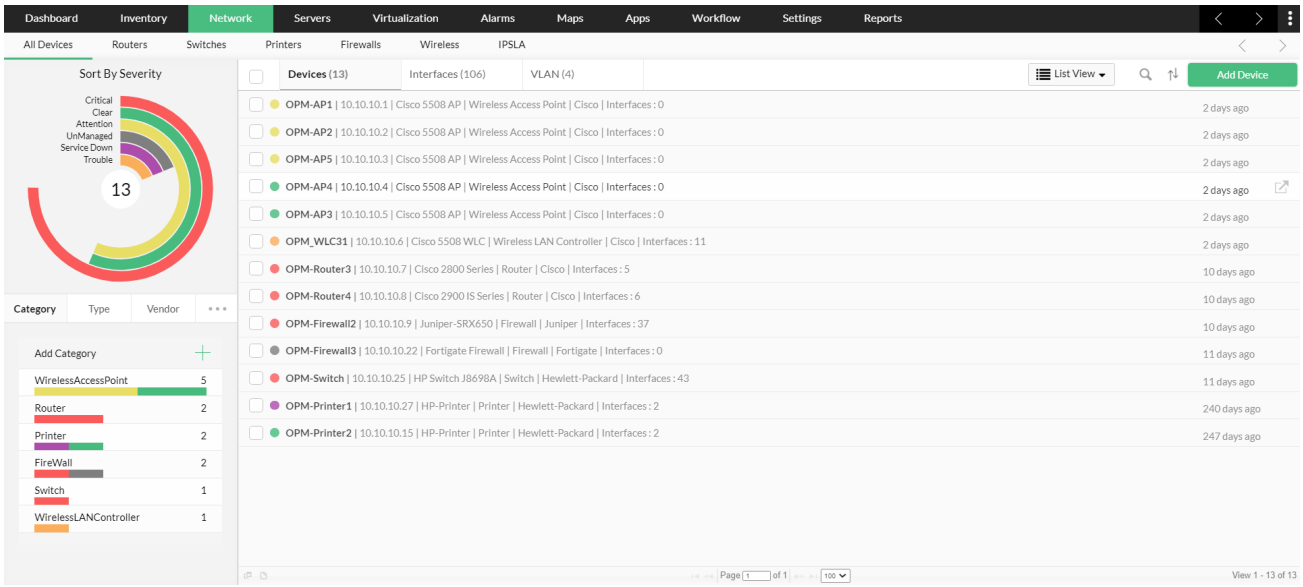
Table View

This view is similar to that of an Inventory. You can find details such as the device name, its availability status, the interfaces associated, type, vendor, etc.



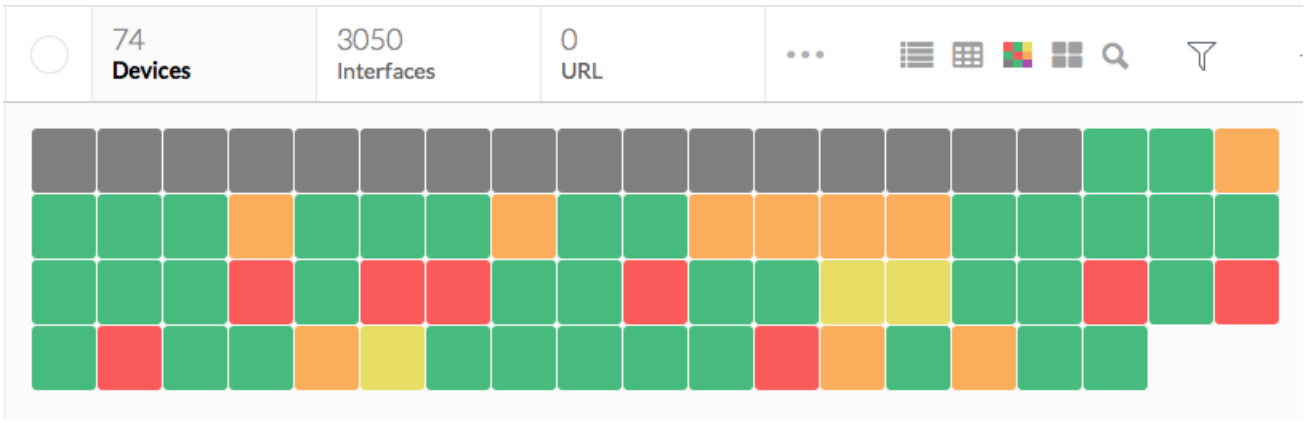
List View

Lists the devices in your network with basic information such as IP address, name and type.



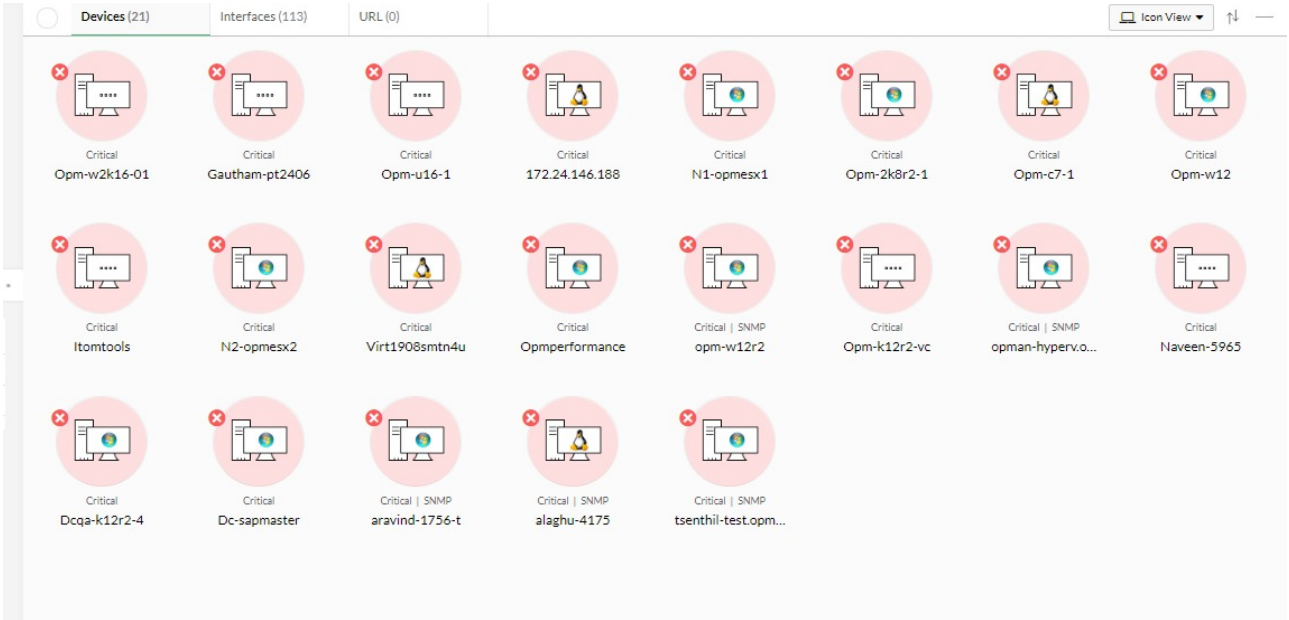
Heat Map View

Helps you visualize your network health with the help of color codes to communicate the severity of the monitored device.



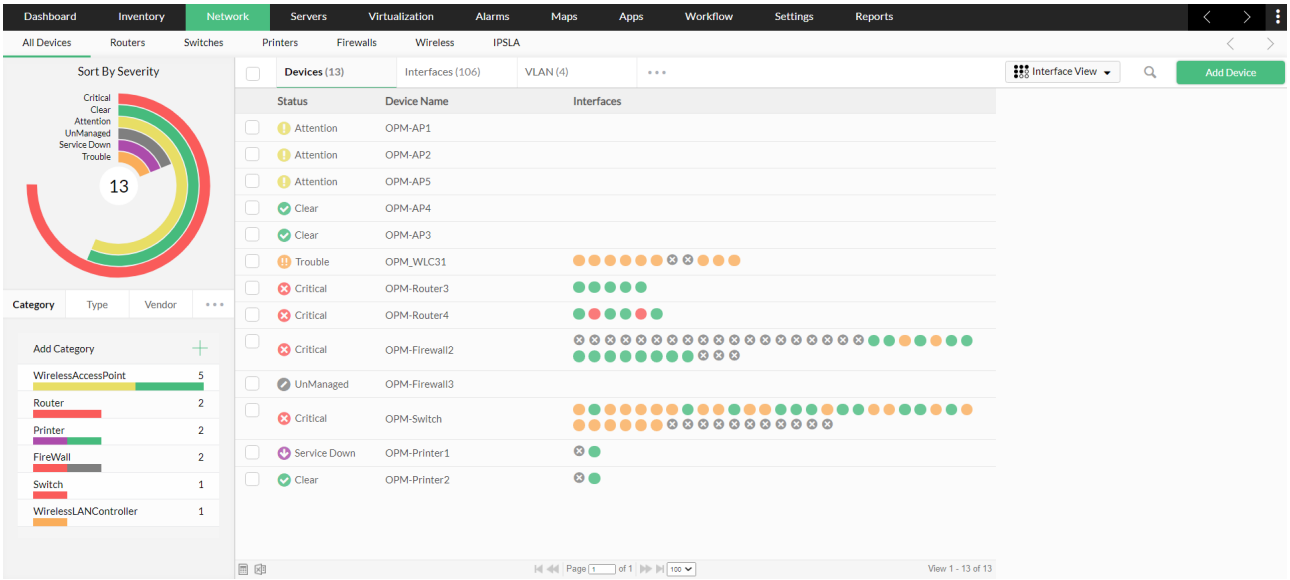
Icon View

The devices in your network will be displayed in the form of icons with the respective device name and its availability status.



Interface View

This view lists devices with the associated interfaces in the form of colour codes. These color codes represent the current status of the interface.



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.

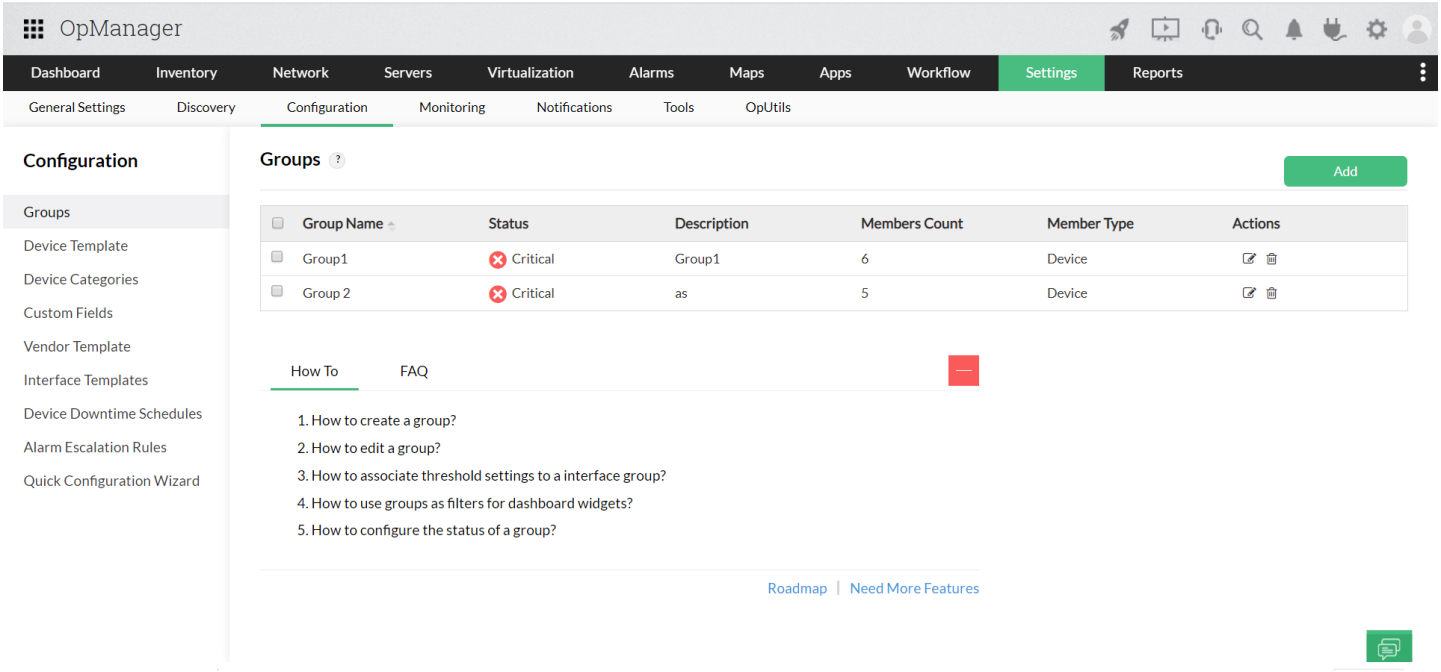
In Reports/Widgets, when "Network devices in India" group is selected, OpManager provides a detailed report of all the devices under the subgroups present under the parent group -&#65533; "Network devices in India".

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

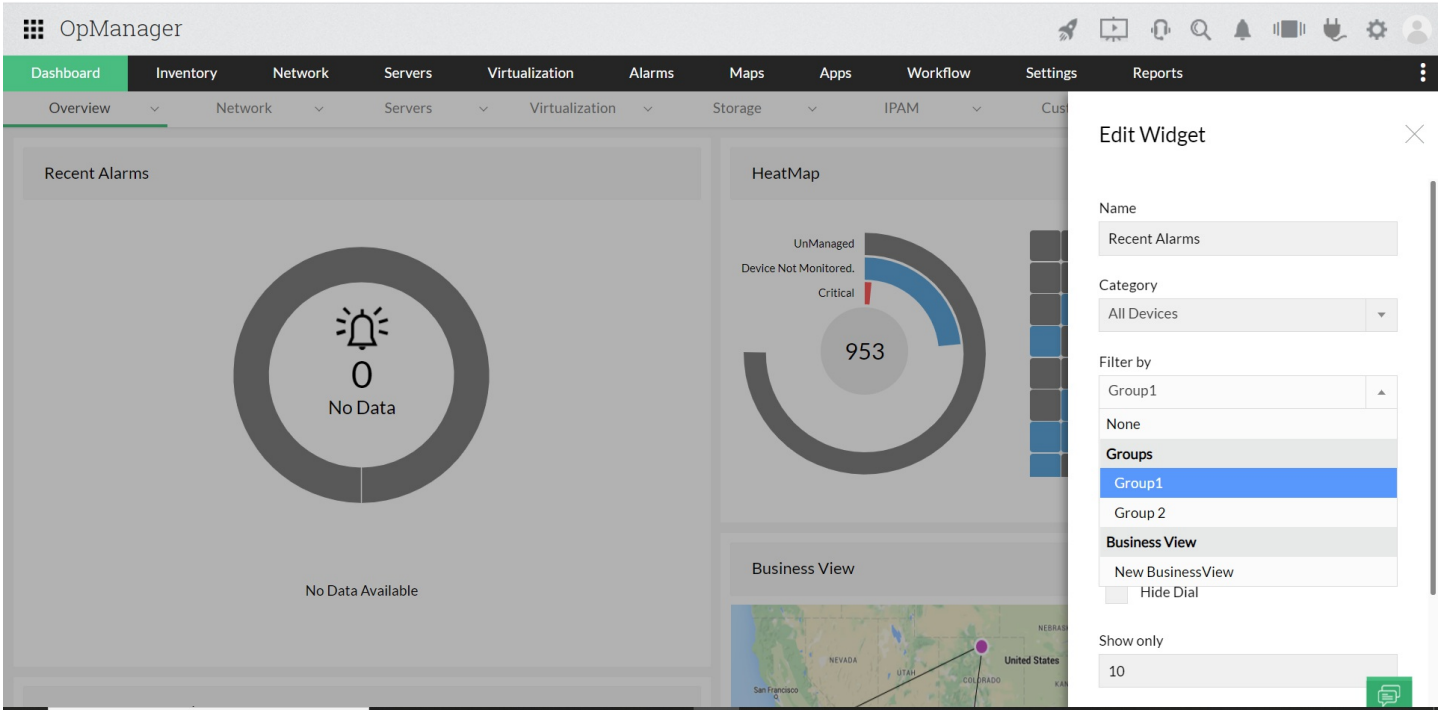
selected. If no member is selected, by default the health status will depend on all available group members.

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'**.

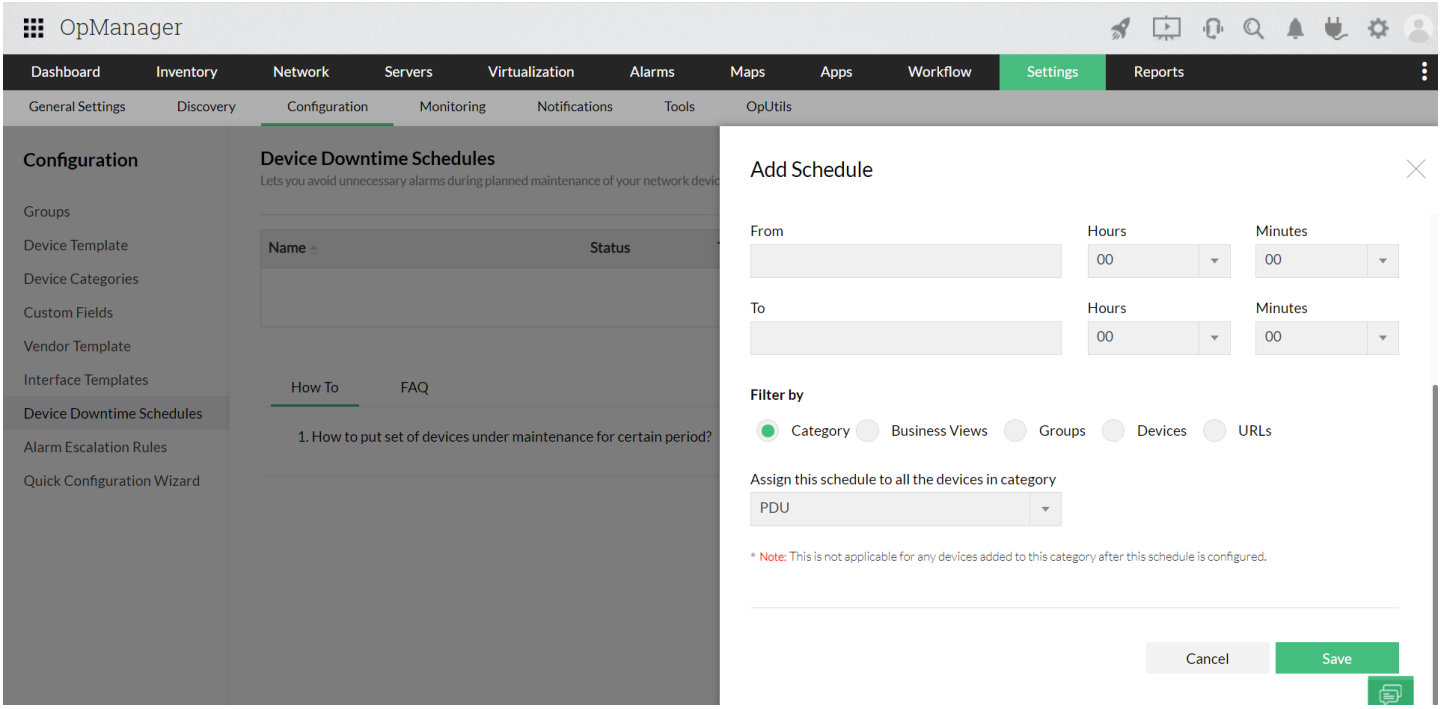


You can also view the availability data in the 'all groups' widget in the dashboard of OpManager.

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

User Roles, User Types and Access

User Roles

There are two primary **User Roles** in OpManager:

- Administrator User
- Operator User

1. 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.

2. Operator User:

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

User Types

Furthermore, there are three different **User Types** in OpManager, depending on the type of authentication:

- Local Authentication
- AD Authentication
- Radius Authentication

1. Local Authentication:

These are the users that are created locally in the product. The credentials for this user are created locally and stored in the server. The password can be changed by the user and it can also be reset by an Administrator User.

2. AD Authentication:

These are the users which are authenticated based on the credentials present in the domain. If Auto-login is enabled during AD configuration, then the user will be created automatically during the first login.

3. Radius Authentication:

There are users which are authenticated based on the credentials present in the radius server. Radius users should be created in OpManager during Radius configuration.

User Access

Access to users is either provided for all devices by selecting the "All devices" option during user creation (both for Administrator User and Operator User) or it can be provided for selective devices based on the available business views by choosing the "Selected Business Views" option.

To learn more about Business Views, please click here.

Password Policy

A password policy is a set of rules designed to enhance security by encouraging users to employ strong passwords. Another possible defense against password-guessing attacks is enabling an account-lockout, which means the account will be locked after a specified number of invalid or failed login attempts.

To configure a password policy in OpManager, go to **Settings -> Basic Settings -> User Management -> Password Policy**.

Minimum password length: Specify the minimum number of characters required in a password. It should be within 5-25 characters.

Enforce password history: Number of unique passwords that must be associated with a user account before re-using an old password.

Password complexity: Level of complexity to be associated with a password.

Simple

1. Minimum characters as specified above
2. Maximum 25 characters

Complex

1. Minimum characters as specified above
2. Maximum 25 characters
3. Minimum 1 uppercase, 1 lowercase and 1 special character (! ~ @ # $ % ^ & + = _ *).

Password should not be same as username: Enable this to option to prevent duplication of a username in the password.

User Account Lockout Policy: The User Account Lockout setting allows the administrator to lockout accounts after a specified number of invalid login attempts. A locked out account cannot be used until reset by an administrator or until the account lockout duration has expired. For instance, if invalid credentials have been provided for over 5 times, the account will be locked out for 2 mins. This lockout interval and the number of bad login attempts can be configured.

Maximum invalid login attempts: Specify the maximum invalid login attempts before an account gets locked out.

Lockout period: Specify the lockout duration in minutes.

Authorize AD group Users

User Group Details:

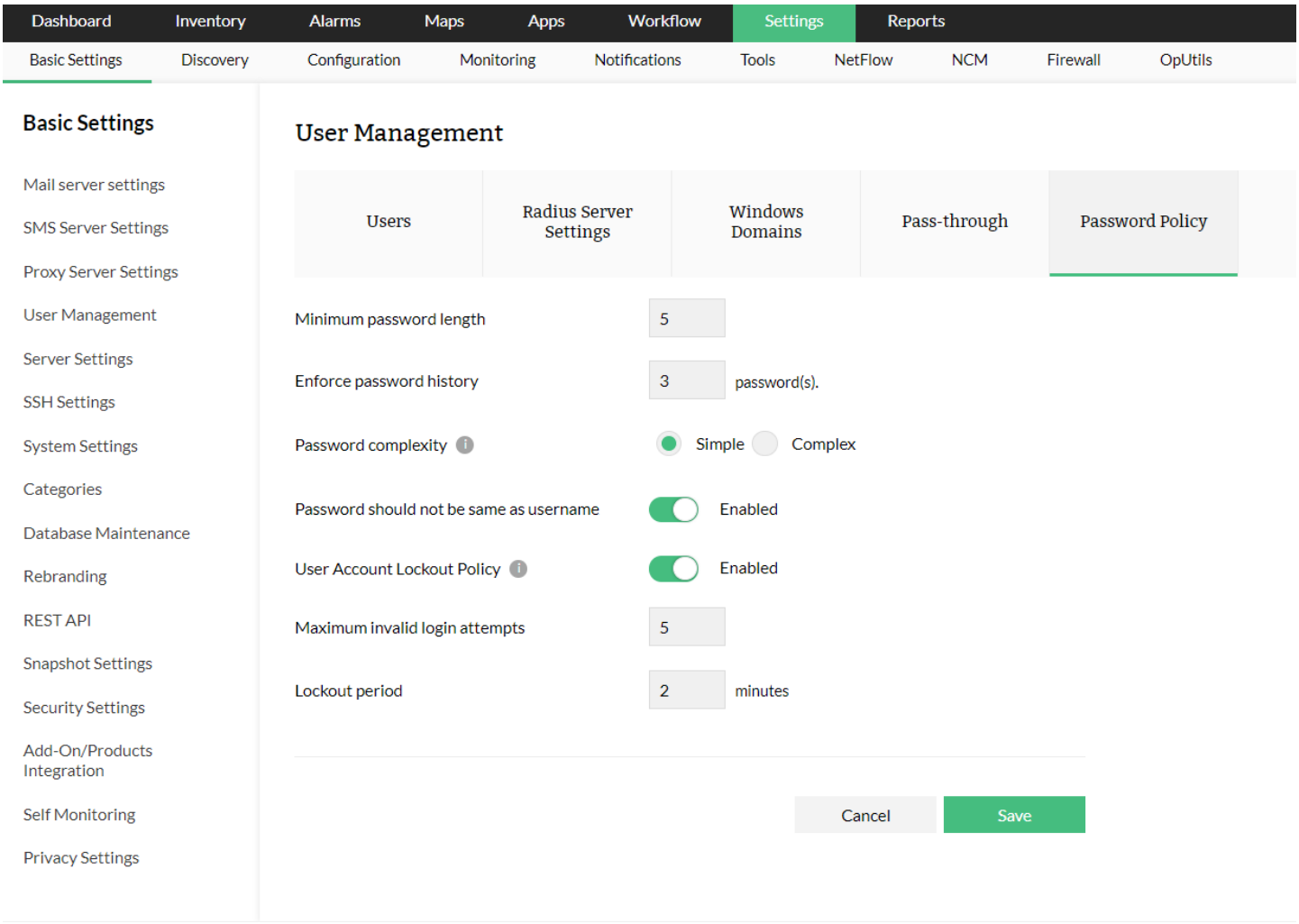
1. **Select AD Domain:** Click on the drop down menu and select the desired AD domain from the list of available domains or Click **Add Domain** to add a new domain.
2. **Domain Controller:** Update/provide the name of the AD domain controller. The domain controller name gets loaded automatically, once you select an existing AD domain.
3. **Enabling auto login:** You can allow "All Users" (or) "Users from Selected Groups" under the chosen AD domain to access OpManager using their AD credentials. If you have chosen Selected Groups, provide the list of group names that require full or read-only access control. In case if the same user exist in both groups with read only and full control user permissions. The user with read only permission gets the preference over the other.

Access Details:

1. User Permissions: Select "Full Control" to provide complete read/write control to the user to monitor resources using OpManager. Select "Read Only Access" if the user is allowed only to view the resources.
2. Select the **Social IT Plus Account** check box to enable the user to access Social IT page
3. Click **Save**.

Note: The password policy is applicable only to local users. We do not have any control over the AD and radius user passwords.

Their password policies completely depend on the respective AD and Radius server settings.



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

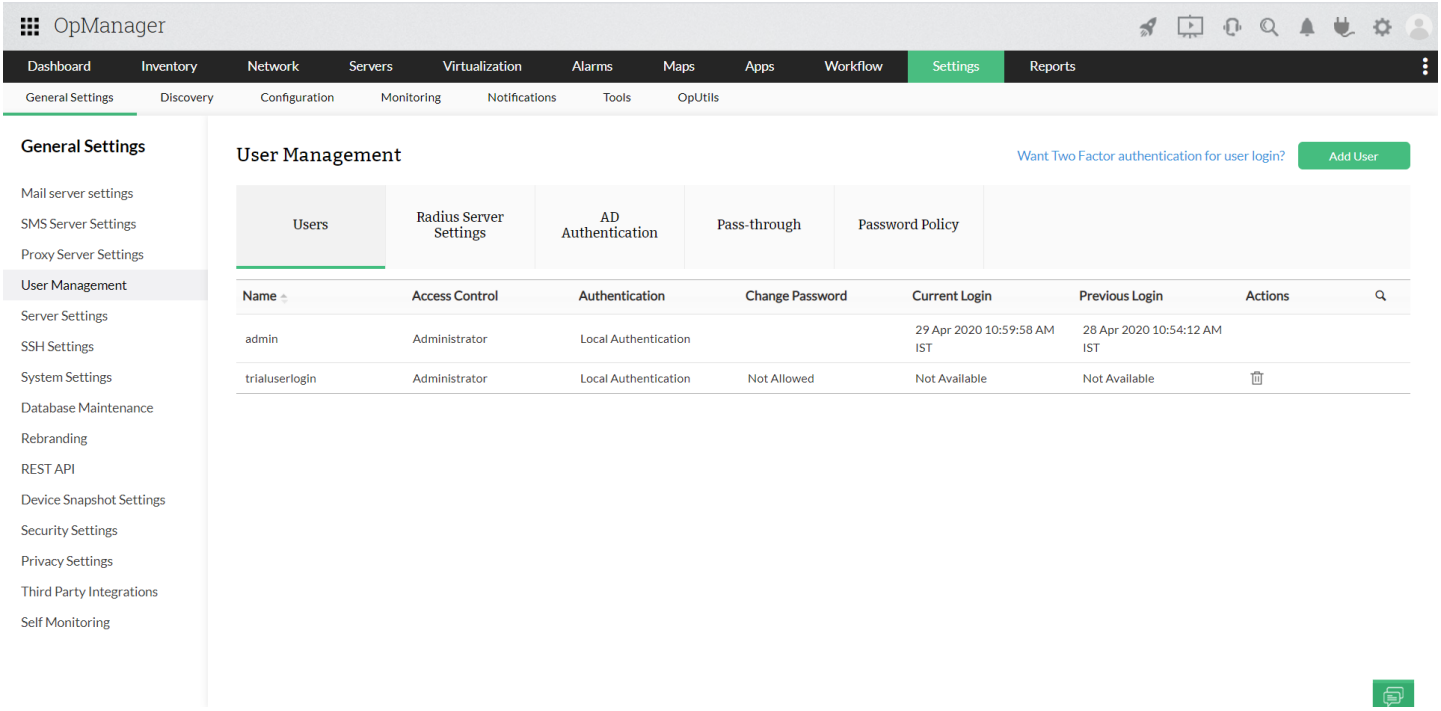
1. **User Details**:

    - 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 - Email ID 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 - 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 an AD user

1. **User Details**:
    - User Name - Name of the AD user to be added
    - Email ID - Email ID for the AD user
    - Phone Number: Enter the user's phone number
    - Mobile Number: Enter the user's mobile number
    - Domain Name - 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 - 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**&#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

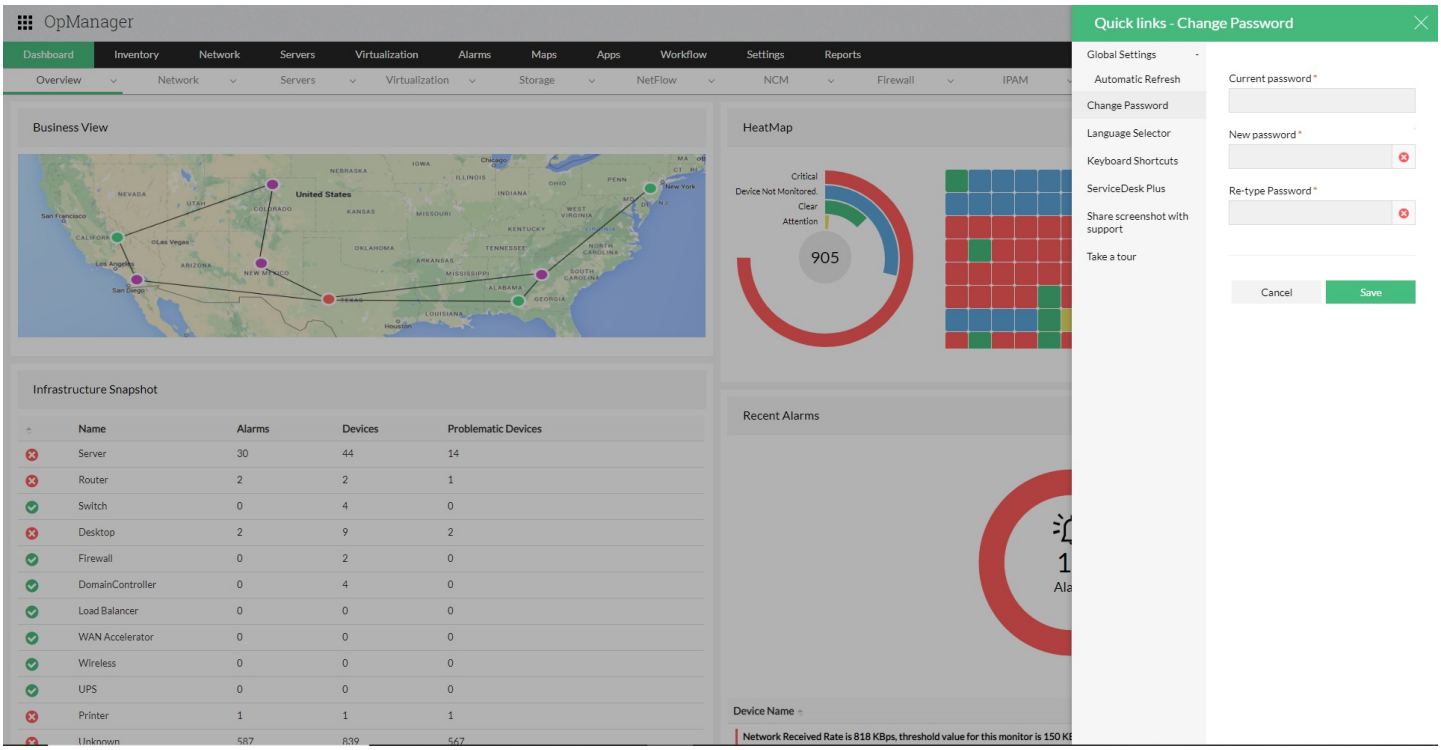
   Mobile number: The user's mobile number

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.

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.

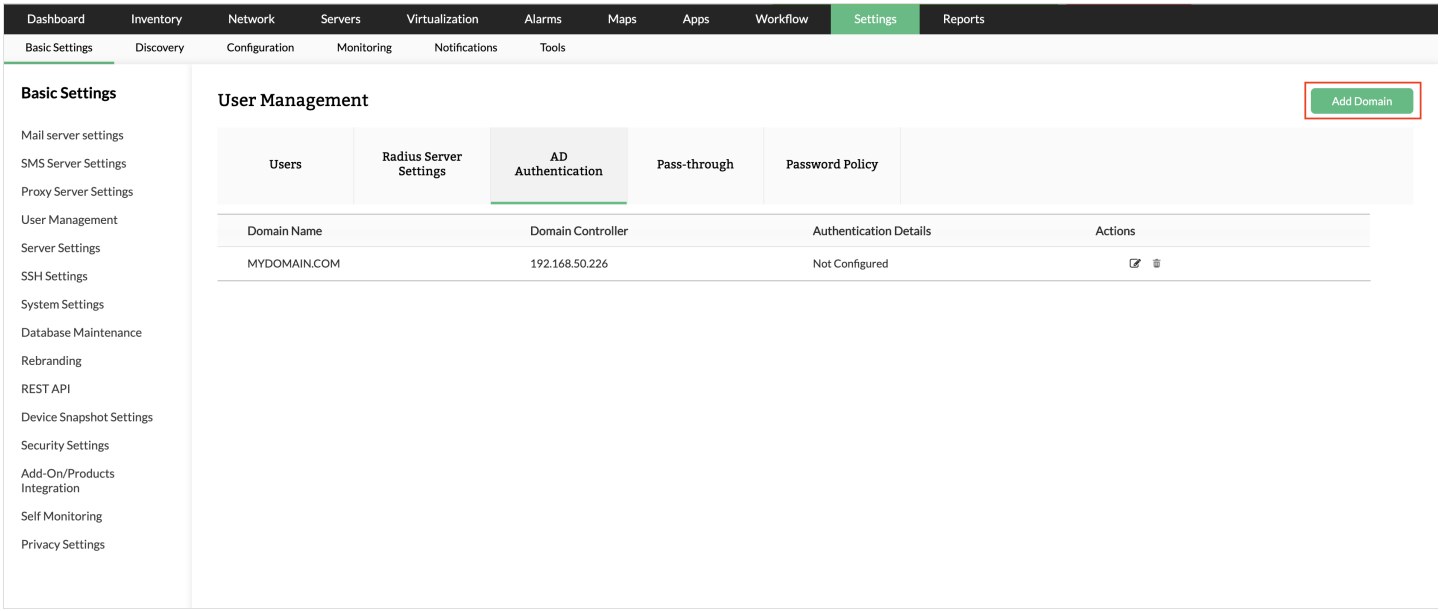
With the increase in software applications, each with their own authentication and password complexity levels, this feature also saves you the trouble of having to remember way too many passwords.

Add an AD Domain

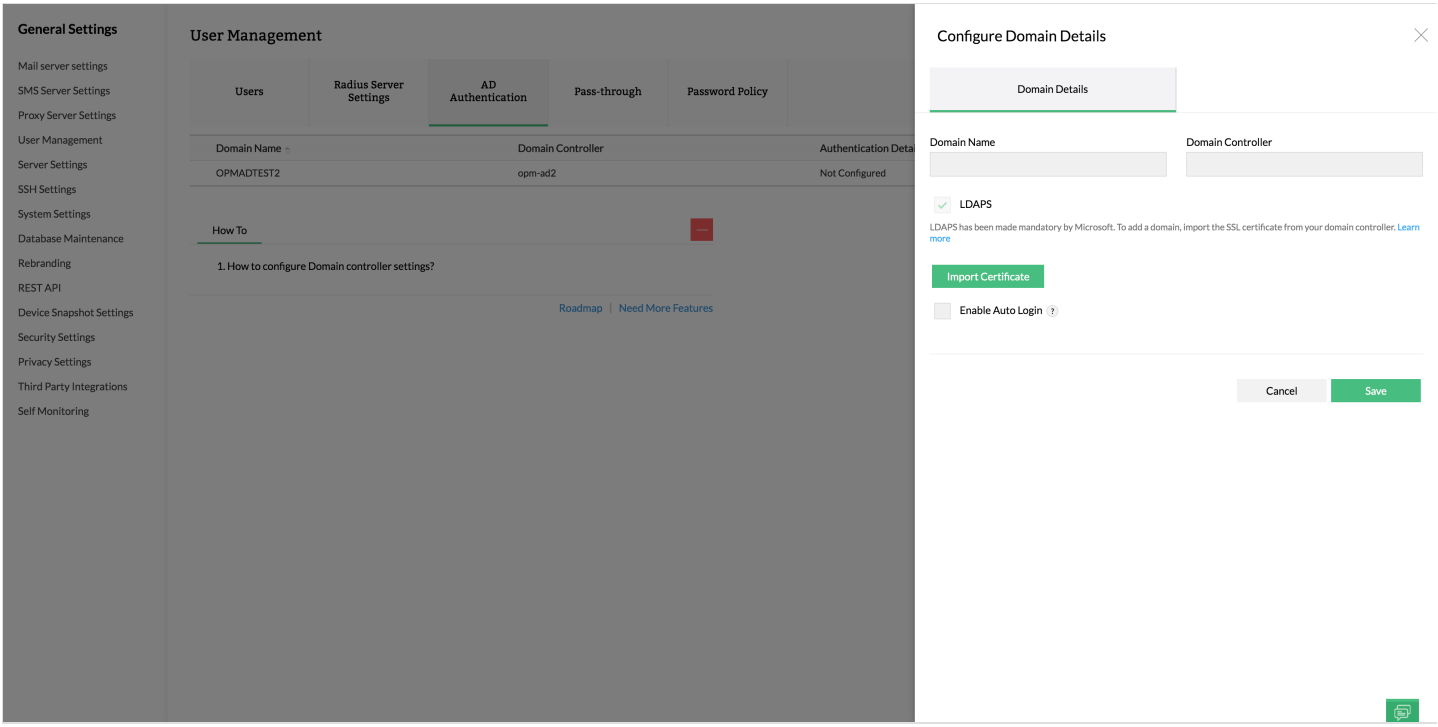
You can create Domains in OpManager and users manually in OpManager with the AD Authentication and User Management features.

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:

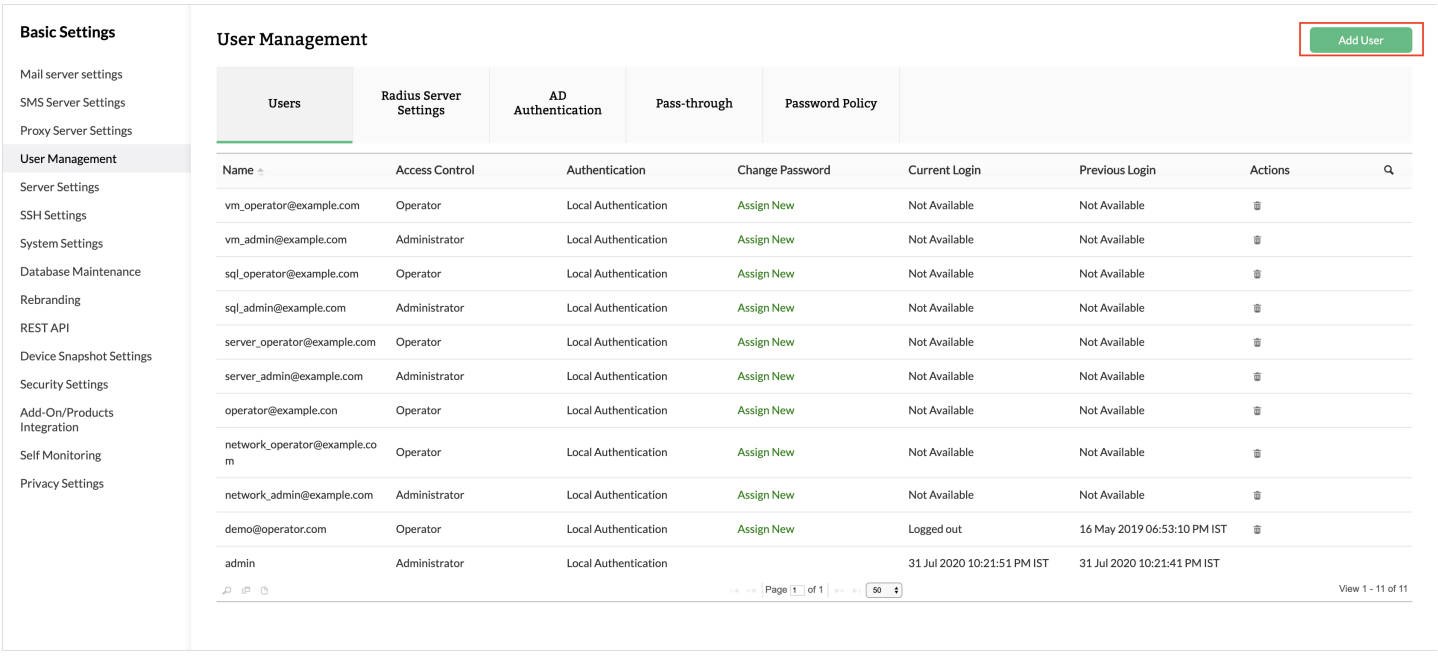
1. Exporting the LDAPS Certificate and Importing for use with AD DS
2. LDAP over SSL (LDAPS) Certificate

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.

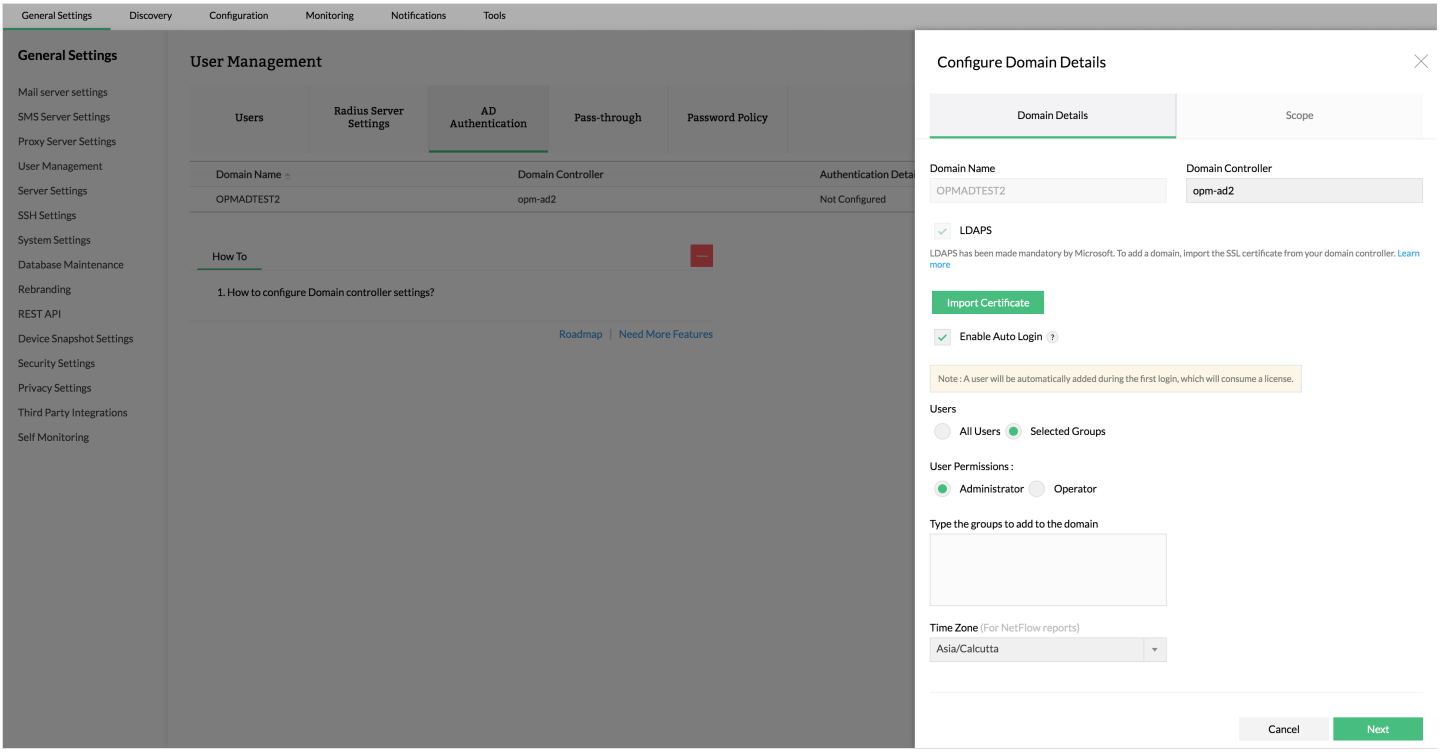
6. Once the domain is added, you can manually add users in the **Users** tab.



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.

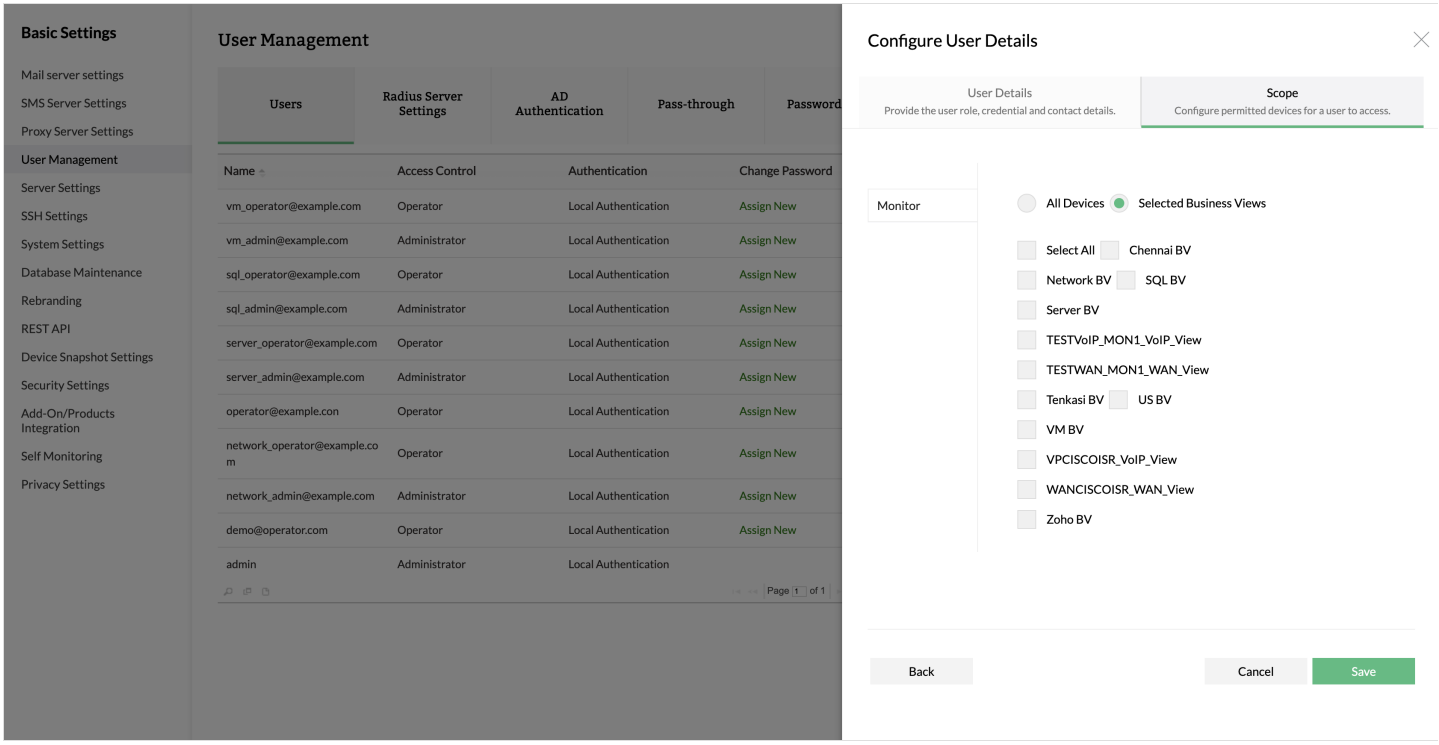
3. **Configuring Auto-login for**

- **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.



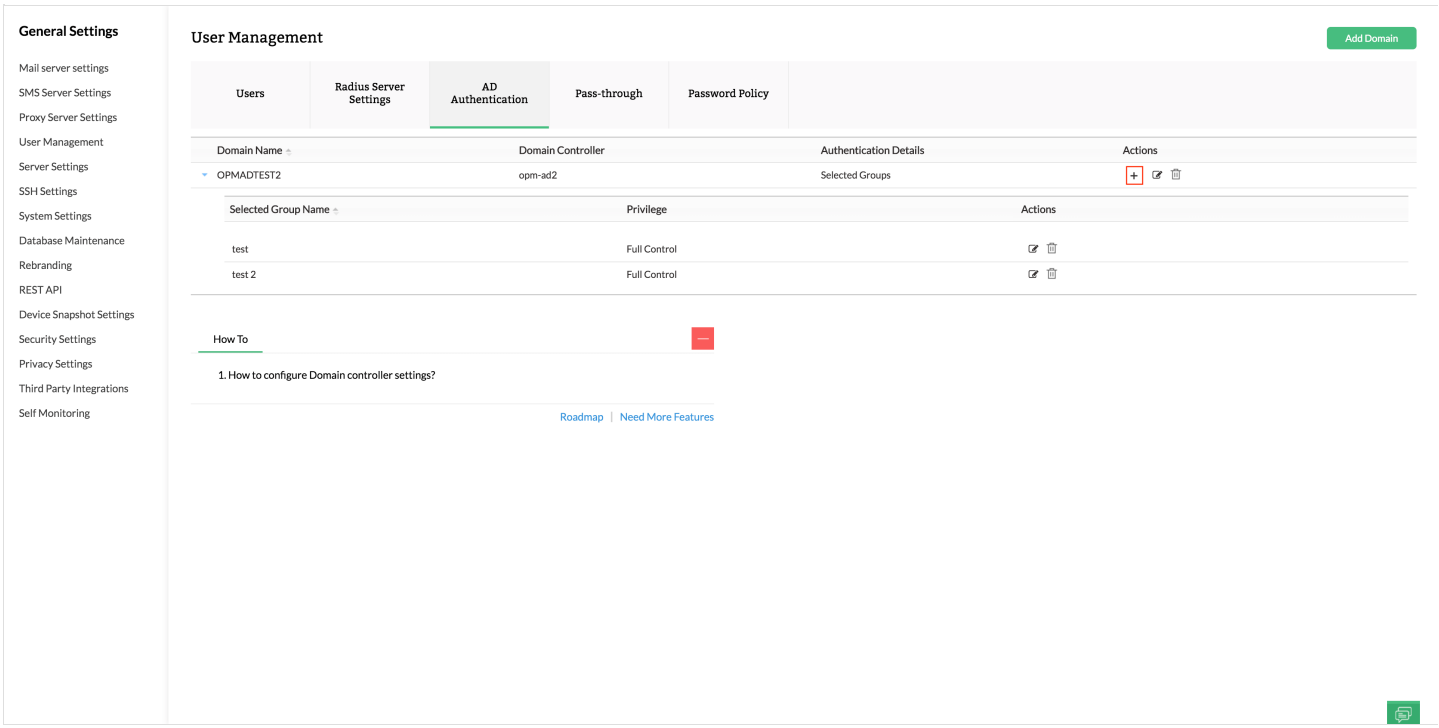
6. **Save** the settings.

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.

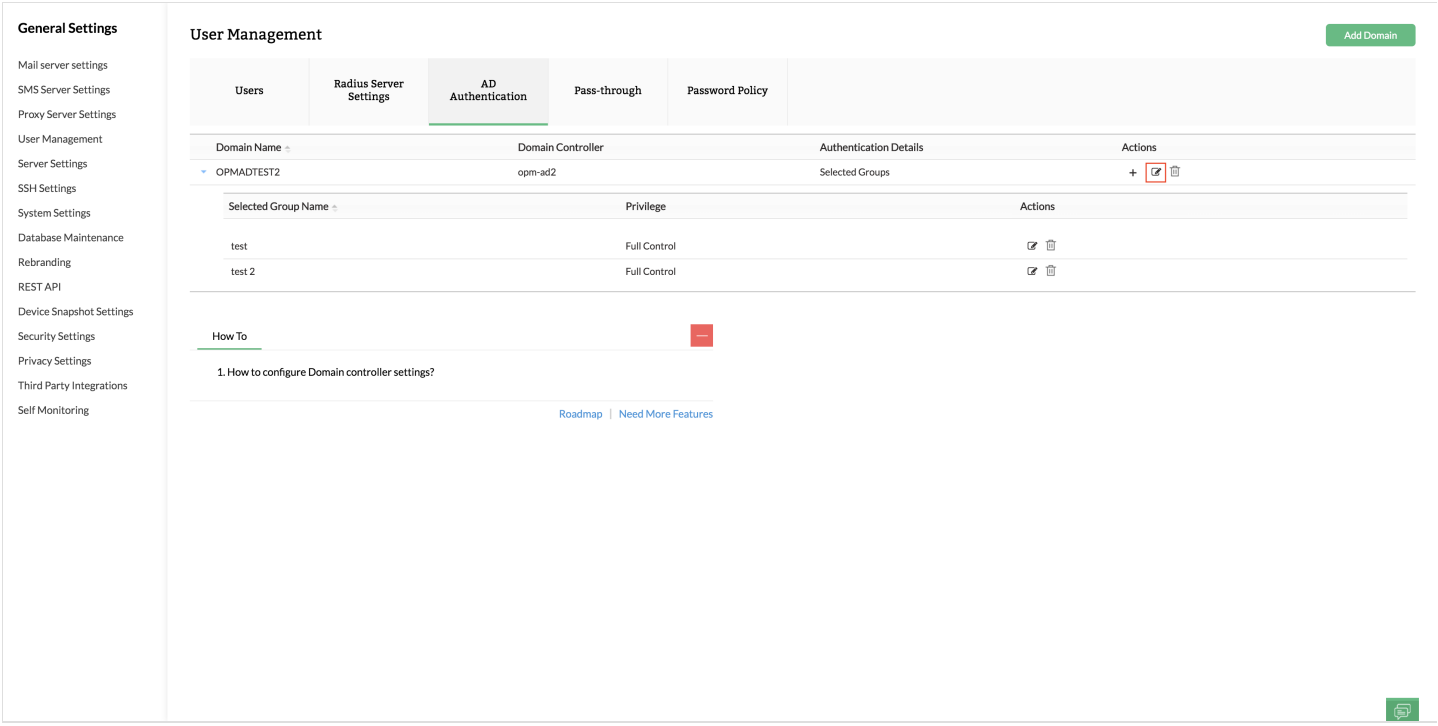
To add AD groups:

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



To edit timezone:

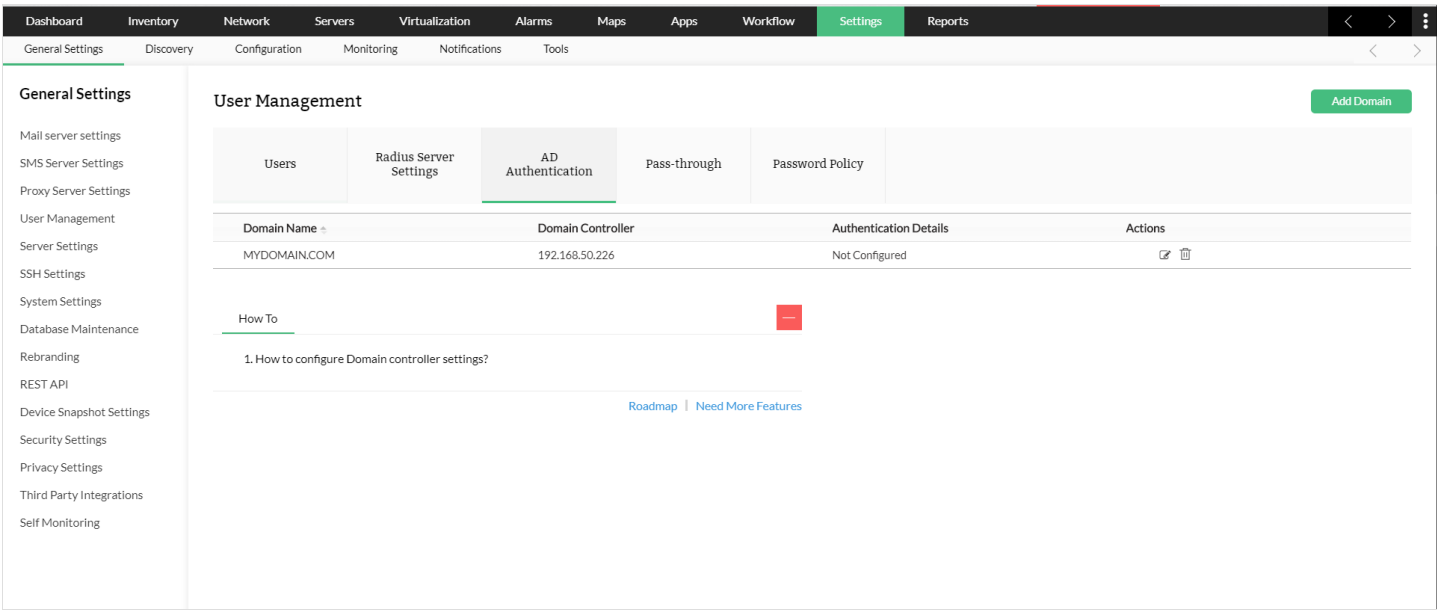
Select **Edit** under **Actions** for the domain you want to edit, change the timezone as per your requirement, and click **'Save'.**



To Edit/Delete AD groups:

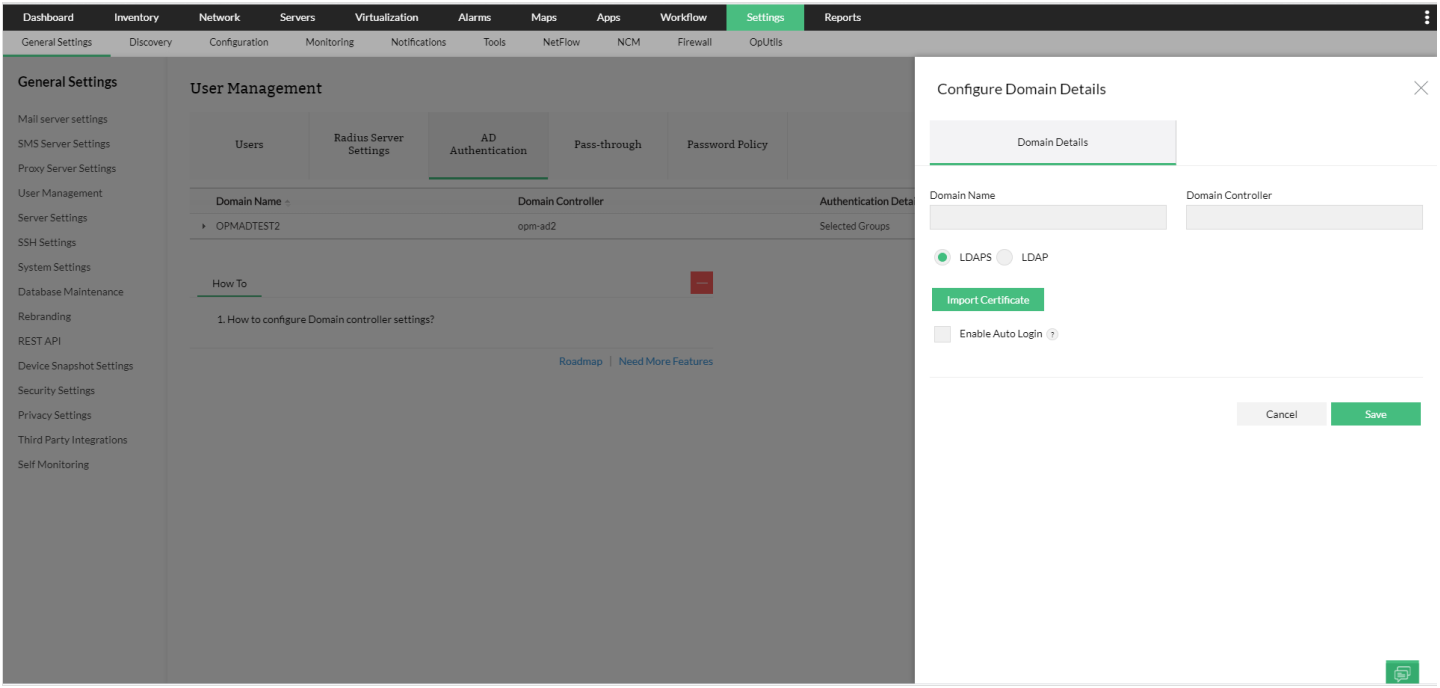
1. Click on the arrow mark next to the name of your domain to display all AD groups under it.

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.

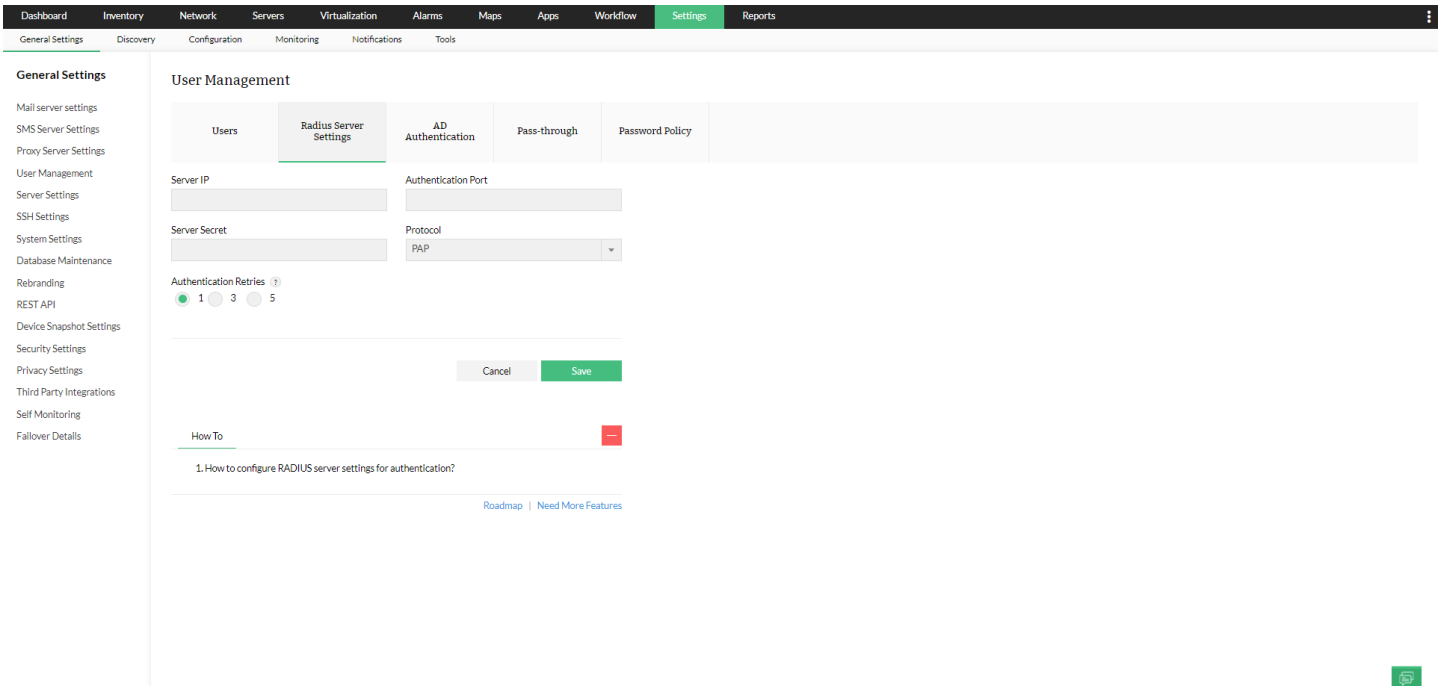
For AD Authentication, we support on-premise AD with LDAP query access to the domain controller in the network.

Radius Server Settings

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol. RADIUS is used to enable communication between a remote access server and a central server to authenticate and authorize dial-in users and grant them access to the required system or service.

How to Configure Radius Server Settings?

To configure radius server settings, go to **Settings** -> **General Settings** -> **User Management** and enter the required details:



1. **Server IP:** Enter the IP of the server where the radius server is running.
2. **Authentication Port:** Port in which the server is running it (Normally 1812).
3. **Server Secret:** Its the master password with which the details of the user configured in the radius server are retrieved.
4. **Protocol:** Select the desired protocol from the list - PAP/CHAP/MSCHAP/MSCHAP2. This should be the protocol that the radius server uses for communication.
5. **Authentications Retries:** Choose the amount of times that OPM should retry if there is a connection issue.
6. Click on '**Save**'.

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.)

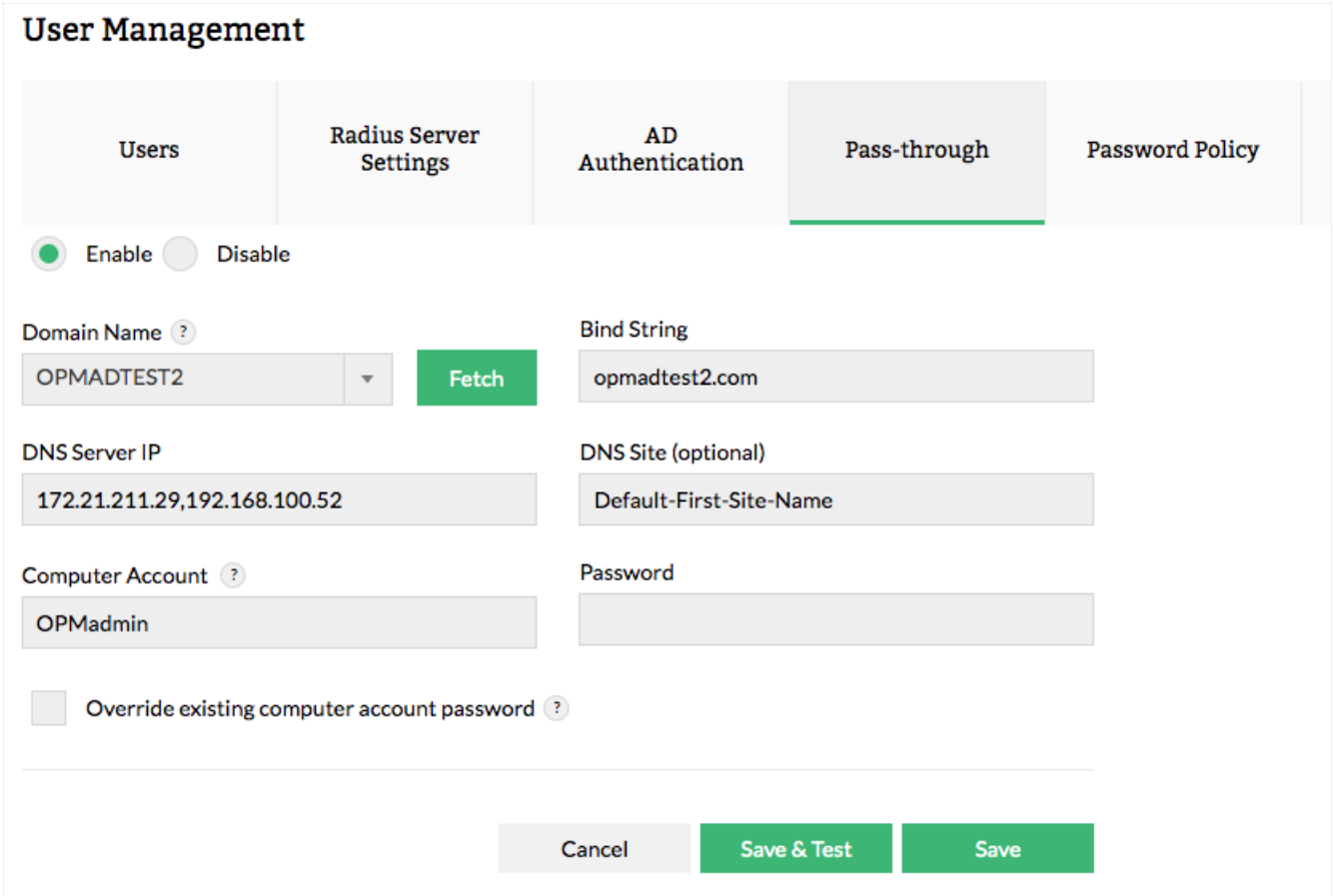
Configuring Passthrough Authentication in OpManager:

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

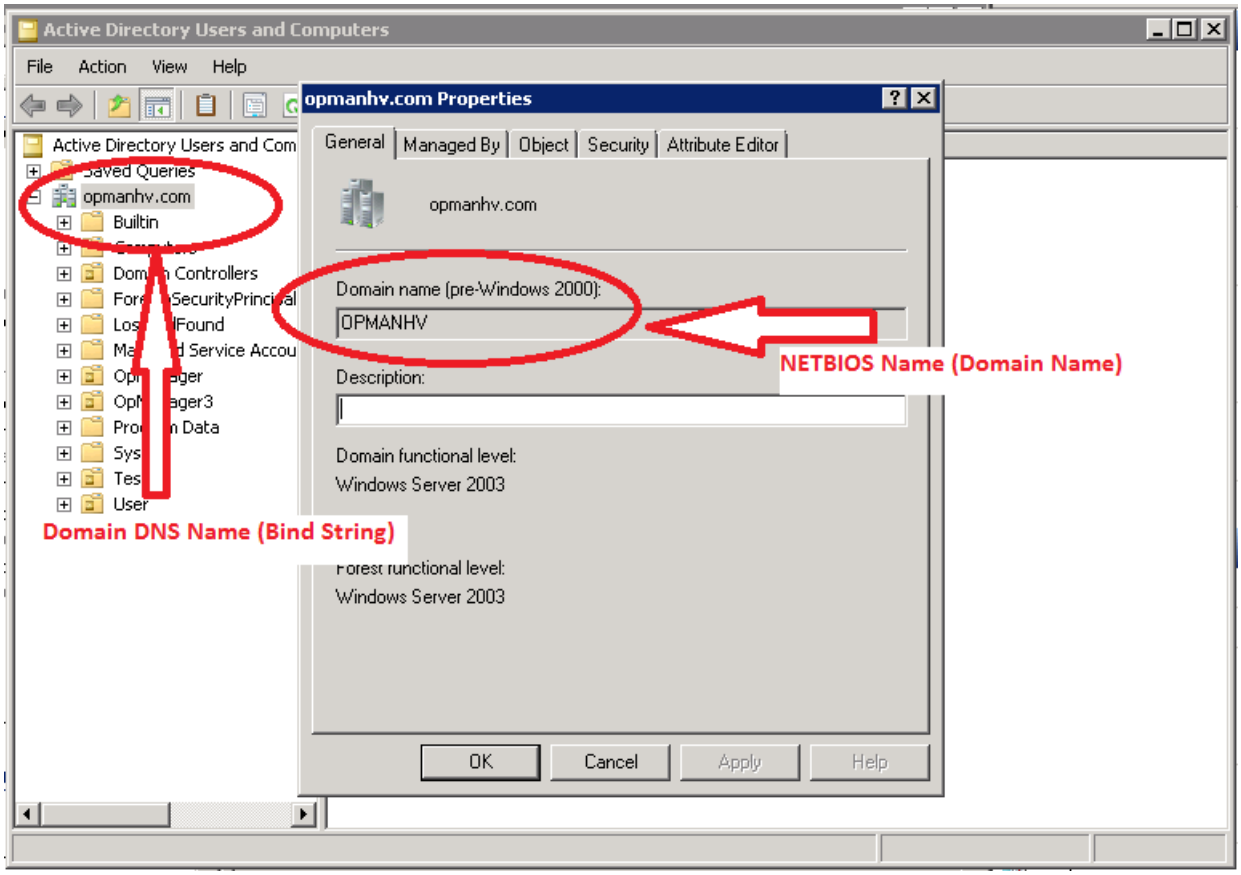
To manually configure Passthrough authentication, you'll need the following details:

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

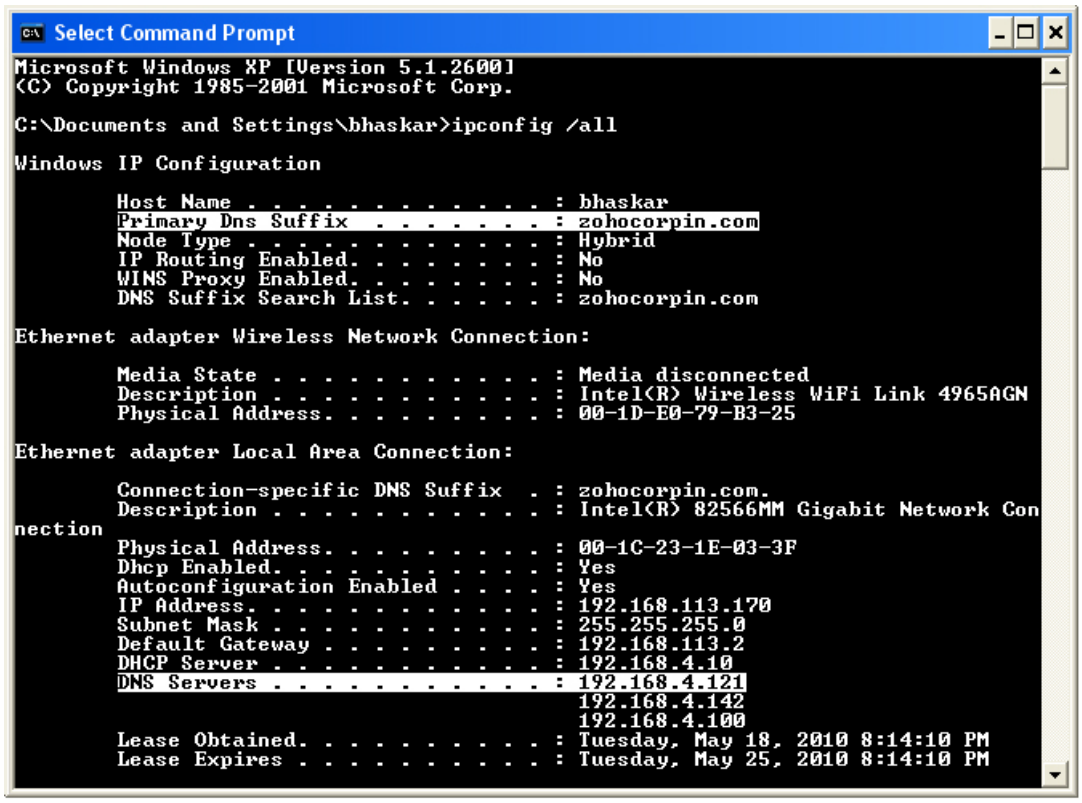
1 & 2 - Getting Domain DNS Name and NETBIOS Name:

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



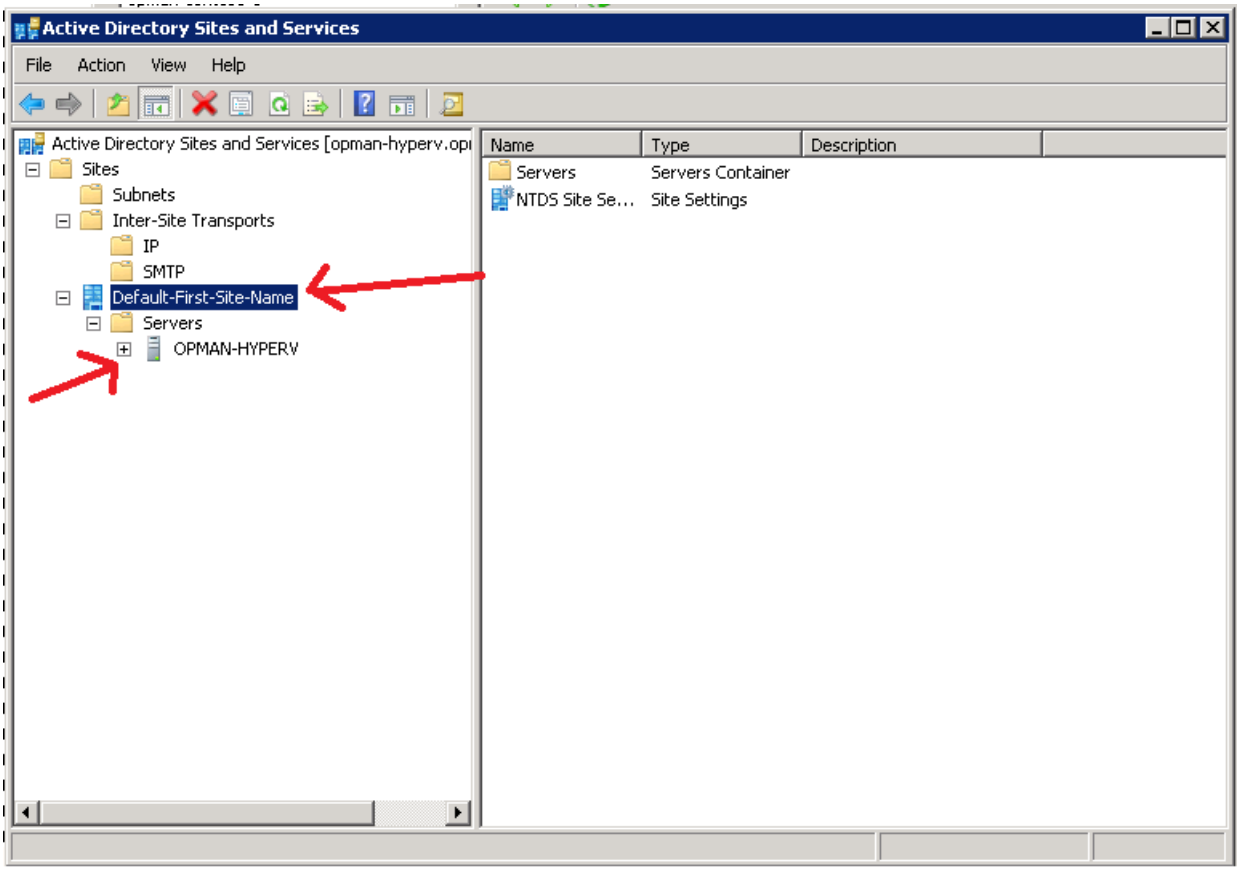
3 - Getting DNS Server IP:

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.

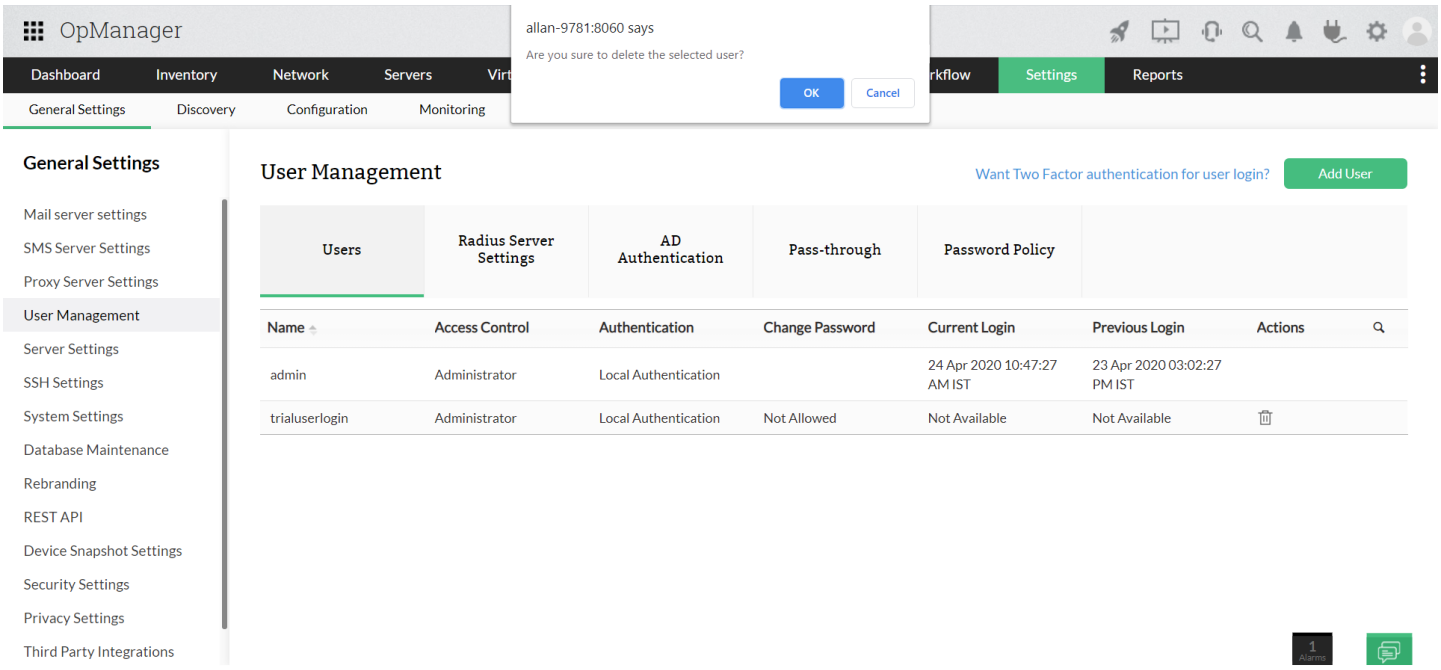
Log File:

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

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.



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:

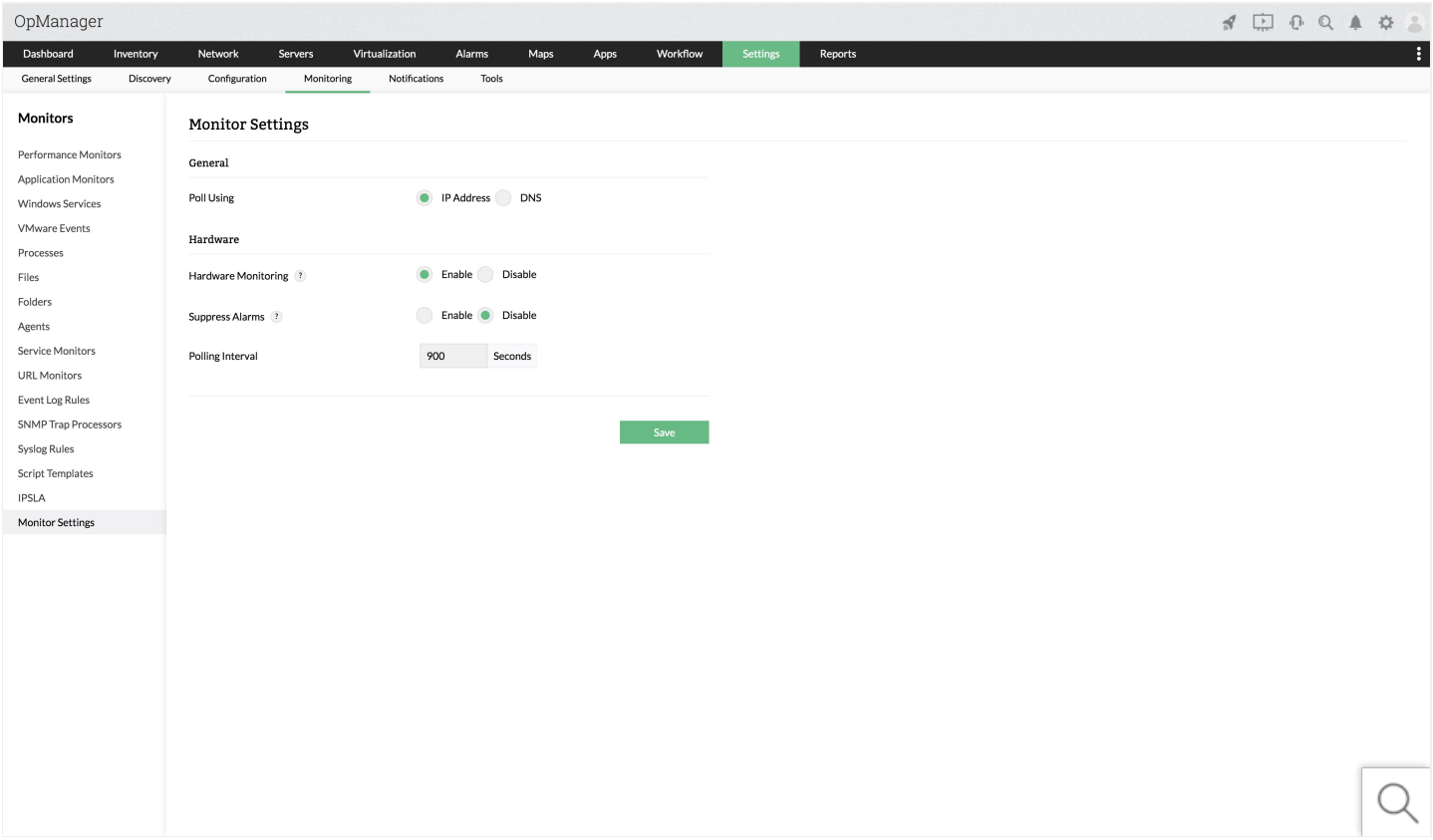
1. Go to the snapshot page of any device you wish to monitor.
2. Click the **Actions** button.
3. Now, from the list of resource monitors, select the CPU, Memory, and Disk Utilization monitors which has the protocol name as CLI against the monitor name.
4. Once done, click **Add**. The monitors are added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

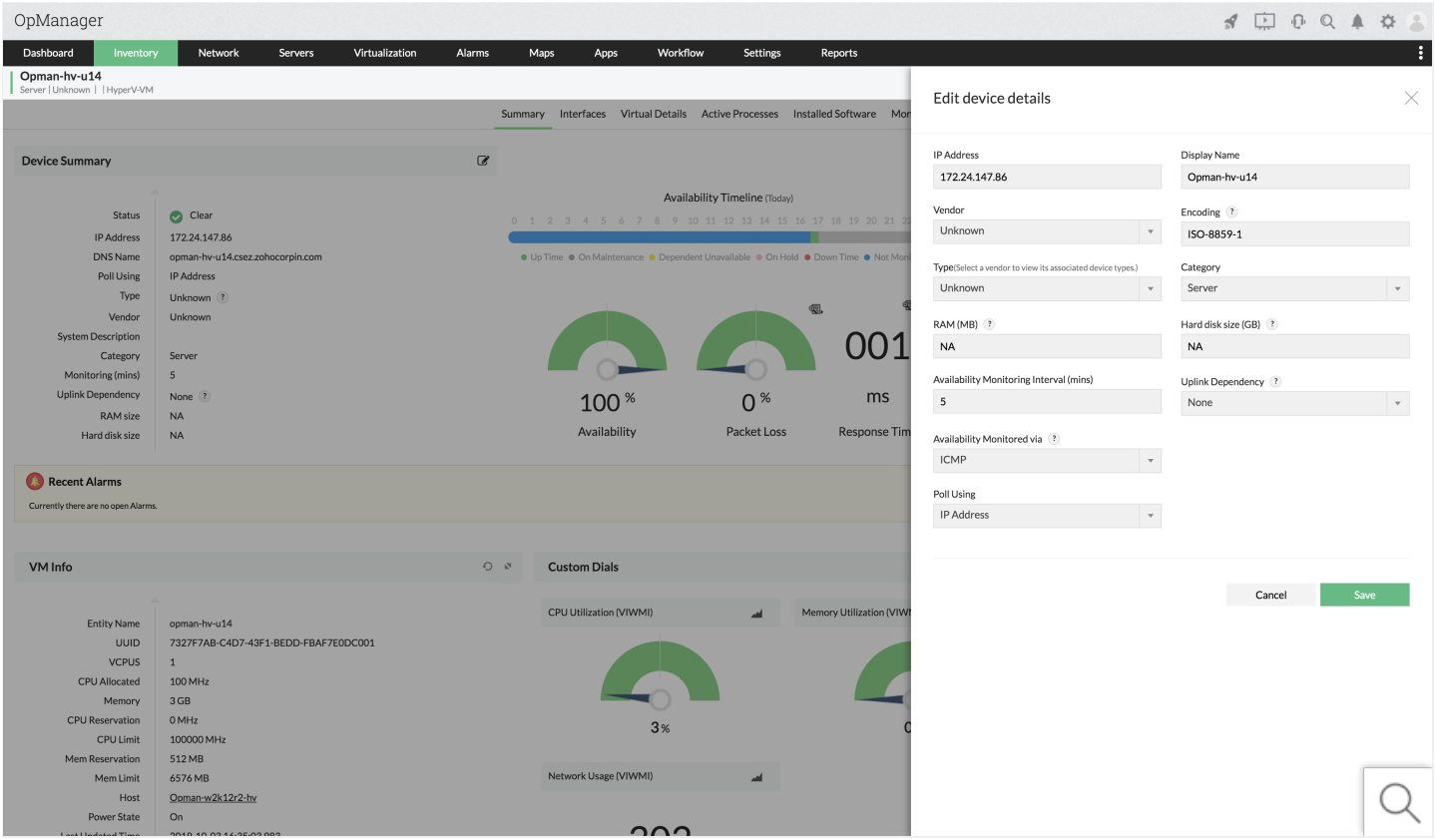


Note: Changes in the global setting apply only for devices that will be discovered in the future. The polling method of devices already discovered will not be affected in any way.

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, Partition Details
- **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.

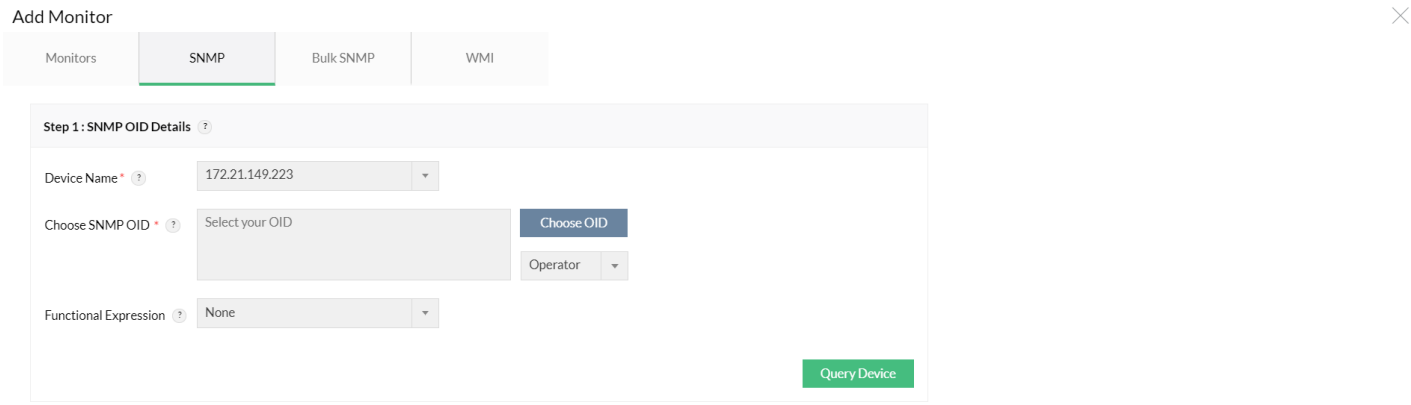
To add a custom monitor for a resource of a particular device type, the device template must be modified. The new monitor should be defined in the device template so that the monitor is associated for all devices of that type. Here are the steps.

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

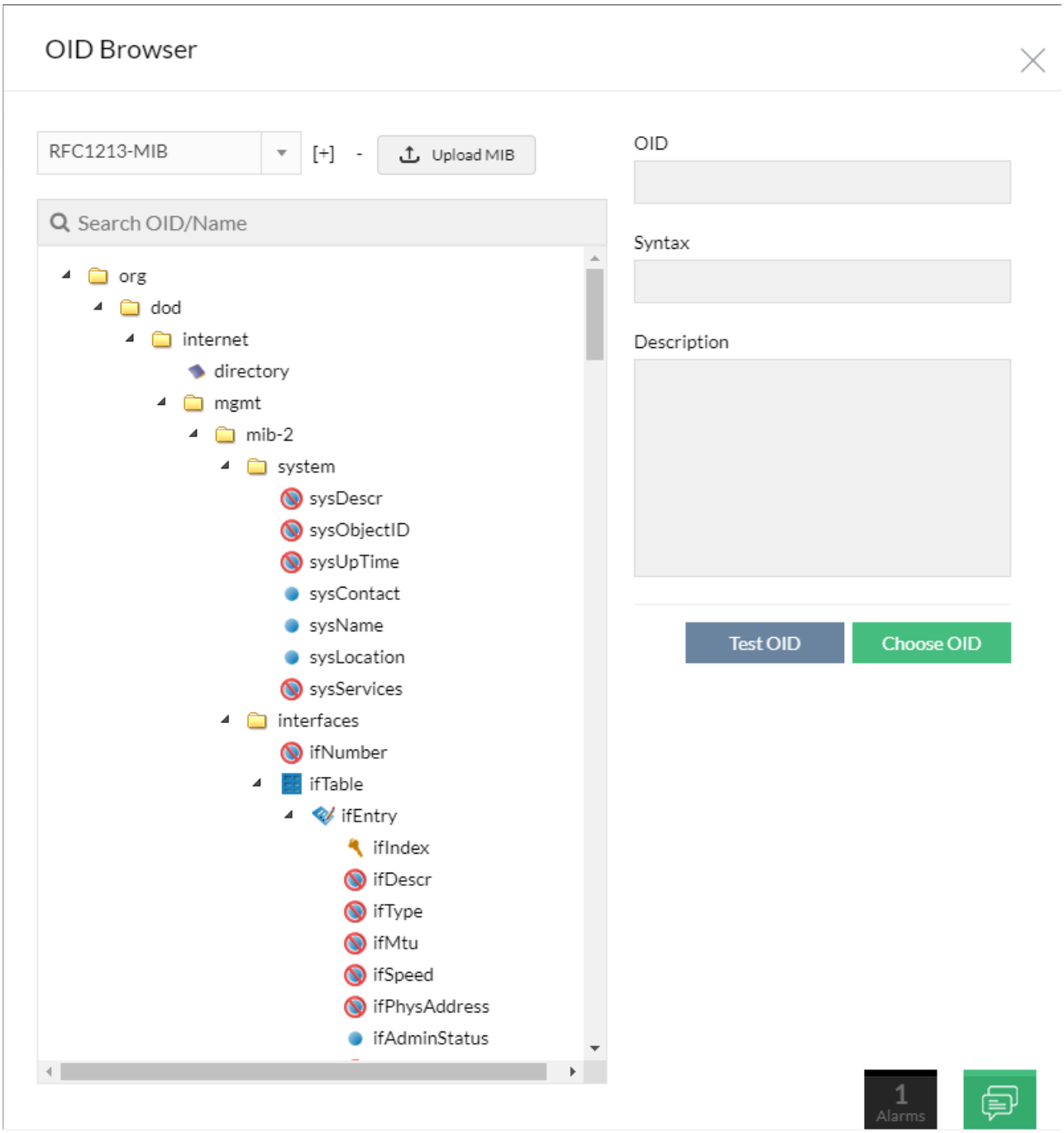
To add an SNMP monitor, you need to first provide the OID based on which OpManager will fetch data related to the required metric from a device.

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.

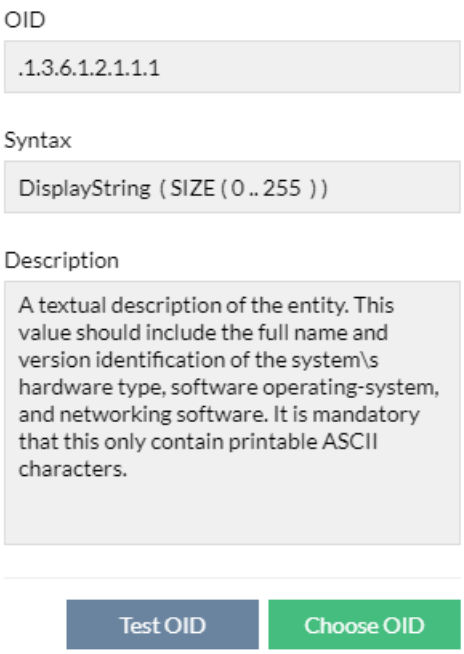
Step 2: Select OID

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:

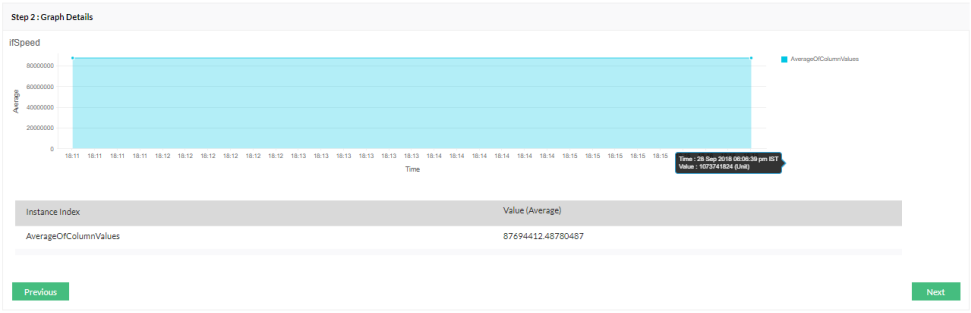
1. If more than one Multiple Instance OID is present in the expression, then it should be of the same parent node.
2. Monitor involving both Scalar and Multiple OIDs are not supported.
3. Monitor involving both String and Numeric OIDs are not supported.
4. You cannot use string monitors to create expressions.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

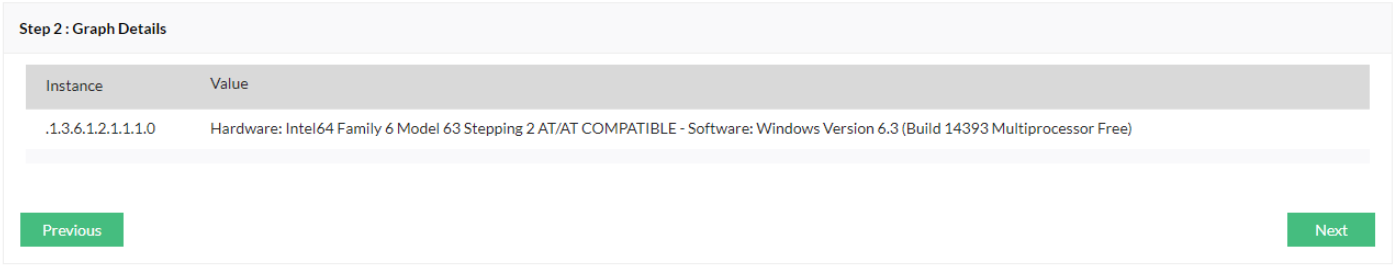
Object identifiers (OIDs) have both a type and a value. It is on this basis that they are classified into **Scalar Objects** and **Tabular Objects**. A **scalar object** is a managed object that always has a **single instance**, whereas, **tabular objects** have **multiple instances**. In both these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

Graph Details

i) Scalar Objects:

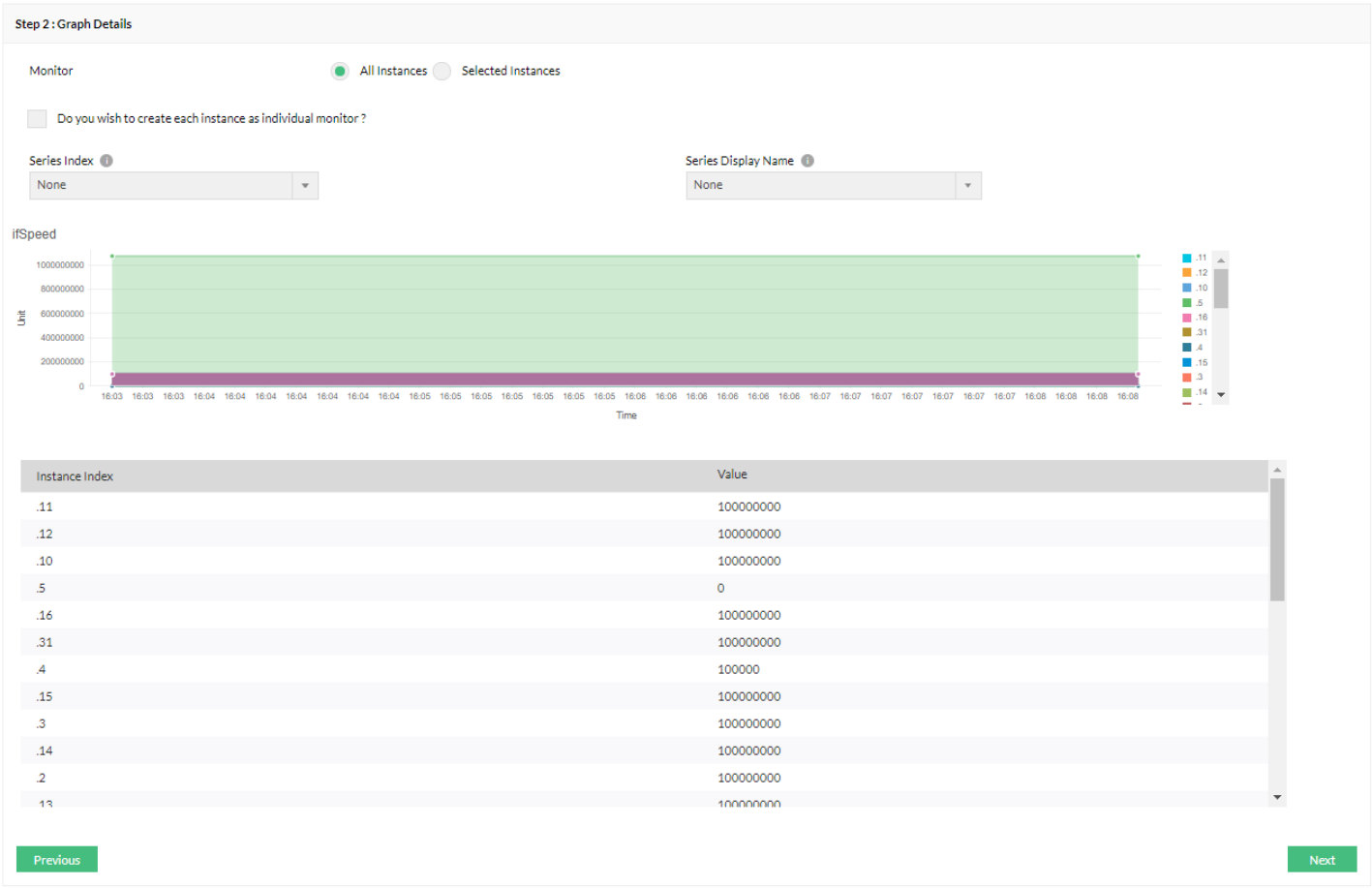
1. Scalar objects with a numerical output will display a table containing the instance and the value along with a graph.

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

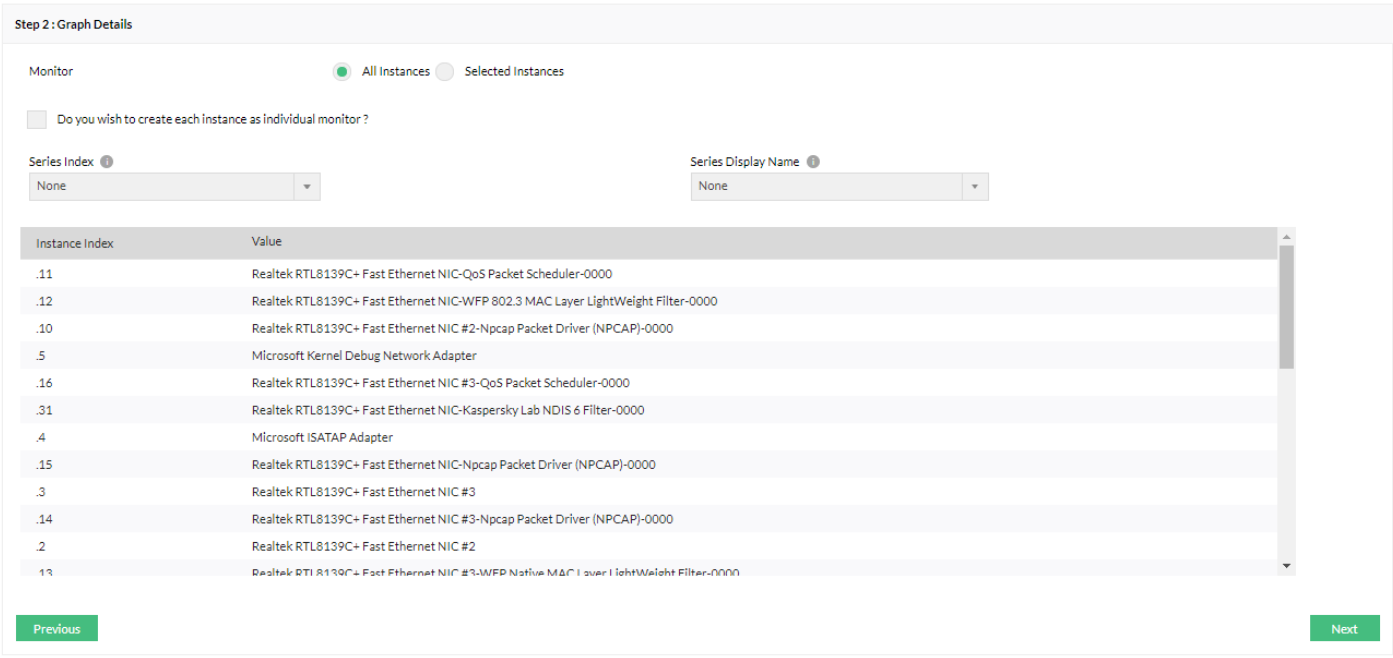


ii) Tabular Objects:

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

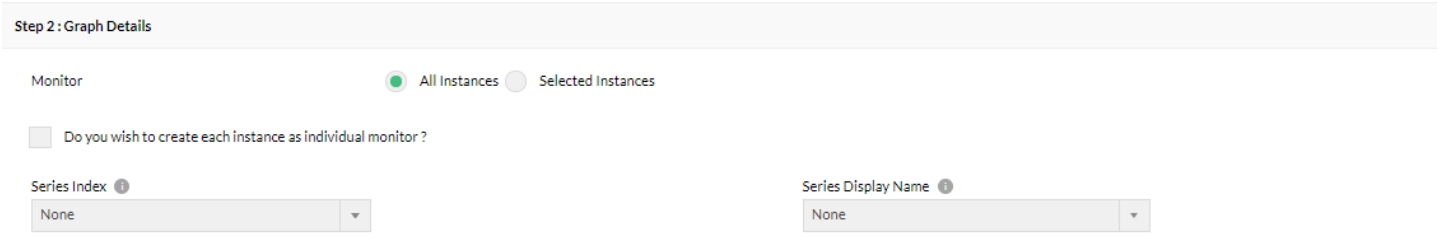


2. Tabular objects with a string output will only display the instance and the value.



Monitor Instances

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



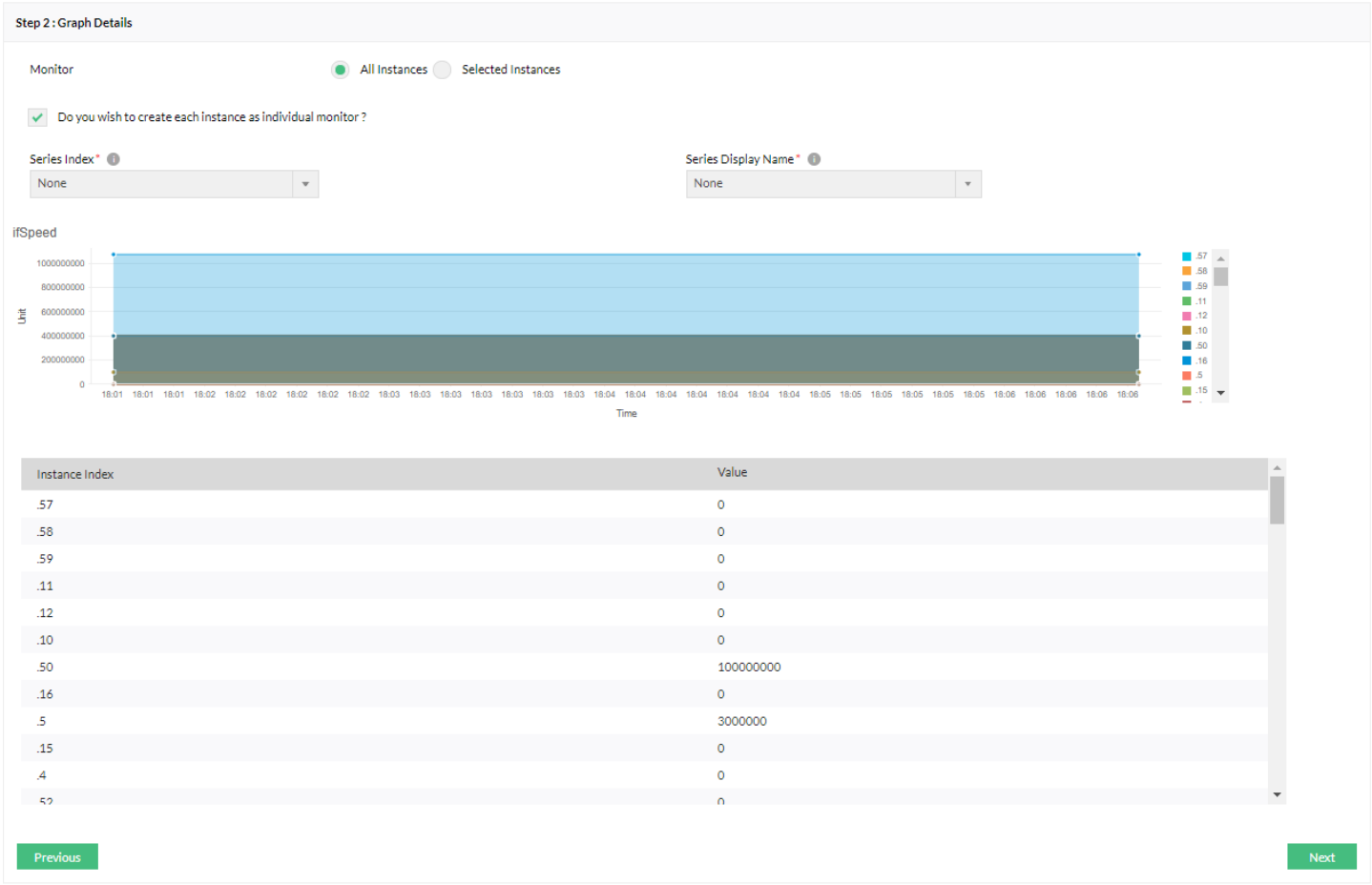
All Instances: A single SNMP monitor that monitors multiple instances will be created.

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.

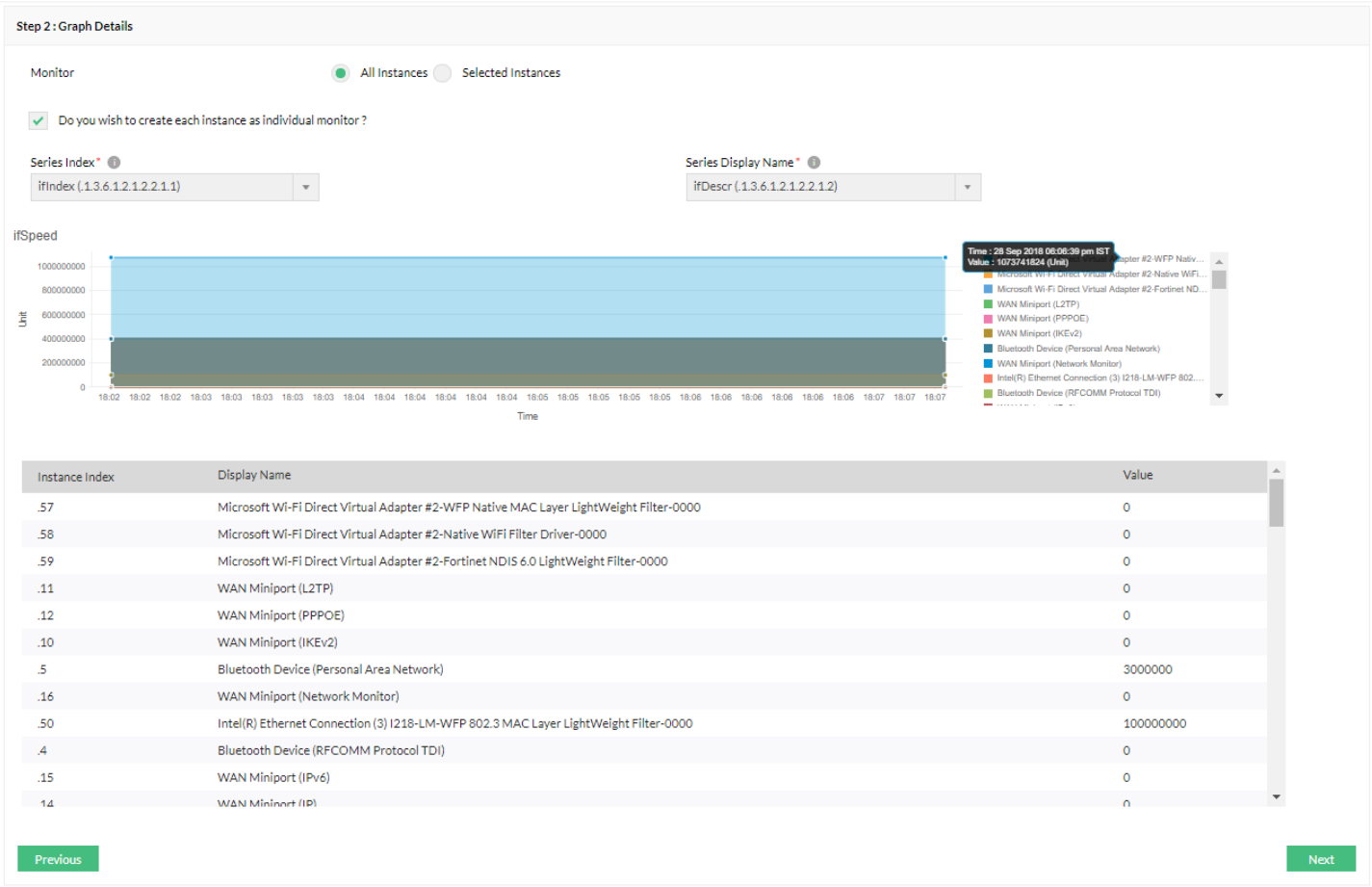
If you choose to select this option, it is mandatory that you provide inputs to the **Series Index** and the **Series Display Name** fields.



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.

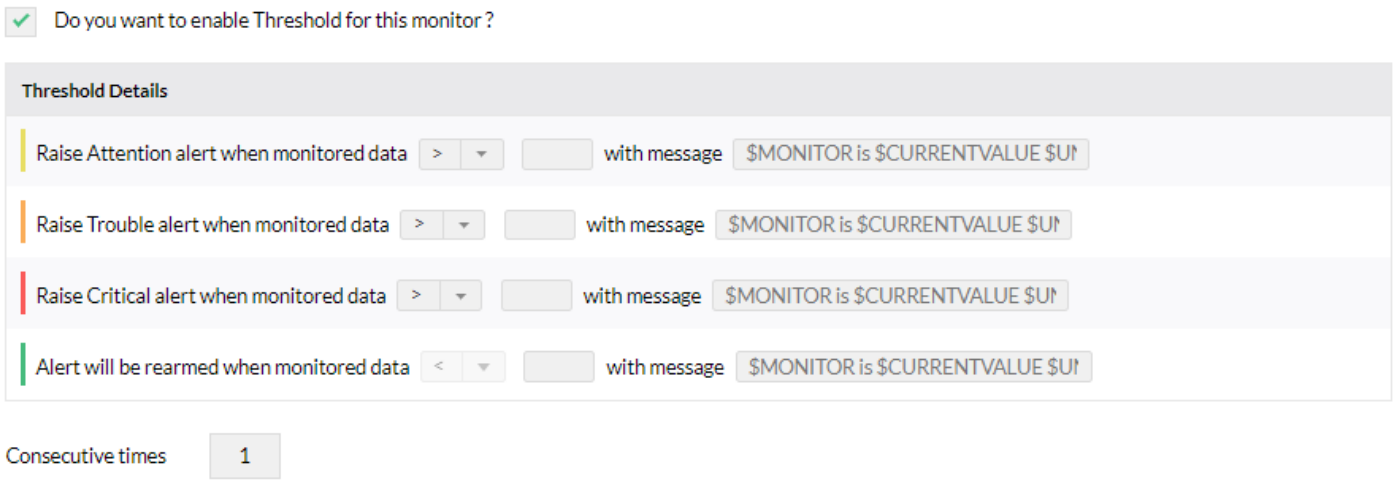
2. Interval (Mins): This value specifies the time interval in which you want to re-run the monitor to fetch the corresponding values.

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.

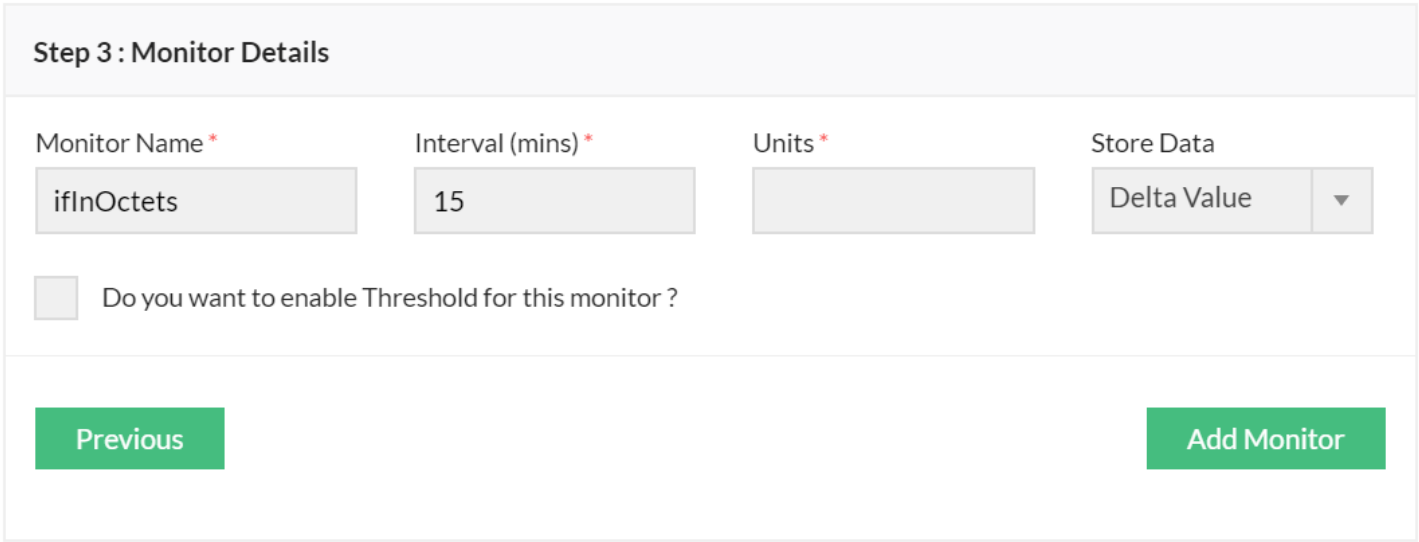
In the **Consecutive Times** field, enter the value of how many consecutive times the thresholds (Attention, Trouble and Critical) can be violated for an alert to be generated.

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.

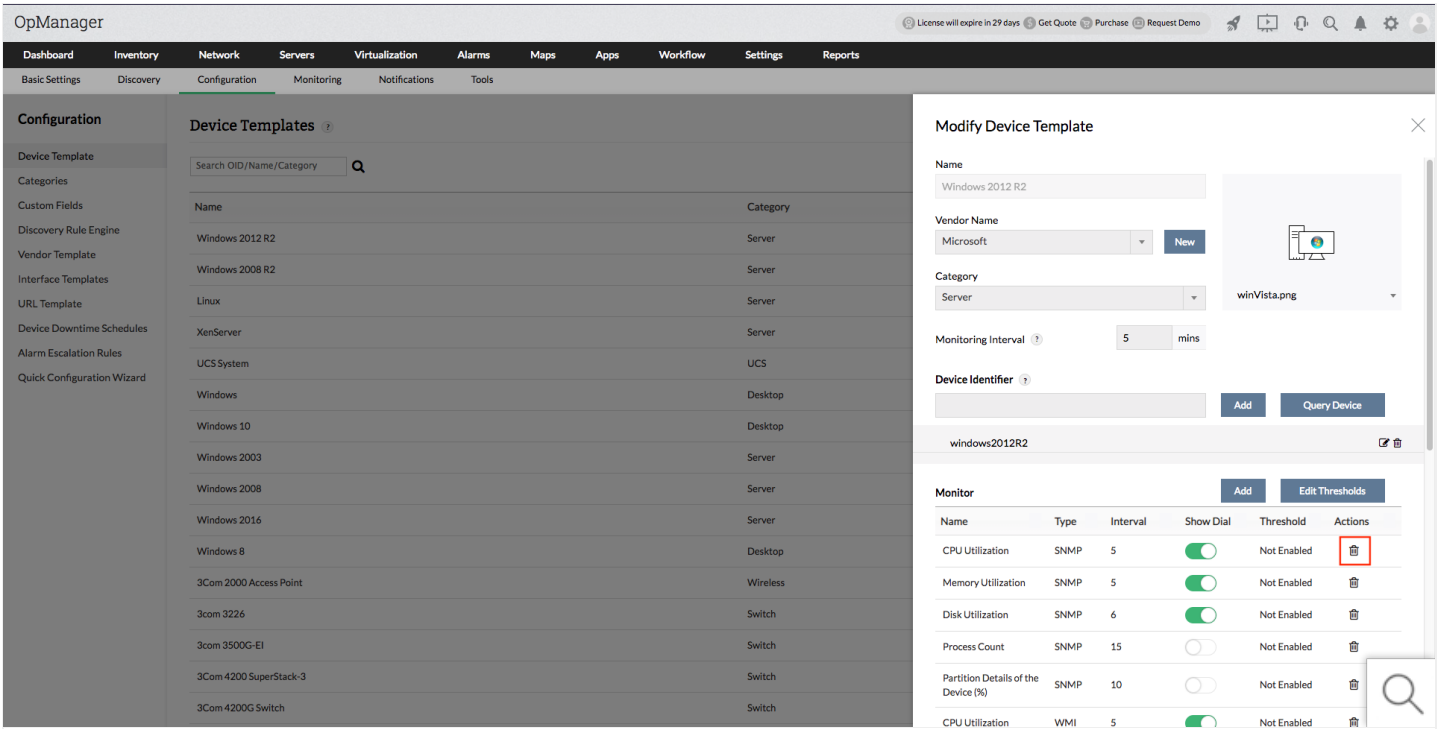
Counter Type OIDs

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.



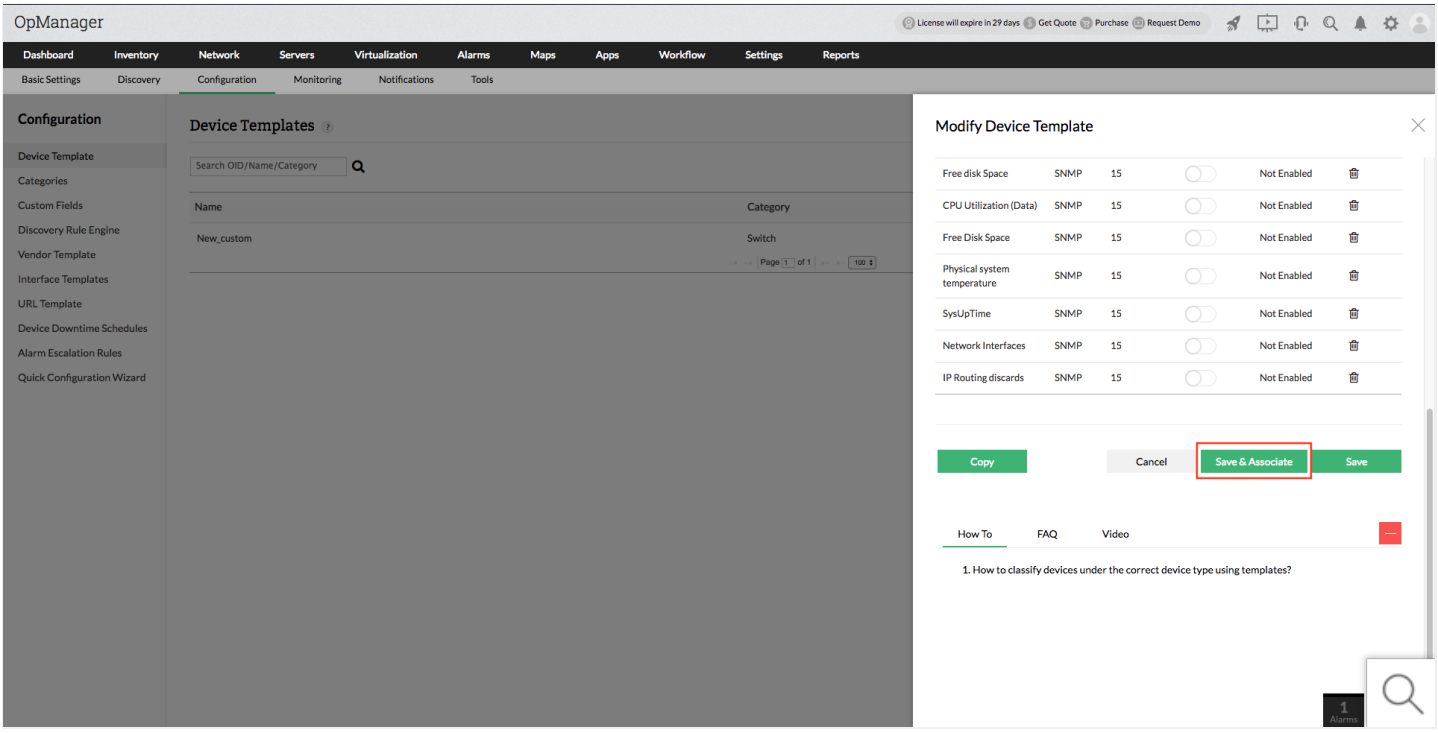
Deleting performance monitors

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'**.

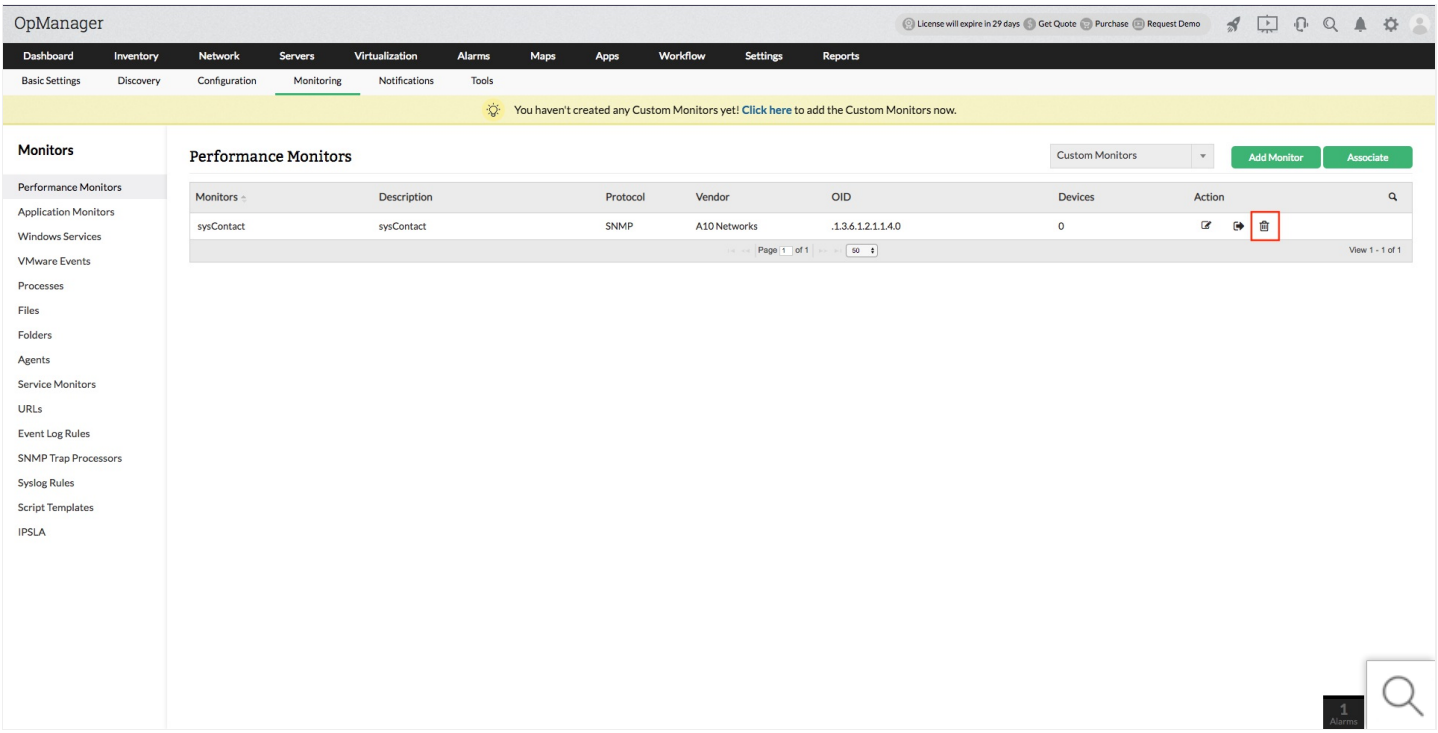
Deleting a monitor from this page is reflected instantly and the devices that will be associated with that template in the future, but it still remains in all the devices that have been already associated with that template. To apply the changes to all these devices, click on **'Save and Associate'**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



2. Deleting a monitor from Performance monitors page:

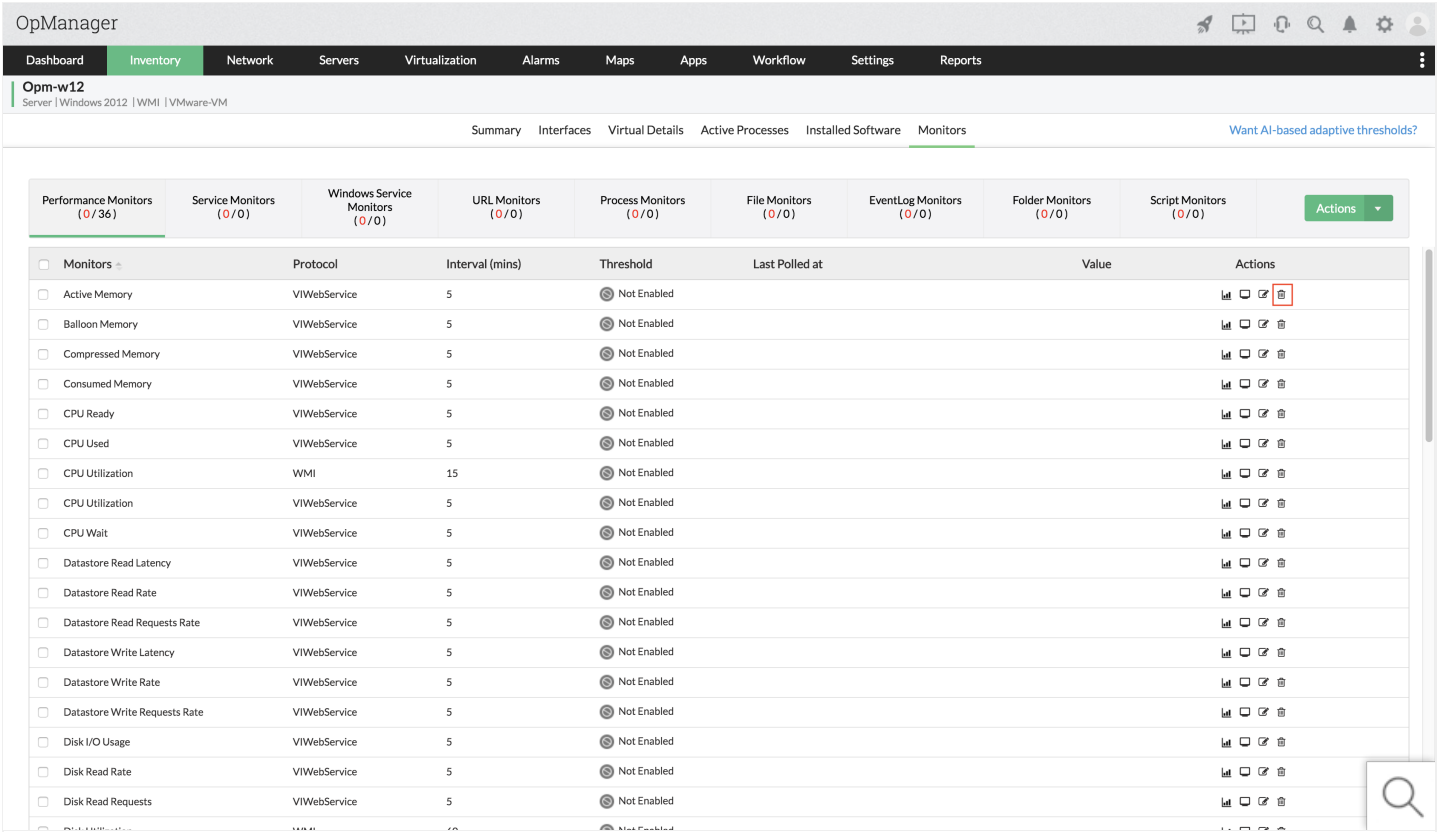
Only custom monitors created by the users can be deleted from this page.

- 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.



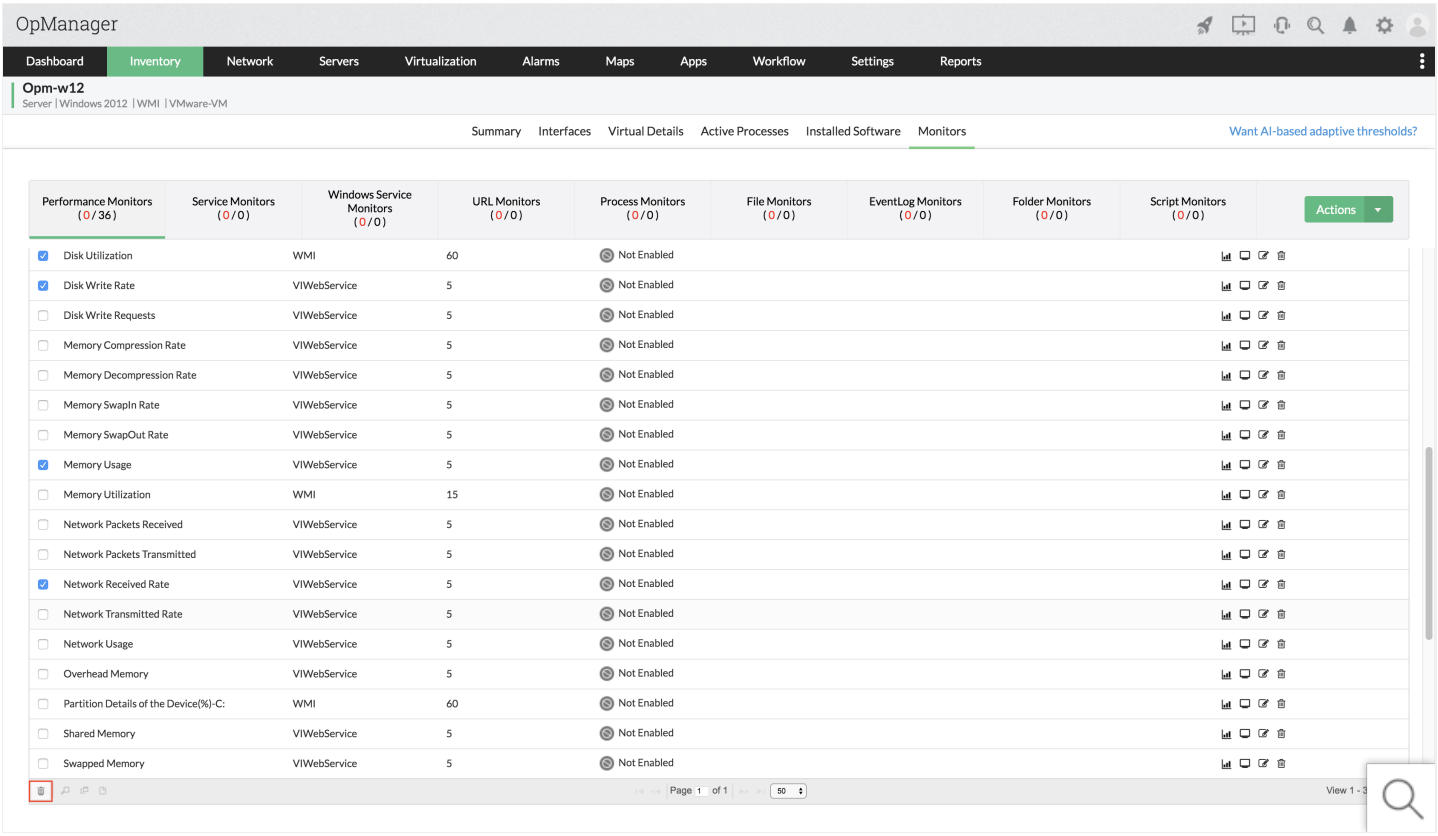
Deleting a custom monitor from here **removes it permanently from OpManager**, and from any device/device template that has this monitor configured already.

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	Alert	Custom Monitor	SNMP	Networking Device
Dell	CPU Utilization	CPU Utilization for Dell	SNMP	Switch
Dell	CPU Utilization	Monitors the CPU of DELL_Force10_S25N switch	SNMP	Switch

Dell	Memory Utilization	Monitors the Memory of DELL_Force10_S25N switch	SNMP	Switch
Dell	Memory Utilization	Memory Utilization for Dell	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
Microsoft	Memory Used in MB	Memory that is currently being used	WMI	Server / Desktop
Microsoft	Available Memory in %	Amount of memory available	WMI	Server / Desktop
Microsoft	Average Disk Latency	Average time taken in milliseconds for a complete disk (read + write + transfer) operaton	WMI	Server / Desktop
Microsoft	Average Disk Read Latency	Average time taken in milliseconds for a read operation from the disk	WMI	Server / Desktop
Microsoft	Average Disk Write Latency	Average time taken in milliseconds for a write operation from the disk	WMI	Server / Desktop
Microsoft	Cached Memory in MB	Amount of memory that contains cached data and code for rapid access by processes, drivers, and the operating system	WMI	Server / Desktop
Microsoft	Committed Memory in MB	This counter indicates the total amount of memory that has been committed for the exclusive use of any of the services or processes on Windows NT	WMI	Server / Desktop
Microsoft	CPU Interrupts per second	The numbers of interrupts the processor needs to respond to in a second	WMI	Server / Desktop
Microsoft	Disk Active Time in %	Percentage of time the disk is not idle	WMI	Server / Desktop
Microsoft	Disk Read Speed in kbps	The rate of data transfer from the disk during read operations, in kilobytes per second	WMI	Server / Desktop
Microsoft	Disk Speed in kbps	The rate of data transfer from the disk during read or write operations, in kilobytes per second	WMI	Server / Desktop
Microsoft	Disk Transfer Rate	The number of read and write operations completed on the disk in a second	WMI	Server / Desktop
Microsoft	Disk Write Speed in kbps	The rate of data transfer from the disk during write operations, in kilobytes per second	WMI	Server / Desktop
Microsoft	Disk Free Space in MB	Amount of free space available in the disk drive	WMI	Server / Desktop

Microsoft	Free Physical Memory in GB	Memory that does not contain any valuable data and that will be used first when processes, drivers, or the operating system need more memory	WMI	Server / Desktop
Microsoft	Handle count	The number of handles in the computer	WMI	Server / Desktop
Microsoft	IO Read and Write Rate	The rate of IO Read and Write operations performed on the server	WMI	Server / Desktop
Microsoft	IO Read and Write Speed in Kbps	The rate at which the process is reading and writing bytes for I/O operations. This property counts all I/O activity generated by the process to include file, network, and device I/Os	WMI	Server / Desktop
Microsoft	IO Read Rate	The rate of IO Read operations performed on the server	WMI	Server / Desktop
Microsoft	IO Read Speed in Kbps	The rate at which the process is reading bytes from I/O operations. This property counts all I/O activity generated by the process to include file, network, and device I/Os	WMI	Server / Desktop
Microsoft	IO Write Rate	The rate of IO Write operations performed on the server	WMI	Server / Desktop
Microsoft	IO Write Speed in Kbps	The rate at which the process is writing bytes to I/O operations. This property counts all I/O activity generated by the process to include file, network, and device I/Os	WMI	Server / Desktop
Microsoft	Number of Processes	Number of processes in the computer	WMI	Server / Desktop
Microsoft	Percent DPC Time	Percentage of time that the processor spent receiving and servicing deferred procedure calls during the sample interval	WMI	Server / Desktop
Microsoft	CPU Interrupts %	Percentage of time that the processor is spending on handling Interrupts	WMI	Server / Desktop
Microsoft	Nonpageable Pool Memory in MB	This provides an indication of how NT has divided up the physical memory resource. An uncontrolled increase in this value would be indicative of a memory leak in a Kernel-level service or driver	WMI	Server / Desktop
Microsoft	Pageable Pool Memory in MB	An uncontrolled increase in this counter, with the corresponding decrease in the available memory, would be indicative of a process taking more memory than it should and not giving it back	WMI	Server / Desktop

Microsoft	Run Queue Length of CPU	The Run Queue length of the CPU	WMI	Server / Desktop
Microsoft	System Calls per second	The rate of calls to Windows system service routines by all processes running on the computer	WMI	Server / Desktop
Microsoft	System UpTime in minutes	Number of minutes the computer has been running after it was last started	WMI	Server / Desktop
Microsoft	Thread Count	The number of threads in the computer	WMI	Server / Desktop
Microsoft	Total Virtual Memory in GB	Total Virtual memory Size in GB	WMI	Server / Desktop
Microsoft	Used Mounted Partition Space in GB	Monitoring the Used Mounted partitions space in GB using WMI	WMI	Server / Desktop
Microsoft	Mounted Partition of the Device(%)	Monitoring the usage in each Mounted Partition of the device using WMI	WMI	Server / Desktop
Microsoft	Free Mounted Partition Space in GB	Monitoring the Free Mounted partitions space in GB using WMI	WMI	Server / Desktop
Microsoft	Used Virtual Memory in GB	Amount of Virtual memory currently used in GB	WMI	Server / Desktop
Microsoft	Used Virtual Memory in %	Percent of Virtual memory currently used	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
Nutanix (Cluster)	IO Bandwidth	Data transferred from Cluster (in KB/second)	Prism API	Server
Nutanix (Cluster)	CPU Utilization	CPU Usage (%) of cluster as reported by hypervisor	Prism API	Server
Nutanix (Cluster)	Memory Utilization	Memory Usage (%) of cluster as reported by hypervisor	Prism API	Server
Nutanix (Cluster)	Read IO Bandwidth	Read data transferred from cluster (in KB/second)	Prism API	Server
Nutanix (Cluster)	Write IO Bandwidth	Write data transferred from cluster (in KB/second)	Prism API	Server
Nutanix (Cluster)	Number Of IOPS	Number of I/O operations per second from cluster	Prism API	Server
Nutanix (Cluster)	IO Latency	Average latency of cluster in microseconds	Prism API	Server
Nutanix (Cluster)	Content cache physical memory usage	Real memory (in Megabytes) used to cache data by the content cache for cluster	Prism API	Server

Nutanix (Cluster)	Content cache logical memory Usage	Logical memory (in Megabytes) used to cache data without deduplication by the cluster	Prism API	Server
Nutanix (Cluster)	Storage usage	Percent of storage used by the cluster	Prism API	Server
Nutanix (Host)	IO Bandwidth	Data transferred per second in KB/second from hypervisor	Prism API	Server
Nutanix (Host)	CPU Utilization	Percent of CPU used by the hypervisor	Prism API	Server
Nutanix (Host)	Memory Utilization	Percent of memory used by the hypervisor	Prism API	Server
Nutanix (Host)	Content cache physical memory Usage	Real memory (in Megabytes) used to cache data by the content cache for hypervisor	Prism API	Server
Nutanix (Host)	Content cache logical memory Usage	Logical memory (in Megabytes) used to cache data without deduplication by the hypervisor	Prism API	Server
Nutanix (Host)	Write IO Bandwidth	Write data transferred per second in KB/second from hypervisor	Prism API	Server
Nutanix (Host)	Read IO Bandwidth	Read data transferred per second in KB/second from hypervisor	Prism API	Server
Nutanix (Host)	Storage Used	Percent of storage used by the hypervisor	Prism API	Server
Nutanix (Host)	Read IOPS	Input/Output read operations per second from hypervisor	Prism API	Server
Nutanix (Host)	Write IOPS	Input/Output write operations per second from hypervisor	Prism API	Server
Nutanix (Host)	Number Of IOPS	Input/Output operations per second from hypervisor	Prism API	Server
Nutanix (Host)	Average IO Latency	Average latency of host in microseconds	Prism API	Server
Nutanix (VM)	IO Bandwidth	I/O bandwidth in KBps used by Controller VM	Prism API	Server
Nutanix (VM)	CPU Utilization	Percent of allocated CPU capacity currently being used by VM	Prism API	Server
Nutanix (VM)	Memory Utilization	Percent of allocated memory capacity currently being used by VM	Prism API	Server
Nutanix (VM)	Read IO Bandwidth	Read I/O speed in terms of KBps	Prism API	Server
Nutanix (VM)	Write IO Bandwidth	Write I/O speed in terms of KBps	Prism API	Server
Nutanix (VM)	Read IOPS	Number of Read I/O operations per second for Controller VM	Prism API	Server
Nutanix (VM)	Write IOPS	Number of Write I/O operations per second for Controller VM	Prism API	Server

Nutanix (VM)	Average Controller IO Latency	Average I/O latency of controller VM in microseconds	Prism API	Server
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.
6. You can also add a WMI custom monitor for a single device, by navigating to the device's Snapshot page and clicking on **Monitors tab ? Actions ? Add WMI monitor.**

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, go to **Settings ? Monitoring ? Service Monitors.** Select the required service and enable **'Scan during discovery',** and click **'Save'.**

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 of a device ? Monitors ? Service Monitors.** You can see the list of services managed in the device (if any), with their status and current response time.
- You can also click on 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 N number of times consecutively.
- Go to the **Device Snapshot ? Monitors ? Service Monitors,** and click the Edit icon against the service on which you wish to configure the threshold or to modify the consecutive times condition.

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

To start monitoring a TCP service in OpManager:

1. Go to **Settings ? Monitoring ? Service Monitors ? 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 **'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.

Adding a monitor from the Device Snapshot Page

1. Navigate to the Snapshot page of the device you wish to add the monitor to, and click on **Monitors ? Service Monitors.**
2. Click **Add Monitor,** and provide the necessary details - **the service name, port number and the timeout.**
3. You can test if the provided details are correct by using the **'Test Service'** option.
4. Also, mention the number of polls before OpManager raises an alert for that service monitor.
5. Finally, choose if you want to scan the mentioned port during discovery of new devices by toggling the **'Scan during Discovery?'** option. If this option is enabled, any device that is discovered in the future with this service/port combination will be automatically associated with this monitor.
6. Once you have provided all these details, click **'Save'** to associate the monitor to the device.

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

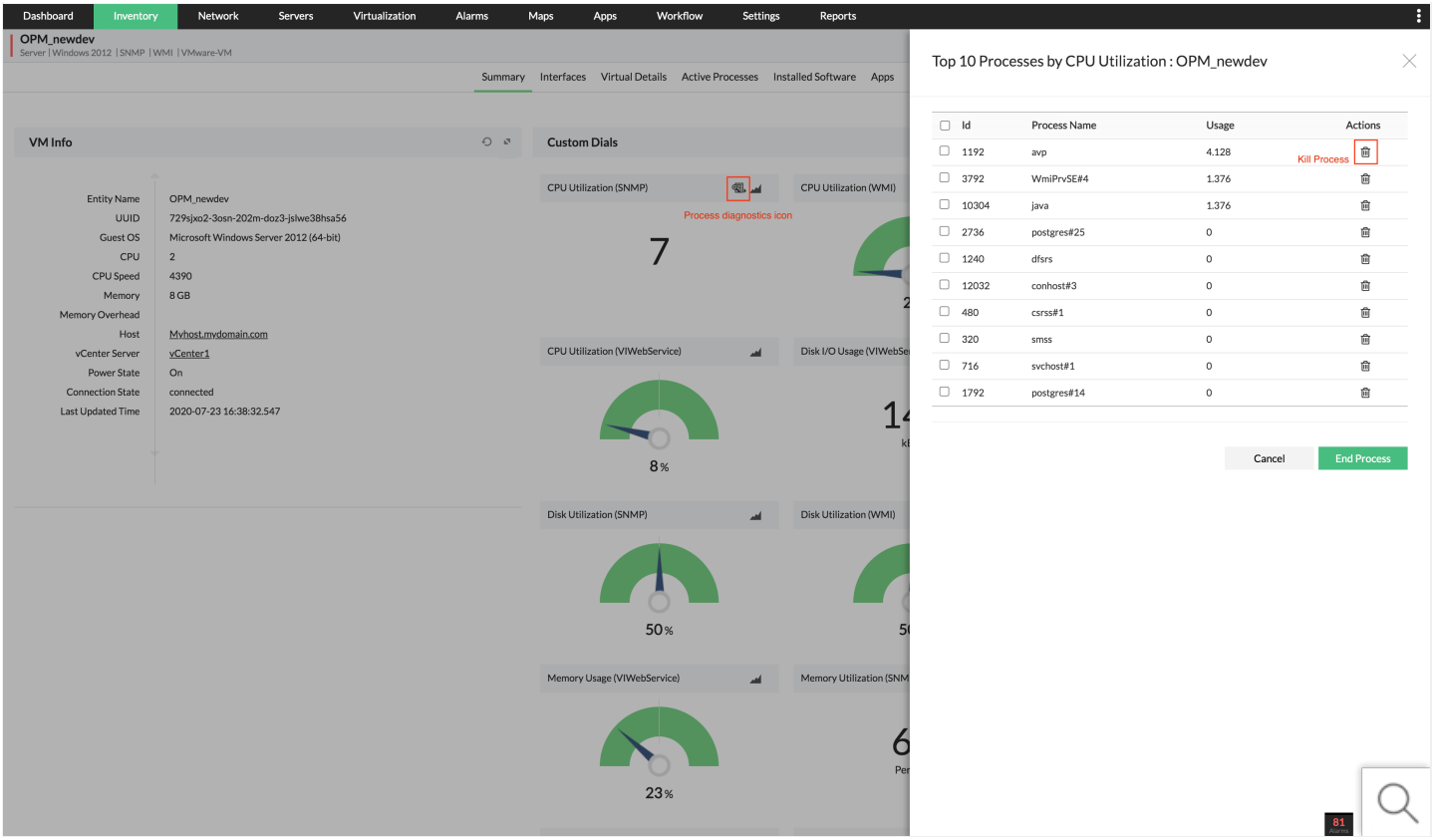
OpManager provides you the information on the processes that are currently running on the managed device. For this, OpManager uses the protocol of the default credential of that device (SNMP / WMI / CLI).

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/processes that needs to be converted into template(s).
3. **Protocol**: Select the relevant protocol to access the device.
4. Select the relevant credential from the drop-down by clicking on the **Credential** radio button or click **Associated username password** to associate the associated 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/processes.
7. From here, you can either choose to just save the template, or immediately associate it to devices. To associate it to devices right away, click **'Save and Associate'.** Select the devices you wish to monitor in the next window, and click 'Save'.
8. Else, if you just want to save the process template for now, click **Save.**

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 .

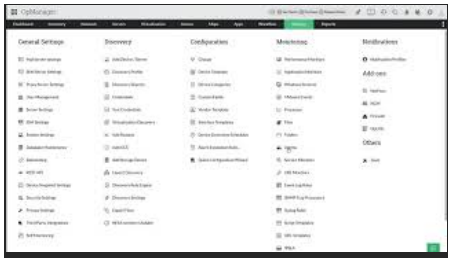
Follow the steps given below to add script templates

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.

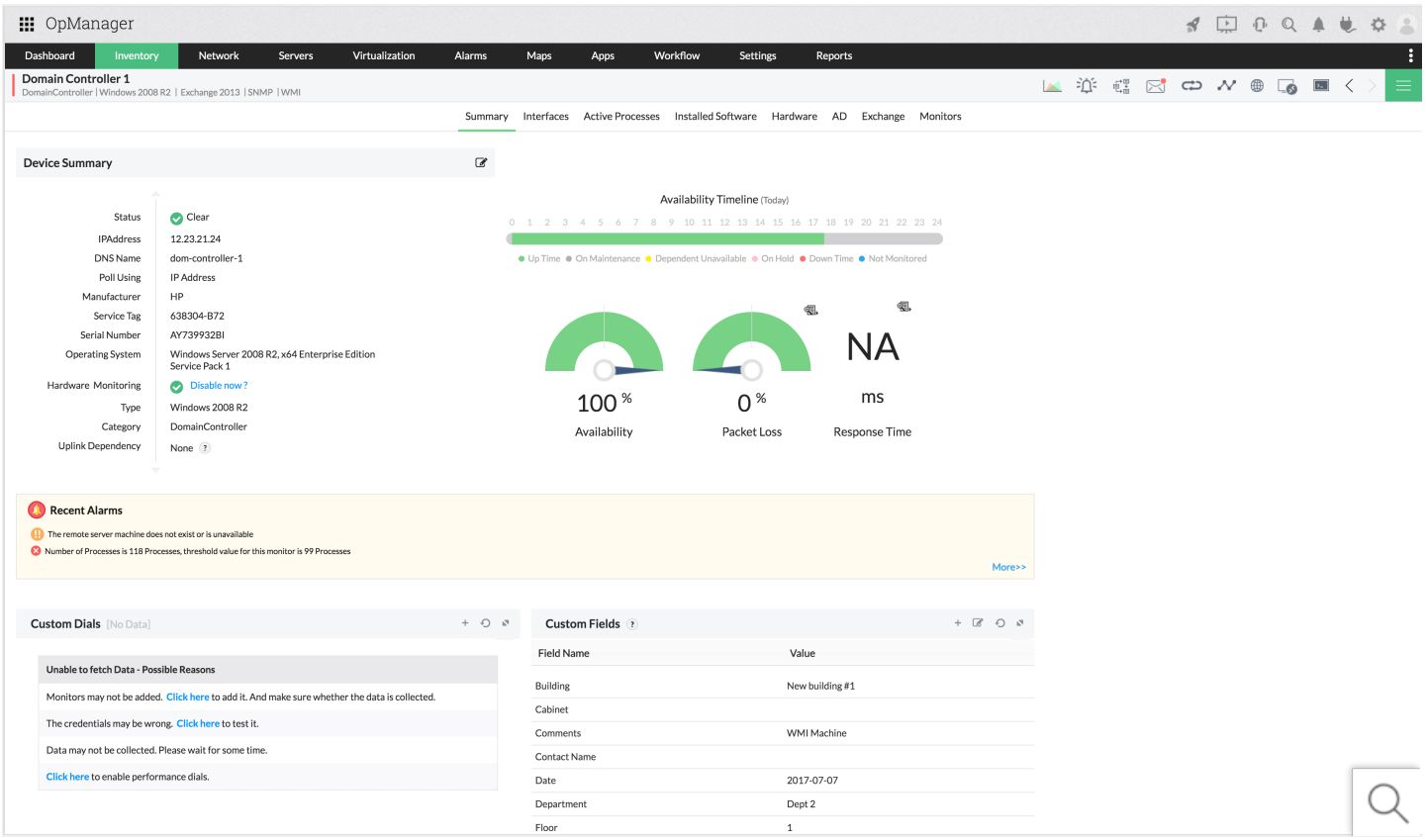
1. Go to **Settings ? Monitoring ? Folders.**
2. Click **Associate**
3. Selecte the required Template from the drop-down
4. Select the devices for which you want to apply this template and move them to the right.
5. Click on **Associate** button at the bottom of the column to associate the template to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

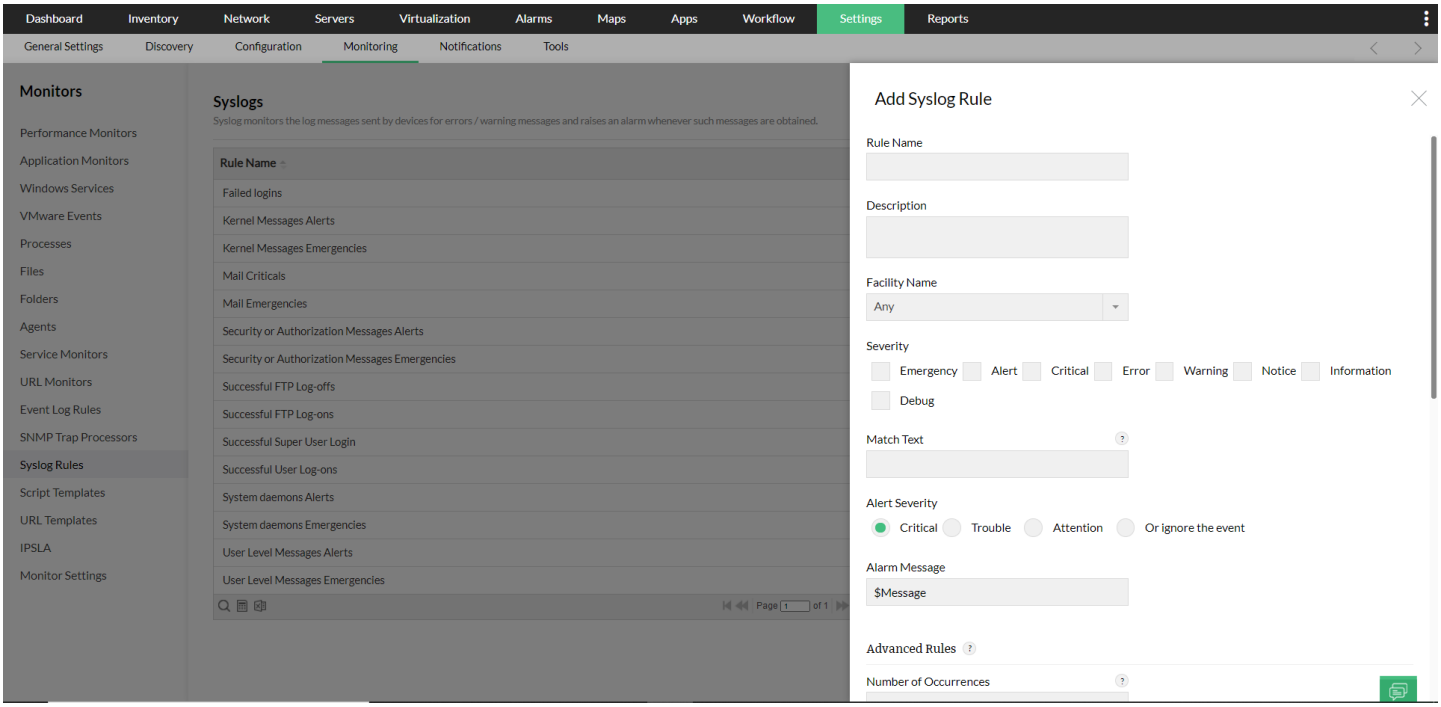
1. Go to the device snapshot page.
2. Click **Monitors ? URL Monitors**.
3. Click the **Actions** button and select **'Add monitor'.**
4. Configure all the values for the URL Monitor and Click **'Save'**.

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.

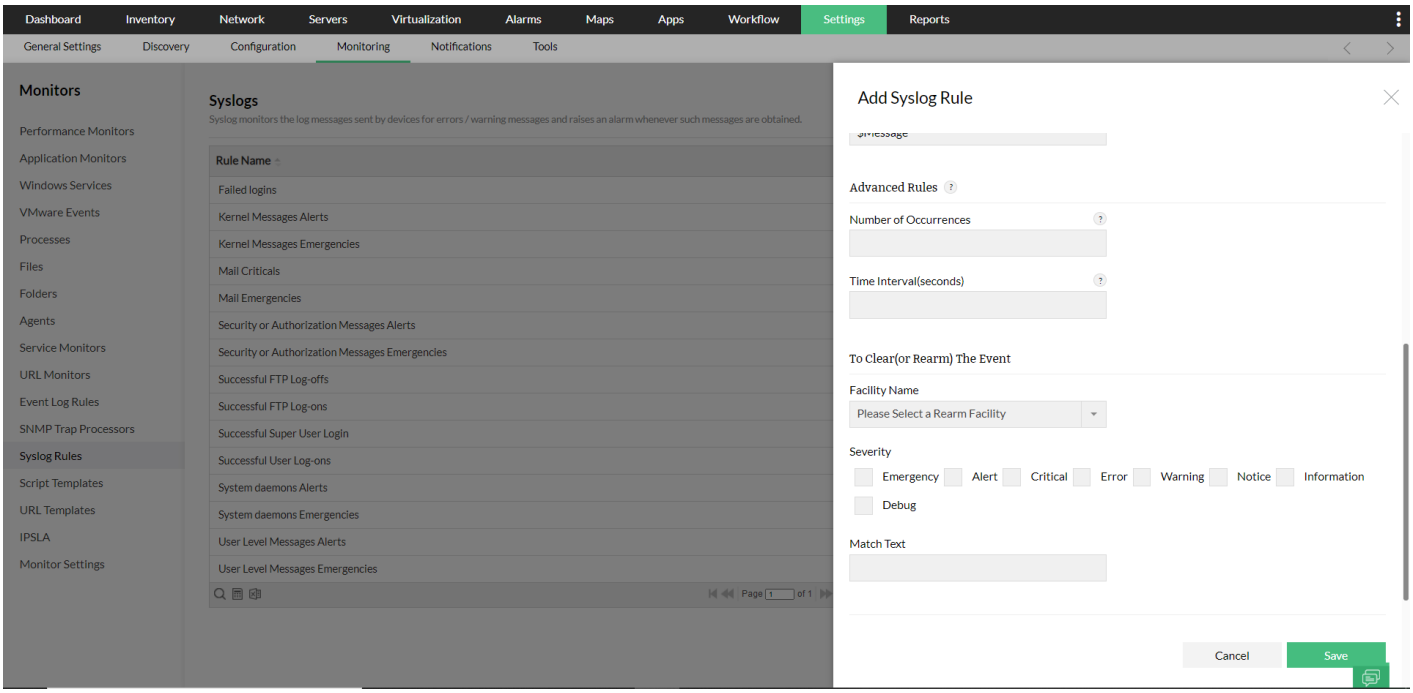
Adding Syslog Rules

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)

  Temperature in Cisco Nexus devices: For temperature, a different MIB (CISCO-ENTITY-SENSOR-MIB.php) is also being used here.

  To check if the temperature sensors are responding properly, follow these steps:

  - Perform an SNMP walk on the following OID: **.1.3.6.1.4.1.9.9.91.1.1.1.1.1 (entPhySensorType)**
  - In the list of responses received, find which OID has responded with **"Celsius(8)"** and note it down. This is the instance ID of

the temperature sensor. For example, consider the OID **.1.3.6.1.4.1.9.9.91.1.1.1.1.1.X** has responded with **"Celsius(8)".**

- The instance ID **X** can now be used to query temperature-related data from the device:
  - .1.3.6.1.2.1.47.1.1.1.1.7.X - entPhysicalName (from ENTITY-MIB)
  - .1.3.6.1.4.1.9.9.91.1.1.1.1.5.X - entSensorStatus (CISCO-ENTITY-SENSOR-MIB.php)
  - .1.3.6.1.4.1.9.9.91.1.1.1.1.4.X - entSensorValue (CISCO-ENTITY-SENSOR-MIB.php)
- **Example:**
  - A walk is performed on .1.3.6.1.4.1.9.9.91.1.1.1.1.1 (entPhySensorType).
  - The OID **.1.3.6.1.4.1.9.9.91.1.1.1.1.1.A** has responded with **"Celsius(8)".** Now A is our instance ID.
    Now we can use this instance ID to get the corresponding instance's data from the device:

OID	Description	MIB being used	Obtained response
.1.3.6.1.2.1.47.1.1.1.1.7.A	entPhysicalName	ENTITY-MIB	module-1 FRONT
.1.3.6.1.4.1.9.9.91.1.1.1.1.5.A	entSensorStatus	CISCO-ENTITY-SENSOR-MIB.php	ok(1)
.1.3.6.1.4.1.9.9.91.1.1.1.1.4.A	entSensorValue	CISCO-ENTITY-SENSOR-MIB.php	37

- **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

- **For Supermicro devices (supported from OpManager v12.5.216):**

  Supported MIB: SUPERMICRO-SSM-MIB

  Prerequisite: Supermicro's **Superdoctor agent** has to be installed to monitor hardware metrics through OpManager.

  Hardware Manufacturer - .1.3.6.1.4.1.10876.100.1.6.1.10.1
  OS - .1.3.6.1.4.1.10876.100.1.7.1.6.1
  OS Version - .1.3.6.1.4.1.10876.100.1.7.1.7.1

  - For Supermicro devices, the process is similar to the one mentioned above for Juniper devices.
  - Initially, an SNMP walk has to be performed on this OID: **.1.3.6.1.4.1.10876.2.1.1.1.1.3**. The OIDs that provide either of these responses are noted down:

    0 - Fan | 1 - Voltage | 2 - Temperature | 8 - Power

  - The instance ID X from the OID that provided any of these responses (.1.3.6.1.4.1.10876.2.1.1.1.1.3.**X**) can then be used to get the values of that hardware metric.

    - **.1.3.6.1.4.1.10876.2.1.1.1.1.2.X - smHealthMonitorName** - Name

- **.1.3.6.1.4.1.10876.2.1.1.1.1.4.X - smHealthMonitorReading** - Value
- **.1.3.6.1.4.1.10876.2.1.1.1.1.10.X - smHealthMonitorMonitor** - Status
- **.1.3.6.1.4.1.10876.2.1.1.1.1.5.X - smHealthMonitorHighLimit** - Max threshold
- **.1.3.6.1.4.1.10876.2.1.1.1.1.6.X - smHealthMonitorLowLimit** - Min threshold

EXAMPLE:

- Consider an SNMP walk being performed on the smHealthMonitorType OID (.1.3.6.1.4.1.10876.2.1.1.1.1.3.). The following responses are received:
  - .1.3.6.1.4.1.10876.2.1.1.1.1.3.**A** ? 0
  - .1.3.6.1.4.1.10876.2.1.1.1.1.3.**B** ? 8
  - .1.3.6.1.4.1.10876.2.1.1.1.1.3.**C** ? 7
  - .1.3.6.1.4.1.10876.2.1.1.1.1.3.**D** ? 2
  - .1.3.6.1.4.1.10876.2.1.1.1.1.3.**E** ? 1
- The OIDs that responded with either 0 (Fan), 1 (Voltage), 2 (Temperature) or 8 (Power) are taken, and their instance IDs are noted. In this case, the instances are **A (for Fan), B (for Power), D (for Temperature) and E (for Voltage).**
- Now these instance IDs can be used to poll the related information for that sensor from the device.

Response / Metric type / Instance ID	OID of metric name	OID of metric value	OID of metric status	OID of metric's Max threshold	OID of metric's Min threshold
0 / Fan / A	.1.3.6.1.4.1.10876.2.1.1.1.1.2.**A**	.1.3.6.1.4.1.10876.2.1.1.1.1.4.**A**	.1.3.6.1.4.1.10876.2.1.1.1.1.10.**A**	.1.3.6.1.4.1.10876.2.1.1.1.1.5.**A**	.1.3.6.1.4.1.10876.2.1.1.1.1.6.**A**
8 / Power / B	.1.3.6.1.4.1.10876.2.1.1.1.1.2.**B**	.1.3.6.1.4.1.10876.2.1.1.1.1.4.**B**	.1.3.6.1.4.1.10876.2.1.1.1.1.10.**B**	.1.3.6.1.4.1.10876.2.1.1.1.1.5.**B**	.1.3.6.1.4.1.10876.2.1.1.1.1.6.**B**
2 / Temp / D	.1.3.6.1.4.1.10876.2.1.1.1.1.2.**D**	.1.3.6.1.4.1.10876.2.1.1.1.1.4.**D**	.1.3.6.1.4.1.10876.2.1.1.1.1.10.**D**	.1.3.6.1.4.1.10876.2.1.1.1.1.5.**D**	.1.3.6.1.4.1.10876.2.1.1.1.1.6.**D**
1 / Voltage / E	.1.3.6.1.4.1.10876.2.1.1.1.1.2.**E**	.1.3.6.1.4.1.10876.2.1.1.1.1.4.**E**	.1.3.6.1.4.1.10876.2.1.1.1.1.10.**E**	.1.3.6.1.4.1.10876.2.1.1.1.1.5.**E**	.1.3.6.1.4.1.10876.2.1.1.1.1.6.**E**

For Power and Voltage, we will divide the obtained values by 1000 to show the correct values.

- The status metric usually responds only with two values - **1 - Manage/Clear status** or **2 - Unmanaged/Unknown status**, so it is not possible for OpManager to determine if the device is critical. For displaying critical status for devices, OpManager uses the Max Threshold and Min Threshold values to determine if the performance is abnormal. The criteria for threshold violation for different sensor types are as below:
  - **Fan:** If the status is 1 (Manage) AND fan sensor value is less than the Minimum Threshold Value, the status will be considered as **Critical.** For example, if **FV** is the current value of fan:

```
if (smHealthMonitorMonitor == 1 && (FV < smHealthMonitorLowLimit) )
{
??Status = "Critical"
}
else
{
??Status = "Clear"
}
```

- **Temperature:** If the status is 1 (Manage) AND the **temperature sensor value is greater than the Maximum Threshold Value,** the status will be considered as **Critical.** For example, if **TV** is the current value of temperature:

```
if (smHealthMonitorMonitor == 1 && (TV > smHealthMonitorHighLimit) )
{
??Status = "Critical"
}
else
{
??Status = "Clear"
}
```

- Voltage and power: If the status is 1 (Manage) AND sensor value is **less than the minThresholdVal OR greater than the maxThresholdVal,** we will consider that as **Critical.** For example, if **PV** is the current value of power/voltage:

```
if( (smHealthMonitorMonitor == 1) && ((PV < Min threshold value) || (PV > Max threshold value)) )
{
??Status = "Critical"
}
else
{
??Status = "Clear"
}
```

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')

Cisco Nexus (temperature): 1 - Clear | 2 - Attention (unavailable) | 3 - Critical (not operational) | 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

Supermicro: 1 - Manage/Clear | 2 - Unmanaged/Unknown status

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 monitors related to Hosts and VMs
- Automatically maps the VMs migrated (via vMotion) to the corresponding Hosts
- Also supports VMware vCenter 7 (from OpManager version 125181)

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.

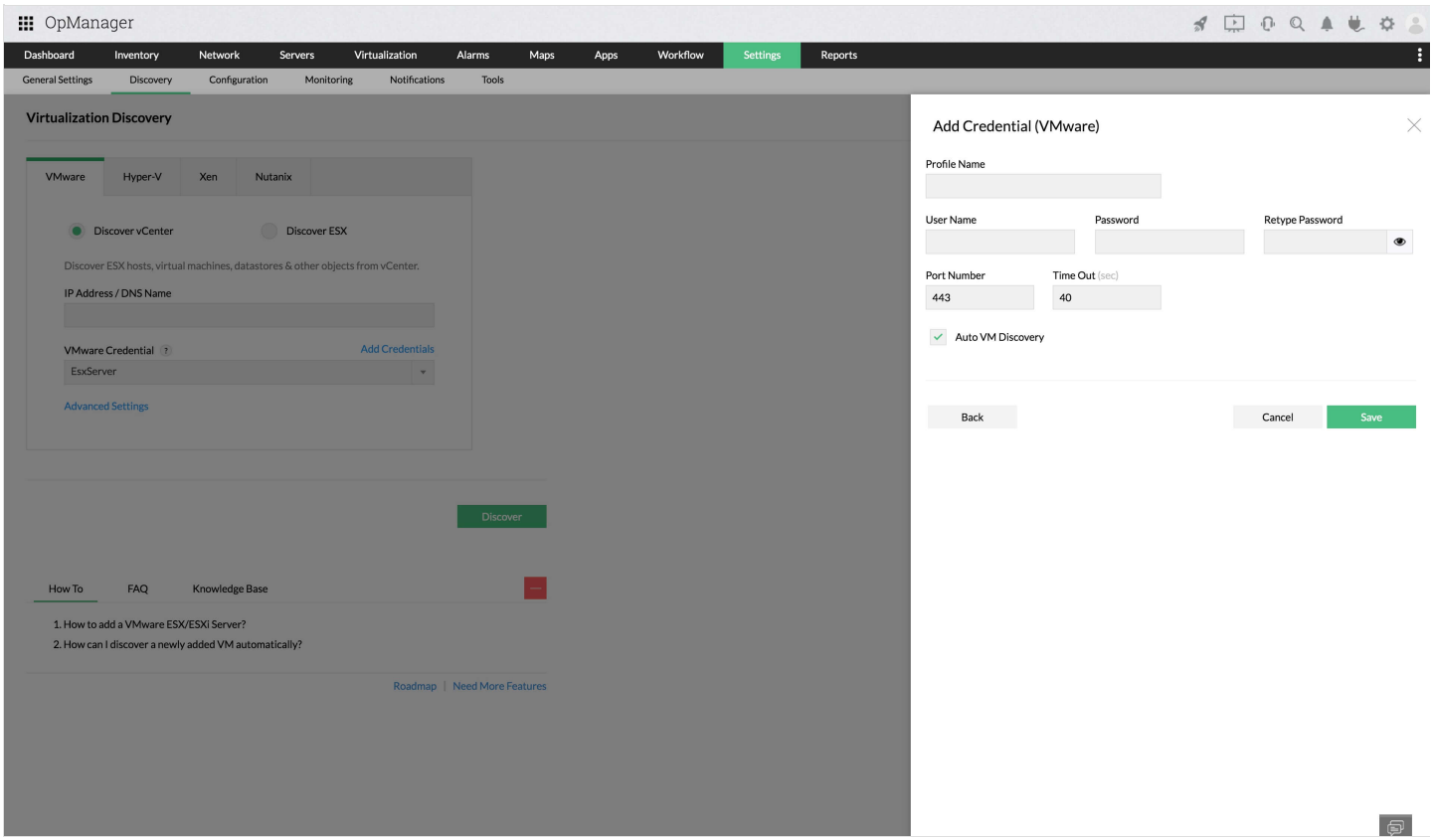
Note that the vSphere user must have access to all hosts and VMs (at least Read access) in order to monitor the devices without any issues. In case a user wants to execute actions like powering on/off VMs, please make sure that user has sufficient privileges for those actions (providing Administrator 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

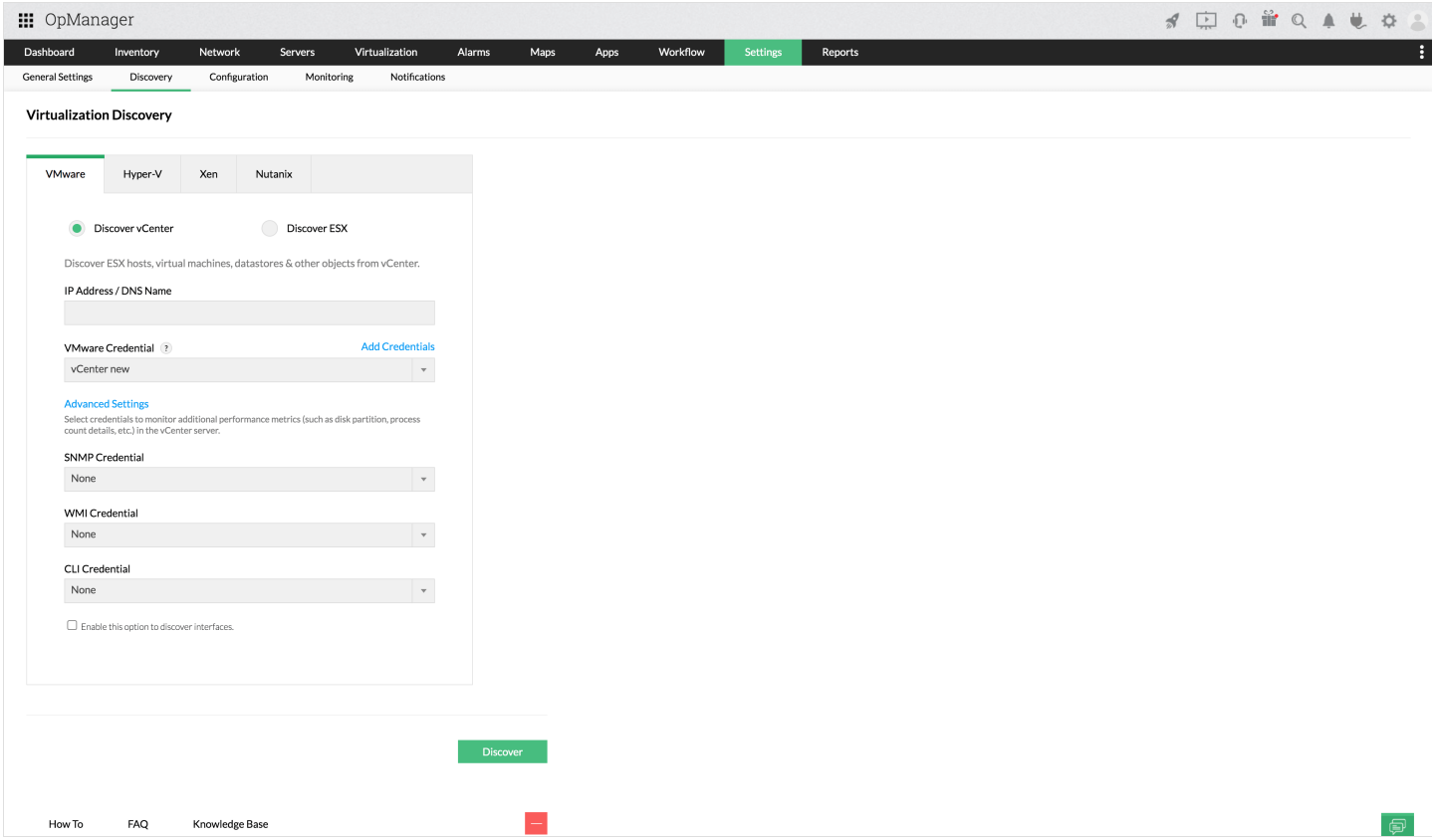
Before proceeding, ensure that you have configured the VMware credentials for the vCenter/ ESX host and the SNMP and WMI credentials for the VMs in the credential library.



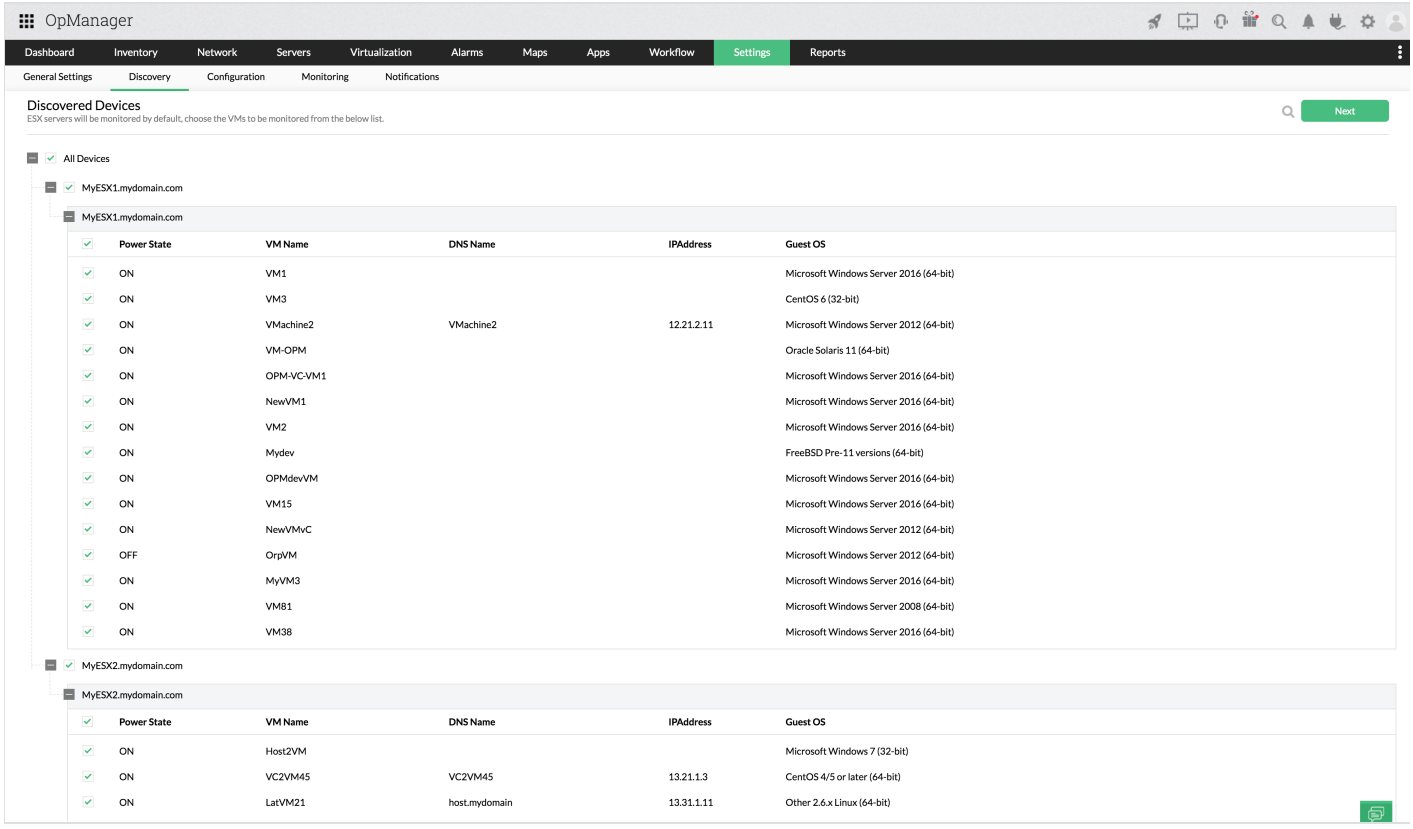
1. Go to **Settings ? Discovery ? Credentials ? Add Credentials** (or) **Settings ? Discovery ? Virtualization Discovery ? Add Credential**.
2. Select VMware as the **Credential type** and enter the vCenter/ Host's vSphere login Username and Password.
3. Enter the HTTPS (VMware web service's) **port 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.

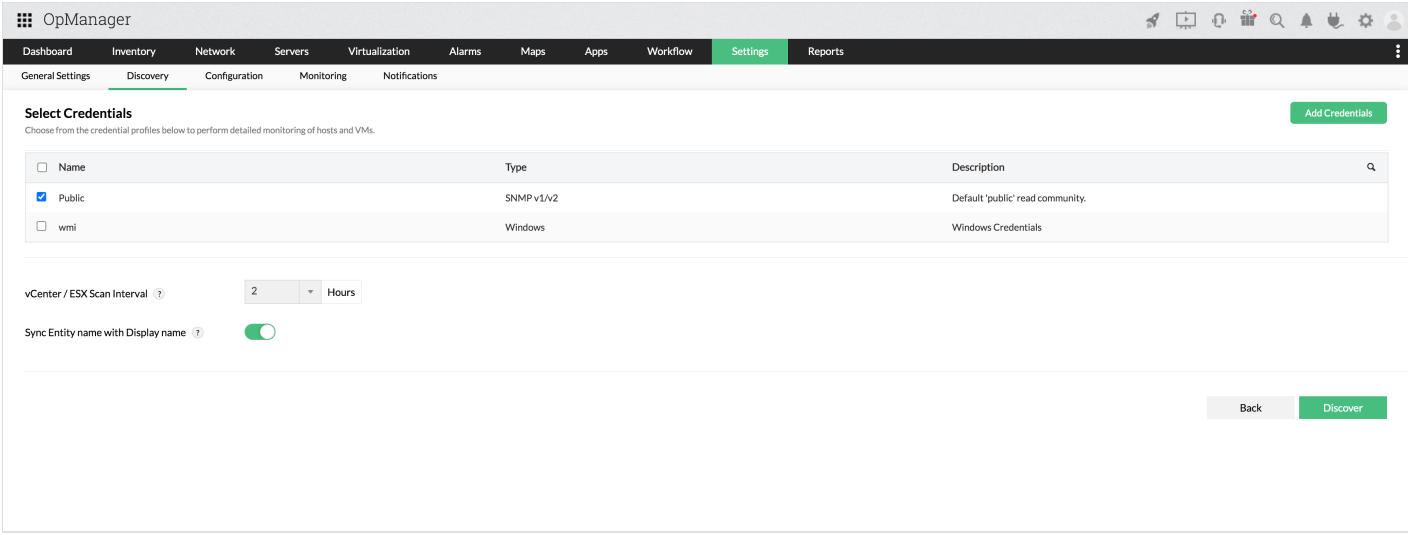
Discovering vCenter/Host



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.



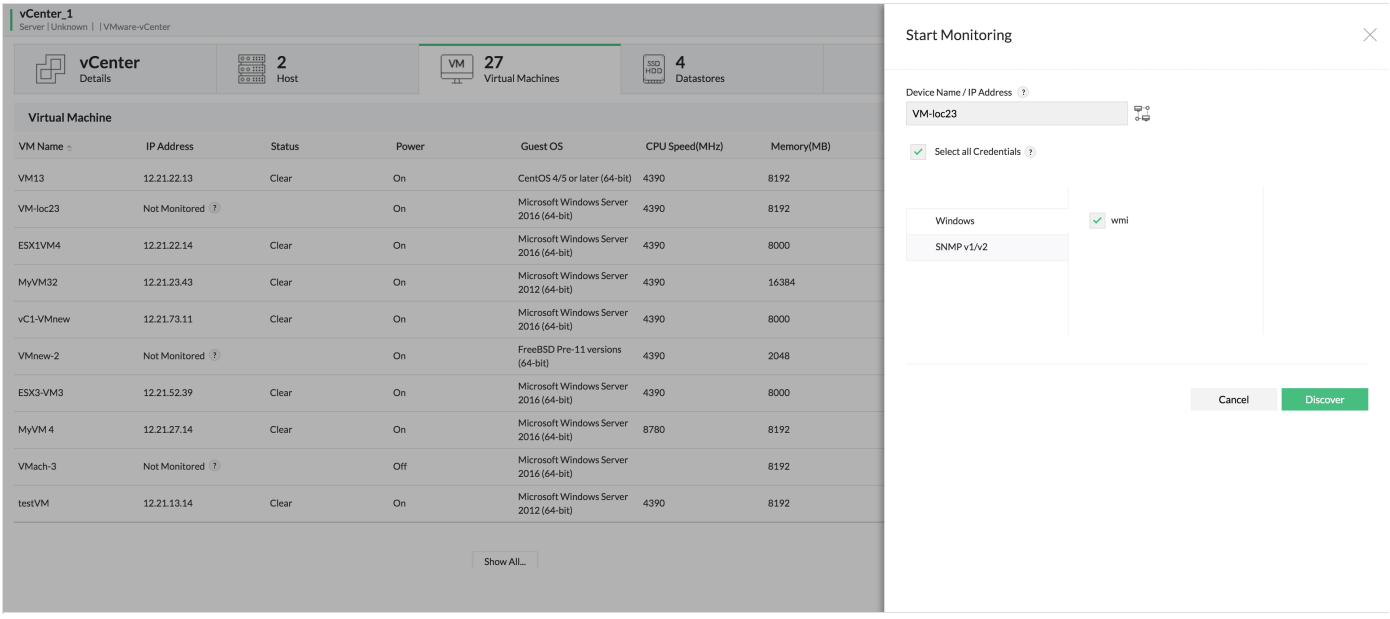
3. You can choose the time interval in which want any changes in the vCenter environment should be automatically updated in OpManager by choosing a value for **Scan vCenter/ ESX Interval (hrs).** This will automatically rediscover any changes in the vCenter environment.
3. Also, you can choose whether 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.

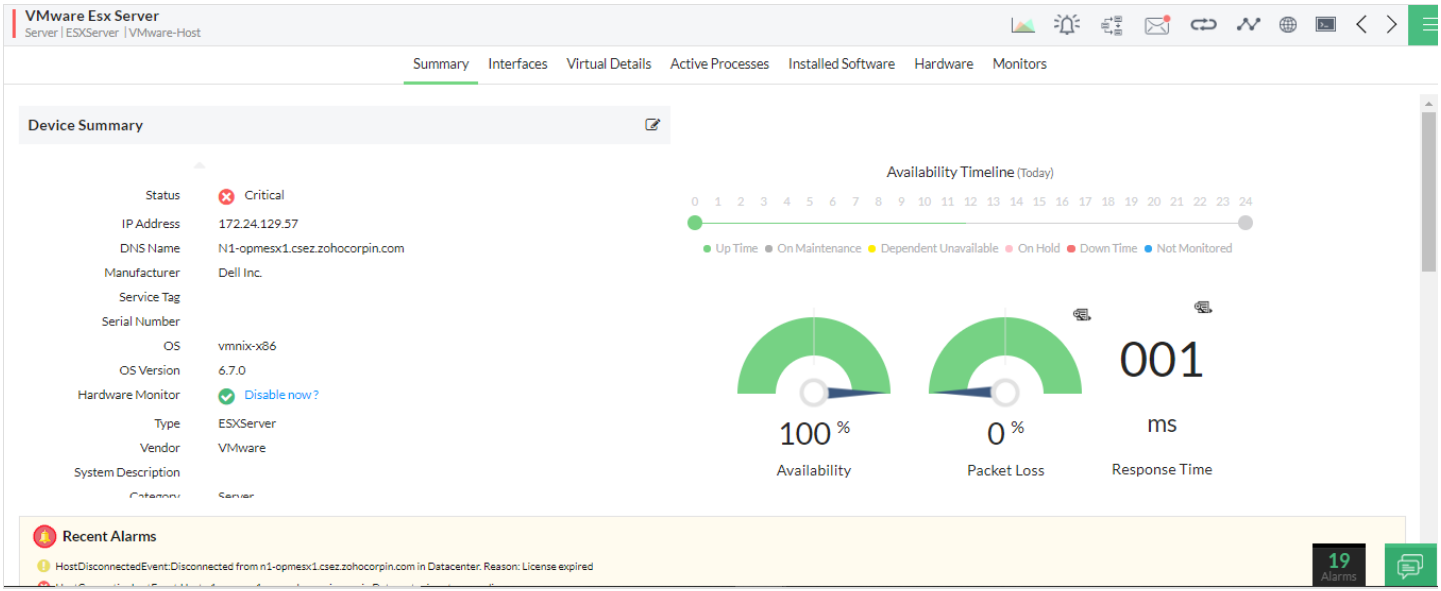
Top VMs	Top Hosts
1. Top CPU Consumers 2. Top CPU Ready Consumers 3. Top Memory Consumers 4. Top Swap Memory Consumers 5. Top Disk I/O Consumers 6. Top Network Consumers	1. Top CPU Consumers 2. Top Memory Consumers 3. Top Swap Memory Consumers 4. Top Network Consumers 5. Top Disk I/O Consumers 6. Top 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.

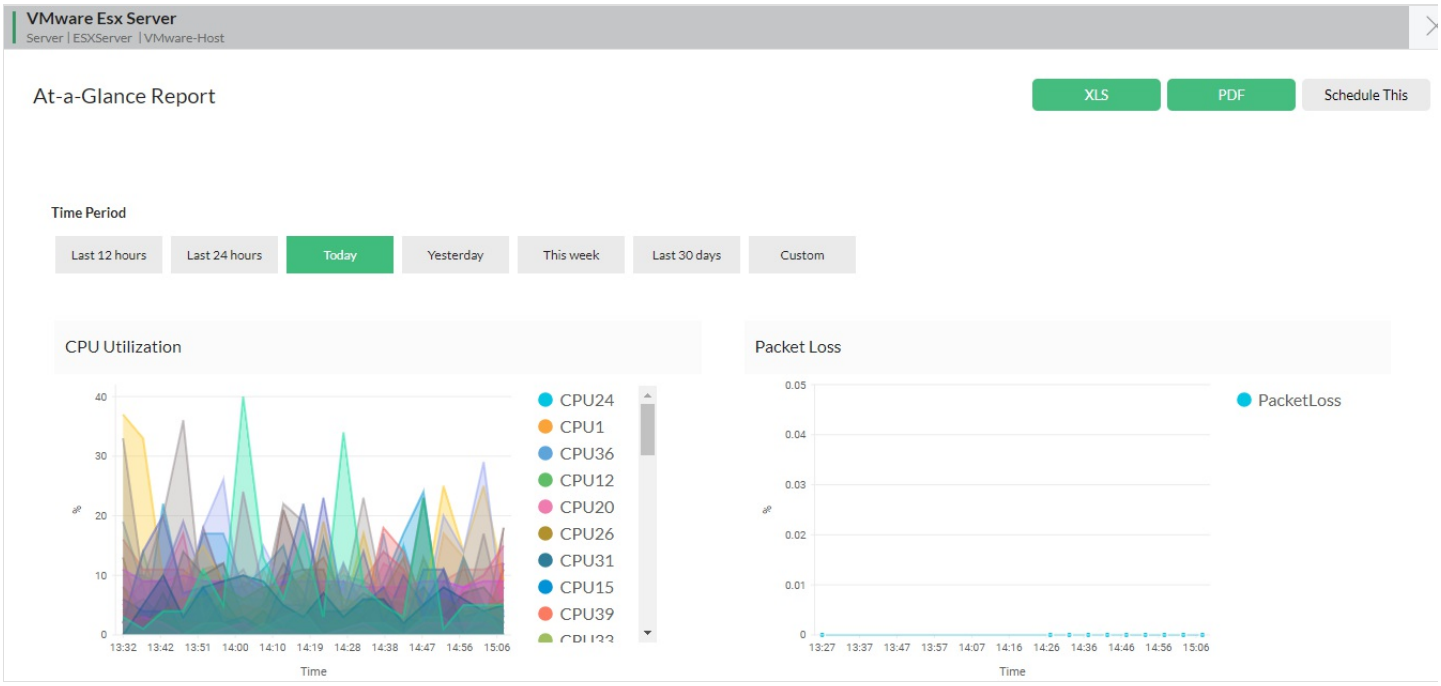
Host Details and Performance Charts

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.

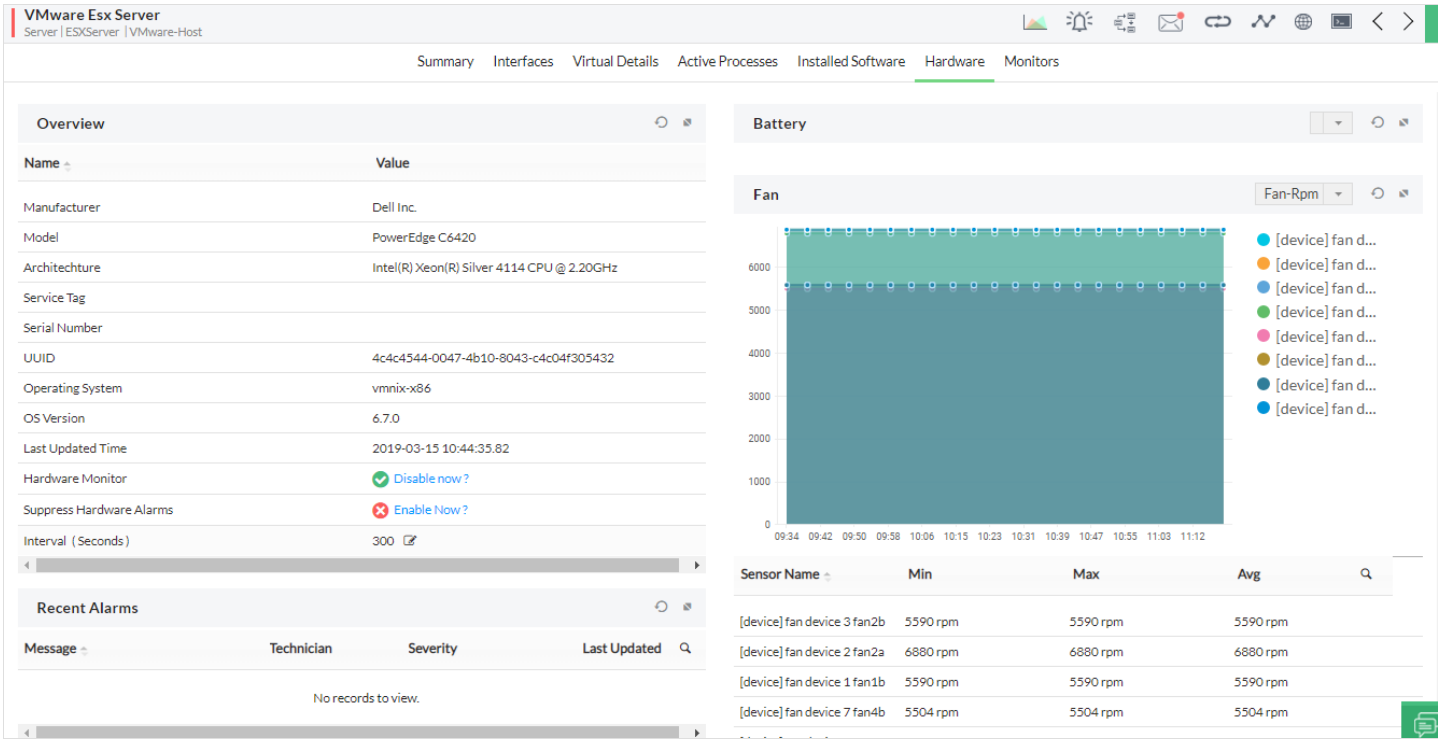


Host Health At-a-Glance

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.



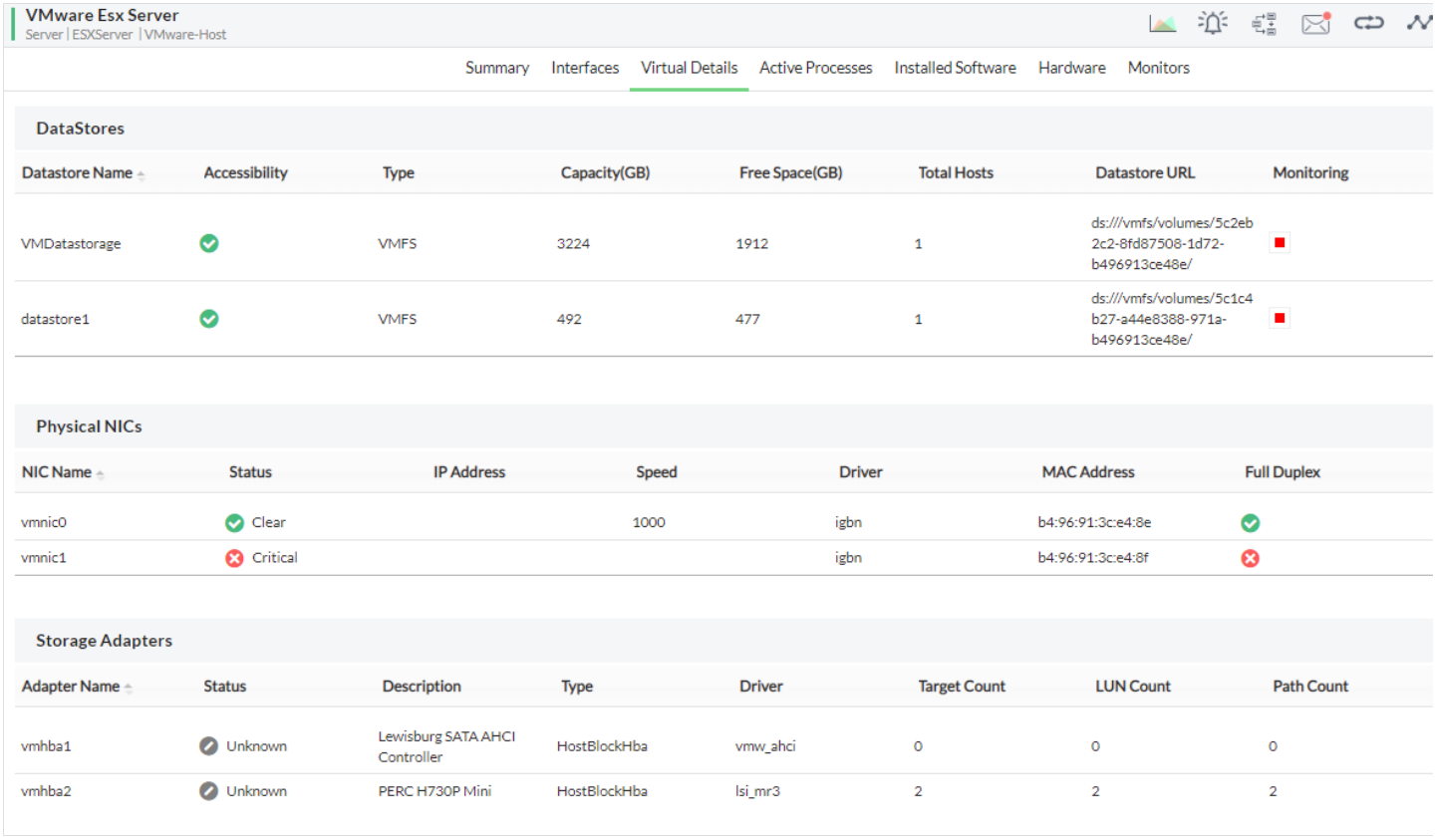
Hardware details



- 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.



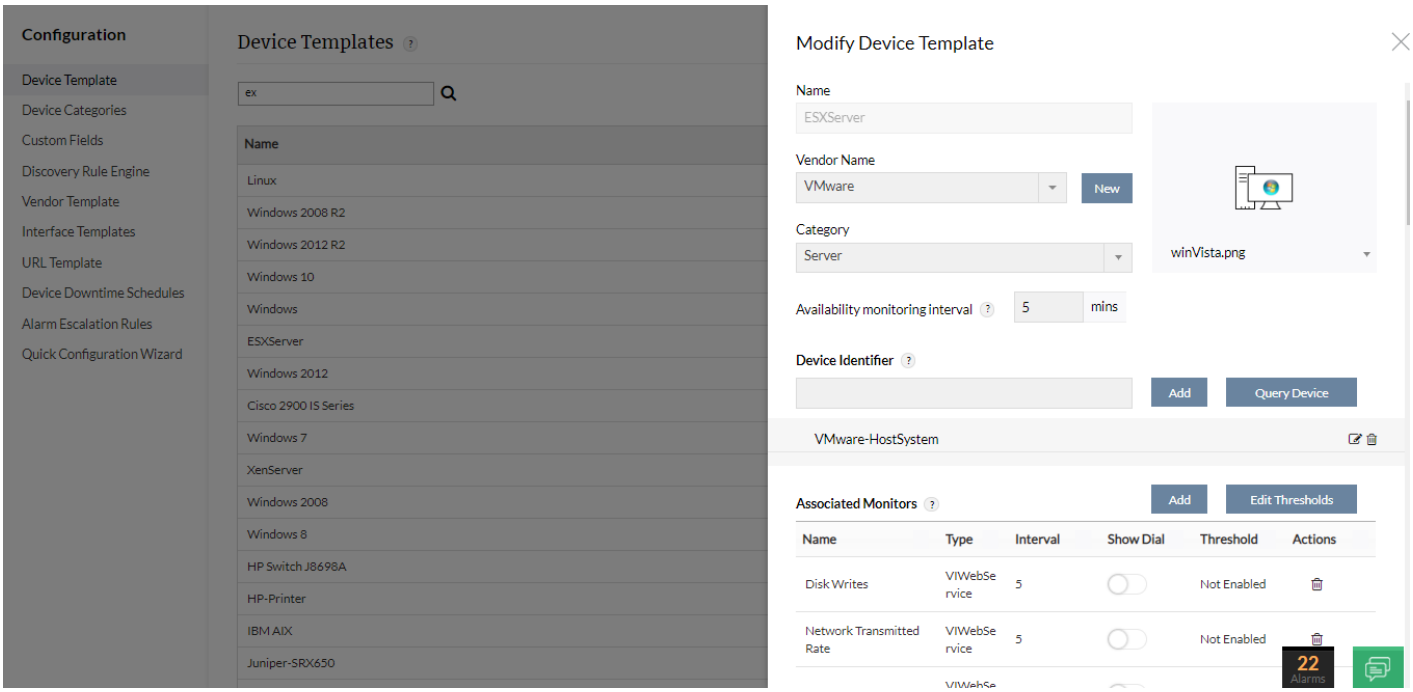
Click on the VM name to see its snapshot page. The snapshot page of the VM is similar to that of any Windows or Linux Server's snapshot page. It also displays the VMs virtual details.

Configuring Thresholds for VMware ESX and VMs

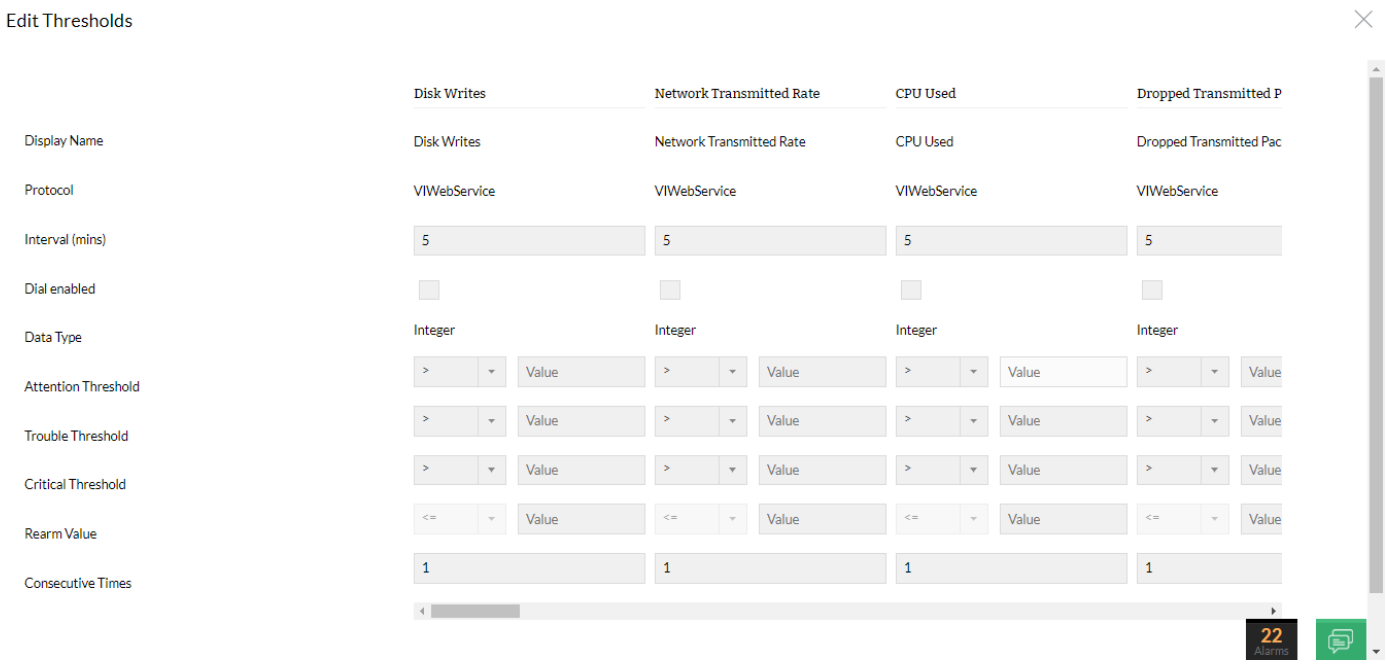
OpManager out-of-the-box offers monitoring templates for ESX hosts and VMs. The templates help you configure thresholds for multiple ESX hosts and VMs at one shot. For each performance metric you can configure Warning Threshold as well as Error Threshold, and receive proactive alerts if they are violated.

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 **Virtualization ? Hyper-V ? Add Hyper-V**.
2. Enter the **Host Name/IP Address** of the Hyper-V server.
3. Select the appropriate credential profile. You can also add a new credential profile by clicking on the **Add Credentials** button.
4. Click **Discover** button to start the discovery process.
5. OpManager detects all VMs under the server and lists them. You can choose which VMs to monitor by simply selecting/unselecting the VMs. Once you're done, click **Next.**
6. In the final step of discovery, you can choose any SNMP/WMI/CLI credential profile to perform in-depth monitoring of your VMs. This will enable you to monitor metrics that are otherwise not possible using the primary WMI credential provided for the Hyper-V server.
7. Choose a suitable **Hyper-V scan interval** to scan your server periodically for changes. You can also choose if you want to enable Auto VM Discovery by toggling the **Discover new VMs automatically** option.
8. Once you're done selecting, click **'Discover'** to initiate the discovery process. OpManager will continue to discover VMs in the background, and will alert you when it is completed.

If any of the VMs are already discovered or added, OpManager automatically maps them as a virtual Device.

Note: If the device has been added successfully, but not displayed under the 'Virtualization' tab, search for that device in OpManager. Once you find it, go to the Snapshot page and look for the device type. If it is mentioned as **'Unknown',** it means that wrong credentials have been provided or it was not reachable during discovery. Provide the correct credentials and click on **'Rediscover Now'** present under the sandwich 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.

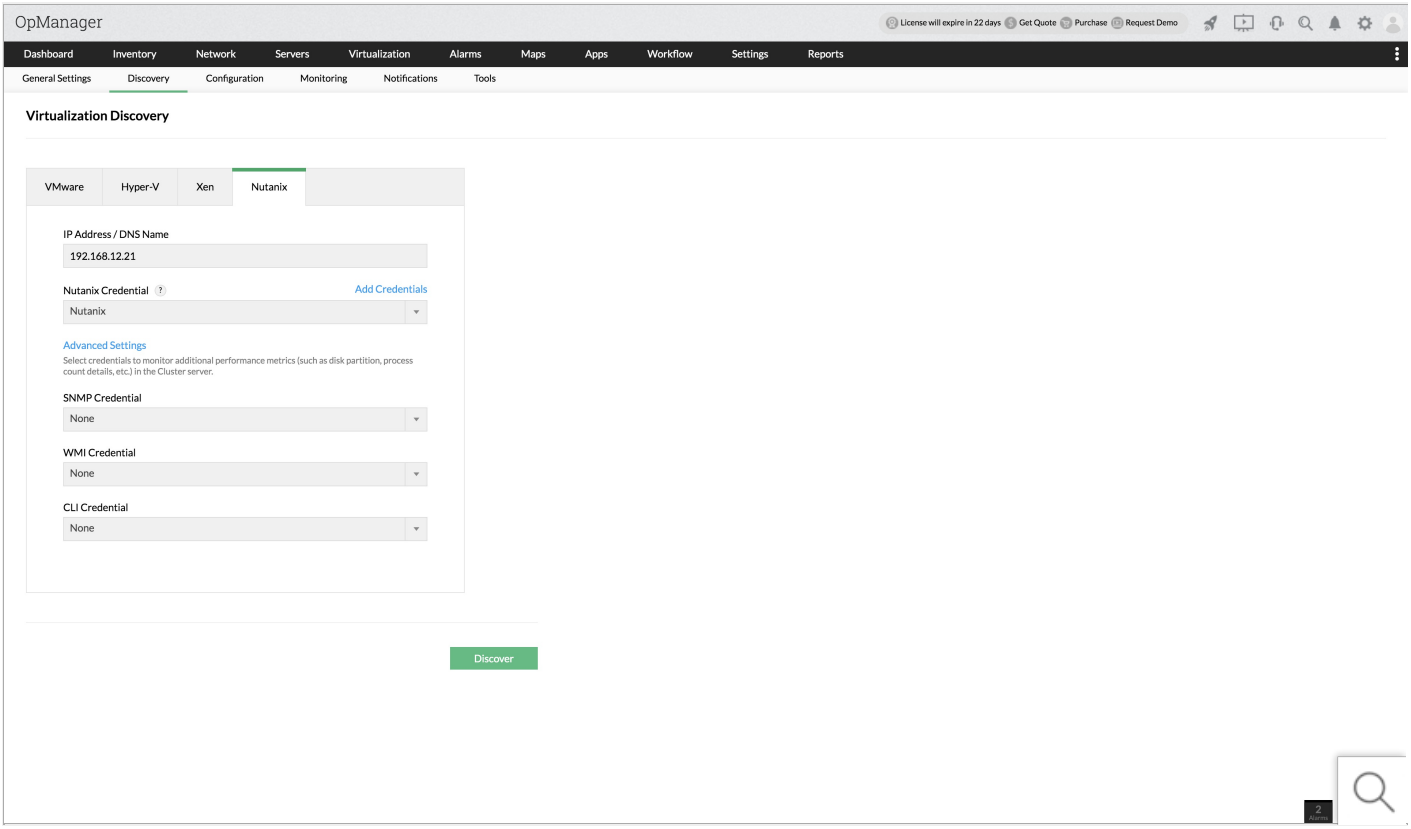
Discovering Nutanix clusters in OpManager

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.

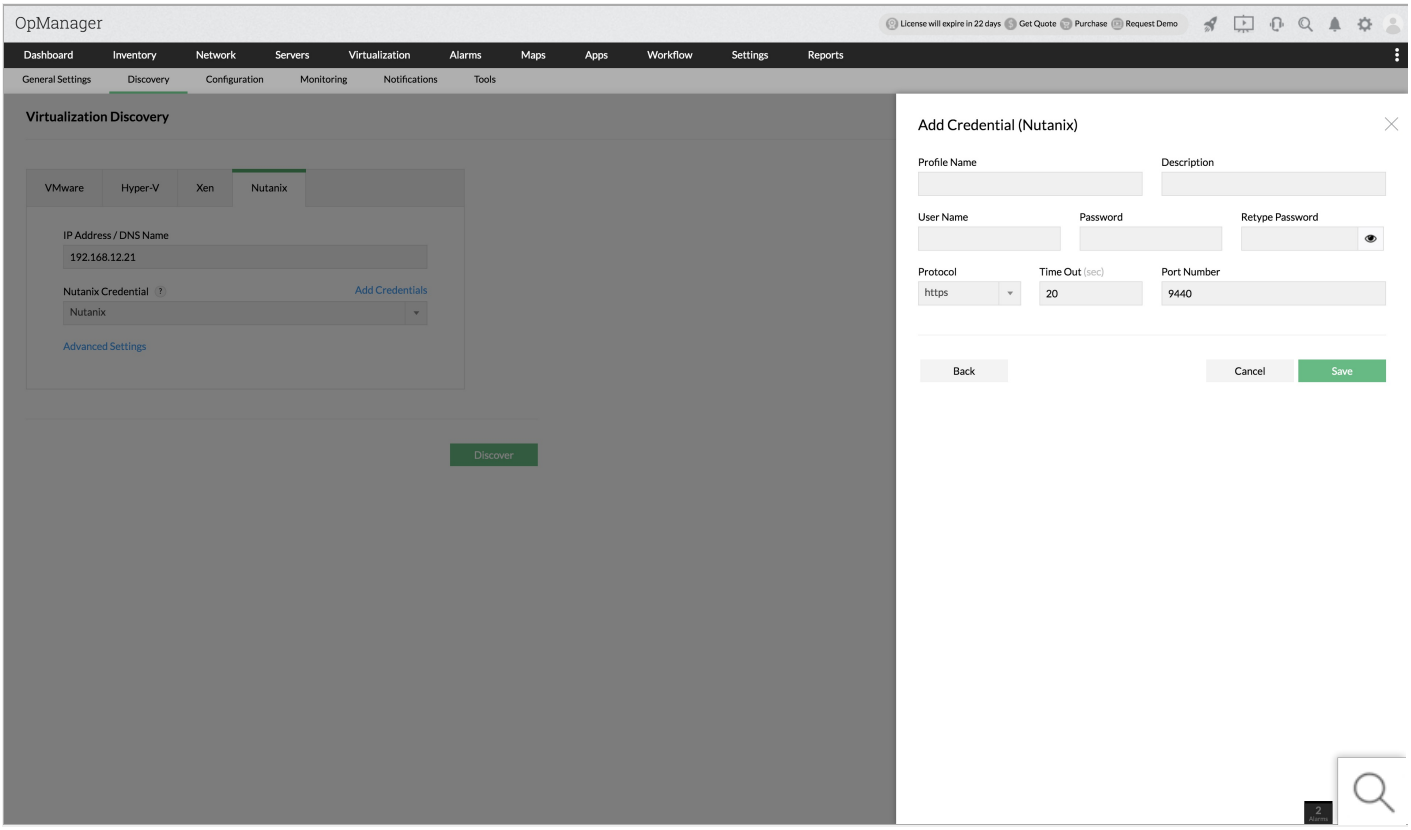
OpManager makes use of the **Prism API** framework to fetch performance metrics from the devices in the Nutanix environment.

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.



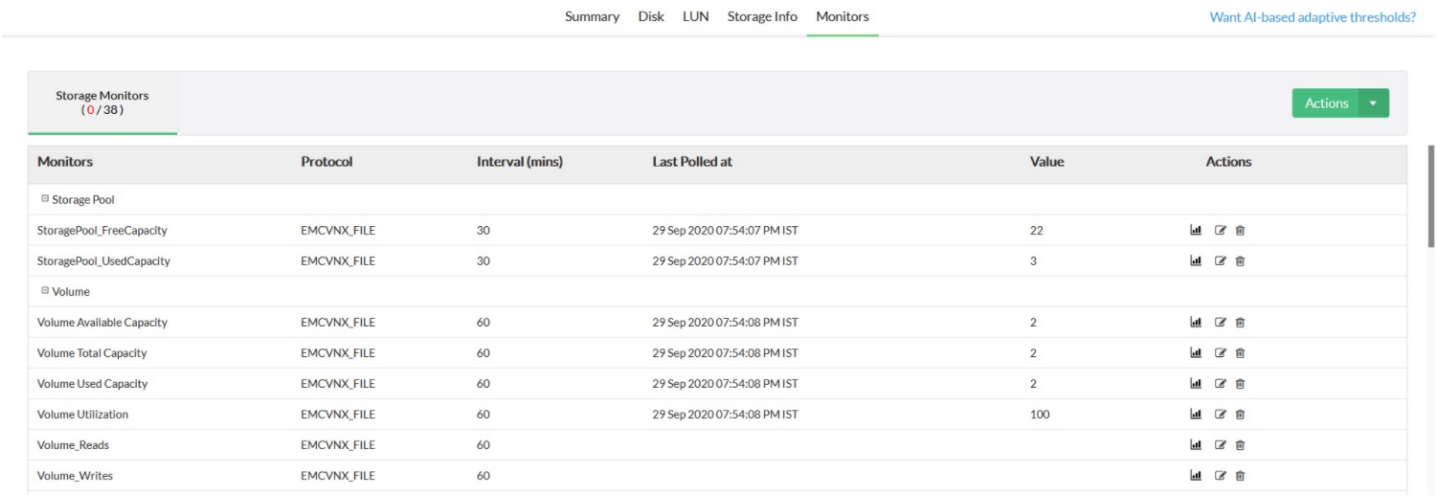
3. In the credentials field, select the credentials of the cluster. If you haven't already added it, you can click on 'Add Credentials' and create a credential profile right away. Click on 'Add Credentials', select 'Nutanix' and provide the following details:
    1. Profile name (mandatory): A name for 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.



Monitors	Protocol	Interval (mins)	Last Polled at	Value	Actions
Storage Pool					
StoragePool_FreeCapacity	EMCVNX_FILE	30	29 Sep 2020 07:54:07 PM IST	22	
StoragePool_UsedCapacity	EMCVNX_FILE	30	29 Sep 2020 07:54:07 PM IST	3	
Volume					
Volume Available Capacity	EMCVNX_FILE	60	29 Sep 2020 07:54:08 PM IST	2	
Volume Total Capacity	EMCVNX_FILE	60	29 Sep 2020 07:54:08 PM IST	2	
Volume Used Capacity	EMCVNX_FILE	60	29 Sep 2020 07:54:08 PM IST	2	
Volume Utilization	EMCVNX_FILE	60	29 Sep 2020 07:54:08 PM IST	100	
Volume_Reads	EMCVNX_FILE	60			
Volume_Writes	EMCVNX_FILE	60			

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.

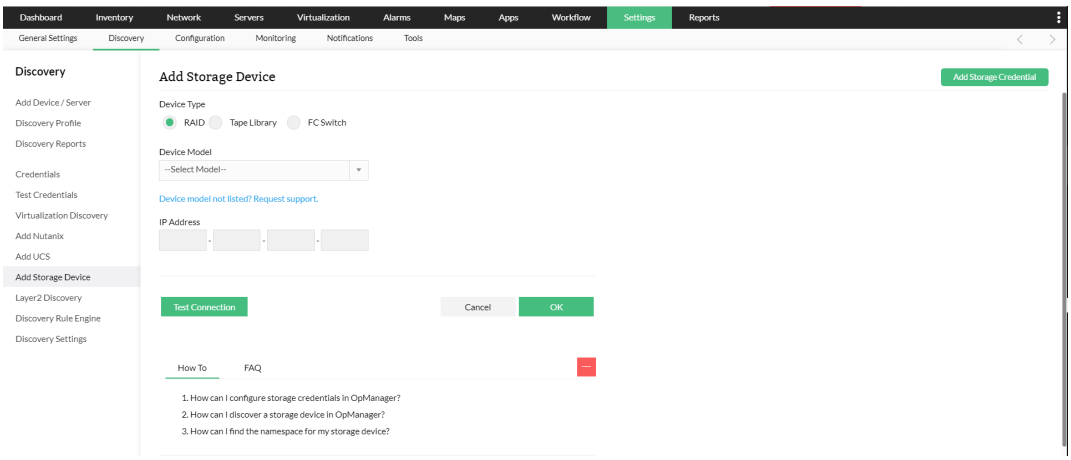
Steps for adding a Device :

- 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.

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.

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.

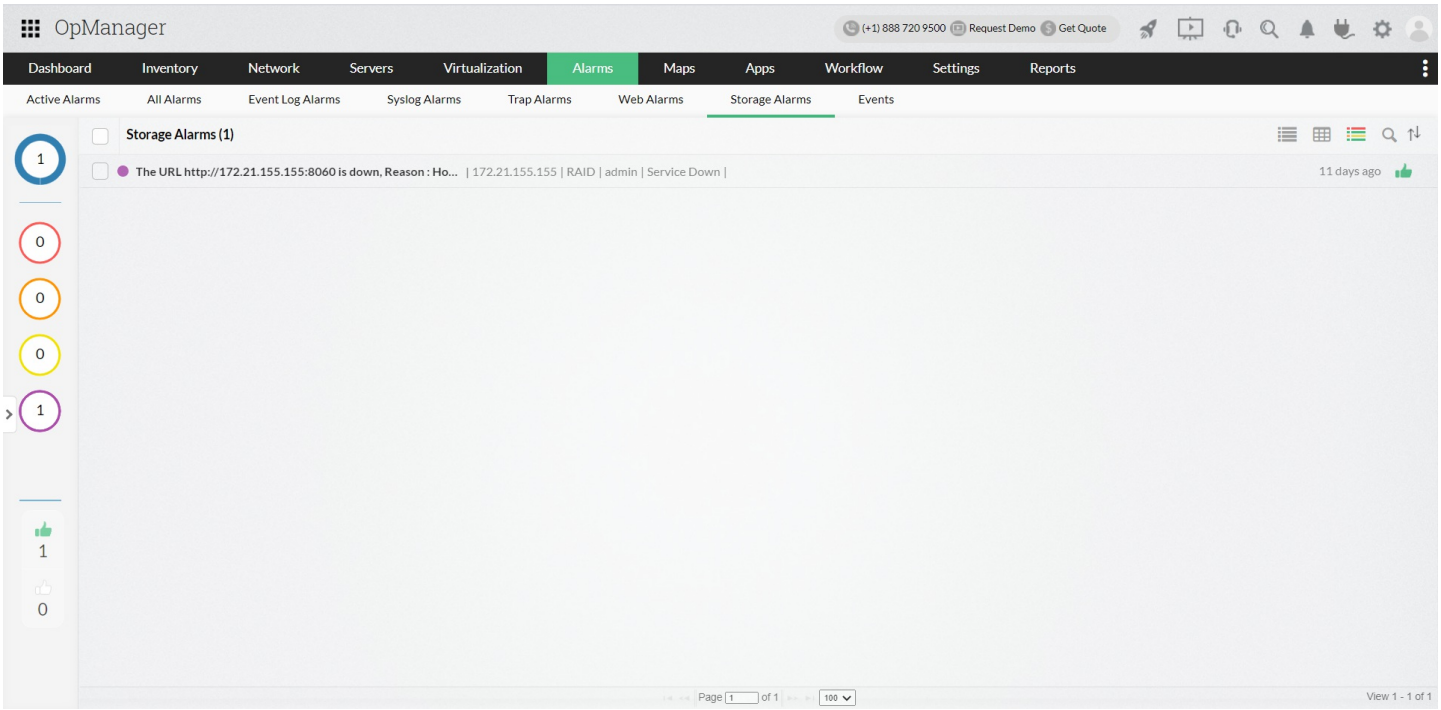
The topics covered under this section are :

- 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.

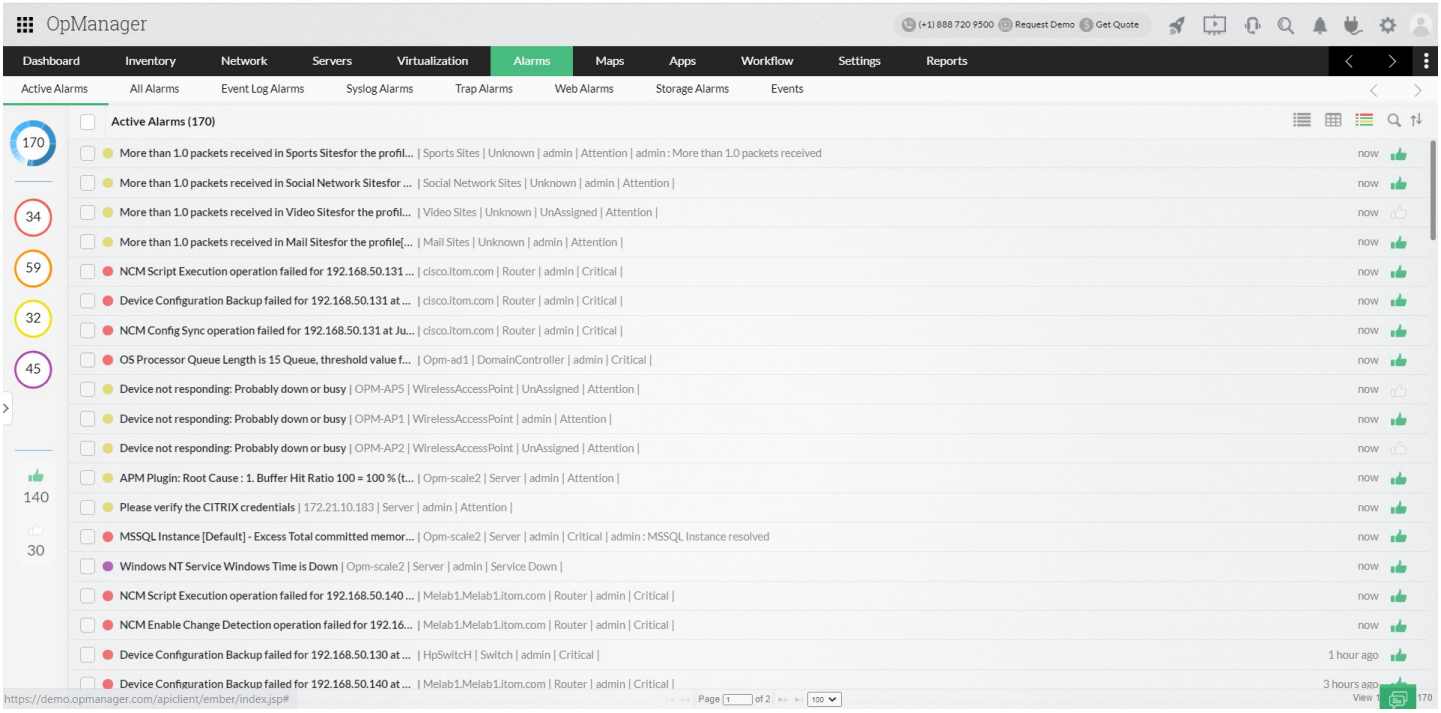
You can even view the alarms depending on the criteria like Severity, Category or alarms generated between a specific time

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.

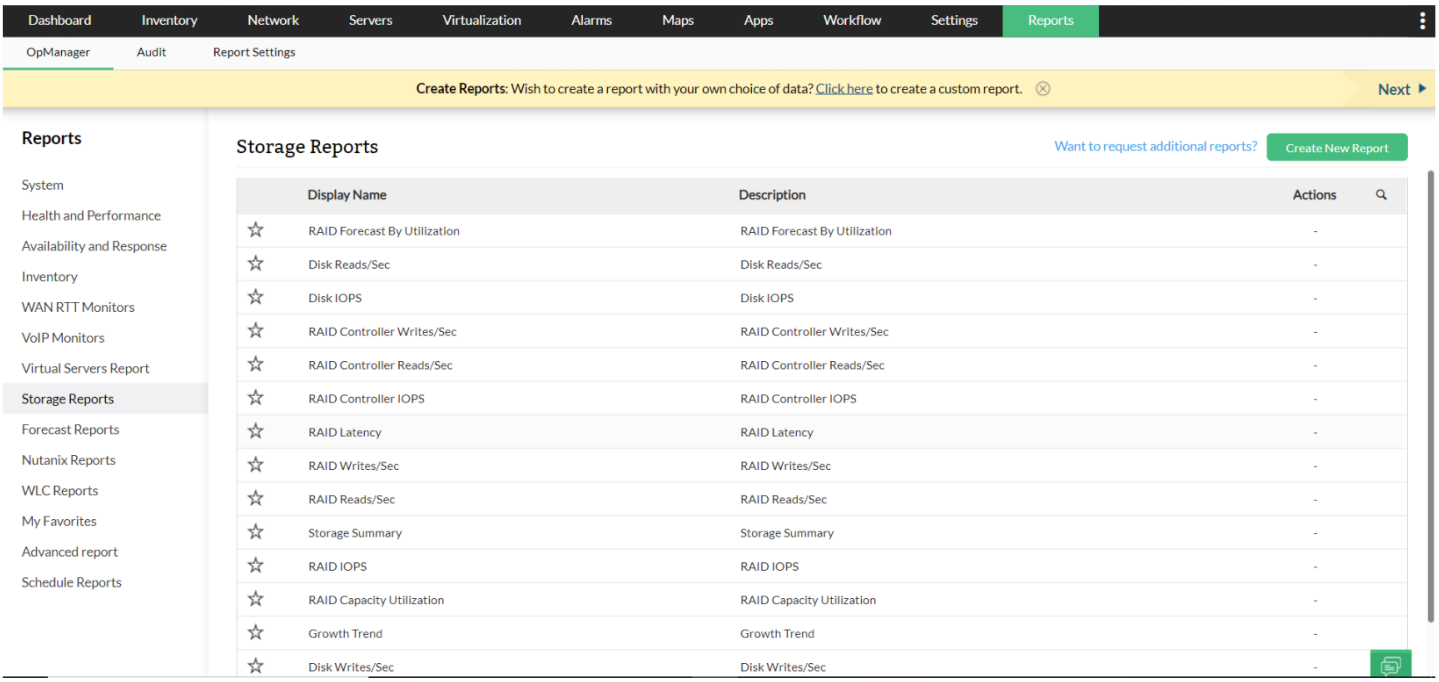
- The configured values are shown in the form below.
- You can edit the required values and click ‘Save’.

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

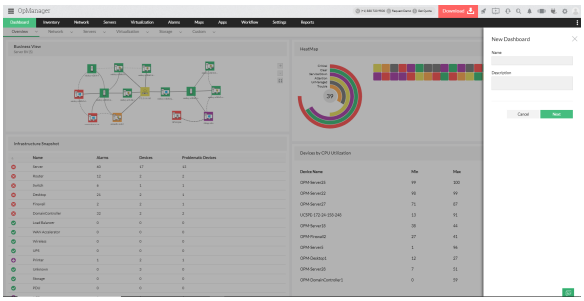
More reports for storage monitoring are available under **Reports ? Storage Reports.**

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.**

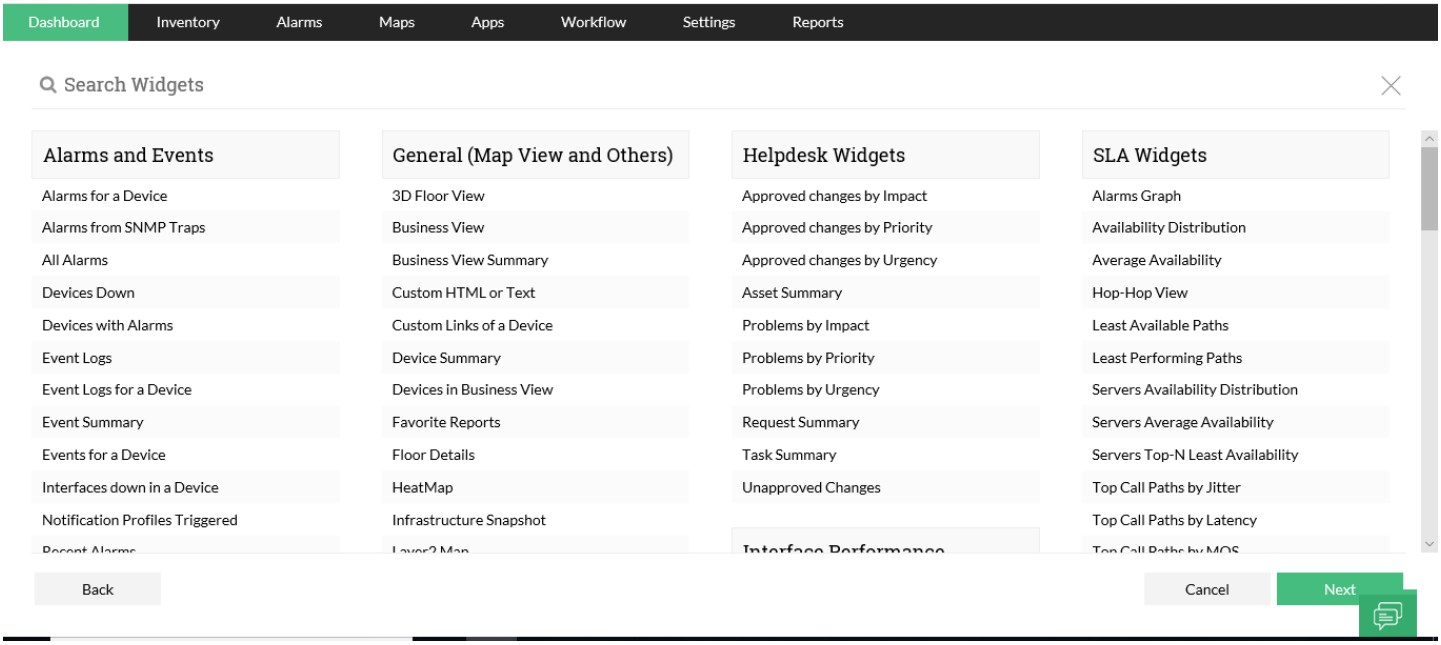
1. Click on **Dashboard.** In the top right corner of the screen, click on the icon with + symbol. Create **New Dashboard** page opens [screen shots given below].



2. **Name**: Enter a unique name for the dashboard.

3. **Description**: Enter a description about the dashboard.

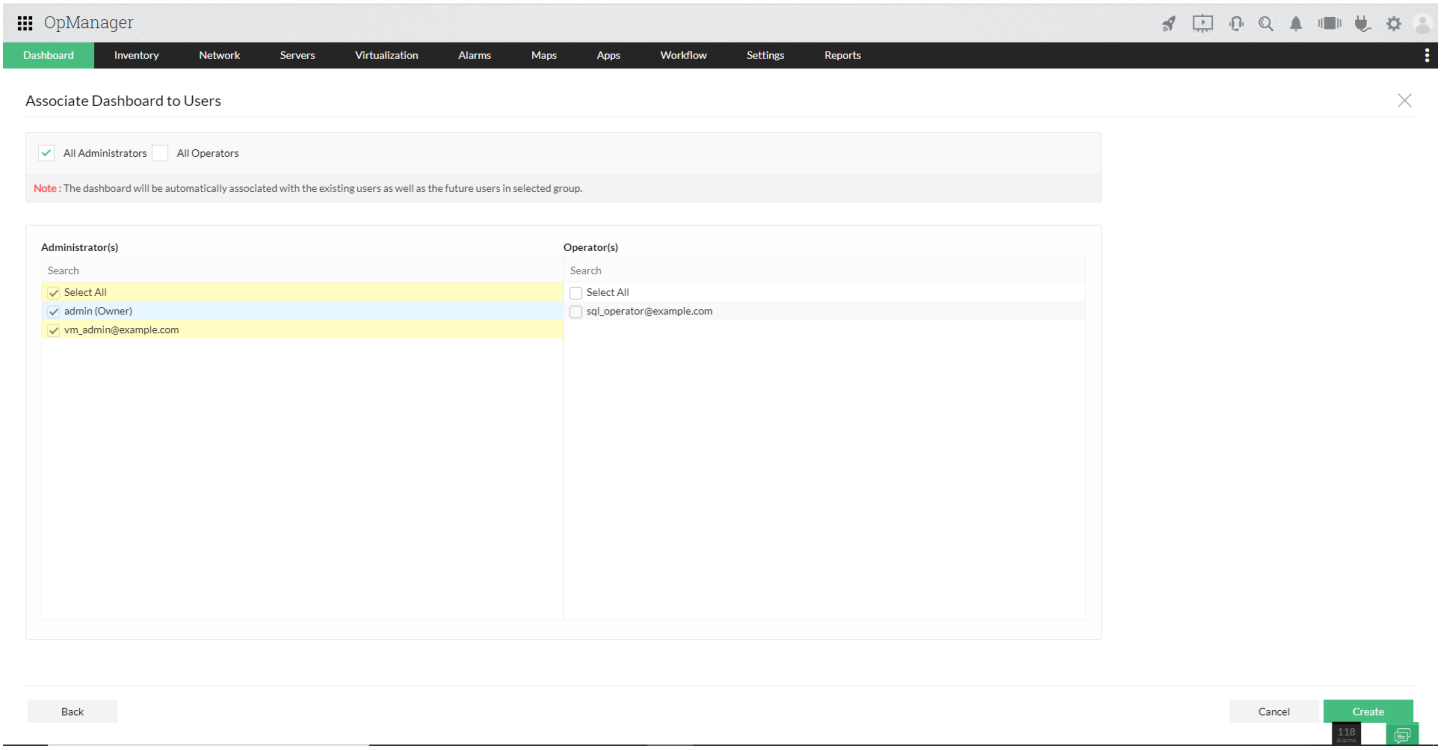
4. Click **Next**.



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.

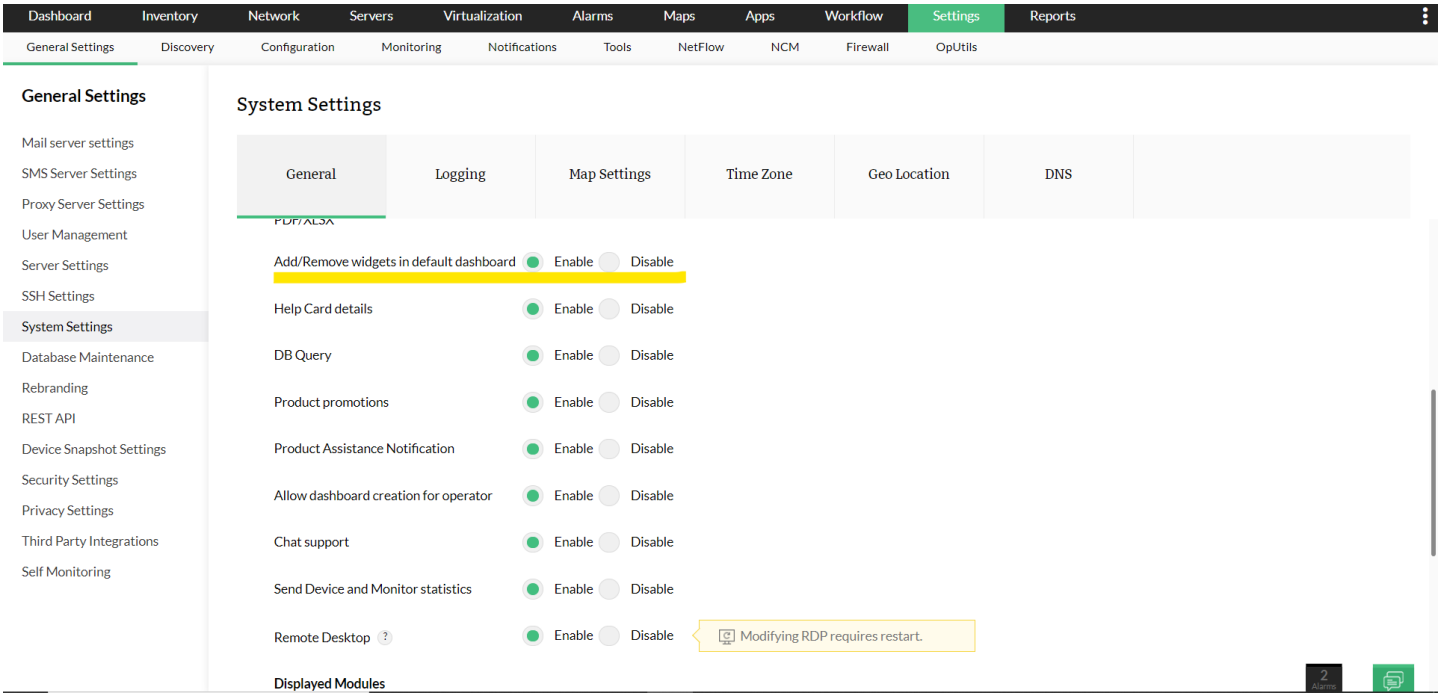
Privilege-based actions allowed for admins/operators on custom dashboards

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

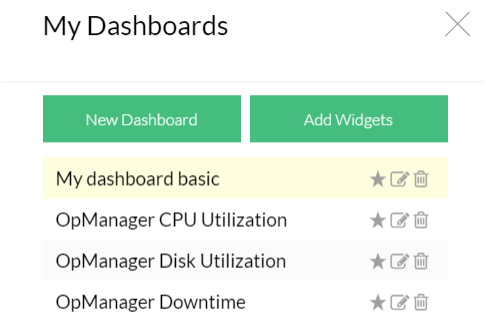
To delete a dashboard, follow the steps given below:

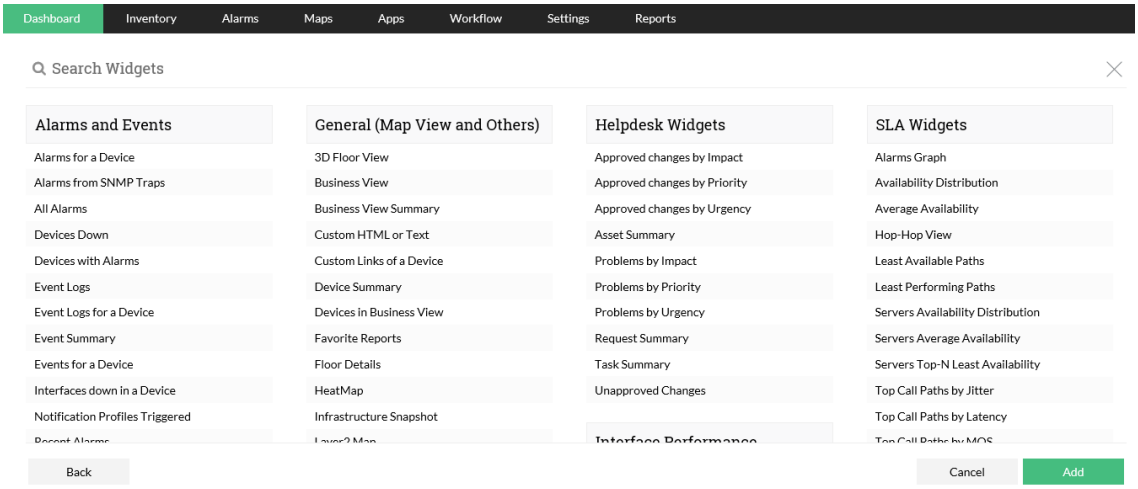
1. Go to **Dashboard** > **My Dashboard** page
2. Click **Delete** icon of the **Dashboard** that you want to delete. A confirmation window pops-up.
3. Click **OK** to confirm deleting.

Adding New Widgets

To add a new widget to a dashboard follow the steps given below:

1. Click on **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 **My Dashboards.** If you want to know the steps to create a new custom dashboard, click here
2. Click on **Add Widgets** seen at the bottom of the page.
3. Select the Widget(s) that you want to add to the dashboard.
4. Click **Add** button to add the selected widget(s) to the dashboard.

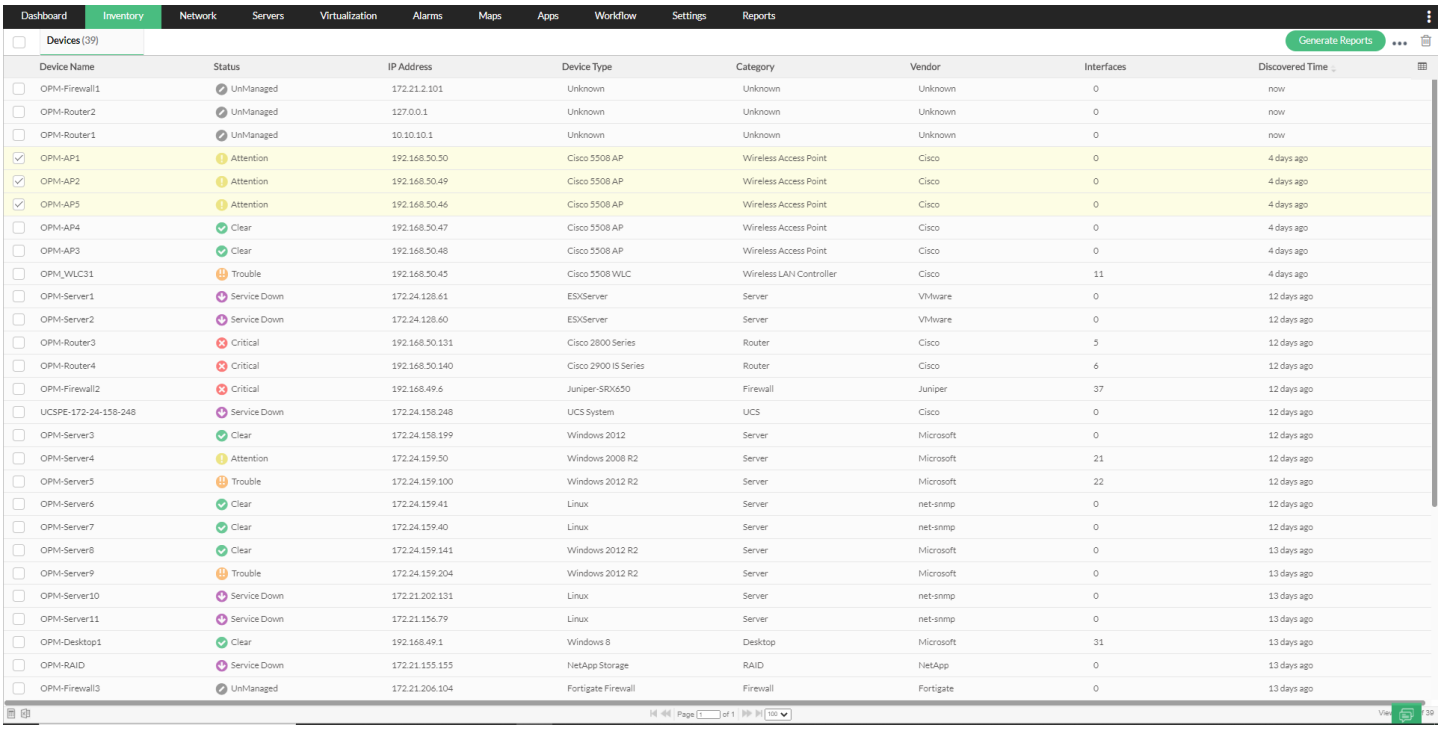


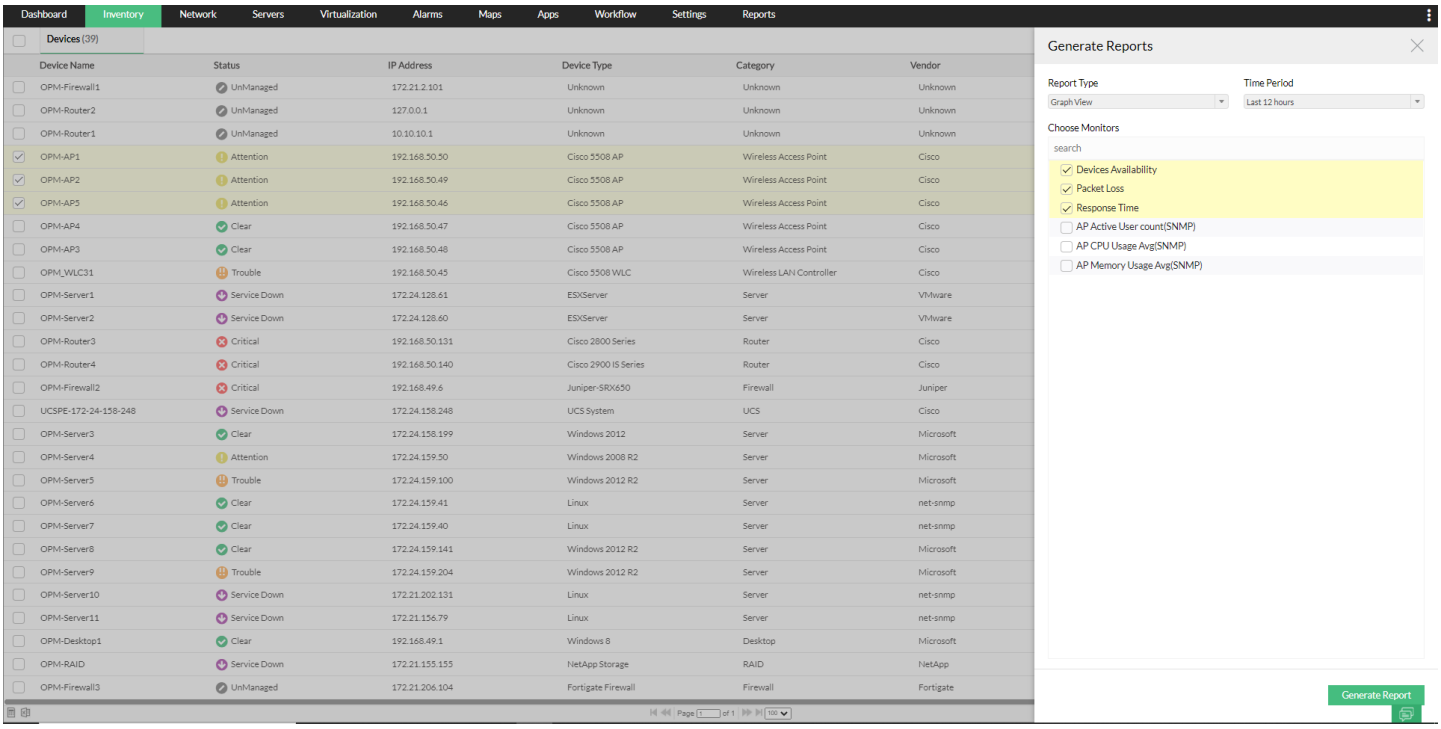


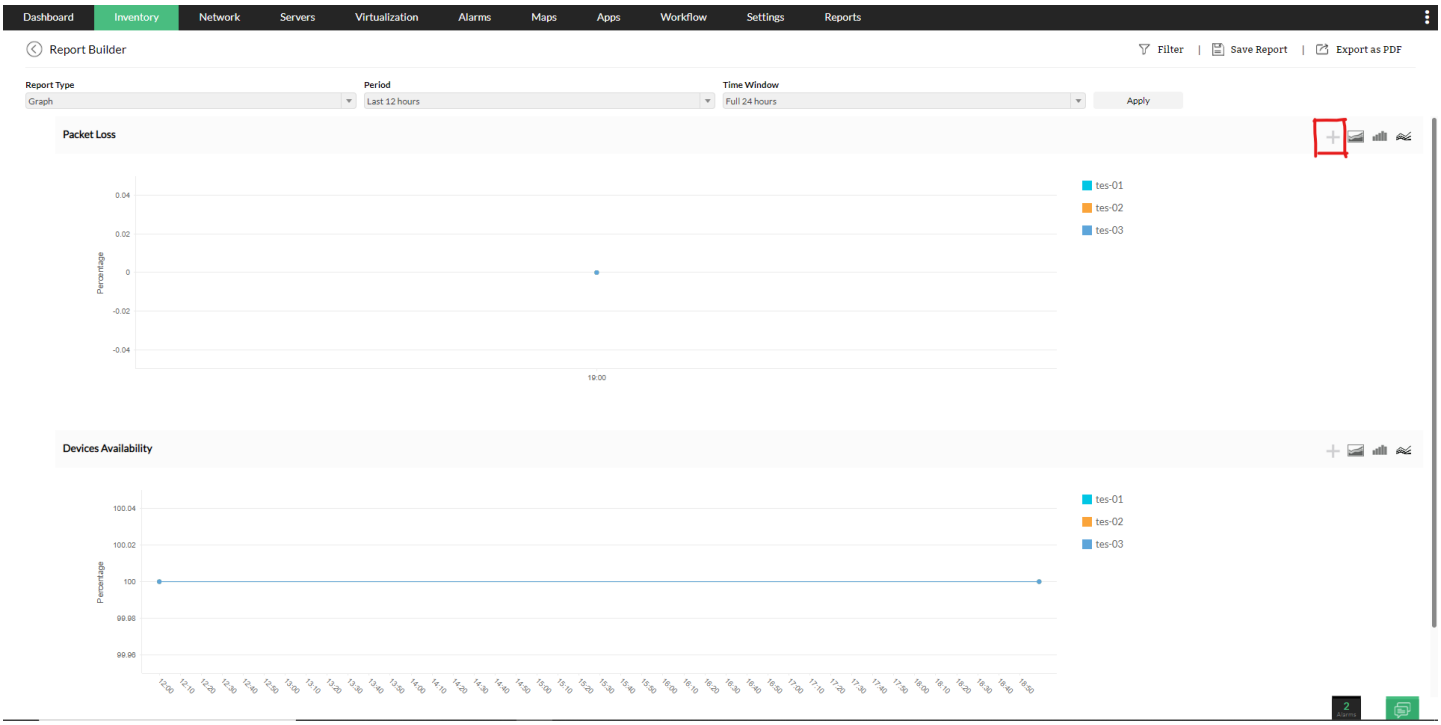
Adding Widgets from Report Builder

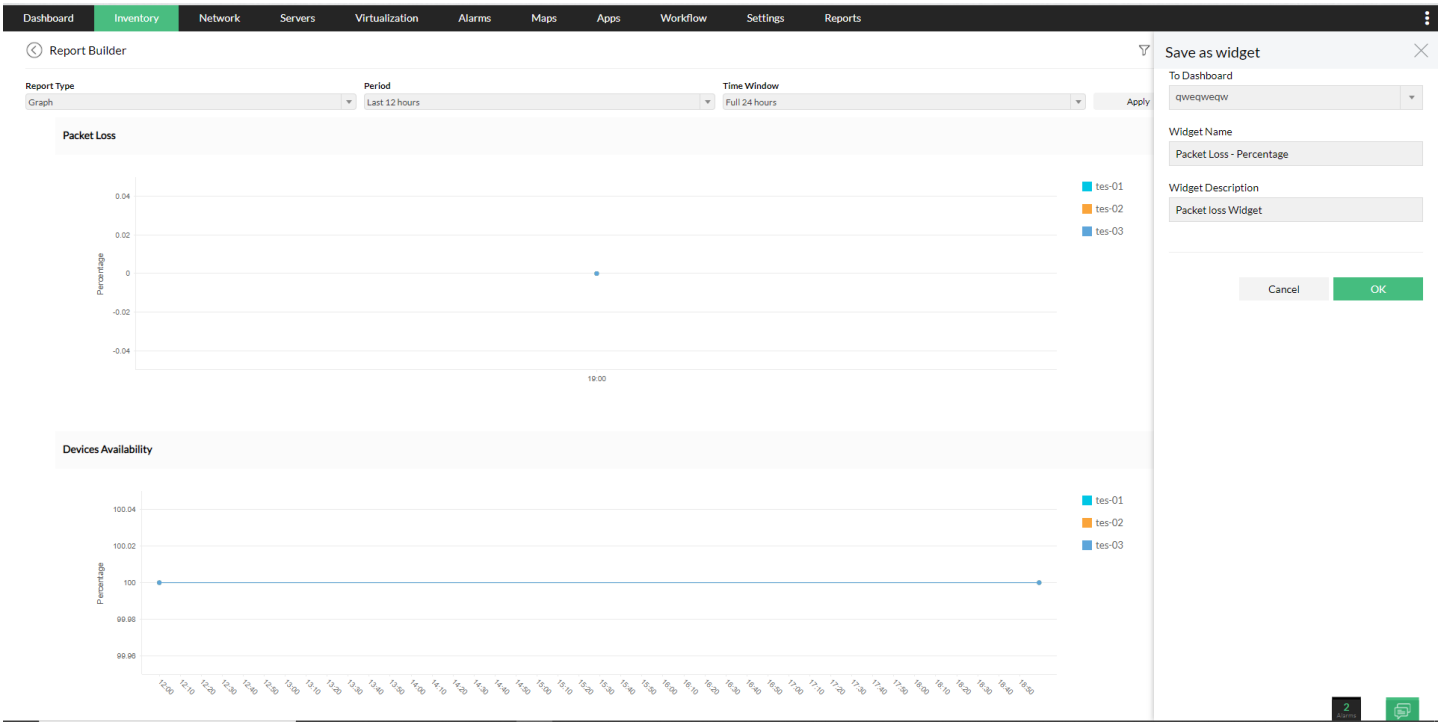
You can also add widgets for specific set of devices and monitors using the 'Generate Reports' option:

1. Create a **Custom Dashboard**. (if you dont have an existing Custom Dashboard or If you want a new Custom Dashboard for these widgets)
2. Go to **Inventory** -> **Devices** -> select the check box next to '**Device Name**' for one or more devices.
3. Click on the '**Generate Reports**' option on the top right.
4. Choose the desired '**Report Type**' and '**Time Period**' for these reports
5. Now choose the desired Monitors for these devices and click on '**Generate Report**'.
6. Now click on the Add as widget or the '**+**' button in the report builder screen.
7. Select desired **Dashboard**, **Widget Name**, and **Description** and click '**OK**'.
8. You can now access this widget from the selected Custom Dashboard.


Dashboard
Inventory
Network
Servers
Virtualization
Alarms
Maps
Apps
Workflow
Settings
Reports
Devices (39)
Generate Reports
Device Name
Status
IP Address
Device Type
Category
Vendor
Interfaces
Discovered Time
OPM-Firewall1 UnManaged 172.21.2.101 Unknown Unknown Unknown 0 now
OPM-Router2 UnManaged 127.0.0.1 Unknown Unknown Unknown 0 now
OPM-Router1 UnManaged 10.10.10.1 Unknown Unknown Unknown 0 now
OPM-AP1 Attention 192.168.50.50 Cisco 5508 AP Wireless Access Point Cisco 0 4 days ago
OPM-AP2 Attention 192.168.50.49 Cisco 5508 AP Wireless Access Point Cisco 0 4 days ago
OPM-AP5 Attention 192.168.50.46 Cisco 5508 AP Wireless Access Point Cisco 0 4 days ago
OPM-AP4 Clear 192.168.50.47 Cisco 5508 AP Wireless Access Point Cisco 0 4 days ago
OPM-AP3 Clear 192.168.50.48 Cisco 5508 AP Wireless Access Point Cisco 0 4 days ago
OPM_WLC31 Trouble 192.168.50.45 Cisco 5508 WLC Wireless LAN Controller Cisco 11 4 days ago
OPM-Server1 Service Down 172.24.128.61 ESXServer Server VMware 0 12 days ago
OPM-Server2 Service Down 172.24.128.60 ESXServer Server VMware 0 12 days ago
OPM-Router3 Critical 192.168.50.131 Cisco 2800 Series Router Cisco 5 12 days ago
OPM-Router4 Critical 192.168.50.140 Cisco 2900 IS Series Router Cisco 6 12 days ago
OPM-Firewall2 Critical 192.168.49.6 Juniper-SRX650 Firewall Juniper 37 12 days ago
UCSPE-172-24-158-248 Service Down 172.24.158.248 UCS System UCS Cisco 0 12 days ago
OPM-Server3 Clear 172.24.158.199 Windows 2012 Server Microsoft 0 12 days ago
OPM-Server4 Attention 172.24.159.50 Windows 2008 R2 Server Microsoft 21 12 days ago
OPM-Server5 Trouble 172.24.159.100 Windows 2012 R2 Server Microsoft 22 12 days ago
OPM-Server6 Clear 172.24.159.41 Linux Server net-snmp 0 12 days ago
OPM-Server7 Clear 172.24.159.40 Linux Server net-snmp 0 12 days ago
OPM-Server8 Clear 172.24.159.141 Windows 2012 R2 Server Microsoft 0 13 days ago
OPM-Server9 Trouble 172.24.159.204 Windows 2012 R2 Server Microsoft 0 13 days ago
OPM-Server10 Service Down 172.21.202.131 Linux Server net-snmp 0 13 days ago
OPM-Server11 Service Down 172.21.156.79 Linux Server net-snmp 0 13 days ago
OPM-Desktop1 Clear 192.168.49.1 Windows 8 Desktop Microsoft 31 13 days ago
OPM-RAID Service Down 172.21.155.155 NetApp Storage RAID NetApp 0 13 days ago
OPM-Firewall3 UnManaged 172.21.206.104 Fortigate Firewall Firewall Fortigate 0 13 days ago


Dashboard
Inventory
Network
Servers
Virtualization
Alarms
Maps
Apps
Workflow
Settings
Reports
Devices (39)
Generate Reports
Report Type
Graph View
Time Period
Last 12 hours
Choose Monitors
search
Devices Availability
Packet Loss
Response Time
AP Active User count(SNMP)
AP CPU Usage Avg(SNMP)
AP Memory Usage Avg(SNMP)
Generate Report

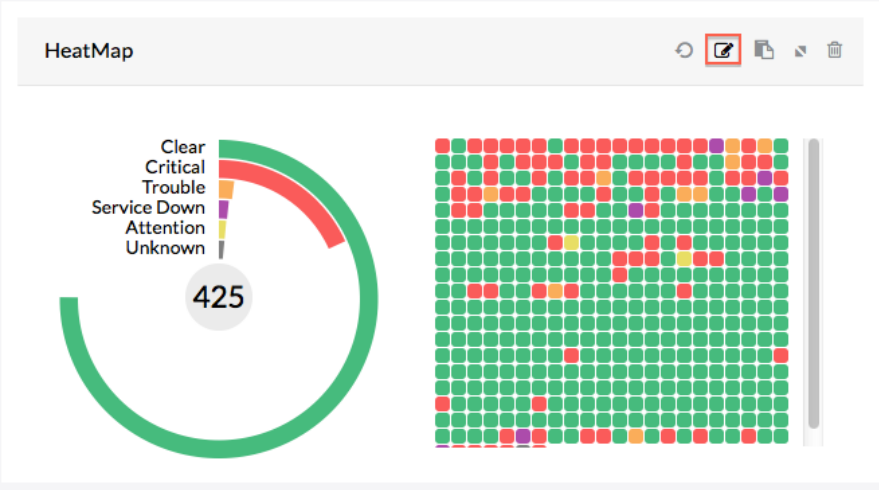


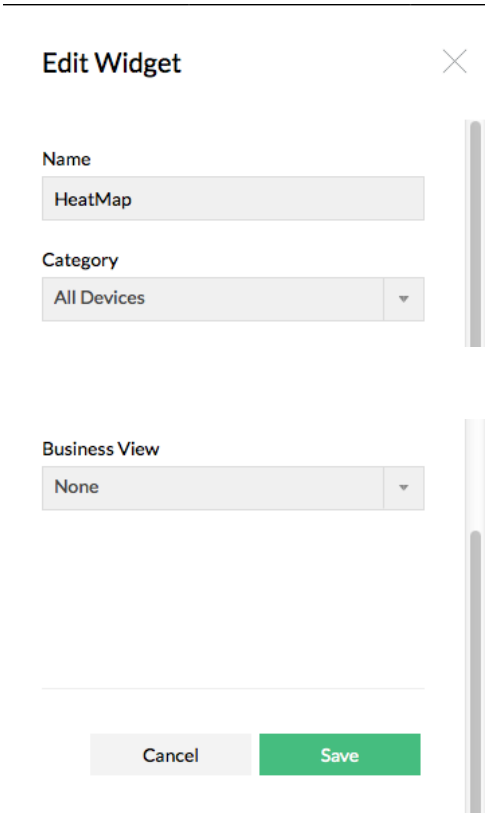


Editing Widgets

To modify the existing widgets go through the steps given below:

1. Click on the **Edit** against the widget on which you wish to modify the fields.
2. Modify the required fields.
3. Click **Save** to effect the changes.



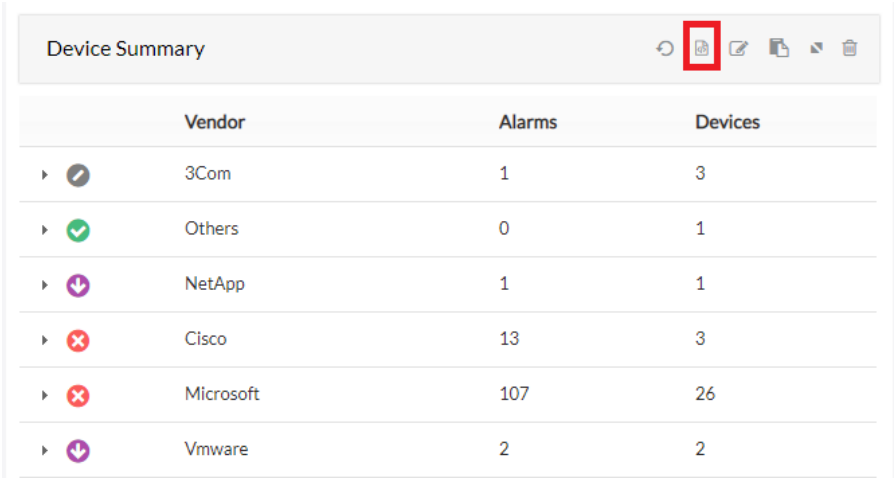


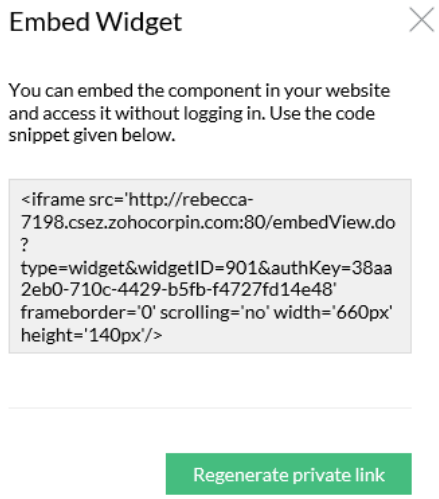
Embedding widgets

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.



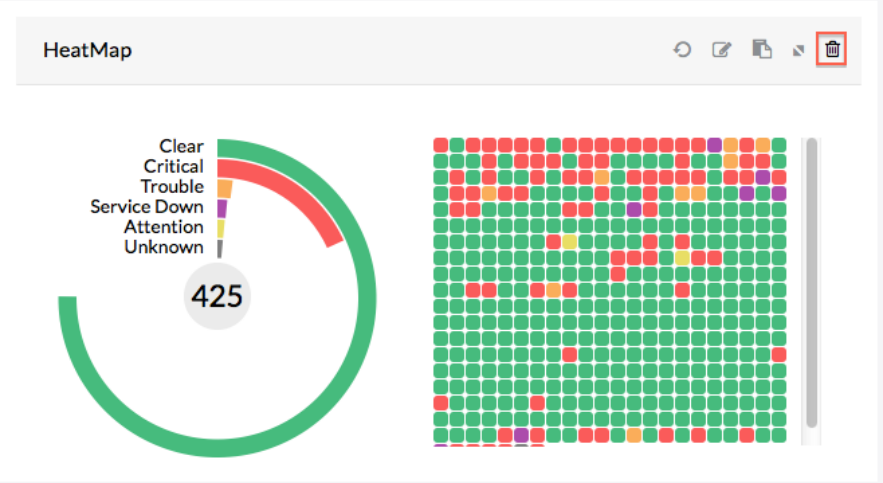


Note: The regenerate private link option generates a new authentication key for a widget. If you click on this option, the previously generated code snippet for the widget will no longer be valid.

Deleting widgets

To delete a widget go through the steps given below:

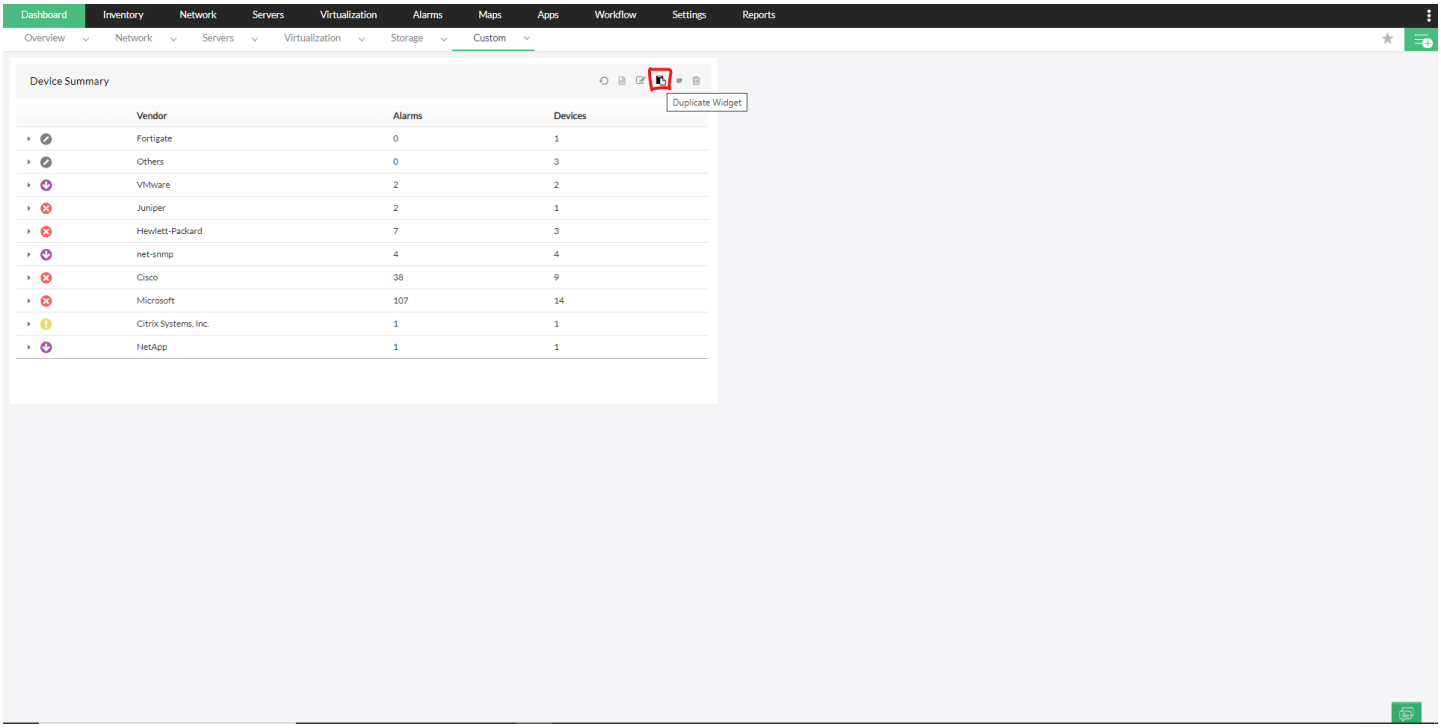
1. Click on **Delete** icon available on the widget box. A confirmation window pops up.
2. Click **OK** to confirm deleting the widget.

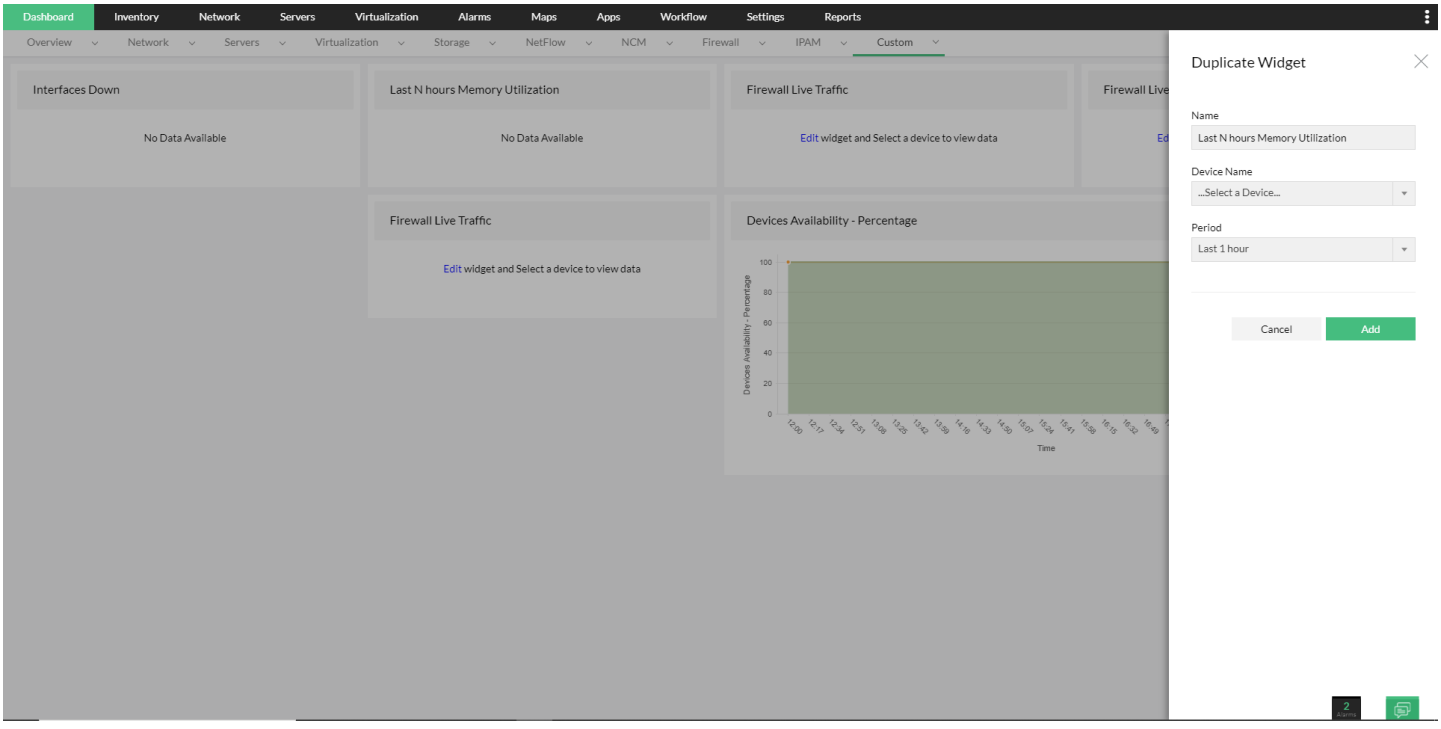


Duplicating Widgets

You can duplicate widgets that have already been added to use the same widget for another purpose:

1. Go to **Dashboard** -> **Custom** -> the Custom Dashboard containing the widget that you want to duplicate.
2. Hover your mouse pointer over the widget you want to duplicate, and click on the **'Duplicate Widget'** icon in the header.
3. Select the desired **'Name'**, time **'Period'**, **'Devices'**, **'Interval'**, and **'GraphUnit'** for the duplicated widget.
4. Click on the **'Add'** button to add the duplicated widget to the Dashboard.





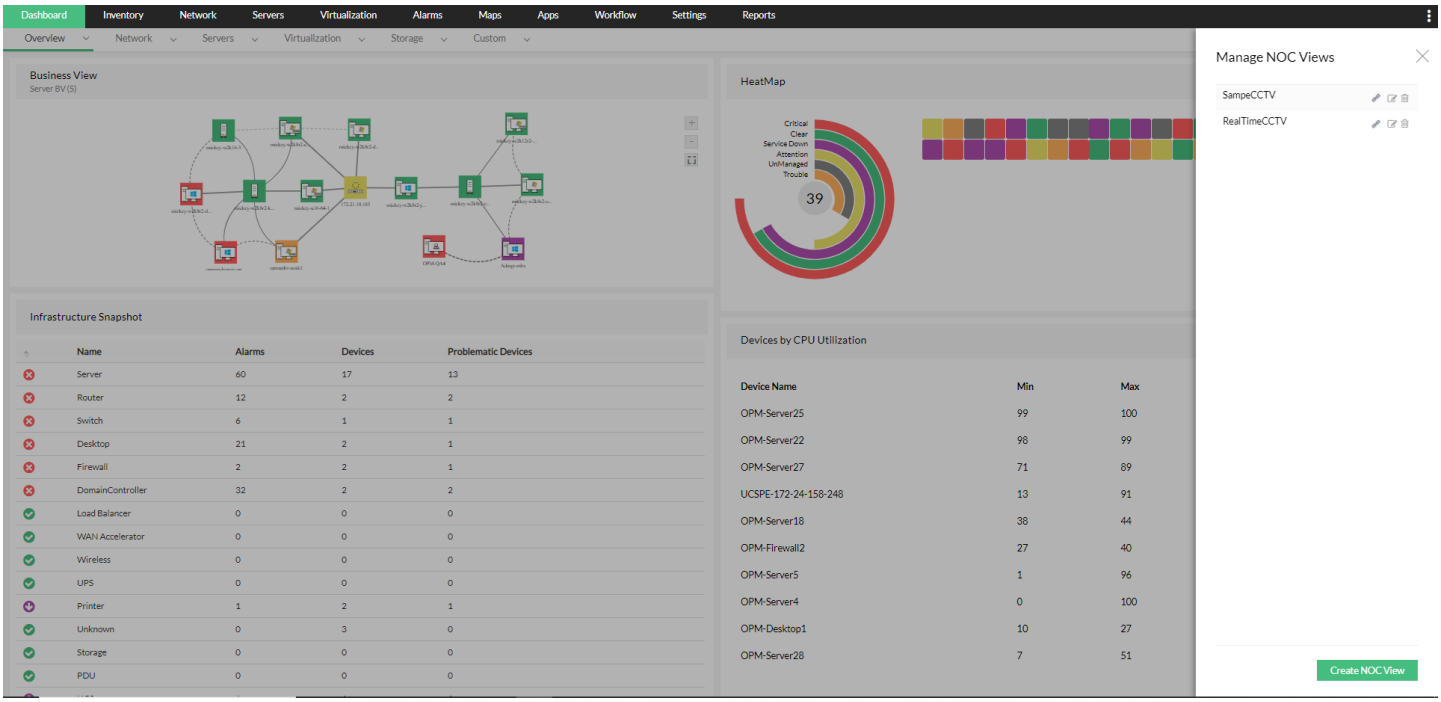
Repositioning Widgets

To reposition widgets:

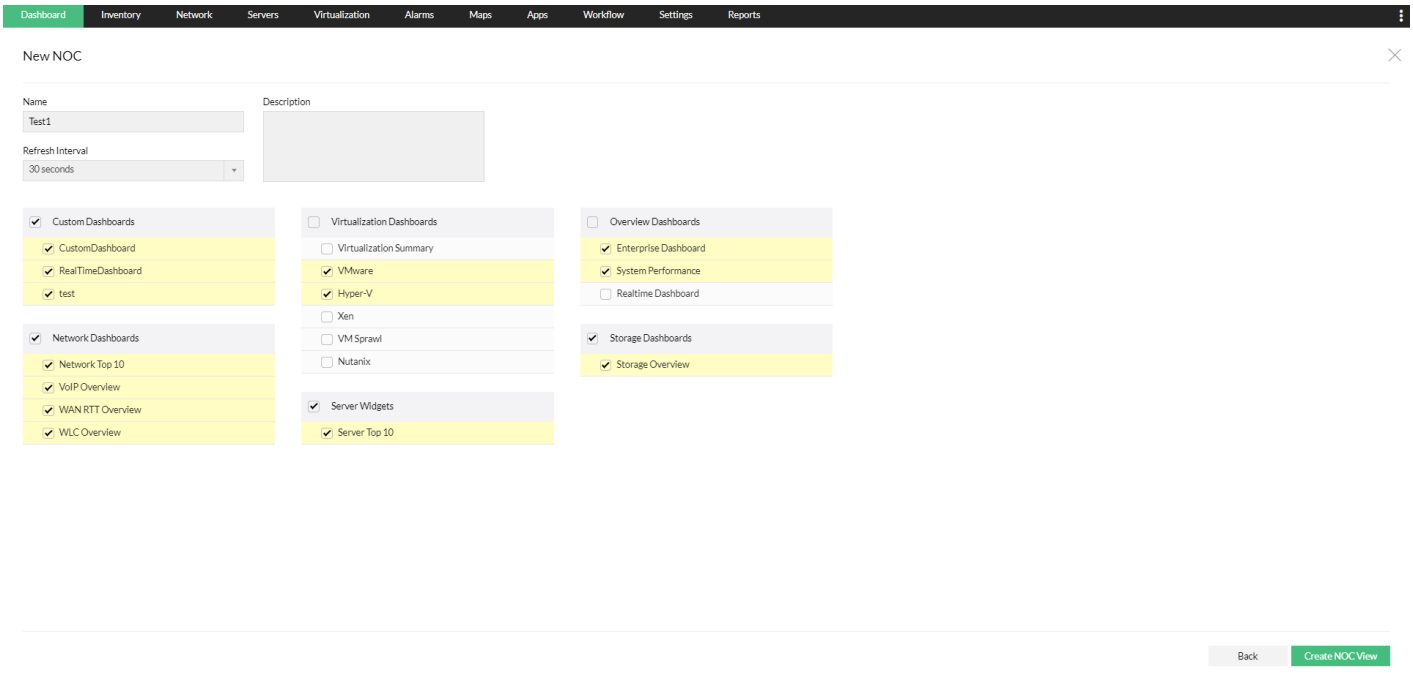
1. Go to **Dashboard** -> **Custom** -> choose the dashboard you want to reposition widgets for.
2. **Drag and drop** to change the position of the widgets.
3. Click '**Save**' on the top right.

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:

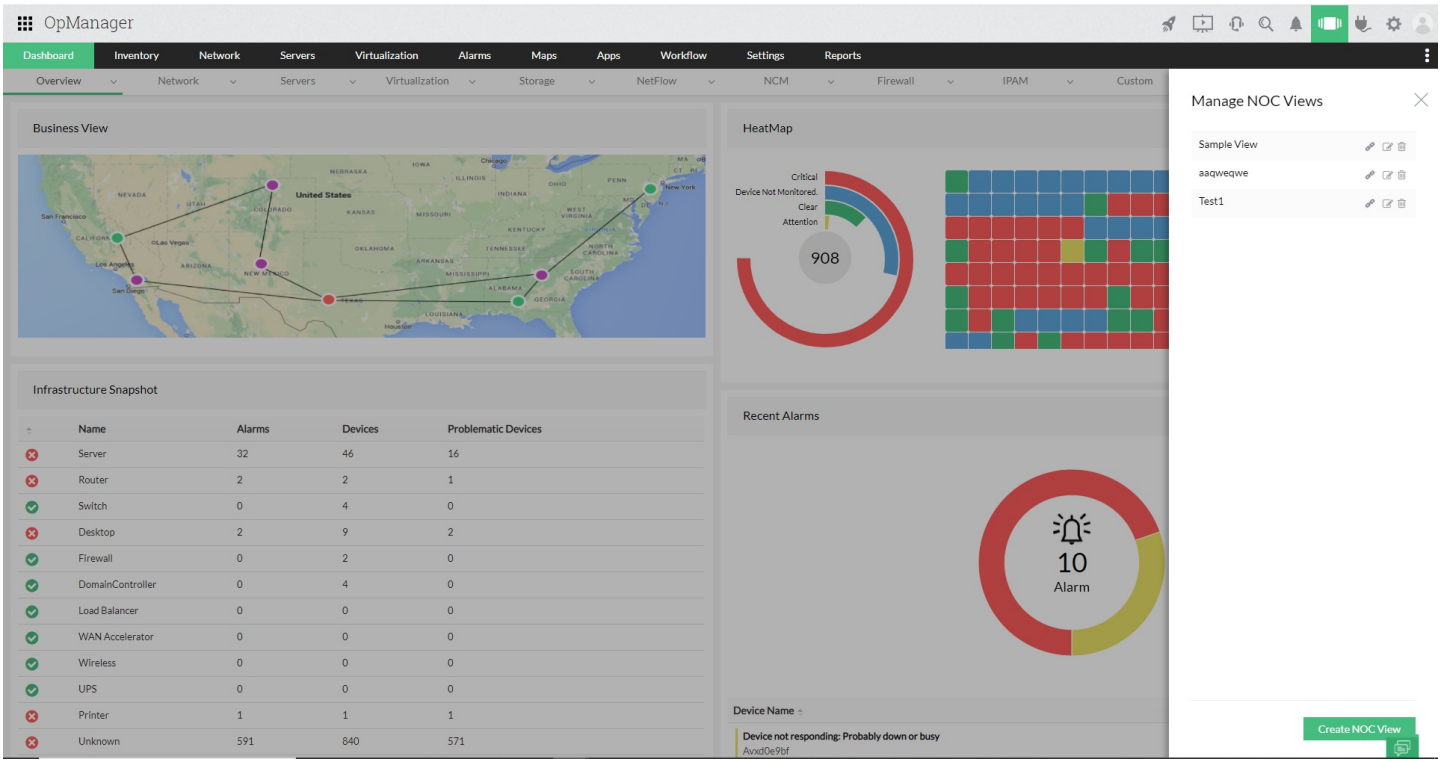


1. Go to **Dashboard** page and click NOC views**.**
2. Click **Create NOC View**. New NOC page opens.
3. **Name**: Enter a unique NOC name.
4. **Refresh Interval**: Select the interval required to switch over to the next dashboard.
5. **Description**: Enter a brief description about this NOC view.
6. 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

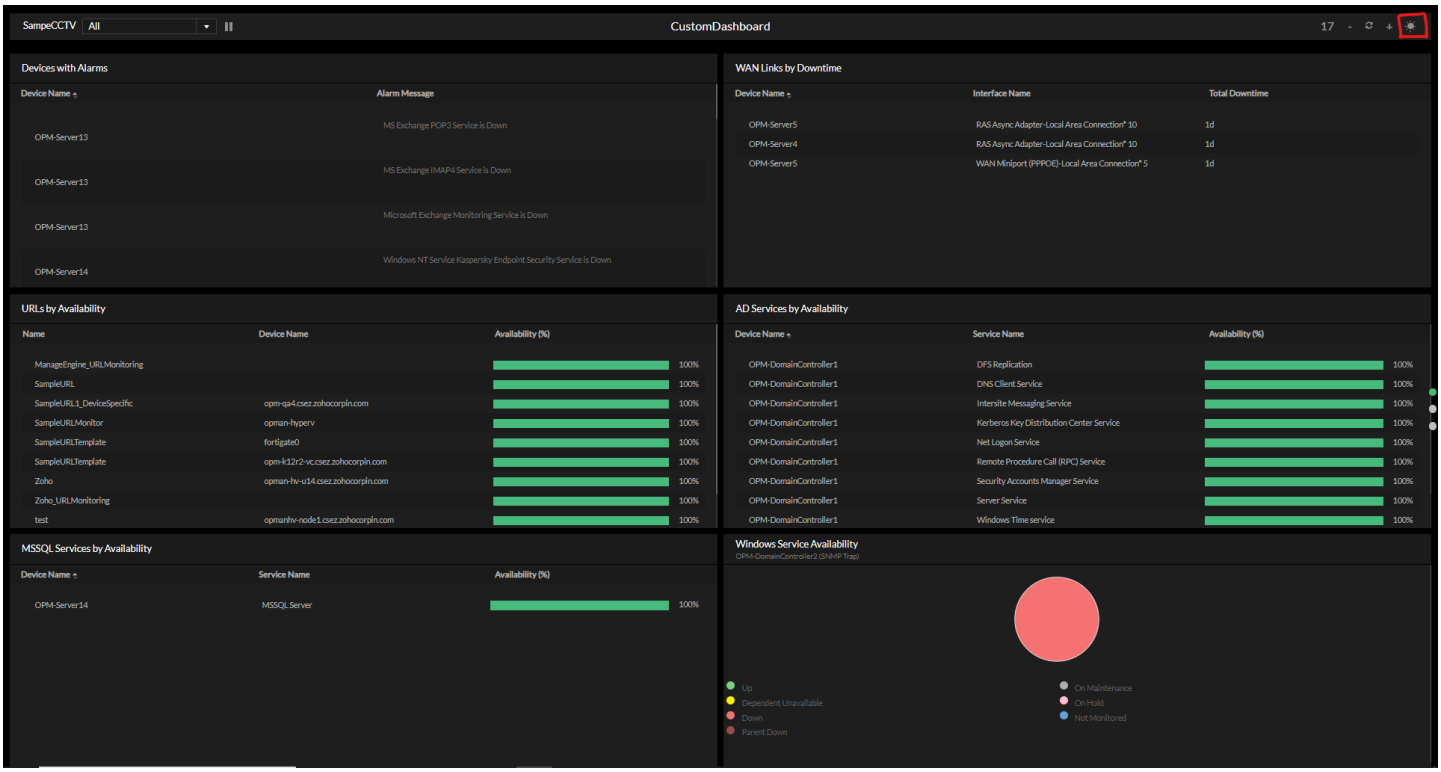
To edit a NOC view follow the steps given below:

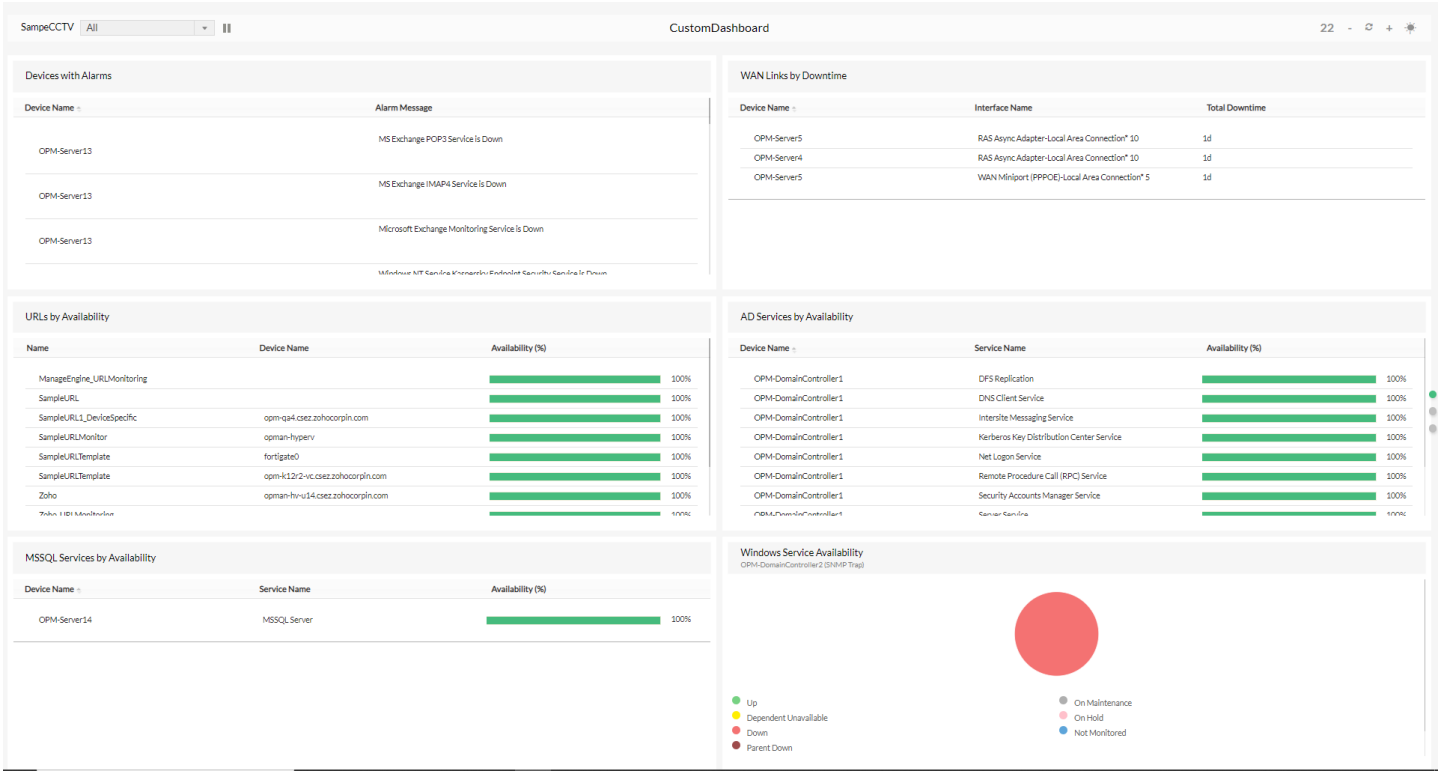
1. Go to **Dashboard** > **NOC Views** on the top right > Click on the edit icon against the NOC name that you want to edit.
2. Make the necessary changes.
3. Click **Edit NOC View** to effect the changes.

Day/Night view

To switch between the Day/Night views in NOC window:

1. Go to **Dashboard** > **NOC Views** > Click on the name of the NOC view that you want to view. That particular NOC view opens in a new window.
2. Click on the day/night icon in the top right to switch between Day and Night views.

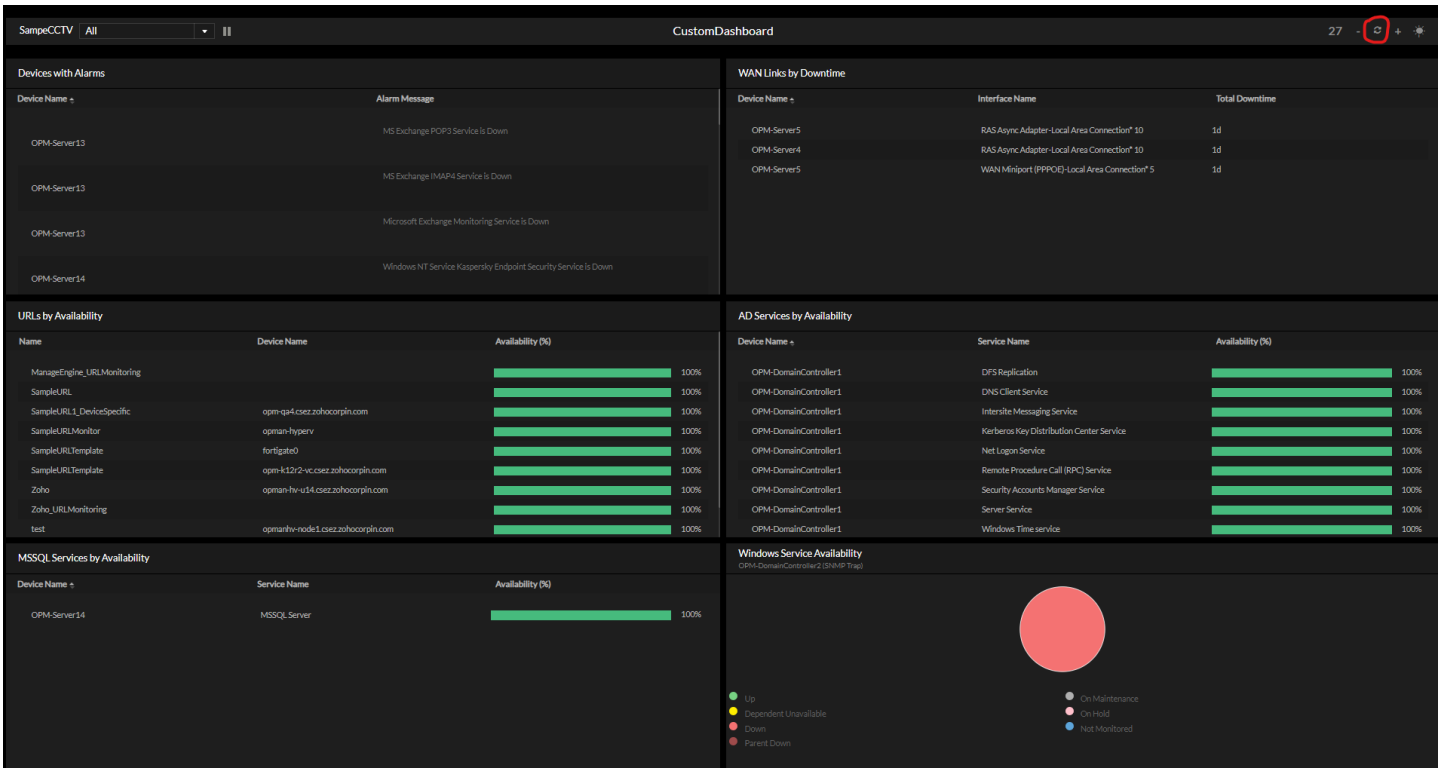




Resetting Refresh Interval

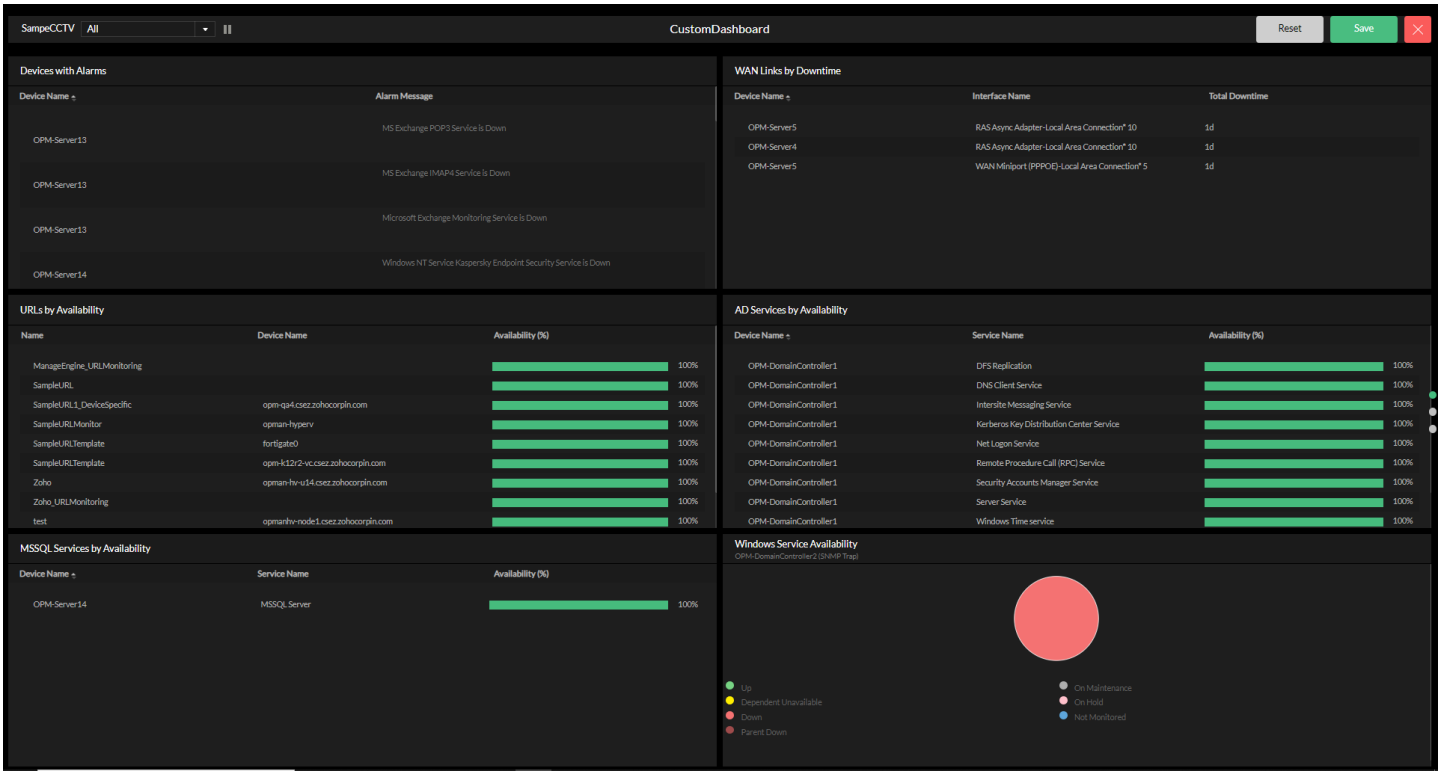
You can reset the refresh interval in the NOC window by clicking on the refresh interval icon on the top right. This also takes you back to the first page of the NOC window.

1. Go to **Dashboard** > **NOC Views** > Click on the name of the NOC view that you want to view. That particular NOC view opens in a new window.
2. Click on the Refresh Interval icon in the top right.



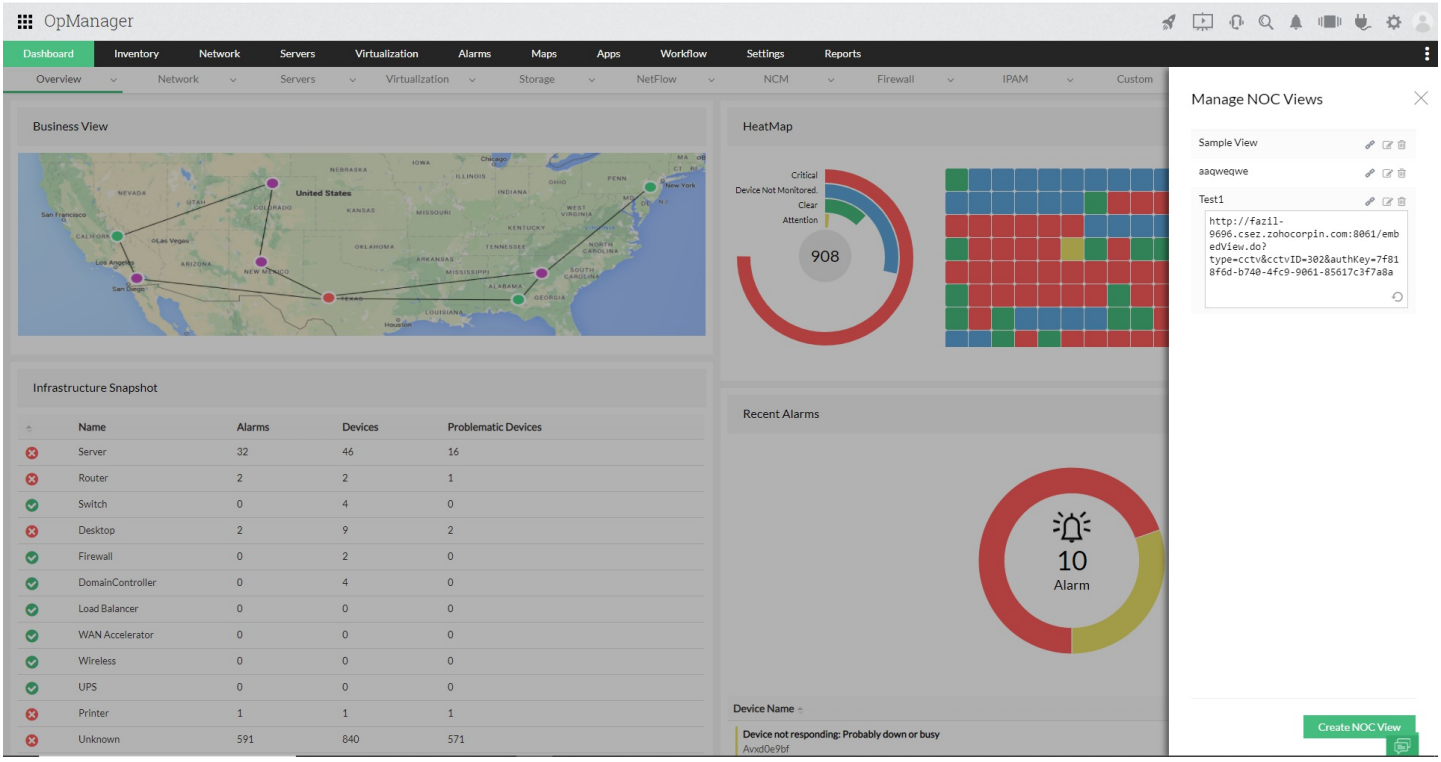
Reposition Widgets in NOC window

You can reposition widgets in the NOC window by means of a simple drag and drop. Click '**Save**' after you have repositioned the widgets for the changes to take effect.



Embedding a NOC view

To embed a NOC view link, follow the steps below.



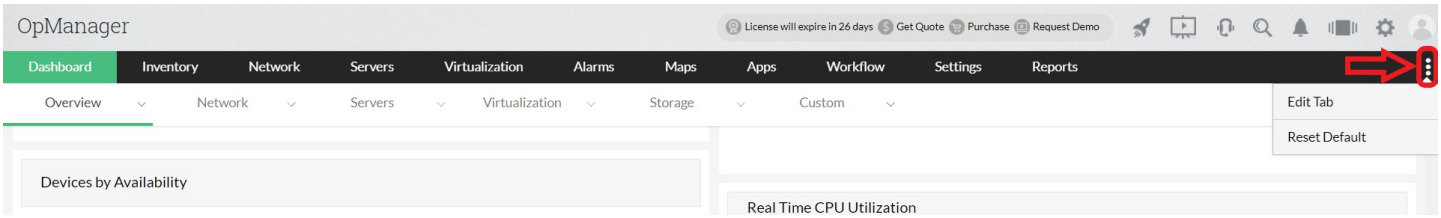
1. Go to the **Dashboard** page and click **NOC** Views on the top right.
2. Click the **Embed icon** present next to the **NOC Name**. The **Embed link** will be displayed.
3. Click the link to copy it to your clipboard. The **NOC Embed link** is ready to be shared.
4. Click the **Regenerative Private 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.
- You can access the specific NOC view using the embedded URL without logging into OpManager.

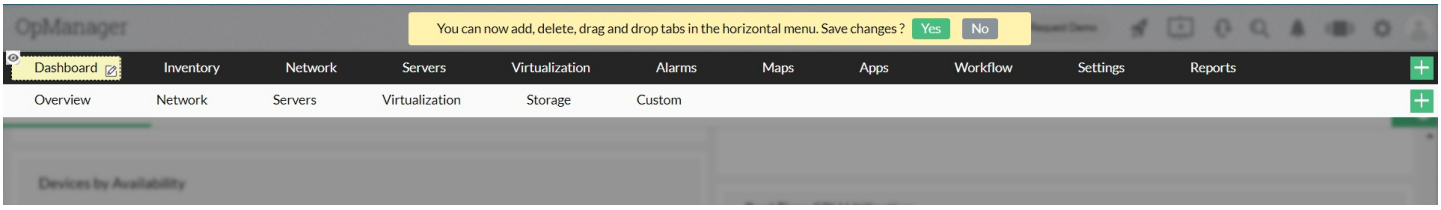
Menu Tab Customization

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.

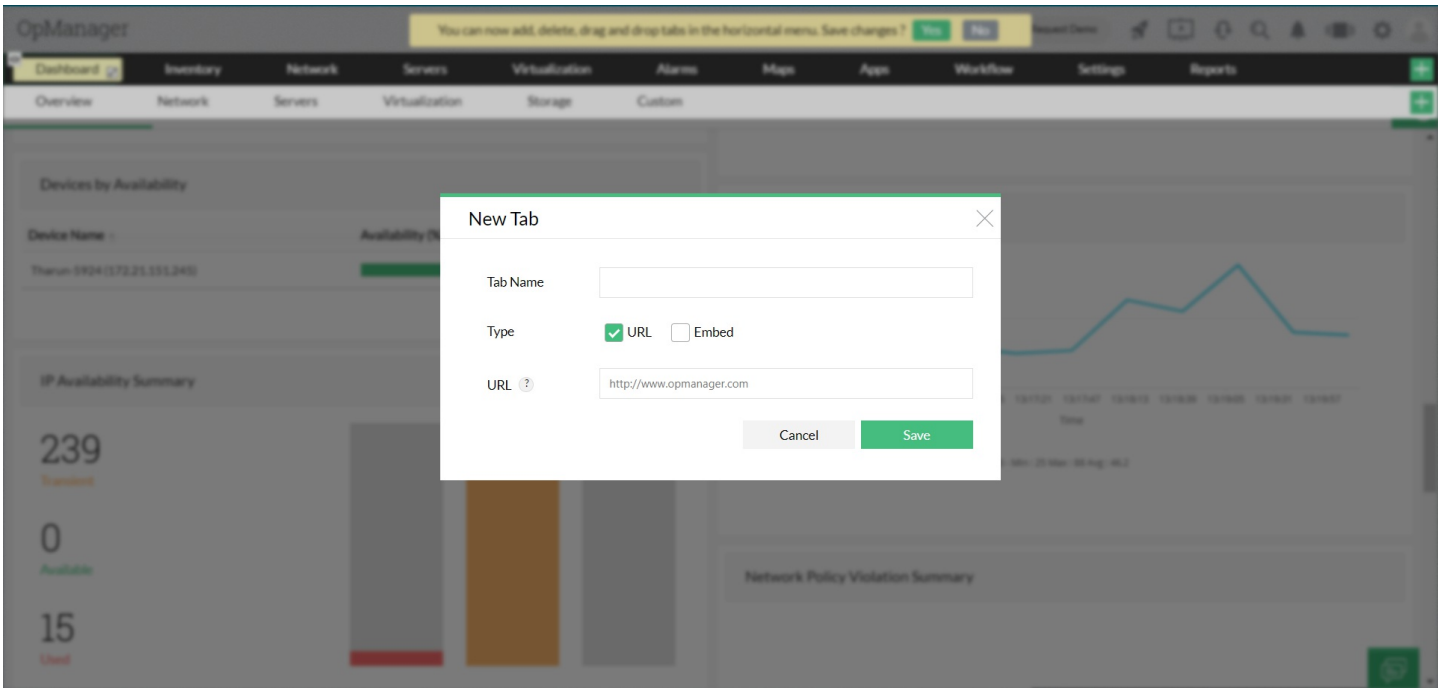


2. Add a menu / submenu tabs (with URL / Embed URL in it)

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.

Settings

Changing Password

- To change the login password, click on the **Settings ? 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 and Traditional), Japanese, French, German, Russian, Korean and Italian languages. The following are the steps to change the OpManager user interface from one language to another:

- To change the OpManager language, click **Settings icon ? Language Selector.**
- Select your preferred language.

Keyboard Shortcuts for Quick Navigation

Click **Client Settings icon ? Keyboard Shortcuts.**

/	Global search
SHIFT + D	Home Dashboard
ALT + I	Inventory
ALT + A	Alarms
ALT + M	Maps
ALT + W	Workflow
ALT + V	Virtualization
ALT + C	Clear Alarm
ALT + L	View Logs
ALT + Q	Submit Query
ALT + SHIFT + A	About
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 **Settings icon ? ServiceDesk Plus**
- Configure all the required parameters.
- Click **Save.**

Sending a screenshot feedback to OpManager support

- To send a screenshot feedback to OpManager support, click **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.**

Signing out as current user from OpManager client

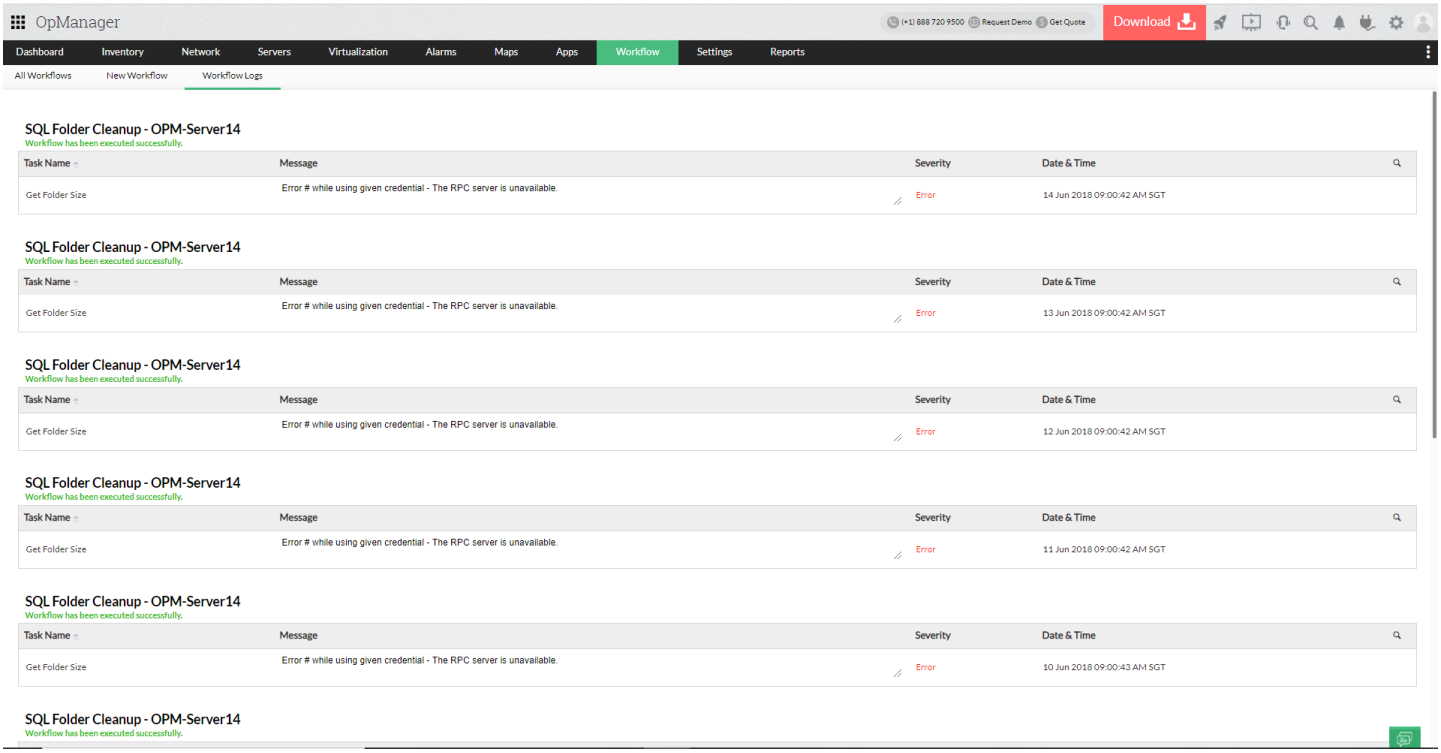
- To sign out as current user from OpManager client, click **Client Settings ? Sign Out.**

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 the**&#65533;** **Workflow&#65533;** tab and select **Workflow Logs**. Workflow output for each of the associated device is listed along with the executed date & time, the name of task and its severity status and message.



To view individual workflow logs:

- Navigate to **Workflow--> All Workflows**.**&#65533;**
- A list of workflows will be displayed.**&#65533;**
- Click on the second icon (*View Logs*) under the Actions column of a workflow to view the log of that particular workflow.

Severity

Each task once executed is logged with its severity for understanding its execution status. Following are the severities in Workflow:

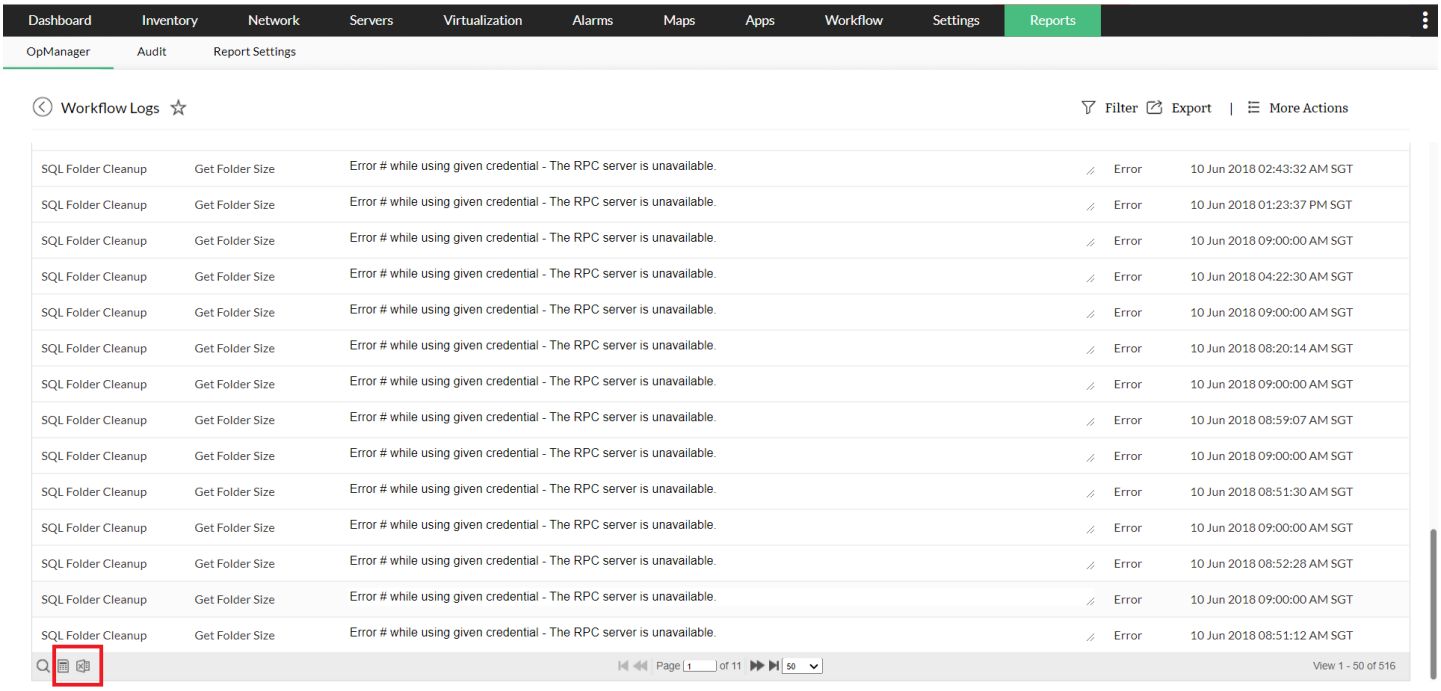
- **Info**: Notifies a task has been executed successfully.
- **Error**: Notifies a task has been failed.
- **Warning**: Notifies that a task cannot be performed. Eg.: A delete file action cannot be performed when the directory does not have the specified file. In such cases, the delete file actions is marked as warning

Exporting workflow logs

Users can export workflow logs in PDF and XLS formats. Follow the steps given below.

- Navigate to **Reports--> System --> Workflow logs**.

- Scroll down to the end.
- Click on the icon Export as CSV/ Export as Excel to download the report.



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	
Test a Process	Test whether a process is running or not.
Actions	
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.
HTTP & FTP	
Check	
Check URL	Test the availability of a URL.
Actions	
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.
File	
Checks	
Check File	Checks the availability of a file.
Get File Size	Gets the size of a file.
Actions	
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.
Folder	
Checks	
Check Drive Free Space	Checks for free space available in a drive.
Get Folder Size	Gets the size of a folder.
Actions	
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.
VMware	
Actions	
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.
OpManager	
Check	
Check Device Status	Checks the availability status of a device.
Actions	
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.
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. 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.

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 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

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. OpManager will replace this variable during runtime. Supported Variables : ${DeviceName} - will replace the executing devicename druing 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.
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 OpManager temporary directory during runtime.
Response Timeout	Timeout interval for the response from the device for the script execution status.

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.

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

OpManager sends in a slack message as a notification for the completion of a task in the workflow.

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.

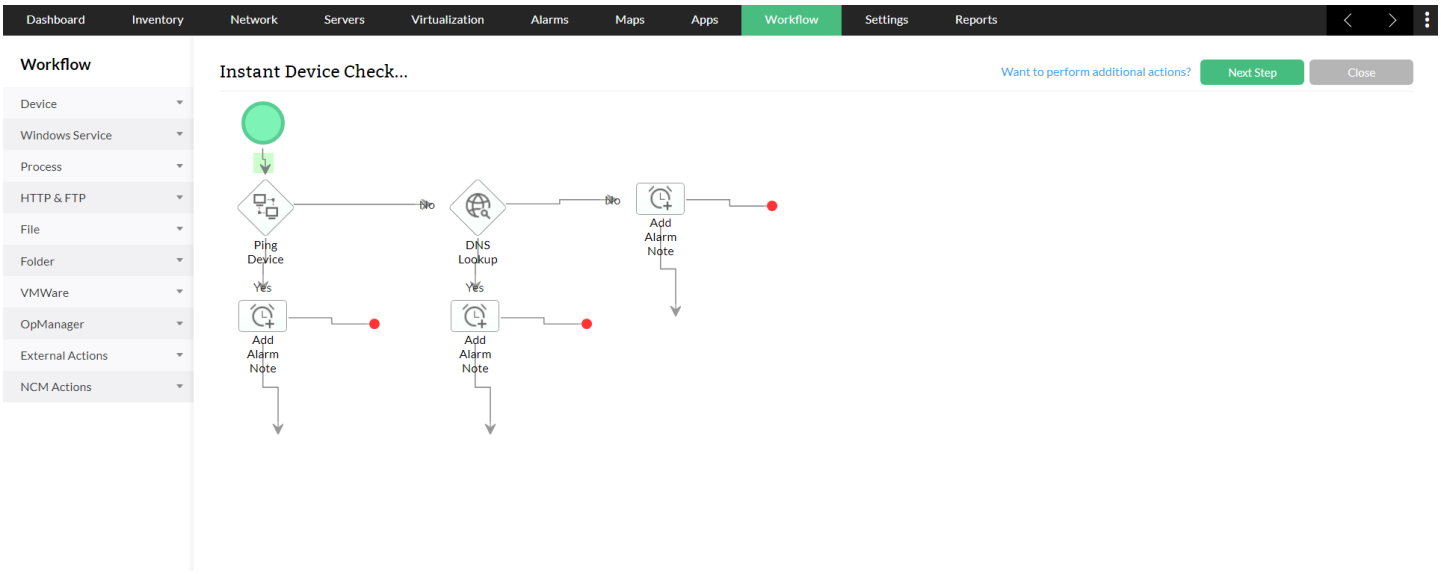
${Device.DisplayName} - Display name of the device for which an alarm is raised.

${Alarm.ProcessName} - Name of the process for which an alarm is raised.

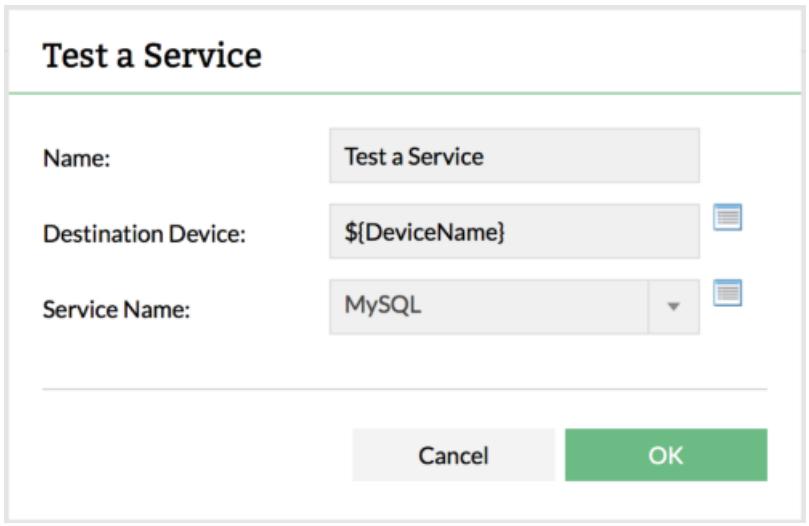
$message - Alarm message will be displayed

Using Variables

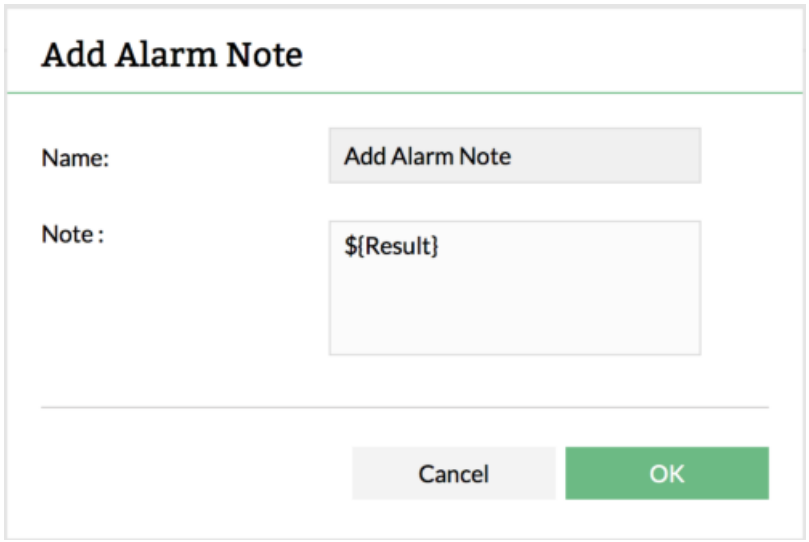
Variables can be better understood with an example. Following is the workflow that has to be triggered as an action whenever a service down alarm is raised.



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



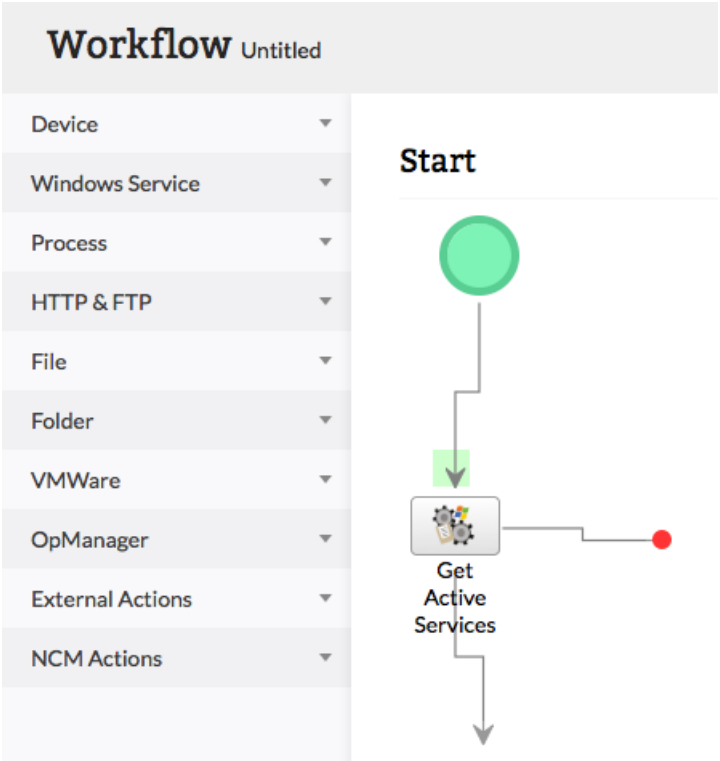
Task 2: The result of previous task (service up or down) is added as notes to the alarm using ${Result} variable.



Adding a Workflow

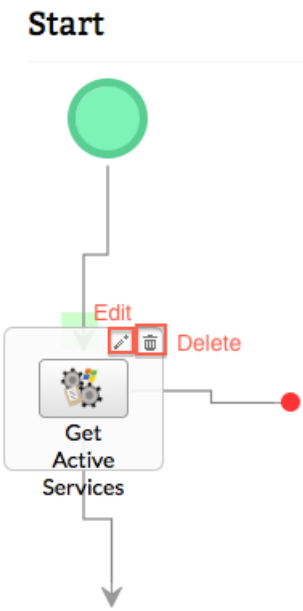
To add a workflow, follow the steps given below:

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.





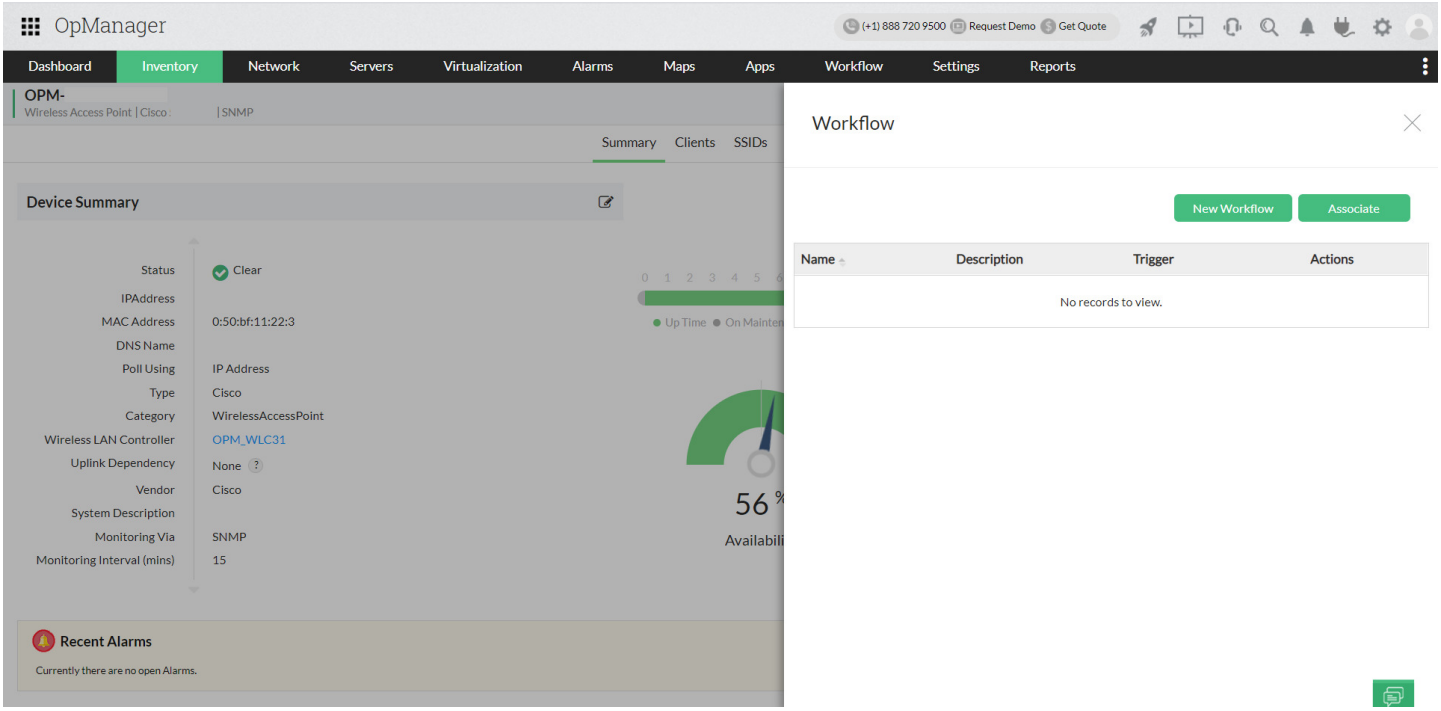
1. Click **Trigger**&#65533; at the top of the page.&#65533;
2. Associate the workflow to the devices.
    a. Click on the&#65533; **Devices** tab.
    b. Select the devices in Available Devices column and move to Selected devices column. Use the search box to search the devices.
    c. Click **Next**
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?

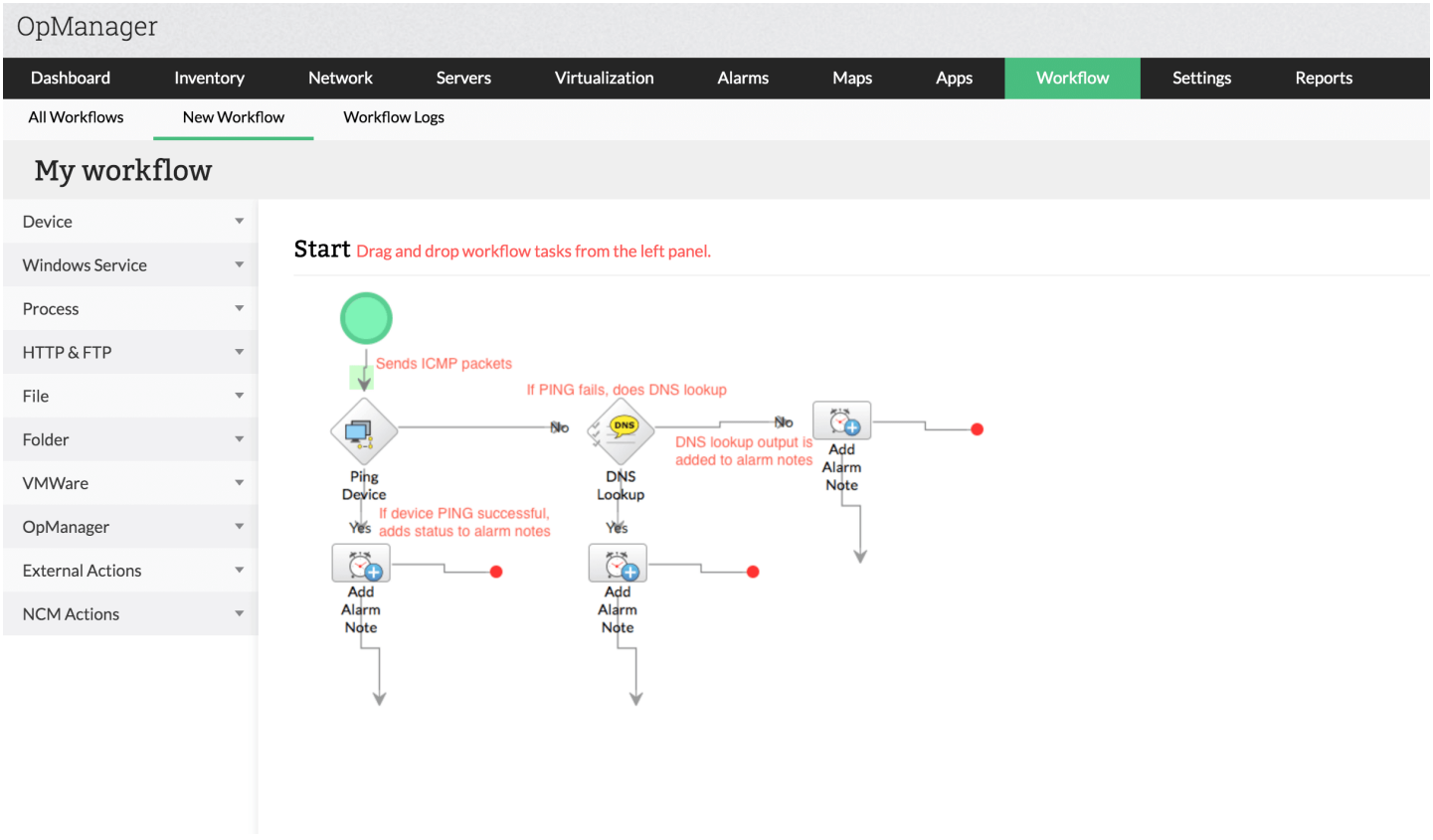
- Navigate to **Inventory** --> **Devices**.
- Click on a particular device, to open its corresponding snapshot page.
- On the top right tab having a list of icons click the workflow icon.
- Click on **New Workflow**. (This will take you to the Workflow page in OpManager)
- You can design your own workflow here.

&#65533;



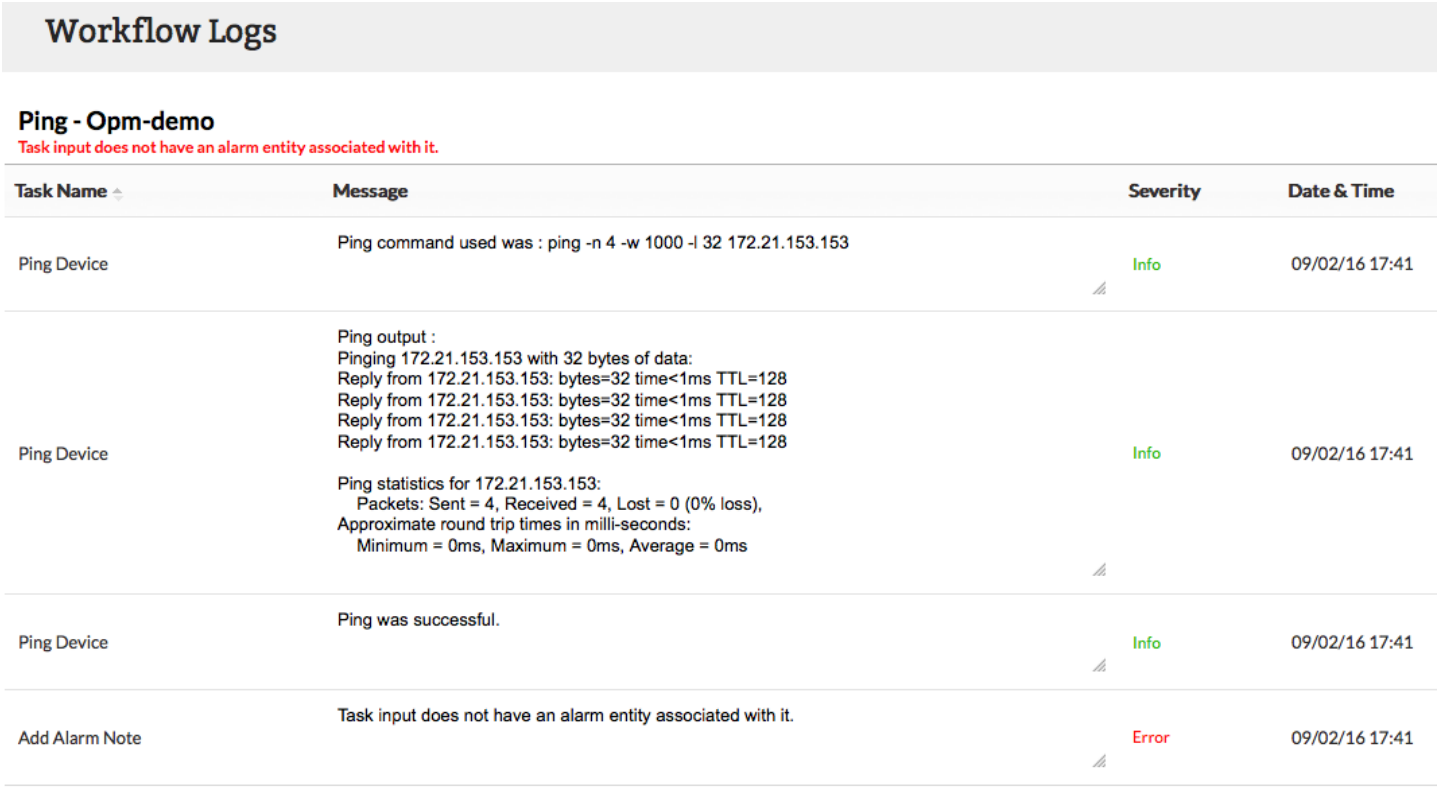
Sample Workflow

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.**

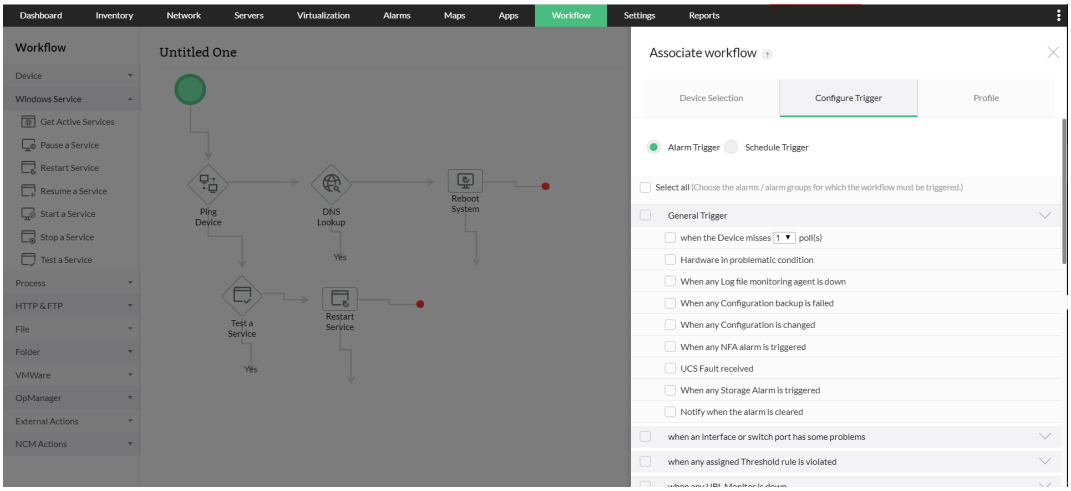
Triggers in Workflow

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

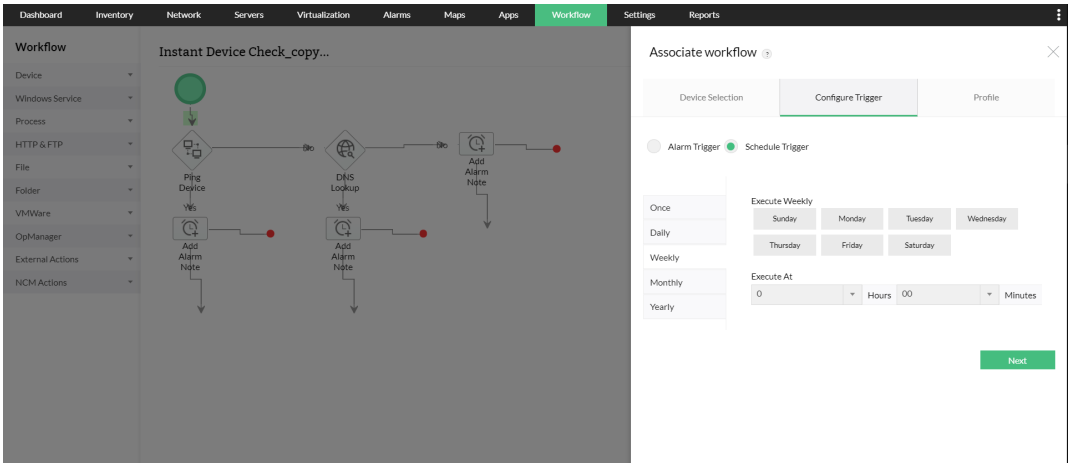
Alarm Trigger

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.

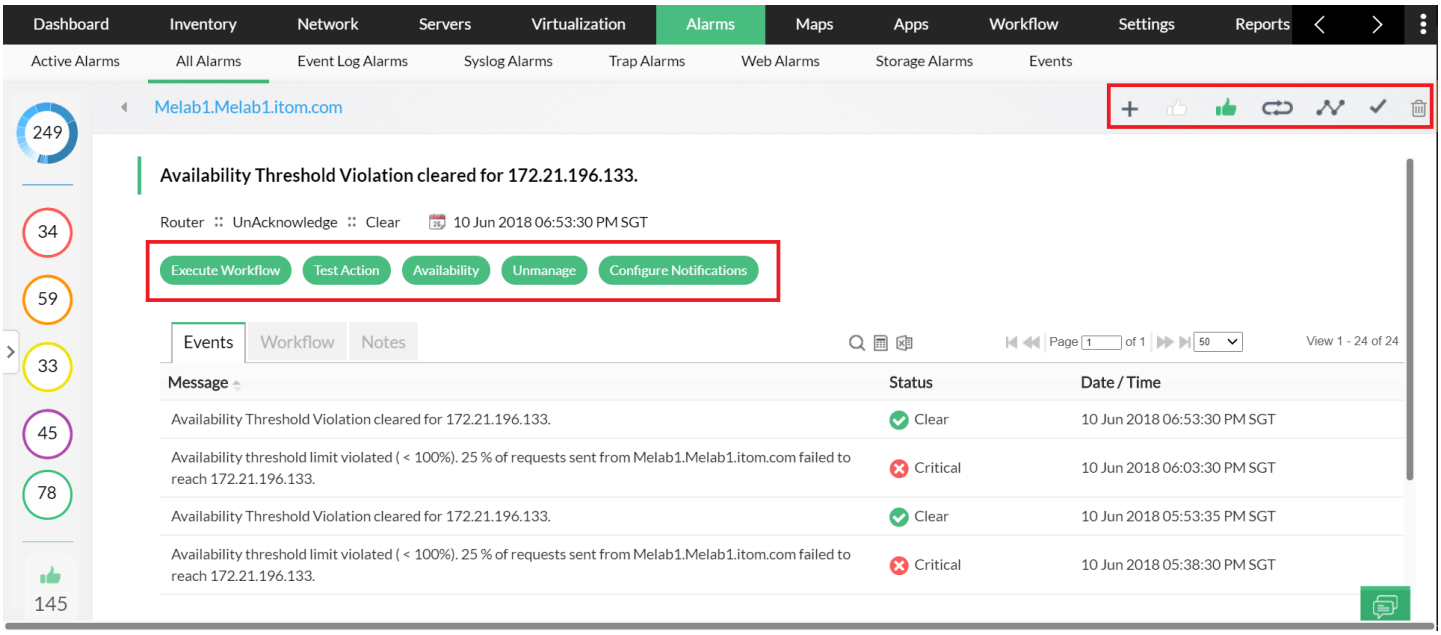
Alert Actions

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.
- **RDP:** Perform a remote desktop action to the monitored machine via Remote Desktop Protocol (RDP). Applicable only for WMI based devices.


Dashboard
Inventory
Network
Servers
Virtualization
Alarms
Maps
Apps
Workflow
Settings
Reports
Active Alarms
All Alarms
Event Log Alarms
Syslog Alarms
Trap Alarms
Web Alarms
Storage Alarms
Events
249
34
59
33
45
78
145
Melab1.Melab1.itom.com
Availability Threshold Violation cleared for 172.21.196.133.
Router :: UnAcknowledge :: Clear
10 Jun 2018 06:53:30 PM SGT
Execute Workflow
Test Action
Availability
Unmanage
Configure Notifications
Events
Workflow
Notes
Page 1 of 1
50
View 1 - 24 of 24
Message
Status
Date / Time
Availability Threshold Violation cleared for 172.21.196.133.
Clear
10 Jun 2018 06:53:30 PM SGT
Availability threshold limit violated (< 100%). 25 % of requests sent from Melab1.Melab1.itom.com failed to reach 172.21.196.133.
Critical
10 Jun 2018 06:03:30 PM SGT
Availability Threshold Violation cleared for 172.21.196.133.
Clear
10 Jun 2018 05:53:35 PM SGT
Availability threshold limit violated (< 100%). 25 % of requests sent from Melab1.Melab1.itom.com failed to reach 172.21.196.133.
Critical
10 Jun 2018 05:38:30 PM SGT

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.

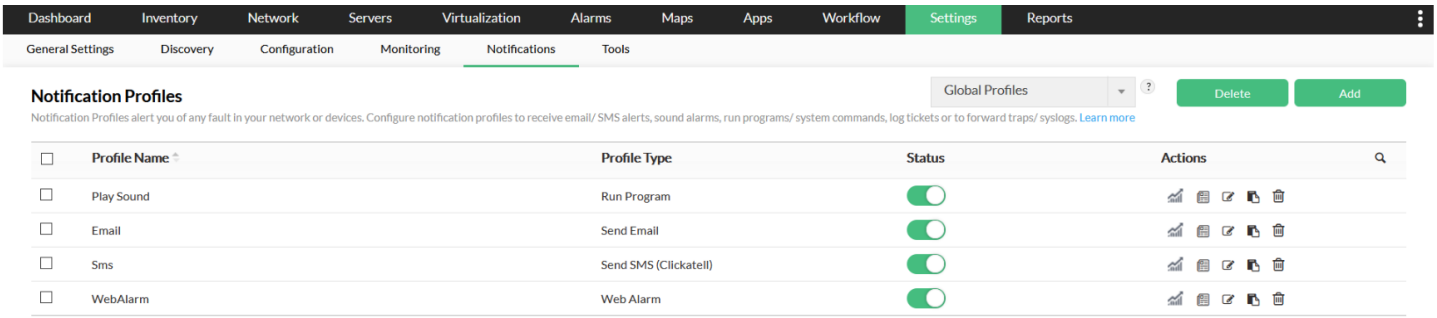
Other Configurations of Notification Profiles

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**'.

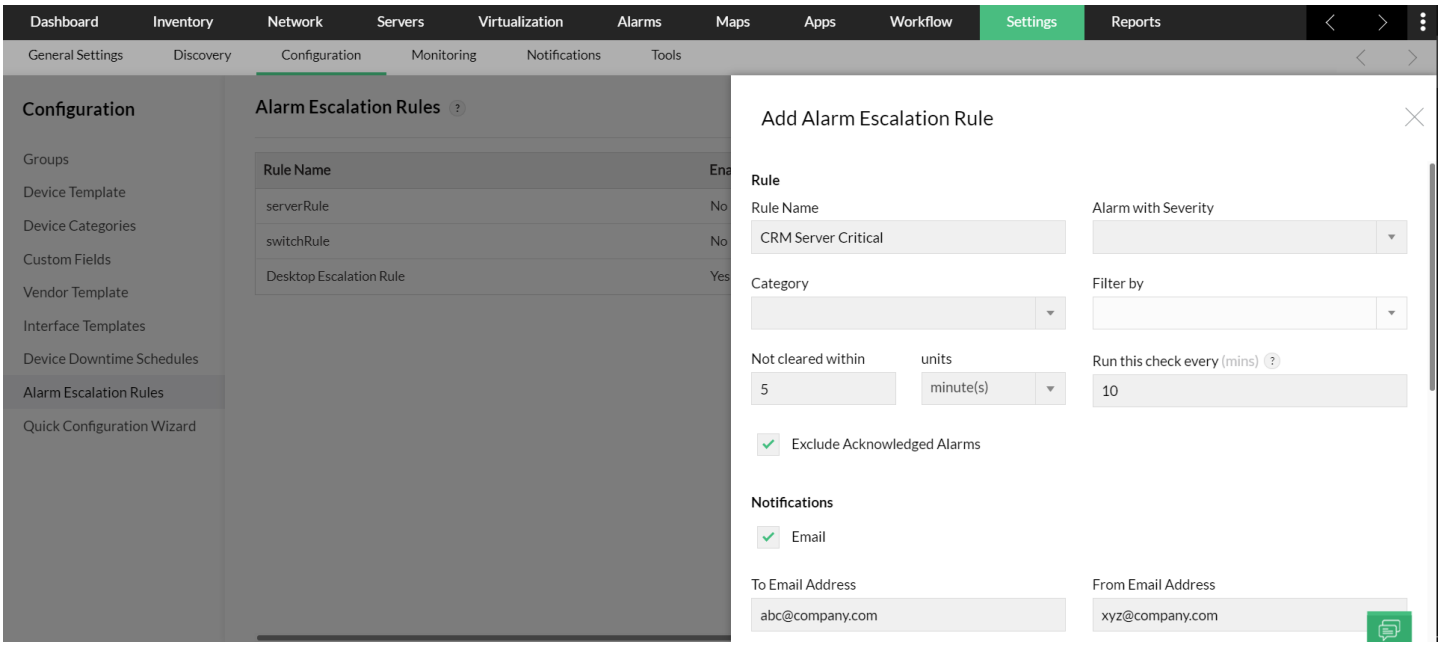
Now, you have successfully disabled a notification profile. If you wish to re-enable a notification profile, you simply enable it by clicking on the slider again.

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.

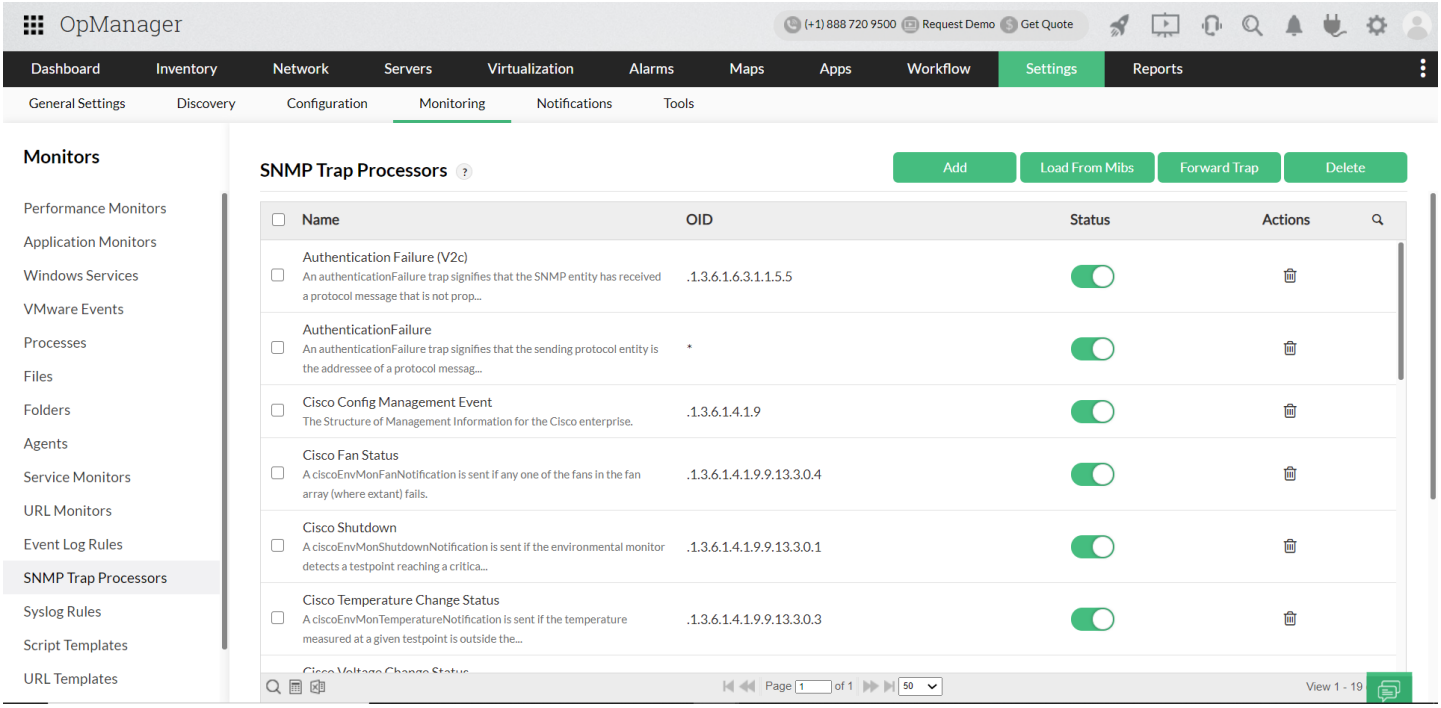
Processing SNMP Traps into Alarms
OpManager enables you to process the traps from the managed devices.

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:** 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.

- **SNMP V3 Properties:**
  - **Trap OID:** For devices with SNMP v3 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:** 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.

Loading Trap Parsers from a MIB

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

- Go to **Settings ? Monitoring ? SNMP Trap Processors**. 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.

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.

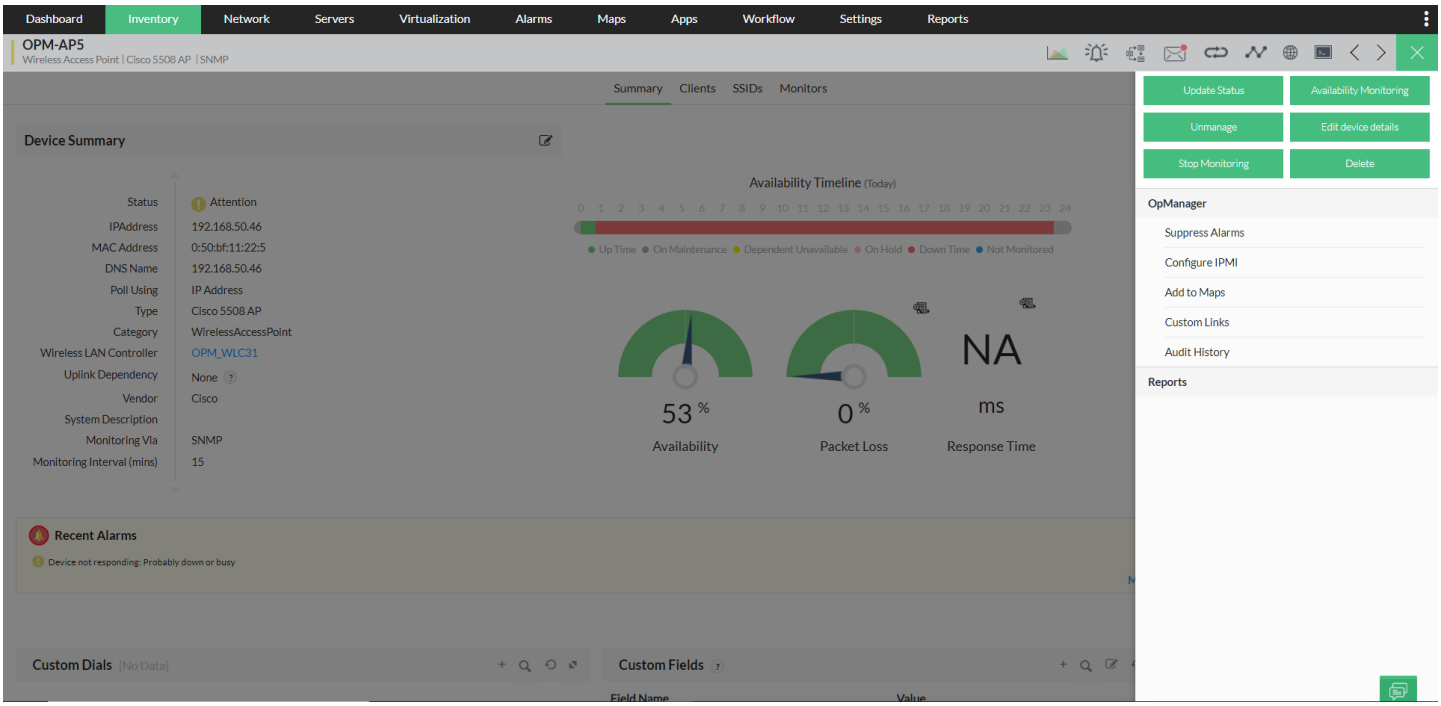
Receiving SNMP Traps in OpManager

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.

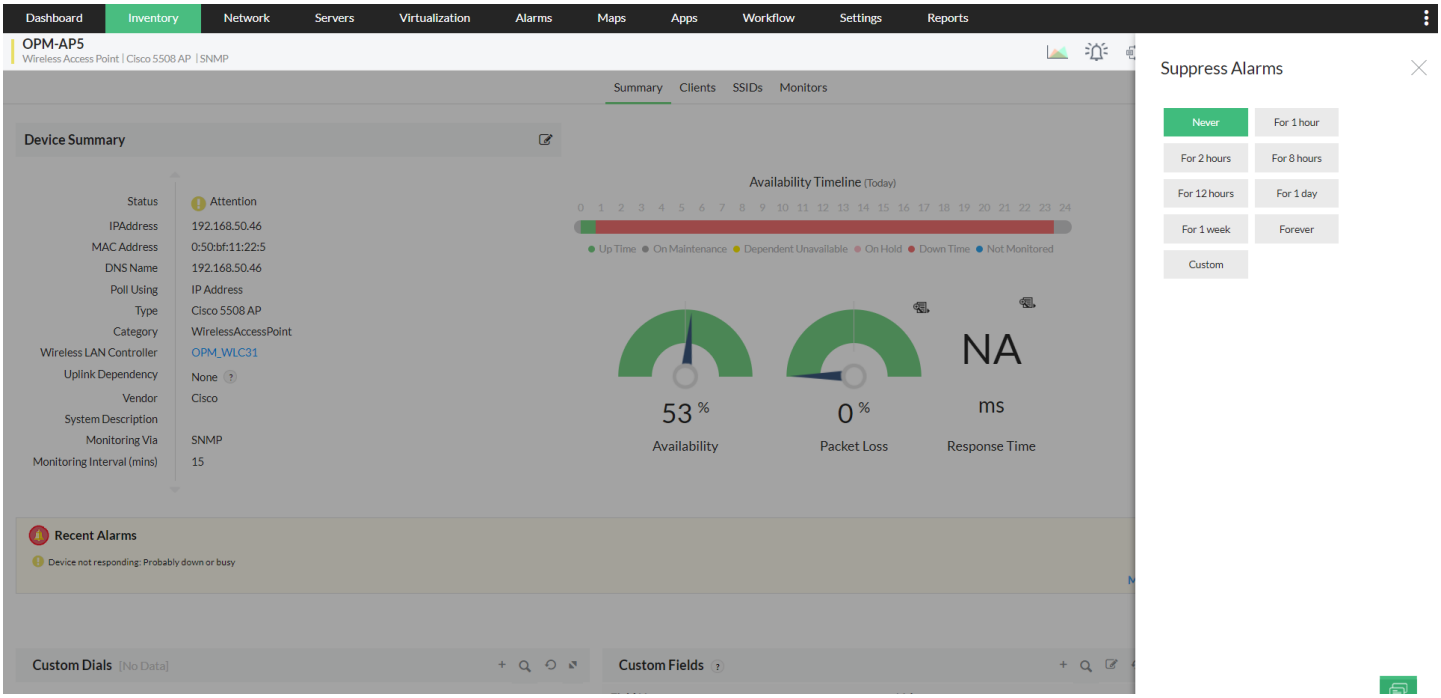
Alarm Suppression

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

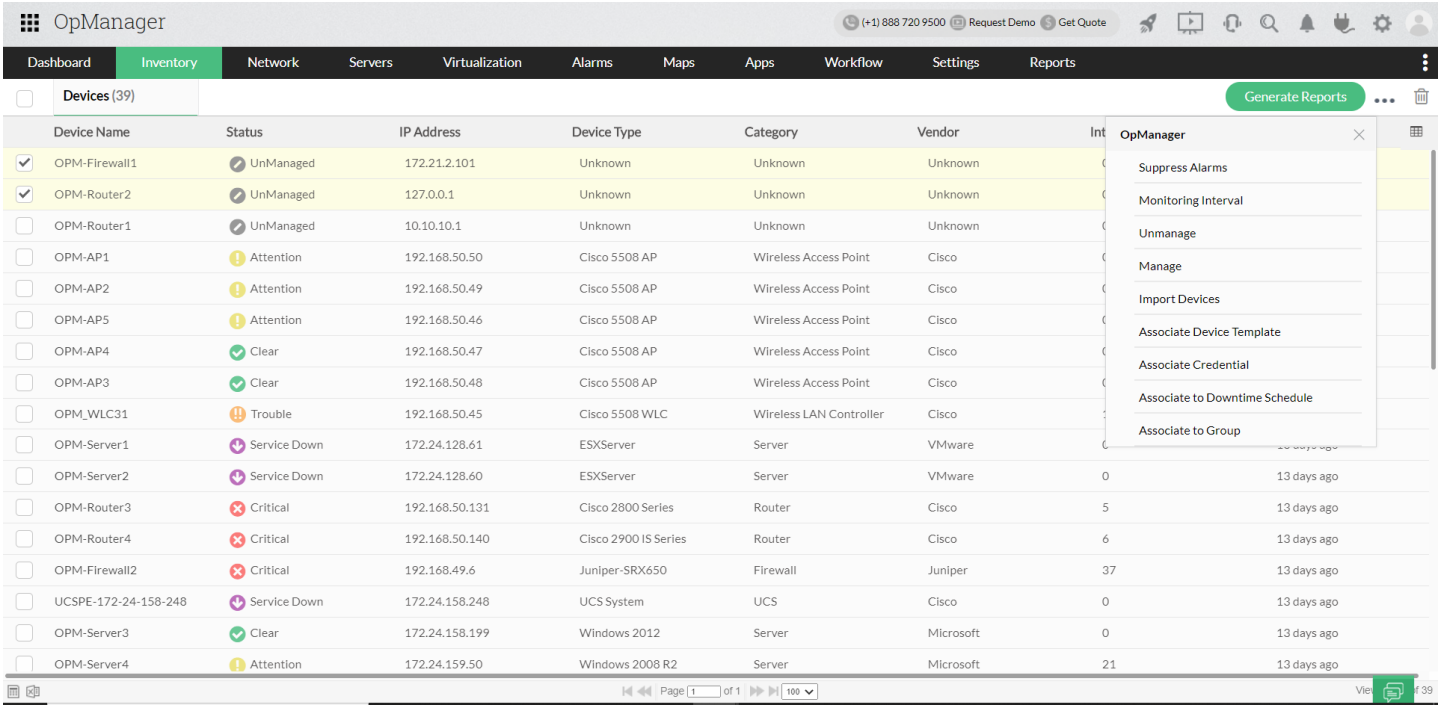


1. Go to the device snapshot page.
2. Click on **Actions** and select **Suppress Alarms**.
3. Select the period for which you want to suppress the alarm.

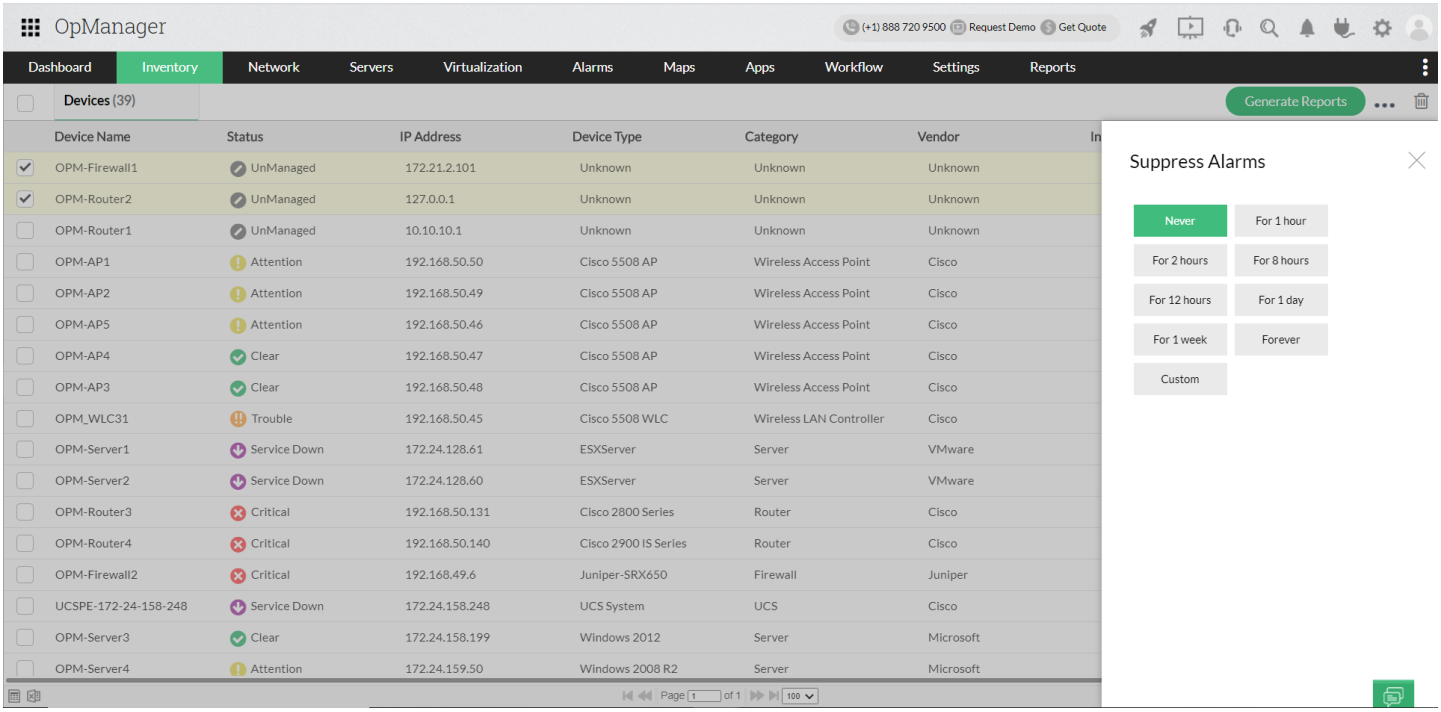


Alarms of this device will be suppressed for the selected period. You can also suppress alarms for devices in a bulk.

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.

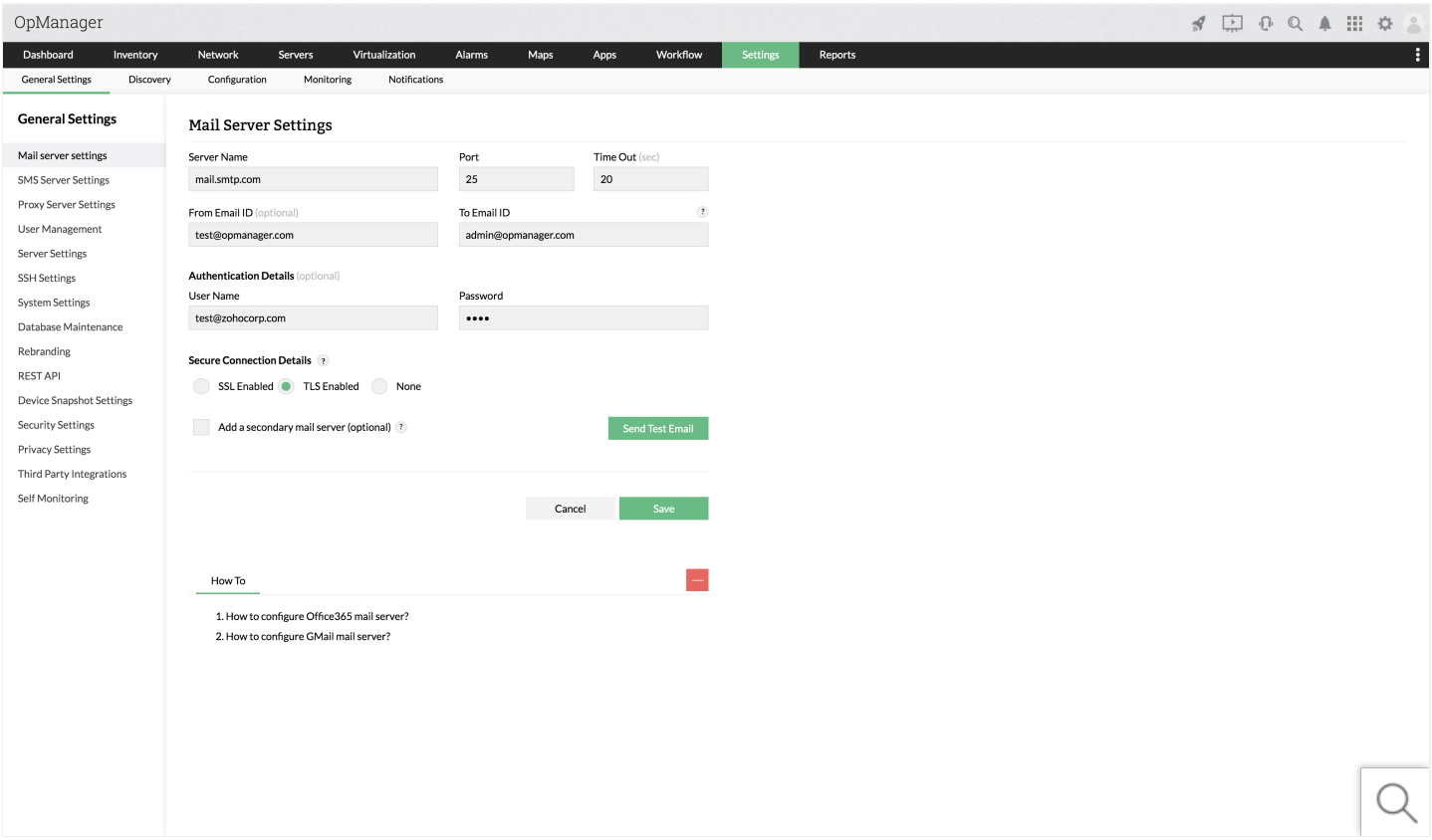
From the list box on the top right corner, you can access the following:

- **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.

Important Note: Prior to mail server configuration, go through this mandatory check list to avoid connection issues.



To configure the SMTP server settings globally and to provide the secondary mail server settings, follow the steps given below:

1. Go to **Settings ? General 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 ? General Settings**, and 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.

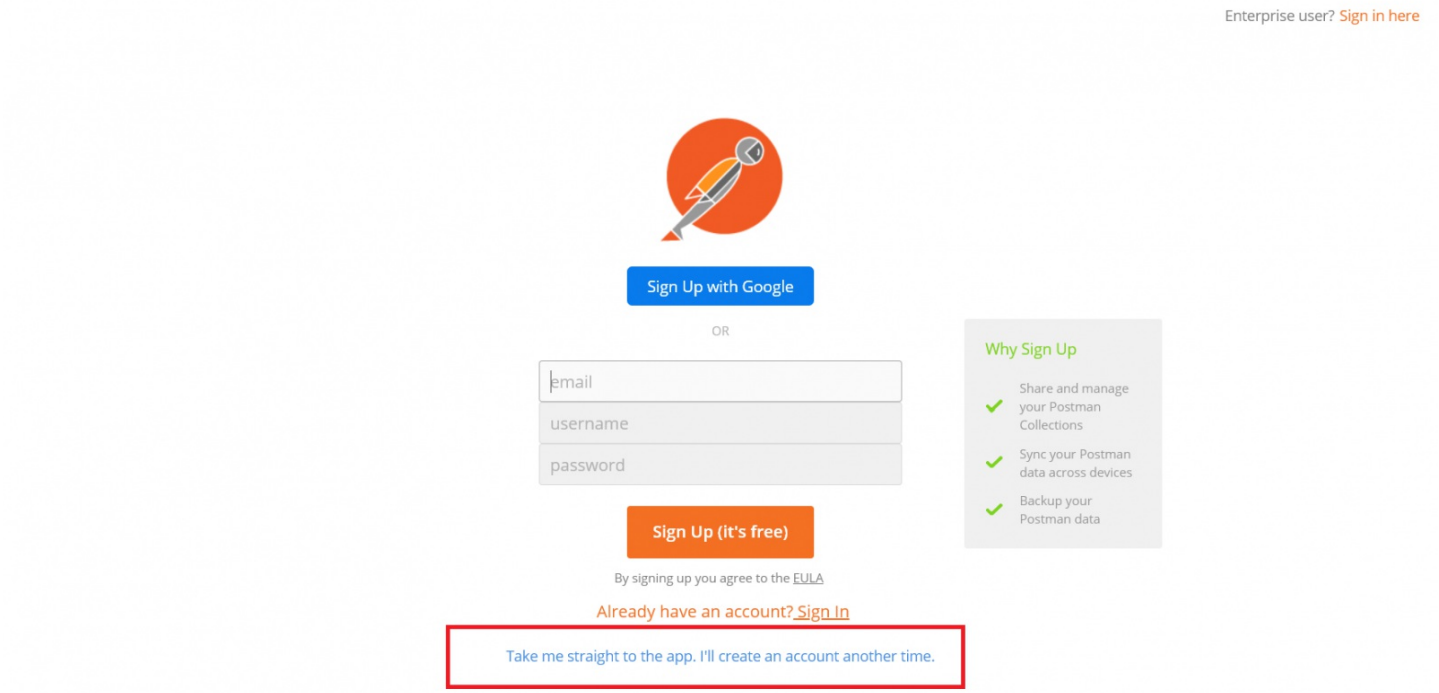
8) **Destination Address's TON:** Denotes Type of Number for the destination address.

9) **Destination Address's NPI:** Denotes Numbering Plan Indicator for Numbering Plan Indicator for the source address.

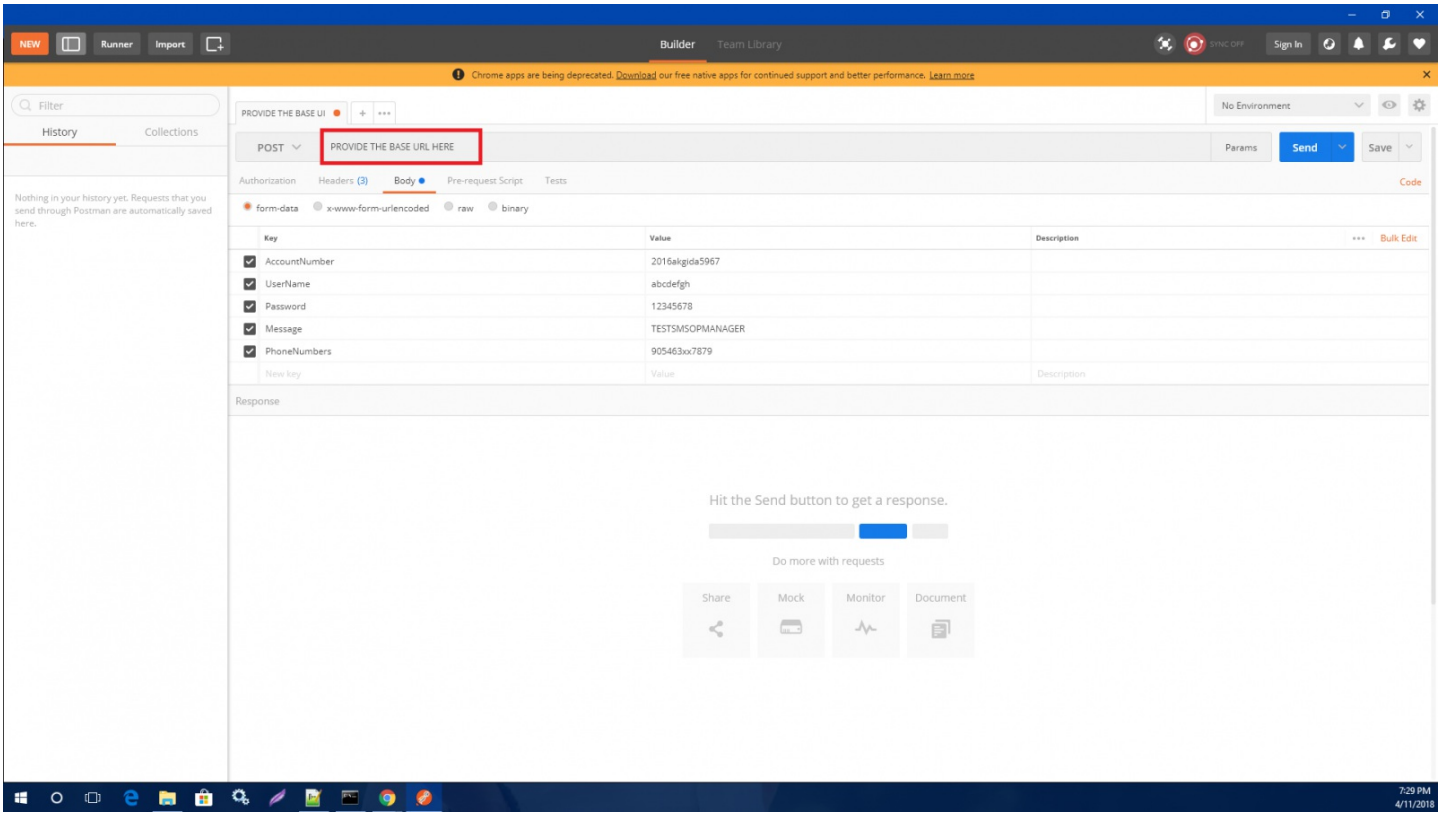
POSTMAN - Third party API tool - An App in chrome

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".

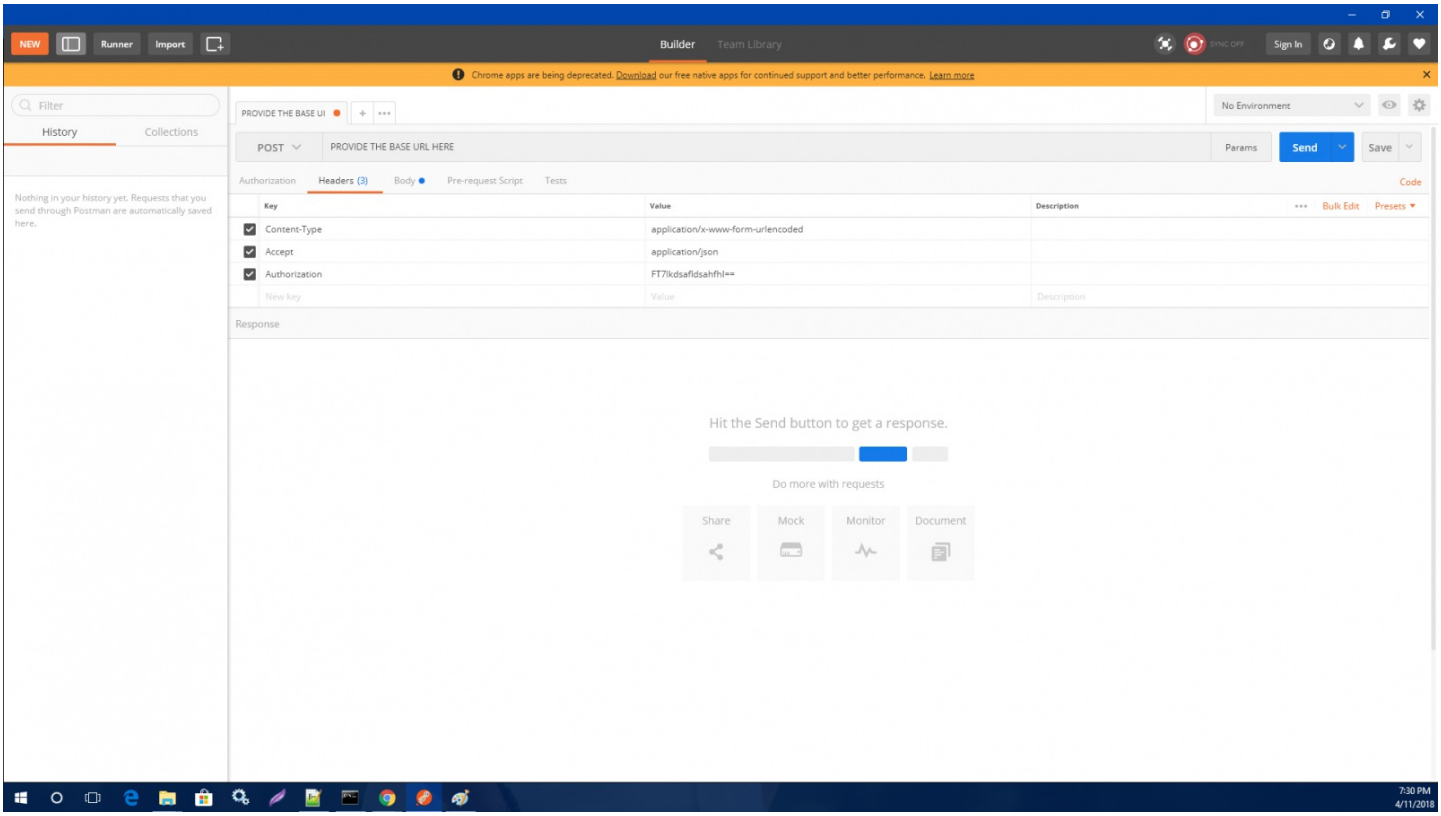


1.Please provide the base URL of the SMS gateway provider and select the API method as POST or GET.



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.

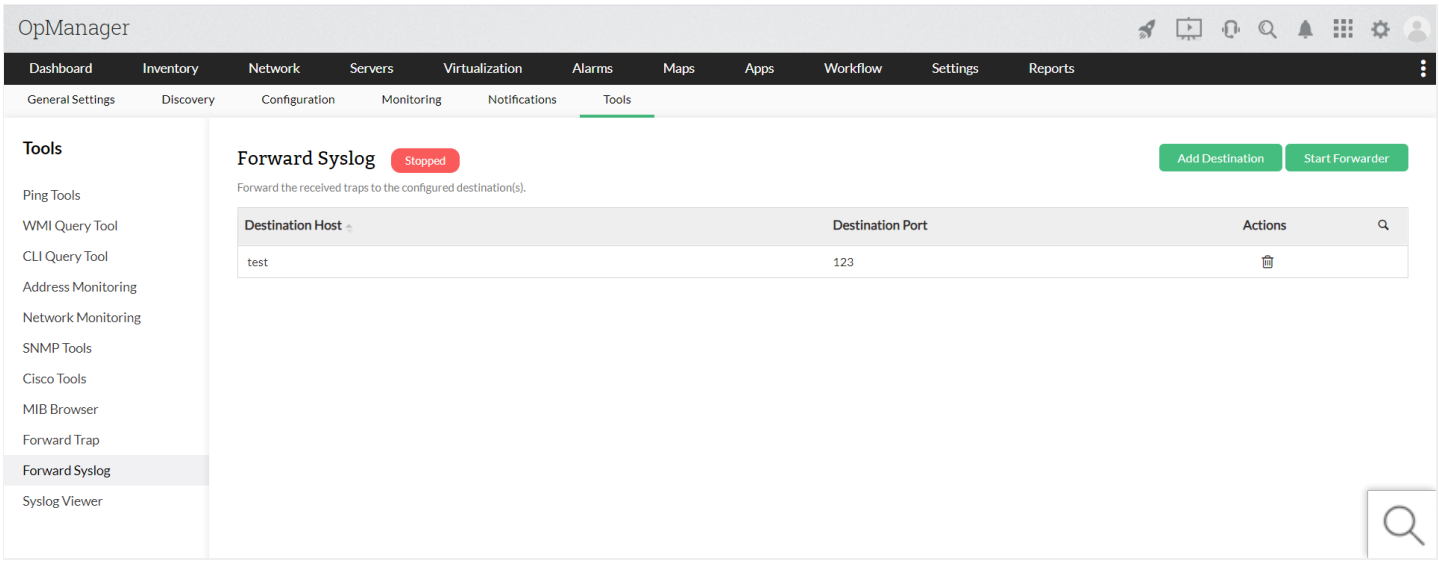


4.Click "Send" and check the status.

Forwarding Syslog

You can forward the syslog received in OpManager to any NMS.

Prev Next



Steps to forward syslog:

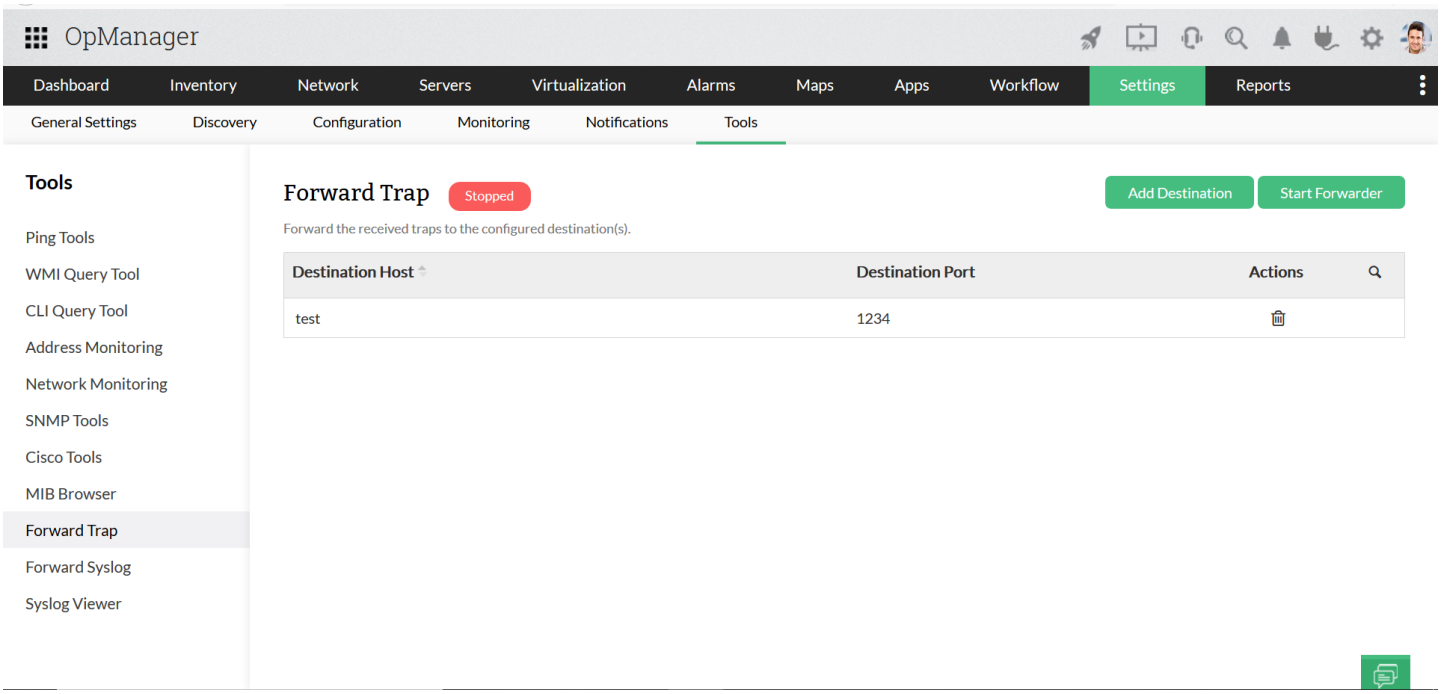
1. Go to **Settings ? Monitoring ? Syslog rules** and click on 'Forward Syslog'.
2. Click on **Add Destination** button.
3. Provide the Name/IP address of the NMS Host to which SysLog has to be forwarded.
4. Provide the SysLog listening port number of the NMS to which SysLog has to be forwarded.
5. Click on **Start Forwarder** to initiate sending of SysLog to the destination NMS. You can also **Stop forwarder** at any desired time.

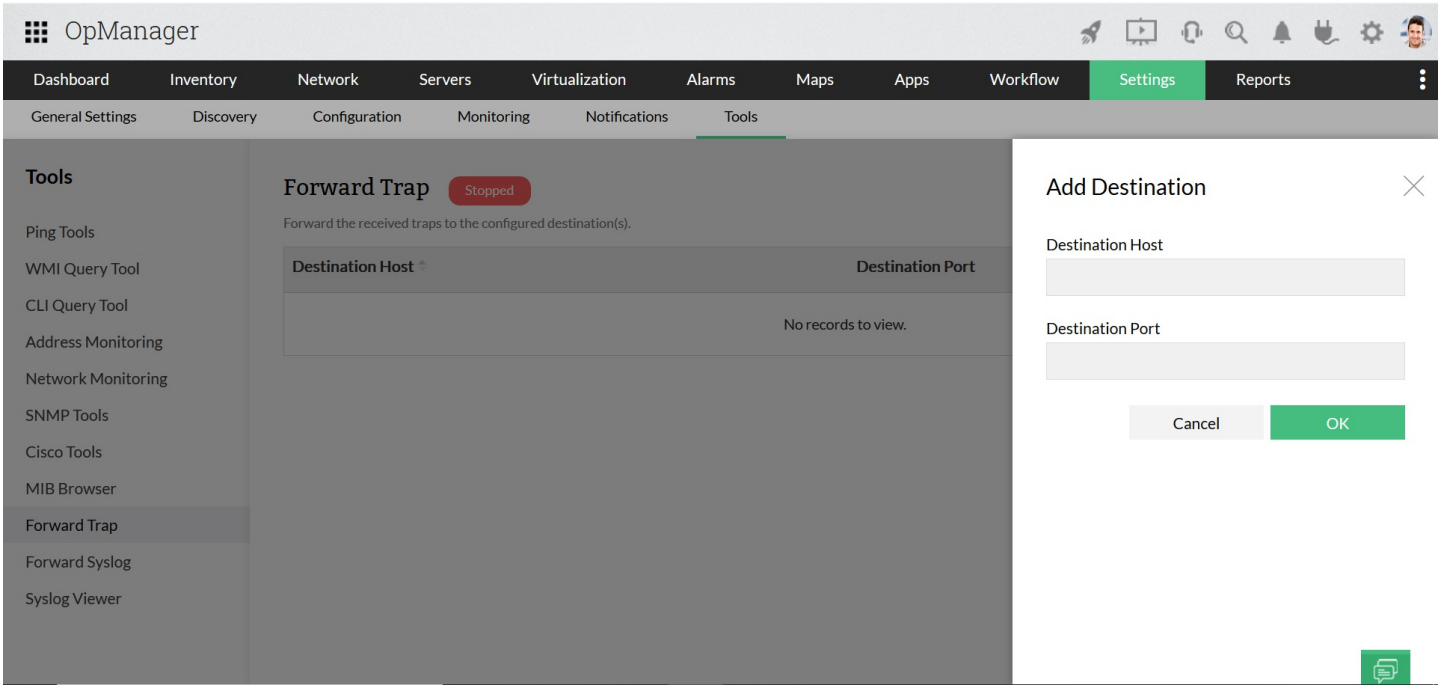
Forwarding Traps

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.**





What is the purpose of BGP?

The Border Gateway Protocol (BGP) facilitates the process of transferring the data over the internet. BGP traces all the possible paths that data can take to reach its destination and chooses the best path to make data transfer efficiently.

In simple words, BGP decides the shortest path between any two routers, between which there occurs a data exchange.

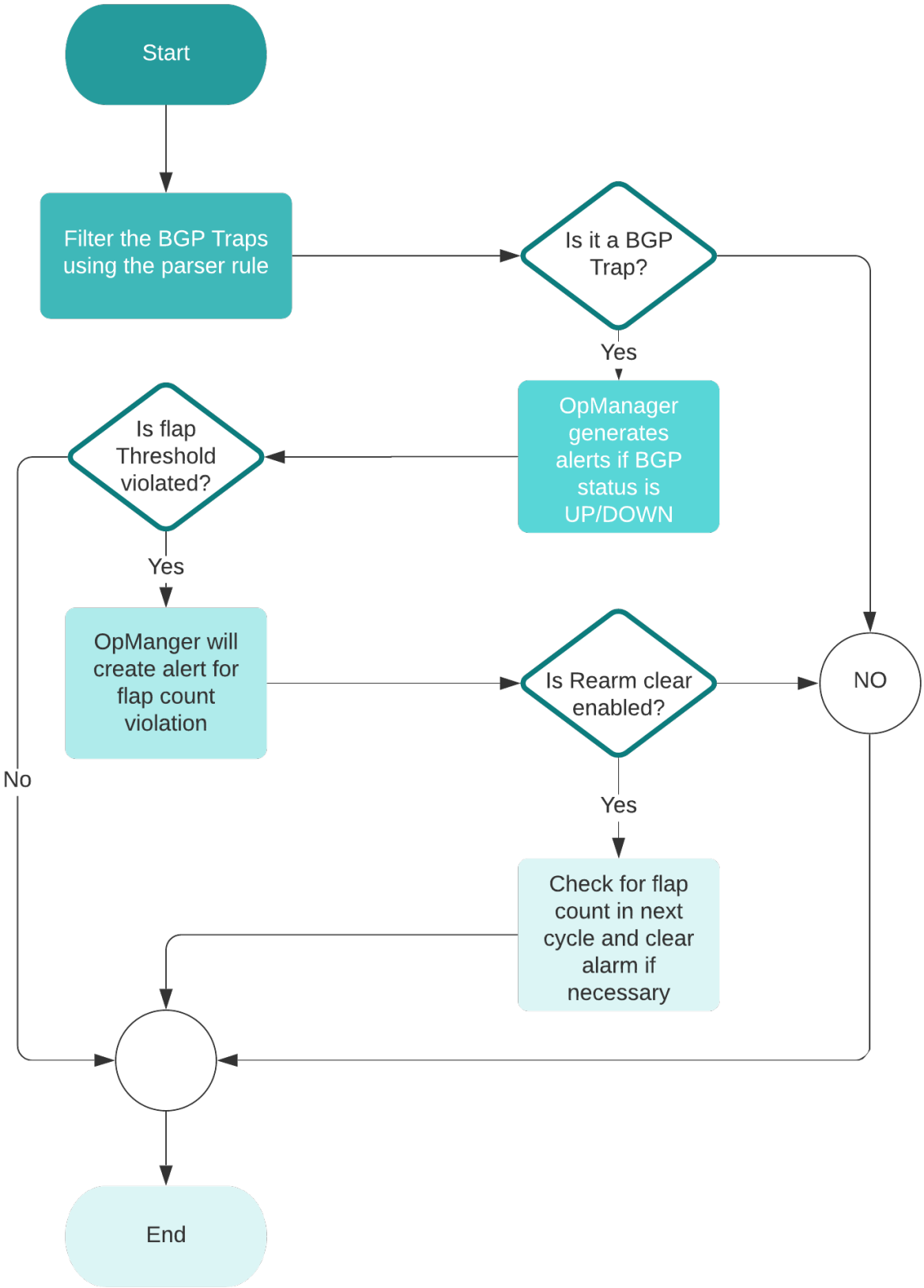
BGP Traps in OpManager

When traps are sent to OpManager, it uses the parser rule to determine whether the trap is a BGP trap. If the trap happens to be a BGP trap, then OpManager monitors the status and generates an alert - as up/down. The combination of an up and a down indication constitutes a Flap and OpManager monitors Flaps as well.

When the Flap count exceeds 5 within a span of 30 minutes (which is the default threshold specified), a Critical alert is raised. On further monitoring, if the Flap count falls below 5, then the alarm will be automatically cleared as it attains Rearm.

The entire functioning of how OpManager processes a BGP trap is depicted in the flow diagram below.

BGP PROCESS


Start
Filter the BGP Traps using the parser rule
Is it a BGP Trap?
Yes
OpManager generates alerts if BGP status is UP/DOWN
Is flap Threshold violated?
Yes
OpManger will create alert for flap count violation
Is Rearm clear enabled?
NO
Yes
Check for flap count in next cycle and clear alarm if necessary
No
End

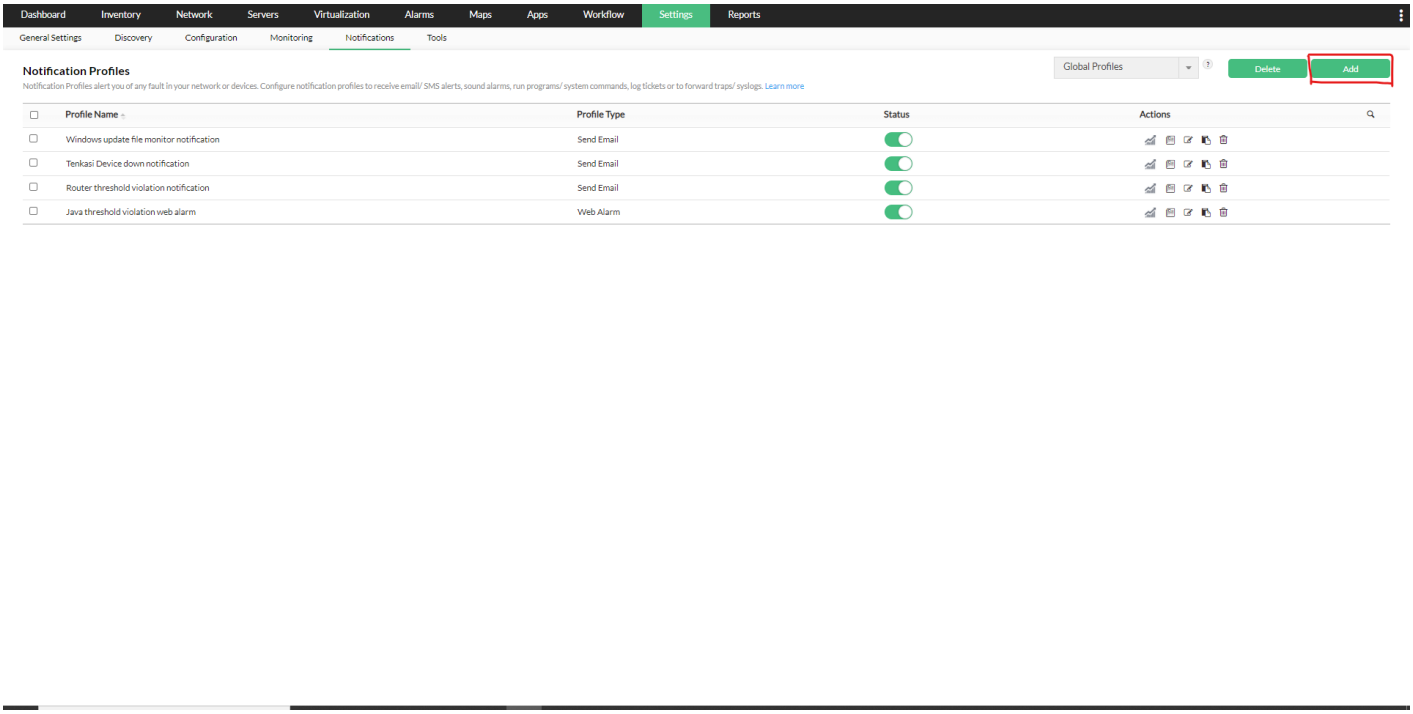
Email Notification Profile

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.

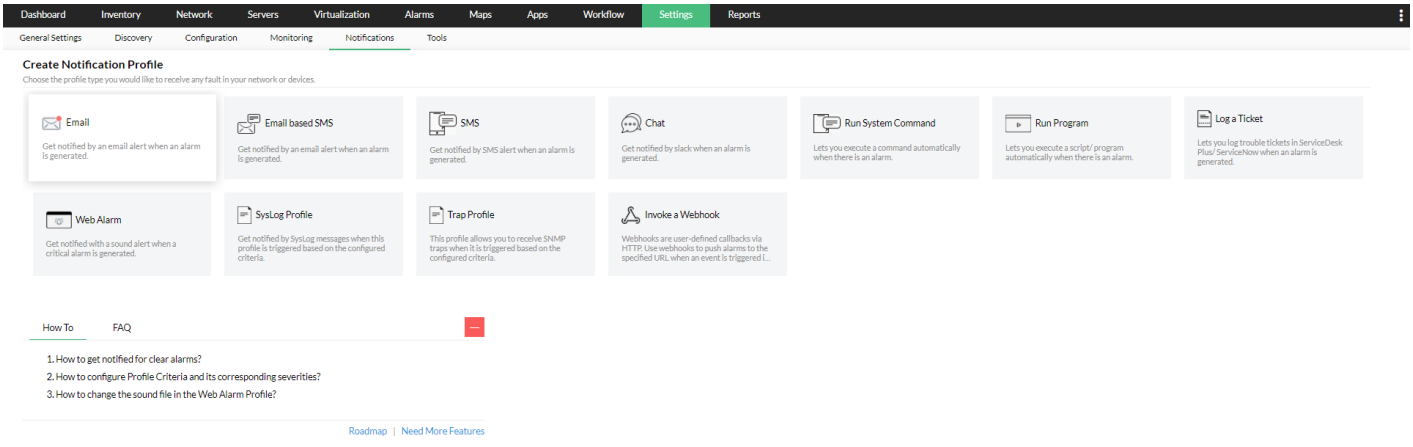
Configuring an Email Alert

To create an email alert profile, follow the steps given below:

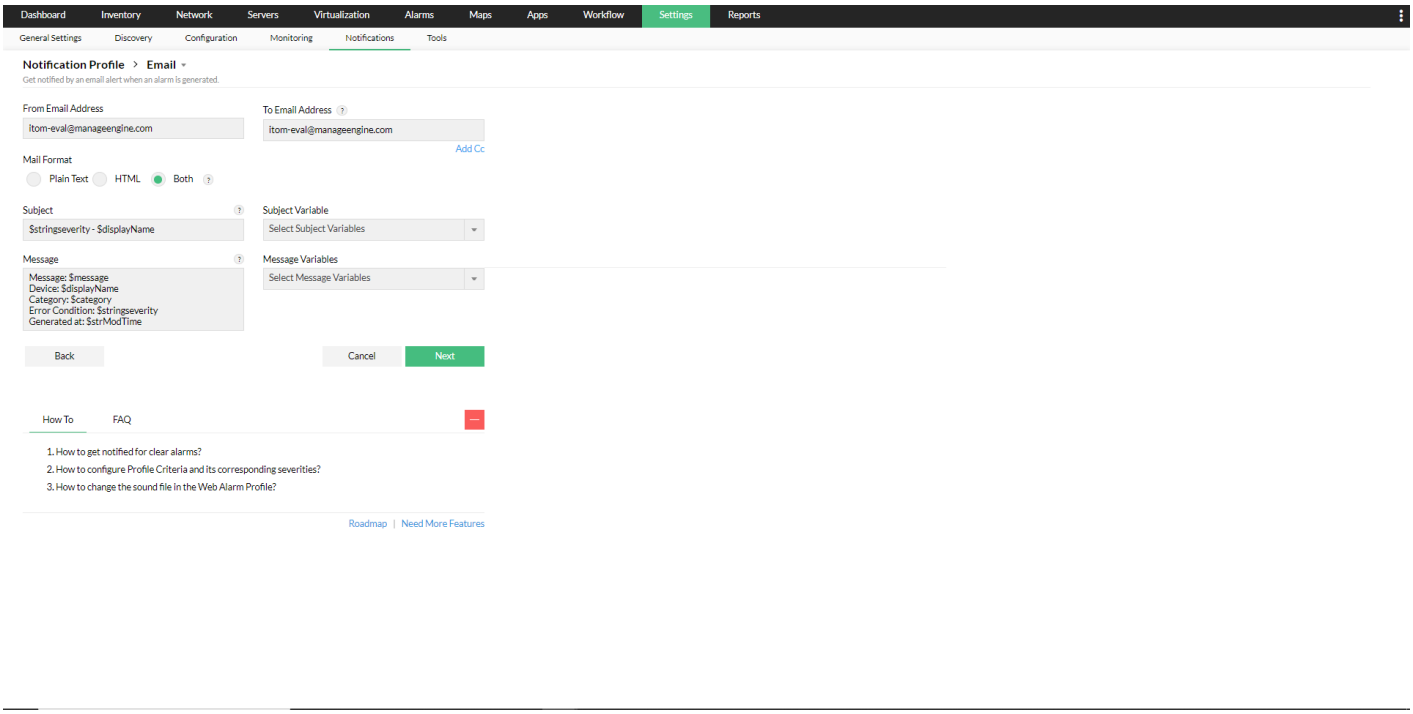
1. Go to **Settings** > **Notifications**
2. Click **Add**.



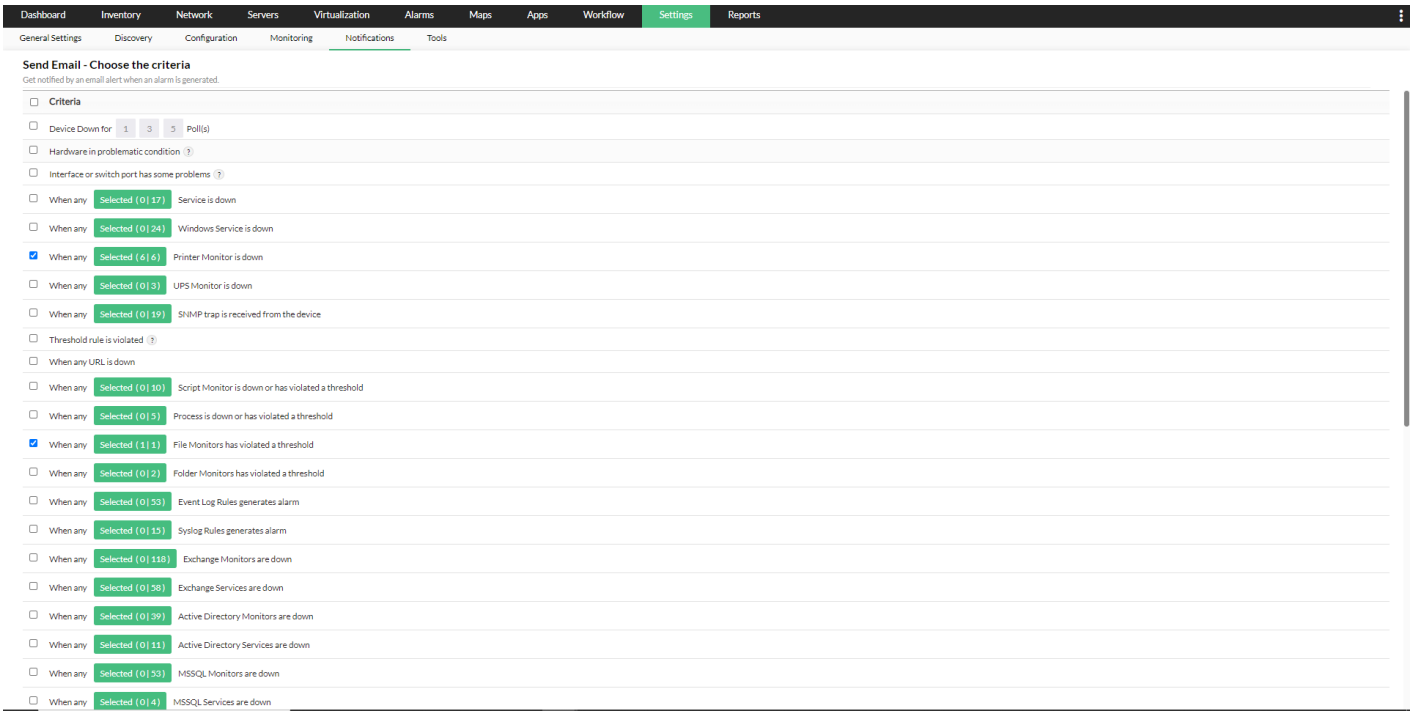
3. Select the Notification type as **Email.**



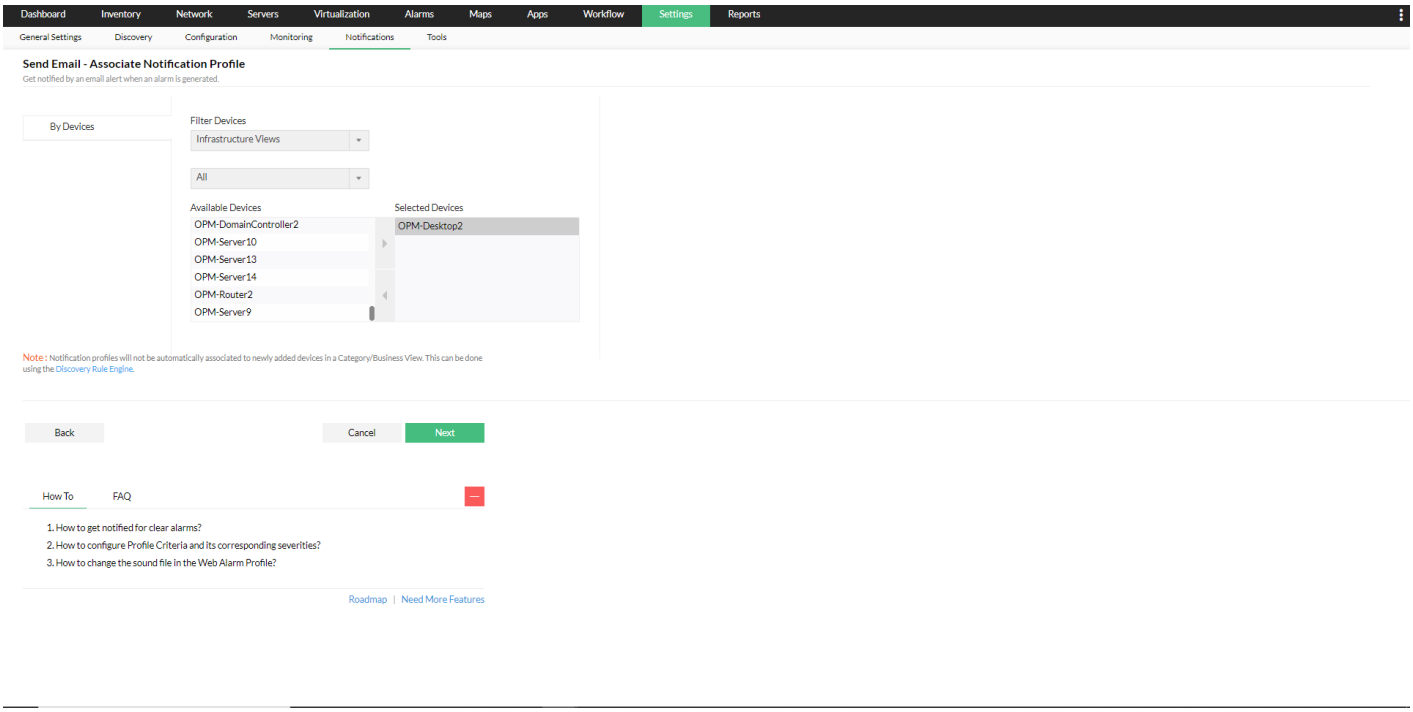
4. Provide the **From, To,** and **CC Email Address** in addition to **Subject** and **Message** (select the required alarm variables which is to be displayed on the email subject and message). Click **Next**.



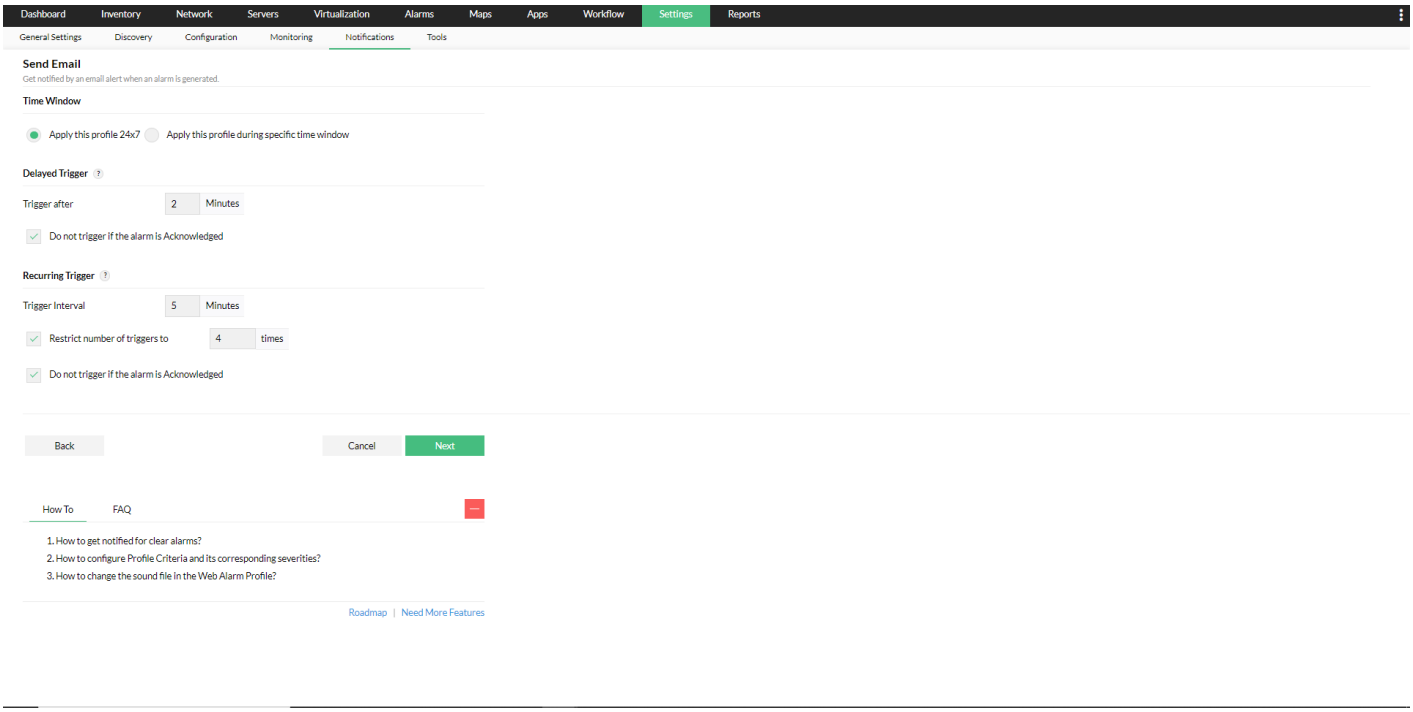
5. Select the fault criteria for which you need to be notified. For instance, if you want to be notified of threshold violation, select 'Threshold rule is violated'. Additionally notify only when any or all the severity: Critical, Trouble, Attention, Service Down. Click **Next**



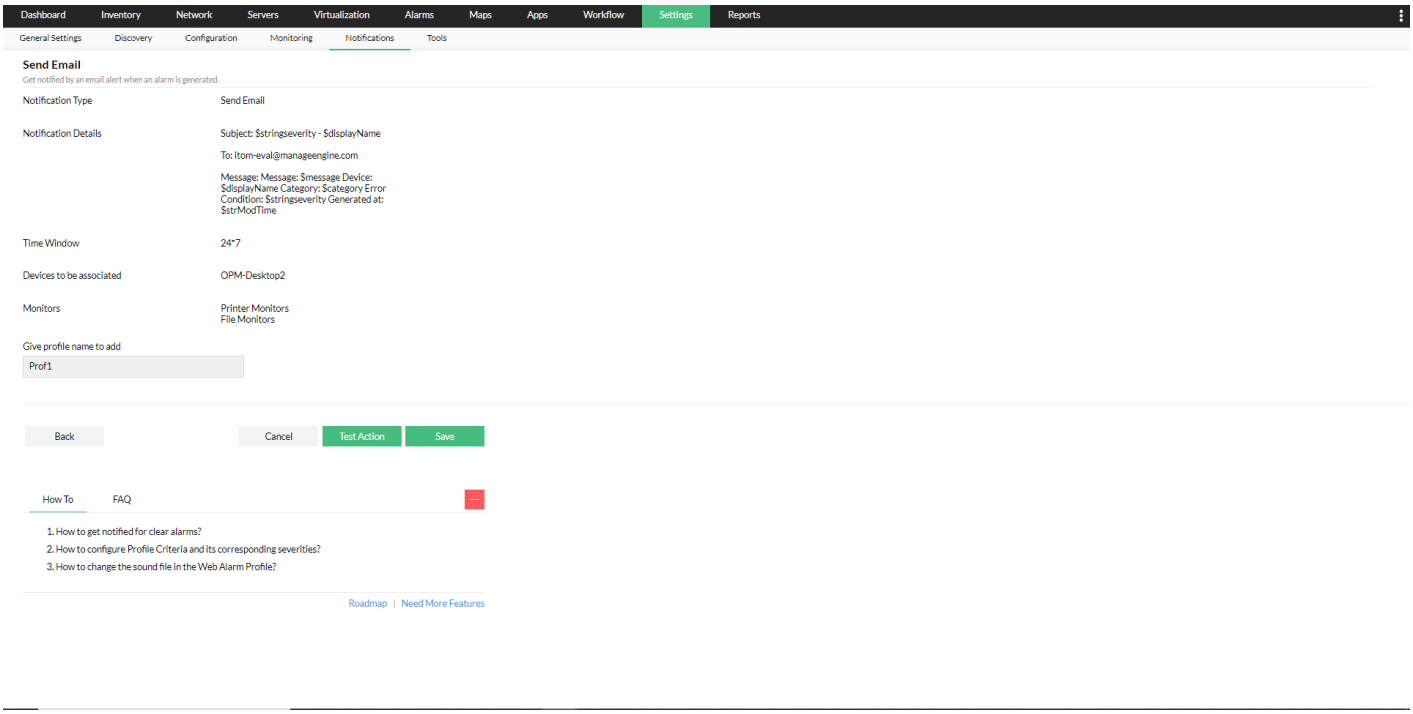
6. Select the devices either **By Category** or **By Business View** or **By Devices** and click **Next**.



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.

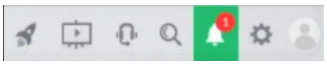
The profile is associated to the selected devices. A notification is sent every time a threshold is violated for a server. To configure SMS server settings, click here.

OpManager also sends Email based SMS alerts, click here to know more.

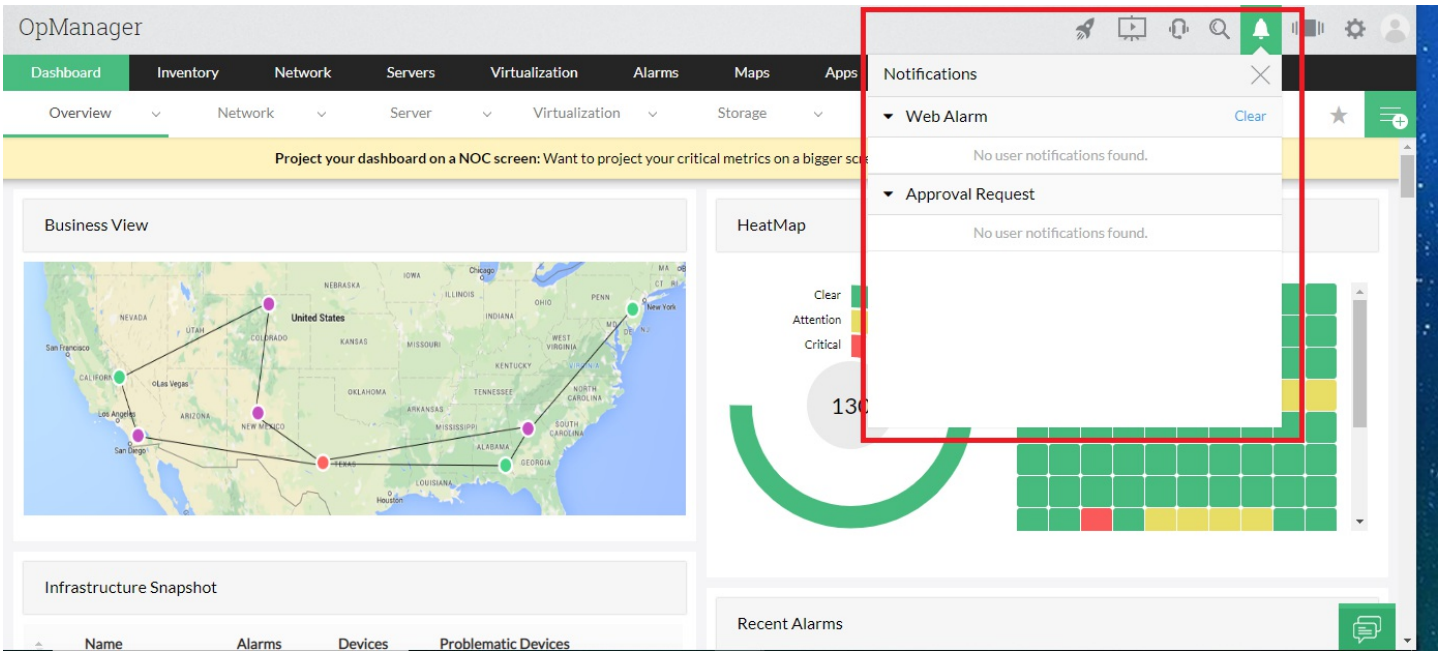
Web Alarm Notification Profile

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.

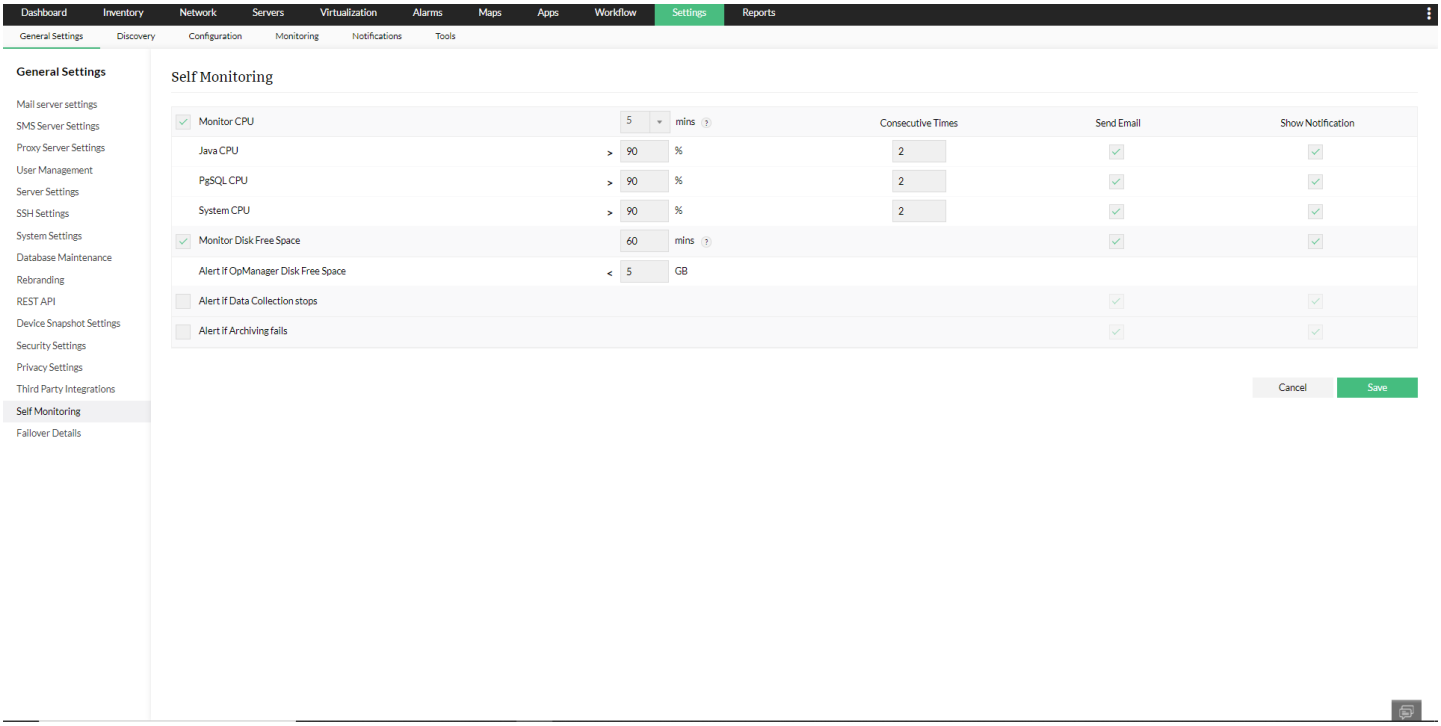
Self Monitoring

Self Monitoring in OpManager helps to monitor the device in which OpManager is running.

With Self Monitoring, you can monitor CPU usage (Java CPU, PGSQL CPU and system CPU), free disk space, receive alerts via email/notifications if data collection stops and if archiving fails. This helps to ensure that the device in which OpManager is installed and running from, is constantly healthy and helps you fix potential issues immediately.

Configuring Self Monitoring in OpManager:

To configure Self Monitoring go to Settings -> General Settings -> Self Monitoring



Monitor CPU:

Select this option to monitor the CPU usage and choose the monitoring interval from the drop down available. This is the frequency of polling for CPU monitoring.

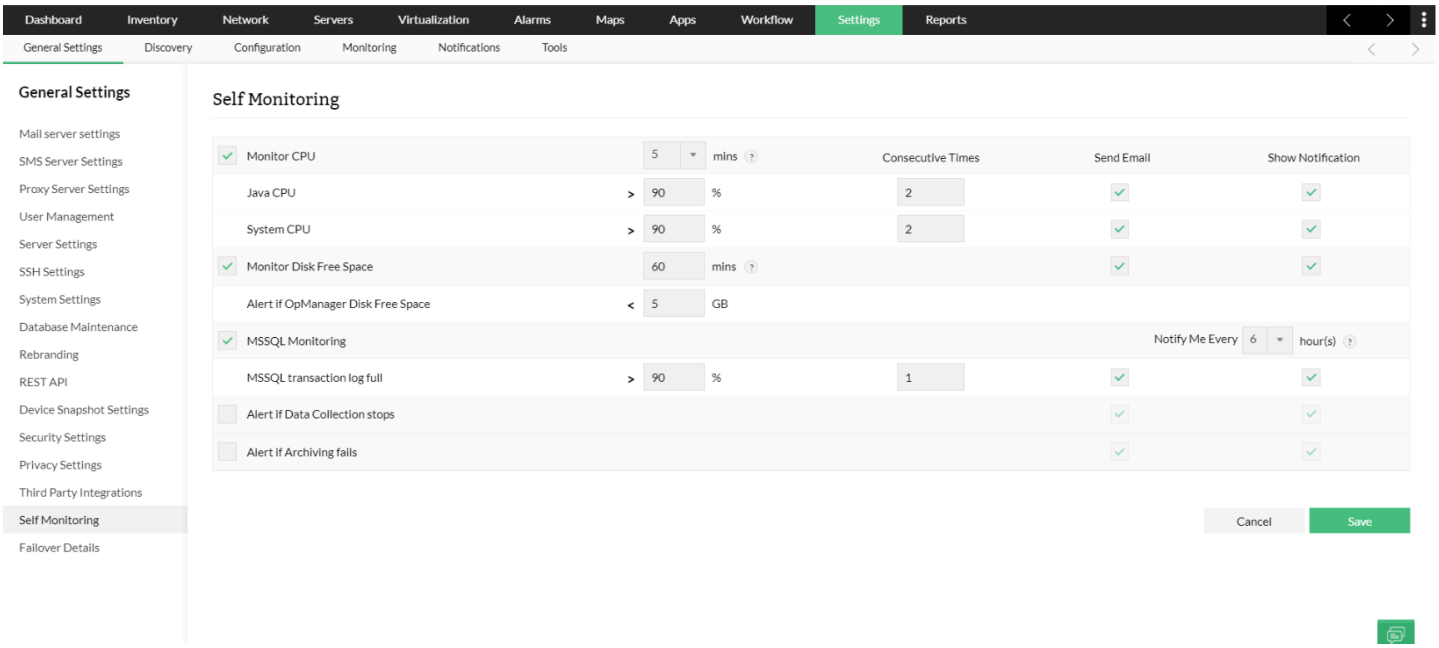
1. Java CPU:

Monitors the CPU usage by Java, the process on which the OpManager application works, and collects the CPU usage data in percentage at regular intervals.

2. PgSQL CPU:

Monitors the CPU usage by PgSQL, the process on which the OpManager database works, and collects the CPU usage data in percentage at regular intervals.

Note: If the OpManager is using the MSSQL database, then the option to configure self monitoring threshold for PGSQL CPU usage is replaced by 'MSSQL transaction log full' percentage. 'MSSQL transaction log full' once detected will be notified at regular intervals.



3. System CPU:

Monitor the overall CPU usage by the system in which OpManager is running.

> **Note:** The default threshold values set for polling interval, consecutive times, percentage of usage and disk free space are recommended not to be changed. Change the predefined values only if required.

1. Increase or decrease the threshold values for CPU usage percentage by Java applications used by OpManager, PgSQL databases used by OpManager, and the overall System CPU usage for which alerts need to be sent respectively. However, increasing the threshold values is not recommended.

2. Increase or decrease the 'Consecutive Times' of exceeding the CPU usage percentage of Java CPU usage, PgSQL CPU usage and System CPU usage specified that you want an alert for.

3. Select if you want to receive alerts via email and/or notifications.

Monitor Disk Free Space:

Monitor the free space available in the drive in which OpManager is installed by selecting this option.

1. Alter the time interval for monitoring and Disk Free Space if so desired.

2. Select if you want to receive alerts via email and/or notifications.

Alert if Data Collection Stops:

Select this option if you want to receive an alert when data collection in OpManager stops.

Alert if Archiving Fails:

OpManager archives data on a regular basis (hourly and daily) in order to free up space for newer data. Select this option if you want to receive an alert when this regular archiving of data does not take place.

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. Configure the name of the program with its absolute path. For example, if you want to run a script called 'test.bat' located in a particular directory (D:\Testing\Script) the input must be in the same directory (D:\Testing\Script\test.bat).

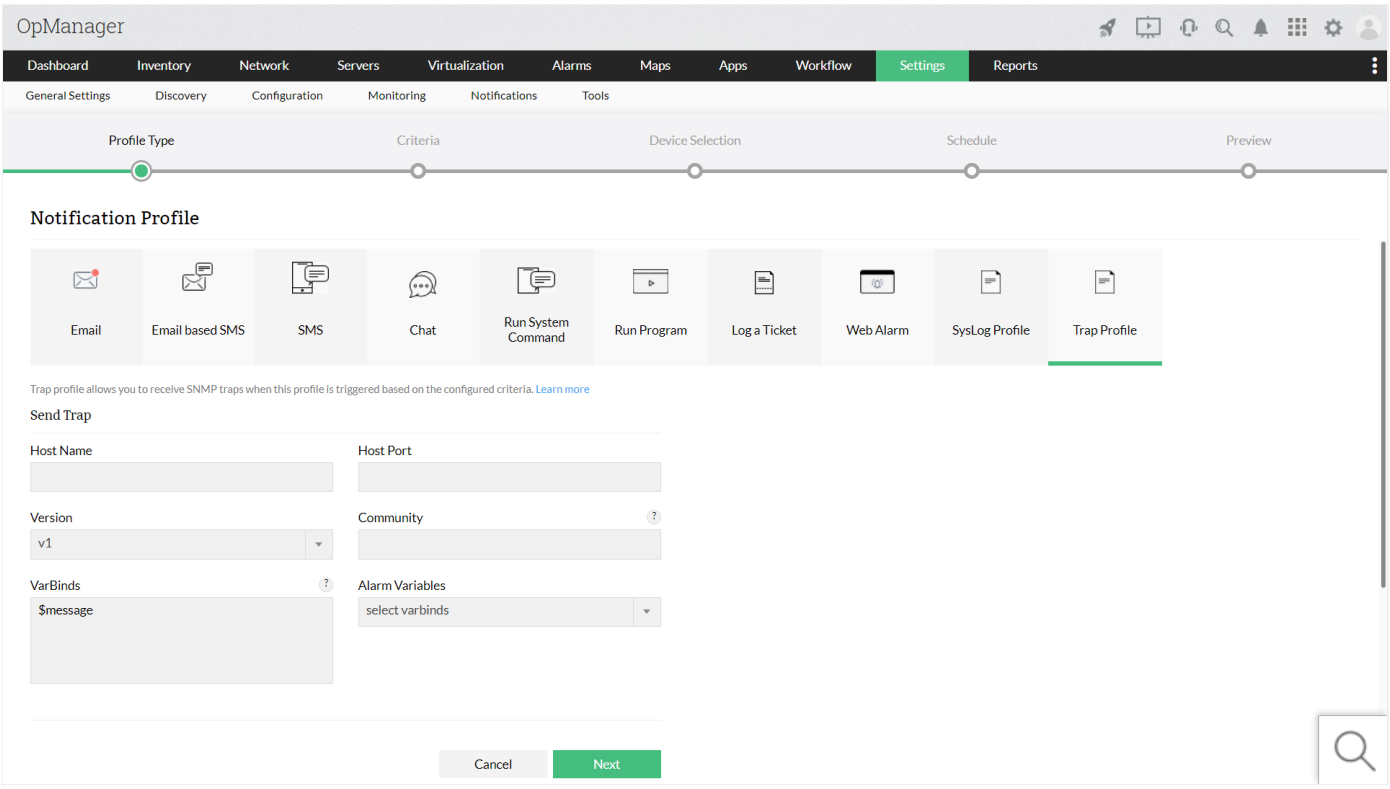
   Note: These commands will be executed in the OpManager installed server. Please verify the source of the commands before using it here, to prevent any unexpected behaviour or vulnerabilities.

5. 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.

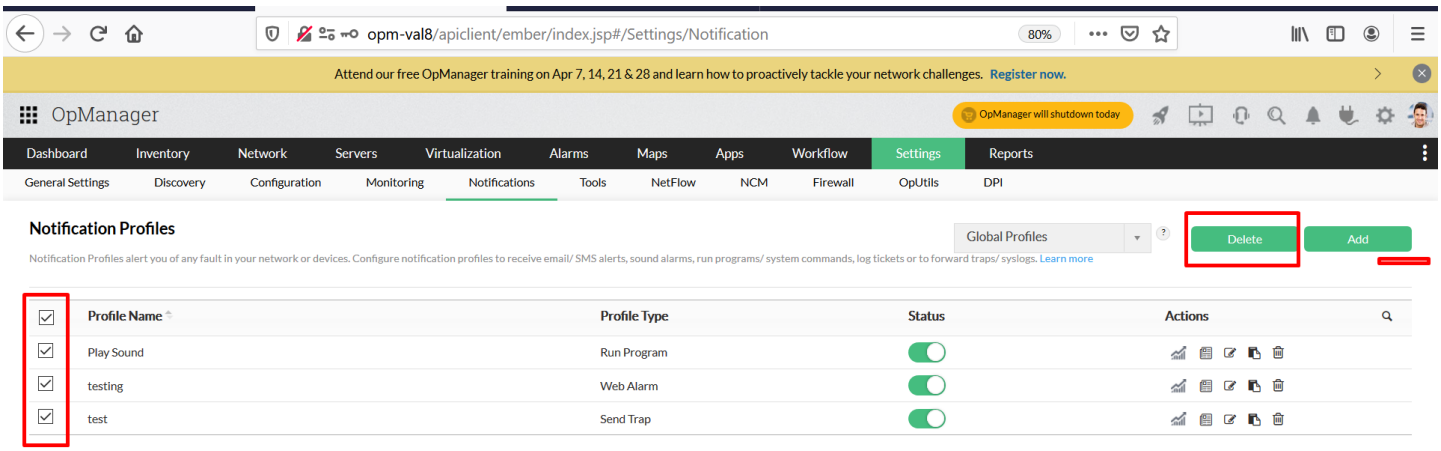
Points to remember:

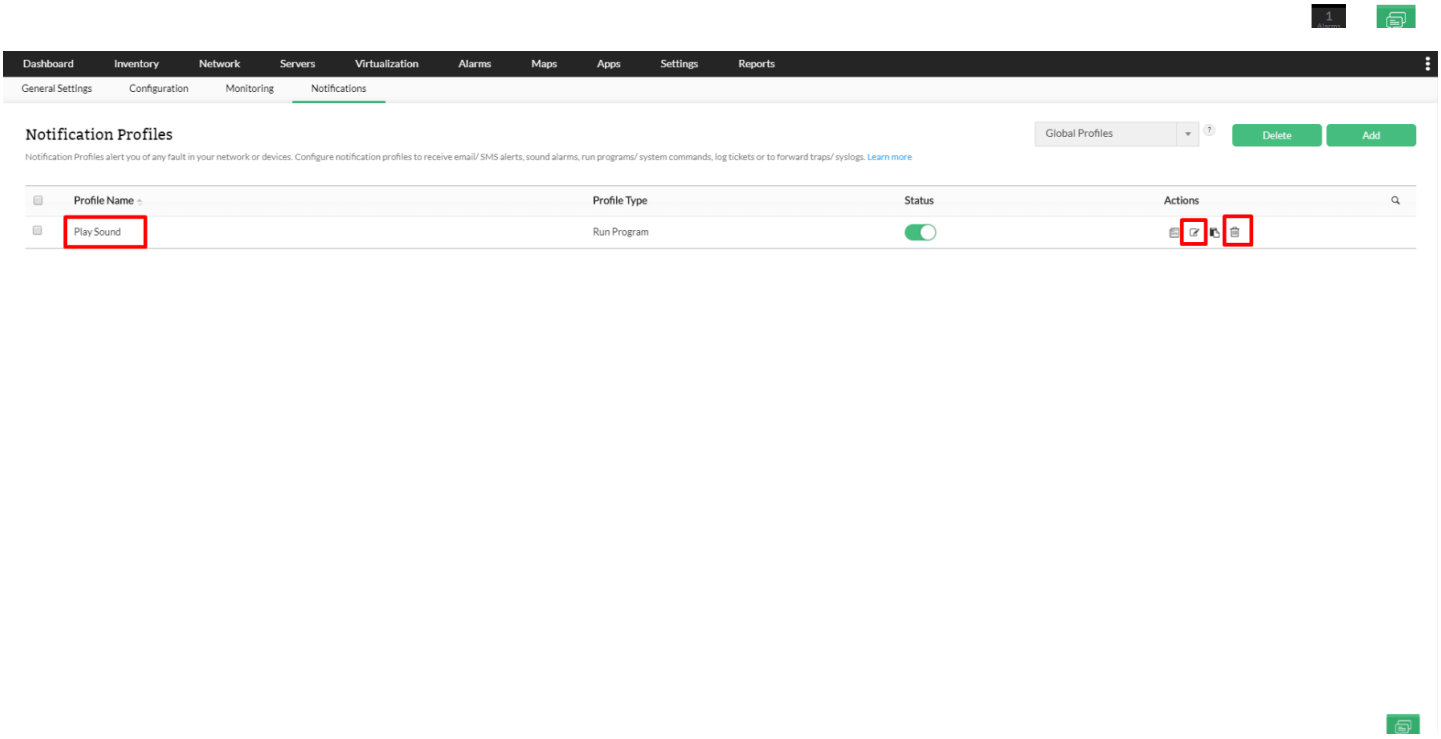
- If a device is added under multiple device downtime schedules, chances are that one of the device downtime schedules under which the device is specified may still be in running state. Hence, the specific device will continue to remain in downtime.
- When the parent device is on maintenance, the child 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

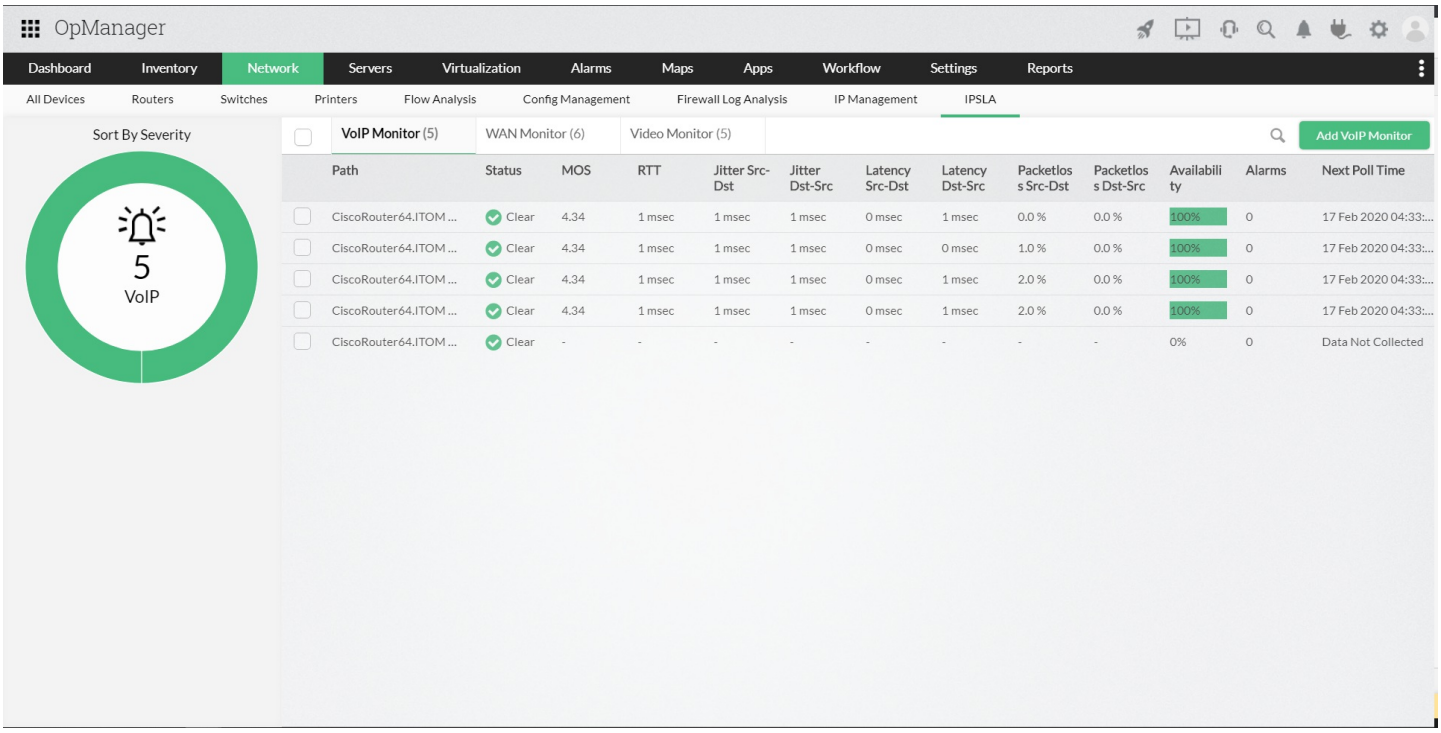
3. Enable the IP SLA responder:

   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

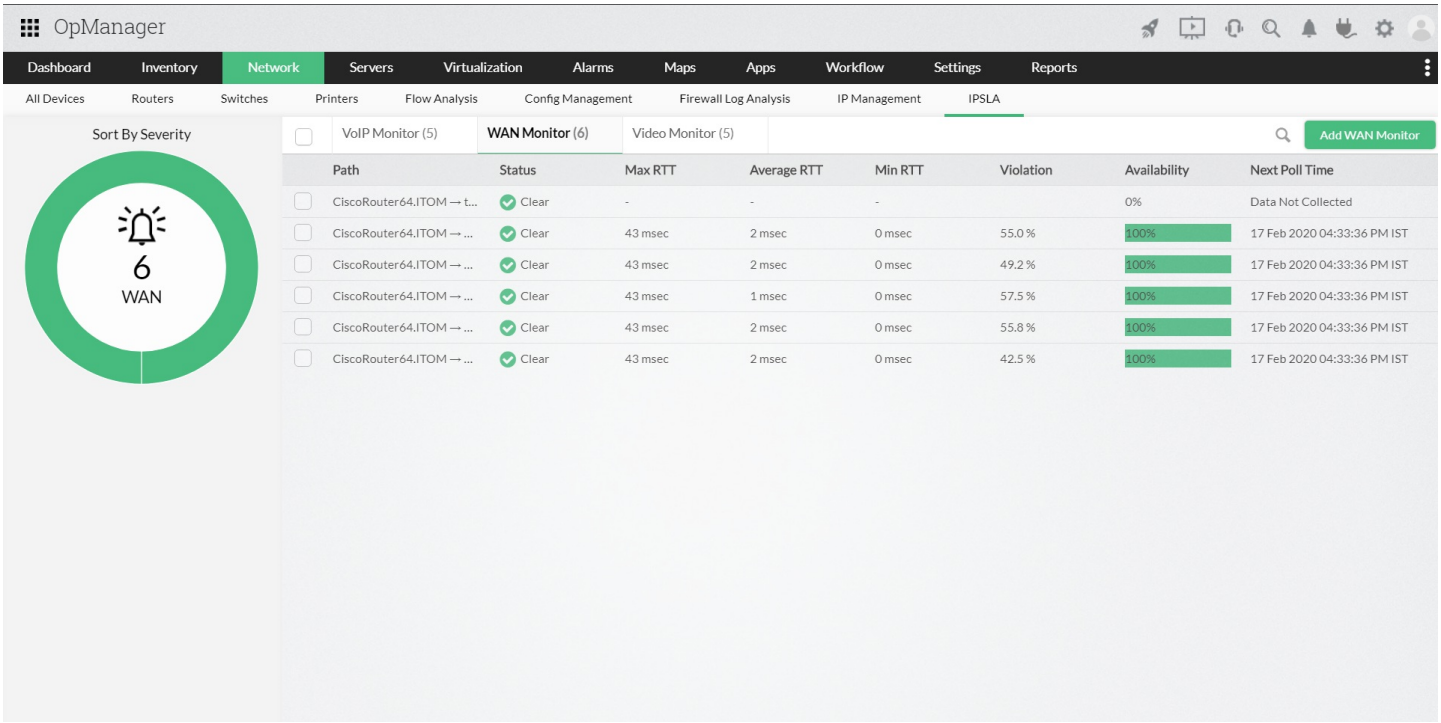
Configure the cisco router to send traps to OpManager. Alerts are shown based on the traps received in OpManager. To configure OpManager server as the SNMP Server receiving traps for the routers, telnet the router and type the following command:

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

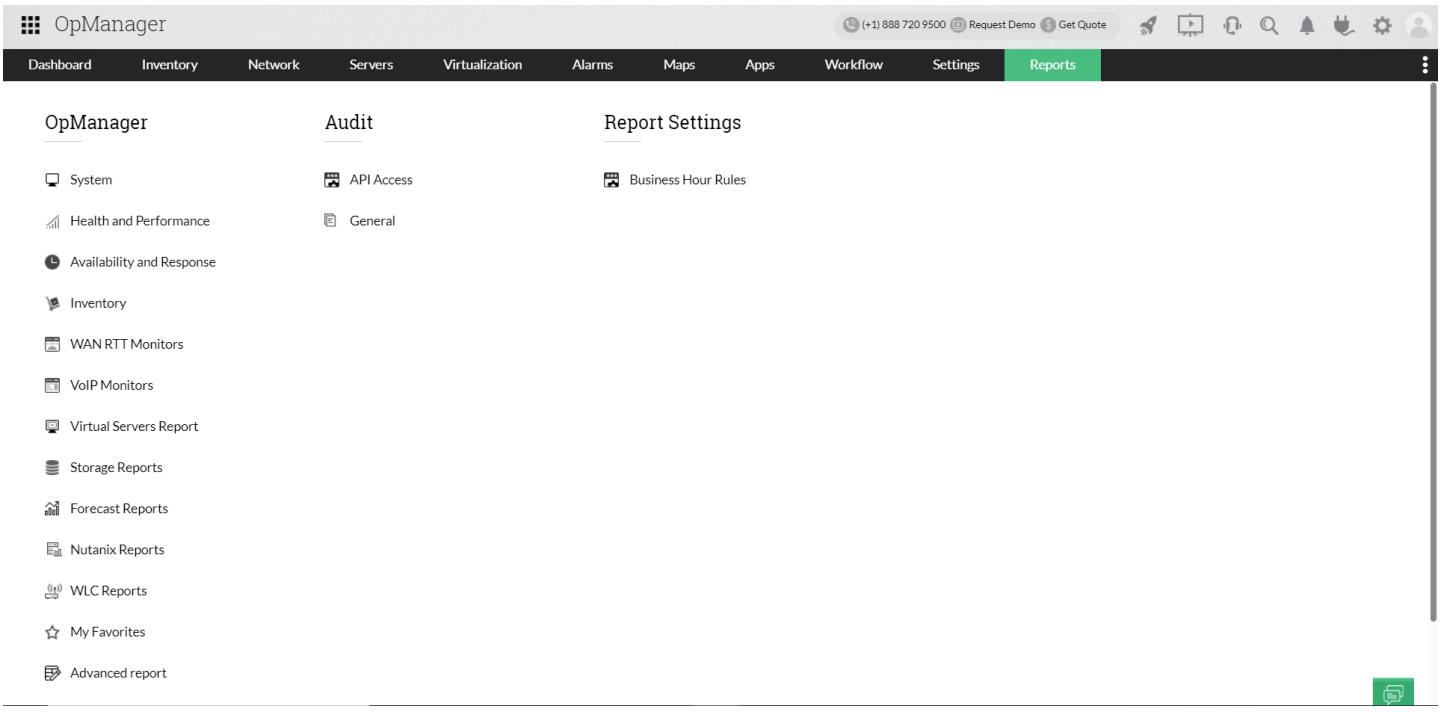
Go to Inventory ? Select IPSLA from three line menu ? Select VoIP (Select any monitor) ? Alarms (present at the end of the page) to view the alerts raised by WAN Monitor.

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.
- **WLC reports:** Get detailed availability and inventory reports of access point and rouge SSIDs. Also, the access points that are discovered in OpManager (advanced monitoring enabled) will have full access to all types of reports based on the type of device.
- **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**.
- **Integrated Reports:** Users can generate reports for devices and interfaces in OpManager. While generating reports the time window, the type of the report and monitors associated to the device can be specified. These reports can be saved and accessed by navigating to **Reports --> Integrated Reports** in OpManager.



Advaned Reports: OpManager has advanced report generation capabilities that enable users to create and view data on multiple monitoring parameters in a single report. There will be as many columns as per the number of monitoring parameters specified. Click here for a more detailed description about the Advanced report feature.

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:

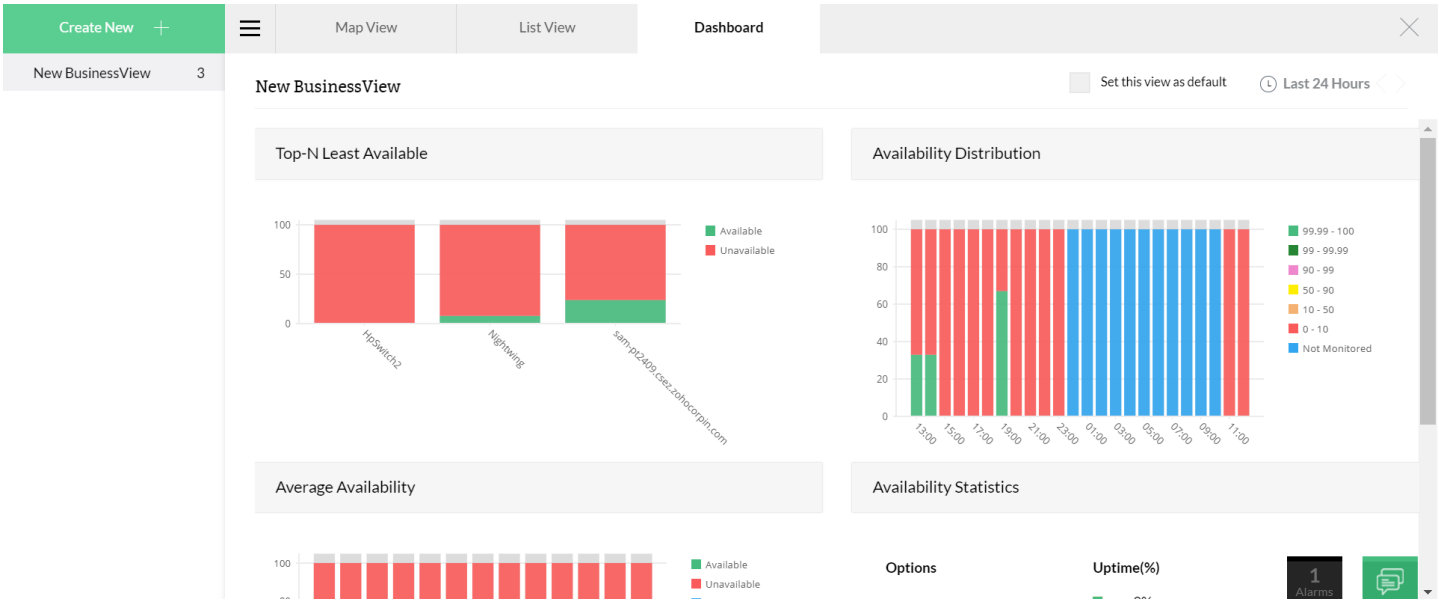
1. Go to the snapshot page of the interface whose health report you want to generate.
2. Go to **Reports** > available on the right pane of the page. All the default reports that can be generated are listed.
3. Click on the preferred time window for which you want to view the report. The default Time 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.



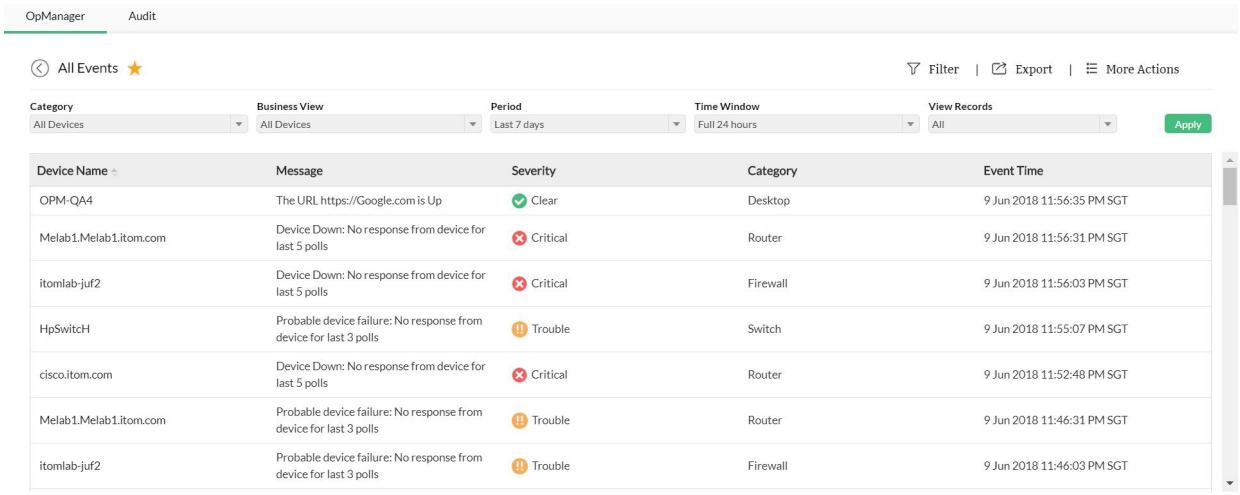
To access the business view dashboard, follow the steps below:

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.

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.



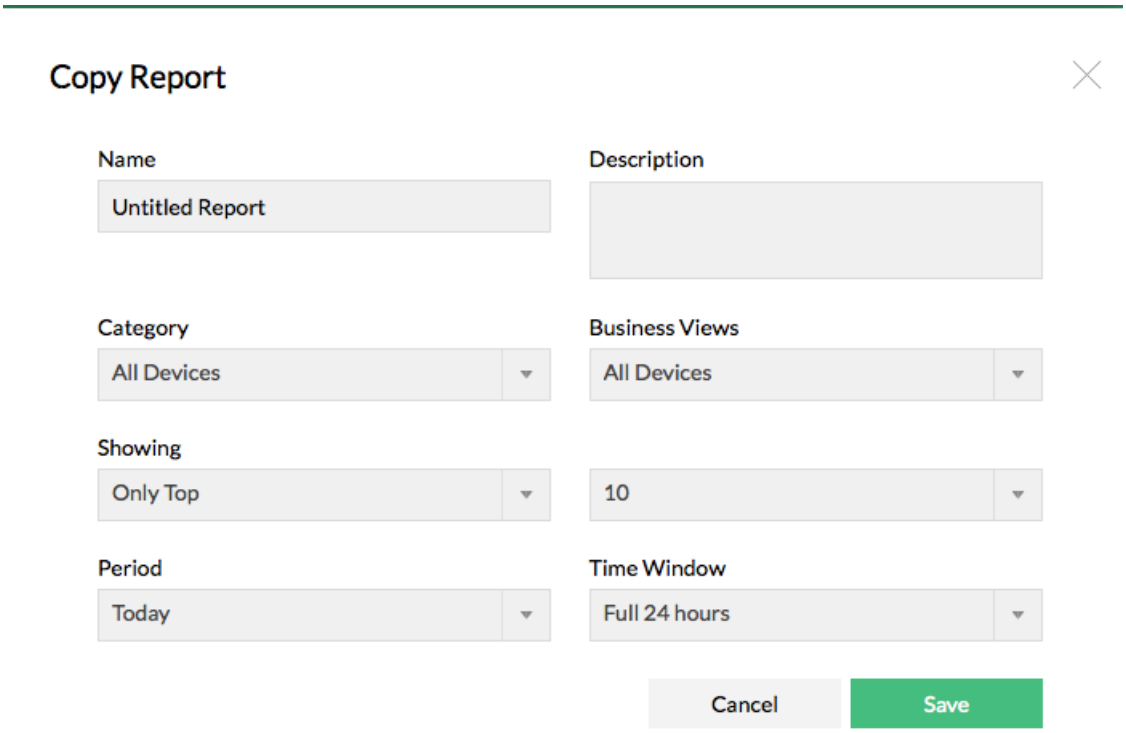
4. Change the required fields. The various fields that can be altered are Category, Business Views, Period, Time Window, Business Hour, Exclude Days, View Records.
5. After modifying the required fields, click on **Apply** to generate the report effecting the changes made.

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;

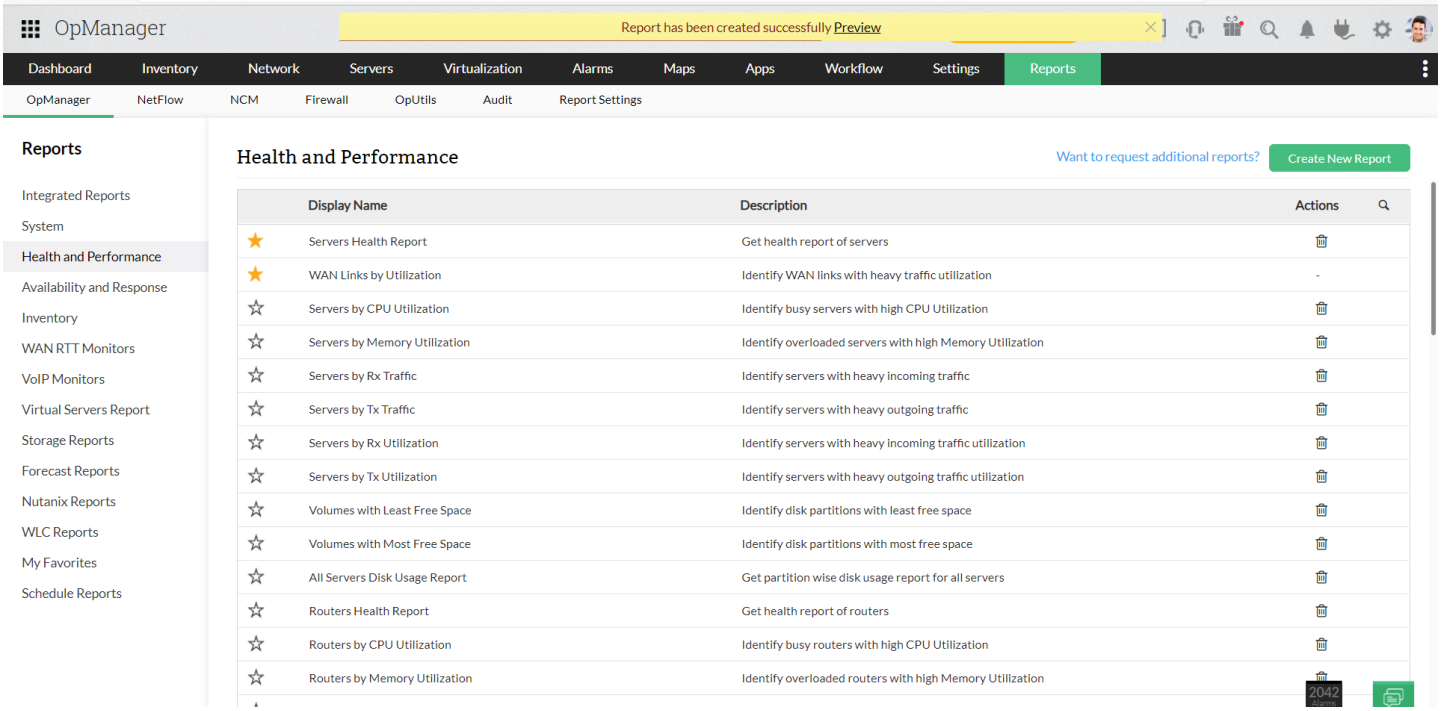
1. Navigate to **Reports -> OpManager.**
2. Choose the report that you want to copy.
3. After choosing the report, click on More Actions&#65533; on the top right corner.&#65533;
4. Click **Copy As** icon available on the top&#65533; of the report that is generated. A small window opens.

&#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

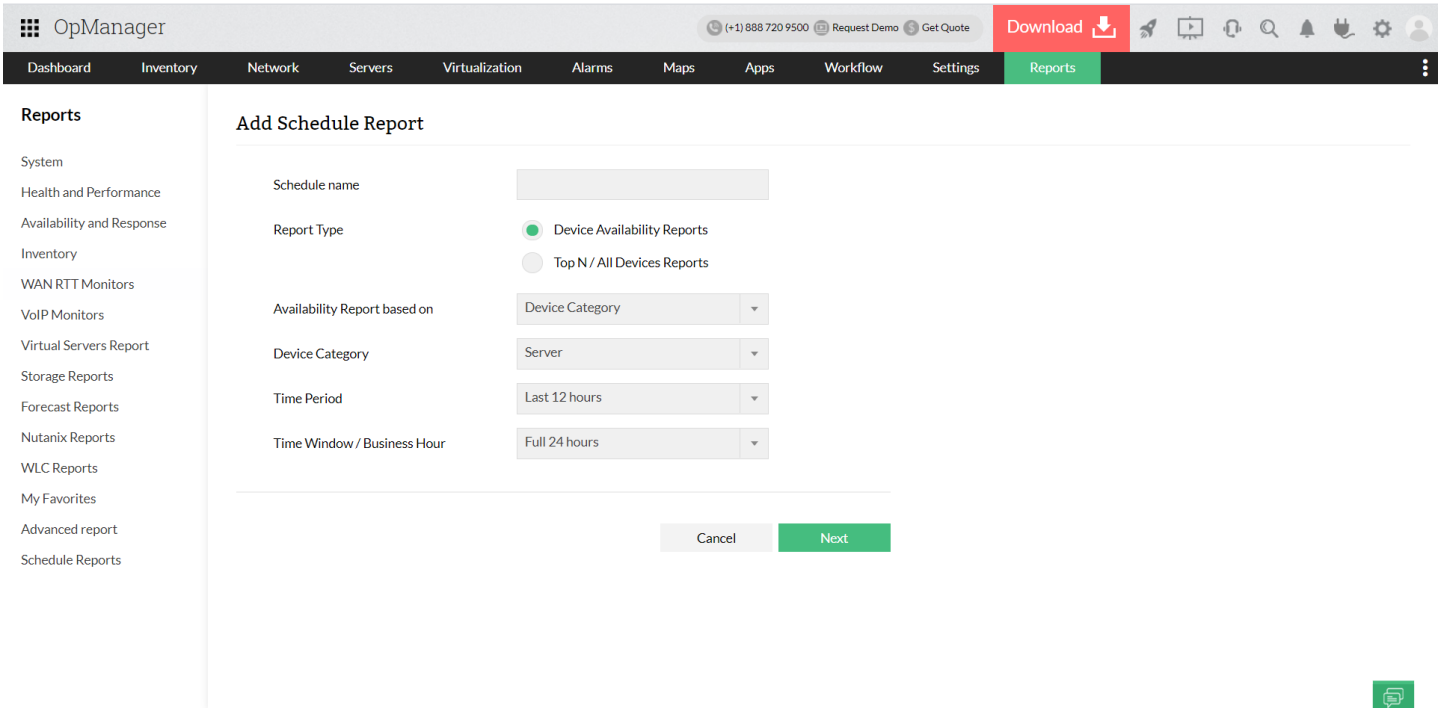
Scheduling Reports

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:

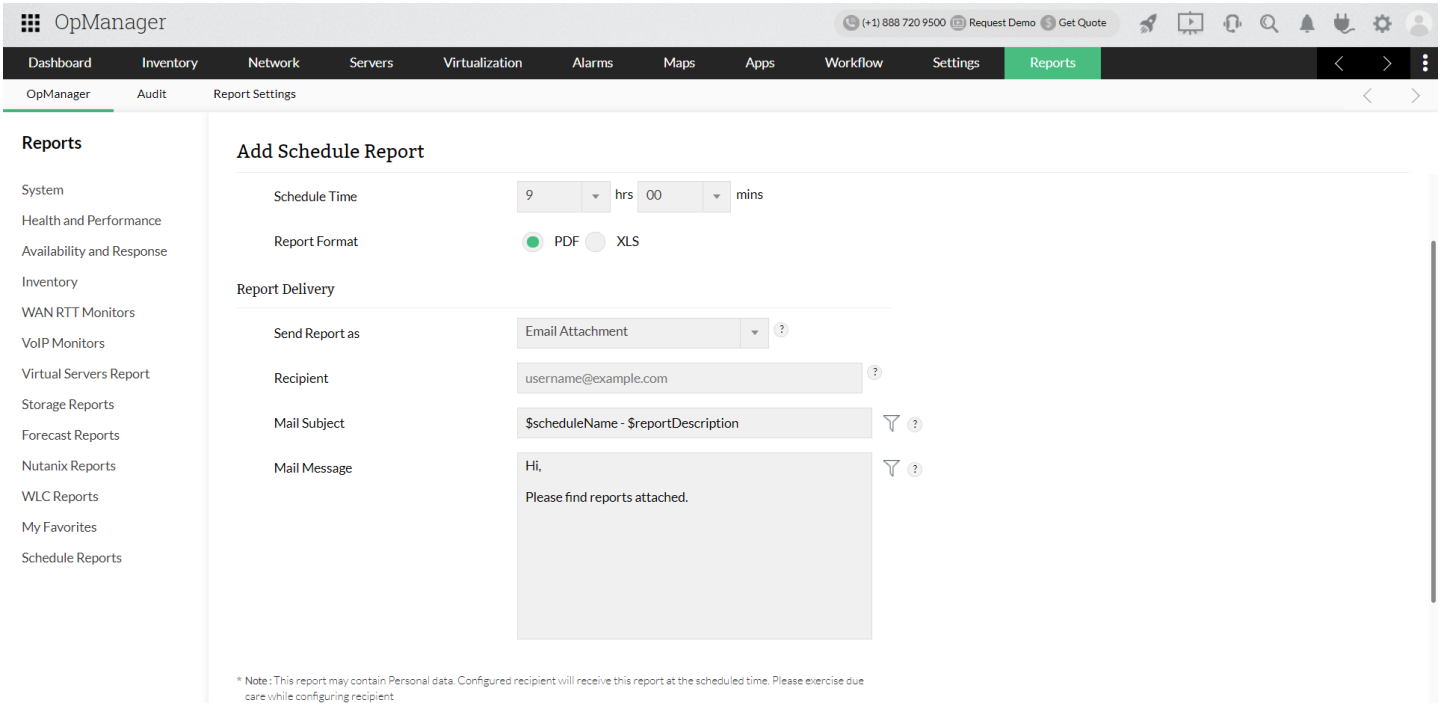
- If you have selected to schedule the Top N Reports, configure the following details:
- **Top N Reports**: Select from Top 10/25/50/100/1000 reports.
- **Period and Time Window**: Choose the Period and Time Window for which you want the report scheduled. In time period, select the days for which you 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:**

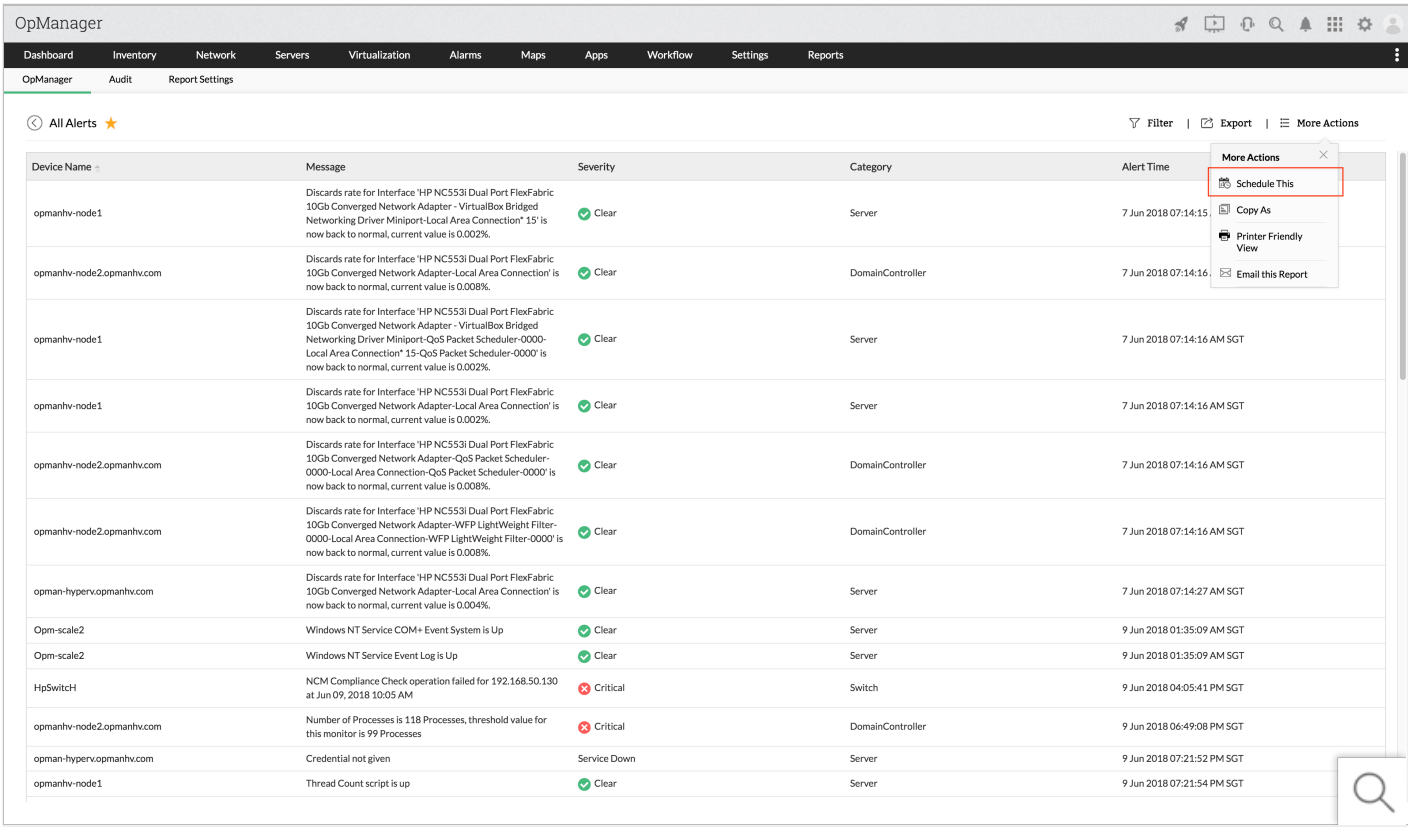
- **Daily**: Select the time at which the reports must be generated every day
- **Weekly**: Select the time and also the days on which the reports must be generated
- **Monthly**: Select the time, day, and the months for which the reports must be generated
- **Report Format Type**: Select either PDF 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**:**ð** Configure the url where the reports can be published
    - Add **Mail Subject** and **Mail Message**

5. Verify the details of the configured schedule and hit **Add Schedule** for the schedule to take effect

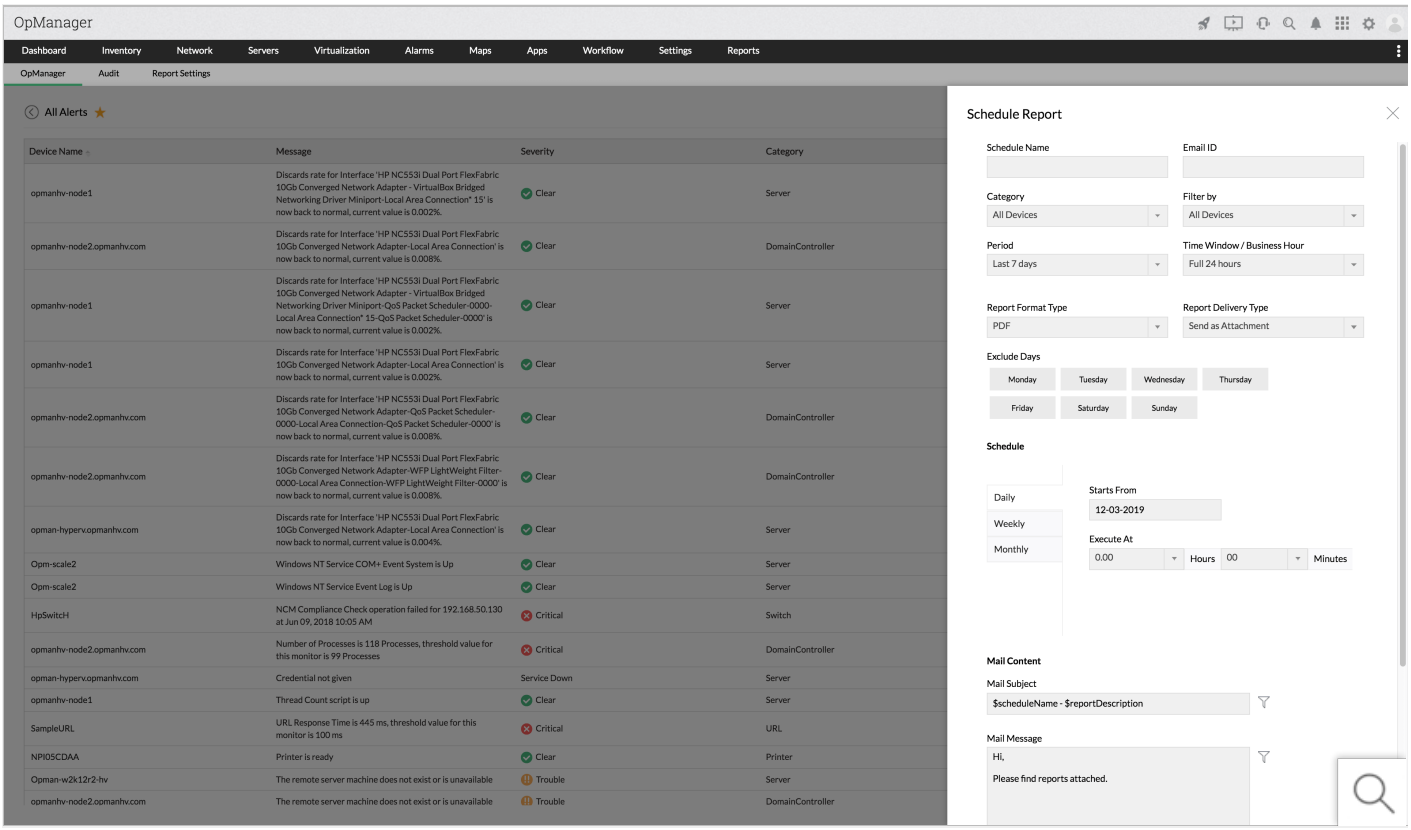


Scheduling a generated report

1. In the report page that is generated, click **Schedule This**icon to schedule the report.



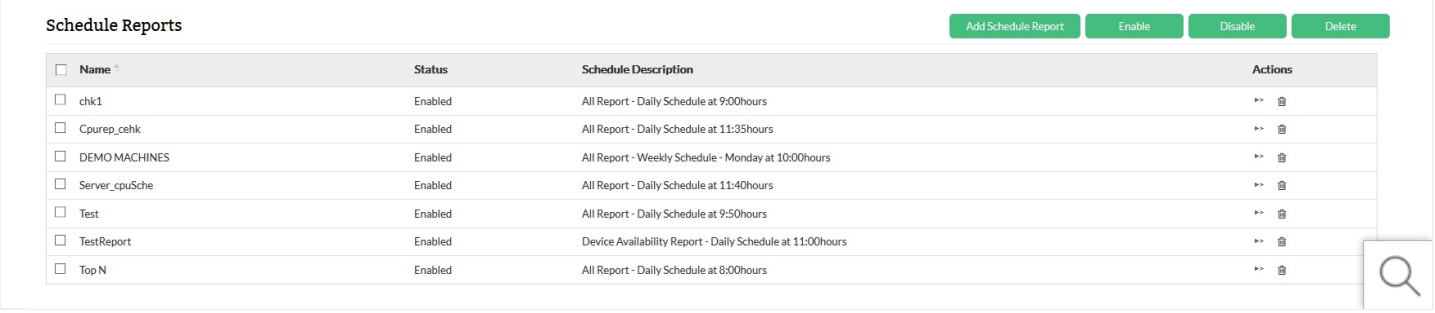
2. Enter the **Schedule Name**
3. Enter the**&#65533; Email ID&#65533;** to which the report has to be delivered
4. Select the **Category** followed by**&#65533; Business View**
5. Select the **Period** and **Time Window**. In time period, you can select the days for which you want to exclude data in 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**



). Click **Save** to create a schedule for the generated report.

Viewing the Scheduled Report

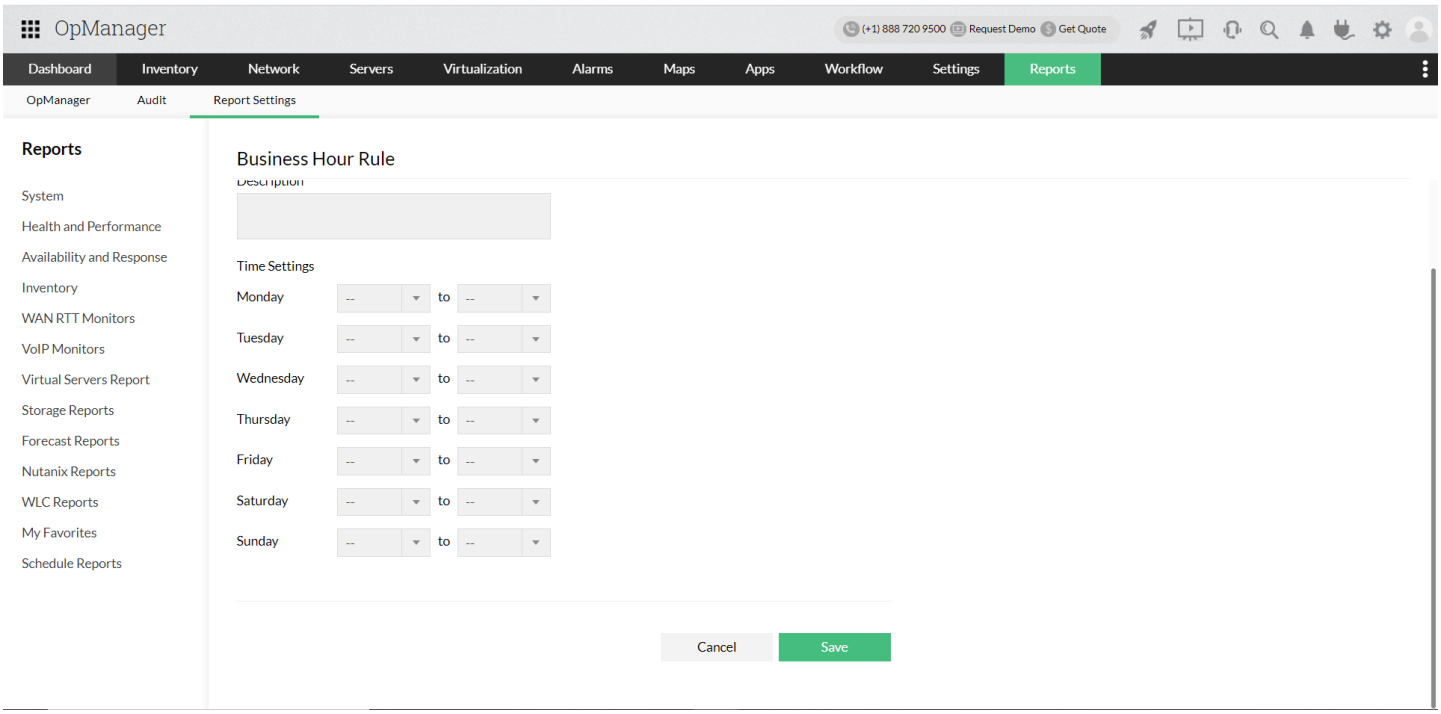
1. Go to Reports → Schedule reports
2. Click against the **View** icon on the required report that you wish to see.
3. The list of generated reports for the selected report will appear.



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**.

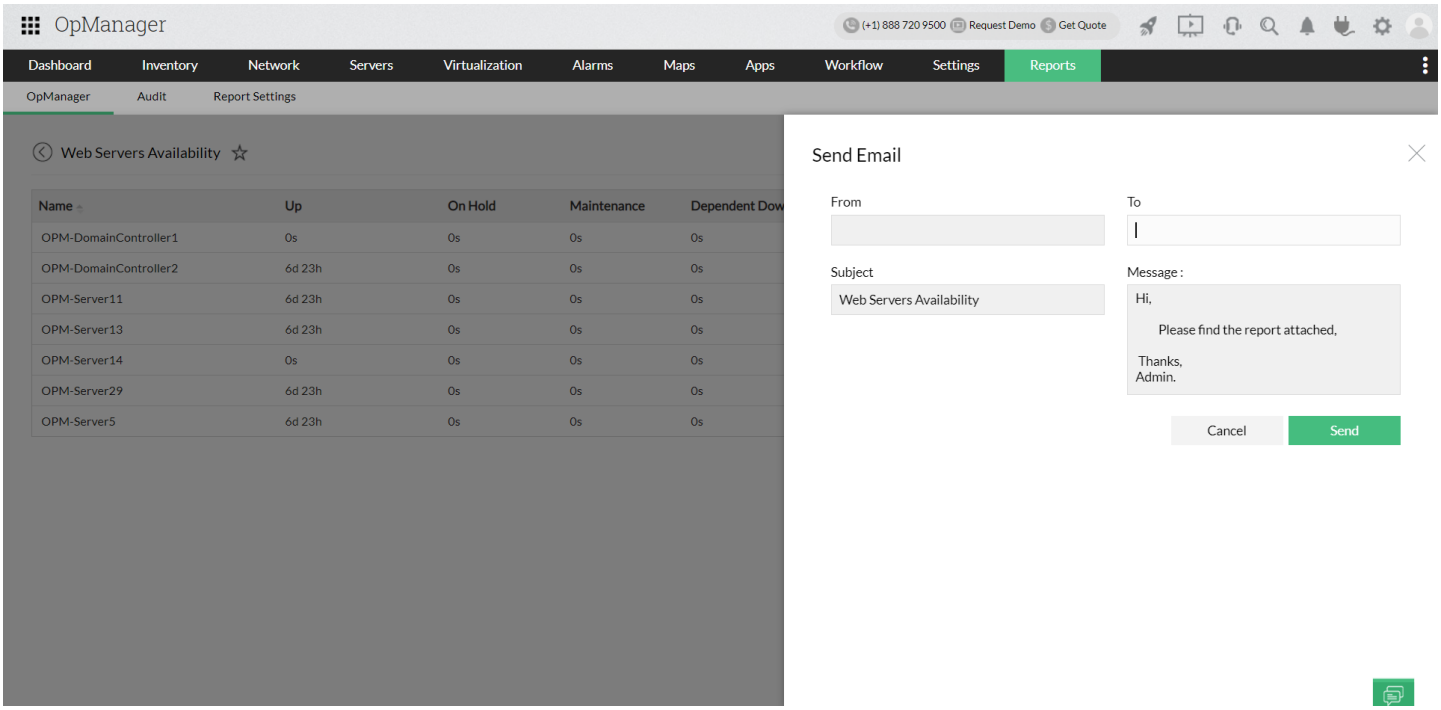


How to disable or enable scheduled reports in bulk

- 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

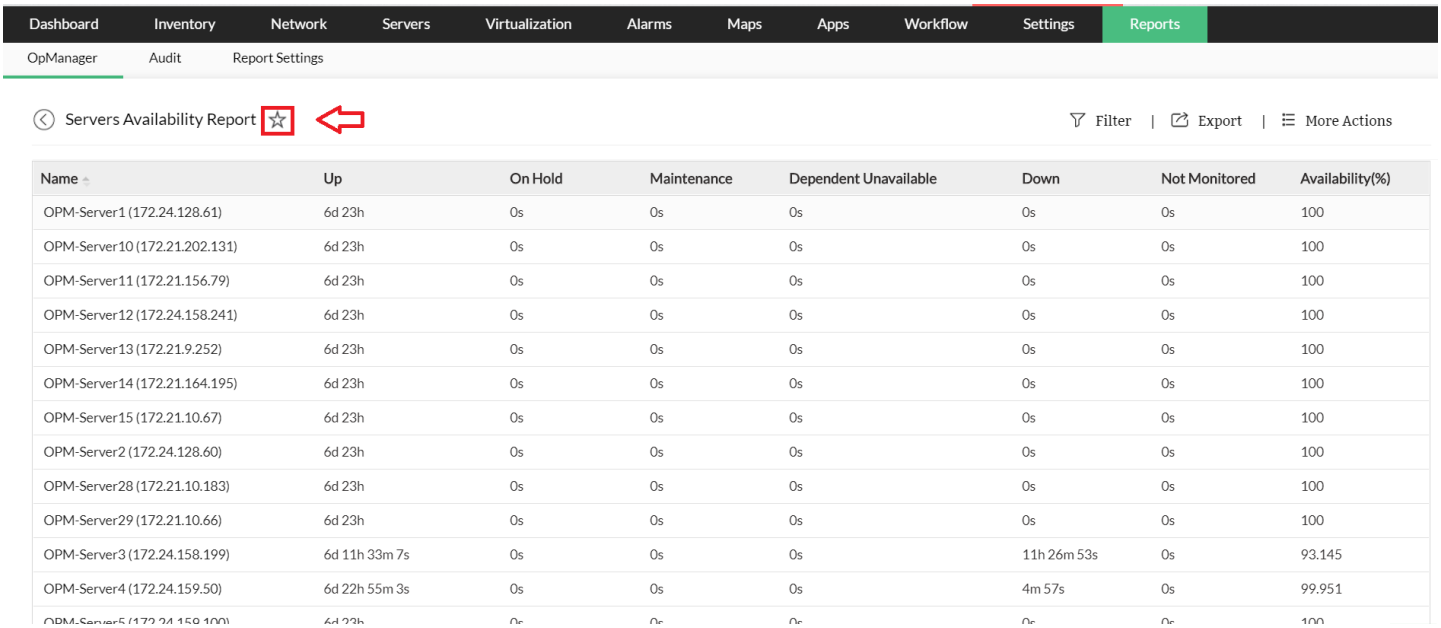
- Navigate to **Reports --> OpManager**.
- Select the particular report from a report category. (For Eg: Availability and Response --> Web Servers Availability)
- Click on *More Actions* on the top right corner.
- And click on *Email this Report*.
- Then enter the *From* and *To* mail IDs along with the *Subject* and *Message.*
- Finally click *Send*.



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".

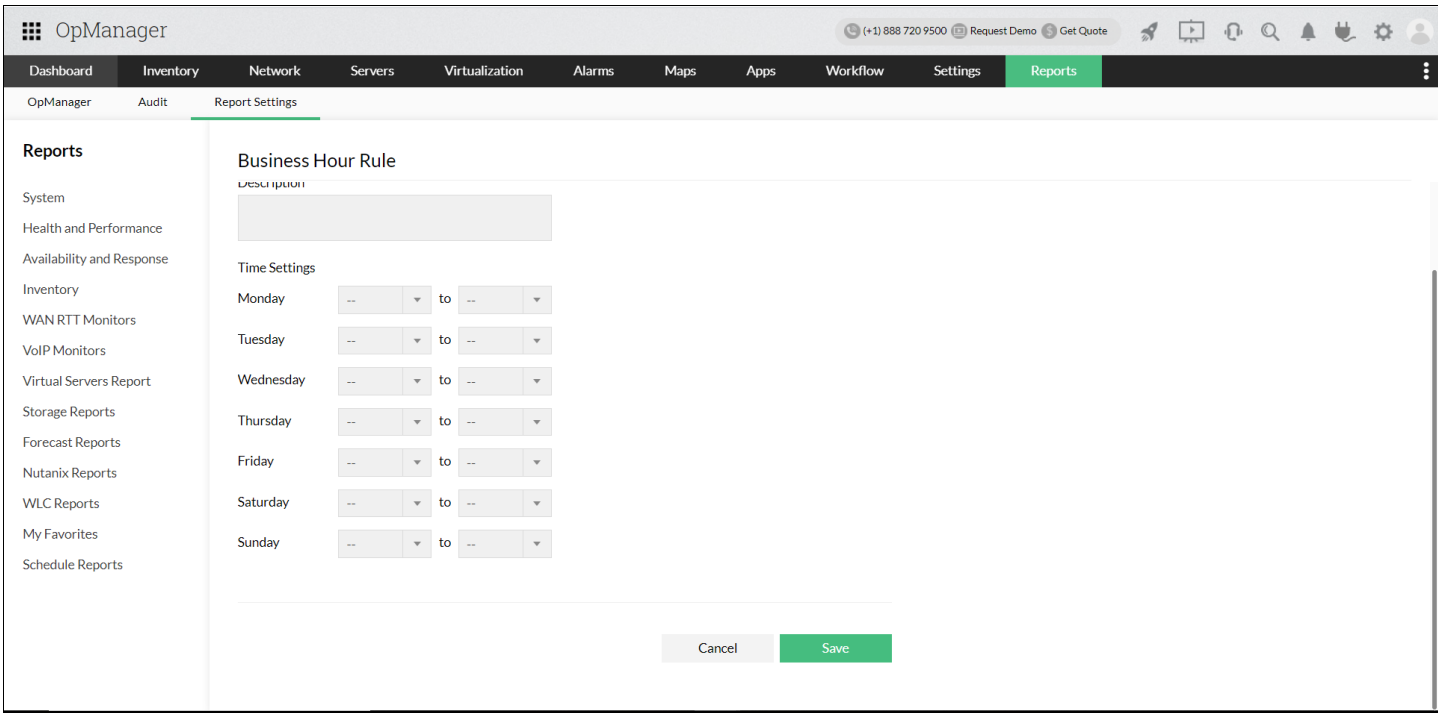
Report Settings

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.

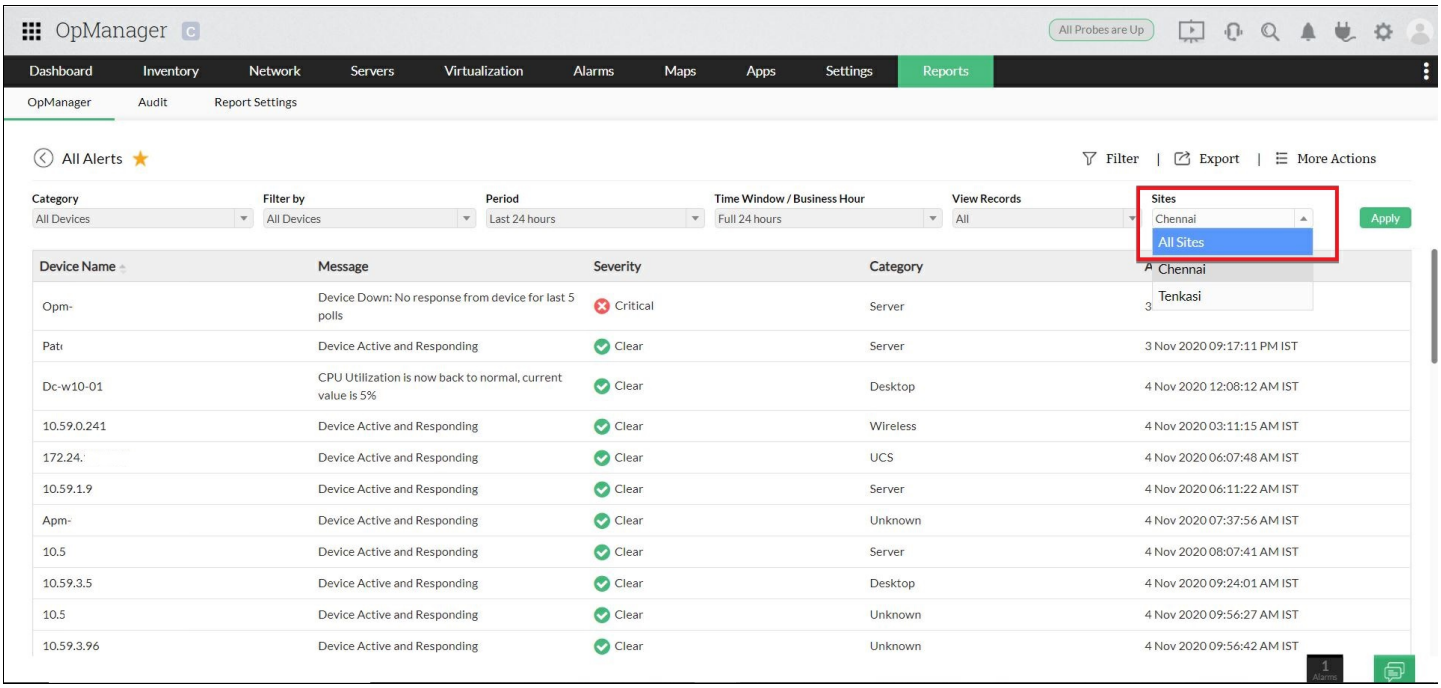
How to configure Business Hour Rule?

- 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**.

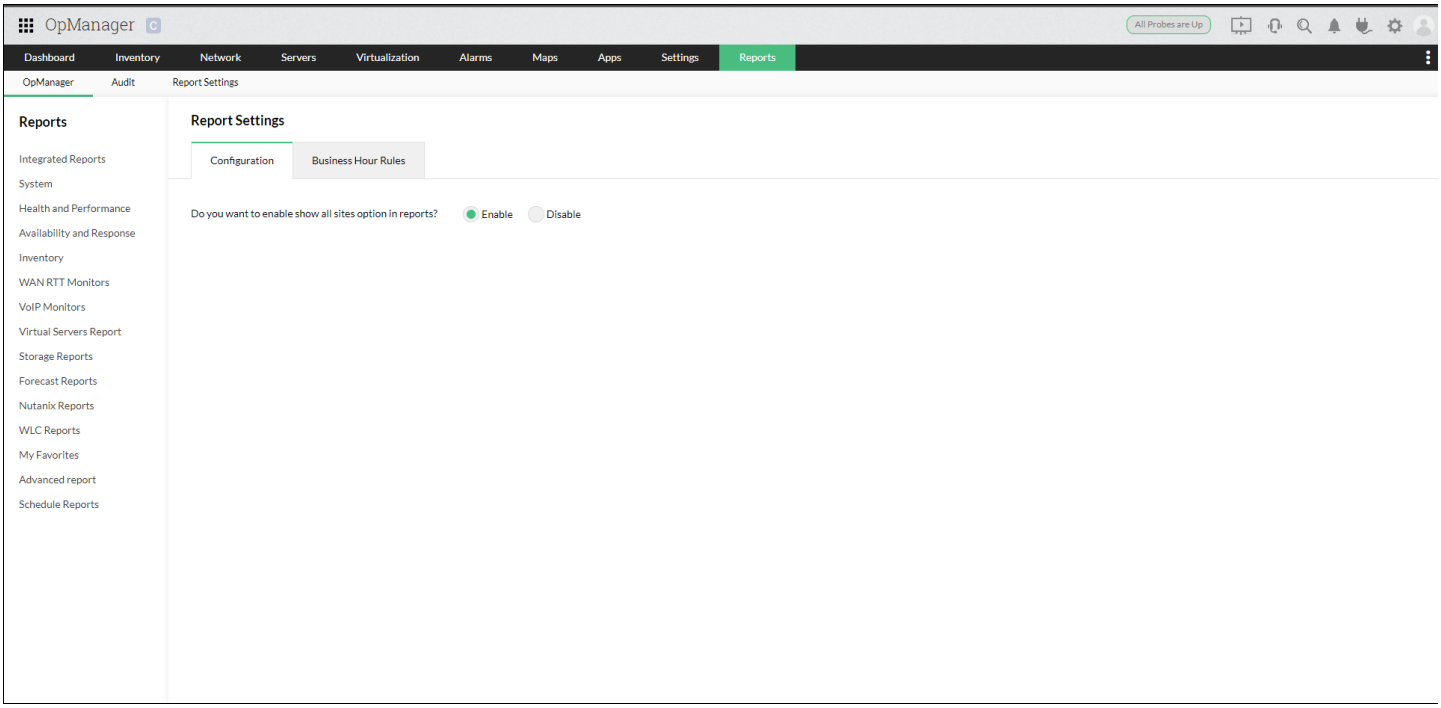


Configuration

While creating filters for reports from the Central, users can configure to show or hide the All Sites option in the drop down. Choosing the All Sites option lists the data of all the probes connected to the Central.



To enable or disable All Sites option, navigate to **Reports --> Report Settings --> Configuration**.



Advanced Reports

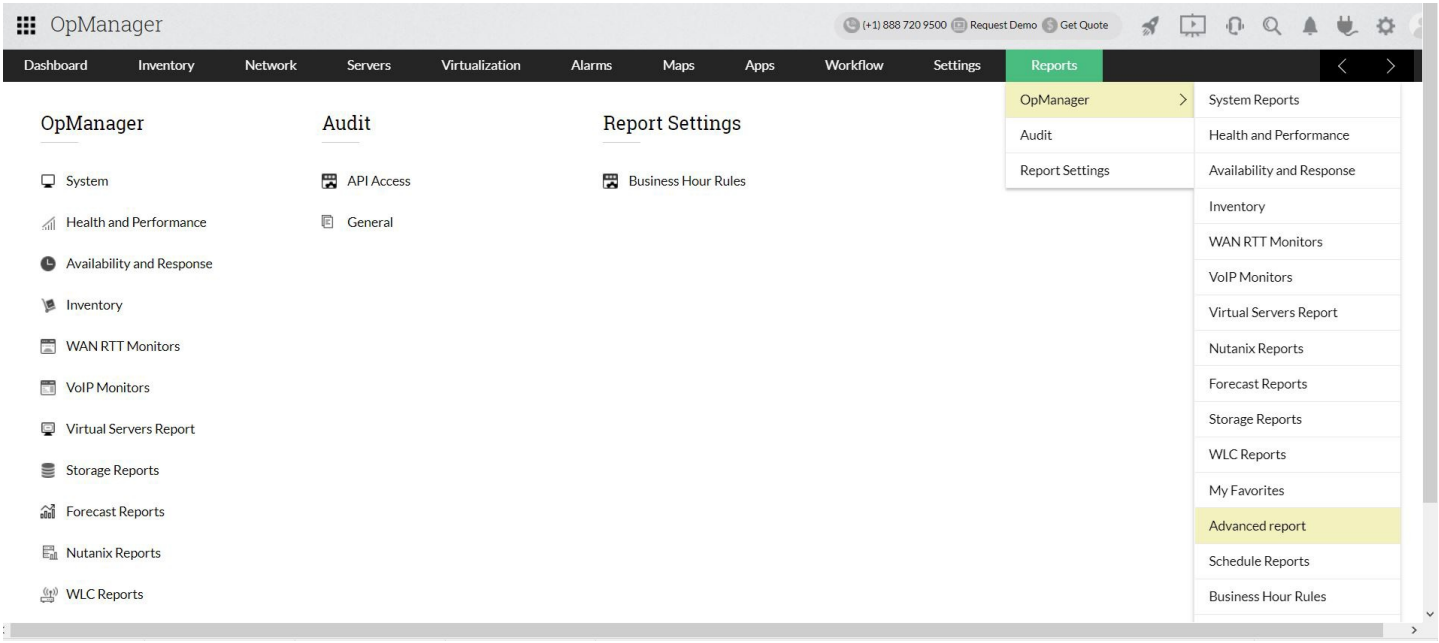
OpManager constantly monitors the network for performance and availability and records the data in the form of reports. There are about 100+ default intuitive reports in OpManager that enable the users to understand the trends based on the monitoring parameters.

Previously, users could create reports with anyone of the following categories: Performance/Availability/Response Time and Packet Loss/ Inventory.

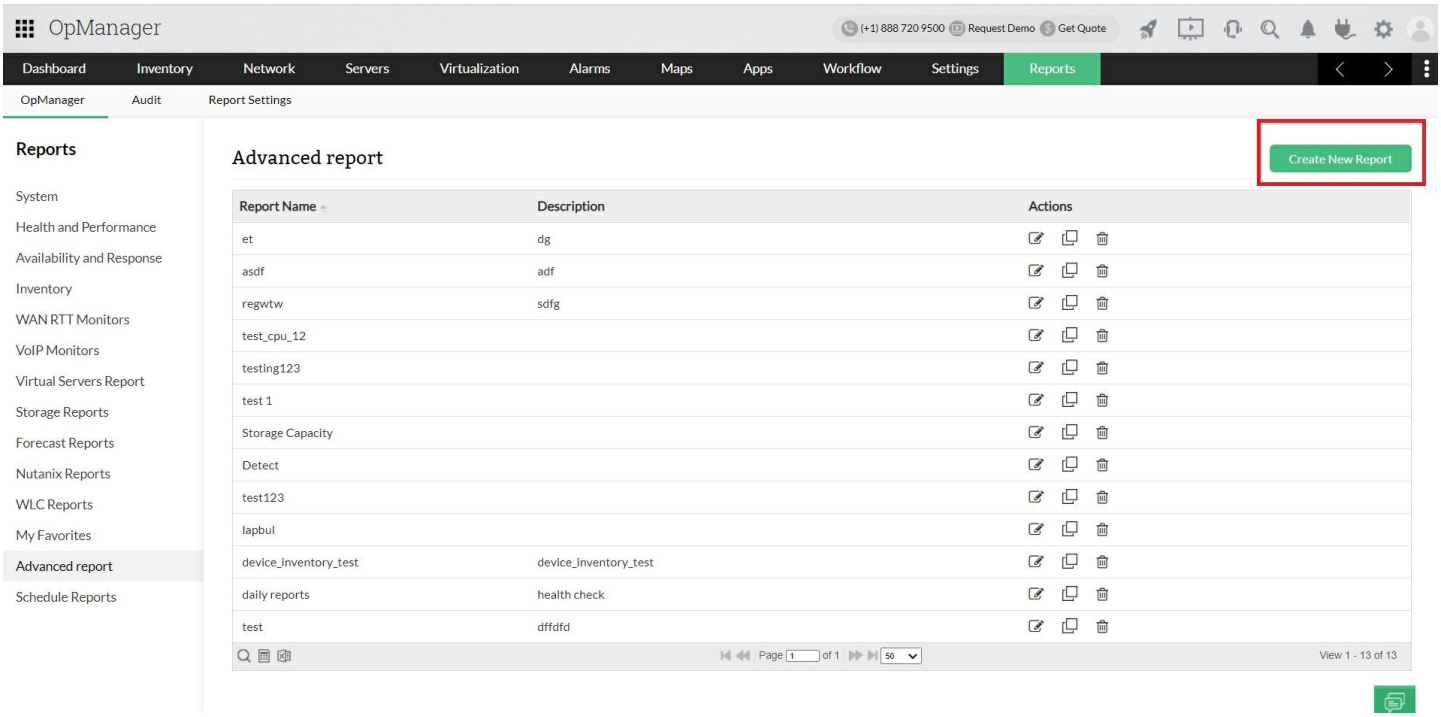
Now OpManager has advanced report creation capabilities and allows its users to create reports covering multiple categories. There will be as many columns as the number of monitoring parameters specified.

How to create New Advanced Report?

- Navigate to **Reports OpManager --> Advanced report.**

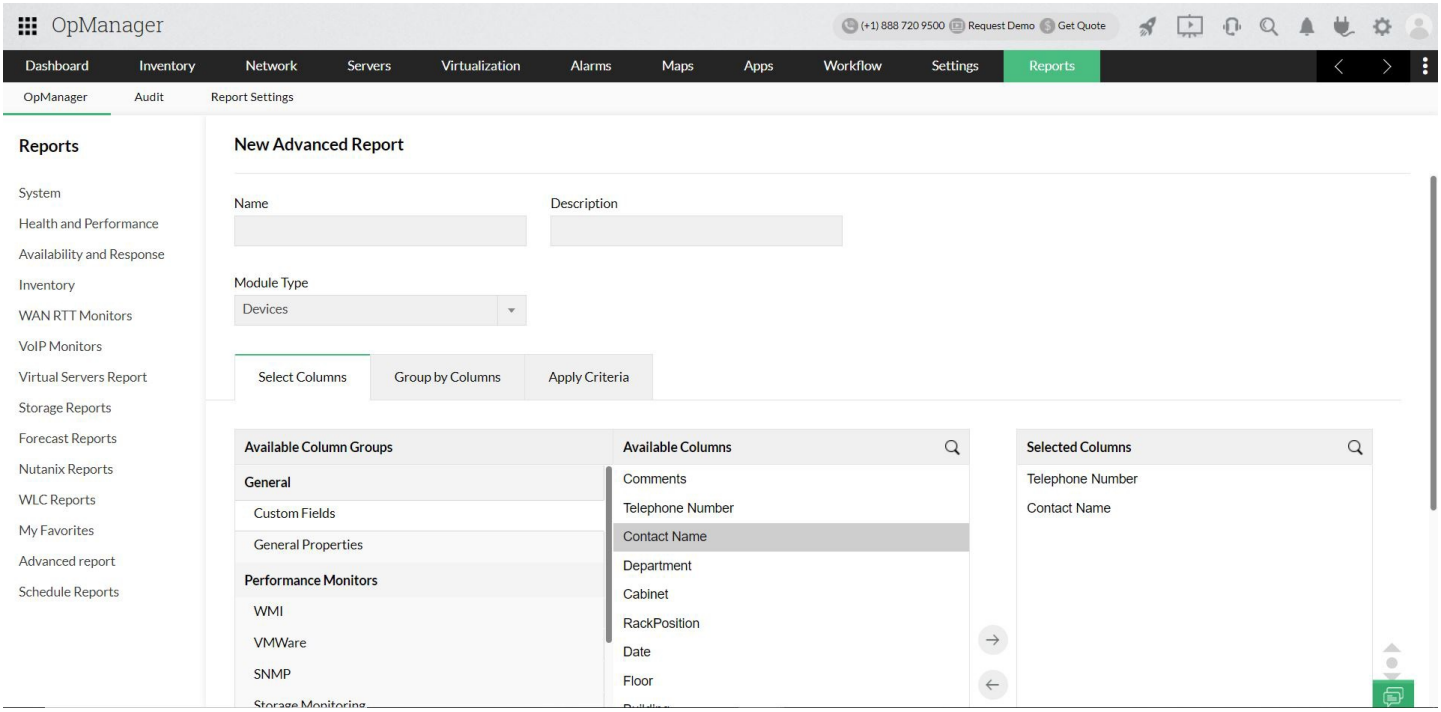


- Click on **Create New Report** button available on the top right corner.

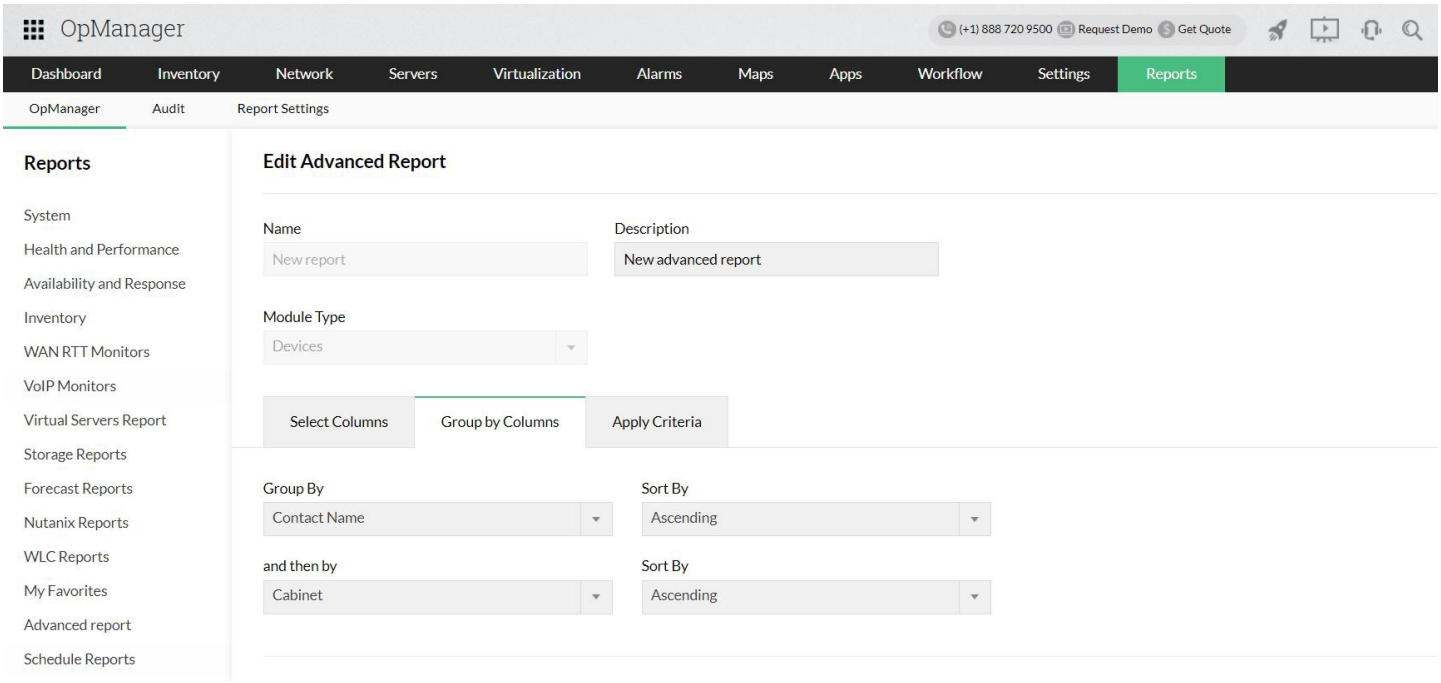


- Enter a suitable *Name* and *Description* for the report.

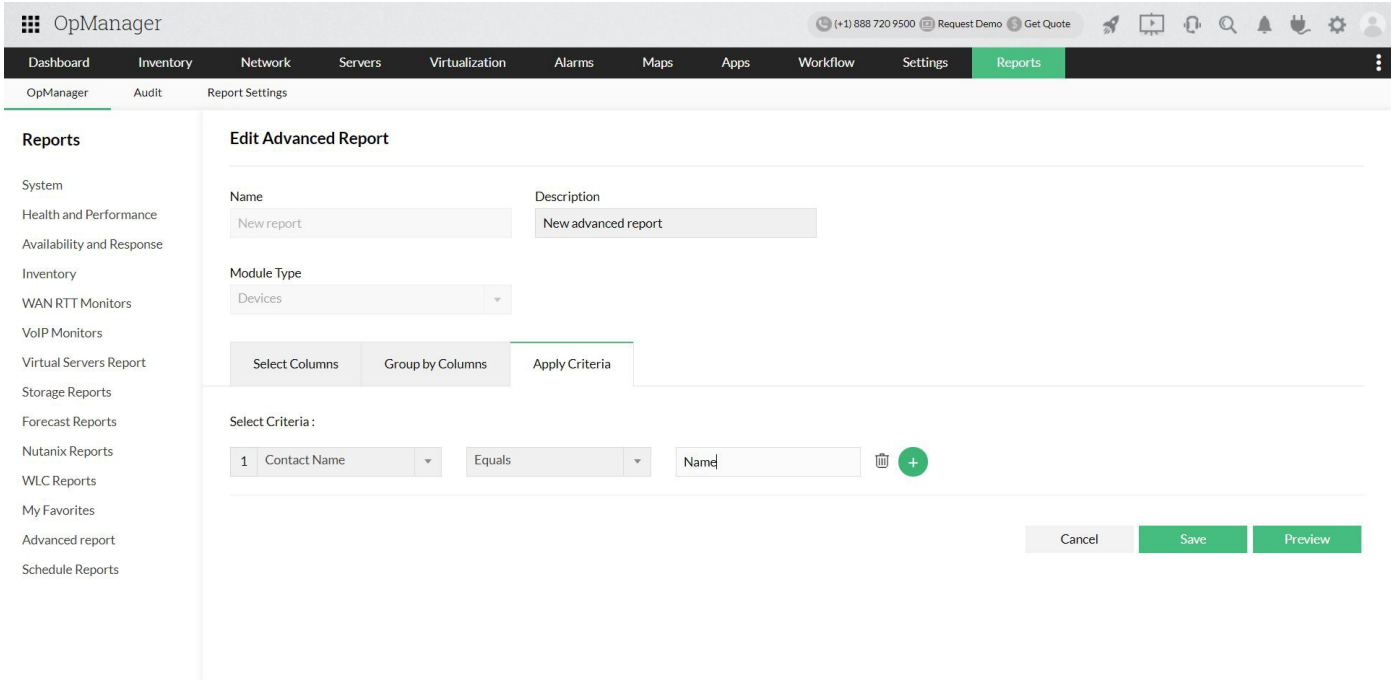
- Select a *Module* from the available list of modules - Devices, Interfaces, Service Monitors, URL Monitors, Alarms.
- Select your preferred parameter categories from the *Available Column Groups*. Within each parameter category, there are multiple properties. (Advanced reports give users the option to view inventory data and performance monitors in a single report.)
- Now select the properties in each chosen category from the *Available Columns*, and move them to the *Selected Columns*. (Users can view upto a maximum of 5 performance monitors in the report)



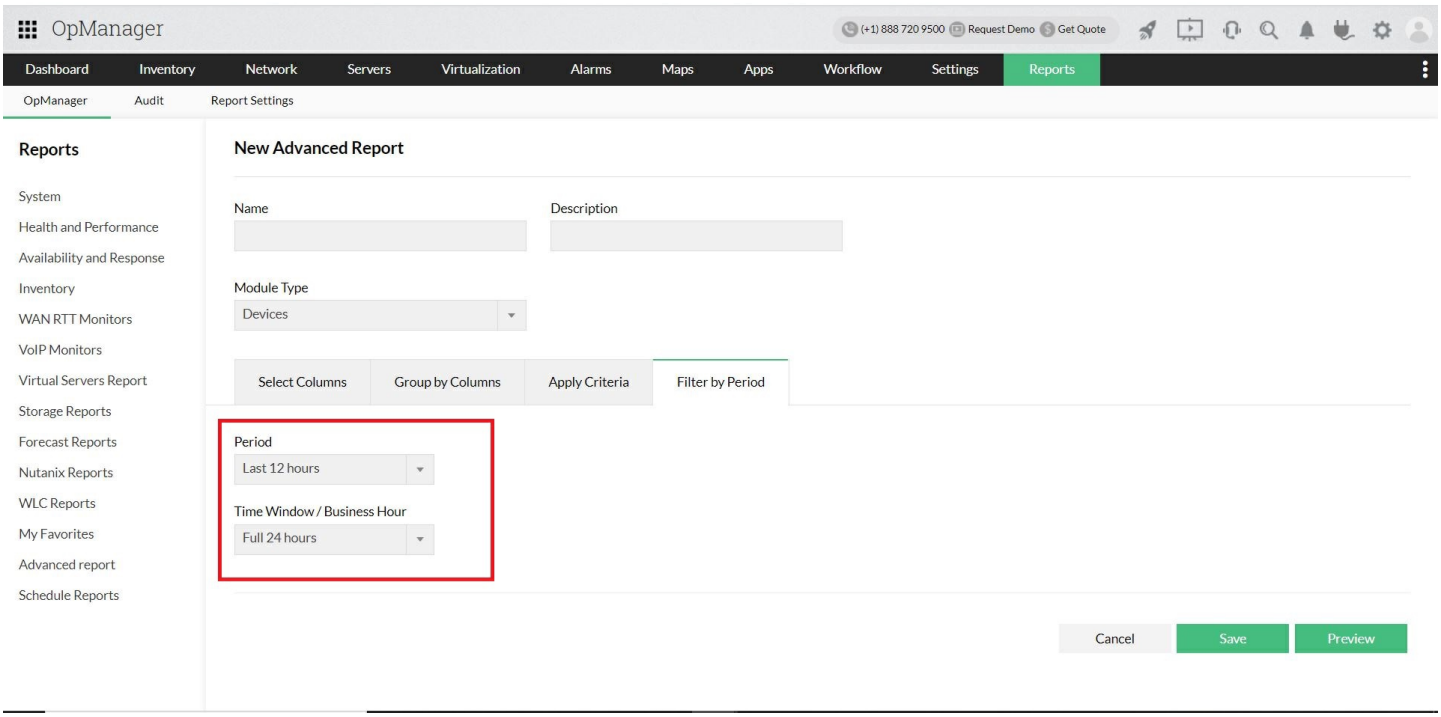
- Click on the **Group by Columns** button, if you want to sort the elements in the report. (For instance, if you choose to sort by Contact Name, the data will be displayed in alphabetical order of Contact Name.)



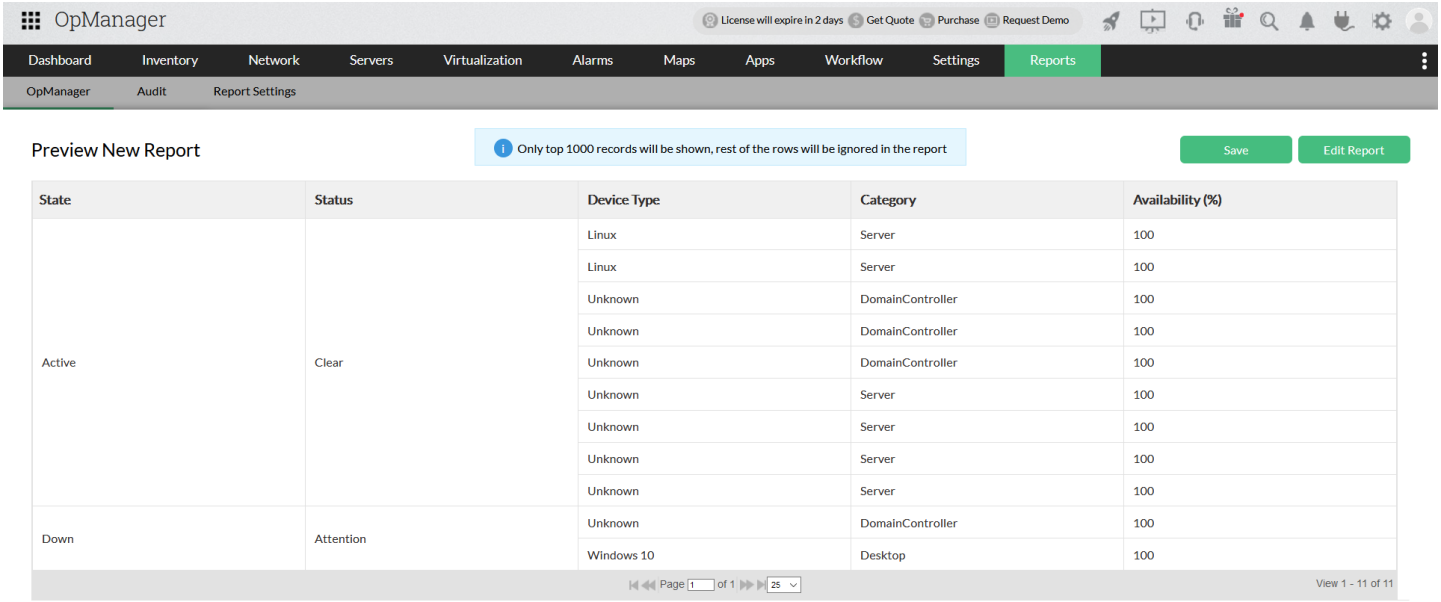
- Click on the **Apply Criteria** button and add the criteria to fetch a report based on that criteria. (Optional)



- If you happen to choose a performance monitor, a new tab - **Filter by Period** - appears. Specify the mandatory fields of filtering time period and the Business Hour of your organization. (The filtering period by default takes the value of 12 hours. But you can choose a different value from the dropdown list.)

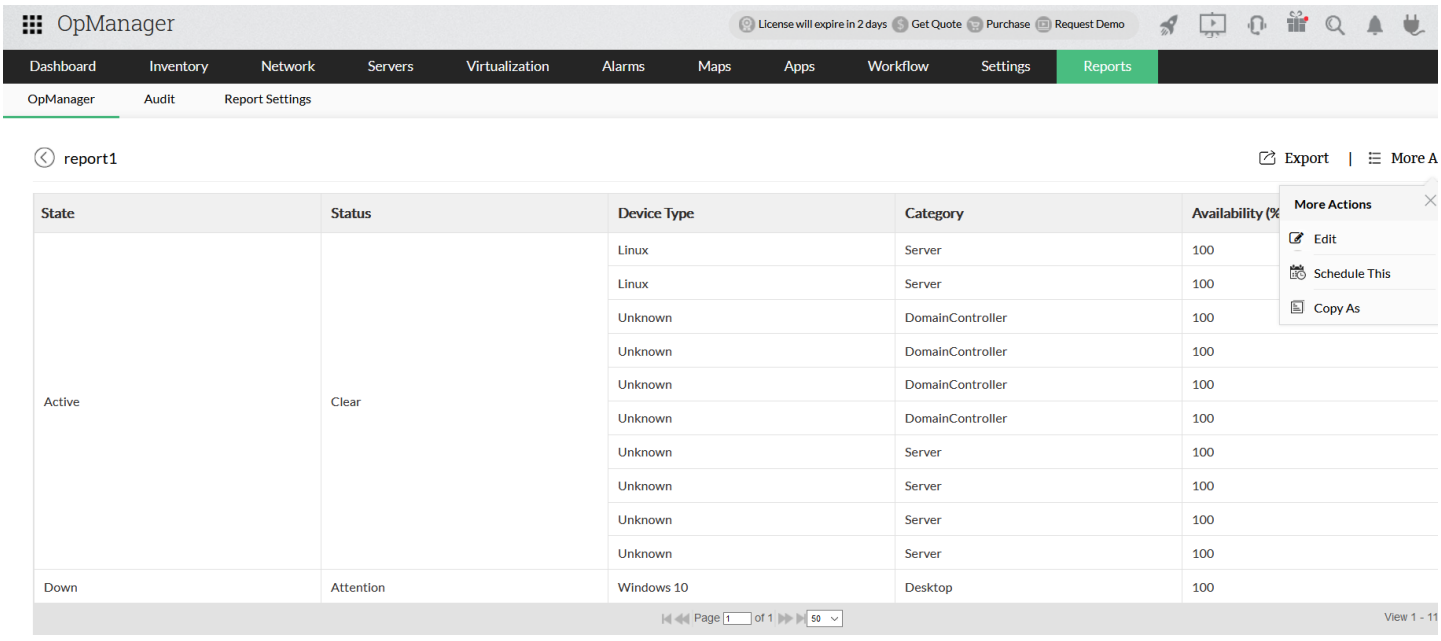


- Click on **Preview** to view the report before being created. Click on Edit Report button to return to the previous page.

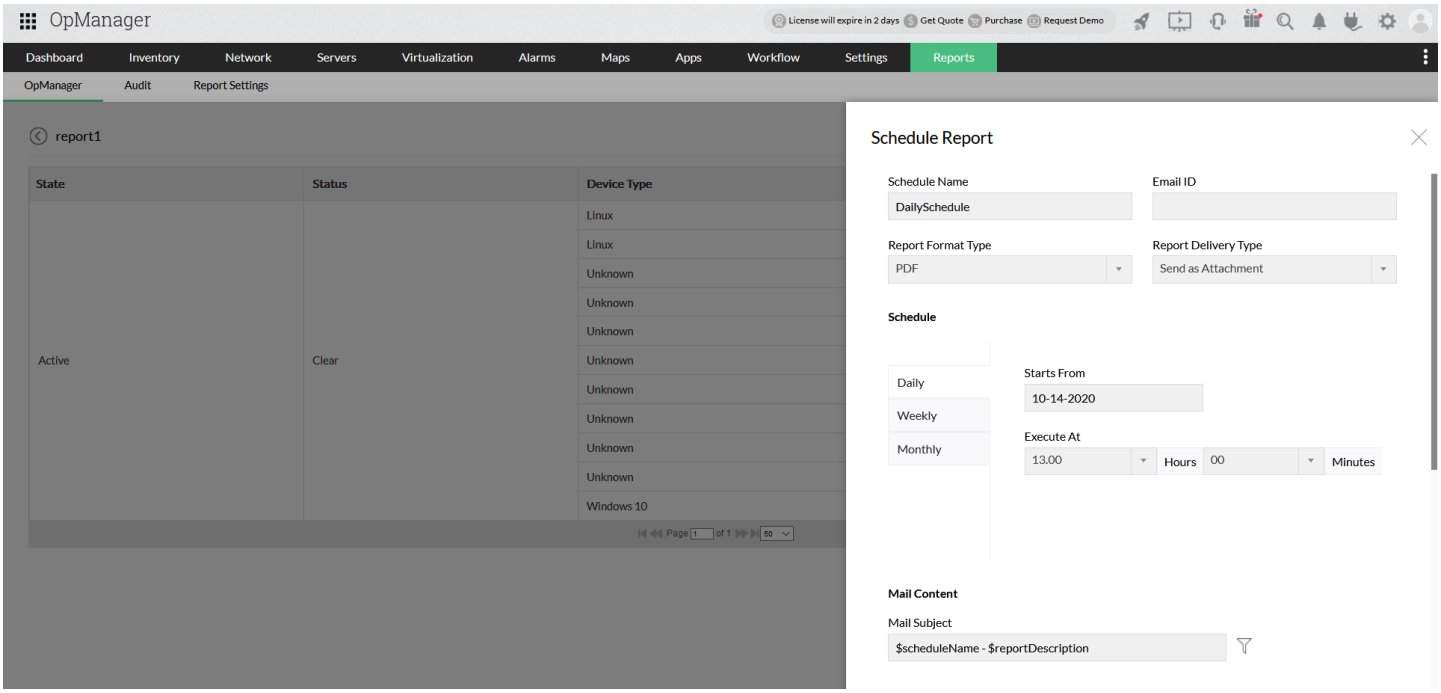


- Then click on **Save**.
- The report will be generated and stored and can be accessed in **Reports --> OpManager --> Advanced report**. (Users can view the top 1000 rows of the report.)

Useful features in advanced reports



- **Export:** The report can be exported and downloaded in PDF/Excel format. (Reports having upto 8 columns can be exported as PDF)
- **Edit:** Using the edit option users can add/remove or replace columns. It essentially gives the user a chance to re-design the report completely.
- **Copy As:** It enables the users to copy the report. Users can give a Name and Description for this copied report.
- **Schedule this:** This option enables users to send this report to a specified mail id at specific time intervals. Users can enter the Schedule Name, Mail id, Report Format, Schedule time - Daily, Weekly, Monthly and Mail Content.

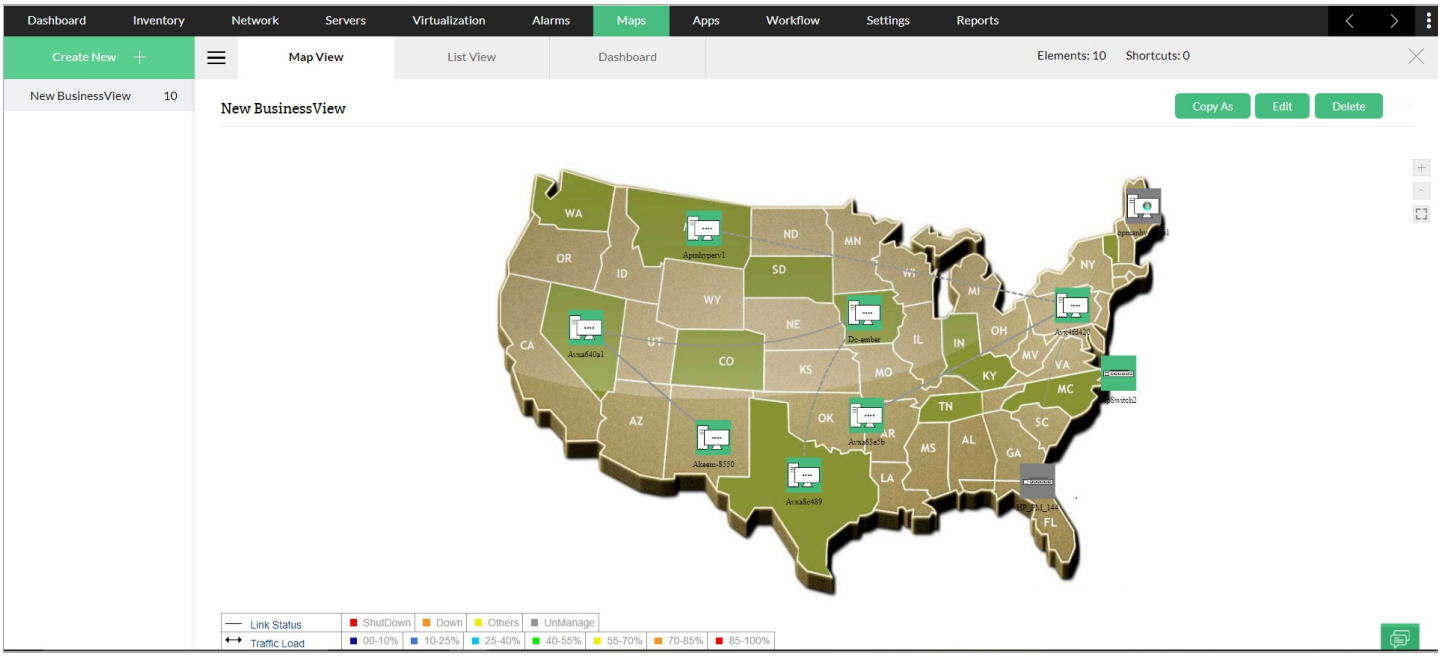

OpManager
License will expire in 2 days
Get Quote
Purchase
Request Demo
Dashboard
Inventory
Network
Servers
Virtualization
Alarms
Maps
Apps
Workflow
Settings
Reports
OpManager
Audit
Report Settings
report1
State
Status
Device Type
Active
Clear
Linux
Linux
Unknown
Unknown
Unknown
Unknown
Unknown
Unknown
Unknown
Unknown
Windows 10
Page 1 of 1
50
Schedule Report
Schedule Name
DailySchedule
Email ID
Report Format Type
PDF
Report Delivery Type
Send as Attachment
Schedule
Daily
Weekly
Monthly
Starts From
10-14-2020
Execute At
13.00
Hours
00
Minutes
Mail Content
Mail Subject
$scheduleName - $reportDescription

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:

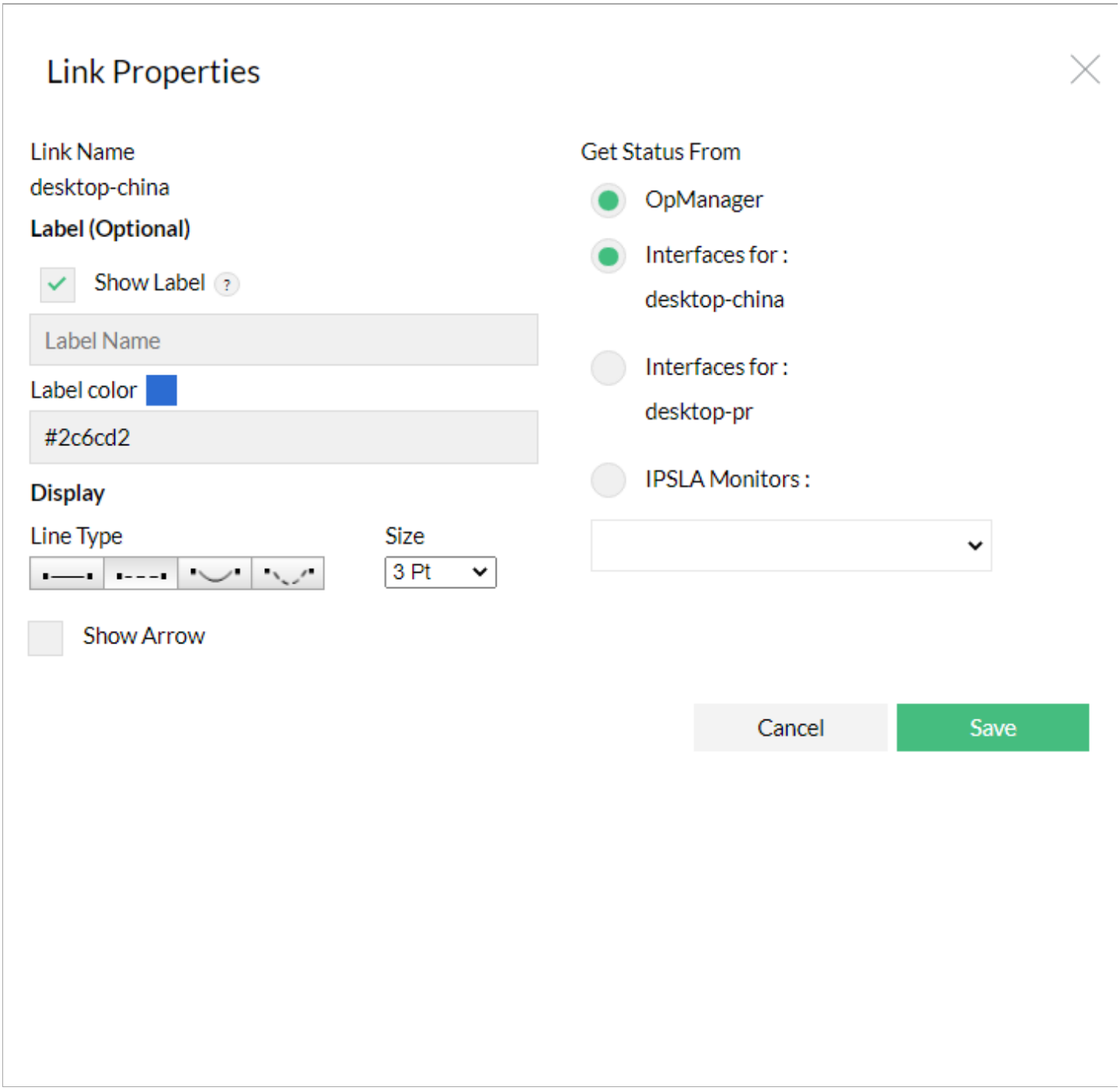
Adding links between devices in business views, helps to represent network diagram on the map. These links can be configured based on user requirements.

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:

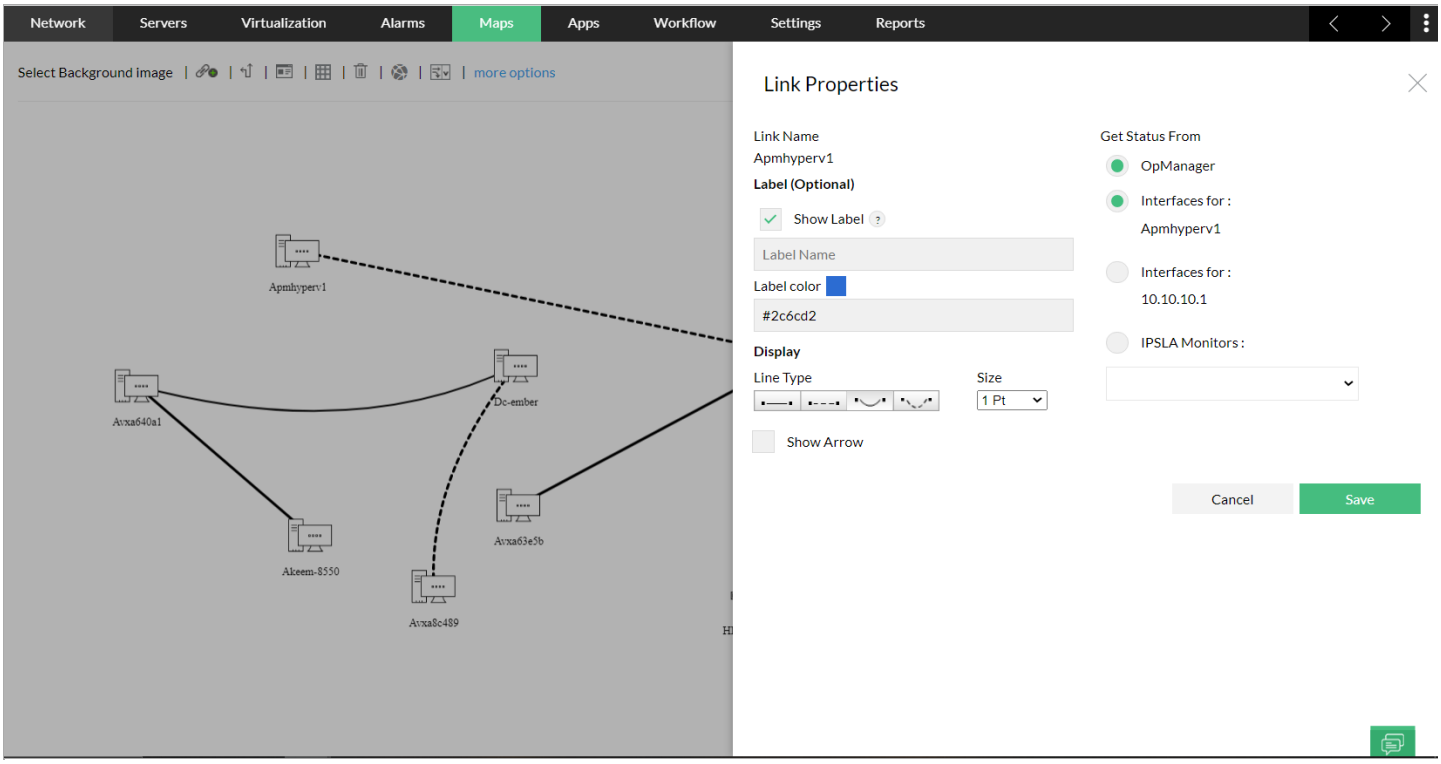
1. To make changes to the existing business views, Access the business view from the **Maps** tab.
2. Click the **Edit** icon to modify the view properties.
3. After modifying the properties like adding/removing links, adding more devices to the view, adding shortcuts on the view, changing background 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.
6. 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

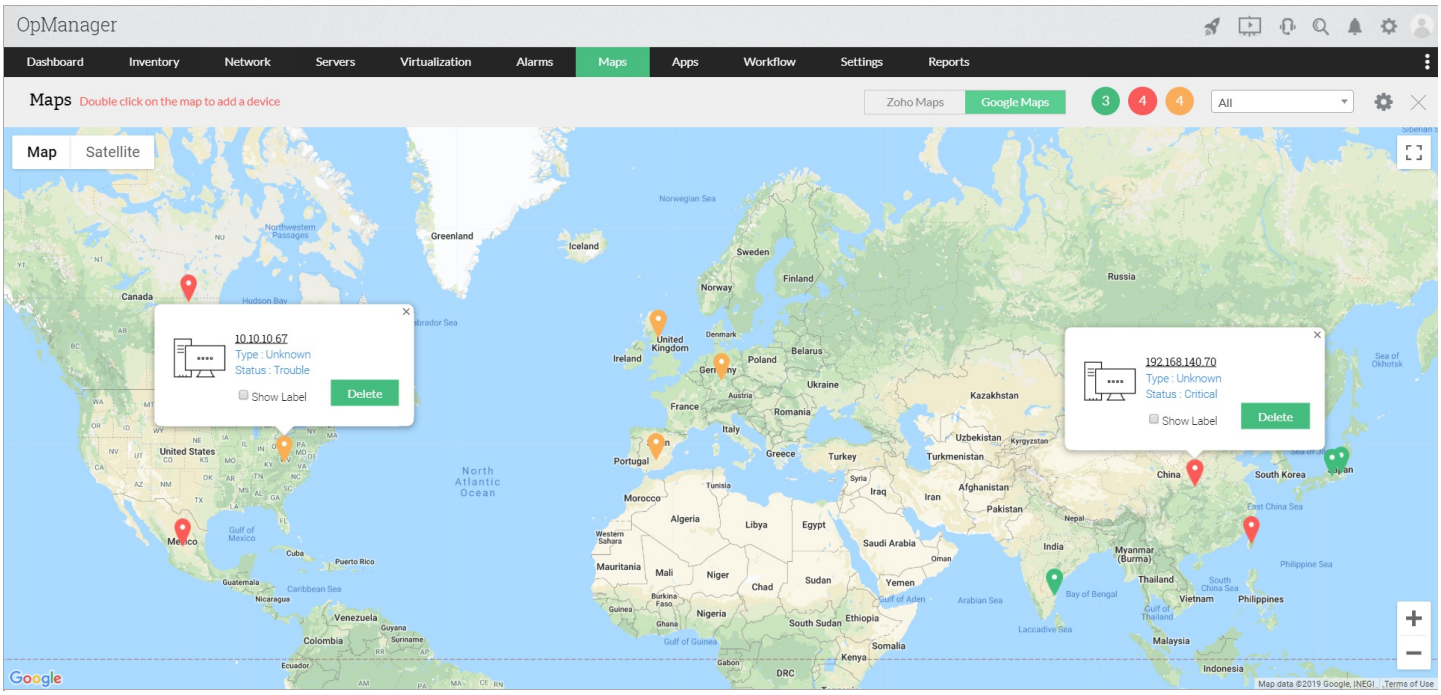
1. Click on the device marker on the Google Map to see the device information popup.
2. Click the device name/IP address on this popup to get into the device snapshot page.
3. The popup also shows the device status.

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.

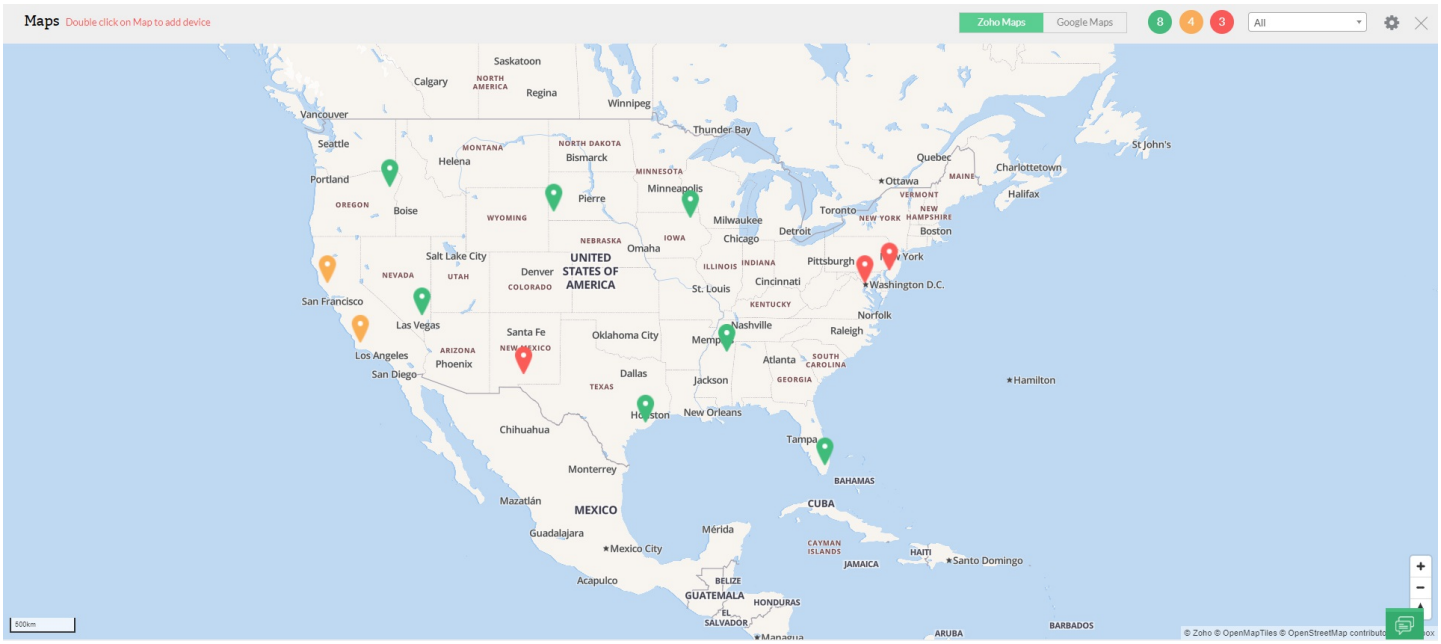
Viewing Device Details from Zoho Map

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

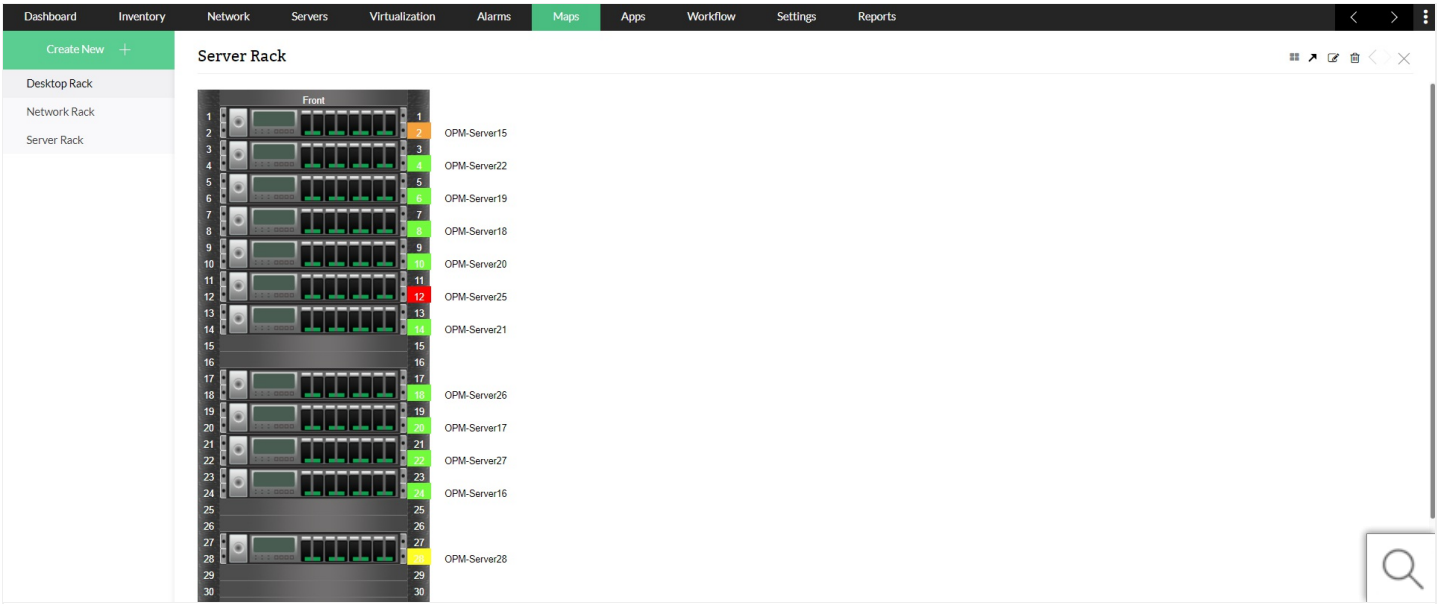
OpManager helps in creating a virtual replication of Datacenter floors and racks to enable 24x7 monitoring. Datacenter visualization is one among the many features of OpManager's data center networking tool.

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**.

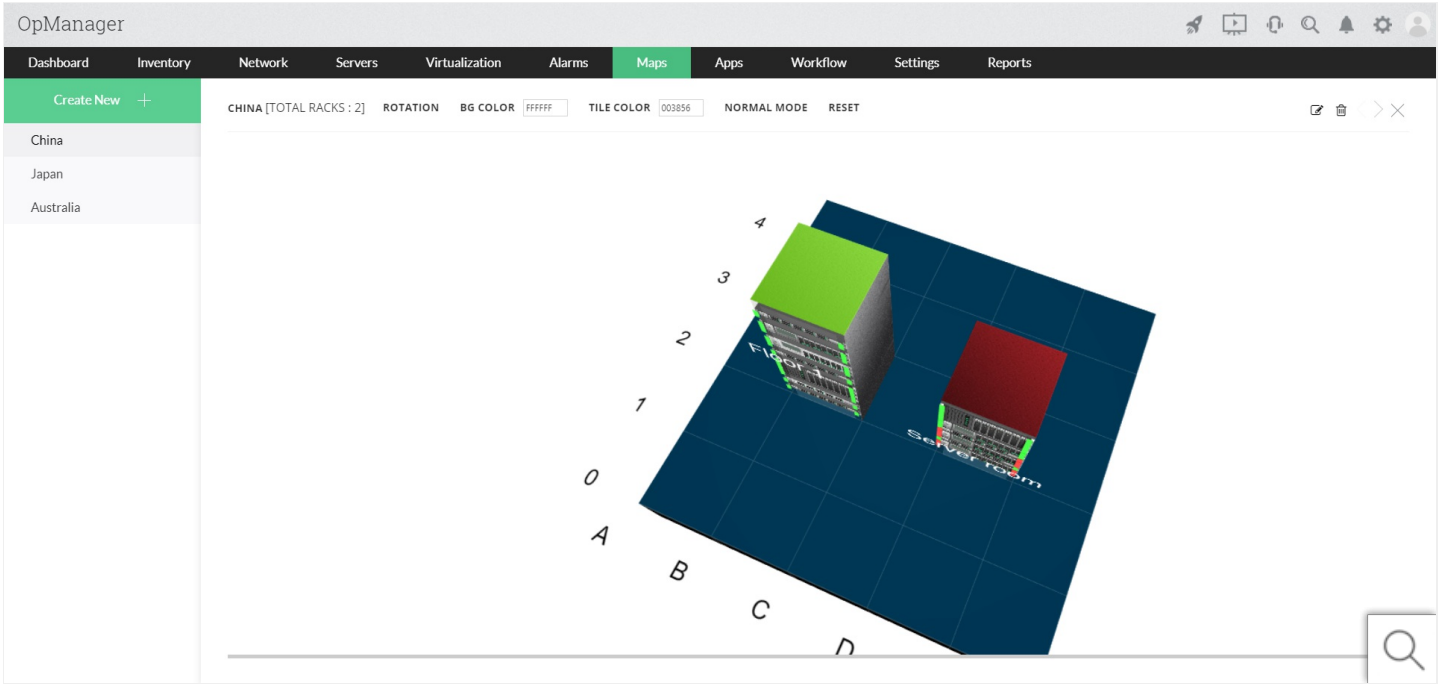


3D Floor View:

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:

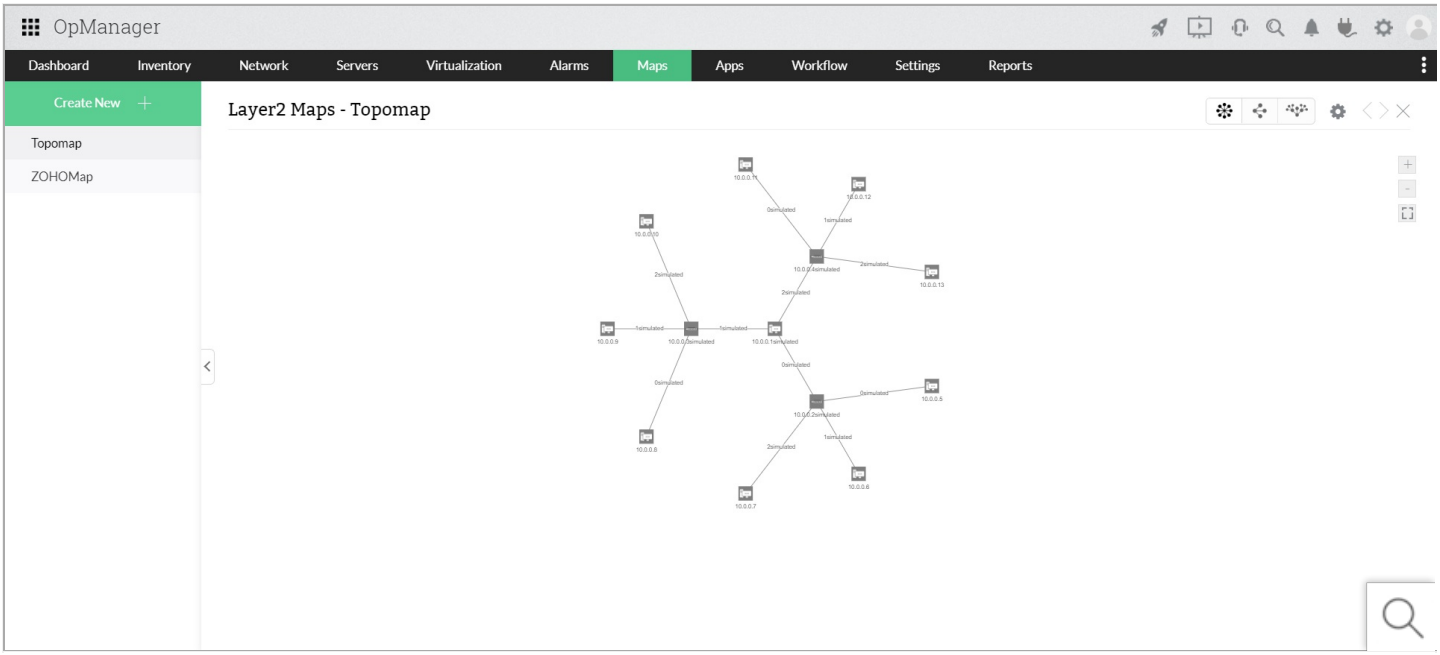
OpManager automatically maps L2 devices when Layer 2 discovery is done. The resultant map can be viewed under the Layer 2 tab

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.

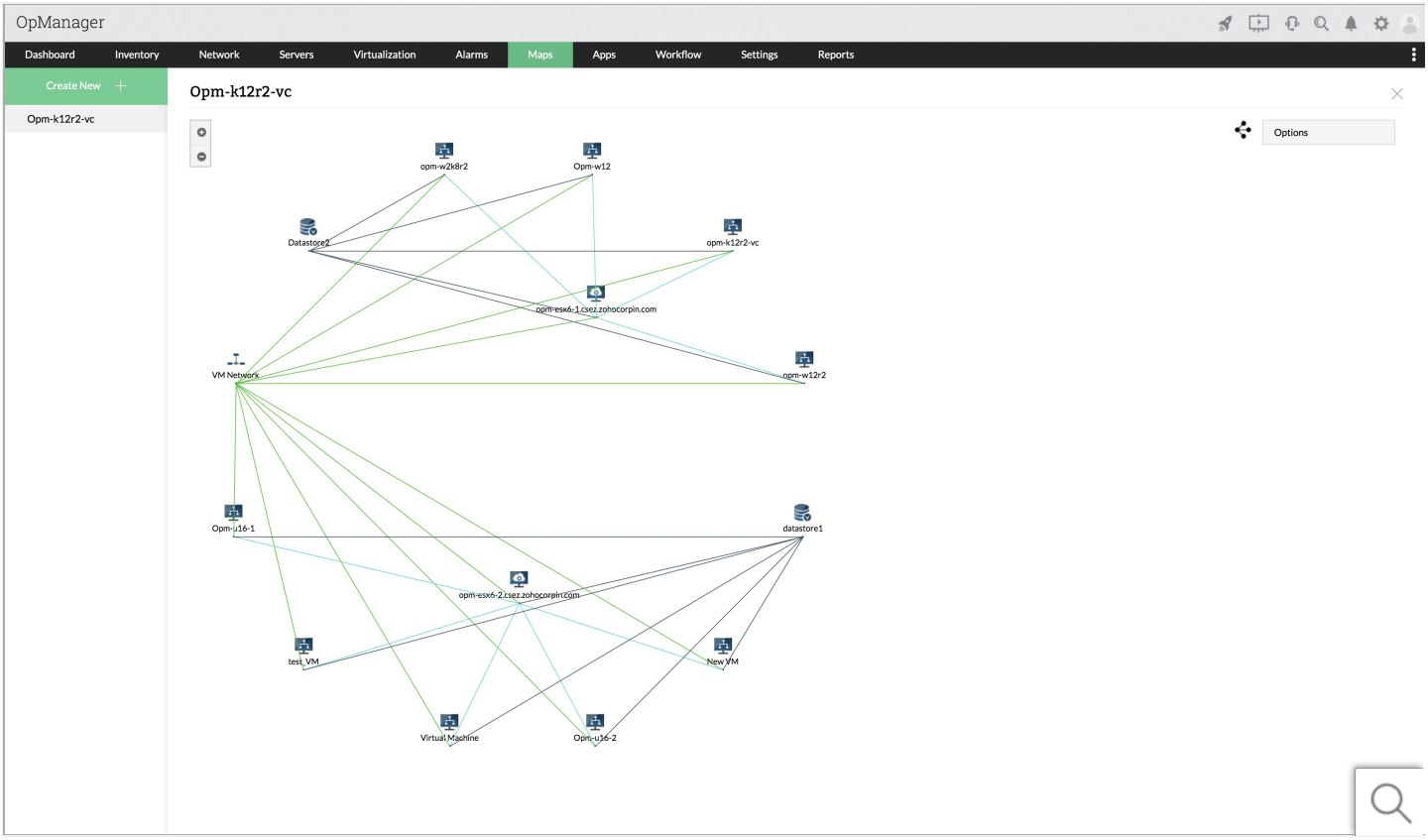


Virtual network maps

OpManager provides you the option to visualise your entire virtual infrastructure based on the vendor, allowing you to take a quick glance of all your hosts and VMs (and clusters, in the case of Nutanix) and their current status.

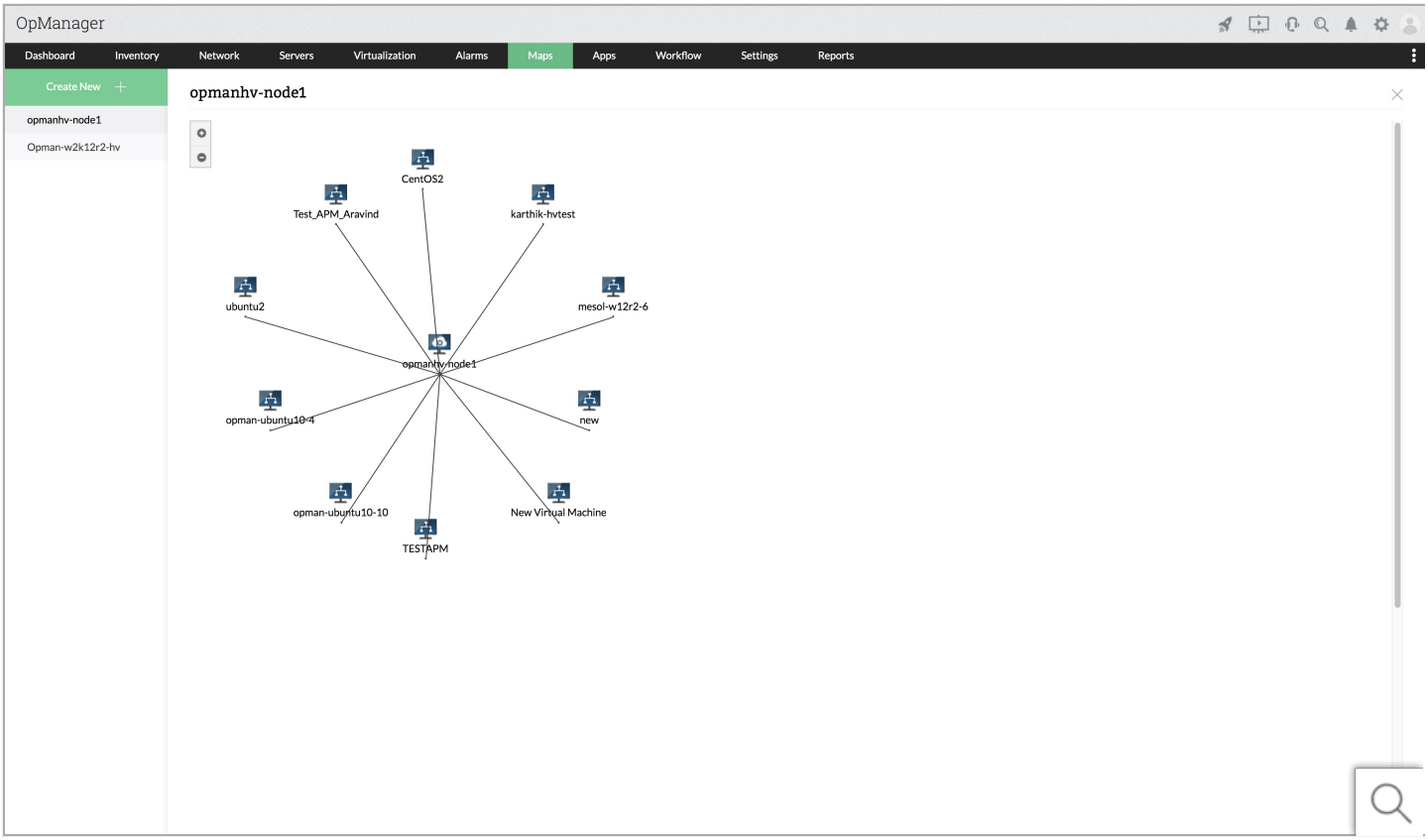
VMware Maps:

To access VMware maps, click on Maps and the click the VMware tab. The list of vCenter servers available in your network will be displayed, along with general info about your server such as number of hosts and number of VMs. Click on any of the servers listed to view the visual mapping of vCenter, its hosts and VMs.



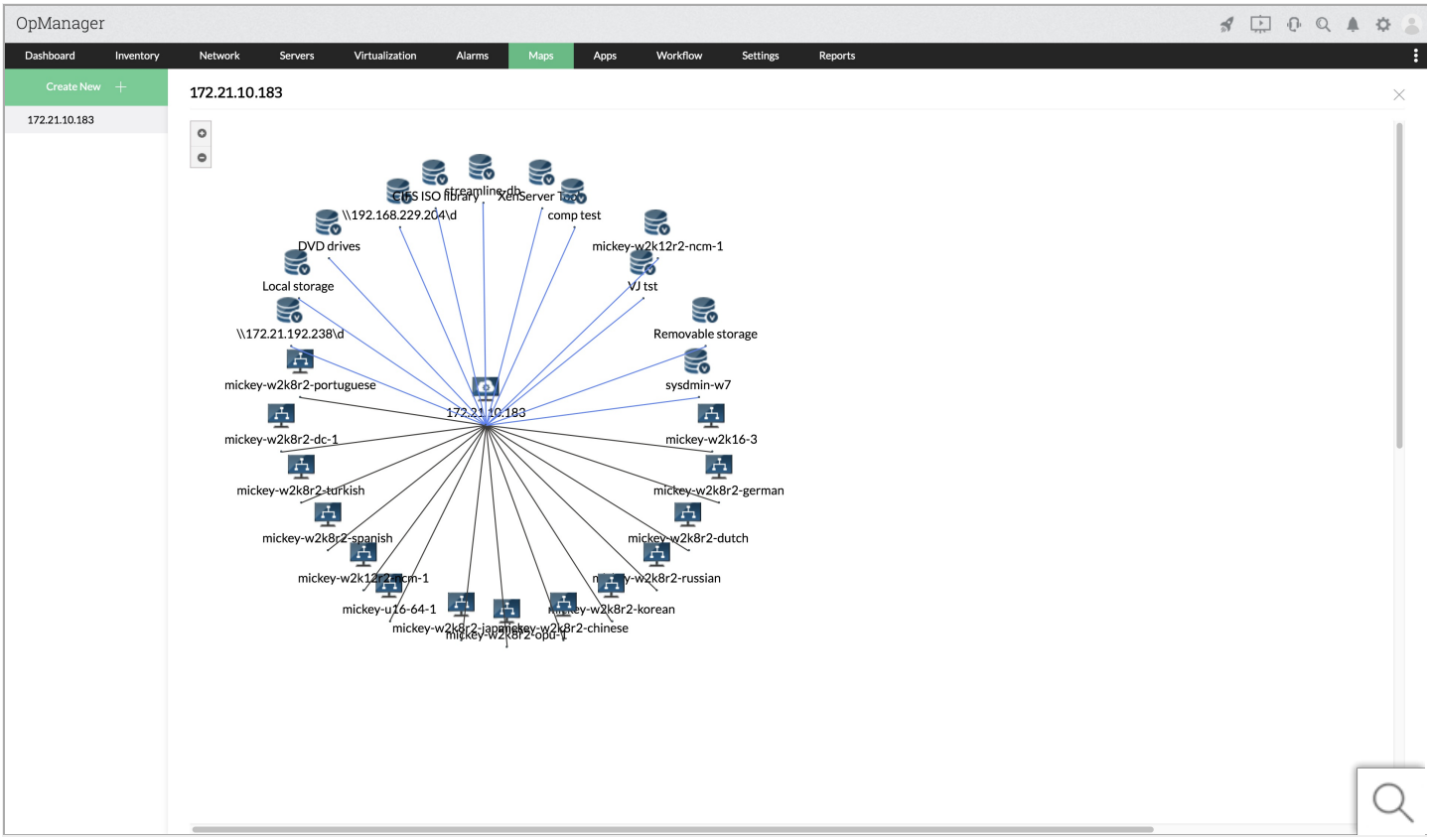
Hyper-V Maps:

To view the dependency map of your Hyper-V devices, go to the Hyper-V tab under Maps. You can see the Hyper-V hosts with info such as number of VMs, CPU and memory info. To view the visual representation of the mapping, click on any of the hosts to open up its map.



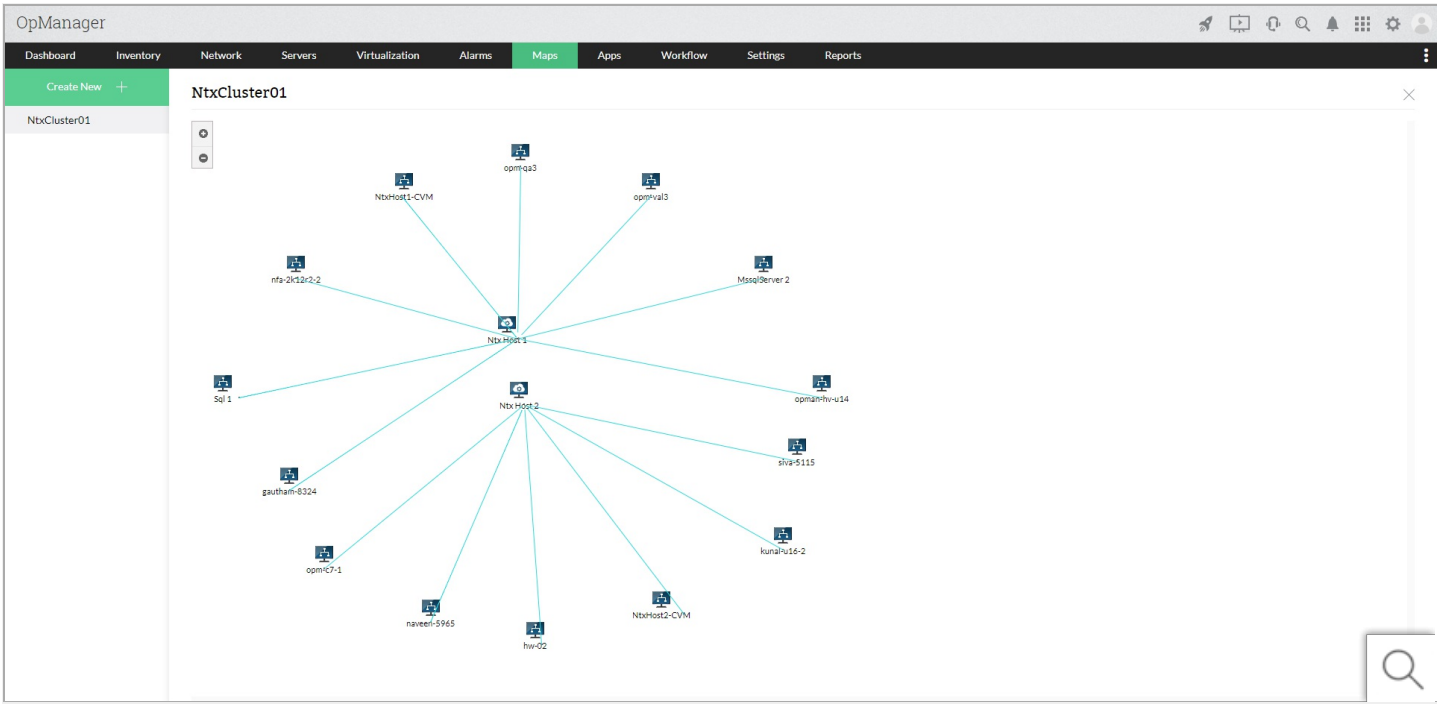
Xen Maps:

OpManager automatically provides a map of your Xen hypervisor, guest and host machines, once they have been discovered. The list of Xen pools available can be viewed under Xen section in Maps section, along with general info about it such as number of hosts and VMs, total memory and number of CPU cores in use in that pool. Clicking on any of the listed IP addresses takes you to the map of that specific Xen pool, where the dependency between the master, the hosts and the VMs are displayed.



Nutanix maps:

On opening the Nutanix tab under Maps section, the list of clusters available are displayed along with their total hosts and VMs. To view the dependency under any of the clusters, click on it and the related hosts and VMs will be displayed in the Map view.



Cisco UCS Monitoring:

OpManager monitors Cisco UCS System using XML SOAP protocol. Cisco's Unified Computing System integrates computing, networking, virtualization and other datacenter components for cost effective and efficient datacenter management.

> **Note:** Cisco UCS Manager is a prerequisite for monitoring UCS systems in OpManager.

UCS Discovery:

UCS discovery in OpManager is similar to the discovery of other devices.

1. Go to **Settings** -> **Discovery Module**
2. Select the option **Add UCS**
3. Input the **Device Name/IP Address**
4. Select the **Add UCS Manager Credential** to input credential details.
5. Configure credentials by providing the appropriate Profile Name, User Name, Password, Port Number, Time Out and Protocol details.

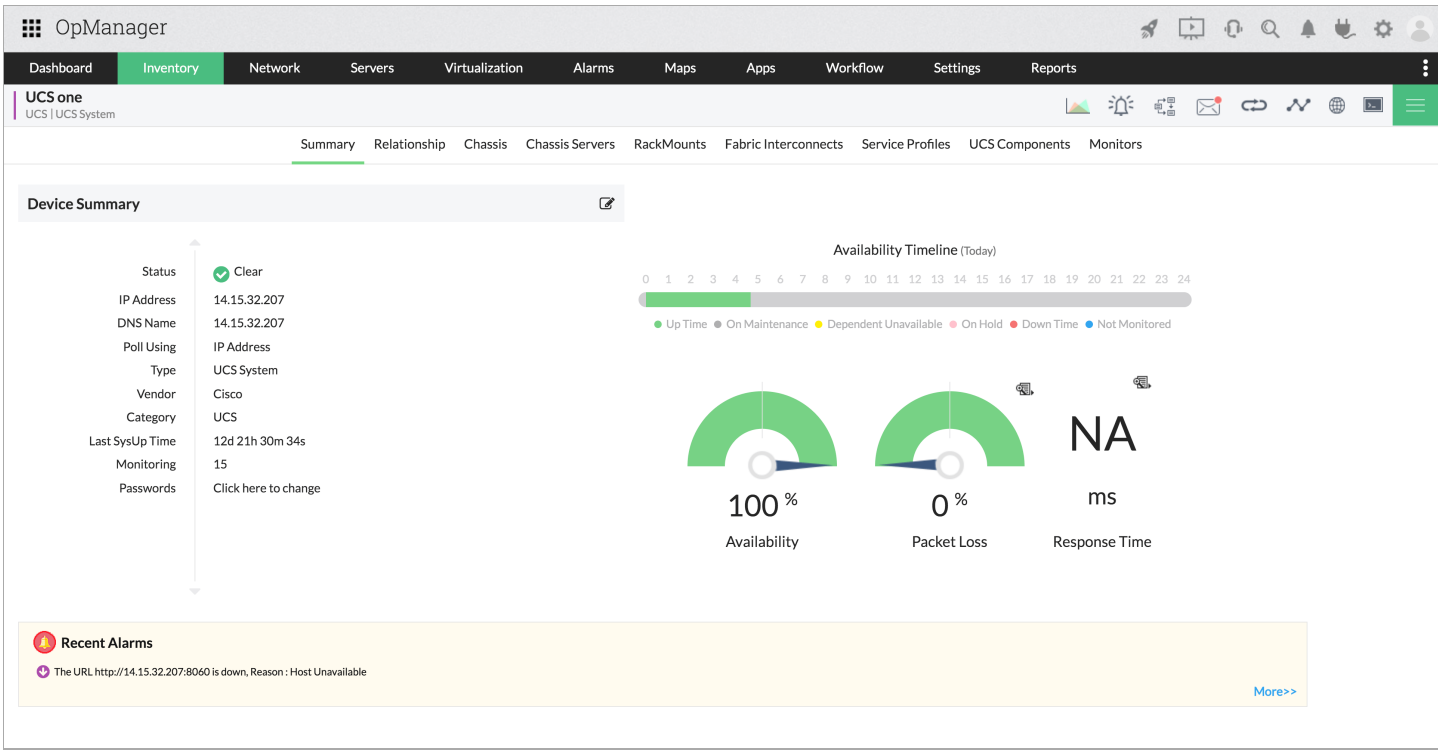
Once the device is discovered, it is listed under OpManager's inventory.

Monitoring:

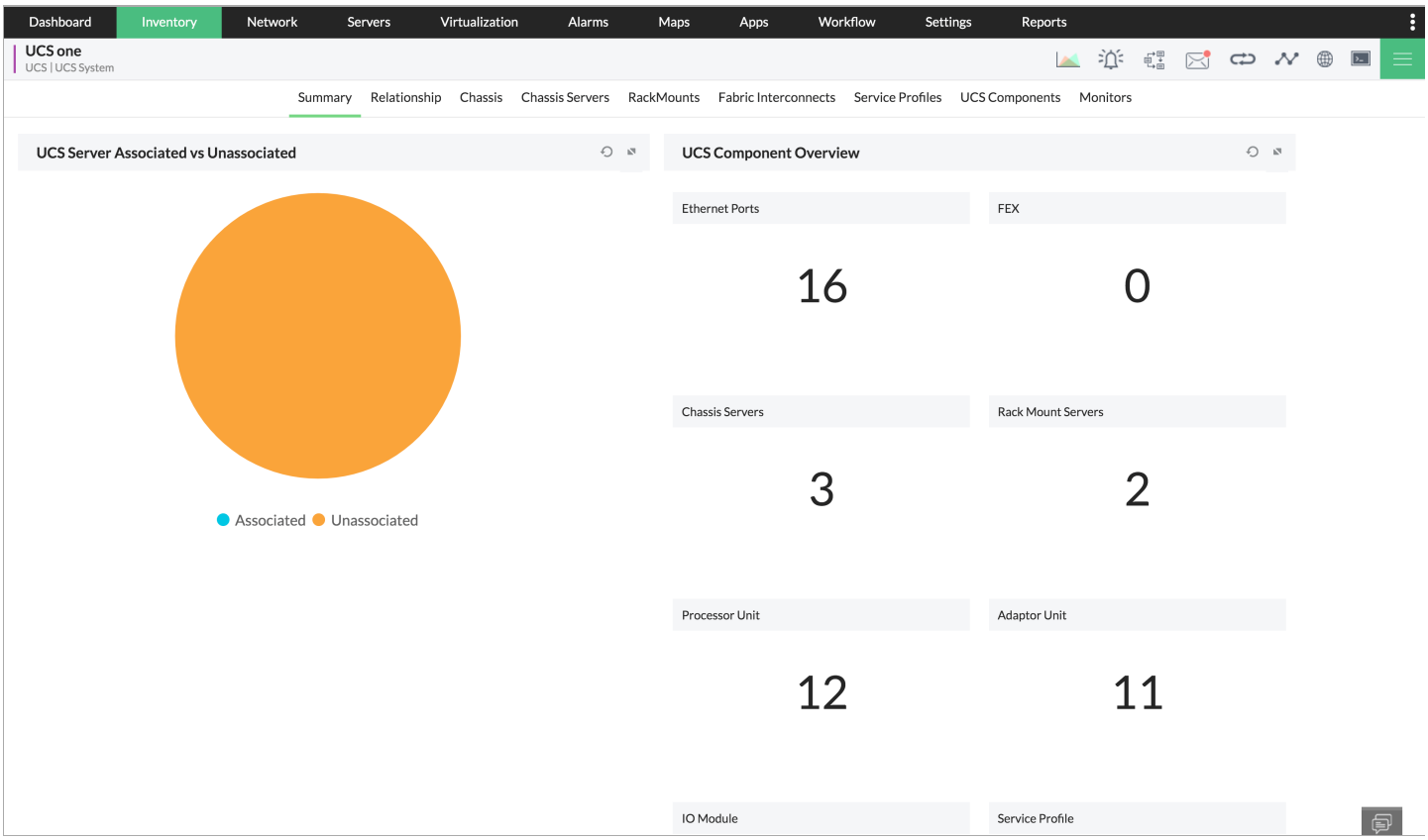
OpManager's cisco monitoring feature helps you monitor the status and availability of UCS devices. Detailed information like UCS components, their relationship charts, Chassis information etc., is also monitored by OpManager.

UCS Snapshot Page:

The Snapshot page provides details like IP Address, Monitoring Intervals, Passwords, Status and Response Times of the Device



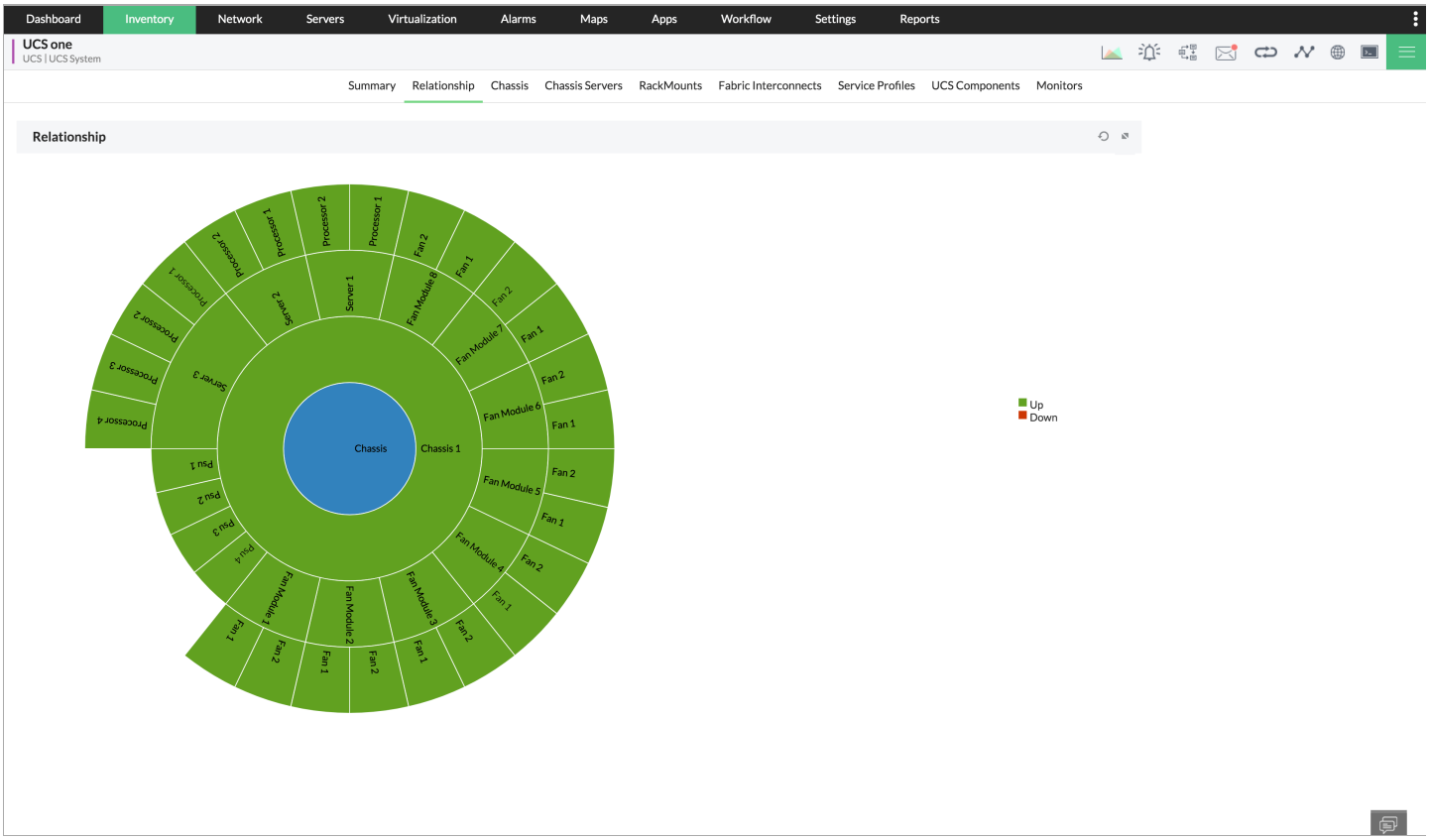
OpManager also provides the status of service profiles associated with UCS servers and an overview of UCS components that includes Chassis, Chassis servers, rack mount servers, FEX, ethernet ports etc. These can be viewed in the UCS Snapshot page.



Chassis Information:

OpManager provides a graphical representation of Chassis components that includes Servers, Fan Modules, Power Supply Units, IO

Modules etc. This can also be viewed under the snapshot page of the UCS device in OpManager.



Apart from this, OpManager also provides information on the number of chassis, and detailed data on the chassis servers like cores, memory, NICs, operability, Power and association State.

Rack Mounts:

Rack mounts are frames where the servers are enclosed. Several servers can be mounted on the rack as per requirement.

OpManager monitors

- Cores
- Adaptors
- NICs
- Operability
- Associated State

Fabric Interconnectors:

These are a part of UCS devices that acts as a switch, and helps in connecting servers to networks or storage networks.

OpManager monitors

- Fans
- Power Supply Units

- IO Modules

Other UCS Components:

OpManager also monitors and provides detailed information on the other UCS device components such as,

1. Fan Modules
2. Ethernet Ports
3. IO Modules
4. FEX
5. Adaptor Unit
6. Processor Unit

Performance Monitors:

Whenever OpManager discovers UCS devices, UCS performance monitors are automatically associated with it. Thresholds can be set to receive alarms, when breached.

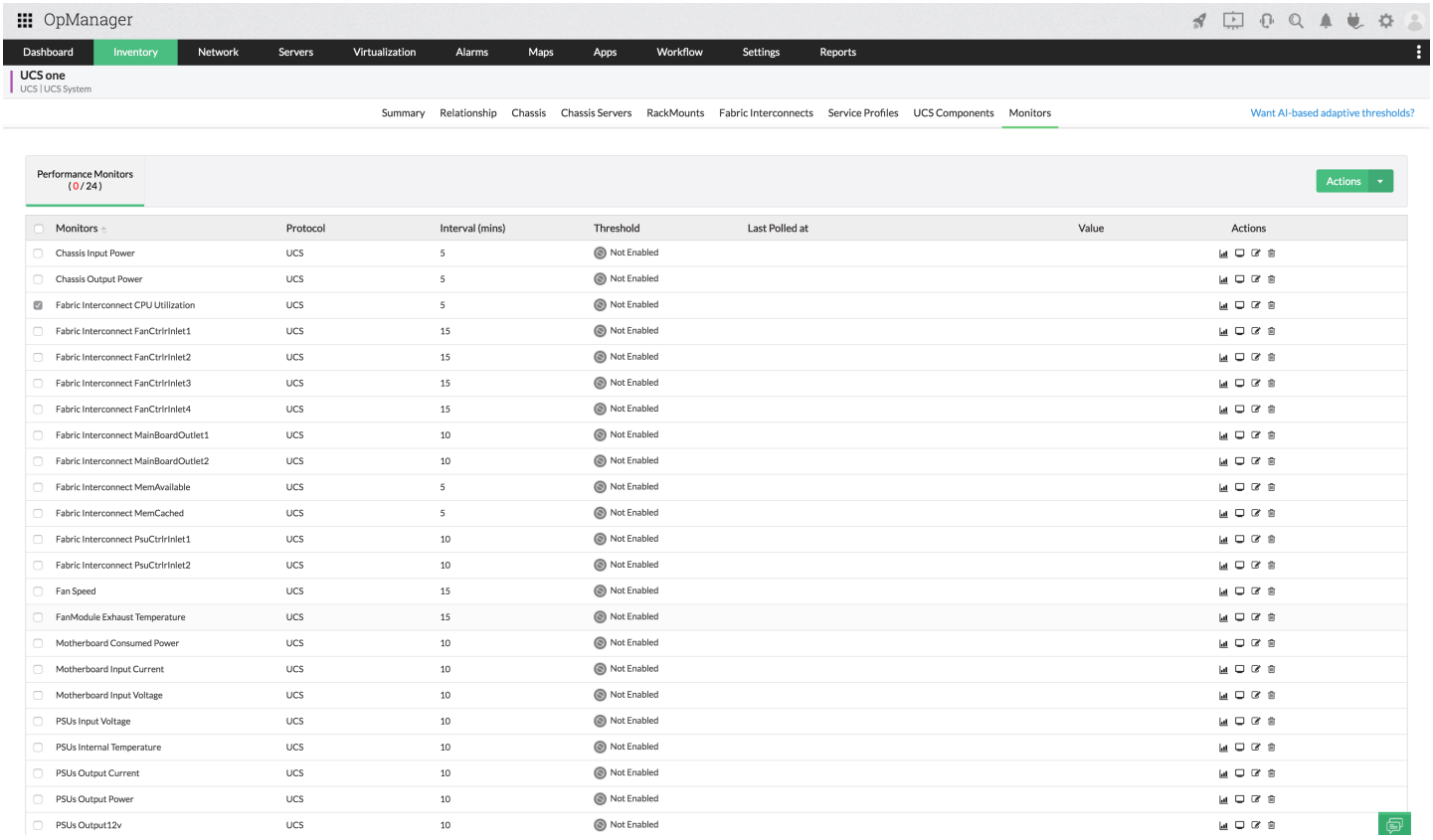
&#65533; To set thresholds for a performance monitor,

1. Navigate to&#65533; **Inventory** ->&#65533; **Category** ->&#65533; **UCS** and go to the Snapshot Page of the device.
2. Go to **Monitors**. Performance monitors would already have been added to the device.
3. Select the monitor that you wish to edit.
4. Configure&#65533; Monitoring Interval,&#65533; Units,&#65533; Threshold Details and click on&#65533; Save.

&#65533;

OpManager sends alarms if the threshold levels are breached.

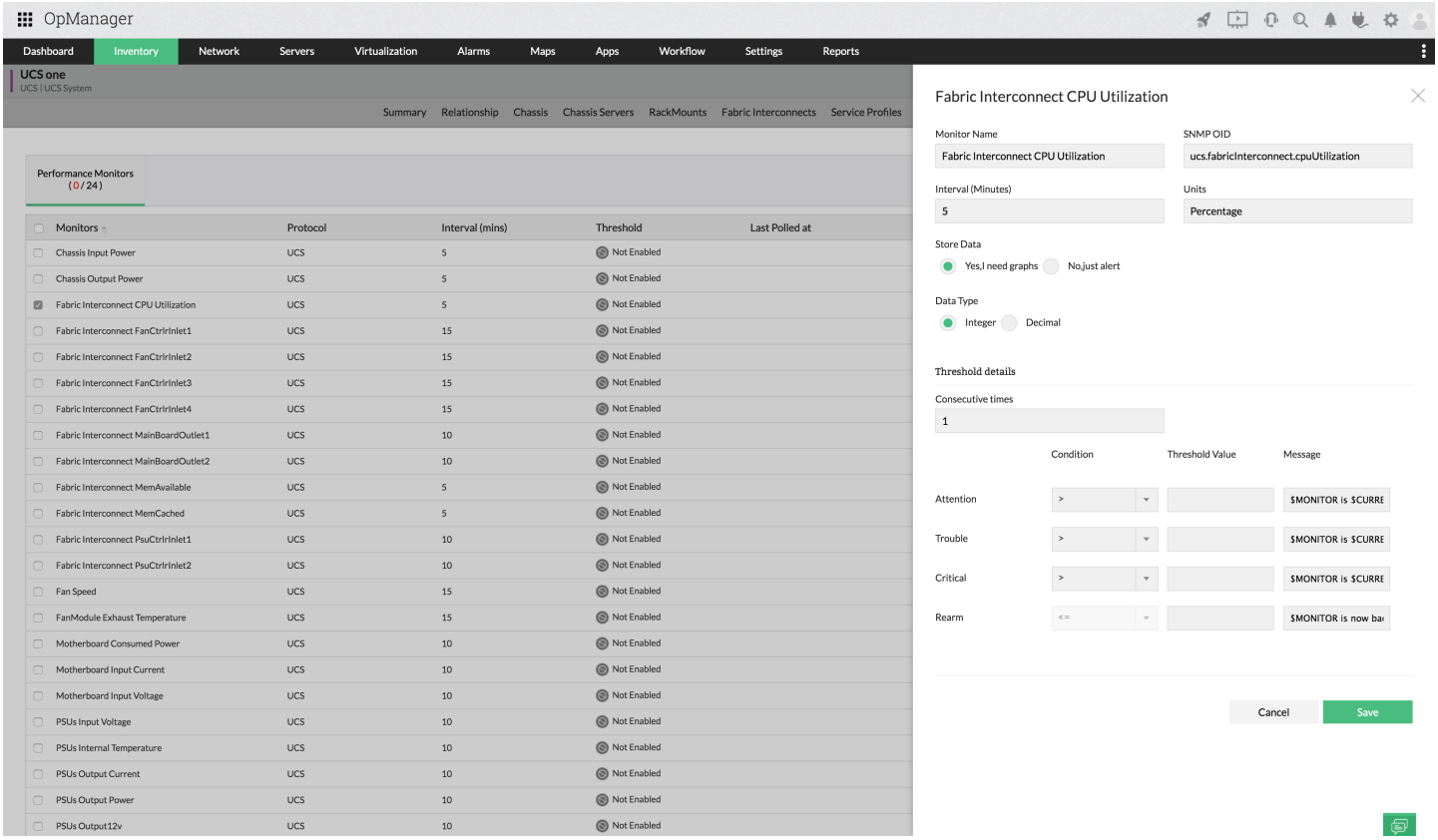
&#65533;

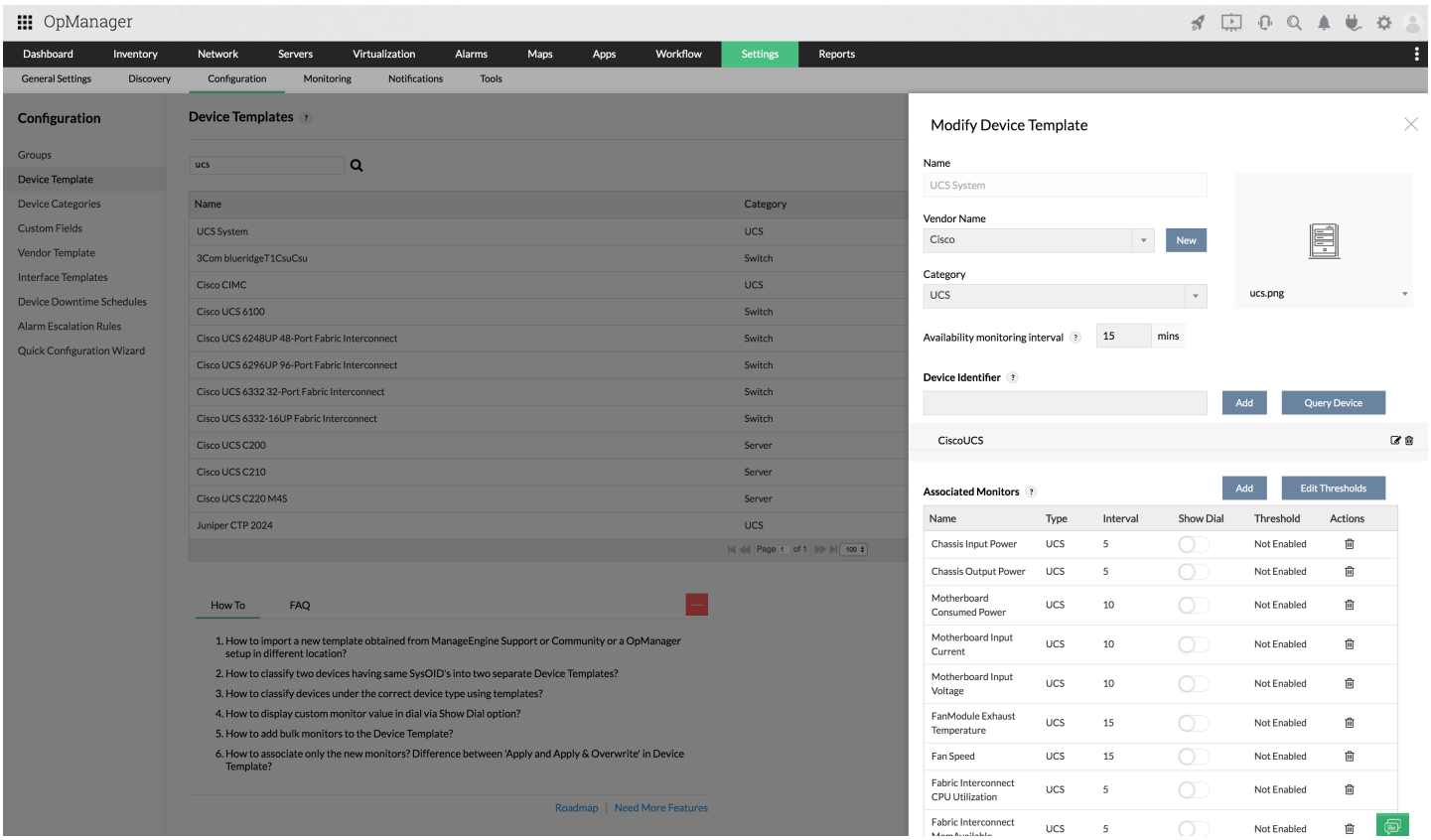


&#65533;

&#65533;

&#65533;





To add performance monitors for more than one UCS device,

1. Navigate to **Settings** -> **Monitoring** -> **Device Templates**
2. Locate **UCS** device template
3. Input the **Device Identifier** (sysOID), query the device and add them
4. Add the required monitor and configure threshold details.

What is Deep Packet Inspection?

Deep Packet Inspection (DPI) is a process to know what is been received and transmitted by a network device. It is the most accurate technique to monitor and analyze the application problems and regulate traffic in best suitable way. With DPI's packet level analysis, it is easy to make decisions on capacity planning and achieve better network performance and management. DPI helps determine the root cause for performance related issues with the complete traffic picture (both network and application) in a single view.

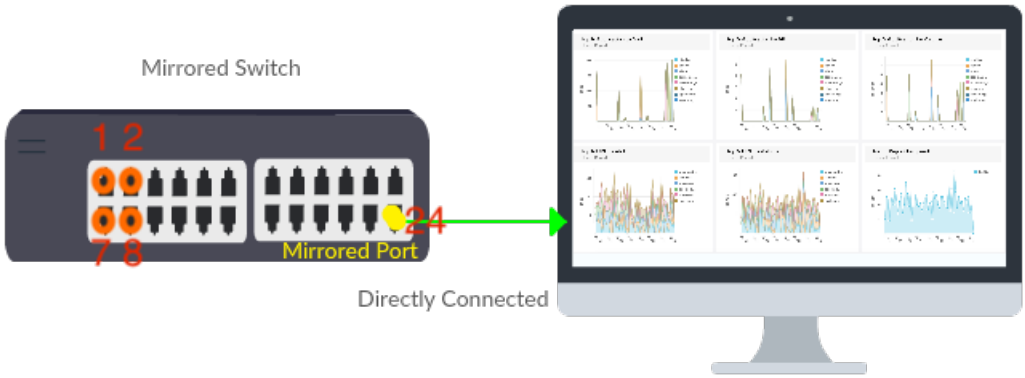
OpManager's Deep Packet Inspection allows you to capture network packets and analyzes packet capture (PCAP) files. The DPI capabilities rely on packet-level analysis to determine whether the network or an application is at fault and react quickly to the issues before they impact users. It gives clear visibility to network administrators about the volumes, application and network performances of application traffic for their enterprise network and helps them to diagnose application performance problems with response time details and drill even further to the root cause of performance degradation issues.

With DPI you can:

- Pinpoint whether the delay is on the network side or application side comparing NRT vs. ART
- Pull the list of affected users for slow apps and communicate them in advance
- Increase application availability and meet SLAs
- Know who is using your bandwidth and regulate them using traffic shaping
- Pull reports on historic data and perform forensics

Understanding DPI in OpManager

Traffic packets passing through the network device, can be mirrored to a port of the same device for inspection. Also multiple (WAN/LAN /Uplink) port traffic can be mirrored and set for inspection. In case you wish to inspect packets from multiple devices, You can save the mirrored packets and upload it to NetFlow Analyzer server. Real time packet capture works only when NetFlow Analyzer server is directly connected to the mirrored port.



In the above diagram, ports 1, 2, 7 & 8 are mirrored for monitoring to the last port (port 24) of device . Here all the mirrored network packets reaches the OpManager server as it is directly connected.

Note : If you want to monitor multiple devices, You need to save the mirrored packets individually and import it to opmanager to generate offline reports.

Port mirroring commands vary from vendor to vendor. You can check with the respective device vendor for commands.

Below is an example for port mirroring on a HP Switch.

```
HPSwitch# configure terminal
HPSwitch(config)# mirror 1 port a24
HPSwitch(config)# int a1-a4
HPSwitch(eth-A1-A4)# monitor all both mirror 1
HPSwitch(eth-A1-A4)#
```

Below is the detailed cmd structure to mirror all the 23 ports to the last 24th port.

```
HPSwitch(config)# sh monitor 1
Network Monitoring

   Session: 1    Session Name:
      Mirror Destination:  A24   (Port)

      Monitoring Sources  Direction Truncation Mirror Policy
      ------------------  --------- ---------- -------------
      Port: A1            Both      No         -
      Port: A2            Both      No         -
      Port: A3            Both      No         -
      Port: A4            Both      No         -
      Port: A5            Both      No         -
      Port: A6            Both      No         -
      Port: A7            Both      No         -
      Port: A8            Both      No         -
      Port: A9            Both      No         -
      Port: A10           Both      No         -
      Port: A11           Both      No         -
      Port: A12           Both      No         -
      Port: A13           Both      No         -
      Port: A14           Both      No         -
      Port: A15           Both      No         -
      Port: A16           Both      No         -
      Port: A17           Both      No         -
      Port: A18           Both      No         -
      Port: A19           Both      No         -
      Port: A20           Both      No         -
      Port: A21           Both      No         -
      Port: A22           Both      No         -
      Port: A23           Both      No         -

HPSwitch(config)#
```

With these recieved network packets ManageEngine will analyze the captured packets and generate reports.

TCP analysis

As Initial phase, ManageEngine has introduced analysis for TCP packets even though it captures all packets. Rest will be supported in future. Using the DPI feature, we can calculate Application Response Time (ART), Network Response Time (NRT), url's used and traffic utilization (productive\non-productive).

With these reports a network administrator can have a clear picture of what is consuming the bandwidth at what time and so, he can regulate it cost efficiently.

In DPI we get information about ART,NRT and URLs

NRT : Network Response Time is the time difference between TCP_SYN packet and its ACK (acknowledgement).

ART : Application Response Time is the time difference between TCP_DATA packet and its ACK (acknowledgement flag).

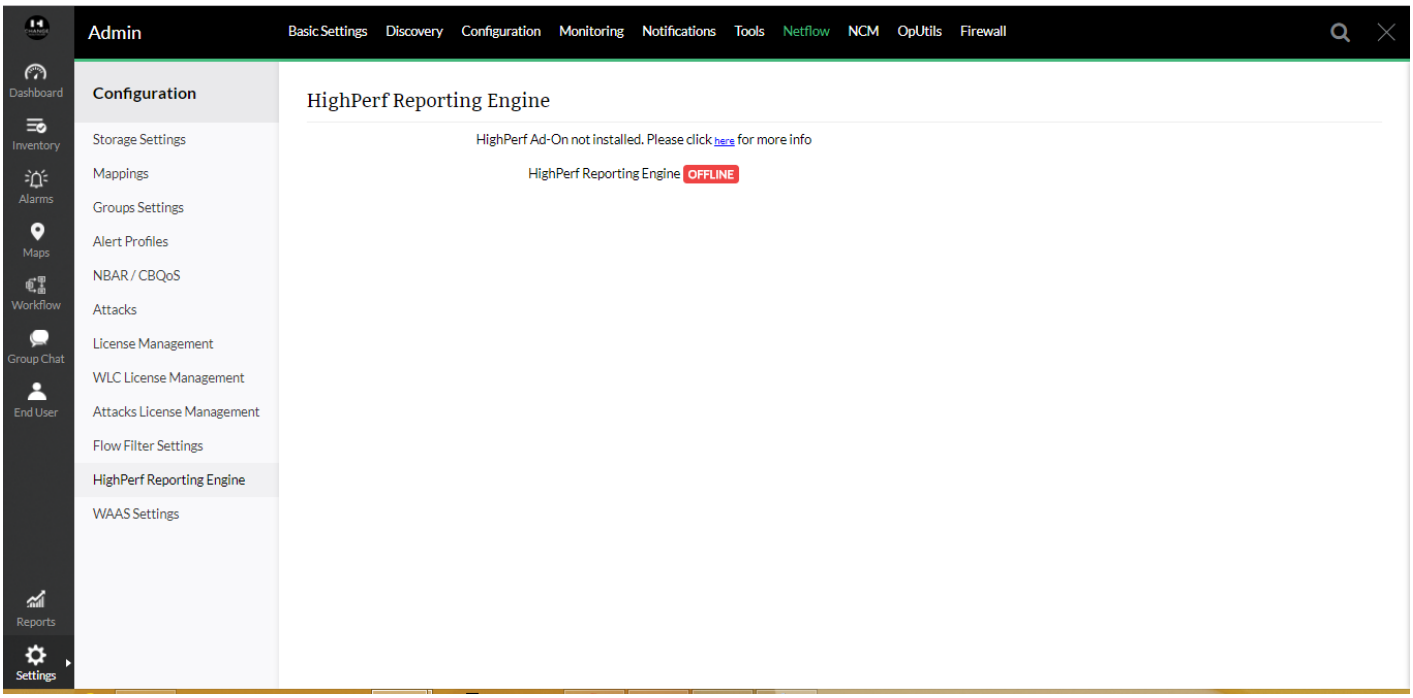
URL : URL details contained in data packets.

Configuring DPI

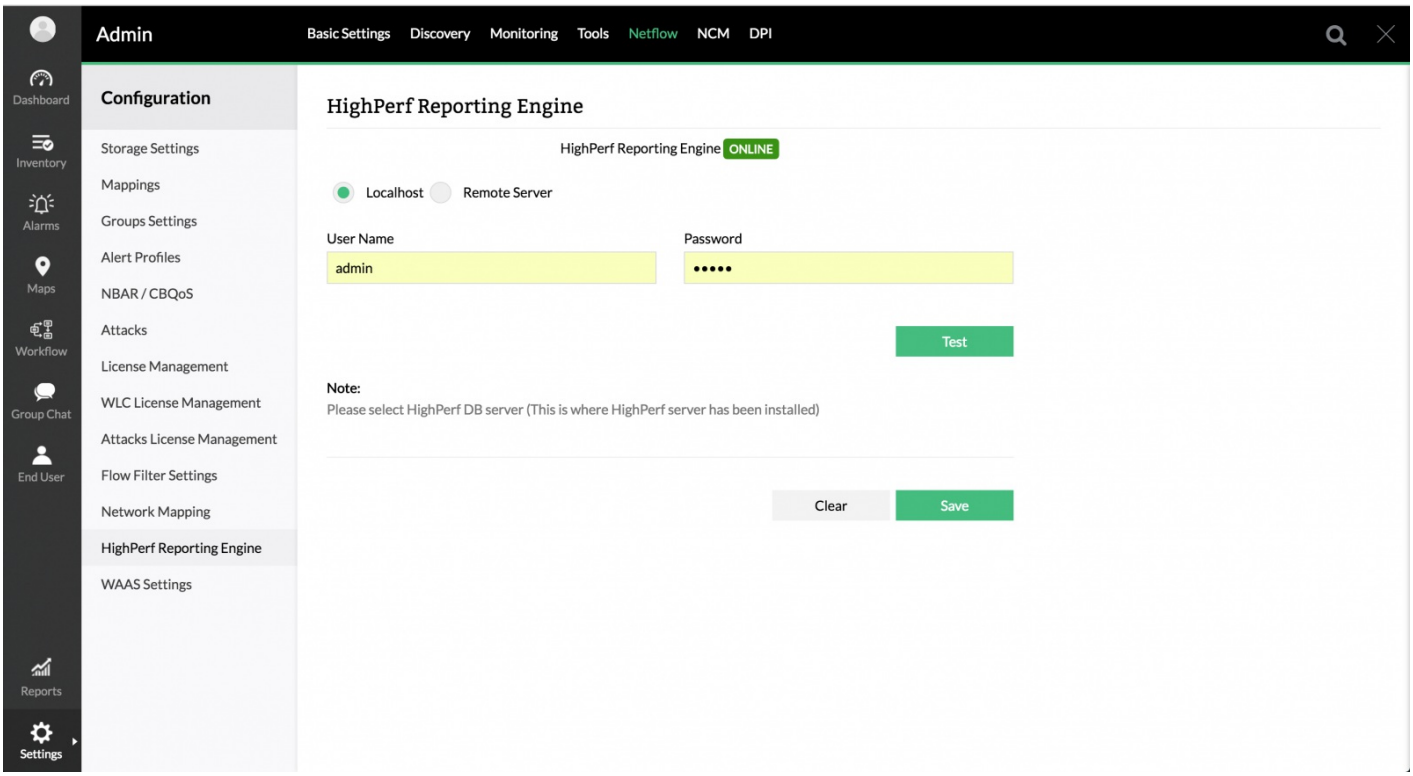
In OpManager, DPI works with winPcap and High performance reporting engine add-on. To configure DPI, follow the steps and screenshots below to enable DPI.

For Windows machine, download and install winpcap packages from the below link : https://www.winpcap.org/install/ , skip this step for Linux OS.

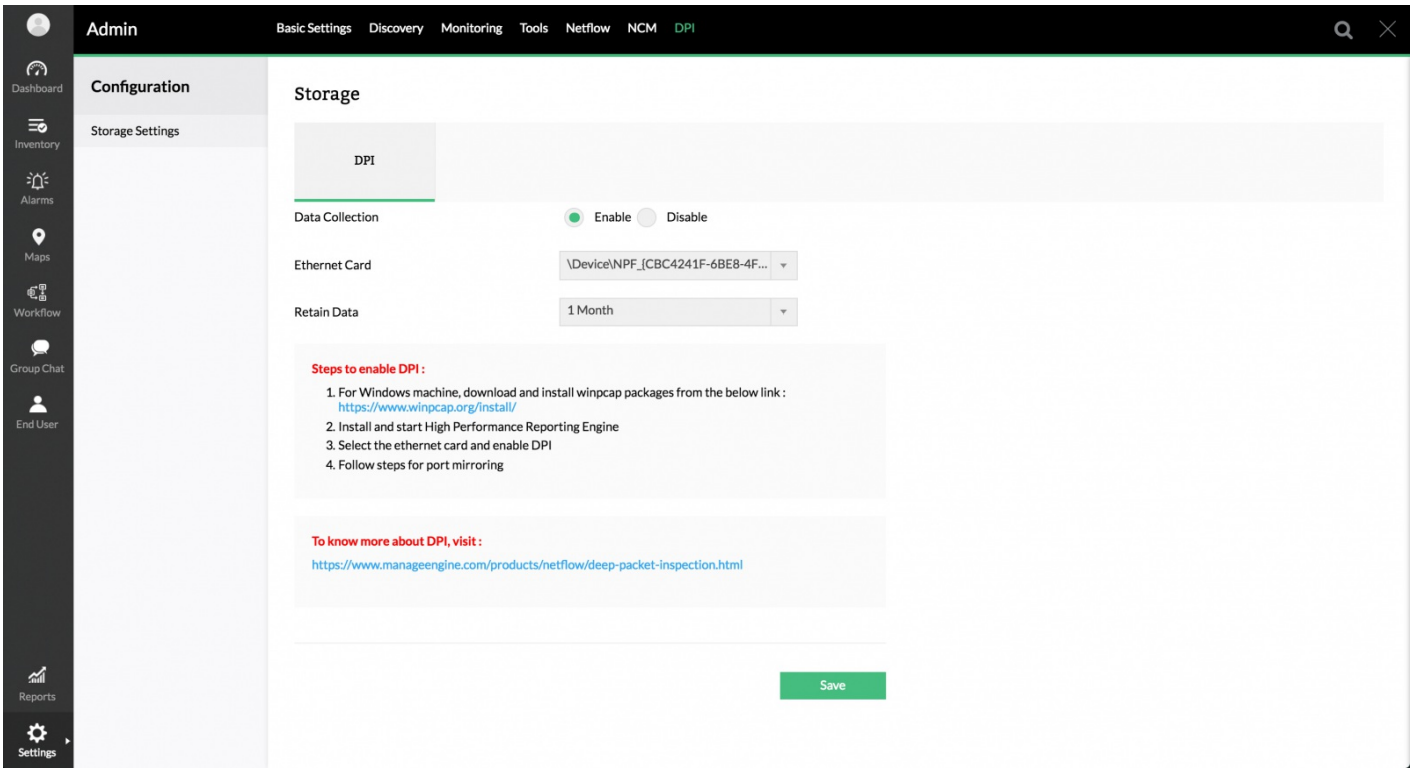
1. Download and install HighPerformance reporting engine under More downloads from the linkhttps://www.manageengine.com/products/netflow/2028821/ME_NFA_HighPerf_Add-On_64bit.exe



2. Navigate to Settings > NetFlow > HighPerf Reporting Engine, Provide installed servers login credentials, test and save.

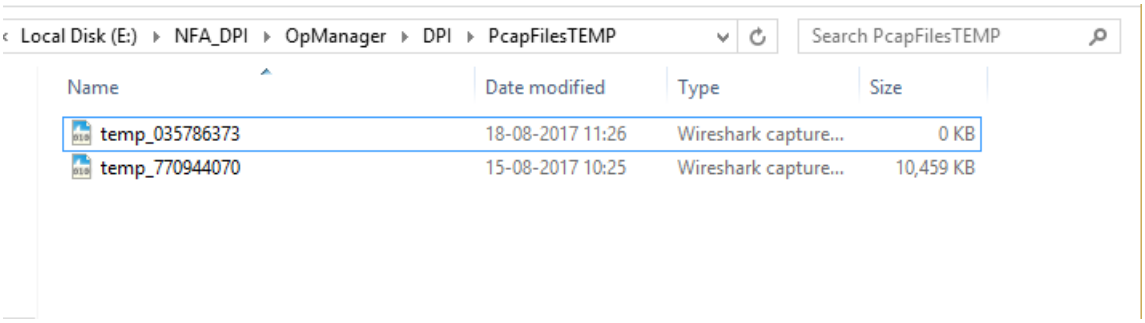


3. Navigate to Settings > DPI , Enable DataCollection, select the ethernet card , select the data retention period and save.



Note : To find the respective Network card (in windows) , open regedit, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards\ . Here you can find the respective name of network card in readable format.

4. To Verify navigate to **<Opmanager>\DPI\PcapFilesTemp**strong> and check if new file is generated.

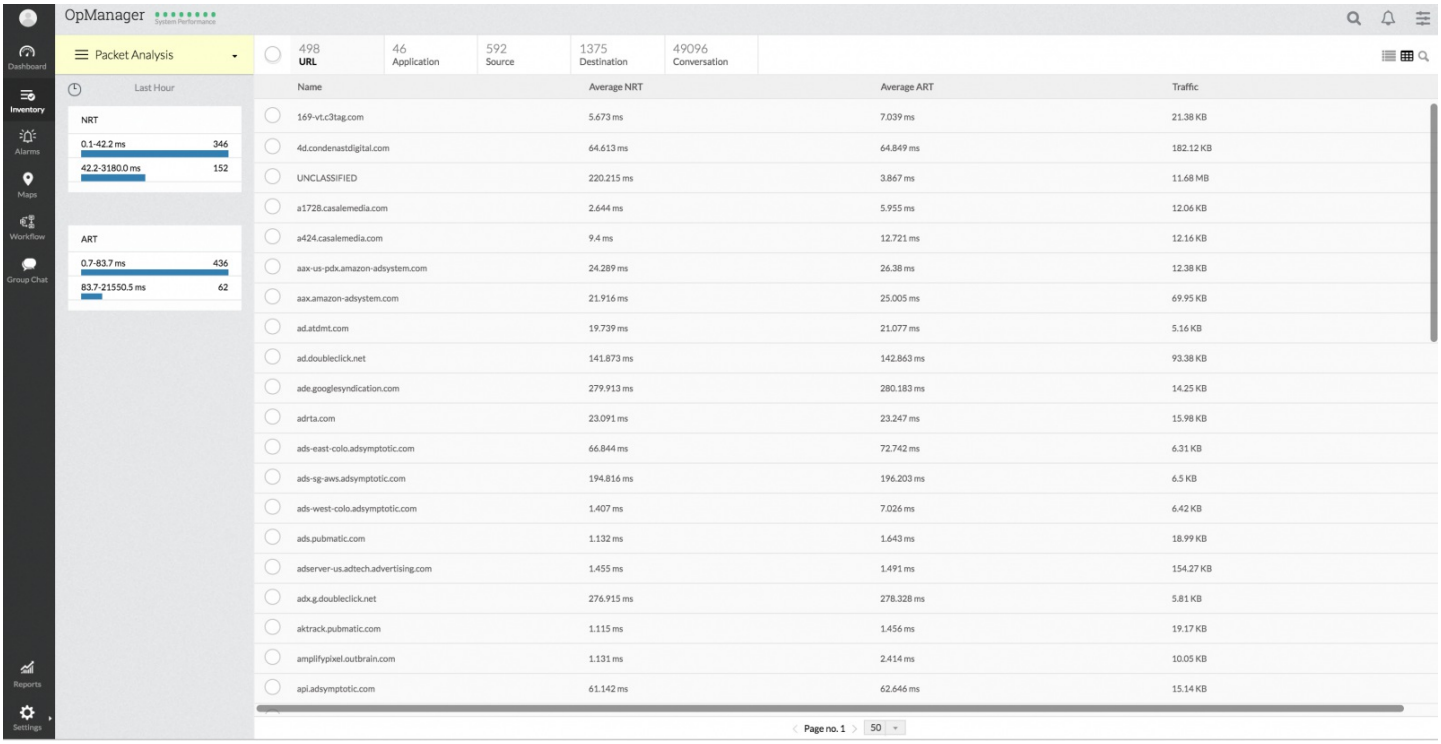


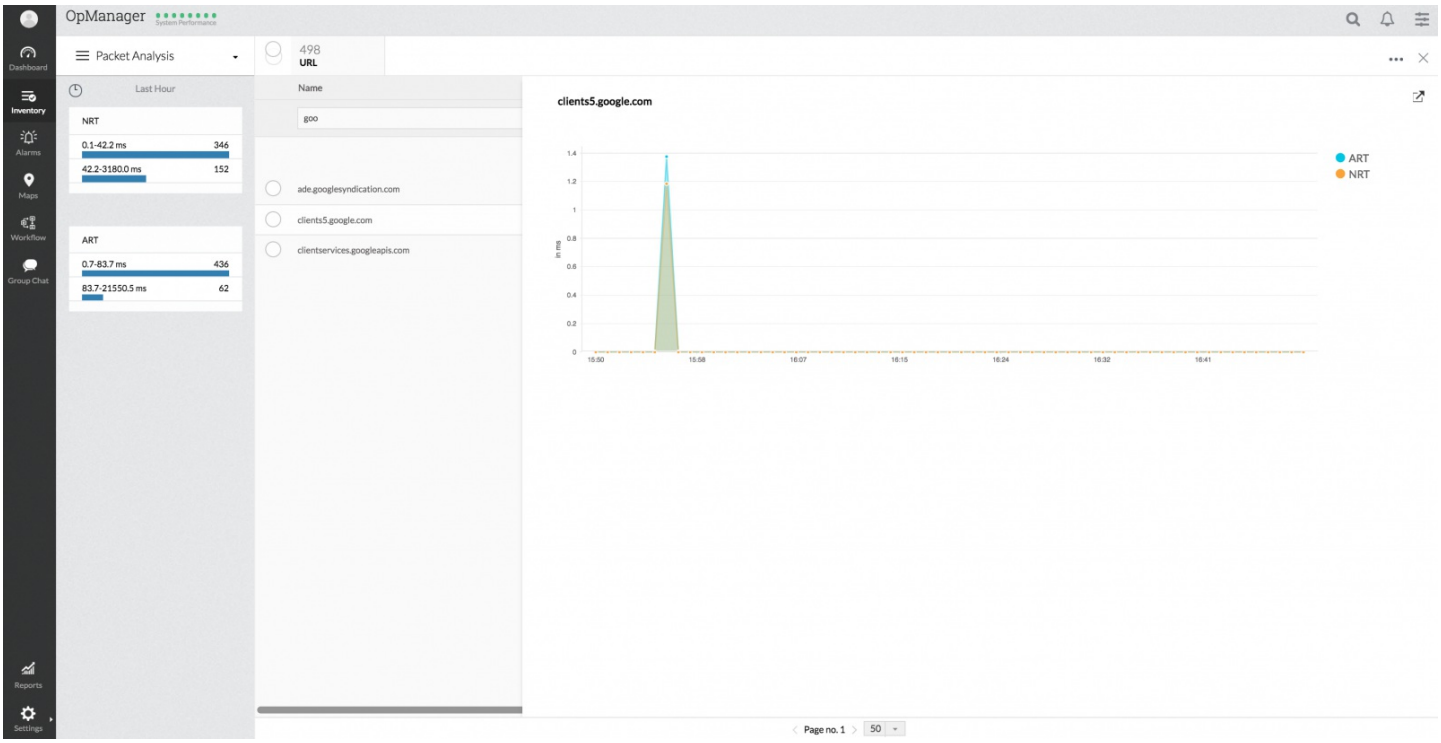
OpManager Packet Analysis

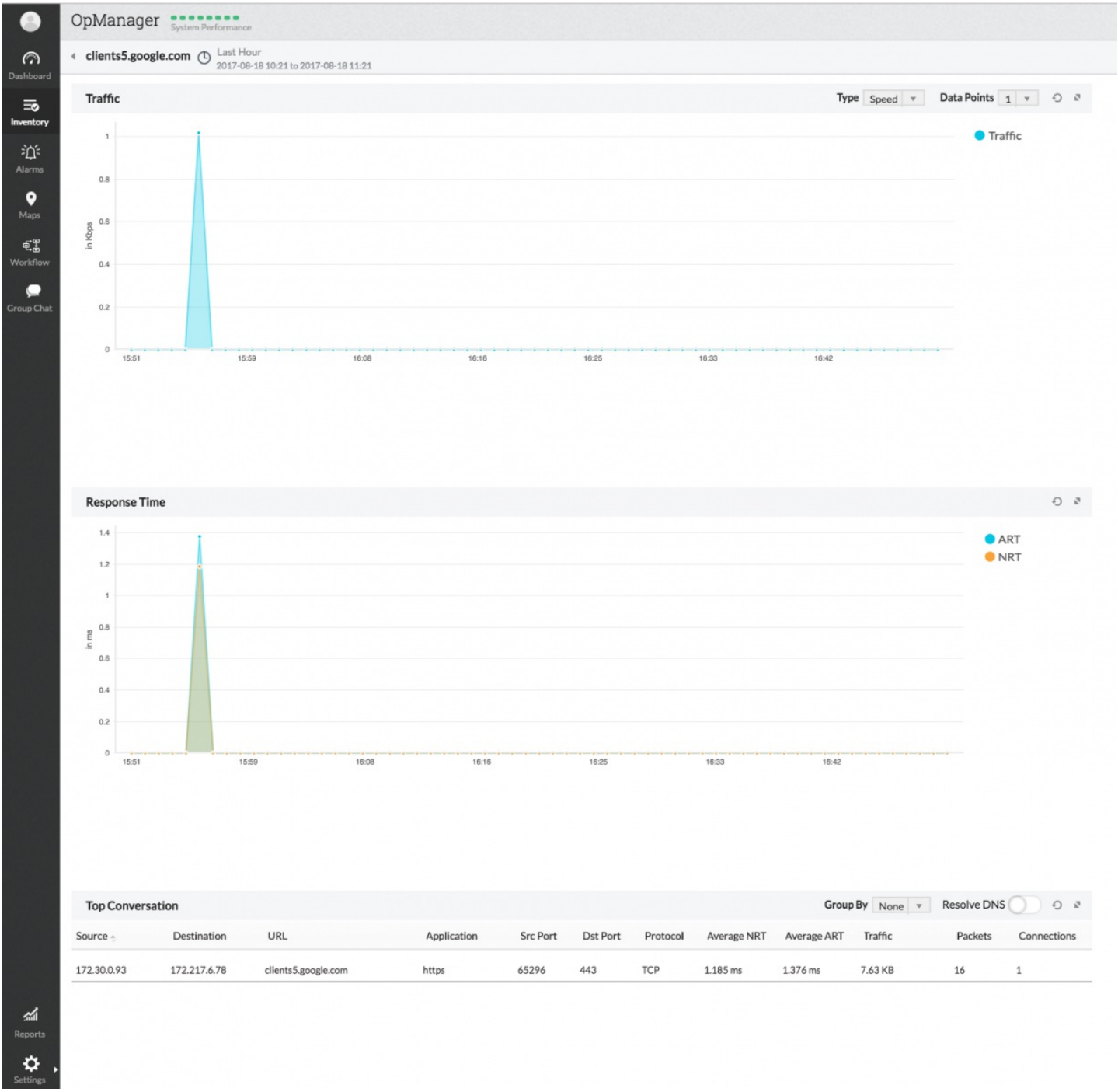
Once Packet capture is started, the high perf database stores the infomation of URL's, applications, sources, destinations and conversation. To access the information, you can navigate to Inventory > Packet Analysis. Here you can see the URL wise response time where you can drill down to any URL and see who/what caused this traffc.

Statistics can be viewed with respect to any below mentioned criteria.

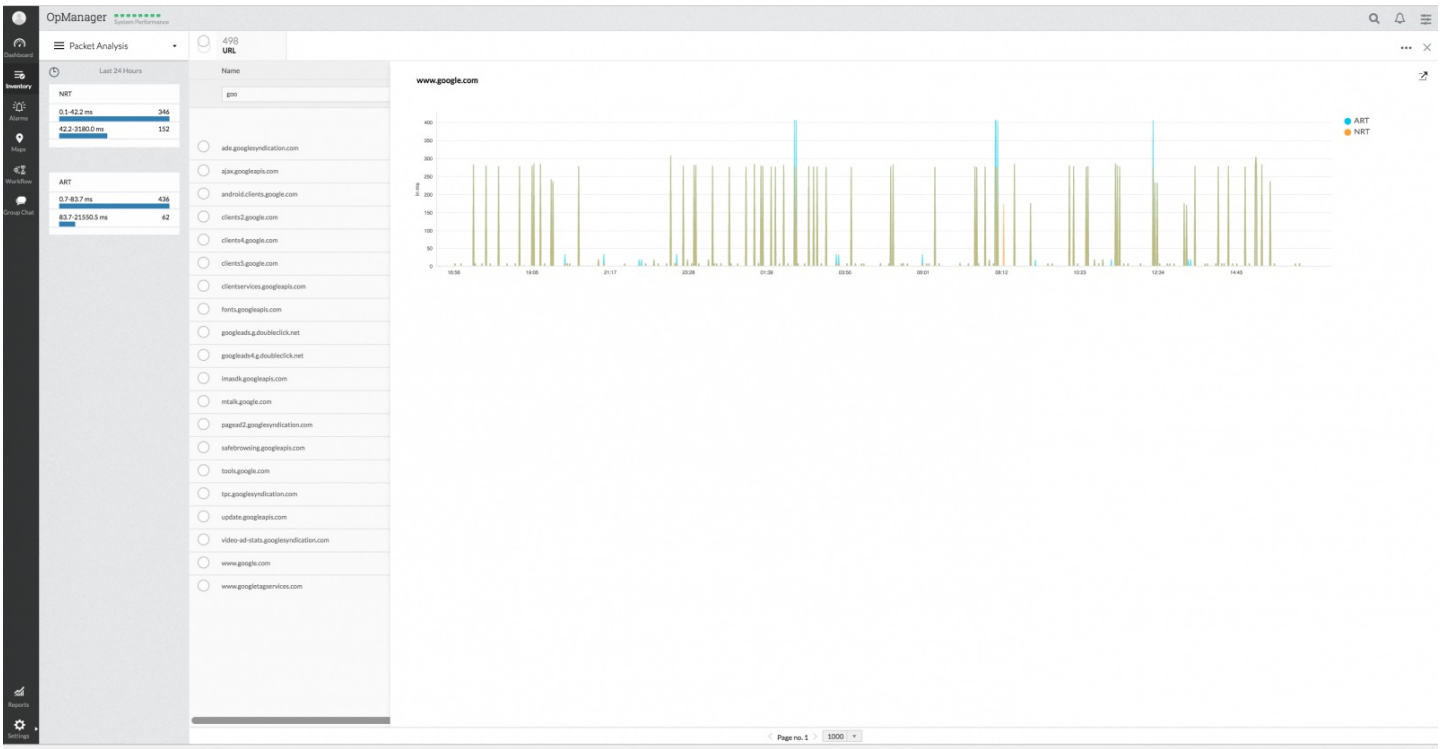
URL Drill down :

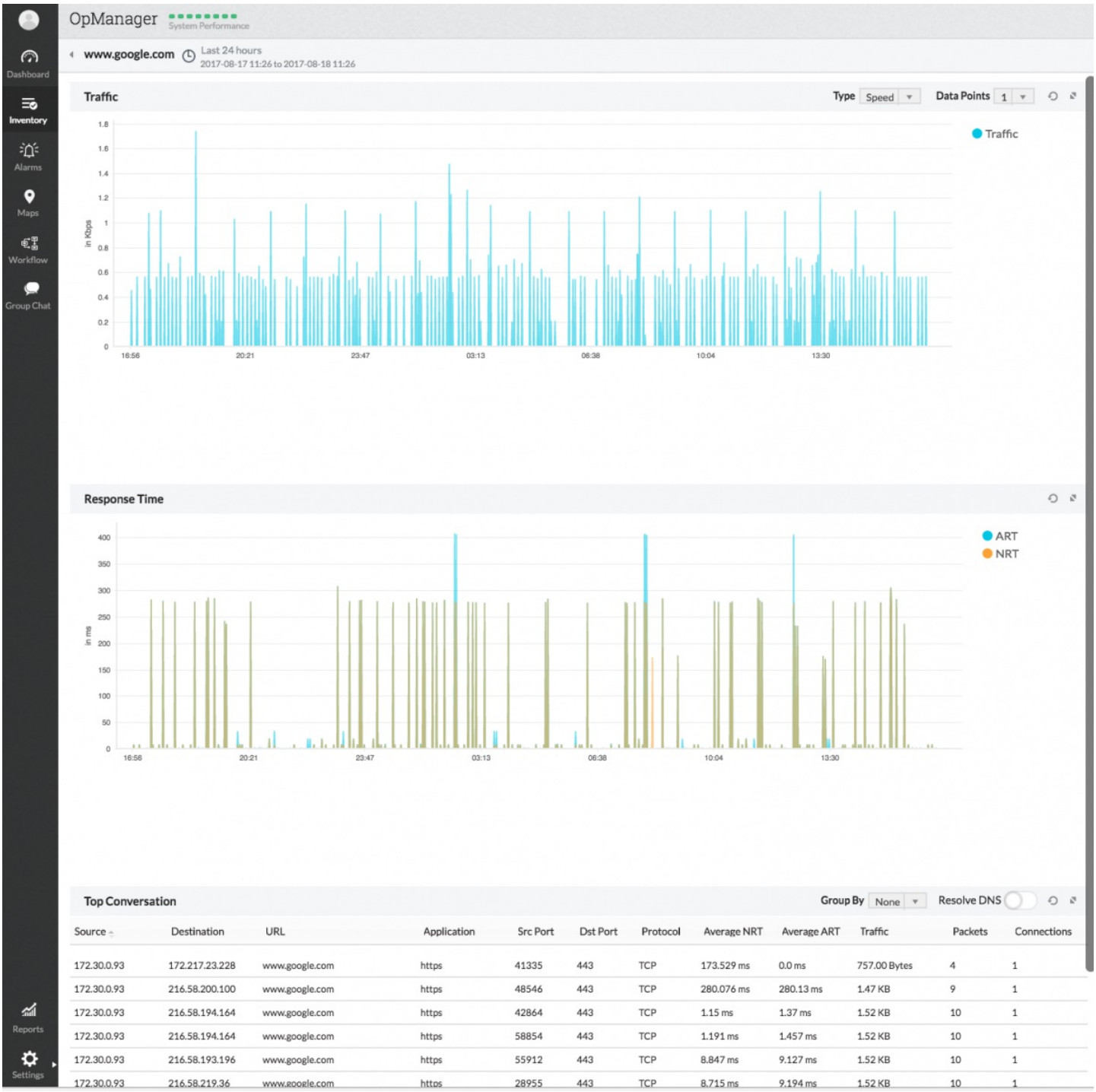




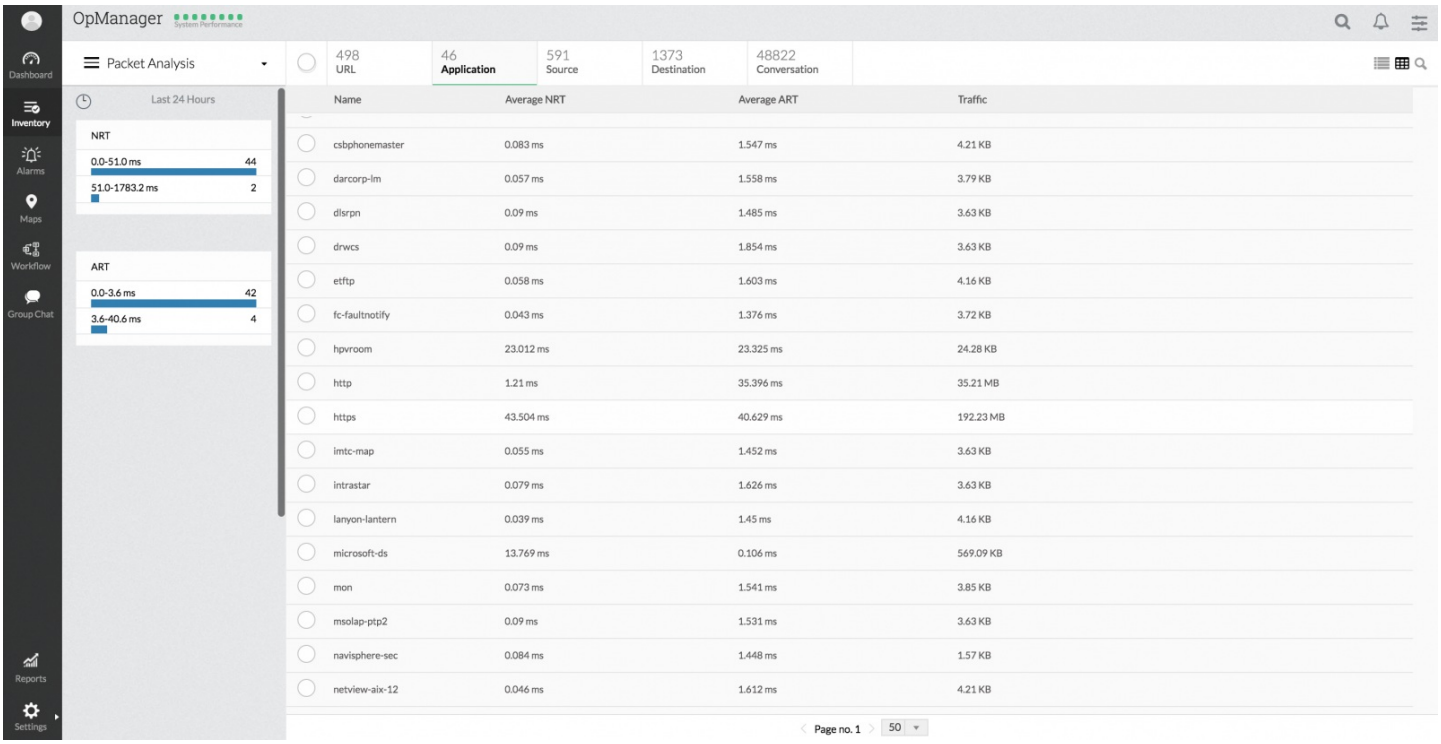


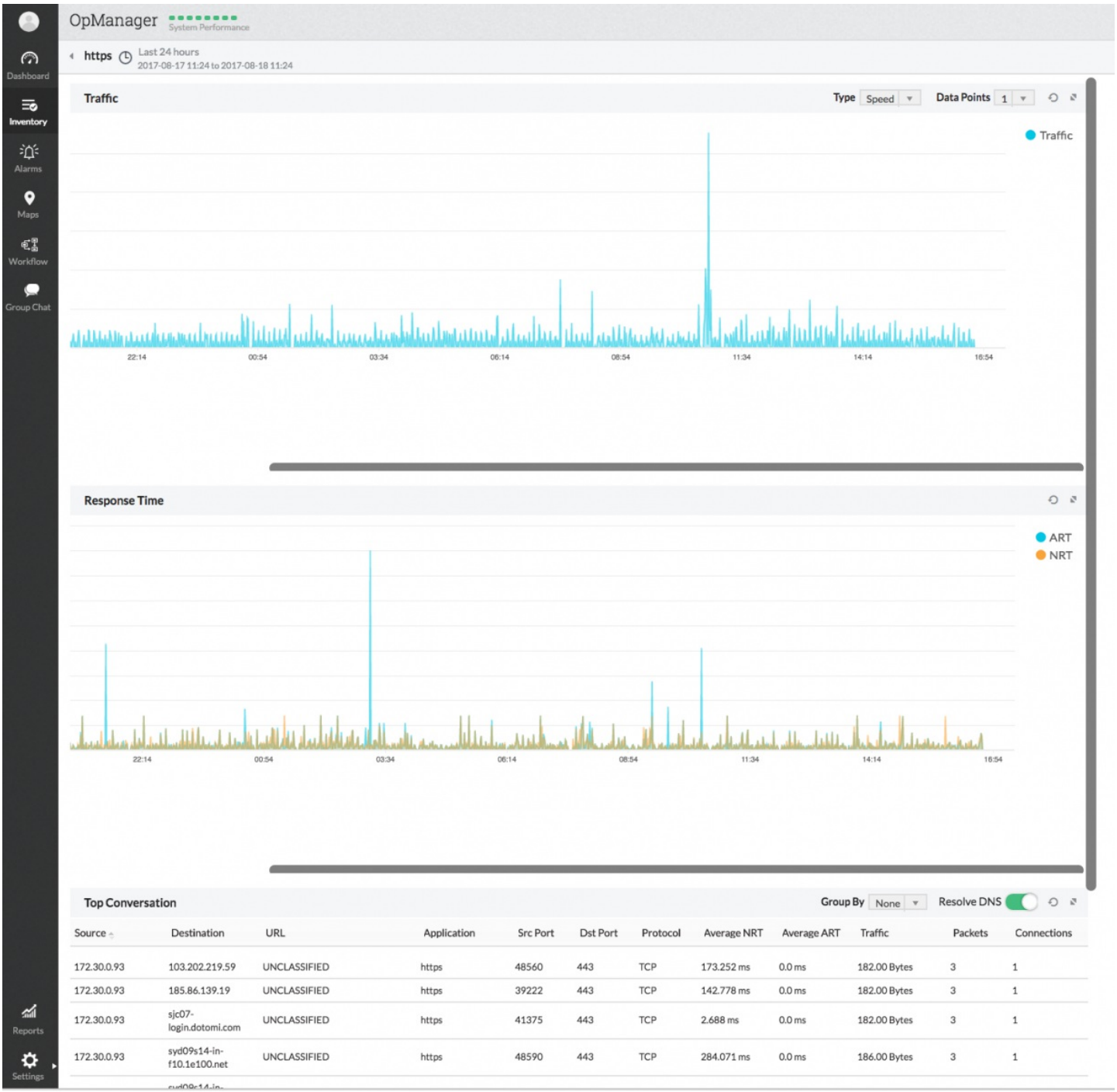
Searching a URL :


OpManager
System Performance
Dashboard
Inventory
Alarms
Maps
Workflow
Group Chat
Reports
Settings
Packet Analysis
Last 24 Hours
NRT
0.1-42.2 ms 346
42.2-3180.0 ms 152
ART
0.7-83.7 ms 436
83.7-21550.5 ms 62
498
URL
Name
goo
ade.googlesyndication.com
ajax.googleapis.com
android.clients.google.com
clients2.google.com
clients4.google.com
clients5.google.com
clientservices.googleapis.com
fonts.googleapis.com
googleads.g.doubleclick.net
googleads4.g.doubleclick.net
imasdk.googleapis.com
mtalk.google.com
pagead2.googlesyndication.com
safebrowsing.googleapis.com
tools.google.com
tpc.googlesyndication.com
update.googleapis.com
video-ad-stats.googlesyndication.com
www.google.com
www.googletagservices.com
www.google.com
ART
NRT
Page no. 1
1000



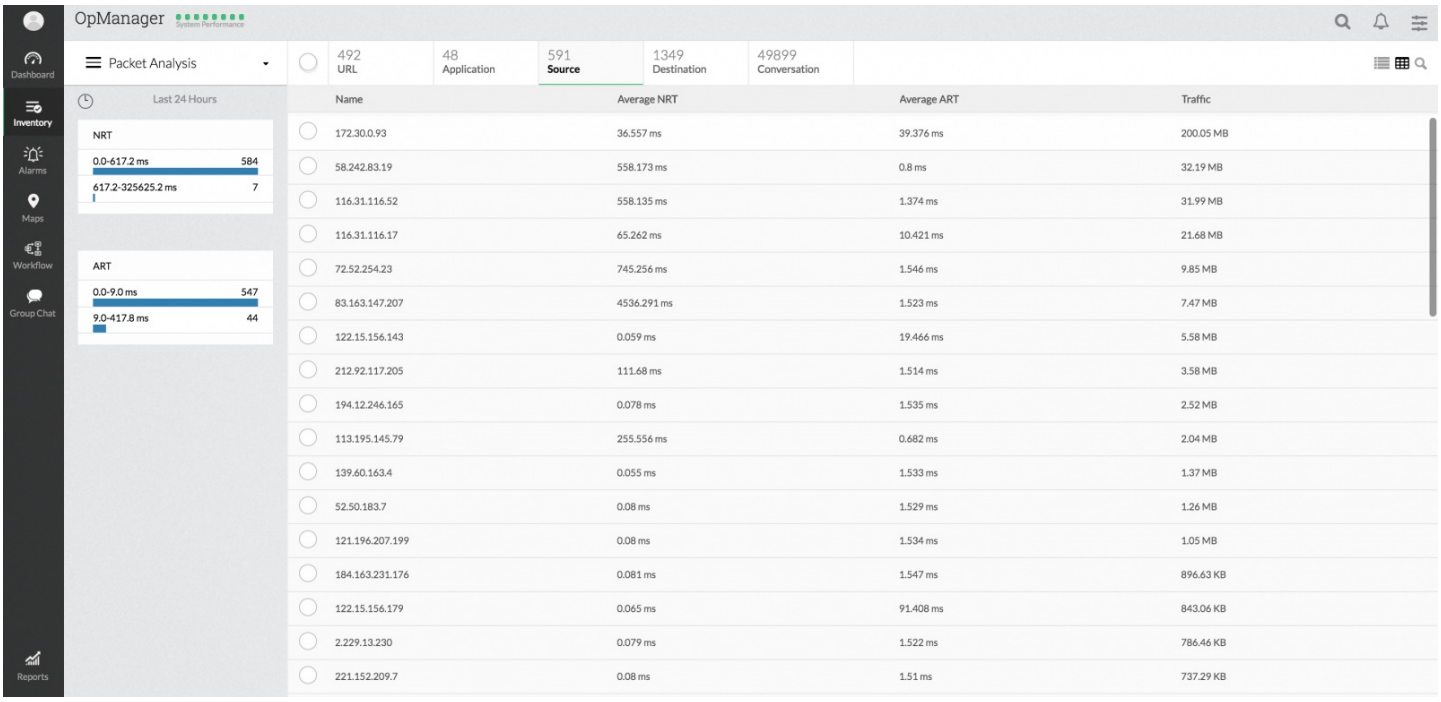
Application Drill down :

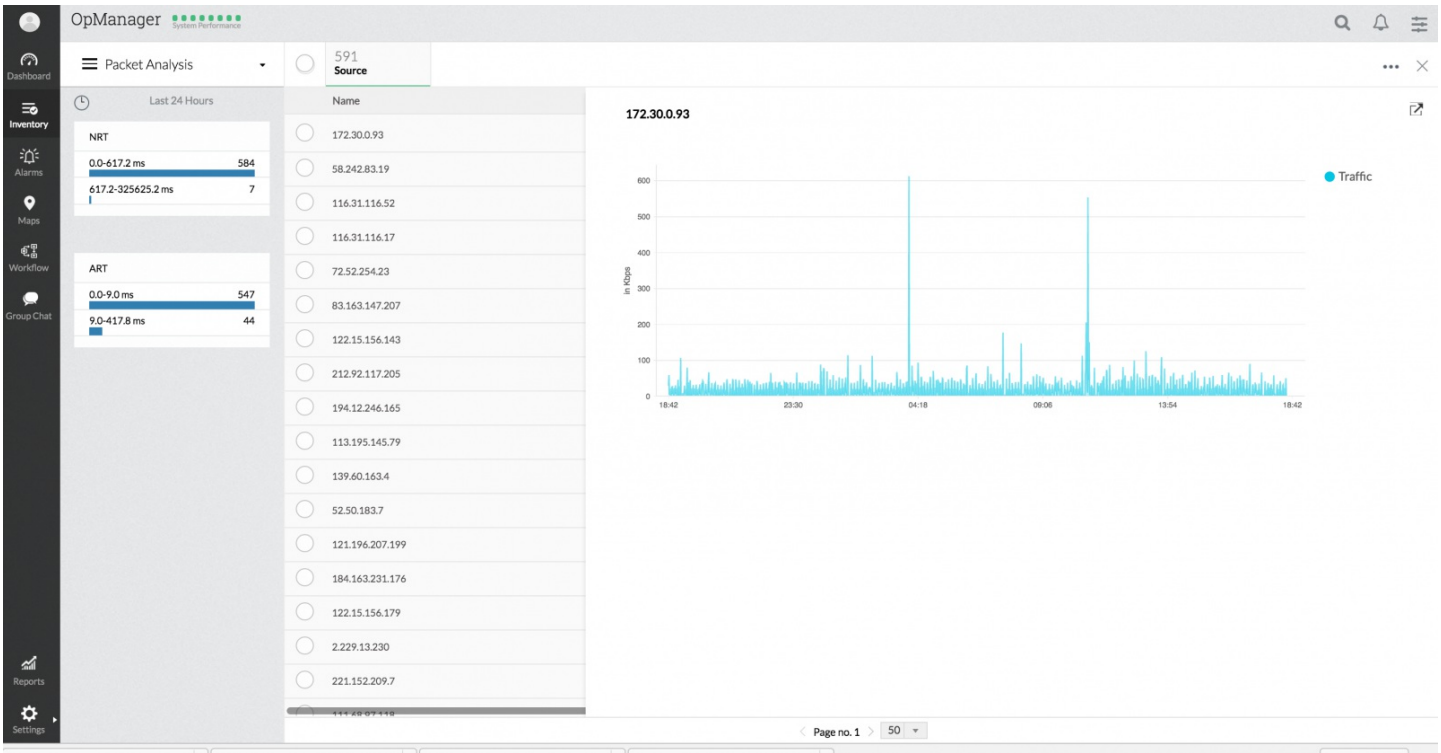

OpManager
System Performance
Dashboard
Inventory
Alarms
Maps
Workflow
Group Chat
Reports
Settings
Packet Analysis
498 URL
46 Application
591 Source
1373 Destination
48822 Conversation
Last 24 Hours
NRT
0.0-51.0 ms 44
51.0-1783.2 ms 2
ART
0.0-3.6 ms 42
3.6-40.6 ms 4
Name
Average NRT
Average ART
Traffic
csbphonemaster 0.083 ms 1.547 ms 4.21 KB
darcorp-lm 0.057 ms 1.558 ms 3.79 KB
dlsrpn 0.09 ms 1.485 ms 3.63 KB
drwcs 0.09 ms 1.854 ms 3.63 KB
etftp 0.058 ms 1.603 ms 4.16 KB
fc-faultnotify 0.043 ms 1.376 ms 3.72 KB
hpvroom 23.012 ms 23.325 ms 24.28 KB
http 1.21 ms 35.396 ms 35.21 MB
https 43.504 ms 40.629 ms 192.23 MB
imtc-map 0.055 ms 1.452 ms 3.63 KB
intrastar 0.079 ms 1.626 ms 3.63 KB
lanyon-lantern 0.039 ms 1.45 ms 4.16 KB
microsoft-ds 13.769 ms 0.106 ms 569.09 KB
mon 0.073 ms 1.541 ms 3.85 KB
msolap-ptp2 0.09 ms 1.531 ms 3.63 KB
navisphere-sec 0.084 ms 1.448 ms 1.57 KB
netview-aix-12 0.046 ms 1.612 ms 4.21 KB
Page no. 1
50

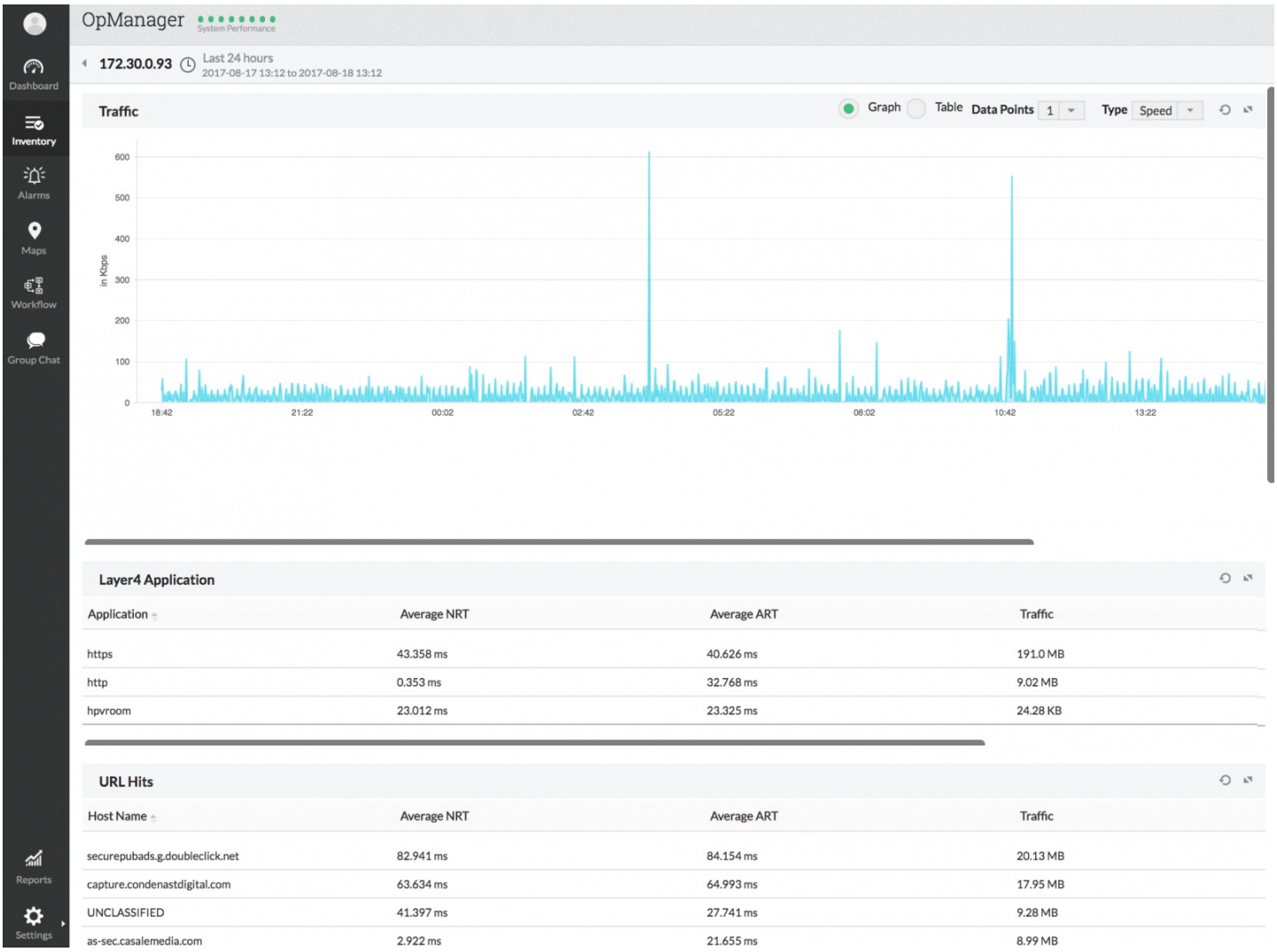


Drill down based on Source /Destination IP address:

Source :


OpManager
System Performance
Dashboard
Inventory
Alarms
Maps
Workflow
Group Chat
Reports
Packet Analysis
492 URL
48 Application
591 Source
1349 Destination
49899 Conversation
Last 24 Hours
NRT
0.0-617.2 ms 584
617.2-325625.2 ms 7
ART
0.0-9.0 ms 547
9.0-417.8 ms 44
Name
Average NRT
Average ART
Traffic
172.30.0.93 36.557 ms 39.376 ms 200.05 MB
58.242.83.19 558.173 ms 0.8 ms 32.19 MB
116.31.116.52 558.135 ms 1.374 ms 31.99 MB
116.31.116.17 65.262 ms 10.421 ms 21.68 MB
72.52.254.23 745.256 ms 1.546 ms 9.85 MB
83.163.147.207 4536.291 ms 1.523 ms 7.47 MB
122.15.156.143 0.059 ms 19.466 ms 5.58 MB
212.92.117.205 111.68 ms 1.514 ms 3.58 MB
194.12.246.165 0.078 ms 1.535 ms 2.52 MB
113.195.145.79 255.556 ms 0.682 ms 2.04 MB
139.60.163.4 0.055 ms 1.533 ms 1.37 MB
52.50.183.7 0.08 ms 1.529 ms 1.26 MB
121.196.207.199 0.08 ms 1.534 ms 1.05 MB
184.163.231.176 0.081 ms 1.547 ms 896.63 KB
122.15.156.179 0.065 ms 91.408 ms 843.06 KB
2.229.13.230 0.079 ms 1.522 ms 786.46 KB
221.152.209.7 0.08 ms 1.51 ms 737.29 KB


OpManager
System Performance
Dashboard
Inventory
Alarms
Maps
Workflow
Group Chat
Reports
Settings
Packet Analysis
591 Source
Last 24 Hours
NRT
0.0-617.2 ms 584
617.2-325625.2 ms 7
ART
0.0-9.0 ms 547
9.0-417.8 ms 44
Name
172.30.0.93
58.242.83.19
116.31.116.52
116.31.116.17
72.52.254.23
83.163.147.207
122.15.156.143
212.92.117.205
194.12.246.165
113.195.145.79
139.60.163.4
52.50.183.7
121.196.207.199
184.163.231.176
122.15.156.179
2.229.13.230
221.152.209.7
172.30.0.93
Traffic
in Kbps
600
500
400
300
200
100
0
18:42
23:30
04:18
09:06
13:54
18:42
Page no. 1
50

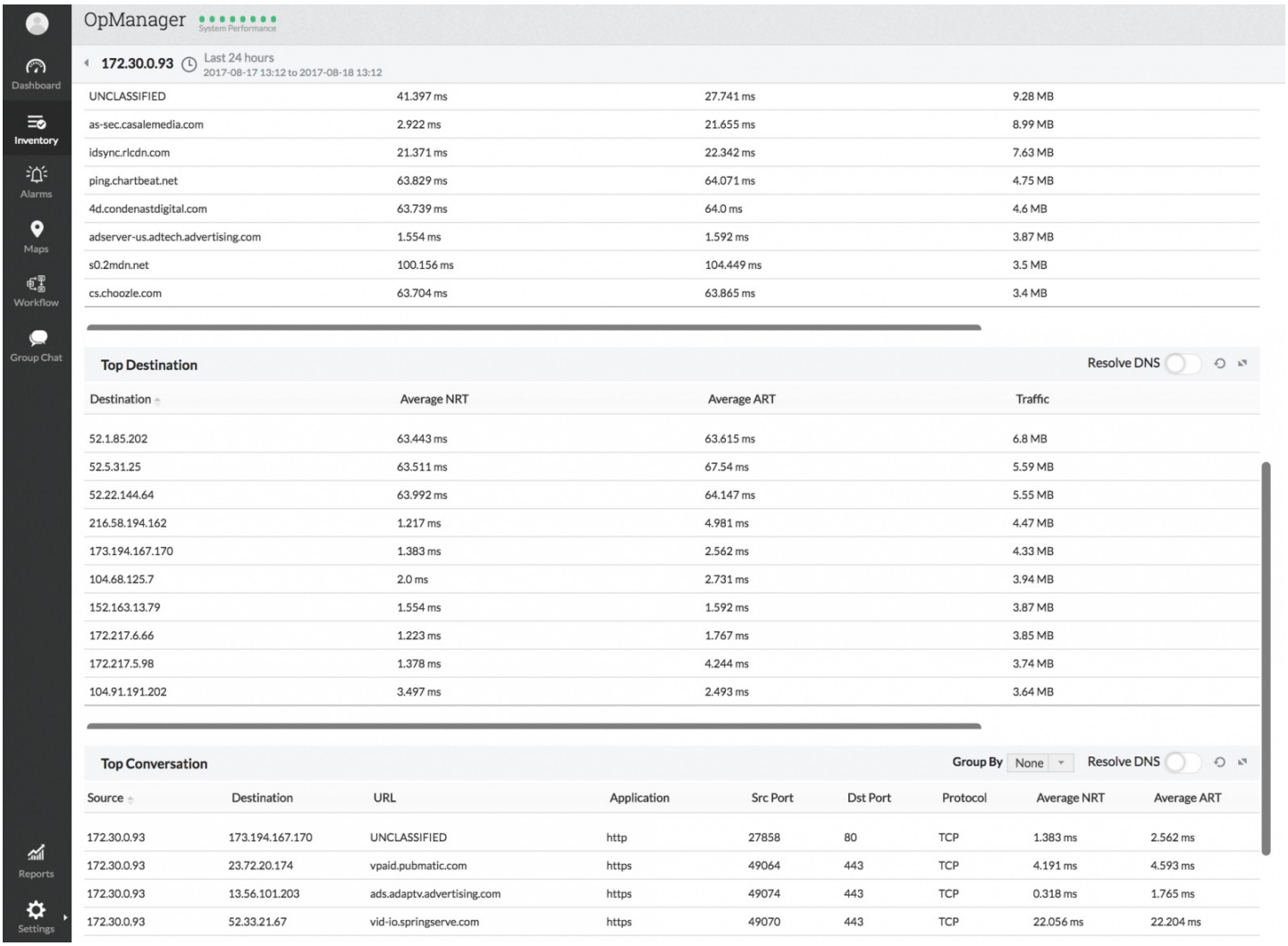


Layer4 Application

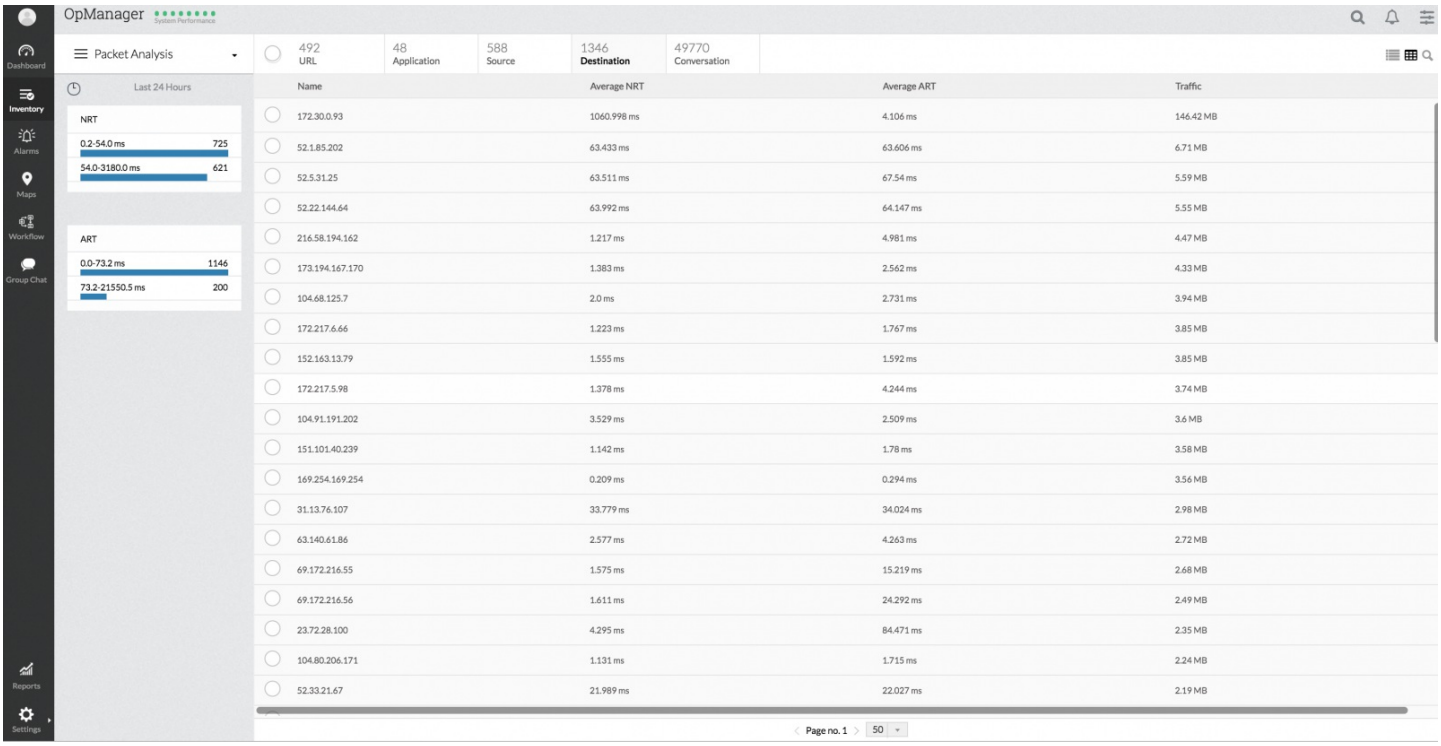
Application	Average NRT	Average ART	Traffic
https	43.358 ms	40.626 ms	191.0 MB
http	0.353 ms	32.768 ms	9.02 MB
hpvroom	23.012 ms	23.325 ms	24.28 KB

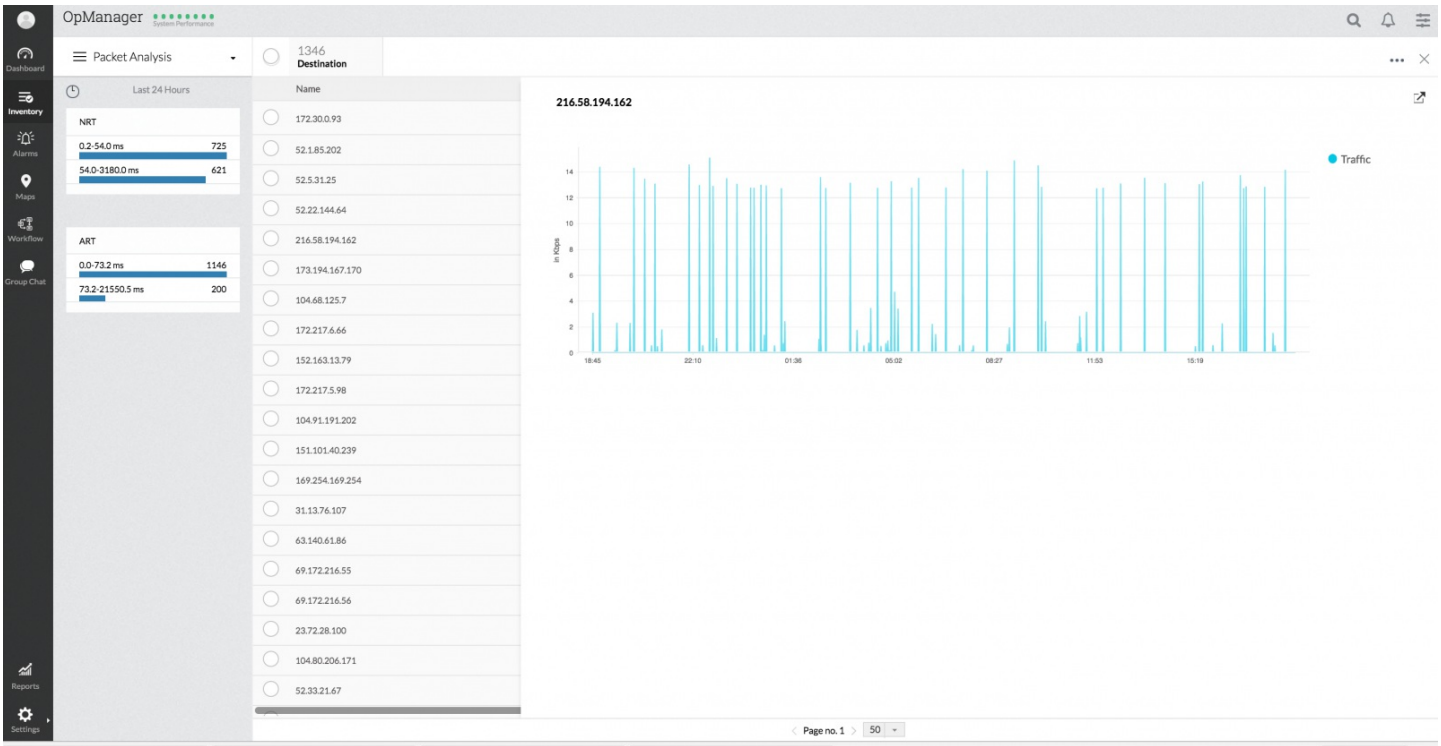
URL Hits

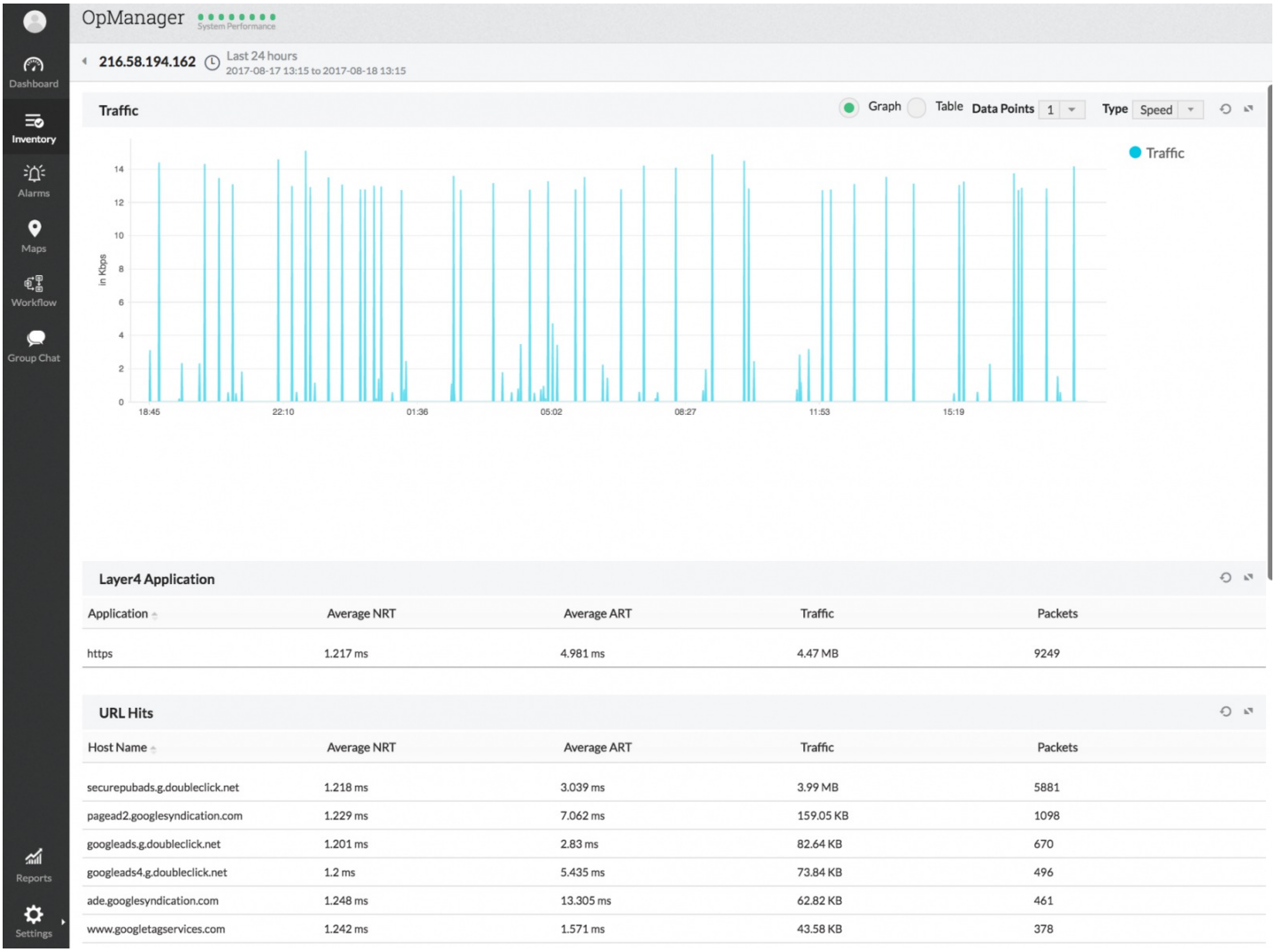
Host Name	Average NRT	Average ART	Traffic
securepubads.g.doubleclick.net	82.941 ms	84.154 ms	20.13 MB
capture.condenastdigital.com	63.634 ms	64.993 ms	17.95 MB
UNCLASSIFIED	41.397 ms	27.741 ms	9.28 MB
as-sec.casalemedia.com	2.922 ms	21.655 ms	8.99 MB



Destination:





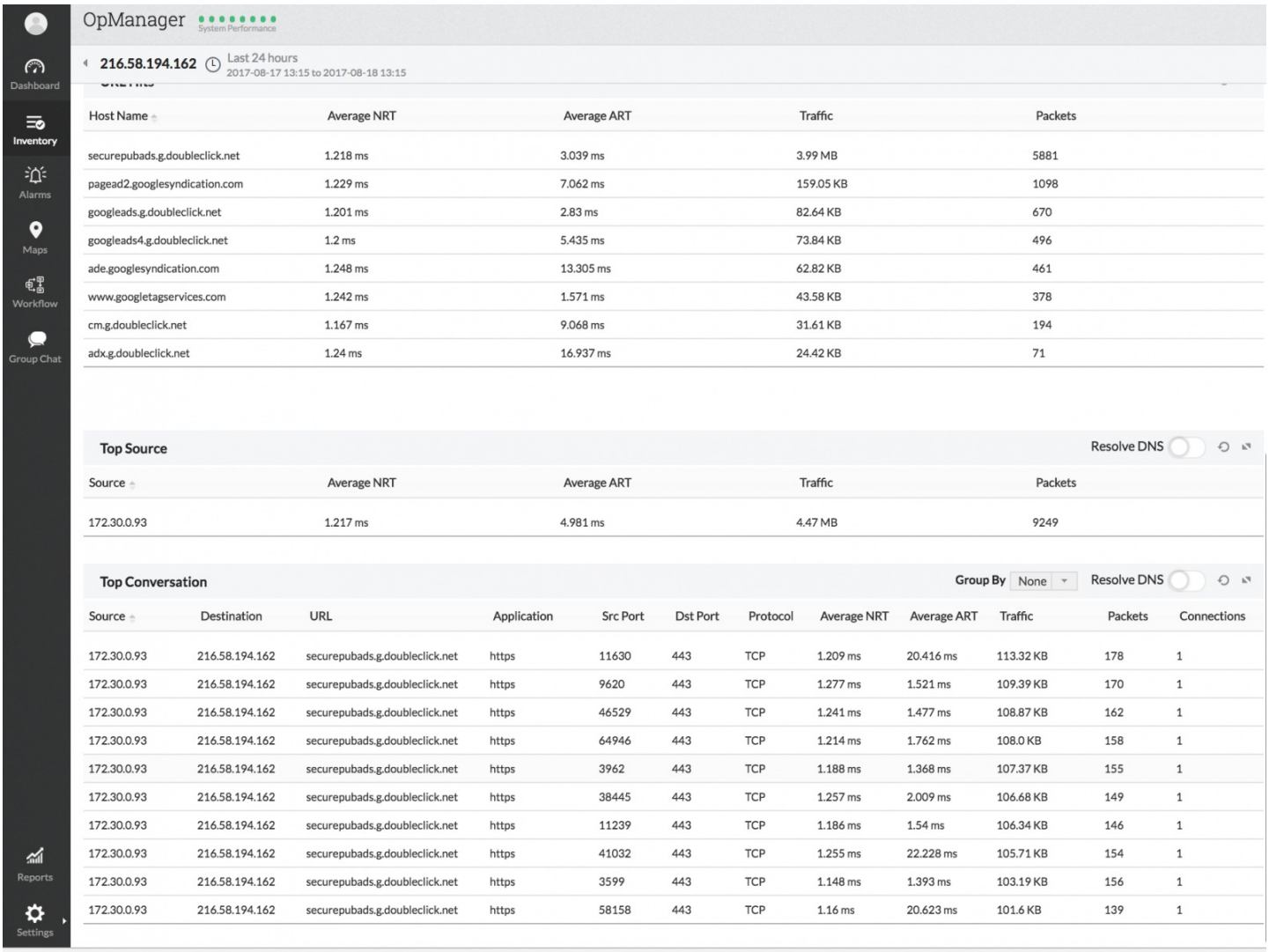


Layer4 Application

Application	Average NRT	Average ART	Traffic	Packets
https	1.217 ms	4.981 ms	4.47 MB	9249

URL Hits

Host Name	Average NRT	Average ART	Traffic	Packets
securepubads.g.doubleclick.net	1.218 ms	3.039 ms	3.99 MB	5881
pagead2.googlesyndication.com	1.229 ms	7.062 ms	159.05 KB	1098
googleads.g.doubleclick.net	1.201 ms	2.83 ms	82.64 KB	670
googleads4.g.doubleclick.net	1.2 ms	5.435 ms	73.84 KB	496
ade.googlesyndication.com	1.248 ms	13.305 ms	62.82 KB	461
www.googletagservices.com	1.242 ms	1.571 ms	43.58 KB	378



Host Name	Average NRT	Average ART	Traffic	Packets
securepubads.g.doubleclick.net	1.218 ms	3.039 ms	3.99 MB	5881
pagead2.googlesyndication.com	1.229 ms	7.062 ms	159.05 KB	1098
googleads.g.doubleclick.net	1.201 ms	2.83 ms	82.64 KB	670
googleads4.g.doubleclick.net	1.2 ms	5.435 ms	73.84 KB	496
ade.googlesyndication.com	1.248 ms	13.305 ms	62.82 KB	461
www.googletagservices.com	1.242 ms	1.571 ms	43.58 KB	378
cm.g.doubleclick.net	1.167 ms	9.068 ms	31.61 KB	194
adx.g.doubleclick.net	1.24 ms	16.937 ms	24.42 KB	71

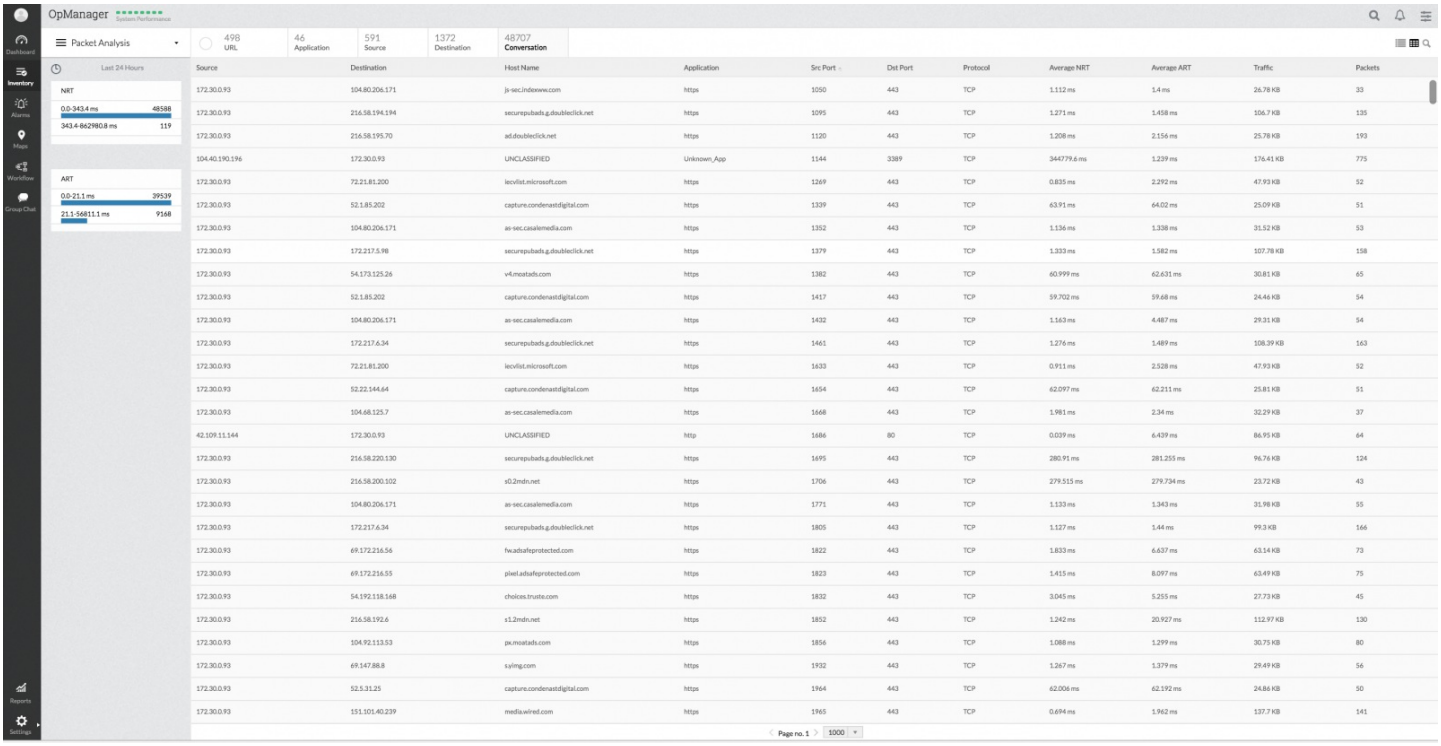
Top Source — Resolve DNS

Source	Average NRT	Average ART	Traffic	Packets
172.30.0.93	1.217 ms	4.981 ms	4.47 MB	9249

Top Conversation — Group By None — Resolve DNS

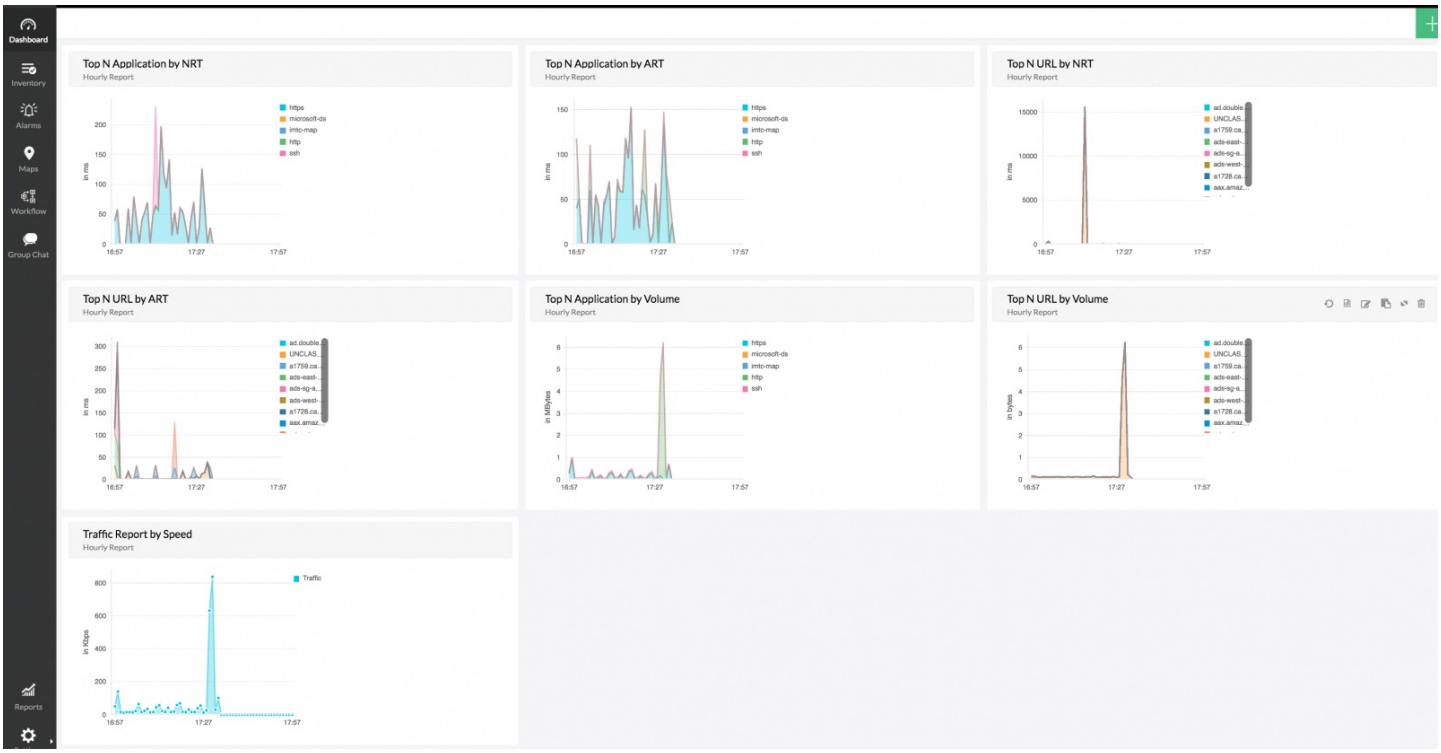
Source	Destination	URL	Application	Src Port	Dst Port	Protocol	Average NRT	Average ART	Traffic	Packets	Connections
172.30.0.93	216.58.194.162	securepubads.g.doubleclick.net	https	11630	443	TCP	1.209 ms	20.416 ms	113.32 KB	178	1
172.30.0.93	216.58.194.162	securepubads.g.doubleclick.net	https	9620	443	TCP	1.277 ms	1.521 ms	109.39 KB	170	1
172.30.0.93	216.58.194.162	securepubads.g.doubleclick.net	https	46529	443	TCP	1.241 ms	1.477 ms	108.87 KB	162	1
172.30.0.93	216.58.194.162	securepubads.g.doubleclick.net	https	64946	443	TCP	1.214 ms	1.762 ms	108.0 KB	158	1
172.30.0.93	216.58.194.162	securepubads.g.doubleclick.net	https	3962	443	TCP	1.188 ms	1.368 ms	107.37 KB	155	1
172.30.0.93	216.58.194.162	securepubads.g.doubleclick.net	https	38445	443	TCP	1.257 ms	2.009 ms	106.68 KB	149	1
172.30.0.93	216.58.194.162	securepubads.g.doubleclick.net	https	11239	443	TCP	1.186 ms	1.54 ms	106.34 KB	146	1
172.30.0.93	216.58.194.162	securepubads.g.doubleclick.net	https	41032	443	TCP	1.255 ms	22.228 ms	105.71 KB	154	1
172.30.0.93	216.58.194.162	securepubads.g.doubleclick.net	https	3599	443	TCP	1.148 ms	1.393 ms	103.19 KB	156	1
172.30.0.93	216.58.194.162	securepubads.g.doubleclick.net	https	58158	443	TCP	1.16 ms	20.623 ms	101.6 KB	139	1

Conversation :



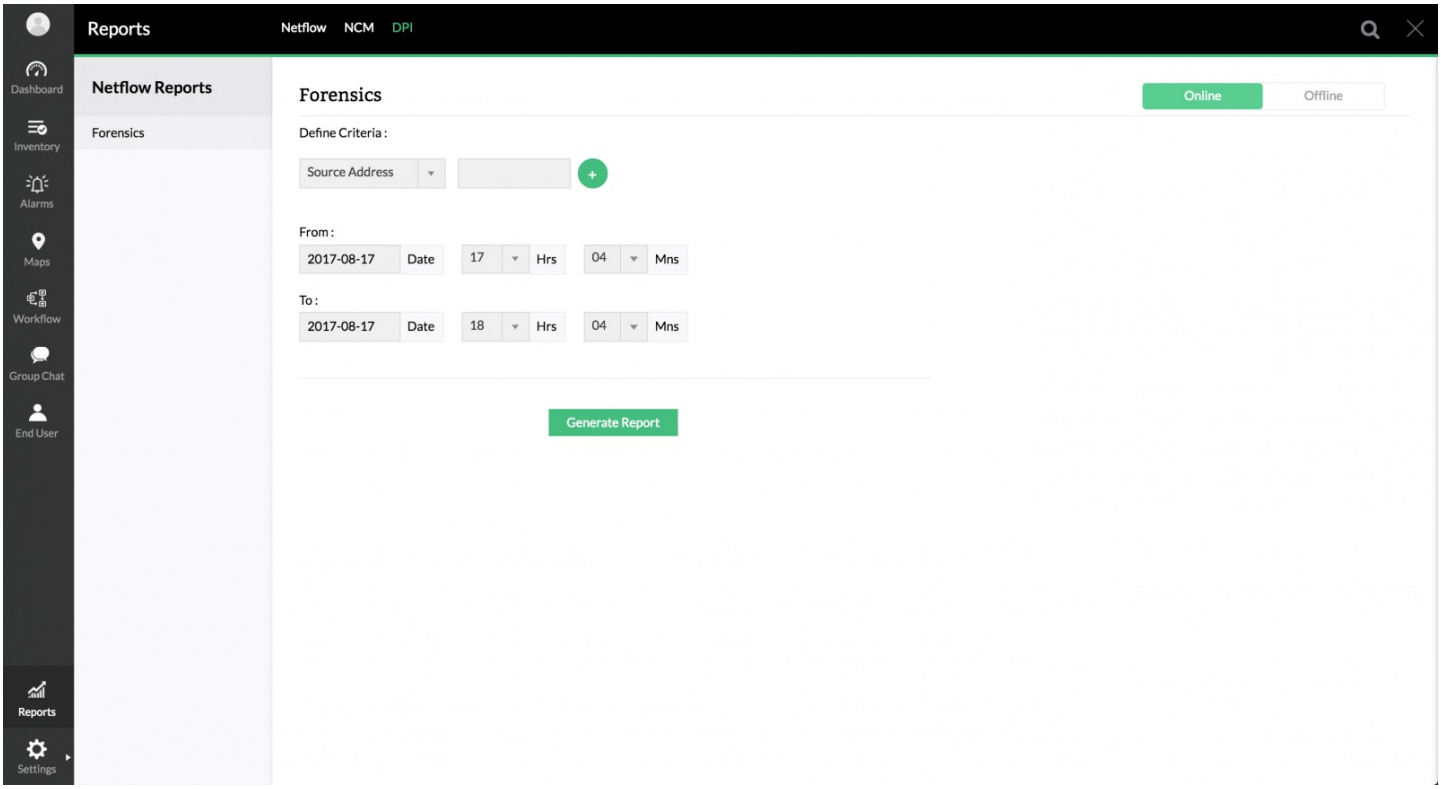
Reports

DPI widgets can be accessed from default dashboard under DPI tab. Custom dashboard can also be created using DPI related widgets.

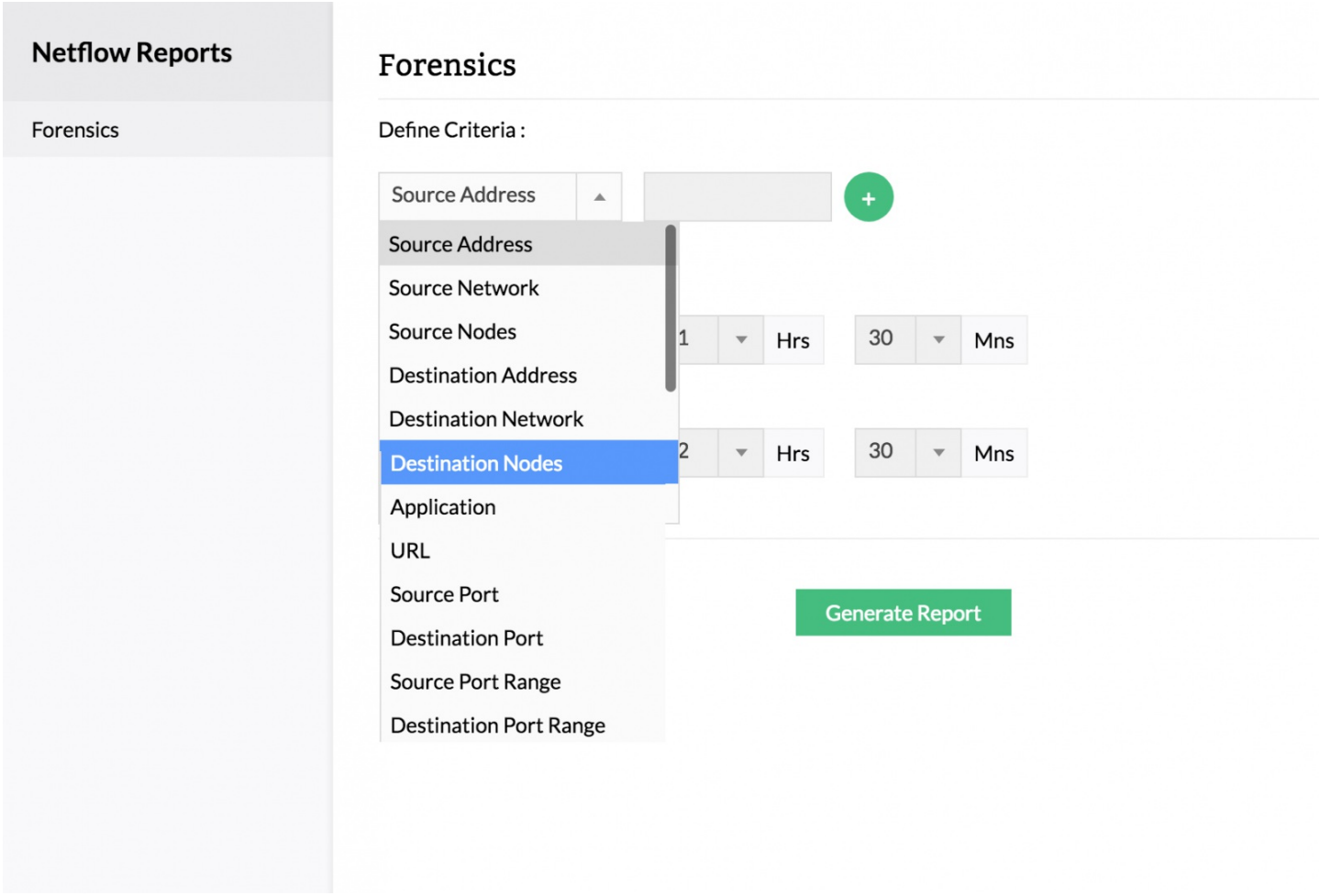


To access reports from UI, navigate to Reports > DPI. Here we have 2 types, Online/Offline reports. Online reports are generated from embedded in-built database. You can also have the packets captured in PCAP format and generate reports for the same.

ManageEngine DPI reports are based on Time and criteria. DPI reports are mainly concentrated on 3 metrics URL, NRT, ART.

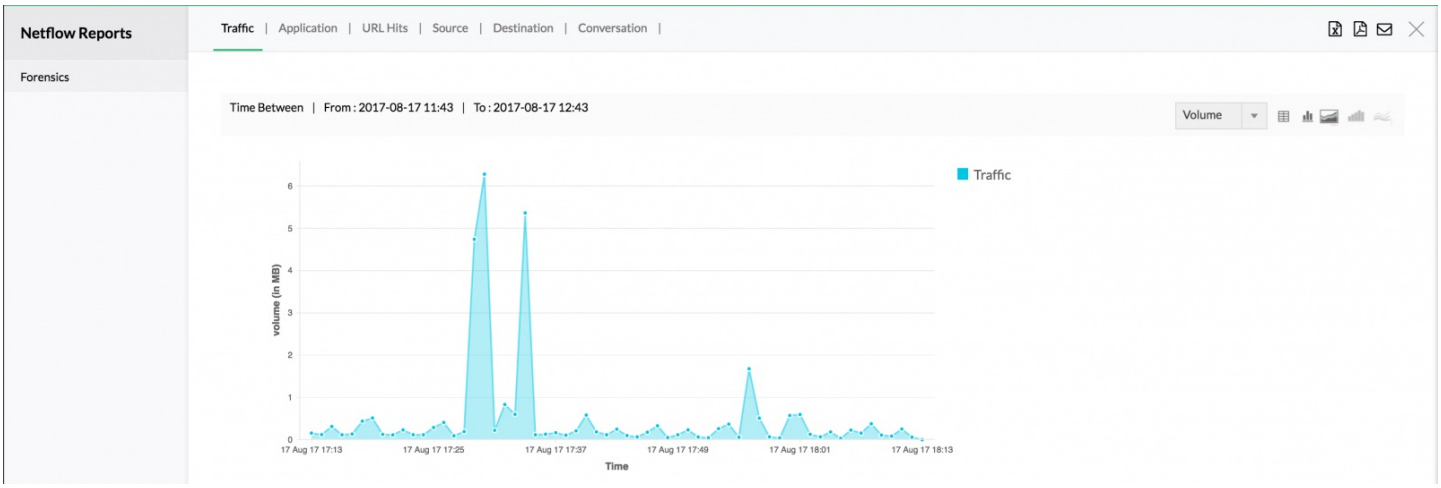


Criteria can be **none** or **any** or **multiple** of the list.



Next the time period should be within the DPI data storage time period.

When you generate reports , you can see reports based on Traffic, Application (Layer 4), URL hits , Source, Destination, Conversation.



Netflow Reports

Forensics

Traffic | Application | URL Hits | Source | Destination | Conversation |

Time Between | From : 2017-08-17 11:43 | To : 2017-08-17 12:43

1 to 8

Application	Average NRT	Average ART	Traffic	Packets
http	4.118 ms	24.127 ms	19.01 MB	17140
https	49.368 ms	39.992 ms	6.93 MB	21382
ssh	3.755 ms	2.77 ms	2.92 MB	19042
Unknown_App	10.618 ms	1.505 ms	1.59 MB	6964
microsoft-ds	0.085 ms	0.1 ms	28.76 KB	311
mon	0.073 ms	1.541 ms	3.85 KB	19
imtc-map	0.055 ms	1.452 ms	3.63 KB	15
opalis-rdv	0.053 ms	1.501 ms	414.00 Bytes	6

Netflow Reports

Forensics

Traffic | Application | URL Hits | Source | Destination | Conversation |

Time Between | From : 2017-08-17 11:43 | To : 2017-08-17 12:43

1 to 163

URL	Average NRT	Average ART	Traffic	Packets
z.moatads.com	1.93 ms	2.253 ms	6.89 KB	33
www.youtube.com	1.225 ms	10.427 ms	20.85 KB	120
www.wired.com	1.082 ms	2.412 ms	76.78 KB	85
www.proximic.com	0.11 ms	1.331 ms	1.0 KB	10
www.googletagservices.com	112.716 ms	113.319 ms	22.86 KB	173
www.google.com	108.685 ms	109.029 ms	42.03 KB	326
www.facebook.com	37.948 ms	38.188 ms	87.1 KB	589
www.agkn.com	43.142 ms	43.181 ms	8.4 KB	21
v4.moatads.com	69.373 ms	91.671 ms	51.05 KB	166
use.typekit.net	2.004 ms	3.396 ms	49.88 KB	148
us-u.openx.net	8.021 ms	14.779 ms	6.87 KB	36
update.googleapis.com	1.237 ms	2.258 ms	18.4 KB	71
UNCLASSIFIED	10.127 ms	11.973 ms	23.57 MB	43607
ums.adtechus.com	85.023 ms	72.671 ms	5.88 KB	21
tubemogul154237275611.s.moatpixel.com	1.664 ms	4.342 ms	19.15 KB	93
tubemogul-sync.dotomi.com	2.883 ms	8.102 ms	7.85 KB	18
tps30.doubleverify.com	1.43 ms	3.423 ms	20.1 KB	29

Netflow Reports

Forensics

Traffic | Application | URL Hits | **Source** | Destination | Conversation |

Time Between | From : 2017-08-17 11:43 | To : 2017-08-17 12:43

1 to 104

Source	Average NRT	Average ART	Traffic	Packets
122.15.156.179	6.506 ms	29.571 ms	11.13 MB	9353
172.30.0.93	40.235 ms	33.635 ms	7.15 MB	23111
42.109.11.144	0.048 ms	11.188 ms	5.68 MB	4129
122.15.156.141	0.049 ms	25.241 ms	1.89 MB	1772
58.242.83.15	0.078 ms	1.027 ms	1.68 MB	11673
116.31.116.17	9.884 ms	0.585 ms	899.19 KB	5245
212.92.124.131	42.547 ms	1.499 ms	384.01 KB	1606
72.52.254.23	0.074 ms	1.512 ms	340.52 KB	1591
116.31.116.52	0.076 ms	0.891 ms	314.55 KB	1955
194.12.246.165	0.071 ms	1.503 ms	105.38 KB	433
52.50.183.7	0.075 ms	1.537 ms	52.88 KB	247
184.163.231.176	0.087 ms	1.539 ms	40.47 KB	169
2.229.13.230	0.065 ms	1.501 ms	31.87 KB	129
221.152.209.7	0.065 ms	1.501 ms	29.97 KB	136
79.127.125.230	0.089 ms	1.512 ms	28.81 KB	122
66.191.79.94	0.06 ms	1.504 ms	28.57 KB	108
122.15.156.143	0.048 ms	77.241 ms	26.07 KB	102

Netflow Reports

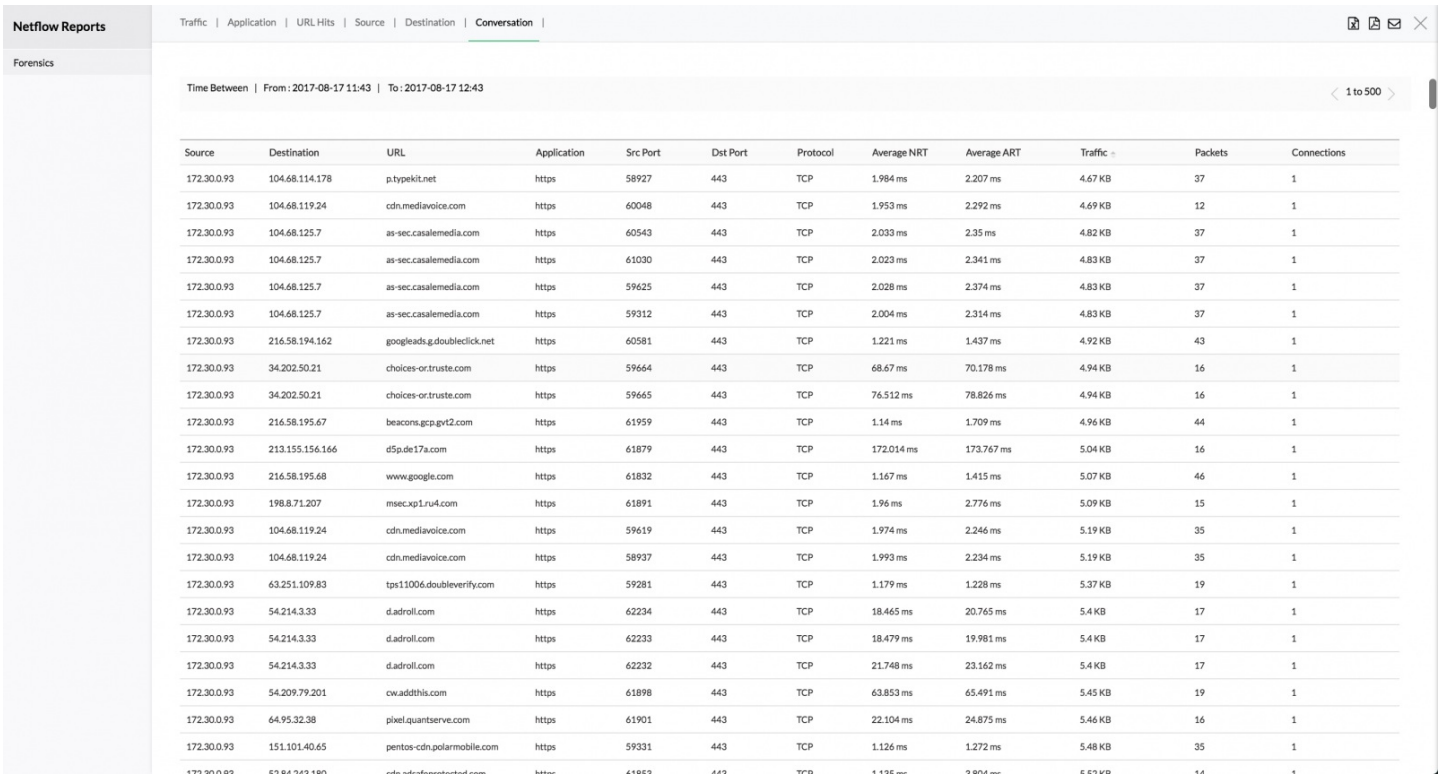
Forensics

Traffic | Application | URL Hits | Source | **Destination** | Conversation |

Time Between | From : 2017-08-17 11:43 | To : 2017-08-17 12:43

1 to 253

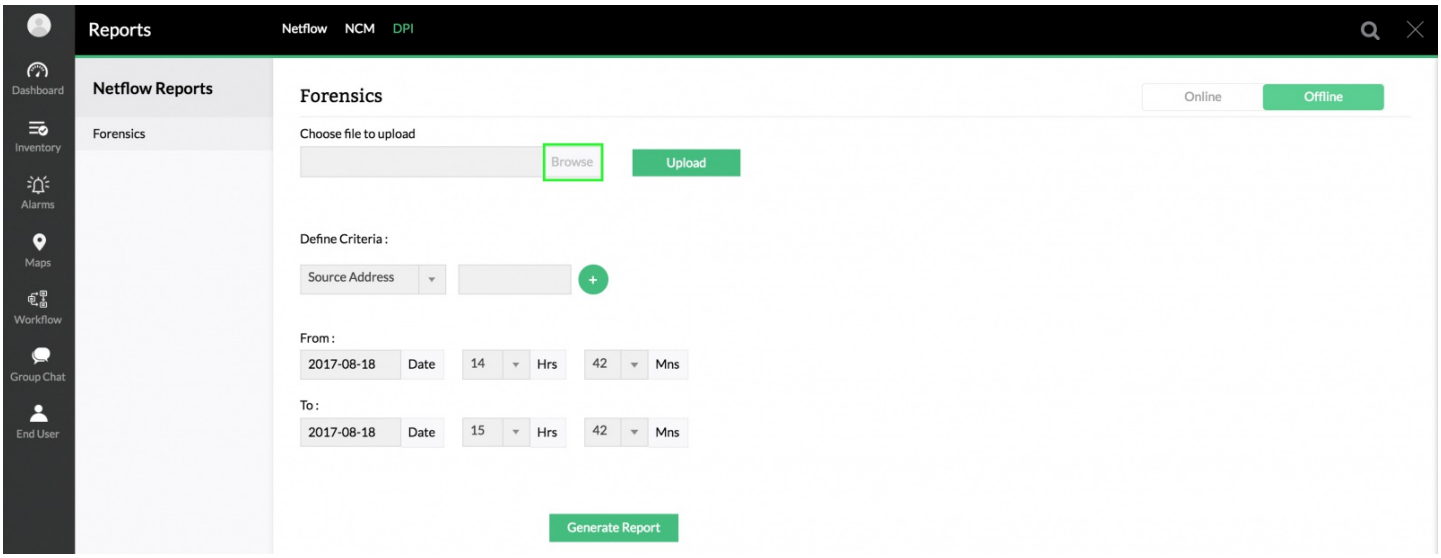
Destination	Average NRT	Average ART	Traffic	Packets
172.30.0.93	6.204 ms	12.863 ms	23.34 MB	41768
104.68.125.7	1.988 ms	2.357 ms	390.37 KB	1723
52.5.31.25	64.83 ms	65.117 ms	339.77 KB	804
172.217.25.34	281.541 ms	168.671 ms	302.87 KB	445
52.1.85.202	63.24 ms	63.395 ms	265.81 KB	717
172.217.25.130	282.628 ms	141.815 ms	212.37 KB	358
69.172.216.55	1.552 ms	6.124 ms	197.86 KB	244
104.68.119.24	2.004 ms	2.255 ms	184.01 KB	336
169.254.169.254	0.21 ms	0.322 ms	151.59 KB	1478
152.163.13.79	1.479 ms	1.493 ms	148.13 KB	317
216.58.194.162	1.218 ms	5.531 ms	138.8 KB	434
69.172.216.56	1.584 ms	6.816 ms	129.2 KB	149
31.13.76.107	37.427 ms	37.7 ms	126.41 KB	250
216.58.194.194	1.199 ms	1.499 ms	122.36 KB	365
172.217.6.34	1.209 ms	20.447 ms	110.48 KB	155
216.58.195.66	1.2 ms	1.418 ms	107.64 KB	156
151.101.40.239	1.05 ms	1.655 ms	94.59 KB	410

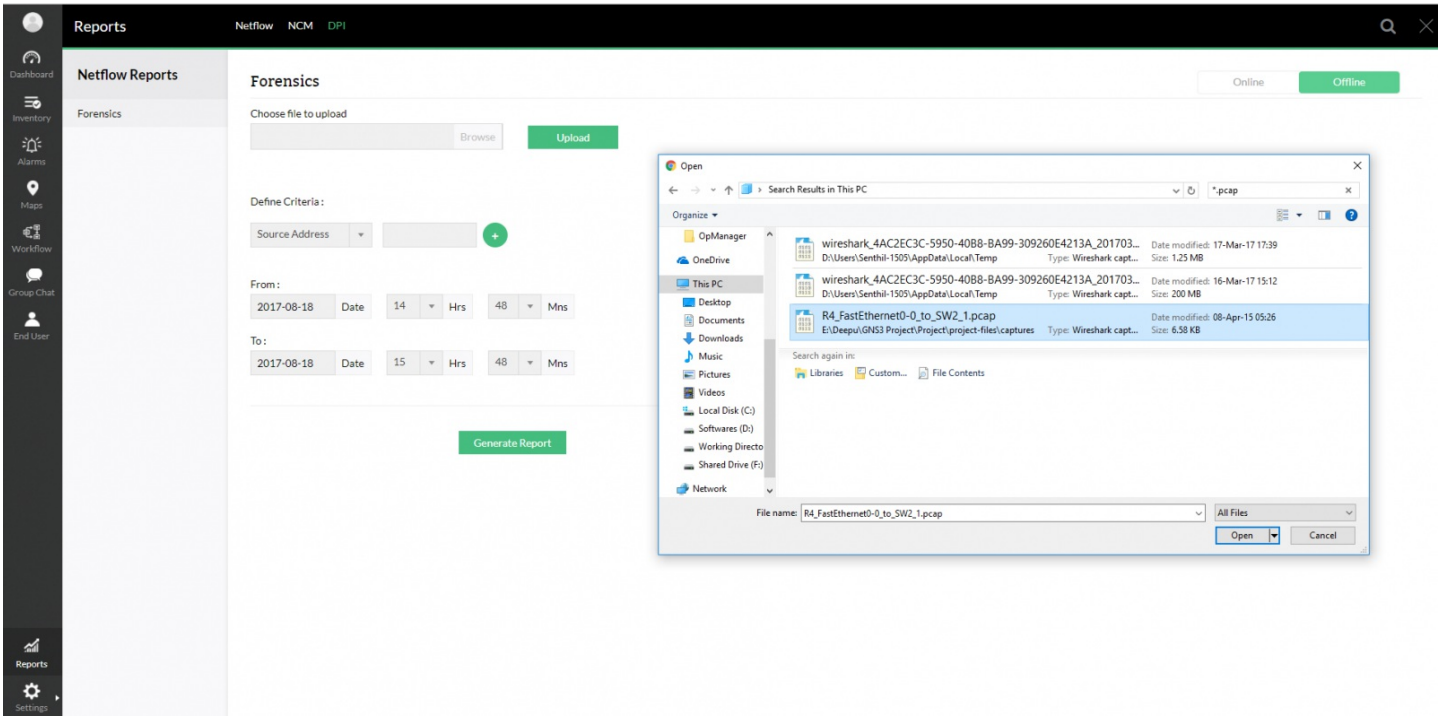


Source	Destination	URL	Application	Src Port	Dst Port	Protocol	Average NRT	Average ART	Traffic	Packets	Connections
172.30.0.93	104.68.114.178	p.typekit.net	https	58927	443	TCP	1.984 ms	2.207 ms	4.67 KB	37	1
172.30.0.93	104.68.119.24	cdn.mediavoice.com	https	60048	443	TCP	1.953 ms	2.292 ms	4.69 KB	12	1
172.30.0.93	104.68.125.7	as-sec.casalemedia.com	https	60543	443	TCP	2.033 ms	2.35 ms	4.82 KB	37	1
172.30.0.93	104.68.125.7	as-sec.casalemedia.com	https	61030	443	TCP	2.023 ms	2.341 ms	4.83 KB	37	1
172.30.0.93	104.68.125.7	as-sec.casalemedia.com	https	59625	443	TCP	2.028 ms	2.374 ms	4.83 KB	37	1
172.30.0.93	104.68.125.7	as-sec.casalemedia.com	https	59312	443	TCP	2.004 ms	2.314 ms	4.83 KB	37	1
172.30.0.93	216.58.194.162	googleads.g.doubleclick.net	https	60581	443	TCP	1.221 ms	1.437 ms	4.92 KB	43	1
172.30.0.93	34.202.50.21	choices-or.truste.com	https	59664	443	TCP	68.67 ms	70.178 ms	4.94 KB	16	1
172.30.0.93	34.202.50.21	choices-or.truste.com	https	59665	443	TCP	76.512 ms	78.826 ms	4.94 KB	16	1
172.30.0.93	216.58.195.67	beacons.gcp.gvt2.com	https	61959	443	TCP	1.14 ms	1.709 ms	4.96 KB	44	1
172.30.0.93	213.155.156.166	d5p.de17a.com	https	61879	443	TCP	172.014 ms	173.767 ms	5.04 KB	16	1
172.30.0.93	216.58.195.68	www.google.com	https	61832	443	TCP	1.167 ms	1.415 ms	5.07 KB	46	1
172.30.0.93	198.8.71.207	msec.xp1.ru4.com	https	61891	443	TCP	1.96 ms	2.776 ms	5.09 KB	15	1
172.30.0.93	104.68.119.24	cdn.mediavoice.com	https	59619	443	TCP	1.974 ms	2.246 ms	5.19 KB	35	1
172.30.0.93	104.68.119.24	cdn.mediavoice.com	https	58937	443	TCP	1.993 ms	2.234 ms	5.19 KB	35	1
172.30.0.93	63.251.109.83	tps11006.doubleverify.com	https	59281	443	TCP	1.179 ms	1.228 ms	5.37 KB	19	1
172.30.0.93	54.214.3.33	d.adroll.com	https	62234	443	TCP	18.465 ms	20.765 ms	5.4 KB	17	1
172.30.0.93	54.214.3.33	d.adroll.com	https	62233	443	TCP	18.479 ms	19.981 ms	5.4 KB	17	1
172.30.0.93	54.214.3.33	d.adroll.com	https	62232	443	TCP	21.748 ms	23.162 ms	5.4 KB	17	1
172.30.0.93	54.209.79.201	cw.addthis.com	https	61898	443	TCP	63.853 ms	65.491 ms	5.45 KB	19	1
172.30.0.93	64.95.32.38	pixel.quantserve.com	https	61901	443	TCP	22.104 ms	24.875 ms	5.46 KB	16	1
172.30.0.93	151.101.40.65	pentos-cdn.polarmobile.com	https	59331	443	TCP	1.126 ms	1.272 ms	5.48 KB	35	1

Offline Reports

Here we also have offline reports where you can save the captured packets (in PCAP format) seperately and generate the same above graphs.




Reports
Netflow
NCM
DPI
Dashboard
Inventory
Alarms
Maps
Workflow
Group Chat
End User
Reports
Settings
Netflow Reports
Forensics
Forensics
Online
Offline
Choose file to upload
Browse
Upload
Define Criteria :
Source Address
From :
2017-08-18
Date
14
Hrs
48
Mns
To :
2017-08-18
Date
15
Hrs
48
Mns
Generate Report
Open
Search Results in This PC
*.pcap
Organize
OpManager
OneDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Softwares (D:)
Working Directo
Shared Drive (F:)
Network
wireshark_4AC2EC3C-5950-40B8-BA99-309260E4213A_201703...
D:\Users\Senthil-1505\AppData\Local\Temp
Type: Wireshark capt...
Date modified: 17-Mar-17 17:39
Size: 1.25 MB
wireshark_4AC2EC3C-5950-40B8-BA99-309260E4213A_201703...
D:\Users\Senthil-1505\AppData\Local\Temp
Type: Wireshark capt...
Date modified: 16-Mar-17 15:12
Size: 200 MB
R4_FastEthernet0-0_to_SW2_1.pcap
E:\Deepu\GNS3 Project\Project\project-files\captures
Type: Wireshark capt...
Date modified: 08-Apr-15 05:26
Size: 6.58 KB
Search again in:
Libraries
Custom...
File Contents
File name:
R4_FastEthernet0-0_to_SW2_1.pcap
All Files
Open
Cancel

End User Monitoring

End User Monitoring in OpManager aims at visualizing the entire bandwidth data of every user in your network. This helps to respond quickly to any performance issues or wireless network congestions that might otherwise affect the quality of user experience.

OpManager correlates the data obtained through Firewall Analyzer add ons, to provide detailed insights on the user's bandwidth consumption, top accessed sites and Applications and the location of the user.

Adding Users:

To enable end user monitoring, the device details/IP addresses are imported from the Active Directory

To import Users via Active directory,

1. Go to **End User Monitoring** Tab.
2. Locate the **+** icon, and select **AD**, from the **Import Profile** Tab, to start importing Users from the Active Directory.
3. Provide the User Name, Password and click on the **Import** button to get details of devices/IP addresses.

Note: The device details can also be added manually.

To configure manually,

1. Select the **Manual** Option from the **Import Profile** Tab
2. Configure the end user details and select the **Import** button, to add the user.

Once the import is done, the details can be viewed under the People tab of the End User Monitoring module.

User Snapshot:

The user snapshot lists user details. It contains

- Number of devices
- Bandwidth consumed
- Top accessed Applications
- Top accessed URLs

To identify the bandwidth consumed or to identify top accessed Applications and URLs, or firewall logs have to be enabled in OpManager.

Connections:

OpManager helps to identify the users connected to your network. It also lists the number of devices, recently connected users and the top 3 Access points.

These user connections can be monitored by fetching details from a wireless controller device(WLC)

To add a WLC device,

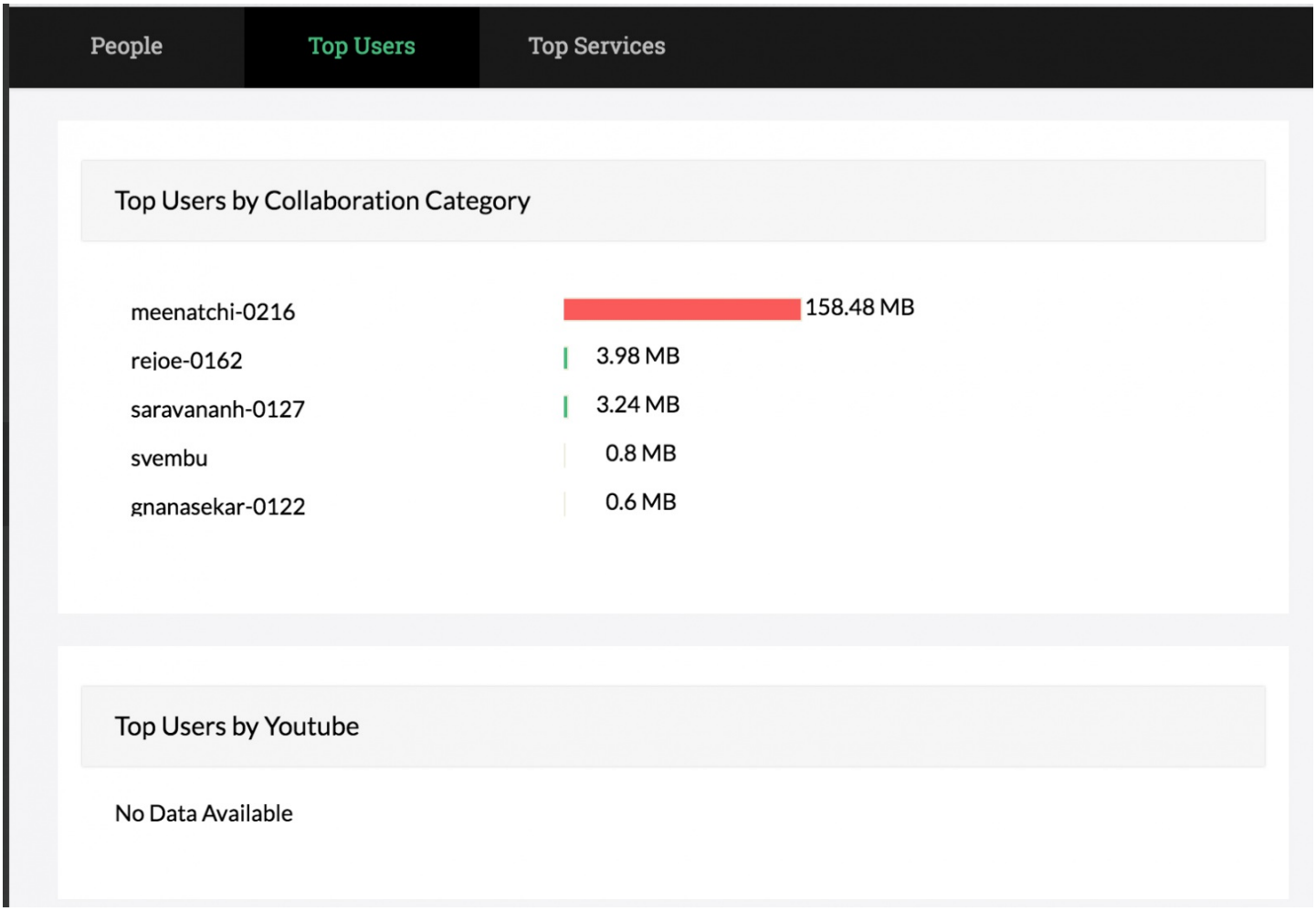
1. Go to **Settings**->**Discovery**-> **Add Device**
2. Provide the Device Name/IP Address of the device.
3. Configure SNMP credentials, and discover the device.

Note: OpManager supports Aruba wireless LAN controller at present. More models will be included with further releases.

Top Users:

OpManager allows to identify the top users of every application. It lists the amount of data used by the top users of various Applications.

OpManager currently includes around 100 Applications to identify the top user of every application. More Applications would be added in further releases.



Top Services:

OpManager allows you to identify top services category wise. It lists the total data used by top Applications.

OpManager includes 25 categories, that helps in listing the top data consuming Applications in the required categories.

Applications Supported By OpManager Out-of-the-box

Microsoft Exchange

MS Exchange 2000
MS Exchange 2003
MS Exchange 2007
MS Exchange 2010
MS Exchange 2013
MS Exchange 2016

Microsoft SQL

MSSQL 2005
MSSQL 2008
MSSQL 2008R2
MSSQL 2012
MSSQL 2014
MSSQL 2016

Microsoft Active Directory

Windows 2003
Windows 2003 R2
Windows 2008
Windows 2008 R2
Windows 2012
Windows 2012 R2
Windows 2016

Via Application Monitoring Plugin

Applications Server Monitoring	Database Monitoring	System Management	Virtualization Monitoring
Microsoft .Net JBoss Tomcat Oracle VMware vFabric tc Server BEA WebLogic SilverStream IBM WebSphere GlassFish Server	Oracle Management MySQL Management SQL Server Management DB2 Management Sybase Management PostgreSQL Monitoring Memcached Monitoring Database Query Monitor MongoDB Monitoring Cassandra Monitoring Redis Monitoring	Windows Monitoring Linux Monitoring Solaris Monitoring AIX Monitoring AS400 Monitoring HP-Unix / Tru64 Unix Monitoring FreeBSD Monitoring Novell Monitoring Mac OS Monitoring User Defined Custom Monitors Windows Event Log Monitoring File System Monitor Windows Performance Counters	VMware Monitoring Microsoft Hyper-V Monitor Virtual Machine Monitor Automatic Virtual Resource Provisioning Citrix XenServer Monitoring

ERP Monitoring	Web Server / Web Services	Website Monitoring	Cloud Monitoring

ERP Monitoring	Web Server / Web Services	Website Monitoring	Cloud Monitoring
SAP Monitor Oracle E-Business Suite Monitor	Web Services (SOAP) Apache Monitoring IIS Monitoring Nginx Monitoringnew PHP Monitoring SSL Certificate Monitoring Active Directory Monitor LDAP Monitoring DNS Monitoring FTP, SFTP Monitoring Other Web Servers	URL Monitoring Record & Playback HTTP Requests URL Content Monitoring Real Browser Monitor	Amazon EC2 Monitoring Amazon RDS Monitoring Automated Cloud Resource Management Windows Azure Monitoring
Middleware/Portal Monitoring	**Web Transaction Monitoring**	**End User Monitoring**	**Custom Monitoring**
WebSphere MQ Monitor MS Office SharePoint Monitor WebLogic Integration Monitor Microsoft Message Queue (MSMQ) VMware vFabric RabbitMQ	Java Web Transaction Monitoring (APM Insight) .NET Web Transaction Monitoring Ruby on Rails Web Transaction Monitoring Java Runtime Monitoring JMX Monitoring | SNMP Monitoring	End User Management End User Monitoring from branch offices	JMX Consoles SNMP Consoles File System Monitor Windows Performance Counters Script Monitoring Database Query Monitor

Integrating with ServiceDesk Plus

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

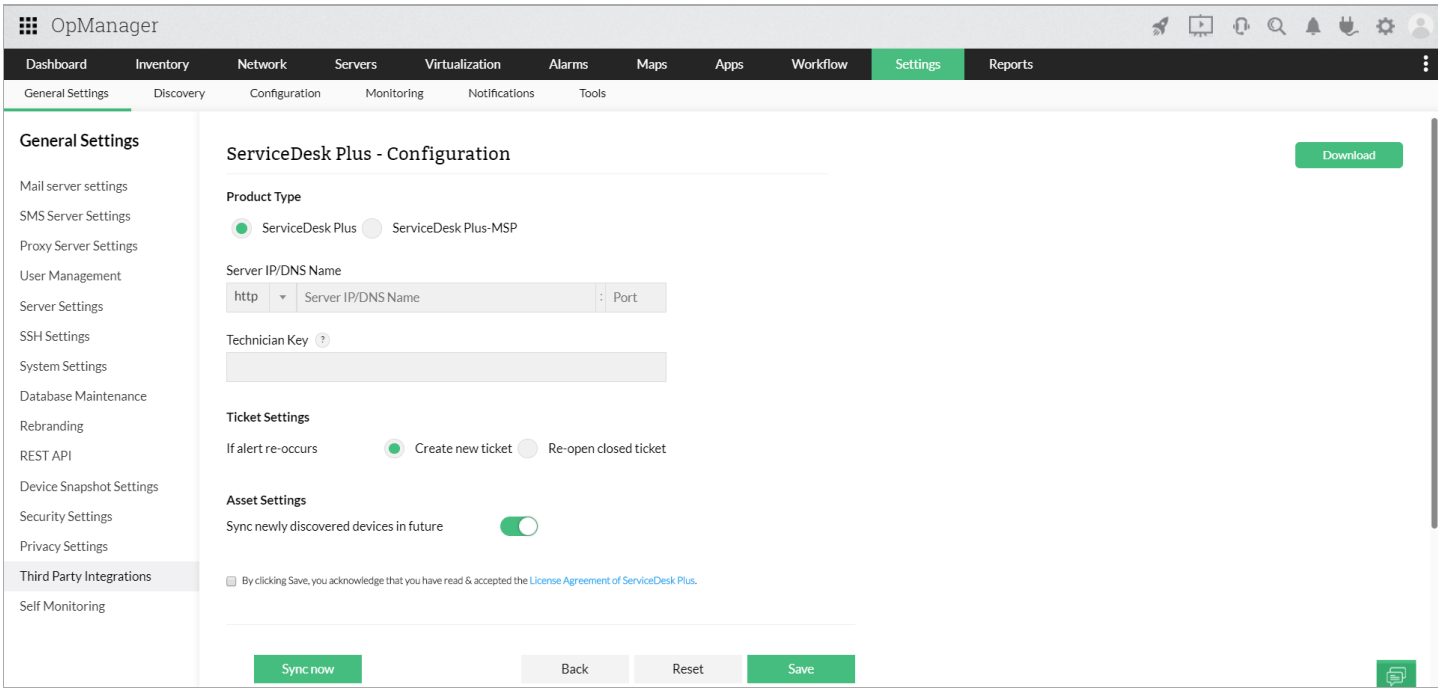
For logging the trouble ticket to ServiceDesk Plus correctly, you need to ensure the following:

1. ServiceDesk Plus Settings must be configured in OpManager
2. A notification profile to log a trouble ticket to ServiceDesk Plus must be configured and associated.

OpManager talks to ServiceDesk Plus via its API. Click here to know how to generate the API key for integrating ServiceDesk Plus with OpManager.

Configure Server's Settings

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



1. OpManager must 'know' where ServiceDesk Plus is running to log the ticket. To configure the ServiceDesk Plus settings details, follow the steps given below

2. Click **Settings** → **General Settings** → **Third Party Integrations** → **ServiceDesk Plus** and configure the following values:

- ***Product type***: Select the product type (ServiceDesk Plus or ServiceDesk Plus-MSP) with which you are trying to integrate OpManager.
- ***Server IP / DNS Name:*** Name or the IP address of the machine where ServiceDesk Plus is installed and running.
- ***ServiceDesk Plus Technician Key:*** Enter the API key generated using API Key Generation in ServiceDesk Plus. Click here to learn how to get the Technician key.
- ***Ticket Reopen Settings*** *:* If an alert re-occurs, this setting will allow you re-open an old ticket or create a new one.
- ***Sync newly discovered devices in future:*** This option will automaticlly sync your asset details with ServiceDesk Plus whenever a new device is discovered in OpManager. The following fields will be synced from OpManager to Service Desk Plus whenever an asset sync happens - Asset Name, Asset Type [Category], IP Address, RAM Size, OS Name, Vendor, Site Name [Probe Name] (for

OpManager enterprise edition only).

3. The **Sync now** option will let you sync the devices in OpManager with ServiceDesk Plus

4. Now, click **Save**.

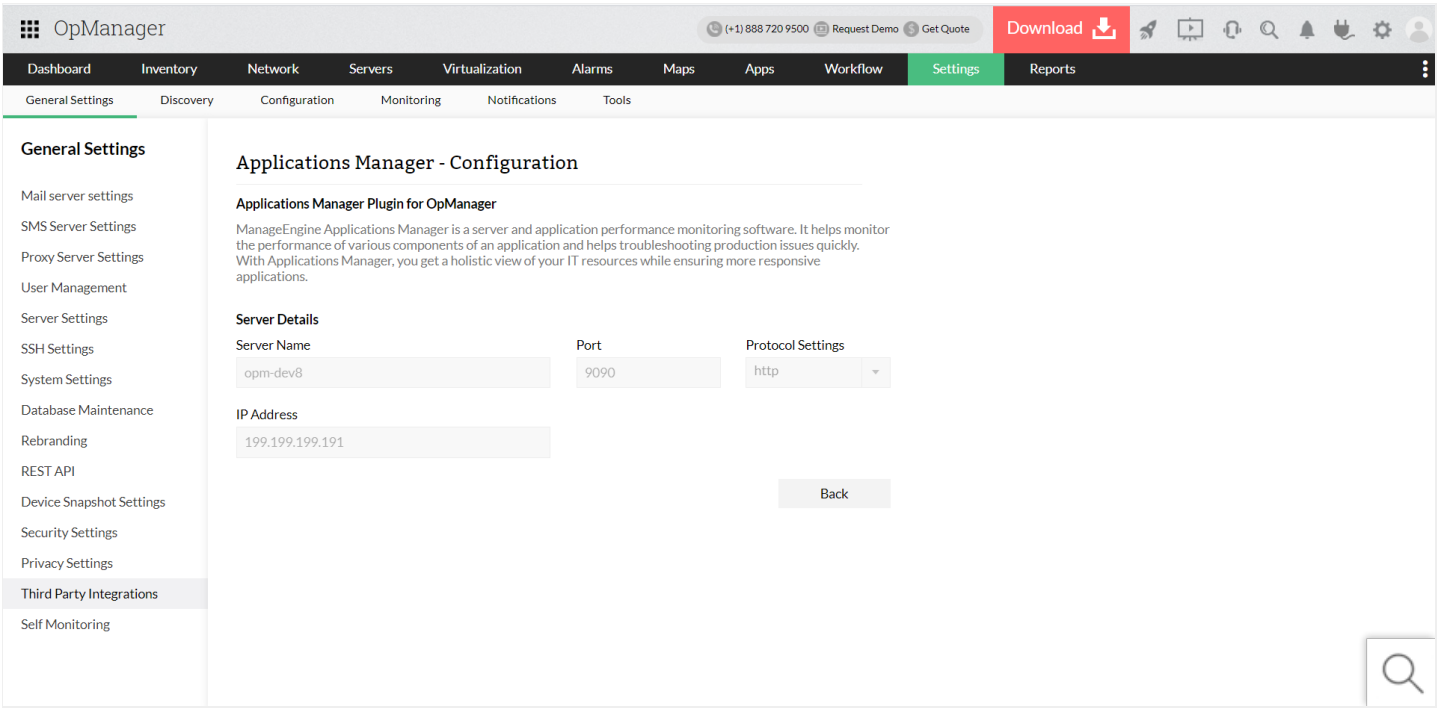
Note:

- It is highly recommended that you use the latest/ updated versions of both OpManager and ServiceDesk Plus. Because the latest versions communicate via API-based integration unlike older versions.
- If an alarm is raised as a ticket in ServiceDesk Plus and the ticket is not closed (or) if the ticket is reopened, any change in severity of the alarm will be updated in the same ticket as notes.
- Whenever a ticket is being raised in ServiceDesk Plus, it will be raised with requester name as **administrator**.

Integrating with Applications Manager

By integrating with Applications Manager, OpManager helps you to keep track over the performance of critical applications and thereby ensuring high availability. You can monitor the performance of various components of an application and provides quick resolution in case of any outages.

An easy installation and integration procedure helps connect your APM plugin to your OpManager installation in no time. This means, you don't have to do anything from your end to configure the plugin. Once you install the APM plugin, all necessary server details **are automatically populated** in OpManager and in the APM plugin.



AlarmsOne integration:

ManageEngine AlarmsOne is a SaaS-based alert management tool that helps IT admins manage alerts from all their IT management applications in one place. With AlarmsOne, you can reduce alert noise, create on-call schedules to notify your technicians about incidents through email, SMS, and call alerts, escalate unattended alerts, modify alert content to create actionable alerts, and so on.

Integrating AlarmsOne with OpManager:
Follow the below steps to integrate AlarmsOne with OpManager and start managing your OpManager alerts in AlarmsOne. If you don't have an AlarmsOne account,&#65533; click here to create one.

1. Log in to your AlarmsOne account and go to&#65533; **Settings >&#65533; Show API** key. Copy the API key.
2. Log in to OpManager and go to the **Settings > Third Party Integrations** section.
3. Select&#65533; **AlarmsOne**. Now, paste the copied AlarmsOne API key.
4. Read our privacy policy and tick the check box if you agree, and then click the&#65533; **Integrate** button.

This completes the integration process. Now you can view and manage your OpManager alerts in AlarmsOne. You can&#65533; add your team in AlarmsOne,&#65533; integrate the other applications you use with AlarmsOne and manage alerts from all the apps in one place.&#65533; Click here to learn how to configure AlarmsOne's features such as&#65533; noise reduction, &#65533; escalations, &#65533; on-call scheduling,&#65533; alarm modifier,&#65533; downtime, etc.

Note: This integration needs an active internet connection to send alarms from OpManager to AlarmsOne in real time.

How to enable/disable AlarmsOne configuration?

- Open OpManager
- Navigate to **Settings -> General Settings -> Third Party Configurations -> AlarmsOne**
- Click&#65533; *Disable*&#65533; button to disable the configuration.

Note:&#65533; You can re-enable the configuration, by clicking on&#65533; *Enable* on the same page.

Integrating OpManager with ServiceNow

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

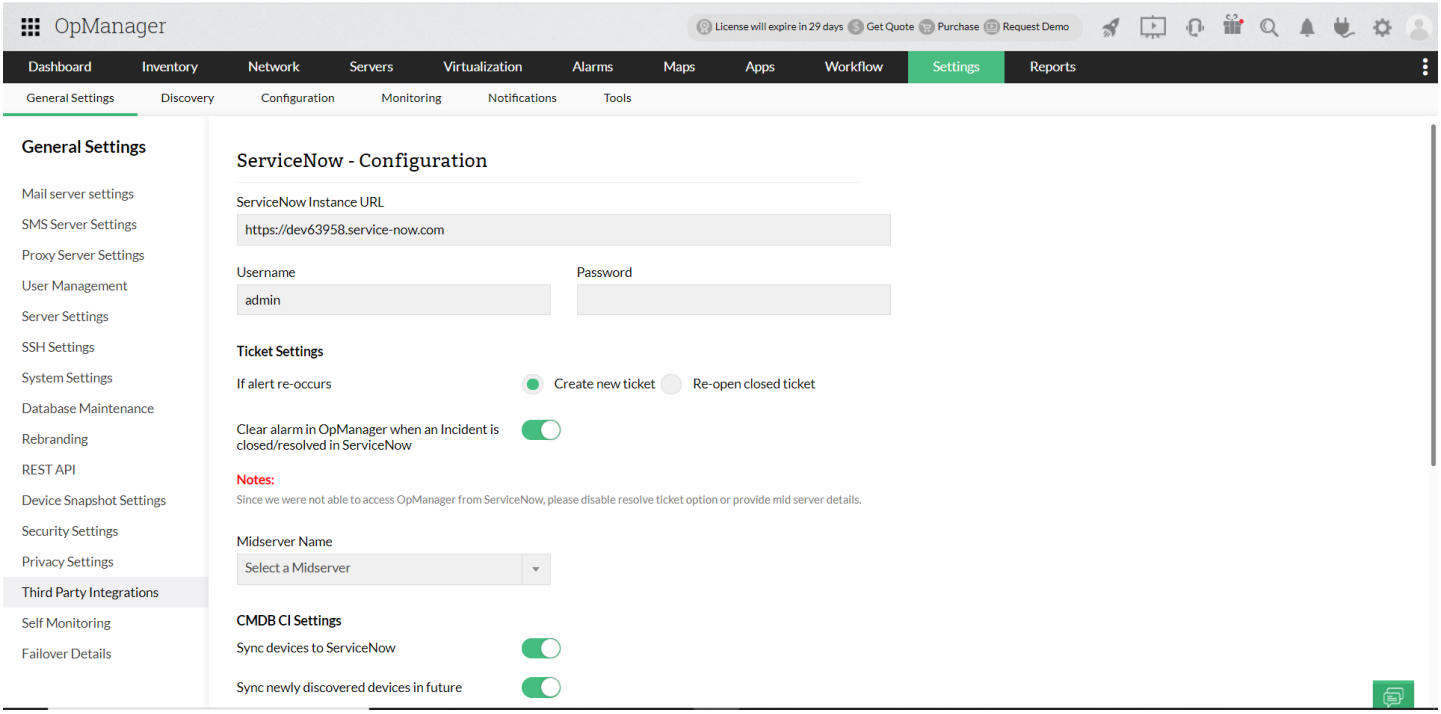
For logging the trouble ticket to ServiceNow correctly, you need to ensure the following:

1. ServiceNow Settings must be configured in OpManager
2. A notification profile to log a trouble ticket to ServiceNow must be configured and associated.

Configure Server Settings

Following are the steps to configure the ServiceNow and OpManager Server settings:

1. Go to **Settings ? General Settings ? Third Party Integrations ? ServiceNow** and configure the following values:



- **ServiceNow URL**: The URL for your ServiceNow Connection
- **ServiceNow UserName** & **Password**
- **Ticket Settings:**
    - **If alert re-occurs:** Instruct OpManager to perform an operation if an alert re-occurs. **Create new ticket** will raise the alert as a new ticket in ServiceNow while **Re-open closed ticket** will re-open the ticket raised for the corresponding alert in ServiceNow.

- **Clear alarm in OpManager when an Incident is closed/resolved in ServiceNow:** Automatically clears the alarm when the corresponding incident is closed / resolved in ServiceNow. (or)
- **Midserver**: Choose the Midserver name from the dropdown. It establishes the connection between OpManager and ServiceNow.

- **CMDB CI Settings:**
  - **Sync devices to ServiceNow:** Add existing devices from OpManager to ServiceNow.
  - **Sync newly discovered devices in future:** When new devices are added in OpManager, automatically add them to ServiceNow.
  - **Remove CI from ServiceNow when a device is deleted from OpManager:**Remove a device from ServiceNow when it is removed from OpManager.

1. Click on **Save** to save your configurations and complete the integration process successfully.
2. Click on **Sync now** to sync the Assets from OpManager with ServiceNow using the saved configurations.

Integrating OpManager with ServiceNow using 3rd party / self-signed SSL Certificate

OpManager can be integrated easily with ServiceNow using a 3rd party / self-signed SSL Certificate by using the following steps:

Step 1: Get the keystore file and password

- Get the key store file and password used while generating the SSL certificates in OpManager. If certificate is present already, skip to step 3.
- To get the file path and password, open the file "**server.xml**" located under "**<OpManager_Installed_Dir>/conf/server.xml**" and check for the **<Connector>** tag.

```
<Connector port="8443" SSLEnabled="true" URIEncoding="UTF-8" acceptCount="100" address="0.0.0.0"
clientAuth="false" compressableMimeType="text/html,text/xml" compression="force"
compressionMinSize="1024" connectionTimeout="20000" disableUploadTimeout="true"
enableLookups="false" keystoreFile="<Keystore Path>" keystorePass="<Keystore Password>"
maxSpareThreads="75" maxThreads="150" minSpareThreads="25" noCompressionUserAgents="gozilla,
traviata" protocol="HTTP/1.1" scheme="https" secure="true" sslProtocol="TLS"/>
```

```
<Connector SSLEnabled="true" URIEncoding="UTF-
8" compressableMimeType="text/html,text/xml" compression="force" compressionMinSize="1024" connect
ionTimeout="20000" noCompressionUserAgents="gozilla,
traviata" port="WEBSERVER_PORT" protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="http
s" secure="true">
 <UpgradeProtocol className="org.apache.coyote.http2.Http2Protocol"/>
 <SSLHostConfig sslProtocol="all" ciphers="${server.https.ciphers}" >
 <Certificate certificateKeystoreFile="<Keystore Path>" certificateKeystorePassword="<Keystore
Password>"/>
 </SSLHostConfig>
</Connector>
```

Step 2: Export the SSL certificate from keystore file.

- To export SSL certificate from keystore file, run the following command and if prompted for password, enter the password from Step 1

```
<OpManager_Installed_Dir>\jre\bin\keytool -export -alias <Alias Name> -keystore <Keystore Path> -rfc -file opmssl.cert
```

  where Alias Name is the certificate alias name.
- You can get list of aliases from key store using the following command

```
<OpManager_Installed_Dir>\jre\bin\keytool -list -keystore <Keystore Path>
```

Step 3: Import the SSL Certificate.

To import the SSL certificate to a new trust store, run the following command

- If SSL Certificate is self-signed:

```
<OpManager_Installed_Dir>\jre\bin\keytool -importcert -alias opmssl -file opmssl.cert -keystore opmservicenow.truststore -storepass
<Truststore Password>
```

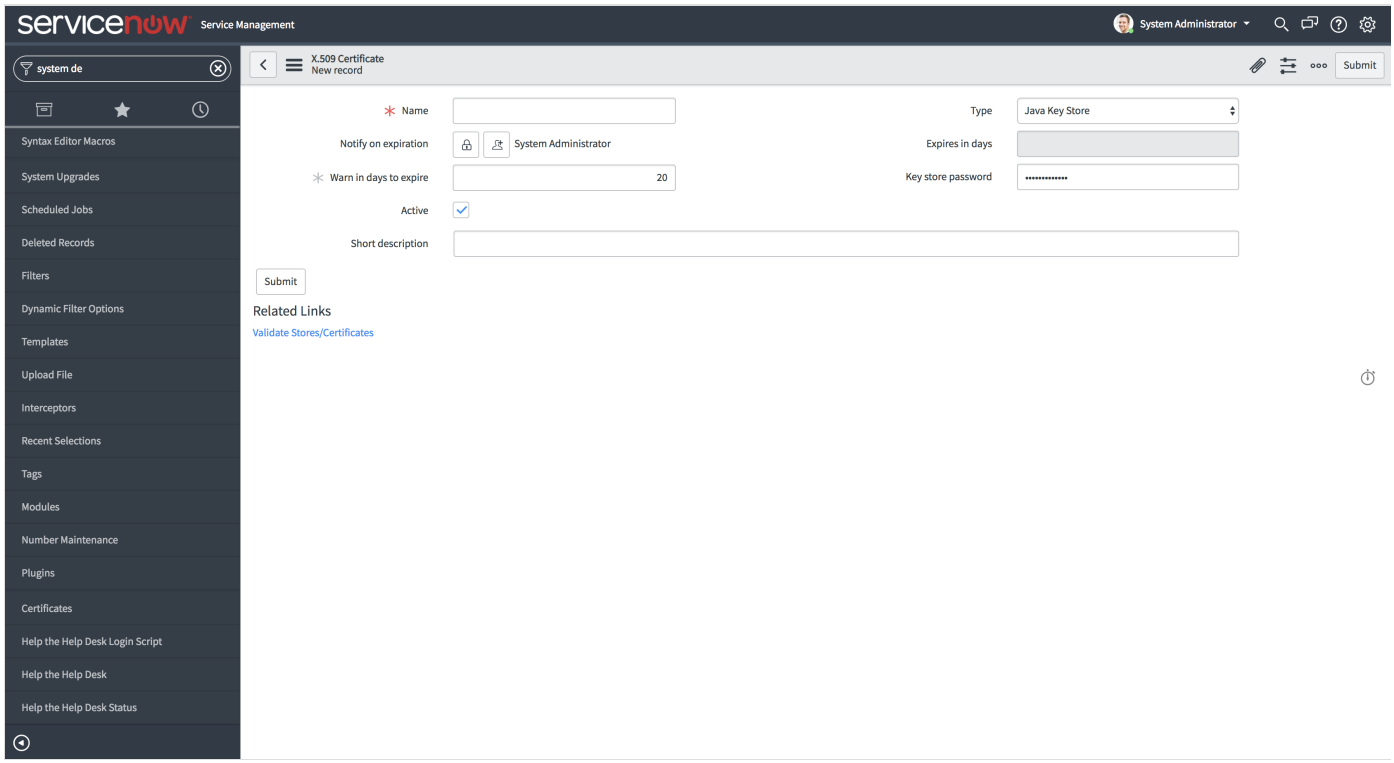
- If SSL Certificate is CA-signed:

```
<OpManager_Installed_Dir>\jre\bin\keytool -import -trustcacerts -alias opmssl -file opmssl.cert -keystore opmservicenow.truststore -
storepass <Truststore Password>
```

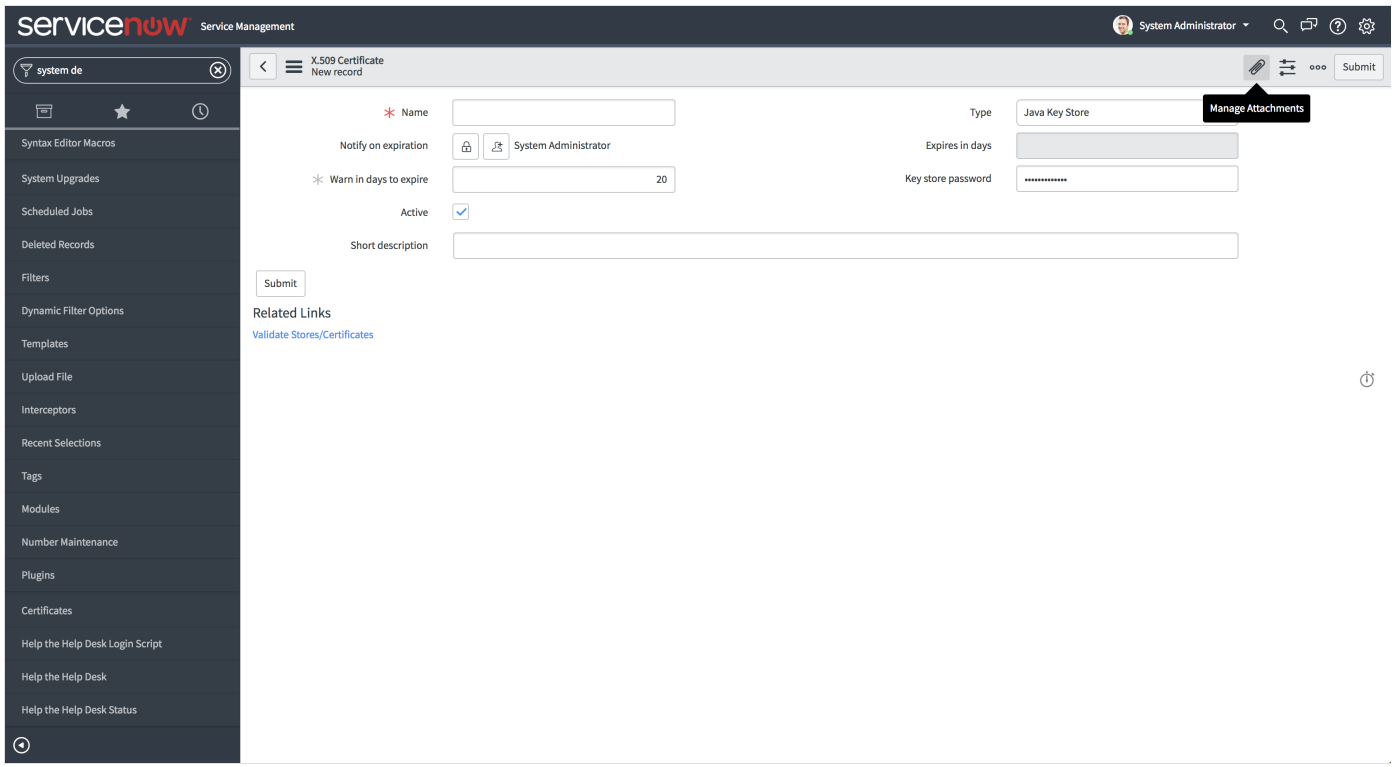
  Note: The Truststore password can be any password.

Step 4: Import Truststore to ServiceNow:

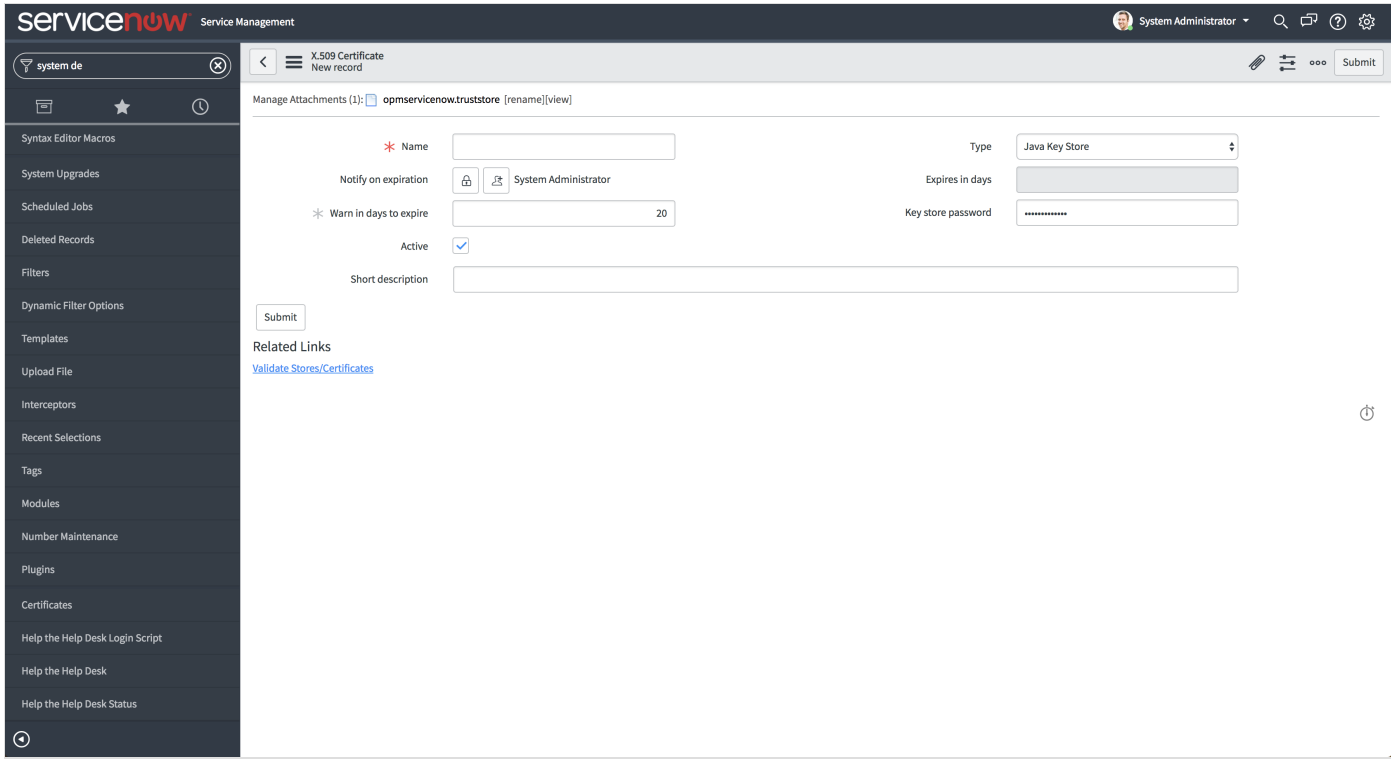
- Go to the ServiceNow Instance and select **System Definition ? Certificates ? New.**
- Select **Type** as **Java Key Store** and provide Truststore Password in the **Key Store Password** field



- Now select the message attachments and add the **opmservicenow.truststore** file.

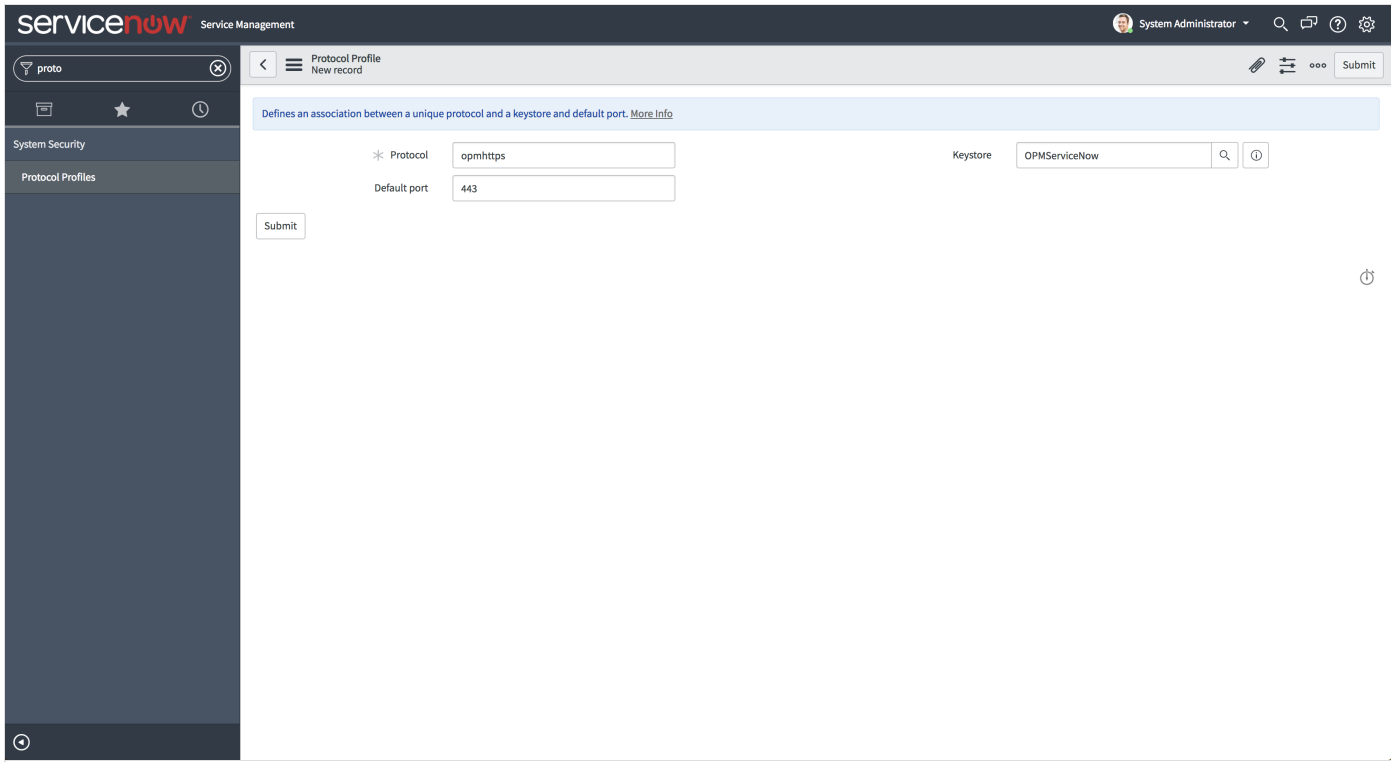


- Validate files before updating using **Validate Stores/Certificates** option and click on **Submit.**.



Step 5: Create a protocol profile in ServiceNow

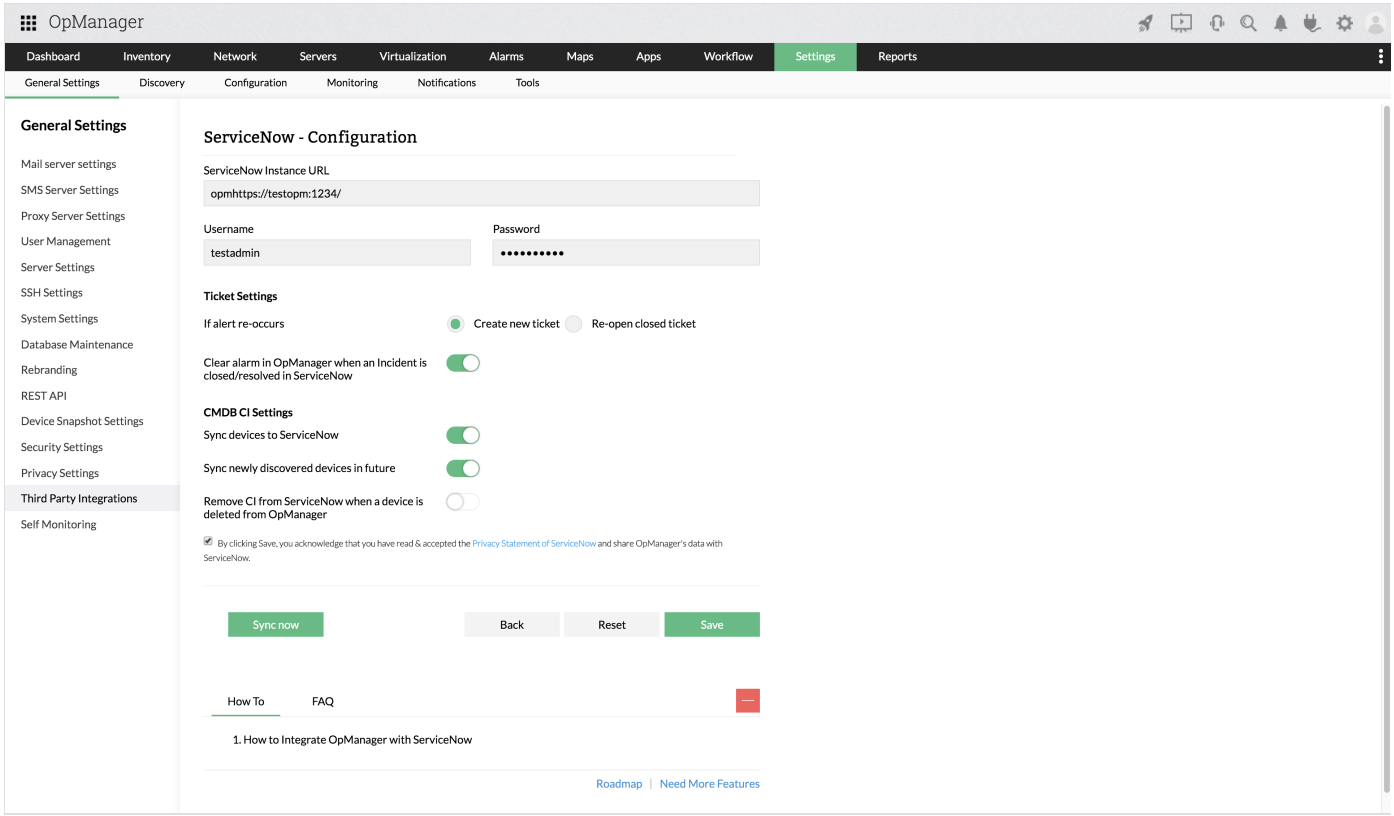
- Go to **ServiceNow Instance ? System Security ? Protocol Profiles ? New**
- Set Protocol field as **opmhttps** and select the previously created Certificate entry in Keystore field and click on **Submit**.



Step 6: Set the OPM host URL in OpManager.

- In OpManager go to **Settings ? General Settings ? Third Party Integrations ? ServiceNow** and click **'Configure'.**
- Provide the ServiceNow instance details, and click **'Save'.** Note that the URL should be of the form **opmhttps:**//*host_name*:*web_port*/ where the *web_port* is OpManager's web port and *host_name* refers to the host name or IP

Address of the OpManager instance.



Integrating Slack with OpManager

Slack is like a chatroom for your whole team. Slack can help your team collaborate and coordinate their work no matter where they are in the field office, at home, or out knocking doors. By integrating Slack with OpManager, you can receive real time notification of the alarms raised in OpManager, even if the administrator is not able to access OpManager.

How to integrate OpManager with Slack?

Steps to integrate Slack:

- After logging into OpManager, In Third Party Integration page under Settings, click on 'Get Auth-Code from Slack' or visit this page and click on 'Add to Slack' button.
- An authorization prompt will be displayed, which will lists all the permissions required for OpManager app to integrate with your workspace.
- Click on "Authorize" button after reviewing all the permissions.
- You will be redirected to another site where the Auth-Code will be provided. Copy this Auth-Code.
- After logging into OpManager, click on 'Settings' ? 'General Settings' ? 'Third Party Integration' settings and select Slack. Paste the 'Auth-Code' in the space provided and click on 'Save'.
- After clicking on save, a success message "Slack details updated successfully" will be displayed stating the successful integration of Slack with OpManager.

Configuring 'Notification profile':

You can create individual notification profiles for easier access to Work groups.

- Navigate to 'Settings' ? 'Notifications' ? 'Notification Profile' ? 'Add' ? 'Chat'.
- Specify the recipient of the Slack message from the options provided.
- Choose the channel or a member to which the message has to be sent to. All the channels and the members present in your workspace will be listed in the drop downs.
- Specify the required fields of the Slack message and click on 'Save' after the notification profile has been configured based on your requirements.

All the alerts raised, which satisfy the "Chat Notification Profile" criteria will be sent to Slack. You can configure different notification profiles based on your requirements.

Configure workflow:

You can automate alerts to be sent to the Slack app by configuring Workflows in OpManager.

- Click on Workflow ? New workflow. Slack will be present under "External actions" in the left pane of the workflow configuration window.
- Drag and drop Slack in order to redirect alerts to Slack workspace after designing the workflow.
- Specify the channel/user, title and the content of the message which should be sent to Slack in the next window.

- Messages can be sent to both individual users or a channel using Workflow.
- All the channels and members present in your workspace will be listed in the drop downs. Select the required channel/user and specify the title and description. Click on 'OK'.
- Set the required criteria and schedule the workflow by clicking on 'Trigger' and save the configuration.
- Alerts will be redirected to Slack based on the workflow execution.

Integrating Microsoft Teams with OpManager

Microsoft Teams is a personal/workplace communication and collaboration platform that helps you stay connected over chat, calls, and video meetings. Using webhook, you can now integrate Microsoft Teams with OpManager. Upon integration, you can receive real time alerts on network faults right in your team channel.

Supported Version: OpManager 12.5.192 & above

Step 1: Configuring MS Teams

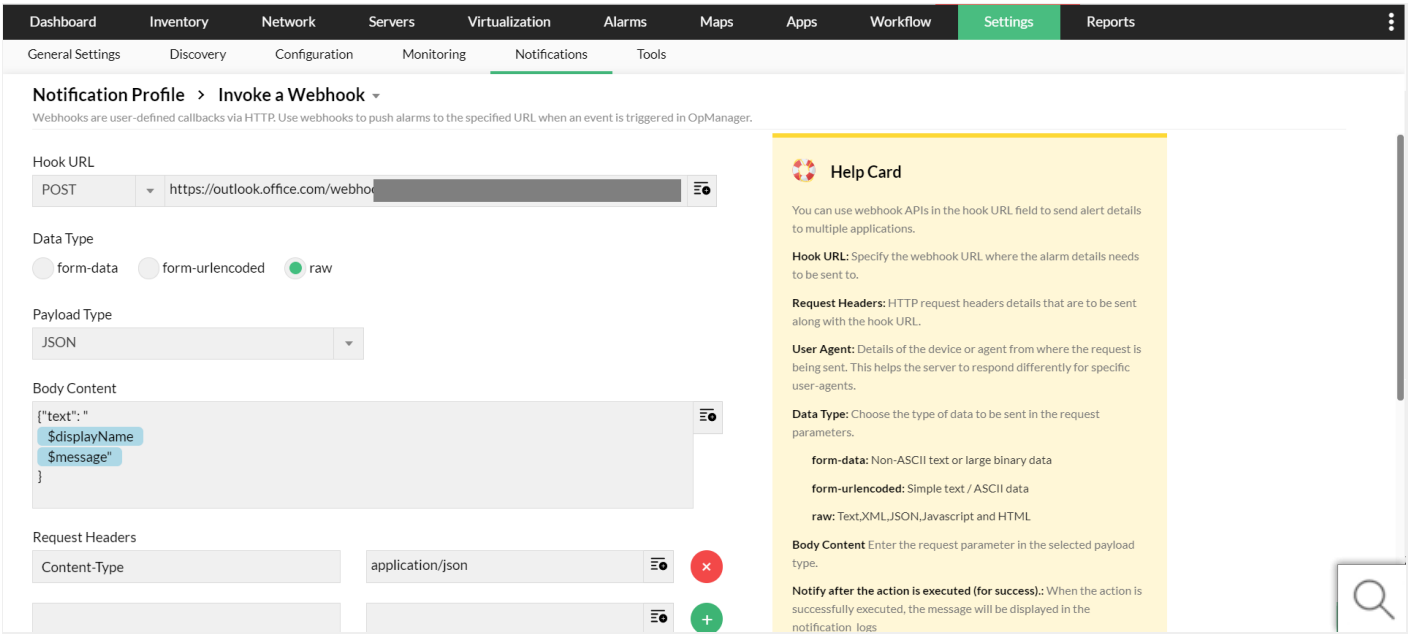
1. Open the required Microsoft Teams channel to which OpManager alert has to be communicated.
2. Click on *More options* (•••) next to the channel name and then choose *Connectors*.
3. Select *Incoming Webhook* from the list of options displayed.
4. In the new window, provide a name for the webhook and click on *Create*.
5. Copy the webhook URL generated by MS Teams.

Step 2: Configuring OpManager

1. In OpManager webclient, go to *Settings* > *Notifications* > *Add Profile.*
2. Choose *Invoke a Webhook*.
3. After selecting HTTP Method POST, paste the webhook URL generated by Microsoft Teams.
4. Choose *raw* as the Data Type and *JSON* as the Payload Type.
5. Under the field Body Content, add the text in the following JSON format:

   a. **{"text": "**
   $displayName
   $message"
   }

6. Add the required alert variables (IP Address, Source of the alarm, etc.,) within the curly braces.



7. Click on *Next*.
8. Select the criteria, filter the devices, and choose your Time Window for which the alerts need to be communicated to MS Teams channel.
9. Finally, provide a name for the webhook notification, and click on *Save*.

Integrating Telegram with OpManager

Telegram is a cloud-based instant messaging, video telephony and VoIP service with end-to-end encryption. Users can send messages and exchange photos, videos, stickers, audio and files of any type in Telegram. Using webhook, you can now integrate Telegram with OpManager and receive instant alerts on networks faults in your Telegram Group.

Supported Version: OpManager 12.5.192 & above

Step 1: Creating a new bot in Telegram

1. In Telegram, search for BotFather. BotFather is a program that helps you create custom bots for your preferences.
2. Enter the command */start*.
3. In the response, click on */newbot*.
4. Follow the responses and provide a custom name and a unique username for your bot.
5. Once the bot is created, a unique **<<token>>** is generated which helps you control the bot.

Step 2: Providing Admin privileges to the newly created bot

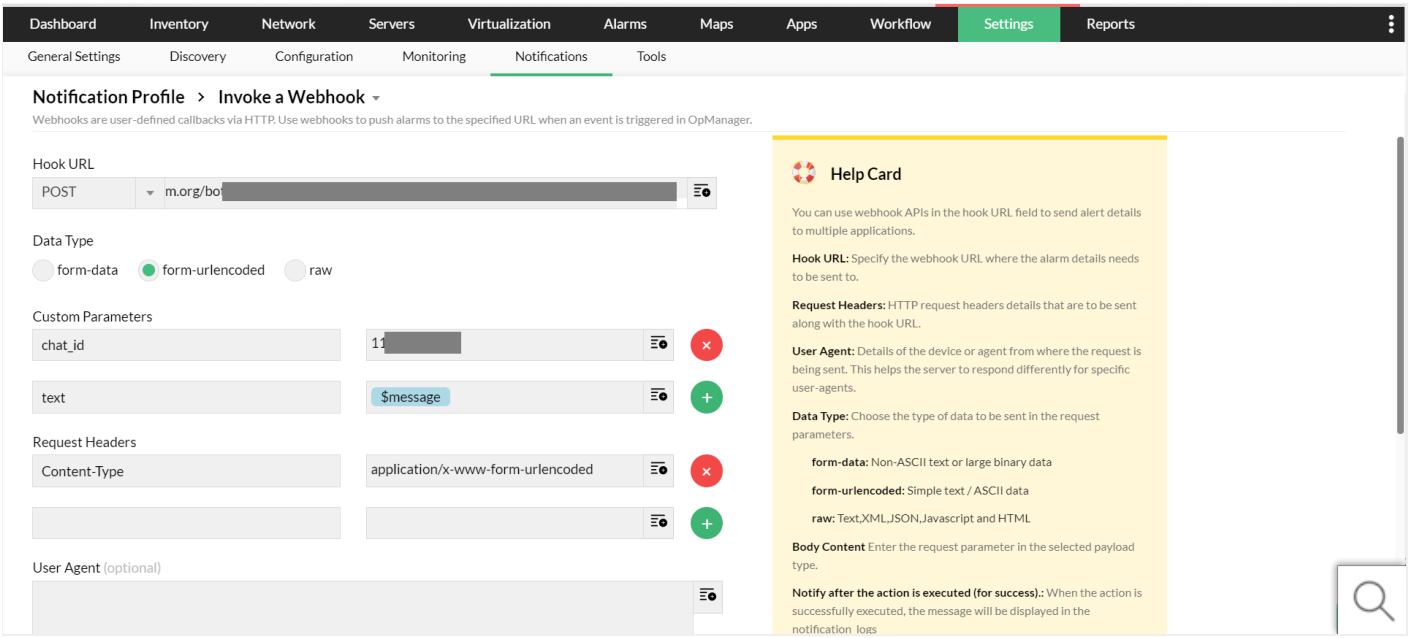
1. Add the newly created bot to the Group to which OpManager alerts have to be notified.
2. Provide Admin privileges to the bot.

Step 3: Retrieving the <<chat_id>> and verifying the <<token>>

1. Hit the request **https://api.telegram.org/bot<<token>>/getUpdates** in your browser.
2. In the response, verify the name of your Group and copy the **<<chat_id>>**
3. To check the **<<token>>**, hit the request **https://api.telegram.org/bot<<token>>/sendMessage?chat_id=<<chat_id>>&text=<<custom_message>>**
4. Check if the **<<custom_message>>** is delivered to your Telegram Group.

Step 4: Configuring webhook in OpManager

1. In OpManager webclient, go to *Settings* > *Notifications* > *Add Profile*.
2. Choose *Invoke a Webhook*.
3. After selecting HTTP Method POST, paste the webhook URL **https://api.telegram.org/bot<<token>>/sendMessage**
4. Choose *form_urlencoded* as the DataType.
5. In the Custom Parameters box,
    1. Type *chat_id* and enter its corresponding value <<chat_id>>
    2. Add another field text and select the required variable such as *Message of the alarm.*
6. Click on *Next*.
7. Select the criteria, filter the devices, and choose your Time Window for which the alerts need to be communicated to the Telegram Group.



3. Finally, provide a name for the webhook notification, and click on *Save*.

Applications Monitoring Plug-in

ManageEngine Applications Monitoring Plug-in is a comprehensive application monitoring software that helps businesses keep track over the performance of critical applications and thereby ensuring high availability. It helps monitoring the performance of various components of an application and provides quick resolution in case of any outages. This improves the quality of service to end-users.

Applications Monitoring plug-in offers out-of-the-box monitoring support for 50+ applications such as such Oracle, SAP, Sharepoint, Websphere and much more.

Installing Applications Monitoring plug-in

Check our installation guide to know the steps to install Applications Monitoring plug-in.

Using Applications Monitoring Plug-in

Click here to access the Applications Monitoring plug-in user guide.

Scheduling Reports

OpManager allows you schedule a new report and also to schedule a generated report.

Schedule a new report

1. From Reports tab, select **Schedule Reports**
2. In thatpage, click the **Add Schedule** button on the top right.
3. Configure the following details:

    - **Choose Report Type**: All the available reports types can be scheduled.
    - Click **Next**.

Scheduling Device specific Availability reports:

If you have chosen to schedule reports for device specific availability details, configure the following:

1. Select either a category of devices, or the required business view, or select specific devices manually for generating the availability reports.
2. Select the period and time window for which you want to generate the reports.
3. Click **Next**.

Scheduling Top N Reports/All Devices reports:

If you have selected to schedule the Top N Reports, configure the following details:

1. **Top N Reports**: Select from Top 10/25/50/100/1000 reports.
2. **Period**: Choose the period and time window for which you want the report scheduled.
3. **Select Report(s)**: Select the required resource reports to be scheduled.
4. **Business View Reports**: Select the relevant check-box and the business view to generate reports specific to the devices in that business view.
5. Click **Next**.

Configuring the Time Settings for generating reports:

1. **Daily**: Select the time at which the reports must be generated every day.
2. **Weekly**: Select the time and also the days on which the reports must be generated.
3. **Monthly**: Select the time, day, and the months for which the reports must be generated.
4. **Report Format Type**: Select either PDF or XLS to receive the report in the respective formats.
5. **Report Delivery**: Select any one of the following options.

    - Configure the email ids to which the reports are to be sent as attachments. [or]
    - Configure the url where the reports can be published.

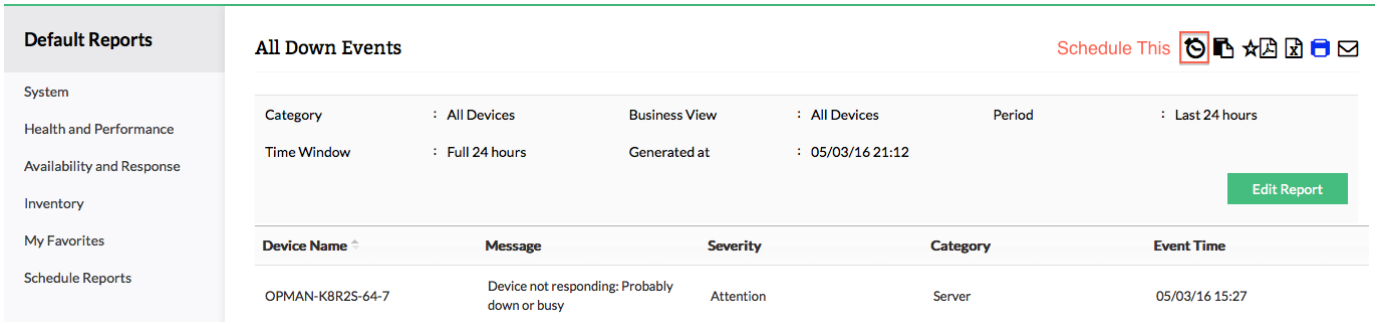
6. Click **Next**.

- **Schedule Name**: Configure a name for the schedule.

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** icon to schedule the report.



2. Enter the schedule name.
3. Enter the email ID to which the report has to be delivered.
4. Select either a category of devices, or the required business view
5. Select the period and time window for which you want to generate the reports.
6. **Report Format Type**: Select either PDF or XLS to receive the report in the respective formats.
7. **Report Delivery**: Select any one of the following options.

    - Send as attachments
    - Send as URL

8. **Daily**: Select the time at which the reports must be generated every day.
9. **Weekly**: Select the time and also the days on which the reports must be generated.
10. **Monthly**: Select the time, day, and the months for which the reports must be generated.
11. Click **Save**.

Enabling the Configured Schedule

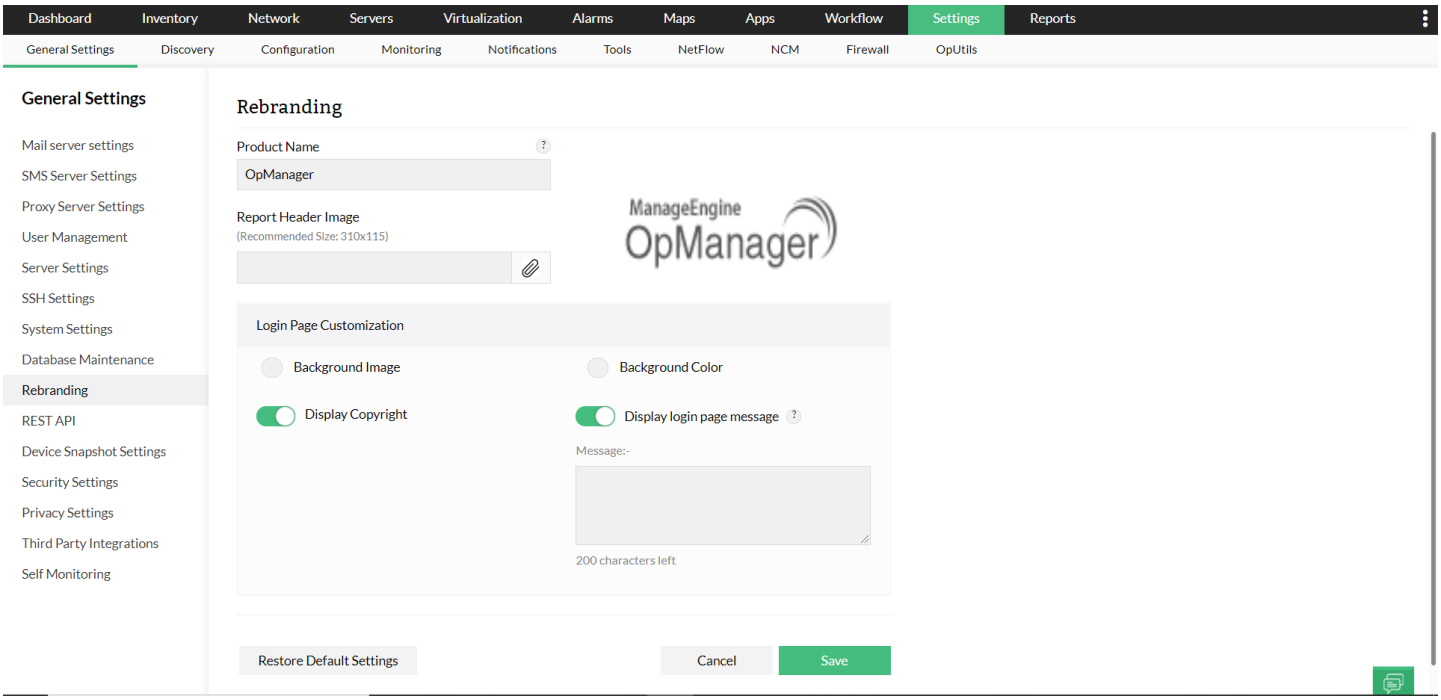
Once you configure the report schedules, they are listed in the Schedule Reports page (Reports > Schedule Reports page). Select the required schedules and click on the **Enable** button at the bottom of the list. You can also disable or delete a schedule from here.

Rebranding OpManager

Rebranding helps you customize OpManager by replacing the OpManager Logo that is displayed in the OpManager web client as well as in the downloaded reports, with your company's logo.

OpManager gives you the flexibility to change the product name, company name and copyright details and also allows you to customize the appearence of your OpManager login page.

To replace OpManager's logo with your Company's logo in the OpManager web client and reports, follow the steps given below.



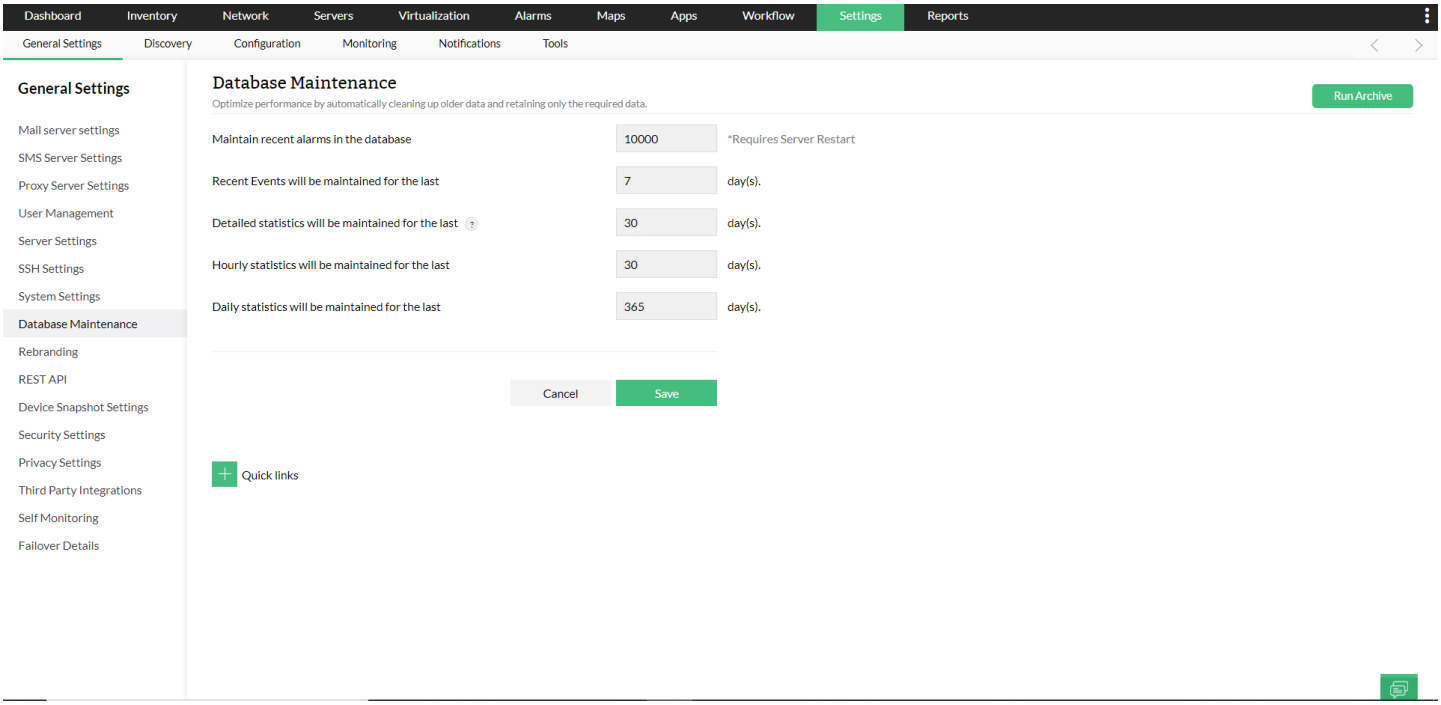
- Go to **Settings > General Settings > Rebranding.**
- Enter the new name in the **Product Name** field.
- Import the new logo under the **Report Header** field.
- Under **Login Page Customization**, customize the appearance of your OpManager login page.
  - To change the **Background Image** or **Background Color**, click on the respective options and upload an image of your choice.
  - Use the toggle buttons to **enable/disable** the **display of copyright information** and **login page message**.
- When the required changes are done, click on **Save.**

Configuring Database Maintenance

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

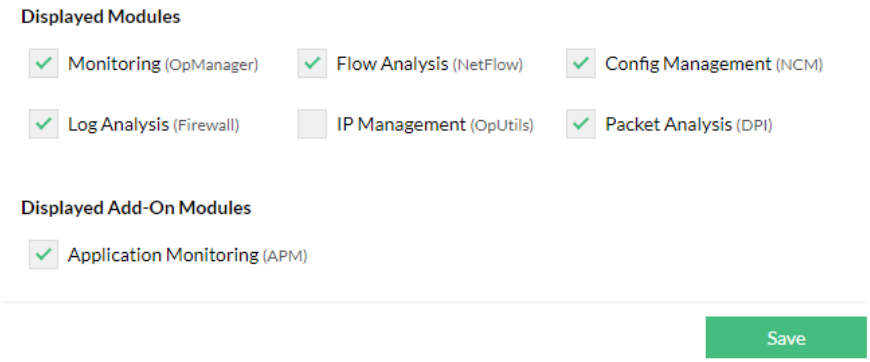
OpManager allows you to maintain the database with the required data. By default, the detailed data will be maintained for 7 days, the hourly data for 30 days and the daily data for 365 days. After the specified period, the database will be cleaned up automatically.

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



1. Click **Settings** → **General Settings** → **Database Maintenance**.
2. Specify the values for the following fields:
    a. **Maintain recent alarms in the database** - the maximum number of recent alarms to be maintained must be specified here. For instance, if you want an history of last 500 alarms, specify the value as 500 here.
    b. **Recent Events will be maintained for the last _ days** - represents the maximum number of days upto which the recent events data will be maintained. By default, it takes a value of 7, i.e., the recent events of the previous 7 days are maintained.
    c. **Detailed statistics will be maintained for the last _ days** - the detailed data will be maintained for 7 days
    d. **Hourly statistics will be maintained for the last _ days** - the hourly data for 30 days
    e. **Daily statistics will be maintained for the last _ days** - the cleanup interval of the raw data as well as the archived data must be specified here.
3. Click **Save** to apply the changes.

Enabling and disabling modules



Admin user can enable or disable displayed modules. Operator user can only view modules that are enabled by the admin user. If the module is disabled, it will no longer be visible to any of the users. This holds good for Add-On modules as well.

To enable/disable module click on **Settings ? General settings ? System Settings,** and select the modules that you would like to be displayed from **'Displayed modules'** and click on **Save**. The enable/disable changes will be applied immediately.

Enabling SSL in OpManager

Steps to enable SSL for OpManager build 8050 upto 123180

In build 8050 we have removed Apache from OpManager. Follow the steps given below to enable SSL:

1. Open a command prompt (Run > cmd) and change directory to /opmanager/bin.
2. Execute the following command
   ssl_gen.bat -f Enable

You have successfully enabled self signed SSL certificate for OpManager. Now you can access OpManager web client in the same port number with **https://**.

Steps to disable SSL:

1. Open a command prompt (Run > cmd) and change directory to /opmanager/bin.
2. Execute the following command
   ssl_gen.bat Disable

This will disable SSL for OpManager. The web client can be accessed in the same port number with **http://**.

Steps to enable SSL for NetFlow plug-in

Steps to enable SSL:

- Open a command prompt (Run > cmd) and change directory to /opmanager/NetFlow/bin.
- Execute the following command

  ssl_gen.bat -f Enable

Steps to disable SSL:

- Open a command prompt (Run-> cmd) and change directory to /opmanager/NetFlow/bin..
- Execute the following command

  ssl_gen.bat Disable

Steps to enable third-party SSL in OpManager

1. Open a command prompt (Run > cmd) and change directory to /opmanager.
2. **Generate a Keystore file.** Execute the following command and provide requested details to create OpManager.truststore file under conf folder.
   >jrebin\keytool.exe -v -genkey -keyalg RSA -keystore confOpManager.truststore -alias opmanager (Press Enter) (OR)
   >jre\bin\keytool.exe -v -genkey -keyalg RSA -keystore conf\OpManager.truststore -alias opmanager -keysize 2048 (for 2048

bit key) **Enter keystore password**:(Enter a password for this keystore. atleast 6 characters long. Press Enter)
What is your first and last name?
[Unknown]: (Enter the Server's name in which OpManager is running. It must be a FQDN [Fully Qualified Domain Name] Ex.: opmserver.manageengine.com. Press Enter.)
What is the name of your organizational unit?
[Unknown]: (Name of your Organization Unit. Ex: SYSADMIN. Press Enter.)
What is the name of your organization?
[Unknown]: (Your Organization Name. Ex:Zoho Corp. Press Enter.)
What is the name of your City or Locality?
[Unknown]: (Your city name. Ex:Pleasanton. Press Enter.)
What is the name of your State or Province?
[Unknown]: (Your state name. Ex:California. Press Enter.)
What is the two-letter country code for this unit?
[Unknown]: (Your country's two letter code. Ex:US. Press Enter.)
Is CN=opmserver.manageengine.com, OU=SYSADMIN, O=Zoho Corp, L=Pleasanton, ST=California, C=US correct?
[no]: (Check the details and if it is correct type yes and press enter. If else just press Enter to modify)
Generating 1,024 bit RSA key pair and self-signed certificate (MD5WithRSA)
for CN=opmserver.manageengine.com, OU=SYSADMIN, O=Zoho Corp, L=Pleasanton, ST=California, C=US
Enter key password for <opmanager>
(RETURN if same as keystore password): (Just press enter. For tomcat both keystore password and key [alias] password must be the same)
[Storing confOpManager.truststore]

3. **Generating CSR File** (Certificate Signing Request). Execute the following commands to create opmssl.csr file under conf folder:
   >jre\bin\keytool.exe -v -certreq -file conf\opmssl.csr -keystore conf\OpManager.truststore -alias opmanager
   Enter keystore password: (Enter the password for the keystore file)
   Certification request stored in file <confopmssl.csr>
   Submit this to your CA
4. **Get certificates from CA** (Certification Authority):
   Contact a CA like Verisign, Equifax, with the csr file generated in the previous step to get ssl certificate. Mostly you have to copy and paste the content of the csr file in a text area of their website. After verifying your request, mostly they will sent you the certificate content through mail. Copy and paste the content in a text editor and save it as "ServerCert.cer" under OpManager_Homeconf folder. Be cautious that while doing copy-paste, no extra space added at the end of lines.
5. **Import root and intermediate certificates:**
   Before importing our certificate, we have to import the CA's root and intermediate certificates into the keystore file we generated at the second step. While mailing you the certificate, CA's will mention the link to their root and intermediate certificates. Save them under conf directory in the name "CARoot.cer" and "CAIntermediate.cer" respectively. Some CAs may have two or more intermediate certificates. Refer their document clearly before importing.

   To import root certificate:
   >jre\bin\keytool.exe -import -trustcacerts -file conf\CARoot.cer -keystore conf\OpManager.truststore -alias CARootCert
   Enter keystore password: (Enter the keystore password)
   (Root Certificate's information will be printed)
   Trust this certificate? [no]: (type yes and press enter if it is the certificate of your CA)
   Certificate was added to keystore

   To import intermediate certificate:
   >jre\bin\keytool.exe -import -trustcacerts -file conf\CAIntermediate.cer -keystore conf\OpManager.truststore -alias CAInterCert
   Enter keystore password: (Enter the keystore password)
   Certificate was added to keystore

6. **Import Server's Certificate.** Execute the following command to add the certificate received from CA to the keystore file:
   >jre\bin\keytool.exe -import -trustcacerts -file conf\ServerCert.cer -keystore conf\OpManager.truststore -alias opmanager
   Enter keystore password: (Enter the keystore password)

Certificate reply was installed in keystore

7. **Configure Tomcat:**

    1. **Open "ssl_server.xml" file (under OpManager_Hometomcatconfbackup) in a text editor.**
    2. **Search for term "keystoreFile". It will be an attribute for connector tag. Set the value as "WEBNMS_ROOT_DIR/conf/OpManager.truststore".**
    3. **Change the value for "keystorePass" attribute with your keystore file password.**

8. **Modify conf file:**

    1. Open "OpManagerStartUp.properties" file (under OpManager_Homeconf) in a text editor.
    2. Set the value of the parameter "https" as "Enable".

9. Start OpManager server. Connect client with https. Ex:https://opmserver:80

Note:

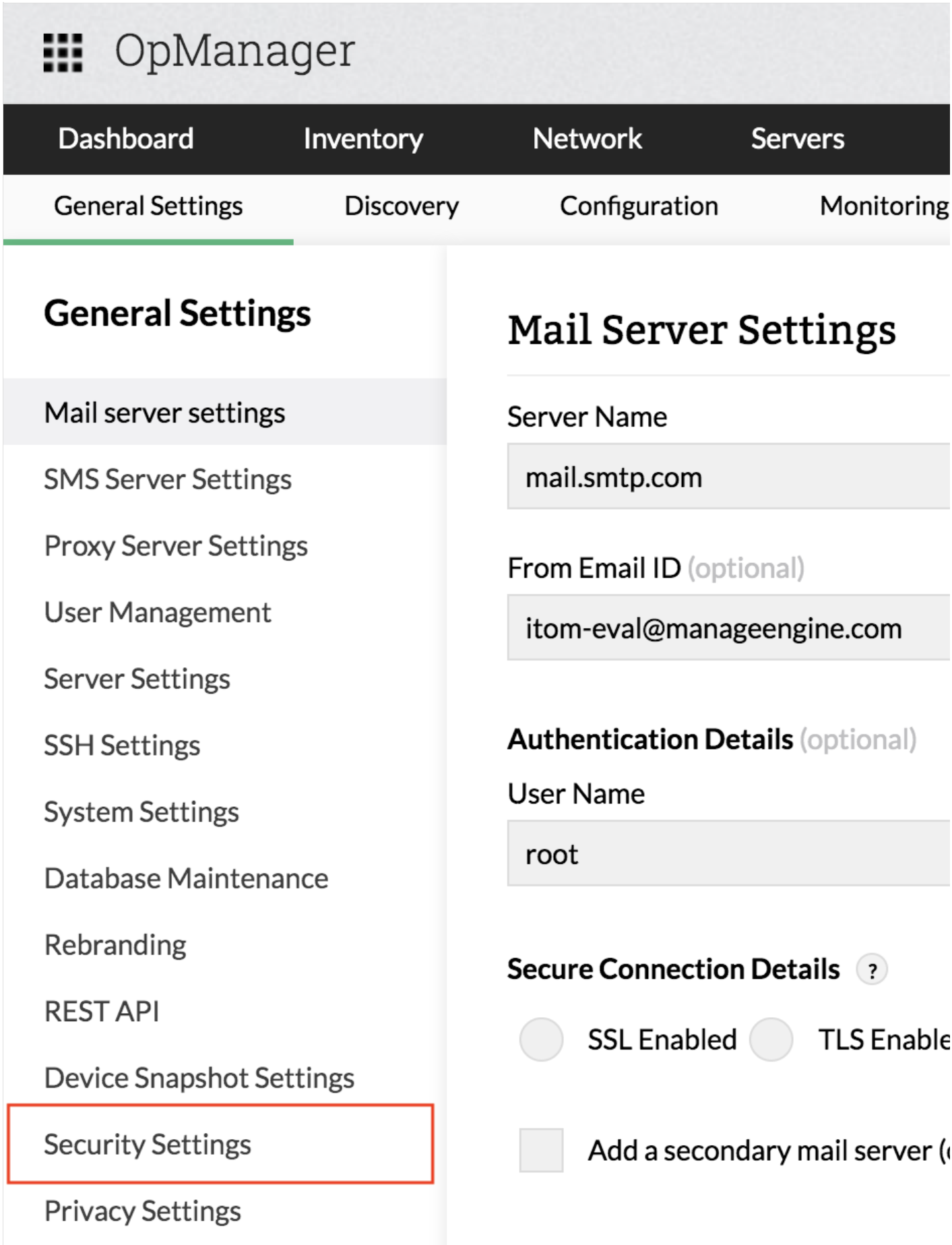
If you are already having a certificate for this server and that certificate was requested by the keystore file generated using Java keytool, you may use it for SSL configuration. Just copy and paste the keystore file under OpManager_Homeconf and rename it to "OpManager.truststore" and follow the steps from 5.

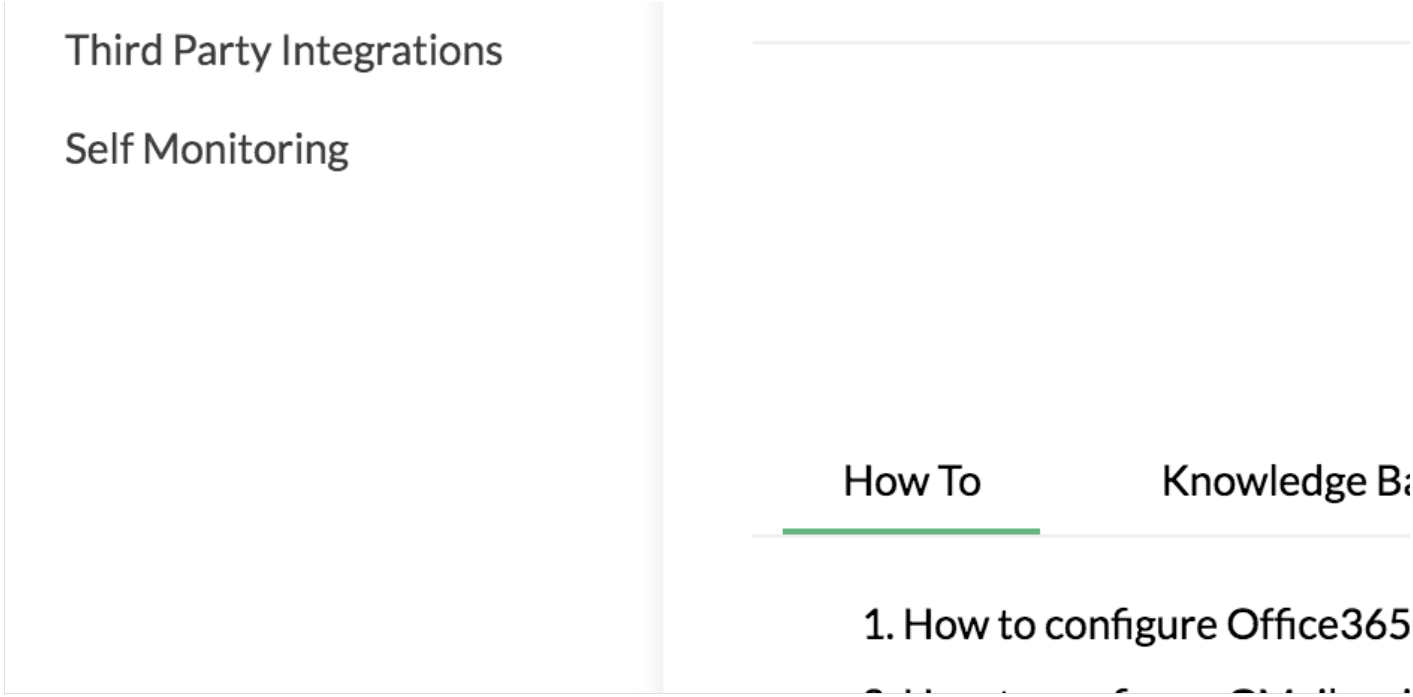
(Provide full path of conf\OpManager.truststore ex: c:\ProgramFiles\Manageengine\OpManager\conf\OpManager.truststore instead of conf\OpManager.truststore on all locations above)

Enabling HTTPS Configuration

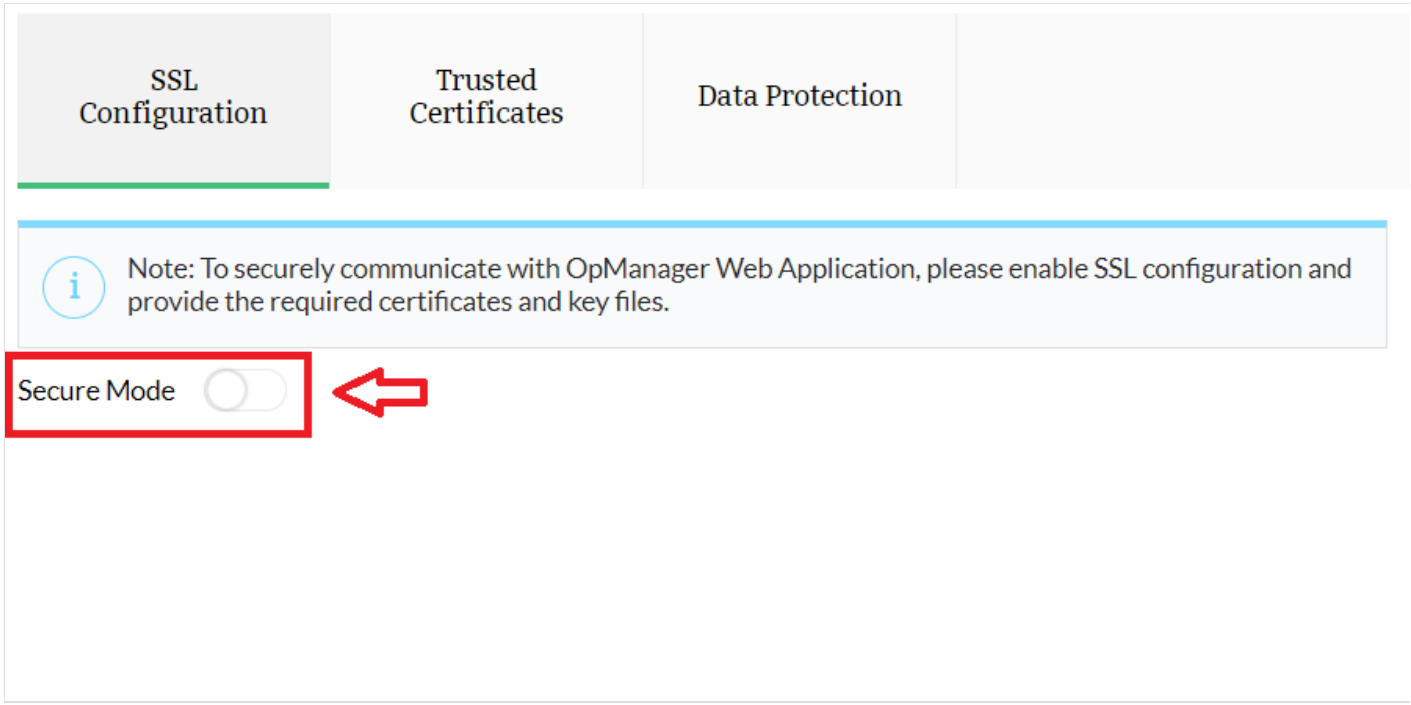
Steps to enable HTTPS in OpManager: (for version 123181 and above)

1. Go to Settings ? Basic Settings ? Security Settings.



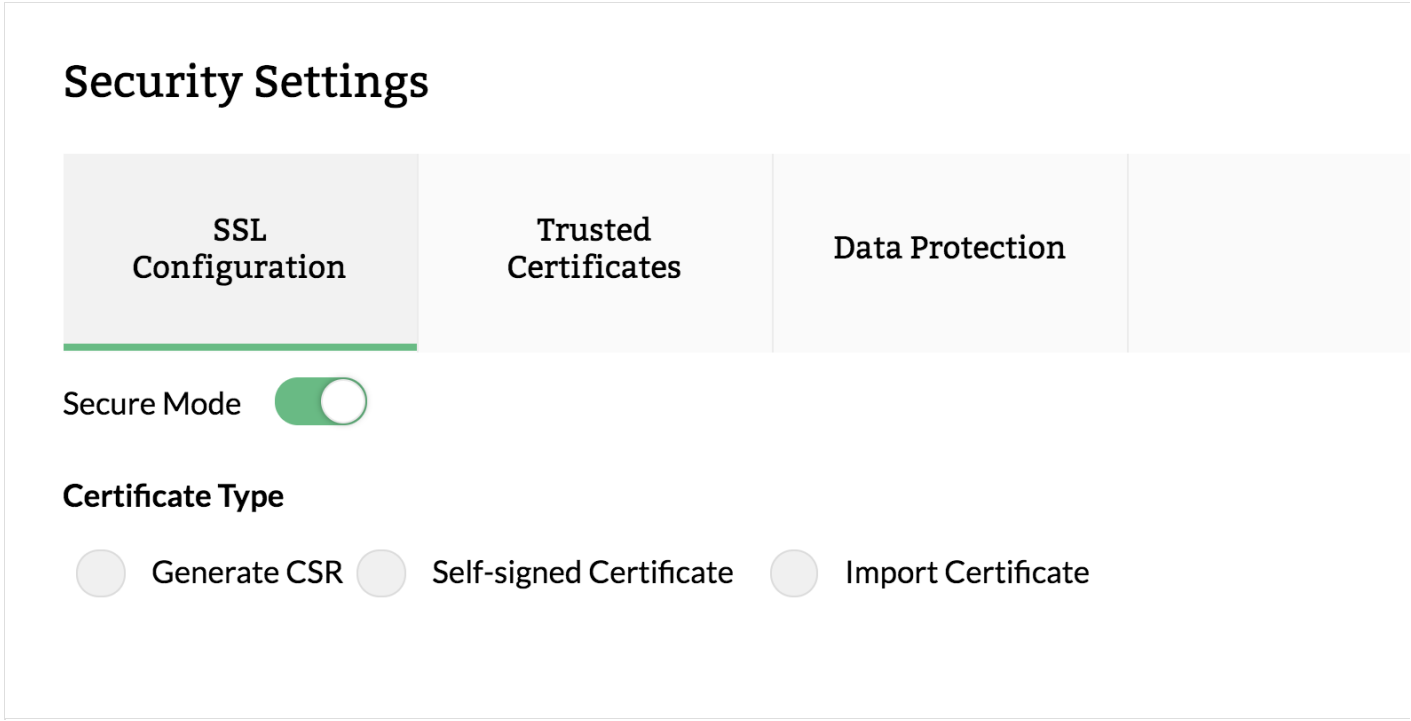


2. Enable the "Secure Mode" button.



3. Once the button is enabled, you will be prompted to choose from three options, namely:

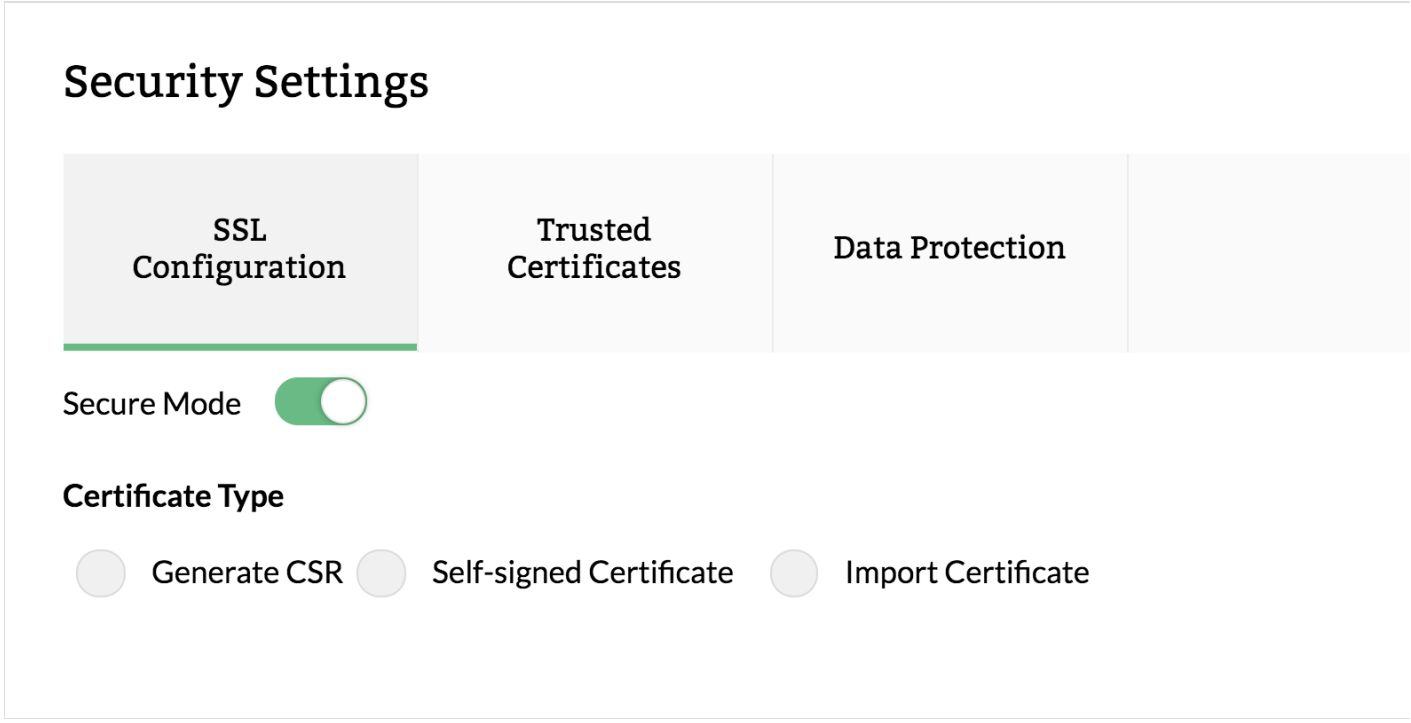
- Generate a CSR
- Self-signed Certificate
- Import Certificate



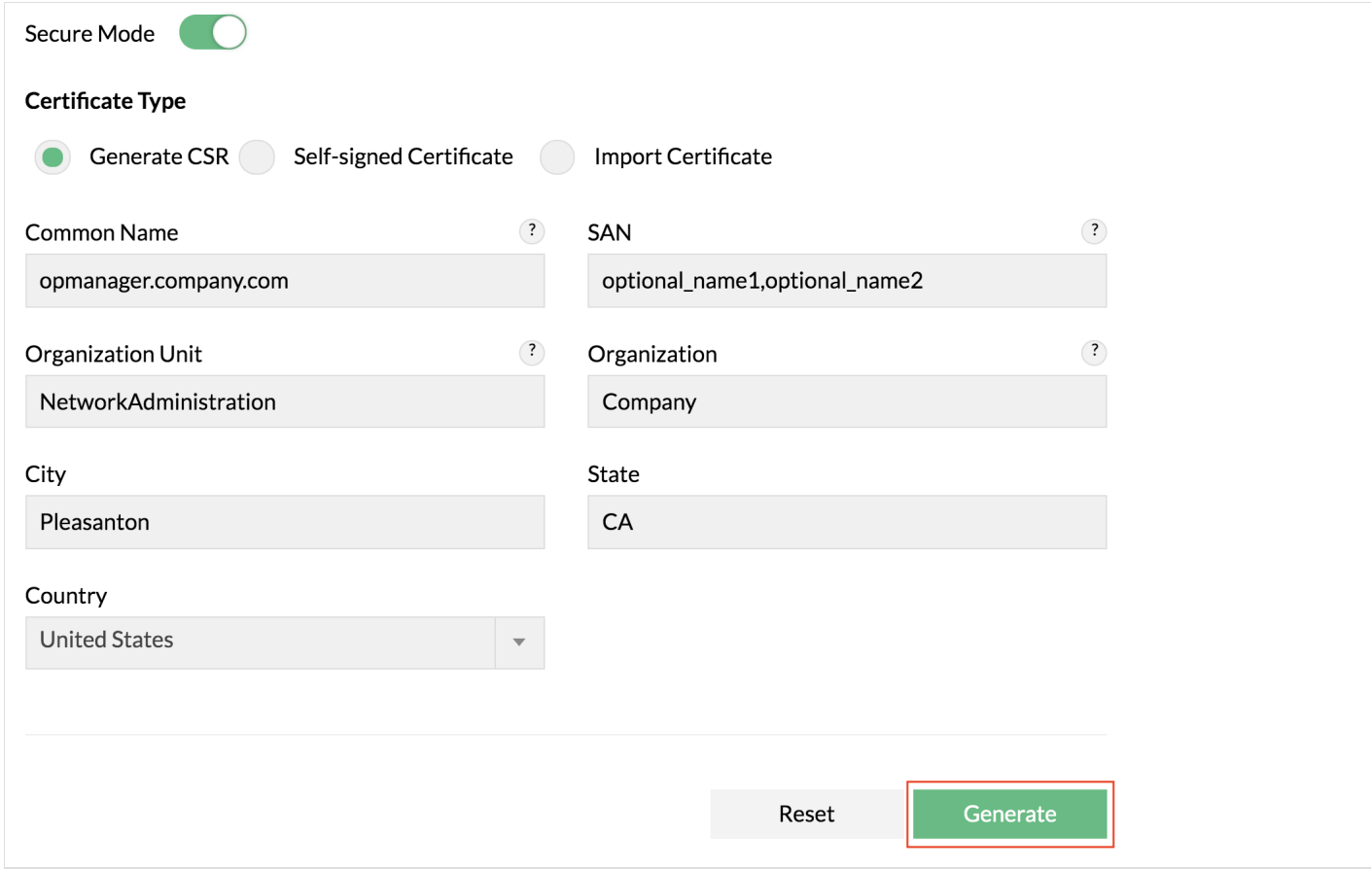
4. **Generate CSR:**

   This option helps you generate a Certificate Signing Request (CSR). A CSR or Certificate Signing request is a block of encoded text that is given to a Certificate Authority when applying for an SSL Certificate. It is usually generated on the server where the certificate will be installed and contains information that will be included in the certificate such as the organization name, common name (domain name), locality, and country. It also contains the public key that will be included in the certificate. A private key is usually created at the same time that you create the CSR, making a key pair. A CSR is generally encoded using ASN.1 according to the PKCS #10 specification.

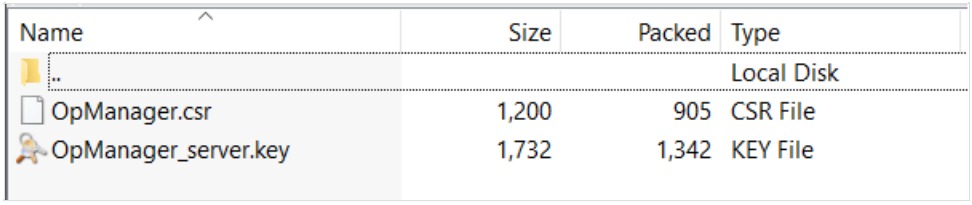
5. A certificate authority will use a CSR to create your SSL certificate, but it does not need your private key. You need to keep your private key secret. The certificate created with a particular CSR will only work with the private key that was generated by it. So if you lose the private key, the certificate will no longer work.



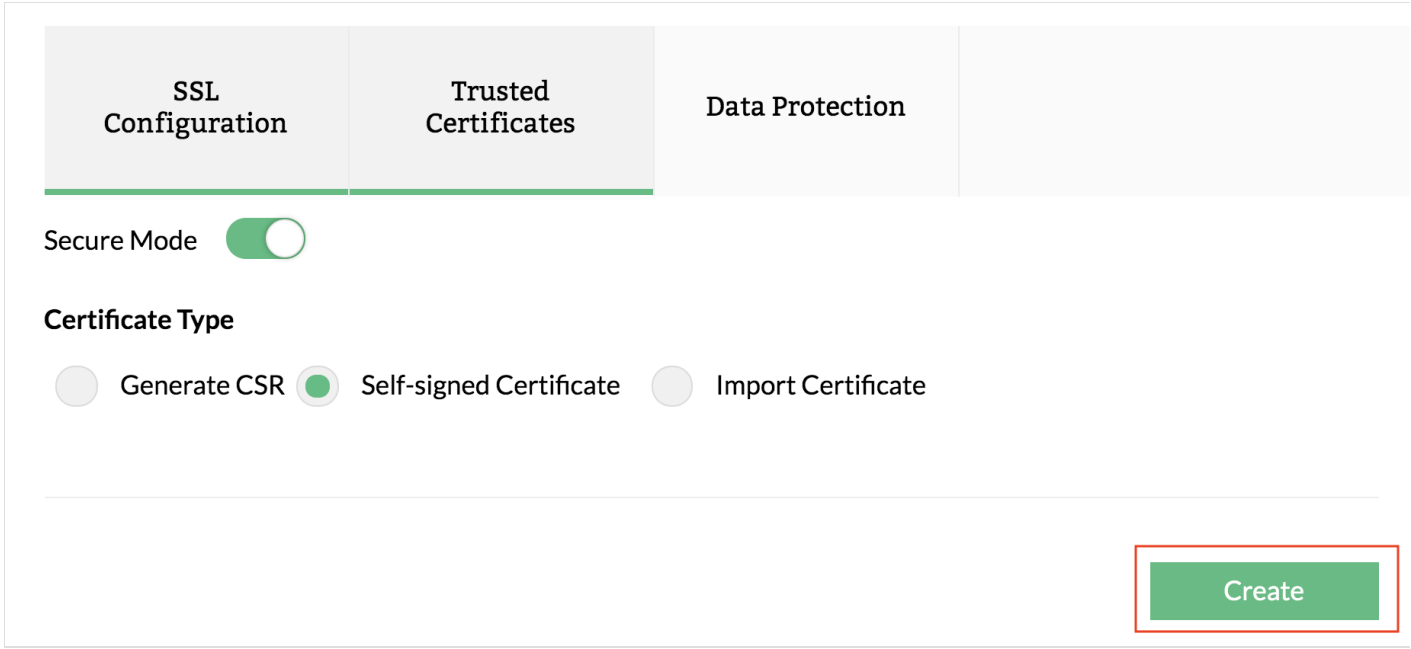
6. Once you click on **'Generate CSR'**, you will have to fill out a few information for the certificate you want to create for use in OpManager Server.



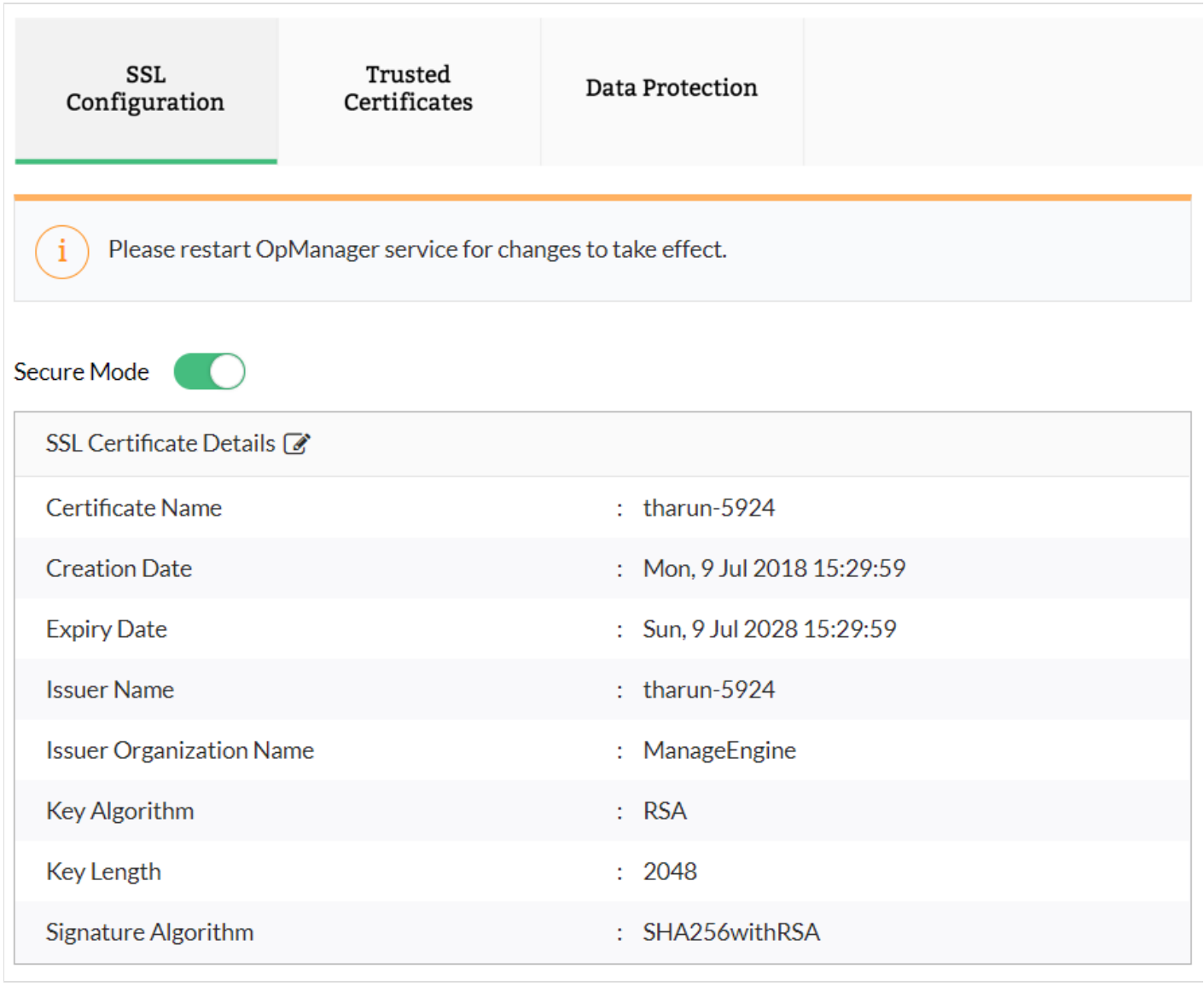
7. On clicking the Generate button, your CSR and Server Key files will be downloaded as a ZIP file. Extract the file and use the "OpManager.csr" file to get a signed certificate from a CA of your choice.



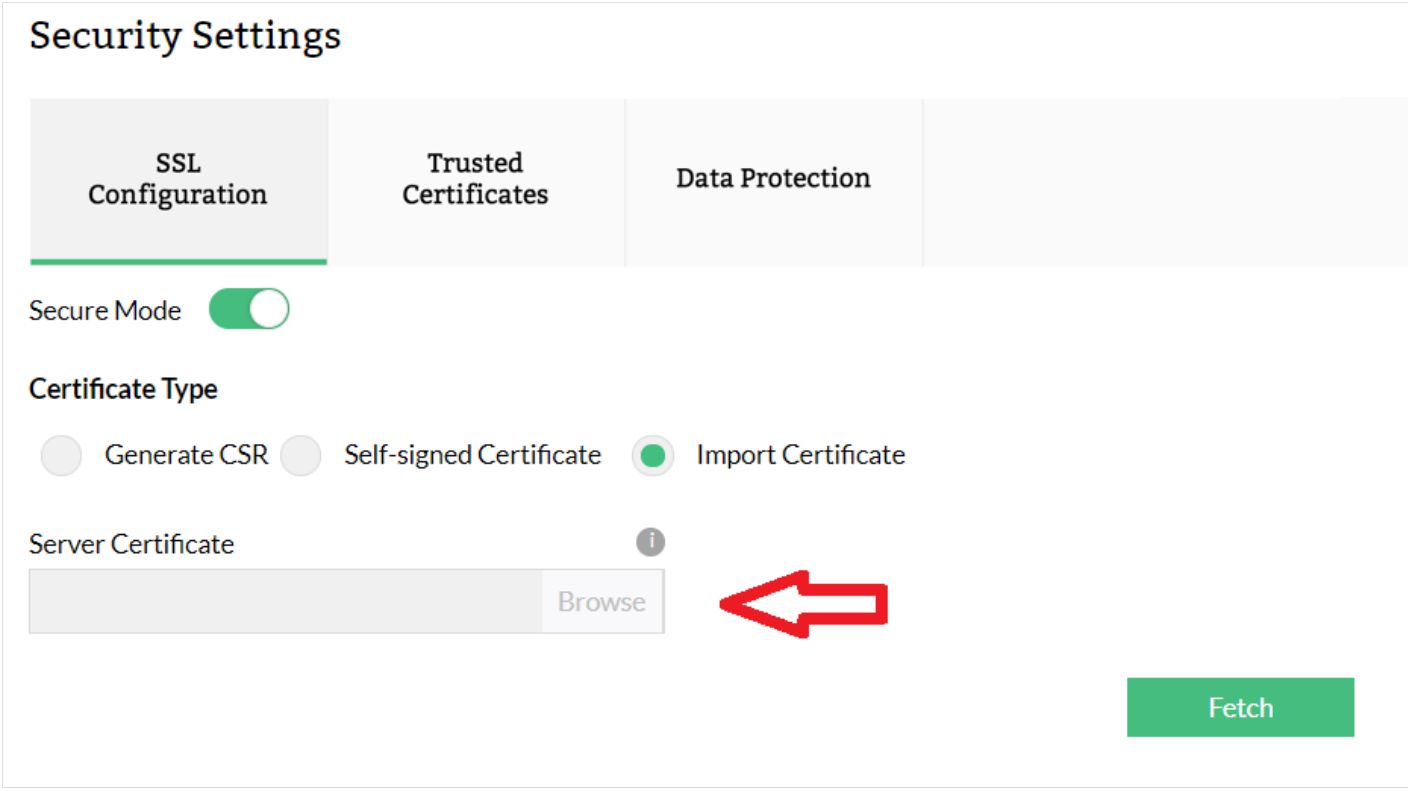
8. After getting signed by the CA, you will get a certificate file which you can import into OpManager using the Import Certificate option discussed below.
9. **Self-Signed Certificate:** This option lets you enable SSL in OpManager with a self-generated and self-signed certificate. This certificate is safe to use and is equally secure. But browsers may display them as untrusted since it is not signed by a Valid CA (Certificate Authority).



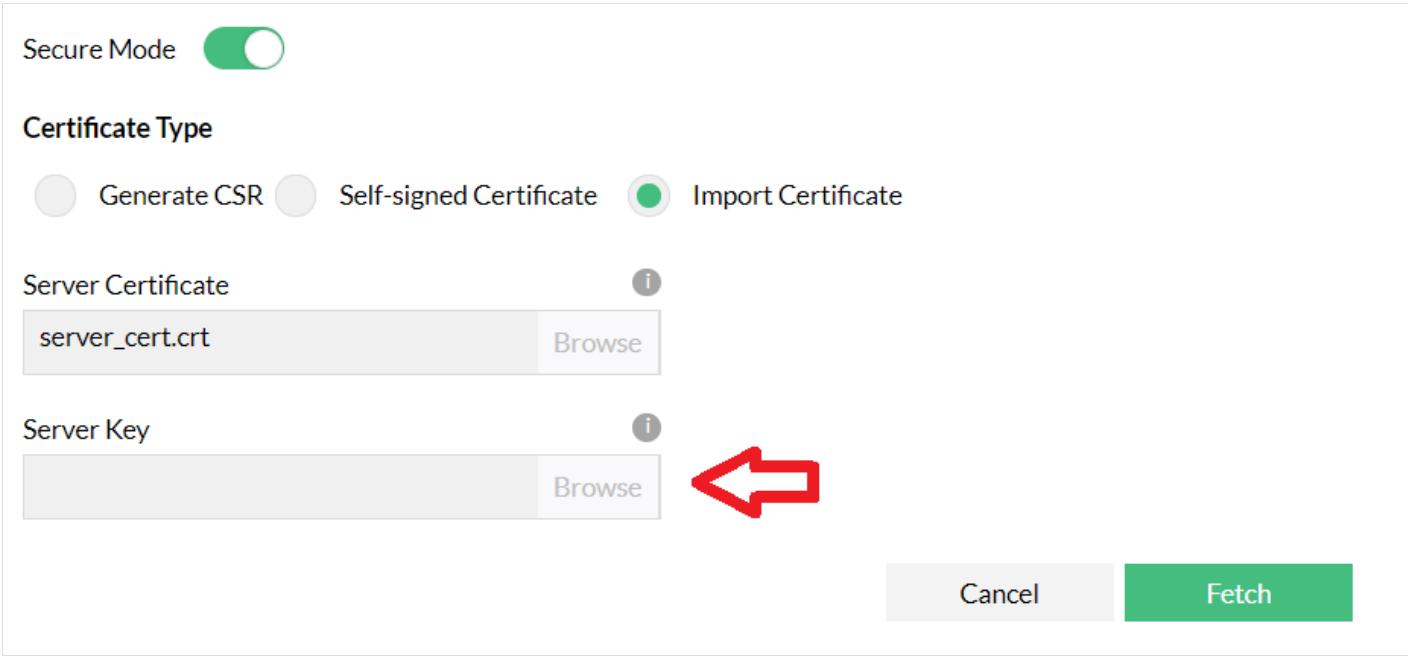
). You will be prompted to restart OpManager for the changes to take effect.



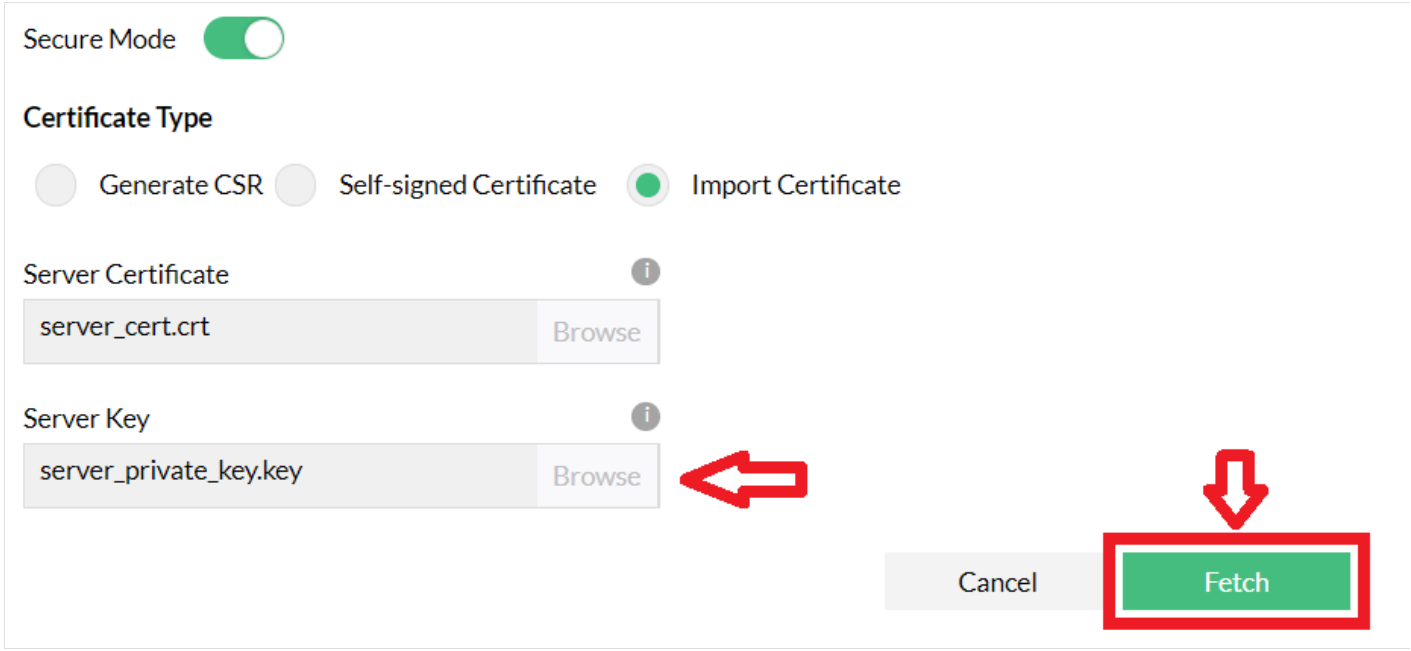
1. **Import Certificate:**
   Use this option if you already have a valid certificate and key files (or) a keystore or a PFX file with the certificate.



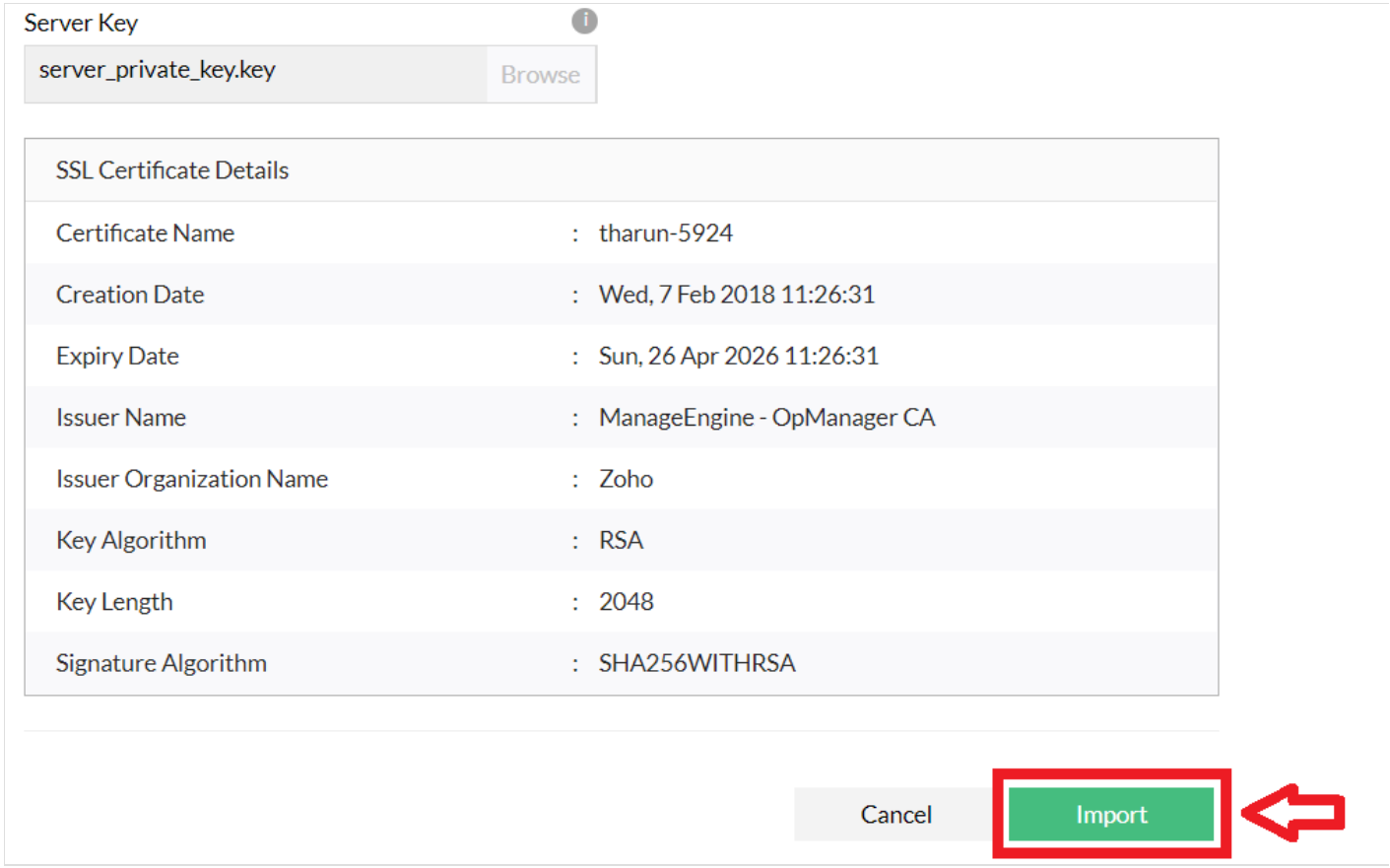
2. Select a certificate file.



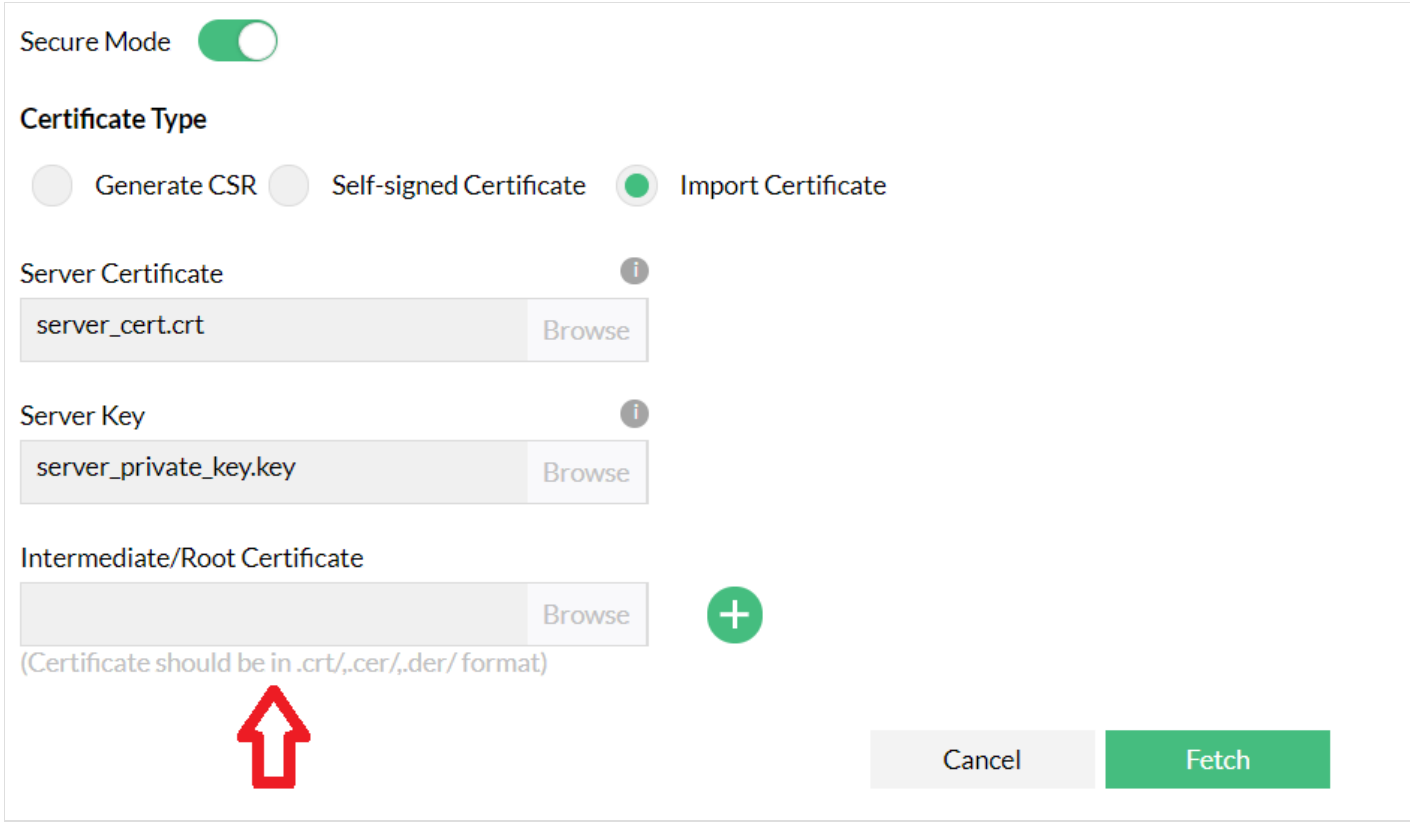
3. Select the appropriate "key" file.



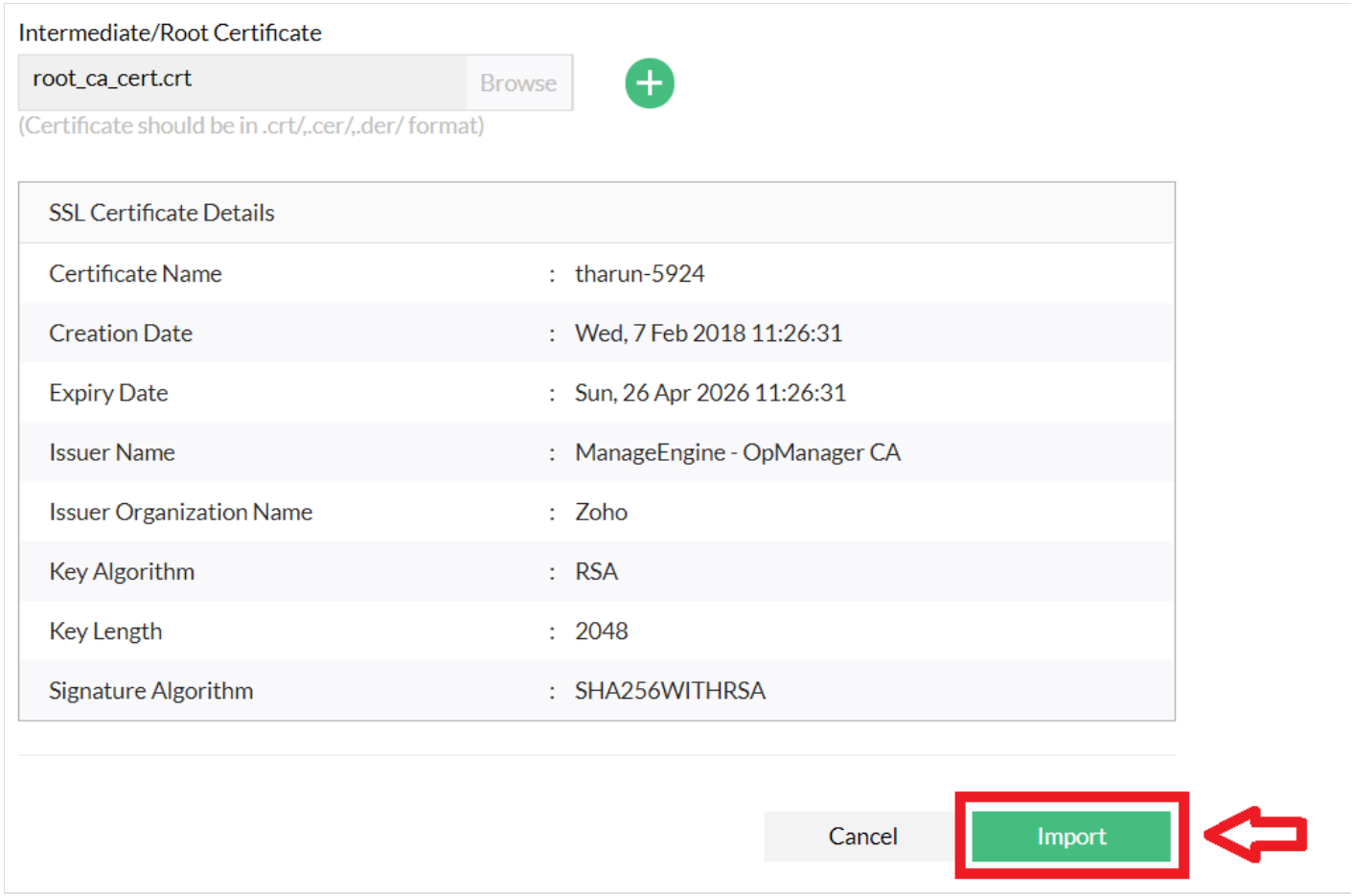
4. Verify and choose **Import**.



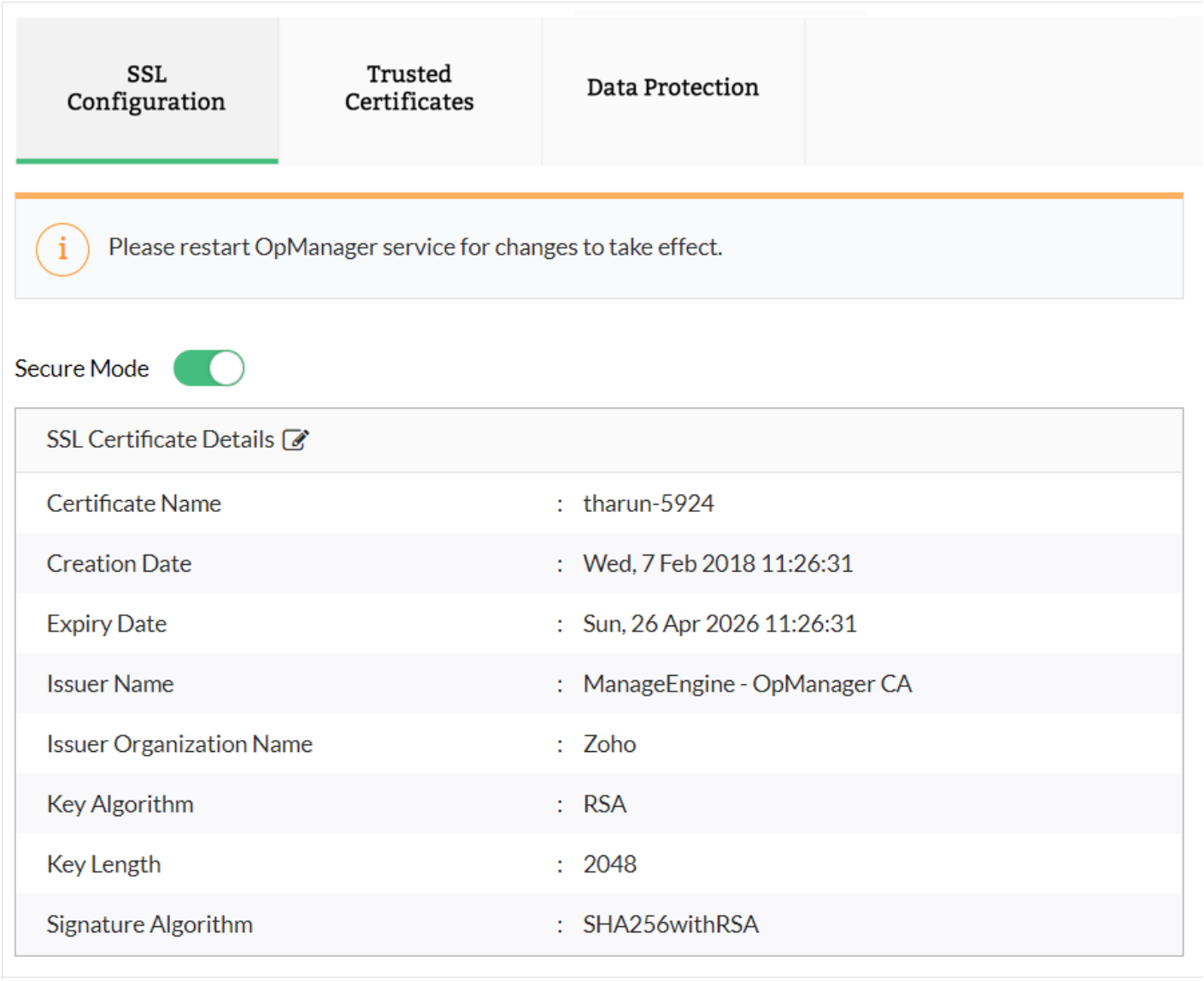
5. If the certificate cannot be validated with trusted sources, you will be asked to provide the intermediate certificates and root certificate files.



5. Once uploaded, verify the certificate and click **Import**.

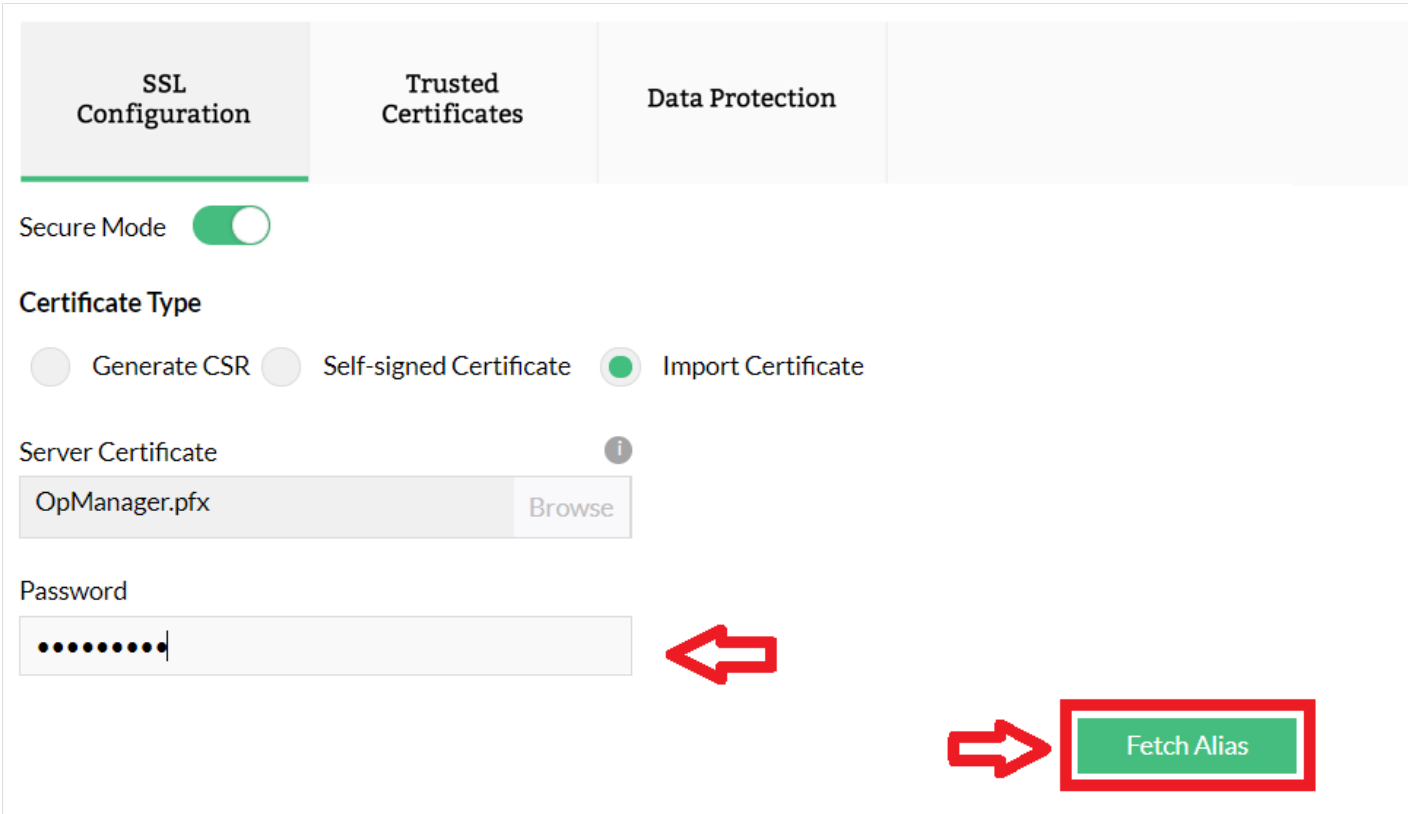


7. On successful import, you will be prompted to restart OpManager.

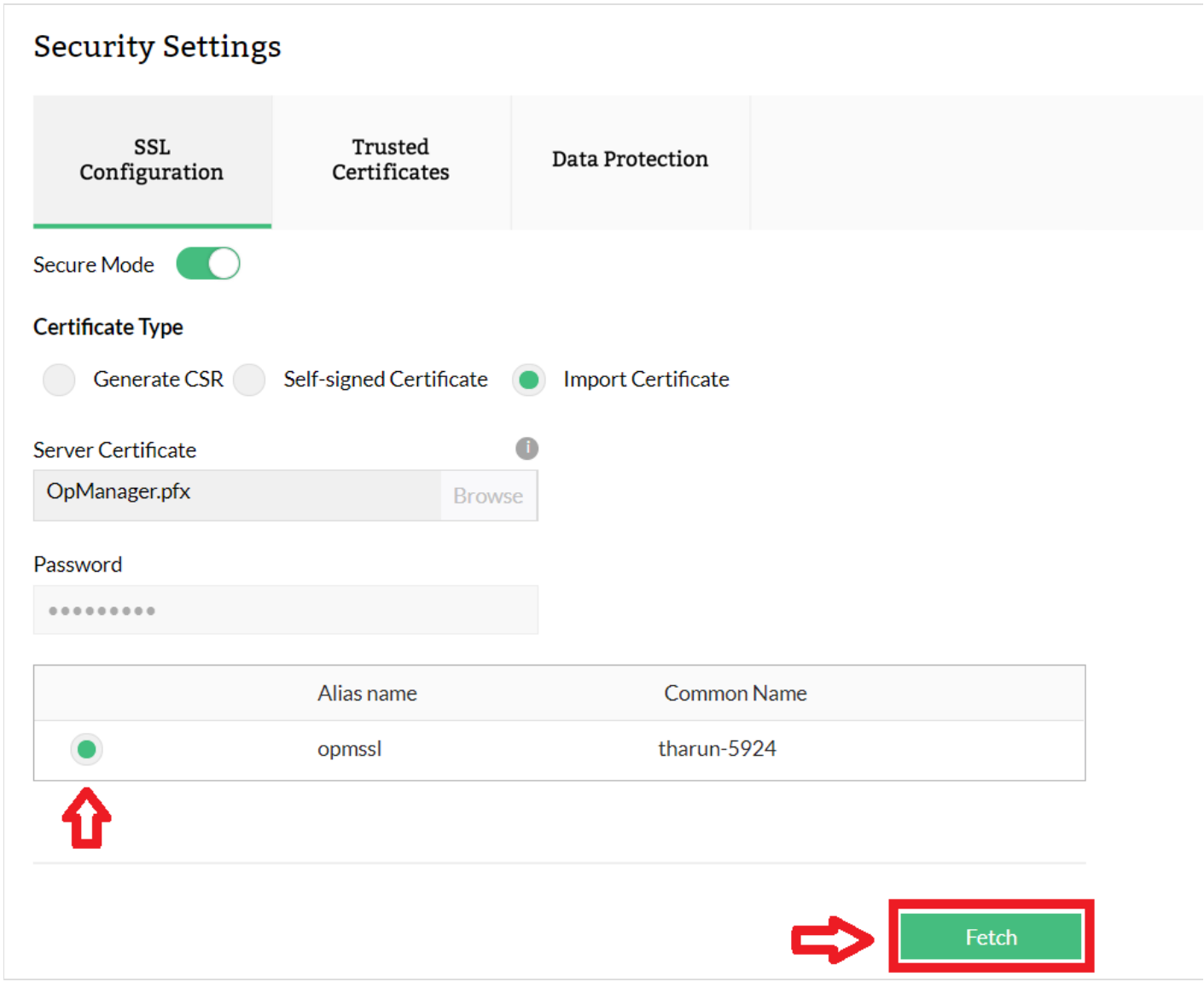


3. **Importing from PFX or Keystore:**

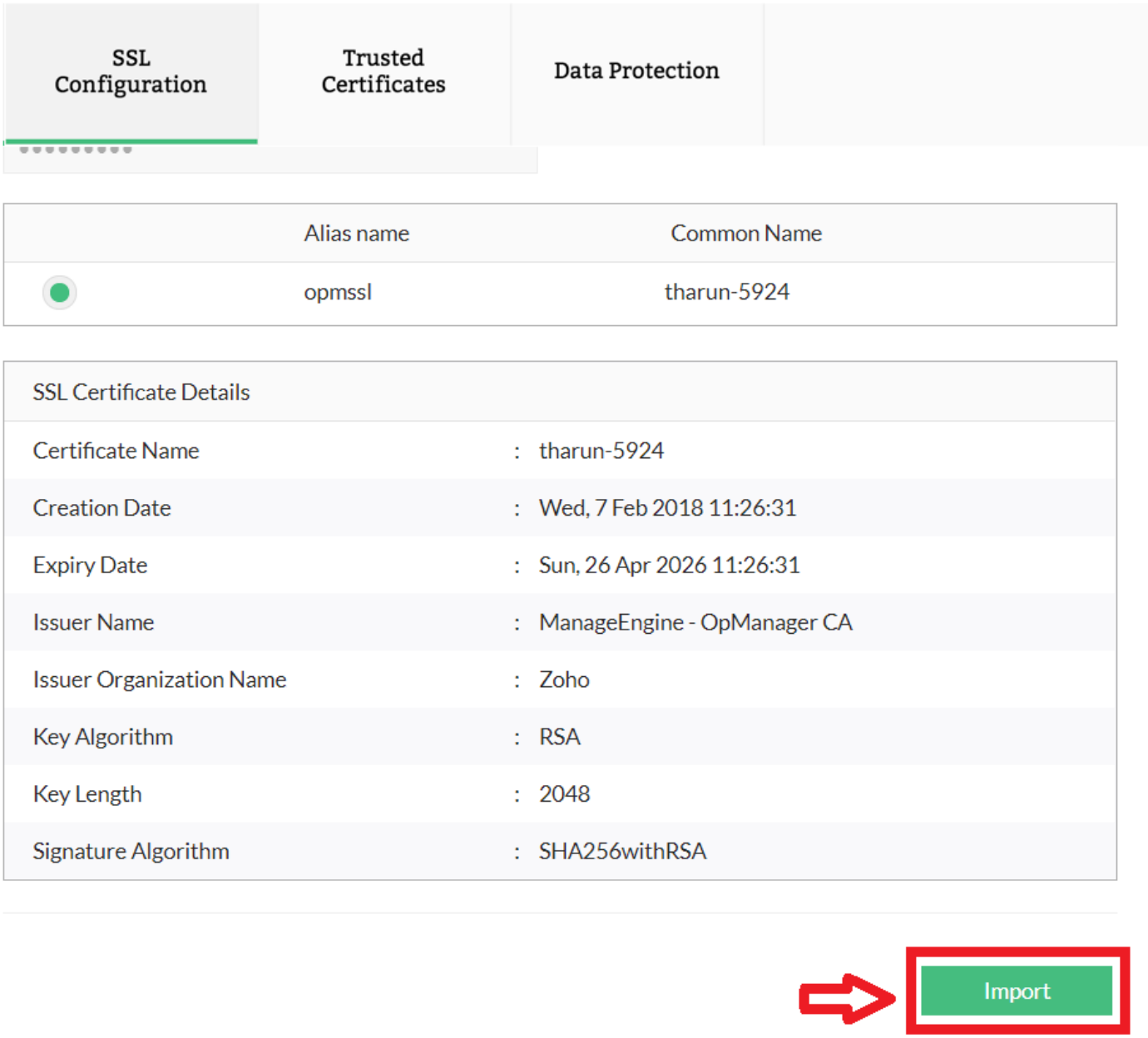
If you are using a Keystore or a PFX file, you will be prompted to input the password for opening the file.



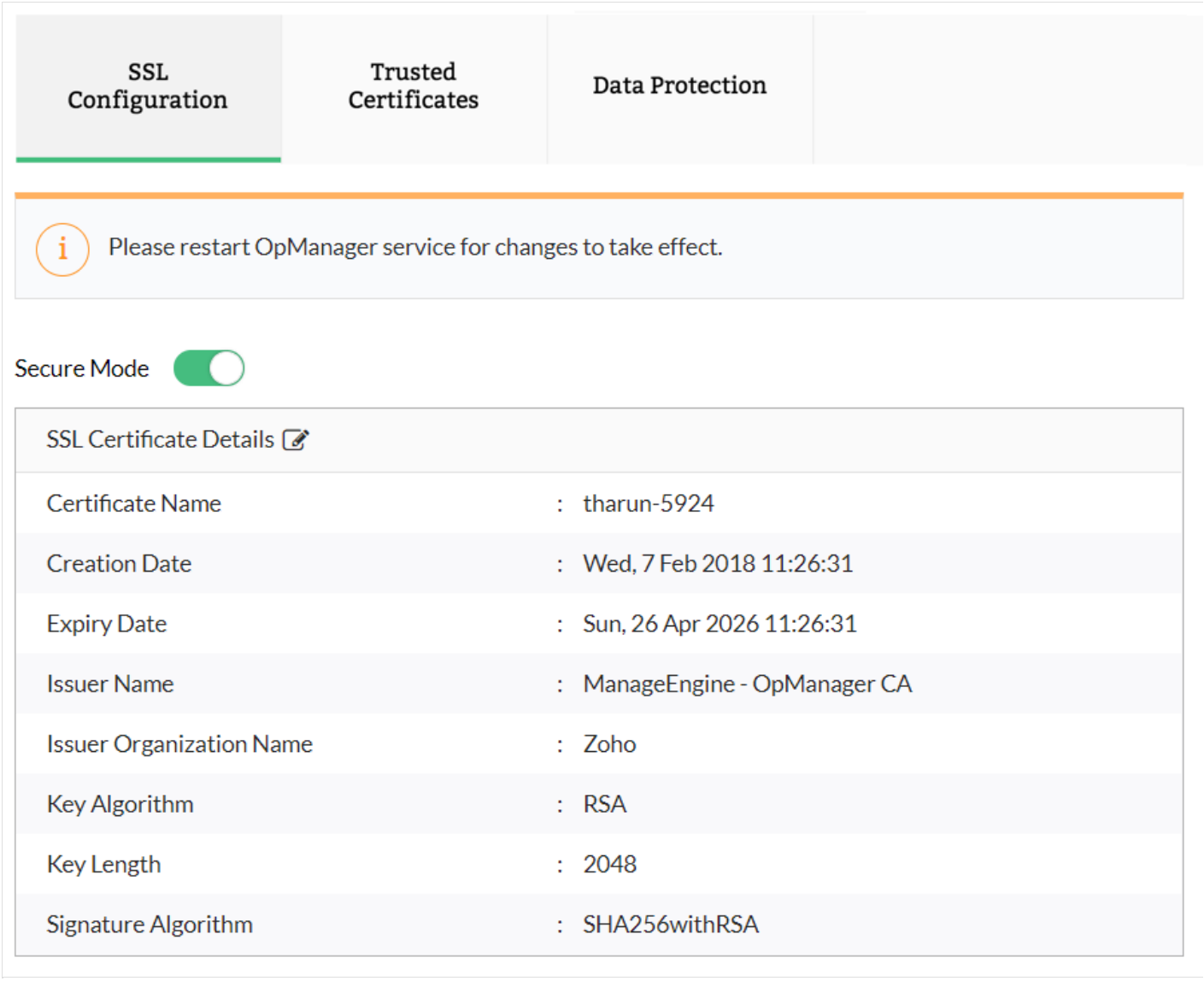
9. On clicking Fetch, you will be provided with a list of Key-entries present in the keystore. Choose a specific alias which is to be used to enable SSL in OpManager.



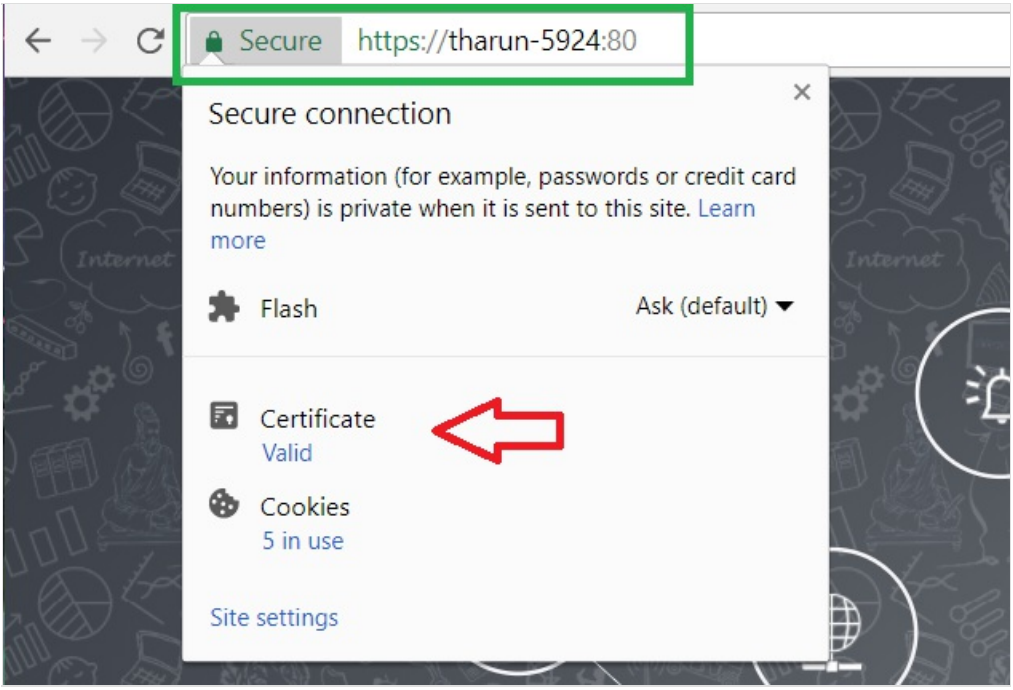
10. You will be shown a preview of the certificate information, verify and click on **Import** for using the certificate.



1. Finally you will be prompted to restart OpManager for the changes to take effect.



2. Finally, after enabling SSL through one of the above ways, you will be able to connect to OpManager in secure mode:

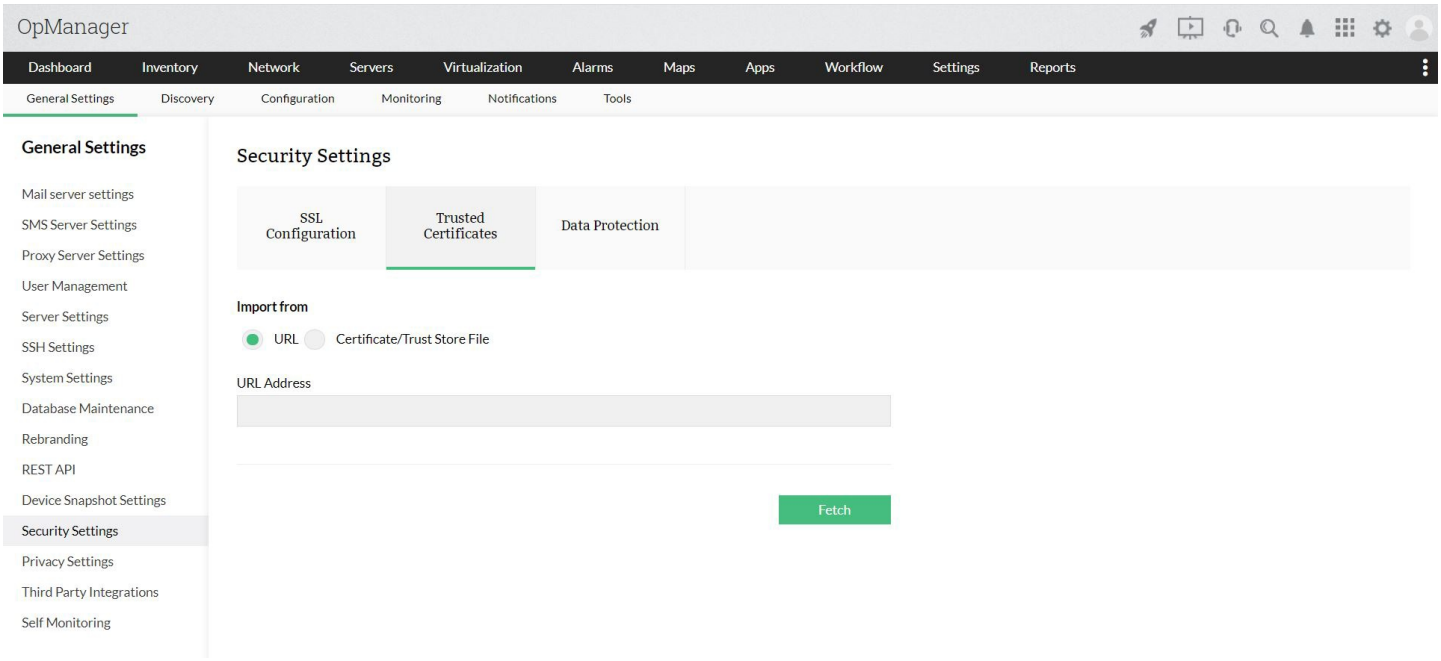


Importing Trusted Certificates in OpManager

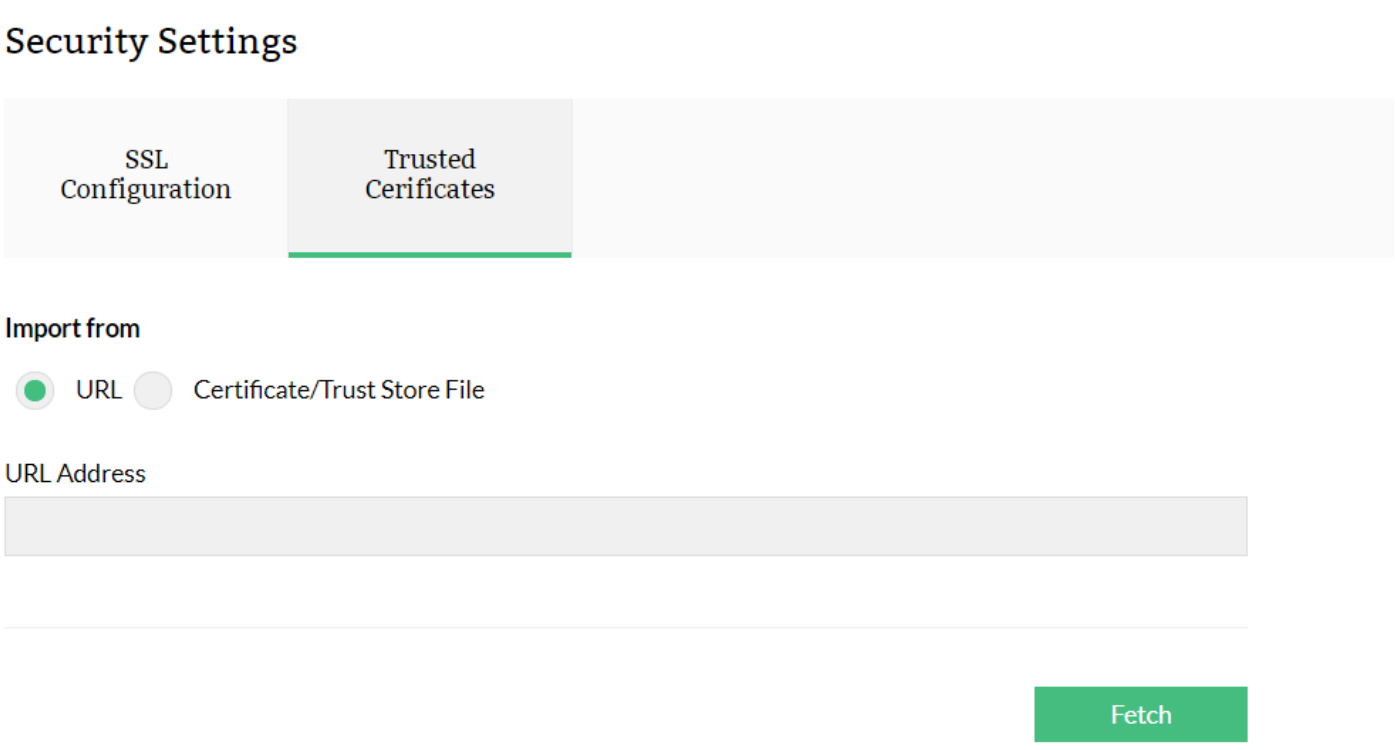
OpManager validates the trusted sources with the help of certificates in OpManager trust store. By default OpManager trusts all major CA signed certs. If a specific certificate or service has to be trusted, the certificate has to be added to this truststore.

Note: These steps are only applicable for OpManager versions 123181 and above.

1) Navigate to Settings-> General Settings-> Security Settings



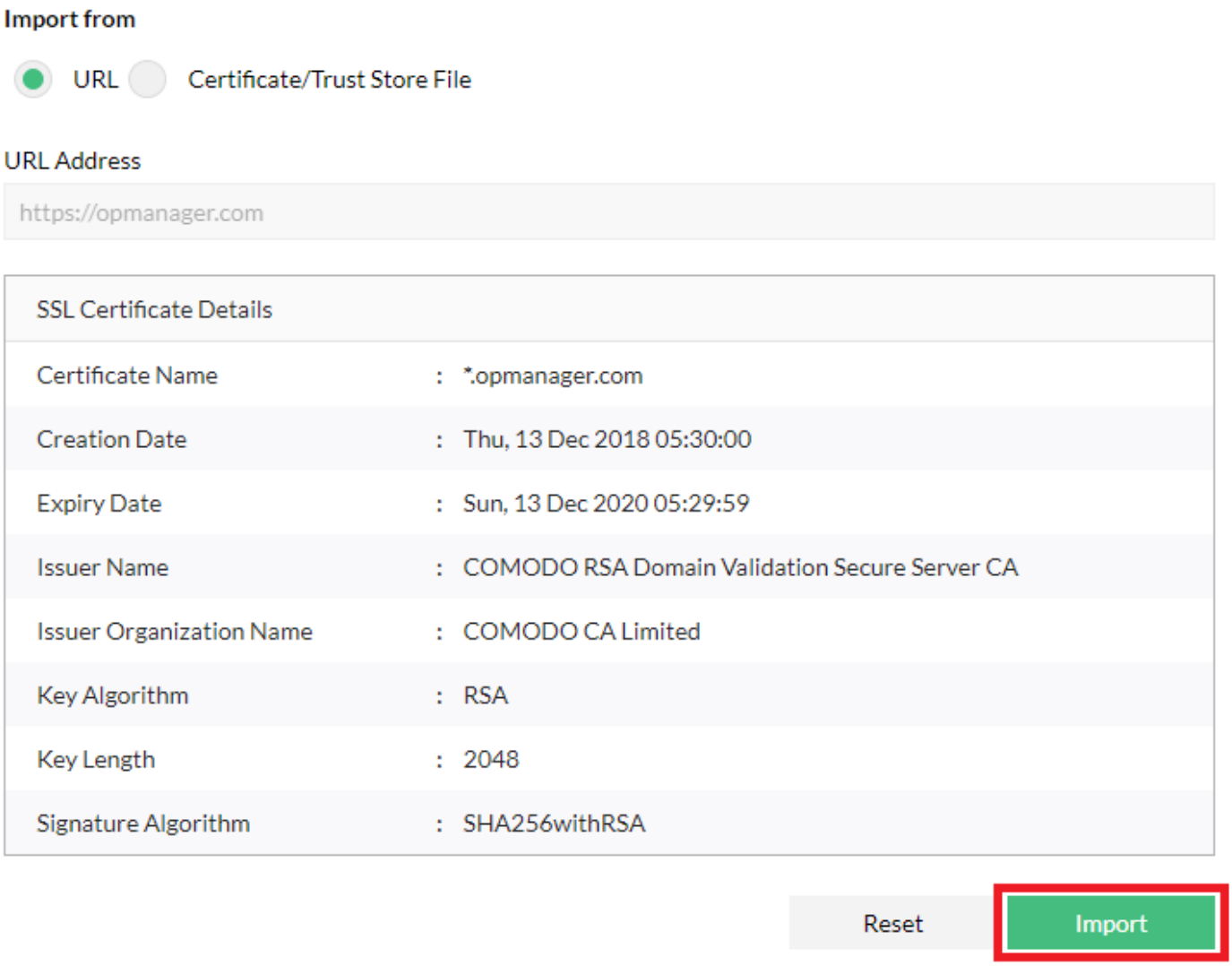
2) Go to the Trusted Certificates tab.



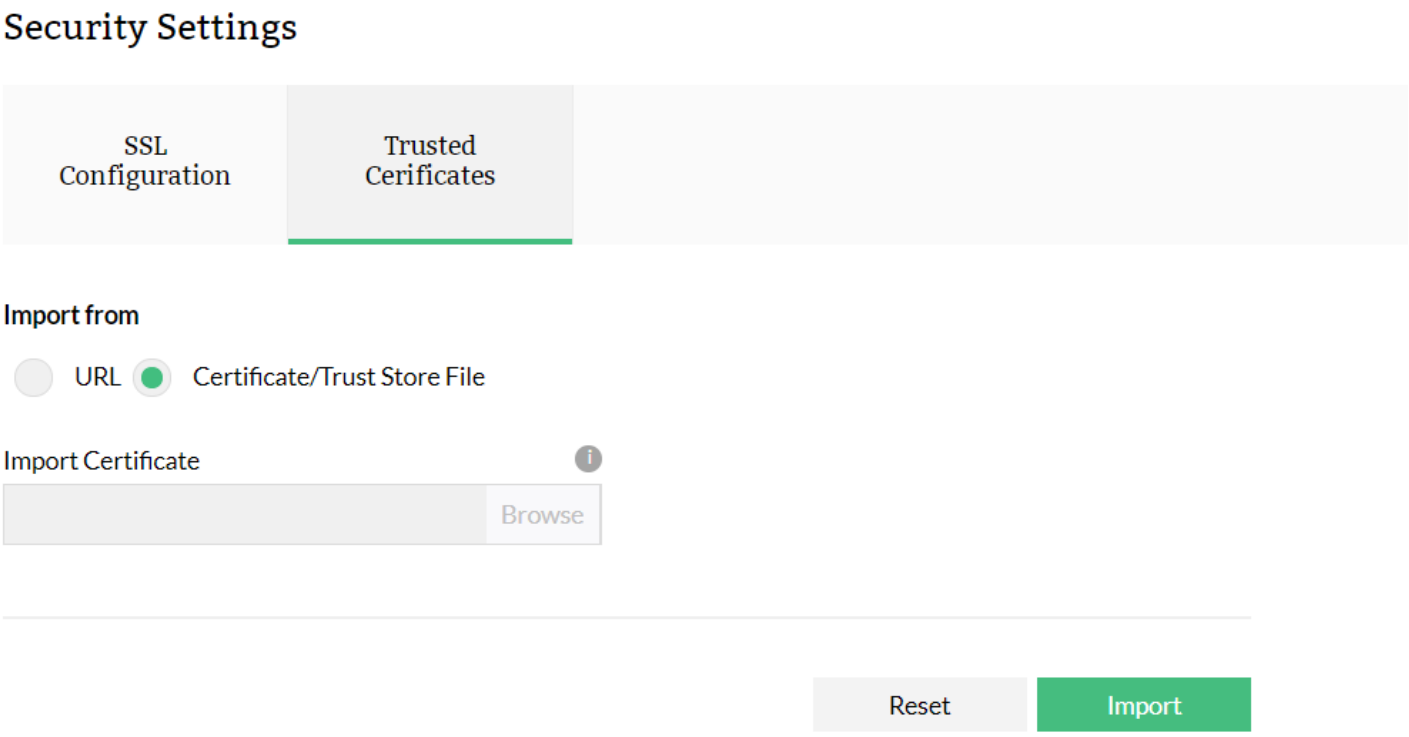
3) Here you have 2 options to import certificates into trusted sources.

- Fetch certificate from a URL reachable from OpManager server
- Directly upload certificates as files or from a keystore/truststore.

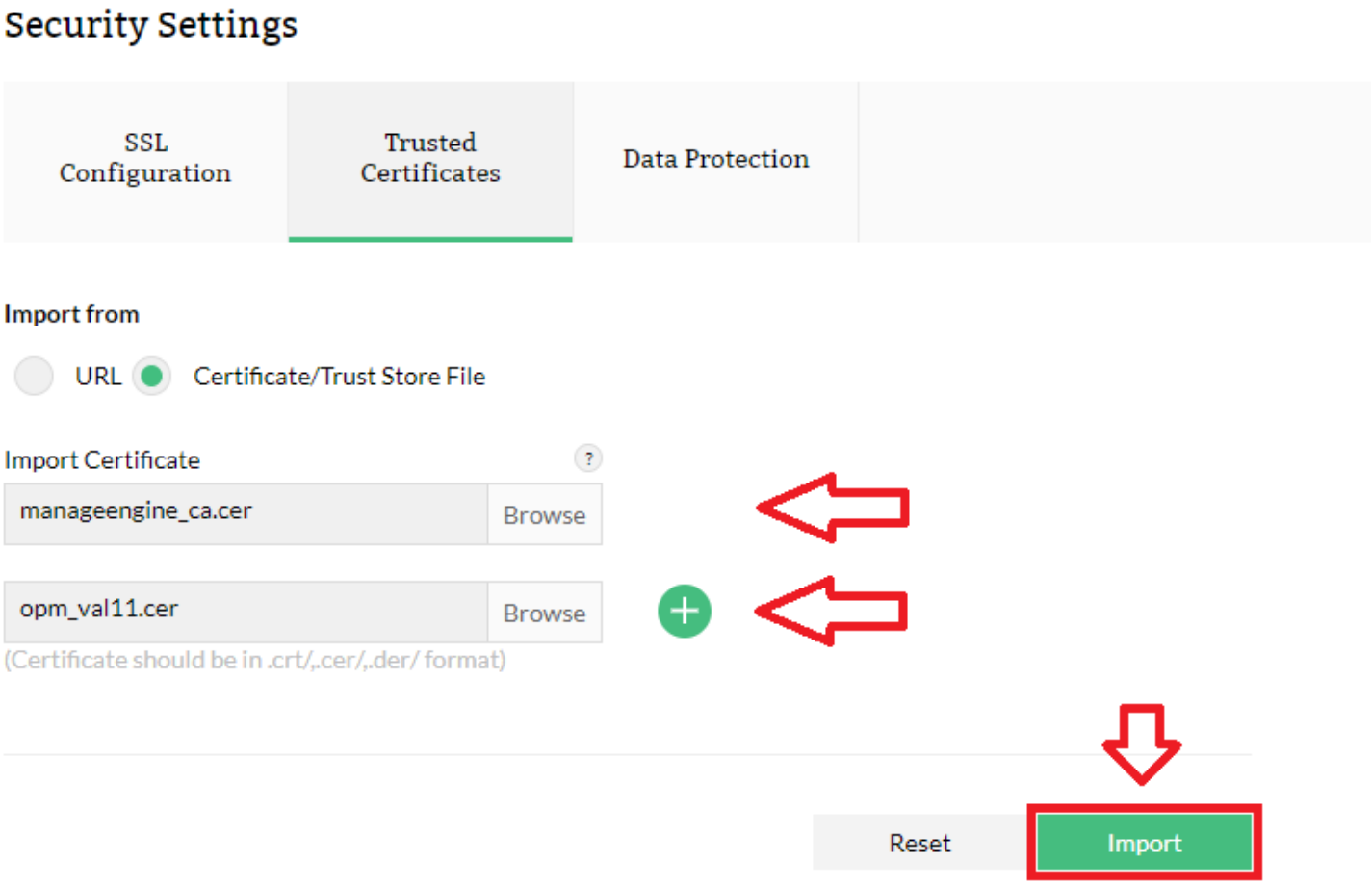
4) If you choose URL and provide the url of the service you want to trust, you will be prompted to verify and import the fetched certificate. Click Import and it will be added to the trusted sources.



5) If you choose the second option, Certificate/ Trust Store file, then you will have to browse and select the files.



6) In the below case, certificate crt files are chosen to add to trust store. On clicking import, it will be added to OpManager's trust store.



7) In case you have a keystore / truststore / pfx of the source you want to trust, browse and choose the appropriate truststore file. Input the password and click Fetch.You will be shown a list of aliases availale in the truststore you can choose the ones you want and click Import.

Import from

URL Certificate/Trust Store File

Import Certificate

Certificates.pfx Browse

Password

••••••••

	Alias name	Common Name
☐	manageengine ca	ManageEngine CA
☐	opm-val11	opm-val11

Reset Import

Configuring Failover Support for OpManager

Failover or redundancy support for OpManager is necessary to achieve uninterrupted service. It becomes cumbersome if the OpManger DB crashes or loses its network connectivity and not monitoring your network. Though regular backups help you recover from DB crashes, but it takes time for OpManger to resume its service. However, in the mean time your network will be left unmonitored and some other critical devices such as routers, mail servers etc. may go down and affect your business. Implementing a redundancy system helps you to overcome such failures.

Failover support requires you to configure OpManager Secondary or Standby server and keep monitoring the OpManager Primary server. Incase the Primary server fails the Standby server automatically starts monitoring the network. The transition is so quick and smooth that the end user does not feel the impact of the failure of the Primary server or the subsequent taking over by Standby. In parallely the Standby server triggers an email alert (email ID entered configured in the mail server settings) about the Primary's failure. Once the Primary server is restored back to operation the Standby server automatically goes back to standby mode.

Note: This page is relevant for OpManager build versions **125139** and older. For newer versions (from build version **125140**), refer this page.

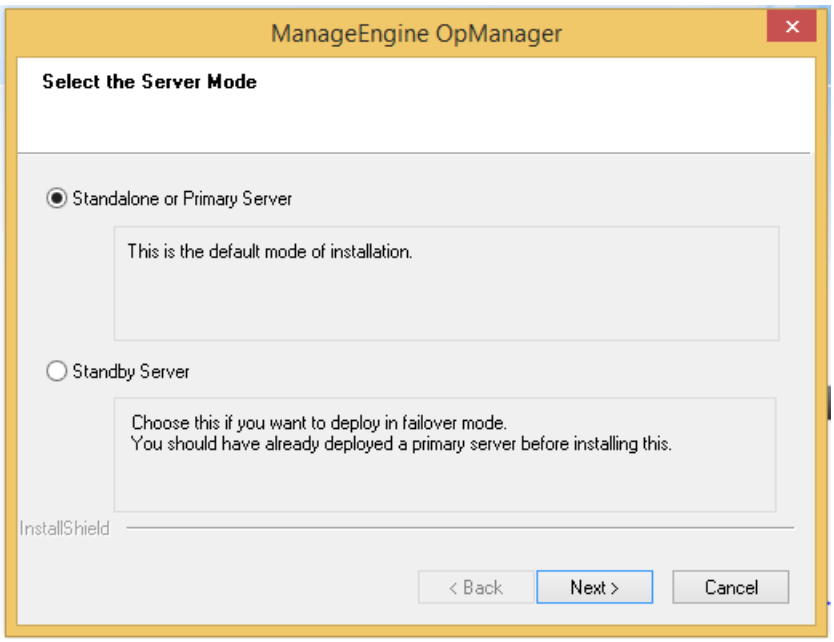
Working Mechanism

The Primary server updates its presence with a symbolic count in the BEFailover table at a specified interval known as the HEART_BEAT_INTERVAL. With every update the count gets incremented. This count is known as LASTCOUNT. Similarly the standby server also updates the its presence by updating the LASTCOUNT in the BEFailover table.

When the Primary server fails, it fails to update the LASTCOUNT. The Standby server keeps monitoring the Primary's LASTCOUNT at a specified periodic interval known as FAIL_OVER_INTERVAL. By default the FAIL_OVER_INTERVAL value is 60 seconds. If required you can modify it in the Failover.xml file (<OpManager_Standby_home>\conf). Supposing, you have specified FAIL_OVER_INTERVAL as 50 seconds, the standby will monitor the Primary's LASTCOUNT for every 50 seconds. Every time, when the Standby server looks up the LASTCOUNT, it compares the previous and present counts. When the Primary server fails to update the LASTCOUNT, consecutive counts will be the same and the Standby assumes that the Primary server has failed and starts monitoring the network.

Installing the Primary Server

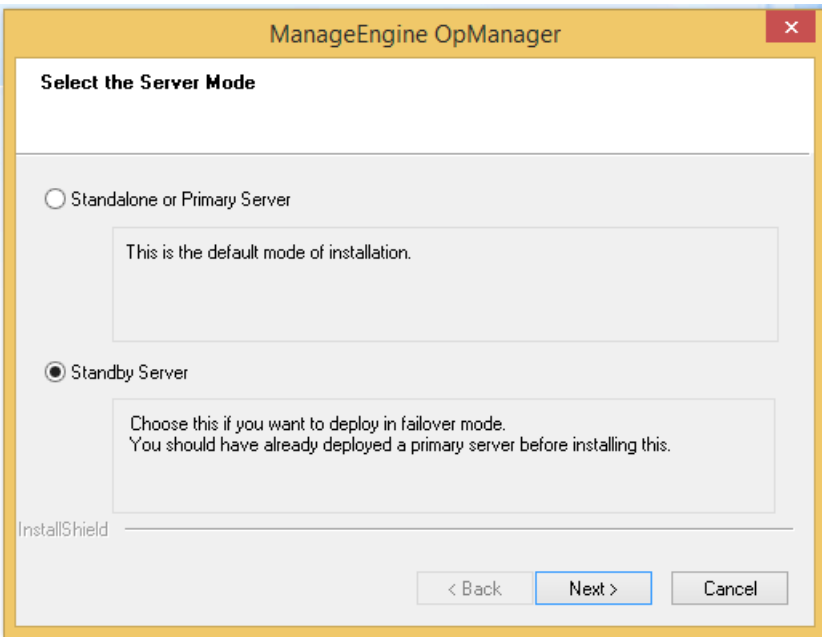
While installing OpManger on the Primary server, select as Primary server in the installation wizard and complete the installation process. Start the Primary server.



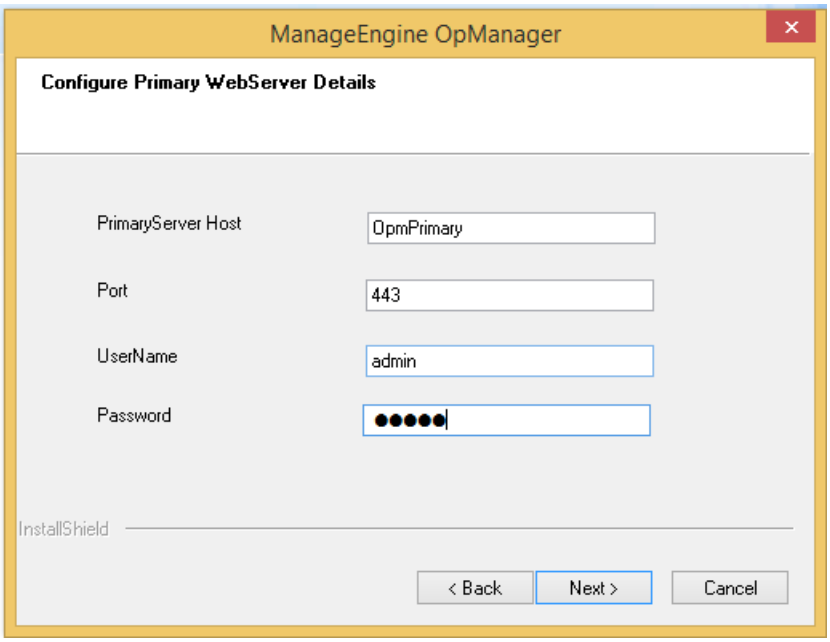
Installing the Standby Server

While installing OpManager on the standby server,

1. Select as Standby server mode in the installation wizard.



2. Enter the Primary webserver host, port and login details (any administrator username & password from the Primary server) and complete the installation. Do not start the Standby server.



Note: The Date and Time settings of the Primary and the Standby should be same.

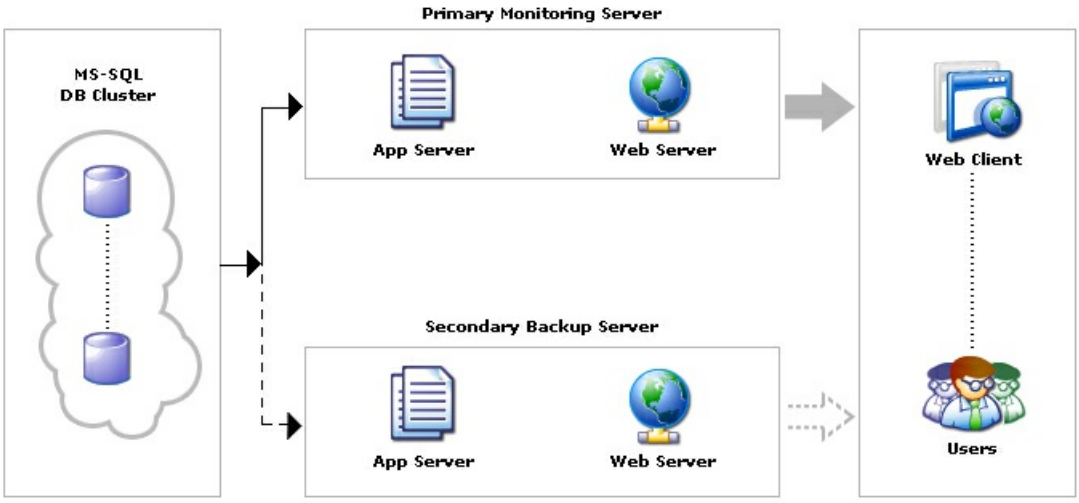
Configuring Failover

While running OpManager with MSSQL as the backend DB, implement clustering. Clustering refers to an array of databases in which the data are stored and have a single virtual IP. If any of the DB in the cluster environment fails the other DBs have the data thereby providing high availability of data. The Primary server sends all its data to a virtual IP and the data gets stored in multiple locations. The Standby server that takes control over the network in case the primary fails, then the standby server also sends the data to the same virtual IP.

If you want a specific file to be synced between the primary and standby servers, you can add the required directory in the Failover.xml file (OpManager\conf\OpManager\Failover.xml).

For configuring MSSQL server clustering visit the below link published by Microsoft.

https://technet.microsoft.com/en-us/library/hh231721(v=sql.110).aspx



Standby OpManager server can be started once the installation is completed, provided you have already configured MSSQL clustering for Primary server.

Once the Primary server fails, the Standby server assumes itself as the Primary server and starts monitoring the network. Once the Primary server is up, the Standby server goes back to its standby mode and monitors the Primary server.

Migrating OpManager Database

- Version 125230
- Version 12.5
- Version 12.4
- Versions below 11600

For OpManager version 125230:

PGSQL to MSSQL Migration Steps :

1. In the PGSQL setup, go to OpManager home ? bin, start Command Prompt with administrator privilege from this path and run DBConfiguration.bat.
2. In the popup shown, please chose MSSQL, check "Migrate data from the existing database" option and click OK.
3. After the migration is complete, start the product and check if it is working properly

MSSQL to PGSQL Migration (For Prepopulated and non prepopulated setups):

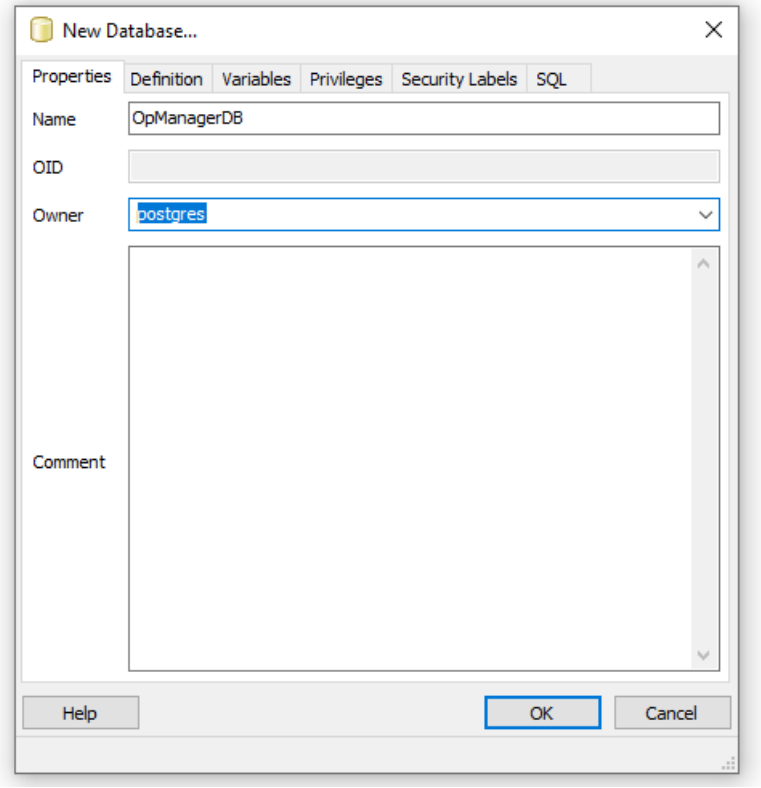
1. In the MSSQL setup, make the below changes in db_migration.conf in the <OpManagerHome>\conf directory.
2. Change the value of **dest.db.postgres.dir** to <OpManagerHome>/pgsql directory (E.g., dest.db.postgres.dir = <OpManager Base Home>/pgsql).

   Note: It is mandatory to use "/" as a directory separator.

3. Now go to OpManager home ? bin, start Command Prompt with administrator privilege from this path and run DBConfiguration.bat.
4. In the popup shown, please chose PostgreSQL and check "Migrate data from the existing database" option and click OK.
5. After the migration is complete, start the product and check if it is working properly.

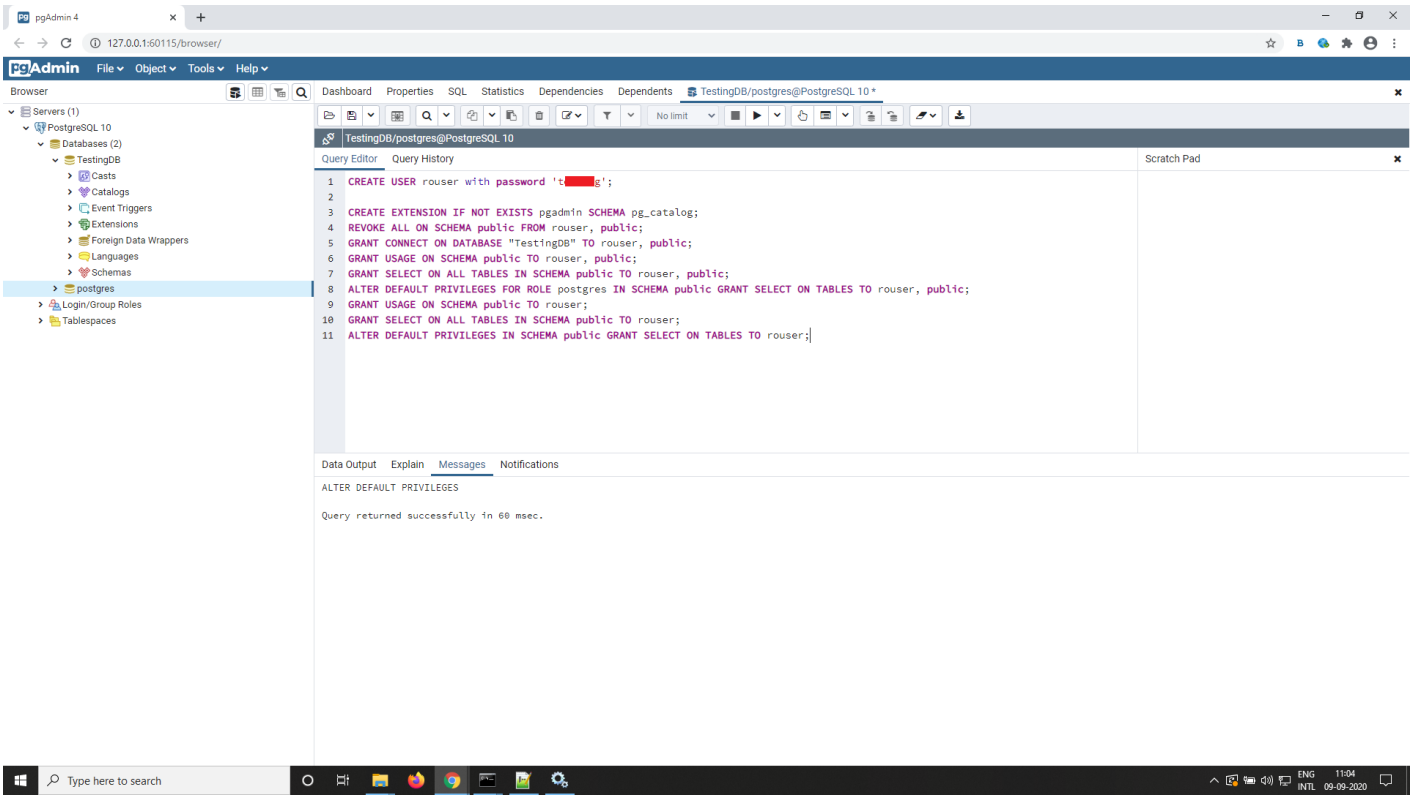
MSSQL to PGSQL Migration (Remote PGSQL)

1. In the MSSQL setup, make the below changes in db_migration.conf in <OpManager Base Home>\conf directory.
   a. **create.dest.db=false**
   b. **start.dest.postgres.server=false**
2. Rename the **database_params_dbconfig.conf.bkp** file in <OpManagerHome></OpManagerHome>\conf\OpManager\POSTGRESQL folder if it exists.
3. Create a database in Remote PostgreSQL server.



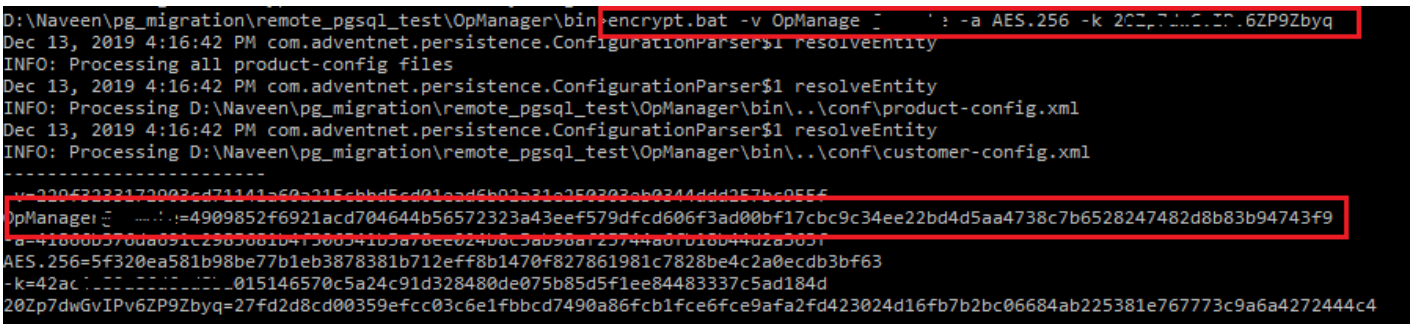
4. Create 'rouser' for read-only permissions. Connect to pgAdmin and execute the below queries:

   - CREATE USER rouser with password **'<ROPASSWORD>'**;
   - CREATE EXTENSION IF NOT EXISTS pgadmin SCHEMA pg_catalog;
   - REVOKE ALL ON SCHEMA public FROM rouser, public;
   - GRANT CONNECT ON DATABASE "**<DatabaseName>**" TO rouser, public;
   - GRANT USAGE ON SCHEMA public TO rouser, public;
   - GRANT SELECT ON ALL TABLES IN SCHEMA public TO rouser, public;
   - ALTER DEFAULT PRIVILEGES FOR ROLE postgres IN SCHEMA public GRANT SELECT ON TABLES TO rouser, public;
   - GRANT USAGE ON SCHEMA public TO rouser;
   - GRANT SELECT ON ALL TABLES IN SCHEMA public TO rouser;
   - ALTER DEFAULT PRIVILEGES IN SCHEMA public GRANT SELECT ON TABLES TO rouser;

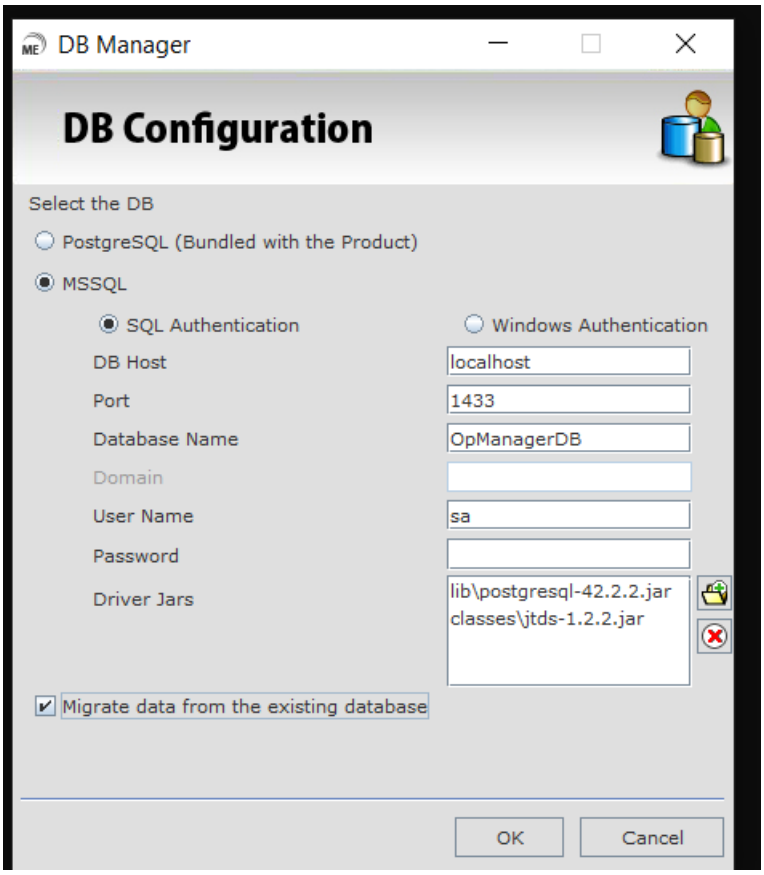


5. **Changes to be made in the <OpManagerHome>\conf\OpManager\POSTGRESQL\database_params.conf**

   - Make the changes in URL field **jdbc:postgresql://<remotePgSQLInstalledIPAddress>:<PortNumber>/<DBName>?dontTrackOpenResources=true&useUnicode=true&characterEncoding=utf8**
   - Change the username to postgres. (username=postgres)
   - Encrypt the password of the postgres user and change the same in the above mentioned. file (**password=<EncryptedPassword>**)
   - Add the property **isBundledPgSQL=false** as well in the same file.
   - Change the **ro_password** to the password supplied in point 4 **<ROPassword>**. Encrypt the same and include it in the same file (**ro_password=<ROPassword>**)
   - Encryption of the plain text can be done using <OpManagerHome>\bin\encrypt.bat by specifying the algorithm as **AES.256** and by using **CryptTag** which can be found in <OpManagerHome>\conf\customer-config.xml (**Usage:: encrypt.bat -v <Password> -a AES.256 -k <CryptTag>**)



5. Now go to OpManager home ? bin, start Command Prompt with administrator privilege from this path and run DBConfiguration.bat.
7. In the popup shown, please chose PostgreSQL and check the "Migrate data from the existing database" option and click OK.
8. After the migration is complete, start the product and check if it is working properly.



Migrating SQL server from one machine to another

Note: These steps are applicable for all versions of OpManager.

1. Stop OpManager Service.
2. Take a SQL DB backup using the SQL Management tool.
3. Restore the MSSQL DB backup(taken from old server) in the new server using the SQL Management tool.
4. Open cmd with admin privelege and go to <OPMHome>/bin and run DBConfiguration.bat. Provide new sql details and save.
5. Start OpManager Service.

For OpManager version 12.5

Note: The following steps are only applicable for Windows installations. The supported PgSQL versions are 10.12 and above.

Migrating from PgSQL to MSSQL

1. Download and install the latest version of OpManager (choose MSSQL DB while installing).
2. **Do not hit 'Finish'** at the end of installation.
3. In the old PGSQL setup, go to **<OpManagerHome>\bin>**, start Command Prompt from that path and run the **'MigrateDB.bat'**file with the required parameters.

```
MigrateDB.bat mssql <opm_home_from_new_MSSQL_setup>/conf/databaseParams.conf
```

4. After migration, navigate to **<OpManagerHome>\conf\OpManager** in the old PgSQL setup, copy the **data-dictionary.xml** file and replace it under the same directory in the new MSSQL setup.
5. Start the OpManager service and check if it works properly.

Migrating from MSSQL to PgSQL (Pre-populated setup)

1. Download and install the latest version of OpManager (choose PGSQL DB while installing).
2. **Do not hit 'Finish'** at the end of installation.
3. Provide a new DBNAME for **database_params.conf** in the new PGSQL setup.
4. Make the below changes in the db_migration.conf file under**<OpManager Base Home>\conf:**

```
create.dest.db=true
start.dest.postgres.server=true
```

5. In the **db_migration.conf** file under<OpManager Base Home>\conf, change the value of **dest.db.postgres.dir**

```
dest.db.postgres.dir = <OpManager New PgSQL Home>/pgsql
```

Note: It is mandatory to use "/" as the directory separator

6. In the old MSSQL setup, go to **<OpManagerHome>\bin**, start Command Prompt with administrative privilege from the same path and run the **'MigrateDB.bat'** file with the required parameters.

```
MigrateDB.bat postgres <OpManager New PgSQL Home>\conf\database_params.conf
```

7. After migration, navigate to **<OpManagerHome>\conf\OpManager** in the old MSSQL setup, copy the **data-dictionary.xml** file and replace it under the same directory in the new PgSQL setup
8. Now, start OpManager Service from the new PGSQL setup and check.

Migrating from MSSQL to PgSQL (Non Pre-populated setup - All 32 bits and EE setups)

1. Download and install latest(same) version of OpManager (Choose PGSQL DB while installing).
2. **Do not hit 'Finish'** at the end of installation.
3. Make the below changes in the db_migration.conf file under**<OpManager Base Home>\conf:**

```
create.dest.db=true
start.dest.postgres.server=true
```

4. In the **db_migration.conf** file under<OpManager Base Home>\conf, change the value of **dest.db.postgres.dir**

```
dest.db.postgres.dir = <OpManager New PgSQL Home>/pgsql
```

Note: It is mandatory to use "/" as the directory separator

5. In the old MSSQL setup, go to **<OpManagerHome>\bin**, start Command Prompt with administrative privilege from the same path and run the **'MigrateDB.bat'** file with the required parameters.

```
MigrateDB.bat postgres <OpManager New PgSQL Home>\conf\database_params.conf
```

6. After migration, navigate to **<OpManagerHome>\conf\OpManager** in the old MSSQL setup, copy the **data-dictionary.xml** file and replace it under the same directory in the new PgSQL setup.
7. Now, start OpManager Service from the new PGSQL setup and check.

Migrating from MSSQL to Remote PgSQL

1. Download and install latest version of OpManager (Choose PGSQL DB while installing).
2. **Do not hit 'Finish'** at the end of installation.

3. Create a new database in the Remote PgSQL server. Provide the new DBNAME and its remote server details in the **database_params.conf** file of the new PGSQL setup.
4. Change the value of 'isBundledPgSQL' in the **database_params.conf** filrto **false**.
5. In the **db_migration.conf** file under<OpManager Base Home>\conf, change the value of **dest.db.postgres.dir**

```
dest.db.postgres.dir = <OpManager New PgSQL Home>/pgsql
```

Note: It is mandatory to use "/" as the directory separator

6. In the old MSSQL setup, go to **<OpManagerHome>\bin**, start Command Prompt with administrative privilege from the same path and run the **'MigrateDB.bat'** file with the required parameters

```
MigrateDB.bat postgres <OpManager New PgSQL Home>\conf\database_params.conf
```

7. After migration, navigate to **<OpManagerHome>\conf\OpManager** in the old MSSQL setup, copy the **data-dictionary.xml** file and replace it under the same directory in the new PGSQL setup.
8. Now start OpManager Service from new PGSQL setup.

For OpManager version 12.4

Migrating from PGSQL TO MSSQL

- Download the latest version of OpManager (.exe/.bin)
- After the installation is complete, **do not hit the 'Finish' button.**
- In the old PGSQL setup, go to OpManager home ? bin, start Command Prompt from this path and run the **'MigrateDB.bat'** file with the required parameters.

  ```
  MigrateDB.bat mssql <opm_home_from_new_MSSQL_setup>/conf/databaseParams.conf
  ```

  (Pointing the newly created MSSQL database from the old PGSQL database)
- After migration is complete, copy the **data-dictionary.xml** file from the 'pgsql' folder of the old installation to the 'mssql' folder of the new installation.
- Start the product, and check if it's working properly.

Migrating from MSSQL TO PGSQL

- Download the latest version of OpManager (.exe/.bin)
- After the installation is complete, **do not hit the 'Finish' button.**
- In the old MSSQL setup, go to OpManager home directory ? pgsql ? bin, start Command Prompt from this path and run the following command:

  ```
  psql.exe -U postgres -p <postgre_port_number> -h 127.0.0.1
  ```

  This establishes a connection between OpManager and the PGSQL server.
- Next, invoke the **create database** command with a DB name of your choice.

  ```
  create database <New_database_name>;
  ```

- Now, copy the name of the newly created database, and replace it in the **databaseParams.conf** file in the 'conf' directory.
- Go to the OpManager home directory of the old PGSQL setup, and run the **'MigrateDB.bat'** file with the required parameters.

```
MigrateDB.bat postgres <opm_home_from_new_PGSQL_setup>/conf/databaseParams.conf
```

(Pointing the newly created PGSQL database from the old MSSQL database)

- After migration is complete, copy the **data-dictionary.xml** file from the 'mssql' folder of the old installation to the 'pgsql' folder of the new installation.
- Start the product, and check if it's working properly.

For builds earlier than 11600, follow the steps below to migrate from MySQL to PGSQL/MSSQL.

Migrating from MySQL to PGSQL

1. Stop OpManager.
2. Take a backup: cmd > OpManager\bin\backup
3. Execute **BackupDB.bat -targetdb pgsql** (proceed to next step after the backup is completed).
4. Since PGSQL was not bundled with earlier versions, take a complete OpManager backup and save it on different location as folder backup.
5. Uninstall OpManager completely and delete OpManager folder.
6. Install same build of OpManager with PGSQL database option and make sure OpManager works fine. (link to download older builds of OpManager: http://archives.manageengine.com/opmanager/)
7. Stop OpManager service and copy the backup folder located under OpManager from the backup folder to the newly installed folder under the same location.
8. Restore the database using **RestoreDB.bat** present under OpManager/bin/backup directory and restart OpManager.

   For ex : C:\<OpManager Home>\bin\backup>**RestoreDB.bat "c:\OpManager\backup\BackUp_APR3_2009_17_43_38_8100.zip"**

   Note : For linux - please use BackupDB.sh

Migrating from MySQL to MSSQL

1. Take a backup: cmd > OpManager\bin\backup
2. Execute **BackupDB.bat -targetdb mssql** (proceed to next step after the backup is completed)
3. Select Start > Programs > ManageEngine OpManager > DB Manager > DB Configuration
4. A DB Configuration window pops up. Select MSSQL and click on Save.
   Configure the following information:
   a. **DB Host :** The name or the IP address of the machine where MSSQL is installed.
   b. **Port:** The port number in which OpManager must connect with the database. Default is 1433.
   c. **User Name and Password:** The user name and password with which OpManager needs to connect to the database.
   d. **Driver Jars:** Specify the path of the Database driver
   e. Click OK.
5. Restore the data using **RestoreDB.bat** present under OpManager/bin/backup directory and restart OpManager.

   For ex : C:\<OpManager Home>\bin\backup>**RestoreDB.bat "c:\OpManager\backup\BackUp_APR3_2009_17_43_38_8100.zip"**

Migrating OpManager from one server to another

Here are the steps to go about migrating OpManager to a new server:

1. Please click on **Support->About** clicking on the Image icon at the top right of OpManager web client to make a note of the build number of the existing OpManager installation.

2. Take a backup of your existing database by following the instructions on the below link, https://www.manageengine.com/network-monitoring/help/data-backup-and-restoration.html

3. On the new server, download the same build of OpManager from the link below and install it:
http://archives.manageengine.com/opmanager/

4. Install OpManager first and see if it starts fine, once it is started, please stop the OpManager service and proceed with the restoration process as stated below,
Copy the backup files to the new server.
Open a command prompt (as an administrator) & navigate to **\\OpManager\bin\backup** directory.
You can then restore the backup file using the RestoreDB.bat followed by the path of the backup file on the new server
For example :**...\OpManager\bin\backup>RestoreDB.bat "D:\backup\BackUp_APR25_2010_01_17_21_8051.zip"**
Once the restoration is complete, start OpManager service.

5. Copy the files AdventNetLicense.xml, petinfo.dat and product.dat from the OpManager/ Lib folder (For Version 12 and above) folder of your old server and paste in under the same location of the new server, restart the OpManager service and this will have your license updated.

Migrating OpManager from Linux installation to Windows installation

Migrating OpManager from Linux installation to Windows installation

1.On the Linux installation of OpManager, click About and check what is the build number of OpManager, download the windows setup of the same build from the link below and install it on a test machine.
http://archives.manageengine.com/opmanager/

2. On the older server installation, take a backup by running the BackupDB.sh file under **\OpManager\bin\backup** folder. Once the backup is a complete, a file named **BackUp_FEB28_2005_15_51.zip** [with the current date and time] will be created under **\OpManager\backup** folder.

3. On the windows installation, create a folder called **backup under \OpManager folder** and paste the backup file from the Linux installation.

4. Now run the RestoreDB.bat file under **\OpManager\bin\backup** folder on the windows installation with the arguments as below.

RestoreDB.bat **"C:\Program files\ManageEngine\OpManager\backup\BackUp_AUG10_2012_02_39_44_9101.zip"** Provide the full path of the file

5. Once the restoration is complete, start OpManager.

Limitations of migrating to Linux from Windows:

1. WMI based monitoring functionality is not available on Linux.
2. Monitoring of MSSQL/Exchange is not available on Linux.
3. Hyper-V monitoring does not work on the Linux server.
4. Active Directory performance counter will not work.

Data Backup and Restoration

Periodically backing up the database is very essential, as it helps you restore OpManager service back during planned maintenance as well as unplanned mishaps. OpManager database contains two types of data:

Performance data: This is the data gathered by OpManager by periodically polling or querying the resources on a monitored device to determine its performance. This includes resources like CPU, Memory, Response time, Traffic etc.

Configuration data: There are quite a few configurations an administrator effects in OpManager for easy management and monitoring. The configurations include user settings, details of discovered devices, custom monitors, threshold settings, notification profiles, etc.

Steps to backup data:

- Open command prompt with administrative privileges and go to <OpManagerHome>/bin/backup directory.
- Execute **BackupDB.bat** (use **BackupDB.sh** for Linux) from the command prompt as shown below:

<OpManagerHome>/bin/backup>BackupDB.bat

Note: This utility does a backup of the complete database, i.e., performance and configuration data. Only the configuration data will be backed up for Netflow Analyzer and Firewall Analyzer modules.

- The backup file created will be stored in <OpManagerHome>\backup directory. To store the backup file in a different directory, use the command given below:BackupDB.bat -destination "<DestinationFolderPath>" (Eg : BackupDB.bat -destination "C:\Backup")

To backup only the configuration data:

- Open command prompt with administrative privileges and go to <OpManagerHome>/bin/backup directory and execute the below command:

<OpManagerHome>/bin/backup>BackupDB.bat -mode configdata

- This is used to backup only the configuration data (Backup Conf., Images folder, the details of Devices, Device Templates, Interfaces, Interface Template, Dashboards & Widgets, Infrastructure Views, Business Views, Credentials, Notification Profiles and Users) and not the performance data.

Steps to restore data:

- Open command prompt with administrative privileges and go to <OpManagerHome>/bin/backup directory.
- Execute **RestoreDB.bat** (use **RestoreDB.sh** for Linux) with the backup file name as argument from the command prompt as shown below:

<OpManagerHome>/bin/backup>RestoreDB.bat "<Backup file name with path>"
(Eg: RestoreDB.bat "C:\backup\Backup_Pgsql_Mar8_125128_123313.zip")

Note: For MSSQL database, find the files bcp.exe and bcp.rll in MSSQL server and ensure to copy it to OpManager home folder. If the MSSQL server is installed on a 64-bit OS, and OpManager is installed on 32-bit server, the bcp.exe and bcp.rll copied from the

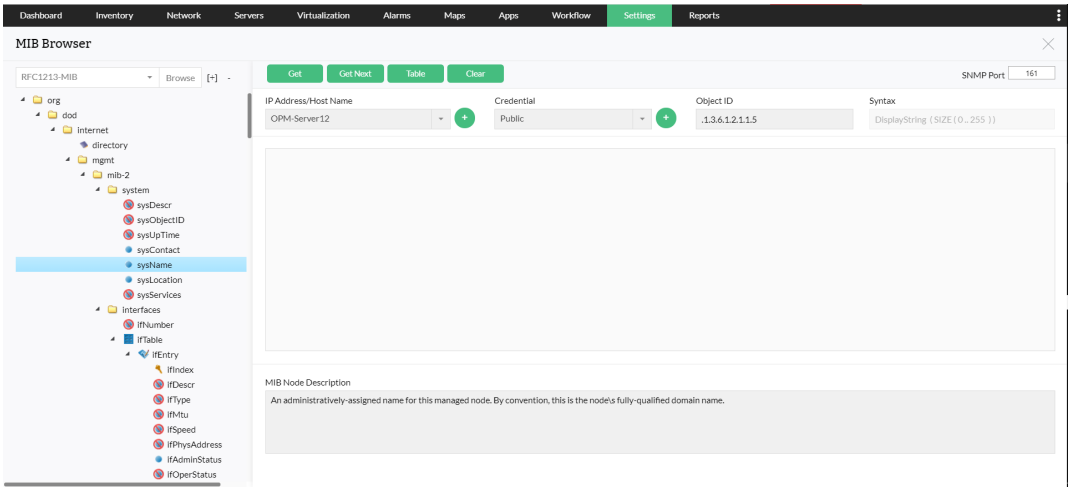
MSSQL server will not work on the OpManager machine. You'll need a 32-bit bcp.exe and bcp.rll

MIB Browser: Overview

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

The features of MIB Browser include the following:

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

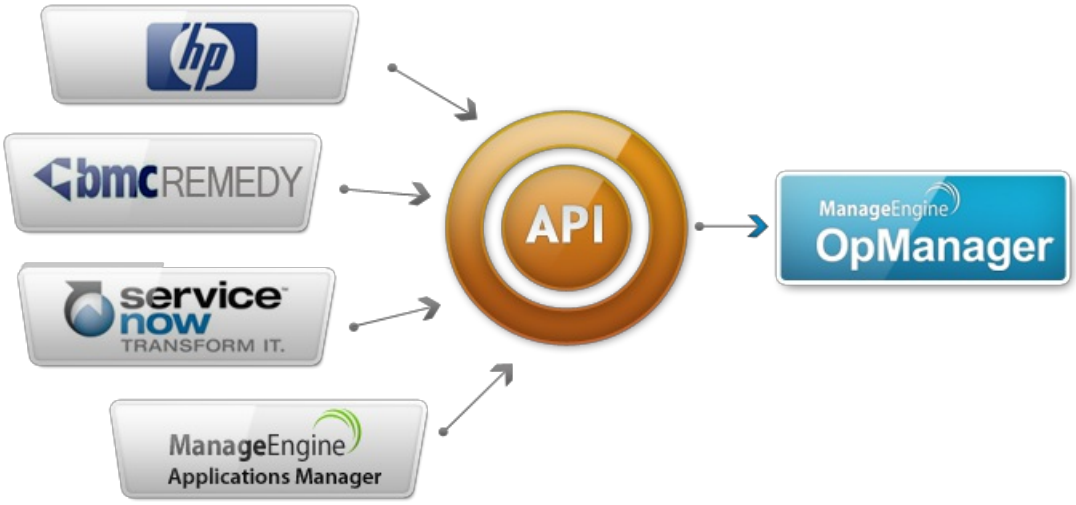


MIB Browser Interface

- **Menu bar**: Contains menus with related commands to perform all administrative operations.
- **Toolbar**: Contains frequently used administrative commands for easy access.
- **MIB Tree**: Shows all the loaded MIBs. You can traverse the tree and view the definition of each node in the tree.
- **SNMP Settings**: Displays the SNMP settings of the selected node.
- **Result Display Area**: Displays the result of the SNMP operations.
- **Object Attributes**: Shows the attributes of the selected node

OpManager REST API

OpManager offers REST APIs for adding and fetching data from OpManager. Using these APIs, you can integrate OpManager with 3rd party IT management/service desk software.



How OpManager REST APIs work?

The APIs work with an API key. The API key is unique for each OpManager account and has to passed as a parameter in every API request made. First, generate an API key.

Generate API Key

To generate an API key, go to **Settings** > **Basic Settings** > **REST API** in OpManager web client and click on **Regenerate Key**.

API List

API Name	API Format	Method	Description
Add User	addUser	post	Adds an user in OpManager.
Add Domain	addDomain	post	Adds a domain in OpManager.
Delete Domain	deleteDomain	post	Deletes a domain in OpManager.
List Credentials	listCredentials	get	Gives the list of credentials created in OpManager.
List Users	listUsers	get	Lists all users created in OpManager.
Delete User	deleteUser	post	Deletes a user.
Change Password	changePassword	post	Allows you to change the password of a user.
Update user contact details	updateContactDetails	post	Allows you to update the contact details of a user.
Add Downtime Schedule	addDowntimeSchedule	post	Adds a new downtime schedule
Update Downtime Schedule	updateDowntimeSchedule	post	Updates a specific downtime schedule

Get Downtime Schedule	getDowntimeSchedule	get	Used to get all details about a particular downtime schedule
List Downtime Schedules	listDownTimeSchedules	get	Gives the list of downtime schedules created.
Delete Downtime Schedules	deleteDownTimeSchedules	post	Deletes a particular downtime scheduler.
List Device Templates	listDeviceTemplates	get	Lists all the device templates created in OpManager.
List Notification Profiles	listNotificationProfiles	get	Lists all the notification profiles created in OpManager.
List Syslog rules	listSysLogRules	get	Lists all the syslog rules created.
List Url monitors	listURLMonitors	get	Lists all teh URL monitors created.
Trap Processors	listTrapProcessors	get	Lists all the trap processor created.
Script Monitors	listScriptMonitors	get	Lists all the script monitors created.
Get Proxy Settings	GetProxyServerSettings	get	Provides the details of proxy server settings.
Get SMS Server Settings	GetSMSServerSettings	get	Provides the details of SMS server settings.
Add SMS Server Settings	configureSMSServerSettings	post	Allows to configure the SMS server settings.
List Alarm Escalation rules	listAlarmEscalationRules	get	Lists all the alarm escalation rules created.
List Probes	listProbes	get	Lists all the probes available in OpManager.
List Perfomance Monitors	listPerformanceMonitors	get	Lists all the performance monitors added.
List Interface Templates	listInterfaceTemplates	get	Lists all the interface templates created.
Get Mail Server Settings	GetMailServerSettings	get	Provides the details of mail server settings.
Add device	addDevice	post	Add a device.
Delete Device	deleteDevice	post	Deletes a device.
Add device to BV	addDeviceToBV	post	Adds devices to a Business View that is already created.
Add device to Google Map	addDeviceToGMap	post	Adds devices to Google map.
Add Business view	addBusinessView	post	Adds a new business view.
Get Infrastructure Details	getInfrastructureDetailsView	get	Provides the details of the infrastructure i.e., servers, routers, etc. managed by OpManager.
Get Infrastructure Views	getInfrastructureView	get	Provides the details of a particular infrastructure type. eg.: servers.
Get Down devices	getDownDevices	get	Provides the details of devices that are down.
Search device	searchDevice	get	Allows you to search for a device.
All WAN Metrics	getAllWanMetrics	get	Lists all the WAN monitors created.
All VOIP Metrics	getAllVoipMetrics	get	Lists all the VoIP monitors created.
Re discover Interfaces	reDiscoverInterfaces	post	Rediscovers interfaces.
Discover Interface	discoverInterface	post	Discovers an interface.
Add Layer2Map	addLayer2Map	post	Add a new Layer2 Map in OpManager

Discover Layer2map	discoverLayer2Map	post	Discover an existing Layer2 map
Delete Layer2Map	deleteLayer2Map	post	Remove a Layer2 map
Discover Layer2 devices	discoverLayer2Devices	post	Add new Layer2 devices
Get Discovered Layer2 Devices	getDiscoveredLayer2Map	get	Get a list of Layer2 devices already discovered
Add Event	addEvent	post	Adds an event.
Top Devices By Events	getTopDevicesByEvents	get	Lists the top devices by events count.
List Alarms	listAlarms	get	List all the alarms available.
Acknowledge Alarm	acknowledgeAlarm	post	Allows to acknowledge an alarm.
Un Acknowledge Alarm	unAcknowledgeAlarm	post	Allows to unacknowledge an alarm.
Clear an Alarm	clearAlarm	post	Clears an alarm.
Delete Alarm	deleteAlarm	post	Deletes an alarm.
Add Notes to Alarm	addNotes	post	Adds notes to an alarm.
Get Notes	getAnnotation	get	Provides the notes available for an alarm.
Get Alarm Details	alarmProperties	get	Provides the details of an alarm eg: status, acknowledgement
Top Devices By Alarms	getTopDevicesByAlarms	get	Provides the list of top devices by alarms count.
Ping device	getPingResponse	get	Pings a device and provides the response.
Trace device	getTraceResponse	get	Allows you to get the traceroute to a device.
List devices	listDevices	get	Lists all the devices added in OpManager.
Device Summary	getDeviceSummary	get	Provides the summary details of a device.
Associated Notification Profiles	getNotificationProfiles	get	Provides the list of notification associated profiles to a device.
Associated Workflows	getWorkFlows	get	Provides the list of workflows associated to a device.
Device Notes	getDeviceNotes	get	Provides the details of notes such as floor no. and department name added to a device.
Associated Monitors	getAssociatedMonitors	get	Provides the list of monitors associated to a device.
Update Device Status	updateDeviceStatus	get	Pings the device and updates the correct status of a device.
List Interfaces	listInterfaces	get	Lists all the interfaces in OpManager.
Get Interfaces of Device	getInterfaces	get	Provides the list of interfaces in a device.
Probe URL	getProbeURL	get	Provides the URL of the probe.
Add notes to Device	addNotesToDevice	post	Adds notes to a device.
Interface Summary	getInterfaceSummary	get	Provides the summary details of an interface.
Availability graph data	getAvailabiltyGraphData	get	Provides the data used to calculate the availability graph.
Interface notes	getInterfaceNotes	get	Provides the details of the notes added to an interface.
Interface Monitors	getInterfaceMonitors	get	Provides the list of monitors associated to an interface.
Interface Types	getInterfaceTypes	get	Provides the type of interface. eg: serial, ethernet.
Workflow List for Device	getWorkflowList	get	Lists all the workflows associated to a device.

Trigger Workflow for Device	triggerWorkflow	post	Allows to trigger a workflow on a device.
Business view Details	getBusinessDetailsView	get	Lists all the devices available in a business view.
Business views	getBusinessView	get	Lists all the business views created.
List Racks	listRacks	get	Lists all the racks created.
List Floors	listFloors	get	Lists all the floors created.
Get Floor details	getFloorDetails	get	Provides the details of floor. eg: floor size, tile size.
Get Layer2Map details	getLayer2Maps	get	Provides all details about the specified Layer2 map(s).
Get Polls per second	getPollsPerSec	get	Provides the current polls per second value of OpManager.
System Settings	getSystemSettingsDetails	get	Provides the details of OpManager System Settings.
Update System settings	updateSystemSettingsDetails	get	Allows to update the system settings.
Associate Notification Profile	associateNotificationProfiles	post	Allows to associate multiple Notification Profiles to Multiple devices

Criteria	**Criteria ID**
Status Poll (Device misses 1/3/5 polls)	#00000000000000000000000000000000 (# represents the number of polls, it can be replaced by 1 or 3 or 5 or a ; 1 to select 1 polls or 3 to select 3 polls or 5 to select 5 polls or a to select 1,3,5 polls)
Trap received	01000000000000000000000000000000
Interface - problems	00100000000000000000000000000000
Service down	00010000000000000000000000000000
Windows Service down	00001000000000000000000000000000
Event Log generates alarm	00000100000000000000000000000000
SysLog generated alarm	00000010000000000000000000000000
AdMonitor down	00000001000000000000000000000000
Exchange Monitor down	00000000100000000000000000000000
MSSQL Monitor violated	00000000010000000000000000000000
AdService down	00000000001000000000000000000000
Exchange Service down	00000000000100000000000000000000
MSSQL Service down	00000000000010000000000000000000
Threshold violated	00000000000001000000000000000000
Process Monitor violated	00000000000000100000000000000000
IPSLA Monitor violated	00000000000000010000000000000000
File Monitor violated	00000000000000001000000000000000
Folder Monitor violated	00000000000000000100000000000000
Printer Monitor violated	00000000000000000010000000000000

UPS Monitor &#65533; down	00000000000000000001000000000000
URL &#65533; down	00000000000000000010000000000000
Virtual Device Monitor &#65533; down	00000000000000000100000000000000
Script Monitor &#65533; down	00000000000000001000000000000000
Probe &#65533; down	00000000000000010000000000000000
Agent &#65533; down	00000000000000100000000000000000
Hardware monitor &#65533; down	00000000000001000000000000000000
NCM Backup &#65533; Failed	00000000000010000000000000000000
NCM Config &#65533; changes	00000000000100000000000000000000
NFA Alarm &#65533; generates alarm	00000000001000000000000000000000
UCS Fault received	00000000010000000000000000000000
Storage Alarm	00000000100000000000000000000000
Alarm &#65533; cleared	00000001000000000000000000000000

Large Enterprise Edition REST API Details:

OpManager REST API Documentation				
REST API	**Method**	**Description**	**Parameters**	**Sample URL**
Admin Module				
addSysLogForwarder	POST	Add SysLog Forwarder	**apiKey* -** API Key to access your OpManager server. **destHost* -** Destination Host. **destPort* -** Destination Port(0 &#65533; 65536)	http://localhost:8060/api/json/admin/addSysLogForwarder?apiKey=081c9ac51ba16ab061d5efee583dcd2f&destHost=opman-k8r2s-64-3&destPort=515

addSysLogRule	POST	Add SysLog Rule	**apiKey* -** API Key to access your OpManager server. **ruleName* -** Name of the rule **facilityName*** - SysLog Facility **severityList* -** SysLog Severity(Comma Separated) **alertSeverity* -** OpManager Alert Severity **alarmMessage* -** OpManager Alert Message **matchString -** String matched with incoming syslog message **consecutiveTime* -** consecutive time **timeInterval* -** time interval (if rearmFacilityName is selected then rearmSeverityList should be selected) **rearmFacilityName -** facility name for rearm syslog **rearmSeverityList -** severity list for rearm syslog **rearmMatchString -** String matched with incoming syslog for rearm	http://localhost:8060/api/json/admin/addSysLogRule?apiKey=081c9ac51ba16ab061d5efee583dcd2f&alertSeverity=1&facilityName=auth&ruleName=test11&alarmMessage=test&severityList=alert

addTrapForwarder	POST	Add Trap Forwarder	**apiKey* -** API Key to access your OpManager server. **destHost* -** Destination Host. **destPort* -** Destination Port.	http://localhost:8060/api/json/admin/addTrapForwarder?apiKey=081c9ac51ba16ab061d5efee583dcd2f&destHost=opman-k8r2s-64-6&destPort=165
deleteCredential	POST	Delete Credentials	**apiKey* -** API Key to access your OpManager server. **credentialName* -** Name of the credential. **isSNMPV3 ?** true or false.	http://localhost:8060/api/json/admin/deleteCredential?apiKey=081c9ac51ba16ab061d5efee583dcd2f&credentialName=Public
getCredentialDetails	GET	Get Credential details	**apiKey* -** API Key to access your OpManager server. **credentialName* -** Name of the credential. **type* -** Type of the device eg. Windows, Linux, SNMP v1/v2, SNMP v3 or Vmware.	http://localhost:8060/api/json/admin/getCredentialDetails?apiKey=081c9ac51ba16ab061d5efee583dcd2f&credentialName=Public&type=SNMP v1/v2
getFlowRate	GET	Get SysLog Flow Rate	**apiKey* -** API Key to access your OpManager server.	http://localhost:8060/api/json/admin/getFlowRate?apiKey=081c9ac51ba16ab061d5efee583dcd2f
getSystemSettingsDetails	GET	Provides the details of OpManager System Settings.	**apiKey* -** API Key to access your OpManager server.	http://localhost:8060/api/json/admin/getSystemSettingsDetails?apiKey=081c9ac51ba16ab061d5efee583dcd2f

updateSystemSettingsDetails	GET	Allows to update the system settings.	**apiKey* -** API Key to access your OpManager server**.** **ALARMMESSAGELENGTH -**Any positive Integer. **CLILOG** **&#65533;** false/true**.** **DATACOLLECTIONRATE -**true/false **DEBUGPRINTS -** false/true **POLLPERSECOND -** true/false **SCHEDULERRATE -** false/true **SNMPLOG** - false/true **SNMPV3LOG -** false/true **ShowAds -** true/false **WMILOG -** false/true **benchmarkupload -** enable/disable **metrackupload -** enable/disable **quicklinks** **&#65533;** enable/disable	http://localhost:8060/api/json/admin/updateSystemSettingsDetails?apiKey=081c9ac51ba16ab061d5efee583dcd2f&SNMPV3LOG=false&ShowAds=true&ALARMMESSAGELENGTH=100&DATACOLLECTIONRATE=true&metrackupload=enable&quicklinks=enable&POLLPERSECOND=true&DEBUGPRINTS=false&WMILOG=false&SCHEDULERRATE=false&SNMPLOG=false&benchmarkupload=enable&CLILOG=false
listPluginEvents	GET	Get events raised by the installed plugin application	**apiKey*** - API Key to access your OpManager server. **pluginName*** - Name of the plugin whose event is needed. **eventTime*** - Period in which event generated (for all events, say All).	http://localhost:8060/api/json/alarm/listPluginEvents?apiKey=6d36ff8426cff396b81b248e5c458604&pluginName=All&eventTime=All

getPluginEventCount	GET	Get count of events raised by the installed plugin application	**apiKey*** - API Key to access your OpManager server. **fromTime*** - Start time. **toTime*** - End time.	http://localhost:8060/api/json/alarm/getPluginEventCount?apiKey=6d36ff8426cff396b81b248e5c458604&fromTime=2014-2-20 13:32:8&toTime=2014-2-20 14:2:8
getPluginDetails	GET	Fetches information of the installed plugins	**apiKey*** - API Key to access your OpManager server.	http://localhost:8060/api/json/admin/getPluginDetails?apiKey=081c9ac51ba16ab061d5efee583dcd2f
upadateTrapParser	POST	Update trap parser	**apiKey*** - API Key to access your OpManager server. **version*** - Version. **oid*** - Device OID. **TrapParserName*** - Name of the trap parser.	http://localhost:8060/api/json/admin/upadateTrapParser?apiKey=081c9ac51ba16ab061d5efee583dcd2f&version=v2&oid='.2.2.2.2.2.'&trapParserName=testing
updateLanguageSettings	POST	Update language settings	**apiKey*** - API Key to access your OpManager server. **languageSelected*** - Selected language.	http://localhost:8060/api/json/admin/updateLanguageSettings?apiKey=6d36ff8426cff396b81b248e5c458604&languageSelected=fr_FR
getLanguageSettings	GET	Obtains language settings.	**apiKey*** - API Key to access your OpManager server.	http://localhost:8060/api/json/admin/getLanguageSettings?apiKey=1d626117b2ac31145ce6bca49bb0458b
addDeviceToNProfile *API applicable from 123307	POST	Adds devices to a notification profile that is already created.	**apiKey* - API Key to access your OpManager server.** **deviceName*** - MO Name of the device to which the notification profile has to be associated. MO Name of the device can be fetched using device displayName(Select Name,DisplayName from ManagedObject where DisplayName='<deviceDi	http://localhost/api/json/discovery/addDeviceToNProfile?apiKey=ac130763a309fcb1613e0b8a551950a2&deviceName=localhost.testdomainin.com&profileName=TestNotify&criteria=3100110000101000000000011000001 1&performanceMonitors=DiskUtilization,Win-CPUUtilization

			splayName>') **profileName*** - Name of the notification profile. **criteria*** - There are 32 criteria. mentioned required criteriaid(**Refer the list mentioned at the end of this table. **selectedseverities** - There are 4 severities. (1,2,3,4 for Critical,Trouble,Attention ,ServiceDown or 1,3 for Critical,Attention and like) Severities to be selected for which you want to trigger the notification profile. Add multiple severities by a comma. If param not given by default all severites will be selected. **performanceMonitors** - List of monitors for which you want to trigger the notification profile when threshold is violated. Add multiple monitors separated by a comma. **probeName** - [additional param- Only for Central] - name of the probe	
triggerWorkflow	POST	Allows to trigger a workflow on a device.	**apiKey* - API Key to access your OpManager server.** **workflowName* - Name of the workflow that has to be executed.** **deviceName* -** Name of the device on which the workflow has to be executed.	http://localhost:8060/api/json/workflow/triggerWorkflow?apiKey=081c9ac51ba16ab061d5efee583dcd2f&deviceName=opman-k8r2s-64-3.testdomain.com&workflowName=Instant Device Check

deleteFailOverDetails	POST	Deletes the fail-over server details	**apiKey*** - API Key to access your OpManager server.	http://localhost:8070/api/json/admin/deleteFailOverDetails?apiKey=6d36ff8426cff396b81b248e5c458604
updateFailOverDetails	POST	Updates fail-over server details	**apiKey*** - API Key to access your OpManager server.	http://localhost:8070/api/json/admin/updateFailOverDetails?apiKey=6d36ff8426cff396b81b248e5c458604
listFailOverDetails	GET	Lists the fail-over server details	**apiKey*** - API Key to access your OpManager server. **serviceName*** - Failover device name.	http://localhost:8060/api/json/admin/listFailOverDetails?serviceName=DNS&apiKey=081c9ac51ba16ab061d5efee583dcd2f
registerLicense	POST	Registers the license file	**apiKey*** - API Key to access your OpManager server. **fileName*** - License File name.	http://localhost:8060/api/json/admin/registerLicense?apiKey=6d36ff8426cff396b81b248e5c458604
licenseDetails	GET	Fetches license details	**apiKey*** - API Key to access your OpManager server.	http://localhost:8060/api/json/admin/licenseDetails?apiKey=081c9ac51ba16ab061d5efee583dcd2f
getCredentialMappedDevices	GET	Lists devices mapped to the given credential	**apiKey*** - API Key to access your OpManager server. **credentialName*** - License File name.	http://localhost:8060/api/json/admin/getCredentialMappedDevices?apiKey=081c9ac51ba16ab061d5efee583dcd2f&credentialName=Public

sendSIF	POST	Sends support information file.	**apiKey*** - API Key to access your OpManager server. **customerName*** - Customer name/email ID. **phone*** - Contact number. **subject*** - Mail subject. **userMessage*** - Mail body message. **fromAddress*** - From email address. **supportFile*** - File name or zip file.	http://localhost:8060/api/json/admin/sendSIF?apiKey=6d36ff8426cff396b81b248e5c458604&customerName=administrator@opmanager.com&phone=7781&subject=OpmLogs&userMessage=opm logs for analyzing issue&fromAddress=mohamedthahir.n@testdomain.com&supportFile=OpMan_11200_Feb_20_2014_15_58_30.zip
createSIF	GET	Creates a support information zip file	**apiKey*** - API Key to access your OpManager server.	http://localhost:8060/api/json/admin/createSIF?apiKey=081c9ac51ba16ab061d5efee583dcd2f
viewLogs	GET	Lists all the OpManager logs	**apiKey*** - API Key to access your OpManager server.	http://localhost:8060/api/json/admin/viewLogs?apiKey=081c9ac51ba16ab061d5efee583dcd2f
updateJvmHeapSize	POST	Updates JVM Heap size	**apiKey*** - API Key to access your OpManager server. **jvmHeapSize*** - New JVM Heap size	http://localhost:8060/api/json/admin/updateJvmHeapSize?apiKey=6d36ff8426cff396b81b248e5c458604&JvmHeapSize=5120
generateHeapDump	POST	Generates Heap dump file..	**apiKey*** - API Key to access your OpManager server.	http://localhost:8060/api/json/admin/generateHeapDump?apiKey=081c9ac51ba16ab061d5efee583dcd2f
GetThreadDump	GET	Fetches thread dump.	**apiKey*** - API Key to access your OpManager server.	http://localhost:8060/api/json/admin/GetThreadDump?apiKey=83155f195334a19df5e58a8a33a6f804
GetSystemInformation	GET	Obtains System information.	**apiKey*** - API Key to access your OpManager server.	http://localhost:8060/api/json/admin/GetSystemInformation?apiKey=081c9ac51ba16ab061d5efee583dcd2f

GetRebrandDetails	GET	Fetches the rebrand details.	**apiKey*** - API Key to access your OpManager server. **alarmscount*** - Alarms count. **rawdata*** - Raw data (number of days). **hourlydata*** - Hourly data (number of days).	http://localhost:8060/api/json/admin/GetRebrandDetails?apiKey=081c9ac51ba16ab061d5efee583dcd2f&alarmscount=10000&rawdata=7&hourlydata=30
rebrandOpManager	GET	Rebrands the product.	**apiKey*** - API Key to access your OpManager server. **productName*** - Rebranded product name.	http://localhost:8060/api/json/admin/rebrandOpManager?apiKey=6d36ff8426cff396b81b248e5c458604&productName=ServerMonitoringTool
regenerateAPIKey	GET	Regenerates API Key	**apiKey*** - API Key to access your OpManager server.	http://localhost:8060/api/json/admin/regenerateAPIKey?apiKey=081c9ac51ba16ab061d5efee583dcd2f
getActualScheduleRate	GET	Gets actual schedule rate	**apiKey* -** API Key to access your OpManager server. **fromTime* -** Data collection From time **ToTime* ** Data collected To time.	http://localhost:8060/api/json/diagnostics/getActualScheduleRate?apiKey=081c9ac51ba16ab061d5efee583dcd2f&fromTime=2013-12-21 00:01:15&toTime=2013-12-21 23:59:15
deleteDomain	POST	Deletes the domain name.	**apiKey*** - API Key to access your OpManager server. **domainName*** - Name of the domain.	http://localhost:8060/api/json/admin/deleteDomain?apiKey=081c9ac51ba16ab061d5efee583dcd2f&domainName=ZOHOCORP
Alarm Escalation				

addAlarmEscalationRules	POST	Add Alarm Escalation rules	**apiKey* -** API Key to access your OpManager server. **rulename* -** Alarm escalation rule name. **interval* -** interval for escalation. **alarmlife* -** period of alarm. **units* -** quantity/count. **severity* -** severity of escalation. **category* -** alarm escalation category. **notificationType* -** Type of notification eg., SMS or EMAIL. **ackStatus** **acknowledgeme**nt status eg. diable. Will be enabled by default. if notificationType=**SMS**, number **&#65533;** number to which sms is to be sent. smsMessage **&#65533;** SMS message. if notificationType=**EMAIL**, fromemailid **&#65533;** Email id from which the escalate notification being sent. **toemailid &#65533;** Email id to whom the notification has to be sent. **subject &#65533;** Subject of escalate notification. **message &#65533;** Alarm escalation message.	http://localhost:8060/api/json/admin/addAlarmEscalationRules?apiKey=081c9ac51ba16ab061d5efee583dcd2f&category=Server&emailNotify=true&alarmlife=1&severity=1&message=test&interval=5&fromemailid=rejoe@testdomain.com&period=1&server=smtp&portNumber=25&smsNotify=false&rulename=test2&units=un&alarmLifeUnit=1&toemailid=rejoe@testdomain.com&selectedBV=test&subject=test
deleteAlarmEscalationRules	POST	Deletes alarm escalation rules.	**apiKey* -** api key. **rulename* -** Alarm escalation rule names. **(comma-separated)**	http://localhost:8060/api/json/admin/deleteAlarmEscalationRules?apiKey=081c9ac51ba16ab061d5efee583dcd2f&rulename=test2

showEscalationRules	GET	Provides all Alarm Escalation rules available.	**apiKey* -** api key.	http://localhost:8060/api/json/admin/showEscalationRules?apiKey=081c9ac51ba16ab061d5efee583dcd2f
updateAlarmEscalationRules	POST	Updates the Alarm Escalation Rule.	**apiKey* -** api key. **rulename* -** Alarm escalation rule name. **interval* -** interval for escalation. **alarmlife* -** period of alarm. **units* -** quantity/count. **severity* -** severity of escalation. **category* -** alarm escalation category. **notificationType* -** Type of notification eg., SMS or EMAIL. if notificationType=SMS, number **&#65533;** number to which sms is to be sent. **smsMessage &#65533;** SMS message. if notificationType=**EMAIL,** fromemailid **&#65533;** Email id from which the escalate notification being sent. **toemailid &#65533;** Email id to whom the notification has to be sent. **subject &#65533;** Subject of escalate notification. **message &#65533;** Alarm escalation message.	http://localhost:8060/api/json/admin/updateAlarmEscalationRules?apiKey=081c9ac51ba16ab061d5efee583dcd2f&category=Server&emailNotify=true&alarmlife=1&severity=1&message=test&interval=5&fromemailid=rejoe@testdomain.com&period=1&notificationType=Email&portNumber=25&smsNotify=false&rulename=test2&units=un&alarmLifeUnit=1&server=smtp&selectedBV=test20&toemailid=rejoe@testdomain.com&subject=test
viewAlarmEscalationRules	GET	Provides information about the Alarm Escalation rule	**apiKey* -** API Key to access your OpManager server. **rulename* -** Alarm escalation rule name.	http://localhost:8060/api/json/admin/viewAlarmEscalationRules?apiKey=081c9ac51ba16ab061d5efee583dcd2f&rulename=test2
Alerts				

acknowledgeAlarm	POST	Allows to acknowledge an alarm.	**apiKey* -** API Key to access your OpManager server. **entity -** Entity of the alarm.	http://localhost:8060/api/json/alarm/acknowledgeAlarm?apiKey=081c9ac51ba16ab061d5efee583dcd2f&entity=222222222
addEvent	POST	Adds an event.	**apiKey* -** API Key to access your OpManager server. **source* -** Name of the source device of the event. **severity* -** The severity of the event. Following are the severity levels and its ID: Critical - 1 Trouble - 2 Attention - 3 Service Down - 4 **message* -** The message that is displayed when the event is generated. **alarmCode -** 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. **eventType -** Description of the event type	http://localhost:80/api/json/events/addEvent?apiKey=3d4d1f45e4c445eb52b9f1c51bc7c1ca&source=Cisco2081_router&severity=1&message=DownStatus&alarmCode=Threshold-DOWN&entity=Cisco2081_router

addNotes	POST	Adds notes to an alarm.	**apiKey* -** API Key to access your OpManager server. **entity* -**Entity of the alarm. **notes*** **&#65533;** Text that has to be added as notes to the alarm**.**	http://localhost:8060/api/json/alarm/addNotes?apiKey=081c9ac51ba16ab061d5efee583dcd2f&notes=test&entity=222222222
alarmProperties	GET	Provides the details of an alarm eg: status, acknowledgement	**apiKey* - API Key to access your OpManager server.** **entity* - Entity of the alarm.**	http://localhost:8060/api/json/alarm/alarmProperties?apiKey=081c9ac51ba16ab061d5efee583dcd2f&entity=222222222
clearAlarm	POST	Clears an alarm.	**apiKey* - API Key to access your OpManager server.** **entity* - Entity of the alarm.**	http://localhost:8060/api/json/alarm/clearAlarm?apiKey=081c9ac51ba16ab061d5efee583dcd2f&entity=222222222
deleteAlarm	POST	Deletes an alarm.	**apiKey* - API Key to access your OpManager server.** **entity* - Entity of the alarm.**	http://localhost:8060/api/json/alarm/deleteAlarm?apiKey=081c9ac51ba16ab061d5efee583dcd2f&entity=222222222
getAnnotation	GET	Provides the notes available for an alarm.	**apiKey* - API Key to access your OpManager server.** **entity* - Entity of the alarm.**	http://localhost:8060/api/json/alarm/getAnnotation?apiKey=081c9ac51ba16ab061d5efee583dcd2f&entity=222222222
getTopDevicesByAlarms	GET	Provides the list of top devices by alarms count.	**apiKey* - API Key to access your OpManager server.** **eventType* - Type of the Event eg. Trap or Eventlog Alarm**	http://localhost:8060/api/json/alarm/getTopDevicesByAlarms?apiKey=081c9ac51ba16ab061d5efee583dcd2f&eventType=THRESHOLD-DOWN
getTopDevicesByEvents	GET	Lists the top devices by events count.	**apiKey* - API Key to access your OpManager server.** **eventType* - Type of the Event eg. Trap or Eventlog Alarm**	http://localhost:8060/api/json/events/getTopDevicesByEvents?apiKey=081c9ac51ba16ab061d5efee583dcd2f&eventType=THRESHOLD-DOWN

listAlarmEscalationRules	GET	Lists all the alarm escalation rules created.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/listAlarmEscalationRules?apiKey=081c9ac51ba16ab061d5efee583dcd2f
listAlarms	GET	List all the alarms available.	**apiKey* - API Key to access your OpManager server.** **deviceName - Name of the device whose alarms alone has to be filtered** **severity - The severity of the alarm. Following are the severity levels and its ID:** **Critical - 1** **Trouble - 2** **Attention - 3** **Service Down - 4** **Category - The category to which the device belongs to. Eg. Router** **fromTime - The beginning time for the filter. It should be in yyyy-mm-dd hh:mm:ss format.** **toTime - The end time for the filter. It should also be in yyyy-mm-dd hh:mm:ss format.**	http://localhost:8060/api/json/alarm/listAlarms?apiKey=081c9ac51ba16ab061d5efee583dcd2f&Category=Server&deviceName=opman-k8r2s-64-3..testdomain.com&severity=1&toTime=2014-02-12 23:59:00&fromTime=2014-02-12 00:01:01
listNotificationProfiles	GET	Lists all the notification profiles created in OpManager.	**apiKey* - API Key to access your OpManager server.** profileFilter- All - For Global profiles and for other type of profiles(Send+Email, Send+SMS, Send+Modem+SMS, Run+System+Command, etc..) isGlobal- false - for Device Specific Profiles Filter.	http://localhost:8060/api/json/admin/listNotificationProfiles?apiKey=641dc197c94dcabb6af38c64352e5954&isFluidic=true&profileFilter=All

associateNotificationProfiles	POST	Associate Notification Profiles	**apiKey*** - API Key to access your OpManager server. **profiles*** - ProfileID of the profiles to be associated. **deviceName*** - Name of the devices to be associated	http://localhost:80/api/json/admin/associateNotificationProfiles?apiKey=9c6f010cad72bc32abc984143cc5d505**&profiles**=301,302**&deviceName**=opman-k8r2s-64-3.testdomain.com,opman-k8r2s-64-4.testdomain.com
unAcknowledgeAlarm	POST	Allows to unacknowledge an alarm.	**apiKey* - API Key to access your OpManager server.** **entity - Entity of the alarm.**	http://localhost:8060/api/json/alarm/unAcknowledgeAlarm?apiKey=081c9ac51ba16ab061d5efee583dcd2f&entity= 222222222
alarmProperties	GET	Obtains information of the given alarm	apiKey* - API Key to access your OpManager server. entity* - Entity (alarm ID)	http://localhost:8060/api/json/alarm/alarmProperties?apiKey=081c9ac51ba16ab061d5efee583dcd2f&entity=222222222
getAlarmList	GET	Lists all the alarms irrespective of the device/category	apiKey* - API Key to access your OpManager server.	http://localhost:8060/api/json/alarm/getAlarmList?apiKey=081c9ac51ba16ab061d5efee583dcd2f
listEvents	GET	Lists all generated events	apiKey* - API Key to access your OpManager server.	http://localhost:8060/api/json/events/listEvents?apiKey=6d36ff8426cff396b81b248e5c458604
Device discovery				

addDevice	POST	Add a device.	**apiKey* - API Key to access your OpManager server.** **deviceName* - Name of the device to be added.** **netmask - Enter the netmask for discovering the device.** **credentialName - Enter the appropriate credential.** **type - Type of the device. Eg. Windows 2008 R2.** **displayName - Name of the device that has to be displayed in OpManager.**	http://localhost:8060/api/json/discovery/addDevice?apiKey=081c9ac51ba16ab061d5efee583dcd2f&deviceName=opman-k8r2s-64-2.testdomain.com&displayName=opman-k8r2s-64-2.testdomain.com&credentialName=win&netmask=255.255.255.0&type=Windows 2008 R2
addDeviceToGMap	POST	Adds devices to Google map.	**apiKey* - API Key to access your OpManager server.** **deviceName* - Name of the device to be added in business view.** **latitude* - Latitude of the location where the device is present.** **longitude* - Longitude of the location where the device is present.**	http://localhost:8060/api/json/discovery/addDeviceToGMap?apiKey=081c9ac51ba16ab061d5efee583dcd2f&latitude=38.625453&deviceName=opman-k8r2s-64-3.testdomain.com&longitude=120.145568
addDomain	POST	Adds a domain in OpManager.	**apiKey* - API Key to access your OpManager server.** **domainName - Name of the domain that has to be added.** **domainController - Name of the domain controller.** **autoLogin - Enable or Disable are the values that has to be entered.**	http://localhost:8060/api/json/admin/addDomain?apiKey=081c9ac51ba16ab061d5efee583dcd2f&domainController=win2k8master.testdomain.com&autoLogin=true&loginType=All Users&domainName=testdomain

			Enable - Allow the AD user to login into OpManager even if he/she does not have an account in OpManager. Disable - Does not allow the AD user to login into OpManager if he/she does not have an account in OpManager **loginType** - All users - Allows all users from the AD in that domain. Selected Groups - Allows selected user groups from the AD in that domain** **privilege - Operators - Allows the users in that domain to have Read Only permission to OpManager. Administrators - Allows the users in that domain to have Full Access permission to OpManager.** **readOnlyGroups - Allows the users in that group to have Read Only permission to OpManager.** **fullControlGroups - Allows the users in that group to have Full Access permission to OpManager.**	
deleteDevice	POST	Deletes a device.	**apiKey* - API Key to access your OpManager server.** **deviceName* - Name of the device to be deleted.**	http://localhost:8060/api/json/discovery/deleteDevice?apiKey=081c9ac51ba16ab061d5efee583dcd2f&deviceName=opman-k8r2s-64-3.testdomain.com

deleteDomain	POST	Deletes a domain in OpManager.	**apiKey* - API Key to access your OpManager server.** **domainName - Name of the domain that has to be deleted.**	http://localhost:8060/api/json/admin/deleteDomain?apiKey=081c9ac51ba16ab061d5efee583dcd2f&domainName=ZOHOCORP
listCredentials	GET	Gives the list of credentials created in OpManager.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/listCredentials?apiKey=081c9ac51ba16ab061d5efee583dcd2f
listDownTimeSchedules	GET	Gives the list of downtime schedules created.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/listDownTimeSchedules?apiKey=83155f195334a19df5e58a8a33a6f804
RediscoverDevice	POST	Rediscovers a device	apiKey* - API Key to access your OpManager server. name* - Name of the device. snmpCredentialNames* - SNMP Credentials.	http://localhost:8060/api/json/device/RediscoverDevice?apiKey=081c9ac51ba16ab061d5efee583dcd2f&snmpCredentialNames=Public&name=opman-k8r2s-64-3.testdomain.com
reDiscoverInterfaces	POST	Rediscovers the interfaces	apiKey* - API Key to access your OpManager server. deviceName* - Name of the device.	http://localhost:8060/api/json/discovery/reDiscoverInterfaces?deviceName=opman-k8r2s-64-3.testdomain.com&apiKey=081c9ac51ba16ab061d5efee583dcd2f
doSearch	GET	Search a device/interface	apiKey* - API Key to access your OpManager server. type* - Type of the device (DEVICE,INTERFACE, etc). searchString* - Search string (device name, interface name etc).	http://localhost:8060/api/json/discovery/doSearch?apiKey=081c9ac51ba16ab061d5efee583dcd2f&type=DEVICE,INTERFACE&searchString=opman-k8r2s-64-3.testdomain.com

searchDevice	GET	Allows you to search for a device.	apiKey* - API Key to access your OpManager server. deviceName* - Name of the device whose route has to be traced	http://localhost:8060/api/json/discovery/searchDevice?apiKey=081c9ac51ba16ab061d5efee583dcd2f&deviceName=opman-k8r2s-64-3.testdomain.com
Device Snapshot				
addNotesToDevice	POST	Adds notes to a device.	**apiKey* - API Key to access your OpManager server.** **deviceName* - Name of the device to be added** **FIELD_NAMES - List of fields to be added to the device. Eg.: Department=IT**	http://localhost:8060/api/json/device/addNotesToDevice?apiKey=081c9ac51ba16ab061d5efee583dcd2f&deviceName=opman-k8r2s-64-3.testdomain.com&Cabinet=cubicle
associateServiceMonitor	POST	Associate Service monitors to the specified device	**apiKey* - API Key to access your OpManager server.** **deviceName* - Name of the device for which the service to be associated. Give the names by comma separated for bulk association** **serviceName* - Name of the service in comma-separated format.**	http://localhost:8060/api/json/admin/associateServiceMonitor?deviceName=ctestlab-w2012.testdomain.com&apiKey=6d36ff8426cff396b81b248e5c458604&serviceName=WebLogic,Web,Telnet,SMTP
getAssociatedMonitors	GET	Provides the list of monitors associated to a device.	**apiKey* - API Key to access your OpManager server.** **name - name of the device.**	http://localhost:8060/api/json/device/getAssociatedMonitors?apiKey=081c9ac51ba16ab061d5efee583dcd2f&name=opman-k8r2s-64-3.testdomain.com
getAssociatedServiceMonitors	GET	Provides the service monitors associated with the specified device	**apiKey* - API Key to access your OpManager server.** **name* - Name of the device.**	http://localhost:8060/api/json/device/getAssociatedServiceMonitors?apiKey=081c9ac51ba16ab061d5efee583dcd2f&name=opman-k8r2s-64-3.testdomain.com

getDeviceNotes	GET	Provides the details of notes such as floor no. and department name added to a device.	**apiKey* - API Key to access your OpManager server.** **name* - name of the device.**	http://localhost:8060/api/json/device/getDeviceNotes?apiKey=081c9ac51ba16ab061d5efee583dcd2f&name=opman-k8r2s-64-3.testdomain.com
getDeviceSummary	GET	Provides the summary details of a device.	**apiKey* - API Key to access your OpManager server.** **name* - name of the device.**	http://localhost:8060/api/json/device/getDeviceSummary?apiKey=081c9ac51ba16ab061d5efee583dcd2f&name=opman-k8r2s-64-3.testdomain.com
getNotificationProfiles	GET	Provides the list of notification profiles associated to a device.	**apiKey* - API Key to access your OpManager server.** **name* - name of the device.**	http://localhost:8060/api/json/device/getNotificationProfiles?apiKey=83155f195334a19df5e58a8a33a6f804&name=opman-k8r2s-64-3.testdomain.com
getWorkFlows	GET	Provides the list of workflows associated to a device.	**apiKey* - API Key to access your OpManager server.** **name* - name of the device.**	http://localhost:8060/api/json/device/getWorkFlows?apiKey=83155f195334a19df5e58a8a33a6f804&name=opman-k8r2s-64-3.testdomain.com
getAssociatedCredentials	GET	Obtains information on the credentials associated to a device	apiKey* - API Key to access your OpManager server. name* – Name of the device whose credentials need to be fetched.	http://localhost:8060/api/json/device/getAssociatedCredentials?apiKey=081c9ac51ba16ab061d5efee583dcd2f&name=opman-k8r2s-64-3.testdomain.com
getPerfomanceMonitorDetails	GET	Obtains information of the performance monitors for a device	apiKey* - API Key to access your OpManager server. policyName* - Name of the performance monitor. graphName* - Graph name of the performance monitor. name* - Name of the device. checkNumeric* - true or false.	http://localhost:8060/api/json/device/getPerfomanceMonitorDetails?apiKey=6d36ff8426cff396b81b248e5c458604&policyName=WMI-CPUUtilization&graphName=WMI-CPUUtilization&name=172.18.100.130&checkNumeric=true

EditPerfomanceMonitor	POST	Enables editing the configuration of a performance monitor	TroubleThresholdType* - Type of threshold. TroubleThresholdValue* - Trouble threshold value. RearmValue* - Trouble threshold rearm value. Interval – monitoring Interval in mins. TimeAvg – Average time. ThresholdEnabled – true or false. GraphName – Name of the performance monitor graph. WarningThresholdValue – Warning threshold value. Type – threshold type. OidType – OID Type. TroubleMessage – Message to be populated on violating threshold. TroubleThresholdTextValue – Trouble threshold value. TroubleThresholdTextualType – Trouble threshold textual type (equals, contains etc) Oid – OID of the performance monitor. SendClear – True or false. ClrMessage – Message to be displayed when	http://localhost:8060/api/json/device/EditPerfomanceMonitor?troubleThresholdType=max&troubleThresholdValue=25&rearmValue=23&interval=5&timeAvg=&thresholdEnabled=true&graphName=WMI-CPUUtilization&warningThresholdValue=&type=multiple&oidType=&apiKey=6d36ff8426cff396b81b248e5c458604&troubleMessage=$MONITOR is $CURRENTVALUE%, threshold value for this monitor is $THRESHOLDVALUE%&troubleThresholdTextValue=25&troubleThresholdTextualType=Contains&oid=CPU Utilization&sendClear=true&clrMessage=$MONITOR is now back to normal, current value is $CURRENTVALUE%&name=172.18.100.130&criticalThresholdTextValue=&criticalMessage=$MONITOR is $CURRENTVALUE%, threshold value for this monitor is $THRESHOLDVALUE%&criticalThresholdType=max&rearmTextValue=23&criticalThresholdValue=&warningMessage=$MONITOR is $CURRENTVALUE%, threshold value for this monitor is $THRESHOLDVALUE%&yaxisText=Percentage&warningThresholdTextualType=Contains&failureThreshold=1&vendor=&criticalThresholdTextualType=Contains&thresholdName=&warningThresholdType=max&checkNumeric=true&firstTime=false&policyName=WMI-CPUUtilization&instanceName=&rearmTextualType=Not Contains&clearThresholdType=min&displayName=CPU Utilization&warningThresholdTextValue=

			the threshold is cleared. Name &#65533; Device name. CriticalThresholdTextValue &#65533; Critical threshold text value. CriticalMessage &#65533; Message to be displayed on violating critical threshold. CriticalThresholdType &#65533; Type of critical threshold (max, min) RearmTextValue &#65533; Rearm value of critical threshold. CriticalThresholdValue &#65533; Threshold value of the critical alarm. WarningMessage &#65533; Warning message. YaxisText &#65533; Text representing the values in y-axis. WarningThresholdTextualType &#65533; warning threshold text type. FailureThreshold &#65533; Failure threshold value. Vendor &#65533; Vendor of the device. CriticalThresholdTextualType &#65533; Critical threshold textual type. ThresholdName &#65533; name of the threshold. WarningThresholdType &#65533; Type of the warning threshold. CheckNumeric &#65533; True		

			or False. FirstTime &#65533; True or False. PolicyName &#65533; Name of the performance monitor. InstanceName &#65533; Name of the monitor instance. RearmTextualType &#65533; Rearm Textual type. ClearThresholdType &#65533; Clear threshold type. DisplayName &#65533; Displayname of the performance monitor. WarningThresholdTextValue &#65533; Warning threshold text value.	
addPerfomanceMonitors	POST	Adds a new performance monitor for the given device	apiKey* - API Key to access your OpManager server. name* - Name of the device. selectedMonitors* - Name of the performance monitors.	http://localhost:8060/api/json/device/addPerfomanceMonitors?apiKey=6d36ff8426cff396b81b248e5c458604&name=172.18.100.130&selectedMonitors=693,692,203,204,205,304
getPerformanceMonitors	GET	Lists the performance monitors for the given device	apiKey* - API Key to access your OpManager server. deviceName* - Name of the device. category* - Name of the performance monitors. type* - Type of the device	http://localhost:8060/api/json/device/getPerformanceMonitors?apiKey=081c9ac51ba16ab061d5efee583dcd2f&category=Server&deviceName=opman-k8r2s-64-3.testdomain.com&type=Windows 2008 R2

UpdateAdditionalFields	POST	Updates the additional fields present in the device snapshot page	apiKey* - API Key to access your OpManager server. firstTime* - true or false. interfacename* - Name of the interface. type* - Type of the device. UDF1* - Field value. UDF2 ◆ Filed value. UDF3 ◆ Field value. UDF4 ◆ Field value. UDF5 ◆ Field value.	http://localhost:8060/api/json/device/UpdateAdditionalFields?UDF1=qq22&UDF2=&firstTime=true&UDF5=&UDF3=&UDF4=&interfacename=IF-192.168.50.130-399&type=Interface&apiKey=6d36ff8426cff396b81b248e5c458604
UpdateDeviceDetails	POST	Updates device details	apiKey* - API Key to access your OpManager server. vendor* - Vendor of the device. name* - Device name. monitoring* - Monitoring interval. netmask* - Netmask address. displayName* - Displayname of the device. ipAddress* - Device IP address.	http://localhost:8060/api/json/device/UpdateDeviceDetails?apiKey=081c9ac51ba16ab061d5efee583dcd2f&vendor=Microsoft&name=opman-k8r2s-64-2.testdomain.com&Monitoring=60&Netmask=25.255.255.0&displayName=TEST11&ipAddress=172.18.155.78
GetCredentialsForDevice	GET	Obtains the credentials mapped to a device	apiKey* - API Key to access your OpManager server. name* - Name of the device.	http://localhost:8060/api/json/device/GetCredentialsForDevice?apiKey=081c9ac51ba16ab061d5efee583dcd2f&name=opman-k8r2s-64-3.testdomain.com

GetMonitoringInterval	GET	Obtains the configured monitoring interval	apiKey* - API Key to access your OpManager server. name* - Name of the device.	http://localhost:8060/api/json/device/GetMonitoringInterval?apiKey=081c9ac51ba16ab061d5efee583dcd2f&name=opman-k8r2s-64-3.testdomain.com
ConfigureMonitoringInterval	POST	Enables configuration of the monitoring interval	apiKey* - API Key to access your OpManager server. pollenabled* - on or off. protocol* - protocol of the device. name* - Device name. interval* - Monitoring interval.	http://localhost:8060/api/json/device/ConfigureMonitoringInterval?apiKey=081c9ac51ba16ab061d5efee583dcd2f&pollenabled=on&protocol=SNMP&name=opman-k8r2s-64-3.testdomain.com&interval=15
GetSuppressAlarmDetails	GET	Obtains the suppress alarm details of a device	apiKey* - API Key to access your OpManager server. name* - Name of the device.	http://localhost:8060/api/json/device/GetSuppressAlarmDetails?apiKey=081c9ac51ba16ab061d5efee583dcd2f&name=opman-k8r2s-64-3.testdomain.com
ConfigureSuppressAlarm	POST	Configures suppress alarm for a device	apiKey* - API Key to access your OpManager server. name* - Name of the device. suppressInterval* - Alarm suppress interval.	http://localhost:8060/api/json/device/ConfigureSuppressAlarm?apiKey=081c9ac51ba16ab061d5efee583dcd2f&name=opman-k8r2s-64-3.testdomain.com&suppressInterval=3600000
setManaged	POST	Enables the device to be in managed state	apiKey* - API Key to access your OpManager server. name* - Name of the device. manage* - Set device in managed statue (true or false).	http://localhost:8060/api/json/device/setManaged?apiKey=081c9ac51ba16ab061d5efee583dcd2f&manage=false&name=opman-k8r2s-64-3.testdomain.com

deletePerfomanceMonitors	POST	Deletes the performance monitor from the given device	apiKey* - API Key to access your OpManager server. name* ⦁ Name of the device whose credentials need to be fetched. policyName* - Name of the performance monitor.	http://localhost:8060/api/json/device/deletePerfomanceMonitors?apiKey=081c9ac51ba16ab061d5efee583dcd2f&policyName=Win-CPUUtilization&name=opman-k8r2s-64-2.testdomain.com
getInterfaceGraphs	GET	Show graph values for a interface	apiKey* - API Key to access your OpManager server. interfaceName* - Name of the interface. graphName* - Graph name of the performance monitor.	http://localhost:8060/api/json/device/getInterfaceGraphs?interfaceName=IF-192.168.49.106-329&graphName=rxutilization&apiKey=6d36ff8426cff396b81b248e5c458604
fetchMonitorsList	POST	Fetches all configured monitors of a device	apiKey* - API Key to access your OpManager server. username* - Username. category* - Device category. deviceList* - List of devices.	http://localhost:8060/api/json/device/fetchMonitorsList?apiKey=081c9ac51ba16ab061d5efee583dcd2f&username=admin&category=Server&deviceList=opman-k8r2s-64-3.testdomain.com

getInterfaceUtilization	GET	Get utilization of the given interfaces	apiKey* - API Key to access your OpManager server. period* - Period for which graph is required. (fourhours, twohours etc) interfaceList* - List of interfaces.	http://localhost:8060/api/json/device/getInterfaceUtilization?interfaceList=IF-192.168.49.106-335,IF-192.168.49.101-497,IF-192.168.50.7-343,IF-192.168.50.7-338,IF-192.168.50.7-339,IF-192.168.49.101-503,IF-192.168.49.101-504,IF-192.168.49.101-495,IF-192.168.49.101-490,IF-192.168.49.101-494,IF-192.168.49.101-513,IF-192.168.49.101-502,IF-192.168.49.101-512,IF-192.168.49.101-492,IF-192.168.49.101-505,IF-192.168.49.101-498,IF-192.168.49.101-514,IF-cisco2081.testdomain.com-672,IF-192.168.50.7-337,IF-cisco2081.testdomain.com-563,IF-cisco2081.testdomain.com-667,IF-cisco2081.testdomain.com-670,IF-192.168.49.101-549,IF-192.168.49.101-547,IF-192.168.49.101-556,IF-192.168.49.101-558,IF-192.168.49.101-516,IF-192.168.49.101-511,IF-192.168.49.101-520,IF-192.168.49.101-519,IF-192.168.49.101-496,IF-192.168.49.106-330,IF-192.168.49.101-552,IF-192.168.49.101-515,IF-192.168.49.101-550,IF-cisco2081.testdomain.com-995,IF-192.168.49.106-331,IF-192.168.49.146-324,IF-192.168.49.146-322,IF-192.168.49.146-323,IF-192.168.49.106-329&period=twfourhours&apiKey=6d36ff8426cff396b81b248e5c458604
getGraphData	GET	Fetches graph value for the given monitors	apiKey* - API Key to access your OpManager server. index* - Name of the performance monitor. name* - Name of the device. policyName* - Name of the performance monitor.	http://localhost:8060/api/json/device/getGraphData?index=WMI-CPUUtilization&policyName=WMI-CPUUtilization&name=172.18.99.60&apiKey=6d36ff8426cff396b81b248e5c458604
getGraphNames	GET	Obtains the name of all available graphs for the given device	apiKey* - API Key to access your OpManager server. name* - Name of the device.	http://localhost:8060/api/json/device/getGraphNames?apiKey=081c9ac51ba16ab061d5efee583dcd2f&name=opman-k8r2s-64-3.testdomain.com

associateServiceMonitor	POST	Associate service monitor to the device.	apiKey* - API Key to access your OpManager server. deviceName* - Type of the device. serviceName* - Name of the service monitors.	http://localhost:8060/api/json/admin/associateServiceMonitor?apiKey=6d36ff8426cff396b81b248e5c458604&deviceName=msp-k8r2e-64-1.testdomain.com&serviceName=SMTP(25),Web(80),DNS(53),LDAP(389),WebLogic(7001),Telnet(23)
getIPMIDetails	GET	Gets IPMI details for the specified device	apiKey* - API Key to access your OpManager server. deviceName* - Name of the device	http://localhost:8060/api/json/discovery/getIPMIDetails?apiKey=081c9ac51ba16ab061d5efee583dcd2f&deviceName=test
updateIPMIDetails	POST	Allows you to update IPMI details of a device	apiKey* - API Key to access your OpManager server. deviceName* - Name of the device ipmiIP* - IPMI IP address	http://localhost:8060/api/json/discovery/updateIPMIDetails?apiKey=081c9ac51ba16ab061d5efee583dcd2f&deviceName=test&ipmiIP=10.10.10.10
Interface discovery				
discoverInterface	POST	Discovers an interface.	**apiKey* - API Key to access your OpManager server.** **devicesList* - DeviceNames(moname) as comma separated** **intftypes* - Intf types as numeric numbers(E.g: Ethernet=6)** **adminStates* - Interface AdminStatus as numeric numbers(UP=1, DOWN=2)** **operStates* - Interface OperStatus as numeric numbers(UP=1, DOWN=2)**	http://localhost:8060/api/json/discovery/discoverInterface?apiKey=081c9ac51ba16ab061d5efee583dcd2f&adminStates=1&operStates=1&devicesList=opman-k8r2s-64-3.testdomain.com

getInterfaces	GET	Provides the list of interfaces in a device.	**apiKey* - API Key to access your OpManager server.** **name* - name of the device.**	http://localhost:8060/api/json/device/getInterfaces?apiKey=081c9ac51ba16ab061d5efee583dcd2f&name=opman-k8r2s-64-3.testdomain.com
getInterfaceSummary	GET	Provides the summary details of an interface.	**apiKey* - API Key to access your OpManager server.** **interfaceName - name of the interface**	http://localhost:8060/api/json/device/getInterfaceSummary?apiKey=83155f195334a19df5e58a8a33a6f804&interfaceName=IF-opman-k8r2s-64-3.testdomain.com-4505
Inventory				
getInterfaceTypes	GET	Provides the type of interface. eg: serial, ethernet.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/device/getInterfaceTypes?apiKey=081c9ac51ba16ab061d5efee583dcd2f
getProbeURL	GET	Provides the URL of the probe.	**apiKey* - API Key to access your OpManager server.** **name - name of the device.**	http://localhost/api/json/device/addNotesToDevice?apiKey=ac130763a309fcb1613e0b8a551950a2&name=localhost.testdomain.com
listVirtualDevices	GET	Lists all the available virtual devices	**apiKey* - API Key to access your OpManager server.** **virtualDeviceType* - Type of the virtual device.**	http://localhost:8060/api/json/device/listVirtualDevices?virtualDeviceType=VM&apiKey=1d626117b2ac31145ce6bca49bb0458b
fetchInterfacesList	GET	Fetches all interfaces of the given device and category	apiKey* - API Key to access your OpManager server. username* ⦁ username. category* ⦁ Device category. deviceList* ⦁ Device name.	http://localhost:8060/api/json/device/fetchInterfacesList?apiKey=081c9ac51ba16ab061d5efee583dcd2f&username=admin&category=Server&deviceList=opman-k8r2s-64-3.testdomain.com

fetchDevicesList	GET	Fetches all devices available in the given category	apiKey* - API Key to access your OpManager server. username* – username. category* – Device category.	http://localhost:8060/api/json/device/fetchDevicesList?apiKey=081c9ac51ba16ab061d5efee583dcd2f&username=admin&category=Server
listDevices	GET	Lists all the devices added in OpManager.	**apiKey* - API Key to access your OpManager server.** **deviceName - Name of the device that has to be filtered** **type - The device type which has to be filtered. Eg.Windows 7** **Category - The category to which the device belongs to. Eg. Router**	http://localhost:8060/api/json/device/listDevices?apiKey=081c9ac51ba16ab061d5efee583dcd2f&Category=Server&deviceName=opman-k8r2s-64-3.testdomain.com&type=Windows 2008 R2
listInterfaces	GET	Lists all the interfaces in OpManager.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/device/listInterfaces?apiKey=83155f195334a19df5e58a8a33a6f804
getDevicePackageList	GET	Lists device package	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/device/getDevicePackageList?apiKey=081c9ac51ba16ab061d5efee583dcd2f
getCategoryList	GET	Lists all the available device categories	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/device/getCategoryList?apiKey=081c9ac51ba16ab061d5efee583dcd2f
getVendorList	GET	Lists all the vendors	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/device/getVendorList?apiKey=081c9ac51ba16ab061d5efee583dcd2f
Layer2 discovery				

addLayer2Map	POST	Adds a Layer2 devices Map	**apiKey* - API Key to access your OpManager server.** **mapName* - Name of the Map** **seedDevice* - Seed Router Or L3 Switch Address** **startAddr* - Start IpAddress of the network** **endAddr* - End IpAddress of the network** **subnetMask* - Subnet Mask for the network** **credentialName* - Array of credentials existing in Opmanager in comma separated format** **scheduleInterval* - Scheduling Interval (Number Of Days) default 5 days** **discoverNow* - true/false. if true, Add the Layer2 Configuration and discover it. If false, add only the Layer2 Configuration and discover after the schedule period.**	http://localhost:8060/api/json/discovery/addLayer2Map?apiKey=081c9ac51ba16ab061d5efee583dcd2f&credentialName=Public&seedDevice=192.168.49.1&startAddr=192.168.49.1&mapName=Testmap&endAddr=192.168.50.130&discoverNow=true&scheduleInterval=5
deleteLayer2Map	POST	Allows to delete Layer2 map.	**apiKey* - API Key to access your OpManager server.** **mapName* - Name Of the Map to be deleted**	http://localhost:8060/api/json/discovery/deleteLayer2Map?apiKey=081c9ac51ba16ab061d5efee583dcd2f&mapName=Testmap

discoverLayer2Devices	POST	Discovers Layer2 devices	**apiKey* - API Key to access your OpManager server.** **deviceNames* - Array Of Devices in comma-separated format**	http://localhost/api/json/discovery/discoverLayer2Devices?apiKey=ac130763a309fcb1613e0b8a551950a2&deviceNames=192.168.49.1,192.168.50.130
discoverLayer2Map	POST	Discovers Layer2 Map	**apiKey* - API Key to access your OpManager server.** **mapName* - Name Of the Map to be discovered/updated**	http://localhost:8060/api/json/discovery/discoverLayer2Map?apiKey=081c9ac51ba16ab061d5efee583dcd2f&mapName=TestMap
getDiscoveredLayer2Map	GET	Allows you to view the discovered Layer2 Map	**apiKey* - API Key to access your OpManager server.** **mapName* - Name Of the Map to be shown**	http://localhost:8060/api/json/discovery/getDiscoveredLayer2Map?apiKey=081c9ac51ba16ab061d5efee583dcd2f&mapName=TestMap
getLayer2ScanDetails	GET	Obtains information regarding the Layer 2 scans ran up-to-date	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/maps/getLayer2ScanDetails?apiKey=5022357be4231edff71ed25cf960457a
getLayer2Maps	GET	Lists all the Layer2 Maps available in Opmanager	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/maps/getLayer2Maps?apiKey=081c9ac51ba16ab061d5efee583dcd2f
Mail Server Settings				
GetMailServerSettings	GET	Provides the details of mail server settings.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/GetMailServerSettings?apiKey=081c9ac51ba16ab061d5efee583dcd2f
getMailVariables	GET	Get send mail parameters	apiKey* - API Key to access your OpManager server.	http://localhost:8060/api/json/admin/getMailVariables?apiKey=081c9ac51ba16ab061d5efee583dcd2f
Maps				
addBusinessView	POST	Adds a new business view.	**apiKey* - API Key to access your OpManager server.** **bvName* - Name of the Business View.**	http://localhost:8060/api/json/discovery/addBusinessView?apiKey=081c9ac51ba16ab061d5efee583dcd2f&bvName=test

addDeviceToBV	POST	Adds devices to a Business View that is already created.	**apiKey* - API Key to access your OpManager server.** **deviceName* - Name of the device to be added in business view. Enter multiple device names separated by a comma.** **bvName* - Name of the business view.**	http://localhost:8060/api/json/discovery/addDeviceToBV?apiKey=081c9ac51ba16ab061d5efee583dcd2f&deviceName=opman-k8r2s-64-3.testdomain.com&bvName=test
getBusinessDetailsView	GET	Lists all the devices available in a business view.	**apiKey* - API Key to access your OpManager server.** **bvName* - Name of the business view.** **viewLength - Length of the data. If not provided, default length 250 will be used.** **startPoint - data from startPoint Example 1 means, fetch data from 1 - optional parameter**	http://localhost:8060/api/json/businessview/getBusinessDetailsView?apiKey=081c9ac51ba16ab061d5efee583dcd2f&viewLength=250&startPoint=1&bvName=test
getBusinessView	GET	Lists all the business views created.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/businessview/getBusinessView?apiKey=081c9ac51ba16ab061d5efee583dcd2f
getFloorDetails	GET	Provides the details of floor. eg, floor size, tile size.	**apiKey* - API Key to access your OpManager server.** **floorId* - Floor ID obtained from listFloors**	http://localhost:8060/api/json/maps/getFloorDetails?apiKey=83155f195334a19df5e58a8a33a6f804&floorId=1
getInfrastructureView	GET	Provides the details of a particular infrastructure type. eg.: servers.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/discovery/getInfrastructureView?apiKey=081c9ac51ba16ab061d5efee583dcd2f
listFloors	GET	Lists all the floors created.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/maps/listFloors?apiKey=1d626117b2ac31145ce6bca49bb0458b

listRacks	GET	Lists all the racks created.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/maps/listRacks?apiKey=83155f195334a19df5e58a8a33a6f804
getUsersAssociatedToBV	GET	Displays all the users associated to the given business view	**apiKey* - API Key to access your OpManager server.** **BvName* - Business view name.**	http://localhost:8060/api/json/businessview/getUsersAssociatedToBV?apiKey=83155f195334a19df5e58a8a33a6f804&bvName=test
getBVDetails	GET	Fetches information of the given BusinessView	**apiKey* - API Key to access your OpManager server.** **BvName* - Business view name.** **viewId* - Business view Id.**	http://localhost:8060/api/json/businessview/getBVDetails?apiKey=081c9ac51ba16ab061d5efee583dcd2f&viewId=1&bvName=test
Monitoring				
deleteDownTimeSchedules	POST	Deletes a particular downtime scheduler.	**apiKey* - API Key to access your OpManager server.** **scheduleId* ﷼ ID of the schedule**	http://localhost:8060/api/json/admin/deleteDownTimeSchedules?apiKey=83155f195334a19df5e58a8a33a6f804&scheduleId=1
addDowntimeSchedule	POST	Used to add a new downtime schedule.	**apiKey* - API Key to access your OpManager server.** **operation* - Add operation for adding a schedule (Add)** **scheduleName* - name of the downtime scheduler** **status* - status of the schedule (enabled by default)** **scheduleDesc - Description about the downtime schedule** **recurrence* - Downtime frequency (OnceOnly | Daily | Weekly | Monthly)** **selectDevicesMethod* - filter by option (Category | BV | Device | URL | GROUP)**	http://localhost/api/json/admin/addDowntimeSchedule?operation=Add&apiKey=83155f195334a19df5e58a8a33a6f804

			(Only one param will be sent from below 5 params based on the selected filter) selectedCateg - selected category selectedDevices - selected devices selectedBV - selected Business view selectedURL - selected URLs selectedLogicalGroup - selected logical group (Below two params will be used only for onceOnly downtime frequency) once_startat - yyyy-mm-dd hh:mm (year-month-date hour:min) once_endat - yyyy-mm-dd hh:mm (year-month-date hour:min) (Below three params will be used only for Daily downtime frequency) from_time - hh:mm (hour:min) to_time - hh:mm (hour:min) daily_effectfrom - yyyy-mm-dd (year-month-date) (Below four params will be used only for Weekly downtime frequency) startday - (Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday) endday - (Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday) from_time - hh:mm (hour:min)		

			to_time - hh:mm (hour:min) (Below param will be used only for Monthly downtime frequency) monthlyType - (monthlyDate|monthlyDay) (Below params will be used for monthly date wise frequency) startday -month date (32 for last date of every month) endday - month date (32 for last date of every month) from_mins - minutes 00 to 59 to_mins - minutes 00 to 59 from_hrs - hours 00 to 23 to_hrs - hours 00 to 23 (Below params will be used for monthly day wise frequency) weekOfMonth - week of the month (monthlyDate | monthlyDay) weekday - day (Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday) from_mins - minutes 00 to 59 to_mins - minutes 00 to 59 from_hrs - hours 00 to 23 to_hrs - hours 00 to 23	
updateDowntimeSchedule	POST	Used to update a downtime schedule.	**apiKey* - API Key to access your OpManager server.** **operation* - Edit operation for editing a**	http://localhost/api/json/admin/updateDowntimeSchedule?operation=Edit&MS_INSTANCEID=14&scheduleId=14&apiKey=83155f195334a19df5e58a8a33a6f804

			schedule (Edit) **MS_INSTANCEID* - Downtime scheduler id** **scheduleId* - Downtime scheduler id** **scheduleName* - name of the downtime scheduler** **status* - status of the schedule (enabled by default)** **scheduleDesc* - Description about the downtime schedule** **recurrence* - Downtime frequency (OnceOnly|Daily|Weekly|Monthly)** **selectDevicesMethod* - filter by option (Category|BV|Device|URL|GROUP)** (Only one param will be sent from below 5 params based on the selected filter) selectedCateg - selected category selectedDevices - selected devices selectedBV - selected Business view selectedURL - selected URLs selectedLogicalGroup - selected logical group (Below two params will be used only for onceOnly downtime frequency) once_startat - yyyy-mm-dd hh:mm (year-month-date hour:min) once_endat - yyyy-mm-dd hh:mm (year-month-date hour:min) (Below three params will be used only for Daily downtime frequency)	

			from_time - hh:mm (hour:min) to_time - hh:mm (hour:min) daily_effectfrom - yyyy-mm-dd (year-month-date) (Below four params will be used only for Weekly downtime frequency) startday - (Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday) endday - (Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday) from_time - hh:mm (hour:min) to_time - hh:mm (hour:min) (Below param will be used only for Monthly downtime frequency) monthlyType - (monthlyDate | monthlyDay) (Below params will be used for monthly date wise frequency) startday -month date (32 for last date of every month) endday - month date (32 for last date of every month) from_mins - minutes 00 to 59 to_mins - minutes 00 to 59 from_hrs - hours 00 to 23 to_hrs - hours 00 to 23 (Below params will be used for monthly day		

			wise frequency) weekOfMonth - week of the month (monthlyDate | monthlyDay) weekday - day (Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday) from_mins - minutes 00 to 59 to_mins - minutes 00 to 59 from_hrs - hours 00 to 23 to_hrs - hours 00 to 23	
getDownTimeSchedule	GET	Used to fetch details about a particular downtime schedule	**apiKey* - API Key to access your OpManager server.** **scheduleName* - Name of the downtime scheduler**	http://localhost/api/json/admin/getDowntimeSchedule?scheduleName=test&apiKey=83155f195334a19df5e58a8a33a6f804
getAllVoipMetrics	GET	Lists all the VoIP monitors created.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/discovery/getAllVoipMetrics?apiKey=83155f195334a19df5e58a8a33a6f804
getAllWanMetrics	GET	Lists all the WAN monitors created.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/discovery/getAllWanMetrics?apiKey=83155f195334a19df5e58a8a33a6f804

getAvailabiltyGraphData	GET	Provides the data used to calculate the availability graph.	**apiKey* - API Key to access your OpManager server.** **period* - period for which availability graph is required.** **Parameters:** **LAST_12_HOURS** **LAST_24_HOURS** **TODAY** **YESTERDAY** **LAST_7_DAYS** **LAST_30_DAYS** **THIS_WEEK** **LAST_WEEK** **THIS_MONTH** **LAST_MONTH** **deviceName* - name of the device OR elementID* - MOID of the Interface.**	http://localhost:8060/api/json/device/getAvailabiltyGraphData?apiKey=081c9ac51ba16ab061d5efee583dcd2f&deviceName=opman-k8r2s-64-3.testdomain.com&period=LAST_12_HOURS
getDownDevices	GET	Provides the details of devices that are down.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/discovery/getDownDevices?apiKey=83155f195334a19df5e58a8a33a6f804
getInterfaceMonitors	GET	Provides the list of monitors associated to an interface.	**apiKey* - API Key to access your OpManager server.** **interfaceName - name of the interface.**	http://localhost:8060/api/json/device/getInterfaceMonitors?apiKey=83155f195334a19df5e58a8a33a6f804&interfaceName=IF-opman-k8r2s-64-3.testdomain.com-4505
getInterfaceNotes	GET	Provides the details of the notes added to an interface.	**apiKey* - API Key to access your OpManager server.** **interfaceName - name of the interface**	http://localhost:8060/api/json/device/getInterfaceNotes?apiKey=83155f195334a19df5e58a8a33a6f804&interfaceName=IF-opman-k8r2s-64-3.testdomain.com-4505
getPingResponse	GET	Pings a device and provides the response.	**apiKey* - API Key to access your OpManager server.** **deviceName* - Name of the device which has to be pinged.**	http://localhost:8060/api/json/device/getPingResponse?apiKey=081c9ac51ba16ab061d5efee583dcd2f&deviceName=opman-k8r2s-64-3.testdomain.com

getPollsPerSec	GET	Provides the current polls per second value of OpManager.	**apiKey* - API Key to access your OpManager server.** **graphType* – Type of graph required ie. Pollpersec.** **fromTime* – date string in the format: yyyy-MM-dd HH:mm:ss** **toTime* - date string in the format: yyyy-MM-dd HH:mm:ss**	http://localhost:8060/api/json/diagnostics/getPollsPerSec?apiKey=081c9ac51ba16ab061d5efee583dcd2f&fromTime=2013-12-21 00:01:15&graphType=Pollpersec&toTime=2013-12-21 23:59:15
getTraceResponse	GET	Allows you to get the traceroute to a device.	**apiKey* - API Key to access your OpManager server.** **deviceName* - Name of the device which has to be pinged.**	http://localhost:8060/api/json/device/getTraceResponse?apiKey=081c9ac51ba16ab061d5efee583dcd2f&deviceName=opman-k8r2s-64-3.testdomain.com
listPerformanceMonitors	GET	Lists all the performance monitors added.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/listPerformanceMonitors?apiKey=081c9ac51ba16ab061d5efee583dcd2f
listScriptMonitors	GET	Lists all the script monitors created.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/listScriptMonitors?apiKey=081c9ac51ba16ab061d5efee583dcd2f
listSysLogRules	GET	Lists all the syslog rules created.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/listSysLogRules?apiKey=081c9ac51ba16ab061d5efee583dcd2f
listTrapProcessors	GET	Lists all the trap processor created.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/listTrapProcessors?apiKey=081c9ac51ba16ab061d5efee583dcd2f
listURLMonitors	GET	Lists all the URL monitors created.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/listURLMonitors?apiKey=5070623c57db770f93ca914dc7b598f8
listStatusPollDetails	GET	List status poll details of particular interface type.	apiKey* - API Key to access your OpManager server. typeName* - Type of the device/interface	http://localhost:8060/api/json/admin/listStatusPollDetails?apiKey=081c9ac51ba16ab061d5efee583dcd2f&typeName=Ethernet

TestMonitor	GET	Test Monitor action	**apiKey* - API Key to access your OpManager server.** **name* - Name of the device.** **policyName* - Policy name of the monitor.** **graphName - Graph name.** **instanceName ⁄ Instance name.**	http://localhost:8060/api/json/device/TestMonitor?apiKey=081c9ac51ba16ab061d5efee583dcd2f&policyName=Win-CPUUtilization&graphName=Win-CPUUtilization&name=opman-k8r2s-64-3.testdomain.com
updateDeviceStatus	GET	Pings the device and updates the correct status of a device.	**apiKey* - API Key to access your OpManager server.** **name* - name of the device.**	http://localhost:8060/api/json/device/updateDeviceStatus?apiKey=081c9ac51ba16ab061d5efee583dcd2f&name=opman-k8r2s-64-3.testdomain.com
Proxy Server Settings				
GetProxyServerSettings	GET	Provides the details of proxy server settings.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/GetProxyServerSettings?apiKey=081c9ac51ba16ab061d5efee583dcd2f
SMS Server Settings				
configureSMSServerSettings	POST	Allows to configure the SMS server settings.	**apiKey* - API Key to access your OpManager server.** **portno* - <Name of the Port(eg. COM1).** **mobileno* - Mobile number from which the SMS to be sent**	http://localhost:8060/api/json/admin/configureSMSServerSettings?apiKey=081c9ac51ba16ab061d5efee583dcd2f&mobileno=9840833757&portno=COM21
GetSMSServerSettings	GET	Provides the details of SMS server settings.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/GetSMSServerSettings?apiKey=081c9ac51ba16ab061d5efee583dcd2f
SysLogs				

deleteSysLogForwarder	POST	Delete SysLog Forwarder	**apiKey* - API Key to access your OpManager server.** **destHost* - Destination Host.** **destPort* - Destination Port.**	http://localhost:8060/api/json/admin/deleteSysLogForwarder?apiKey=081c9ac51ba16ab061d5efee583dcd2f&destHost=opman-k8r2s-64-2&destPort=516
deleteSysLogRule	POST	Delete SysLog Rule	**apiKey* - API Key to access your OpManager server.** **ruleName* - Name of the rule**	http://localhost:8060/api/json/admin/deleteSysLogRule?apiKey=081c9ac51ba16ab061d5efee583dcd2f&ruleName=test11
getSysLogAlertSeverityMap	GET	List SysLog AlertSeverityMap	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/getSysLogAlertSeverityMap?apiKey=081c9ac51ba16ab061d5efee583dcd2f
getSysLogFacilityMap	GET	List SysLog FacilitiesMap	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/getSysLogFacilityMap?apiKey=081c9ac51ba16ab061d5efee583dcd2f
getSysLogForwarders	GET	List SysLog Forwarders	**apiKey* - API Key to access your OpManager server.** **ruleName* - Sys Log Rule Name.**	http://localhost:8060/api/json/admin/getSysLogForwarders?apiKey=081c9ac51ba16ab061d5efee583dcd2f
getSysLogPort	GET	Get SysLog Ports	**apiKey* - API Key to access your OpManager server.** **portNumber*- port Numbers(comma separated)**	http://localhost:8060/api/json/admin/getSysLogPort?apiKey=081c9ac51ba16ab061d5efee583dcd2f
getSysLogRuleContent	GET	SysLog Rule Info	**apiKey* - API Key to access your OpManager server.** **ruleName* - Sys Log Rule Name**	http://localhost:8060/api/json/admin/getSysLogRuleContent?apiKey=081c9ac51ba16ab061d5efee583dcd2f&ruleName=Failed logins
getSysLogSeverityMap	GET	List SysLog SeverityMap	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/getSysLogSeverityMap?apiKey=081c9ac51ba16ab061d5efee583dcd2f

isSysLogRuleExists	GET	Is SysLog Rule Exists	**apiKey* - API Key to access your OpManager server.** **ruleName* - Sys Log Rule Name.**	http://localhost:8060/api/json/admin/isSysLogRuleExists?apiKey=081c9ac51ba16ab061d5efee583dcd2f&ruleName=Failed logins
startSysLogForwarder	POST	Start SysLog Forwarder	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/startSysLogForwarder?apiKey=081c9ac51ba16ab061d5efee583dcd2f
stopSysLogForwarder	POST	Stop SysLog Forwarder	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/stopSysLogForwarder?apiKey=081c9ac51ba16ab061d5efee583dcd2f
updateSysLogForwarder	POST	Update SysLog Forwarder	**apiKey* - API Key to access your OpManager server.** **destHost* - Previous Destination Host.** **destPort* - Previous Destination Port.** **newDestHost* - New Destination Host.** **newDestPort* - New Destination Port.**	http://localhost:8060/api/json/admin/updateSysLogForwarder?apiKey=081c9ac51ba16ab061d5efee583dcd2f&newDestPort=516&destHost=opman-k8r2s-64-3&destPort=515&newDestHost=opman-k8r2s-64-2

updateSysLogRule	POST	Update SysLog Rule	**apiKey* - API Key to access your OpManager server.** **ruleName* - Name of the rule** **facilityName - SysLog Facility** **severityList - SysLog Severity(Comma Separated)** **alertSeverity - OpManager Alert Severity** **alarmMessage - OpManager Alert Message** **matchString - String matched with incoming syslog message** **consecutiveTime - consecutive time** **timeInterval - time interval (if rearmFacilityName is selected then rearmSeverityList should be selected)** **rearmFacilityName - facility name for rearm syslog** **rearmSeverityList : severity list for rearm syslog** **rearmMatchString : String matched with incoming syslog for rearm**	http://localhost:8060/api/json/admin/updateSysLogRule?apiKey=081c9ac51ba16ab061d5efee583dcd2f&description=auth alert rule&alertSeverity=2&matchString=matchstring&facilityName=auth&ruleName=test11&alarmMessage=test&severityList=alert
Templates				

addVendor	POST	Add new vendor name.	apiKey* - api key. vendor* - Vendor name of the device.	http://localhost:8060/api/json/admin/addVendor?apiKey=081c9ac51ba16ab061d5efee583dcd2f&vendor=testvendor3
associateDeviceTemplate	POST	Associate templates to the device.	**apiKey* - API key.** **selectedDevices* - device name (comma-separated).** **typeName* - Device type.**	http://localhost:8060/api/json/admin/associateDeviceTemplate?apiKey=1d626117b2ac31145ce6bca49bb0458b&typeName=Windows 2008 R2&selectedDevices=opman-k8r2s-64-2.testdomain.com
deleteDeviceTemplate	POST	Enables deletion of Device Templates.	**apiKey* - API Key to access your OpManager server.** **typeName* - Template type name.**	http://localhost:8060/api/json/admin/deleteDeviceTemplate?apiKey=081c9ac51ba16ab061d5efee583dcd2f&typeName=3com 3500G-EI
deleteSysoid	POST	Enables deletion of SysOID	**apiKey* - API Key to access your OpManager server.** **typeName* - Template type name.**	http://localhost:8060/api/json/admin/deleteSysoid?apiKey=081c9ac51ba16ab061d5efee583dcd2f&typeName=3com 3500G-EI
editInterfaceTemplates	POST	Edit Interface Template	**apiKey* - API Key to access your OpManager server.** **typeName* - Template type name.** **intfEnabled* - on or off.** **statusPoll* - on.** **enableIntfUtilTemplate – on or off.** **enableIntfErrorTemplate – on or off.** **enableIntfDiscTemplate – on or off.** **If enableIntfUtilTemplate is on, pollInterval* – Polling interval (integer).** **failureThreshold* – Threshold failure value**	http://localhost:8060/api/json/admin/editInterfaceTemplates?apiKey=081c9ac51ba16ab061d5efee583dcd2f&intfEnabled=on&utilRearm=89&discCondition=>&errorRearm=89&discThreshold=90&statusPollFT=2&typeName=Ethernet&statusPoll=on&utilCondition=>&discRearm=89&utilThreshold=90&enableIntfDiscTemplate=on&errorThreshold=90&errorCondition=>&pollInterval=900&enableIntfErrorTemplate=on&enableIntfUtilTemplate=on&failureThreshold=9

			(integer). **statusPollFT* – Status polling (integer).** **if enableIntfErrorTemplate is on, utilThreshold* – threshold value (integer).** **utilRearm* – threshold rearm value (integer).** **utilCondition* – threshold condition (integer).** **if enableIntfDiscTemplate is on, errorThreshold* - error threshold value (integer).** **errorRearm* - error Rearm value (integer).** **errorCondition* - error condition value (integer)**	
listDeviceTemplates	GET	Lists all the device templates created in OpManager.	**apiKey* - API Key to access your OpManager server.** **rows - Number of records per page (default is 100)** **page - Current page count**	http://localhost:8060/api/json/admin/listDeviceTemplates?apiKey=081c9ac51bad5efee583dcd2f&rows=100&page=1&sortByColumn=totaldevices&sortByType=desc

	GET	Lists all the custom device templates created in OpManager.	**apiKey* - API Key to access your OpManager server.** **rows - Number of records per page (default is 100)** **page - Current page count** **type - type of device template (custom/default)**	http://localhost:8060/api/json/admin/listDeviceTemplates?apiKey=081c9ac51bad5efee583dcd2f&type=Custom&rows=100&page=1&sortByColumn=totaldevices&sortByType=desc
listInterfaceTemplates	GET	Lists all the interface templates created.	**apiKey* - API Key to access your OpManager server.** **showMode* - allInterfaces or commonInterfaces**	http://localhost:8060/api/json/admin/listInterfaceTemplates?apiKey=081c9ac51ba16ab061d5efee583dcd2f&showMode=commonInterfaces
updateDeviceTemplate	POST	Updates the device template.	**apiKey* - API Key to access your OpManager server.** **typeName* - Template type name.** **IconName* - Template icon name.** **pingInterval* - Ping Interval.** **category* - Category of Device.** **vendor* - Vendor of device.** **isOidUpdated* - true or false.** **oidStr* - OID String value.** **isMonitorChanged* - true or false.**	http://localhost:8060/api/json/admin/updateDeviceTemplate?apiKey=081c9ac51ba16ab061d5efee583dcd2f&category=switch&vendor=3com&IconName=switch.png&isOidUpdated=no&oidStr=.1.3.6.1.4.1.43.1.8.41&isMonitorChanged=no&typeName=3com 3500G-EI&pingInterval=60

viewDeviceTemplate	GET	Provides information on the template associated to the device	apiKey* - api key. typeID* - Provide Type name.	http://localhost:8060/api/json/admin/viewDeviceTemplate?apiKey=081c9ac51ba16ab061d5efee583dcd2f&typeID=22
viewInterfaceTemplates	GET	View All interface templates	apiKey* - api key. typeName* - Template type name.	http://localhost:8060/api/json/admin/viewInterfaceTemplates?apiKey=081c9ac51ba16ab061d5efee583dcd2f&typeName=Ethernet
getAssociatedCredentials	GET	Obtains information on the credentials associated to a device	apiKey* - API Key to access your OpManager server. name* ⦁ Name of the device whose credentials need to be fetched.	http://localhost:8060/api/json/device/getAssociatedCredentials?apiKey=081c9ac51ba16ab061d5efee583dcd2f&name=opman-k8r2s-64-3.testdomain.com
deletePerfomanceMonitors	POST	Deletes the performance monitor from the given device	apiKey* - API Key to access your OpManager server. name* ⦁ Name of the device whose credentials need to be fetched. policyName* - Name of the performance monitor.	http://localhost:8060/api/json/device/deletePerfomanceMonitors?apiKey=081c9ac51ba16ab061d5efee583dcd2f&policyName=Win-CPUUtilization&name=opman-k8r2s-64-2.testdomain.com
Traps				
deleteTrapForwarder	POST	Delete Trap Forwarder	apiKey* - api Key. destHost* - Destination Host. destPort* - Destination Port.	http://localhost:8060/api/json/admin/deleteTrapForwarder?apiKey=081c9ac51ba16ab061d5efee583dcd2f&destHost=opman-k8r2s-64-4&destPort=170
deleteTrapParser	POST	Delete Trap Parser	**apiKey*- API Key to access your OpManager server.** **trapParserName* - name of the trap parser**	http://localhost:8060/api/json/admin/deleteTrapParser?apiKey=081c9ac51ba16ab061d5efee583dcd2f&trapParserName=testing

disableTrapParser	POST	Disable Trap Parser	**apiKey*- API Key to access your OpManager server.** **trapParserName* - name of the trap parser**	http://localhost:8060/api/json/admin/disableTrapParser?apiKey=081c9ac51ba16ab061d5efee583dcd2f&trapParserName=LinkDown
enableTrapParser	POST	Enable Trap Parser	**apiKey*- API Key to access your OpManager server.** **trapParserName* - name of the trap parser**	http://localhost:8060/api/json/admin/enableTrapParser?apiKey=081c9ac51ba16ab061d5efee583dcd2f&trapParserName=LinkDown
getGenericTypes	GET	Get Trap Generic Types	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/getGenericTypes?apiKey=081c9ac51ba16ab061d5efee583dcd2f
getTrapForwarders	GET	List Trap Forwarders	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/getTrapForwarders?apiKey=081c9ac51ba16ab061d5efee583dcd2f
getTrapParserInfo	GET	Get Trap Parser Details	**apiKey*- API Key to access your OpManager server.** **trapParserName* - name of the trap parser**	http://localhost:8060/api/json/admin/getTrapParserInfo?apiKey=081c9ac51ba16ab061d5efee583dcd2f&trapParserName=LinkDown
startTrapForwarder	POST	Start Trap Forwarder	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/startTrapForwarder?apiKey=081c9ac51ba16ab061d5efee583dcd2f
stopTrapForwarder	POST	Stop Trap Forwarder	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/stopTrapForwarder?apiKey=081c9ac51ba16ab061d5efee583dcd2f
updateTrapForwarder	POST	Update Trap Forwarder	**apiKey*: API Key to access your OpManager server.** **destHost* : Previous Destination Host** **destPort* : Previous Destination Port** **newDestHost* : new Destination Host.** **newDestPort* : new Destination Port**	http://localhost:8060/api/json/admin/updateTrapForwarder?apiKey=081c9ac51ba16ab061d5efee583dcd2f&newDestPort=170&destHost=opman-k8r2s-64-6&destPort=165&newDestHost=opman-k8r2s-64-4
User Management				

addUser	POST	Adds an user in OpManager.	**apiKey* - API Key to access your OpManager server.** **userName* - User name** **password* - password** **privilege* - Privilege for the user. Following privileges are available** *** Administrators - Full Access** *** Operators - Restricted Access.** **bvName - Provides access to the devices devices grouped in the specified business view. Multiple business views can be given by comma separated.** **emailId - Email ID of the user.** **landLine - Land line number of the user.** **mobileNo - Mobile number of the user.** **domainName - Name of the domain to which the user belongs to.**	http://localhost:8060/api/json/admin/addUser?apiKey=081c9ac51ba16ab061d5efee583dcd2f&userName=rejoe@testdomain.com&privilege=Administrators&password=r&emailId=rejoe@testdomain.com

changePassword	POST	Allows you to change the password of a user.	**apiKey* - API Key to access your OpManager server.** **userName* - User name.** **userId* &#65533; User ID.** **domainName - Name of the domain.** **oldPassword* &#65533; old password of the user.** **newPassword* &#65533; new password of the user**	http://localhost:8060/api/json/admin/changePassword?apiKey=081c9ac51ba16ab061d5efee583dcd2f&userName=rejoe@testdomain.com&newPassword=rr&userId=2&oldPassword=r
deleteUser	POST	Deletes a user.	**apiKey* - API Key to access your OpManager server.** **userName* - User name**	http://localhost:8060/api/json/admin/deleteUser?apiKey=081c9ac51ba16ab061d5efee583dcd2f&userName=rejoe@testdomain.com
listUsers	GET	Lists all users created in OpManager.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/admin/listUsers?apiKey=081c9ac51ba16ab061d5efee583dcd2f
updateContactDetails	POST	Allows you to update the contact details of a user.	**apiKey* - API Key to access your OpManager server.** **userName* - User name.** **userId* &#65533; User ID.** **domainName - Name of the domain.** **emailId* - emailid of the user.** **phoneNumber &#65533; phone number of the user.** **mobileNumber &#65533; mobile number of the user**	http://localhost:8060/api/json/admin/updateContactDetails?apiKey=081c9ac51ba16ab061d5efee583dcd2f&userName=rejoe@testdomain.com&emailId=user1@testing.com&domainName=testdomain&userId=10&phoneNumber=04424453446&mobileNumber=04424453446
Virtualization				
Dashboard				

listCCTVView	GET	Lists all the CCTV views	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/dashboard/listCCTVView?apiKey=081c9ac51ba16ab061d5efee583dcd2f
getCCTVView	GET	Gets CCTV view widgets/dashboards	**apiKey* - API Key to access your OpManager server.** **cctvID* - cctv ID.**	http://localhost:8060/api/json/dashboard/getCCTVView?apiKey=081c9ac51ba16ab061d5efee583dcd2f&cctvID=1
deleteCCTVView	POST	Deletes CCTV view	**apiKey* - API Key to access your OpManager server.** **cctvID* - cctv ID.**	http://localhost:8060/api/json/dashboard/deleteCCTVView&cctvID=2&apiKey=081c9ac51ba16ab061d5efee583dcd2f
addCCTVView	POST	Add new CCTV view	dashboardId* - dashboard ID. cctvName* - name of the cctv. cctvDescription* - CCTV id time* - refreshing time interval	http://localhost:8060/api/json/dashboard/addCCTVView?apiKey=081c9ac51ba16ab061d5efee583dcd2f&dashboardId=1&cctvName=testcctv&cctvDescription=newcctv&time=5
getDashBoardsForCCTV	GET	Get dashboards for the given CCTV view	**apiKey* - API Key to access your OpManager server.** **cctvID* - cctv ID.**	http://localhost:8060/api/json/dashboard/getDashBoardsForCCTV?apiKey=081c9ac51ba16ab061d5efee583dcd2f&cctvID=1
deleteWidget	POST	Deletes the widget in dashboard page	**apiKey* - API Key to access your OpManager server.** **widgetID* - Widget ID**	http://localhost:8060/api/json/dashboard/deleteWidget?apiKey=081c9ac51ba16ab061d5efee583dcd2f&widgetID=240

embedWidget	POST	Embeds URL of a widget	apiKey* - API Key to access your OpManager server. regenerate* - true or false height* - height of the widget width* - width of the widget content	http://localhost:8060/api/json/dashboard/embedWidget?apiKey=081c9ac51ba16ab061d5efee583dcd2f&widgetID=144&regenerate=true&height=10&width=10
showWidgets	GET	Display all available widgets in a dashboard	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/dashboard/showWidgets?apiKey=081c9ac51ba16ab061d5efee583dcd2f
deleteDashboard	POST	Deletes a dashboard	apiKey* - API Key to access your OpManager server. dashboardID* - dashboard ID.	http://localhost:8060/api/json/dashboard/deleteDashboard?apiKey=081c9ac51ba16ab061d5efee583dcd2f&dashboardID=7
updateDashboardLayout	POST	Updates dashboard layout	apiKey* - API Key to access your OpManager server. dashboardName* - name of the dashboard. columnWidth* - width. numberOfColumns* - Number of the columns. dashboardID* - ID of the dashboard. dashboardDescription – Description of the dashboard.	http://localhost:8060/api/json/dashboard/updateDashboardLayout?apiKey=081c9ac51ba16ab061d5efee583dcd2f&dashboardName=test&columnWidth=100&numberOfColumns=1&dashboardID=7&dashboardDescription=dess

createDashboard	POST	Creates new dashboard view	apiKey* - API Key to access to your OpManager. dashboardName* - Name of the dashboard. columnWidth* - column width numberOfColumns* - number of columns. selectedWidgets* - widget Ids dashboardDescription – Description of the dashboard.	http://localhost:8060/api/json/dashboard/createDashboard?apiKey=081c9ac51ba16ab061d5efee583dcd2f&dashboardName=test&columnWidth=100&numberOfColumns=1&selectedWidgets=144&dashboardDescription=desssc
getWidget	GET	Fetches all widgets available in the given dashboard	apiKey* - API Key to access your OpManager server. dashboardName* - dashboard ID.	http://localhost:8060/api/json/dashboard/getWidgetsList?dashboardName=ThahirDashboard&apiKey=6d36ff8426cff396b81b248e5c458604
getWidgetData	GET	Displays the data present in the given widget	apiKey* - API Key to access your OpManager server. widgetID* - Widget ID	http://localhost:8060/api/json/dashboard/getWidgetData?apiKey=83155f195334a19df5e58a8a33a6f804&widgetID=255
getWidgetsList	GET	Fetches all widgets available in the given dashboard	apiKey* - API Key to access your OpManager server. dashboardName* - dashboard ID.	http://localhost:8060/api/json/dashboard/getWidgetsList?apiKey=081c9ac51ba16ab061d5efee583dcd2f&dashboardName=dashboardoverview

editCCTVView	POST	Enables editing the CCTV view for configuring CCTV columns	apiKey* - API Key to access your OpManager server. cctvName* - Name of the CCTV view. cctvDescription &#65533; Description of the CCTV view. cctvID* - CCTV Id. time* - Refreshing interval. dashboardId* - Dashboard ID.	http://localhost:8060/api/json/dashboard/editCCTVView?apiKey=081c9ac51ba16ab061d5efee583dcd2f&cctvName=testcctv&cctvDescription=newcctv&cctvID=2&time=5&dashboardId=2
getDashboardList	GET	Fetches all available dashboards	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/dashboard/getDashboardList?apiKey=081c9ac51ba16ab061d5efee583dcd2f
Credential Manager				

addSNMPV3Credential	POST	Add new SNMP V3 credential	apiKey* - API Key to access your OpManager server. port* – Protocol port number. authPwd* - Credential username. privPwd* – Credential password. update – true or false. credentialName* - Credential name. desc – Credential description. privProtocol* – Type of encryption for the protocol. username* - Username for the encryption. retries* - Connection retries count. contextname* - Context name. timeout* - Connection timeout. authProtocol* - Authentication protocol.	http://localhost:8060/api/json/admin/addSNMPV3Credential?apiKey=1d626117b2ac31145ce6bca49bb0458b&port=161&privPwd=privUser&update=false&credentialName=snmpV3credential&desc=v3 credential&privProtocol=DES&authPwd=authUser&username=auth&retries=1&contextname=authUser&timeout=10&authProtocol=MD5

addLinuxCredential	POST	Adds a Linux credential	apiKey* - API Key to access your OpManager server. update* - true or false. pwpmt* - Prompt for password (true or false). credentialName* - Credential name. cmdpmt* - Command prompt (credentials). protocol* - Protocol name. username* - Username. portno* - Port number. logpmt* - Log prompt. password* - Credential password. cliTimeout* - CLI credential timeout.	http://localhost:8060/api/json/admin/addLinuxCredential?update=false&pwpmt=:&credentialName=LinuxTelnet&cmdpmt=$&protocol=telnet&username=test&portno=23&logpmt=:&password=test123&apiKey=83155f195334a19df5e58a8a33a6f804&cliTimeout=10
addWindowsCredential	POST	Add new windows credential.	apiKey* - API Key to access your OpManager server. credentialName* - Credential name. username* - Username (domainname\username). password* - Password.	http://localhost:8060/api/json/admin/addWindowsCredential?apiKey=081c9ac51ba16ab061d5efee583dcd2f&credentialName=win&username=workgroup\administrator&password=Vembu123

addSNMPV1Credential	POST	Add new SNMP V1 credential.	apiKey* - API Key to access your OpManager server. credentialName* - Credential name. writeCommunity* - Write community password. readCommunity* - Read community password.	http://localhost:8060/api/json/admin/addSNMPV1Credential?apiKey=081c9ac51ba16ab061d5efee583dcd2f&credentialName=test1&writeCommunity=Public&readCommunity=Public
WorkFlow				
getWorkflowList	GET	Lists all the workflows associated to a device.	**apiKey* - API Key to access your OpManager server.**	http://localhost:8060/api/json/workflow/getWorkflowList?apiKey=081c9ac51ba16ab061d5efee583dcd2f
*** Mandatory parameters** **** Mandatory if Auto-login is enabled.**				

CMDB Plugin API Beta.

REST API	Method	Description	Parameters	Sample URL
getCIList	GET	List all configuration item	**TECHNICIAN_KEY* - API Key to access server.**	http://172.18.10.195:8080/sdplus/CMDB/getCIList?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97
getAllChanges	GET	List all Changes	**TECHNICIAN_KEY* - API Key to access server.**	http://172.18.10.195:8080/sdplus/Change/getAllChanges?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97
getAllContracts	GET	List all Contract	**TECHNICIAN_KEY* - API Key to access server.**	http://172.18.10.195:8080/sdplus/Contract/getAllContracts?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97
getAllPurchase	GET	List all Purchases	**TECHNICIAN_KEY* - API Key to access server.**	http://172.18.10.195:8080/sdplus/Purchase/getAllPurchase?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97
getAllProblems	GET	List all Problems	**TECHNICIAN_KEY* - API Key to access server.**	http://172.18.10.195:8080/sdplus/Problem/getAllProblems?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97
getCIInfo	GET	Get details of configuration items	**TECHNICIAN_KEY* - API Key to access server.**	http://172.18.10.195:8080/sdplus/CMDB/getCIInfo?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&ciID=603
getAssetRelationShips	GET	Get Map details of Relationship	**TECHNICIAN_KEY* - API Key to access server.**	http://172.18.10.195:8080/sdplus/CMDB/getAssetRelationShips?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&ciID=603

getHardwareDetails	GET	Get details of CI Hardware	**TECHNICIAN_KEY* - API Key to access server.** **ciID* - Configuration Item ID**	http://172.18.10.195:8080/sdplus/CMDB/getHardwareDetails?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&ciID=603
getSoftwareDetails	GET	get details of asset - software	**TECHNICIAN_KEY* - API Key to access server.** **ciID* - Configuration Item ID**	http://172.18.10.195:8080/sdplus/CMDB/getSoftwareDetails?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&format=json&ciID=603
getSystemDetails	GET	Get details of asset - system	**TECHNICIAN_KEY* - API Key to access server.** **ciID* - Configuration Item ID**	http://172.18.10.195:8080/sdplus/CMDB/getSystemDetails?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&ciID=603
getRPCDetails	GET	Get details of asset associated - Request,change, problem	**TECHNICIAN_KEY* - API Key to access server.** **ciID* - Configuration Item ID**	http://172.18.10.195:8080/sdplus/CMDB/getRPCDetails?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&ciID=603
getScanDetails	GET	Get details of asset - Scan	**TECHNICIAN_KEY* - API Key to access server.** **ciID* - Configuration Item ID**	http://172.18.10.195:8080/sdplus/CMDB/getScanDetails?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&ciID=603
getContractsForAsset	GET	Get details of asset associated contracts	**TECHNICIAN_KEY* - API Key to access server.** **ciID* - Configuration Item ID**	http://172.18.10.195:8080/sdplus/CMDB/getContractsForAsset?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&ciID=603
getCostDetails	GET	Get cost details of asset	**TECHNICIAN_KEY* - API Key to access server.** **ciID* - Configuration Item ID**	http://172.18.10.195:8080/sdplus/CMDB/getCostDetails?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&ciID=603
getProblemsInfo	GET	Get problem details	**TECHNICIAN_KEY* - API Key to access server.** **ProblemID* - Problem ID**	http://172.18.10.195:8080/sdplus/Problem/getProblemsInfo?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&ProblemID=1

getProblemAnalysis	GET	Get problem analysis details	**TECHNICIAN_KEY* - API Key to access server.** **ProblemID* - Problem ID**	http://172.18.10.195:8080/sdplus/Problem/getProblemAnalysis?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&ProblemID=1
getProblemSolution	GET	Get solution details for problem	**TECHNICIAN_KEY* - API Key to access server.** **ProblemID* - Problem ID**	http://172.18.10.195:8080/sdplus/Problem/getProblemSolution?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&ProblemID=1
getProblemTask	GET	Get task to be performed for problem	**TECHNICIAN_KEY* - API Key to access server.** **ProblemID* - Problem ID**	http://172.18.10.195:8080/sdplus/Problem/getProblemTask?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&ProblemID=1
getProblemIncidents	GET	Get associated incident/request for problem	**TECHNICIAN_KEY* - API Key to access server.** **ProblemID* - Problem ID**	http://172.18.10.195:8080/sdplus/Problem/getProblemIncidents?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&ProblemID=1
getProblemHistory	GET	Get problem history	**TECHNICIAN_KEY* - API Key to access server.** **ProblemID* - Problem ID**	http://172.18.10.195:8080/sdplus/Problem/getProblemHistory?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&ProblemID=1
getChangeInfo	GET	Get change details	**TECHNICIAN_KEY* - API Key to access server.** **ChangeID* - Change ID**	http://172.18.10.195:8080/sdplus/Change/getChangeInfo?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&ChangeID=2
getContractDetails	GET	Get Contract details	**TECHNICIAN_KEY* - API Key to access server.** **contractID* - Contract ID**	http://172.18.10.195:8080/sdplus/Contract/getContractDetails?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&contractID=303
getContractedAssets	GET	Get asset associated with the contract	**TECHNICIAN_KEY* - API Key to access server.** **contractID* - Contract ID**	http://172.18.10.195:8080/sdplus/Contract/getContractedAssets?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&format=json&contractID=303
getContractRenewal	GET	Get contract renewal details	**TECHNICIAN_KEY* - API Key to access server.** **contractID* - Contract ID**	http://172.18.10.195:8080/sdplus/Contract/getContractRenewal?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&contractID=303

getChildContract	GET	Get child contract details	**TECHNICIAN_KEY*** - **API Key to access server.** **contractID* - Contract ID**	http://172.18.10.195:8080/sdplus/Contract/getChildContract?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&contractID=303
getPoDetails	GET	Get purchase order details	**TECHNICIAN_KEY*** - **API Key to access server.** **PoID* - Purchase order ID**	http://172.18.10.195:8080/sdplus/Purchase/getPoDetails?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&PoID=1
getInvoiceAndPayment	GET	Get invoice and payments details of PO	**TECHNICIAN_KEY*** - **API Key to access server.** **PoID* - Purchase order ID**	http://172.18.10.195:8080/sdplus/Purchase/getInvoiceAndPayment?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&PoID=1
getPoRequest	GET	Get Request associated with PO	**TECHNICIAN_KEY*** - **API Key to access server.** **PoID* - Purchase order ID**	http://172.18.10.195:8080/sdplus/Purchase/getPoRequest?TECHNICIAN_KEY=979ED357-447B-405E-AD74-F9B3EF4B1A97&PoID=1

Third party JavaSCript dependency:

Below is the list of third party code and libraries that OpManager makes use of:

JS File Name	Version	License Type	License File
calendar.js	1.1.6.1	LGPL	LICENSE_JSCALENDAR.html
canvg.js		MIT	MIT-LICENSE.txt
colorpicker.js	1	MIT	LICENSE_COLORPICKER.txt
cropper.min.js	1	MIT	_LICENSE.MD
d3.min.js	3.4.8	BSD	LICENSE_D3.txt
d3.tip.v0.6.3.js	0.6.3	MIT	MIT-LICENSE.txt
ember-shortcuts.js	0.0.3	MIT	LICENSE_SHORTCUTS.txt
ember.min.js	1.9.1	MIT	LICENSE_EMBERJS.txt
filesaver.js		MIT	MIT-LICENSE.txt
Fontello	1	SIL	LICENSE_FONTELLO.txt
Google Fonts - Bitter-Regular.ttf	1.1	SIL Open Font License 1.1	LICENSE_LATO_GOOGLE_FONTS.txt
Google Fonts - Lato-Light.ttf, Lato-Regular.ttf, Lato-Bold.ttf	1.1	SIL Open Font License 1.1	LICENSE_LATO_GOOGLE_FONTS.txt
Google Fonts - RobotoSlab-Thin.ttf, RobotoSlab-Light.ttf, RobotoSlab-Regular.ttf	2	Apache 2.0	LICENSE_LATO_GOOGLE_FONTS.txt
gridstack.min.js	0.2.5	MIT	GRIDSTACK_LICENSE

handlebars.min.js	2.0.0	MIT	LICENSE_HANDLEBARS.txt
html2canvas.js	0.5.0-beta3	MIT	HTML2CANVAS_LICENSE
intro.js	2.3.0	Commercial	INTROJS_LICENSE.txt
jquery-1.9.0.min.js	1.9.0	MIT	LICENSE_JQUERY.txt
jquery-2.1.1.min.js	2.1.1	MIT	LICENSE_JQUERY.txt
jquery-migrate-1.2.1.min.js	1.2.1	MIT	LICENSE_JQUERY_MIGRATE.txt
jquery-ui-1.10.1.custom.min.js	1.10.1	MIT	LICENSE_JQUERY_UI_1_5_3.html
jquery-ui.min.js	2.1.1	MIT	LICENSE_JQUERY_UI.txt
jquery.cookie.js	1	MIT	cm_license_info.html
jQuery.dPassword.js	0.1	MIT	http://www.opensource.org/licenses/mit-license.php
jquery.easing.min.js	1.3	BSD	jQuery_Easing_Plugin_1.3_License
jquery.elastic.source.js	1.6.11	MIT	LICENSE_JQUERY_ELASTIC.txt
jquery.event.drag-2.2.js	2.2	MIT	MIT-LICENSE.txt
jquery.event.drag.live-2.2.js	2.2	MIT	MIT-LICENSE.txt
jquery.event.drop-2.2.js	2.2	MIT	MIT-LICENSE.txt
jquery.event.drop.live-2.2.js	2.2	MIT	MIT-LICENSE.txt
jquery.flot.js	0.8.1.	MIT	LICENSE_FLOT.txt
jquery.flot.pie.js	0.7	MIT	LICENSE_FLOT.txt
jquery.flot.tooltip.js	0.6.1	MIT	LICENSE_FLOT.txt

jquery.gridster.min.js	v0.5.6	MIT	DUCKSBOARD_GRIDSTER_JS_V0_5_6_0_G3140374_LICENSE.txt
jquery.inlineStyler.min.js	1.0.1	MIT	JQUERY.INLINESTYLER_LICENSE
jquery.jqGrid.src.js	4.4.4	MIT	MIT-LICENSE.txt
jquery.mCustomScrollbar.min.js	3.1.5	MIT	LICENSE_CUSTOM_SCROLLBAR_PLUGIN.txt
jquery.mentionsInput.js	1.0.2	MIT	LICENSE_JQUERY_MENTIONS_INPUT.txt
jquery.mousewheel.min.js	3.1.12	MIT	jquery_mousewheel_3_1_12jQuery_Mousewheel_3.1.12_License.txt
jquery.qrcode.min.js	1	MIT	JQUERY-QRCODE_MIT-LICENSE.TXT
jquery.smooth-scroll.min.js	v1.3+	MIT	LICENSE_NMAP.txt
jscolor.js	1.4.0	LGPL	LICENSE_JSCOLOR.txt
jspdf.js	0.9.0	MIT	MIT-LICENSE.txt
jspdf.plugin.addimage.js	0.9.0	MIT	MIT-LICENSE.txt
jsPlumb-1.7.10.js	1.7.10	MIT	LICENSE_JSPLUMB.txt
jstree.min.js	3.0.8	MIT	JSTREE_LICENSE-MIT
lightbox.js	2.51	MIT	MIT-LICENSE.txt
moment-timezone-with-data.min.js	0.5.4	MIT	MOMENT_TIMEZONE_LICENSE
moment.min.js	2.13.0	MIT	MOMENT_LICENSE.txt
morris.js	0.5.0	BSD	MORRIS_LICENSE.txt
PointerLockControls.js	1	MIT	Threejs_License.txt
radialProgress.js		MIT	LICENSE_RADIALPROGRESS.txt
raphael-min.js	2.1.0	MIT	LICENSE_RAPHAEL.txt

rgbcolor.js	1	MIT	CANVG_MIT-LICENSE.TXT
rickshaw.js		MIT	LICENSE_RICKSHAW.txt
select2.min.js	4.0.3	MIT	select2_LICENSE.html
Three.js	Revision 49	MIT	LICENSE_THREE_JS.txt
timeline.js	3.3.10	MPL	TIMELINEJS3_3_0_0_LICENSE.html
underscore-min.js	1.3.3	MIT	LICENSE_JQUERY_UNDERSCORE.txt
vis.min.js	4.16.1	Apache 2.0	VISJS_LICENSE.html

Third-party Library dependency

Below is the list of code and libraries OpManager makes use of:

JAR Name	Version Number	License Type	3rd Party Organization
Java	1.8.0.181	Sun Microsystems, Inc. Binary Code License Agreement	Sun Microsystems, Inc.
Postgresql	10.12	Postgresql License	Postgresql
Apache Tomcat	8.5.43	Apache License, Version 2.0	Apache Software Foundation
activation.jar	1.0.2	Sun Microsystems, Inc. Binary Code License Agreement	Sun Microsystems, Inc.
activation.jar	1.0.2	Sun Microsystems, Inc. Binary Code License Agreement	Sun Microsystems Inc.
annotations-api.jar	3.0.FR	Apache License, Version 2.0	Apache Software Foundation
antisamy-1.5.3.jar	1.5.3	The BSD 3-Clause License	The Open Web Application Security Project (OWASP)
axis.jar	1.4	Apache License, Version 2.0	Apache Web Services
batik-awt-util.jar	1.0	Apache License, Version 2.0	Apache Software Foundation
batik-dom.jar	1.0	Apache License, Version 2.0	Apache Software Foundation
batik-svggen.jar	1.0	Apache License Version 2.0	Apache Software Foundation
batik-util.jar	1.7+r608262	Apache License, Version 2.0	The Apache Software Foundation
batik-util.jar	1.0	Apache License, Version 2.0	Apache Software Foundation
batik-xml.jar	1.0	Apache License, Version 2.0	Apache Software Foundation
bcpkix-jdk15on-1.59 jar	1.59	MIT License	BouncyCastle.org
bcprov-jdk15on-1.59.jar	1.59.0	MIT License	BouncyCastle.org

catalina-ant.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
catalina-ha.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
catalina-storeconfig.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
catalina-tribes.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
catalina.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
cewolf.jar	1.4.2	LGPLv2	Sun Microsystems, Inc.
commons-beanutils-1.9.3.jar	1.9.3	Apache License, Version 2.0	Apache Software Foundation
commons-beanutils.jar	1.6	Apache License, Version 2.0	Apache Software Foundation
commons-chain-1.2.jar	1.2	Apache License, Version 2.0	The Apache Software Foundation
commons-codec-1.3.jar	1.3	Apache License, Version 2.0	Apache Software Foundation
commons-codec-1.3.jar	1.3	Apache License Version 2.0	Apache Software Foundation
commons-codec-1.4.jar	1.4	Apache License, Version 2.0	Apache Software Foundation
commons-codec-1.7.jar	1.7	Apache License, Version 2.0	Apache Software Foundation
commons-codec-1.7.jar	1.7	Apache License, Version 2.0	Apache Software Foundation
commons-collections.jar	3.2.2	Apache License, Version 2.0	Apache Software Foundation
commons-daemon.jar	1.0.15	Apache License, Version 2.0	Apache Software Foundation
commons-digester.jar	1.8	Apache License, Version 2.0	Apache Software Foundation
commons-fileupload-1.3.3.jar	1.3.3	Apache License, Version 2.0	Apache Software Foundation
commons-httpclient-3.0-rc1.jar	3.0-rc1	Apache License Version 2.0	Apache Software Foundation

commons-httpclient-3.1.jar	3.1	Apache License, Version 2.0	Apache Software Foundation
commons-io-1.2.jar	1.2	Apache License, Version 2.0	Apache Software Foundation
commons-lang-2.0.jar	2.0	Apache Software License, Version 1.1	Apache Software Foundation
commons-lang3-3.1.jar	3.1	Apache License, Version 2.0	Apache Software Foundation
commons-logging-1.1.jar	1.1	Apache License, Version 2.0	Apache Software Foundation
commons-logging-api.jar	1.1	Apache License, Version 2.0	Apache Software Foundation
commons-logging.jar	1.1	Apache License Version 2.0	Apache Software Foundation
commons-logging.jar	1.1	Apache License, Version 2.0	Apache Software Foundation
commons-math3-3.6.1.jar	3.6.1	Apache Commons, License agreement	Apache Software Foundation
commons-net-2.0.jar	2.0	Apache License Version 2.0	Apache Software Foundation
commons-net-3.3.jar	3.3	Apache License, Version 2.0	Apache Software Foundation
commons-pool-1.5.6.jar	1.5.6	Apache License, Version 2.0	Apache Software Foundation
commons-pool-1.6.jar	1.6	Apache License, Version 2.0	Apache Software Foundation
commons-validator-1.3.1.jar	1.3.1	Apache License, Version 2.0	Apache Software Foundation
commons-vfs-2.1.jar	2.1	Apache License, Version 2.0	Apache Software Foundation
concurrent.jar	1.3.3	GPL	oswego.edu
diffutils-1.2.1.jar	1.2.1	Apache License, Version 2.0	diffutils
dnsjava-2.0.6.jar	2.0.6	BSD License	dnsjava
dnsjava-2.0.6.jar	2.0.6	BSD License	dnsjava
dom4j-1.6.1.jar	1.6.1	BSD license	MetaStuff Ltd.

dom4j-1.6.1.jar	1.6.1	BSD	MetaStuff Ltd.
ecj-4.4.1.jar	4.4.1	Eclipse Public License Version 1.0	Eclipse
ecj-4.6.3.jar	4.6.3	Eclipse Public License Version 1.0	Eclipse
edtftpj.jar	2.0.5	LGPL	Enterprise Distributed Technologies
ehcache-core-2.6.3.jar	2.6.3	Apache 2.0	Ehcache Core
el-api.jar	3.0.FR	Apache License, Version 2.0	Apache Software Foundation
esapi-2.1.0.jar	2.1.0	Code License - New BSD License,Content License - Create Commons 3.0 BY-SA	The Open Web Application Security Project (OWASP)
fontbox-2.0.8 jar	2.0.8	Apache 2.0	Apache Software Foundation
gson-1.3.jar	1.3	Apache License Version 2.0	Google GSON
guava.jar	14.0.1	Apache License, Version 2.0	Guava: Google Core Libraries for Java
htmlparser.jar	1.5	LGPL Version 2.1	htmlparser.org
httpclient-4.2.5.jar	4.2.5	Apache License Version 2.0	The Apache Software Foundation
httpcore-4.3.2.jar	4.3.2	Apache License Version 2.0	The Apache Software Foundation
httpmime-4.3.4.jar	4.3.4	Apache License Version 2.0	The Apache Software Foundation
iijdbc.jar	4.0.9	GPL 2.0	Actian Corporation
IntelDCM.jar	3.7	Intel Software License Agreement	Intel DCM
iText-2.1.7.jar	2.1.7	MPL 1.1	lowagie.com
j2ssh-common.jar	0.2.7	LPGL 2.1	J2SSH
j2ssh-core.jar	0.2.7	LPGL 2.1	J2SSH
jasper-el.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
jasper.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
jasperreports-3.7.3.jar	3.7.3	LGPL 3	Jaspersoft

jasperreports-fonts.jar	3.7.3	LGPL 3	Jaspersoft
jaspic-api.jar	1.1.FR	Apache License, Version 2.0	Apache Software Foundation
javacsv.jar	2.0	LGPL 2.1	Java CSV
javassist-3.12.1.GA.jar	3.12.0.GA	Usually Distributed-MPL 1.1 ,Bundled with jboss- LGPL 2.1	Shigeru Chiba, Tokyo Institute of Technology
JavaPNS_2.2.jar	2.2 r000	LGPL	Google Code Archive
jaxb-api.jar	2.1	BSD license	Sun Microsystems, Inc.
jaxb-impl.jar	2.1.3	BSD license	Sun Microsystems, Inc.
jaxrpc.jar	1.1	Java Specifications	JCP
jboss-j2ee.jar	3.2.6	LGPL 2.1	JBoss
jcifs-1.3.16.jar	1.3.16	LGPL Version 2.1	jcifs
jcommon.jar	3.8	ManageEngine Internal Software	JUnit
jdt-compiler-3.1.1.jar	3.1.1	EPL 1.0	Eclipse
j*s*a-1.0.17.jar	1.0.17	EULA	IOPLEX Software
j*s*a-1.0.17.jar	1.0.17	IOPLEX Software EULA	IOPLEX Software
jfreechart.jar	3.8	LGPL Version 2.1	JUnit
jlibdiff.jar	1.1	LGPLv2	JLibDiff
json-20190722.jar	20190722	JSON License	JSON.org
jsp-api.jar	2.3.FR	Apache License, Version 2.0	Apache Software Foundation
jstl.jar	1.0.3	CDDL, GPL 2	JavaServer Pages Standard Tag Library (JSTL)
jta.jar	1.0.1a	Binary Code License	Java Transaction API
jtds-1.2.2.jar	1.2.2	LGPL Version 2.1	jTDS JDBC Driver
log4j-1.2.8.jar	1.2.8	Apache License, Version 2.0	Apache Software Foundation
log4j-boot.jar	3.2.6	Apache 1.1	JBoss
lucene-analyzers-common.jar	4.2.6	Apache License, Version 2.0	The Apache Software Foundation

lucene-core.jar	4.6.0	Apache License, Version 2.0	The Apache Software Foundation
lucene-highlighter.jar	4.6.0	Apache License, Version 2.0	The Apache Software Foundation
lucene-misc.jar	4.6.0	Apache License, Version 2.0	The Apache Software Foundation
lucene-queryparser.jar	4.6.0	Apache License, Version 2.0	The Apache Software Foundation
lucene-suggest.jar	4.6.0	Apache License, Version 2.0	The Apache Software Foundation
Mail.jar	1.4.7	CDDL Version 1.0	Sun Microsystems, Inc.
Mail.jar	1.4.7	Binary Code License	JavaMail API
maverick-all.jar	1.4.18	SSHTOOLS SOFTWARE LICENSE	J2SSH Maverick
maverick-legacy-client-all.jar	1.6.28	OEM	Maverick Legacy
maverick-legacy-server-all.jar	1.6.28	OEM	Maverick Legacy
msgpack-0.6.7.jar	0.6.7	Apache License, Version 2.0	MessagePack for Java
NamedRegEx.jar	0.2.5	Apache 2.0	named-regexp
nekohtml.jar	1.9.17	Apache License Version 2.0	World Wide Web Consortium (W3C)
nekohtml.jar	1.9.21	Apache License, Version 2.0	Andy Clark, Marc Guillemot
nipper.exe	1.3.17	GPL 3	Nipper Software products
opencsv.jar	2.4	Apache 2.0	OpenCSV
OpenForecast-0.4.0.jar	0.4	LGPLv2	OpenForecast
oscache.jar	1.1	The OpenSymphony Software License, Version 1.1	The OpenSymphony Group
phantomjs.exe	2.1.1	BSD	Phantom JS
poi-3.0.1-FINAL-20070705.jar	3.0.1-FINAL-20070705	Apache License Version 2.0	Apache Software Foundation
poi-3.9-20121203.jar	3.9	Apache License, Version 2.0	Apache Software Foundation

poi-ooxml-3.9-20121203.jar	3.9	Apache License, Version 2.0	Apache Software Foundation
poi-ooxml-schemas-3.9-20121203.jar	3.9	Apache License, Version 2.0	Apache Software Foundation
postgresql_jdbc4.jar	9.2.1	BSD	Postgres
prefuse.jar	beta version	BSD License	Prefuse
radclient3.jar	3.43p	Radius Client License	AXL Software
rocksaw-1.0.1.jar	1.0.1	Apache 2.0	RockSaw
RXTXcomm.jar	2.2	LGPL 2.1	RXTX
saaj.jar	1.2	Java Specifications	JCP
servlet-api.jar	3.1.FR	Apache License, Version 2.0	Apache Software Foundation
slf4j-api-1.6.1.jar	1.6.1	MIT License	SLF4J
slf4j-jdk14-1.6.1.jar	1.6.1	MIT License	SLF4J
SMSLib.jar	3.5.3	Apache License Version 2.0	SMSLIB
SMSServer.jar	3.5.3	Apache License Version 2.0	SMSLIB
snakeyaml-1.11.jar	1.11.0	Apache 2.0	SnakeYAML
SparkGateway.jar	5.0.0	OEM	Remote Spark Corp.
ss_css2.jar	1.4.1	LGPLv2.1	Silicon Graphics, Inc.
standard.jar	1.0.3	Apache 1.0	Apache Software Foundation
struts-core-1.3.11.jar	1.3.11-SNAPSHOT	Apache License, Version 2.0	Apache Software Foundation
struts-el-1.3.11.jar	1.3.11-SNAPSHOT	Apache License, Version 2.0	Apache Software Foundation
struts-extras-1.3.11.jar	1.3.11-SNAPSHOT	Apache License, Version 2.0	Apache Software Foundation
struts-taglib-1.3.11.jar	1.3.11-SNAPSHOT	Apache License, Version 2.0	Apache Software Foundation
struts-tiles-1.3.11.jar	1.3.11-SNAPSHOT	Apache License, Version 2.0	Apache Software Foundation
struts.jar	1.1	Apache License, Version 1.1	Apache Software Foundation

syslog4j-0.9.46-bin.jar	0.9.46	LGPL Version 2.1	Productivity.ORG
terminal-ssh-maverick.jar	2.0.9	MIT	Terminal Components Maverick SSH
terminal-web.jar	2.0.9	MIT	Terminal Components Maverick SSH
terminal.jar	2.0.9	MIT	Terminal Components Maverick SSH
tomcat-api.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
tomcat-coyote.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
tomcat-dbcp.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
tomcat-i18n-es.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
tomcat-i18n-fr.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
tomcat-i18n-ja.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
tomcat-jdbc.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
tomcat-jni.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
tomcat-juli.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
tomcat-util-scan.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
tomcat-util.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
tomcat-websocket.jar	8.5.13	Apache License, Version 2.0	Apache Software Foundation
ua-parser.jar	-	BSD	UA Parser
velocity-1.4.jar	1.4	Apache 2.0	Velocity
velocity-dep-1.4.jar	1.4	Apache 2.0	Velocity
vijava5120121125.jar	5.1	BSD License	VMWare

vim.jar	VMware® Software Developer Kit (SDK) Agreement	VMWare	VMware Inc.
vimsamples.jar	VMware® Software Developer Kit (SDK) Agreement	VMWare	VMware Inc.
virtualsession.jar	2.0.9	MIT	Terminal Components Maverick SSH
vserv-tcpip-0.9.2.jar	0.9.2	Apache License Version 2.0	Virtual Services TCP/IP
websocket-api.jar	1.1.FR	Apache License, Version 2.0	Apache Software Foundation
winpcap-nmap-4.12.exe	4.12	GPL	Winpcap
wrapper.exe	3.5.15	Commercial- Tanuki Software, Ltd.Development Software License Agreement Version 1.1	Tanuki Software, Ltd.
wrapper.jar	3.5.15	Tanuki Software, Development Software License Agreement Version 1.1	Tanuki Software, Ltd.
wrapper.jar	3.5.15	Commercial- Tanuki Software, Ltd.Development Software License Agreement Version 1.1	Tanuki Software, Ltd.
ws-commons-util-1.0.2.jar	1.0.2	Apache 2.0	Apache WebServices Common Utilities
ws-commons-util-1.0.2.jar	1.0.2	Apache 2.0	Apache WebServices Common Utilities
wsdl4j-1.5.1.jar	1.5.1	Apache 2.0	IBM
wss4j-1.5.8.jar	1.5.8	Apache License, Version 2.0	Apache Software Foundation
xalan.jar	2.7.0	Apache License, Version 2.0	Princeton University
xenserver-6.1.0-1.jar	6.1.0-1	Apache 2.0	XenServer Java
xercesImpl.jar	2.11.0	Apache License, Version 2.0	Apache Software Foundation
xml-apis-ext.jar	1.3	Apache License, Version 2.0	World Wide Web Consortium
xml-apis.jar	1.4.01	Apache License, Version 2.0	Apache Software Foundation

xmlbeans-2.3.0.jar	2.3.0-r540734	Apache License, Version 2.0	Apache Software Foundation
xmlrpc-client-3.1.2.jar	3.1.2	Apache License, Version 2.0	Apache Software Foundation
xmlrpc-client-3.1.jar	3.1	Apache License Version 2.0	Apache Software Foundation
xmlrpc-common-3.1.2.jar	3.1.2	Apache License, Version 2.0	Apache Software Foundation
xmlrpc-common-3.1.jar	3.1	Apache License Version 2.0	Apache Software Foundation
xmlrpc-server-3.1.2.jar	3.1.2	Apache License, Version 2.0	Apache Software Foundation
xmlsec-1.4.1.jar	1.4.1	Apache License, Version 2.0	Apache Software Foundation

Installing SNMP Agent on Windows System

(Adapted from Windows help)

- Installing SNMP Agent on Windows XP/2000/2003
- Installing SNMP Agent on Windows NT

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

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

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

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

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

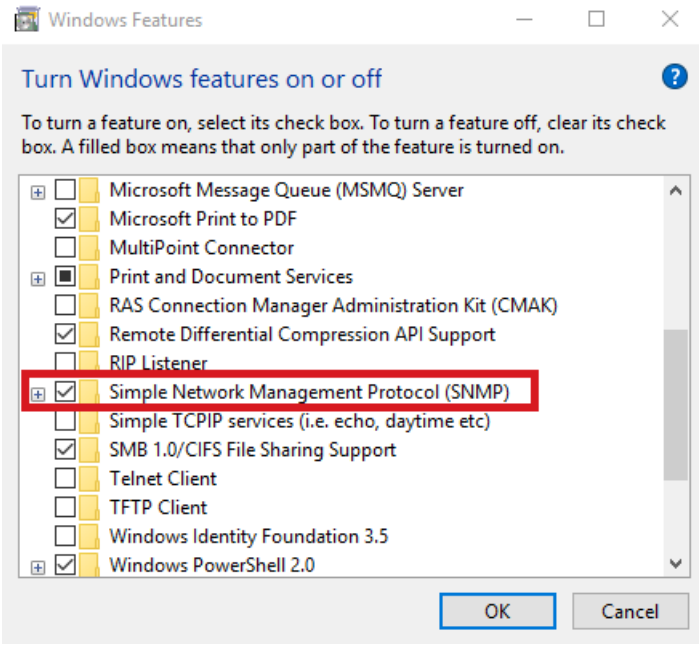
This completes the installation process. This also implements the Host Resources MIB automatically. To configure SNMP agents respond to SNMP requests, refer to Configuring SNMP agents.

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

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

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

Enabling SNMP in Windows:



1. Go to **Control Panel > Programs > Programs and Features > Turn Windows Features on or off.**
2. Choose **'Simple Network Management Protocol (SNMP)'** from the list.
3. Click **OK.**
4. Restart the SNMP Service.

Installing SNMP on Linux Systems

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

Download the latest rpm version of SNMP using the following URL:
http://prdownloads.sourceforge.net/net-snmp/net-snmp-5.1.1-1.rh9.i686.rpm?download

Download the zip version of SNMP using the following URL:
https://sourceforge.net/projects/net-snmp/files/OldFiles/ucd-snmp/4.2.6/

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

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

   rpm -qa | grep "net-snmp"
3. If there are already installed version in your machine, remove them using the command:

   rpm -e <version of net-snmp listed as the output for previous command> --nodeps
4. If there are no previously installed versions in your machine, then execute the following command to install the new version:

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

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

Extract the file using following command:
tar -zxvf ucd-snmp-4.2.6.tar.gz

To install SNMP, follow the steps given below:

1. Login as root user.
2. Execute the command to set the path of the C compiler:
   export PATH=<gcc path>:$PATH
3. Execute the following four commands from the directory where you have extracted the ucd-snmp:

   - *./configure --prefix=<**directory_name***> *--with-mib-modules="host"*

     directory_name is the directory to install SNMP agent. Preferably choose a directory under /root. The directories /usr and /local might contain the files of an older version of SNMP and so do not choose these directories to ensure proper installation.
   - make
   - umask 022
   - make install

This completes the installation process. For configuring SNMP agents to respond to SNMP requests, refer to Configuring SNMP agents.

Installing SNMP Agent on Solaris Systems

Download the latest version of SNMP using the following URL:
https://sourceforge.net/projects/net-snmp/files/OldFiles/ucd-snmp/4.2.6/

Extract the file using following command:
tar -zxvf ucd-snmp-4.2.6.tar.gz

To install SNMP, follow the steps given below:

1. Login as root user.
2. Execute the command to set the path of the C compiler:
   export PATH=<gcc path>:$PATH
3. Execute the following four commands from the directory where you have extracted the ucd-snmp:

   - ./configure --prefix=<**directory_name**> --with-mib-modules="host"

     directory_name is the directory to install SNMP agent. Preferably choose a directory under /root. The directories /usr and /local might contain the files of an older version of SNMP and so do not choose these directories to ensure proper installation.
   - make
   - umask 022
   - make install

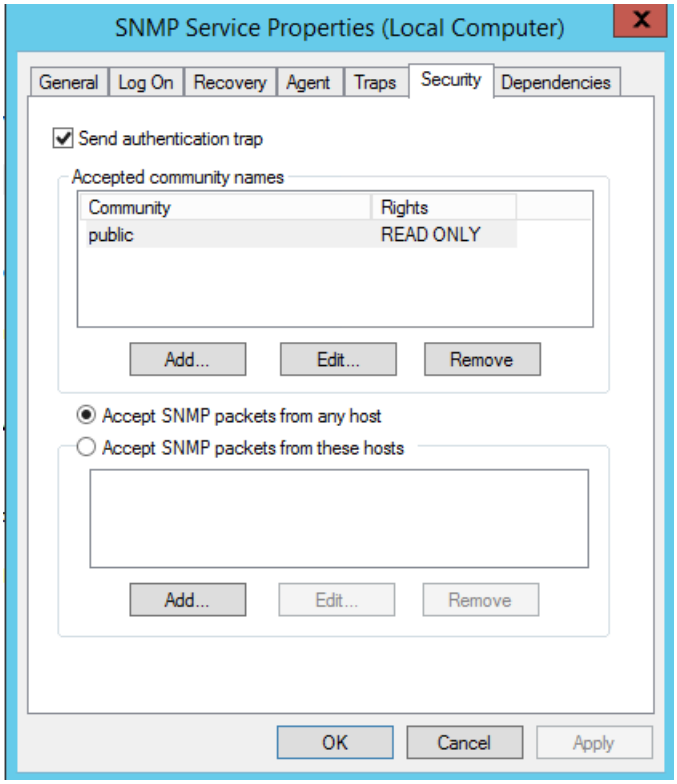
This completes the installation process. To configure SNMP agents respond to SNMP requests, refer to Configuring SNMP agents.

Configuring SNMP Agents

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

For details about installing SNMP agents in Windows systems, refer to Installing SNMP Agent on Windows Systems.

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



1. Click **Start**, point to **Settings**, click **Control Panel**.
2. Under Administrative Tools, click **Services**.
3. In the details pane, right-click **SNMP Service** and select **Properties**.
4. In the **Security** tab, select **Send authentication trap** if you want a trap message to be sent whenever authentication fails.
5. Under Accepted community names, click **Add.**
6. Under **Community Rights**, select a permission level for this host to process SNMP requests from the selected community.
7. In **Community Name**, type a case-sensitive community name, and then click **Add**.
8. Specify whether or not to accept SNMP packets from a host:

    - To accept SNMP requests from any host on the network, regardless of identity, click **Accept SNMP packets from any host**.
    - To limit acceptance of SNMP packets, click **Accept SNMP packets from these hosts,** click **Add**, type the appropriate host name, IP or IPX address, and then click **Add** again.

9. Click **Apply** to apply the changes.

To configure SNMP traps, follow the steps given below:

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

Configuring SNMP Agent in Windows NT Systems

For details about installing SNMP agents in Windows systems, refer to Installing SNMP Agent on Windows Systems.

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

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

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

Note: Windows NT 4.0 Server does NOT come with a Host Resource MIB.

If you are running Windows NT Service Pack 6a, and have a Windows 2000 Server:

Step 1. Copy the %SystemRoot%\System32\hostmib.dll file from the Windows 2000 Server to the %SystemRoot%\System32

folder on your Windows NT 4.0 Server.

Notes :

- C:\WinNT is the value of %SystemRoot%
- If you don't have a Windows 2000 Server, you can download the hostmib.dll file from http://bonitas2.zohocorp.com/zipUploads/2018_06_01_09_53_53_o_1cespfn5tllr1hc5uv9uc8rmi1.tar.gz
- If the above file is not compatible, you may download the compatible version from below page:https://www.pconlife.com/fileinfo/hostmib.dll-info/

Step 2. From cmd-prompt > Run regedit or Regedt32 and Add the following keys and values:

Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HostMIB\CurrentVersion
Value Name: Pathname
Type: REG_SZ
Data: C:\WinNT\system32\hostmib.dll

Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents
Value Name: 3
Type: REG_SZ
Data: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HostMIB\CurrentVersion

For registering the DLL using Microsoft REGSVR utility, follow below steps :

- Copy the file to "C:\Windows\SysWOW64\" (for 32bit) **OR** Copy the file to "C:\Windows\System32\" (for 64bit)
- You should be able to copy the .dll file in both above said system folders without any problems. In order to complete this step, you must run the Command Prompt as administrator.
- Open the Start Menu and type "cmd" on your keyboard. Right-click the "Command Prompt" search result and click the "Run as administrator" option.
- Paste the following command into the Command Line window that opens up and press Enter key.

  For 32 bit :

  %windir%\System32\regsvr32.exe hostmib.dll

  For 64 bit :

  %windir%\SysWoW64\regsvr32.exe hostmib.dll

- Restart your Windows NT box.

To Configure SNMP Traps, follow the steps given below:

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

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

Configuring the Agent in Linux versions prior to 8

For details about installing SNMP agents in Linux systems, refer to Installing SNMP Agent on Linux Systems.

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

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

Configuring the Agent in Linux versions 8 and above

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

- Insert the line
  view allview included .1.3.6
  next to the line
  # name incl/excl subtree mask(optional)

- Change the line
  access notConfigGroup "" any noauth exact systemview none none
  next to the line
  # group context sec.model sec.level prefix read write notif
  as
  access notConfigGroup "" any noauth exact allview none none

- Then restart the snmp agent using the following command:

  /etc/rc.d/init.d/snmpd restart

Configuring the Agent in Solaris Systems

For details about installing SNMP agents in Solaris systems, refer to Installing SNMP Agent on Solaris Systems.

- Stop the agent if it is running already using the following command:
  /etc/init.d/init.snmpdx stop

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

  - Replace the lines

    if [-f /etc/snmp/conf/snmpdx.rsrc -a -x /usr/lib/snmp/snmpdx]; then
    /usr/lib/snmp/snmpdx -y -c /etc/snmp/conf -d 3 -f 0
    fi
    with
    <Installation Directory>/sbin/snmpd

  - Replace the line

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

- Restart the agent using the following command:
  /etc/init.d/init.snmpdx start.

Configuring SNMP Agent in Cisco Devices

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

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

To enable SNMP:

From the command prompt, run the following commands:

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

To enable trap:

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

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

To set OpManager as host:

Run the following commands from the command prompt:

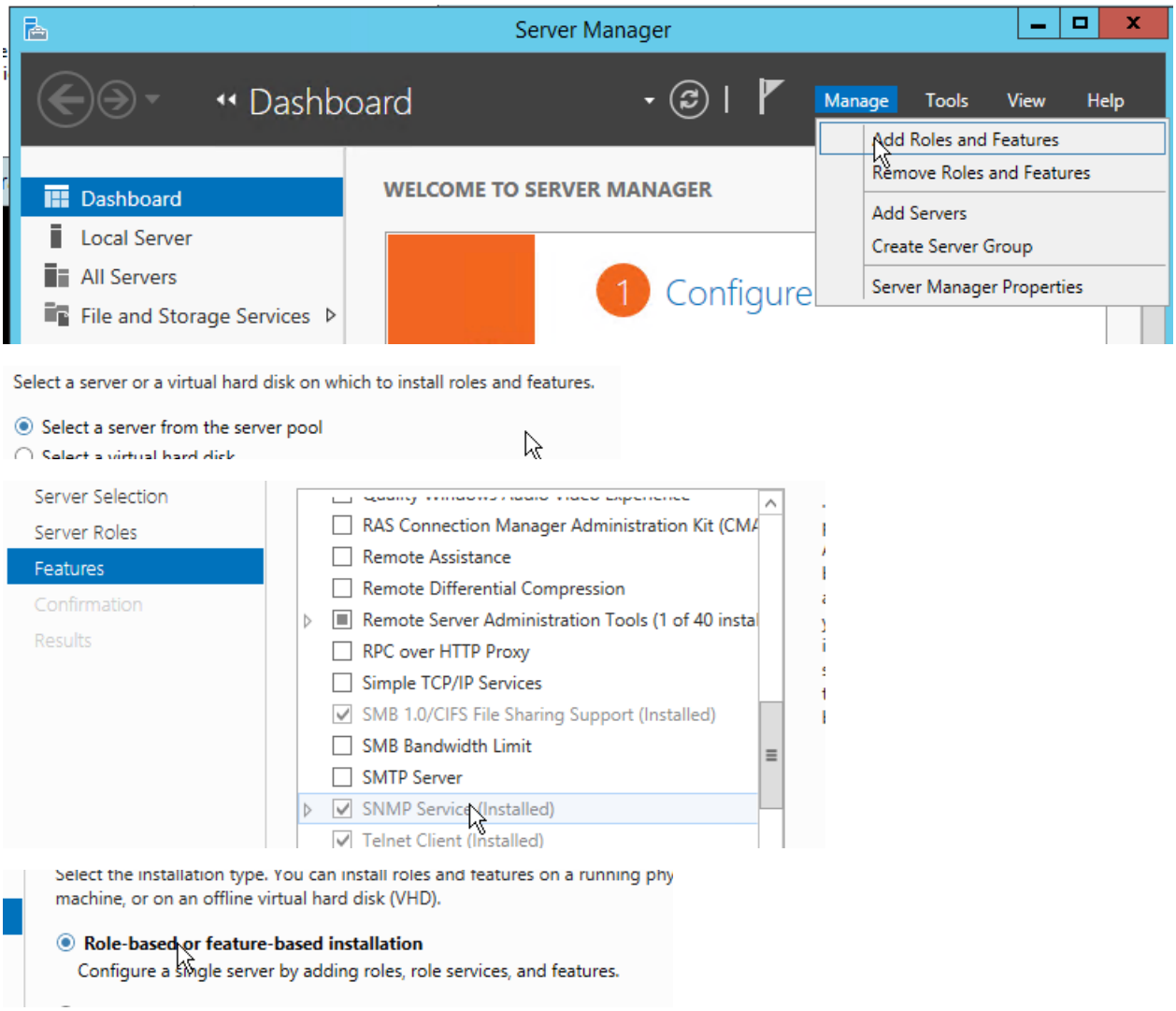
#configure terminal
#snmp-server host <OpManager server running system's IP> <Trap community string> snmp (example: snmp-server host 192.168.9.58 public snmp)
#end
#copy running-config startup-config

For more information, visit  CISCO.

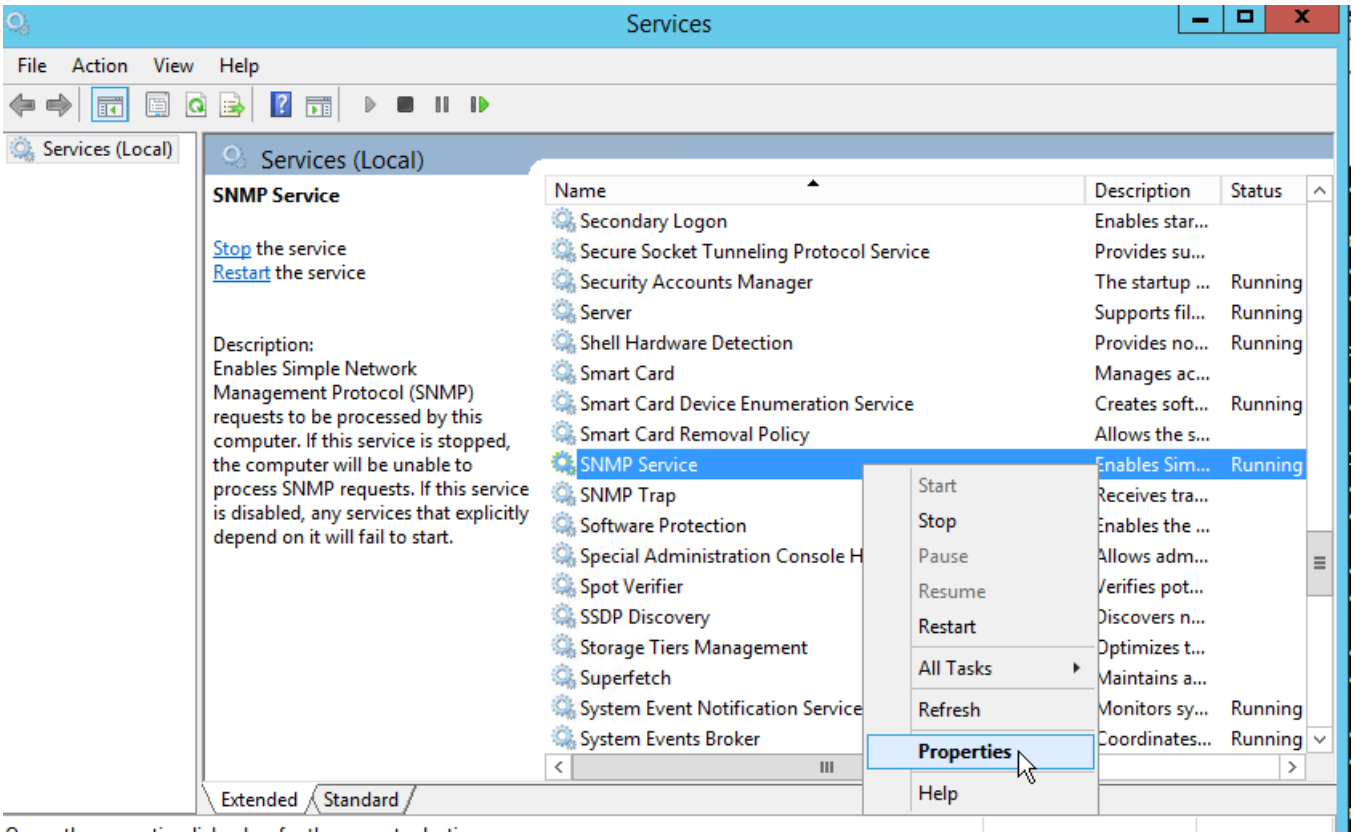
Configuring SNMP Agent in Lotus Domino Server

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

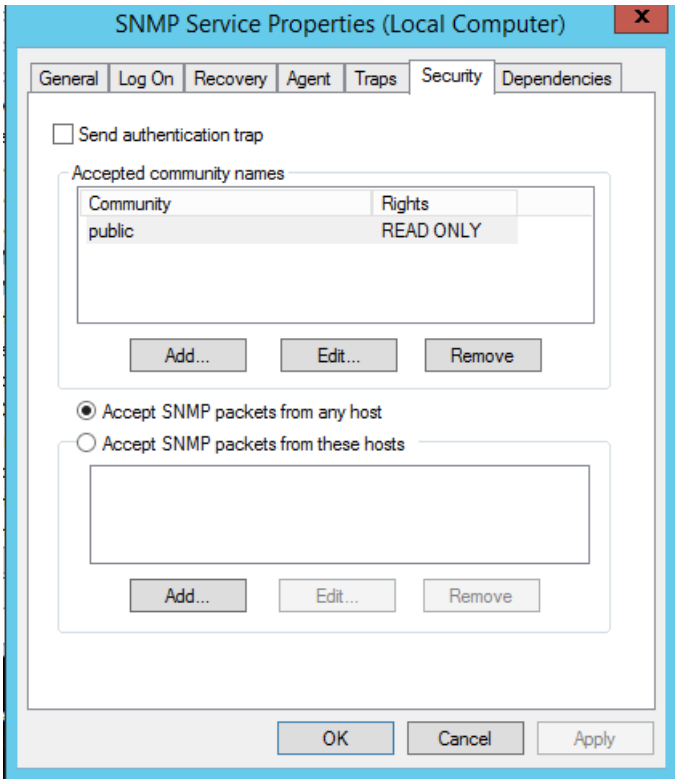
1. Use the Server Manager to add the SNMP Service to you windows installation. This installation process generally does not require a reboot.



2. Once the installation process is complete and the service has been installed successfully, right-click the SNMP Service in the services console, and select Properties.

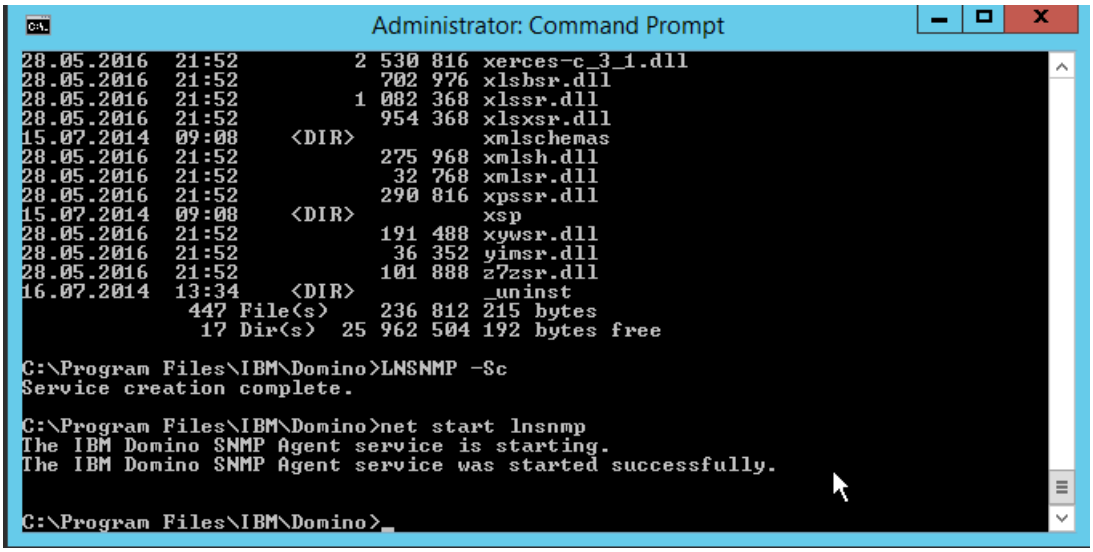


3. In Properties, under Security tab, the ﷺSend Authentication trapﷺ has to be disabled. Now, please add a Community, e.g. ﷺpublicﷺ and assign "Read Only"rights for monitoring purposes.
4. Now, allow any host/ hosts of your preference, to access the SNMP data.



5. Now, let us install the Domino SNMP Agent service. This service will feed data to the Windows SNMP agent:
5. Please open Command Prompt with Administrative privileges, and write the following code:

```
CD C:\Program Files\IBM\Domino
LNSNMP -Sc
net start lnsnmp
```



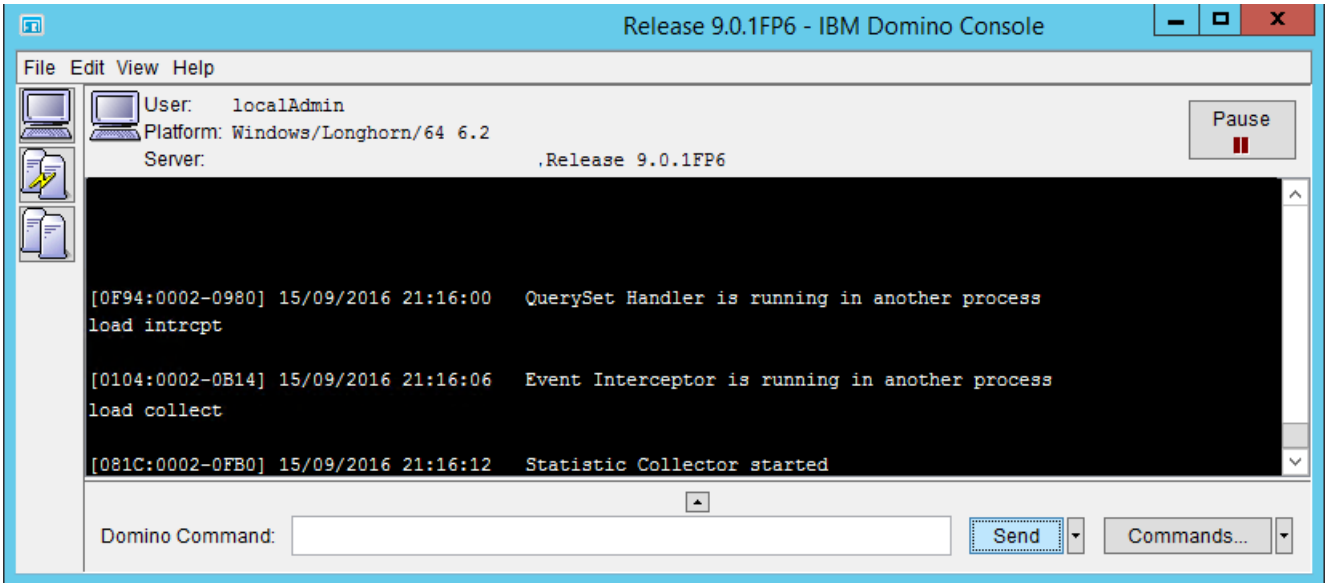
TIP!

If you get the following error when trying to install the Domino SNMP Agent service (LNSNMP -Sc), make sure you have installed the Windows SNMP Service correctly.

```
Error opening registry key "SNMP"
Error Detail: RegOpenKeyEx error code 2 (The system cannot find the file specified.)
Full key: SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents
Service deletion failed.
```

7. Lastly, you need to ensure that Domino, sends Stats to the SNMP Agent. To do this, launch the Domino Console and send the following commands:

```
load quryset
load intrcpt
load collect
```



8. This process is to be repeated everytime the Domino server is restarted. Therefore, add it to the Domino Server's "notes.ini" file. Eg:ServerTasks=Replica,Router,Update,AMgr,Adminp,Sched,POP3,quryset,intrcpt,collect
9. The Domino.mib will be located in the ﷼C:\Program Files\IBM\Domino﷼ folder. You can use this with OpManager.

For more information, visit http://www-01.ibm.com/support/docview.wss?uid=swg21169283.

Configuring SNMP Agent in Oracle Server

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

In Windows machines

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

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

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

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

Specify an unused port where the encapsulated agent, Microsoft SNMP Service, should be listening. Microsoft SNMP Service typically uses port 1161. The port is specified in the SERVICES file located in the NT_HOMESYSTEM32DRIVERSETC directory.

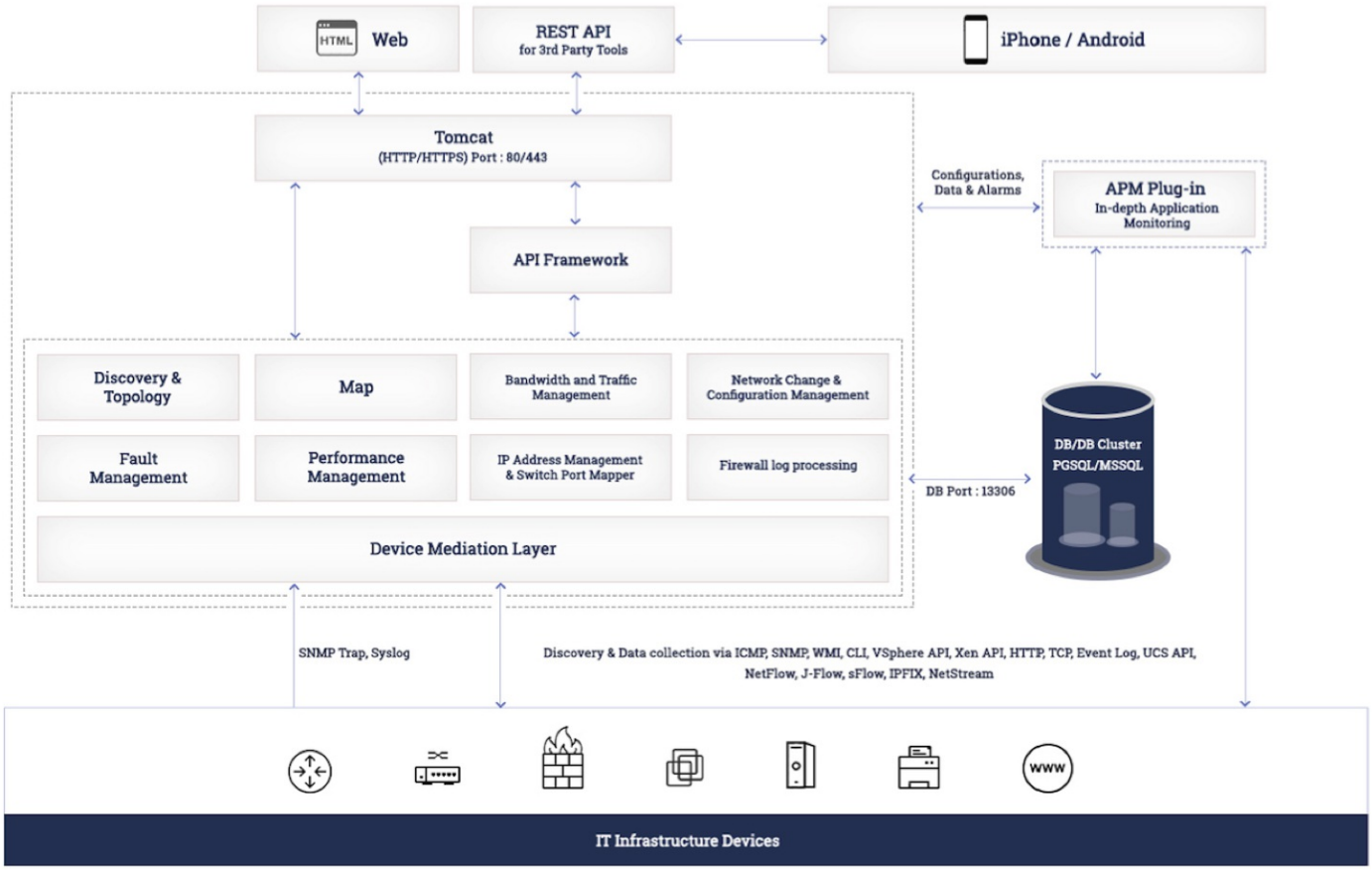
Make sure that you have the following lines in the file:
snmp 1161/udp snmp
snmp-trap 1162/udp snmp

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

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

For more information visit, https://docs.oracle.com/cd/B19306_01/em.102/b16244/chap2.htm.

OpManager Architecture



-
-
-
-
-

OpManager v12.5

Build No 125182 - September 18, 2020

- OpManager: Push Notifications were not received in iOS mobile application due to issue in existing APNs certificate. This issue has now been fixed.

Build No 125166 - August 24, 2020

- General: Garbled characters (non-English languages) appeared in the Web client due to the introduction of encoding in JVM. This issue has now been fixed.
- OpManager: While executing internal VB scripts, there was a password vulnerability discovered in OpManager. This has been fixed now.
- OpManager: Entries will now be created in Audit History for add/edit/associate/delete operations in Script monitors and Script templates and also for RDP access and Terminal access operations.
- OpManager: Now, tree view has been enabled for the left pane in the Inventory page. Users can group devices under this tree based on these criteria: Vendor, Category, Business View and Device groups.
- OpManager: The tree view is available in the Enterprise dashboard too, and it is also available as a widget to be added to custom dashboards.
- OpManager: Now, a number of additional device properties will be pushed to ServiceDesk Plus when assets are being synced from OpManager.
- General: Previously, the product startup was failed if the IP address was not resolved. This has now been fixed.
- General: Previously, in the API Access Audit report, there were issues with sorting reports based on date. This has now been fixed.
- General: Previously, it was unable to delete credentials that had ',' character in it. This has now been fixed.
- OpManager: EMC Isilon storage device can now be monitored by OpManager using Rest API.
- Enterprise Edition: When the Probe name consisted of a non-ASCII character, the communication between the Central and the Probe failed. This issue has now been fixed.
- OpManager: Previously, any graphs in the Graphs tab in Device Snapshot page had loading issues when the graph name contained special characters or characters from other languages. This has been fixed.
- OpManager: There were issues in displaying data in the graphs of MSSQL$ WMI monitor. This has been fixed now.
- OpManager: Previously, there were sorting issues in the Top N Monitored values of any performance monitor widget. This has been fixed.
- OpManager: Since the display name of script monitors were internationalised, it wasn't possible to edit script monitors post-creation due to an internal issue. This has been fixed.

Build No 125150 - August 13, 2020

- OpManager: Push Notifications were not received in iOS mobile application due to issue in existing APNs certificate. This issue has now been fixed.

Build No 125149 - July 21, 2020

- OpManager: An issue while viewing the short summary page of an alarm in the external monitor is fixed.
- OpManager: Unable to redirect to Device Snapshot Page from the Short Summary page of an alarm. This issue has been fixed.

Build No 125148 - July 7, 2020

- Enterprise Edition: When the Probe name consisted of a non-ASCII character, the communication between the Central and the Probe failed. This issue has now been fixed.
- OpManager : In the Device Snapshot page, there was an issue with displaying custom SNMP monitor data in graphs for other language installations. This has been fixed now.
- OpManager : Previously, importing custom fields was not possible if the CSV file had random Chinese characters in it. This issue has now been fixed.

Build No 125129 - July 6, 2020

- General : After upgrading the product, there was an "Unable to start the product" error. This issue has now been fixed.
- General: Previously, the backup functionality was not working for non-English installations. This issue has now been fixed.
- OpManager : Previously, the 'Search' option in the Interfaces list view page under Inventory was not working. This issue has now been fixed.
- OpManager : OpManager : Previously, the 'View Records' filter was missing in the 'All Interfaces by Utilization' report, making it unable to view all the interfaces at once. This issue has now been fixed.
- OpManager : Previously, device and interface Custom Fields were not properly updated in the alert notifications for languages other than English. This issue has now been fixed.
- OpManager : Previously, importing custom fields was not possible if the CSV file had random Chinese characters in it. This issue has now been fixed.
- OpManager : Previously, there were issues while initiating network discovery via CSV file, if the CSV file had random Chinese characters in it. This has now been fixed.
- OpManager : In the Device Snapshot page, there was an issue with displaying custom SNMP monitor data in graphs for other language installations. This has been fixed now.
- OpManager : In the "Notification Profiles Triggered" report, even if the profile trigger was successful, sometimes it was recorded as a failure. This issue has now been fixed.
- OpManager: The connectivity issues of RDP/Terminal in https mode has now been fixed.
- Enterprise Edition: When the Probe name consisted of a non-ASCII character, the communication between the Central and the Probe failed. This issue has now been fixed.

Build No 125128 - June 24, 2020

- General: Garbled characters (non English languages) appeared in the Web client due to the introduction of encoding in JVM. This issue has now been fixed.

Build No 125127 - June 23, 2020

- General: PostgreSQL has now been updated to version 10.12.
- General: The PostgreSQL vulnerability issues from version 10.10 have now been fixed.
- General: Directory Traversal validation was being bypassed when using <cachestart>. This issue has now been fixed. (Reported by Yazhi Wang of Trend Micro and zerodayinitiative)

Build No 125125 - April 29, 2020

- General: Path Traversal vulnerability in URLs starting with <cachestart> has now been fixed. (Reported by R.J.McDown) (Refer CVE-2020-12116)

Build No 125124 - April 27, 2020

- General: Users will now be able to select from the default list of SMS providers (Clickatell, Twilio, SMSEagle) while configuring SMS Gateway, in the SMS Server Settings page.
- General: Previously, the recipient mobile number was not auto-populated while editing the SMS Notification Profile. This issue has now been fixed.
- General: Previously, the edit page for credentials did not show the saved details when non-English characters were present in the name of the credential. This issue has now been fixed.

Build No 125123 - April 23, 2020

- OpManager: Interfaces will now be managed and removed from Idle interfaces once the In/Out speed is updated.
- OpManager: Previously, when rediscovery was scheduled for existing devices, the primary interfaces that had subinterfaces were automatically unmanaged. This issue has now been fixed.
- OpManager: Previously, the Packet loss dial was collecting incorrect data in the Spanish version of Windows machines. This issue has now been fixed.
- OpManager: Previously, in some cases, the packet loss value was updated as '0' in the Packet loss dial when the corresponding devices were down. This issue has now been fixed.
- OpManager: Previously, the Availability dials were displaying incorrect data when multiple tables were combined. This issue has now been fixed.

Build No 125121 - April 17, 2020

- OpManager: For HP 3PAR storage devices, statuspoll performance has been improved and the discovery time has also been optimized.
- NCM: The discovery API has now been upgraded to version 2.

Build No 125120 - April 16, 2020

- General: Unauthenticated access to API key disclosure from a servlet call. CVE-2020-11946 - @kuncho, an independent security researcher, has reported this vulnerability to SSD Secure Disclosure program. This issue has now been fixed.

Build No 125118 - April 9, 2020

- OpManager: Previously, there were issues with UnManaging and Managing of interfaces. This has now been fixed.
- OpManager: Previously, there was an issue in deleting interfaces during rediscovery. This has now been fixed.
- OpManager: Issues with the 'Type' filter in 'listInterfaces' API have now been fixed.
- OpManager: You can now fetch and sync device templates from OpManager's shared repository.
- OpManager: A new option 'Sync and Rediscover' has now been added to the Device Snapshot page. It allows you to update specific sysOID based device templates from OpManager's shared repository and rediscover devices with unknown type/category.
- OpManager: An enhancement to the Shortcut icon in Business View Widget has been made. You can now view the higher severity alarms triggered by the devices in a Shortcut by hovering your mouse over it.
- OpManager: The Group Snapshot page has now been optimized to load faster.
- OpManager: The number of packets sent for polling (ping) has now been reduced to 2.
- OpManager: Previously, for devices discovered through CSV files, the DisplayName did not support Non-English characters. This issue has now been fixed.
- OpManager: Any change in the IP address will now be logged in the audit report.
- OpManager: Previously, Group Status was displayed incorrectly when downtime was scheduled for it. This issue has now been

fixed.

- OpManager: Top band will be hidden while scrolling down specific pages.
- OpManager: Previously, UCS devices were discovered as 'Unknown' when added from the 'Add UCS page'. This issue has now been fixed.

Build No 125117 - April 8, 2020

- General: Previously, the error/success message for the Mail Server Settings was not shown in IE browser. This issue has now been fixed.
- General: User-based licensing has now been introduced in all ITOM products.
- General: Previously, the bcp.exe file execution test failed when the installation folder had a white space character in it. This issue has now been fixed.
- General: Previously, the widget tooltip message was not getting closed even after navigating to other pages. This issue has now been fixed.
- OpManager: Previously, there was an out of memory error due to load in availability monitoring after 124156 release. This issue has been fixed now.

Build No 125116 - April 2, 2020

- General: Previously, there was an issue in APM plugin startup when the backend MSSQL database was authenticated using Windows credentials. This has been fixed now.
- OpManager: There was an XSS vulnerability present during creation of new workflows. This has been fixed now.
- OpManager: There were issues with data collection in Process Monitors, when Poll using DNS name was selected. These have been fixed now.

Build No 125114 - March 26, 2020

- General: jQUERY has been migrated to version 3.4.1 to avoid vulnerabilities.
- OpManager: For downtime schedulers, there was a mismatch between the date in the list and the actual date that was set during configuration. This issue has now been fixed.
- OpManager: Previously,the threshold and rearm values for packet loss and response time monitors did not allow '0' in QCW. This issue has now been fixed.
- OpManager: For devices in the 'Not Monitored' state, Unmanage option will now be shown by default instead of Manage option.
- OpManager: Previously, the netmask was never retained when the discovery profile was edited. This issue has now been fixed.

Build No 125113 - March 23, 2020

- OpManager : Hyper-V polling mechanism has been changed for better performance.
- OpManager : VMware tags will be updated in Custom Fields for all VMware-based devices (applicable only for vCenter-based discovery).
- OpManager : Previously, when the monitor name included a backslash (\), there was an issue when the user tried to edit the Performance Monitor from Threshold Severity column. This has been fixed now.
- OpManager : Special characters (except underscore) have been restricted when trying to name Custom SNMP monitors.
- OpManager : Previously, there was an issue when adding Service monitors from Firefox, where it did not get displayed as soon as it was added. This has been fixed now.
- OpManager : There was an issue in adding a performance monitor from drop down in Internet Explorer. This has been fixed now.

- OpManager : Issues related to Internet Explorer such as graph overlap in Service Monitors, Displacement of Outage History icon, Graph icon misalignment in Monitors page and Graph display issue in Availability timeline graph have been resolved.
- OpManager : Previously Update Inventory operation for VMware was not allowed for BV admin users. The same has been allowed now.
- OpManager : Table View icon was previously hidden under Device Snapshot ? Monitors ? Performance Monitors ? Graphs page. This has been fixed now, and the icon is displayed.
- OpManager : The user is notified 10 days prior to the Apple Push Notification Service (APNS) certificate expiry.

Build No 125112 - March 17, 2020

- OpManager : The user interface for Notification Profiles has been revamped.
- OpManager : Now, ITIL as well as ITIL Admin roles can be used to configure ServiceNow.
- OpManager : Previously, the user interface crashed when large number of items were listed from ServiceNow while creating a notification profile. This issue has been fixed by loading the items dynamically.

Build No 125111 - March 13, 2020

- General: Previously, in the SystemPerformance dashboard, there was an issue with the loading of the Disk Space Monitor widget. This has now been fixed.
- General: Previously, the 'Forgot Password' option did not work when the authentication details were removed from the Mail Server Settings. This issue has now been fixed.
- General: Now, users can utilise LDAPS during AD authentication to establish secure communication with domain controllers.
- OpManager: Previously, in the Notification Profile, there were issues with the save and update option when more trap monitors or devices were selected. This has now been fixed.
- OpManager: A proper warning will now be shown while editing a profile that has recurring/delay scheduled to it.
- OpManager: Previously, AM/PM was displayed even in 24 hours time format. This has now been removed.
- OpManager: Problematic devices redirection link has been given for the Infrastructure snapshot widget.
- OpManager: Previously, the timezone IDs were displayed incorrectly across the product. This has now been fixed by providing an option to customize the timezone for specific regions/countries.
- OpManager: When searching for an IP using global search, devices which had the same IP address assigned previously were also displayed in the results. This issue has now been fixed.
- OpManager: An option to enable/disable Terminal has now been provided in the System Settings page.
- OpManager: Previously, the default device credentials were used to connect the terminal in the device snapshot page. Now, the user will have to enter the necessary credential in order to connect to the SSH/Telnet terminal.

Build No 125110 - March 10, 2020

- OpManager: Support has been added for new storage device - Infinibox.
- OpManager: Previously, there were issues in adding the generated report as a widget. This has now been fixed.
- OpManager: Issues with the alarm being deleted from the Central server has now been fixed.

Build No 125108 - March 4, 2020

- General: The obsolete code causing Remote Code Execution vulnerability in Mail Server Settings v1 APIs have been removed.

Build No 125102 - March 3, 2020

- OpManager: Previously, when devices were added in the Add-on modules (such as NFA, NCM,etc) they were automatically added as UnManaged in OpManager. This issue has been fixed now.
- OpManager: In Google Maps, you can now choose between Satellite, Terrain and Hybrid views in addition to the default RoadMap view.
- OpManager: In Zoho Maps, the equivalent ground distance can now be displayed either in kilometers or miles.
- OpManager: When the Custom Fields of a device is updated and they match the criteria of a Device Group, the device will automatically get added to the respective group.
- OpManager: Interfaces that do not collect data for a long time will now be unmanaged and moved to Idle Interfaces.
- OpManager: Time period selection has now been included in the Embed Interface graphs page.
- OpManager: Previously, in some cases, the device templates associated in Central were not reflected in Probe. This issue has now been fixed.
- OpManager: Around 50 new Device Templates and 80 new SNMP based performance monitors have been added.
- OpManager: Previously, credentials were not associated to devices when rediscovered from the Device Snapshot page. This issue has now been fixed.

Build No 125101 - February 25, 2020

- OpManager: Negative values can now be provided as thresholds in Performance Monitors.
- OpManager: When a monitor's name contained backslash (\), the graph page of the monitor was not accessible. This has been fixed.
- OpManager: Now, users can also take snapshots of a VM using the new 'Take Snapshot' function under Virtual Machine tasks, either from Workflows or from the Device Snapshot page of the VM (applicable to VMware VMs only).
- OpManager: Now, show/hide dial option for the Custom Dials has also been provided in the Device Snapshot page.
- OpManager: OpManager can now fetch the value for the 'Serial number' custom field using WMI.

Build No 125100 - February 20, 2020

- General: You can now export thread dumps as text files.
- OpManager: Minor enhancements have been done in Virtualization polling for improved performance.

Build No 125002 - April 2, 2020

- General : Previously, there was an issue in APM plugin startup when the backend MSSQL database was authenticated using Windows credentials. This has been fixed now.

Build No 125000 - February 19, 2020

- General: PostgreSQL has now been migrated to version 10.10.
- General: The PostgreSQL vulnerability issues from version 9.2.4 have now been fixed.
- Enterprise Edition: Previously, there were issues with starting the primary probe after a failover. This has now been fixed.

Build No: 124196 - April 29, 2020

- General: Path Traversal vulnerability in URLs starting with <cachestart> has now been fixed (Refer CVE-2020-12116).

Build No: 124188 - April 20, 2020

- OpManager: Previously, credentials were not associated to devices when rediscovered from the Device Snapshot page. This

issue has now been fixed.

- General: Unauthenticated access to API key disclosure from a servlet call. CVE-2020-11946 - @kuncho, an independent security researcher, has reported this vulnerability to SSD Secure Disclosure program. This issue has now been fixed.

Build No 124189 - Build No 124191 - February 26, 2020

- General: Previously, upgrade failed due to an issue in database entry. This issue has now been fixed.
- OpManager: The device deletion of VMware and Nutanix from the inventory has been optimized.
- OpManager Storage Monitoring: Some IBM storage devices were getting deleted automatically in certain cases. This issue has been fixed now.
- OpManager: Support for new storage device: v5/v6 arrays in Huawei OceanStor
- OpManager: Monitor availability and flapping for BGP links
- OpManager: Previously, there were issues in saving the reports generated for Interfaces. This has now been fixed.
- OpManager: Device down report has been newly added under Inventory report type.
- OpManager: The following reports have been added under Performance report type - Devices with Performance Monitors, Devices with File Monitors, Devices with Folder Monitors, Devices with Process Monitors, Devices with AD Monitors, Devices with Exchange Monitors, Devices with MSSQL Monitors, Devices with ADService Monitors, Devices with MSSQL Service Monitors, Devices with Exchange Service Monitors, Devices with NT Service Monitors, Devices with URL Service Monitors and Devices with Service Monitors.
- Enterprise Edition: False alarm generation in central has been fixed by disabling the active PDs.
- Enterprise Edition: When the license expired for OpManager Essential to Enterprise migrated probes, it was automatically switched to free version. This issue has now been fixed.

Build No: 124175 - 124186 - March 23, 2020

- OpManager : In the Devices tab under Inventory, you can now choose to display multiple Custom field values along with existing device details.
- OpManager : For Interface, Severity can be customized based on Admin and Operational Status.
- OpManager : During Layer 2 Discovery Schedule, when new devices are added, their respective Layer 2 Map was not loading properly. This issue has now been fixed.
- OpManager : An option has been provided to Import/Export Business Views between Central and Probe.
- OpManager : In the Business View Summary Widget, an option to filter Business View data has been added.
- OpManager : Export to PDF and Export to Excel options have now been included in the Embed Interface Graphs page.
- General: The Workflow page has been revamped to offer better user experience.
- OpManager Storage Monitoring: Support for new storage device - Synology DSM has been added.
- OpManager Storage Monitoring: Duplicate templates for storage devices have now been removed.
- OpManager: Credential-associated report that lists devices with the credentials associated has been added under Inventory reports.
- OpManager: There was an issue in exporting data to XLS format in getXLData API. This issue has now been fixed.
- OpManager: In Notification Profiles, there was an issue in sending alarm notifications when the UPS monitor(s) went down. This has been fixed now.
- OpManager : The Apps tab has now been moved to the Snapshot page for better visibility.
- OpManager : Previously, the virtual network discovery in the Discovery wizard had issues when no VMs were found under a host. This has now been fixed.
- OpManager : Previously, there were issues with the vCenter discovery when a different port number was used. This has now been fixed.

- OpManager : Previously, alerts were being raised with the wrong entity name even after changing it in the environment. This issue has now been fixed.
- OpManager : The VMSprawl dashboard was not populated properly in certain scenarios. This issue has now been addressed.
- OpManager : A Top band has been introduced in the Snapshot page for vCenter and ESX for better visibility of data.
- OpManager : The vCenter details widget in the vCenter snapshot page has been revamped for better usability.
- OpManager : Issues with the data displayed in the Forecast reports have now been fixed.
- OpManager : During migration from Essential to Enterprise,the SQL server transaction log file limit was exhausted when 1100000 rows or more were inserted in a table. This issue has now been fixed.
- OpManager : Previously, the users were able to read the Arbitrary file. This file read vulnerability has now been fixed. (Reported by jacky.xing@dbappsecurity.com.cn) (Refer: CVE-2020-11527)
- OpManager: To improve usability, Custom Field update using CSV file import has been enhanced. You can now map the user defined headers in the CSV file with the default Custom Fields of OpManager.
- OpManager: In the email notification for Interface Bandwidth Alarms, there were issues in fetching the Interface IPAddress Custom Fields. This issue has now been fixed.
- OpManager: In the device snapshot page for Router device, the Router graphs were plotted incorrectly. This issue has now been fixed.
- OpManager: Previously, some devices and interfaces were duplicated during discovery. This issue has now been fixed.
- OpManager: The HTTP requests for 'getInterfaceUtilization' API's have been changed from POST to GET.
- OpManager: Utilization alerts will now be raised even when one among the two (Rx/Tx) values violates the threshold.
- OpManager: The dependent device name will now be available along with the interface name in all Interface audit reports.
- OpManager: Previously, there were issues in the status alarm of UPS devices. This has now been fixed.
- OpManager: There were issues in data collection for specific models of Printer device as it returned special characters in the OID response. This has now been fixed.
- OpManager: The option to configure VRF Name and Poll Interval has been added in the IP SLA Configuration page.
- OpManager: Source Interface IP Address can be viewed in IP SLA Monitor Snapshot Summary page.
- OpManager: Previously, VoIP Monitor Total Statistics Data was displayed incorrectly. This issue has now been fixed.
- OpManager: Previously, Devices were not properly listed in NetFlow Analyzer Add IP SLA page. This has now been fixed.
- OpManager: You can now choose the Time Frame for the Availability Pie Chart under IP SLA Monitor Snapshot page in Expanded Mode.
- OpManager: Previously, when the graph monitors page was refreshed, the graphs displayed were smaller in size. This issue has been fixed.
- General: In the snapshot page, when switching between tabs, the widgets displayed were overlapping. This issue has been fixed.
- General: Option to switch between full view and tab view in device snapshot settings page has been removed.
- General: Left and center screen alignment views has been removed from global settings.
- OpManager: Previously, StringData tables were not cleared when cleanup of old data was performed. This has been fixed, and now StringData will also be cleared based on provided Database Maintenance settings.

Build No: 124172 - March 11, 2020

- General: The obsolete code causing Remote Code Execution (RCE) vulnerability in Mail Server Settings v1 APIs have been removed. (Reported by Jason Nordenstam) (Refer: CVE-2020-10541)

Build No: 124171 - January 20, 2020

- OpManager: The device deletion of VMware and Nutanix from the inventory has been optimized.

Build No 124081 - 124103 - January 23, 2020

- OpManager: Previously, there was an issue with virtual network discovery in the Discovery wizard, when no virtual machines were found under a host. This issue has been fixed.
- OpManager: Previously, product upgrade was terminated due to incomplete population of 'ReportDetails_VMSprawl.xml' file. This issue has been fixed.
- OpManager: Previously there were issues with deleting and associating credentials that had special characters in its name. This has now been fixed.
- OpManager: During Scheduled Discovery, the devices added to the Ignore List were rediscovered along with their interfaces. This issue has been fixed.
- OpManager: While rediscovering existing devices, the rediscovery rule was not properly applied for devices that were down. This issue has now been fixed.
- OpManager: Previously, Add Device fails when the device's Syslocation length was more than 200. This issue has now been fixed.
- OpManager: Previously, Add Device fails when the device's Syscontact length was more than 100. This issue has now been fixed.
- OpManager: Previously, there was a variation in the ping response for the linux devices that were intermittently reachable. This issue has now been fixed.
- OpManager: Previously, Custom Field values with non-english characters were not updated in OpManager. This has now been fixed.
- OpManager: Previously, the listDowntimeSchedule api was not accessible externally. This issue has now been fixed.
- OpManager: Previously, in the Dashboard HeatMap widget, the status of the 'Not-Monitored' devices was displayed as Clear. This has been fixed now.
- OpManager: The option to update Display Name of devices in Bulk has been added. This can be done using CSV file import or set Hostname/FQDN/SysName as your device's Display Name.
- OpManager: 'Filter by Groups' feature is added to the All Groups Widget under Dashboard. With this, you can now choose to filter the displayed groups.
- OpManager: In OpManager, Operator users now have the privilege to access Groups in Read-Only format.
- OpManager: Subgroups are now listed under 'Devices in Group' and 'Interfaces in Group' widgets.
- OpManager: Previously, the Report builder had issues with displaying data when multiple tables were being queried by the interface. This issue has been fixed.
- OpManager: Interface data collection failure due to DNS name mismatch has now been fixed.
- OpManager: Previously, the stale entries present in the deletedInterface table were getting duplicated during Rediscovery. This issue has now been fixed.
- OpManager: New Report : All Alerts with Notes added.
- OpManager: Previously, there were issues in loading MIB files when the file name contains special character (.). This has now been fixed.
- OpManager: Weaker file permission for Nipper file has been fixed (CVE-2019-17421 - bug found by: Guy Levin (@va_start)).
- Enterprise Edition: The files extracted during installation will be removed if the probe is not compatible with Central or if the installation is cancelled.
- Enterprise Edition: The probe download link in Central will redirect to archives. In Japanese setup, you will be redirected to product support for further assistance.
- OpManager: OpManager now provides support for Nutanix HCI monitoring. Also, a separate report category for Nutanix and a separate dashboard with Nutanix-related widgets have been added.
- OpManager: Previously, there were SQL injection vulnerabilities in the 'deviceName' parameter of 'deleteUrl', 'addUrl' and 'getURLSummary'. These have been fixed now.
- OpManager: When there were a large number of vCenters / ESX parent servers present in OpManager, VMware events were not

raised properly. This issue has been fixed now.

- OpManager: In the 'Performance monitors' tab under Device Snapshot, when the value for the threshold was normal, it was displayed as 'Not Enabled' in all languages except English. This has been fixed now.
- OpManager: In the Alarms page, edit thresholds option was not working properly for Datastore-related alerts. This has been fixed now.
- OpManager: URL templates have now been moved from 'Configuration' tab in Settings to 'Monitoring' tab.
- OpManager: Discovery Rule Engine has now been moved from 'Configuration' tab in Settings to 'Discovery' tab.
- OpManager: 'View report' option has been provided in the Notification profile list page to view the logs for the notifications triggered from a particular profile.
- OpManager: A new feature, 'Business Hour Rule' has been introduced under Reports. This helps the user to filter reports based on the specified Business hours.
- OpManager: Previously, an OutofMemory exception message was thrown while Scheduling Reports. This issue has now been fixed.
- OpManager: Previously, there was an issue with the XLS Export option when multiple instances was present in the reports. This has now been fixed.
- OpManager: Previously, there was an issue with the exported Report displaying MO name instead of Business View Displayname. This has now been fixed.
- OpManager: Previously, Default My Favorite Reports were not listed in Probe. This issue has now been fixed.
- OpManager: Previously, there were issues with exporting Reports when Fully Qualified Domain Name had '.' at the end. This has now been fixed.
- OpManager: Issues with the Business View filter in the Service Monitor Report has now been fixed.
- OpManager: Previously, there was an issue with few columns being displayed as strings while exporting reports in XLS format. This has now been fixed.
- OpManager: Previously, the Graph Reports displayed data only from a single instance, even when data from multiple instances were available. This issue has now been fixed.
- OpManager: Issues with the URLs by Response Time Report has now been fixed.
- OpManager: Issues with Interface Link in Alarm Snapshot page has now been fixed.
- OpManager: Previously, there was an issue while exporting data from Central Snapshot page. This has now been fixed.
- OpManager: A new option 'Click here for Preview' has been added to the Reports page.
- OpManager: Reports are now sorted in the descending order based on time.
- OpManager: The 'Back' option in the Schedule Report page has now been hidden for some reports.
- OpManager: In the Alarms page, the limit on the number of alarms that can be exported has now been removed.
- OpManager: The Report builder page has been completely revamped to provide better user experience.
- OpManager: When any special characters are present in the custom Dashboard name, there were issues with the 'Set as default Dashboard' option. This has now been fixed.
- OpManager: The 'CPU' and 'Memory Utilization' graphs in system performance dashboard were not updated properly. This issue has now been fixed.
- Enterprise Edition: If the probe version does not match with the Central version, an error message will be displayed with a link to download the appropriate version. This has been implemented in the probe registration panel (during installation)
- Enterprise Edition: If the Probe is unavailable, the Central start up page will now have the link to download the appropriate version of the Probe.
- Enterprise Edition: The Probe details page in the Central Server will now have the link to download the appropriate version of the Probe.
- Enterprise Edition: When installing probe in Linux machines, the proxy details usage were not displayed. This issue has now been fixed.

- Enterprise Edition: Previously, probe registration failed when the probe name has whitespace character. This has been restricted and a warning message will now be displayed.
- Enterprise Edition: If the Central is installed with PostgreSQL database and the probe is installed with MSSQL database, installation will be blocked and a warning message will be displayed.
- Enterprise Edition: An option to export data from the diagnostics table has now been introduced in the Diagnostics page.
- Enterprise Edition: Previously, there was communication failure between the Probe and Central when a non-English character was present in the Probe name. This issue has now been fixed.
- Enterprise Edition: Previously, the SmartUpgrade was failed when the installation folder name had space in it. This issue has now been fixed.
- Enterprise Edition: Previously, there were issues with the Probe not starting automatically after an upgrade. This issue has now been fixed.
- OpManager: Apps menu has been added in the product top band next to the Settings Icon, to enable easy access to third party integrations in OpManager.
- OpManager: Now, change in severity for any alarm in OpManager will be updated under the Notes section of that request/incident in ServiceDesk Plus/ServiceNow.
- OpManager: A new feature called 'request call back' is available for integration with ServiceDesk Plus versions greater than 9413. With this feature, if an alarm is marked as resolved in SDP, it will be automatically cleared in OpManager too.
- OpManager: A new command called 'Log a ticket (ServiceNow)' has been added under External Actions in OpManager workflows, which allows the user to create tickets in ServiceNow.
- OpManager: Previously, the RAM and Hard disk details of any device had to be updated manually if it was upgraded/modified. This issue has now been fixed, and these details are updated automatically once in every 12 hours.
- OpManager: Now, users can select whether to poll their devices based on IP address or DNS name. This setting can be controlled throughout OpManager (from Settings > Monitoring), or can also be configured for individual devices.
- OpManager: The device discovery pages for VMware, Hyper-V and XenServer have been combined under 'Virtualization discovery', and its usability has also been improved.
- OpManager: Previously, it was possible to make Authenticated/Unauthenticated SQL injections in OPMDeviceDetailsServlet. This has been fixed now. (Refer CVE-2019-17602)
- OpManager: In some cases, there was an alarm status mismatch between OpManager and Applications Manager's connector module. This issue has been fixed now.
- OpManager: Previously, if too many dials were configured for a device, the device snapshot page of that device had a very high loading time. This has been fixed now.
- OpManager: In a few cases, data collection for CLI monitors stopped abruptly. This issue has now been fixed.
- OpManager: In Central, interface templates can now be configured and associated to probes and the related interfaces.
- OpManager: Over 60 new interface templates have been added.
- OpManager: In the Devices Availability Dashboard Report, previously the device list was not fetched based on the availability graph chosen. This has now been fixed.
- OpManager: Availability data has now been added in All Groups widget under the Dashboard.
- OpManager: XSS vulnerability in Remote Desktop is now been fixed.
- OpManager: The Workflow page has been completely revamped to provide better user experience.
- OpManager: Previously, the Device Name was not displayed in the Alarm suppression Audit Report. This issue has now been fixed.
- OpManager: New Reports have been added for Alarm Suppressed Devices, Top Trap Count by Source, Top EventLog Count by Source and Top SysLog Count by Source.
- OpManager: Under Inventory Reports, exporting individual reports in Device by Device Types & Device by Category had an error. This issue has now been fixed.

- OpManager: While using the Filter option under Health and Performance Reports, data has not been displayed for an hour's interval for the previous day, when custom time is selected. This issue has now been fixed.
- OpManager: On creating a new report in Inventory Snapshot page, time period for the report was always displayed as Last 12 hours. This issue has now been fixed.
- OpManager Storage Monitoring: Custom fields have been provided for Storage Devices.
- OpManager Storage Monitoring: Existing OpManager customers are now eligible for a Free 30 days trial for Storage Monitoring Add-ons.
- OpManager Storage Monitoring: OpManager now supports monitoring the following storage devices - Huawei 9000 series, Huawei 18800 series,Fusion Block,Fujitsu DX series.
- OpManager Storage Monitoring: There was an issue with selecting the storage devices in the pop-up window when exceeding the storage license limit. This has now been fixed.
- OpManager: Previously, there was an issue in saving the 'Severity' and 'Rearm Severity' of Syslog rules in other languages apart from English. This issue has now been fixed.
- OpManager: In Notification profiles, there was an issue with the sort option for Profile name. This has now been fixed.
- OpManager: Previously, there was an issue with creating new URL Templates. This has now been fixed.
- OpManager: Previously, there was an issue with the automatic shutdown of enterprise setup even after the expiry of evaluation/extended license. This issue has now been fixed.
- OpManager: Previously, there was an issue with the working of addBulkMonitors API in other languages apart from English. This issue has now been fixed.
- OpManager: XSS vulnerability in Performance monitors under the Monitors Tab in Device snapshot page has now been fixed.
- OpManager: Using report builder, you can now fetch device availability, response time and packet loss data.
- OpManager: A new dashboard widget has been added to display the list of interfaces that are down.
- OpManager: You can now filter devices based on groups and business view in the 'Infrastructure Snapshot' widget.
- OpManager: During scheduled network discovery, deleted interfaces were rediscovered. This issue has now been fixed.
- OpManager: There was a downtime data mismatch issue between device availability report and downtime report in terms of seconds. This issue has been fixed.
- OpManager: In the downtime scheduler page, the 'Next scheduled at' will be displayed as '-' when the current schedule is running for the schedule type 'Once'.
- OpManager: Over 300 new Device Templates and default performance monitors have now been added.
- OpManager: Support is provided for AES-192 and AES-256 encryption methods in SNMPv3 credential.
- OpManager: SNMPv3 support for APC UPS devices is provided.
- OpManager: SNMPv3 support for ESXi servers is provided.
- OpManager: When exporting the availability dashboard report as a PDF, there were issues with sorting for the custom time period filter. This issue has now been fixed.
- OpManager: In Interface snapshot page, the 'Disable Admin status' option was not displayed if the product language was set to Chinese. This issue has now been fixed.
- OpManager: Users can now export the list of devices and interfaces in CSV and XLS format.
- OpManager: Under System Settings, Group chat option has been hided.
- OpManager: When adding devices in Business View, device type icons will be displayed instead of the default icons.
- OpManager: Previously, the Map Widget was vulnerable to Cross-Site Scripting(XSS). This issue has now been fixed.
- General: The JCE compatibility issue that occurred during PPM migration has now been fixed.
- General: Previously, the 'Export to PDF' option was not working for customers who had upgraded from version 12.200 to the latest build. This issue has now been fixed.
- General: OpManager now supports domains secured with NTLMv2 protocol for Windows authentication in MSSQL databases.

- General: There was an issue in the area-graph widgets, resulting in the text in the graph not being displayed completely. This has been fixed now.
- General: Issues with the 'Keep me signed in' functionality for AD Authenticated users has now been fixed.
- General: Previously, there was an issue with the silent patch not getting applied for directory names with space. This has now been fixed.
- General: Previously, the License expiration message was displayed in the header even after the successful registration of the product. This issue has now been fixed.
- General: For registered users, the CustomerID and LicenseID will now be shown in Product Details page.
- General: Previously, there was an issue with uploading specific mp3 sound files in the Web Alarm profile. This issue has now been fixed.
- General: Issues with PGSQL to MSSQL migration when there were duplicate values in datetime column has now been fixed.
- General: For Windows AD authentication, Passthrough login is now supported even if SMBv1 protocol is disabled in Domain Controller.
- General: Previously, Passthrough settings configuration had to be entered manually. Now the details can be auto-configured using the 'Fetch' option.
- General: 'Save and Test' option has been introduced for Passthrough configuration to validate the settings.

Build No 124079 - November 26, 2019

- General: Weaker file permission for Nipper file has been fixed (CVE-2019-17421 - bug found by: Guy Levin (@va_start)).

Build No 124078 - November 21, 2019

- OpManager: Previously there were issues with deleting and associating credentials that had special characters in its name. This has now been fixed.
- OpManager: Previously, it was possible to make Authenticated/Unauthenticated SQL injections in OPMDeviceDetailsServlet. This has been fixed now. (Refer: CVE-2019-17602)
- OpManager: Issues with the getAssociatedMonitors API has now been fixed.

Build No 124051 - 124077 - October 22, 2019

- OpManager: The issues with hardware report filter has now been fixed.
- OpManager: Issues regarding the empty status for ESX processor sensor has now been fixed.
- OpManager: Previously, it was not possible to disable hardware monitors in 'Checkpoint' firewall device.This issue has now been fixed.
- OpManager: Previously, the hardware tab for router/switch/firewall with NFA/NCM was missing. This has been included now.
- OpManager: Previously, Device model name was being displayed in the 'Hardware Information' report instead of the Display name. This issue has now been fixed.
- OpManager: The product was slow when the alarms were cleared or deleted. This issue has been fixed.
- OpManager: The 'Device status' was not displayed while navigating through pages under Sensor Info. This issue has now been fixed.
- OpManager: Previously, data was not displayed for hardware monitoring graph. This issue has now been fixed.
- OpManager: In the 'Add Performance Monitor' page, the XSS vulnerability that has been affecting the Add VendorName option under Bulk SNMP has now been fixed.
- OpManager: Remote desktop authorization issue has been fixed.
- OpManager: The 'Performance Monitors' list has now been optimized to load faster.
- OpManager: Issues with the threshold configurations inconsistency for String performance monitors has now been fixed.

- OpManager: In case of EventLog poll failure due to RPC server unavailability, the successive poll will now fetch the data of the previous failed poll along with the current poll data.
- OpManager: For PGSQL database, the 'URL Response Time' graph displays no data if the selected time period is more than 7 days. This issue has now been fixed.
- OpManager: Data was not displayed for URLs by Response Time under Availability and Response reports. This issue has now been fixed.
- OpManager: Previously, when there were a large number of widgets in the dashboard, few widgets had an issue with displaying data. This issue has now been fixed.
- OpManager: Previously, it was unable to configure the threshold for the script monitor in the device snapshot page when the != operator is selected. This issue has been fixed.
- OpManager: Index ID of instances were displayed instead of Display name for certain multiple instances of performance monitors even after configuring Display OID. This issue has now been fixed.
- OpManager: Under Network Tab, Printers category has been introduced with enhanced Icon View.
- OpManager: Errors in editing URL Monitors have now been fixed.
- OpManager Storage Monitoring: HP 3PAR Devices with TLS 1.2 certification can now be added to storage devices and Data collection issues for HP 3PAR devices with older TLS certifications have now been fixed
- OpManager Storage Monitoring: Issues with EMC Clariion and EMC UNITY have now been fixed
- OpManager Storage Monitoring: New options have been introduced: Addition and Deletion of monitors for storage devices
- OpManager: Push Notifications are not received due to expiry of APNS certificates in iOS mobile application. This issue has now been fixed.
- OpManager: Errors have now been fixed in SNMP Trap Processors: Addition of Match Criteria and Rearm Criteria
- OpManager: Errors have now been fixed in SNMP Trap Processors: Deletion of final entries of Match Criteria and Rearm Criteria
- OpManager: There was a user login bypass vulnerability in APM plugin for OpManager. This issue has now been fixed. (Refer CVE-2019-15106)
- OpManager: SMS sent by recurring notification profile, was not routed via actual SMS Gateway. This issue has now been fixed.
- OpManager: In the Groups tab under Inventory, the availability status for individual groups will be displayed.
- OpManager: The 'Associate Device Template' page under 'Device Template' has been optimized to load faster
- OpManager: Option to remove devices from 'Business Views' list page has been introduced.
- OpManager: Option to delete multiple Business Views, Rack Views and 3D Floor Views has been introduced.
- OpManager: Under Inventory, a product assistance notification message to enable a Displayed Module IP management(OpUtils) in OpManager's system settings has been added.
- OpManager: In interface reports, the 'Min' values were displayed as '0' due to type casting. This issue has now been fixed.
- OpManager: There was a difference in the color code for legend between interface traffic widget and interface graph. This issue has now been fixed.
- OpManager: In interface graphs, when the value of 'InOctets' were very high, there was no data displayed in the graph. This issue has now been fixed.
- OpManager: The Layer 2 map discovery issue due to partial SNMP OID response has now been fixed.
- OpManager: Around 14000 new vendor templates have been added to avert devices from being classified as 'Unknown'.
- OpManager: In the devices availability dashboard report, incorrect data was displayed when filters were applied. This issue has now been fixed.
- OpManager: The IP address was displayed as undefined in the heat-map widget tooltip under NOC view. This issue has been fixed.
- OpManager: Previously, it was not possible for a user to delete multiple URL monitors. This issue has been fixed now.
- OpManager: Previously, it was not possible to install standby service if the product build number was above 12.4.056. This issue

has been fixed.

- OpManager: Hyper-V server's disk related monitors displayed mismatched data. This issue has been fixed.
- OpManager: The Hyper-V VMs under type 2 hypervisor host did not display any data for disk related monitors. This issue has been fixed.
- OpManager: During Hyper-V host discovery, Hyper-V VMs were not discovered since their DNS was not reachable. This issue has now been fixed.
- OpManager: The devices in the local network will be automatically added and monitored when OpManager is installed.
- OpManager: In Layer 2 maps, you can now drag and drop nodes.
- OpManager: In the Layer 2 maps page, the zoom in and out option has been enhanced and a new 'Fit to screen' option has been added.
- OpManager: After generating a report from the interface snapshot page, there was an issue with exporting the PDF in other languages apart from English. This issue has now been fixed.
- OpManager: In the 'Test credentials' page under Discovery, the test credential status was displayed as 'Passed' even if the SNMPv3 credentials were incorrect. This has now been fixed.
- OpManager: Dumping data to SQL database using bcp Utility failed when the path to the OpManager installation directory contained whitespace character(s). This issue has now been fixed.
- OpManager: Forecasting reports based on machine learning has been added for memory, disk and CPU utilization monitors.
- OpManager: In a VMotion environment, VMware ESXi host discovery failed in a few cases. This issue has now been fixed.
- OpManager: Data collection failure issue for VMware ESXi host Hardware has now been fixed.
- OpManager: A new performance monitor 'CPU Utilization per core' has been added for Hyper-V VM servers.
- OpManager: A new performance monitor 'Datastore free space in percentage' has been added for VMware related datastores.
- OpManager: The virtual NICs' data related to Hyper-V virtual machines was not displayed under virtual details. This issue has now been fixed.
- OpManager: Network monitor data related to Hyper-V VM's were not collected. This issue has now been fixed.
- OpManager: During vCenter discovery, the VM OS type will be displayed even when the specific VM's credentials were not passed (only for Windows devices).
- OpManager: When the vCenter inventory is updated, it will be audited in the device level and reports.
- OpManager: Data was not displayed properly for Cisco MDS fibre channel switch due to an UI issue. This has now been fixed.
- OpManager: There was an issue in accessing the terminal from the device snapshot page. This issue has now been fixed.
- OpManager: In the new reports page, support for custom field reports has been added for interfaces.
- OpManager: In a few cases, associating performance monitors to a device/devices failed due to a database error. This issue has been fixed now.
- OpManager: Under inventory, 'Add as widget' icon has been included for interface reports.
- OpManager: 'Table view' tab has been included for interface reports generated from the inventory.
- OpManager: When the interface name contained forward slash character (/), the name was not displayed properly in the Business view link label. This issue has been fixed.
- OpManager: The mail ID validation issue has now been fixed.
- OpManager Enterprise Edition: Due to event flooding, event processing was terminated in Central. This issue has been fixed.
- OpManager: Under Inventory, when editing the interface speed from the interfaces tab, it was not possible to update the speed up to 1Tbps. This issue has been fixed.
- OpManager Storage Monitoring: In Storage Monitoring, spare disks will not be considered under License Count
- OpManager Storage Monitoring: OpManager now supports monitoring of the following storage devices - Hitachi VSP, Hitachi AMS, Huawei (API Support), NetApp ONTAP 9
- Enterprise Edition: An audit entry will now be made in the Central for probe addition, updation or deletion.

- General: A new option has been introduced in the Rebranding page under settings where a custom message can be configured to be displayed in the login page.
- General: The changes made in the system settings page were not updated when the default domain was deleted in the AD authentication page. This issue has now been fixed.
- General: If the SMPP server responds with empty SystemID, SMS via SMPP server will not work. This issue has now been fixed.
- General: Database reconnection timeout was wrongly configured in the upgraded setup. This issue has now been fixed.
- General: Basic Settings has been renamed to General Settings.
- General: Privacy settings has been reordered under General Settings tab
- General: Add-On/Product Integration has been renamed to Third Party Integrations
- General: Groups option has been reordered under Configuration tab

Build No 124034 - 124047 - August 22, 2019

- Previously, upgrade failed when a large number of duplicate NT Service entries were present. This issue has now been fixed.
- OpManager: There was a **user login bypass vulnerability** in APM plugin for OpManager. This has been fixed now. (Refer: CVE-2019-15106)
- General: You can now edit, re-arrange and hide the default tabs in the horizontal menu. New custom tabs can also be added, edited, rearranged and deleted from the horizontal menu.
- OpManager: When the user is logged in as a Business view admin user, there were alignment issues in the admin tab and the product details were not displayed. This issue has now been fixed.
- OpManager Enterprise Edition: Under Settings ? Configurations, a new ﷺCentral details﷽ page has been added to update Central server﷽s host name, protocol and port details. Manual entry in the 'NOCServerDetails' file and ﷺCommunicationInfo﷽ XML file is not required and its dependency has been removed.
- OpManager: Previously, creating trap processor from unsolicited traps failed. This issue has now been fixed.
- OpManager: Due to a timeout issue in workflow, the status of the workflow task was displayed incorrectly. This has now been fixed.
- OpManager: When two or more workflows scheduled at the same time had a similar file or folder task, the output filename/ foldername was displayed incorrectly. This issue has now been fixed.
- OpManager: When alarm notes were updated, the value of the previous severity was updated to -1. This issue has now been fixed.
- OpManager: ${message} variable is now supported in workflow for executing Windows script and Linux script tasks.
- OpManager: When adding traps from 'Load from MIBs', the trap description was not added. This issue has now been fixed.
- OpManager: Previously, if storage device details were updated from the device snapshot page, the changes were not reflected. This has now been fixed.
- OpManager: There was an issue with the multiple delete option for traps. This has now been fixed.
- OpManager: For storage devices, storage dial data was not displayed in the device snapshot page. This issue has now been fixed.
- OpManager: In API access reports, the sorting issue in the column 'Process time (ms)' has now been fixed.
- OpManager: For certain interface based reports, the device group was listed. This issue has now been fixed.
- OpManager: In groups, when a 'Custom field' of numeric type is selected in criteria, the group could not be created. This issue has been fixed.
- OpManager: Bulk delete option is now supported for groups.
- OpManager: IPv6 network discovery issue has now been fixed.
- OpManager: In Reports, under the devices availability dashboard there was a graph loading issue for other languages. This

issue has now been fixed.

- OpManager: In Zoho maps, the tool-tip with the option to delete a device was not displayed when the device was clicked on the map. This issue has now been fixed.
- OpManager : Under Interfaces in the device snapshot page, the option to sort Rx and Tx traffic based on units has been enhanced.
- OpManager: In the device availability dashboard report, there were issues with the 'Exclude days' option. This has now been fixed.
- OpManager: When drilling down on specifics under the monitors tab from the device snapshot page, users were redirected to the edit threshold page instead of the graph view page for application monitors. This issue has now been fixed.
- OpManager: The HTML injection vulnerability issue in Google maps has now been fixed. (CVE-2017-11560)
- OpManager: Now, when you select a storage device model in the 'Add storage device' screen, the supported models and prerequisites for that device model will be displayed.
- OpManager: Unwanted Protocol names which are being displayed in graphs and reports for storage devices are removed.
- OpManager: Now supports storage monitoring for the following device series in NetApp: E2600, E2700, E2800, E5400, E5500, E5600, EF540, EF550, EF560.
- OpManager: In trap processors, there were issues with the bulk delete option. This has now been fixed.
- OpManager: For trap processors, 'greater than' and 'lesser than' support has been added in the match criteria condition.
- OpManager: In graphs, it was not possible to view the data for last 24 hours as the 'STATSDATA' table was not renamed in PGSQL essential to enterprise migration. This issue has been fixed.
- OpManager: In mobile application, notification messages were still sent to a deleted user account. This issue has been fixed.
- OpManager Enterprise Edition: The status of Central will be displayed in the header band of all probes connected to it. The number of probes up or down will now be displayed in the header band of the central.
- OpManager Enterprise Edition: In Professional to Enterprise migration, a warning message displayed for installing a new probe. This has now been fixed.
- OpManager Enterprise Edition: When SSL is enabled in Central and a proxy is used, the probe registration failed. This issue has now been fixed.
- OpManager Enterprise Edition: If the probe is updated manually when there is no communication between Central and probe, the probe start up failed when the communication was established after upgrade. This issue has been fixed.
- OpManager Enterprise Edition: When the probe and Central is migrated from pgSQL to MSSQL when there is no communication between Central and probe, probe start up failed when communication was re-established. This issue has now been fixed
- OpManager Enterprise Edition: Upgrading the probe to a higher version than Central caused the probe to shutdown automatically. This issue has now been fixed.
- OpManager Enterprise Edition: When the probe is deleted from Central, all related probe communication alerts will also be deleted.
- OpManager Enterprise Edition: During installation/migration of Essential(Professional) edition to Enterprise edition, a warning message will be displayed if an existing probe is added.
- OpManager Enterprise Edition: The 'Servername' and 'Serverport' of the last deleted probe was displayed for a newly installed probe. This issue has now been fixed.
- OpManager Enterprise Edition: When the Central was not reachable, there was a delay in logging into probe as the IPSLA monitor count had to be fetched from Central. This issue has now been fixed.
- OpManager Enterprise Edition: In Central, the device discovered time was not displayed in the inventory. This issue has now been fixed.
- OpManager Enterprise Edition: In probe, there was a delay when fetching &#65533;licenseDetails&#65533; from Central. This has now been fixed.
- OpManager Enterprise Edition: The probe name is now specified in the home page of Probe.

- OpManager Enterprise Edition: In the case of Central failure, archived files were moved to an unprocessed directory. This issue has now been fixed.
- OpManager Enterprise Edition: When connectivity to the Central server was disrupted, trying to associate any monitors to a device in a Probe would be unsuccessful. This issue has been resolved now.
- OpManager: Over 18 new device models and default performance monitors have now been added in OpManager.
- OpManager: When the dynamic IP address option is enabled in Windows, the localhost status was displayed as down. This issue has been fixed.
- OpManager: For the Spanish version of Windows operating system, the ICMP ping method was not successful. This issue has been fixed.
- OpManager: In Layer2 discovery, devices not in the specified IP range were being discovered. This issue has now been fixed.
- OpManager: In Map settings under system settings, admin users can now customize the color codes that indicates link traffic in Business views.
- OpManager: Color coding was not shown in availability dashboard report while exporting as PDF.This issue has been fixed.
- OpManager: Interface status was not cleared when all the threshold values are given.This issue has been fixed.

Build No 124016 - 124033 - July 22, 2019

- OpManager: SQL injection and other vulnerability issues in application monitors/servers, UCS monitoring, database maintenance, archiving & performance monitors, file/folder monitoring, URL/script templates have been fixed.
- OpManager: Data collection in URL monitors failed due to few URLs that required cookies to be accepted in browser. This issue has now been fixed.
- OpManager: Hyper-V servers can now be discovered automatically by configuring the ﷽schedule discovery﷽ option. It updates the Hyper-V server inventory automatically once in every two hours.
- OpManager: Due to the page loading issue in performance monitors page, the data displayed was overlapped when navigating to another page in the monitoring tab. This issue has now been fixed.
- OpManager: Incorrect ﷽Windows service down﷽ alerts were raised during device downtime. This issue has now been fixed.
- OpManager: In URL monitors, no data was displayed for ﷽Last n hours response time﷽ monitor. This issue has now been fixed.
- OpManager: In health and performance reports, the sorting for ﷽Volumes with most free space﷽ report was incorrect. This issue has been fixed.
- OpManager: For health and performance reports, language localization option was missing. This has been fixed now.
- OpManager: When generating a new report for performance monitors from category under monitors, there was a mismatch of data between the header and data. This issue has been fixed.
- OpManager: When a Windows service monitor with a display name similar to another Windows service monitor is added, false alerts were raised even when the service name is different. This issue has now been fixed.
- OpManager: When a monitor associated with a device is removed from the windows service monitors page, the related alerts were not deleted. This issue has now been fixed.
- OpManager: If a Windows device contains special characters, workflow involving the 'NT Service' and 'NT Service Polling' were not executed for the device. This issue has now been fixed.
- OpManager: In Windows service monitors page, issues related to sorting and searching with display name have been fixed.
- OpManager: In file monitors, there were issues with the configured ﷽consecutive times﷽ parameter for 'FileExists'. This has now been fixed.
- OpManager: Integration with Slack is now supported in OpManager.
- OpManager: Shift key support has been added for device associations.
- OpManager: Issue when resizing the Device summary widget in dashboard has been fixed.

- OpManager: Redirection issue in Business view, created using flash has been fixed.
- OpManager: Encryption for Trap Profile's community and SNMPv3 credentials has been improved with a stronger encryption algorithm for enhanced security.
- OpManager: Previously, it was not possible to edit and save scheduled reports created from the device snapshot page. This issue has now been fixed.
- OpManager Storage Monitoring: OpManager now supports monitoring of the following storage devices - HPE Nimble, Pure Storage, Dell Compellent SC4020, SC5020, SC7020, SC8000, SC9000, SCv3000, SCv3020.
- General: HTML Injection vulnerability issue in Google maps has now been fixed.(CVE-2017-11560)
- General: The SQL injection vulnerability in 'Reports' page has been fixed.
- General: The SQL injection vulnerability in 'SubmitQuery' page has been fixed.
- General: Previously, when HTTPS was enabled in the WebClient, some unexpected loading issues were observed. This has now been resolved by upgrading the Tomcat version used in the product.
- General: Scroll issue while listing custom dashboards has been fixed now.
- General: The 'local privilege escalation' vulnerability has now been fixed.
- General: Apache's 'commons-fileupload' jar has been updated to version 1.3.3 due to 'Remote Code Execution' vulnerability through manipulation of the 'DiskFileItem' in an older version.

Build No 123329 - 124016 - June 25, 2019

- OpManager: You can now configure notifications for alarms from VMware datastores by associating these datastores to Global Notification Profiles.
- OpManager: An option to verify the Service Up/Down Status while adding Service Monitor has been provided now.
- OpManager: SQLInjection and other Vulnerability Issues for Edit Threshold, Delete Performance Monitor & Adding Script Template action has been fixed now.
- OpManager: Negative Values were recorded for the monitors like Committed Bytes and Registry Quota for some of the servers and desktops. This has been fixed now.
- OpManager: OpManager Standard Edition has been launched for SMEs with basic network and server monitoring requirements.
- OpManager: The OpManager Essential Edition is now renamed as the OpManager Professional Edition.
- OpManager: From the Central device template page, option has been added to associate device templates directly to devices.
- OpManager: You can now configure alerts for the 'bandwidth has exceeded specified limit' criteria from 'Notification Profiles'.
- OpManager: Duplicate performance monitors have now been removed from the list of performance monitors.
- OpManager: When a large number of VLANs are monitored, the data-collection process was slow. This has now been optimized.
- OpManager: In 'Add Device', if serial number is enabled in custom fields, it will automatically be displayed in the device's snapshot page.
- OpManager: In the device snapshot page, the availability graph displayed incorrect time values. This issue has been fixed.
- OpManager: In availability reports, the reports displayed data only for a few days when the 'last month' filter was selected. This issue has been fixed.
- OpManager: In discovery profile, when a considerably large IP range was configured, an 'OutOfMemoryException' was thrown. This issue has been fixed.
- OpManager: The IP address was set as the display name even when the DNS name was resolved. This issue has been fixed.
- OpManager: Status update is restricted for an active downtime schedule. A warning message will now be displayed.
- OpManager: In the Inventory, 'sort by' option has now been provided for heat map and icon view.
- OpManager: Previously, rediscovered interfaces were not updated in the interface list and had to be refreshed. This issue has

been fixed.

- OpManager: In the device interface list, the option to bulk delete interfaces has now been enhanced.
- OpManager: Basic monitors and template for Nutanix device monitoring using SNMP has now been added.
- OpManager: Monitors that provide the mounted partition details for a device has been added.
- OpManager: Previously, VMware rediscovery for host based monitoring failed due to similar moRef ID for different VMs. This issue has now been fixed.
- OpManager: In the performance monitors page under settings and device snapshot page, auditing for add/edit/delete operations of monitors has now been added.
- OpManager: In the performance monitors page under settings, SQL injection vulnerability and other vulnerability issues have now been fixed.
- OpManager: In at-a-glance report for virtual devices, empty graphs with no data were displayed for few servers. This has now been fixed.
- OpManager: In a few rare cases, there was no communication between OpManager and APM plugin in the mobile application. This issue has now been fixed.
- NetFlow: Total Volume consumption details have been added in Schedule Consolidated Report.
- NetFlow : There was an issue in HighPerf Reporting Engine, where raw table split occurred frequently when more routers were added. This issue has been fixed.
- NetFlow : The issue where Security Settings was not visible in the Central Server, has been fixed.
- NetFlow : New flow export templates have been added to the Export Flow database.
- OpUtils: Previously under Network Monitor tool, the Read community was being queried while adding or importing devices. It has now been replaced by an option in which users could select the credential from the credential list.
- OpUtils: Path Traversal vulnerability in getSPMSettings API has been fixed.
- OpUtils : Previously on adding or scanning DHCP server, the scan failed due to missing AD domain username and password. Now those details are obtained from the user while adding.
- OpUtils : Previously under IP usage summary report, the used IP addresses were not displayed when "All" category was chosen. The issue is fixed now.
- OpUtils : Previously, the MIB browser tool did not display the assigned credential names having whitespaces for selected IP addresses. This issue is fixed now.
- OpUtils : Under Scheduler of SPM, the switches in 'selected switches column' present in edit task option were not sorted. The issue is fixed now.
- General: Users can now enable or disable 'Chat support' option under settings.
- General: 'Chat support' for Chinese language has been added.
- General: In Reports, access to 'API Access' page under 'Audit' has been restricted for Operator type users.
- JRE has been migrated to 1.8 and various vulnerabilities from JRE 1.7 have been eliminated. Highlights of JRE 1.8 migration:
    - OpManager: 2048 bit key length algorithm is supported for URL monitoring.
    - General: Cipher algorithms AES-192 and AES-256 are supported in addition to AES-128 algorithm.
    - General: TLSv1.2 protocol is now supported by default.

Build No 123329 - May 23, 2019

- OpManager: Storage report name was displayed as 'undefined' instead of 'Storage summary'. This issue has been fixed now.

Build No 123327 - April 03, 2019

- NetFlow: XSS vulnerability in the Attacks settings page has been fixed now.
- NetFlow: Dashboard graph issue has been fixed.
- NetFlow: Custom time selection option has been added for multiple-device compare report.
- NetFlow: Previously, FlowRate in forensics was calculated for Bytes/sec. It can now be calculated for bits/sec.
- NetFlow: Geo Location has been updated with the latest details.
- NetFlow: The issue with scheduling Compare Reports for custom time period has now been fixed.
- NetFlow: 0.0.0.0 invalid IP address validation has been added to Applications Names creation.
- NetFlow: NetFlow database has been updated with the latest Application names.
- NetFlow: Each API request's parameter type and value in settings module is now verified before processing it, to avoid any vulnerabilities.
- NetFlow: NFA now supports user defined data units.
- NetFlow: Binary / Decimal notation for data units has been introduced in NFA.
- NCM: NCM now supports regular expression login prompt, enable prompt and configlet prompt (only for SSH protocol).
- NCM: Earlier, taking backups of multiple devices, with some of them being unmanaged devices, resulted in an error message. Now, NCM takes backup of the managed devices, ignoring the unmanaged devices.
- NCM: There was an issue with the EOL/EOS data updation while discovering new devices into NCM. This issue has been fixed.
- NCM: Earlier, the NCM server CPU usage went up to 100%, in a few cases, while executing a scheduled backup. This issue has been fixed.
- NCM: Earlier, there was a delay while updating device credentials. This issue has been fixed.
- NCM: Earlier, there was an issue while trying to view Security Audit and Configuration Analysis report. This issue has been fixed.
- NCM: The backup failure issue while using the SNMP-TFTP protocol has been fixed.
- NCM: There was an issue with the detailed view of Compliance Reports in Custom Reports. It has been fixed.

Build No 123326 - March 29, 2019

- OpManager: In the device snapshot page, the custom dial color is now displayed based on the threshold severity level. The default color will be displayed if no threshold is configured.
- OpManager: In the add trap processor page, the version was displayed incorrectly. This issue has now been fixed.
- OpManager: In the interface configuration page, there were issues with the 'Select all' option in the 'Manage' and 'Status poll' columns. This issue has been fixed.
- OpManager: In the interface rediscovery page, the interface status was represented with brown color instead of green color when interface rediscovery was performed more than once. This issue has been fixed.
- OpManager: When an interface's counter type is changed from 32-bit to 64-bit or vice versa, it can be updated during interface rediscovery.
- OpManager: In Enterprise edition, when the probe was running as a service with central in HTTPS mode, there were issues with smart upgrade option in builds after the 123181 release. This has now been fixed.
- OpManager: The alarms raised were not cleared automatically due to a thread lock issue. This has now been fixed.
- OpManager: In Reports, a few parameter requests were passed as a query string. This has now been converted to form-data.
- OpManager: XSS vulnerability affecting report name and description has now been fixed.
- OpManager: XSS vulnerability in notes column has now been fixed.
- OpManager: In availability reports, there were issues with exporting the report in XLS format. This issue has been fixed.
- OpManager: When scheduling reports, if the '-' symbol is used in the schedule name, an empty page was displayed. This issue has now been fixed.
- OpManager: Previously, the delete older files task deleted all the files in the folder. This issue has now been fixed.

- OpManager: Previously, the move older files task moved all the files in the folder. This issue has been fixed.
- OpManager: Previously, the compress older files task compressed all the files in the folder. This issue has now been fixed.
- OpManager: The XSS vulnerability in workflow name has now been fixed.
- OpManager: The XSS vulnerability in destination host column under Forward traps has now been fixed.
- OpManager Storage Monitoring: There were some issues with discovery of HP 3Par devices. It has been fixed now.
- OpManager Storage Monitoring: In rare cases, there were issues in downloading PDF files (from Graphs section). It has been resolved now.
- NetFlow: Upgrade Issue on 123294 has been fixed.

Build No 123325 - March 27, 2019

- OpManager: New chart types (line, bar, area, scattered) have been added for interface graph widgets.
- OpManager: In map widget, the zoom option was not available unless the widget was edited. This has now been fixed.
- OpManager: When an ongoing downtime schedule is edited, an alert message will be displayed with an option to end the schedule process.
- OpManager: Option has now been provided to delete an active downtime schedule.
- OpManager: Over 1000 new device models and default performance monitors have now been added in OpManager.
- OpManager: Previously, while editing a Downtime Schedule assigned to Business Views, there was a mismatch between the previously selected business view and the one displayed (although the latter is not affected). This issue has now been fixed.

Build No 123323 - March 21, 2019

- OpManager: Earlier OpManager Central server had issues with stopping the service. This has been fixed now.
- General: In AD authentication, you can now configure scope to be auto-assigned to users logging-in for the first time, when auto-login is enabled.

Build No 123322 - March 18, 2019

- OpManager: The new grouping feature enables the user to classify a set of devices or interfaces or both, as a single functioning node. The following functions can be performed on groups: Checking for availability of group members, configuring alarms for a group, applying bulk monitoring thresholds to a group, generating group reports, monitoring group widgets ,applying filters to groups, and more.

Build No 123320 - March 12, 2019

- General: Windows AD based authentication is now supported on Linux installations.
- General: Due to Google Play Store restrictions, support for SMS notifications through AppSMS has been revoked.
- OpManager: In web alarm notification profile, the option to upload sound files has now been added.
- OpManager: In web alarm notification profile, option has been added to associate all the administrators and operators.
- OpManager: During product startup, deadlocks occurred in a few rare cases.This issue has now been fixed.
- OpManager: In the login page, a '400 bad request' occurred when the 'Keep me signed in' option was enabled. This issue has now been fixed.

Build No 123314 - March 8, 2019

- OpManager: In Device Snapshot page of hardware supported devices, ﷺOperating Systemﷺ was wrongly displayed as 'OS Version'. This has now been corrected.
- OpManager: ﷺPage not foundﷺ was displayed when the URL contained ﷺ/ﷺ character at the end. This error has been fixed.
- OpManager: Disk utilization values for high capacity hard disks were displayed incorrectly when fetched through SNMP. This has been fixed now.
- OpManager: It was not possible to set rearm value as zero for File/Folder monitors. This has been addressed.
- OpManager: When multiple instances of Hyper-V VM was running, CPU utilization was displayed incorrectly. This has been fixed.
- OpManager: When creating custom SNMP monitors, ﷺSave Absolutesﷺ option has been added for Integer type OIDs.
- OpManager: Username and password fields are now optional for setting up proxy in the install shield wizard. However, the password field cannot be blank if a username is specified.

Build No 123313 - March 5, 2019

- OpManager: The real time graph for interfaces displayed values exceeding the configured speed. This issue has now been fixed.
- OpManager: Previously, when an interface name contained special characters, the specific interface was not saved during rediscovery.This issue has now been fixed.
- OpManager: The downtime schedule process was triggered automatically even after the schedule was completed. This has now been fixed.
- OpManager: In some cases, device availability and the device status was displayed incorrectly. This issue has now been fixed.
- OpManager: The page loading time for Discovery reports was slow when there were a large number of entries. This issue has been fixed.
- OpManager: For a few devices, the category was displayed as 'Unknown' for a device template associated with a custom category. This issue has been fixed now.
- OpManager: In device templates, the OIDs with SysDescription criteria were not working properly. This issue has been fixed.
- OpManager: Operator users can now view the at-a-glance report and bandwidth report.
- OpManager: The interface archiving failure issue has now been fixed.

Build No 123312 - February 28, 2019

- NetFlow : The option to log SDP/ SDP-MSP tickets has now been added for LinkDown alerts.
- NCM: Discovery reports have been added newly to allow users to see the discovery progress live.
- NCM: A new option has been provided in discovery reports for adding devices which were not reachable during the discovery process.
- NCM: Users can now choose the devices they wish to add to Inventory, from the list of discovered devices, instead of adding all the discovered devices automatically.
- NCM: How To and FAQ's are provided for all the major settings pages, Devices Tab in Inventory and Device Snapshot page.
- NCM: New Messaging Framework has been implemented for NCM. Users can now see the appropriate messages on all the important pages to help them use NCM better.
- NCM: The discovery tab has been simplified to make device discovery process easier.

Build No 123311 - February 26, 2019

- OpManager: In the Alarm page, link has been provided to view interface Snapshot page.
- OpManager: Previously, the option to export a report in XLS format was not available when there were more than 32000 rows. This issue has now been fixed.
- OpManager: The option to export a report in XLS format was not available when specific styles were applied to the rows. This issue has now been fixed.
- OpManager: In the data collection log report, the agent dropdown box was not displayed. This issue has now been fixed.
- OpManager: In reports, when the specific time window condition was applied, data was not displayed. This issue has now been fixed.
- OpManager: Previously, when an availability report was scheduled, a report was created but the mail with the attached report was not sent. This issue has now been fixed.
- OpManager: Previously, while editing the SNMP trap processors, removing the contents of the message box resulted in a missing field. This issue has been resolved.
- OpManager: There were issues in data collection and alarm notifications for NetApp storage devices when added as a generic device from 'Add device' menu. This has been resolved now.
- OpManager: For at-a-glance report, the option to export the report as XLS was not working. This issue has now been fixed.
- OpManager: Integrated reports have been hidden from the edit and schedule report option.
- OpManager: The help-desk widgets and dashboards have been removed from the product.
- OpManager Storage Monitoring: There were issues with data collection in IBM v7000 storage devices. This has been fixed now.
- OpManager Storage Monitoring: Storage device support has been added for the following devices: IBM Storwize V5000, V3500, V3700.
- OpManager Storage Monitoring: Previously, there were issues in discovery and data collection in EMC VMAX. This has been fixed now.

Build No 123308 - February 19, 2019

- NetFlow : HighPerf installation error in the Japan language server has been fixed.
- NetFlow : Users can now configure tax or additional fees in Billing.
- NetFlow : Notification messages for product assistance have been included to help users. They can be enabled or disabled under general settings.

Build No 123307 - February 15, 2019

- General: User Notifications (notifications listed under bell icon) will now be grouped and will have options to be hidden.
- OpManager: Previously, there was an issue in loading the probe's dashboard from Central. This issue has now been fixed.
- OpManager: During probe installation in linux systems, there was an issue with proxy configuration. This issue has now been fixed.
- OpManager: Associating devices of more than one category/business view is now supported while adding or updating notification profiles.
- OpManager: Devices will now be listed based on category/business view while using the Quick Configuration Wizard (QCW) to associate notification profiles.
- OpManager: In Notification Profile, an option is now provided to select between 1/3/5 polls to trigger alerts based on the 'Device misses poll(s)' criteria.
- OpManager: In 'Notification Profiles Triggered' report, there was an issue in the displayed tabular information when it was

exported in PDF format. This issue has been fixed.

Build No 123306 - February 13, 2019

- NCM: Previously, there was an inaccuracy in percentage values in the compliance snapshot piechart. This issue has been fixed by removing the percentage marker.
- NCM: Now, Nipper Report filenames include the device hostname or IP address.

Build No 123305 - February 12, 2019

- OpManager: In 'Network discovery', there were issues with the 'ignore' filter in custom category. This has now been fixed.
- OpManager: In 'Device templates' under Configuration, clicking on a device template number displayed the devices list instead of the respective devices in that device template. This issue has now been fixed.
- OpManager: In interface graphs, it was not possible to modify and set a custom time period. This issue has now been fixed.
- OpManager: In Device Categories, all device categories are now displayed along with the custom categories.
- OpManager: In Maps, it was possible to export the map to excel and download it even if there are no devices present in the map. This issue has been fixed.
- OpManager: In the Device List view under Inventory, when sorting devices by 'Device Name', the devices with names starting with an upper case were displayed at the top. This issue has been fixed.
- OpManager: In probe setup, during rediscovery the device name was not displayed properly for non-SNMP devices. This issue has been fixed.
- OpManager: Previously, it was not possible to add the devices that could not be reached through ICMP in CSV discovery. This has now been implemented.
- OpManager: The device status for devices that cannot be pinged was not properly updated in the Central server. This issue has now been fixed.
- OpManager: The display name for SNMP enabled devices was different from the name provided in the CSV file. This issue has been fixed.
- OpManager: The Layer2 map discovery failed when multiple incorrect SNMPv3 credentials were selected. This issue has now been fixed.
- OpManager: There was a data collection failure when 'engineID' was changed in the device. This has now been fixed.
- OpManager: There was an issue in data collection for SNMP string monitors with 'StringToNumeric' expression, when the response was a float value. This issue has now been fixed.
- OpManager: There were issues with auto dependency classification for imported Layer 2 devices. This issue has been fixed.
- OpManager: When scheduled rediscovery was executed, the device template applied manually kept rolling back to the default template. This issue has now been fixed.
- OpManager: For devices added from the OpManager's add-ons, the encoding details were not defined in the device snapshot page. This issue has been fixed.
- OpManager: In the snapshot page, it was not possible to edit device details for domain controllers. This issue has been fixed.
- OpManager: In Layer 2 maps, while importing devices, it was not possible to select and discover a single device. This issue has now been fixed.
- OpManager: In NOC view, garbled characters were displayed in the widget's display name. This issue has now been fixed.

Build No 123304 - February 8, 2019

- General: Previously, validation of session failed when the URL contained two or more consecutive backslashes. This vulnerability has been fixed now.

Build No 123303 - February 7, 2019

- OpManager: Performance monitors now also support float values along with integer and string values.

Build No 123295 - February 4, 2019

- General : For Windows firewall, TCP port unblock rules added for Tomcat webserver port.
- General: An error message will show details regarding the number of remaining login attempts or the lockout duration, when there is an invalid login attempt based on the configured password policy.
- General: 'Mail Server Settings' and 'Notification Profile' will now support mail addresses with special characters and gateway (IP) addresses.
- General: In Linux installation, the issue affecting the free space validation has now been fixed.
- OpManager: An option is now provided to 'Enable/Disable' notification profiles.
- OpManager: Previously, notification profiles sent 'Alarm Cleared' alerts for all the selected monitors that rearmed, despite configured severities in the profiles. This issue has been fixed.
- OpManager: In 'Notification Profile', users were notified of cleared alarms for UPS monitors when the only criteria selected was "When any UPS monitor is down" and not "Notify when the alarm is cleared". This issue has been fixed.
- OpManager: Notification profiles triggered down alerts after the configured delay even when the alarms were cleared. This issue has been fixed.
- OpManager: Notification messages for product assistance have been included to help users. They can be enabled or disabled under settings.

Build No 123293 - January 28, 2019

- OpManager: In 'Alarms', there was an issue in sorting alarms based on criteria. This issue has been fixed.

Build No 123292 - January 25, 2019

- OpUtils: Hint messages that helps in knowing intricate details of the product has been shown in various pages now.
- OpUtils: Global Search enabled for IPAM & SPM.
- OpUtils: Previously, Sorting of columns in Bandwidth Monitor was not working properly as expected. This has been fixed now.

Build No 123291 - January 24, 2019

- OpManager: Service Now Integration has now been introduced in OpManager.
- OpManager: Support for monitoring Microsoft Windows 2019 & Microsoft HyperV 2019 servers has now been added.
- OpManager: The option to add a custom SNMP monitor has been improved and simplified. Users can now add multiple node type of monitor for devices from within the UI.
- OpManager: In device templates, there were issues with adding custom SNMP monitors from the central server. This has now been fixed.
- OpManager: In the performance monitors page under settings, a new filtered view has been added for custom monitors and default monitors.
- OpManager: When adding or editing string monitors, the threshold field validation was missing. This has now been handled.
- OpManager: When a monitor was edited and saved, the changes made in 'Consecutive time' and 'Save Absolute value' were not reflected. This has now been fixed.
- OpManager: In application monitors under settings, big integer values were restricted for thresholds. This has now been removed.
- OpManager: Security issues in VMware/HyperV/Xen specific APIs have now been fixed.
- OpManager: The PPM upgrade issue due to missing entries related to hardware from previous upgrades has now been fixed.

- OpManager: There were issues with the time filter option when editing any monitor apart from performance monitors. This has now been fixed.
- OpManager: File monitors could not be added when special character like '/' was used in the search string for match option. This has now been fixed.
- OpManager: Event logs raised with description messages having accent characters in the Russian language were not displayed properly in OpManager. This has been fixed now.
- OpManager: When adding or editing the performance monitor under settings, if incorrect threshold values were configured, the error message was displayed incorrectly in the Japanese language. This has been fixed now.
- OpManager: When loading a specific graph page from the device snapshot page, the page was not loaded properly. This has now been fixed.
- OpManager: From the VM list widget inside vCenter/ESX/HyperV/XenServer snapshot pages, the 'Start monitoring' option to start/stop VM monitoring as virtual server was not working when accessed from other pages apart from the first. This has now been fixed.
- OpManager: In inventory, the alignment issue inside the exported XLS sheet for process monitors has now been fixed.
- OpManager: Under monitors tab in the device snapshot page, the maximum number of configured monitors for a certain type will now be listed first.
- OpManager: In the VMware discovery page, when the drop-down box to increase the display count of VMs was clicked, the previously selected VMs were unselected. This issue has been fixed.

Build No 123290 - January 22, 2019

- OpManager : The archiving failure issue in OpManager Central has now been fixed.

Build No 123289 - January 18, 2019

- OpManager : When clicking on a device in an embedded business view widget, the device page did not display any information and was blank. This issue has been fixed.
- OpManager : In Maps, after navigating to a device snapshot page from business view, it was not possible to go back to the business view page by clicking on the 'back' button. This issue has been fixed.
- OpManager : If a device filter was applied to the 'Devices' list in the inventory page, it was also reflected in the 'Business View' device list. This issue has been fixed.
- OpManager : When clicking on an existing business view a blank page was displayed in the Map view. This issue has now been fixed.
- OpManager : In Business view, there were issues with uploading a new background image. This has now been fixed.

Build No 123288 - January 17, 2019

- NetFlow: Introduced an option to view raw data storage information.
- NetFlow: Introduced multiple combinations of IP address for "From" and "To" in Between Sites IP Grouping bulk load.
- NetFlow: The bulk load feature in IP group and application mapping has been enhanced with options to download and upload sample .xml files.
- NetFlow: This issue with wrong Maximum value displayed in the Compare Report Graph Table has been fixed.
- NetFlow: The issue with schedule deletion, update and audit in Schedule Report has been fixed.
- NCM : Now you can transfer files from NCM server to devices using Configlets via SCP client

Build No 123287 - January 14, 2019

- General: There was an OOM (out of memory) issue due to the unused ports that collect data in OpManager. This issue has been

fixed.

- General: In the login-page, the 'Keep me signed in' check box was selected after every login even when it was unchecked. This issue has now been fixed.
- General: In the device snapshot page, the 'Terminal' icon is now hidden for the operator user.
- OpManager: The XSS vulnerability in 'Notification Profile name' has now been fixed.
- OpManager: In Notification profile, ﷺ field has been included for email notifications in addition to the 'To' and 'From' address fields.
- OpManager: RADIUS authentication protocol is now supported in OpManager mobile application.

Build No 123281 - January 10, 2019

- Firewall: Cisco FirePOWER - Firewall policy, rule analysis, and compliance report support using CLI to fetch configurations.
- Firewall: To prevent vulnerabilities, Firewall Analyzer now verifies each request parameters type and value before it is processed.
- Firewall: Support-ID: 4882018 - In Japanese installation, if 'Trend graph' report is exported, it displays the same graph for hourly and weekly comparison graphs. This issue is fixed.
- Firewall: Cisco Meraki is discovered as 'proxy server' instead 'firewall' in Firewall Analyzer. This issue is fixed.
- Firewall: When server side PDF export is set as 'All', it is not working. This issue is fixed.
- Firewall: When 'Denied User Report' is drilled down from Dashboard, page is empty. This issue is fixed.
- Firewall: Raw search result displayed in the UI is grouped based on the specified criteria.
- Firewall: Quick links are added for 'Credential Profile' page.
- Firewall: Quick links are added for 'Archive Encryption' page under Security settings.

Build No 123280 - January 8, 2019

- OpManager: Storage device support has been added for EMC Unity and EMC VNXe3200.
- OpManager: There were issues with discovery and data collection in EMC VNXe3150, EMC VNXe3300 and EMC Isilon. This has been fixed now.
- OpManager: Previously, it was not possible to clean up the Event Table manually. This can now be configured from the Database Maintenance page.
- OpManager: Alarm notes continued to exist even after the associated alarm was deleted. This issue has now been fixed.
- OpManager: The XSS vulnerability in report name and description has now been fixed.

Build No 123279 - January 7, 2019

- OpManager: In Maps, option to filter devices based on category has now been added for 'Rack Builder'.
- NCM: The XSS Vulnerability in 'addScheduleforConfig', 'addLabel', 'updateLabel', 'addShowCommand', 'addSharedCredentialProfile', 'updateSharedCredentialProfile' API's has been fixed.

Build No 123278 - January 4, 2019

- OpManager: Probe installation has been authenticated.
- OpManager: The unauthenticated access to Enterprise edition servlets has now been fixed.

Build No 123277 - January 3, 2019

- OpManager: The SQL injection vulnerability in 'getDeviceCompleteDetails' and 'getAssociatedCredentials' API's have been fixed.

Build No 123276 - January 3, 2019

- OpManager: Unauthenticated access to 'AgentActionServlet', 'DataAgentHandlerServlet', 'FileCollector', 'RegisterAgent' and 'StatusUpdateServlet' used for agent based file monitoring functionality has now been restricted.

Build No 123241 - 123275 - December 31, 2018

- OpUtils : Under Inventory, Actions column with scan and delete option is made available which makes it easier to do these functions.
- OpUtils : Under Inventory, approving of subnets can be done in a few clicks now by selecting the 'Approve' option found in discovered subnets.
- OpUtils : Previously under Inventory, 'Approve Subnets' tab didn't display the subnet address and mask values of a selected subnet. The issue is fixed now.
- OpUtils : Under Inventory, 'Added Time' column is added and many other irrelavant columns are removed from the discovered subnets of IPAM.
- OpUtils : Under Inventory, an appropriate message is now displayed when bulk subnets are selected for approval.
- NCM: "Grid view" option has been introduced in the Device Group page. Now, users can switch between "Grid View" and "Widget View" as per their need.
- NCM: Look and feel for info messages in all the forms have been changed.
- NCM: All the reports can be generated in both Widget and Grid View for device groups directly from the Device Group page.
- NCM: Tasks can be scheduled for all the device groups directly from Device Group page.
- NCM: Users can now run compliance check and associate groups to compliance policies directly from Device Group page.
- OpManager: Under Server dashboard, two new types of Heat maps have been introduced to represent all file and folder monitors associated to the respected devices in OpManager.
- OpManager: New default reports have been introduced for VM Sprawl data under Virtual server reports.
- OpManager: 34 new monitors for disk, memory and processor have been added in addition to the existing WMI monitors.
- OpManager: In VMware/ESX discovery, VMware datastore of type 'VSAN' were not discovered. 'VSAN' support has now been included.
- OpManager: If VMware ESX had either a 'HostPortGroup' or a 'HostVirtualSwitch' with the same name (case insensitive), there were issues with vCenter/ESX server discovery. This has now been fixed.
- OpManager: When an unmonitored ESX host under vCenter is monitored by mapping from the vCenter snapshot page, hardware monitor for that ESX Server was not initiated even when it was enabled. This issue has now been fixed.
- OpManager: During HyperV server discovery, some HyperV server entities were not discovered in certain cases. This issue has been fixed.
- OpManager: When a large number of VMware events were raised, they were not reflected in the monitored vCenter/ESX servers. This issue has been fixed.
- OpManager: During multiple XenServer or server pool discovery, storage repositories and networks were discovered only for one pool. This issue has been fixed.
- OpManager: Under Discovery, when multiple credentials were selected, the device was discovered under 'unknown' category. This issue has been fixed.
- OpManager: Previously, in SNMPv3 discovery, engineID was duplicated for different devices. This has been fixed and now if engineID matches with engineID of already added device, then the device will be added as Non-SNMP Device.
- OpManager: Rebooting the device caused SNMPv3 data collection to stop. This issue has been fixed.
- OpManager: Previously, Test credentials displayed status as 'Pass' even when the credentials were wrong. This has been fixed now.
- OpManager: No proper error message was displayed when MIB browser was not working with SNMPv3 credentials. This has

now been fixed.

- OpManager: The flash Business view was not accessible by the operator user. This issue has been fixed.
- OpManager: The link generated using 'Embed widget' was not working for Rack view, 3D Floor view and Floor details widget. This issue has now been fixed.
- OpManager: When editing custom fields in device snapshot page, the encoded characters were displayed for all other languages apart from English. This issue has now been fixed.
- OpManager: For CLI snapshot page credentials, the prompt value for 'Command', 'Login' and 'Password' were displayed as an encoded character. This issue has been fixed.
- OpManager: In Interfaces view under 'Inventory', the interfaces are now sorted based on 'ifIndex'.
- OpManager: Previously, accessing Downtime Schedules from Settings --> Configuration--> Downtime Schedules displayed a blank page. This issue has been fixed.
- OpManager: Previously, accessing Rule Engine from Settings --> Configuration --> Rule Engine displayed a blank page. This issue has been fixed.
- OpManager: In Maps, when refreshing the tab after selecting and saving 'Google Maps' as the primary option, 'Zoho Maps' was displayed again. This issue has been fixed.
- OpManager: Warning messages for certain actions has been added to provide better clarity.
- OpManager: The link status and traffic load were missing in the NOC view and Dashboard. This has been fixed.
- OpManager: The loading time for all devices in business view has been optimized.
- OpManager: It was not possible to generate interface graphs for a custom time period. This issue has now been fixed.
- OpManager: The loading speed has been optimized for:
    - Device Template list page.
    - Vendor Template list page.
    - Edit Device details page.
- OpUtils: Under Settings of Switch Port Mapper, dropdown options such as port number and interface name are given inorder to show port label text in switch snapshot page.
- OpUtils : The Community Checker tool, which scans the range of IP Addresses to get their SNMP read and write community strings in the network, has been brought back under SNMP tools.
- General: SQL injection vulnerabilities in unauthenticated servlets has been fixed.
- OpUtils : Under Mac-to-IP Mapping, The XSS vulnerability issue in addRouter API has been fixed.
- OpUtils : Under IPAM Settings, The XSS vulnerability issue in addIPAMScheduler API has been fixed.
- NetFlow : Inventory updater feature that fetches device details on scheduled time, has been introduced.
- NCM : Automatic Change Detection was not working. This issue has now been fixed.
- General : SMS notifications via the SMS gateway was not working properly when the proxy settings were configured. This issue has now been fixed.
- General : Password length of Mail Server Settings and Proxy Server Settings have been increased.
- General : Quicklinks and info messages have been added to help the user with 'How-To' and 'FAQ' in the Notification Profile, User Management, Mail Server Settings, Proxy Settings and Rebranding pages.
- General : When a CCTV view was deleted from the CCTV list, the Dashboard kept loading for a long time. This issue has been fixed.
- General : In CCTV view, the seconds timer sometimes displayed a negative value. This issue has been fixed.
- General : In some cases, there was an out of memory (OOM) issue during product startup. This has now been fixed.
- OpManager : A message variable has been added to include Probe Name details in alerts from the Central's Notification Profile.
- OpManager : Unable to save Run Program Notification Profile, when Arguments length exceeded 250 chars. This issue has now

been fixed.

- OpManager : Unable to save Run System Command Notification Profile, when Command String length exceeded 250 chars. This issue has now been fixed.
- NetFlow : WLC widgets now support SSID Group resource type.
- NetFlow : Schedule reports have been added for Access Point Group and SSID Group.
- NetFlow : Autonomous System details have been updated.
- Firewall : Vendor API based Compliance-Standards report for CheckPoint devices.
- Firewall : Export as CSV and Excel option has been provided for all Inventory and Reports drill-down pages.
- Firewall : Delete button alignment issue in Device-Rule list page issue fixed.
- Firewall : Fixed the 'Grey' color assigned to one of the Protocol-groups in the 'Traffic Statistics' graph which looks odd with the graph background.
- Firewall : Some unwanted resource check has been removed in the dashboard pages to improve the page loading.
- Firewall : 'Delete' option is shown as button now in Imported Logs, Device-Rule, Exclude-Criteria, Credential Profiles and Archived Files list pages.
- Firewall : Removed the 'Group Chat' icon in vertical tab UI.
- Firewall : CheckPoint log-import issue fixed for non-English OS installations.
- OpManager : In Notifications Profile, SNMPv3 support has been provided for trap forwarding. This option can be found in the Trap Profile section.
- OpManager: In Workflow, info messages have been added to indicate the types of scripts supported in 'Execute Windows Script' and 'Execute Linux Script', and to indicate the supported command line arguments in 'Execute Scripts'.
- OpManager: While creating a new workflow, each action will display a note of supported devices on which that particular action can be executed.
- OpManager: Confirmation messages will now be displayed before redirecting to the 'Log a Ticket (SDP) Configuration' or 'Mail Configuration' pages.
- OpManager: The 'Traps' heading has been changed to 'SNMP Trap Processors' in the Trap Processor list view page.
- OpManager: Learn more and quick links have been provided for 'Alarm Escalation', 'Workflow' and 'SNMP Trap Processors'.
- OpManager: In the Alarms page, there was an alarm count mismatch issue with the total alarms displayed as a pie-chart and the alarms displayed based on the severity. This issue has been fixed.
- OpManager: Previously, a few search filters in the Alarms page were not working properly. This issue has now been fixed.
- OpManager: In the Inventory page, while using 'filter by probe' option, the page count was displayed as zero. This issue has now been fixed.
- OpManager: "Log a ticket" task does not work when SDP or SDP-MSP is integrated after the Servlet API is upgraded to Rest API. This has been fixed now.
- OpManager: When Execute Workflow is clicked, the workflow executes more than once. This has been fixed now.
- General: The XSS vulnerability in alarm escalation has been fixed.
- OpManager: Previously, it was not possible to export a PDF in Russian language. This has now been fixed.
- OpManager: Timeout configuration is now available for SPD/SDP MSP.
- OpManager: It is now possible to configure the ﷺ format.
- OpManager: Option has been added to configure image position for ﷺ.
- OpManager: The message box in ﷺ option is now customizable with additional params.
- OpManager: Previously, it was not possible to properly identify the utilization peaks in ﷺ' interface. This has now been fixed.
- OpManager: In snapshot page, host name alias support is now provided for on click PDF.
- OpManager: There were issues with the option to exclude days in ﷺ reports. This has now been fixed.

- OpManager: The reports triggered from the ﷺNotification profileﷺ had a few issues in other languages apart from English. This has now been fixed.
- OpManager : Storage Monitoring : Previously, there were issues in discovery and data collection in PureStorage storage devices. This has been fixed now.
- OpManager : Domain controller devices were not categorized as "Domain controller" when they were discovered through Network discovery. This issue has been fixed.
- OpManager : Layer2 Discovery failed when the length of the discovered device type exceeded 50 characters. This issue has now been fixed.
- OpManager : In Discovery, the rule engine to associate script monitor failed when the threshold was configured. This issue has now been fixed.
- OpManager : While saving SNMP credential, it was not possible to save the credential type as "None". This issue has been fixed.
- OpManager : Under Discovery settings, a new option "Use DNS as DisplayName" is provided to set the DNS name as the display name after discovery.
- OpManager : The 'Edit Threshold' button was hidden when importing device templates. This has been fixed.
- OpManager : In the bulk credentials association page, there was no option to filter results based on 'Category' or 'Business view'. This has been added.
- OpManager : From the interface configuration page, when navigating to other listed pages from the first page, the selected configuration options were not updated. This issue has been fixed.
- OpManager : In the import devices page, there was no search option. This has now been added.
- OpManager : The discovery settings configuration page has been moved from Settings > Basic Settings > System settings to Settings > Discovery
- OpManager : Previously, there was an issue with Lucent-Xedia and Nortel Networks' device templates. This issue has been fixed.
- OpManager : Previously, interface data collection stopped when bandwidth exceeded the specified value. This issue has been fixed.
- OpManager : Previously, Bandwidth Utilization was calculated based on IFSPEED. Now, the same calculation is performed based on INSPEED and OUTSPEED.
- OpManager : Previously, configuring an unmanaged interface caused OpManager to manage that interface. This issue has been fixed.
- OpManager : Previously, there was a '?' (Question mark character) in the device template's Name and OID for Intel device templates. This issue has been fixed.
- OpManager : Previously, it was not possible to view interface reports due to big values in the interface data. This issue has now been fixed.
- OpManager : Ping failure case has been implemented for TTL (Time-to-live) expired message.
- OpManager : In the Dashboard, same data was displayed in all the interface bandwidth widgets. This issue has now been fixed.
- OpManager : Metrics for '95th percentile value' has been included along with the '95th percentile average' in Interface graphs.
- OpManager : For newer versions of Windows, the type will be classified in OpManager with an entry in the XML file.
- OpManager : In the Inventory page, bulk deletion of devices was time consuming .This issue has been fixed.
- OpManager : The Linux FreeBSD device was not classified properly. This issue has been fixed.
- OpManager : During scheduled discovery, the RAM and HardDisk size were not updated in the device snapshot page. This issue has been fixed.
- OpManager : Previously, the 'Packet Loss' dial in snapshot page displayed the day's average value instead of the last packet loss value. This has now been fixed.
- OpManager : In e-mails sent using the 'Send Email' notification profile with the custom message variable '$IntfField(ipAddress)', the device IP Address was displayed instead of the interface IP Address in the 'Interface Details' section of the message. This issue has been fixed.

- OpManager : The Downtime report displayed incorrect devices for the selected interval. This has been fixed.
- OpManager : For Business View users, the 'Device Availability Dashboard' report displayed devices that the user was not authorized to view. This issue has been fixed.
- OpManager : There were a few usability issues in the Device Template page.This has now been fixed.
- OpManager : In the Interface graph widget, there was an overlap issue with the graph.This has now been fixed.
- OpManager : In the Discovery page, 'Execute Now' option has been added to instantly start discovery.
- OpManager : Usability issues in the Discovery page have been fixed.
- OpManager : In BusinessView, the status did not get updated when the BusinessView shortcut was placed in a circular manner. This issue has been fixed.
- OpManager : In Maps, the satellite view button was not displayed for Google Maps. This issue has been fixed.
- OpManager : In the Downtime Scheduler page, option to Enable/Disable schedules has now been provided.
- OpManager : The Interface Bandwidth report has been renamed as Interface Speed Report. The columns 'Transmit Bandwidth' and 'Receive Bandwidth' have been renamed as 'Out Speed' and 'In Speed' respectively.
- OpManager : Adding a discovery rule engine can now be done from the 'Discovery Profile'.
- OpManager : The following titles/labels have been renamed across the product.
    - 'Downtime Schedules' to 'Device Downtime Schedules'.
    - 'Telnet/SSH/SNMP' in NCM to 'Backup Credential'.
    - 'Rule Engine' to 'Discovery Rule Engine'.
    - In Custom Fields, 'Import field properties from CSV' to 'Import from CSV'.
    - In Discovery profile, the 'Add filter' button as 'Add Discovery Filter'.
- OpManager: The navigation for the following pages have been changed.
    - The Categories tab has been moved to 'Configuration' from 'Basic settings'.
    - The IPSLA tab has been moved from 'Configuration' page to 'Monitoring' tab under Settings.
    - The 'Monitoring Interval' tab has been moved to 'Quick Configuration Wizard' page under Configuration.
- OpManager: Under 'Reports', a new hardware information report to show the basic hardware information has been included for all the hardware monitoring enabled devices.
- OpManager: A dedicated tab has been introduced for all the monitors in the device snapshot page.
- OpManager: In the Inventory, new main level tabs have been introduced for 'Network', 'Server' and 'Virtual' devices for easier navigation and sorting.
- OpManager: Previously, exchange monitors could not be saved if the path name of the storage location had '.' character. This has now been fixed.
- OpManager: When a new event rule was added with an existing rule name, the action was not restricted and actual events were not generated due to a change in Eventlog ID. This has now been fixed.
- OpManager: Events with the Eventlog ID set as '0' were not received. This issue has been fixed.
- OpManager: Without enabling the monitoring interval for 'Event Log', when trying to associate event log monitors to a device in OpManager from the 'Quick Configuration Wizard', 'Snapshot page' or 'Rule Engine', event log monitoring for those devices were not enabled automatically. This issue has been fixed.
- OpManager: If any new event log rule was associated to the device using 'Rule Engine', the event log monitoring interval for that device was set to 5 minutes by default. This has been fixed.
- OpManager: It was not possible to reset the uplink dependency for the device once it was set to some value, even after selecting the value as 'None'. This has been fixed.
- NetFlow : Added options to Create, Modify, and Delete SSID groups.

- NetFlow : In the Inventory, Snapshot reports have been added for SSID groups.
- NetFlow : SSID groups now support Capacity planning and Consolidated reports.
- NetFlow : An option to assign SSID Groups for Operator, and Guest users has been provided.
- OpUtils: For other language installation, iTextAsian.jar file has to be downloaded by the user. This download message has been enhanced and is displayed clearly in OpUtils's UI.
- OpUtils : Under Bandwidth Monitor in Inventory, the page was redirected to 'Add switch' page when Edit option of ifName is clicked. This issue is fixed now.
- OpUtils : Under Inventory, the "No records to view" message was not shown even when there is no data available. This issue is fixed now.
- OpUtils : Under Bandwidth Monitor in Inventory, when 'List Tools' icon is clicked the page is redirected to device snapshot page after the tools list is shown. This issue is fixed now.
- OpUtils : Added 'Tray' Icon for Windows installation to start, stop, and get status of OpUtils.
- OpUtils : Action class has been removed as it causes vulnerabilities in the product.
- OpUtils : The Horizontal menu in the UI is enhanced in such a way that an "Add Device" option is added to Inventory, IP address manager, switch port mapper, etc. when the mouse hovers over it.
- OpUtils : Under Settings, the "Maintain scan result of last 7 days" option of publish function didn't work properly. The issue is fixed now.
- OpUtils : Under Switch Snapshot page, the custom column's validation doesn't work when updating the boolean and integer data type. The issue is fixed now.
- OpManager : When functional expressions are applied to an SNMP monitor, the value of the monitor was duplicated with the other SNMP monitors. This issue has been fixed.
- OpManager : OpManager now supports Layer2 discovery for other devices apart from routers and switches. This can be configured by making an entry in the "layer2Discovery.properties".
- Firewall : New device log support - VarioSecure firewall.
- Firewall : Automatic Security Audit report generation for Check Point (R-80.10 and above) devices using API.
- Firewall : CLI based Policy analysis, Rule management and Compliance support for pfSense firewalls.
- Firewall : Added Line and Bar graph options for device and interface Live reports.
- Firewall : XML External Entity Injection(XXE) vulnerability raised in report-profiles import.
- Firewall : Cross Site Scripting Vulnerability raised in ManualDns-Mapping entry.
- Firewall : Support-Id: 4811677 : Raw Search returned no data, if the search period is more than a month.
- Firewall : Support ID 4909346: Fixed the Device Rule configuration failure issue, in HA mode of FortiGate with VDOM setup.
- Firewall : Support ID 4909346: Fixed the issue of showing password in plain text, in the Device Rule submit response.
- Firewall : Support ID 4919514: Fixed the issue of embed widget not working, in CCTV view.
- Firewall : Support ID 4927087: New column added to display Cisco ACE hex code in Raw search results page.
- Firewall : Support ID 4553065: Fixed Squid proxy server parsing issue.
- Firewall : Support ID 4934078, 4950793: Fixed the issue of wrong client IP assignment for Cisco VPN.
- Firewall : Fixed the issue of Scheduled Rule fetching failure for Check Point, due to CLI connection attempt.
- Firewall : Huawei device change management reports are loaded with full configuration instead of changes alone. Fixed the issue.
- Firewall : Added default exclude criteria for SonicWall devices to remove dynamic key updates as changes from Change Management Report. Fixed the issue.
- Firewall : Policy Overview Schedule list page displayed schedule details of all the devices. Fixed the issue to display the schedule details of only selected devices.
- Firewall : Was able to configure SNMP for Unmanaged devices. Fixed the issue.

- Firewall : No criteria is displayed for Policy Overview Scheduled reports when report specific criteria is provided. Fixed the issue.
- Firewall : For proxy devices Live Traffic is displayed in dashboard but not in Inventory page. Fixed the issue.
- Firewall : In Raw Search mail content PDF Report, Criteria value had extra details other than user configured criteria. Removed those unconfigured criteria and fixed the issue.
- Firewall : Exception thrown when Diagnose connections page is clicked in Settings tab. Fixed the issue.
- Firewall : In Settings, under User Management - Add/Edit User - Device list page, the deleted devices are also listed. Fixed the issue.
- Firewall : In Configuration Changes Mail Notification, Mail content has Disable link in the start of the mail. Moved the Disable link message to end of the Mail to fix the issue.
- Firewall : Fixed the issue of custom widget addition for Live Traffic without selecting a device, by ignoring the status message.
- Firewall : Fixed the issue of no redirection to reports page when the 'Unknown' user is clicked in Inventory > Users tab.
- Firewall : Added the missing 'Security settings' option in Admin server.
- Firewall : When device configuration fetching is in progress, other tabs cannot be accessed. This issue is fixed.
- Firewall : Due to pagination, in Rule Management page the 'Export to Excel' option was hidden. The issue is fixed to display the option.
- Firewall : In menu hover option, configured custom reports are displayed.
- Firewall : New help page links provided for Syslog server, Manual DNS and Security Audit report pages.
- Firewall : Minor UI issues are fixes.
- NetFlow : The currency list for billing feature is updated.
- NetFlow : Introduced an option to select multiple combinations of IP address for "From" and "To" in Between Sites IP Grouping.
- NetFlow : Bulk load option to upload multiple unmapped applications is introduced in Application Mapping.
- General : During API calls, there was an 'APIKey' exposure vulnerability. This issue has been fixed now.
- General : There was an issue with the timezone displayed in the graph of an embedded NFA widget. This has now been fixed.
- OpManager : Support for alarm variables as in Notification profile has been provided for 'Send email' task in Workflows.
- OpManager : Previously, there was a compatibility issue with EMC VNX File devices. It has been fixed now.
- OpManager : There were issues with adding a single RAID device under any Dell EqualLogic device. This has been fixed now.
- OpManager : Clickjacking vulnerability in Reports has been fixed now.
- OpManager : Previously, when OpManager was loaded with the 'Check URL' task in Workflows, the web client became unresponsive. This issue has been fixed now.
- OpManager : The create new report UI has been revamped.
- OpManager : The create new virtual server report has been revamped.
- OpManager : The schedule reports list view has been revamped.
- OpManager : The create schedule report UI has been revamped.
- OpManager : An empty schedule report page has been added.
- OpManager : The reports list UI has been revamped.
- OpManager : Create new reports, the monitor field displayed undefined values for certain vendors. This issue has been fixed.
- OpManager : In the OpManager mobile application, support has been added for alarms to be pushed as notifications based on the user's role.
- OpManager : Option to filter alarms based on the device and their severity level has been included in the mobile application.
- OpManager : Option to 'Acknowledge', 'Unacknowledge' or 'Clear' alarms has been provided based on the alarm.
- OpManager : Alarm Escalation feature has now been extended for URL Monitoring.
- OpManager : Custom Time Period option has been added for Alarm Suppression.

- OpManager: Usability issues in the Discovery page have been fixed.
- OpManager: There were a few usability issues in the Rule Engine page. This has now been fixed.
- OpManager : Previously, Devices are not listing properly in Packetloss/Response time global threshold page.This issue is fixed now.
- OpManager : Previously, Devices Availability Dashboard Report graph time format issue occurred when a period 7 days or 30days, was selected. This issue is fixed now.
- OpManager : The "Configure Interface" option provided for Firewall devices.
- OpManager : 'Disk' and 'RAM' details are now hidden in Switch and Router device summary.
- OpManager : Previously, there were issues with the associate credentials action. This has now been fixed.
- OpManager : In Maps page, the Device count was only shown in the Business View section. This issue has now been fixed.
- OpManager : In device snapshot page, Interface's real time graph was not shown if there were special characters in the interface name. This issue has now been fixed.
- OpManager : When rediscovering interfaces, rediscovery failed when the interface count exceeded 500. This issue has been fixed.
- OpManager: Previously, subInterfaces were not being rediscovered during Rediscovery process. This issue has been fixed.
- OpManager: While rediscovering interfaces, there was an issue with rediscovering interfaces of Fortinet devices. This has now been fixed.
- OpManager : In Device templates, there was a problem with 'StringtoNumeric' dials. This issue has been fixed.
- OpManager : The category of Eaton 9SX 5000 has been changed from Desktop to UPS.
- OpManager: Language localisation for several values and fields is now done for Spanish, German, Korean, France and Italian languages.
- OpManager: While adding monitors in the 'Monitoring' page under settings, an option has been provided to associate the monitors directly to device, without having to come back to Monitoring page again.
- OpManager: In the 'Monitoring' page under settings, a link has been provided for all monitors to view the respective devices linked to that specific monitor.
- OpManager: While adding URL Monitor, if 'Check URL' operation is performed, then it led to a vulnerability if user has given any concealed javascript code in the url address field. This issue has now been fixed.
- General : Pre-populated Database has been bundled with the Windows 64Bit build.
- OpManager : The 'Last Polled Value' and 'Last Polled Time' have been added in script monitors.
- OpManager : The custom script template webpage can now be accessed from the OpManager UI.
- OpManager : In the 'Test credential' page under device snapshot, the SSH key file update issue has now been fixed.

Build No - 123240 - December 24, 2018

- OpManager: The SQL injection vulnerability in 'getDeviceCompleteDetails' and 'getAssociatedCredentials' API's have been fixed.

Build No - 123239 - December 20, 2018

- General : There was an SQL injection vulnerability in the Alarms section. This issue has been fixed. (Refer: CVE-2018-20338)
- General : In Alarms, there was an XSS vulnerability in the Notes column. This issue has been fixed. (Refer: CVE-2018-20339)

Build No - 123238 - December 14, 2018

- OpManager: The SQL injection vulnerability in 'getGraphData' API has now been fixed. (Refer: CVE-2018-20173)
- Firewall: For Firewall Alarms, Alert details were not shown. Now the issue is fixed.

Build No - 123237 - December 6, 2018

- General: XSS vulnerability issue in domain controller has been fixed. (Refer: CVE-2018-19921)
- OpManager: In script templates, the XSS vulnerability in name and description field has now been fixed.

Build No - 123231 - November 29, 2018

- General: Apache's 'commons-beanutils' jar has been updated to version 1.9.3 due to 'Remote Code Execution' vulnerability in an older version. (Refer: CVE-2018-19403)
- General: Unauthenticated access to 'DataMigrationServlet' has been fixed. (Refer: CVE-2018-19403)
- General: The 'Browser Cookie theft' vulnerability has been fixed.
- General: XSS vulnerability in alarm escalation has been fixed.

Build No - 123230 - November 15, 2018

- NetFlow: The issue with NBAR application data in Wireless Controllers has been fixed.
- NetFlow: Missing I18N keys have been added for Chinese language.

Build No - 123229 - November 15, 2018

- General: Under Tools, The XSS vulnerability issue in getPing API has been fixed.
- General: Under Tools, The XSS vulnerability issue in getTraceRoute API has been fixed.
- General: Under Tools, The XSS vulnerability issue in saveSystemDetails API has been fixed.
- OpUtils: Under Config File Manager, the history of an IP was not properly displayed and it showed 'Undefined'. This issue is fixed now.
- OpUtils: Under Config File Manager, the upload config option did not enlist the device name that is selected. This issue is fixed now.

Build No - 123224 - November 14, 2018

- Firewall: XML External Entity Injection Vulnerability is fixed, while importing Custom Report/Alert profile.xml
- Firewall: Cross Site Scripting Vulnerability is fixed, while adding User defined DNS name.
- Firewall: Raw Search returned no data if search period is more than a month. This issue is fixed (Support-4811677)

Build No - 123223 - November 13, 2018

- NCM: Syslog Change Detection issue has been fixed.
- General: In the Inventory Snapshot page, there was a colour mismatch issue with the legend status color in the pie-chart. This issue has been fixed.
- General: The XSS vulnerability issue in updateWidget API has now been fixed. (Refer: CVE-2018-19288)

Build No - 123222 - November 2, 2018

- General: SQL injection vulnerability in Mail Server settings has been fixed. (Refer: CVE-2018-18949)
- General: Previously, there was an exception while processing clear cache requests. This has now been fixed.
- OpManager: While adding an email-notification profile, email fields were not being populated from the mail-server settings. This issue has now been fixed.

Build No - 123221 - October 31, 2018

- Oputils: Under Inventory, details were not properly displayed under sub filters, in the left side of the page.This issue is fixed now.
- OpUtils: Under IP Address Manager in Inventory, the IP -> DNS column data was not displayed. This issue is fixed now.

Build No - 123220 - October 30, 2018

- OpManager: Issue in SNMP Test credential has been fixed.

Build No - 123219 - October 25, 2018

- OpManager: When importing a URL using CSV action/API, the header information from the CSV file was reflected to the user. This lead to a vulnerability of concealed Javascript code being executed. This issue has now been fixed.
- OpManager: Previously, there were issues in saving email addresses in the notification profile because of newly added security restrictions. They have now been fixed.
- OpManager: The XSS vulnerability issue in addNewAdditionalField API has been fixed.

Build No - 123218 - October 19, 2018

- Firewall: New Log Format Supported - **Barracuda Email Security Gateway**
- Firewall: Policy/Rule analysis, compliance report support and fetching configuration using firewall vendor API
    - Check Point devices
- Firewall: Policy/Rule analysis, compliance report support and fetching configuration using CLI
    - Vyatta firewalls
    - Huawei firewalls
- Firewall: Added 'Tray' Icon for Windows installation to start, stop, and get status of Firewall Analyzer.
- Firewall: Changed 'Support' tab look and feel.
- Firewall: New reports 'Active VPN Users' and 'VPN User Session Details' added under VPN reports.
- Firewall: Quick links and Help cards provided for Discovery and Search reports.
- Firewall: Selected 'Time Period' retained in all drill down snapshot reports, after zooming the time in live traffic widget.
- Firewall: Enterprise Edition data exchange between Admin and Collector servers made secure for each requests and response.
- Firewall: Firewall Analyzer startup time optimized; Made the internal modules to start in parallel.
- Firewall: 'Raw Settings' page moved to 'Search' tab from 'Settings' page to avoid shuffling between tabs.
- Firewall: (Support ID: 4795348) Change Management report for SonicWALL displays user names, who do not have access to firewall configuration. Fixed the issue.
- Firewall: Cisco-Meraki log parsing issue fixed.
- Firewall: Log parsing of Sophos and Cyberoam devices tuned to handle more log rate.
- Firewall: Occasionally, 'Raw Tables' are not split properly, when log rate is high. Fixed the issue.
- Firewall: In 'Rules Report' page, if the number of rows is less than 10, the CSV, Excel export option is missing. Fixed the issue.
- Firewall: SNMP settings page is not closed automatically on successful configuration from 'Inventory' snapshot and list page.
- Firewall: Fixed the issue of removing unnecessary API calls when criteria based 'Search' reports is loaded.
- Firewall: Fixed the issue of table border misalignment for all the report table grids.
- Firewall: Fixed the issue of headers for PaloAlto and NetScreen devices in 'Policy Overview' report by changing the 'Source

Interface' & 'Destination Interface' headers to 'Source Zone' & 'Destination Zone'.

- Firewall: When 'Only on Week Days' option is selected in 'Daily-Schedule', it was not working. This issue is fixed.
- Firewall: 'Policy Overview' tab name changed.
- Firewall: 'Unused Rule' header name changed.
- Firewall: In 'Remote Host' option of 'Import Logs' page, the selected file is not getting marked. This issue is fixed.
- Firewall: Fixed the issue of device name display in 'Live Traffic' widget even after the device is unselected.
- Firewall: Fixed the issue of unrestricted 'Save' in 'Live Traffic' widget, if no device is selected.
- Firewall: Fixed the issue of 'Icon' only option for horizontal menu change is not working in Central-Server.
- Firewall: Fixed the issue of empty 'Standards' page, when the status of all firewall devices is 'UnManaged'.
- Firewall: When 'Intranet Settings' is saved without any criteria, instead of alert message, it is getting saved. Fixed the issue to show alert message.
- Firewall: In the 'Inventory - Device' detail widget, page redirection happens only when text is clicked. Fixed the issue for page redirection when clicked anywhere in the device row.
- Firewall: Fixed the issue of missing 'On Demand' column header in 'Device Rule' settings page.
- Firewall: Fixed the issue of missing tool tips for few icons.
- Firewall: For Windows firewall, UDP port unblock rules added for Syslogs packets.
- Firewall: For Windows firewall, TCP port unblock rules added for Telnet and SSH.
- NCM: Configlet execution results of multiple devices can now be exported as PDF in bulk.

Build No - 123217 - October 17, 2018

- General: TCP / UDP port unblock rules for NetFlow packets / Syslogs packets have now been added in Windows Firewall.
- NCM: Upload request option which was previously in settings tab, can now be easily accessed from the "Change Management" tab in the main menu.
- NCM: While exporting configurations, you can now give the folder name in both text and numeric formats.
- NCM: The start date issue of the daily schedule feature has been fixed.
- NCM: Form validations throughout NCM have been revamped.
- NCM: Issue while swapping configuration versions in the Config Diff view has been fixed.
- NCM: The TFTP service had an issue when the central and probe were installed on the same machine, this has been fixed now.
- NCM: SysOID finder's timeout issue has been fixed.
- NetFlow: Export Flow option has been added for NetFlow, and Flows can now be exported from the GUI.
- NetFlow: How-To's and FAQ's have been added for Settings and Report pages.
- NetFlow: An option has been added to view the Menu tab horizontally with mouseover links.
- NetFlow: Added summary pages for Reports and Settings to list all menus in a single page.
- NetFlow: WLC widgets now support Access Point and Access Point groups resource types.

Build No - 123216 - October 15, 2018

- General: After the upgrade, the web client failed to load successfully, because the REST API tables were not properly populated. This issue has been fixed.
- General: In Submit Query, an option has been provided to export the query as a CSV file.
- General: Port dependencies for unused ports (NMS_FE_SECONDARY_PORT, PORT_TO_LISTEN) have been removed.
- OpManager: '&' character is now supported in Notification Profile email addresses.
- OpManager: In the Dashboard, Google/Zoho maps did not load properly in the widget. This issue has been fixed.

Build No - 123215 - October 12, 2018

- OpUtils: A 'Getting Started' page has been added to guide the users with a step-by-step procedure for using OpUtils.
- OpUtils: Added an option to switch menu bar from vertical alignment to horizontal alignment and vice versa.
- OpUtils: Under Reports option, the 'Connected IP Details' report which provides details about the ports connected to the corresponding switches, and IP addresses has been added.
- OpUtils: IPAM now supports IPv6.
- OpUtils: Under settings, the 'Add Device' in MAC-to-IP mapping is enhanced such that it supports import option for SNMPv3 now.
- OpUtils: Under settings, the 'Add Device' in MAC-to-IP mapping is enhanced such that it supports CLI settings(available only for switches and routers) now.
- OpUtils: Under Inventory, the snapshot page of SPM, IPAM, Config management and Bandwidth Monitor is enhanced such that it provides quick links like 'How-to', 'faq's', etc now.
- OpUtils: Previously, the MIB browser tool didn't respond to the SNMP version 2 credentials. The issue is fixed now.
- OpUtils: Previously, there were issues in restoring backed up database if the custom columns are created. The issue is fixed now.

Build No - 123214 - October 10, 2018

- OpManager: Previously, data collection in UCS devices stopped due to an expiration in the login session. This has now been fixed.
- OpManager: In Dashboard, widgets that included real-time data now have an image mode option for rendering graphs.
- OpManager: Previously, there was no option to include SNMP v3 credentials in the credentials list for vCenter/ESX discovery. This has been included now.
- OpManager: For vCenter discovery, if two or more datastores were found with identical path names and characters (with same or different letter case), the entire discovery process failed. This has been fixed now.
- OpManager: When no credentials were passed for a VM during VMware discovery, the vendor was updated as 'Unknown'. This has been fixed now, and the vendor will be updated as 'VMware' if no credentials are passed during discovery.
- OpManager: For HyperV VMs, it was not possible to add VIWMI monitors if the device type was Linux. This has been fixed now.
- OpManager: The XSS vulnerability issue in addCategory API has now been fixed. (Refer: CVE-2018-18262)
- OpManager: There was an unrestricted file upload vulnerability while uploading a background image in Business view. This has now been fixed. (Refer: CVE-2018-18475)
- OpManager: The XML External Entity (XXE) vulnerability in maps module has been fixed.(Reported by jacky.xing@dbappsecurity.com.cn) (Refer: CVE-2018-18980)
- OpManager: There was a resizing issue with the BusinessView Map, in both the Map View page as well as the dashboard widget. This has now been fixed.
- OpManager: If a router was being monitored with flow monitoring and hardware monitoring enabled, some users had trouble accessing the device's snapshot page from Inventory. This issue has been fixed now.
- NCM: Information regarding the usage of SysOID in the UI has been added.
- NCM: An option to view the password for all password fields in NCM has been added.
- NCM: The grid row size selection is retained based on the user.

Build No - 123208 - October 8, 2018

- OpManager: In the Heatmap widget, the option to filter devices based on severity was not working. This has now been fixed.
- OpManager: The registration process for Probe-Central was not successful, causing a communication failure in Linux systems. This issue has been fixed.
- Firewall: Menu hover feature helps to access all sub tab options without the hassle of navigation.
- General: After updating to build 123181, there was a password mismatch issue for customers using the same password for 'OpManager.truststore' and 'server keystore' prior to the upgrade. This issue has now been handled.

Build No - 123207 - October 1, 2018

- OpManager : OpManager now provides the option of configuring multiple threshold severities for interfaces - Attention, Trouble and Critical.
- NCM: Now get faster fixes to your issues using self-support in the ﷺ section of NCM.

Build No - 123206 - September 27, 2018

- OpManager : You can now directly access specific pages in OpManager without the hassle of navigating through multiple options by using the Hover Menu.

Build No - 123205 - September 19, 2018

- General : Previously, a blank screen showing "Loading" was displayed while trying to access a default dashboard which was deleted in an older version of OpManager. This has now been fixed.
- General : Users can now embed CCTVs using the shareable link generated from the NOC view menu.
- General : SQL Injection vulnerability in Global Search has been fixed.
- General: Users with restricted access to devices were able to create another user account with unrestricted access to all devices. This issue has been fixed.
- General : The product web-client now supports Russian and Chinese(Taiwan) languages.
- General : OpManager will now only support IE versions 10 and above.
- OpManager : The Install Shield Wizard now supports Japanese and Chinese languages.
- OpManager : In the NFA/NCM Dashboard, there was a widget overlapping issue while switching between Probes. This issue has been fixed.
- OpManager : Previously, Central did not properly load the Probe data in the NFA/NCM Dashboard. This issue has now been fixed.

Build No - 123204 - September 17, 2018

- OpManager: Module Activation option has been provided for Storage Monitoring.
- OpManager: Template operations like 'Edit', 'Delete' and 'Copy' has been restricted for Storage devices.
- OpManager: XSS vulnerability issue in Storage Credentials has been fixed.
- OpManager: Support has been provided for wildcards in workflow actions. E.g. delete *.log or *.txt files, etc.
- OpManager: Changes have been made in Storage Monitoring to make it GDPR compliant.

- OpManager: Help links (How-to) has been added for Storage Monitoring.

Build No - 123198 - September 13, 2018

- OpManager : Option has now been added to save Layer2 maps as Business view.
- OpManager : Unauthenticated folder and file access has been restricted and the related vulnerability has been fixed.
- OpManager : A drop down box to change the device icon size has been added in Business views.
- OpManager : SQL injection vulnerability in setManaged API has been fixed.
- OpManager : In embed widget option, the images were not loading for the operator user. This issue has been fixed.
- OpManager : In businessview, the user was unable to edit the shortcut name. This issue has now been fixed.
- OpManager : In businessview, while performing the 'copy as' operation, some of the shortcuts went missing. This issue has been fixed.
- OpManager : In Maps page, there was an issue with the Businessview severity tooltip. This has now been fixed.
- OpManager : In addition to the existing monitors, more than 1000 new monitors have been added to OpManager. Now you can monitor more metrics and also monitor the metrics of various vendors.
- OpManager : Discover and auto-classify an even wider range of devices in OpManager with over 4000 newly added device templates.
- OpManager : Previously, adding more than two links between devices in a Business view caused the links to overlap. This issue has been fixed.
- OpManager : New line types have been introduced for links in Business views. Also, an option to manipulate the curved links for interface connections in Business view has been added.
- OpManager : When rediscovering a device after updating the pingable IP address in Device snapshot page, a duplicate device will be added. This issue has been fixed.
- OpManager : Previously, under 'Network' overview in the Dashboard, there was a mismatch in the Alarm count. This issue has been fixed.
- OpManager : Previously, there was a UI issue in the alert box displayed when closing a Business view without saving it. This has now been fixed.
- OpManager : 'Ping' option has been added to the 'Add Device' page. Users can now ping the device before device addition.
- OpManager : Now, an alert message is shown in the 'Inventory list' page when only a single device is listed. This helps the User redirect to the 'Discovery' page to add more devices.
- OpManager : Users can now view the total number of interfaces and down status for interfaces in the device snapshot page.
- OpManager : The usability of listing credentials in the 'Add Device' page has now been enhanced.
- OpManager : 'Add Device to IPAM' and 'Add Device to NCM' options have been moved to the settings tab in the 'Add Device' page.
- OpManager : In 'Add Device' page, if only the default credentials are available, an alert message is shown requesting the User to add their own credentials.
- OpManager: Tips have been provided when there is a device discovery failure to troubleshoot issues.
- OpManager: Device Type & Category has been included as part of Device Summary.
- OpManager: The Device Notes and Additional Fields, have been renamed as Custom Field across the platform/webclient.
- OpManager: The 'Rediscover Device' icon has been changed in the Device Snapshot page.
- OpManager: The 'Configure Interfaces' icon has been changed in the Interfaces Summary widget.

Build No - 123197 - September 10, 2018

- Firewall: F5 Firewall device support added.
- Firewall: Horizontal menu bar made as default.
- Firewall: 'Add-Device' menu added to export Syslogs from firewalls.
- Firewall: SSH or Telnet based 'CLI terminal' to access firewalls from Firewall Analyzer.
- Firewall: 'Getting Started GUI' to guide the user to add devices and reports.
- Firewall: 'Quick links' and 'Help cards' for settings and report pages.
- Firewall: For trial and registered users, 'Live Chat' facility to contact sales-engineering team.
- Firewall: Introduced 'Password Policy' configuration for user management.
- Firewall: Login page customization for rebranding custom images.
- Firewall: In all report pages, optimized alignment of widgets.
- Firewall: Firewall Analyzer users can set their default menu bar (horizontal or vertical) using 'Menu Bar' menu.
- Firewall: Fixed the issue of failure to fetch the device rule for Fortigate Vdom, because 'Pager' command was not working.
- Firewall: Fixed the issue of failure to display of rule management reports for Vdom firewalls.
- Firewall: 'Select Policy' menu not working properly in Firefox browser. Fixed the issue.
- Firewall: Fixed the drill down issue in 'Dashboard - Security - Top N Attacks by Hits'.
- Firewall: Single device and all devices selection not working in 'Short summary' page of 'Inventory' device lists. Fixed the issue.
- Firewall: If the widget subtitle contains 'drill down link' - we need to provide the drill down/redirect to inventory action, when we click the link alone
- Firewall: In the 'Inventory - Short summary' page, 'Create Report/Alert Profile' tabs missing, navigating after add or edit from the 'Intranet, Exclude Host, Availability Alert' pages. Fixed the issue.
- Firewall: Minor UI enhancements in 'Inventory' page.
- Firewall: In the Firewall Analyzer - Distributed Edition - Admin Server, when a firewall was deleted, there was no processing message shown. Fixed the issue to show firewall delete processing message.
- Firewall: 'Delete widget' was not working in the 'Reports - Standard Report' page. Fixed the issue.
- Firewall: In the 'Inventory - Devices - Protocols' page, 'Protocol identifier' options were missing. Fixed the issue.
- Firewall: In the 'Active VPN Trend Report' page, Y-axis values were not displayed properly & was throwing NullPointerException while drill-down. Fixed these issues.
- Firewall: In the 'Device Rule, Exclude Criteria, Protocol Groups, Device Groups, Intranet Settings, Cloud-Repository, Exclude Hosts, SNMP settings, Alarm Profiles and User-IP Mapping (DHCP, AD/Proxy, Manual Mapping)' pages, to edit an entry you have to click on it. Now a proper 'Edit' icon is provided for each entry.

Build No - 123196 - September 07, 2018

- General: The 'oputilsServlet' which was previously unauthenticated has now been removed (Reported by jacky.xing@dbappsecurity.com.cn).
- OpUtils: Previously, there was an issue in sending alert mails from IP address manager. The issue has been fixed now.

Build No - 123195 - September 06, 2018

- OpManager: Previously, the Remote desktop was possible only from old IE Versions. Now, Remote Desktop connection for windows can be accessed irrespective of the browser type i.e. Chrome/ Firefox/ IE.
- OpManager: Previously, 'Active Process' and 'Installed Software Details' was fetched only if WMI or SNMP credentials were passed. Now, It can also be fetched using CLI.
- OpManager: Previously, in Hardware Monitoring, options like Enable Hardware Monitoring, Suppress Hardware Alarm, Modify Monitoring Interval options were available only at the Global level i.e. applicable to either all or none of the devices. Now users

can configure/update those options at each device level from the Hardware Monitor Tab inside the Device Snapshot page.

- OpManager: Now, the Hard Disk and RAM value will be updated using WMI, if WMI credentials are passed. Earlier, it was updated only using SNMP.
- OpManager: A new Recent Alarms specific widget has been included in the Hardware monitor tab of the Device Snapshot page to provide visibility into recent hardware alarms for that specific device.
- OpManager: Now, the 'Sensor Specific Graphs' widget inside the Hardware monitor tab has been grouped into widgets of specific sensor types for better visibility into sensor-specific data. It is provided as a separate Tab inside device snapshot page.
- OpManager: If RAM or HD value is greater than 1024 MB, then the value will be shown in terms of GB and further into TB along with the units for easy readability.
- OpManager: Notification Profile was not triggered when it was configured with 'Select All' option in criteria for IPSLA. This issue has now been fixed.
- OpManager: The option to enable/disable Traceroute from IPSLA Monitor snapshot page has been included now.
- OpManager: Path Details of the IPSLA Monitor was missing in the Alarm Message, for IPSLA specific alarms. This issue has been resolved now and the Path details have been appended to the IPSLA Monitor Name.
- OpManager: In the IPSLA Monitor snapshot page, all the alarms from the OpManager were shown under Alarms Tab. This has now been fixed and only the alarms specific to that particular IPSLA Monitor will be shown.
- OpManager: For IPSLA Monitor, inside snapshot page, Packet Loss history was shown for Source to Destination packets. This has been corrected and currently, the Destination To Source specific history will be shown.
- OpManager: Option to include IPSLA Monitor path details as Subject in Notification Mail has been included now.
- OpManager: The attempt to add IPSLA Monitor failed when a device returned invalid values such as 'NO SAA'. This has been fixed now.
- OpManager: For Hop By Hop View specific Graphs in widgets, the time frame value for which the data is shown has been provided.
- OpManager: Polling Interval value(in seconds) will be shown inside the summary details widget of IPSLA Monitor snapshot page.
- OpManager: In some cases, whenever OpManager service was restarted, false alerts were generated for all the https URLs. This issue has been fixed now.
- OpManager: If the configured dependency parent device was down for any device, then unnecessary alerts were raised in related to URL down for all URL's configured under the device. This issue has now been fixed.
- OpManager: The Edit operation for Threshold was not getting saved for URL Monitors and MSSQL Monitors when the edit was tried from the Alarm page after selecting the specific URL Monitor alarm or MSSQL Monitor. This issue has now been fixed.
- OpManager: Event logs with event code as '0' were not handled and ignored. This has been fixed now and such event logs will be received.
- OpManager: Users were able to associate Event Log rules to device from the snapshot page even without enabling event log monitoring. This has now been fixed.
- OpManager: Validation for Start and End Time fields was improper for 'Run Archive' option in the client. This issue has now been fixed.
- OpManager: Monitors were added as String Monitors by default while being added from Settings in the Performance Monitors page when the OID was manually copy-pasted into the OID field. This issue has now been fixed and it will be added as a Numeric type Monitor.
- OpManager: If there were no VM's inside the HyperV Server then it was leading to HyperV Discovery failure. This issue has now been fixed.
- OpManager: If the process names fetched from the device had a space character in any specific Process Name, while using CLI for adding Process Monitors, the Process Name was not getting added to the device. This issue has now been fixed.
- OpManager: In the Central installation set up, the polling for HyperV monitors leads to invalid credentials failed alerts. This issue has now been fixed.
- OpManager: If any of the VM's inside the HyperV Server contained more than 10 CPU instances, it was leading to HyperV

discovery failure. This has now been fixed.

- OpManager: If any of the selected credentials(SNMP/WMI/CLI) for VM's during VMware discovery had space characters in its name, it ignored all the selected credentials for the discovery of VMs. This issue has now been fixed.

Build No - 123194 - September 03, 2018

- OpManager: Recent Alarms are now displayed in the Device Snapshot page.
- OpManager: Alarm Suppression status is now displayed in the Device Snapshot page.
- OpManager: The user interface for reports has been improved and enhanced. The related issues have also been fixed.
- OpManager: OpManager now extends customization options to the login page. You can now choose to show/hide the copyrights and also change the background to an image of your choice.
- OpManager: Count of managed devices and interfaces will be displayed in the Probe details page.
- OpManager: In the 'Probe Details' page, edit option can be viewed by clicking on the probe name.
- OpManager: Alarm count has now been fixed in the Dashboard.
- OpManager: Device and alarm count of 'Site snapshot' widget in the Dashboard has been fixed.
- OpManager: Option to delete the probe has been moved inside the 'Edit probe details' page.
- OpManager: Previously, there were issues when probe details were edited after sorting. This has now been fixed.
- OpManager: Linux auto upgrade has been fixed.
- OpManager: Smart upgrade previously failed for directory names with spaces. This issue has been fixed now.
- OpManager: Smart upgrade previously failed when Central server was running in HTTPS and Probe was running in Command Prompt. This has been fixed now.
- OpManager: While fetching 'deviceName' instead of 'ipaddress', trap was not received for a few devices. This issue can be fixed.
- OpManager: When deleting a device from probe, the related alarms were not deleted in Central. This issue has been fixed.
- OpManager: Previously, for traps with failure component not ending with "_trap", the related notification profile was not triggered. This issue has been fixed.
- OpManager: 'OpManagerTrapNotification' trap is now implemented in OPMANAGER-MIB.
- OpManager: In 'TopoDBSpecialKey' table, 'category' is empty when the default interface entry is missed. This issue has been fixed.
- OpManager: In alarm details page, 'matched rule name' has been included for Trap / EventLog / Syslog

Build No - 123193 - August 29, 2018

- NetFlow: Added options to Create, Modify, Delete access point groups.
- NetFlow: Snapshot reports in Inventory have been added for access point groups.
- NetFlow: Tooltip information added in the Settings page.
- NetFlow: In the dashboard, Inventory list, Inventory snapshot, Heat maps and license pages, the Interface status color code mismatch has been fixed and the status names have been changed.
- NetFlow: The 95th percentile line has been added to the Traffic graphs in the Snapshot page, Reports and exported PDF.
- NetFlow: The issue with enabling polling for NBAR configuration, when the first interface is disabled, has been fixed.

Build No - 123192 - August 27, 2018

- OpManager : Interface graphs can now scale automatically to Mbps and Gbps based on the data in XLS report.
- OpManager : Under 'Devices in Business view' widget, the 'Device name' column disappears while sorting the widget. This issue

has been fixed.

- OpManager : SNMP Write community is now optional while adding SNMP v1/v2 credential. Retype password for SNMP v1/v2 has also been removed.
- OpManager : URL monitor and Service monitor options have been removed from the Switch and Router snapshot page.
- OpManager : Previously, Device template search results kept shuffling when any template from the result was edited or modified. This issue has been fixed.
- OpManager : Previously, Operator users were not able to edit the 'Availability outage reason'. This issue has been fixed.
- OpManager : Users can be able to view and hide the password while adding credentials.
- OpManager : Previously, there was an issue with rediscovering interfaces when the 'IFDESCRIPTION' was 'NULL'. This issue has been fixed.
- OpManager : Previously, there was an issue while associating device templates with devices. This has now been fixed.
- OpManager : While editing 'Map' widget, users can now choose between Google Maps or Zoho Maps.
- OpManager : Previously, option to change the position of the device label was missing in Business view. This issue has been fixed.
- General: OpManager/NetFlow now integrates with Zoho Maps and devices can be placed on the map according to the geographic distribution.

Build No - 123191 - August 22, 2018

- NCM: Comparing any two configuration files from anywhere within NCM is now through the 'diff view' page.
- NCM: The diff view page is now enhanced to show details like 'Annotation', 'Last Modified By' and 'Timestamp of configuration backup'
- NCM: Now, you can access 'select' boxes in the UI using focus, and also toggle them directly with the keyboard.
- NCM: While setting email for any notification/schedule in NCM, if the mail server settings is not pre-configured, a warning message will be displayed.
- NCM: Now, NCM supports 700 new models and we have updated the series and model data for a few existing devices.
- OpManager: The issue of Close icon not being shown in alarm details page has been fixed

Build No - 123190 - August 21, 2018

- General: PushNotification - Information about ManageEngine events will be published only for the selected countries.
- General: Password policies have been implemented as a fix for 'Brute Force Attack' vulnerability.
- General: In add/edit user page, 'Username' field has been added and the 'Email-id' field has been made mandatory.
- General: Now, resetting the Admin password can be done using 'ResetPassword' script. The previously used 'ChangePassword' API has been removed.
- General: Previously, in SMS settings, SMPP password was displayed as plain text. This has now been fixed.
- General : Previously, SMS notifications were not received via SMPP. This issue has now been fixed.
- General : Previously, SMS notifications via Serial modem was not working after upgrading OpManager to 123090. This issue has been fixed.
- General: Opt in 'Breach notification' support has been added to provide instant alerts along with relevant fixes when a data breach is detected.
- General: Cross site Scripting(XSS) vulnerability in login page has been fixed.
- General: Previously, in certain Linux machines, when embed widget link was generated, the URL contained "localhost" instead of the server name. This issue has now been fixed.
- OpManager: Previously, in SSH discovery, it was not possible to determine the device type from the welcome message after login. This issue has been fixed.

- OpManager: Terminal has been updated to open for all SSH monitoring machines. In case of NCM devices, NCM credential will be used; else OpManager's CLI credential will be used.
- OpManager: Proper Encoding on sending syslog from Notification Profile has added.
- OpManager: In the 'Time window' page under Notification Profile, there were issues with overnight scheduling. This has been fixed.
- OpManager: After the upgrade, certain users were experiencing issues with the Add user functionality. This issue has now been fixed.

Build No - 123189 - August 17, 2018

- OpManager: You can now export a PDF with the chart option of your choice.
- OpManager: 'Report Builder' reports can now be saved with the chart option of your choice.
- OpManager: Support has been added to schedule reports with the selected chart option.
- OpManager: Under 'Report Builder', MultipleNode monitors now have the respective instance/drives name with the deviceName in the legend.
- OpManager: Previously, there was an issue with creating Reports by selecting performance monitors. This has now been fixed.
- OpManager: While selecting 'table' view format in report builder, data was not being displayed. This issue has been fixed.
- OpManager: When exporting 'snapshot performance monitor' graph, the 'table' view overlapped with the graph. This has now been fixed.
- OpManager: In PDFs' exported from interface report builder, some data was not displayed on the right side of the PDF. This has now been fixed.
- OpManager: In 'Reports', it was not possible to create and choose a custom time window. This issue has been fixed.
- OpManager: 'At a glance' report displayed a few keys in the graph when it was scheduled (I18N Issue). This issue has now been fixed.
- OpManager: 'Process monitor snapshot' report displayed a key in the graph when the report was scheduled (I18N Issue). This has been fixed.
- OpManager: Previously, it was not possible to create a device report for custom time period. This issue has now been fixed.
- OpManager: Users were not able to view the full custom period in exported PDF's. This issue has been fixed.
- OpManager: Previously, workflow was not triggered on threshold violation. This issue has been fixed.
- OpManager: Threshold monitors listed in the workflow was vague. Display name has also been added for clarity.
- OpManager: In Workflow, the traps criteria was not working properly. This has now been fixed.
- OpManager: When a special character is used in the 'Report Name', the report was not being sent as an email while scheduling it. This issue has been fixed.
- OpManager: Facile support for SDP SSL Third party certificate & PFX certificate has now been added.
- OpManager: Standalone to Probe Migration Support for Storage Monitoring.

Build No - 123188 - August 13, 2018

- OpManager: Option to Add Custom WMI Monitor under Performance Monitor from Settings Page has been provided now, which can be later on associated to any template or device directly.
- OpManager: While configuring Notification Profile for the device, the user can now configure or append the Performance, AD, MSSQL, Exchange Monitor specific data like Monitor Name, Instance, and Protocol to a Subject and Message field of the Notification.
- OpManager: If Event Log Monitors are received in huge numbers from any device then it leads to delay and slow downs the data collection of event log monitors. Now it has been improved.
- OpManager: Hyper-V discovery was getting failed if duplication or change in DNS name of the server was found during

discovery. This has been fixed now.

- OpManager: RAM usage values were not shown if the user selected the custom time period. This has been fixed now.
- OpManager: Due to the similarity in the sensor name with Multiple Instances, the Hardware monitoring specific alerts were being cleared inaccurately. This has been fixed now.
- OpManager: If the custom Monitors has the space character in the name field given by the user, then after adding it to the device, while trying to redirect to Graph page from Monitors list, it was getting redirected to device snapshot page. This has been fixed now.
- OpManager: Users can now enable/disable "Dynamic IP Address" option under System Settings.
- OpManager: Previously, data collection by CLI monitors failed when both the SNMP and CLI credential were passed via Network Discovery. This has now been fixed.
- OpManager: Previously, the 'Unique System DisplayName' criteria failed when we had multiple discovery profiles. This issue has now been fixed.

Build No - 123186 - October 10, 2018

- General : SQL Injection vulnerability in Global Search has been fixed.

Build No - 123185 - September 11, 2018

- General: SQL injection vulnerabilities in unauthenticated servlets has been fixed.
- OpUtils: Previously, there was an issue in sending alert mails from IP address manager. The issue has been fixed now.

Build No - 123184 - August 23, 2018

- OpManager: Close icon not shown in alarm details page issue has been fixed.

Build No - 123183 - August 7, 2018

- NetFlow: New widgets for Top N Device by Speed (as table, line graph, pie chart), has been added.
- NetFlow: The issue with Interface Traffic Graph in Custom Schedule Report has been fixed.
- NetFlow: SQL injection vulnerabilities in java APIs has been fixed.
- NetFlow: In End User tab, user data was vulnerable to XSS. This issue has been fixed.
- OpManager: The issue with Application Growth report has now been fixed.
- OpManager: The issue with the interface count mismatch in Dashboard has been fixed.

Build No - 123182 - August 2, 2018

- General : The issue of client loading failure in IE and Firefox older version has been fixed now.
- OpUtils: The Config File Manager tool, which helps to download/upload the StartUp and/or the Running config files of Cisco devices and also helps to compare different versions, has been brought back under inventory.
- OpUtils: The Config File Manager tool is enhanced with the capability of scheduling to take a backup of the config files from the

Cisco devices at the specified interval.

- OpUtils: Audit Information for Add/Edit/Delete User Operations for IPAM, SPM & Rogue has been included.
- Firewall: When exporting Alarm Profile, the xml file didn't contain other user created alarm profiles. Now this issues is fixed to show all profiles.
- Firewall: While importing syslog, the IP address of the device was updated with link local ip. Now the device will be added with local ip.
- Firewall: Device-rule configured firewall is listed as first resource in drop-down of configuration related Reports.
- Firewall: In policy overview page, drill-down on some of the services showed no data. This issue is now fixed
- Firewall: When we change credential profile while editing DeviceRule, it created another entry for the device. This issue is fixed.
- Firewall: SMS Setting was showing as 'Not Configured' when SMPP or SMS Gateway was configured already. This issue is fixed.
- Firewall: Unknown protocol drill-down report was showing sent and received as KB. But in actual, they are in bytes. The header is changed appropriately.
- Firewall: While editing the "Report-Profile" page, "Run on Week Days" was not selected. This issues is fixed now.
- Firewall: When a schedule was created for search report, it added as nullschedule. This issue is fixed now.
- Firewall: We were not showing executed report profiles details under "Device Detail" page. now the issue is fixed.
- Firewall: Sorting was not working in Raw search result page. It is fixed now.
- Firewall: While configuring Working-hour, range like (8-12,15-18,19,20,21) was not allowed. Now the issue is fixed.
- Firewall: Assigning Credential Profile without selecting a profile didn't throw any error. This is fixed.
- Firewall: Not able to do raw search if only 'Traffic Log' was selected. It is fixed.
- Firewall: Page seems to refresh and go to different device after clicking "Save" in edit settings page of standards page. This is fixed
- Firewall: In Inventory snapshot page device edit slide comes over user settings page.This issues is now fixed.
- Firewall: 'All device' option for operator in Snapshot page has been removed.
- Firewall: Auto refresh will be done if any action is performed in collector list page.
- Firewall: Username search is not working in users list page under inventory. This issue is fixed
- Firewall: Icon-title is not shown properly on hover in alarms page. Now the title is shown properly.
- Firewall: Free-license text is removed from the DE Alert image
- Firewall: Support page icon was not working for Operator user. Now it is working

Build No - 123181 - August 1, 2018

- OpManager : Hardware Monitoring Support for Cisco Nexus and Checkpoint Firewall has been provided now.
- OpManager: Admin users can now enable or disable HTTPS under settings. SSL certificates (cer, crt, der, truststore, keystore, PFX) can be uploaded, verified and imported into OpManager to run in HTTPS mode.
- OpManager: Certificates of external services can now be added to the truststore by uploading them (in cer, crt, der, truststore, keystore, PFX formats) or can be fetched directly from the service's URL.

Build No - 123180 - July 30, 2018

- OpManager now supports ManageEngine's AlarmsOne integration.

Build No - 123179 - July 24, 2018

- General: Previously, the upgradation to build 123158 and above caused network interruptions in Windows 7 & 2008 R2. The

issue is fixed now.

Build No - 123178 - July 24, 2018

- General : HSTS header has been introduced as an option that can be enabled to prevent SSL stripping.
- General : Unauthenticated Folder and File Access has been restricted and the vulnerability has been fixed.
- OpManager : In Notification Profile, if the device misses one poll and "notify when the alarm is cleared" criteria is selected, the 'clear alarm' alert that comes after trouble alarm (Attention-Trouble-Clear[THREE-POLL_CLEAR]) was not notified to user. This usability issue has been fixed now.
- OpManager : In Reports, for 'Notification Profiles Triggered' report, the message column displayed junk characters for a few MSSQL setups. This issue has been fixed now.
- OpManager : Users can now enable/disable OpManager Monitoring from within the UI.
- OpManager : We have done a minor change at the license level to differentiate OpManager & OpManagerPlus licenses. Hence, we recommend our OpManager Plus customers to upgrade to build number 123178 before applying any new licenses

Build No - 123177 - July 20, 2018

- Firewall: Added SSH protocol to fetch WatchGuard firewall configuration.
- Firewall: Local File Inclusion vulnerability is fixed.
- Firewall: SNMP based Live Report of PaloAlto devices was not working properly. This issue is fixed.
- Firewall: In Anomaly alert criteria page, a help message 'CIDR and CSV formats are allowed' has been added to Source and Destination fields..
- Firewall: When Report Profiles are created, removed unnecessary API call to improve UI performance.
- Firewall: In Cloud Services page of Inventory, 'Add repository' option is provided.
- Firewall: Device drill down from Policy Optimization page of Dashboard was not working. The issues is fixed and redirected to Optimization page.
- Firewall: In Firewall Live Traffic widget of Inventory page, when 'Gbps' is selected as unit, the values shown were not accurate. The issue is fixed to plot the graph with granular values.
- Firewall: Alarm Profile notification option 'Run As Script' didn't accept arguments. The issue is fixed.
- Firewall: In Import Log page, Local Schedule option was not shown even when the client can be accessed from localhost. This issue is fixed now.
- Firewall: In Fortigate syslog, VPN close log has duplicate entry which led to incorrect data. Handled it to fix the issue.
- Firewall: Traffic Trend Report graph was not plotted in order. This issue is fixed.
- Firewall: Syslog port details were not shown properly in Device Details Page of Settings tab. The issue is fixed
- Firewall: When a PaloAlto Rule Name contains 'index' value, wrong unused rule list is displayed. The issue is fixed.
- Firewall: Checkpoint VPN log parsing issue is fixed.
- Firewall: In MSSQL setup, Yearly tables were not dropped properly. The issue is fixed
- Firewall: When extra device license was applied in the product, the manage and unmanage actions couldn't be performed till user restarts the product. This issue is fixed.
- Firewall: Header of SMS notification in Alert Profile page changed from 'Send Email based SMS' to 'Send SMS' to avoid misunderstanding.
- Firewall: In the Report Profile Notification page, a message "Use comma ',' separator for multiple mail ids" has been added for clear understanding.
- Firewall: Edit and Save Report Profile action returned wrong status message. The issue is fixed to show proper status message.
- Firewall: While saving Compliance Report Schedule, there was no status message. This issue is fixed to show the status message.
- NCM: EOL/EOS data is now updated from local database.

- NCM: Now you can discover devices in single step.
- NCM: XML External Entity vulnerability security patch is released.
- NCM: SNMP profile is now unified and can be accessed in single place.
- NCM: Now you can request for latest EOL/EOS data with NCM support from product.
- NCM: Now you can update SysOID for multiple devices in single shot.

Build No - 123176 - July 18, 2018

- General: Previously, Audit report was not working in NFA and NCM. This issue has been fixed.
- Netflow: Security Patch to handle Zip Slip Attack.

Build No - 123175 - July 13, 2018

- OpManager: Previously, the password field for the getProcessesForWorkflow API was exposed. This issue has now been fixed.
- OpManager: Exclude Days option provided in Reports and Schedule Reports.
- OpManager: Inside Availability and Response Reports page, for 'URLs Availability' report the URL Name field was left blank without any value. This has been fixed now.
- OpManager: Previously, OpManager agent was vulnerable due to Zip Slip Attack. This has been handled now.

Build No - 123169 - July 11, 2018

- General: Cross site scripting(XSS) and arbitrary file read vulnerability in Fail Over has been fixed. [CVE-2018-12997, CVE-2018-12998]
- NetFlow: Data encryption has been provided for attachments in 'Schedule Report Mail'.
- NetFlow: Under DNS Settings, the issue with Cross-site Scripting (XSS) on DNS Name has been fixed.
- NCM: Security Patch to handle Zip Slip Attack.
- NCM: Security Patch to handle Local File Inclusion Attack.

Build No - 123168 - July 6, 2018

- OpManager: Previously, the IPSLA monitor was not getting deleted for OpManger running with MSSQL DB. This has been fixed now.
- OpManager: OpManager will now fetch the device serial number and software version using SNMP based on the device type configured in HardwareInfo.xml (conf\OpManager).
- OpManager: Under System Settings page, a filter option has been provided in Interface discovery for single device additions.
- OpManager: Audit logs will now be recorded whenever a user:
- creates a custom category.
- deletes a custom category.
- OpManager: Dial enabling issue has been fixed for all the monitors.
- OpManager: Previously, Data collection failed for String monitors with StringToNumeric expression. This issue has been fixed.
- OpManager: Users can now choose the uplink dependency for devices in Layer2Discovery.
- OpManager: Previously, in non-monitored state, device availability status was displayed as 'UP' instead of 'Not Monitored'. This has been fixed.
- OpManager: Previously sorting of columns inside widgets of Virtual Servers snapshots was not working properly as expected. This has been fixed now.

- OpManager: While adding Process Template, the displayName of the process was getting updated same as Name parameter. This has been fixed now.
- OpManager: Previously sorting of columns inside Monitoring page from Settings was not working properly as expected for all types of monitors. This has been fixed now.
- OpManager: While configuring File/Folder monitors, sometimes, the same monitor was getting added more than once. This has been fixed now.
- OpManager: While performing edit operation, field validations was not done for Non-Numerical values of Threshold and Rearm values for Performance Monitors from Settings page.

Build No - 123167 - July 5, 2018

- General: Database migration from MSSQL to PostgreSQL has been implemented.
- General: Previously, it was mandatory to configure Mail server settings before configuring Notification Profile. This has now been modified to allow direct configuration of other notification services.
- General: Previously, after clicking on the DNS tab in System Settings page, content for the other tabs did not load. This issue has been fixed.
- General: In Server settings page, the 'Cancel' button was unresponsive. This issue has been fixed.
- General: The Dashboard action button was unresponsive for local operator user. This issue has been fixed.
- General: Previously, there was a UI issue in the global search bar when a set of operations was performed by Read Only user. This issue has been fixed.
- OpManager: ZipSlip Vulnerability issue has been fixed.
- OpManager: Support Information File (SIF) can be accessed only by admin user through API calls.
- OpManager: EncryptPassword.bat has been removed due to DOS attack.

Build No - 123166 - July 3, 2018

- OpManager: Previously, when 'Process Monitor' report was exported as a PDF, data was not displayed even when it was available in the UI. This issue has been fixed.
- OpManager: 'Date' variable has been introduced in the 'Workflow'.
- OpManager: Previously, under 'Schedule Reports', the time period was displayed incorrectly in a few reports. This issue has been fixed.
- OpManager: In the Snapshot page, visibility of 'Schedule This' option has been restricted hidden for operator users.
- OpManager: Previously, in some rare cases, it was not possible to copy workflow. This issue has been fixed.
- OpManager: Previously, under 'Schedule This' option, weekly/monthly UI elements were displayed incorrectly for different options. This issue has been fixed.
- OpManager: 'Execute Template' workflow task failed to work. This issue has been fixed

Build No - 123165 - July 2, 2018

- OpManager: Previously, unauthenticated users were able to access the device's custom icons in businessview. This issue has now been fixed.
- OpManager: Previously, empty floors were visible to the operator user. This issue has now been fixed.
- OpManager: Previously, empty racks were visible to the operator user. This issue has now been fixed.
- OpManager: Floors with racks to which operator users have no accessible devices will not be displayed.
- OpManager: Racks with devices to which operator users have no access will not be displayed.
- OpManager: Previously, in Business views under Maps, the device icon was unresponsive. This issue has been fixed.

Build No - 123164 - June 29, 2018

- Firewall: A new device 'MicroTik' is now supported.
- Firewall: Simulate firewall logs - You can simulate firewall logs for different vendors to check all the reports in Firewall Analyzer. Log simulation is available for Fortigate, PaloAlto, CheckPoint, Juniper SRX and Squid Proxy devices.
- Firewall: Added more than 3000 websites to the Cloud Repository.
- Firewall: Option to plot Dashboard Live traffic graph in 'Kbps/Mbps/Gbps' is available.
- Firewall: Support ID: 4598454 - Updated IP to Country database.
- Firewall: Support ID: 4573349 - When you import syslog, you can map the logs to the existing device.
- Firewall: Support ID: 4590527 - Export to CSV format option is available for expanded view of all 'Inventory' page widgets.
- Firewall: 'Admin Report' for PaloAlto available. It covers details of user login, log out, and commands executed.
- Firewall: Auto refresh option provide to 'Live Syslog Viewer' page.
- Firewall: Mail content format enhanced for scheduled 'Standards' report.
- Firewall: More tabs are added in Device inventory snapshot page for better access.
- Firewall: License count, number of managed devices and remaining devices count now available under ' License Management' page.
- Firewall: Now 'bps' value is formatted to readable format in Bandwidth Alert mail content.
- Firewall: Support ID: 4588018 - While creating Alarm profile, configuring more than 50 criteria makes the page unresponsive. This issue is now fixed.
- Firewall: Refresh option in 'Dashboard Live Traffic' widget was not working. Now the issue is resolved.
- Firewall: AD User-IP Mapping had two entry for an user with Old and New IP. The duplication issue is rectified now.
- Firewall: Support ID: 4579510 - Incorrect Rule Name was shown for Zyxel firewall. This issue is now fixed.
- Firewall: Support ID: 4480507 - Invalid Byte Sequence Error while loading FirewallRecords table is fixed.
- Firewall: While parsing Sonicwall configuration, network objects with IP-range and IPv6 objects were not handled properly. It is fixed now.

- Firewall: Finding 'Unused Objects' from configuration file had discrepancy. Now it is rectified.

- Firewall: In Japanese Installation, when logs are imported, reports were generated for current time instead of log time. This issue is resolved.

- Firewall: 'Edit Interface' & 'Edit Interface Names' were not working, when edited for the second time. This issue is now fixed.

- Firewall: Occasionally, the 'Inventory' page became empty when 'Back' icon was clicked. This issue is now resolved.

- Firewall: Even after changing display name of Firewall, ' Resource Name' was displayed when user was added from User Management page. Now the issue is fixed to show the device list with display name while assigning device.

- Firewall: When Credential Profile was edited, the 'Email' field became empty. Now the issue is fixed to show the given Email Id in that field.

Build No - 123163 - June 27, 2018

- NetFlow: Option for IP group bulk-upload between sites is added.
- NetFlow: NetFlow supports Resolve DNS option in Report profile.
- NetFlow: NetFlow now provides detailed report for AS View.
- NetFlow: The issue with data mismatch for devices in Inventory and Map module has been fixed.
- NetFlow: The issue with the interface count mismatch has been fixed.

Build No - 123162 - June 25, 2018

- General: A new icon has been introduced in the top right corner of the product's header which contain links to the respective product's training videos.
- OpManager: Option to bulk Deletion of File, Folder, Process, Service, WindowsService and URL Monitors from Device snapshot pages has been included now.
- OpManager: Previously, the Active Processes and Installed Software data was pulled from device only if SNMP Protocol was passed. Now the data will be pulled also for the device associated only with WMI Credential.
- OpManager: Previously, the password of the device was visible in the URL if ListActiveWindowsServices Api was invoked. This has been fixed now.
- OpManager: The encryption level of device password credentials has been increased.
- OpManager: Previously, when a Business View Administrator user was trying to view the Graphs from Device Snapshot -> Monitors page, it was redirecting to blank page. This has been handled now.
- OpManager: While associating monitors from Settings -> Performance Monitors page, the threshold values were not getting updated to the device. This has been fixed now.
- OpManager: In Probe set up, the test credential for VMware/Xen and UCS devices was not working due to incorrect parameter. This has been fixed now.
- OpManager: Previous, Proper validation was not done for Monitoring interval field for all the monitors. This has been handled and validation check has been included now limiting the monitoring interval max value to 24 hours.
- OpManager: Audit logs were not shown in device snapshot for Process Templates association details. This has been fixed now.
- OpManager: Previously, WMI protocol based Process monitors were shown in Linux installation inside process templates, leading to incorrect association of those monitors and unnecessarily slowing down of data collection. This has been handled now and

those invalid monitors will not be shown.

- OpManager: Sometimes, creation of raw stats data table was getting stopped and was leading to data collection failure. This has been handled now.
- OpManager: Previously, VMware discovery was getting failed if, for any datastore mount location value was not received from API. This has been fixed now.
- OpManager: Language Localisation of the Sensor Status was not done under Hardware Monitoring for Chinese Language. This has been done now.
- OpManager: Language Localisation for the 1Month field inside graph was not done for Chinese/Japanese Language. This has been done now.

Build No - 123161 - June 21, 2018

- OpManager: Previously, users with "Operator Permission" were able to Create/ Delete URLs. This issue has now been fixed.
- OpManager: Previously, users with "Operator Permission" were able to access the URL Snapshot page by using the page's link copied from the address bar of the "Administrator" profile. This issue has now been fixed.
- OpManager: Previously, users with "Operator Permission" were able to create business views. This issue has now been fixed.
- OpManager: Previously, users with "Operator Permission" were able to access the 'getSociallTPostDetails' API. This issue has now been fixed.
- OpManager: Previously, Custom link content was vulnerable to Cross-Site Scripting (XSS). This issue has now been fixed.
- OpManager: Previously, the password field for the QueryDeviceForSysOID API was exposed. This issue has now been fixed.
- OpManager: Previously, Import Device Template was vulnerable to Cross-Site Scripting (XSS). This issue has now been fixed.
- OpManager: LFI vulnerability while uploading device custom icon in businessview is fixed now.
- OpManager: While exporting the 'Interface Bandwidth' report in PDF format, the date and time values were displayed incorrectly. This issue has been fixed.
- OpManager: Previously, VLAN and Configure Interface option was displayed twice for networking devices. This issue has been fixed.
- OpManager: Previously, data displayed in the 'Last polled bandwidth utilization' widget was incorrect in NOC view. This issue has been fixed.
- OpManager: Previously, under Inventory, while using the Filter by severity option for Interface and URLs, there was a count mismatch issue. This issue has been fixed.
- OpManager: Previously, under Inventory, the User had to click twice to view the Device/Interface snapshot pages. Now, the short summary page has been removed and a single click will take the User to the snapshot pages.
- OpManager: Previously, under Device Template, there were issues while selecting multiple monitors during addition. This issue has been fixed.

Build No - 123160 - June 19, 2018

- OpManager: The RemodeCodeExecution(RCE) vulnerability occurring while testing scripts has been fixed (Reported by Pulse Security).
- OpManager: Path Traversal vulnerability in uploadMib API has been fixed (Reported by Pulse Security).
- OpManager: Unauthorized access for uploadMib API has been restricted. It can be accessed only by users with admin privileges.
- OpManager: Previously, any type of input was accepted in UpdateDeviceDetails API's parameter. This issue has been fixed (Reported by Pulse Security).

- OpManager: Previously, OpManager files could be changed or modified by exploiting LFI vulnerability in uploadBusinessViewBG, importDeviceTemplate API. This issue has been fixed.

Build No - 123159 - June 18, 2018

- NCM: Export the devices listed in device inventory page as PDF.
- NCM: A device group that is listed as a sub group in another device group cannot be deleted.
- NCM: Issue of database backup and restore failure after importing new device template is now fixed.
- NCM: Issue of upgrade failure due to ncm personality-configuration is now fixed.
- NetFlow: NetFlow now Supports remote PostgreSQL database.

Build No - 123158 - June 14, 2018

- OpUtils : Under Inventory, the UI of MAC, IP address and DNS is improved in the ports section by making multiple addresses now visible in a separate slide window when "more..." is clicked.
- OpUtils : In the Switch snapshot page under Inventory, the UI of MAC, IP address and DNS is improved in the ports section by making multiple addresses now visible in a separate slide window when "more..." is clicked.
- OpUtils : Under privacy settings, Personally Identifiable Information(PII) search and update has been implemented. (PII Search helps identify the PII Details given by the user across various modules. The PII data can also be updated as anonymous to maintain privacy).

Build No - 123157 - June 14, 2018

- OpManager : The SQL injection vulnerability in "FailOverHelperServlet" for the operation 'standbyprobestatus' has been fixed (CVE-2018-9087, CVE-2018-9089).
- OpManager : The SQL injection vulnerability in "FailOverHelperServlet" for the operation 'getprobenetworkshare' has been fixed (CVE-2018-9088).
- 4692934 - The "Integration User" option under 'User Management' has been removed.
- OpManager: The Interface discovery timeout which was by default set to 5 seconds, will now fetch the timeout value from the SNMP credential.
- OpManager: Users can now configure the number of parallel threads for Trap discovery in "threads.conf"
- OpManager: Discovery delay has been introduced for Trap based discovery and the default interval has been set to 20 seconds. The user can configure this delay and set a custom interval in "discovery.properties".
- OpManager: Discovery debug prints have now been introduced for the purpose of troubleshooting.
- OpManager: Previously, the SNMPV3 EngineID request was queried only once with a timeout of 5 seconds. Now, the timeout and retries count will be fetched from the credential.
- OpManager: Previously, devices running the latest build of Windows 10 was being discovered and classified as Windows 8. This issue has been fixed.
- OpManager: Audit logs will now be recorded whenever a user
    - modifies the name of the Business view
    - modifies the name of the Floor view
    - modifies the name of the Rack view
- OpManager: Process names printed in the "Discovery logs" have been modified as "Debug prints" and names with ".exe" have been removed.
- OpManager: Previously, the Palo Alto device templates were set with the wrong vendor 'APC'. This has now been updated as

'Palo Alto Networks'.

- OpManager: Previously, the Interface name and Alias had garbled characters during discovery, when the OS and OpManager had French as the primary language. This issue has now been fixed.
- OpManager: Additional SysObjectIDs have been added for the below device template types,
    - Cisco catalyst296024LT
    - Cisco 891
    - Cisco MDS 9148

Build No - 123156 - June 13, 2018

- General: License Agreement has been updated.
- General: Promotions related to ITOM Events will be displayed in the UI header after login.

- OpManager : Enabling proxy settings blocked APM-Plugin communication. Users were unable to login to the plugin and experienced issues with syncing OPM. This has been handled now.
- OpManager : Unable to discover vCenter if proxy settings were enabled in OpManager. Now this has been handled.
- OpManager : Disabling proxy settings from client did not take effect directly, and required a server restart. This issue has been fixed.

Build No - 123150 - June 7, 2018

- OpManager: Audit Information/Logs for Add/Edit/Delete/Associate Operations for URL Monitor has been included.
- OpManager: Audit Information/Logs for Add/Edit/Delete User Operations for APM Plugin has been included.
- OpManager: Previously, it was not possible to perform actions like Clear/Delete/Acknowledge for URL based alarm from url snapshot page, alarms view. The mentioned options have been included now.
- OpManager: Previously, WMI Credential test for device discovered as Unknown was not possible. This has been fixed now.
- OpManager: If both HyperV and WMI devices were being monitored then inside Protocol based Inventory view, the number of devices count was shown incorrectly if VIWMI protocol was chosen. This has been fixed now.
- OpManager: Even though vCenter was UnManaged, the VMware Events based alarms were getting raised. This has been fixed now.
- OpManager: The field validation for alarm message of threshold violation was not done for Performance monitor, leading to inappropriate confirmation message to user of monitor being saved. This has been fixed now.
- OpManager: Once the URL Response Time based only alarm is cleared or deleted, the status of URL monitor is still not updated to Clear. This has been fixed now.
- OpManager: With APM Plugin of version 13730 and above, an inappropriate alert is shown to the user asking to upgrade to the latest version of APM Plugin. This has been fixed now.
- OpManager: The field validation for Threshold parameters was not done for MSSQL Monitors. This has been fixed now.

Build No - 123149 - June 6, 2018

- OpManager: Quicklinks to How-to, Technical videos, and FAQs has been introduced in OpManager to help users easily configure settings and to troubleshoot commonly faced issues.

- OpUtils : Previously under Dashboard, the edit option in "IP Availability Summary HeatMap" widget only had a drop down list of IP's without their subnet mask. The issue is fixed now by listing IP addresses with their subnet masks.
- OpUtils : Previously under Inventory, the edit option in IP address field does not mention the IP Address that is being edited. The issue is fixed now by making the selected IP visible as a header.

- OpUtils : Previously under Inventory, the DHCP option shows an empty page when there is no data. The issue is fixed now as it shows sample data which disappears automatically once data is added.
- OpUtils : Under Ports page of Inventory, five options such as "Modify IfAlias" , "Administratively Disable Interfaces" , "Administratively Enable Interfaces" , "Exclude Port(s)", and "Include Port(s)" were made available. These actions were not available for the ports listed in switch snapshot page. The issue is fixed now.
- OpUtils : Previously under Inventory, the grid is not updated automatically after editing the IP address. The issue is fixed now.
- OpUtils : Under tools, there was an issue in the working of Trace Route when resolving the DNS name. This issue is fixed now.

Build No - 123148 - June 1, 2018

- OpManager: Previously, while configuring 'Send Email' in Workflow, the 'HTML' mail format option was not working. This has now been fixed.
- OpManager: Previously, the option to edit the display name of the IP SLA monitor was unavailable. This option has now been provided.
- OpManager: In Probe/Central set up, IP Address field was displayed incorrectly with the probe ID appended at the end. This issue has been fixed.
- OpManager: "Custom Dials" option has now been added for UCS devices.
- OpManager: Previously, while adding IP SLA Monitor, a proper Field Validation for the Name field was missing. This issue has been fixed.
- OpManager: Previously, redirection to the "VoIP Monitor Snapshot" page using the "Top Call Performance by location" widget was not successful. This issue has now been fixed.
- OpManager: Previously, clicking the IP SLA Monitor link in the Business View did not redirect the User to the respective Monitor/List page. This issue has now been fixed.
- OpManager: WAN RTT Monitor and VoIP Monitor Widgets were missing from the source device of the IP SLA. This has now been included.
- OpManager: Previously, the time period for which the reports were displayed was not shown in the IP SLA Widgets. This has now been included.
- OpManager: For IP SLA Reports, Widgets and Snapshots, the display name of the destination device will be shown instead of its IP Address.
- OpManager: Previously, "Operator" user was not restricted from viewing the URL monitors in the Inventory Page. This issue has been fixed.
- OpManager: Previously, "Operator" user was not restricted from being able to modify the background color and the tile color in the 3D floor view page. This issue has been fixed.
- OpManager: In Group Chat Module, "Operator" user was not restricted from viewing the list of users, their User ID and Email addresses. This issue has been fixed.
- OpManager: In Group Chat Module, the "Delete Post" and "Delete Comment" API was vulnerable to SQL Injection. This issue has been fixed

Build No - 123147 - May 31, 2018

- General: Data encryption has been provided for attachments in 'Schedule Report Mail'.
- OpManager: Spreadsheet format has been updated from XLS to XLSX across the product.
- OpManager: A disclaimer text concerning privacy has been added in exported PDFs and spreadsheets. This can be disabled/enabled in the system settings page.
- OpManager: Alert/Event message showing garbled values has been fixed.
- OpManager: In discovery, it was possible to import CSV files that contained HTML content. This issue is now fixed.

- OpManager: Previously under 'Additional Fields' in 'Configuration' module, it was possible to import CSV files that contained HTML content. This issue is handled now.
- OpManager: In the Group Chat module, getSocialITPost details API was prone to SQL Injection vulnerability with "postID" parameter. This issue is fixed.
- OpManager: Path traversal issue in Group Chat module affecting local drive folders is fixed.

Build No - 123137 - May 25, 2018

- General: Dashboards are now user-specific and allows users to create their own private dashboards. Apart from this, users with administrator privilege can associate dashboards that are created by them with select users.

- NCM: Network Configuration Manager is now **GDPR compliant** with the privacy messages and consent requests displayed in the UI.
- NCM: Increased privacy & security through product enhancements.
- NCM: Custom column names now populate uniformly throughout the UI after a change.
- NCM: More user-friendly with editable Configlet names.

- NetFlow: Distributed Edition for latest version has been released.
- NetFlow: NetFlow Analyzer is now GDPR compliant with consent requests displayed across various modules in the UI.
- NetFlow: Under privacy settings, Personally Identifiable Information (PII) search and update options have been added. (PII Search helps identify the PII Details given by the user across various modules. The PII data can also be updated as anonymous to maintain privacy.)
- NetFlow: A step by step guide on How to use NetFlow Analyzer has been added.
- NetFlow: Resolve DNS handled for Conversation widget in Device snapshot.
- NetFlow: The issue with the wrong granularity values being displayed in Device snapshot page has been fixed.
- NetFlow: Search report and Global search report options have been combined together under Search Report.

- Firewall Analyzer: Introduced 'Audit Report' for all add, delete, and update actions done by Firewall Analyzer user. All the user actions are logged.
- Firewall Analyzer: Option to search personal information like Email, phone number and user name across the product and replace them with another user is available under 'Privacy Settings'.
- Firewall Analyzer: 'Security Audit Report' is now available in PDF format. You can export the report in PDF format from client.
- Firewall Analyzer: Disclaimer added in exported PDF & CSV to convey availability of Personally Identifiable Information (PII) of GDPR.
- Firewall Analyzer: Option to add new Custom Report was not visible in UI. Now the issue is fixed.

Build No - 123136 - May 22, 2018

- General: Previously, Chinese characters sent as parameter in API were saved as garbled characters. This issue has been fixed.
- General: Live chat support has been integrated in OpManager.
- General: System Performance status icon has been removed from the header in OpManager.
- General: Previously, "Arithmetic Exception" error was thrown during a fresh start of OpManager. This has now been fixed.
- General: Triggering an API call for creating a dashboard without choosing any widget is restricted to the web client.
- General: In edit widget page, same value cannot be given in two different criteria. This has been fixed.
- General: Updating a widget without widget name has been fixed.

- General:Previously, when adding the first domain, it was not listed in the Windows Domain until the page was reloaded. This issue has been fixed.
- General: In global search, NCM-Compliance was not redirecting and the Subnets results were not listed. This issue has been fixed.
- General: In global search, showing of undefined value in add-on details from search suggestion has been fixed.
- General: In global search, Device notes were not listed out in the search if the list count is more than 10. This issue has been fixed.
- General: Previously, PostgreSQL to MSSQL migration kept failing due to mismatch of datatype in 'Alert' table and 'Event' table. This issue has been fixed.
- General: License expiry alert mail will be sent with an interval of 5 days between each reminder for the last 15 days and the final remainder will be sent a day before the license expires.
- General: UI Notification displaying license expiry duration in the header has been limited to the last 30 days.

- OpManager: Option to export and download 'Availability Statistics' as PDF and XLS is provided for all monitors including Windows Service Monitors, Service Monitors, Exchange Service Monitors, AD Service Monitors, MSSQL Service Monitors and Process Monitors.
- OpManager: Option has been added to view ﷺReal Time Monitor Graphs﷽ for all the Performance monitors that are available as Dials inside snapshot page.
- OpManager: Saving the Hardware Monitor specific settings was prone to SQL Injection vulnerability. This has been fixed now.
- OpManager: For Process and Service Monitors snapshot page, the selection of Custom Time Period didn't have any effect and used to show the same details based on previously selected time period. This has been fixed now.
- OpManager: Previously, when WMI credential used for monitoring WMI device had space character in its password, the monitored device was experiencing account lock out issue. This has been fixed now.
- OpManager: Previously, File/Folder monitoring was not generating alerts even if the file was modified, especially in cases where the monitored device machine had different date formats. This has been fixed now.
- OpManager: In Event Log Monitoring, if the configured message field had 'tab space' character, the generated event log message was not displayed properly. This has been fixed now.
- OpManager: Previously, Performance monitors' XLS reports were generated with garbled characters for non-english languages. This has been fixed now.
- OpManager: While configuring Event Log Monitors, field validation for Event ID field was not done. This has been fixed now.
- OpManager: Unit for monitors were not shown for File/Folder graphs' tabular view. This has been fixed now.
- OpManager: Language localization for 'Edit Discovery Profile' and 'Never Suppress Alarm' operation specific keys were incorrectly updated for Japanese language. This has been properly updated now.
- OpManager: Under Inventory Reports, for 'Threshold Details of Devices' report, VMware & HyperV specific Monitors﷽ threshold details were not listed. This has been fixed now.
- OpManager: Previously, RuleEngine Re-Run or discovery/rediscovery of device was not getting updated for MSSQL Monitors, even though they were configured in RuleEngine Actions. This issue has been fixed.
- OpManager: While mapping IP to VirtualMachines from vCenter/ESXServer/HyperV/Xen Servers snapshot pages, only IP was allowed previously. Now hostname is also allowed.
- OpManager: Previously, if an incorrect parameter value for Protocol was passed for updateProcessTemplateDetails API, proper error was not thrown. This has been handled now.
- OpManager: In Monitors Tab under Snapshot Page, columns were not being sorted as per data type. This issue has been fixed now.
- OpManager: In ﷺNotification Profile﷽ message box, language localization value for Chinese language has been updated for the message property.
- OpManager: In Add/Edit File Monitor under Settings page, language localization value for Japanese language has been updated.

- OpManager: OpManager agent was getting crashed due to memory leak in the agent while reading the registry data for monitoring. This has been fixed now.
- OpManager: In Performance Monitor Graph page, "Last month" time period option has been added.
- OpManager: In the device snapshot page, PDF option for Single monitor graph page was not working properly. This issue has been fixed.
- OpManager: Test URL option from URL snapshot page failed after the first try. This issue has been fixed.
- OpManager: Previously, users were able to select/deselect the listed Event Log rules while associating it to device from snapshot page even without enabling Event Log Monitor Interval. This has now been fixed.
- OpManager: Windows Services from device were not retrived while configuring Workflow with Restart Service action if device credential had special characters. This has been fixed now.
- OpManager: Unauthorized SIF Activity (Support Information File) has been restricted and can be accessed only using the admin account.
- OpManager: Notification Profile severities will not over write Device Misses 1/3/5 Polls profile Criteria selection any more.
- OpManager: '+' symbol in the beginning of EMail-Id for Mail Server Settings and Notification Profile is supported now.
- OpManager: Previously, Command results of Run Program/System Command Notification Profile appended to alert message were not properly shown. This issue has been fixed.
- OpManager: Run Program/System Command Notification profile's message variables given in next line are not taken as arguments while executing commands on notification profile trigger. This issue has been fixed.
- OpManager: In Settings page, ﷿Mobile number﷿ was shown even after deleting the App SMS settings. This has been fixed.
- OpManager: Previously, trying to uninstall OpManager Central failed with an error popup. This has now been fixed.
- OpManager: Previously, installing standby OpManager with invalid credentials of primary OpManager resulted in the setup getting installed as Standalone OpManager with PGSQL backend. This has now been fixed.
- OpManager: Previously, installing OpManager with MSSQL DB as backend by providing existing database name resulted in the setup getting installed with PGSQL backend. This has now been fixed.
- OpManager: Previously, in Alarm escalation rule, entering multiple mobile numbers, each separated by a comma was not possible. This option has been added.
- OpManager: SSH Discovery will fetch the DeviceType from login message based on availability.
- OpManager: In reports, the 'Server Health Report monitors' name i18n has been updated now.
- OpManager: Users can now select multiple SNMP trap processors and delete them in bulk using the 'multiple delete option'.
- OpManager: Search option for SNMP trap processor is now enabled where the user can search trap processors based on either name or OID.
- OpManager: Multiple delete option is now enabled for unsolicited traps, where the user can select more than one trap and delete them.
- OpManager: Search option for Unsolicited traps is now enabled.
- OpManager: A new option is provided in the widget Edit page to enable and disable the Widget Dials.
- OpManager: Previously, while adding a rule in Rule Engine, 'criteria' drop down field was not populated correctly. This issue has been fixed.

- OpUtils : The Bandwidth monitoring tool, which measures the network traffic utilization/bandwidth usage both at the interface level and at the device level, has been brought back under inventory.
- OpUtils : The Bandwidth monitoring tool is enhanced with the capability of generating alerts based on the configured threshold violation and the same can be notify through email.
- OpUtils : Previously under Oputils option, the SPM General settings could not be saved. This issue is fixed now.
- OpUtils : Previously under Inventory, the option to edit a switch in Switch Port Papper was not working. This issue is fixed now.
- OpUtils : In the Network Scanner page under Settings, when deleting multiple IP Address(es) after selecting them, an error

message was thrown saying "Nothing is selected to delete". This issue has been fixed and multiple IP address(es) can be batch deleted.

- OpUtils : Under "Short Summary" page in Inventory, "Subnet summary", "IP summary", "Switch summary" title was displayed . This has been removed.
- OpUtils : The "Device Type Summary" widget in Dashboard has been renamed to "OS Type Summary" as it represents the OS type installed in the device.
- OpUtils : Constraints have been added to check if the "Custom column" name is numeric. An error message will be displayed stating " Invalid Custom Name " in case the name is numeric.
- OpUtils : In the MAC Address Resolver page under Setting tools tab, "IP to MAC" and "MAC to IP" were displayed in two different lines due to a minor UI alignment issue. This has now been fixed.
- OpUtils : In the Credentials page under SPM in settings, editing an existing credential redirected the page to Discovery"s Edit credential page. This issue has been fixed.
- OpUtils : Under Basic settings, Database Maintenance option has been removed for OpUtils installation.
- OpUtils : In the Scope page for DHCP under Inventory, the "Scope State" column in the table contains two values - "Enabled" and "Disabled" . The "Disabled" option will now be highlighted in red color.
- OpUtils : In the "OS Type Summary" widget (previously called "Device Type Summary"), the "%" symbol was not displayed in the value when hovering the mouse over it. This issue has been fixed.
- OpUtils : The SNMP graph tool, which is used to gather real time data and generates a graph for any SNMP IP node, has been brought back under SNMP tools of OpUtils settings.
- OpUtils : The SNMP graph tool is enhanced with the capability of providing the MIB node information like OID, syntax, description and MIB node properties.

Build No - 123127 - May 14, 2018

- OpManager : Inbuilt Storage Monitoring support has been added.

Build No - 123126 - May 8, 2018

Firewall Analyzer: Admin Server

- Firewall Analyzer: Enterprise edition for 12.3 version
- Firewall Analyzer: Data Migration tool for enterprise edition 8.5 customers to upgrade to 12.3

Firewall Analyzer: Standalone/Collector Server

- Firewall Analyzer: Compliance reports and Policy/Rule Management support for WatchGuard device
- Firewall Analyzer: Compliance reports and Policy/Rule Management support for SonicWALL device.
- Firewall Analyzer: Policy/Rule re-order report for PaloAlto device

Build No - 123125 - May 8, 2018

- OpManager: In Mail Server settings, Authentication Details which was mandatory (from 123108) has been made optional.
- OpManager: Previously, the selected dashboard view was not being highlighted. This issue has been fixed.
- OpManager: When OpManager server rebooted, OpManager service failed to start displaying the error "Unable to start PgSql DB" This has been fixed now.

- OpManager: Consent Implementation has been enforced for various modules.
- OpManager: Under privacy settings, Personally Identifiable Information(PII) search and update has been implemented. (PII Search helps identify the PII Details given by the user across various modules. The PII data can also be updated as anonymous to maintain privacy)
- OpManager: Audit logs will now be recorded whenever a user

- - adds or deletes additional fields.
  - rediscovers a device.
  - uploads a Google Map html file.
  - deletes a device from Google Map.
  - creates or deletes Business views, 3D Floor views and Rack views.
  - creates/modifies/deletes a Discovery Profile.
  - creates or deletes a group in Group chat.

- General: Chrome's latest update(66.0.3359.139) caused OpManager to crash when navigating to any graph pages. This issue has been fixed by updating zoho charts from version 1.0.5 to 1.0.8.

Build No - 123124 - May 3, 2018

- OpManager: Option to copy and modify the Business View (Copy As option) has been added.
- OpManager: Previously, Zoom in/out feature was missing in Business view widget and Maps. This has now been added.
- OpManager: Previously, in 'edit Business view', device and shortcut count was missing. This has been handled now.
- OpManager: Previously, IPSLA monitors were missing in the Business view. This is fixed now.
- OpManager: Under Business views, the device status live update was missing when the page was not refreshed. This has been handled now.
- OpManager: Earlier there was an issue with deleting and re-adding devices in business view. This has now been fixed.
- OpManager: Previously, when changing font type, size or color in business view, the devices were rearranged automatically. This issue has been fixed.
- OpManager: Under Maps, 'Set as default option' for Business view,List and Dashboard has been added.
- OpManager: The back view of the rack was missing in the new version. This is fixed now.
- OpManager: Previously, Rack view and 3D floor embedded view was not working. This issue is now fixed.
- OpManager: Device status mismatch issue under Rack widgets in Dashboard has been fixed.
- OpManager: Previously, in google map widget, probe option was displayed for Essential build. This has been fixed now.
- OpManager: Interface port status icon in inventory list view has been added.
- OpManager: Users can now view device category specific dashboards in the inventory page.
- OpManager: Set as Default view has been added for Inventory Device and Interface List.
- OpManager: Users can enable or disable the Group chat,Rack & 3D floor view features under System Settings. (By default Group Chat feature has been disabled.)
- OpManager: Graph were not displayed for Interface Receive and Transmit dials. This has been fixed now.
- OpManager: Previously, Interface Bandwidth Report schedule won't be generated for the given time period. This has been fixed now.

Build No - 123123 - April 26, 2018

- NCM: Compliance page has been added in left menu bar for quick access. All compliance-related functionalities are now

available under this page.

- NCM: Now, you can share Custom Device Templates to NCM Administrators worldwide in 'Device template >> Custom >> Share'.
- NCM: Additional hardware information for Cisco devices is now displayed in the Device Snapshot page under 'Inventory' tab. We will support other vendors also in the near future.
- NCM: You can now search devices by providing their hardware details, in 'Inventory >> Devices >> Search by hardware details' (Filter icon on top-right corner).
- NCM: Device selection list is sorted in 'Configlets Execution' and 'Schedules' pages with the IP addresses of the devices.
- NCM: 'Should contain exact set' in Compliance rule criteria is now fixed and executes properly.
- NCM: The Rule Compliance page under MSSQL now displays the necessary data.
- NCM: The '%' symbol in labels of configlet parameters from 'Execute Configlet' page has been removed.

Build No - 123122 - April 25, 2018

- OpManager: Previously, it was possible to access the attached html files in GroupChat. This issue has been fixed.
- OpManager: In the GroupChat module, getActivityData api was prone to SQL Injection vulnerability. This issue has been fixed.
- OpManager: In Credential module, Stored Cross-site Scripting (XSS) vulnerability has been fixed (CVE-2018-10803).
- OpManager: Previously, Improper file format was accepted during CSV Discovery. This issue has been fixed.
- OpManager: Previously, Discovery profile name is vulnerable to Cross-site Scripting (XSS). This issue has been fixed.

Build No - 123121 - April 24, 2018

- OpManager: In the Add/Edit Performance Monitor page under Device Snapshot and in Device Template page, Regex pattern threshold field length has been increased from 50 to 100.
- OpManager: In the Add Performance Monitors page under Device Snapshot and in Device Template page, general monitors were not listed for addition. This has been fixed now.
- OpManager: While updating SSH credential from global credential and device snapshot page, SSH key authentication file was stored in an incorrect path. This has been fixed now.
- OpManager: Under System settings page, a unique SysName option has been provided to avoid multiple interfaces of the same device being discovered as new devices.
- OpManager: Previously, option to add a single device using device name was missing under schedule discovery profile. This has been added now.
- OpManager: Previously, Windows 10 device was discovered as Windows 8 via SNMP. This has been fixed now.
- OpManager: Previously, in the device snapshot page, the dials displayed data but the Monitors tab was empty. This has been fixed now.

Build No - 123120 - April 20, 2018

- OpManager: In Quick Configuration Wizard, option to update threshold configuration for a specific group of partition detail monitors for multiple devices has been included.
- OpManager: In Quick Configuration Wizard, option to add or update threshold configuration for multiple VMware datastore monitors has been included.
- OpManager: UI misalignment in the Quick Configuration Wizard page has been fixed.
- OpManager: Previously, in Performance monitor page under Settings, when performing apply and overwrite operation after editing any monitor threshold, Store Data value of the monitor was changed to false by default. This has now been fixed.
- OpManager: Previously, from Performance Monitors under Settings page, VMware and Xen Monitors where not getting applied/associated to devices even for VMware and Xen devices respectively. This has been fixed now.

Build No - 123119 - April 18, 2018

- OpUtils : Under SNMP tools from settings, a tool called MIB node viewer that is used to provide the complete details of the selected MIB has been added.
- OpUtils : Under SNMP tools from settings, a tool called MIB module viewer which is used to provide a snapshot of a given MIB has been added.
- OpUtils: Under Switch Port Mapper(SPM), the tree view has been added.
- OpUtils: The IP snapshot page has been improved by adding missing data and actions.
- OpUtils: The MAC-IP list, which was a missing tool, has been added.
- OpUtils: Under the Subnet snapshot page, the options to edit and scan has been added.
- OpUtils: Under the Subnet snapshot page, the option to delete alerts has been added.

Build No - 123118 - April 17, 2018

- OpManager: Previously, users were unable to export 'Availability Dashboard Report' as PDF and XLS. This issue has been fixed now.
- OpManager: Previously, users were unable to schedule 'Least and Average availability' for the Availability Dashboard Report. This issue has been fixed now.
- OpManager: Users can now navigate to the device snapshot page from HyperV Map.
- OpManager: Previously, Last Polled Bandwidth Utilization widget displayed 'NaN%' as value. This has been fixed.
- OpManager: STP Port Details has been added for devices falling under switch category.
- OpManager: Now, users can associate Device Template and Credential for devices from Inventory list.
- OpManager: Users can now manage, unmanaged and delete devices in BV list view page.
- OpManager: Previously, Interface threshold settings text inside interface snapshot page was wrong without units. It is corrected now.

Build No - 123113 - April 18, 2018

- Firewall : Previously Security Audit page was empty even though the report was generated. Now the issue is fixed.

Build No - 123112 - April 13, 2018

- OpManager: Option to export ﷺ as PDF and Excel has been included for devices.
- OpManager: During Test Monitor, while adding or editing File Monitor, the File path was not displayed . This has been fixed now.
- OpManager: Previously, for Folder Monitor Graphs, Y-axis units were not displayed. This has been fixed.
- General: Previously under Reports/Settings, when the page was either refreshed or when a new tab was opened, the last opened tab was hidden. This issue has now been fixed.
- General: While refreshing the Inventory page, some sub headers went missing. This issue has now been fixed.

Build No - 123111 - April 11, 2018

- General: Previously, Cookies were prone to Cross-site Scripting (XSS) Vulnerability and they were unsecure for HTTPS protocol. This issue has been fixed.
- General: Clickjacking vulnerability has been fixed.
- OpManager: Previously, unauthorized access to APIKey from APM Plugin was possible due to a vulnerability issue. This has now been fixed.
- OpManager: Modifying or Deleting users in OpManager was not being reflected inside APM Plugin. This issue has been fixed.
- OpManager: Previously, APM plugin was not getting started when OpManager with MSSQL Database was using Windows Authentication for database connectivity. This issue has been fixed.

Build No - 123110 - April 10, 2018

- OpManager: The alignment issue with the columns of Event Reports & Alert Reports - pdf is now fixed, so that xls and pdf reports match.
- OpManager: Operator cannot create/schedule a report anymore.
- OpManager: Previously, when SDP details contained special characters, there were issues while editing the 'Log a ticket' notification profile. This has been fixed now.
- OpManager: Issues with downloading PDF reports have been fixed.
- OpManager: 'No data available for this period' alert message is displayed when there is no data in integrated report.
- OpManager: Data older than a week is now available in the Interface report builder.
- OpManager: Under 'Audit' in Reports, users can now view the logs for scheduled operations.
- OpManager: Under 'Audit' in Reports, users can now view the logs for PDF & XLS export operations.
- OpManager: Audit Operation for Device Specific Deletion and Updation has been handled.
- OpManager: While raising event flood warning in OpManager, the message will now specify whether the flood is due to traps or event logs.
- OpManager: Previously, NCM count was not updated in the central server when deleted from the probe. This has been fixed now.
- OpManager: The NCM plug-in URL has been removed in DeviceExpert Change Management & DeviceExpert Operation Failure traps.
- OpManager: Previously, the custom category count of network device's alarms was displayed wrongly in the Network tab under Dashboard. This has been fixed now.
- OpManager: In version 11600, under Data Diagnostics, the Central & Probe table comparison page was missing previously. This has been fixed now.
- OpManager: While migrating from Linux Essential To Enterprise Edition, the migration failed due to the presence of '\' in MigrateToEnterprise.sh file. This has been fixed now.

Build No - 123109 - April 5, 2018

- OpUtils: Under Reports option, the missing reports of the DHCP has been added.
- OpUtils: Previously under Inventory, the option to edit a group of switches in SPM was not available. The issue is fixed now.
- OpUtils: Previously under OpUtils settings, the port history was in General tab. This is moved to cleanup policy tab now.
- OpUtils: Under Inventory, the category sub filter in port field has added an "administrative disabled/enabled" option.
- OpUtils: Previously under Inventory, the 'Add to SPM' option didn't display a proper Success/Error message in UI. The issue is now fixed.
- OpUtils: Under Inventory, the category sub filter "NIC type" table has been updated to match the IEEE oui list.

Build No - 123108 - April 4, 2018

- OpManager : XML External Entity (XXE) Processing attack affecting import of License, Script Template, Device Template and Workflow has been fixed.

- OpManager : Previously, in Mail Server Settings and Radius Server Settings, the password was being shown as "not_to_display". This issue has been fixed and now the password field will be left blank by default.
- OpManager : Cross-site Scripting (XSS) attack has been fixed.

- OpManager : SQL injection in Submit DB Query Page has been fixed.

Build No - 123107 - April 3, 2018

- NetFlow: 'Guest' user privilege has been added for NetFlow installation.
- NetFlow: The issue with the wrong bandwidth value appearing in the "Overview" tab in Interface/Interface Group/IP Group snapshot when custom time period is selected has now been fixed.
- NetFlow: Enhanced raw data dump to avoid increase in tmp/flow_log.txt file size.

Build No - 123106 - April 2, 2018

Bug Fixes in NCM:

- 4439431 - Know which config version is baseline in config diff view. (The Config version that is baseline is mentioned as 'Baseline').
- 4550432 - Layout of NCM Nipper reports has been revamped.
- 4571167 - Issue while finding SysOID has been fixed.

Enhancements in NCM:

- View SNMP profiles from System Location and Description pages.
- Select specific SNMP profiles to be used while updating location and description details for devices.
- Add devices as unmanaged if the total number of devices exceeds the license limit.
- More devices are supported by default with the additional SysOIDs.
- I18N keys are now available.
- Minor UI enhancements.

New feature in NCM - Terminal:

- Terminal page can be used to open a terminal to any device in the network.
- Terminal connection to the inventoried devices can be opened under *Settings >> NCM >> Inventoried*.
- For devices that support terminal function but are not included in Inventory, the session can be initiated by *Settings >> NCM >> Terminal >> Custom*.
- All the terminal sessions will be logged and can be viewed in *Settings >> NCM >> Terminal >> Audit History*.

Build No - 123105 - March 29, 2018

- NCM: Network Configuration Manager now scales more. A single server supports 10000 devices. If you need to manage more than 2000 devices, configure the number of parallel job count to a minimum of 50 in 'Settings >> NCM >> Server settings' and restart the server.
- NCM: You can trigger a configuration backup operation for any number of devices in a single schedule in 'Settings >> NCM >> Schedule'.
- NCM: You can now apply the credentials for any number of devices successfully from 'Device Group' page under Inventory section.

Build No - 123104 - March 28, 2018

- OpManager: Previously, 'Schedule Report' did not work for other languages. This issue is now fixed.
- OpManager: Previously, the 'Schedule Report' option was missing in the snapshot pages of all performance monitors, availability, interface metrics, Packet loss, response time, Device(at - glance reports), URL and Script Templates. This has

been fixed now.

- OpManager: SDP Device asset information will now be in the snapshot page of OPM for all the devices synced with SDP.
- OpManager: The issue with the ping.properties file to view device availability for non-english installations, is now fixed.

Build No - 123093 - March 26, 2018

- OpManager: 100% CPU Utilization issue due to AppSMS has been fixed.

Build No - 123092 - March 22, 2018

- Firewall : Default reports enhanced with drill down option to second and third level. Particularly for 'Unknown Protocols', you can drill down up to raw log level.
- Firewall : 'End User' feature moved to 'Firewall Inventory' tab. You can get 'End User' details from 'Users' Tab.
- Firewall : 'Rule Management' and 'Compliance Reports' files stored in Firewall Analyzer server directory are encrypted now.
- Firewall : User information is encrypted at the database storage.
- Firewall : 'CSV Export' option is available for 'Rule Management' reports.
- Firewall : 'Scheduled Report' mail format is enhanced to show properly aligned mail content.
- Firewall : Support - 4458020: In 'Change Management' report, new column has been added to show the IP address of user from which he did configuration changes.
- Firewall : Support - 4429668: 'Admin' report is available for Huawei Firewall. You can view user login, logout and command executed reports.
- Firewall : Support - 4477638: Fixed the issue of incorrect data shown in 'Policy Optimization reports' for some PaloAlto devices.
- Firewall : Support - 4519337: Fixed the issue of not fetching configuration files from SonicWALL firewalls due to incorrect SCP command.
- Firewall : Support - 4497009: Fixed issues in 'Denied Events' and URL log parsing for Juniper SRX devices.
- Firewall : Support - 4510780: Fixed the issue of wrong time period shown in i-Filter reports data, due to non-processing of time stamp available in the logs.
- Firewall : Support - 4496764: Fixed the issue of mismatch in rules count of unused rules and total rules displayed for some PaloAlto firewalls.
- Firewall : In PaloAlto firewall 'Policy Overview' page, no data was displayed when clicked on some source and destination objects. This issue is fixed.
- Firewall : Fixed the issue of no data display in 'Total Bytes' column in Trend Micro device reports, due to non-processing of byte value available in the logs.

Build No - 123091 - March 20, 2018

- OpManager: Added an option to switch menu bar alignment into vertical or horizontal.
- OpUtils: The DHCP Scope Monitor of the SNMP tool is enhanced in a way that helps to monitor the DHCP scopes of a given IP address or DHCP server name and scans intermittently based on the scheduler profile created by the user. It also provides an email alert to the user when an IP address in the DHCP scope falls below a specified count.
- OpUtils: The Network Monitor tool is updated to monitor the response time and packet loss of selected devices, creates a history of details that can be viewed by the user.
- OpUtils: The System Details Update of Network monitoring tool has been enhanced in such a way that it is made possible to edit system details of specific devices like sys name, sys location, sys contact and update these details from the remote device itself. The updated status can also be viewed from the remote device.
- NCM: 100% CPU Utilization issue due to Syslog flooding has been fixed.
- NCM: 100% CPU Utilization issue due to Fortigate Firewall backup has been fixed.

Build No - 123090 - March 19, 2018

- General: OpManager now supports SMS notifications via HTTP SMS Gateway and SMPP server.
- General: 4028582 - Now, SMS server settings can be deleted in the UI.
- General: Previously, server secret was visible in Radius Settings. This option is now hidden.
- General: User access Level can be changed by Operator using API.This issue has been fixed.
- General: 4358794-Product version showed undefined in UI when NCM folder existed under OpManager. This issue has been fixed.
- General: 4447605,4421517,4405385,4382147-Option to apply .XML file type in license has been added.
- OpManager: 4479975,3924891- Previously in Script Template, the html content had visibility issues. This has been fixed.
- OpManager: Device name was not being updated when Last Polled returned null value in CPU/Memory/Disk and Bandwidth utilization widget. This issue has been fixed.
- OpManager: Previously, Script Template had XSS vulnerability issues. This has been fixed.
- OpManager: A new tray icon has been implemented for essential, central and probe setup.
- OpManager: Under User Management, the user photo was not deleted from the saved folder even when the user profile was deleted. This issue has been fixed.
- OpManager: Option to enable / disable DB query from system settings screen has been added. Based on the option selected, the DB query inside support is shown/hidden to the user. By default, the option is disabled.
- OpManager: Partial masking of the API Key in UI has been implemented.
- OpManager: Audit implementation for various modules like rebranding, Add/Edit/Delete Domain, Notification, License and Support has been done.
- OpManager: 4244642 - Previously, Clickatell notifications were not working and displayed "Clickatell authentication failure" error message. This issue is fixed now.
- OpManager: 3893820 - SMS Notifications were not received when multiple mobile numbers were given in the SMS Notification profile.
- OpManager: 4252424 - Failover: For a business view created in the primary server with a custom image as background, the image was not loaded when the standby server took over. This issue is now fixed.
- OpManager: 125561 Failover: Primary server's conf files were not copied to Secondary. This issue is now fixed.
- OpManager: 3835548 - User created dashboards can now be renamed in OpManager.
- OpManager: 4032958 - On embedded 'Heat Map widget', the tooltip was not displayed. This has been fixed now.
- OpManager: 3660586 - Updated commons-collections jar to version 3.2.2 due to 'Remote Code Execution' vulnerability in older version.
- OpManager: 4113354 - In the 'Send Email Notification' profile, the length of 'To Email Address' field is now increased from 255 to 500 characters.

Build No - 123086 - April 19, 2018

- General : Failed to load the client if the MSSQL database collation is 'Danish_Norwegian_CI_AS'. This issue has now been fixed.

Build No - 123084 - March 15, 2018

- OpManager: Thresholds for Response time and Packet loss can be set for multiple devices.
- OpManager: New Availability graph has been introduced in Device snapshot page->Availability dial->History to show the device up, down status using a line graph.
- OpManager: GPS coordinates will be shown in Device summary tab if the device has been added to Google Maps.
- OpManager: Previously, users were unable to add string monitor with a string threshold in Device Templates. This is now fixed.
- OpManager: The "Configure Interface" option was not displayed for routers. This has been fixed now.

- OpManager: Interface Reports are now available by default on Interface snapshot menu.
- OpManager: SNMP text was displayed for Default dials for availability, Response time and Packet loss. This has been fixed now.
- OpManager: Users can able to discovery and add device without credentials in OpManager.
- OpManager: Previously, SNMP v1/v2 credential mismatch error throws while adding credential in discovery wizard page. This has been fixed now.
- OpManager: Search option has been added for interfaces in device snapshot page.
- OpManager: Table values were not displayed for interface error, discard rate,Traffic Utilization graphs. This has been fixed now.
- OpManager: Previously, "Export as PDF" did not work for all the time periods for the "Interface Bandwidth Report" and the "Interface At a Glance Report". This is fixed now.
- OpManager: Previously, Interface graph time format issue occurred when a period 7 days or 30days, was selected. This issue is fixed now.
- OpManager: Users can now navigate to the device snapshot page from the interface snapshot page toolbar.
- OpManager: Previously, users were unable to align custom html widget, when multiple iframes were called. This has been fixed now.
- OpManager: While creating a business view in IE, navigating to the Multi select mode made the device name disappear. This issue has been fixed now.
- OpManager: XSS vulnerability issue while importing Additional fields has been fixed.
- OpManager: SQL Injection vulnerability has been fixed for Downtime scheduler.
- OpManager: Downtime report not showing the status of currently down devices has been fixed.
- OpManager: Previously, wireless devices were not getting pushed to NCM.This has been fixed.
- OpManager: Previously, when a user generated weekly reports, the days of the week were plotted as numbers. This issue is now fixed.
- OpManager: The issue with the ping.properties file to view device availability for non-english installations, is now fixed.

Build No - 123083 - March 12, 2018

- General: Dashboard loading has been revamped and optimized for better performance.
- General: In the Login page, Iphone/Android and Ipad application download links have been included.
- General: License expiry information in header had a few alignment issues. This has now been fixed.
- General: User Icon with product details and about information has been moved to right top corner.
- General: In the Inventory page, product based tabs have been moved horizontally.
- General: Sign out option has been moved from Quick links to User details menu.
- OpManager: In alarm details page, Alarm actions has been moved from Actions menu to Details page .
- General: Support icon has been added for (Mail, Apply license, phone number, SIF, User guide, Videos, Service pack, ThreadDump, DB Query & view Logs) links.
- General: In support page, the Query page under DB Query will be opened in a new window without ember

Build No - 123082 - March 8, 2018

- OpUtils: Previously under Inventory, the port option does not show any differentiation for connected devices. This issue is fixed now as the connected devices are differentiated based on colours such as orange for virtual IP, grey for multi MAC port and yellow for stacked port.
- OpUtils: Previously, only OpManager API has called for adding switches and hence there was an issue in adding switches in SPM. The issue is fixed now.
- OpUtils: Previously while adding devices, the device explorer option under Cisco tools didn't display a proper error message like 'Not a CISCO device' . The issue is fixed now.
- OpUtils: Previously, the Proxy ping option under tools didn't show any proper images for scan results. The issue is fixed now.

- OpUtils: Previously under Oputils option, the field 'Clean up policy location' was not mentioned in Publish directory of IPAM and SPM. The issue is now fixed.
- OpUtils: Previously under sort summary, when clicking on snapshot page, API was called twice. This issue is fixed now.
- OpUtils: Under reports, a field called 'Custom Period' has added in 'Port by Operation Status Last Change Time' report.
- OpUtils : 4249914, 4010627 - Under Inventory, the option to add switches by importing a CSV file was included.

Build No - 123081 - March 7, 2018

- NetFlow: The issue related to export to PDF and mail has now been fixed and enhanced.
- NetFlow: Added an option to export to PDF and mail for Individual graph reports.
- NetFlow: Added an option to export to PDF and mail for DPI snapshot widgets and widget drill down reports in the inventory.
- NetFlow: Added an option to change the graph type for time series graphs in the inventory.
- NetFlow: Inventory page related bugs have been fixed.
- NetFlow: Added an option to select Business hours in the Last Quarter time period while scheduling reports
- NetFlow: SFlow flow format for multiple MPLS can be added now.
- NetFlow: Added an option to configure billing with base cost as zero.
- NetFlow: The loading issue in the Dashboard with NBAR App widget has now been fixed.

Build No - 123080 - March 5, 2018

- OpManager: Previously, installation failed when the installation/default folder name contained spaces or when OpManager was installed under the location C:\Program Files . This has been fixed now.
- OpManager: In Probe, under settings, 'Failover details' tab was not displayed. In Central server, Settings-> Configuration-> Probe Details, Secondary server and its details were also not displayed. Now both the issues have been fixed and they have been displayed in the respective UI.

Build No - 123079 - March 1, 2018

- Even after deleting the MSSQL Instance from the device in the OpManager, false alerts of that mssql service instance being down were getting raised. This has been fixed now.
- The vCenter discovery failed if any VM replica was created with duplicate UUID as of the existing VM in OpManger. This has been fixed now.
- In the case of both vCenter and ESX based monitoring done from OpManager, under Inventory view of Virtualization, the vCenter/Host filter was showing incorrect data. This has been fixed now.
- Although invalid VMware credential was given during vCenter/ESX discovery, the device was getting added as Unknown (normal device). This has been handled and now device will be discovered and added in OpManager only if valid credential is selected.
- If tab space '\t' was included in any monitor name, Monitors page inside the Device Snapshot page was shown blank. This has been fixed and further '\t' space will not be allowed in the monitor name.
- It was not possible to edit custom WMI Monitors like Disk Monitors with special character '\' in its instance name. This has been fixed now.
- While saving URL properties from URL Snapshot, the page was redirected to Settings page instead of the previously selected URL Monitor page. This has been fixed now.
- While trying to add Service Monitors from Device Snapshot page, clicking ﷺCancel redirected the page to Settings page instead of the previously selected Device Monitors page. This has been fixed now.
- While trying to associate devices with File/Folder monitor templates, the eligible devices list shown was not sorted in the alphabetical order. This has been fixed now.
- The validation of various Threshold value-specific fields was not done for File/Folder Monitors addition. This has been handled now.
- For Hardware Monitoring in some cases, only single sensor for FAN Category with multiple instance was getting added and displayed in device snapshot page. This has been fixed now.

- In Hardware page under device snapshot page, the units were not shown under Hardware Monitor graph. This has been fixed now.
- XenServer discovery failed if there were no VM's inside the pool and only Templates existed. This has been fixed now.
- Adding/Updating Event Logs Monitors from Settings page is failed, if rules or logs contained special character '\'. This has been fixed now.

Build No - 123078 - February 27, 2018

- OpManager: Under Alarms, Clear trap events were raised even though suppress alarm was applied to the device. This has been fixed now.
- OpManager: Trap Forwarder automatically stopped while restarting OpManager Service. This has been fixed.
- OpManager: Trap Processors page did not have any description. This has now been fixed.
- OpManager: In 'Load from Mibs' page, the default info message was missing when copying mib file to OpManager/mibs. This has now been fixed.
- OpManager: Trap Forwarder was not showing running/stopped status message. This has been fixed.
- OpManager: The trap description column showed 'More Link' (Old client) in 'Add traps' page from 'Load From Mibs'. This has been fixed.
- OpManager: Last polled value was not being sent in 'Send trap using Notification Profile'. This has been fixed.
- OpManager: Under Unsolicited trap, specific type field was not shown when clicking on 'Create trap processor'. This has been fixed.
- OpManager: Previously added traps in 'Add trap page' from 'Load From Mibs' could not be disabled and selected by default. This has now been fixed.
- OpManager: Serial number looked odd in 'Load from traps' page. This has been fixed.
- OpManager: Search option was not provided in 'Add traps from mibs' and 'Load from mibs'. This has been fixed.

Build No - 123077 - February 23, 2018

- OpManager: Users can now mask/unmask the data of other modules like Flow Analysis, Config Management, Firewall Log Analysis, IP Management, Packet Analysis and Application Monitoring in the UI, by configuring System Settings.

- OpManager: 4465019,4476757,4530031 - On DB Disconnection, the license page displayed a wrong warning message on IPSLA monitors. This has been fixed now.

- General: Previously, an Operator user was able to access log files using direct API's (/apiclient/ember/index.jsp#/ViewLogs/stderr_0.txt) and URLs (/logs/stderr_0.txt). This vulnerability issue has been fixed now.

Build No - 123076 - February 22, 2018

- OpManager: Alarm - Workflow logs can now be categorized into alarm specific and device specific ones on the 11.6 struts client.
- OpManager: Workflow status bar has been given under the Workflow Tab now.
- OpManager: While clicking the PDF option repeatedly, the duplicate element gets created. This issue is fixed now.
- OpManager: In the device snapshot page, authorization to access workflow logs for operator log-in failed. This issue is now fixed.

Build No - 123070 - February 21, 2018

- General : SQL injection vulnerabilities in Servlet's API has been fixed.

Build No - 123069 - February 19, 2018

- OpManager: If a logged in user's account is deleted by an admin, the user will be notified and logged out automatically.
- OpManager: The settings option 'Add/Remove widgets in default dashboard' under System Settings was not preserved during service restart. This

is fixed now.

- The following vulnerability issue has been fixed in OpManager:
    - Unauthenticated Blind SQL Injection via /servlets/FailoverHelperServlet.
- NCM: Backup operation fails for the following device type in builds 12300 to 123064 due to Maverick upgrade. Device backup command response stops in the middle of an execution and expects an enter key (LineFeed) to send the remaining response. This issue has been fixed in this release and now you are able to backup this device type without any issues.
    - Device type: Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),Version 03.07.03E RELEASE SOFTWARE

Build No - 123068 - February 16, 2018

- OpManager: Previously, if a custom category was associated to a device in non-english language web client, the device snapshot page did not open. This has been fixed now.
- OpManager: In the inventory list view page, the device IPs were not in order when sorted by IP Address. This has been fixed now.
- OpManager: Previously, the device IP Address was not available in the Device/Interface Availability reports. This has been added now.
- OpManager: Previously, when a custom category associated to a device was deleted, the device was listed as unknown instead of the parent category. This has been fixed now.

Build No - 123067 - February 14, 2018

- OpManager: Device specific workflow logs are available on the snapshot page now.
- OpManager: Jump To ServiceDeskPlus from OpManager has been handled now.
- OpManager: Previously, retrieving services for different domain users in workflow tasks was not possible. This issue is fixed now
- OpManager: Previously, users were unable to add/edit/update workflow in some special cases like HTML content being present in script body. This issue is fixed now.
- OpManager: Under Workflow tasks, the Reboot and Shut down options did not work properly due to client issue. This has been fixed.
- OpManager: The unwanted scroll bar displayed in the pdf file is fixed now.
- OpManager: Previously, users were unable to schedule report after canceling a monthly scheduled report/weekly scheduled report. This issue has been fixed now.
- OpManager: Usability issue - The error message 'Schedule Report name already exists' was displayed while creating the report name itself. This issue is now fixed.

Build No - 123066 - February 13, 2018

- OpManager: 4175032 - Email notifications are triggered while the Primary server gets back to Active mode and the information is provided in the banner whether the running setup is the primary or the secondary server.
- OpManager: 2826598 - Previously, users were unable to install OpManager as service in RedHat 7.x machines. This issue is now fixed.
- OpManager: 4243641 - Previously, credential test passed but the data collection in some CLI devices failed. This issue is now fixed.
- OpManager: 4368835 - While restoring PGSQL backups, duplicate key and foreign key violation issues have been fixed now.
- OpManager: 4218544 - During PGSQL to MSSQL migration, the time round off issue causing the duplicate key issue on dynamic tables, is fixed.
- OpManager: Previously, BCP file location was not loaded to the bin directory automatically. This is fixed now.

- OpManager: Previously, the secondary server started even when there was a mismatch in the build number with the Primary server. This has been handled now.
- OpManager: DBConfiguration.bat - Previously, while providing a different DB Name displayed "OpManagerDB exists already" error. This is now fixed.
- OpManager: Proper encoding for Chinese messages have been provided now.
- OpManager: The DB restore issue occurring while using remote PGSQL DB with the password, is now fixed.

Build No - 123065 - February 9, 2018

- OpManager: Minor enhancement and bug fixes have been provided for a seamless migration from the Essential Edition to the Enterprise Edition.
- OpManager: The SNMP ping tool under Settings-> Tools now has the option to choose devices and credentials that are already added in the product. You can also manually enter the device name or IP address by clicking on the (+) icon.
- OpManager: The MiB Browser tool under Settings -> Tools now has the option to choose devices and credentials that are already added in the product. You can also manually enter the device name or IP address by clicking on the (+) icon.

Build No - 123064 - February 8, 2018

Enhancements:

- FWA: Provision to configure each device in the Inventory itself. For a single device, you can configure Report, Alert, Device Rule, and SNMP in one place.
- FWA: Ad-hoc reports are listed in the drill down page of 'Device' under Inventory.
- FWA: 'Device' summary widget under Inventory, is enhanced to show more device configuration options
- FWA: Cloud Control Repository updated and new services added.
- FWA: 'No Data' message will be displayed in widget header, if a widget has no data to display. If the widget has data, total number of rows will be displayed.
- FWA: Reduced the 'Inventory' page loading time.
- FWA: By default, indexing enabled for Security Logs.
- FWA: Support Id: 4400799 - New widget added under drill down page of 'Cloud Control'. The widget shows all source IP addresses, who accessed the corresponding 'Cloud' service.

Issue Fixes:

- FWA Support Id: 4223153 - Bandwidth Alert profiles created with criteria 'mbps' were not working. This issue is fixed
- FWA Support Id: 4223153 - URL report, date and priority parsing issues of pfSense firewall is fixed.
- FWA Support Id: 4275699 - When one Juniper SRX device was added it was displayed as two devices. This was due to absence of firewall name in some syslogs. This issue is fixed to show it as a one device.
- FWA Issue Id: 124479 - Earlier user couldn't edit the report filter while creating 'Report Profile'. Now 'Edit' option provided for the report filters to fix the issue.
- FWA Issue Id:126112 - After selecting custom time period in 'Inventory' drill down page, the end time was not shown properly. This issue is fixed.
- FWA Issue Id:126077 - In 'Add Credential Profile' page, 'Device Type' option is moved up near 'Protocol' for better accessibility.
- FWA Issue Id:126332 - In 'Device Rule' list page, sorting of any column, removed 'Fetch Rules' and 'Security Audit Report' icons. This issue is fixed.

- NCM: Alert message for existing device while adding non SNMP devices.

- NCM: Time based report for configuration change.
- NCM: 4318485: Schedule Security Audit Report is now added
- NCM: Now you can view compliance policy violation widget in dashboard
- NCM: View configuration file while uploading labeled configuration.
- NCM: Help document now available on how to execute Configlet.

Build No - 123063 - February 7, 2018

- General: 4209070 - Error code and error message related to mail user authentication from SMTP mailer will now be displayed in the UI, upon testing mail from Mail Server Settings
- General: 4238670 - Under Proxy Server Settings, the 'NoProxyFor' field length is now increased from 255 to 1000 characters.
- OpManager: 4389441 - Under Send Email notification profile, the issue with adding other language characters and HTML tags in the message field has been fixed.
- OpManager: 4397025 - Previously Email based SMS was received as Raw text because of Multipart/Mixed content type. This issue has been fixed. Email SMS will now be sent as plain/text content.
- OpManager: 4335844 - For Traps with Failure Component not ending with "_trap", Notification Profile was not triggered previously. This has been fixed.
- OpManager: 4335844 - Notification Profile was triggered for trap with clear severity, even when the "notify me when clear" profile criteria was not selected. This has been fixed now.
- OpManager: 4139976,4099988 - In Linux Installation, Command arguments in Run Program and Run System Command Notification Profile were getting truncated with space previously. This issue has been fixed now.
- OpManager: 4499794 - Interface specific message variables in Notification profile were not replaced with proper values while sending Notification Alerts. This issue has been fixed now.
- OpManager: 4369593- Uploading MIBs with .txt format in MIBBrowser Tool is supported now.

Build No - 123062 - February 5, 2018

- NetFlow: Now supports Meraki's latest firmware upgrade.
- NetFlow: Removed product version number in the subject line of alert mail.
- NetFlow: Added an option to select number of records as "30" for consolidated report.
- NetFlow: Issue with showing the incorrect cost unit while editing billing profile has been fixed.
- NetFlow: Added the value for MIN and MAX traffic in AS View.
- NetFlow: Issue with generating CSV Report for WLC under Schedule Profile has been fixed.
- NetFlow: Issue with deleting WLC device from inventory page has been fixed now.
- NetFlow: Issue with listing interfaces in Qos drill down view has been fixed.
- NetFlow: Removed the Free Version from the installation shield.
- NetFlow: Issue with listing of interfaces in the Interface widget under Device snapshot has been fixed now and changed to a maximum of 10 interfaces.

Build No - 123057 - January 31, 2018

- OpManager: Outage history details are also generated as a PDF in Availability Statistics Report.
- OpManager: Availability distribution alternatively displaying blue bar (not-monitored status) has been fixed.
- OpManager: Under Interface Snapshot, option to open a new or separate tab has been added in the Interface graph page.

- OpManager: Schedules were not listed under Downtime Scheduler. This has now been fixed.
- OpManager: In downtime scheduler, previously the schedules could be deleted or disabled when they were running. This has now been fixed.
- OpManager: Under Interface Graphs, 'Interface Display name' has been changed to 'Interface name'
- The following vulnerability issues have been fixed in OpManager:
  - DDI-VRT-2018-02 &#65533; Unauthenticated Blind SQL Injection via /servlets/RegisterAgent
  - DDI-VRT-2018-03 &#65533; Unauthenticated Blind SQL Injection via /servlets/StatusUpdateServlet and /servlets/AgentActionServlet
  - DDI-VRT-2018-04 &#65533; Multiple Unauthenticated Blind SQL Injections via /embedWidget
  - DDI-VRT-2018-05 &#65533; Unauthenticated XML External Entity Injection via /SNMPDiscoveryURL
  - DDI-VRT-2018-06 &#65533; Unauthenticated Blind SQL Injection via /unauthenticatedservlets/ELARequestHandler and /unauthenticatedservlets/NPMRequestHandler
  - DDI-VRT-2018-07 &#65533; User Enumeration via /servlets/ConfServlet.
-

Build No - 123056 - January 30, 2018

- OpManager: In device snapshot page, the option to delete Event Log Rule Monitors in bulk has now been added.
- OpManager: Under Exchange Monitors tab in device snapshot page, grouping of Exchange Monitors was not done in Central & Probe installations. This has been fixed now.
- OpManager: While adding Service Monitors, values beyond the range of specified Port values were allowed for Port number. This has been fixed now.
- OpManager: In Virtualization Dashboard, the units of the Monitors were not shown for the widgets. This has been fixed now.
- OpManager: Previously, Associating Event Log Monitor to a device was not working if the event log belonged to a Rule type that has not been associated to that device. This has been fixed now.
- OpManager: Under Virtual Servers, Graphical(Map) View showing the link between Hosts/VM/vCenter for VMware/HyperV/Xen Servers from the snapshot pages has now been added.
- OpManager: Previously, Export to PDF/XLS option in Hardware Monitor Reports returned an empty file. This has been fixed now.
- OpManager: Previously, the Schedule Report option under Hardware Monitor Reports was not working as scheduled with the selected parameters. This has now been fixed.
- OpManager: In Device Snapshot page, the Legend Summary of the Hardware graph was not available. This has been added now.
- OpManager: In Alarms Inventory View, the option to filter VMware Events separately has been added.
- OpManager: In the Add Performance Monitors Page from Device snapshot and Device Template pages, the specific Vendor monitors and WMI monitors, if applicable, were not listed for addition. This has been fixed now.

Build No - 123055 - January 25, 2018

- Advanced Configuration Search in Inventory page with multiple search conditions.
- Shared Device Template and Request New Device Templates options are provided.
- #4224773: List view of devices associated to each credential profile
- Credential profile is now moved under NCM Tab in settings.
- Now access & edit system properties from NCM GUI.
- Device Group widgets with status of Backup, Compliance and Conflict status bar charts now available in inventory.
- Execute Configlets option is provided in the select menu in Devices Inventory at the top right corner.
- Snapshot Configlets without parameters will be executed directly without prompting for parameters.
- SSH Settings: Allow/block Ciphers, Key Exchange and HMACs in product settings page.

- 'User audit clean up' option is now available in Database Administration settings.

Build No - 123054 - January 24, 2018

- General: 4396270 - Self Monitoring - Whenever the server is restarted after low Disk Free Space alert, the monitor shows wrong alerts, even when the required free space is maintained. This issue has been fixed now.
- OpManager: 4351130 - The processing time of notification profile was longer due to many(1000+) trap monitors being selected in the Profile Criteria, causing delay in Mail alerts. This issue has been fixed now.
- OpManager: 4274768 - While loading MIBs from the MIB Browser, the error message is now displayed with the MIB standard version.
- OpManager: In device snapshot page, Audit History filters have been made installation/device type specific.
- OpManager: API Access report's timezone has been changed from UTC to system timezone.

Build No - 123053 - January 19, 2018

- OpManager: Under business views, the link traffic status colors did not change based on the utilization previously. This issue is now fixed.
- OpManager: In the business view widget, the links to access the devices were missing. This issue is fixed now.
- OpManager: Auto-refresh was not working for the dashboards when any tabs from Applications under Servers were clicked. This has been fixed now.
- OpManager: In Business Views created in before version 12(old UI), during mouse over, the device details pop-up in the dashboard continued to display until the page was refreshed(in version 12 and above). This issue is fixed now.
- OpManager: Previously there was no option to change the name of the Rack and Floor View. This is fixed now.
- OpManager: The issue with the Business view widget resizing is fixed now.
- OpManager: While accessing OpManager web client from remote servers, there was a time discrepancy issue with graph and data display when hosted on UTC time zone. This has been fixed now.
- OpManager: Under Link Properties of Business Views, while getting status from NFA The color of the connection mismatched with that of the legend. While clicking on the connection if the utilization was 5% for IN and 11% for OUT, the connection was displayed in green instead of blue. This is now fixed.
- OpManager: Under Business View, upon mouse rollover on NFA links, it did not display the selected data type in the link Properties of the connection. This has been fixed now.
- OpManager: Under Business View, NFA Source and destination links were not retained while editing the link. This issue is now fixed.
- OpManager: In Network discovery, the addition of Partition and disk space monitors failed for CLI credentials. This issue is now fixed.
- OpManager: In VLAN graphs, the data displayed in the graph was not in order. This issue is fixed now.
- OpManager: Under Monitoring tab, in Performance monitors, the description was not displayed for custom monitors. This issue is now fixed.
- OpManager: Under Monitoring tab, in Performance monitors "Delete" option is now added to custom monitors.
- OpManager: In Device rediscovery, Unmanaged devices cannot be rediscovered now.
- OpManager: In Quick Configuration Wizard, Dependency devices listing was not sorted previously. This issue is now fixed.
- OpManager: In Device Templates, the issue with matching SysOID criteria and Custom OID criteria are fixed now.

Build No - 123052 - January 17, 2018

- OpManager, NetFlow Analyzer, Network Configuration Manager, Firewall Analyzer and OpUtils: The possibility to fetch user

details through ConfServlet has been fixed and is secured now.

- NetFlow: Schedule reports for report period as "Previous Week" shows data for current week. This issue has been fixed now.

Build No - 123051 - January 12, 2018

- OpManager: Previously, under group chat option, the Business view users were able to see the alarm discussions for all devices including the devices for which they had no access to. This issue is fixed now.
- OpManager: Previously, the Discussions option under group chat had an issue in viewing the full thread. This issue is now fixed.
- OpManager: Previously, in Business view option, the devices, which were not monitored, were showing their status as clear. This issue is now fixed.
- OpManager: Previously, the option to edit a link in a Business view was not working. This issue is now fixed.
- OpManager: Previously, the Business view status under maps which showed "wrong severity" is fixed now.
- OpManager: Previously, in business view option, the list view device status was displayed as "unknown" instead of unmanaged. This issue is now fixed.
- OpManager: Previously, in business view option, the map view device status was displayed as "unmanaged" instead of "device not monitored". This issue is now fixed.
- OpManager: Under Maps, the device status was displayed as "clear" instead of the "device not monitored" in the graph of business views. This has been fixed now.

Build No - 123050 - January 9, 2018

- Under Alarms tab, I18N for "No Data" & "No Alarms for selected Period" was not present previously. This issue is now fixed.
- Under Reports, the sorting feature was not working. When the first column (min) was sorted, the other columns (max,avg) change randomly. This issue is now fixed.
- Previously, sorting feature did not work for device names in the "DISK USAGE BY DRIVES" report. This issue is now fixed.
- Under reports, while selecting the "last date" in the monthly schedule, the scheduler was not able to identify the last date for that particular month. This issue is now fixed.
- After upgrading to the latest version, the scheduled reports were not listed. This issue is now fixed.

Build No - 123049 - January 8, 2018

- OpUtils: Filters have been added in the device snapshot pages of Ports and IP Address.
- OpUtils: 4249914 - Under reports, the "Export" option is now more visible on the top of the page.
- OpUtils: Previously in the rogue dashboard, 1000 recently discovered devices were displayed. Because of this, the page loading time had increased. This issue is fixed by reducing the number of recently discovered devices from 1000 to 100.
- OpUtils: Under Inventory, wrong tab details were displayed under sub filters, in the left side of the page. This is now fixed.
- OpUtils: 3740821 - Under port snapshot page, the field "Physical Location" can now be edited.
- OpUtils: 4120052 - Previously, DHCP Scopes scanning was not completed due to null values in clientinfo. This issue is now fixed.
- OpUtils: Previously, when license count was 3, users were able to add 4 users (Including admin), but then OpUtils displayed the license activation page in the next login session. This issue is now fixed to add only 3 users including admin.
- OpUtils: After deleting DHCP, the page was not refreshed. This issue is now fixed.
- OpUtils: Under IP address tab in the inventory, the asset tag data was missing previously. This is now fixed.

Build No - 123048 - January 5, 2018

- OpManager: The Delete/Exit action performed on any process template was executed on all the process templates with the same name but different path arguments. This has been fixed, and now the action will be performed only on that specific process.

- OpManager: Language localization has been done for threshold column values inside the performance monitors Page
- OpManager: Under downtime widgets, the downtime of URLs, services, devices, WAN Links were displayed as zero seconds. This issue is fixed now.
- OpManager: For default virtual reports, the user was able to view devices that he did not have access to. This issue is fixed now.
- OpManager: In some cases, the discovery of HyperV-Servers failed when the same HyperV-Server was deleted and discovered again in a short span of time.This has been fixed now.
- OpManager: If the user tried to dissociate all the devices associated to a certain Windows Service Monitor, a false alert was displayed to the user to select at least one monitor. This has been fixed now.
- OpManager: While adding a new windows service monitor from the device snapshot page, the consecutive value and restart actions value were set to default values for the already associated monitors to that device.This has been fixed now.
- OpManager: It was not possible for the user to add any recently deleted VMware/HyperV/Xen monitor to that specific vendor based virtual server from the snapshot page. This has been fixed now.
- OpManager: HyperV specific monitors were added to the normal physical server for Microsoft devices from device snapshot page. This has been fixed now.
- OpManager: While mapping any new device that was monitored in OpManager to "Not Monitored VM's" in a vCenter/ESX Server snapshot page, the existing display name of that device was changed. This has been fixed now.
- OpManager: While adding a new windows service monitor from the device snapshot page by getting a new list from the actual device, the existing associated monitors were deleted from the OpManager when those monitors were not available in the actual device. This issue is now fixed.
- OpManager: The inconsistency in allowing some special characters in the URL Display when added during CSV file Import and from the web client is now fixed.
- OpManager: Previously, while adding URL monitors, the value 0 was allowed for "Time-Out" and "Consecutive Times" field. This has been fixed now.
- OpManager: While associating a URL Template to the device using RuleEngine, the consecutive time value for the monitor was not updated. This has been fixed.
- OpManager: While configuring a URL monitor from the device snapshot page and the URL template page, the "Request Parameters" field did not accept more than one parameter. This has been fixed now.
- OpManager: In the Application Monitors page, for AD/Exchange/MSSQL value with repeated digits for threshold or poll interval fields were not allowed. This has been fixed now.
- OpManager: Previously language localization was not done for the "Path Not Found" text while executing "Test Monitor" from the "Add Folder Monitor" page. This has been fixed now.

Build No - 123047 - January 4, 2018

- NetFlow: The framework for mail generation in NetFlow Analyzer has been revamped.
- NetFlow: The issue with licensing in attacks has been fixed.
- NetFlow: In Attacks module, time zone has been added in message for SMS alert.
- NetFlow: Language translation issue in Attacks snapshot has been fixed now.

Build No - 123046 - January 2, 2018

- OpManager: 4085539 Previously "Export to PDF" and "Export to XLS" option was missing in script monitors' graph. This has been added now.
- OpManager: 4283982 Previously users were able to connect to the device terminal only for routers and switches. Now, the device terminal can be connected from OpManager's device snapshot page, if the NCM credentials are available.
- OpManager: Earlier users were able to edit syslogs while the forwarder was running. This issue is now fixed.
- OpManager: 4277543 While associating script templates, devices can now be sorted by "device name".

- OpManager: 4271014 Linux memory utilization command has been changed to support Red Hat Enterprise Linux 7
- General: SQL injection vulnerabilities in unauthenticated servlets has been fixed.
- General: 4409775 The HTTP PUT method is now blocked, in Tomcat and the vulnerability is fixed.(Refer - CVE-2017-12617)

Build No - 123045 - December 28, 2017

- Firewall: i-FILTER Version10 device logs support.
- Firewall: Previously drill down option was available for tables only. Now user can drill down graph and see relevant data in reports.
- Firewall: X and Y axis labels added in all graphs.
- Firewall: In Live Syslog viewer, Filter option provided for source IP. Now Live Viewer page can be filtered to show syslogs from a single firewall.
- Firewall: In Inventory drill down page, start and end time is shown near clock icon for all time periods.
- Firewall: System settings page is added to Settings. This includes General and Logging configurations.
- Firewall: Previously when custom time period was selected, the time range was not shown. Now the issue is fixed and proper time range is shown.
- Firewall: No data in all reports for Sonicwall Device. The issue was, few logs had large duration value. Due to this, an error occurred and data was not dumped. Now the issue is fixed.
- Firewall: Live traffic drill down data was fetched for a full day before. Now the issue is fixed and 5 min time criteria are applied to fetch data.
- Firewall: Under Credential Profile page, newly added devices are included. Now user can create Credential Profiles for all Supported Devices.
- Firewall: Added i18n support for Graph labels and other reports.
- Firewall: Disabling VDOM in User Config Page deletes all device rules configured. Now the issue is fixed.
- Firewall: Empty table issue while sorting column in Traffic Trend Report is fixed.
- OpManager: In interface snapshot page, the Schedule option under reports have been added to Bandwidth Utilization and At-a-Glance reports
- OpManager: In Interface snapshot page, the PDF option under reports, has been added to At-a-Glance report
- OpManager: In Interface snapshot page, inconsistent traffic data between At-a-Glance and Bandwidth reports. This issue has been fixed
- OpManager: Previously, when clicked on any graph in Interface snapshot page under graphs icon, few interface details such as Circuit Id, IfName, IfIndex, IfDesc, IfAlias, and ParentName were missing in interface reports in PDF format. This issue is fixed now.

Build No - 123044 - December 27, 2017

- General: 4141842 - Restoration failed when instance length exceeded 255 characters in StatsData table. This issue is now fixed.
- General: After expiry, the license can now be applied in the popup that is prompted once OpManager starts, instead of applying at the command prompt.
- General: After applying the license, the state of IPSLAs changed from "unmanaged" to "managed" previously. This issue is now fixed.
- General: Google map was not restored in the backup/restore process previously. This issue is now fixed.
- OpManager: When more than one probe existed, device count was displayed as zero in the probe's license activation page. This is fixed now.
- OpManager: Audit logs were not recorded for some APIs when the REST API was called from external sources. This issue is fixed now.

Build No - 123043 - December 22, 2017

- OpManager: Previously, APM plugin's visible area was too small. This is now moved to Main tabs area, for clearer visibility.
- OpManager: Previously, file monitoring failed when the devices' WMI Credential contained ". This has been fixed now.
- OpManager: For windows servers, adding free/used disk space WMI Monitors and device partition monitors failed due to the parsing problem of credentials with some specific special characters. This has been fixed.
- OpManager: When OpManager web client's local language was changed to Chinese, adding WAN RTT Monitor failed. This issue has been fixed now.
- OpManager: Previously, folder monitoring failed when the devices' WMI credential contained special characters like ",|. This has been fixed now.
- OpManager: When a credential included the special character |, then script execution failed. This has been fixed now.
- OpManager: While adding new monitors from the device snapshot page, users were unable to receive monitors from the device. Also, the same issue was faced when WMI monitors were being added to Device Templates. This happened if the device had the special character (") in its credential. This has been fixed now.
- OpManager: In the global Windows Services template page, previously the success message for add operation was displayed as Failure Message indicator. This issue is fixed now.
- OpManager: Displayed success message, even when the addition of WMI Partition Monitors to devices failed. This has been fixed now.
- OpManager: During workflow execution, the Check File/Folder Tasks failed due to the presence of some special characters in the password. This has been fixed now.
- OpManager: In the virtualization inventory page, filter selection for various tabs did not display the device list as per selection, when any operation like delete was done after the selection or when coming from a different page.
- OpManager: In Reports page, language localization was not done for Reports title and the description message for the default virtual server reports. This has been fixed now.
- OpManager: Under URL availability Widgets, the undefined page was displayed when selecting any URL Monitor, instead of displaying the URL snapshot page.
- OpManager: Previously, CLI Credentials were missing in Add VMware vCenter/ESX page specific to vCenter/ESX. This has been fixed now.
- OpManager: Under Data Maintenance page in Basic Settings, RunArchive button did not work when the Daily Archive option was selected. This has been fixed now.

Build No - 123037 - December 21, 2017

- OpManager: Alarm escalation was not working previously when a business view had been renamed. This issue is now fixed.
- OpManager: Previously under reports, the Audit function did not record workflow logs. This issue is fixed now.
- General: Previously when a user takes a tour of OpManager, the message "Move & Resize widgets by drag and drop" was displayed in English, irrespective of other language installations. This issue is now fixed.
- OpManager: Under reports, while creating a new report, "Inventory Reports" field displayed English characters irrespective of other language installations. This issue is now fixed to support I18N.
- OpManager: Under reports, while scheduling them, the "time field window" field did not support I18N. This is now fixed.
- OpManager: Under inventory, while generating reports for any monitor, the "search" field did not support I18N. This has been fixed now.
- OpManager: Previously under reports, the audit function did not record "schedule reports" logs. This issue is now fixed.

Build No - 123036 - December 19, 2017

- OpManager: While deleting an existing Windows service monitor from the device snapshot page, the list scrolls back to top and page navigation details were reset to

default values, thus making the user reset the required view and proceed with deletion task. This issue has been fixed now.

- OpManager: Under Add Monitors from device snapshot pages, clicking anywhere on the grid view of the add list led to the de-selection of the selected items in the list. This has been fixed now.
- OpManager: Previously when the CCTV dashboard contained only one widget, the widget size was small. Now, this is displayed in the full-screen size.
- OpManager: Under the "widget Traffic Reports", the interface traffic graphs were displayed. When the user created a NOC view, the graphs in the traffic reports widget had the X-axis cut-off. This issue is now fixed.
- OpManager: Under widgets, users were unable to expand the 'Top N Conversation' widgets. This has been fixed now.
- OpManager: From the Virtualization Inventory view, users were unable to delete the Datastore Entity. This has been fixed now.
- OpManager: A link has been provided now to add virtual servers directly from the Virtualization Inventory Page.
- OpManager: For non-english Italian language servers, undefined results were displayed while fetching the Windows Services for "Add Windows Service" operation from the Device Snapshot page. This has been fixed now.
- OpManager: The discovery completion status specific alarm had no differentiation between the discovery from ESX Server or from vCenter. This has been fixed now.
- OpManager: For some upgraded setups, VM sprawl related dashboards and widgets were missing. This has been handled now.
- OpManager: Under Reports, if any of the CPU Utilization/Memory Utilization/Disk Utilization reports were empty, then the entire Health Reports were displayed as empty. This has been handled and fixed.
- OpManager: Xen data collection was not happening for Xen Servers with version 7 and above. This has been fixed now.
- OpManager: While configuring notification profiles, the IPSLA-specific Clear Alarm criteria based notification mail, was received even though the criteria was not selected. This has been fixed now.
- OpManager: Disk Monitors were not added to the local host monitored device when it contained multiple NICs. This has been fixed now.

Build No - 123035 - December 14, 2017

- NCM: Fixed the reporting options (violated rules only, compliant rules only or all rules) in scheduling compliance report for CSV format.
- NCM: Error message for expired time in 'Once' option for add schedule page.
- NCM: 4025368 - Fixed the EOL Report with no data in OpManager Probe server.
- NCM: 4244879 - Compliance validation issue in exact set criteria rule is fixed.
- NCM: Admin has to give annotation while authorizing/unauthorizing configchanges.
- NCM: System settings page is enabled for NCM.
- NCM: Filter by time option is provided in changes page.
- NCM: Aruba Controller backup failure issue is fixed.
- NCM: Now configure the number of parallel threads for SSH connection.

Build No - 123034 - December 12, 2017

- OpManager: While adding a custom category with existing name (case-insensitive), users were redirected to Empty Import Devices page. This has been fixed now.
- OpManager: Custom category devices were associated with incorrect polling interval. This issue is now fixed.
- OpManager: Previously, custom category was not set for Windows 7 and Windows 2008 devices. This issue is now fixed.
- OpManager: Interface Rx/Tx Traffic and Utilization data was unavailable in reports, when data exceeded big int character length (19 char) in MSSQL. This has been fixed now.
- OpManager: Under add category in API, users were allowed to create a blank or empty category name. This has been fixed now.
- OpManager: Users were unable to navigate to the device snapshot page from Interface bandwidth report. This issue is now fixed.

- OpManager: Under inventory, the Subnets list view page's UI was broken previously. This has been fixed now.
- OpManager: Under snapshot page, Graphs icon and click on any graphs show tabular data is not sorted from the last polled value. This issue is now fixed.
- OpManager: Previously, operator users were able to edit outage history reason in device availability reports. This has been fixed now.
- OpManager: Previously under credentials page, the retype password field displayed plain text. This issue is fixed now.
- OpManager: Interface alarm messages were not displayed correctly when the message contained "<<>>" in UI. This issue is now fixed.
- OpManager: The SNMPv3 default port of the MIBBrowser is now changed to 161.
- OpManager: Previously users were unable to update IPv6 IP Address in Edit device details. This issue is now fixed.
- OpManager: Interface graphs can now scale automatically to Mbps or Gbps based on the data.
- OpManager: Previously in real-time traffic widget, the Y axis was not scaled automatically. This issue is now fixed.

Build No - 123033 - December 11, 2017

- NetFlow: Added SNMP support for Wireless LAN Controllers to fetch names of Access Points.
- NetFlow: Client MAC based filter is added newly in Inventory and Snapshot under WLC.
- NetFlow: Widget for Client MAC traffic is added in snapshot view of Client IP.
- NetFlow: Overall Report for IP Groups is added in schedule reports.
- NetFlow: Edit option in Alert profile has been fixed.
- NetFlow: Unwanted vectorwise DB operation is removed to avoid loss of raw data.
- NetFlow: Attacks information is now can be viewed for selected device and interface.
- NetFlow: Issue in attacks search filter has been fixed.
- NetFlow: Option to select Ethernet card name is available in DPI settings.
- NetFlow: Promiscuous mode of ethernet cards has been enabled by default for DPI.

Build No - 123032 - December 6, 2017

- OpUtils: Included actions like add, delete, rename group in IPAM tree under Inventory.
- OpUtils: Option to add/edit subnet location, VLAN name has been provided while modifying a subnet.
- OpUtils: A "Check Now" button is included while adding a switch in the SPM page to verify its presence.
- OpUtils: Under "Switch Ports by ifType" Reports, the IF TYPE was missing for few switch ports previously. This is now fixed
- OpUtils: "M" character had been appending in the total device count in the SPM email alert. This is now fixed
- OpUtils: Previously, WMI query tool was not working due to the presence of "\" in the Name field. This issue is now fixed.
- OpUtils: Under Settings, Active Directory scanning was not working previously, if the password contained special characters. This issue is now fixed.
- OpUtils: Under Add Subnet option, the Redirect link leading to sample csv format was not working. The redirect link is now replaced with a sample csv file.
- OpUtils: In the Mac address resolver under Settings, the error message occurring when SNMP community field was not filled, is now deleted.
- OpUtils: AD Status Summary in Dashboard & IP Addresses was not updated after completing the subnet scan. This issue is now fixed.

Build No - 123031 - December 1, 2017

Issues Fixed

- The Refresh Datastore Workflow task execution displayed success message even when the execution failed. This issue has been fixed.
- If there was any change in Canonical Path Names for the LUN Multipath associated to ESX Servers, then rediscovery of vCenter failed. This has been fixed now.
- AMS Expiry notification was not shown to users irrespective of their version.This has been fixed now.
- AppManager plugin data was not displayed to Read Only users even though they had access to all the devices. This issue has been fixed to display APM Plugin data to all the non business view users.
- NT Services that has comma (,) in their Service Name or Display Names were not added in OpManager. This has been fixed now.

Enhancement

- Once a VMware Datastore was deleted or had stopped monitoring in OpManager, there was no option to re-start monitoring. This option is included now.

Build No - 123030 - November 28, 2017

- OpManager will now integrate with SDP through rest APIs. OpManager build 123030 and above and ServiceDesk Plus build 9329 and above will support API-based integration. However, old method of integration will also be available to support customers in older version.

Build No - 123029 - November 24, 2017

- NetFlow: Resource type and resource category are set by default to Top N Problems widget in dashboard.
- NetFlow: Default name will get changed based on the category for Top N problem widget in dashboard.
- NetFlow: The mismatch in Row Count for the top source, destination, conversation, application (L4,L7) has been fixed now.
- NetFlow: Redirection issue in Dashboard from network-based (Source network, Destination network) widget has been fixed.
- NetFlow: A new column for DSCP has been added to top conversation widget in dashboard.
- NetFlow: Added an option to redirect from meraki device in device summary widget.
- NetFlow: Redirecting to a particular snapshot with the configured timeframe is proper now and has been fixed.
- NetFlow: Redirecting to snapshot from WLC widgets is proper now and has been fixed.
- NetFlow: Enabling CBQoS policies for more than 2 interfaces has been fixed now.
- NetFlow: Listing interfaces with the index -1 has been fixed now.
- NetFlow: WAAS Total Volume graph plotting and time zone is proper now and has been fixed.
- NetFlow: TimeZone issue for Line graph has been fixed now.
- NetFlow: Updating interface name when the speed is 0 is possible now.
- NetFlow: Individual Graph feature across product is proper now and has been fixed.
- NetFlow: Device traffic graph data in device Snapshot page showing incorrect value has been fixed now.
- NetFlow: Error in displaying time across product when the user and browser timezone differs has been fixed.
- NetFlow: Drill down conversation in QoS shows only 50 records (pagination) has been fixed now.
- NetFlow: "Invalid Device selected" displayed in Raw Data Settings while clicking on Save button has been fixed now.
- NetFlow: Raw data was getting duplicated in the database. Now it has been fixed.

Build No - 123028 - November 22, 2017

- OpManager: In the device snapshot page, Response Time and Packet loss report was not working when the time period exceeded 30 days. This issue is now fixed.
- OpManager: In the device snapshot page, a new icon has been added to navigate to Google Map. This icon is displayed only if the device has been already added to the map.
- OpManager: Under Google Map, the "Filter by Type" option in Google Map, did not list any device types in Central. This issue is now fixed.
- OpManager: Under Google Map, the unmanaged state of the severity icon was displayed as undefined. This is fixed now.
- OpManager: In Google Map, the map position will be retained if user redirects to other pages.

Build No - 123027 - November 21, 2017

Enhancements:

- The 'Automatic/On-click/No lookup' options of Resolve DNS in global settings synchronized for all widgets
- Two more SMS service Clickatell and AppSMS supported to send SMS notifications for 'Alarms, Configuration changes, and Availability Alerts'

Issues Fixed:

- 123396 - If dashboard data is with '\', in its drilldown page data is shown without '\' . The issue is resolved to display it properly
- 121669 - When Traffic Conversation Table in Interface drilldown page is expanded, it was displaying only top 10 rows. Issue fixed to display complete data
- 123760 - In CCTV view, Operator can view unauthorized device's Live Traffic. Issue is fixed by hiding it
- 122774 - In one of the 'Proxy Reports', when Search icon is clicked, empty page was displayed. Issue fixed to display appropriate page
- 123955 - 'No Data' message not internationalized in some graphs, issue fixed by internationalizing it.
- 122298 - In dashboard traffic and security statistics report, when Search icon is clicked, empty page was displayed. Issue fixed to display appropriate page
- 124212 - 'In' & 'Out' legends in Device Summary graph were not internationalized, issue fixed by internationalizing it.
- 121712 - Fixed memory handling issue, during user association and manual IP mapping when device is deleted
- 123826 - Fixed an issue in reimport option of manual IP mapping
- 120736 - Fixed issues in FWA Availability alert page UI and Disable notification link in the alert notification mail
- 122140 - Fixed an issue in script error handling, when a schedule is added for Compliance report without selecting any type of standards
- 125095 - In standard compliance reports, if clicked to drill down the report, the table values are not displayed. Fixed the issue for table value display
- 125093 - User with '\' character could not be added, for 'End Users' reports. Fixed the issue to add user
- 123942 - There was an UI alignment issue in NetFlow widget populated in OpManager's End Users report. Fixed the issue to align the UI
- 122493 - In the dashboard, snapshot view of Cloud Users report, fixed the issue of missing 'Expand View' icon
- 124899 - Fixed the issue in Disable notification option of the change management alert notification mail
- 124613 - When TLS option was configured in Mail Server settings, mail notifications for alerts were not sent. Fixed the issue to send mails
- 124090 - Fixed the misalignment issue in Policy Overview report table. This was for MS SQL databse
- 122970 - When a new report type is added with the existing name, 'Success' message is displayed. Fixed the issue to display

'Failed' message

- 125067 - Fixed the issue to populate rule details of SRX devices, when the configuration file is not having network object details
- 125059 - In the 'Unused Rules' report of 'Rule Management', the resource criteria is not applied properly. Fixed the issue to apply the resource criteria properly
- 4245966 - In FWA, log entries for unsuccessful console login attempt on Cisco ASA devices are not there. Fixed the issue to get entries
- 4206352 - Issue, in SonicWALL log parsing for protocol, is fixed
- 4086698 - All the IPs are not getting resolved into names, when 'Resolve DNS' is set to 'Automatic'. Fixed the issue to resolve all IPs
- 4250080 - When scheduled PDF report page count is more than 100, the total page count in PDF footer was not proper. Fixed the issue for proper page count
- 4300246 - Fixed the out of memory error generated when change management report was accessed

Build No - 123026 - November 17, 2017

- An option to associate URL templates to multiple devices from the URL template list has been included.
- An option to view the list of URLs monitors associated to devices has been included in the URL monitors page. Select the Device Specific URLs dropdown to view these monitors.

Build No - 123025 - November 16, 2017

- General: 4139091- User Management - Some users were unable to login the web client after upgrading to the latest service pack. This issue has been now fixed.
- General: 3811324 - When user count exceeded 100, issues were encountered while logging in. This has been fixed now.
- OpManager: Under Notification Profile, email notifications were received as html content, even when plain text format was chosen. This issue is now fixed.
- OpManager: Under Notification Profile, $eventType was not passed in the notification message. This issue is fixed now.
- OpManager: 4099988 - Under notification profile, when html tags were added in the message field, the profile was not saved. This has been fixed now.
- General: SIF upload was not working due to bonitas URL change. This has been fixed now.
- OpManager: 4133567- Under Send Email Notification Profile, while adding special characters in the subject field, the issue where the profile was saved without retaining the special characters or showed errors, has been fixed now.

Build No - 123024 - November 14, 2017

- Under CCTV view, BusinessView did not fit to screen previously. This issue is now fixed.
- Previously, in the device snapshot page, even though the availability of a device was 96%, the dial display was in red color. This issue is now fixed.
- Under Heatmap, device details were not displayed on mouse-over. This issue is now fixed.
- Interface graphs were plotted incorrectly (Graph stack issue, for example, if interface tx is 8 Mbps & Rx is 6 Mbps then we are plotting the graph for 14 Mbps). This has been fixed now.
- The background image was not displayed properly in BusinessViews widget while accessing more than one widget. This issue is now fixed.
- Interface snapshot page, Under Graphs icon -> click on Interface summary graphs -> 95th percentile line was displayed incorrectly.This has been fixed now.
- In business views, LED icons now have a transparent shape instead of a square one.
- 95th percentile min, max, and avg values were missing in the Interface snapshot page. This issue is now fixed.

Build No - 123023 - November 13, 2017

- NCM: Option to clone a device template is provided in GUI.
- NCM: Provided an option to delete existing sysOID in GUI.
- NCM: Schedule actions are removed from device Inventory multi-select actions list and is now added under a new group 'Schedule'.
- NCM: Option to schedule configlets is provided in Configlets list page.
- NCM: 3942442 - Option to retry backup for backup failed devices.
- NCM: 4101225 - Option to add DNS name in reports for application URL instead of IP Address.
- NCM: 4150507 - Search option is provided to select the device in the multi-select box in GUI.
- NCM: Uniform color coding for authorization & unauthorization across the product.
- NCM: Option to edit import devices and values option is provided in the "Configlet Schedule" page.
- NCM: Configuration Change Trend, Compliance Report, Device Audit Report are now provided on the device snapshot page.

Build No - 123022 - November 9, 2017

- OpManager: 3985963 - Multiple Notification Profiles can now be selected and deleted in bulk.
- OpManager: While scheduling a notification profile, the "Do not trigger" option that prevents unnecessary notifications after acknowledging the alarm, can be validated only if the time is set for Delayed Trigger and Trigger Interval.
- OpManager: When configuring notifications from Alarms, the tab that allows the user to select the notification type, was missing previously. This has been fixed now.
- OpManager: Under Device Snapshot page, the notification profiles that have already been associated with the device will be marked as selected, while listing all available notification profiles for association.
- OpManager: A clear error message in the client will be displayed, when a user tries to associate notification profiles without selecting any.
- OpManager: While sending a test mail from the secondary mail server, the primary server message was received, instead of the secondary server message. This has been fixed now.
- OpManager: While adding a new notification profile, configurations of previously added Notification Profile were shown. This issue has been fixed now.
- OpManager: Under SDP Add-on, the "Auto Sync assets" functionality now works seamlessly.

Build No - 123021 - November 8, 2017

- OpManager: When a report created from report builder or snapshot page, is exported to PDF, the device name or the report itself is not properly displayed. This issue has been fixed.
- OpManager: All the data in a report is printed on a single page and when the same is exported to PDF it is improper to view. Now, this issue has been fixed by printing the report in multiple pages for a better view.
- OpManager: Issue in creating a report when it contains a special character. This has been fixed.
- OpManager: Issue in exporting partition details report to PDF. This has been fixed.
- OpManager: Links available in the report for Top N Errors and Discards for device and interface fail to redirect correctly. This issue has been fixed.

(Note: Builds 123016 to 123020 are reserved for internal purpose.)

Build No - 123015 - Nov 2, 2017

- OpManager: For default virtual inventory reports in virtual server reports page, Schedule Reports and Send Mail option were not working and was sending blank attachment in the mail. This issue has been fixed now.
- OpManager: For default virtual inventory reports in virtual server reports page, Export as PDF/Excel options were not working. This has been fixed now.

- OpManager: On editing virtual server reports, the Period and Time Window fields were not shown. This has been fixed now.
- OpManager: VMware discover/rediscovery was getting failed when HostPortGroup is duplicated and both the duplicated HostPortGroups are mapped to the same VM/Host. This issue has been fixed now.
- OpManager: If more than one proper credentials for vCenter were added in OpManager, with Auto-VM discovery enabled for one and disabled for the other, then after some time the mapped credential to vCenter/ESX in OpManager was automatically getting changed. This has been fixed now.
- OpManager: The periodic update of VMware vCenter/ESX Inventory in OpManager was not getting properly updated as per configured Update Interval parameter during vCenter/ESX discovery. This has been fixed now.

Build No - 123014 - October 31, 2017

- NetFlow: The issue with export to CSV in inventory has been fixed and enhanced.
- NetFlow: Added an option to export to CSV for NetFlow Group Configurations. This option is added under "Group Settings".

Build No - 123013 - October 27, 2017

- OpManager: While associating "Remote Script Templates", OpManager listed all devices instead of displaying only CLI supported devices. This issue has been fixed now.
- OpManager: IE browser can now support Japanese Characters in Script Templates.
- OpManager: On adding a Syslog rule, The Rearm Match Text was not saved previously. This issue has been fixed now.
- OpManager: The "Test Script" button is now removed from Script Templates for the Central Server, as the scripts are executed only at the probe. These scripts can be tested at the probe.
- OpManager: When a syslog rule was created at the central server, the same was not synced with the probe. This issue is now fixed.
- OpManager: 4190299 - After adding APM plugin to OpManager, APM monitors were not displayed in the device snapshot page. This has been fixed now.
- OpManager: 4244060 - Mail Server settings were not be saved, when "\" was present in UserName field. This issue is fixed now.

Build No - 123012 - October 26, 2017

- OpManager: On editing the threshold of any performance monitors from the device snapshot page, the consecutive times allowed "0" to be given as input. This has been fixed now.
- OpManager: Few build versions of HyperV2016 were not categorized under "HyperV" due to mismatch in the criteria of HyperV related WMI (Win32_OperatingSystem) class. This issue is now fixed.
- OpManager: Too many unnecessary discovery status popups were displayed while receiving VM events from vCenter environment. This led to slowness due to frequently scheduling inventory updates in OpManager. This has been fixed now.
- OpManager: While editing a process monitor from the device snapshot page, when the instance count criteria matched "=" and if the threshold value was set to "0", the Rearm value was automatically set to "0". This issue is now fixed.

Build No - 123011 - October 24, 2017

- Under VLAN snapshot page, the interface list was not displayed previously. This issue is now fixed.
- The privilege of deleting interfaces from device snapshot page is now restricted to only admin users.
- When navigating from Configuration tab to Monitoring tab in Settings, the Add/Associate buttons in the Performance Monitors page were hidden. This issue is now fixed.
- In the device snapshot page, Interface grid data was displayed even after deleting that particular interface. This issue is now fixed.
- Under Basic Settings, when adding a new category, if the name contained other language characters users were unable to

delete the custom category. This issue is now fixed.

Build No - 123010 - October 20, 2017

- OpManager: While adding Real-Time Traffic widget from the dashboard, y-axis will now scale to bps, Kbps, Mbps, Gbps automatically based on the data.

Build No - 123009 - October 16, 2017

- NetFlow: The issue with IPv4 address based criteria in Alert Profiles has been fixed for V9/IPFIX/SFlow flow format.
- NetFlow: The issue with Raw Data memory storage when toggle between raw ON and OFF for has been fixed for all databases i.e HighPerf, PGSQL and MS SQL.
- NetFlow: Interface group name was missing in the PDF generated through Schedule Reports. Now, this has been fixed.
- NetFlow: Application drill down & conversation reports from Inventory>>Interface has now mapped required Src and Dst port for application mapping when data fetched from raw data. This issue with port and application mapping has been fixed.
- NetFlow: Now there is an option to send an SMS alert to multiple mobile numbers from "Alert Profiles" tab in Settings.

Build No - 123008 - October 12, 2017

- Firewall: 4180774 -- Device rule configuration using SCP protocol was not functioning in build 12300. Now, this issue is fixed.
- Firewall: 124197 -- Sometimes, SRX marked as unsupported device, if Firewall Analyzer receives unsupported log as the very first record. Now, wait time is added to check more received logs to avoid unparsed error.
- Firewall: 120221 -- Previously, there was no option to view the selected time-period of each dashboard widgets. Now, sub-header details will be shown in each widget with device information along with time-period applied.
- Firewall: 122695 -- System performance and custom dashboard views were missing when logged in for the first time. Now the issue is fixed and the user can view both. Firewall: 122785 -- Inventory Interface snapshot traffic conversation report's last row was not shown properly in UI. Now the issue is fixed and the report loads the data properly.
- Firewall: 122055 -- Graph units option provided in the Inventory LiveReports page was not in proper sequence. This issue is fixed and the units are now shown in proper order like kbps, Mbps, and Gbps.
- Firewall: 123774 -- When the user selects all predefined reports while creating a report profile, received PDF shows all the reports name on the home page without proper alignment. Now, Alert Message added for Report Profile reports selection.
- Firewall: 122683 -- Editing widget "Top N Hosts by Traffic" and selecting Protocol under category makes the widget to show data of protocol-group by traffic. Now, the issue is fixed by showing Protocol-Group instead of Protocol in dashboard widget - edit section.
- Firewall: 123865 -- 'Live Syslog Viewer' status shown as 'undefined' when we do a continuous refresh. Now the status message handling issue is fixed on the server side to show proper status in the UI for a continuous refresh.
- Firewall: 124244 -- Increased the data dumb volume from base table 'Firewall Records' to next level data table for database performance increase.
- NCM: 4094309 -- SSH Vulnerability #1: The SSH server is configured to support Cipher Block Chaining (CBC) encryption, which may allow an attacker to recover plaintext message from the ciphertext. We've now fixed this by providing an option to disable the CBC mode encryption using system property.
- NCM: 4094309 -- SSH Vulnerability #2: The remote server is configured to allow MD5 and 96-bit MAC algorithms, both of which are weak algorithms. We have now fixed this by providing the option to disable these algorithms using system property.
- NCM: 1584237 -- Configuration Analysis and Security Audit Reports are now supported for device templates which were not supported in earlier versions.

Build No - 123007 - October 11, 2017

- OpManager: IPSLA monitors were not getting created when the source device does not contain the same notification profiles

available in the WAN Threshold template. Now, this has been fixed.

- OpManager: When two or more hop-by-hop widgets are present in one single dashboard, the widgets either collapse or get misaligned. Now, this issues has been fixed.
- OpManager: Search was not working for "Path" field in IPSLA monitor's inventory page. When searched for values that were present in the middle of a name were not pulled up in the search. Now, this issue has been fixed. Also, now the monitor name is shown upon mouse-hover.
- OpManager: When editing a hop-by-hop widget, instead of highlighting the respective monitor's name, the one that is listed first was selected. Now, this issue has been fixed and the respective monitor name is selected irrespective of the order.
- OpManager: I18N has been done for the word "Get" in Add URL template page by mistake Now we have removed I18N for the word "Get" because it's a technical term.
- OpManager: I18N was not done for the word "Edit" in process monitor page. Now it's been done.

Build No - 123006 - October 9, 2017

- OpManager: 114501/124174 - Option to disable/enable the pop-up that indicates the discovery status.
- OpManager: 122367 - Virtualization related monitors were able to be associated with non-virtual devices also. This issue has been fixed.
- OpManager: 124545 - In the dashboards black color band, "NetFlow" and "transferred" has been misspelled as "Netflow" and "transfered". This has been corrected.
- OpManager: 122340 - Option to configure the polling interval for custom WMI performance monitors was overlooked and because of this, the polling interval time was set to '0' by default. Now we have provided the option to enter the polling interval.
- OpManager: 122294 - When adding a custom SNMP monitor, the "Units" field was still getting displayed even after changing the "Functional exp" filed value to string ("Numeric to string"). This is an issue has been fixed. Now if the value is changed to string, the "Units" field will be hidden.

Build No - 123005 - October 6, 2017

- Under the inventory tab for IP address management, a read-only tree view has been added for easy classification of subnets.
- Under then inventory tab for IP address management, when IP addresses are filtered by the OS category '"Unknown", the list was not loaded. This issue has been fixed.
- Under IP address management, the page loading time for showing the inventory of IP Address, Ports, and Rogue has been improved.
- The changes done in General settings under OpUtils->SPM were not saved in the database. This issue has been fixed.
- When a device that doesn't support the Bridge-MIB was added for IP address and switch port management, no error message was displayed. Now, if such devices are added, an error message will be shown in the UI.

Build No - 123004 - October 3, 2017

- CCTV crash occurring while resizing the widgets has been fixed.
- Option to Add/Remove widgets included in default dashboards.
- The customization done in a dashboard & CCTV with respect to widgets position and size will be retained across users and browsers.

Build No - 123003 - September 28, 2017

Issues fixed in OpManager:

- For other language installation, iTextAsian.jar file has to be downloaded by the user. This download message has been enhanced and is displayed clearly in OpManager's UI.
- The display break issue occurring with "Check URL" feature in Workflows, has been fixed
- Issue with sending SNMP traps containing the variable $entity under notification profile, is fixed

- Issue with the WebAlarms widget where no data was available previously due to DB error, is now fixed.
- Issue with the Trap Processor status handling during sorting/navigation under Monitors, is fixed.
- Issue with trap-version while creating trap processor from unsolicited traps, is fixed.
- The period option missing in Availability Reports after upgrading to 12300 build, is included.
- Schedule Reports Top(10,50,100,1000) and bottom(10,50,100,1000) options are now shown properly.

Build No - 123002 - September 20, 2017

Issues fixed in NetFlow module:

- Router display name was not updated while fetching from Router via SNMP has been fixed.
- Search Filter not working in NetFlow inventory has been fixed.

Build No - 123001 - September 7, 2017

Issues fixed in OpManager:

- Google map widget was not loading properly in CCTV and this has been fixed.
- Browser crash issue when CCTV name has a space has been fixed.
- Issue in adding SNMP v1 and v2 credentials in OpUtils has been fixed.

Build No - 12300

Features and Enhancements in OpManager

- 39,070 Vendor Templates have been added - To avoid devices getting added as "'Unknown", vendor templates have been added. Vendor template also includes monitors such as system up time, the number of Network Interfaces, and IP routing discards.
- Windows 2016 device is now supported.
- Microsoft Exchange 2016 is now supported.
- Microsoft Hyper-V 2016 is now supported.
- Tomcat version has been upgraded to 8.5.13.
- HTTP v1.1 has been changed to HTTP v2 for SSL encrypted servlets.
- When adding credentials, OpManager now asks to retype the password to avoid adding wrong credentials by mistake.
- Web client's loading speed has been improved.
- Google Maps page has been revamped to group devices available in the same coordinates.
- Snapshot pages are now available for VMware datastores.
- Option to discover VMs through vCenter or ESX has been added.
- Option to carry out administrative tasks on VMware Host/VM from respective snapshot pages has been added.
- Test credentials of devices in bulk and also schedule it.
- Performance graphs have been added for file and folder monitors.
- Associate multiple performance monitors to various devices.
- Add a new device via a trap. [Settings-> System Settings-> Discovery]
- VPN Tunnels widgets have been added for ASA firewalls.
- Export PDF option has been introduced for Availability reports and Interface Bandwidth utilization.

Issues fixed in OpManager:

- The issue in updating the modified threshold values in the devices when reapplying the template has been fixed.
- Data collected during one instance is duplicated to other instances for WMI Free/Used disk space and partition monitors. This issues has been fixed.

- Trap alarm message displays OID instead of varbind key even after loading the MIB file has been fixed.
- Rules in Rule Engine getting applied by mistake even though the rule is not satisfied has been fixed.
- The issue with credential password containing special characters has been fixed.
- Issue with adding Process Monitors using bulk select options is fixed.
- For non-English language installations, File/Folder monitor's Age/Size had few issues with the threshold and rearm with hour/day option. This has been fixed.
- Issue with monitoring MSSQL if the instance name has speical characers(_, $, #) characters, has been fixed.
- Issue with View/Update Rack with the different locale for Non-English OS is fixed.
- Issue with the VM Sprawl data not being visible for VMware is fixed and has been included for HyperV VMs as well.
- Issue with not being able to identify Domain Controller with WMI is fixed.
- Issue with Script Monitors not working with other OS apart from Linux is fixed.
- Authorization issues have been fixed .
- Includes Rack/Floor Status updates.
- CLI Discovery (Telnet) issue fixed.

- Issues Fixed: Interface - When Interface speed exceeds bandwidth, an alarm would be raised.
- Virtual Server inventory reports have been introduced.
- Xen Pool Snapshot to view all the Entities List of a Pool in a single snapshot.

Features and Enhancements in NetFlow

- DPI-based bandwidth monitoring to measure NRT vs ART
- Cisco Meraki is now supported.
- sFlow support for Huawei is now added.
- Tab View for NetFlow is provided.
- Drill down from Dashboard option is included.
- Multi select options for Inventory list view for configuration and reports are added.
- Search in inventory, reports, and settings have been enhanced.
- Option to assign an NCM device for Operator role in both standalone version and collector is now added.
- Option to store raw data for 1 year in Highperf add-in is now provided.
- The subject of email and SMS alerts can now be customized.

- Tools in settings White List for Attacks Module is included.
- PDF/CSV enhancement in inventory snapshot.
- Windows authentication for MSSQL.
- Pagination for Autonomous View.
- Basic Audit reporting NetFlow.
- Customizable Email/SMS subject handled in Alerts.
- Resolve DNS option available from the Dashboard.
- Option to add device from NFA to NCM from inventory list.
- Bulk SNMP assignment is provided.
- Unique name association across OPM and NetFlow.

- Report Linking from Inventory.
- Auto selection of SNMP in netflow if the same device is already available in OPM with SNMP credential.
- SFlow support with dual sampling pool for IN and OUT separately.(SFlow negative value)
- QoS drill down from List view
- Clear DNS cache option.
- Option to select the graph type for traffic widget has been included.

Issues fixed in NetFlow module

- SNMP V3/V2 failure issue fixed Alert Mail fails when there is no authentication provided.
- Display Autonomous View issue is fixed.
- Capacity planning issue - Granularity, 97th percentile, on demand bill generation, units, PDF NFA DE - The issue with utilization showing 0 in interface list, is fixed.
- Multiple E-Mail per threshold issue is fixed.
- SFlow parsing handle for PPPOE flows IPGroup with port range data dump handled.
- The issue in updating the modified threshold values in the devices when reapplying the template has been fixed.

Features and Enhancements in NCM module

- Ability to import new Device Templates using XML file.
- Ability to Edit / Delete Device Templates. Real-time notification of Approval requests.
- Real-time GUI update/auto refresh.
- Export options for Custom Template execution result and Custom Reports introduced.
- User specific Retainable filters and column choosers: Option to show/hide columns in list views.
- Schedule option is added for Configuration upload action.
- Ability to create device group by combining more than one device groups and also dynamically create groups based on predefined rules.
- Possible to add / associate / delete flow export configlets in a Template.
- Also, it is possible to add new Device Identifiers (Device SysObjectId) in a Template manually.

Issues fixed in NCM module

- Sysobject Finder SNMPv3 option provided.
- Issues with creating a user with more than 200 devices associated and not able to create a device group when more than 200 devices selected are fixed.
- The issue with viewing configuration change diff with HTML content is fixed.

Features and Enhancements in Firewall module

- Following devices are supported now:
  - TrendMicro IWSVA 6.5
  - PaloAlto VPN logs
  - Fortigate Management logs
  - SRX Management logs
  - SonicWall_IPSec VPN logs
- 'Insider Threat' reports - 'End User Monitoring' Add-On.

- Drill-down for all dashboard reports.
- Exclude IP/IP-range/network from reporting feature.
- URL and VPN reports are provided for Inventory report user-drill down.
- Live report for Proxy servers.
- Live report drill-down for device and interfaces from Inventory.
- Interface Live Traffic widgets in Custom-Dashboard.
- End-User widgets in Custom-Dashboard.
- Anomaly-Alerts based on Country.
- User specific reports for Proxy servers.
- Option to export report as CSV on-demand.
- Option to use Management IP address to fetch device configuration.
- Option to configure 'Row Count' for on-demand PDF/CSV report export.
- More reports for Rules in Device-snapshot.

Issues fixed in Firewall module

- SRX policy parsing issue fixed for Compliance & Policy Overview report.
- Live Report out-traffic spike based on SNMP fixed.
- Fortigate 5.2.4 Device rule SSH connection issue fixed.
- VPN Usage Trend report issue fixed.
- PDF issue in non-English client side language issue fixed.
- Export to PDF issue fixed for Rule-Reorder recommendation report.
- SNMP V3 configuration issue without community fixed.
- The drill-down issue for Usernames which contains slash in it.

Features and Enhancements in IPAM/SPM module

- Microsoft DHCP Server has been supported. Scheduler scan.
- Custom columns have been added in IPAM & SPM.
- Edit IP details have been added.
- OS Type summary widget has been added in IPAM dashboard.
- NIC Type table has been updated to identify the device vendor.
- Include, Exclude ports pages has been added.

Issues fixed in IPAM/SPM module

- Issue with add switch has been fixed.
- Issue with modify switch has been fixed.
- Issue with IPAM Publish, Scheduler is fixed.
- Issue with viewing configuration change diff with HTML content is fixed.
- Issue with sorting in inventory and search issue is fixed.
- Issue in Tools, TCP reset has been fixed.
- Multiple UI issues have been addressed.

OpManager v12.2 Build No - 12200

Features and Enhancements in OpManager

- Plug-ins such as NetFlow, NCM, and OpUtils are merged with OpManager for unified network management. These plug-ins will now be available as add-ons and no additional download or upgrade is required.
- New API-based web-client that includes integrated dashboards, snapshot pages, alarms, inventory, and reports.
- Support for radius server authentication.
- Enhanced charts and graphs with drill-down and filter options.
- Tomcat has been upgraded to version 8.
- JRE has been upgraded to version 1.7.

Limitation:

- Old struts-based web-client will no longer be available with version 12.2

Features and Enhancements in NetFlow Analyzer

- SNMP V1/V2 Mapping issue fixed.
- End user bandwidth monitoring for MSSQL Handled.
- No data for Last 24 hour fixed Device blank page issue fixed (Mapping between OPM and NFA fails/ if deleted from OPM/NCM it is handled).
- Inventory view tab blank out issue fixed. Mailserver setting TLS handled.
- SFlow output interface flow processing handled. SNMP default time and retries handled.
- GRE and ESP include/Exclude handled.
- TimeFrame selection in Expanded Widget View Handled properly NetFlow Issue Fixed : Interface Traffic Widget Table data related Changes
- CBQoS Service Policy Tree Map view First Cut provided in Interface Snapshot Page under CBQoS widget. Device ID assignment fixed in Pagination.

Features and Enhancements in Network Configuration Manager

- TFTP Path Disclosure(Vulnerability) fix
- PCI- Deleted User Reviews cannot be Reviewed issue is fixed.
- Configlet schedule PDF attachment issue is fixed
- Unable to backup more than 50 devices issue is fixed.
- Compliance - Rules/RuleGroups not listed when the count is more than 50 issue fixed
- Alarms and Workflows not working issue fixed.
- "write mem" command execution showed failed even though the command execution success in the device.

Features and Enhancements in Firewall Analyzer

- Inventory - Device drill down - Top 10 widgets - If I expand without refreshing the widgets, scroll down option is missing.
- Check-point device dll & opsec.exe not bundled.
- "View All" option missed in all default Reports.

- URL-Report parsing issue fixed for Palo-Alto
- Cisco-Meraki (Proxy) and FireSight device support
- Administrator/ Operator specific page view issues fixed
- Showing two scroll-bar in Security Audit page.

OpManager v11.6 Build No - 11600 (Jun 16th, 2015)

Features and Enhancements

- Scheduled Discovery: Now network discovery can be scheduled to run periodically. Other enhancements include options to
  - Skip interface discovery
  - Select interface type during discovery
  - Select rule engine
  - Configure discovery reports
  - Add filters and rediscovery rules for actions such as adding, deleting, and un-managing devices or interfaces
- VLAN Discovery now supported.
- Device template for UCS system with 24 new monitors has been added.
- In 3D data center floor view, options to add air aisles, walk paths and walls have been added newly.
- Option to generate QR code for the devices on the rack.
- Now racks and floors can be added in the Business view.
- Connect now feature is added in Business Views to import connections from Layer2 map and draw the connections.
- Option to convert TopoMapper Plus to OpManager free version and vice versa has been added newly.
- Submit Feedback option has been added to capture a screen and submit the feedback to OpManager team for enhancements and bug fixes.
- Bulk edit option for editing thresholds and polling intervals of AD, MSSQL & Exchange monitors.
- XenServer monitoring is now available in OpManager.
- Extensive support for monitoring VMware events.
- Full monitoring support for VMware devices via vCenter. The earlier option available to monitor them via ESXi servers is withdrawn. VMware monitoring is supported from version 4.1 only.
- Now OpManager extends showing configuration details of VMware devices to data centers/clusters.
- New dashboards and widgets for virtualization monitoring have been added.
- Option to configure monitoring interval and threshold settings for monitors of virtual servers has been added newly.
- In addition to VM performance monitors for Virtual Servers , full fledged SNMP/WMI/CLI monitors are also supported now.
- OpStor plug-in 9.0 is compatible with 11400 & 11500 only. So Users upgrading from 11500 to 11600, also need to upgrade OpStor plugin to 9.1 version.
- OpStor plug-in 9.1 is compatible with 11600 only. So customers degrading from 11600 also need to degrade to OpStor 9.0 version.

OpManager v11.5 Build No - 11500 (Feb 5th, 2015)

Features and Enhancements

- Schedule Upgrade - Schedule Upgrade helps to stay up-to-date with the latest version of OpManager. Whenever a new

version/update gets released, OpManager downloads it and starts upgrading automatically during the time scheduled by you.

- Migration Support:Migration from Enterprise Edition to LEE - OpManager now supports data migration from Enterprise Edition to Large Enterprise Edition. It provides an option to automatically migrate configuration data from OpManager EE (Central server & Probes), and populate in its own DB.
- Migration from Standalone To Enterprise Edition - Users running OpManager standalone edition in PostgreSQL database can now seamlesssly migrate to enterprise edition (i.e) central - probe architecture. Earlier this migration feature was supported only for MySQL and MSSQL databases.
- SMS jar file has been upgraded from version 1.2.1 to 3.5.3. With this version upgrade, two new fields are introduced in the SMS server settings. Users are requested to revisit the SMS server settings in OpManager webclient and set up the configuration once again. To see the list of compatible GSM modems/phones, click here.
- Private Groups in Social IT - Private groups in Social IT allows to carryout discussions on a project within the project members. The admin of the group can invite as many people to join the group. Only the group members will have access to view the discussions that happen in these groups.
- It is now possible to add custom dials for for all the performance monitors listed in device snapshot page.
- Support for monitoring Exchange 2013 environment is newly included in OpManager.
- Email attachment size limit for schedule reports has been increased up to 3MB.
- OpManager 11500 supports monitoring the disk array data hardware status of all the DELL servers.
- Interface templates section has been revamped. Earlier there was a single process for applying and associating templates. But now, it's been split into two processes - Apply template and Associate template. Associate template allows you to choose values to associate instead of associating all template values to interfaces.
- New SMS Gateway(Clickatell) has been added for receiving SMS alerts.
- To make initial configuration easier, more than 350 device templates are newly added in OpManager.IPSLA monitors are newly added to the notification criteria.
- OpManager 11500 provides option to select the required discovery mechanisms such as CDP, LLDP, IPROUTE and FDB during Layer 2 discoveryA new widget for Layer 2 maps has been addedExchange monitors are discovered automatically if WMI credentials are passed.

OpManager v11.4 Build No - 11400 (Oct 1st, 2014)

1. **UCS Monitoring:**

UCS Monitoring is an add-on that helps you to monitor all the Cisco UCSes and its components, in your data center. It leverages Cisco UCS XML API to monitor the UCS and instantly notifies you in-case of any fault via email & SMS. Apart from this, the UCS monitor also includes a 2D relationship map that helps you to visualize the relationship among the hosts, clusters, and VMs present in the UCS.

2. **Enhancements in network mapping**

Network mapping functionality in OpManager has got exciting enhancements such as

- LLDP Support Helps to enhance automatic network discovery in multivendor networks
- Multiple Subnet Range support - Allows you to add multiple subnet ranges. This helps you to choose the desired network range and map them together
- Some of the other network mapping features that are newly included in Fluidic webclient are :
  - SNMP V3 support
  - Option to change Layout
  - Export to visio
  - Multiple Parent support

- Options to Edit, Update and Delete a network map
- Support for L2 Switch as Seed device

3. **SIEM Plug-in for OpManager (EventLog Analyzer)**

With the help of ELA Plug-in, you can now effortlessly manage terabytes of machine generated logs, monitor file integrity, conduct log forensics analysis, monitor privileged users, comply to different regulatory bodies and instantly generate variety of reports.

It also offers Real-time Event Correlation with over 70+ out-of-the-box correlation rules for proactive threat management and triggers alert notification via E-mail & SMS or Program execution. In-addition you can also set alerts based on specific type of compliance violation for HIPAA, GLBA, PCI-DSS, SOX, FISMA, etc.

4. **OpStor Plug-in (Storage Management)**

OpStor Plug-in enables 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. It provides a unified view of storage environment along with effective reporting which in-turn increases visibility and reduces the time taken to detect any faults.

Storage Capacity forecasting helps you to predict the future storage needs by analyzing the usage & traffic utilization trends. Further, the OpStor Plug-in also provides topological map, real-time graphs & various reports on resource utilization, device availability and performance trends.

5. Hardware monitoring support is now available for the Domain Controller category

OpManager v11.3 Build No - 11300 (May 19th, 2014)

1. OpManager now includes the highly productive, faster and API driven user interface by default. The new web client will be the default UI for new installations. However, the existing customers can use the same old client and switch to the new UI anytime.
2. OpManager now includes Social IT- a private social networking medium built exclusively for IT folks. Social IT provides a cascading, Facebook-like wall for threaded discussions enabling real-time collaboration/communication between IT staffers. This Social IT integration is available only in the new API webclient.
3. Now you can configure OpManager to detect event floods and anomalous event rates with predefined rules. Click here to know more about OpManager's event flood handling functionality.
4. OpManager now supports monitoring of Windows 2012 R2 & HyperV 2012 R2.

OpManager v11.2 Build No - 11200 (Feb 24th, 2014)

Device Discovery in Large Enterprise Edition:

- With the improved Discovery engine, you can now discover up to 20,000 devices in 5 minutes & 1 million interfaces in 1hour
- In Large Enterprise Edition, device discovery will no longer include the discovery of interfaces. For discovering the interfaces, you will have to use the "Interfaces Discovery" section

API Client Enhancements

- Live popup notifications have been added to instantly alert you about the alarms raised
- Now you can make use of the keyboard shortcuts to traverse between device snapshot pages & alerts. You can also use the shortcut keys to pickup/clear/delete any alerts
- With the help of Heat Map, you can now get the status of all the monitored devices in real-time from a single page
- Virtualization maps for VMware & Hyper-V enable you to view the relationships among hosts, clusters, and virtual machines

REST API Enhancements

- Includes support for more than 330 REST APIs

Layer2 Enhancements:

- Discovery of non cisco devices and end nodes (server, desktop) are now supported
- Now you can also draw the Layer2 Maps for the devices which are not discovered/ monitored in OpManager

Other Enhancements:

- Support for iPad App
- ITPulse tab has been removed from the product as it is EOLed

OpManager v11.1 Build No - 11100 (Nov 15th, 2013)

- CMDB Plug-in Support - The Plug-in helps you to get in-depth visibility of your assets present in your IT environment. This allows you to manage all your IT components based on their business criticality and make informed decisions
- Root Cause Analysis - Enterprise IT departments need sophisticated monitoring for each aspect of their operations, from basic infrastructure to bandwidth, applications and change management. However, these sophisticated tools churn out alerts at an alarming rate and volume, making it difficult to manipulate the alerts and find the root cause of the problem. This is now supported in OpManager
- Functional Expression Support - Functional Expression such as Byte to GB, Celsius to Fahrenheit, String to Numeric, Column Min , Column Max, Numeric to String etc are now supported for SNMP based monitors. Option to store or just alert is also provided now.
- Multi language Support - Language selection options such as Chinese, Japanese, French, Korean etc. are provided in the OpManager webclient
- Notification Profile / Alarm Escalation
    - Option to view the latest Polled Value available for recurring notification and escalation mails
    - Alarm Entity parameter is available now for notification
- Pass Through Authentication support is available now
- Security vulnerability in Postgres database is addressed now.
- Reports - A new report to list all the threshold configured devices is available now
- Around 75 device types are newly added
- Alarm Suppression Configuration is audited now
- Regular expression support provided for Event Log description
- Infrastructure Widget - Option not to show a particular category , if there is no devices present is addressed now

OpManager v11 Build No - 11000 (September 30th, 2013)

OpManager Large Enterprise Edition Release:

1. A single OpManager Large Enterprise Edition server can hold up to 50,000 devices or 1 million interfaces in a single box. It is twenty times more scalable than the enterprise edition.
2. Has twenty times faster discovery engine - Discovers 20,000 servers in 5 mins.
3. Integrated Layer2 Discovery with automated dependency to avoid false alarms.

4. New API client released as THEME for opmanager. Completely built with Ember.js and APIs. Works ten times faster with real-time updates.
5. Multi Language Support.

OpManager v10 Build No - 10200 (July 22nd, 2013)

Widgets

1. In Performance Monitor widget, Sort Column option is added in Top N Monitored Values
2. Business View Summary widget now includes alarm count and list of devices in business view
3. Option to choose a dashboard when creating new tab
4. Embed widget option to hide headers
5. Open CCTV View link from Manage CCTV page
6. Last Polled Value time period option in following widgets

    - Devices by CPU Utilization
    - Devices by Memory Utilization
    - Devices exceeding N % CPU Utilization
    - Devices exceeding N % Memory Utilization
    - Top N Min/Max/Average CPU Utilization
    - Top N Min/Max/Average Memory Utilization

Schedule Reports

Notification subjects and messages can be configured by the user. Default parameters are Scheduler Name, Report Description, Report Period, Report URL etc.

Rule Engine

1. Support for MSSQL monitors & URL Monitors are provided in Rule Engine.
2. Provision to add a URL as templates is available now.

MSSQL Monitors

In MSSQL device snapshot page, Delete Option is provided in MSSQL Instances and MSSQL databases.

Archiving

Option to Re Run Archiving is newly added in the Database maintenance page. This feature will be useful in-case the hourly or daily archiving is missed due various reasons such as server maintenance shutdown, database disconnection etc.

Workflows

NCM Plugin actions such as Backup, Execute command, Execute template, GetLast N Changes are added as Workflows.

Hardware Monitors

1. Option to enable/ disable hardware monitors is added
2. Option to suppress alarms for hardware monitors is supported now

Device Templates

1. Option to configure Sys Description is added
2. Operators such as Equals, Not Equals, Contains, Not Contains, Ends with, Starts with etc are now supported in device templates
3. Option to export and import device templates with multiple rules is provided.

Tabs

New tab link 'All Devices by Disk Usage' is added under Maps tab, with the filtering option and the option to delete drives

Maps

Option to set the view as default for SLA Dashboard is added

Reports

Interface aggregate data graphs are added in the new Opmanager API Client

OpManager v10 ﷺ Build No - 10100 (May 7th, 2013)

1. With OpManager's new 3D Data Center Builder, you can virtually create an exact model of your racks and data centers. You can embed these datacenter designs on your NOC screens and monitor them 24x7 from anywhere, anytime. The 3D data center can also be viewed from iPad and other tablets.
2. A high productive, ultra-fast, responsive, API driven new UI is ready to use. Built completely on a new JavaScript framework it offers you 10x more productivity than the previous one.
3. You can now avail APM plugin in OpManager central webclient also. Previously the plugin was available only in the standalone version.
4. Now you can make you of APC PDU (Series 7800/ 7830 / 8841/8858 / 8858NA3) templates which are newly added to list of OpManager device templates. With the help of these templates, you can monitor parameters such as PDU Phases, PDU Power/Phase Load, PDU Voltage, PDU Bank Load & many more

OpManager v10 ﷺ Build No - 10000 (March 18th, 2013)

1. Now OpManager provides support for monitoring IPv6 network devices and servers. After discovery, device templates along with the essential monitors are applied on the IPv6 devices and monitored for performance.
2. Applications Monitoring plugin for in-depth monitoring of applications such as Oracle, SAP, Sharepoint, Websphere and much more has been added now.
3. Get granular insight into your VMware environment, as OpManager now monitors VMware ESX/ESXi and VMs through vCenter via vSphere API.
4. Now OpManager out-of-the-box monitors hardware health such as temperature, voltage, power, fan speed, status of processors, storage, memory, disk arrays, etc. of HP, Dell, Cisco and Juniper devices, via SNMP. OpManager also supports hardware monitoring for ESX hosts via vSphere API.
5. Failover support for OpManager Central server has been added now. Probe already includes support for failover.
6. Now raise a ticket with OpManager support along with the support information file, in a single click (Support-> Request Support).
7. Adding notes to an alarm has been simplified now. In alarms page, now you can add alarm notes by clicking ontem the "Note addition button" present beside each alarm notification. You can also add alarm notes in bulk by selecting the desired alarm notes and clicking on "Add note" button.
8. In Enterprise Edition, the intelligence to detect build mismatch between Probe and Central has been added.
9. Time Window option has been added in Schedule Reports page (Issue ID 91998)

10. Time out and max hops are now supported in TraceRoute in both RestAPI and Workflows.
11. Search filtering option added in All Devices and All Interfaces page

OpManager v9 🚀 Build No - 9400 (November 29th, 2012)

1. iPhone App for OpManager: Connect to OpManager server and view the performance of all the devices, recent alarms, and business views from your iPhone. Download the App now.
2. OpManager supports monitoring Windows 8, Windows 2012, and MS SQL 2012.
3. OpManager supports monitoring NetApp storage devices. [Watch Video]
4. Now authorize AD group users with different access privileges to access OpManager web-client with the new AD authentication feature. [Instructions to configure]
5. A seamless integration with ManageEngine ITPulse, the private social network for IT. OpManager will posts event status automatically in ITPulse, when a technician acknowledges, unacknowledges, or clears an alarm in OpManager. You can also view the details of such alarms from ITPulse itself and discuss the troubleshooting steps. [Watch Video]
6. The NCM plugin data and reports can be added as widgets in the dashboard page. Also OpManager now raises alarm for change detection and backup operations done by the plugin.
7. OpManager now includes option to view config changes, execute backup/commands from the device snapshot and alarm pages itself.
8. New APIs are available for listing the alarms and devices, triggering a notification profile, and more.
9. OpManager provides option to execute notifications and workflow repeatedly until an alarm gets cleared.
10. To avert false positives, the consecutive times check for status polling is now extended to service monitors, Windows service monitors, interface poll and event log monitors.

Virtualization (VMware & Hyper-V)

1. OpManager includes provision to add event log rules on Hyper-V host server.
2. OpManager includes option to create custom WMI monitors form Hyper-V host and Virtual machines from their respective device template page.
3. OpManager now supports changing the category of virtual devices.
4. IT Automation tab with options to view and create workflows has been introduced in ESX & Hyper-V server snapshot page.

API

1. API now supports JSON output in addition to XML format.
2. In 'Associate device to Notification Profile' API, an option to provide the list of thresholds has been added.
3. In 'Add Device' API, you can now provide the device type and display name in addition to the device name.
4. Support for associating multiple devices has been added in 'Add device to Business View' API.

Workflow

1. Workflow supports new actions like creating OpManager alarms and folder. And also provides wildcard support for file related tasks.
2. The admins can now forcefully shutdown/reboot/logoff the remote machine using shutdown task option in Workflow.
3. Delete older files option in Workflows can now check and delete older files in subfolder also.
4. System Settings
5. OpManager now includes options to configure Date/Time format and also enable logging at runtime, under Admin -> System Settings.

Business view

1. In Business view, now you can zoom in/out.
2. Option to enable/disable traffic arrows for the links is provided now.
3. It is now possible to associate a link to multiple devices in a business view.

Others

1. Options have been included to create charts with data points, stacked area chart and to show the threshold value line in the graph.
2. Separate Alarm is raised for Status Poll, Service down and Windows Service down for better clarity and granular notification handling.
3. Now devices notes can be added in bulk via a CSV import.
4. Option provided to bind OpManager to a particular IP address of the server instead of all IP addresses in the machine.
5. Process monitoring feature is now enhanced to monitor, alert and report on absolute value of process memory in addition to percentage utilization.
6. Delete all option provided to purge the Unsolicited Trap.
7. Discovery Rule Engine now has option to manually rerun the rules against a set of devices.
8. Device Templates has been enhanced to provide a custom OID check in addition to SYSOID for classification.
9. Regex support is now provided for String based threshold setting.
10. The traps raised from the IP address can now be mapped to the source server with option to configure the IPMI address for SNMP traps.
11. License changes - Only managed devices are counted for license.
12. WebAlarm link is now included in CCTV view.

OpManager v9 &#65533; Build No - 9200 (July 10th, 2012)

1. **IPAM Plugin *:** IP Address Management plug-in helps you manage your IP Address. It also includes Switch Port Mapper to identify the switch port to which a device is connected.
2. Discovery Rule Engine: Automate actions such as adding monitors, associating the devices to a business, etc. that you carry out after adding the devices to OpManager.
3. **Tab Customization:** Customize OpManager web client by creating tabs for frequently visited pages, third-party embeds, reports, etc. and navigate easily in a click. You can also modify and delete existing tabs.
4. **Multiple Threshold support:** Configure multiple thresholds for the performance monitors. You can now set multi-level performance thresholds for a monitor and alert at different levels.
5. **Log File Monitoring *:** - Agent based: Monitor log files of mission critical applications such as MSSQL, Oracle, etc. in real-time. The agent constantly monitors the log files for content that may even be a regex.
6. New Audit Report and Enhancements to Monitor Health Report: Get real-time security audit report in OpManager at a mouse click, and also experience some of the high end enhancements made to monitor device health report.
7. You can now forward Traps and Syslog events from OpManager to any other NMS through Trap/Syslog Forwarder from OpManager GUI.
8. The new improved network discovery engine is 5x faster and discovers over 5,000 interfaces in a minute.
9. Faster Discovery Enhancements.
10. Support for VMware UUID & Replicated VM's.
11. Configurable options are provided in SDP to create new ticket or reopen existing ticket on reoccurrence of an alert.
12. New VMware reports for Datastore Top Read & Write Latency are included.
13. New Workflow action "Refresh Datastore" is added to the list of several workflow actions.
14. Configurable Timeout option is included in Mail Server Settings.
15. Option is provided to enable protocol level logging at runtime in System Settings.
16. More enhanced rebranding changes are made configurable via brandprops.properties file.
17. New Category "Storage" has been added to device category list.
18. New device templates are included for NetApp/Cisco Routers.

OpManager v9 &#65533; Build No - 9100 (March 1st, 2012)

1. Major enhancements have gone into the Map Maker which includes curved lines, localized names, customized line thickness, easy drag-drop etc.
2. The long-awaiting option to export and import device templates and share them with the community, is now available. The shared device, workflow, and script templates are listed under the RESOURCES tab in our forums. The shared template are validated and approved before displaying them here.
3. Support for Korean language installation is provided.
4. SSH key authentication for monitoring Unix-based devices, can now be given as file inputs., viz. instead of specifying the user name and password in the OpManager credentials GUI, you can store them in a file and give the file as authentication input.
5. Option to provide timeout in CLI credentials added.
6. You can now test the authentication credentials for multiple devices at one go, instead of testing it for each device.
7. Keep a tab on the monitors for which data is not collected for a specified period by accessing Support Diagnostics GUI.
8. The credentials configured are now grouped by the Protocol and listed for easy manageability. For instance, you&#65533;ll see the grouping when adding a new device for discovery.
9. A new device template is included for Cisco5508WLC devices.

0. When configuring trap processors, you'll be able to select up-to the 20 Varbinds as part of the match criteria.
1. New graph Memory Utilization (UCD SNMP MIB) is added by default.

OpManager v9 – Build No - 9011 (January 5th, 2012)

If OpManager detects a DB collation mismatch during PPM upgrade, a system alert is shown to avoid partial upgrades.

OpManager v9 – Build No - 9000

1. IT Automation Workflows to automate 1st and 2nd level administrative tasks. Few pre-built workflows available out-of-the-box, and intuitive drag and drop GUI to create more custom workflows.
2. A hot-standby for Probe to ensure high availability. Seamless failover and failback between the primary and secondary probes and 100% data integrity.
3. REST API support in OpManager to help integrate with third-party help desk, NMS etc; operations supported include adding a device, adding a notification profile etc.
4. Define custom scripts and leverage OpManager's fault management to the fullest. Supported scripts include Powershell, Linux shell script, VBScript, Phython & Perl.
5. Virtualization management support now extended to Hyper-V devices in addition to VMwares; monitor over 70 deep metrics!
5. The GUI has got a new face-lift with new tabs organization for easier and intuitive navigation.
7. Quick links are included to access help on how to configure tasks in OpManager and perform first level troubleshooting. These can be enabled/disabled from Admin > System settings.
3. Support for NFA and NCM plug-ins in Probe (Enterprise edition).
9. NFA plug-in now supports 64 bit Windows and Linux installation.
0. Dashboards are introduced for Business View users.
1. Configurable color coding is included for Utilization widgets (Red for over 90%, Yellow for over 80%) [Editable range value (Top 10,12,15) for widgets. (Previously it was a drop down box Top 10, 25, 50)]
2. An option to specify the consecutive number of times a device is polled/threshold is violated, is included in the device templates specific to Virtual devices.
3. You can now edit the threshold type/value of resources defined in the Virtual Machine device templates.
4. It is now possible to edit and save the IP address from the ESX Host snapshot page.
5. If you want to configure bulk URL monitors, you can specify the links in a CSV file and bulk-import them into OpManager at one go!
5. The folder monitoring feature enhancement includes wildcard (file filtering) option.
7. Sixteen new templates are included for A10 networks & blackberry devices!
3. An option is included to apply a change made in the interface template to all interfaces.
9. An option to rediscover the interfaces that are deleted from the device, is included.
0. A list-view is now available for Exchange servers with an option to add a server into exchange category directly.
1. The AMS validity is shown in the GUI with a link leading to renewal procedure.
2. New dashboards are included to show top 10 server and top 10 networks.
3. An automatic notification is triggered when the Probe is down (Enterprise edition).
4. A "View Associations" option is included in Admin > Notification Profiles screen to quickly see a summary of the different profiles associated to the monitored devices.
5. A new device down time report is provided. The report also shows the outage history.
5. Localization support is extended to have the Probe name in Japanese or Chinese (in the respective local installations).
7. You can now add Probes in the Google Map.
3. An option is provided to enable/disable the discovery of a VM in a host.
9. For VMs that are also DomainControllers, the snapshot page is enhanced to show the interface details in two different tabs, one for the Virtual NICs and the Interfaces.
0. The performance monitor widgets now show the instance name in addition to the device name.
1. A new device template is included for Windows 2008 R2.
2. When configuring alarm escalation or when scheduling a report, you can now select the site too (specific to Enterprise edition).

OpManager v8 – Build No - 8812 (August 17, 2011)

1. The Alarm reports page now has option to filter alarms based on its properties; This report can be exported to .pdf, excel formats and can be emailed.
2. Option to escalate alarms via SMS in addition to email, is included. Option to configure URLs in Alarm Escalation is also added.
3. You can now associate any type of notification profile to a particular or to a group of URL Monitor. This functionality is available under the individual URL monitor page and at the "Quick Configuration Wizard" option.
4. You can now edit or update or add new mail store location for Exchange monitors.
5. Google map integration is enhanced now to show the location of the device both in the Google Map as well as in the Google Map widget.
5. Device search option is now extended to search "interfaces" using interface name or IP address and for "URLs".

7. When polling devices using ICMP ping for availability, choose which round-trip-time metric (Minimum? Maximum? Average response time) you want to show as Device Response Time under device availability. By default OpManager shows the average response time and you can change this now by editing Ping.properties file.
8. A new widget is added to show the total bytes transferred.
9. When reports are scheduled and emailed, the users with non-admin privilege can also access and view the reports.
0. Alarm ID is now configurable in the notification profile both, as part of the subject or/and the message.
1. In the device template "list of monitors", a multiple-select check box is provided against each group of monitors. The same option is available while associating monitors from the device snapshot page.

OpManager v8 &#65533; Build No - 8810 (May 9, 2011)

1. VMware ESX?ESXi version 4.1 is now supported.
2. View the domain controller dashboard in VM snapshot page.
3. Apply warning and error thresholds across multiple ESX hosts and VMs using Device templates.
4. NFS datastore reports are added for ESX v 4.1. Generate reports such as Disk Read Speed, Disk Write Speed, Write Latency, etc. on datastore.
5. Discover VMs also using the "Add Device" option under the "Admin" tab.
6. Get more meaningful and actionable SNMP Traps by processing every Varbind with intelligent processor.
7. Port? Interface monitoring has been enhanced for better performance.
8. Embed OpManager dashboard widgets as iframes into other sites
9. Network rediscovery now shows split&#65533;up of already discovered devices and new devices count.
0. Web client page loading time is now displayed in every page.
1. Options are included to change the Traffic Counter (32? 64 bit) at individual interface level.
2. Interface parameter (ifalias) can be updated in OpManager by performing interface rediscovery operation.
3. UTF&#65533;8 Unicode is now supported in OpManager.
4. UPS interface details are monitored and shown now.

OpManager v8 &#65533; Build No - 8723 (February 15, 2011)

1. Community page enhanced to reflect industry benchmarks for resource performance.
2. An option is included to configure subject for the email&#65533;based SMS profile.
3. Provision to add STM files besides .edb in Exchange Mail and public store.
4. A new report to reflect total bytes transferred is included in the Reports tab.
5. You can now specify match criteria for threshold values in the Interface templates.
6. Interface properties ? Custom fields for interfaces are added in notification profiles.
7. Interface snap shot page refreshes now based on the refresh interval configured in the &#65533;Personalize&#65533; settings.
8. All Interfaces?Utilization reports are enhanced to show the links capacity. Columns are included to show Inspeed and OutSpeed values
9. A new Widget is included to display tips to troubleshoot and workaround some configurations and tweaks in OpManager.

OpManager v8 &#65533; Build No - 8722 (December 27, 2010)

1. Support for adding non ping-able device is included now.
2. Support for scheduling downtime for consecutive days is provided in Monthly Day-wise option.
3. WAN link report has a link to the interface and device snap shot page.
4. Domain Controller category is now listed in URL response widget.
5. Process monitoring - Down alert is generated if the instance count is 0 and &#65533;consecutive times&#65533; field is configured.
6. Device Templates now have a &#65533;Copy As&#65533; option to enable saving the same template under a different name.
7. During Failover, email notifications are sent when:

    - The Standby server is not started.
    - Data replication process is not completed during standby server startup.
    - If data replication fails during take over.
    - Appropriate message is shown to the user, if the client is connected to standby server in standby mode.

OpManager v8 &#65533; Build No - 8721 (August 30, 2010)

1. The Downtime Scheduler now has an option to schedule a downtime on a monthly basis
2. Monitoring of Exchange 2010 is now supported
3. The notification criteria for the Printer and UPS includes variables like paper jam, low toner, low battery etc.
4. The threshold configuration now allows you to select ﷺNot Equalsﷺ as a match condition
5. OpManager Webclient, if invoked before the OpManager server process, reflects the status of OpManager process
6. The reason for a credential failure is shown on clicking the Test Credentials button
7. More time options such as 1, 2 , 4, 6 hours have been included in Widgets
8. New widgets are included to show devices and services that are down, and also to show the business view traffic map
9. An email notification is sent when OpManager loses connection to the database
10. If the Syslog port is occupied, a message to this effect is shown in the Syslog Rules page
11. A hyperlink to the alarm details page is added in the notification mail message
12. The About page shows the latest build number available for download on the OpManager website

OpManager v8 ﷺ Build No - 8720 (July 16, 2010)

1. Exhaustive ESX VMware Monitoring using VMware APIs. Supports monitoring ESX 3.5, ESX3.5i, ESX4 and ESX4i
2. Automatic Layer 2/ Layer 3 network mapping
3. Supports configuring Mail server with ssl support
4. New collection of widgets for Service and Process Monitoring added
5. New set of device templates and monitors included
6. Category ﷺUnknownﷺ has been introduced
7. NetFlow plugin version 8000 released. Click here to upgrade to the latest NetFlow plugin release.
8. NCM plugin version 5500 released. Click here to upgrade to the latest NCM plugin release.

OpManager v8 ﷺ Build No - 8052 (Apr 27, 2010)

1. A new CLI-based monitor for partition details of a device is included.
2. Alarm Details page has been enhanced to show the name of the log rule that triggered alarms (for Syslogs, Event Logs, and SNMP Trap based alarms). You can also edit the rule from this page.
3. The status of a Downtime Scheduler (in progress or not) is now shown in the schedule listing page.
4. You can now revert a reﷺbranded installation of OpManager to the original settings that will default to OpManager logo and images.

OpManager v8 ﷺ Build No - 8051 (Mar 2, 2010)

1. Link to OpManager Community portal is included as a separate tab.
2. Support extended for managing Windows 7 devices.

OpManager v8 ﷺ Build No - 8050 (Jan 8, 2010)

1. Data is collected every 5 minutes in the WAN RTT Monitor
2. Hop graphs are now shown for every RTT path from source to destination
3. Data is collected every 5 minutes in the VoIP Monitor
4. OpManager now supports 64-bit OS
5. File and folder monitoring for Windows devices
6. Provision to create custom WMI monitors in addition to the already available SNMP-based custom monitors. You can also associate these monitors from the device templates
7. Users can now access the OpManager web client using iPhone or Blackberry user interfaces
8. A new network traffic map to let you quickly identify highly utilized network links
9. OpManager now also alerts via Twitter Direct Messages
10. More device templates included taking the templates count to over 650 device types out-of-the-box
11. Provision to monitor custom event log categories in addition to the default Windows event logs
12. Reports enhanced to include NT Services and Process availability reports
13. Scheduled reports are now available for all reports and monitors
14. Support to export reports as Excel files now extended to all the in-built reports

OpManager v8 &#65533; Build No - 8025 (Nov 23, 2009)

1. Alarm Notifications Include alerting through RSS feeds
2. Provision to edit existing user privileges

OpManager v8 &#65533; Build No - 8024 (Oct 9, 2009)

1. The tools in the Device Snapshot page now includes SSH? HTTPs options
2. Export of Switch Port Mapper Reports as PDF or Excel files. Option to send the report via email also included.
3. Ability to send SMS if the OpManager server loses network connectivity.

OpManager v8 &#65533; Build No - 8022 (Aug 11, 2009)

1. **Notification Profile:** In addition to &#65533;Custom Fields for Devices&#65533; and &#65533;Alarm Variables&#65533;, &#65533;Device Properties&#65533; such as Device Type, Device State, RAM, Disk, IPAddress etc. can now be added to all the notification profiles
2. **Notification Profile:** Option to add &#65533;Custom Fields for Devices&#65533; and &#65533;Device Properties&#65533; as arguments for Run System /Run Program command
3. Option to select the required Devices is provided in the MIB Browser
4. Provision to set the &#65533;List View&#65533; as default map view
5. Option to view the current downtime details in the Outage History reports
6. Interface Real time graphs will be shown by default for all the users, irrespective of license applied
7. The Netflow dashboard can now be seen from the OpManager webclient if the Netflow plugin is installed

OpManager v8 &#65533;Build No - 8021

1. **Enhanced Alarm actions:** Option to perform Ping, Trace Route, Test Monitor, Actions, Manage/ Unmanage devices, RDP & much more for every alarm.
2. Email Notification will have a link to device snapshot page for faster access to OpManager web-client
3. Ability to add Google maps to Custom Dashboards
4. Option to sort entries in Infrastructure view widget
5. WMI&#65533;based partition details are added out&#65533;of&#65533;the&#65533;box

OpManager v8 &#65533;Build No - 8020

1. Alarm Suppression: Suppress the alarms of a specific device for a pre-defined time interval.
2. Faster Backup and Restore utilities
3. I18N Internationalization issues fixed (For Japanese and Chinese Language)

OpManager v8 &#65533;Build No - 8007

1. Provision to add Telnet/SSH port number for devices discovered/monitored though CLI.
2. A new option to configure the consecutive times when the alarm should be generated has been added for URL monitors
3. Option to view the Real time graphs for the premium license users
4. SLA Dashboard now shows for business views
5. Option to configure Notification for interfaces belonging to Servers and Desktop category has been added
6. In the device snap shot page, instead of average data the latest collected traffic data is now shown
7. Configure tab option added in the interface snap shot page
8. Bar image option added in All servers disk usage report
9. Default monitors added for MGE and TrippLite type UPS
10. Provision to view the "About" and "Register" link is removed for Read only users
11. Interface name with special character are listed in customizable dashboard widgets
12. Option to monitor the cumulative resource usage for VMware server is enabled, even without the add-on license. (Note: VMware Dashboard still requires add-on licensing)

OpManager v8 &#65533;Build No - 8000

1. Plug-in for Network Configuration Management (NCCM).
2. Syslog Monitoring.
3. More performance monitors for Windows infrastructure.
4. Customizable dashboards.
5. Plasma TV/CCTV View.
6. List view or Bulk configuration view.
7. Real time graphs for performance Monitors (CPU, Memory, Disk & etc.)
8. Real time Traffic and Bandwidth graphs.
9. More Device Tools (RDP, Telnet apart from Weblinks, Trace Route, Ping and etc).
0. Process Monitoring Template.
1. Superior Interface Snapshot page.
2. Enhanced Reports.
3. Failover Support.
4. Intro Tab - To facilitate fast deployment of OpManager.

OpManager v7 ﷺBuild No - 7204

1. Support for VoIP Monitoring.
2. Plug in for NetFlow monitoring.
3. All new revamped WAN RTT Monitoring (IP SLA based WAN Monitoring).
4. Over 300 new Device templates have been added.
5. Support for integrating NetFlow Analyzer Enterprise Edition (configurable from Admin-> Add-On/Product Settings).
6. Option to configure ICMP ping to the devices using IP Address or DNS Name. (NOTE - The option is provided in ServerParameters.conf file in OpManager\conf folder).
7. Option to select the Exchange server version (2003 or 2007) while configuring the exchange monitors.
8. Provision to add notes on Alarm messages for read only users.
9. Provision to configure the username/password in DBManager, if there is a change in Database credentials.
0. Ability to configure thresholds even for negative value monitors.
1. Support for monitoring OID of type Time-Ticks.

OpManager v7 ﷺBuild No - 7202

1. Ability for the devices in the Custom category to inherit the properties of another selected category.
2. Monitoring and installation support for Windows 2008. A separate device template is also included for Windows 2008.
3. Availability Reports showing the uptime/downtime in day-wise, by hours etc.
4. Provision to delete custom monitors.
5. Option to view current dayﷺs data in Active connections / mobile users / temperature monitors in the snapshot page.

OpManager v7 ﷺBuild No - 7200

1. SNMPv3 support.
2. String OID monitoring.
3. Process Monitoring in Windows and Linux devices.
4. Schedule the reports and export to Excel format.
5. Availability reports - Displays onhold, parent down, dependent unavailable, on maintenance parameters of the devices.
6. Generate Time based availability reports.
7. Sys OIDs are added for the following series Cisco 2800, Catalyst 3750, Cisco PIX.
8. Enhanced Webclient Performance wrt Mysql Database. Reduced the number of queries to access a device snapshot page.

OpManager v7 ﷺBuild No - 7100

1. Add-on for monitoring VMware ESX Servers.
2. Discover devices by importing from a CSV file.
3. Process monitoring on Windows Servers and Desktops.
4. Web-alarm enabling users to be notified of a fault.
5. Determining device availability using TCP Port checks.
6. Provision to add a device directly into a category.
7. Provision to add custom links to devices for ready reference.

3. Provision to select a time-window for a notification to be sent.
9. Exporting reports to XLS file format.
0. Alarm escalation policies can be configured for all devices in a business view.
1. Enhanced switch port mapper showing the ports-devices mapping information.
2. URL password is now in encrypted format.
3. Enhanced the min/max values displayed in the interface reports.
4. MSSQL DB password is now in encrypted format.
5. Top 1000 Reports option is included in scheduled reports.

OpManager Support

Support information for older versions of OpManager is currently unavailable in this portal. Please click on the below links to be redirected.

- OpManager v11
- OpManager v9

Additional Support

11600 Plugin Migration

- Netflow Plugin
- Device Expert Plugin
- OpUtils Plugin

PhantomJS

- Installing PhantomJS in Linux