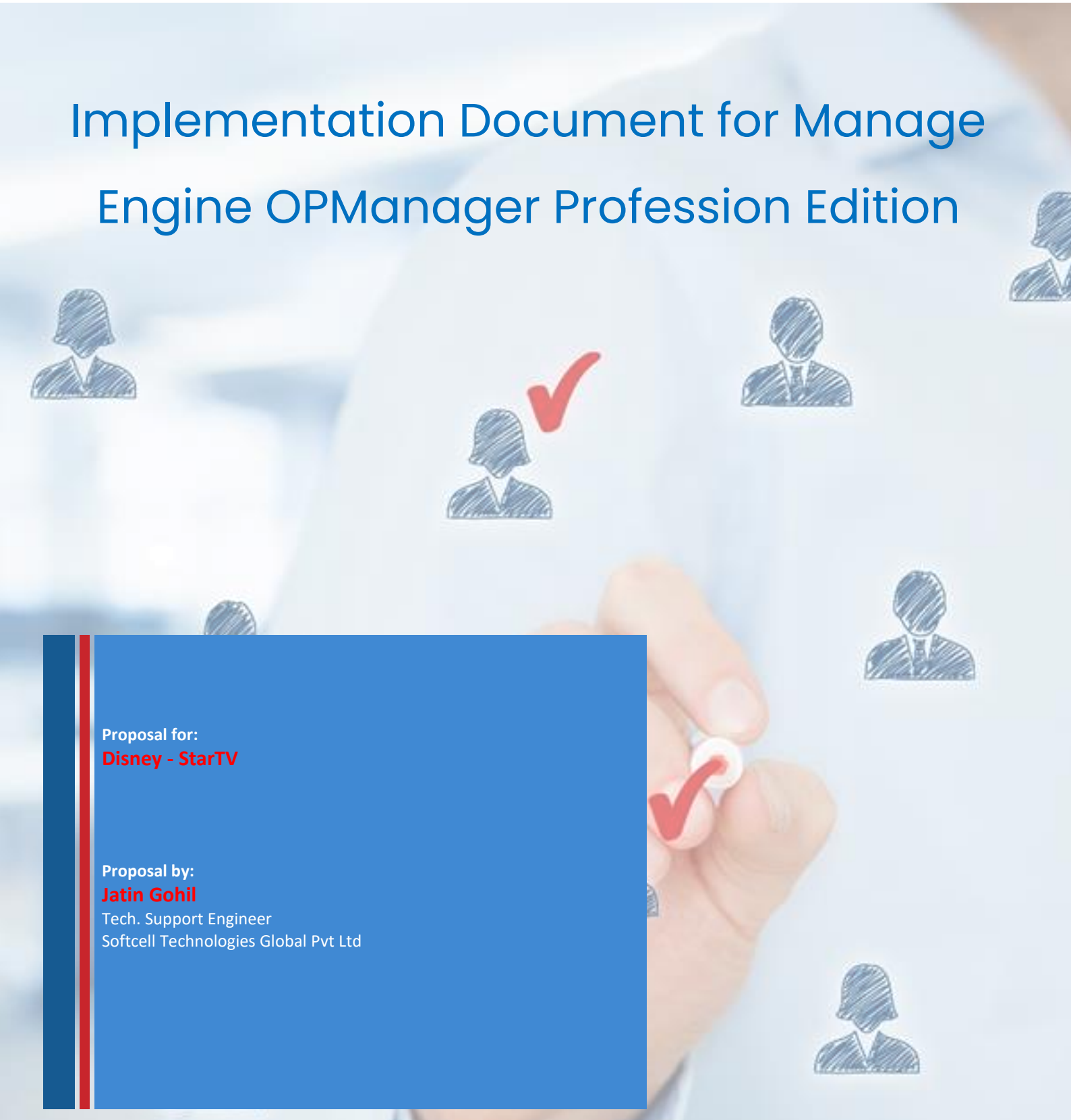
SOFTCELL
303 B-Wing, Commercial-1 Kohinoor City,
Kirol Road, Kurla (W) Mumbai
400070, Maharashtra
CIN: U74210MH1995PLC087330

Implementation Document for Manage Engine OPManager Profession Edition



Proposal for:
Disney - StarTV

Proposal by:
Jatin Gohil
Tech. Support Engineer
Softcell Technologies Global Pvt Ltd

Document Control

Item	Detail
Owner	Softcell Technologies Global Private ltd
Applicability	All teams/resources involved in the development, release, and success of the service: Architects, Consultants, Implemenatation Management, etc.

Revision History

Version	Date	Changes	Author
1	09th Dec 2022	Initial Copy	Jatin Gohil

Distribution Controls

Copy Number	Copy	Distribution
1	Approval Copy	Customer
2	Approval Copy	Account Manager
3	Approval Copy	Reports Repository
4	Other Copy	

Related Documents

Version	Date	Title	Author
1.0	09/12/22	Implemantation document	Jatin Gohil

Approvals

Created by: Jatin Gohil

FOR ANY QUESTIONS ON THIS PROPOSAL, PLEASE CONTACT:

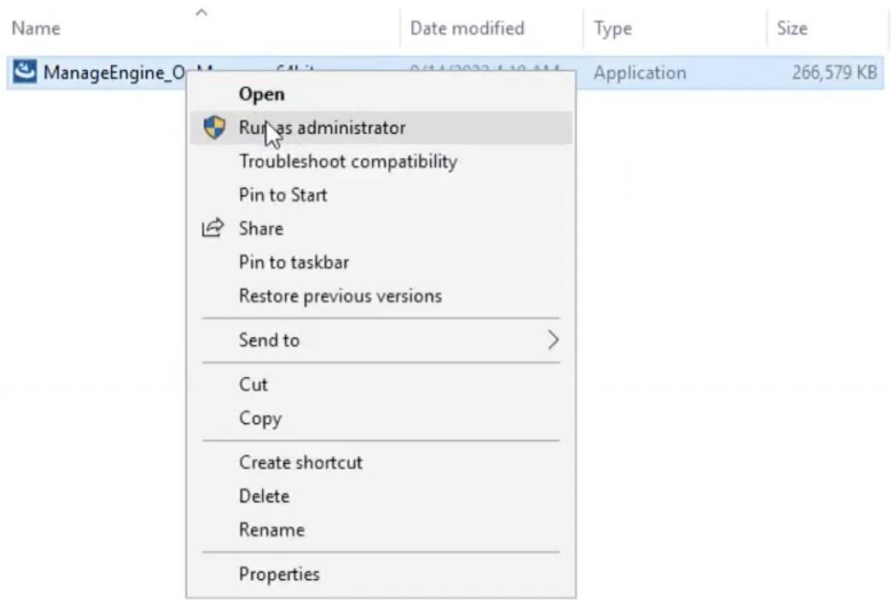
A. Jatin Gohil (jating@softcell.com)
B. Prathamesh Walavalkar (prathmeshw@softcell.com)
C. Kaustubh Deshpande (kaustubhd@softcell.com)
D. Shrikant Iyer (shriiyer@softcell.com)

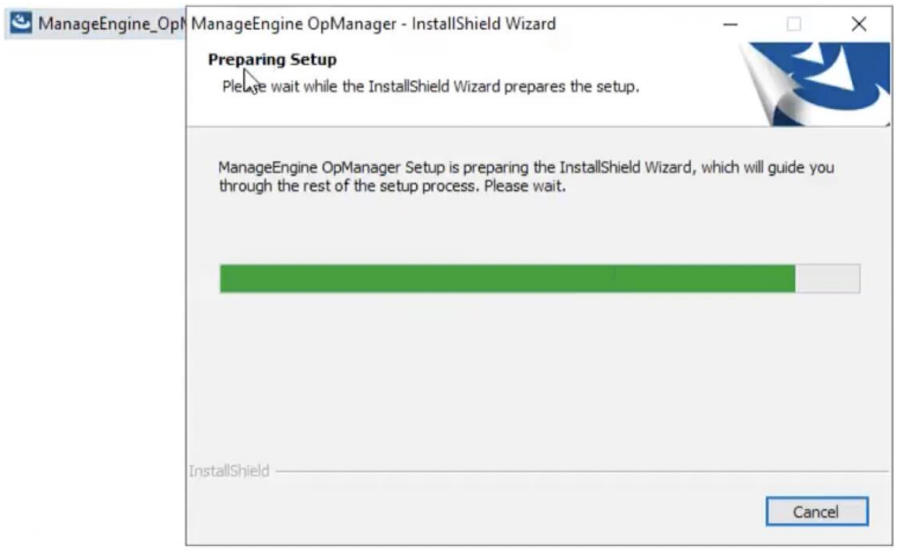
Table of Contents

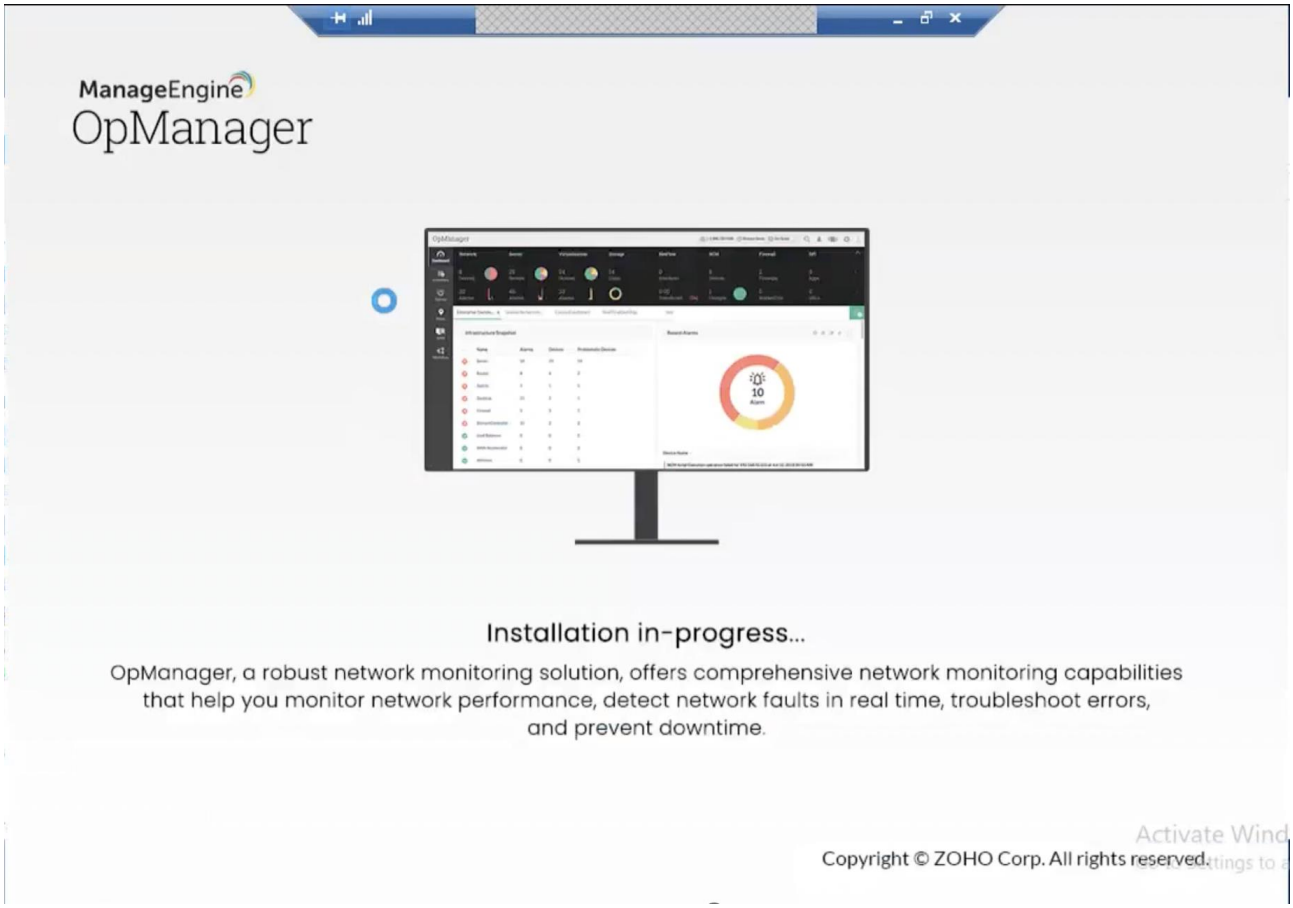
OP Manager

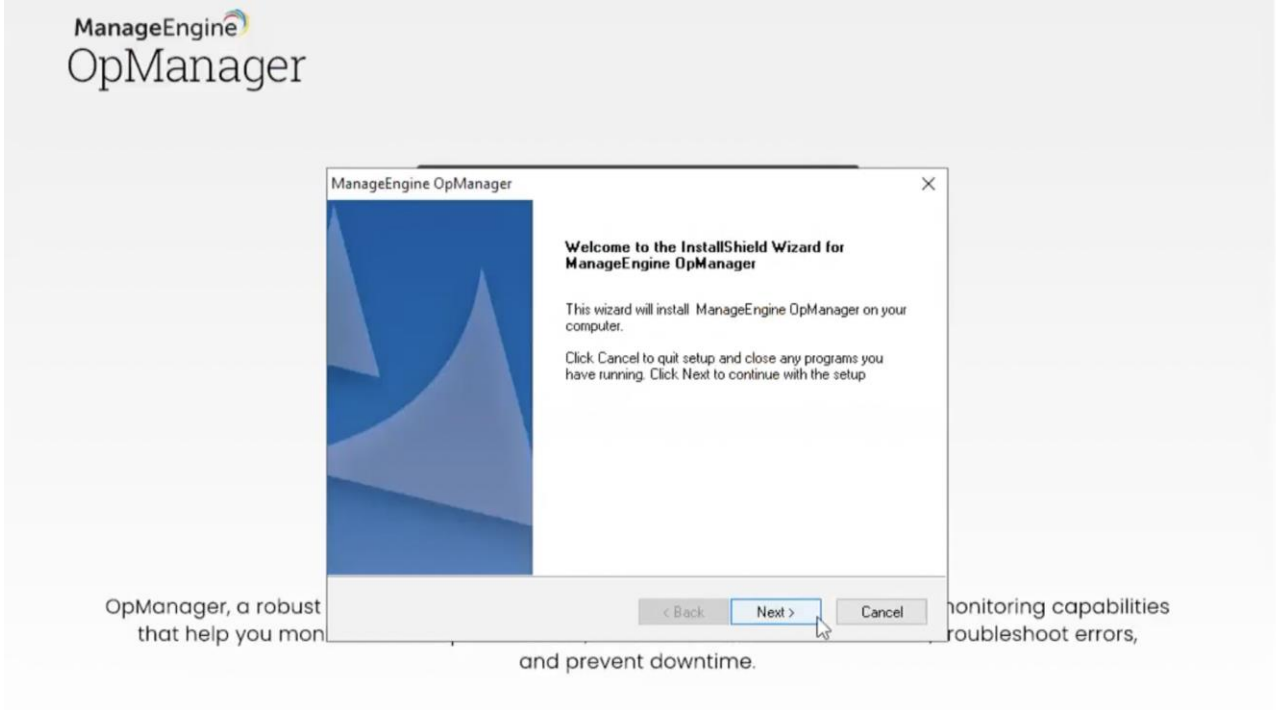
1. Installation of the OP Manager.

Navigate to the application file and click on it.

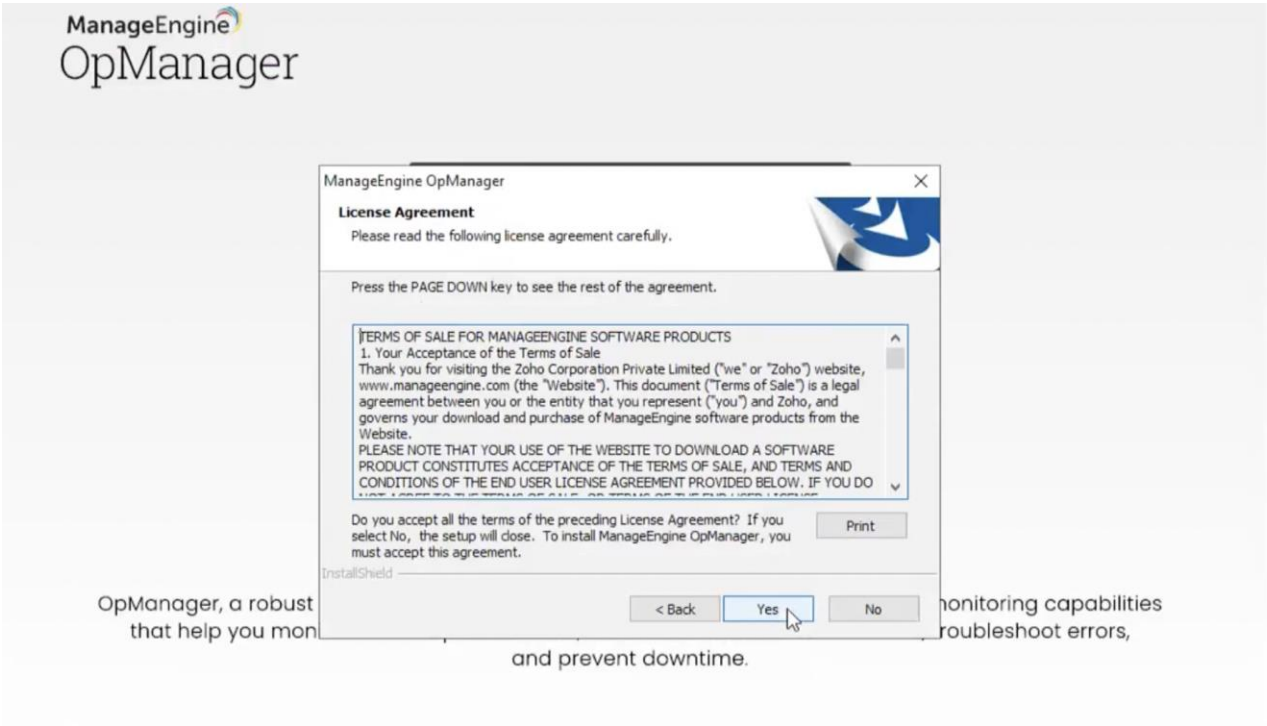




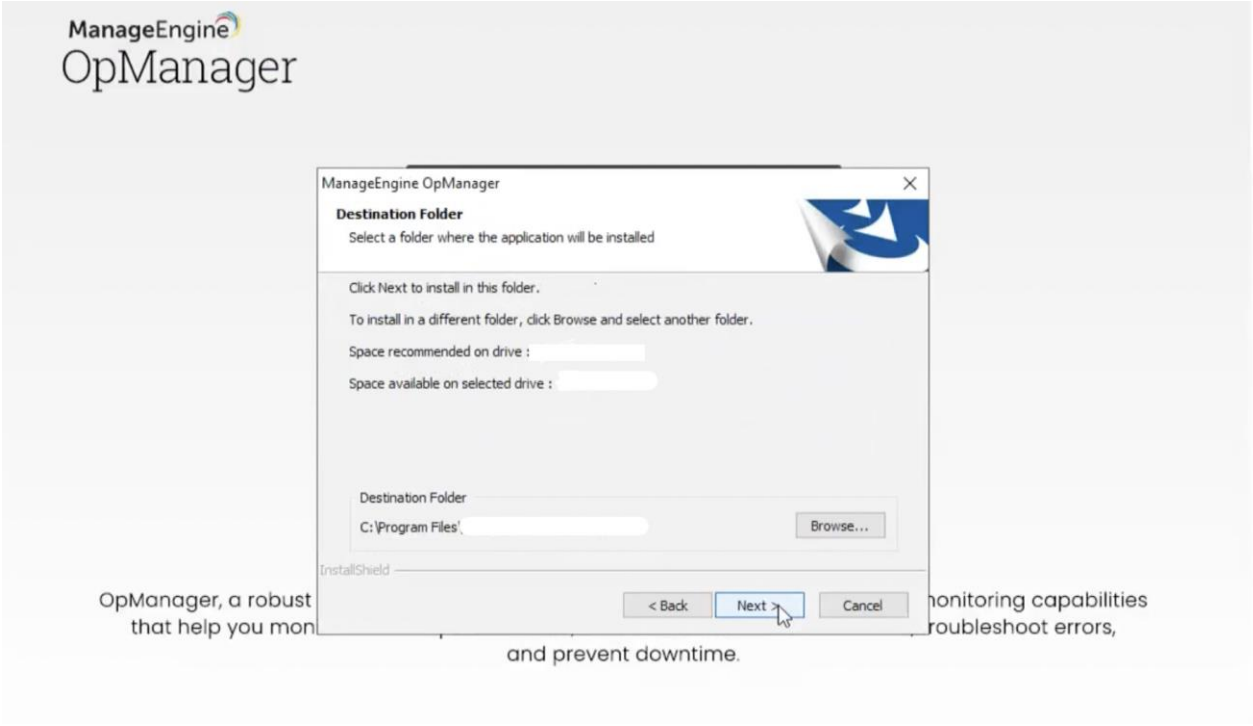

ManageEngine
OpManager
Installation in-progress...
OpManager, a robust network monitoring solution, offers comprehensive network monitoring capabilities that help you monitor network performance, detect network faults in real time, troubleshoot errors, and prevent downtime.
Activate Wind
Copyright © ZOHO Corp. All rights reserved.


ManageEngine
OpManager
ManageEngine OpManager
Welcome to the InstallShield Wizard for ManageEngine OpManager
This wizard will install ManageEngine OpManager on your computer.
Click Cancel to quit setup and close any programs you have running. Click Next to continue with the setup
< Back
Next >
Cancel
OpManager, a robust
that help you mon
onitoring capabilities
roubleshoot errors,
and prevent downtime.

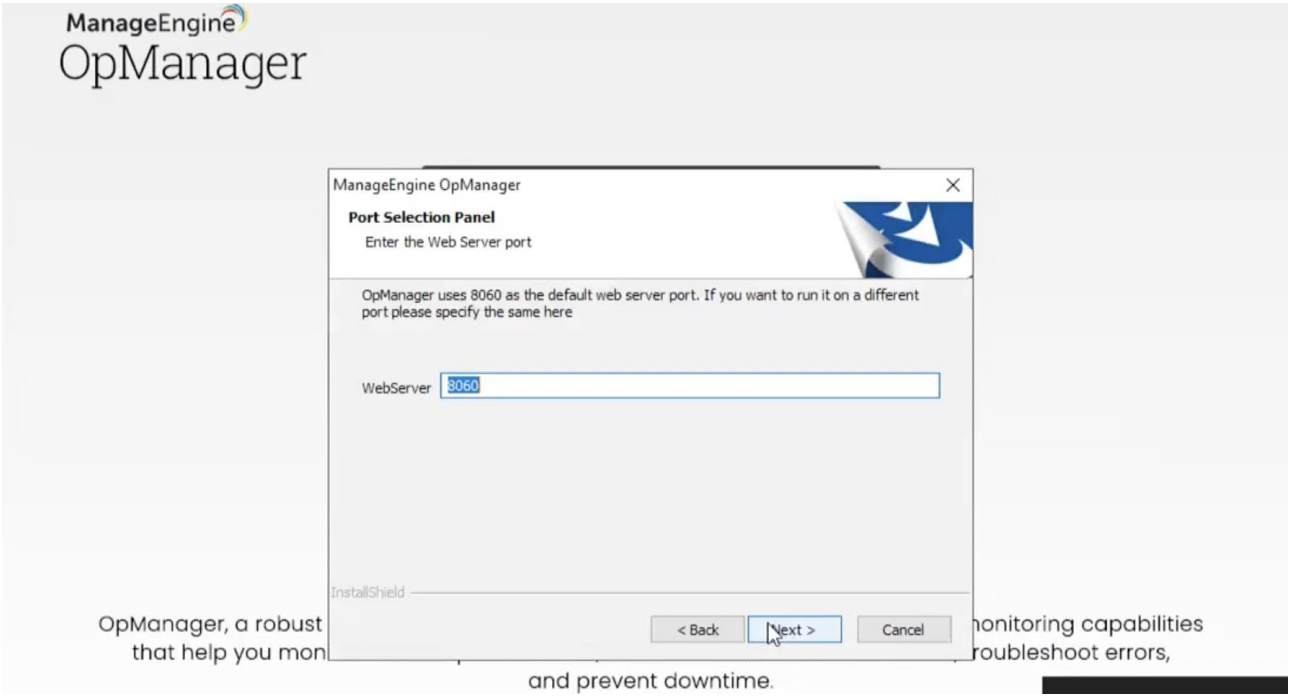
Click 'Next' to begin the installation process. Go through the license agreement and click 'Yes' to proceed to the next step.



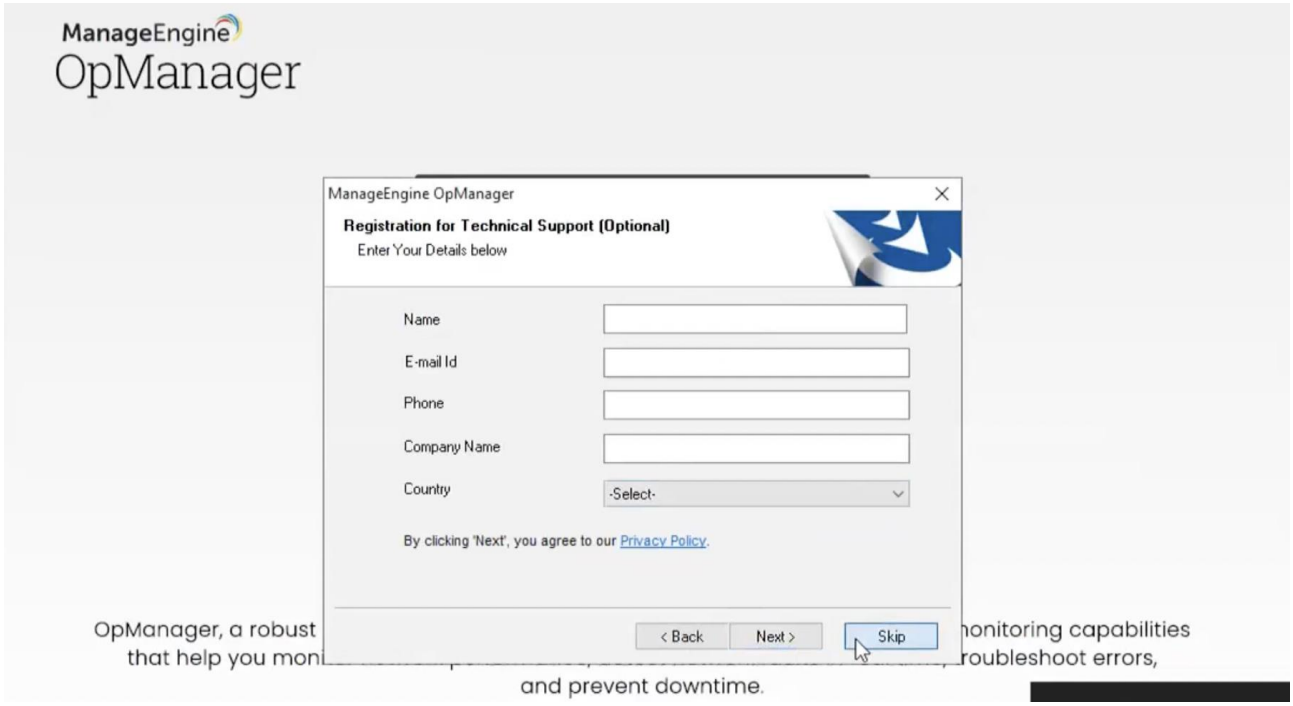
In the subsequent steps of the wizard, select the directory to install OpManager. Proceed to the next step.

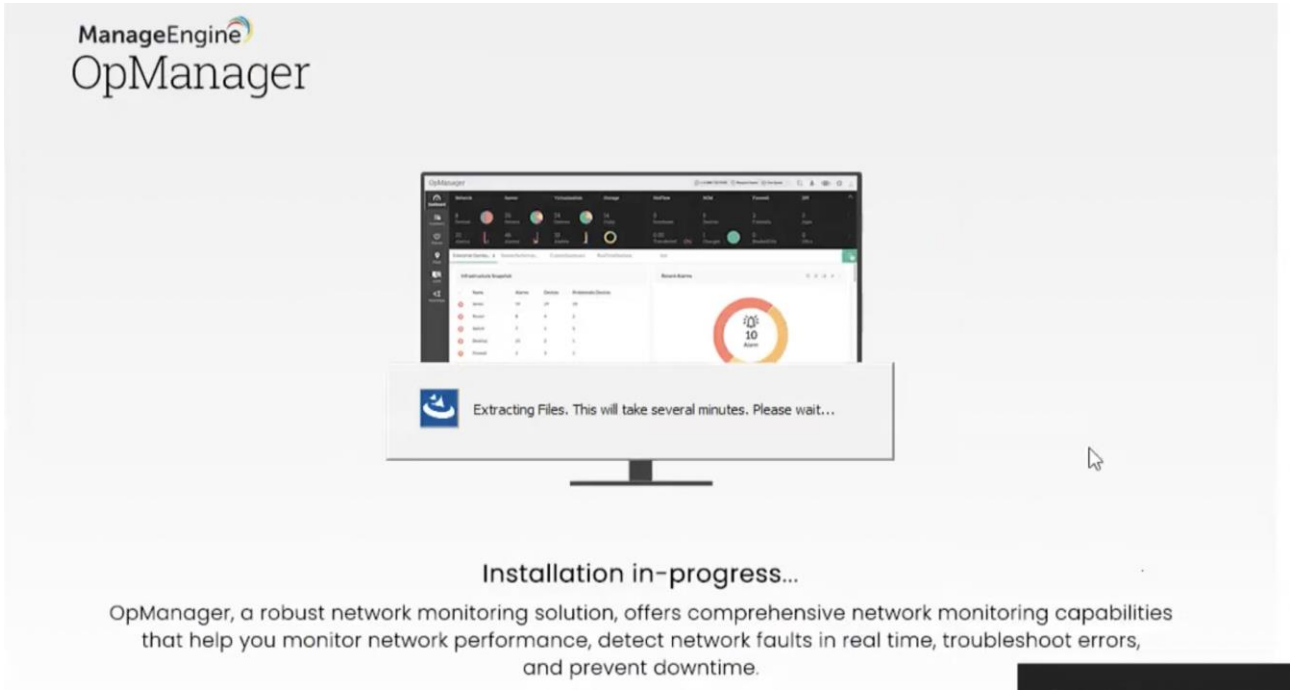


Specify the port number to run OpManager Web Server (OpManager uses 8060 as the default web server port) and click 'Next'.

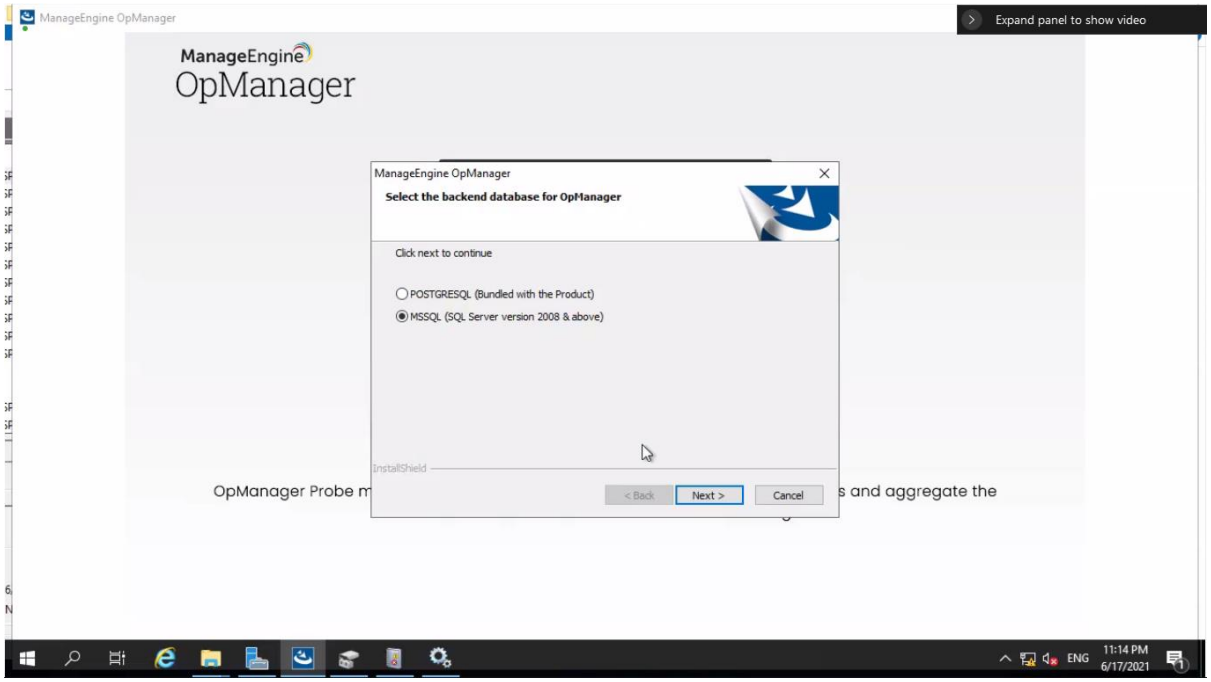


Register for technical support by providing your contact information such as Name, E-mail ID, etc., and click ‘Next'. (It is Optional if you not required you can skip this)

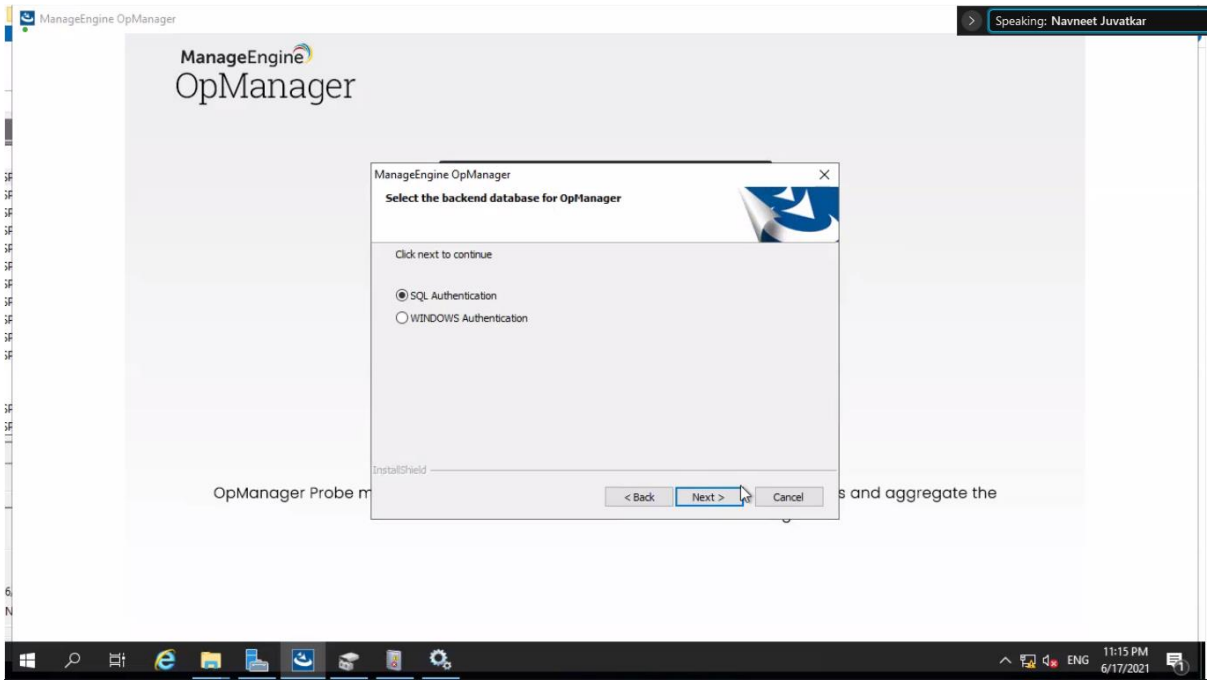




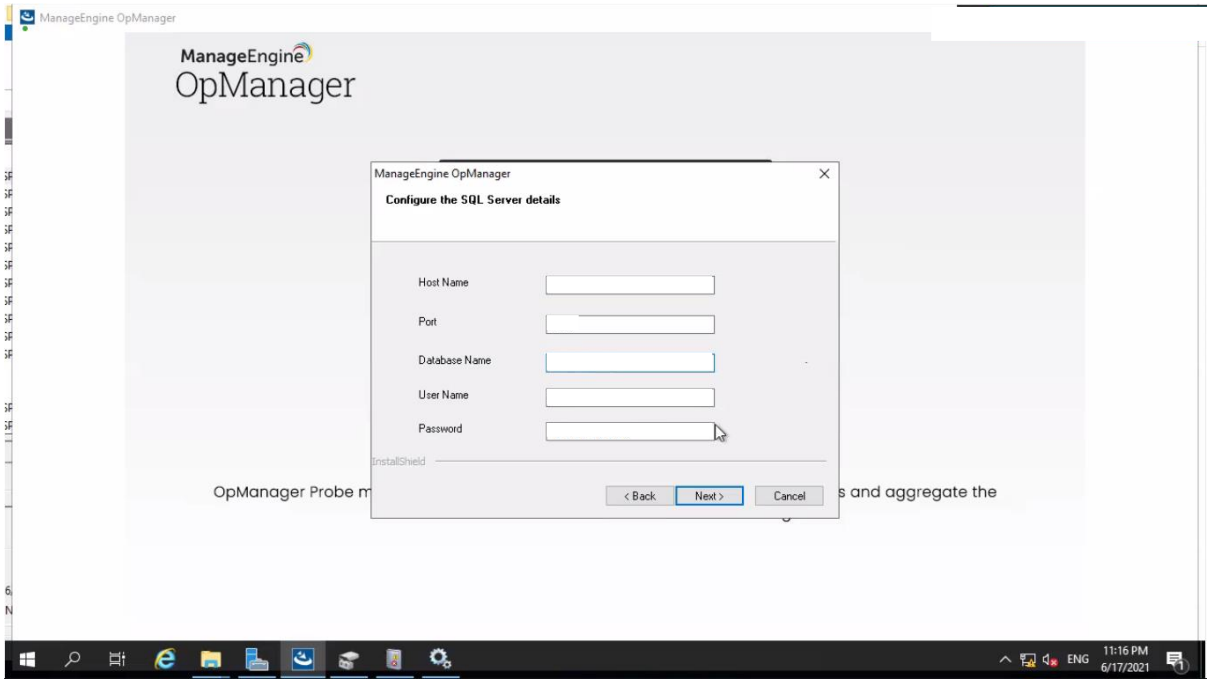
By default, OpManager comes bundled with PostgreSQL. However, OpManager supports both, PostgreSQL and MSSQL databases. Select the required database and click ‘Next'.



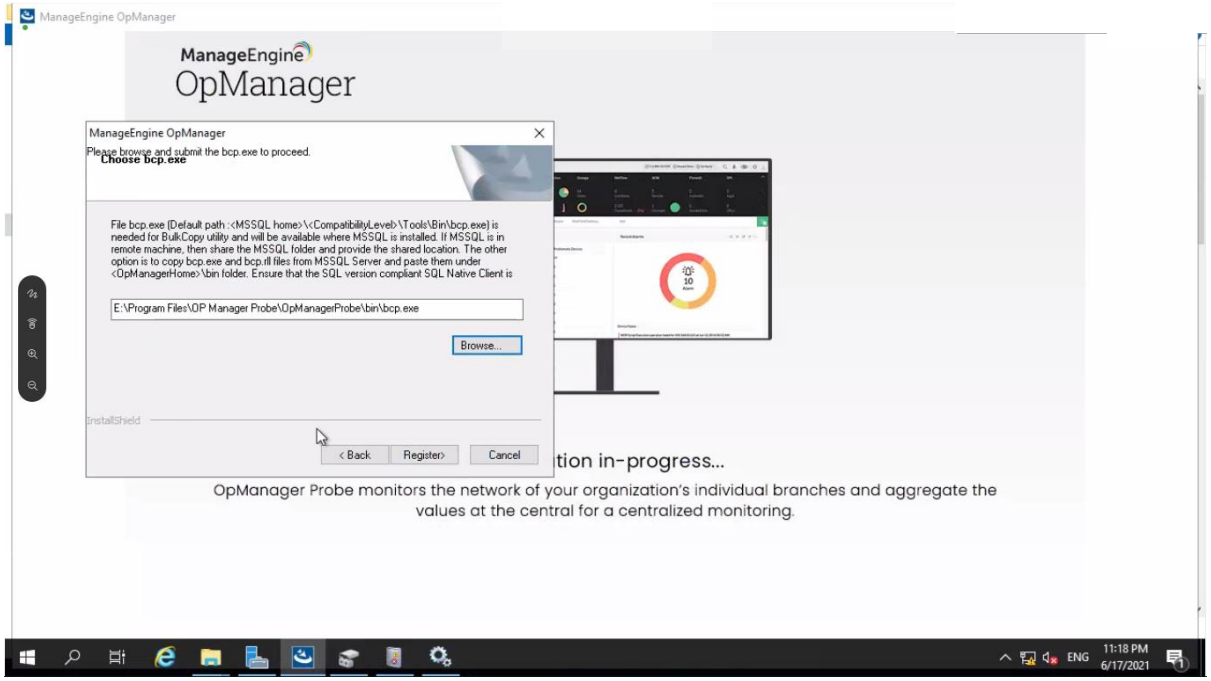
Select correct authentication.



Enter the host name , port number, db name, username and password details and click Next.

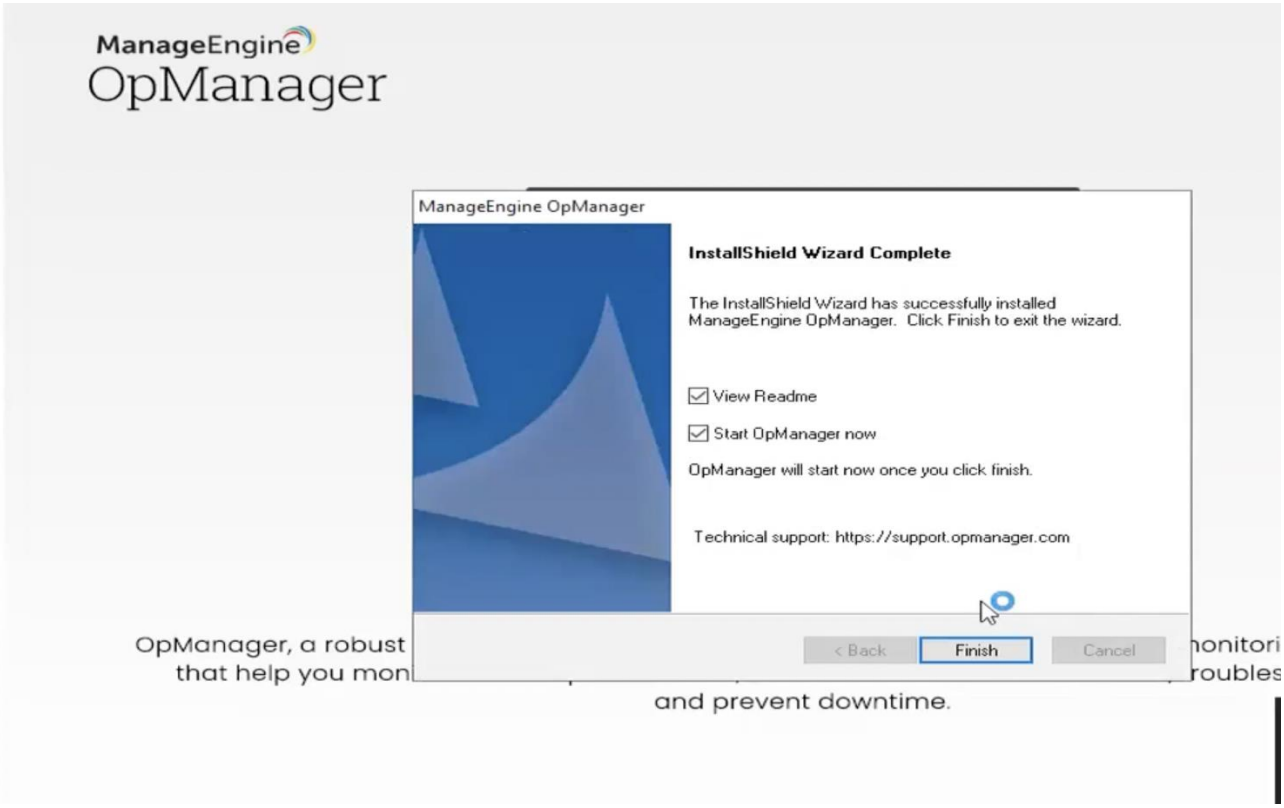


Browse the .bcp file and register.



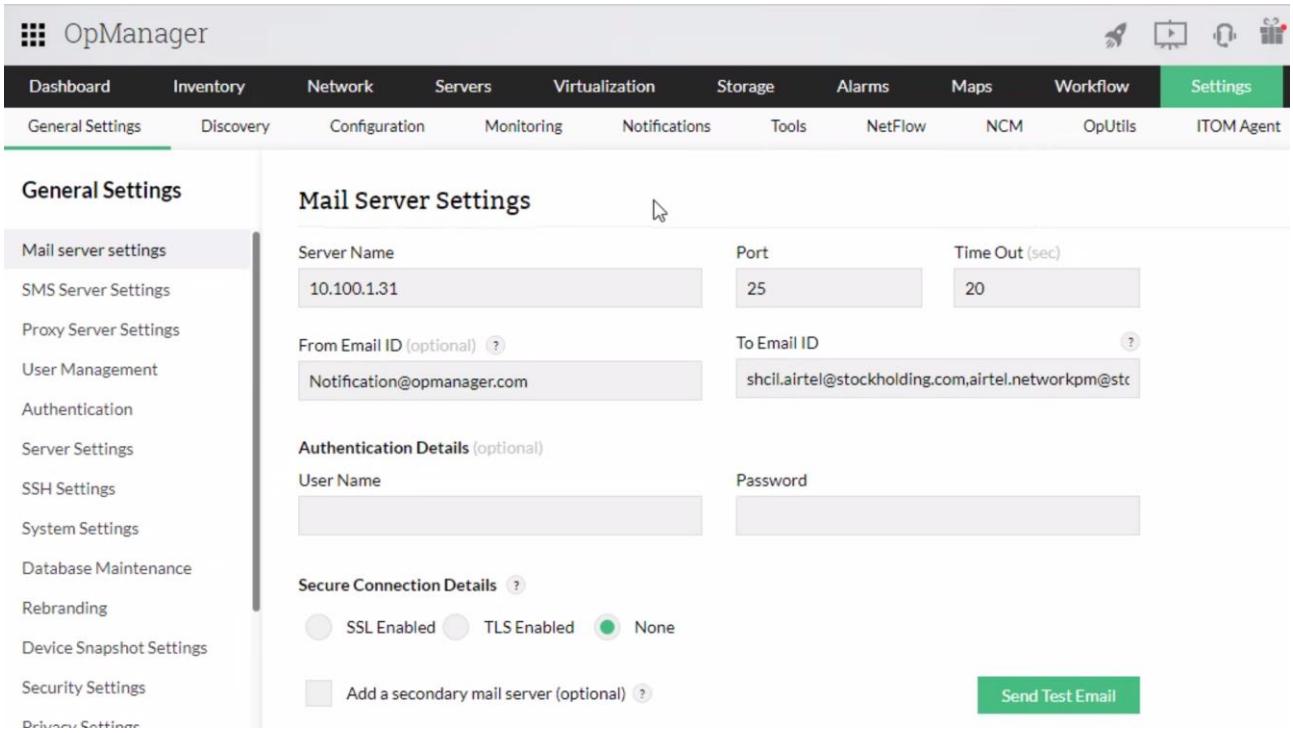
Enter correct details as central url, Probe name, contact name and mail id and installation key.

Click Finish.



2. Configure mail server settings.

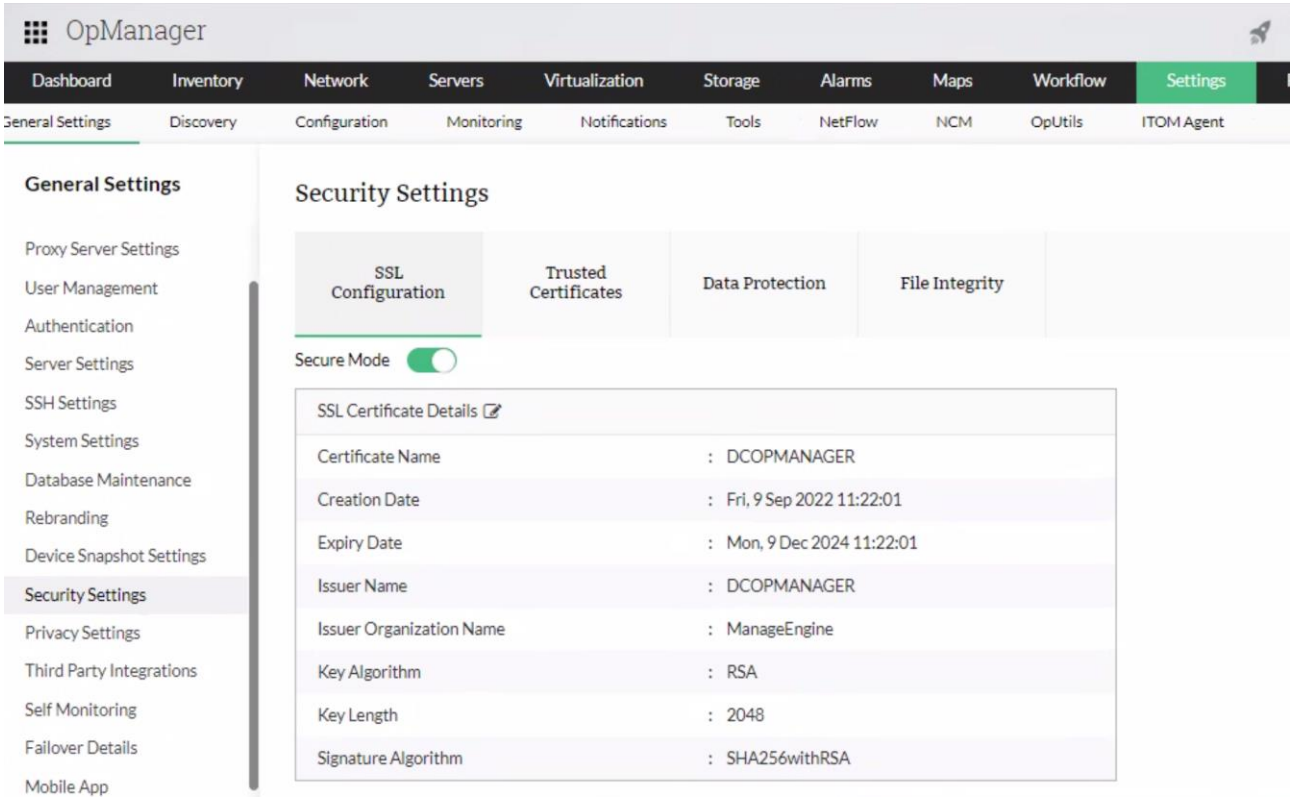
Enter the server name , port number ,From Email :, To email :, and Test the mail.



3. Apply SSL certificate

Go to admin>security settings>SSL config.

Click on Import Certificate and then Browse the .pfx file enter the password and click on Fetch Alias.

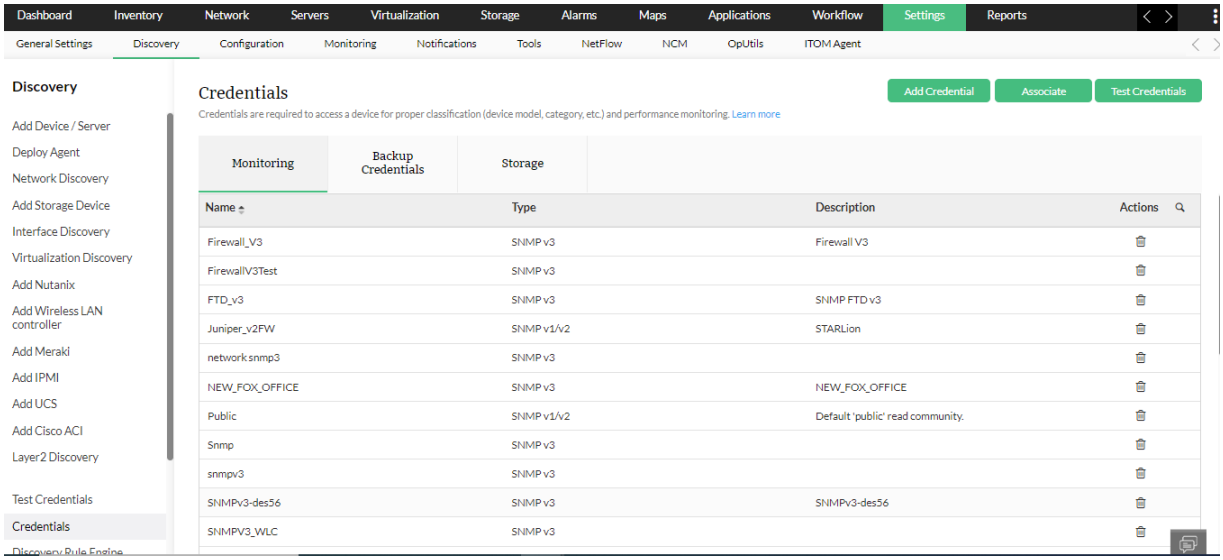


Restart the OP Manager services once the certificate is uploaded.

4. 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.

Listed below are the various types of credentials supported in OpManager:
SNMP v1/v2/v3 - Network Devices
WMI/Windows - Windows
Telnet/SSH - Linux
Vmware - Virtual Machine , V center root access
Citrix - Xen Servers
UCS - Cisco UCS



How to add a new credential in OpManager?

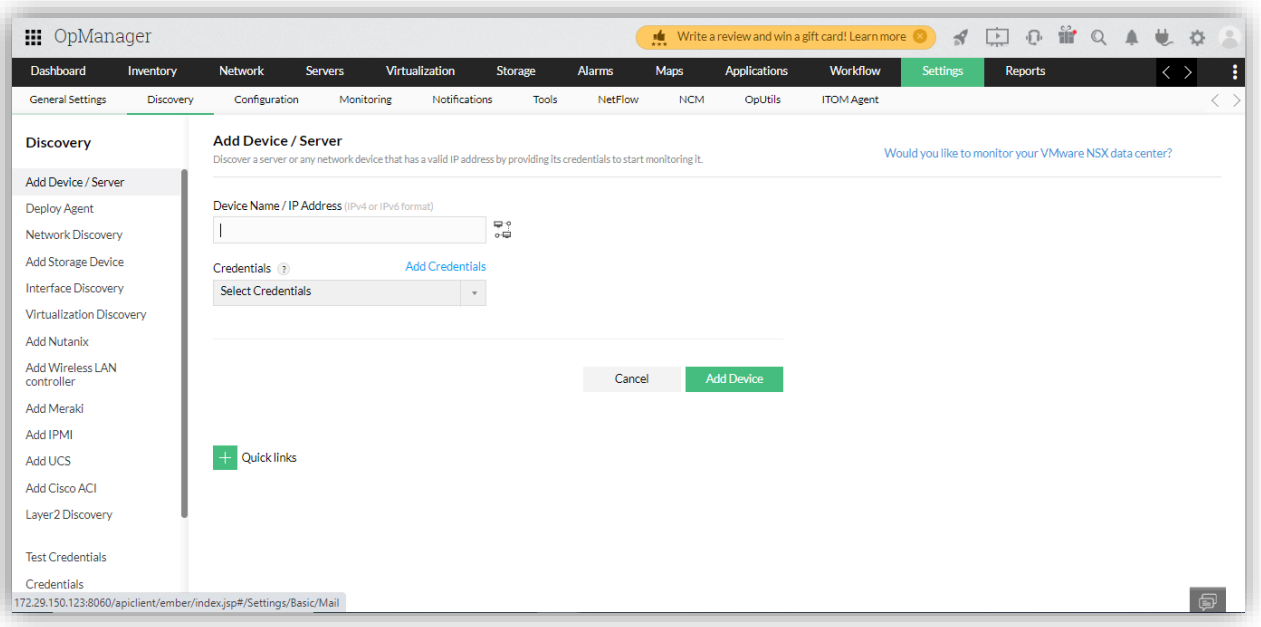
1. Go to **Settings → Discovery → Device Credentials**
2. Click Add Credential
3. Select the required credential category & credential type.
4. Configure the following parameters and click Save to add the credentials

5. Device Discovery

Discovery is a process to add the devices of the network into the OpManager for monitoring its various parameters.Devices can be imported or added into OpManager by various methods. OpManager's network device discovery provides individual discovery options specific to the device type and allows discovery of devices in bulk.

1.Individual discovery of devices

1. Go to Settings → Discovery → Add Device / Server.
2. Type either the IP Address or the Device Name of the device to be discovered.
3. Click on the Ping icon near the Device Name / IP Address section to ping the device and check its availability.
4. Select the required Credentials.
5. Click on Add Device to start discovery

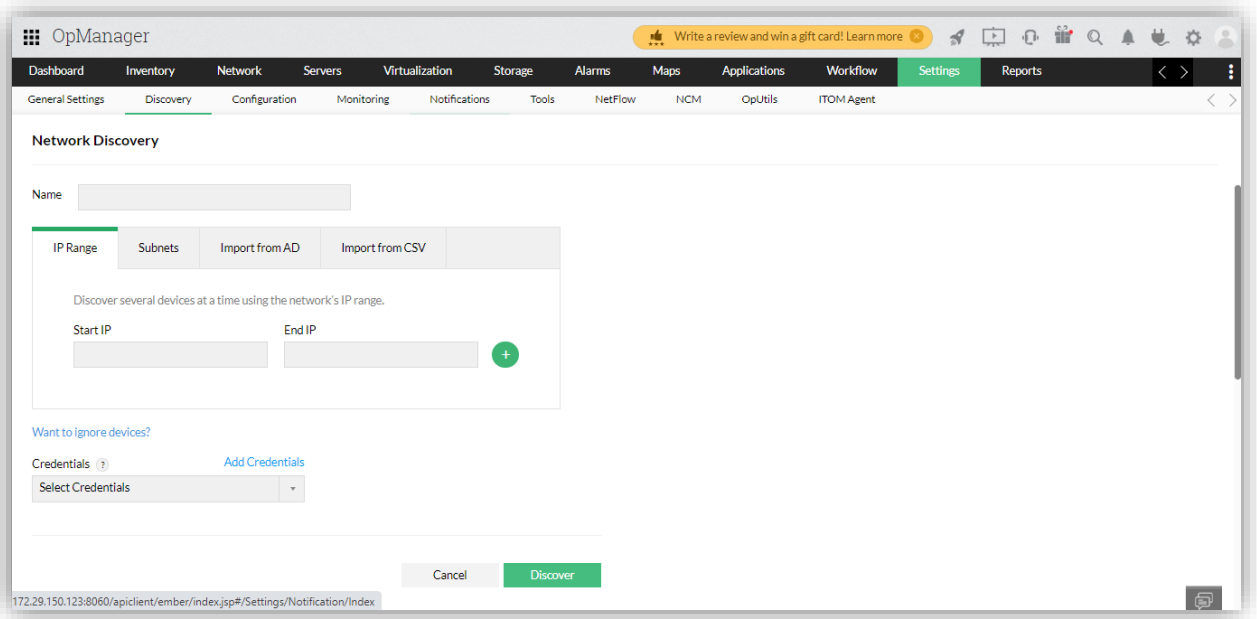


2. Bulk discovery of devices:

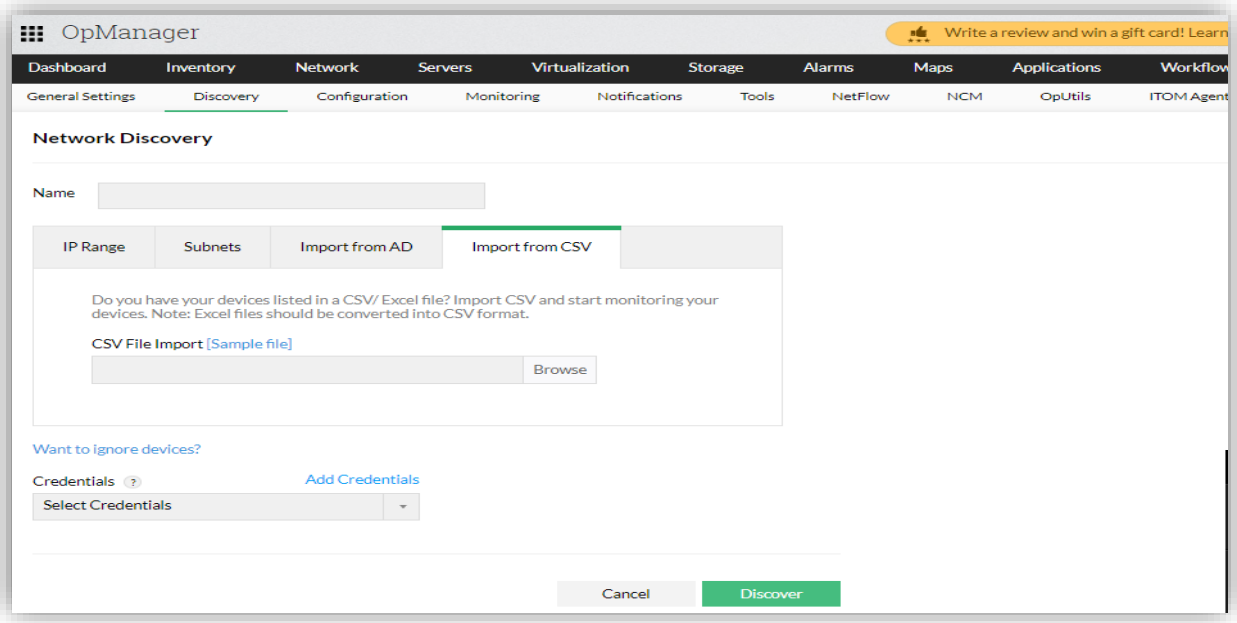
Go to Settings → Discovery → Network Discovery → New Discovery

There are four methods to add device into the product

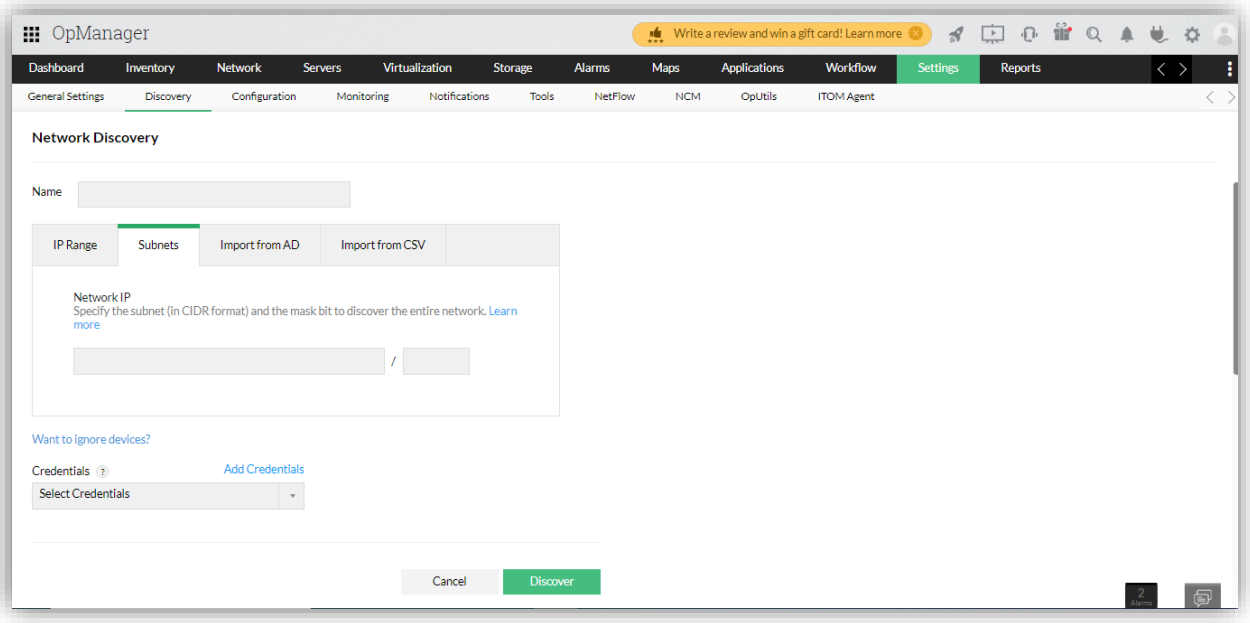
1. Discovering devices from an IP Range



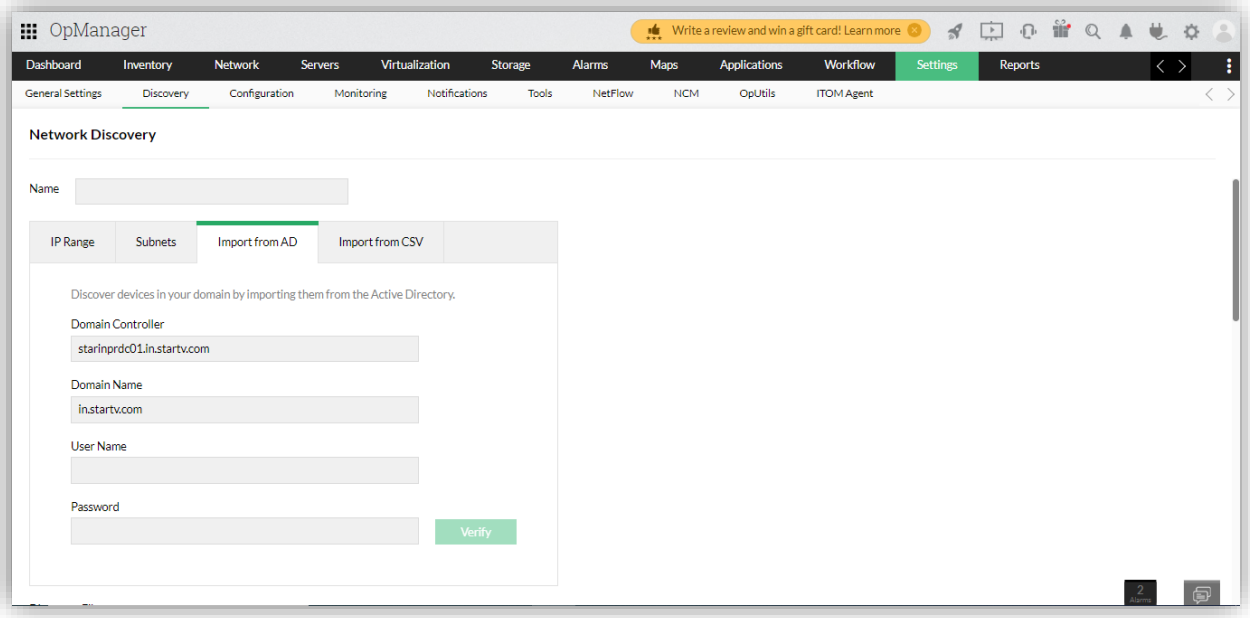
2. Discovering devices by CSV import



3. Discovering a complete network



4. Import devices from Active Directory

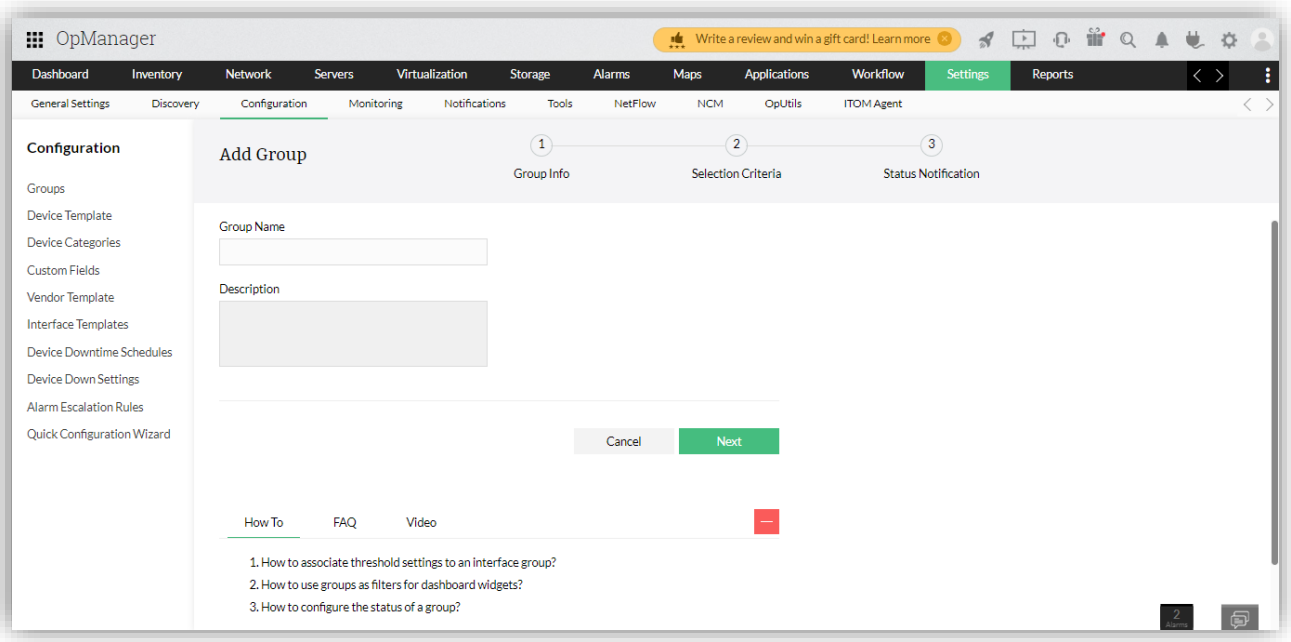


6. Groups

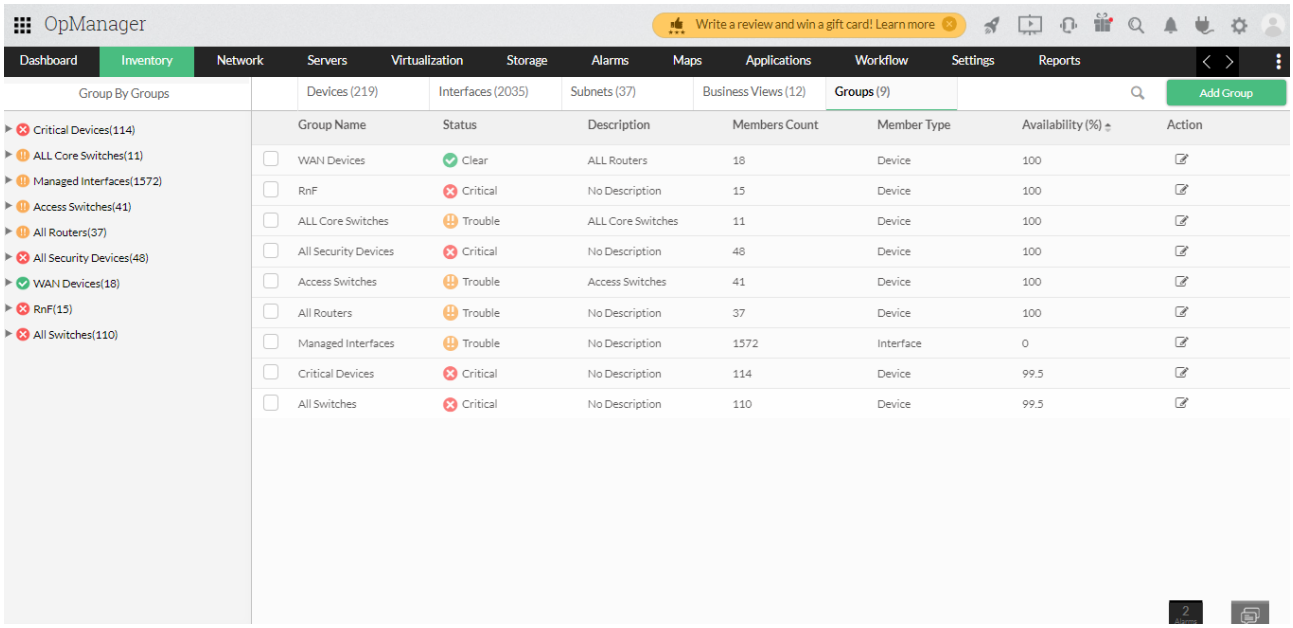
We can group devices or interface together for an organized network management and this will help in bulk configuration throughout the product.Groups and subgroups can be used as a filter in Reports, Widget, Notification Profile, URL Templates, Downtime schedule, Alarm suppression, Device template, Interface template, Test credentials and Workflow.

Steps to create a group

1. **Click on Settings → Configuration → Groups and click on the "Add" button or go to Inventory → Groups → Add Group.**



2. Provide a suitable group name and description and click on Next.
3. Select the type of elements you want to add to this group.
4. Select the method to group the elements. You can group elements either 'Manually' or by 'Criteria'.
5. If you selected the 'Manually' option - Select the group members from the available list and click on 'Next'.
6. 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 '+' icon.
7. Add multiple criteria if needed, along with the logical operation you need to perform based on the criteria. Click on Next.
8. 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 all the available members by default.

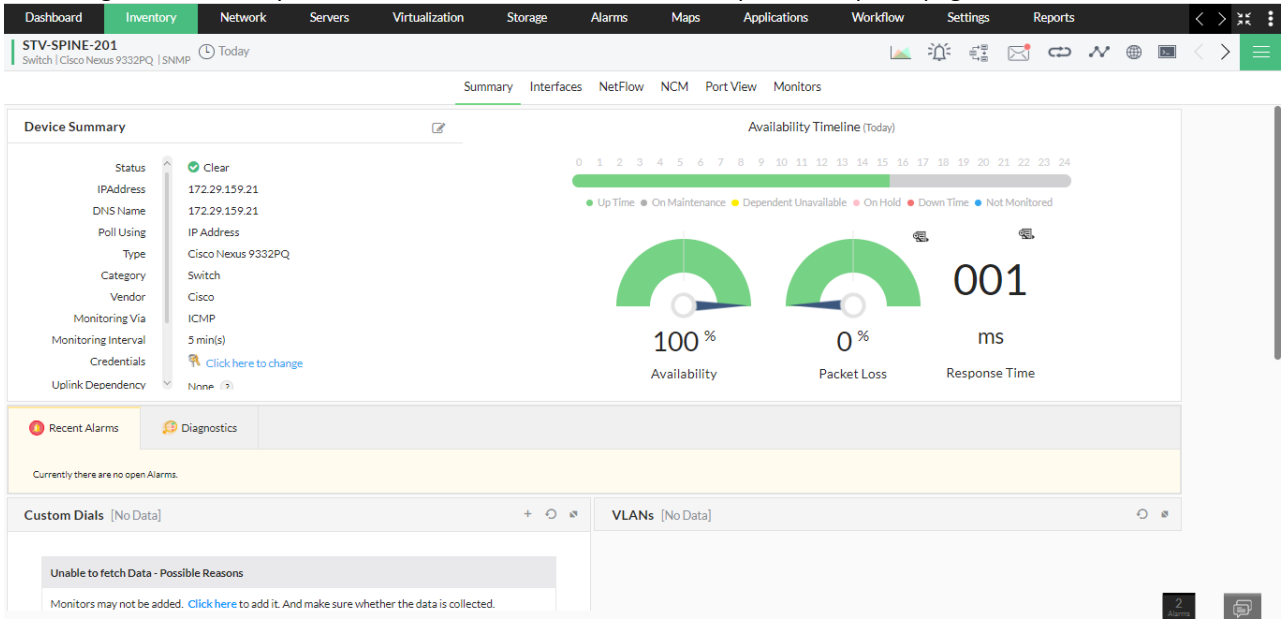

OpManager
Write a review and win a gift card! Learn more
Dashboard
Inventory
Network
Servers
Virtualization
Storage
Alarms
Maps
Applications
Workflow
Settings
Reports
Group By Groups
Devices (219)
Interfaces (2035)
Subnets (37)
Business Views (12)
Groups (9)
Add Group
Critical Devices(114)
ALL Core Switches(11)
Managed Interfaces(1572)
Access Switches(41)
All Routers(37)
All Security Devices(48)
WAN Devices(18)
RnF(15)
All Switches(110)
Group Name
Status
Description
Members Count
Member Type
Availability (%)
Action
WAN Devices
Clear
ALL Routers
18
Device
100
RnF
Critical
No Description
15
Device
100
ALL Core Switches
Trouble
ALL Core Switches
11
Device
100
All Security Devices
Critical
No Description
48
Device
100
Access Switches
Trouble
Access Switches
41
Device
100
All Routers
Trouble
No Description
37
Device
100
Managed Interfaces
Trouble
No Description
1572
Interface
0
Critical Devices
Critical
No Description
114
Device
99.5
All Switches
Critical
No Description
110
Device
99.5

7. Performance Monitors

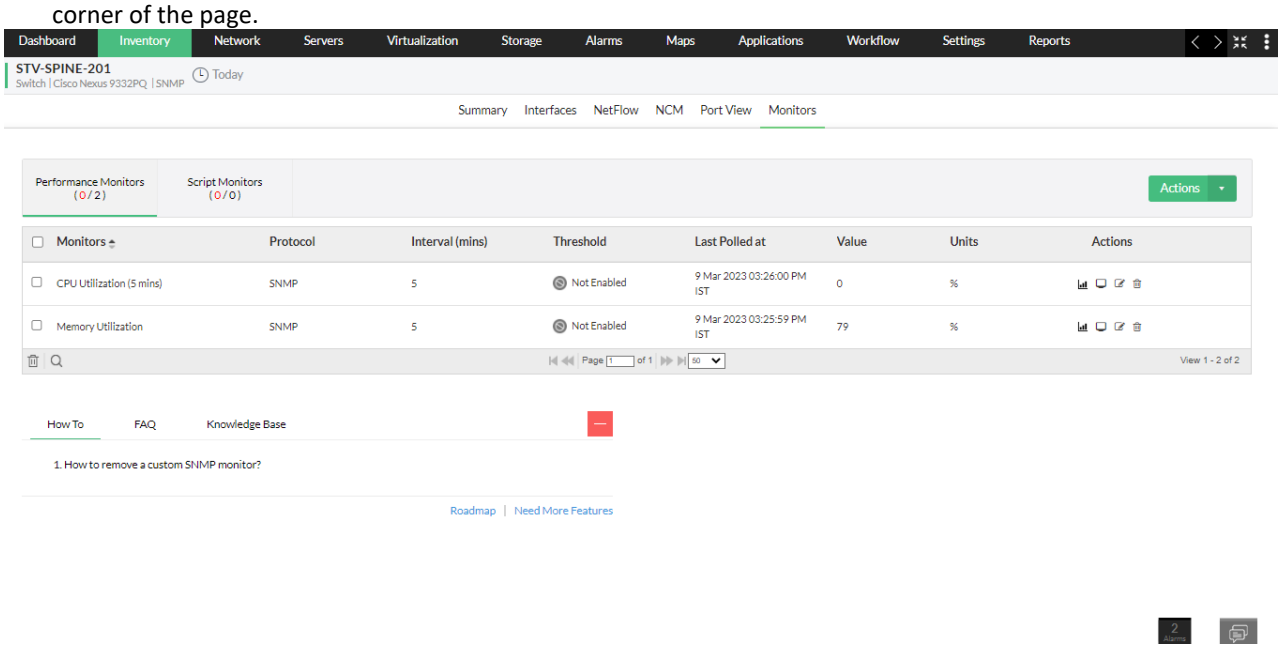
Monitors can be associated with devices in the following ways.

1. From device Snapshot page

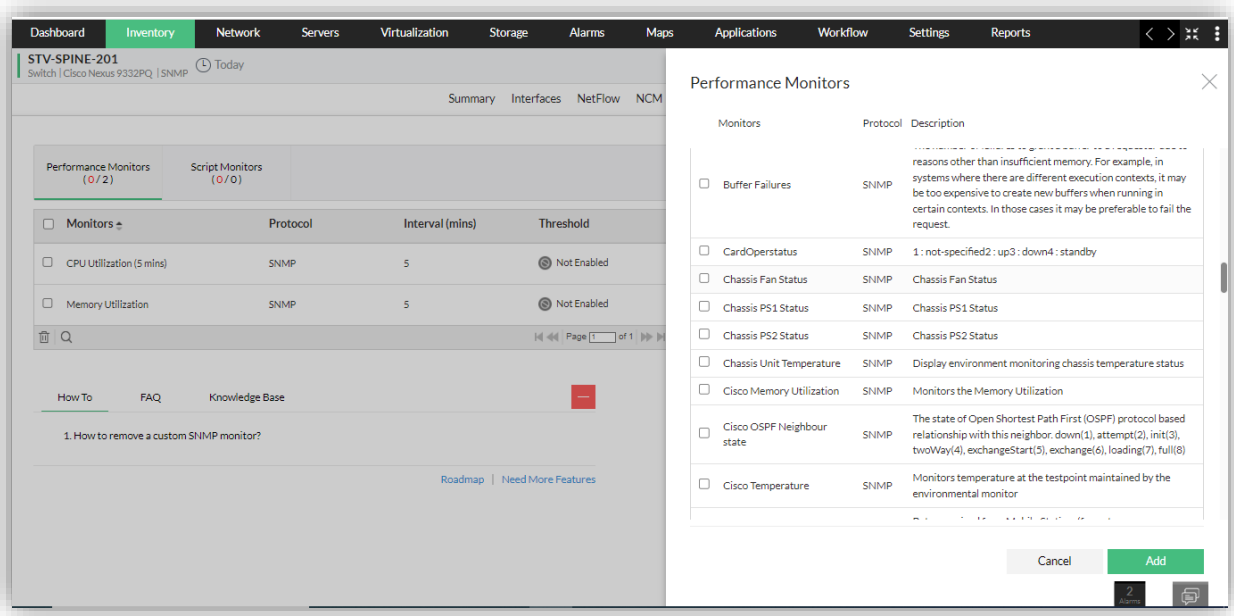
- Navigate to Inventory -> Devices and then click on a device to open its Snapshot page.



- Open the Monitors tab. Under the Performance monitors section, click on the "Actions" button at the top right corner of the page.



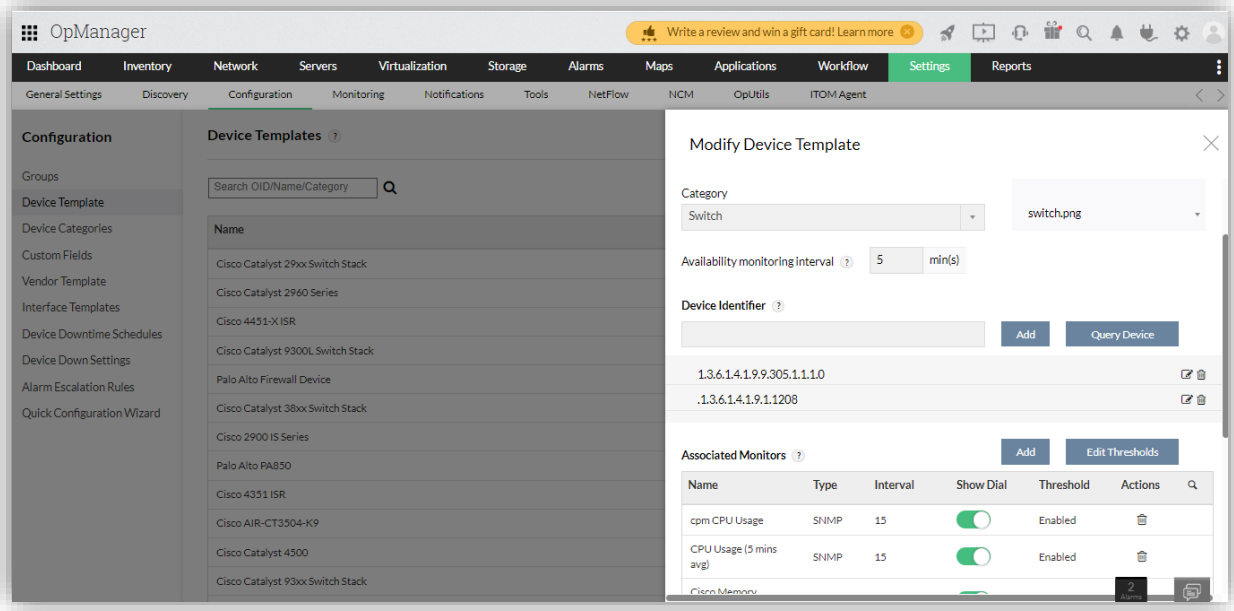
- Now, select the SNMP monitors for Disk, CPU and memory from the list of monitors displayed under the HOST-RESOURCES category.

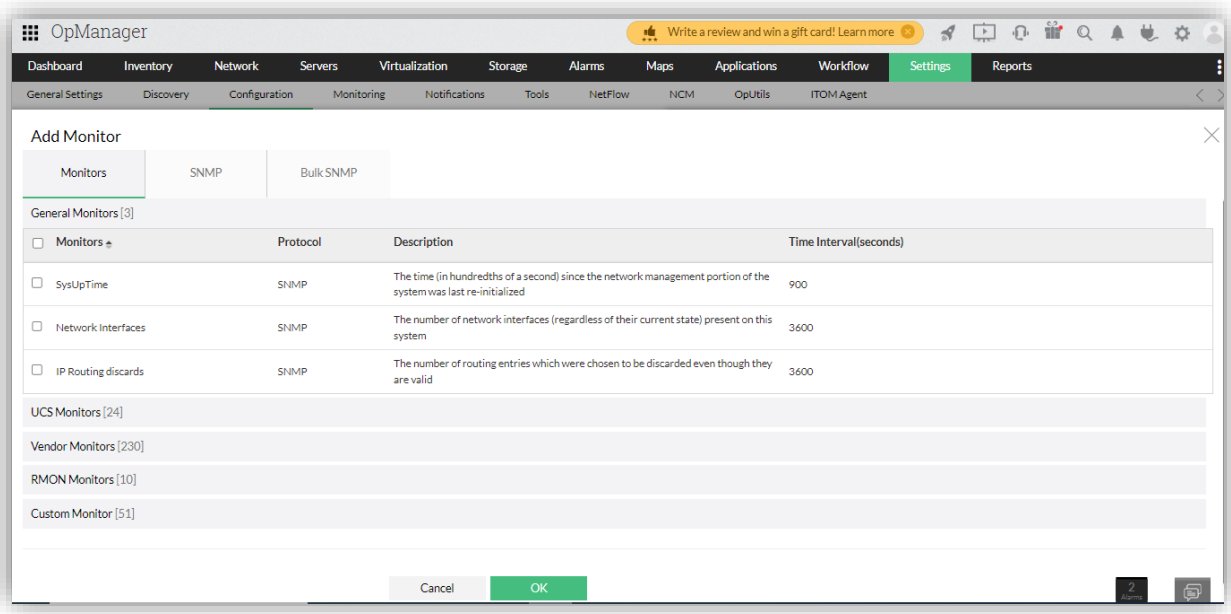


- Click on "Add" to apply the changes.

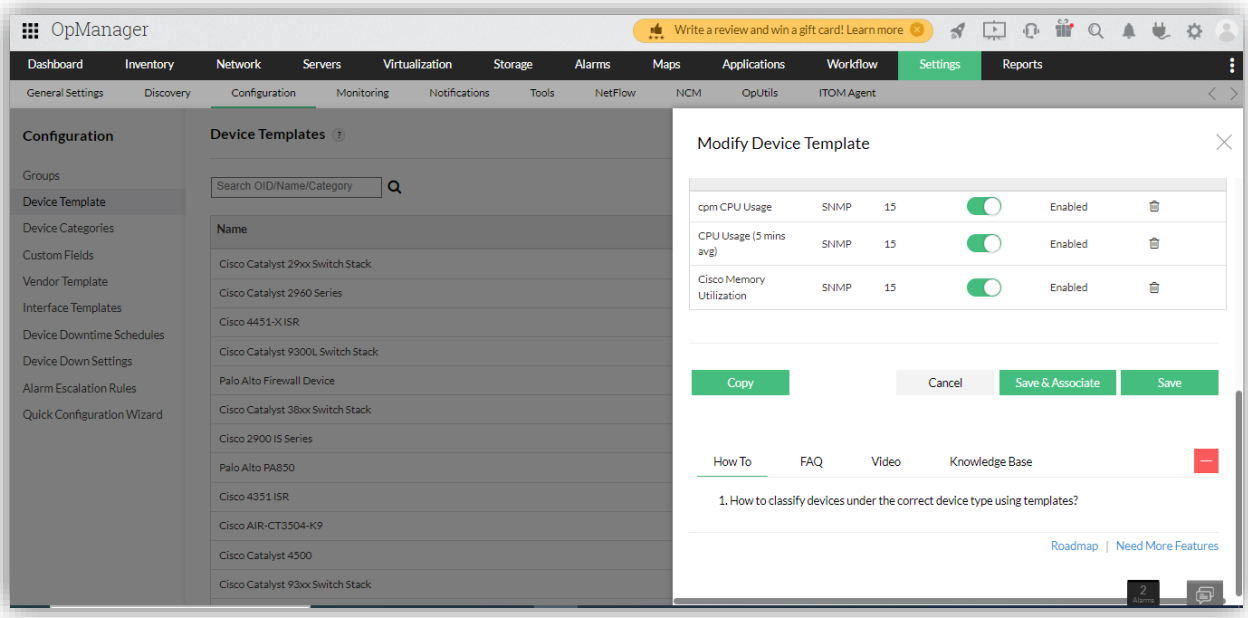
2. From Device Templates:

- Navigate to Settings -> Configuration -> Device Template.
- Open a template and click on the "Add" button that is found at the right of the "Associated Monitors" section.





- Now, select the monitors you want to add and then click on "Save" or "Save & Associate" based on your preference. The monitors will now be associated with the device template. Any new device about to be associated with the template in the future will automatically be associated with these monitors.



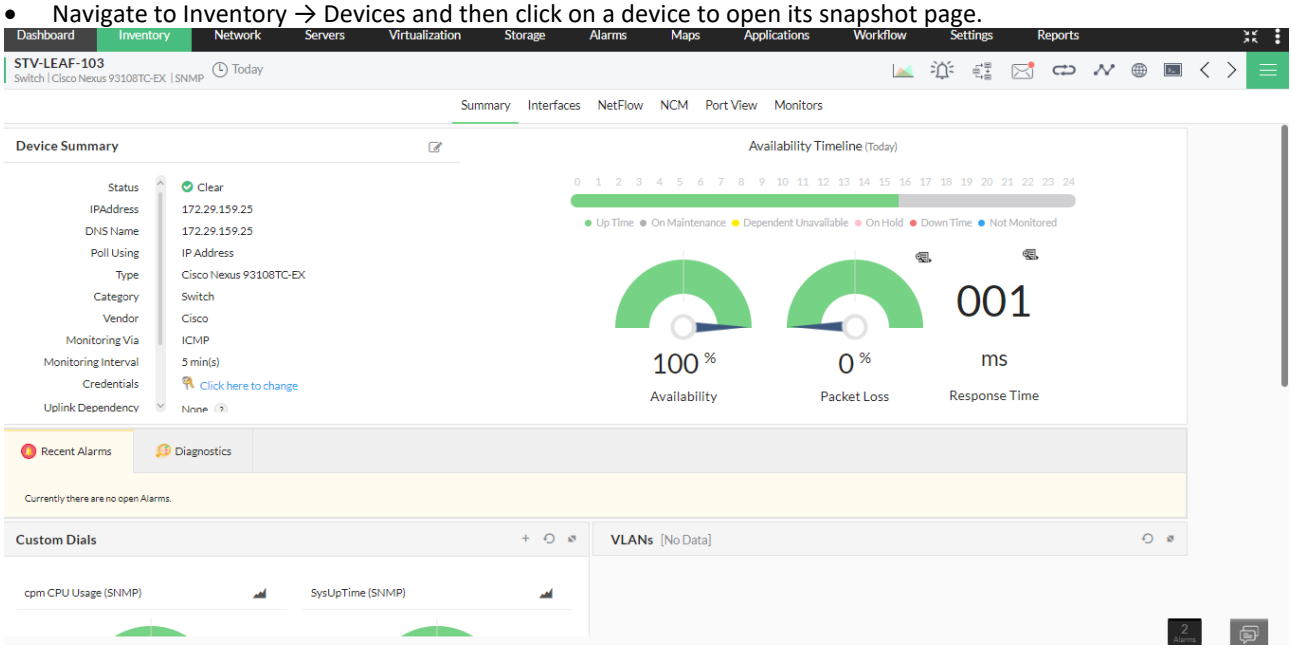
8. Threshold Configuration

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:

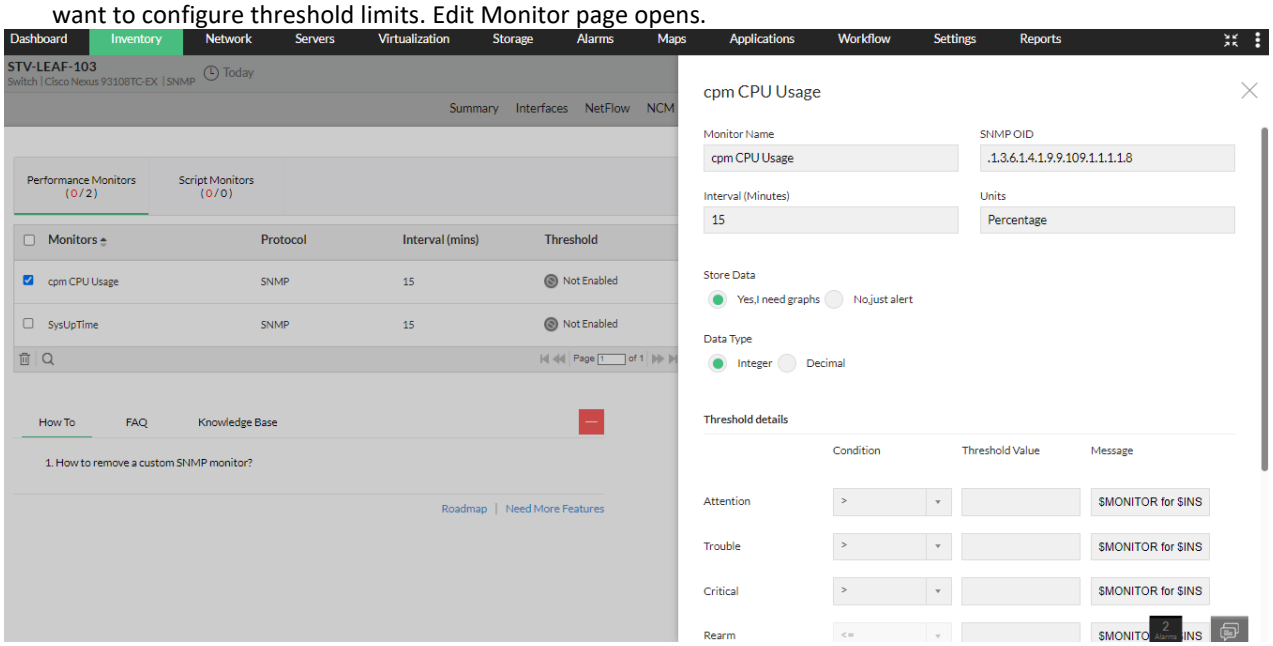
Attention threshold - low severity
Trouble threshold - medium severity
Critical threshold - high severity
Rearm - to rearm the alert after it has been triggered

1. Configure threshold limits for performance monitors in an individual device

- Navigate to Inventory → Devices and then click on a device to open its snapshot page.



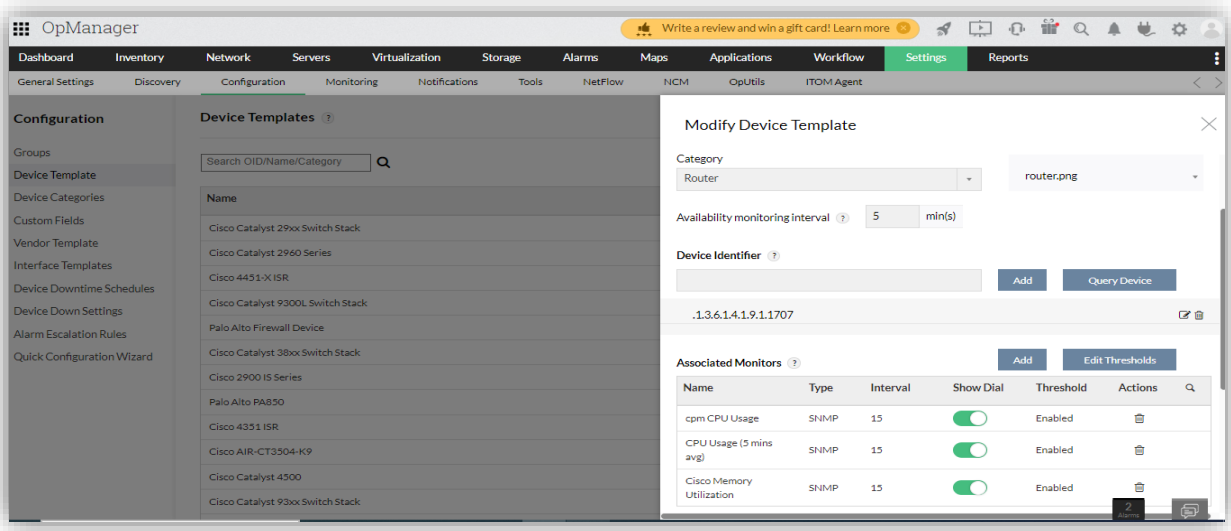
- Click Monitors → Performance Monitors → click on the edit icon corresponding to the monitor for which you want to configure threshold limits. Edit Monitor page opens.



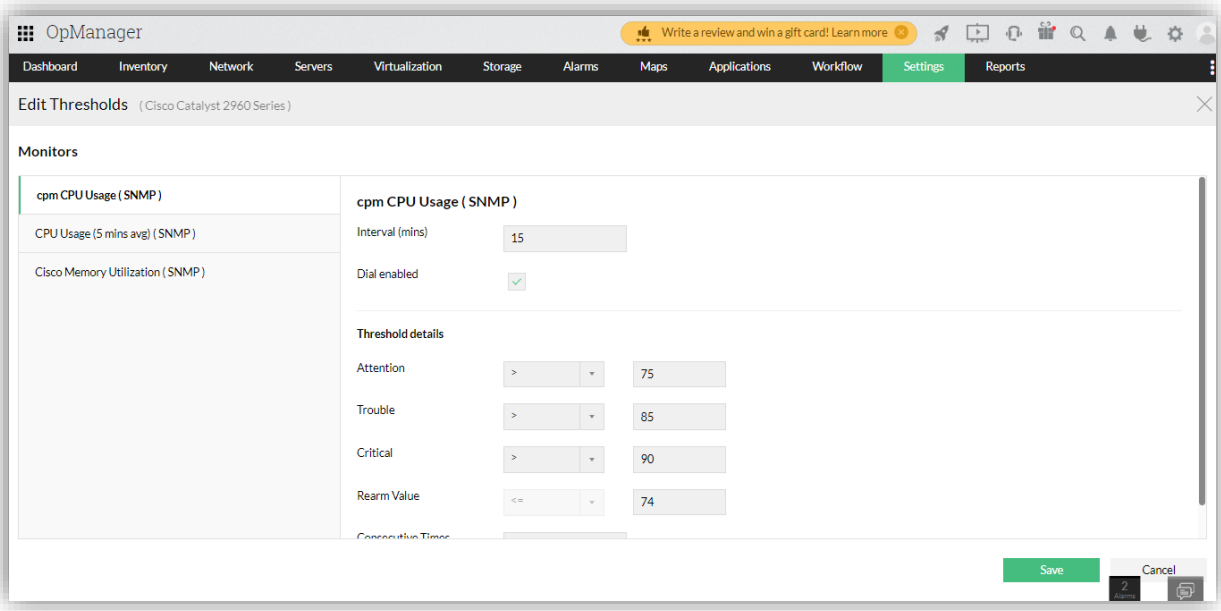
- Ensure that the monitoring Interval is configured.
- Specify the unit for the monitored resource in terms of percentage, MB, KB etc (based on how the parameter is measured).
- Enter the Rearm Value. Rearm is the value that determines when the monitor is reverted to 'Normal' status.
- Click on Save

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

- Go to Settings → Configuration → Device Templates and select the template in which you want to configure the threshold.



- 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.
- Configure the Attention, Trouble, Critical Threshold and the Rearm Value and click on OK



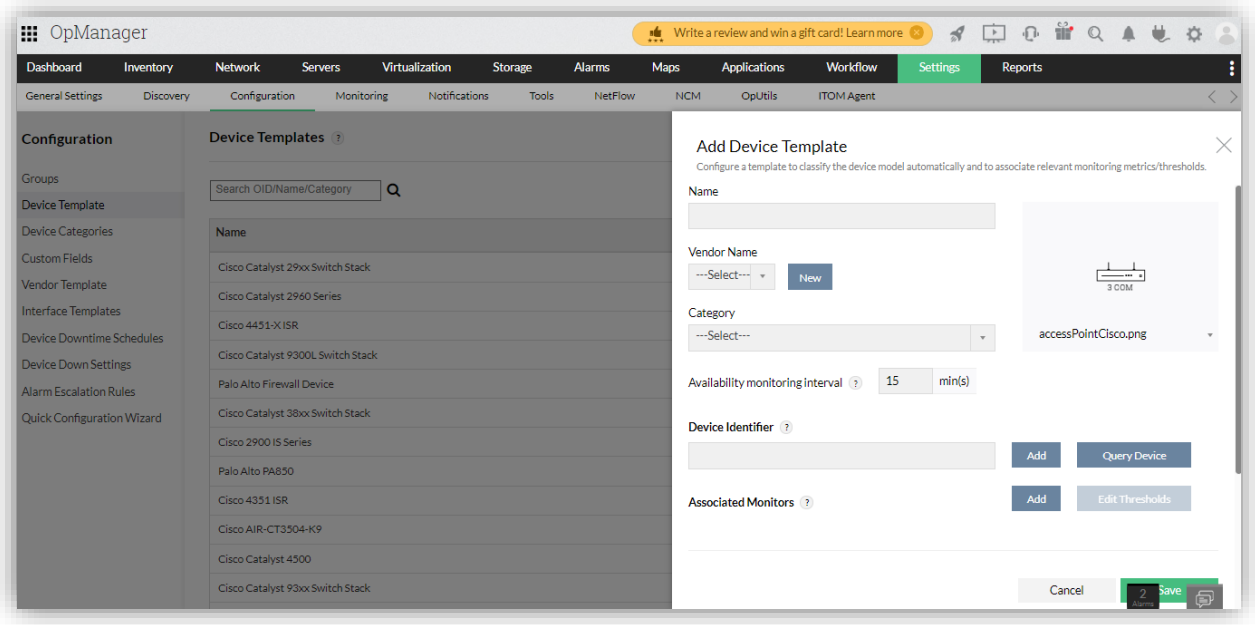
- To save this setup, press Save and press Save and Associate to directly associate the selected monitor to the devices mapped to the Device Template.

9. Device Templates

A Device Template is set of pre-loaded device details such as device type, category, monitoring interval, unique SysObject ID and performance monitors.

Basic configuration

1. **Go to Settings -> Configuration -> Device Templates.**
2. Click on the Add Template option.



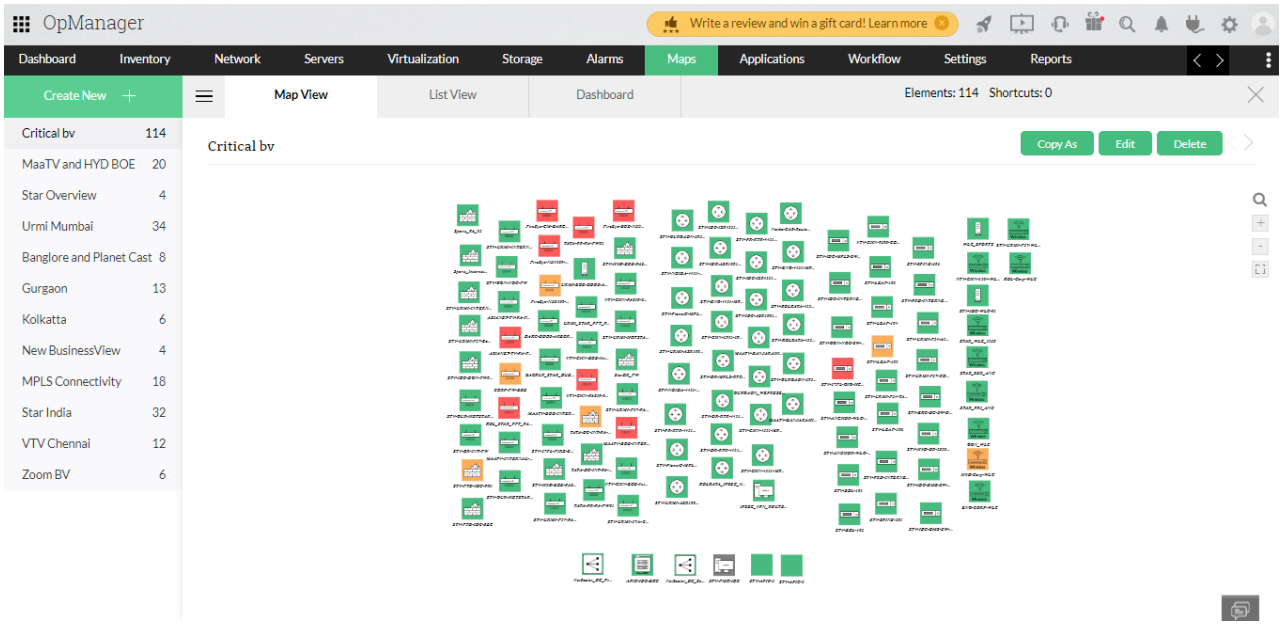
3. Enter the mandatory fields - Device template name, vendor, category, availability monitoring interval and device image.
4. Define a unique device identifier (SysObject ID) received from vendor or by querying the device itself.
5. Click on Save.

10. 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 from both 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.



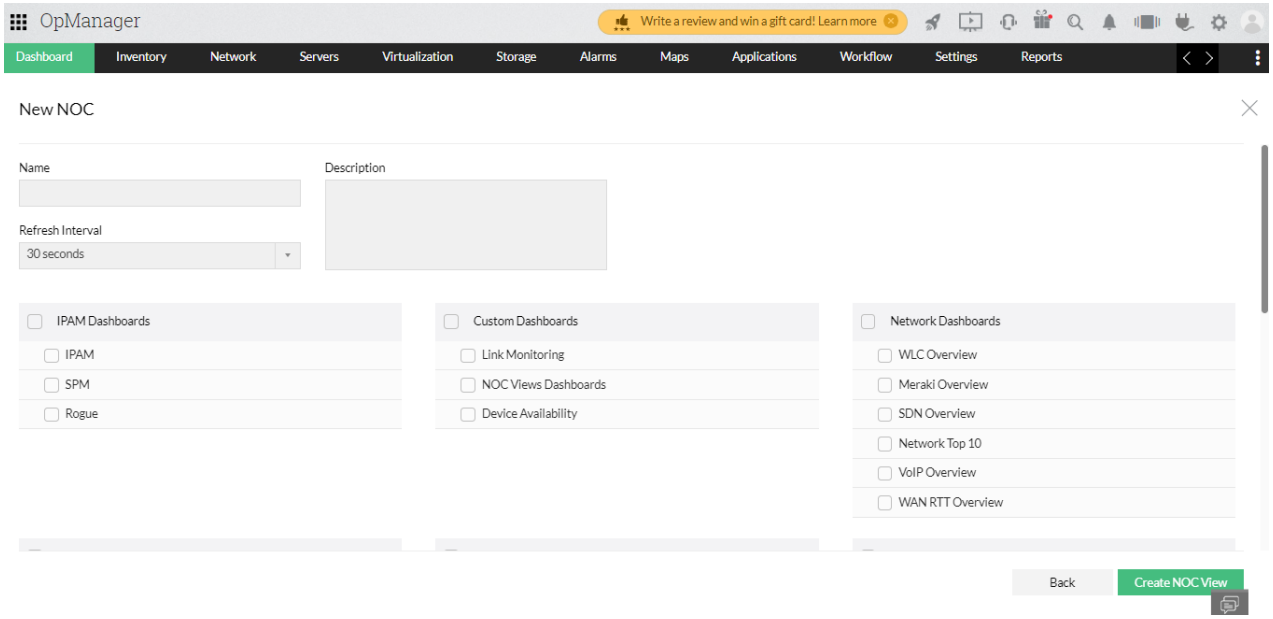
2. From the list of available devices, drag and drop the required devices into the white board individually or add devices in bulk using the Multi select option.
3. Customize the view by changing font type, size or color and edit the background if necessary.
4. Place the selected devices on the Map (background) based on your requirement.
5. Rename and save the created business view.

11. NOC View (CCTV)

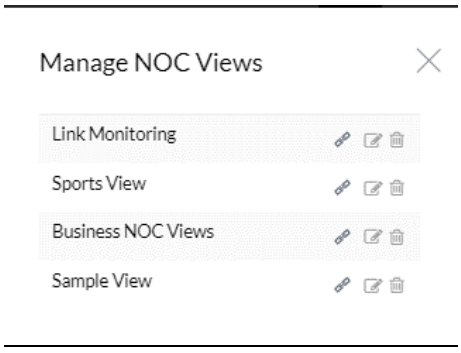
NOC View or CCTV helps you view only the required dashboards repeatedly at required intervals.

Steps to create NOC view:

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.

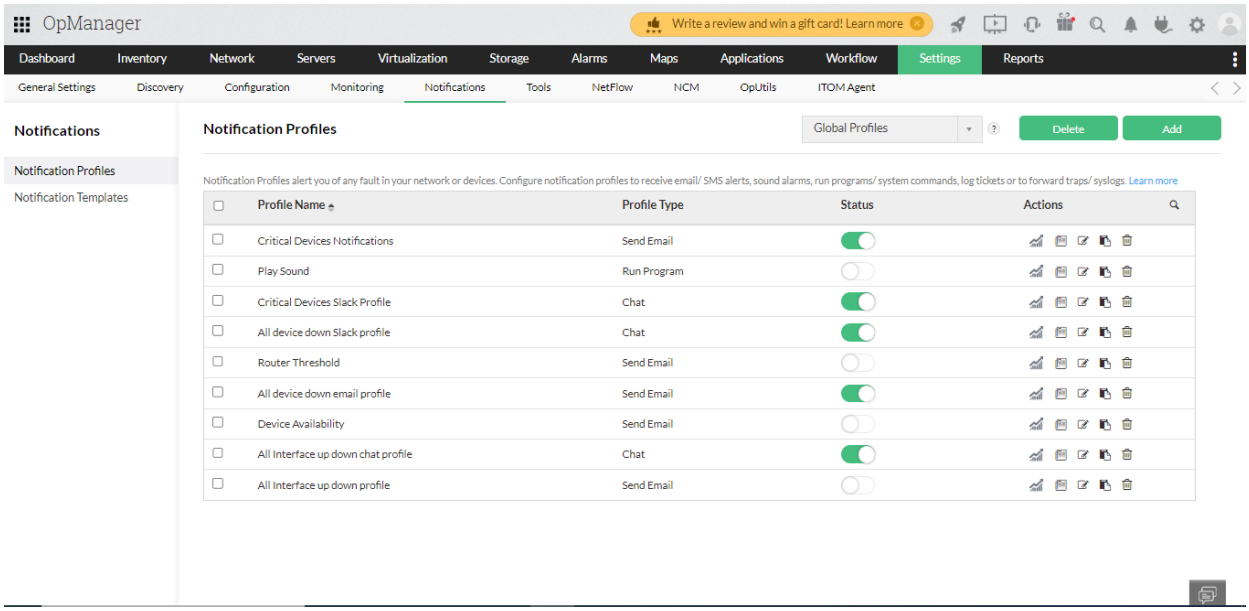


12. Notification Profile

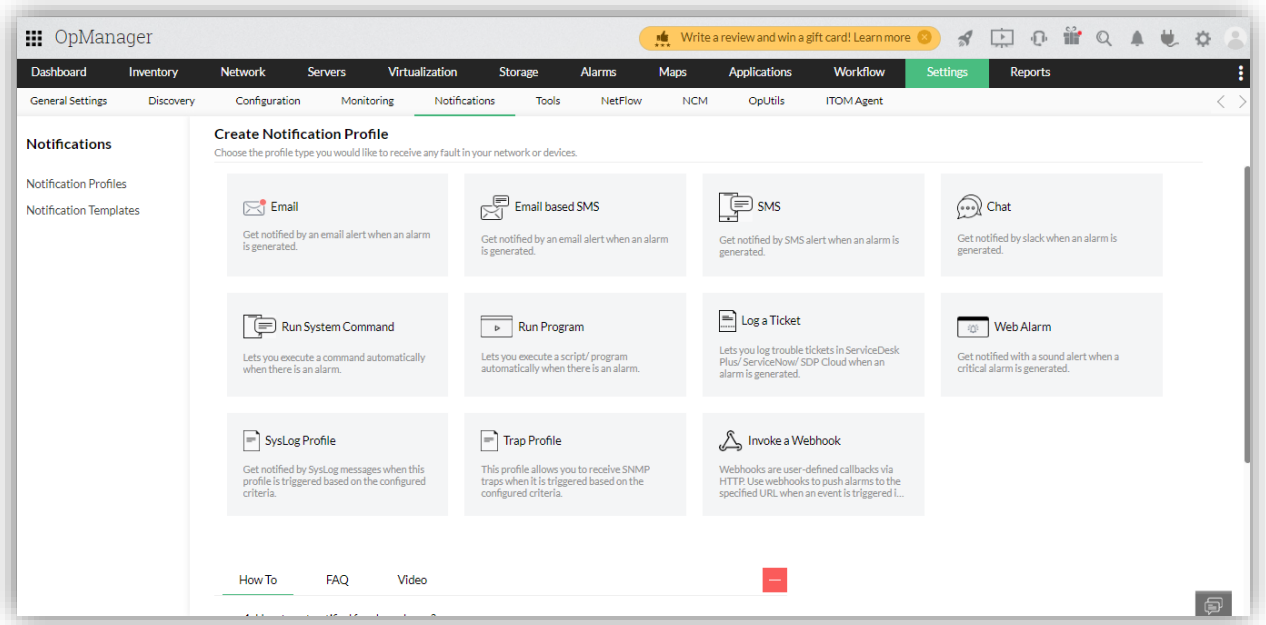
When a fault is detected in your network, an event occurs and multiple events correlate to trigger an alarm. You can configure OpManager to notify the network administrator or perform automatic actions based on the alarm raised for a device using the notification profiles.

Steps to create Notification Profile

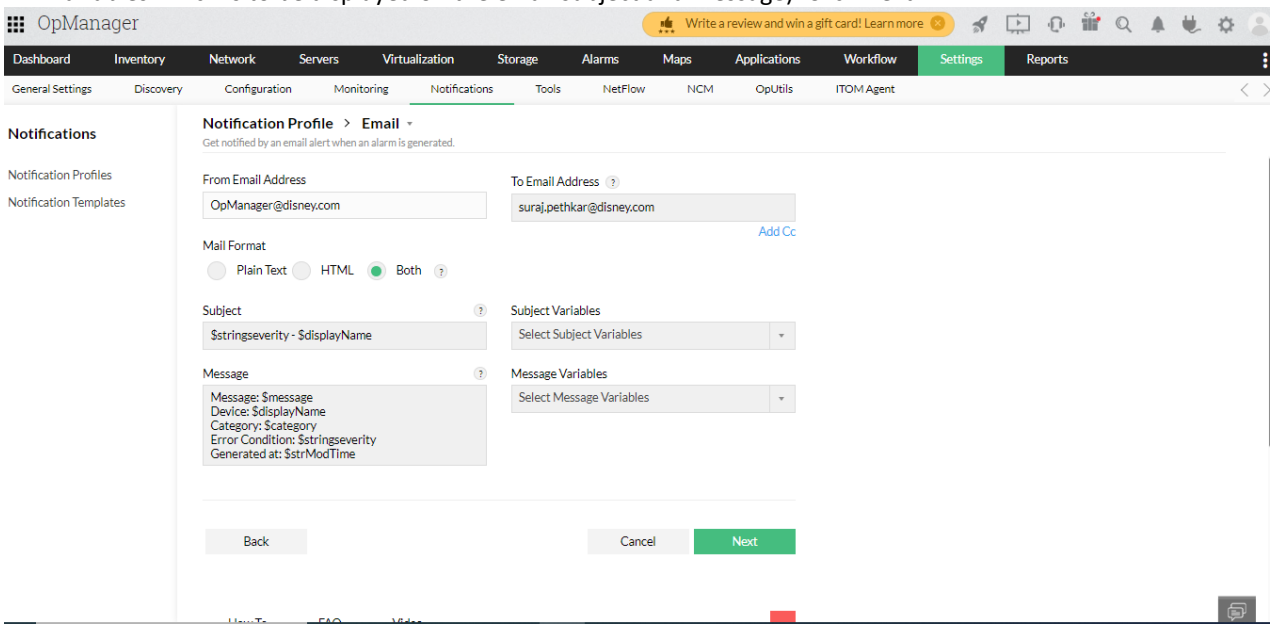
1. Go to Settings > Notifications
2. Click Add.



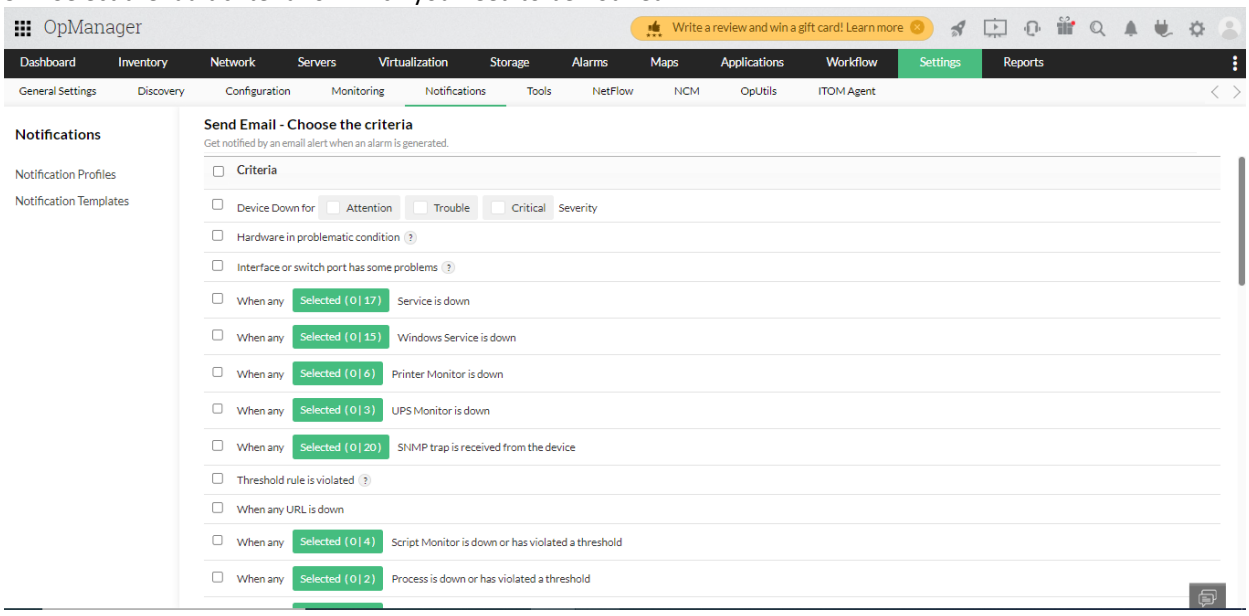
3. Select the Notification type as for example Email.



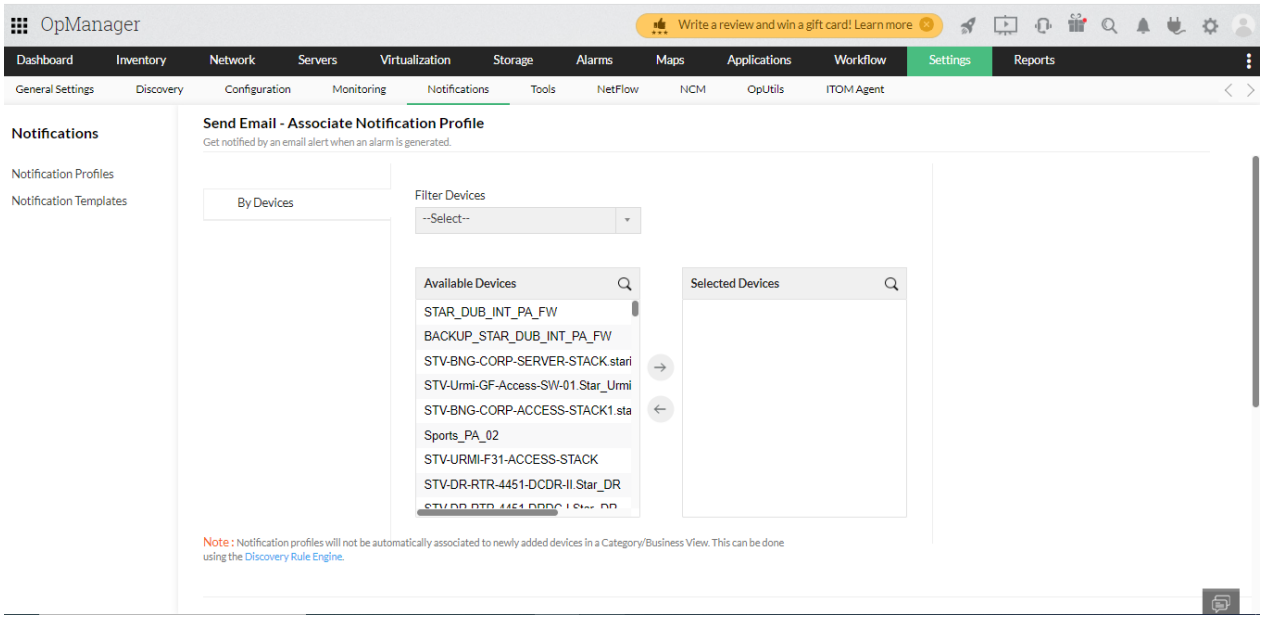
4. Provide the From, To, and CC Email Address in addition to Subject and Message (select the required alarm variables which is to be displayed on the email subject and message). Click Next.



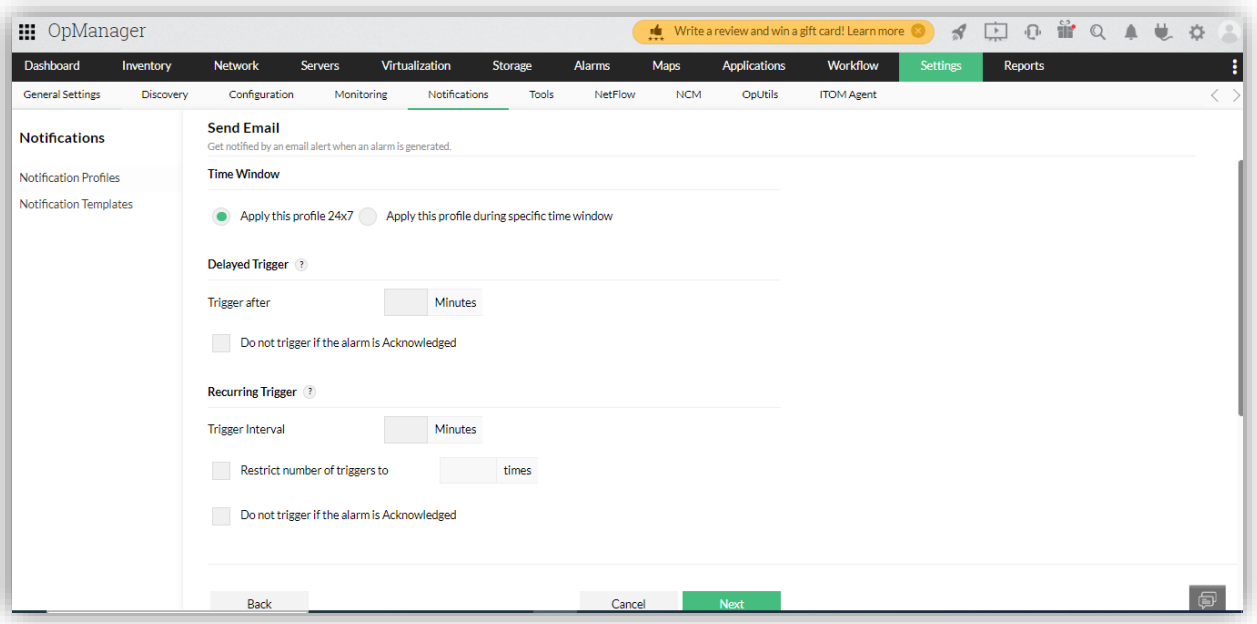
5. Select the fault criteria for which you need to be notified.



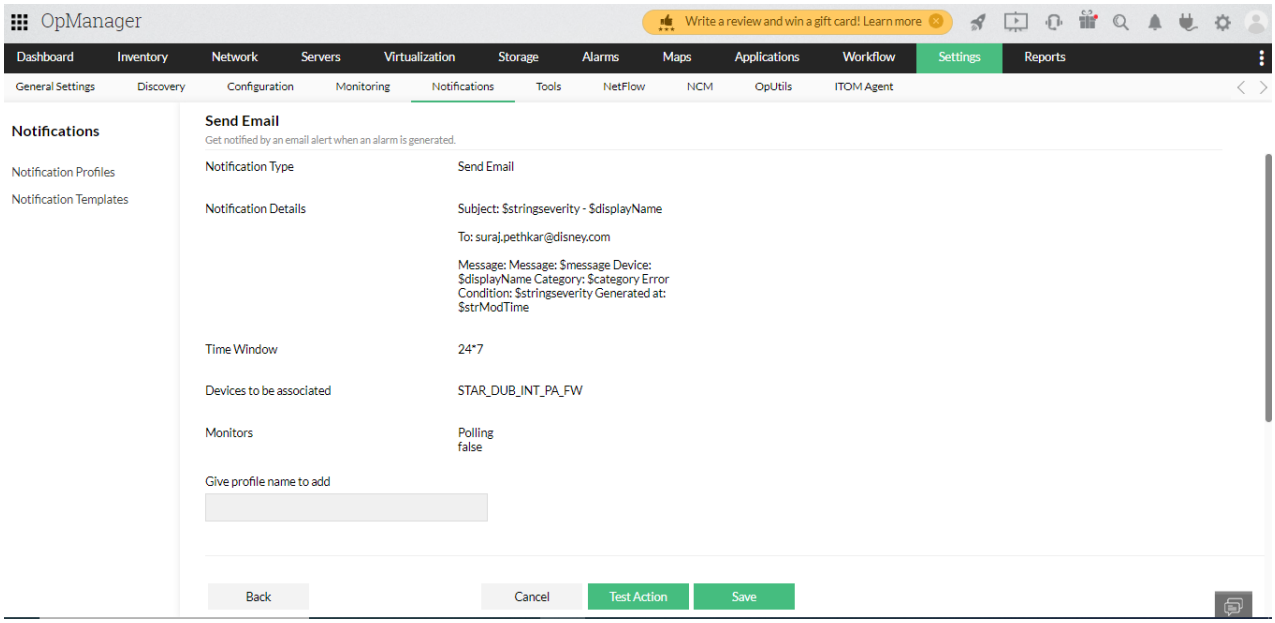
6. Select the devices either By Category or By Business View or By Devices and click Next.



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.



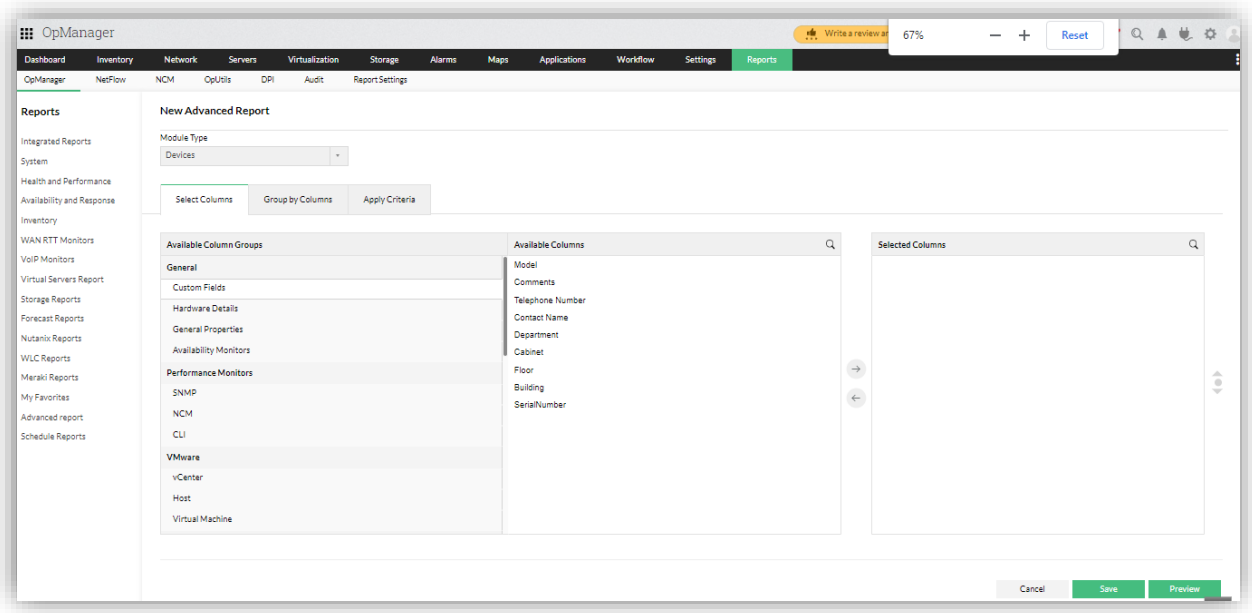
13. Reports

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.

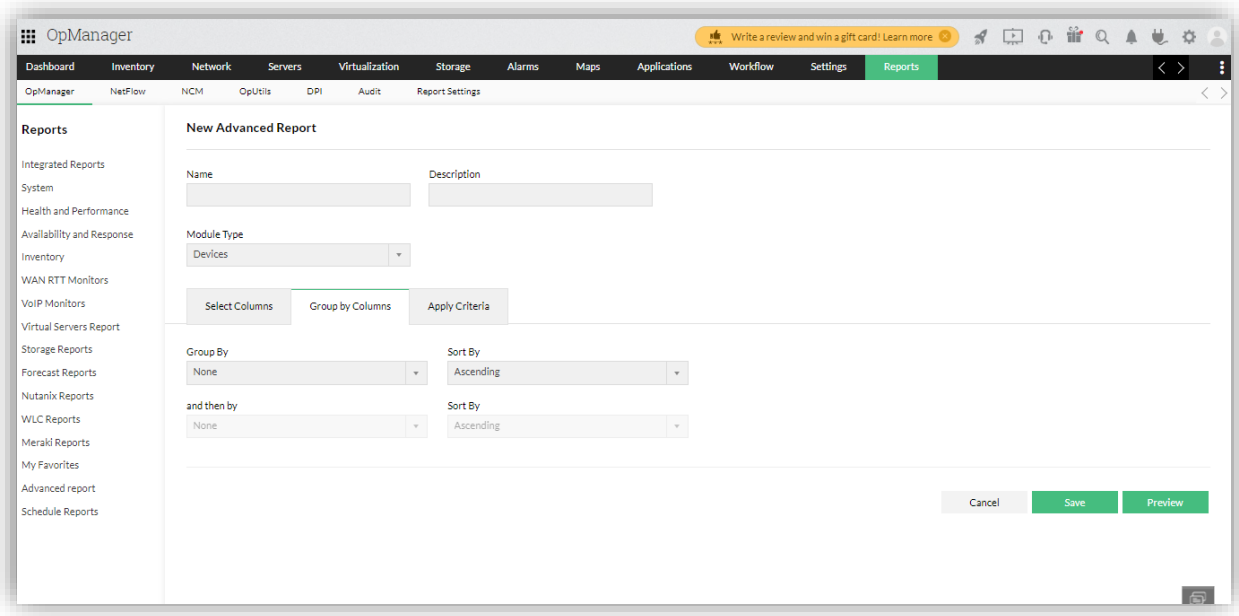
1. How to create New Advanced Report?

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

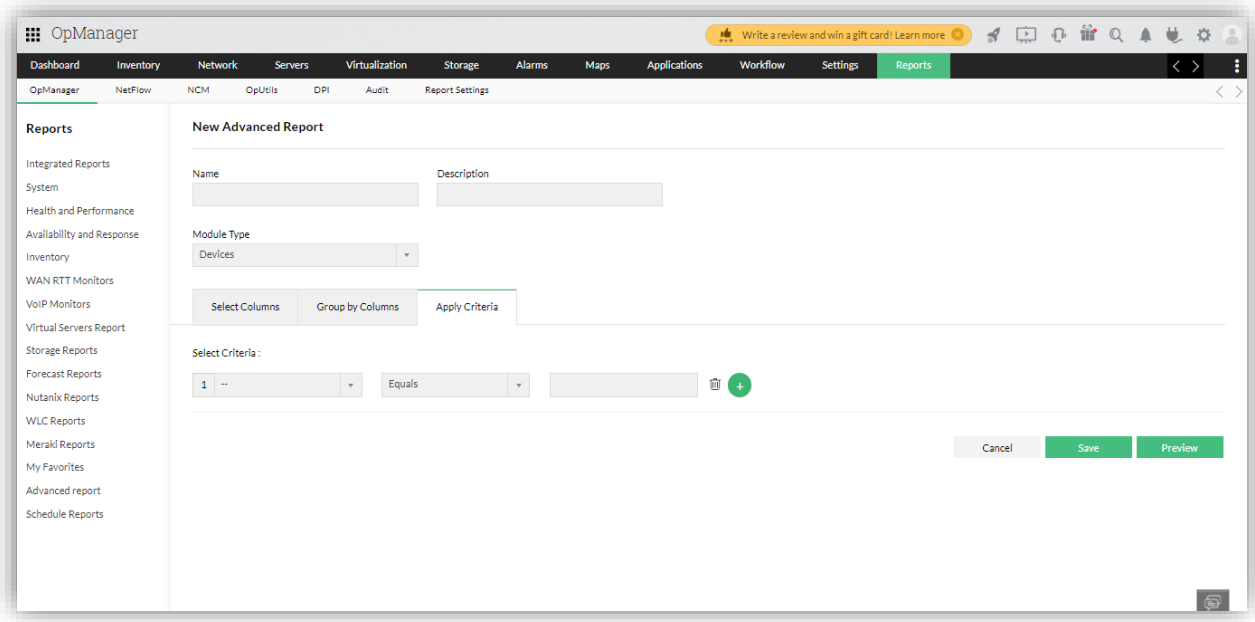
2. Click on Create New Report button available on the top right corner. (This option to create a new report is provided on the top right corner of every default report.)



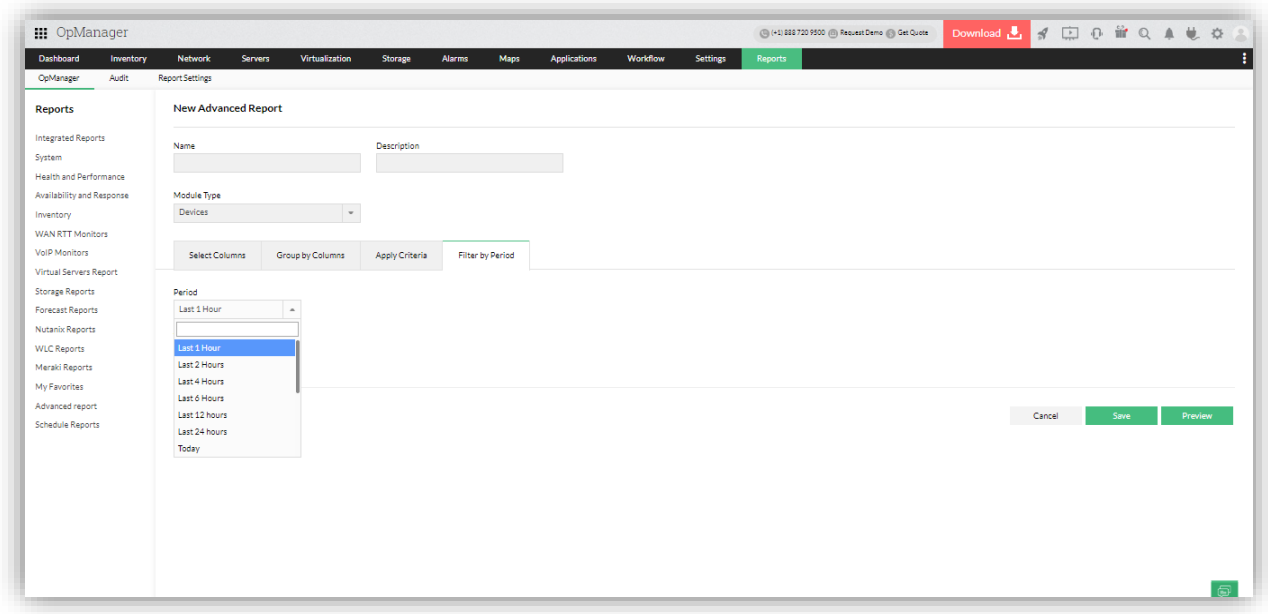
3. Enter a suitable Name and Description for the report.
4. Select a Module from the available list of modules - Devices, Interfaces, Service Monitors, URL Monitors, Alarms.
5. Select your preferred parameter categories from the Available Column Groups. Within each parameter category, there are multiple properties. (Advanced reports give users the option to view inventory data and performance monitors in a single report.)
6. 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)
7. 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.)



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



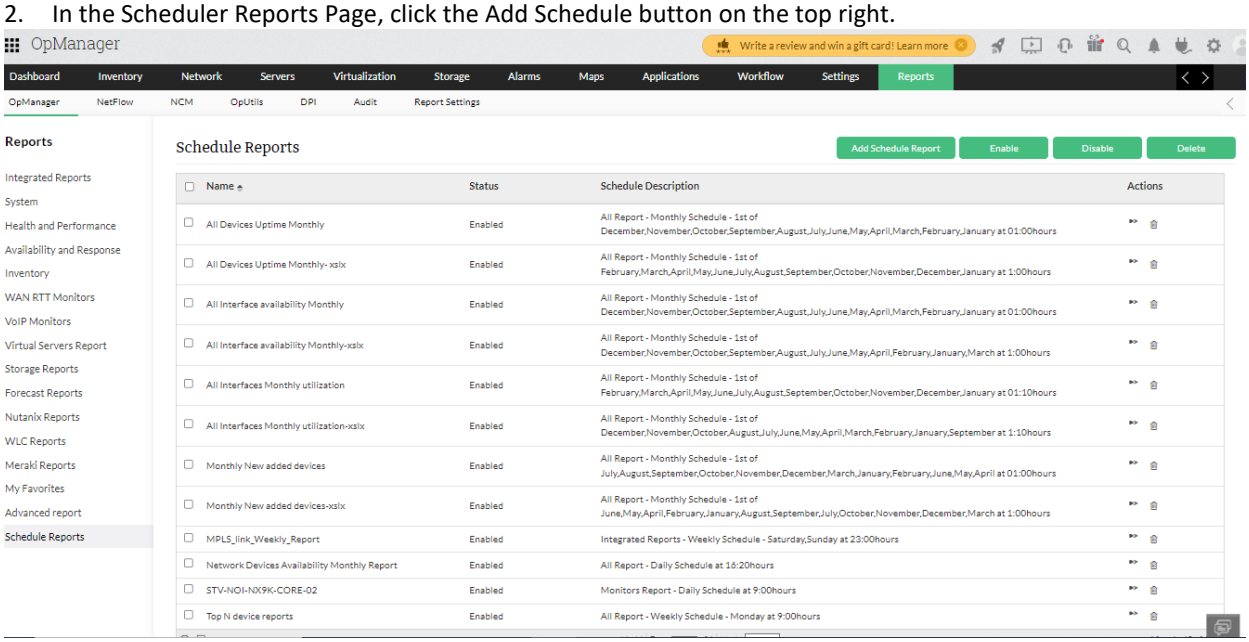
9. If you happen to choose a performance monitor, a new tab - Filter by Period - appears. Specify the mandatory fields of filtering time period and the Business Hour of your organization. (The filtering period by default takes the value of 12 hours. But you can choose a different value from the dropdown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



10. Click on Preview to view the report before being created. Click on Edit Report button to return to the previous page.
11. Then click on Save.
12. The report will be generated and stored and can be accessed in Reports --> OpManager --> Advanced report.

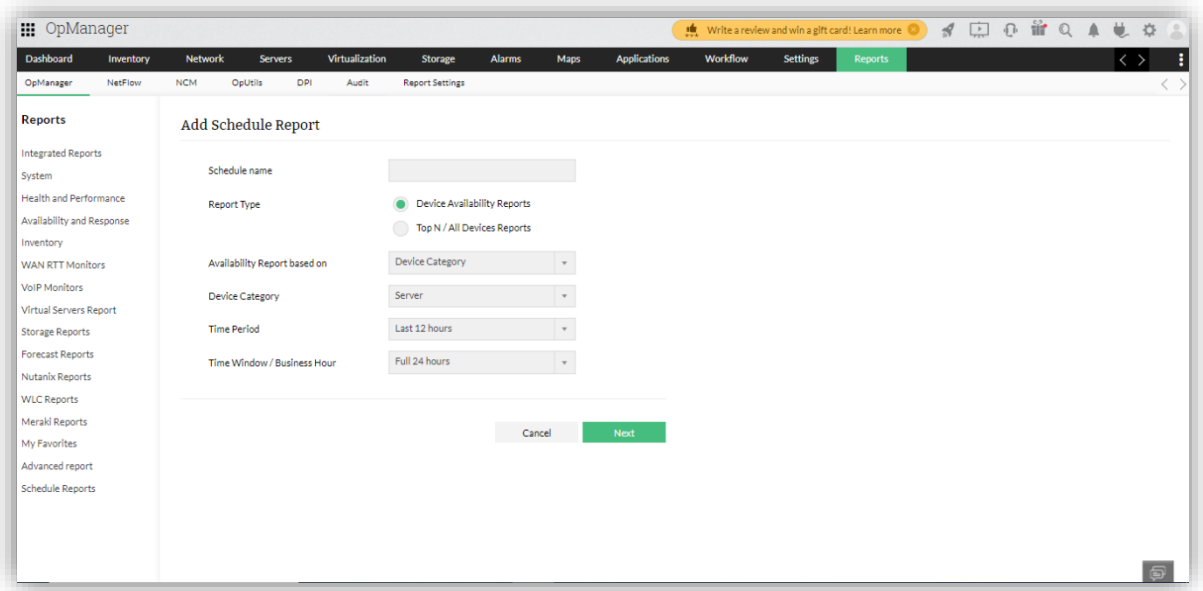
2. Schedule a new report

1. Go to Reports → Schedule Reports.
2. In the Scheduler Reports Page, click the Add Schedule button on the top right.

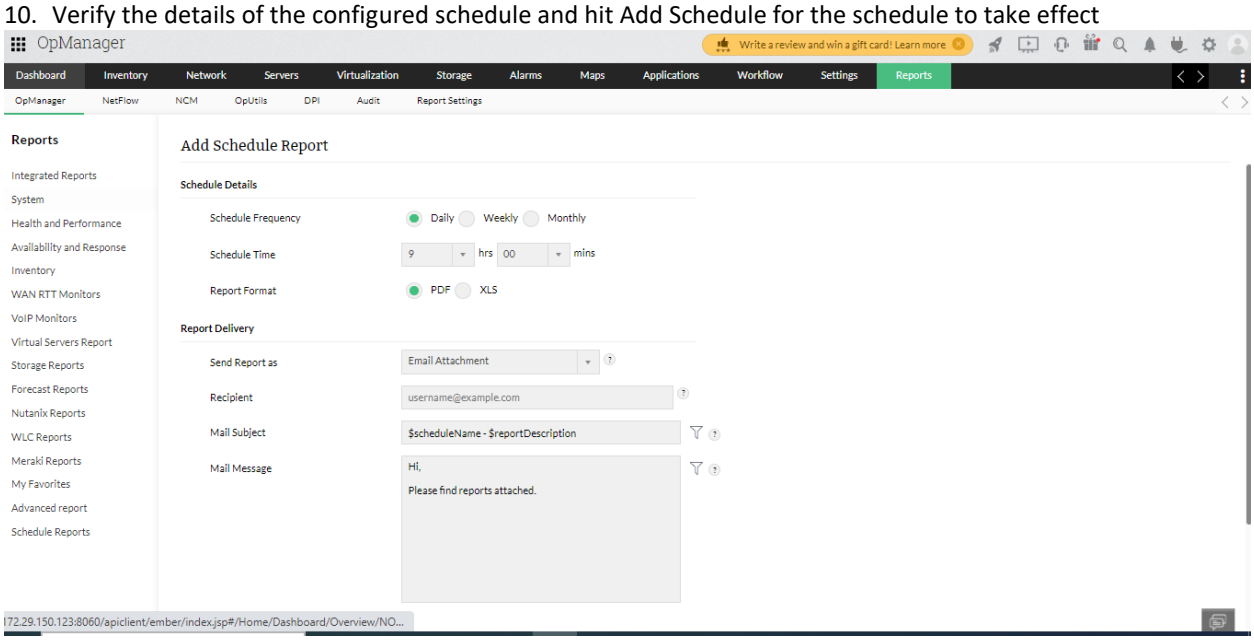


3. Enter Schedule Name
4. Choose Report Type
5. If you have chosen to schedule reports for Device availability reports and configure the following, Select either a category of devices, or the required business view, or select specific devices manually for generating the availability reports.
6. Select the Period and Time Window for which you want to generate the reports.

7. Select the days for which you want to exclude data in report using Exclude Days option.



8. Click Next
9. Configuring the Schedule for generating reports
10. Verify the details of the configured schedule and hit Add Schedule for the schedule to take effect

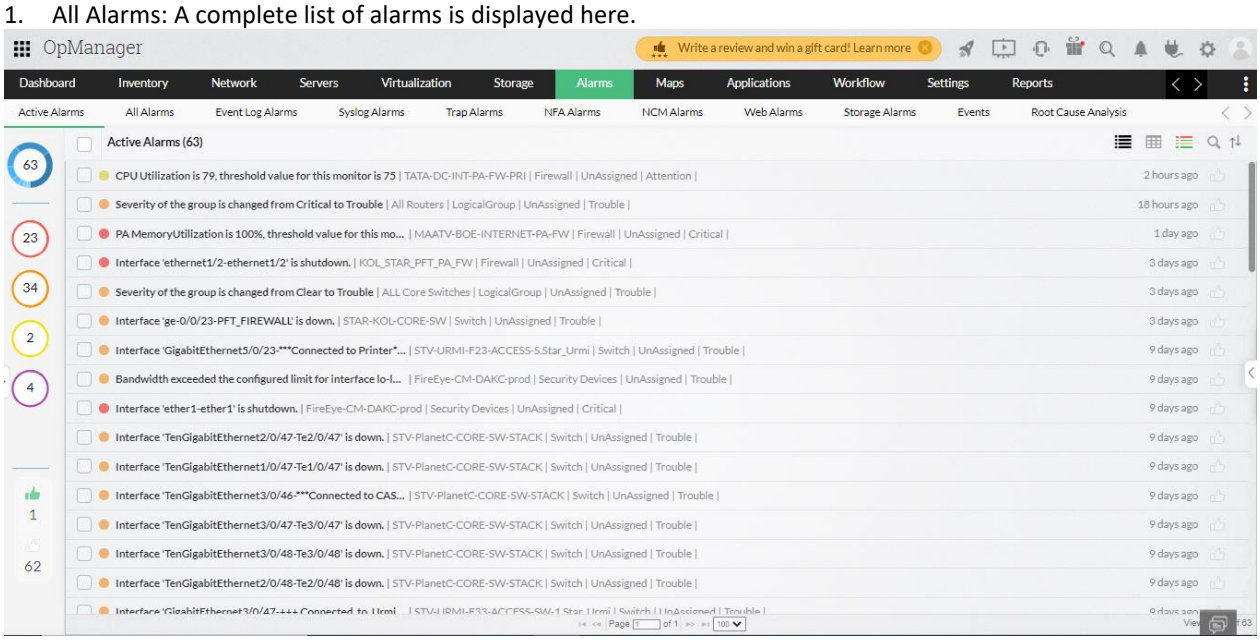


13. Alarms

The Alarms tab in OpManager shows all the latest alerts.

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

1. All Alarms: A complete list of alarms is displayed here.



2. Active Alarms: This view lists only the active alarms that are not yet cleared.
3. EventLog Alarms: This view lists only the alarms that are triggered from Windows event logs as the source.
4. Syslog Alarms: This view lists only the alarms logged via syslog.
5. Trap Alarms: This view lists only the alarms logged via traps.
6. Web Alarms: This view lists web alarms that are triggered via Notification Profiles.
7. Events: This view lists all logged events from all types of alarms.
8. VMware events: Under Events, you can also choose to view VMware events raised from VMware devices in your network (Visit this page to know more about supported VMware events in OpManager).
9. Application alarms: It lists down all the alarms raised for the APM plugin for application related events. Users can also view the application alarms under the All Alarms tab.
10. Addon alarms: You will be able to view alarms raised for monitoring traffic flows, configuration changes and firewall performance under the Alarms tab, if you had purchased licenses to enable NFA, NCM or Firewall addons in OpManager. A separate tab for each of these addons is given under the Alarms tab.
11. Storage alarms: OpManager also has a storage add on and enables you to monitor the performance of a wide range of storage devices including RAIDs, FC swtiches and Tape libraries. All storage network related alarms will be listed under the Storage alarms tab.

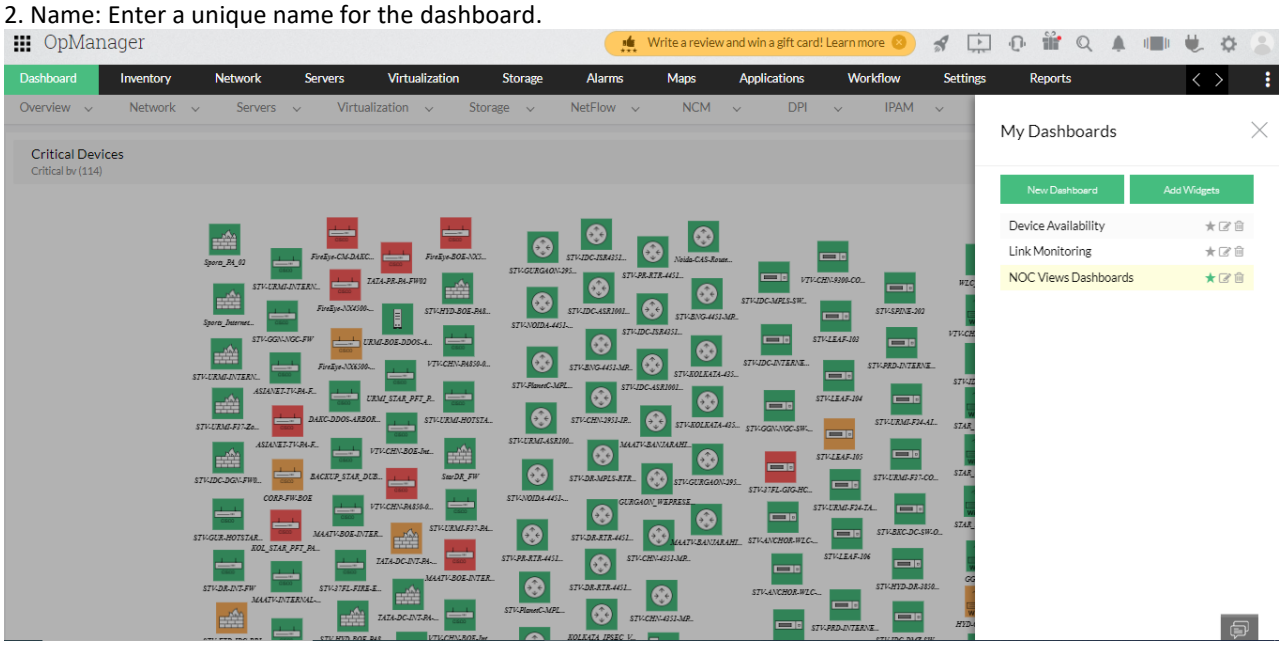
14. Dashboards

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.

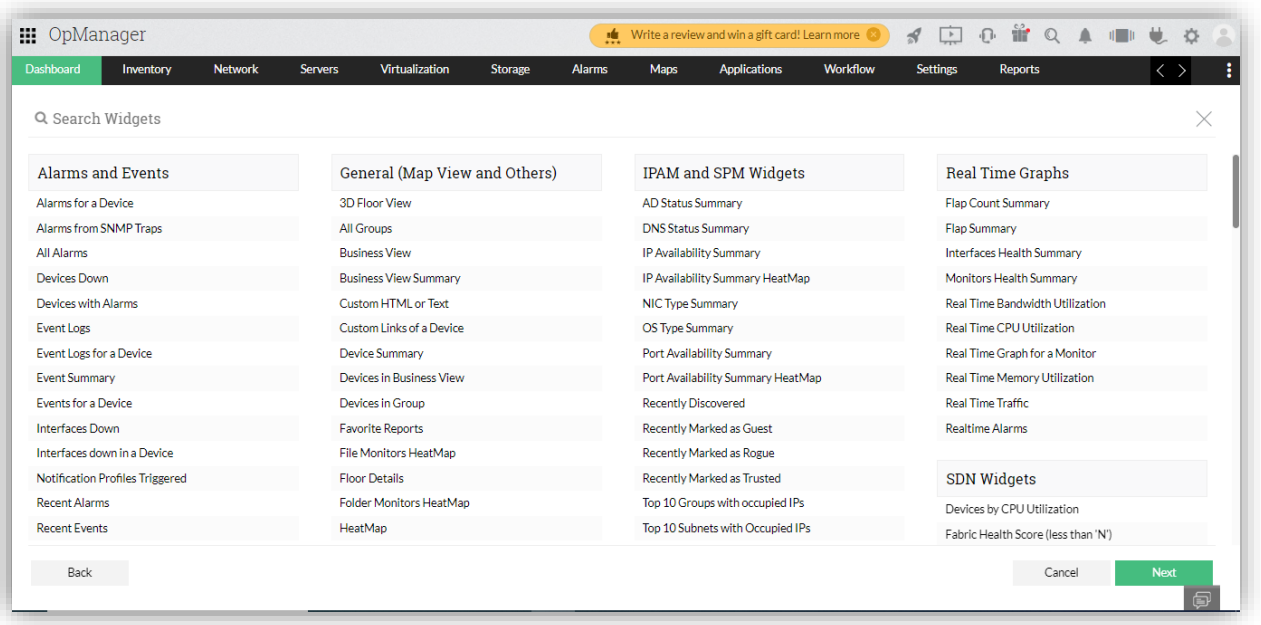
How to create new dashboard?

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].

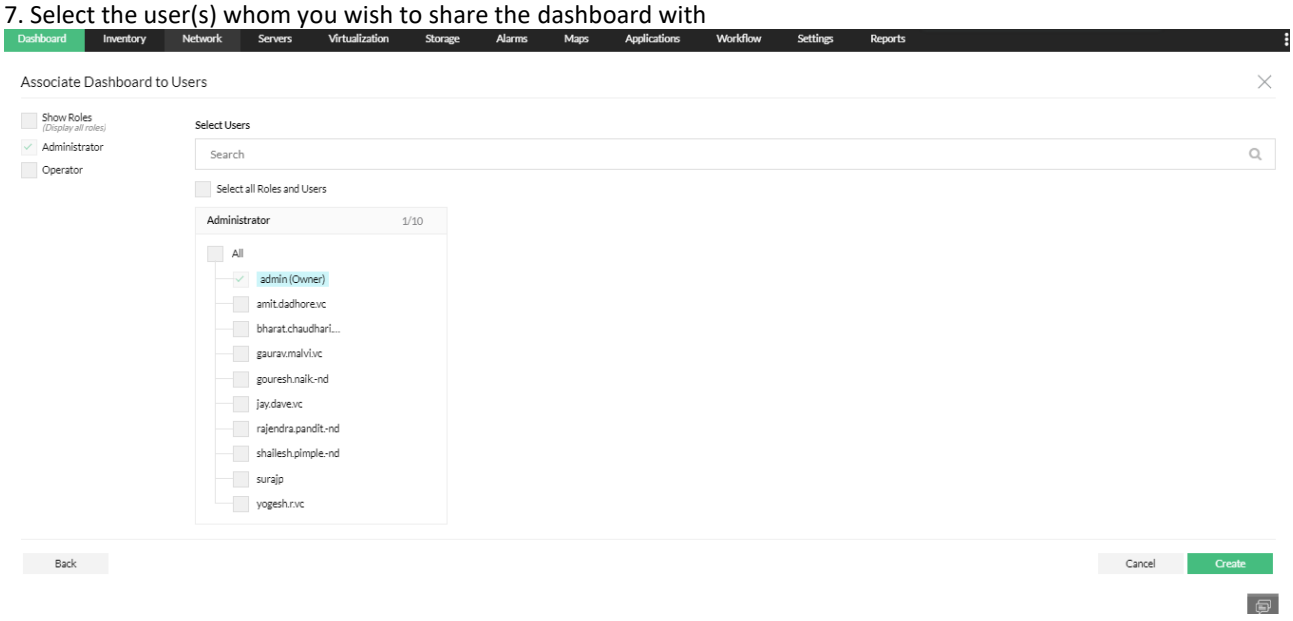
2. Name: Enter a unique name for the dashboard.



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



8. You can associate the dashboards with either of the following
All admins and/or all operators/or all users in a custom role (or)
You can manually select individual users.
9. After selected users to be associated, click on create. A new dashboard is created and listed on the My Dashboard page.

NetFlow Analyzer

ManageEngine NetFlow Analyzer is a web-based **bandwidth monitoring tool** that performs in-depth traffic analysis using data exported from **NetFlow / Netstream / cflowd / J-Flow / sFlow / IPFIX / AppFlow** flows.

15. Interface Discovery

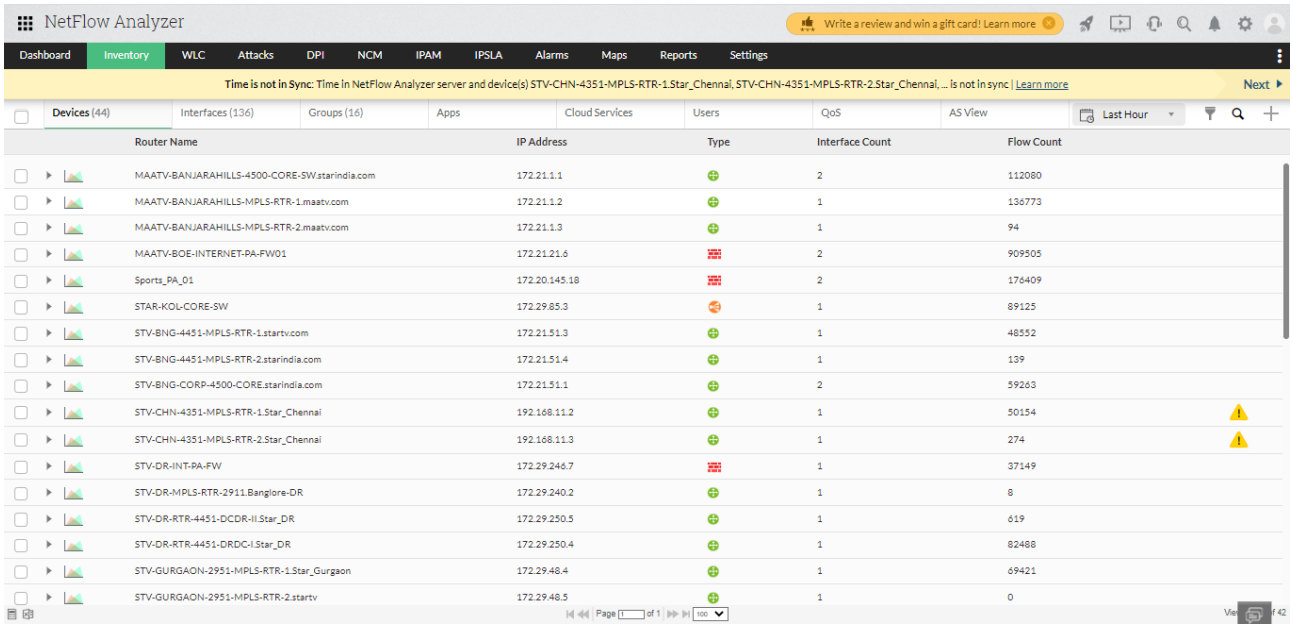
Configure flows in NetFlow Analyzer

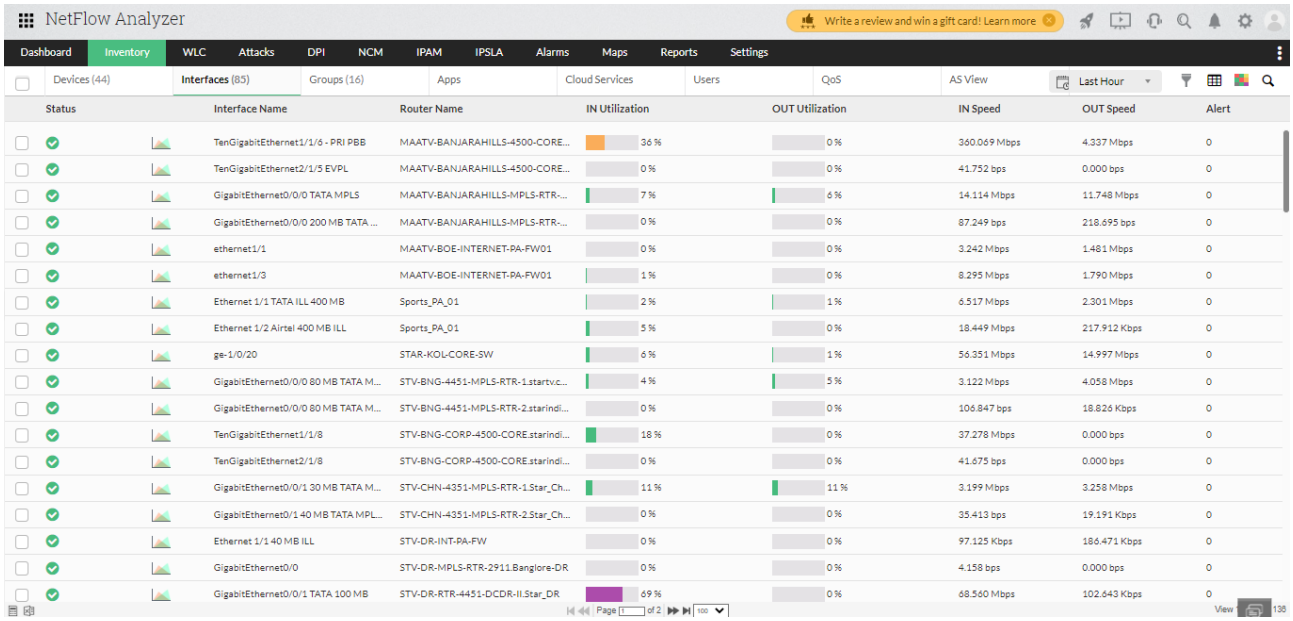
The first step to begin analyzing your flow data, NetFlow Analyzer lets you export flows from your network devices. The different flow formats supported by NetFlow Analyzer are NetFlow, sFLow, jFlow, IPFIX, Netstream, Appflow, etc. Once the flow data is exported from your routers, switches and firewalls, NetFlow Analyzer will show traffic data in the dashboard and inventory tab.

There are two ways of exporting flows in NetFlow Analyzer:

1. Using NetFlow Analyzer export flow tab
2. Using terminal

Device/Vendor	Supported Flow Export
Cisco devices	NetFlow
Juniper devices	cflowd, jFlow
Nortel	IPFIX
Huawei, 3com,H3C	Netstream
Alcatel-Lucent, Extreme Networks, Foundry Networks, HP, Hitachi, NEC, AlaxalA Networks, Allied Telesis, Comtec Systems, Force10 Networks	sFlow
Brocade vrouters	NetFlow
Fortigate	NetFlow
Cybrome firewall	NetFlow
Checkpoint & Sonicwall firewall	sFlow


NetFlow Analyzer
Write a review and win a gift card! Learn more
Dashboard
Inventory
WLC
Attacks
DPI
NCM
IPAM
IPSLA
Alarms
Maps
Reports
Settings
Time is not in Sync: Time in NetFlow Analyzer server and device(s) STV-CHN-4351-MPLS-RTR-1.Star_Chennai, STV-CHN-4351-MPLS-RTR-2.Star_Chennai, ... is not in sync | Learn more
Next
Devices (44)
Interfaces (136)
Groups (16)
Apps
Cloud Services
Users
QoS
AS View
Last Hour
Router Name
IP Address
Type
Interface Count
Flow Count
MAATV-BANJARAHILLS-4500-CORE-SW.starindia.com 172.21.1.1 2 112080
MAATV-BANJARAHILLS-MPLS-RTR-1.maatv.com 172.21.1.2 1 136773
MAATV-BANJARAHILLS-MPLS-RTR-2.maatv.com 172.21.1.3 1 94
MAATV-BOE-INTERNET-PA-FW01 172.21.21.6 2 909505
Sports_PA_01 172.20.145.18 2 176409
STAR-KOL-CORE-SW 172.29.85.3 1 89125
STV-BNG-4451-MPLS-RTR-1.startv.com 172.21.51.3 1 48552
STV-BNG-4451-MPLS-RTR-2.starindia.com 172.21.51.4 1 139
STV-BNG-CORP-4500-CORE.starindia.com 172.21.51.1 2 59263
STV-CHN-4351-MPLS-RTR-1.Star_Chennai 192.168.11.2 1 50154
STV-CHN-4351-MPLS-RTR-2.Star_Chennai 192.168.11.3 1 274
STV-DR-INT-PA-FW 172.29.246.7 1 37149
STV-DR-MPLS-RTR-2911.Banglore-DR 172.29.240.2 1 8
STV-DR-RTR-4451-DCDR-II.Star_DR 172.29.250.5 1 619
STV-DR-RTR-4451-DRDC-I.Star_DR 172.29.250.4 1 82488
STV-GURGAON-2951-MPLS-RTR-1.Star_Gurgaon 172.29.48.4 1 69421
STV-GURGAON-2951-MPLS-RTR-2.startv 172.29.48.5 1 0


NetFlow Analyzer
Write a review and win a gift card! Learn more
Dashboard
Inventory
WLC
Attacks
DPI
NCM
IPAM
IPSLA
Alarms
Maps
Reports
Settings
Devices (44)
Interfaces (85)
Groups (16)
Apps
Cloud Services
Users
QoS
AS View
Last Hour
Status
Interface Name
Router Name
IN Utilization
OUT Utilization
IN Speed
OUT Speed
Alert
TenGigabitEthernet1/1/6 - PRI PBB MAATV-BANJARAHILLS-4500-CORE... 36 % 0 % 360.069 Mbps 4.337 Mbps 0
TenGigabitEthernet2/1/5 EVPL MAATV-BANJARAHILLS-4500-CORE... 0 % 0 % 41.752 bps 0.000 bps 0
GigabitEthernet0/0/0 TATA MPLS MAATV-BANJARAHILLS-MPLS-RTR-... 7 % 6 % 14.114 Mbps 11.748 Mbps 0
GigabitEthernet0/0/0 200 MB TATA ... MAATV-BANJARAHILLS-MPLS-RTR-... 0 % 0 % 87.249 bps 218.695 bps 0
ethernet1/1 MAATV-BOE-INTERNET-PA-FW01 0 % 0 % 3.242 Mbps 1.481 Mbps 0
ethernet1/3 MAATV-BOE-INTERNET-PA-FW01 1 % 0 % 8.295 Mbps 1.790 Mbps 0
Ethernet 1/1 TATA ILL 400 MB Sports_PA_01 2 % 1 % 6.517 Mbps 2.301 Mbps 0
Ethernet 1/2 Airtel 400 MB ILL Sports_PA_01 5 % 0 % 18.449 Mbps 217.912 Kbps 0
ge-1/0/20 STAR-KOL-CORE-SW 6 % 1 % 56.351 Mbps 14.997 Mbps 0
GigabitEthernet0/0/0 80 MB TATA M... STV-BNG-4451-MPLS-RTR-1.startv.c... 4 % 5 % 3.122 Mbps 4.058 Mbps 0
GigabitEthernet0/0/0 80 MB TATA M... STV-BNG-4451-MPLS-RTR-2.starindi... 0 % 0 % 106.847 bps 18.826 Kbps 0
TenGigabitEthernet1/1/8 STV-BNG-CORP-4500-CORE.starindi... 18 % 0 % 37.278 Mbps 0.000 bps 0
TenGigabitEthernet2/1/8 STV-BNG-CORP-4500-CORE.starindi... 0 % 0 % 41.675 bps 0.000 bps 0
GigabitEthernet0/0/1 30 MB TATA M... STV-CHN-4351-MPLS-RTR-1.Star_Ch... 11 % 11 % 3.199 Mbps 3.258 Mbps 0
GigabitEthernet0/1 40 MB TATA MPL... STV-CHN-4351-MPLS-RTR-2.Star_Ch... 0 % 0 % 35.413 bps 19.191 Kbps 0
Ethernet 1/1 40 MB ILL STV-DR-INT-PA-FW 0 % 0 % 97.125 Kbps 186.471 Kbps 0
GigabitEthernet0/0 STV-DR-MPLS-RTR-2911.Banglore-DR 0 % 0 % 4.158 bps 0.000 bps 0
GigabitEthernet0/0/1 TATA 100 MB STV-DR-RTR-4451-DCDR-II.Star_DR 69 % 0 % 68.560 Mbps 102.643 Kbps 0

16. Alert Profiles

An alert profile is created to set the thresholds for generating alerts. The parameters to be set for creating an alert profile are:

1. Real-time alerts

- **Source(Interfaces/ IP Groups / Interface Groups / Access Points / SSID Groups)** - The list of interfaces / IP Groups / Interface Group / Access Points / SSID Groups whose bandwidth utilization must be watched.
- **Traffic pattern** - The traffic to be watched - In Traffic, Out Traffic or a Combination of both.
- **Threshold Settings** - It has 3 settings namely % utilization, no. of times, and duration.
    - **% Utilization/Volume/Speed/Packets** - When the utilization exceeds this limit, it is noted
    - **No. of time** - The number of times the utilization can be allowed to exceed the threshold before an alert is raised
    - **Duration** - The time period within which, if the threshold is exceeded the specified number of times - an alert is created(generated)

2. Aggregated alerts

- **Source(Interfaces/ IP Groups / Interface Groups / Access Points / SSID Groups)** - The list of interfaces / IP Groups / Interface Group / Access Points / SSID Groups whose bandwidth utilization must be watched.
- **Time period**
    - **Custom** - To carry out bandwidth usage monitoring between provided start and end time.
    - **Periodic** - Monitors bandwidth usage at mentioned intervals from the given start time.
- **Threshold Settings** - It has 3 settings namely traffic pattern to be monitored(In Traffic, Out Traffic or a Combination of both), Volume/Packets, and number of bytes/packets.

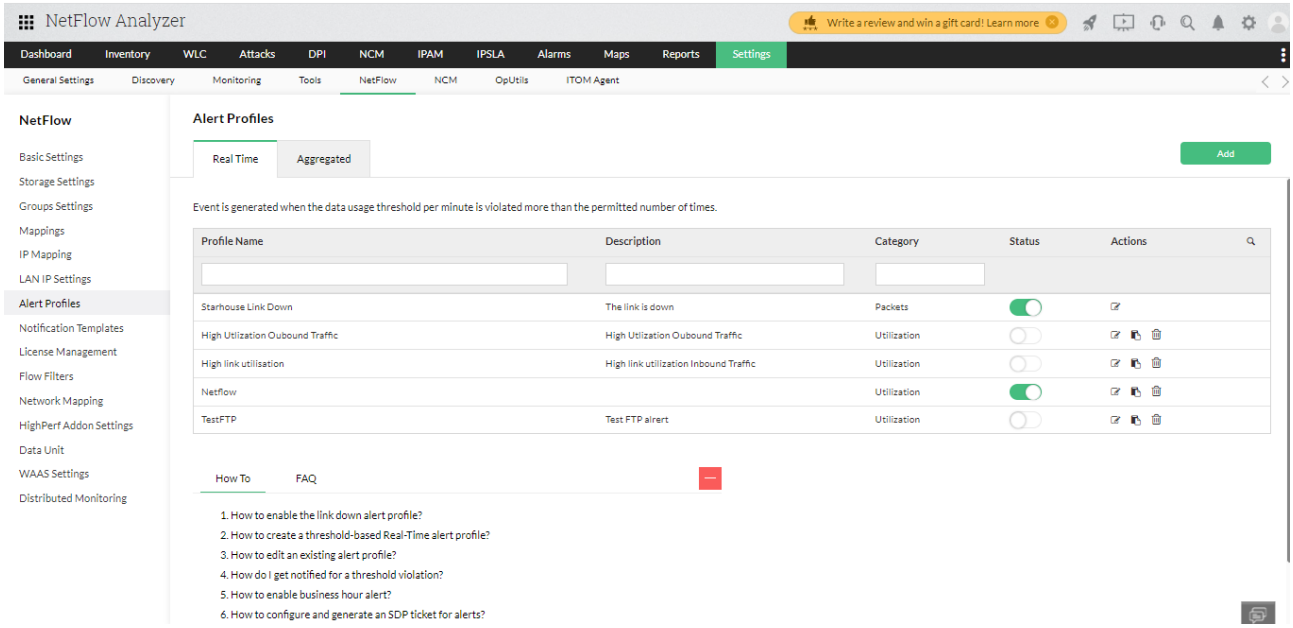
Netflow Analyzer calculates the bandwidth utilization of the specified interfaces/ IP Groups / Interface Group every minute. If the utilization exceeds the threshold value, the time when it exceeded is noted. Subsequently when it exceeds, the corresponding times are noted. If the number of times the utilization exceeds the specified limit, in the specified time duration, an alert is generated. When an alert is generated, you can also send an email to one / more people or send an SNMP trap to a manager application.

The **Alert Profile Management** option lets you create and manage alert profiles. The Alert Profiles page lists all existing alert profiles, along with the number of alerts generated for each profile. The application comes loaded with a preconfigured alert that can trigger an email alert when a link goes down or when there are no flows for more than 5 minutes.

3.Link Down Alert

This is a preconfigured alert to send an email or log an SDP ticket when the link goes down or when there are no flows for more than 5 minutes. By default this profile is disabled. This is similar to other alerts that are manually configured except that it can't be deleted. It is possible to have emails sent by this alert whenever no flows are received for over 5 minutes. It becomes activated only after the mail server settings are configured. You can also create a custom notification template to get alerts every time the link goes down or no flows are received for a time period of 3 minutes to 30 minutes.

4.Operations on Alert Profiles



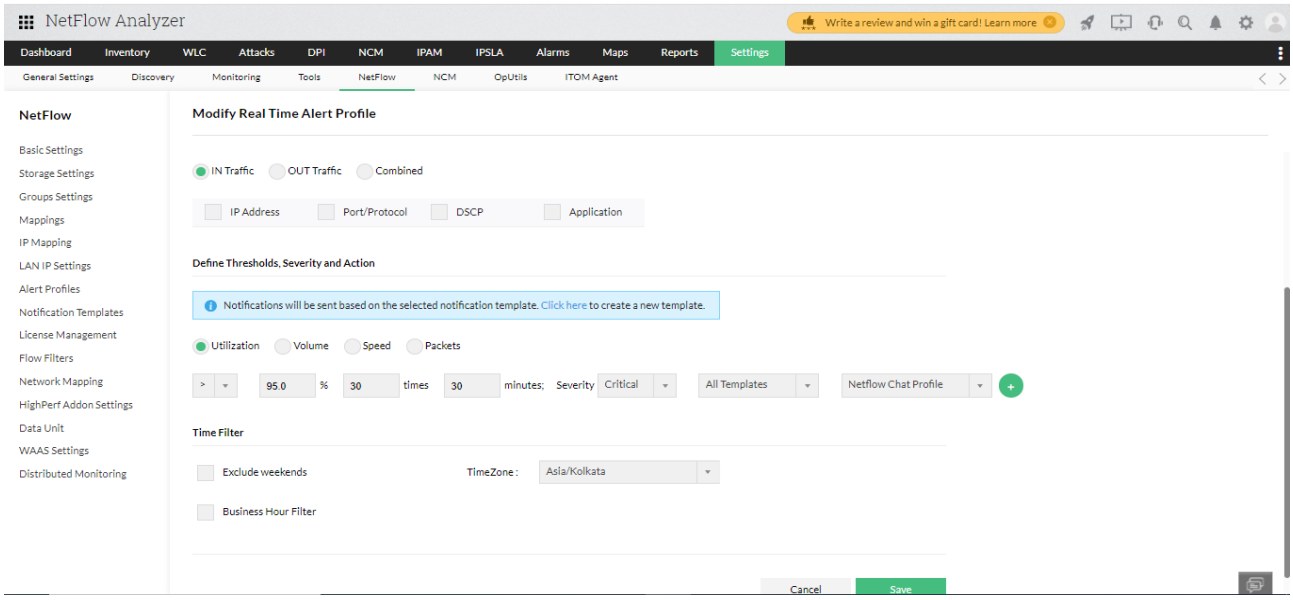
You can create new alert profiles, modify, or delete existing ones from the Alert Profiles page.
Creating a new Alert Profile
The steps to create an Alert Profile are:
Login to the NetFlow Analyzer client and click "**Alert Profile Management**" under "**Admin Operations**" in the left panel
Select the Alert Profile type as Real-Time or Aggregated.
Click "**Add**" to add a new Alert Profile
Fill in the following details

Field	**Description**
Alert Profile Name	Enter a unique name to identify this alert profile
Description	Enter descriptive information for this alert profile to help other operators understand why it was created.
Select Source	By default all Interfaces / IP Groups/ Interface Group sending NetFlow exports are selected. If you want this alert profile to apply to certain interfaces/ ip groups / Interface Groups only, click the **Modify Selection** link. In the pop-up window, select the required devices and interfaces or select the IP Group Names and click **Update** to save your changes.

Define Alert Criteria	Select whether alerts need to be generated based on incoming traffic, outgoing traffic, or both. The default setting is for both(combined).
	Then select the application / port for which the alert has to be generated. This criteria can be very general - Any application traffic can be profiled - or it can be highly specific - Generate the alert only when a specific application, protocol, and/or port is used. To identify the overall link utilization the "No Criteria" option has to be chosen
Define Threshold and Action	Enter the threshold conditions (threshold utilization, no. of times it can exceed and the time duration) exceeding which the alert will be generated. You can also specify an action to be taken during the alert creation. - Email - to send a notification to one or more people. - SNMP Trap - to send a trap to the manager application (specify the <server name>:<port>:<community>). For details on configuring trap forwarding, refer to SNMP Trap Forwarding section under Appendix To add more threshold values, click 'Add Row' and add values
Business Hour Alerts	This option enables alerting only during the configured time range of a day. Alerts will not be generated outside this time range.

You can configure the way you want to receive alerts by creating a notification template that suits your preference.
After setting the required thresholds, click '**Save**'

The new alert profile is created and activated. The system watches the utilization and raises alarms when the specified conditions are met.



17. Reports

NetFlow Analyzer has many reporting options available based on Interfaces and IP groups out of box.

Consolidated Reports

Consolidated reports let you see all the traffic details for an interface, interface group or IP group at a glance.

Click the Reports Tab -> More Reports -> Consolidated Report link to see all traffic details for an interface, interface group or IP Group at one glance.

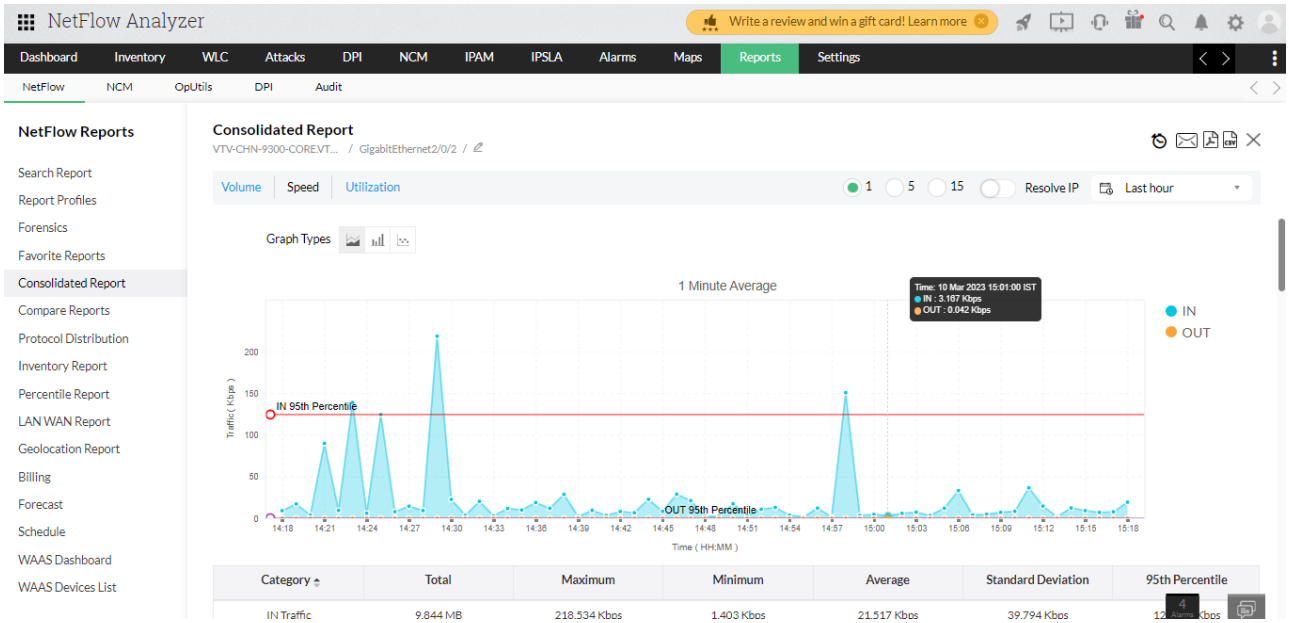
Select the Interface, Interface Group or IP group based on which you need the consolidated report under **Select Source** tab. Once you Select the Interface you will have the option to select the Device and Interface interface based on which you need the report in the same way you can select IP Group and for Interface groups as well.

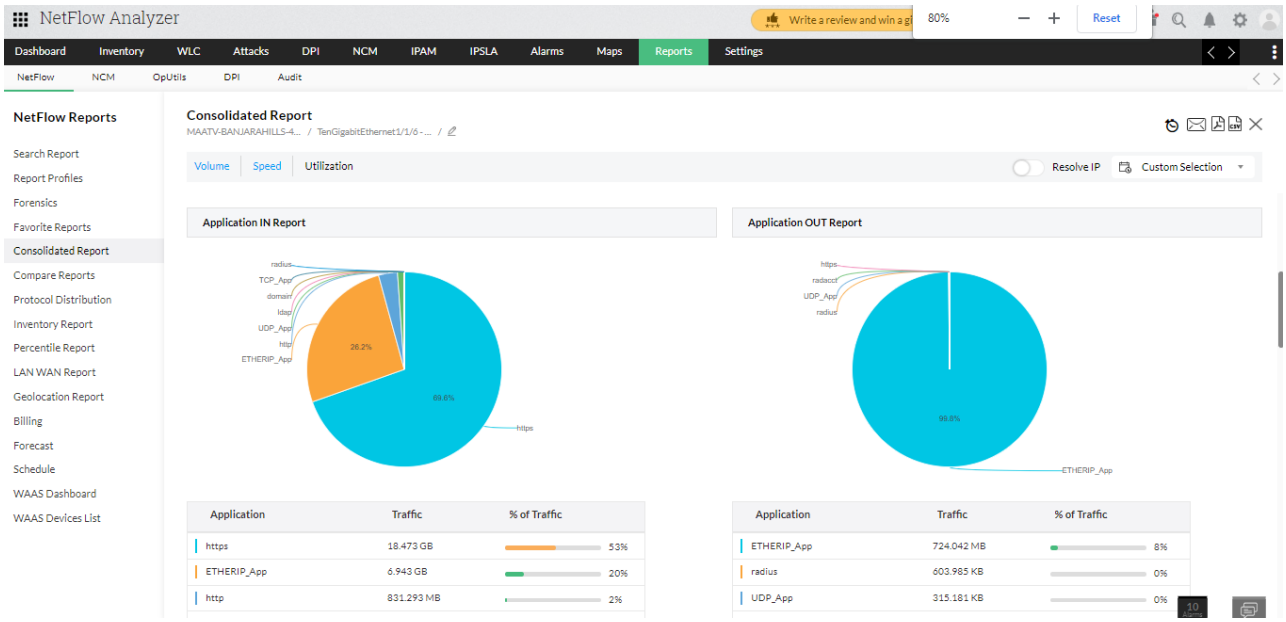
Select Top allows you to show view with top 5,10 or top 20 outputs for top Source, destination and Application.

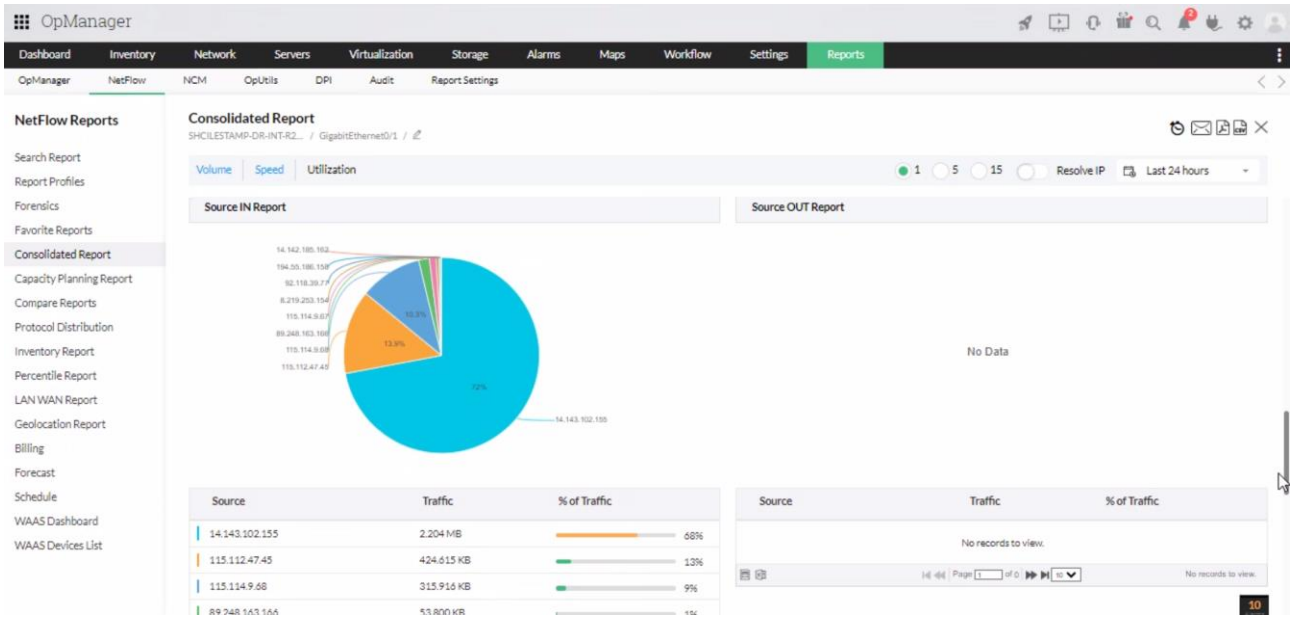
Traffic Type give the option to select the view for the traffic graph details in either Speed, Volume or Utilization.

You can choose to generate hourly, daily or reports based only on business hours and also customise time period by selecting Custom option under **Time Period** option.

Click on Generate Report to generate the report. The report gives the Graphical and Tabular representation for Traffic Graph, Application IN/OUT, Source IN/OUT and Destination IN/OUT

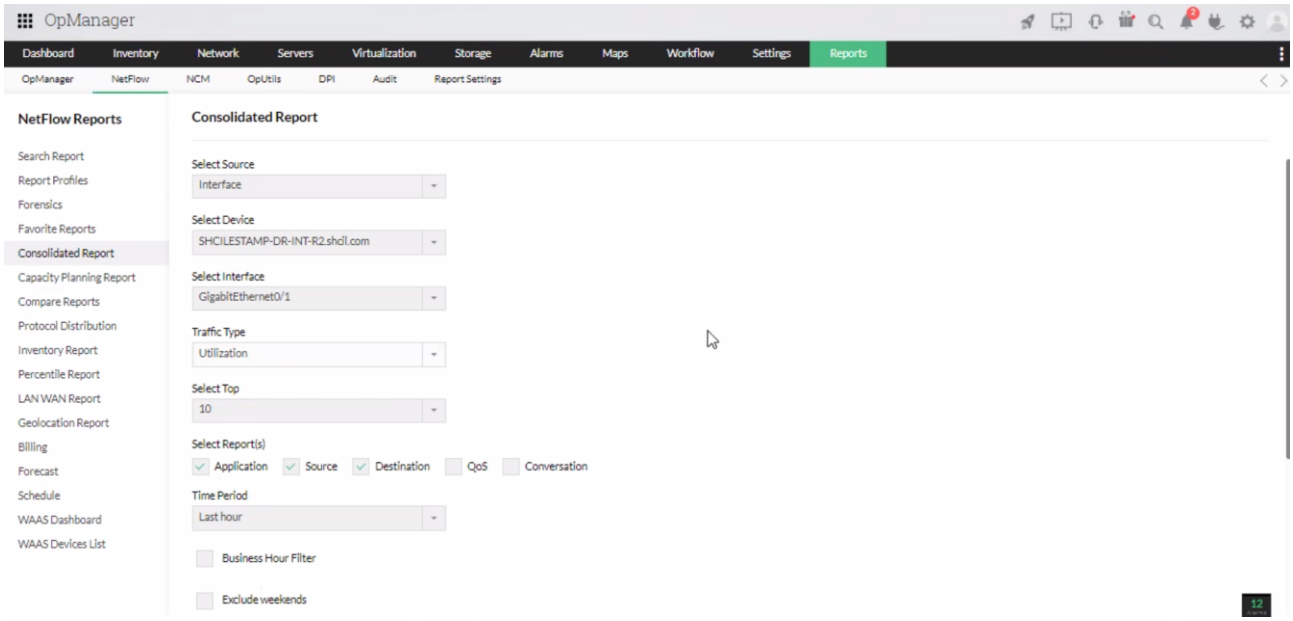

NetFlow Analyzer
Write a review and win a gift card! Learn more
Dashboard
Inventory
WLC
Attacks
DPI
NCM
IPAM
IPSLA
Alarms
Maps
Reports
Settings
NetFlow
NCM
OpUtils
DPI
Audit
NetFlow Reports
Search Report
Report Profiles
Forensics
Favorite Reports
Consolidated Report
Compare Reports
Protocol Distribution
Inventory Report
Percentile Report
LAN WAN Report
Geolocation Report
Billing
Forecast
Schedule
WAAS Dashboard
WAAS Devices List
Consolidated Report
VTV-CHN-9300-CORE.VT... / GigabitEthernet2/0/2 /
Volume
Speed
Utilization
Resolve IP
Last hour
Graph Types
1 Minute Average
IN
OUT
IN 95th Percentile
OUT 95th Percentile
Traffic (Kbps)
Time (HH:MM)
Category
Total
Maximum
Minimum
Average
Standard Deviation
95th Percentile
IN Traffic
9.844 MB
218.534 Kbps
1.403 Kbps
21.517 Kbps
39.794 Kbps

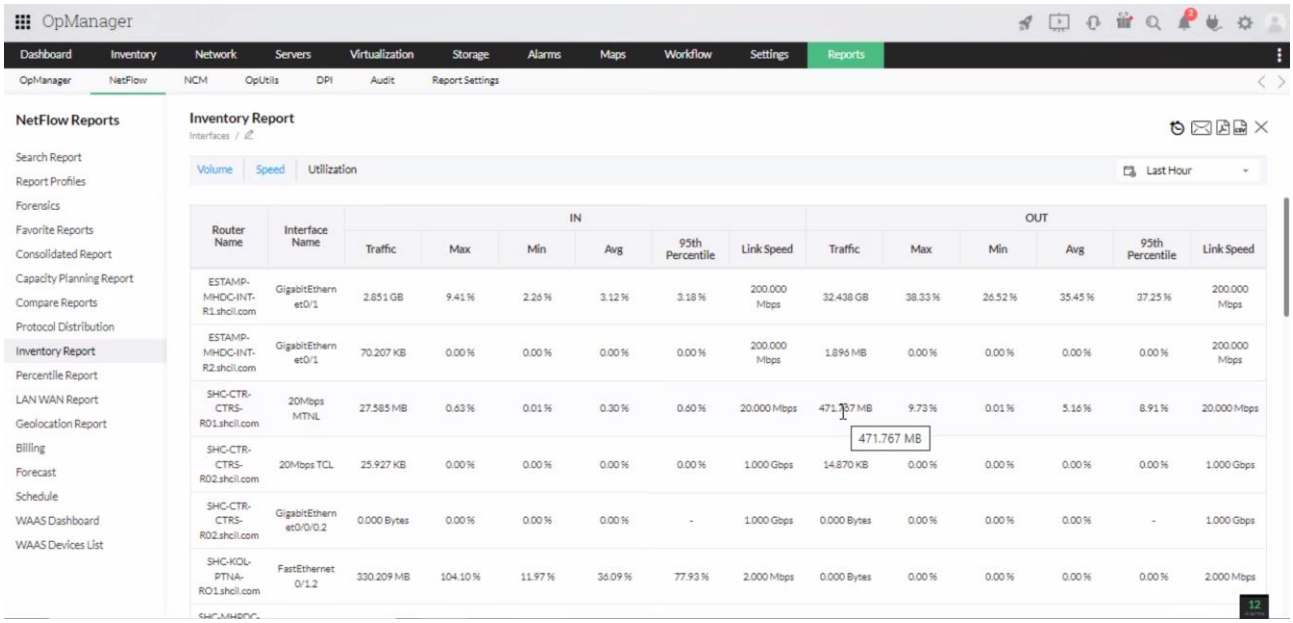

NetFlow Analyzer
Dashboard
Inventory
WLC
Attacks
DPI
NCM
IPAM
IPSLA
Alarms
Maps
Reports
Settings
NetFlow
NCM
OpUtils
DPI
Audit
NetFlow Reports
Search Report
Report Profiles
Forensics
Favorite Reports
Consolidated Report
Compare Reports
Protocol Distribution
Inventory Report
Percentile Report
LAN WAN Report
Geolocation Report
Billing
Forecast
Schedule
WAAS Dashboard
WAAS Devices List
Consolidated Report
Volume
Speed
Utilization
Resolve IP
Custom Selection
Application IN Report
Application OUT Report
Application
Traffic
% of Traffic
https
18.473 GB
53%
ETHERIP_App
6.943 GB
20%
http
831.293 MB
2%
ETHERIP_App
724.042 MB
8%
radius
603.985 KB
0%
UDP_App
315.181 KB
0%



Inventory Report

In the absence of a proactive network monitoring solution, network monitoring can become a daunting task. Network administrators will have to monitor the entire network manually which can be a rather monotonous, time-consuming and error-prone task. With Inventory reports, these repetitive network monitoring tasks have been simplified. With an easy-to-use interface and a consolidated view of your preference, the Inventory report delivers a bird's-eye view over your network traffic.





Inventory report enables you to choose amongst the **traffic source** - Interface/IP Group/Interface Group/Access Point/AS View/Access Point Group/SSID Group.

The **traffic type** allows you to generate a report based on speed, volume or utilization. Furthermore, you can also set the **criteria** based on the selected traffic type.

Inventory report can be generated in the period of your preference and additional **business hour filters** can also be enabled.

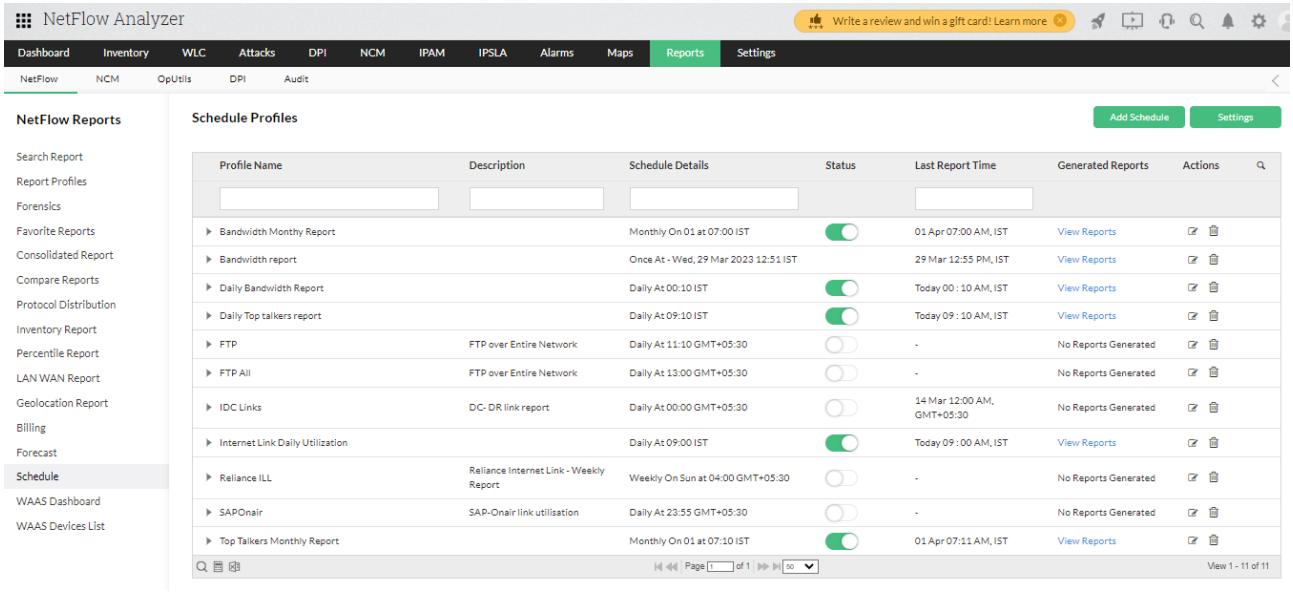
Also note that a **violation report** will be generated if the selected criteria are violated. This report can be viewed by clicking on the graph icon in the generated report.

18. Schedule Reports

Schedule feature in NetFlow Analyzer is an easy way to generate reports in Daily, weekly and Monthly basis. A scheduler is configured to set the parameters for automating the generation of reports.

To create an schedule navigate to reports tab  and click on **Schedule.**

Netflow Analyzer calculates the bandwidth utilization on the specified Interfaces, Interface groups, IP Group, WLC Devices, Access point groups, SSID groups for every minute. Based on the schedule opted for, reports are generated at various time intervals.The Schedule Reports feature lets you Create new Schedules and Delete existing ones. The Scheduler List page lists all existing schedules , along with the Schedule details,Status, Report types,and the Last Report Generated time.



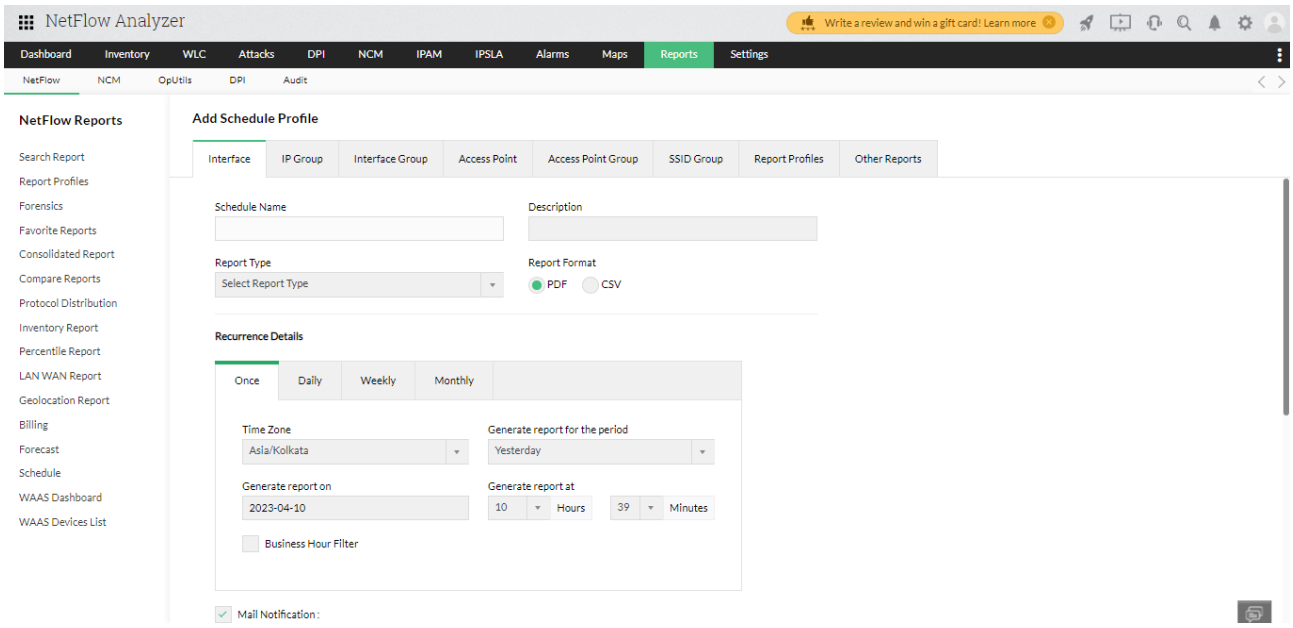
Click on Add Schedule and fill in the necessary details.

Under interface fill in the Schedule name, Report type and report format. Then schedule the report under Recurrence details.

Select if you want the report Once or daily or weekly or monthly.

Select the time it must be generated on and the business hour filter.

Fill in the mail details and click save.



Thank you for choosing us, We value your time and efforts.