



SOFTCELL

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

Implementation Document for Manage Engine OPManger 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, Implementation Management, etc.

Revision History

Version	Date	Changes	Author
1	09 th 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	Implementation 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 (shriiyyer@softcell.com)

Table of Contents

Project Description	Error! Bookmark not defined.
1. Installation of the OP Manager	7
2. Configure mail server settings.....	15
3. Apply SSL certificate.....	16
4. Credentials.....	17
5. Device Discovery	18
1. INDIVIDUAL DISCOVERY OF DEVICES.....	18
2. BULK DISCOVERY OF DEVICES:	18
6. Groups.....	21
STEPS TO CREATE A GROUP	21
7. Performance Monitors	23
1. FROM DEVICE SNAPSHOT PAGE	23
2. FROM DEVICE TEMPLATES:	24
8. Threshold Configuration	26
1. CONFIGURE THRESHOLD LIMITS FOR PERFORMANCE MONITORS IN AN INDIVIDUAL DEVICE	26
2. CONFIGURE THRESHOLD LIMITS FOR MULTIPLE DEVICES OF SAME TYPE USING DEVICE TEMPLATE	27
9. Device Templates	29
BASIC CONFIGURATION	29
10. Business Views	30
CREATING A BUSINESS VIEW:	30
11. NOC View (CCTV)	31
STEPS TO CREATE NOC VIEW:.....	31
12. Notification Profile	32
STEPS TO CREATE NOTIFICATION PROFILE	32
13. Reports.....	36
1. HOW TO CREATE NEW ADVANCED REPORT?	36
2. SCHEDULE A NEW REPORT.....	39
13. Alarms.....	41
14. Dashboards.....	42
HOW TO CREATE NEW DASHBOARD?	42

15. INTERFACE DISCOVERY	CONFIGURE FLOWS IN NETFLOW ANALYZER	44
16.	Alert Profiles.....	46
1. REAL-TIME ALERTS		46
2. AGGREGATED ALERTS.....		46
3.LINK DOWN ALERT		46
4.OPERATIONS ON ALERT PROFILES.....		47
17.	Reports.....	49
CONSOLIDATED REPORTS		49
INVENTORY REPORT.....		51
18. SCHEDULE REPORTS		53
A SIMPLE AND ELEGANT SOLUTION	ERROR! BOOKMARK NOT DEFINED.
19. DEVICE ADDITION.....		ERROR! BOOKMARK NOT DEFINED.
OVERVIEW		ERROR! BOOKMARK NOT DEFINED.
MANUAL ADDITION OF DEVICES		ERROR! BOOKMARK NOT DEFINED.
IMPORTING DEVICES FROM A TEXT FILE		ERROR! BOOKMARK NOT DEFINED.
20. Editing Host Names in Bulk		Error! Bookmark not defined.
21. Adding Schedules	Error! Bookmark not defined.
ADDING SCHEDULES.....		ERROR! BOOKMARK NOT DEFINED.
MANAGING SCHEDULES.....		ERROR! BOOKMARK NOT DEFINED.
22. Backing up Device Configuration.....	Error! Bookmark not defined.
Overview		Error! Bookmark not defined.
TAKING BACKUP OF DEVICE CONFIGURATION		ERROR! BOOKMARK NOT DEFINED.
AUTOMATING BACKUP THROUGH SCHEDULES		ERROR! BOOKMARK NOT DEFINED.
23. Real-time Configuration Change Detection.....	Error! Bookmark not defined.
OVERVIEW.....		ERROR! BOOKMARK NOT DEFINED.
HOW DOES REAL-TIME CHANGE DETECTION WORK?		ERROR! BOOKMARK NOT DEFINED.
HOW DOES REAL-TIME DETECTION BENEFIT ME?		ERROR! BOOKMARK NOT DEFINED.
HOW DO I ENABLE REAL-TIME CHANGE DETECTION?		ERROR! BOOKMARK NOT DEFINED.
LISTENING TO FORWARDED SYSLOG MESSAGES		ERROR! BOOKMARK NOT DEFINED.
AUTOMATED CHANGE DETECTION THROUGH SCHEDULES		ERROR! BOOKMARK NOT DEFINED.
24. Reports	Error! Bookmark not defined.
OVERVIEW.....		ERROR! BOOKMARK NOT DEFINED.
25. Adding Subnets for Scanning	Error! Bookmark not defined.
ADDING SUBNETS MANUALLY		ERROR! BOOKMARK NOT DEFINED.
IMPORTING SUBNETS FROM A CSV FILE		ERROR! BOOKMARK NOT DEFINED.
26. Schedule Subnet Scanning	Error! Bookmark not defined.
27. IP Address Manager Settings.....		Error! Bookmark not defined.

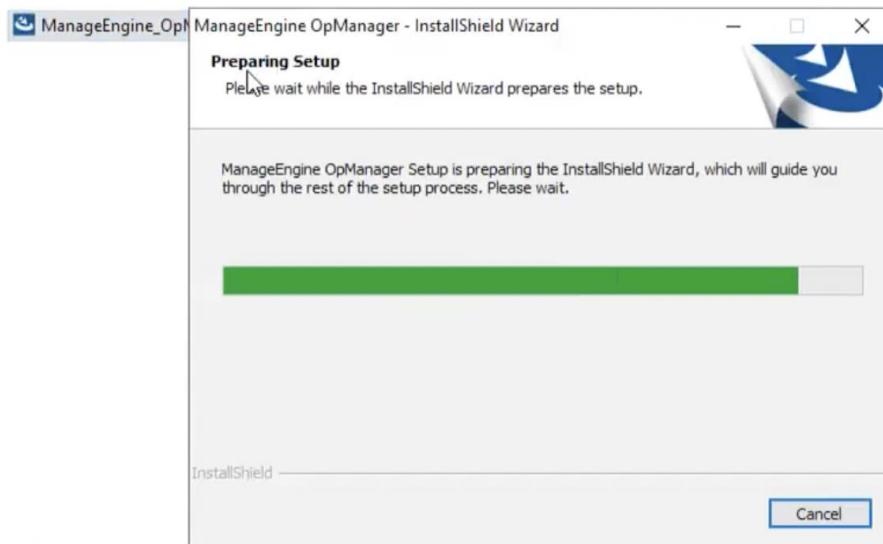
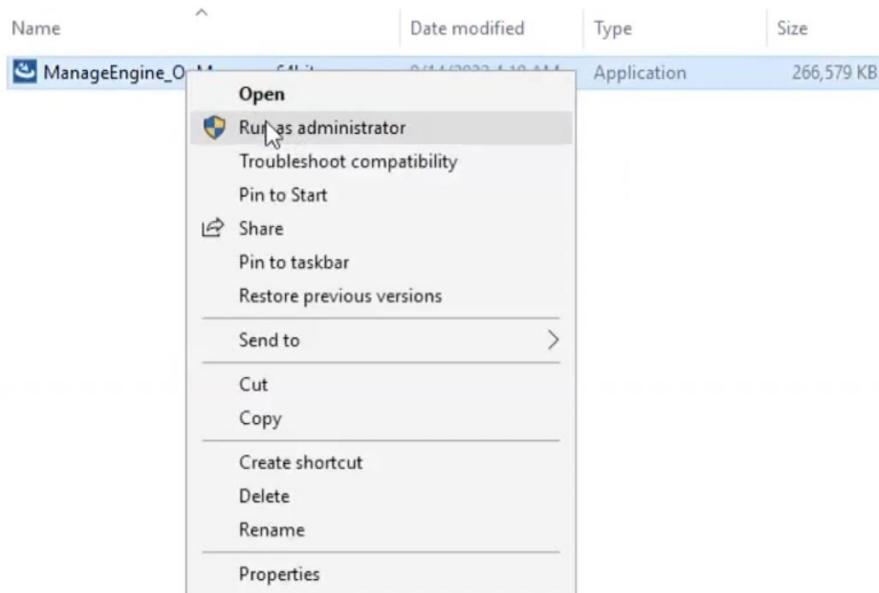
GENERAL SETTINGS.....	ERROR! BOOKMARK NOT DEFINED.
CONFIGURE EMAIL ALERTS TO NOTIFY CHANGE IN STATE	ERROR! BOOKMARK NOT DEFINED.
28. Configuring IP conflict alerts.....	Error! Bookmark not defined.
ADD ACTIVE DIRECTORY DOMAINS	ERROR! BOOKMARK NOT DEFINED.
AUTO-PUBLISHING THE SCANNING RESULTS	ERROR! BOOKMARK NOT DEFINED.
29. Schedule scanning of switches.....	Error! Bookmark not defined.
ADDING CUSTOM COLUMNS TO THE SWITCH PORT MAPPER	ERROR! BOOKMARK NOT DEFINED.
30. Import switch port details	Error! Bookmark not defined.
31. Adding Credentials in OpUtils	Error! Bookmark not defined.
TYPES OF CREDENTIALS SUPPORTED BY OPUTILS:.....	ERROR! BOOKMARK NOT DEFINED.
32. Adding switches for mapping	Error! Bookmark not defined.
ADDING SWITCHES MANUALLY.....	ERROR! BOOKMARK NOT DEFINED.
IMPORTING SWITCH INPUTS FROM A CSV FILE	ERROR! BOOKMARK NOT DEFINED.
33. Discovering switches by scanning IP address range.....	Error! Bookmark not defined.
34. Schedule Scanning of Switches	Error! Bookmark not defined.
35.Configuring Alerts in Switch Port Mapper.....	Error! Bookmark not defined.
SWITCH PORT MAPPER SETTINGS.....	ERROR! BOOKMARK NOT DEFINED.
GENERAL SETTINGS	ERROR! BOOKMARK NOT DEFINED.
PUBLISH MAPPING RESULTS	ERROR! BOOKMARK NOT DEFINED.
CONFIGURE EMAIL ALERTS TO NOTIFY PORT STATE CHANGES	ERROR! BOOKMARK NOT DEFINED.
35. Rogue Detection Tool	Error! Bookmark not defined.
CONFIGURING ROGUE DETECTION TOOL	ERROR! BOOKMARK NOT DEFINED.
37.Discovered Devices	Error! Bookmark not defined.
TRUSTED DEVICES	ERROR! BOOKMARK NOT DEFINED.
TO MARK A DEVICE AS TRUSTED.....	ERROR! BOOKMARK NOT DEFINED.
TO AUTOMATICALLY MARK DEVICES AS TRUSTED.....	ERROR! BOOKMARK NOT DEFINED.
GUEST DEVICES	ERROR! BOOKMARK NOT DEFINED.
TO ALLOW DEVICES FOR A TEMPORARY PERIOD.....	ERROR! BOOKMARK NOT DEFINED.
ROGUE DEVICES.....	ERROR! BOOKMARK NOT DEFINED.
TO MARK A DEVICE AS ROGUE	ERROR! BOOKMARK NOT DEFINED.
38. Block / Unblock Switch Ports.....	Error! Bookmark not defined.
TO VIEW THE SWITCH DETAILS	ERROR! BOOKMARK NOT DEFINED.
TO BLOCK/UNBLOCK A SWITCH PORT.....	ERROR! BOOKMARK NOT DEFINED.
CONFIGURE ALERT NOTIFICATIONS	ERROR! BOOKMARK NOT DEFINED.
TO CONFIGURE E-MAIL ALERTS	ERROR! BOOKMARK NOT DEFINED.
39. Generating Reports in OpUtils	Error! Bookmark not defined.

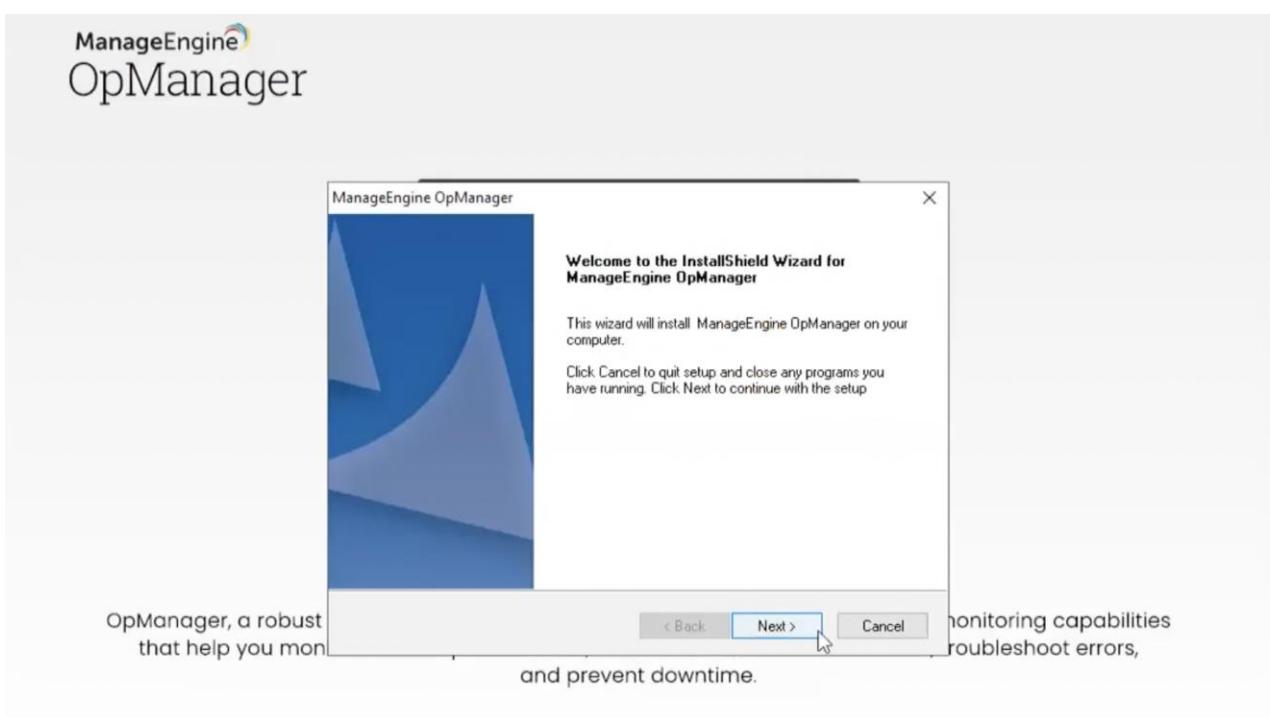
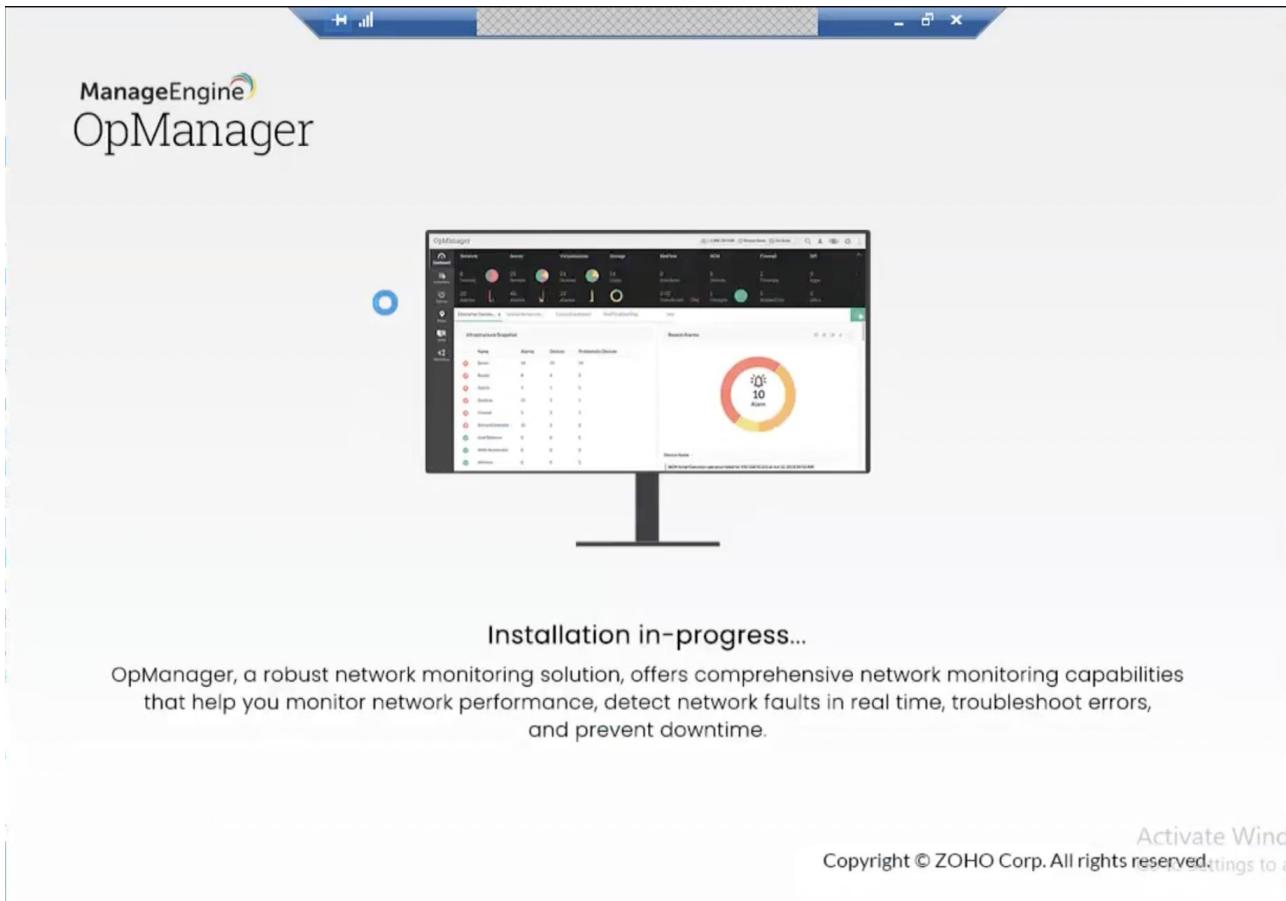
OPUTILS REPORTS.....	ERROR! BOOKMARK NOT DEFINED.
REPORT FEATURES.....	ERROR! BOOKMARK NOT DEFINED.
REPORT TYPES.....	ERROR! BOOKMARK NOT DEFINED.
EXPORT REPORT TO MULTIPLE FORMATS	ERROR! BOOKMARK NOT DEFINED.
40. Configuring WAN Monitor	Error! Bookmark not defined.
41. Configuring Test Parameters and Threshold Template for WAN Monitor	Error! Bookmark not defined.
42. Viewing WAN Monitor Alerts	Error! Bookmark not defined.

OP Manager

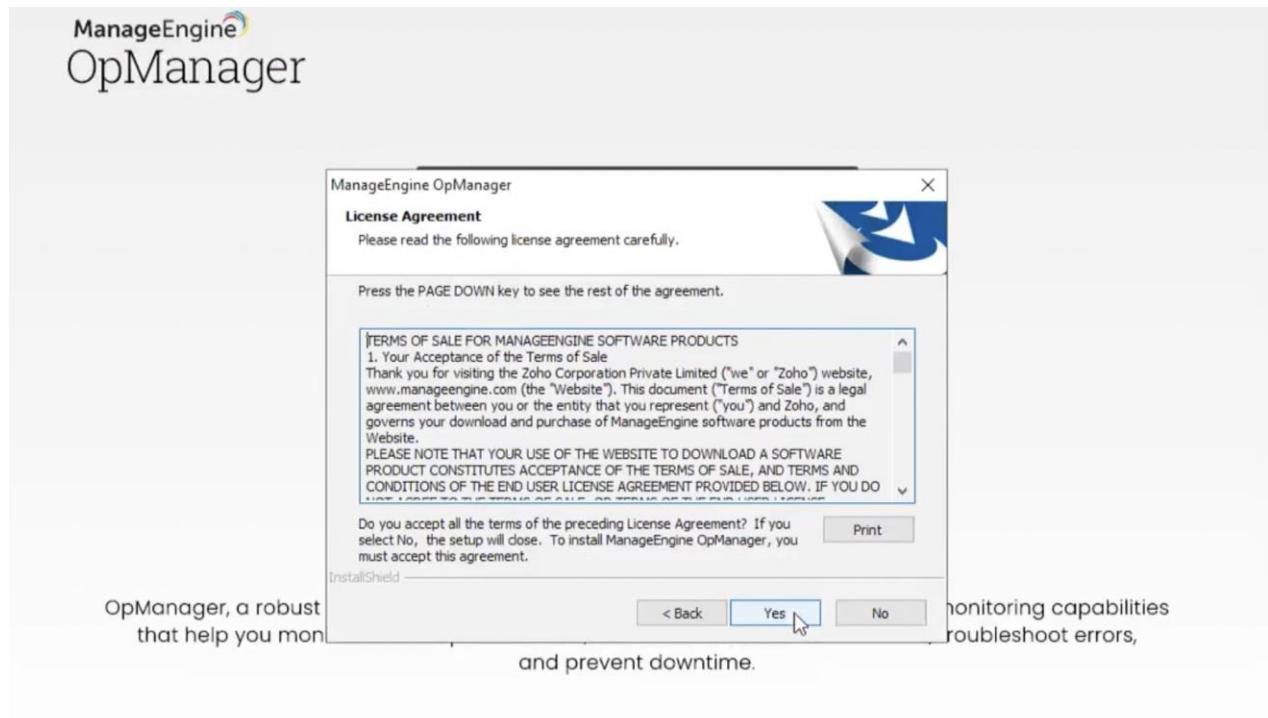
1. Installation of the OP Manager.

Navigate to the application file and click on it.

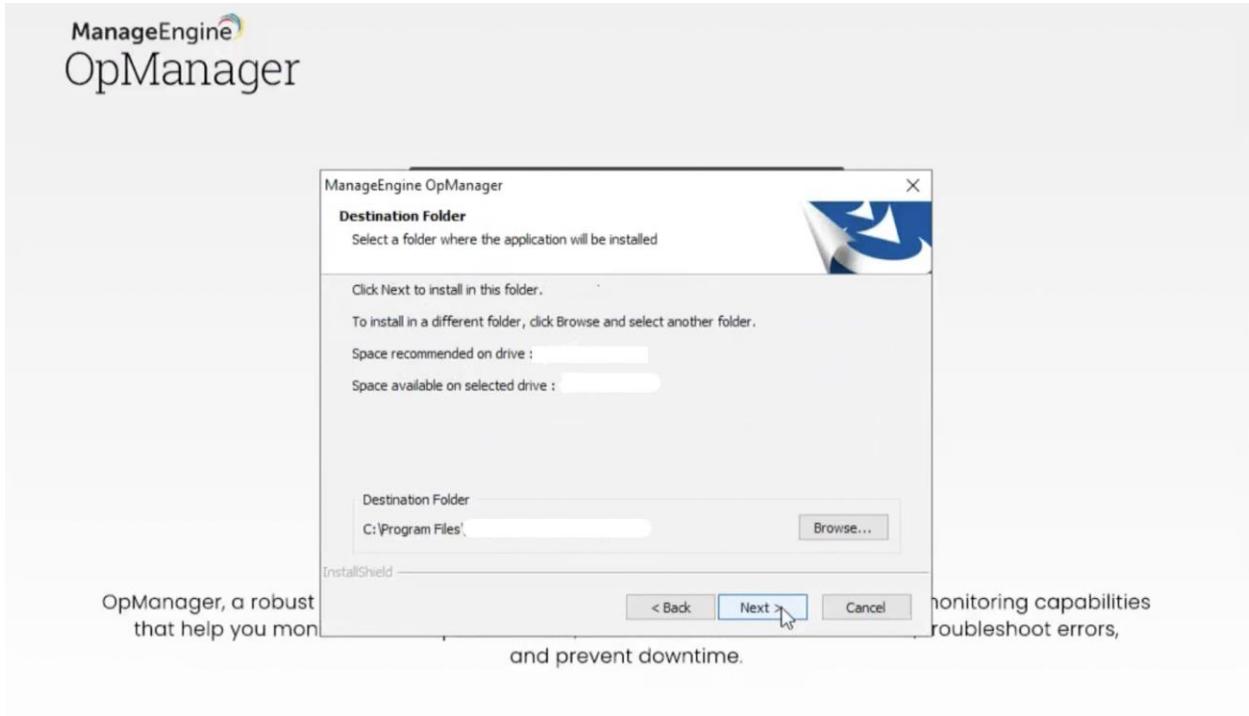




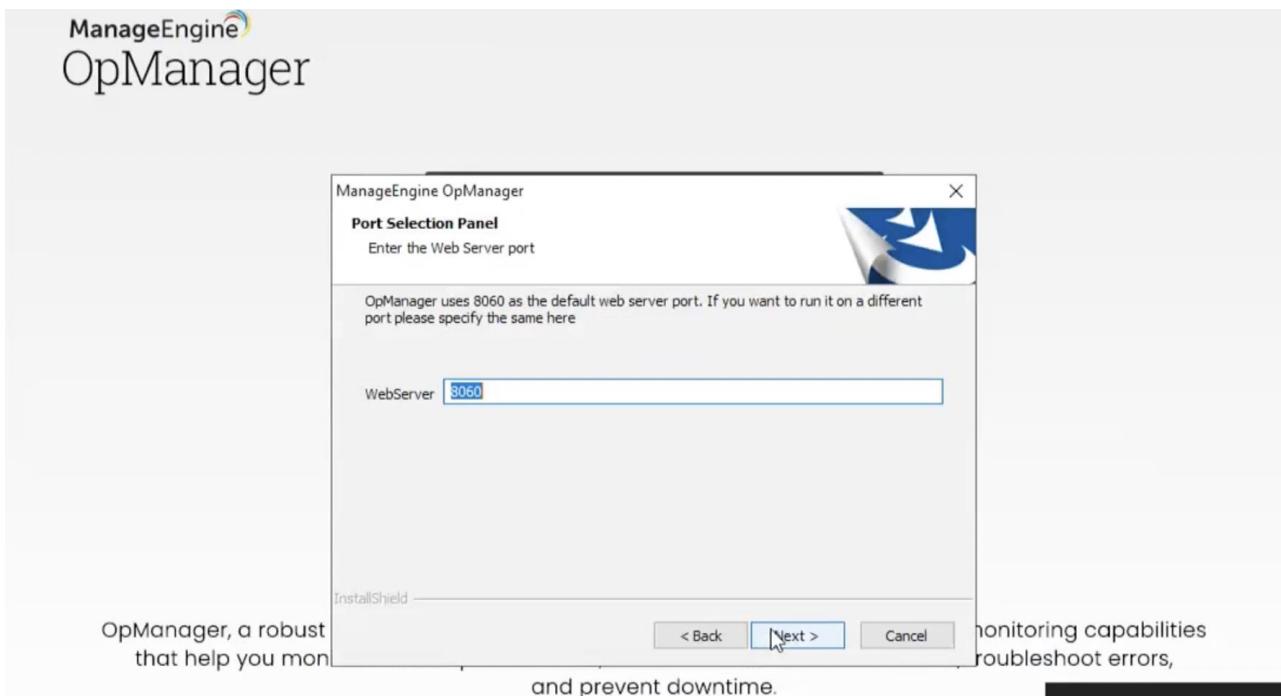
Click 'Next' to begin the installation process. Go through the license agreement and click 'Yes' to proceed to the next step.



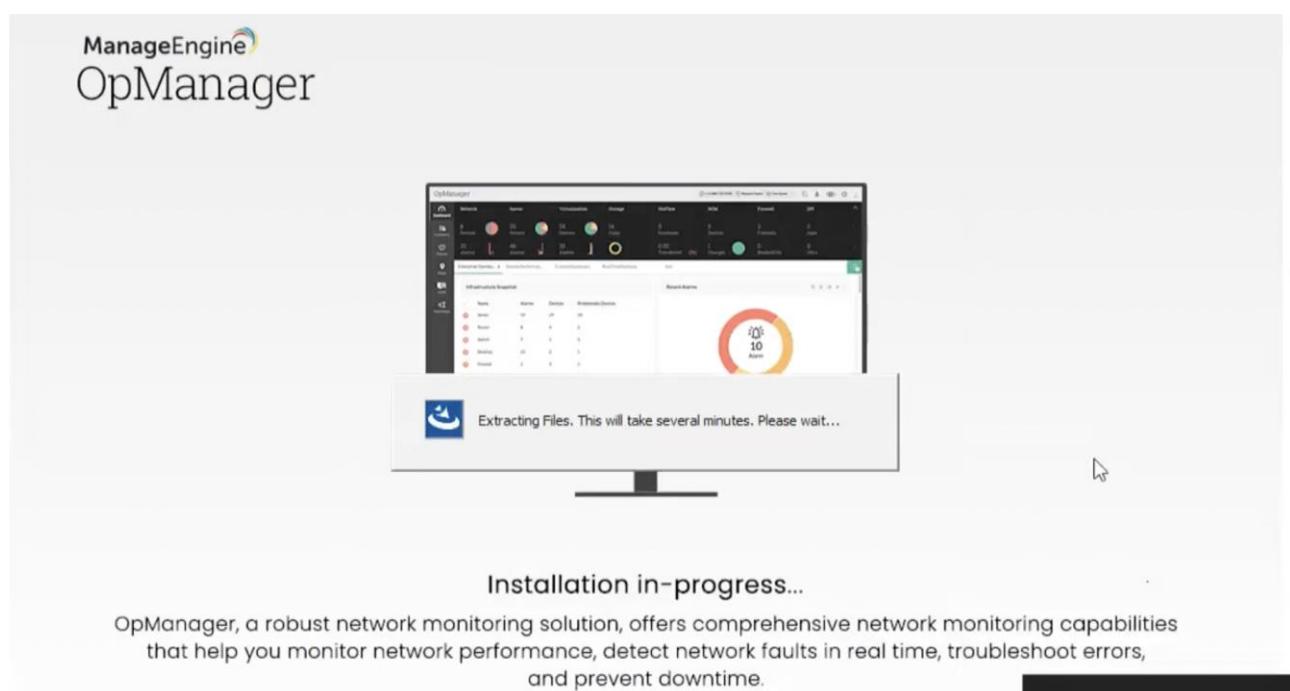
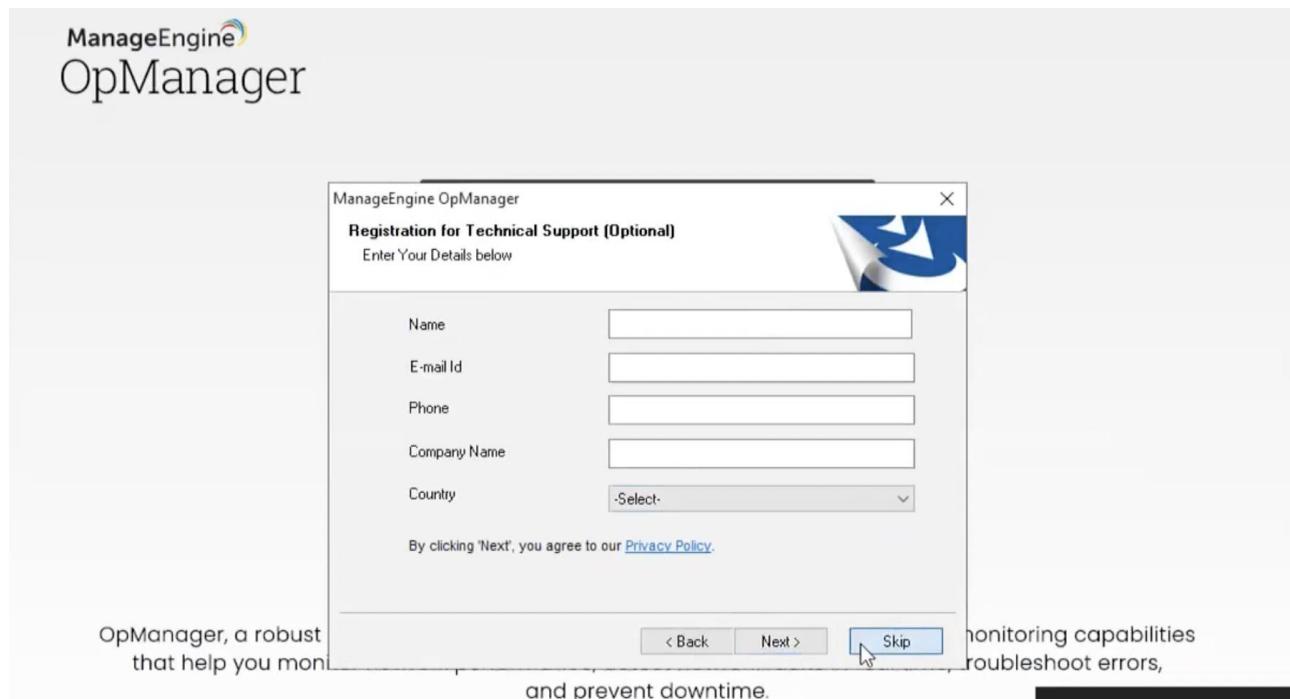
In the subsequent steps of the wizard, select the directory to install OpManager. Proceed to the next step.



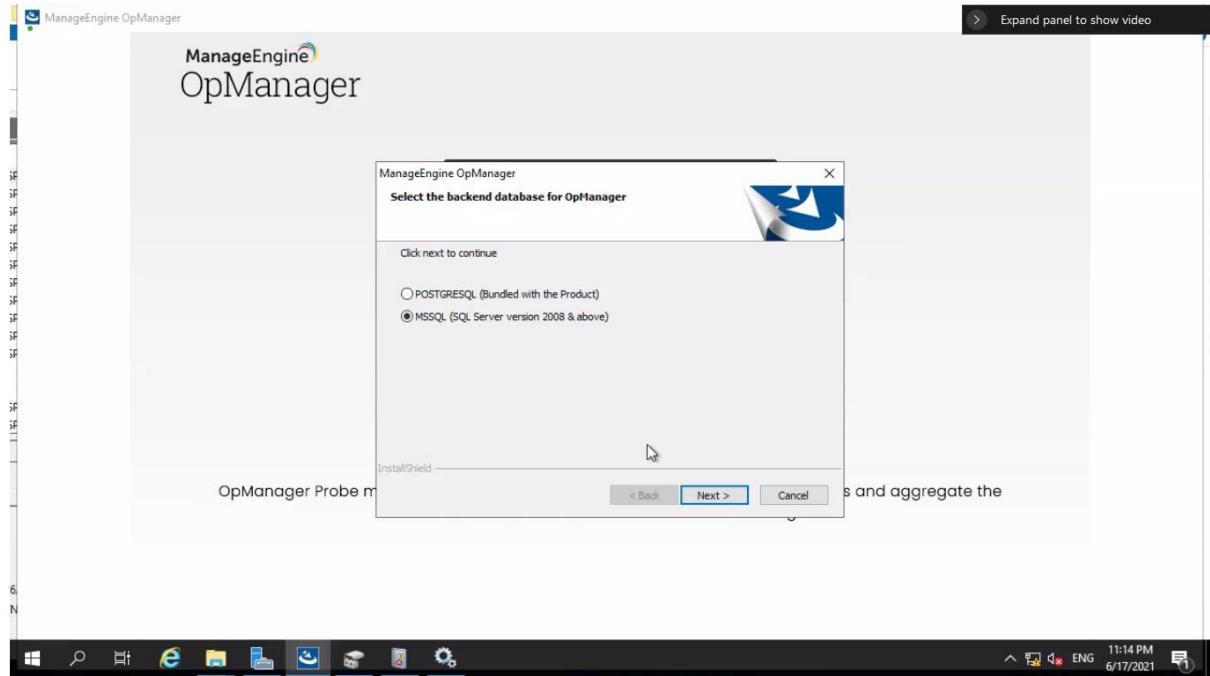
Specify the port number to run OpManager Web Server (OpManager uses 8060 as the default web server port) and click 'Next'.



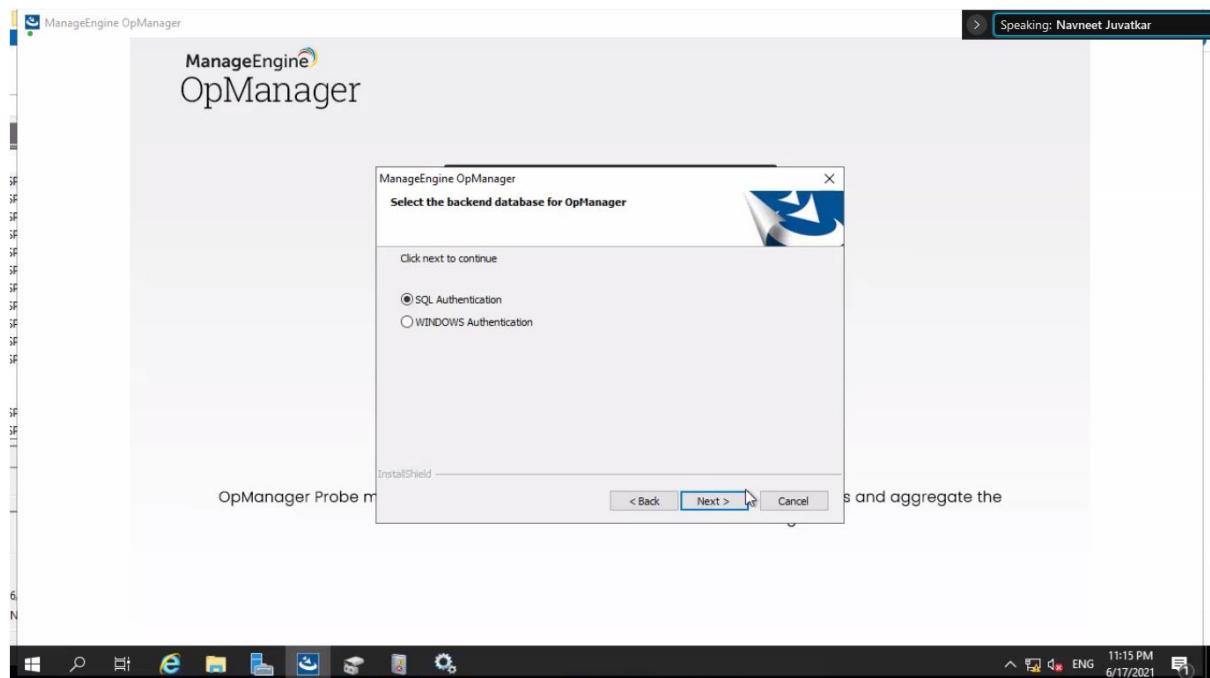
Register for technical support by providing your contact information such as Name, E-mail ID, etc., and click 'Next'. (It is Optional if you not required you can skip this)



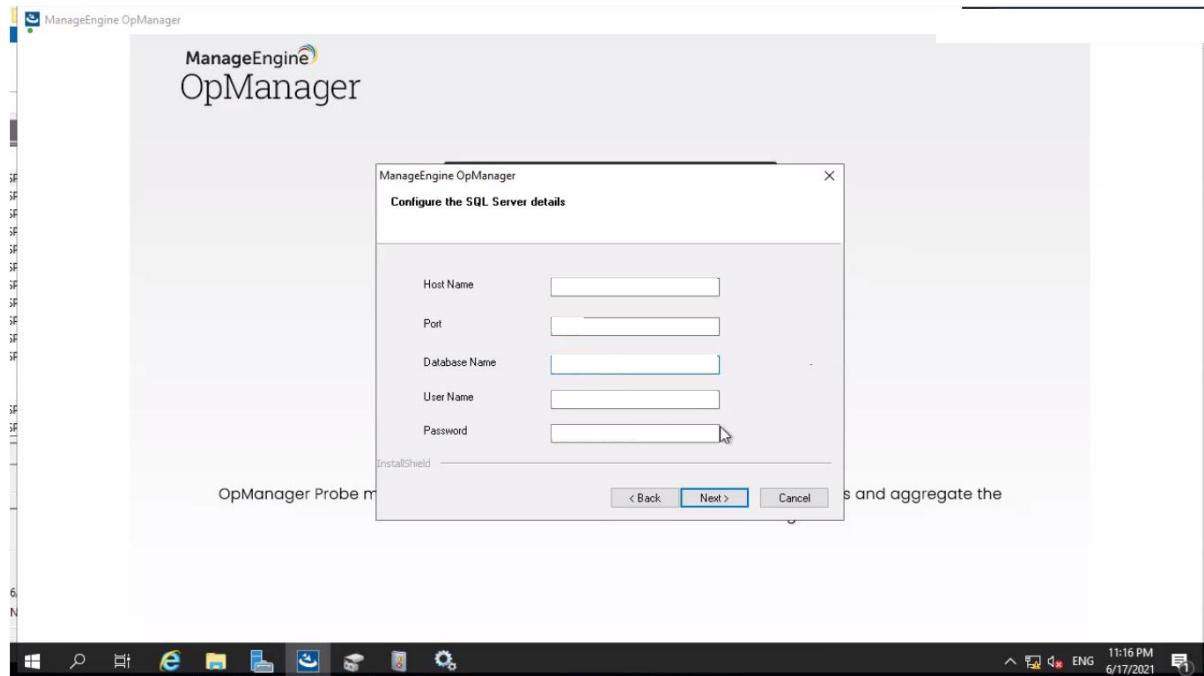
By default, OpManager comes bundled with PostgreSQL. However, OpManager supports both, PostgreSQL and MSSQL databases. Select the required database and click 'Next'.



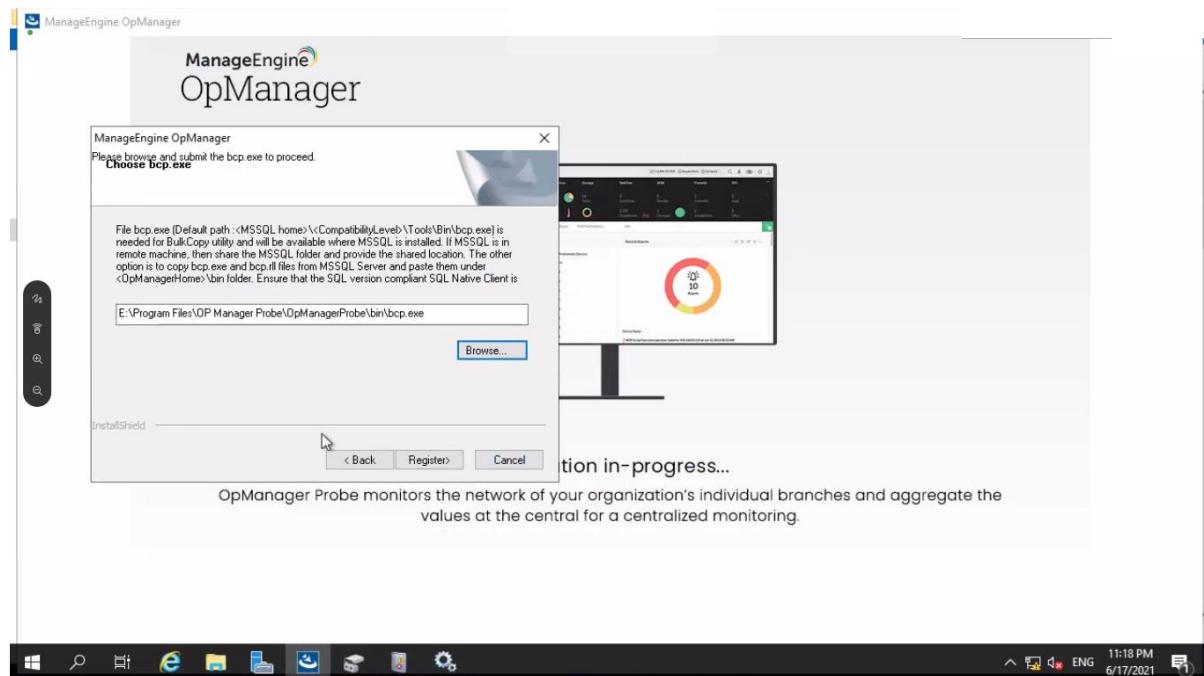
Select correct authentication.



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

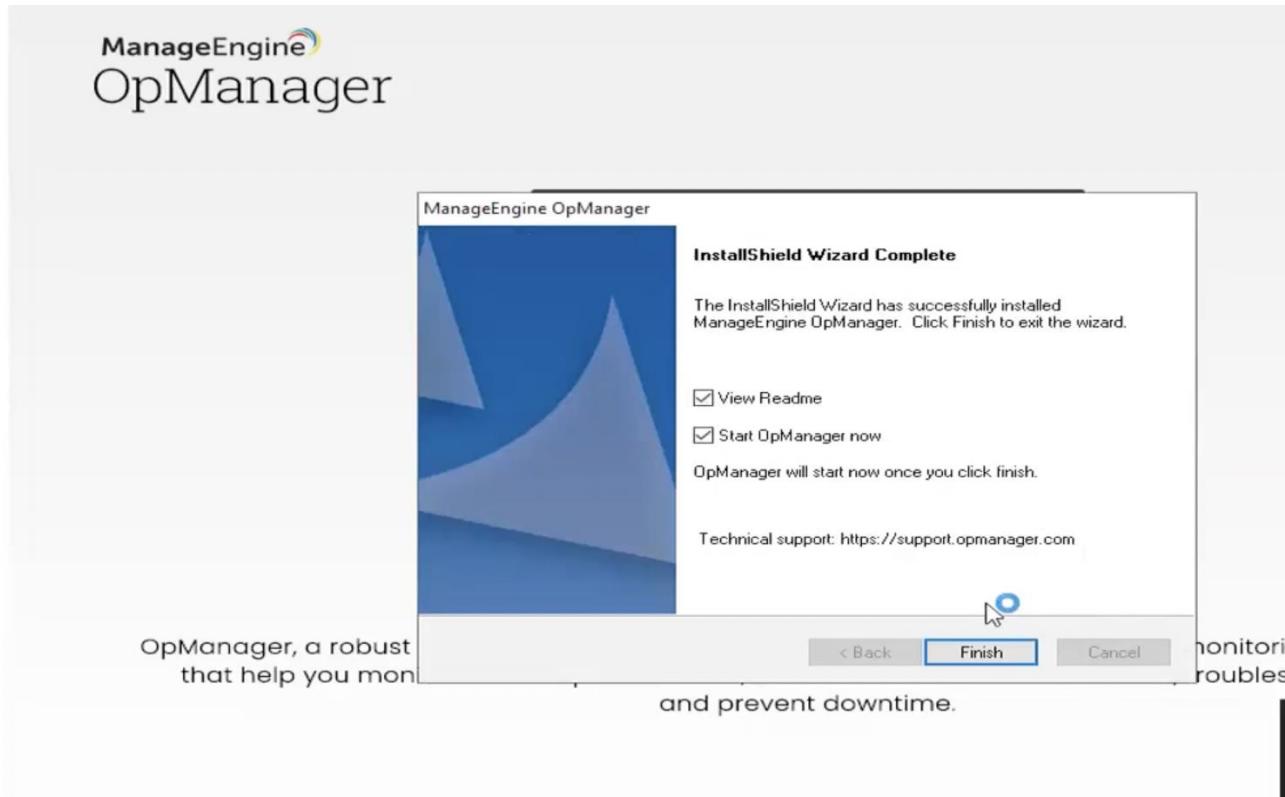


Browse the .bcp file and register.



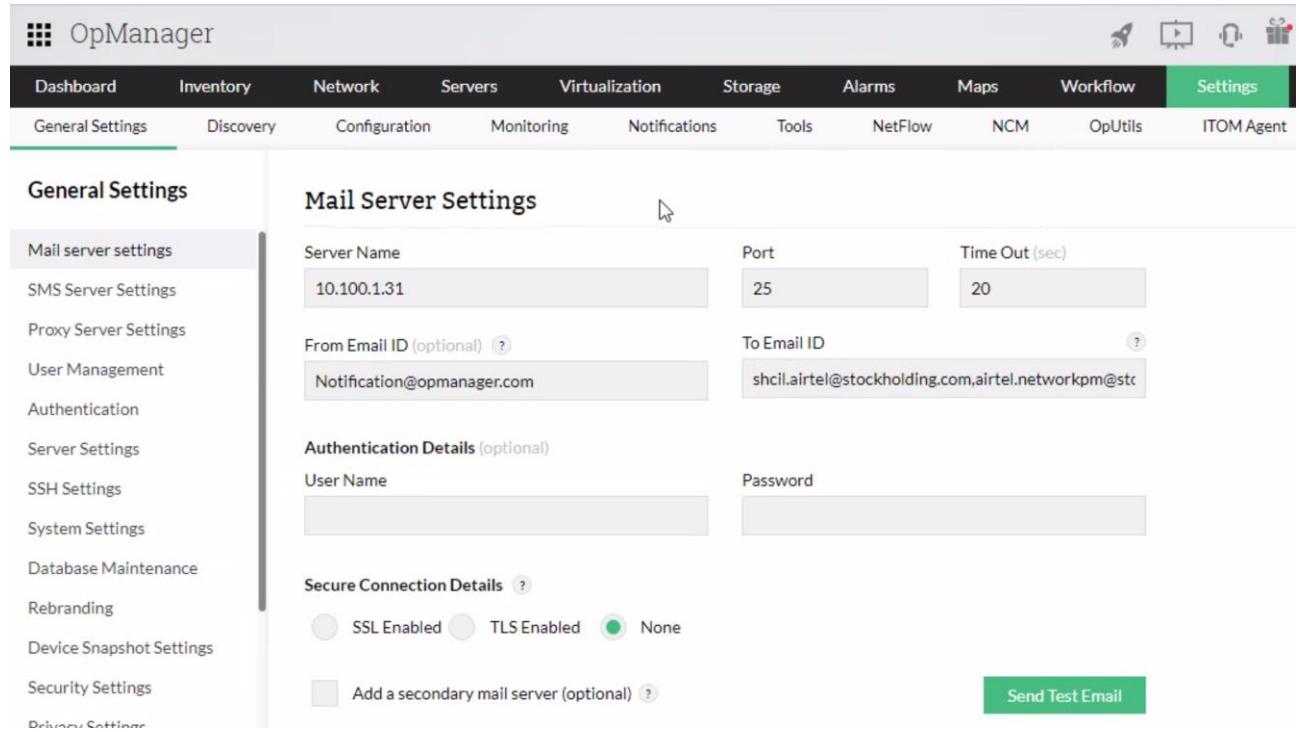
Enter correct details as central url, Probe name, contact name and mail id and installation key.

Click Finish.



2. Configure mail server settings.

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

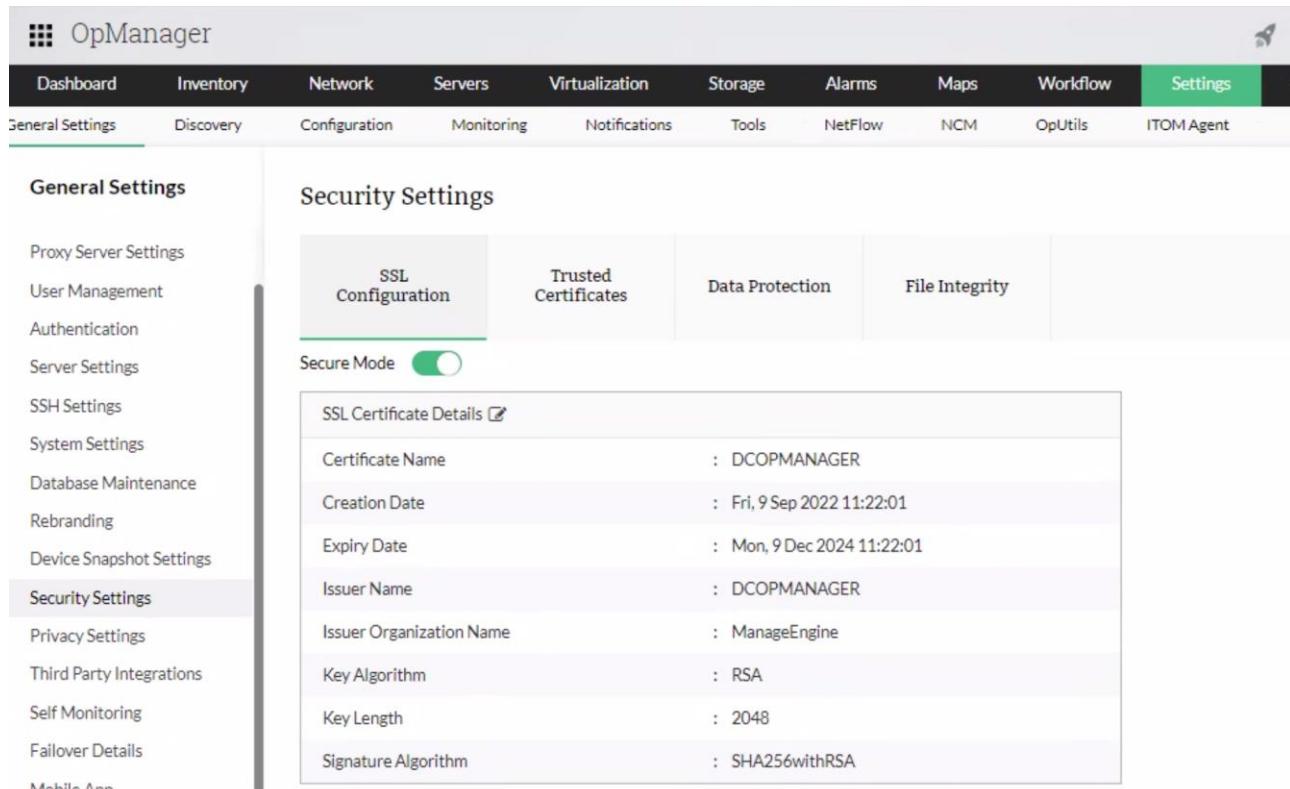


The screenshot shows the 'General Settings' section of the OpManager interface. On the left sidebar, 'Mail server settings' is selected. The main area displays 'Mail Server Settings' with fields for 'Server Name' (10.100.1.31), 'Port' (25), 'Time Out (sec)' (20), 'From Email ID (optional)' (Notification@opmanager.com), and 'To Email ID' (shcil.airtel@stockholding.com,airtel.networkpm@stc). Below these are sections for 'Authentication Details (optional)' (User Name and Password fields) and 'Secure Connection Details' (SSL Enabled, TLS Enabled, None radio buttons). A checkbox for 'Add a secondary mail server (optional)' is present, and a green 'Send Test Email' button is at the bottom right.

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.



The screenshot shows the OpManager interface with the 'Settings' tab selected. Under 'General Settings', 'Security Settings' is highlighted. On the right, the 'SSL Configuration' tab is active, displaying SSL Certificate Details:

SSL Certificate Details	
Certificate Name	: DCOPMANAGER
Creation Date	: Fri, 9 Sep 2022 11:22:01
Expiry Date	: Mon, 9 Dec 2024 11:22:01
Issuer Name	: DCOPMANAGER
Issuer Organization Name	: ManageEngine
Key Algorithm	: RSA
Key Length	: 2048
Signature Algorithm	: SHA256withRSA

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

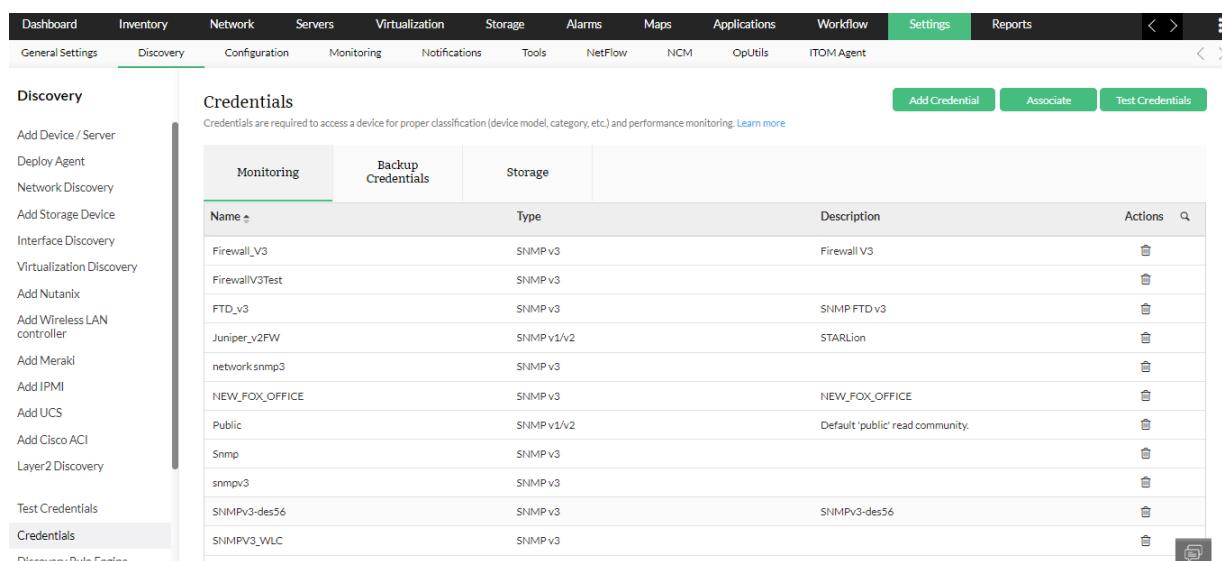
WMI/Windows - Windows

Telnet/SSH - Linux

Vmware - Virtual Machine , V center root access

Citrix - Xen Servers

UCS - Cisco UCS



Name	Type	Description	Actions
Firewall_V3	SNMP v3	Firewall V3	
FirewallV3Test	SNMP v3		
FTD_v3	SNMP v3	SNMP FTD v3	
Juniper_v2FW	SNMP v1/v2	STARLion	
network_snmp3	SNMP v3		
NEW_FOX_OFFICE	SNMP v3	NEW_FOX_OFFICE	
Public	SNMP v1/v2	Default 'public' read community.	
Snmp	SNMP v3		
snmpv3	SNMP v3		
SNMPv3-des56	SNMP v3	SNMPv3-des56	
SNMPV3_WLC	SNMP v3		

How to add a new credential in OpManager?

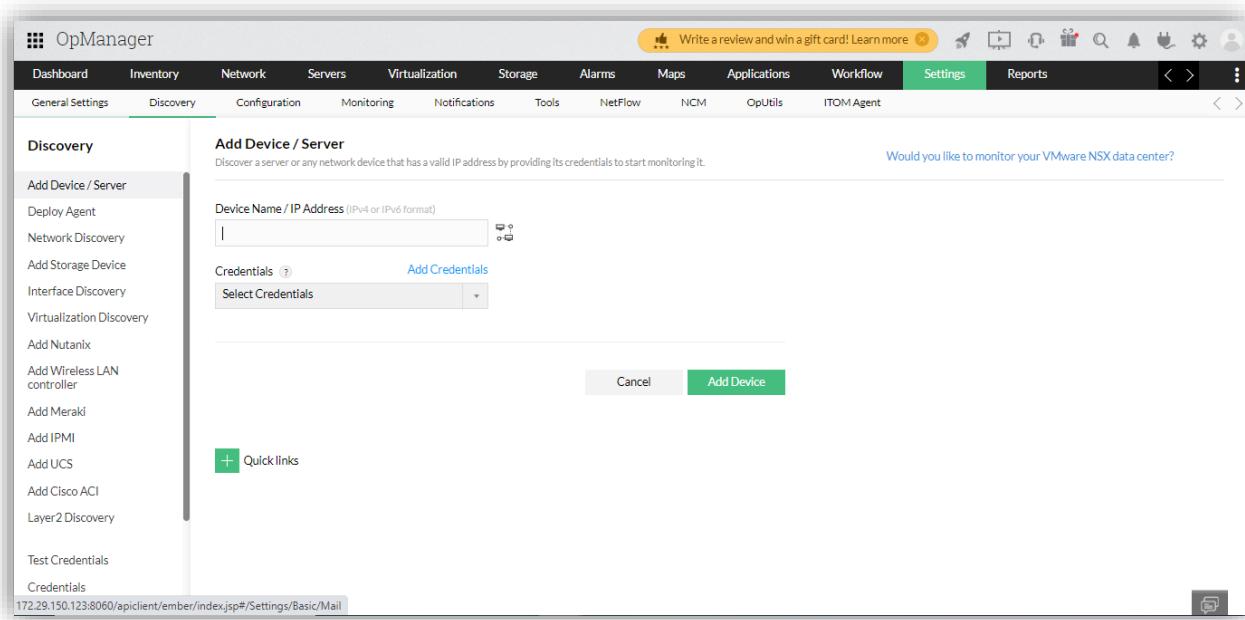
1. Go to **Settings → Discovery → Device Credentials**
2. Click Add Credential
3. Select the required credential category & credential type.
4. Configure the following parameters and click Save to add the credentials

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



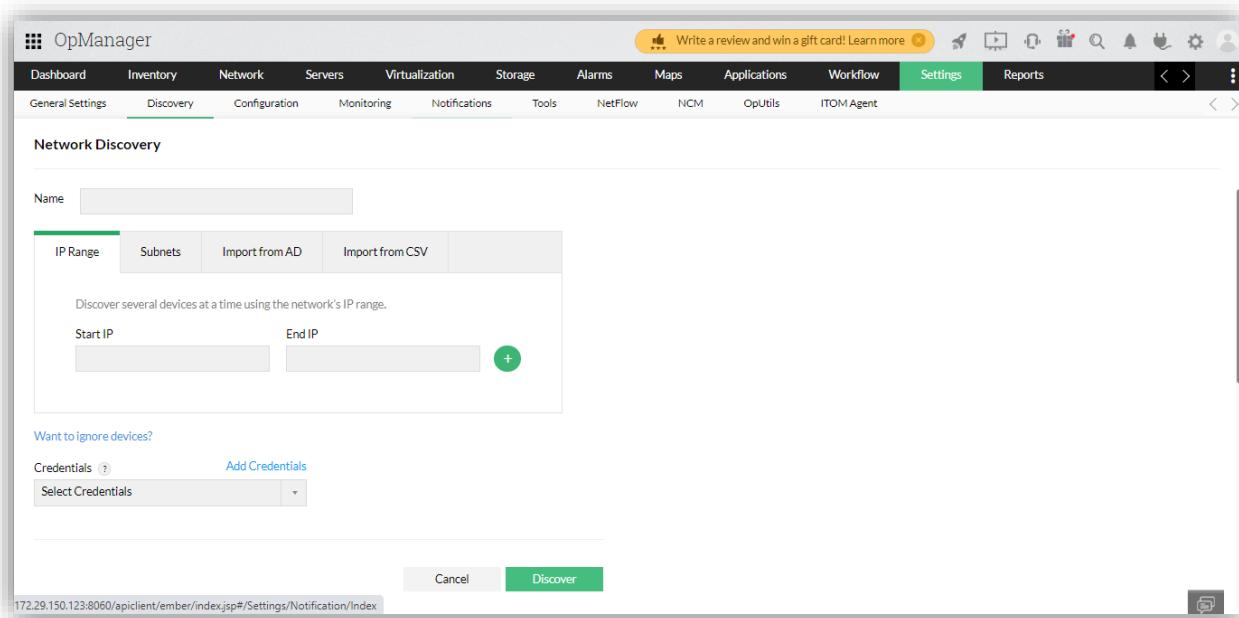
The screenshot shows the OpManager web interface. The top navigation bar includes links for Dashboard, Inventory, Network, Servers, Virtualization, Storage, Alarms, Maps, Applications, Workflow, Settings (which is selected), Reports, and several icons. On the left, a sidebar titled 'Discovery' lists various options: Add Device / Server, Deploy Agent, Network Discovery, Add Storage Device, Interface Discovery, Virtualization Discovery, Add Nutanix, Add Wireless LAN controller, Add Meraki, Add IPMI, Add UCS, Add Cisco ACI, Layer2 Discovery, Test Credentials, and Credentials. Below this is a URL bar with the address 172.29.150.123:8060/apiclient/ember/index.jsp#/Settings/Basic/Mail. The main content area is titled 'Add Device / Server' and contains a sub-section 'Add Device / Server'. It features a text input field for 'Device Name / IP Address (IPv4 or IPv6 format)' with a placeholder 'Enter IP Address' and a 'Ping' button. Below it is a 'Credentials' dropdown menu with 'Select Credentials' and an 'Add Credentials' link. At the bottom are 'Cancel' and 'Add Device' buttons. A 'Quick links' section is also visible.

2. Bulk discovery of devices:

Go to Settings → Discovery → Network Discovery → New Discovery

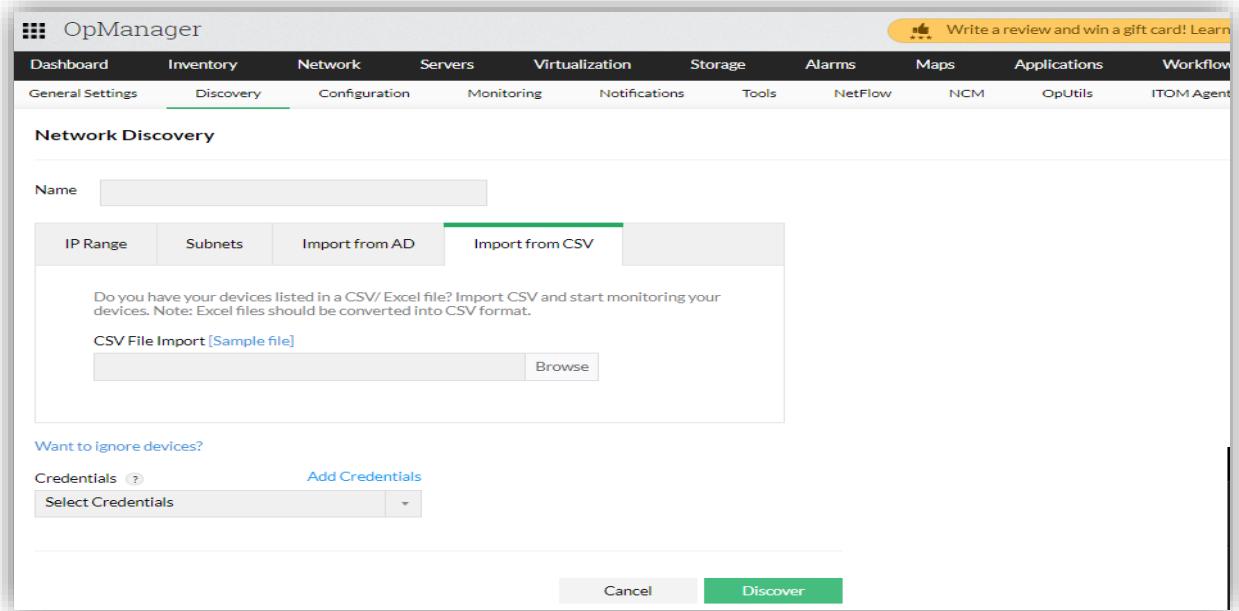
There are four methods to add device into the product

1. Discovering devices from an IP Range



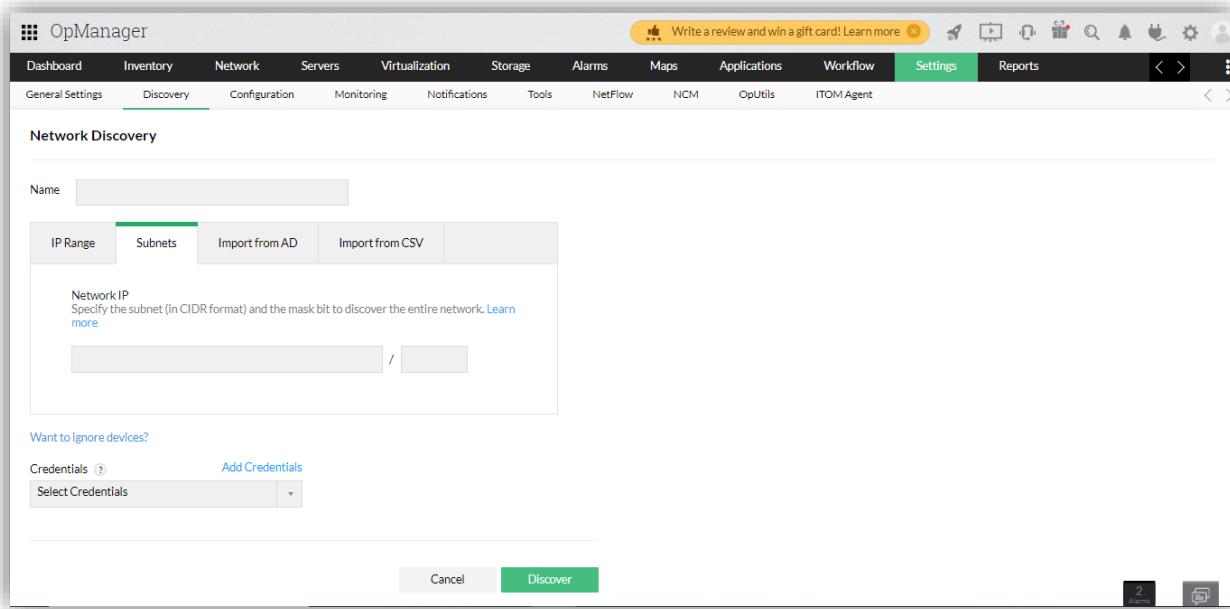
The screenshot shows the OpManager Network Discovery interface. The top navigation bar includes tabs for Dashboard, Inventory, Network, Servers, Virtualization, Storage, Alarms, Maps, Applications, Workflow, Settings (which is selected), and Reports. Below the tabs, there are sub-tabs: General Settings, Discovery, Configuration, Monitoring, Notifications, Tools, NetFlow, NCM, OpUtils, and ITOM Agent. The main content area is titled "Network Discovery" and contains a "Name" input field. Below it is a tab bar with "IP Range" (selected), Subnets, Import from AD, and Import from CSV. A sub-section titled "Discover several devices at a time using the network's IP range." includes "Start IP" and "End IP" input fields and a "+" button. At the bottom of the interface are "Cancel" and "Discover" buttons.

2. Discovering devices by CSV import



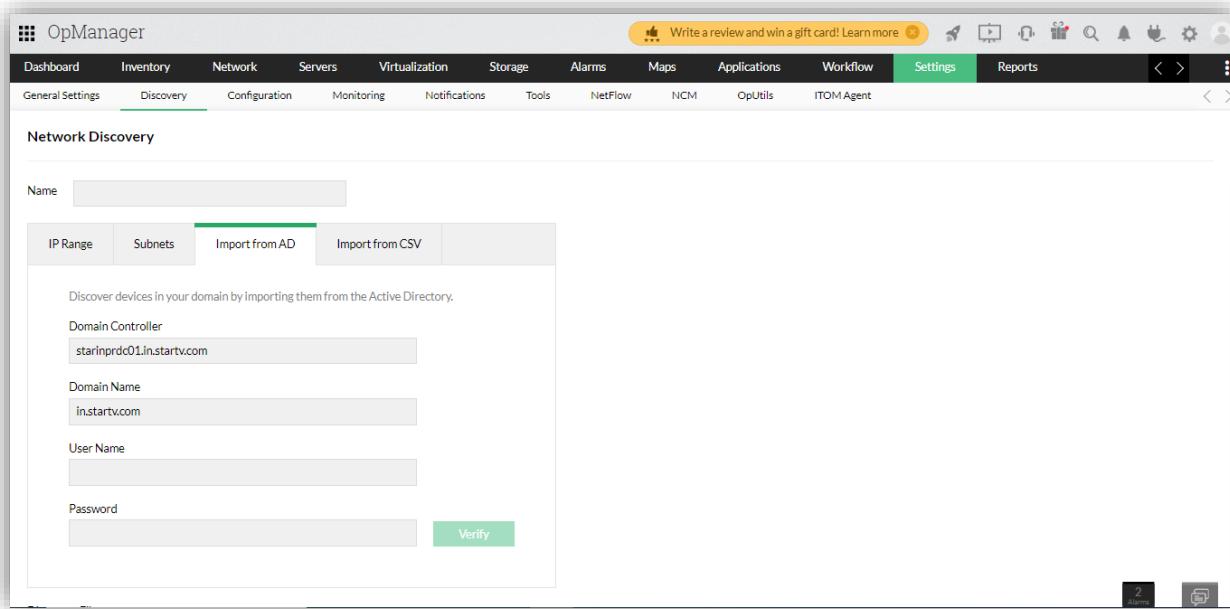
This screenshot shows the same OpManager Network Discovery interface, but the "Import from CSV" tab is now selected in the top navigation bar. The sub-tabs remain the same: General Settings, Discovery, Configuration, Monitoring, Notifications, Tools, NetFlow, NCM, OpUtils, and ITOM Agent. The main content area is titled "Network Discovery" and contains a "Name" input field. Below it is a tab bar with IP Range, Subnets, Import from AD, and Import from CSV (selected). A sub-section titled "Do you have your devices listed in a CSV/ Excel file? Import CSV and start monitoring your devices. Note: Excel files should be converted into CSV format." includes a "CSV File Import [Sample file]" input field and a "Browse" button. At the bottom of the interface are "Cancel" and "Discover" buttons.

3. Discovering a complete network



The screenshot shows the OpManager interface with the 'Discovery' tab selected in the top navigation bar. Under the 'Network Discovery' section, the 'IP Range' tab is active. A text input field for 'Network IP' is present, with a placeholder: 'Specify the subnet (in CIDR format) and the mask bit to discover the entire network.' Below this is a 'Name' input field. At the bottom, there are 'Discover' and 'Cancel' buttons, along with a status bar indicating '2 Alarms'.

4. Import devices from Active Directory



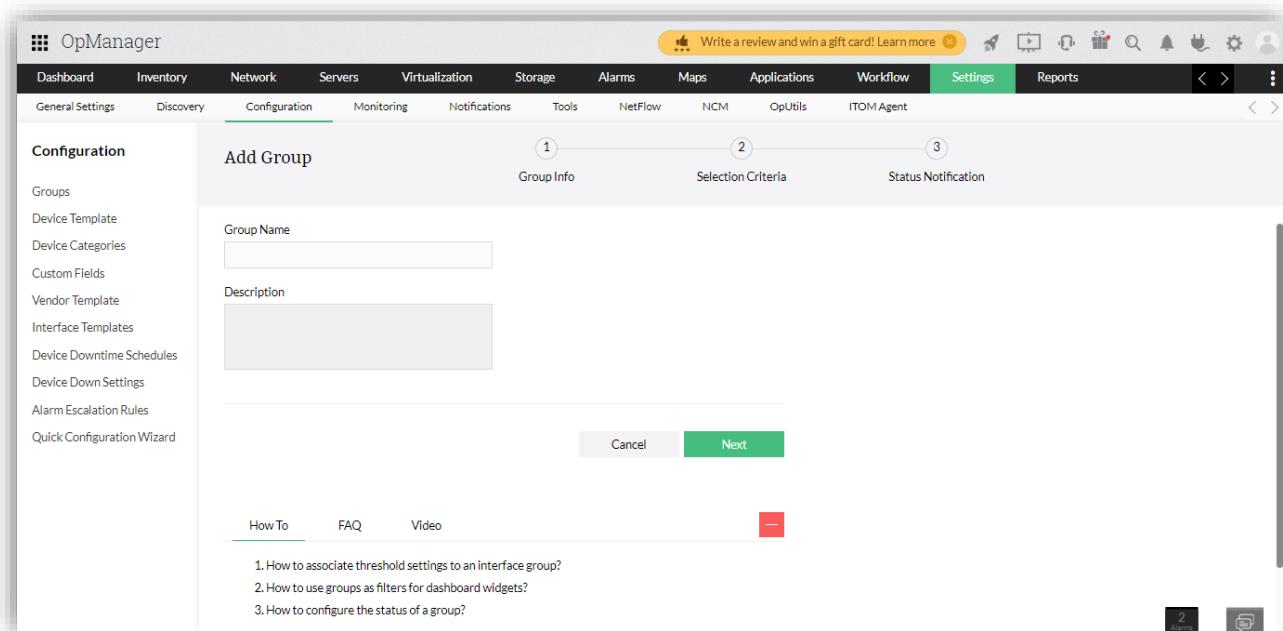
The screenshot shows the OpManager interface with the 'Discovery' tab selected in the top navigation bar. Under the 'Network Discovery' section, the 'Import from AD' tab is active. It displays fields for 'Domain Controller' (starnprdc01.instartv.com), 'Domain Name' (in.startv.com), 'User Name', and 'Password'. A 'Verify' button is located at the bottom right of this group. The status bar at the bottom indicates '2 Alarms'.

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

- 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 '+' icon.
- Add multiple criteria if needed, along with the logical operation 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 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 (?)	 
►  Critical Devices(114)	Group Name	Status	Description	Members Count	Member Type	Availability (%) 
►  ALL Core Switches(11)	<input type="checkbox"/> WAN Devices	 Clear	ALL Routers	18	Device	100 
►  Managed Interfaces(1572)	<input type="checkbox"/> RnF	 Critical	No Description	15	Device	100 
►  Access Switches(41)	<input type="checkbox"/> ALL Core Switches	 Trouble	ALL Core Switches	11	Device	100 
►  All Routers(37)	<input type="checkbox"/> All Security Devices	 Critical	No Description	48	Device	100 
►  All Security Devices(48)	<input type="checkbox"/> Access Switches	 Trouble	Access Switches	41	Device	100 
►  WAN Devices(18)	<input type="checkbox"/> All Routers	 Trouble	No Description	37	Device	100 
►  RnF(15)	<input type="checkbox"/> Managed Interfaces	 Trouble	No Description	1572	Interface	0 
►  All Switches(110)	<input type="checkbox"/> Critical Devices	 Critical	No Description	114	Device	99.5 
	<input type="checkbox"/> 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.

Device Summary

- Status: 17.22.159.21
- Type: Cisco Nexus 9332PQ
- Monitoring Interval: 5 min(s)

Availability Timeline (Today)

Performance Metrics:

- Availability: 100 %
- Packet Loss: 0 %
- Response Time: 001 ms

Recent Alarms: Currently there are no open Alarms.

Custom Dials: [No Data]

VLANs: [No Data]

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

Protocol	Interval (mins)	Threshold	Last Polled at	Value	Units	Actions
SNMP	5	Not Enabled	9 Mar 2023 03:26:00 PM IST	0	%	Edit Delete View
SNMP	5	Not Enabled	9 Mar 2023 03:25:59 PM IST	79	%	Edit Delete View

Actions: [View 1 - 2 of 2](#)

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

The screenshot shows the 'Performance Monitors' configuration page. The main interface has tabs for Summary, Interfaces, NetFlow, and NCM. Below these are sections for 'Performance Monitors' (0/2) and 'Script Monitors' (0/0). A table lists monitors by name, protocol (SNMP), interval (5 mins), and threshold status (Not Enabled). A search bar and a help section are also present. A modal window titled 'Performance Monitors' displays a list of available monitors with their descriptions and protocols. The 'Cisco Temperature' monitor is highlighted.

Monitors	Protocol	Description
Buffer Failures	SNMP	... reasons other than insufficient memory. For example, in systems where there are different execution contexts, it may be too expensive to create new buffers when running in certain contexts. In those cases it may be preferable to fail the request.
CardOperstatus	SNMP	1 : not-specified2 : up3 : down4 : standby
Chassis Fan Status	SNMP	Chassis Fan Status
Chassis PS1 Status	SNMP	Chassis PS1 Status
Chassis PS2 Status	SNMP	Chassis PS2 Status
Chassis Unit Temperature	SNMP	Display environment monitoring chassis temperature status
Cisco Memory Utilization	SNMP	Monitors the Memory Utilization
Cisco OSPF Neighbour state	SNMP	The state of Open Shortest Path First (OSPF) protocol based relationship with this neighbor. down(1), attempt(2), init(3), twoWay(4), exchangeStart(5), exchange(6), loading(7), full(8)
Cisco Temperature	SNMP	Monitors temperature at the testpoint maintained by the environmental monitor

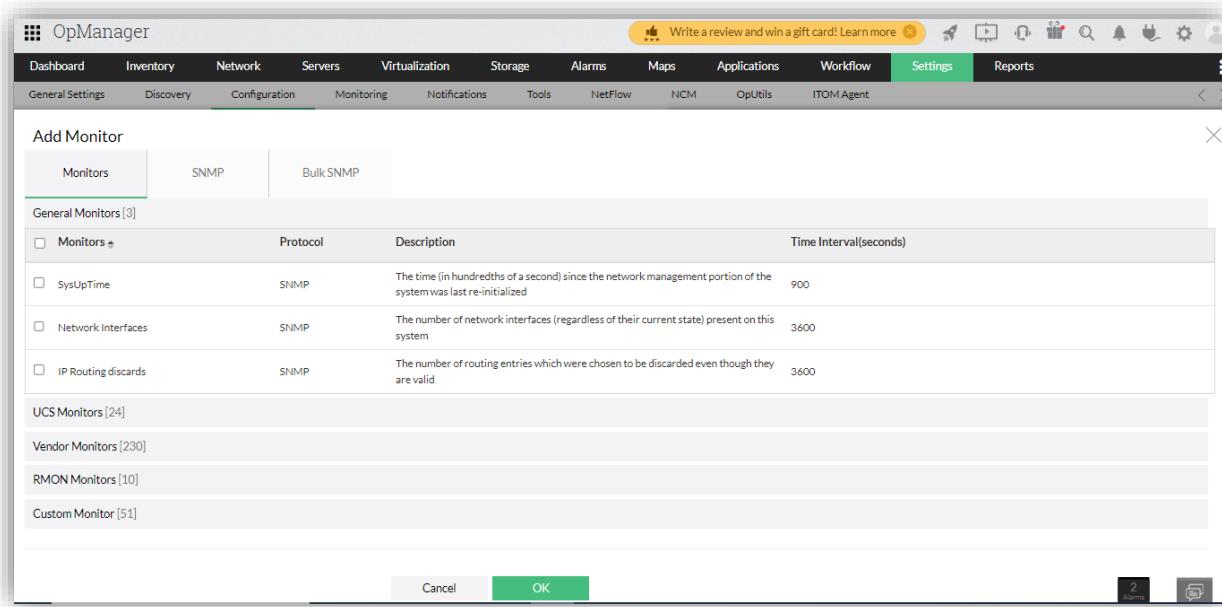
- Click on "Add" to apply the changes.

2. From Device Templates:

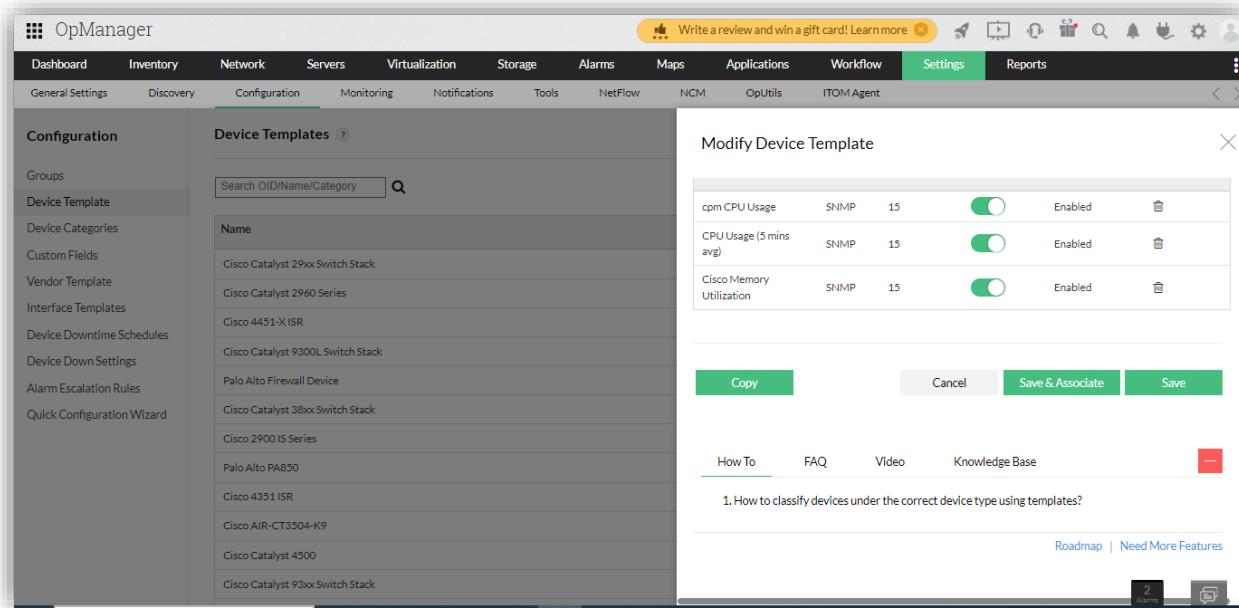
- Navigate to Settings -> Configuration -> Device Template.
- Open a template and click on the "Add" button that is found at the right of the "Associated Monitors" section.

The screenshot shows the 'Device Templates' configuration in OpManager. The left sidebar includes sections for General Settings, Discovery, Configuration (selected), Monitoring, Notifications, Tools, NetFlow, NCM, OpUtils, and ITOM Agent. The main area shows a list of device templates: Cisco Catalyst 29xx Switch Stack, Cisco Catalyst 2960 Series, Cisco 4451-X ISR, Cisco Catalyst 9300L Switch Stack, Palo Alto Firewall Device, Cisco Catalyst 38xx Switch Stack, Cisco 2900 IS Series, Palo Alto PA850, Cisco 4351 ISR, Cisco AIR-CT504-K9, Cisco Catalyst 4500, and Cisco Catalyst 93xx Switch Stack. A modal window titled 'Modify Device Template' is open, showing settings for Category (Switch), Availability monitoring interval (5 min(s)), and Device Identifier (IP address). The 'Associated Monitors' section lists three monitors: cpm CPU Usage, CPU Usage (5 mins avg), and Cisco Memory.

Name	Type	Interval	Show Dial	Threshold	Actions
cpm CPU Usage	SNMP	15	Enabled		
CPU Usage (5 mins avg)	SNMP	15	Enabled		
Cisco Memory					



- 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

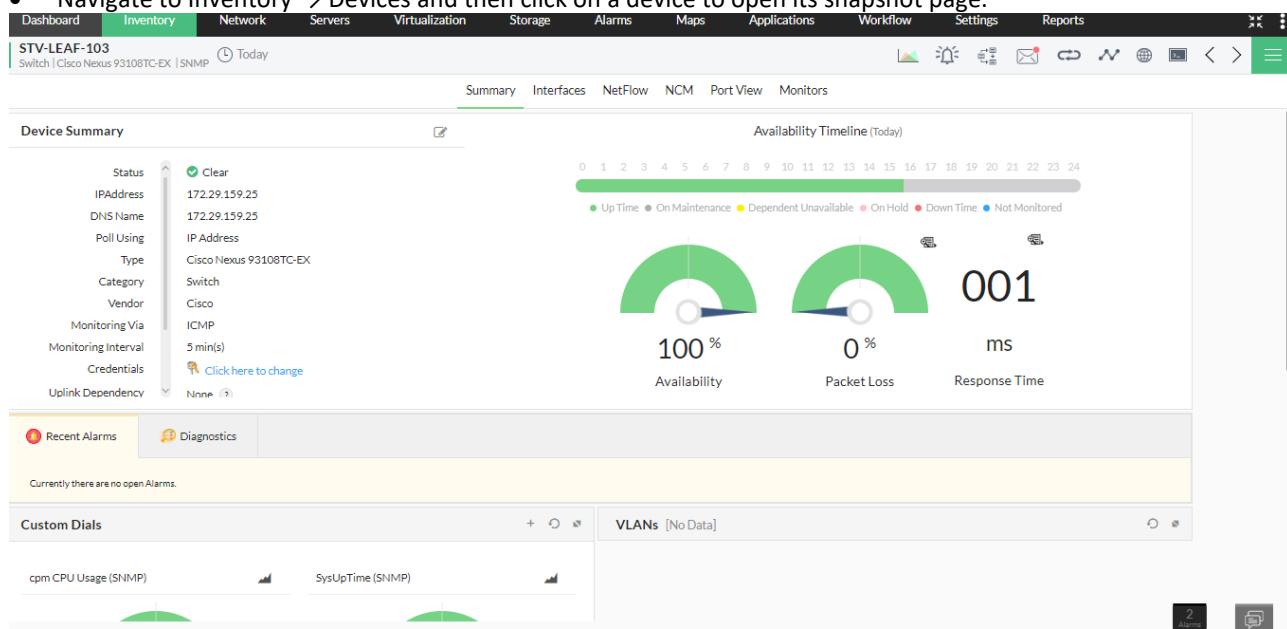
Trouble threshold - medium severity

Critical threshold - high severity

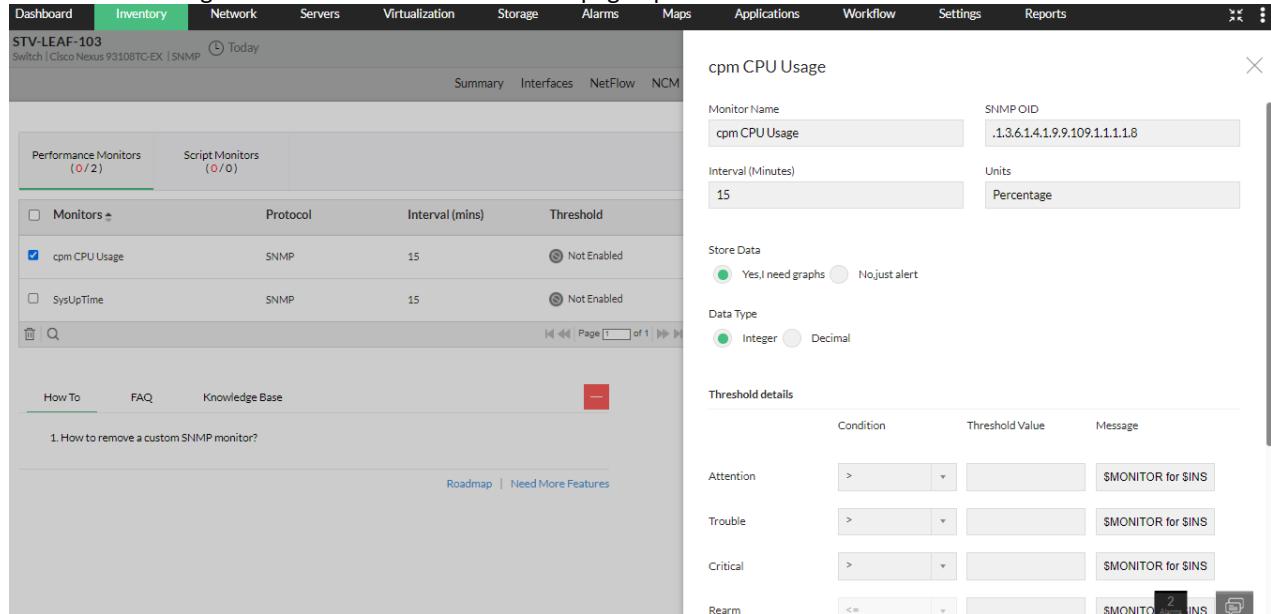
Rearm - to rearm the alert after it has been triggered

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.



cpm CPU Usage

Monitor Name: cpm CPU Usage
SNMP OID: .1.3.6.1.4.19.9.109.1.1.1.8

Interval (Minutes): 15
Units: Percentage

Store Data: Yes, I need graphs
Data Type: Integer

Condition	Threshold Value	Message
Attention	>	\$MONITOR for SINS
Trouble	>	\$MONITOR for SINS
Critical	>	\$MONITOR for SINS
Remail	<=	\$MONITOR for SINS

- 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 Remail Value. Remail 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 Ralarm Value and click on OK

- To save this setup, press Save and press 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.

The screenshot shows the OpManager software interface. The main menu bar includes Dashboard, Inventory, Network, Servers, Virtualization, Storage, Alarms, Maps, Applications, Workflow, Settings (which is selected), Reports, and other system icons. On the left, there's a sidebar with 'Configuration' selected, containing options like Groups, Device Template (which is currently active), Device Categories, Custom Fields, Vendor Template, Interface Templates, Device Downtime Schedules, Device Down Settings, Alarm Escalation Rules, and Quick Configuration Wizard. The central pane displays a list of 'Device Templates' with items such as Cisco Catalyst 29xx Switch Stack, Cisco Catalyst 2960 Series, Cisco 4451-XISR, Cisco Catalyst 9300L Switch Stack, Palo Alto Firewall Device, Cisco Catalyst 38xx Switch Stack, Cisco 2900 I5 Series, Palo Alto PA850, Cisco 4351 ISR, Cisco AIR-CT3504-K9, Cisco Catalyst 4500, and Cisco Catalyst 93xx Switch Stack. A modal dialog box titled 'Add Device Template' is open, prompting for 'Name', 'Vendor Name' (with a 'New' button), 'Category', 'Availability monitoring interval' (set to 15 min(s)), 'Device Identifier', and 'Associated Monitors'. A preview image of a Cisco access point is shown on the right side of the dialog.

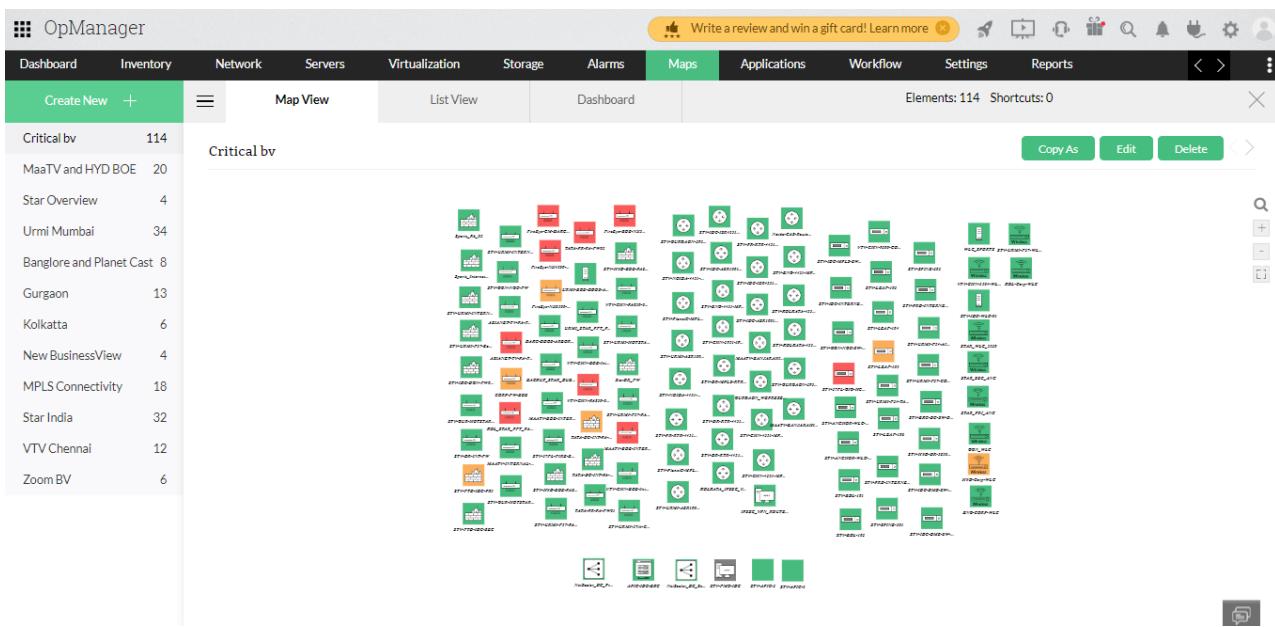
3. Enter the mandatory fields - Device template name, vendor, category, availability monitoring interval and device image.
4. Define a unique device identifier (SysObject ID) received from vendor or by querying the device itself.
5. Click on Save.

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.



Business View	Elements
Critical bv	114
MaaTV and HYD BOE	20
Star Overview	4
Urmil Mumbai	34
Banglore and Planet Cast	8
Gurgaon	13
Kolkatta	6
New BusinessView	4
MPLS Connectivity	18
Star India	32
VTV Chennai	12
Zoom BV	6

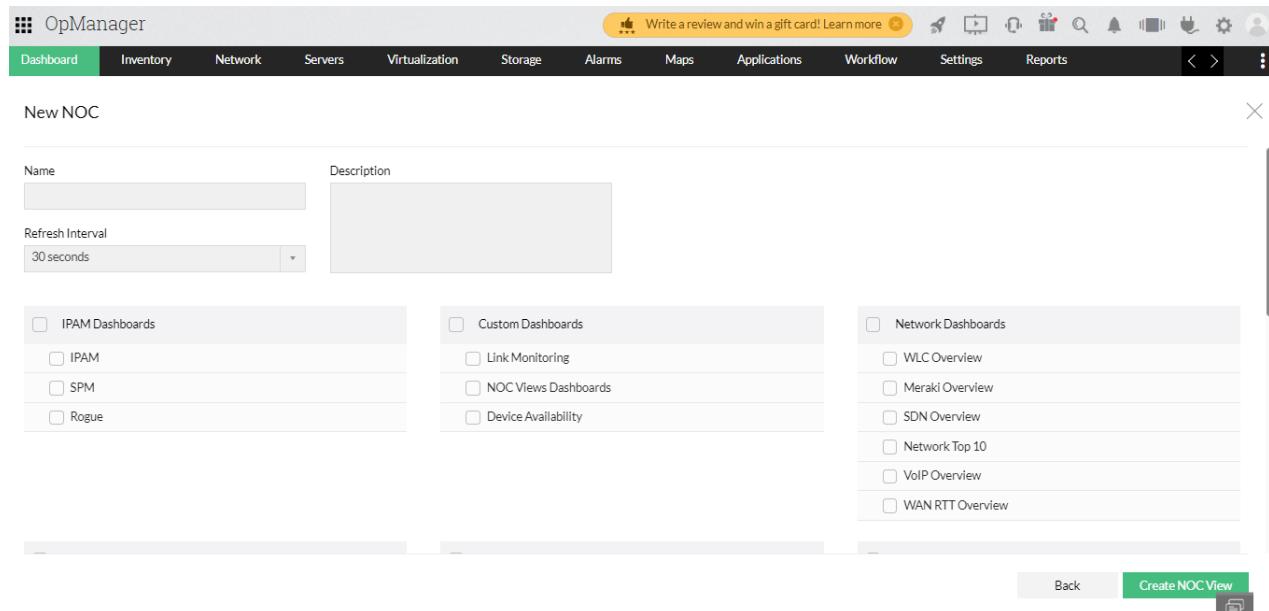
2. From the list of available devices, drag and drop the required devices into the white board individually or add devices in bulk using the Multi select option.
3. Customize the view by changing font type, size or color and edit the background if necessary.
4. Place the selected devices on the Map (background)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



New NOC

Name <input type="text"/>	Description <input type="text"/>	
Refresh Interval 30 seconds		
<input type="checkbox"/> IPAM Dashboards <input type="checkbox"/> IPAM <input type="checkbox"/> SPM <input type="checkbox"/> Rogue	<input type="checkbox"/> Custom Dashboards <input type="checkbox"/> Link Monitoring <input type="checkbox"/> NOC Views Dashboards <input type="checkbox"/> Device Availability	<input type="checkbox"/> Network Dashboards <input type="checkbox"/> WLC Overview <input type="checkbox"/> Meraki Overview <input type="checkbox"/> SDN Overview <input type="checkbox"/> Network Top 10 <input type="checkbox"/> VoIP Overview <input type="checkbox"/> WAN RTT Overview

[Back](#) [Create NOC View](#)

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.

Manage NOC Views

Link Monitoring			
Sports View			
Business NOC Views			
Sample View			

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.

The screenshot shows the 'Notifications' section of the OpManager interface. On the left, there's a sidebar with 'General Settings' and 'Discovery' selected. The main area has tabs for 'Configuration', 'Monitoring', 'Notifications' (which is active), 'Tools', 'NetFlow', 'NCM', 'OpUtils', and 'ITOM Agent'. Below these tabs is a search bar and a 'Global Profiles' dropdown. A green 'Delete' button and a blue 'Add' button are at the bottom right of the main area. The main content area displays a table of notification profiles:

Profile Name	Profile Type	Status	Actions
Critical Devices Notifications	Send Email	On	[Edit, Delete]
Play Sound	Run Program	Off	[Edit, Delete]
Critical Devices Slack Profile	Chat	On	[Edit, Delete]
All device down Slack profile	Chat	On	[Edit, Delete]
Router Threshold	Send Email	Off	[Edit, Delete]
All device down email profile	Send Email	On	[Edit, Delete]
Device Availability	Send Email	Off	[Edit, Delete]
All Interface up down chat profile	Chat	On	[Edit, Delete]
All Interface up down profile	Send Email	Off	[Edit, Delete]

3. Select the Notification type as for example Email.

The screenshot shows the 'Create Notification Profile' page. The left sidebar has 'Notification Profiles' selected. The main area has tabs for 'General Settings', 'Discovery', 'Configuration', 'Monitoring', 'Notifications' (active), 'Tools', 'NetFlow', 'NCM', 'OpUtils', and 'ITOM Agent'. Below these tabs is a search bar and a 'Settings' button. The main content area shows a grid of notification types:

Email Get notified by an email alert when an alarm is generated.	Email based SMS Get notified by an email alert when an alarm is generated.	SMS Get notified by SMS alert when an alarm is generated.	Chat Get notified by slack when an alarm is generated.
Run System Command Lets you execute a command automatically when there is an alarm.	Run Program Lets you execute a script/ program automatically when there is an alarm.	Log a Ticket Lets you log trouble tickets in ServiceDesk Plus/ ServiceNow/ SDP Cloud when an alarm is generated.	Web Alarm Get notified with a sound alert when a critical alarm is generated.
SysLog Profile Get notified by SysLog messages when this profile is triggered based on the configured criteria.	Trap Profile This profile allows you to receive SNMP traps when it is triggered based on the configured criteria.	Invoke a Webhook Webhooks are user-defined callbacks via HTTP. Use webhooks to push alarms to the specified URL when an event is triggered i...	

At the bottom, there are links for 'How To', 'FAQ', and 'Video'.

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.

OpManager

General Settings Discovery Configuration Monitoring Notifications Tools NetFlow NCM OpUtils ITOM Agent

Notifications

Notification Profile > Email

Get notified by an email alert when an alarm is generated.

From Email Address: OpManager@disney.com

To Email Address: suraj.pethkar@disney.com

Add Cc

Mail Format: Plain Text, HTML, Both

Subject: \$stringseverity - \$displayName

Subject Variables: Select Subject Variables

Message: Message: \$message
Device: \$displayName
Category: \$category
Error Condition: \$stringseverity
Generated at: \$strModTime

Message Variables: Select Message Variables

Buttons: Back, Cancel, Next

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

OpManager

General Settings Discovery Configuration Monitoring Notifications Tools NetFlow NCM OpUtils ITOM Agent

Notifications

Send Email - Choose the criteria

Get notified by an email alert when an alarm is generated.

- Criteria
- Device Down for Attention Trouble Critical Severity
- Hardware in problematic condition
- Interface or switch port has some problems
- When any Selected (0|17) Service is down
- When any Selected (0|15) Windows Service is down
- When any Selected (0|6) Printer Monitor is down
- When any Selected (0|3) UPS Monitor is down
- When any Selected (0|20) SNMP trap is received from the device
- Threshold rule is violated
- When any URL is down
- When any Selected (0|4) Script Monitor is down or has violated a threshold
- When any Selected (0|2) Process is down or has violated a threshold

Buttons: Back, Cancel, Next

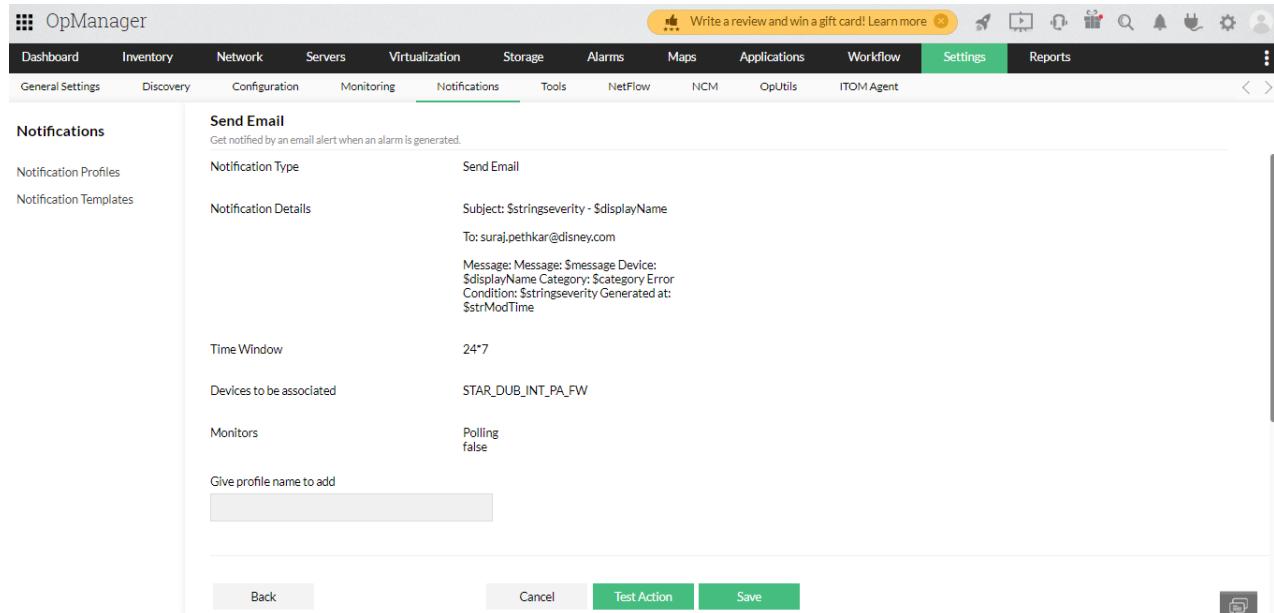
6. Select the devices either By Category or By Business View or By Devices and click Next.

The screenshot shows the 'Send Email - Associate Notification Profile' configuration page in OpManager. On the left, there's a sidebar with 'Notifications' selected, showing 'Notification Profiles' and 'Notification Templates'. The main area has tabs for 'By Category', 'By Business View', and 'By Devices'. Under 'By Devices', there's a 'Filter Devices' dropdown set to '-Select-' and a note about manually associating newly added devices via the Discovery Rule Engine. Below the filter is a list of 'Available Devices' which includes: STAR_DUB_INT_PA_FW, BACKUP_STAR_DUB_INT_PA_FW, STV-BNG-CORP-SERVER-STACK.star1, STV-Urmi-GF-Access-SW-01_Star_Urmi, STV-BNG-CORP-ACCESS-STACK1.star1, Sports_PA_02, STV-URMI-F31-ACCESS-STACK, STV-DR-RTR-4451-DCDR-II_Star_DR, and STV-DR-RTR-4451-DCDR-II_Star_DR. To the right is a 'Selected Devices' list which is currently empty. A note at the bottom states: 'Note : Notification profiles will not be automatically associated to newly added devices in a Category/Business View. This can be done using the Discovery Rule Engine.'

7. Select the required Time Window, Delayed Trigger and Recurring Trigger and click Next.

The screenshot shows the 'Send Email' configuration page in OpManager. The 'Time Window' section has 'Apply this profile 24x7' selected. The 'Delayed Trigger' section includes a 'Trigger after' field set to 'Minutes' and a checkbox 'Do not trigger if the alarm is Acknowledged'. The 'Recurring Trigger' section includes a 'Trigger Interval' field set to 'Minutes', a 'Restrict number of triggers to' field, and a checkbox 'Do not trigger if the alarm is Acknowledged'. At the bottom are 'Back', 'Cancel', and 'Next' buttons.

8. Give a profile name and Click Test Action to test the email profile or Save to save the profile.



The screenshot shows the 'OpManager' interface with the 'Notifications' tab selected. A 'Send Email' profile is being configured. The configuration details are as follows:

- Notification Type:** Send Email
- Subject:** \$stringseverity - \$displayName
- To:** suraj.pethkar@disney.com
- Message:** Message: \$message Device: \$displayName Category: \$category Error Condition: \$stringseverity Generated at: \$strModTime
- Time Window:** 24*7
- Devices to be associated:** STAR_DUB_INT_PA_FW
- Monitors:** Polling false
- Give profile name to add:** (Input field)

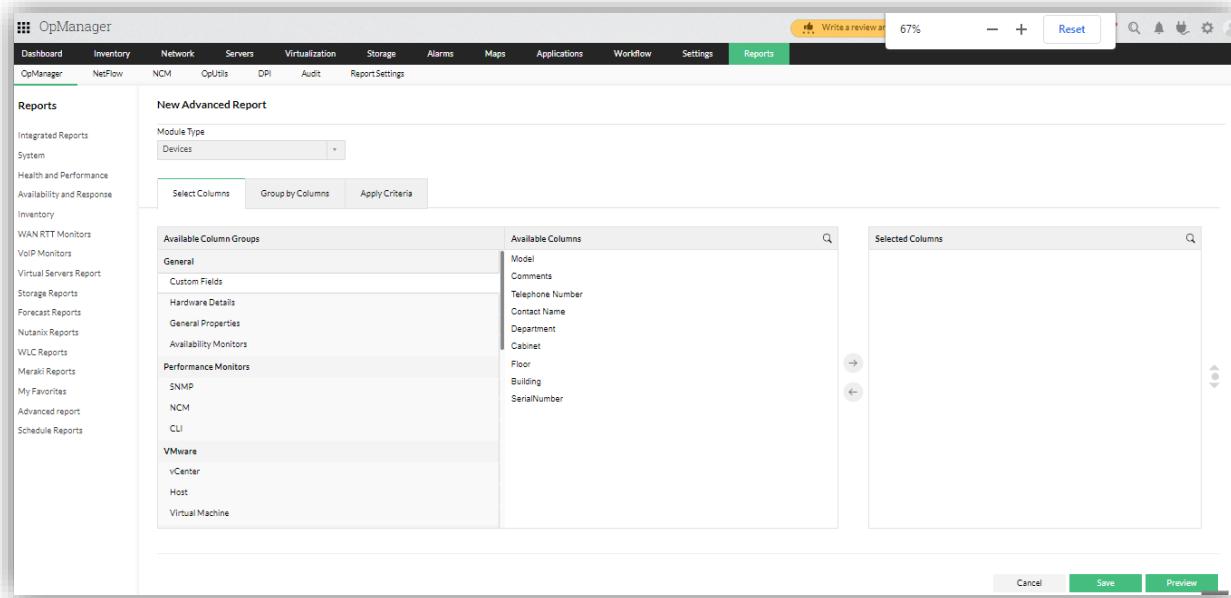
At the bottom, there are buttons for Back, Cancel, Test Action (highlighted in green), and Save.

13. Reports

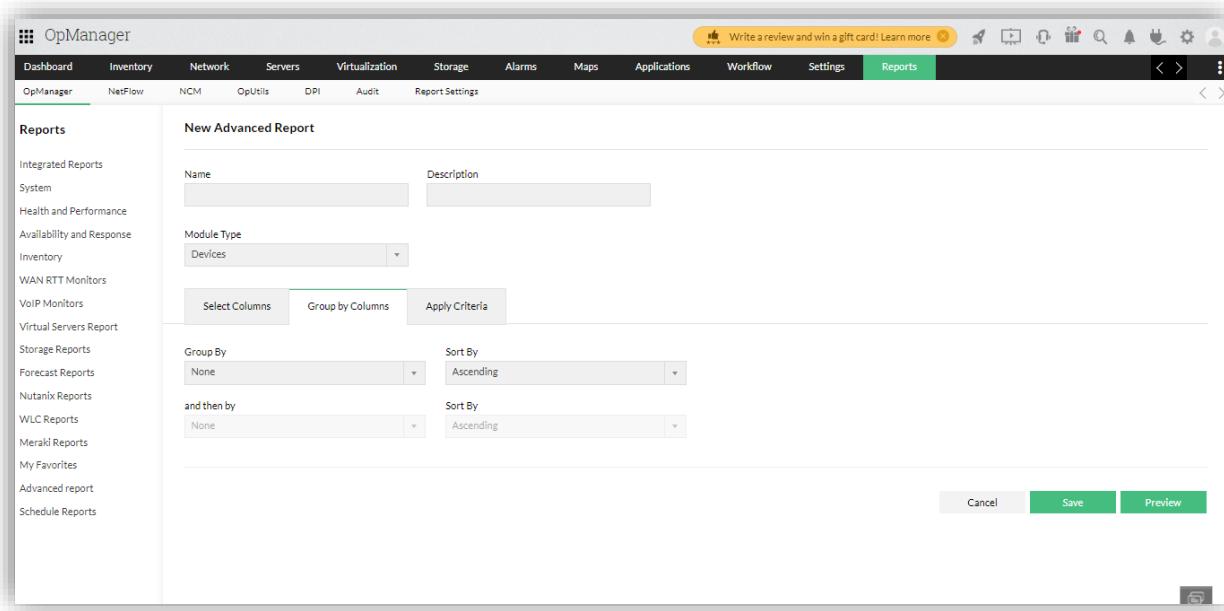
OpManager constantly monitors the network for performance and availability and records the data in the form of reports. There are about 100+ default intuitive reports in OpManager that enable the users to understand the trends based on the monitoring parameters.

1. How to create New Advanced Report?

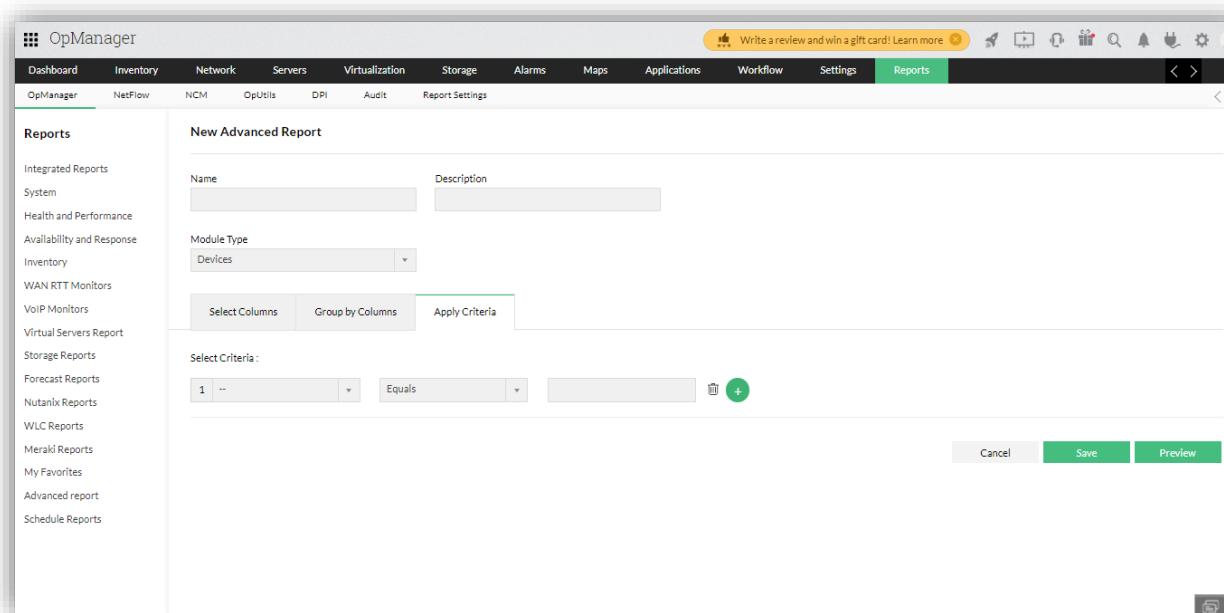
1. Navigate to Reports OpManager --> Advanced report.
2. Click on Create New Report button available on the top right corner. (This option to create a new report is provided on the top right corner of every default report.)



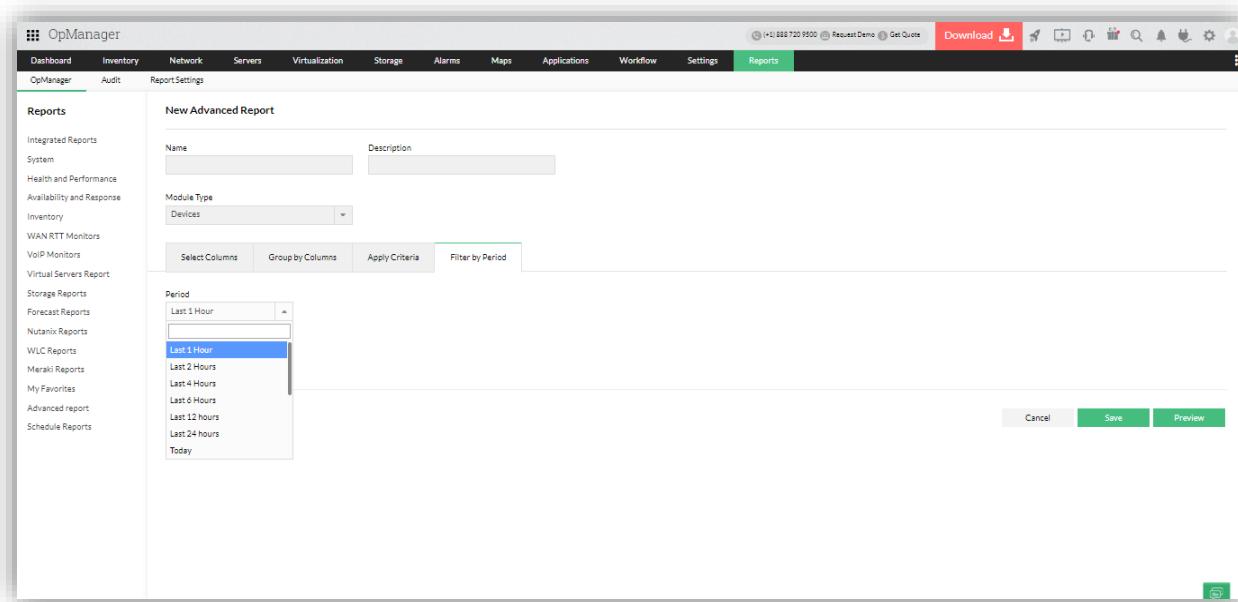
3. Enter a suitable Name and Description for the report.
4. Select a Module from the available list of modules - Devices, Interfaces, Service Monitors, URL Monitors, Alarms.
5. Select your preferred parameter categories from the Available Column Groups. Within each parameter category, there are multiple 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.

The screenshot shows the 'Schedule Reports' section of the OpManager interface. On the left, there's a sidebar with various report categories like Integrated Reports, System, Health and Performance, etc. The main area displays a table of scheduled reports with columns for Name, Status, Schedule Description, and Actions. Some reports listed include 'All Devices Uptime Monthly', 'All Interface availability Monthly', and 'Monthly New added devices'. Buttons for 'Add Schedule Report', 'Enable', 'Disable', and 'Delete' are visible at the top right of the table.

Name	Status	Schedule Description	Actions
All Devices Uptime Monthly	Enabled	All Report - Monthly Schedule - 1st of December,November,October,September,August,July,June,May,April,March,February,January at 01:00hours	
All Devices Uptime Monthly-xlsx	Enabled	All Report - Monthly Schedule - 1st of February,March,April,May,June,July,August,September,October,November,December,January at 1:00hours	
All Interface availability Monthly	Enabled	All Report - Monthly Schedule - 1st of December,November,October,September,August,July,June,May,April,March,February,January at 01:00hours	
All Interface availability Monthly-xlsx	Enabled	All Report - Monthly Schedule - 1st of December,November,October,September,August,July,June,May,April,February,January,March at 1:00hours	
All Interfaces Monthly utilization	Enabled	All Report - Monthly Schedule - 1st of February,March,April,May,June,July,August,September,October,November,December,January at 01:10hours	
All Interfaces Monthly utilization-xlsx	Enabled	All Report - Monthly Schedule - 1st of December,November,October,August,July,June,May,April,March,February,January,September at 1:10hours	
Monthly New added devices	Enabled	All Report - Monthly Schedule - 1st of July,August,September,October,November,December,March,January,February,June,May,April at 01:00hours	
Monthly New added devices-xlsx	Enabled	All Report - Monthly Schedule - 1st of June,May,April,February,January,August,September,July,October,November,December,March at 1:00hours	
MPLS_Link_Weekly_Report	Enabled	Integrated Reports - Weekly Schedule - Saturday,Sunday at 23:00hours	
Network Devices Availability Monthly Report	Enabled	All Report - Daily Schedule at 16:20hours	
STV-NOI-INX9K-CORE-02	Enabled	Monitors Report - Daily Schedule at 9:00hours	
Top N device reports	Enabled	All Report - Weekly Schedule - Monday at 9:00hours	

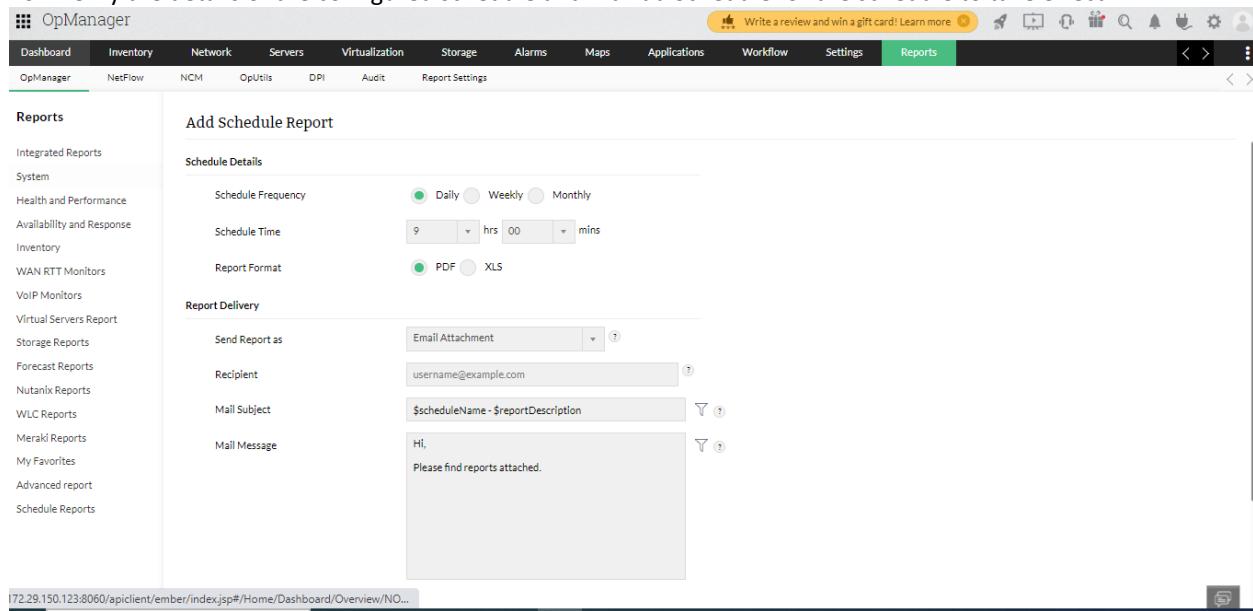
3. Enter Schedule Name
4. Choose Report Type
5. If you have chosen to schedule reports for Device availability reports and configure the following, Select either a category of devices, or the required business view, or select specific devices manually for generating the availability reports.
6. Select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

The screenshot shows the 'Add Schedule Report' dialog box. It has fields for 'Schedule name' (empty), 'Report Type' (set to 'Device Availability Reports'), 'Availability Report based on' (set to 'Device Category'), 'Device Category' (set to 'Server'), 'Time Period' (set to 'Last 12 hours'), and 'Time Window / Business Hour' (set to 'Full 24 hours'). At the bottom are 'Cancel' and 'Next' buttons.

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



The screenshot shows the OpManager web interface. The top navigation bar includes links for Dashboard, Inventory, Network, Servers, Virtualization, Storage, Alarms, Maps, Applications, Workflow, Settings, and Reports. The Reports tab is currently selected. On the left, a sidebar titled 'Reports' lists various report categories: 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, Meraki Reports, My Favorites, Advanced report, and Schedule Reports. The main content area is titled 'Add Schedule Report' and contains two sections: 'Schedule Details' and 'Report Delivery'. In 'Schedule Details', the 'Schedule Frequency' is set to 'Daily' (selected), with 'Weekly' and 'Monthly' options available. The 'Schedule Time' is set to 9:00:00. The 'Report Format' is set to 'PDF' (selected). In 'Report Delivery', the 'Send Report as' option is set to 'Email Attachment'. The 'Recipient' field contains 'username@example.com'. The 'Mail Subject' field contains '\$scheduleName - \$reportDescription'. The 'Mail Message' field contains the text 'Hi,
Please find reports attached.' At the bottom of the form, there is a large 'Add Schedule' button.

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.

Category	Description	Severity	Timestamp
Active Alarms	CPU Utilization is 79, threshold value for this monitor is 75 TATA-DC-INT-PA-FW-PRI Firewall UnAssigned Attention Severity of the group is changed from Critical to Trouble All Routers LogicalGroup UnAssigned Trouble PA MemoryUtilization is 100%, threshold value for this mo... MAATV-BOE-INTERNET-PA-FW Firewall UnAssigned Critical Interface 'ethernet1/2-ethernet2/1' is shutdown. KOL_STAR_PFT_PA_FW Firewall UnAssigned Critical Severity of the group is changed from Clear to Trouble ALL Core Switches LogicalGroup UnAssigned Trouble Interface 'ge-0/0/23-PFT_FIREWALL' is down. STAR-KOL-CORE-SW Switch UnAssigned Trouble Interface 'GigabitEthernet5/0/23***Connected to Printer*'... STV-UML-F23-ACCESS-5Star_Urmi Switch UnAssigned Trouble Bandwidth exceeded the configured limit for interface lo-... FireEye-CM-DAKC-prod Security Devices UnAssigned Trouble Interface 'ether1-ether1' is shutdown. FireEye-CM-DAKC-prod Security Devices UnAssigned Critical Interface 'TenGigabitEthernet2/0/47-Te2/0/47' is down. STV-PlanetC-CORE-SW-STACK Switch UnAssigned Trouble Interface 'TenGigabitEthernet1/0/47-Te1/0/47' is down. STV-PlanetC-CORE-SW-STACK Switch UnAssigned Trouble Interface 'TenGigabitEthernet3/0/46***Connected to CAS...' STV-PlanetC-CORE-SW-STACK Switch UnAssigned Trouble Interface 'TenGigabitEthernet3/0/47-Te3/0/47' is down. STV-PlanetC-CORE-SW-STACK Switch UnAssigned Trouble Interface 'TenGigabitEthernet3/0/48-Te3/0/48' is down. STV-PlanetC-CORE-SW-STACK Switch UnAssigned Trouble Interface 'TenGigabitEthernet2/0/48-Te2/0/48' is down. STV-PlanetC-CORE-SW-STACK Switch UnAssigned Trouble Interface 'GigabitEthernet3/0/47-++Connected to Urmi...' STV-UML-F23-ACCESS-5Star_Urmi Switch UnAssigned Trouble <td rowspan="10">Attention, Trouble, Critical</td> <td rowspan="10">2 hours ago, 18 hours ago, 1 day ago, 3 days ago, 3 days ago, 3 days ago, 3 days ago, 9 days ago, 9 days ago, 9 days ago</td>	Attention, Trouble, Critical	2 hours ago, 18 hours ago, 1 day ago, 3 days ago, 3 days ago, 3 days ago, 3 days ago, 9 days ago, 9 days ago, 9 days ago
	63		
	23		
	34		
	2		
	4		
	1		
	62		

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 switches 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.

The screenshot shows the OpManager interface with the 'Dashboard' tab selected. On the left, there's a sidebar with 'Critical Devices' and a count of 114. The main area displays a grid of icons representing different network and server components. In the top right of the main area, there's a 'New Dashboard' button. To the right of the main dashboard area, there's a sidebar titled 'My Dashboards' which lists categories like 'Device Availability', 'Link Monitoring', and 'NOC Views Dashboards'. The 'NOC Views Dashboards' category is highlighted with a yellow background.

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.

The screenshot shows the OpManager interface with a search bar labeled "Search Widgets". Below it is a grid of widget categories:

- Alarms and Events**: Alarms for a Device, Alarms from SNMP Traps, All Alarms, Devices Down, Devices with Alarms, Event Logs, Event Logs for a Device, Event Summary, Events for a Device, Interfaces Down, Interfaces down in a Device, Notification Profiles Triggered, Recent Alarms, Recent Events.
- General (Map View and Others)**: 3D Floor View, All Groups, Business View, Business View Summary, Custom HTML or Text, Custom Links of a Device, Device Summary, Devices in Business View, Devices in Group, Favorite Reports, File Monitors HeatMap, Floor Details, Folder Monitors HeatMap, HeatMap.
- IPAM and SPM Widgets**: AD Status Summary, DNS Status Summary, IP Availability Summary, IP Availability Summary HeatMap, NIC Type Summary, OS Type Summary, Port Availability Summary, Port Availability Summary HeatMap, Recently Discovered, Recently Marked as Guest, Recently Marked as Rogue, Recently Marked as Trusted, Top 10 Groups with occupied IPs, Top 10 Subnets with Occupied IPs.
- Real Time Graphs**: Flap Count Summary, Flap Summary, Interfaces Health Summary, Monitors Health Summary, Real Time Bandwidth Utilization, Real Time CPU Utilization, Real Time Graph for a Monitor, Real Time Memory Utilization, Real Time Traffic, Realtime Alarm.
- SDN Widgets**: Devices by CPU Utilization, Fabric Health Score (less than 'N').

6. Click Next.

7. Select the user(s) whom you wish to share the dashboard with

The screenshot shows the "Associate Dashboard to Users" interface. On the left, there are checkboxes for "Show Roles" (Display all roles), "Administrator" (checked), and "Operator". A "Select Users" button is next to a search bar. Below is a "Select all Roles and Users" checkbox. A detailed list of users under the "Administrator" role is shown:

	Administrator	1/10
All	admin (Owner)	
	amit.dadhore.vc	
	bharat.chaudhari...	
	gaurav.malvi.vc	
	gouresh.malk-nd	
	jay.dave.vc	
	rajendra.pandit-nd	
	shallesh.plimble-nd	
	suraj	
	yogesh.rvc	

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 vrorouters	NetFlow
Fortigate	NetFlow
Cybrome firewall	NetFlow
Checkpoint & Sonicwall firewall	sFlow

NetFlow Analyzer													
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-1Star_Chennai, STV-CHN-4351-MPLS-RTR-2Star_Chennai, ... is not in sync Learn more													
<input type="checkbox"/>	Devices (44)		Interfaces (136)		Groups (16)		Apps		Cloud Services		Users		QoS
													AS View
													Last Hour
													...
Router Name		IP Address		Type	Interface Count		Flow Count						
<input type="checkbox"/>	MAATV-BANJARAHILLS-4500-CORE-SW.starindia.com	172.21.1.1			2		112080						
<input type="checkbox"/>	MAATV-BANJARAHILLS-MPLS-RTR-1.maatv.com	172.21.1.2			1		136773						
<input type="checkbox"/>	MAATV-BANJARAHILLS-MPLS-RTR-2.maatv.com	172.21.1.3			1		94						
<input type="checkbox"/>	MAATV-BOE-INTERNET-PA-FW01	172.21.21.6			2		909505						
<input type="checkbox"/>	Sports_PA_01	172.20.145.18			2		175409						
<input type="checkbox"/>	STAR-KOL-CORE-SW	172.29.85.3			1		89125						
<input type="checkbox"/>	STV-BNG-4451-MPLS-RTR-1.startv.com	172.21.51.3			1		48552						
<input type="checkbox"/>	STV-BNG-4451-MPLS-RTR-2.starindia.com	172.21.51.4			1		139						
<input type="checkbox"/>	STV-BNG-CORP-4500-CORE.starindia.com	172.21.51.1			2		59263						
<input type="checkbox"/>	STV-CHN-4351-MPLS-RTR-1.Star_Chennai	192.168.11.2			1		50154						
<input type="checkbox"/>	STV-CHN-4351-MPLS-RTR-2.Star_Chennai	192.168.11.3			1		274						
<input type="checkbox"/>	STV-DR-INT-PA-FW	172.29.246.7			1		37149						
<input type="checkbox"/>	STV-DR-MPLS-RTR-2911.Banglore-DR	172.29.240.2			1		8						
<input type="checkbox"/>	STV-DR-RTR-4451-DCDR-II.Star_DR	172.29.250.5			1		619						
<input type="checkbox"/>	STV-DR-RTR-4451-DRDC-I.Star_DR	172.29.250.4			1		82488						
<input type="checkbox"/>	STV-GURGAON-2951-MPLS-RTR-1.Star_Gurgaon	172.29.48.4			1		69421						
<input type="checkbox"/>	STV-GURGAON-2951-MPLS-RTR-2.startv	172.29.48.5			1		0						

NetFlow Analyzer														
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-1Star_Chennai, STV-CHN-4351-MPLS-RTR-2Star_Chennai, ... is not in sync Learn more														
<input type="checkbox"/>	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
<input type="checkbox"/>		TenGigabitEthernet1/1/6 - PRI PBB		MAATV-BANJARAHILLS-4500-CORE...			36 %		0 %	360.069 Mbps	4.337 Mbps			0
<input type="checkbox"/>		TenGigabitEthernet1/2/5 EVPL		MAATV-BANJARAHILLS-4500-CORE...			0 %		0 %	41.752 bps	0.000 bps			0
<input type="checkbox"/>		GigabitEthernet0/0/TATA MPLS		MAATV-BANJARAHILLS-MPLS-RTR...			7 %		6 %	14.114 Mbps	11.748 Mbps			0
<input type="checkbox"/>		GigabitEthernet0/0/200 MB TATA ...		MAATV-BANJARAHILLS-MPLS-RTR...			0 %		0 %	87.249 bps	218.695 bps			0
<input type="checkbox"/>		ethernet1/1		MAATV-BOE-INTERNET-PA-FW01			0 %		0 %	3.242 Mbps	1.481 Mbps			0
<input type="checkbox"/>		ethernet1/3		MAATV-BOE-INTERNET-PA-FW01			1 %		0 %	8.295 Mbps	1.790 Mbps			0
<input type="checkbox"/>		Ethernet 1/1 TATA ILL 400 MB		Sports_PA_01			2 %		1 %	6.517 Mbps	2.301 Mbps			0
<input type="checkbox"/>		Ethernet 1/2 Airtel 400 MB ILL		Sports_PA_01			5 %		0 %	18.449 Mbps	217.912 Kbps			0
<input type="checkbox"/>		ge-1/0/20		STAR-KOL-CORE-SW			6 %		1 %	54.351 Mbps	14.997 Mbps			0
<input type="checkbox"/>		GigabitEthernet0/0/80 MB TATA M...		STV-BNG-4451-MPLS-RTR-1.startv.c...			4 %		5 %	3.122 Mbps	4.058 Mbps			0
<input type="checkbox"/>		GigabitEthernet0/0/80 MB TATA M...		STV-BNG-4451-MPLS-RTR-2.starindia...			0 %		0 %	106.847 bps	18.826 Kbps			0
<input type="checkbox"/>		TenGigabitEthernet1/1/8		STV-BNG-CORP-4500-CORE.starindia...			18 %		0 %	37.278 Mbps	0.000 bps			0
<input type="checkbox"/>		TenGigabitEthernet1/2/8		STV-BNG-CORP-4500-CORE.starindia...			0 %		0 %	41.675 bps	0.000 bps			0
<input type="checkbox"/>		GigabitEthernet0/1/30 MB TATA M...		STV-CHN-4351-MPLS-RTR-1.Star_Ch...			11 %		11 %	3.199 Mbps	3.258 Mbps			0
<input type="checkbox"/>		GigabitEthernet0/1/40 MB TATA MPL...		STV-CHN-4351-MPLS-RTR-2.Star_Ch...			0 %		0 %	35.413 bps	19.191 Kbps			0
<input type="checkbox"/>		Ethernet 1/1 40 MB ILL		STV-DR-INT-PA-FW			0 %		0 %	97.125 Kbps	186.471 Kbps			0
<input type="checkbox"/>		GigabitEthernet0/0		STV-DR-MPLS-RTR-2911.Banglore-DR			0 %		0 %	4.158 bps	0.000 bps			0
<input type="checkbox"/>		GigabitEthernet0/0/1 TATA 100 MB		STV-DR-RTR-4451-DCDR-II.Star_DR			69 %		0 %	68.550 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

Profile Name	Description	Category	Status	Actions
Starhouse Link Down	The link is down	Packets	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
High Utilization Outbound Traffic	High Utilization Outbound Traffic	Utilization	<input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
High link utilisation	High link utilization Inbound Traffic	Utilization	<input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Netflow		Utilization	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
TestFTP	Test FTP alert	Utilization	<input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

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	<p>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.</p> <ul style="list-style-type: none"> - 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 <p>To add more threshold values, click 'Add Row' and add values</p>
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-COREVT... / GigabitEthernet2/0/2 /

Volume | Speed | Utilization

Graph Types

1 Minute Average

Time: 10 Mar 2023 15:01:00 IST
IN : 3.167 Kbps
OUT : 0.042 Kbps

IN OUT

Traffic (Kbps)

Time (HH:MM)

Category **Total** **Maximum** **Minimum** **Average** **Standard Deviation** **95th Percentile**

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	12.123 Kbps

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
MAATV-BANJARAHILLS-4... / TenGigabitEthernet1/1/6... /

Volume | Speed | Utilization

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%

Application	Traffic	% of Traffic
ETHERIP_App	724.042 MB	8%
radius	603.985 KB	0%
UDP_App	315.181 KB	0%

OpManager

Dashboard Inventory Network Servers Virtualization Storage Alarms Maps Workflow Settings Reports

OpManager NetFlow NCM OpUtils DPI Audit Report Settings

NetFlow Reports

Search Report Report Profiles Forensics Favorite Reports Consolidated Report Capacity Planning Report Compare Reports Protocol Distribution Inventory Report Percentile Report LAN WAN Report Geolocation Report Billing Forecast Schedule WAAS Dashboard WAAS Devices List

Consolidated Report
SHCILESTAMP-DR-INT-R2... / GigabitEthernet0/1 /

Volume Speed Utilization

Source IN Report Source OUT Report

No Data

1 5 15 Resolve IP Last 24 hours

Source **Traffic** **% of Traffic**

14.143.102.155	2.204 MB	68%
115.112.47.45	424.615 KB	13%
115.114.9.68	315.916 KB	9%
R9.248.143.165	53.800 KR	1%

Source **Traffic** **% of Traffic**

No records to view.		
---------------------	--	--

Page [0] of 0 | 10 | No records to view.

10

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.

OpManager

Dashboard Inventory Network Servers Virtualization Storage Alarms Maps Workflow Settings Reports

OpManager NetFlow NCM OpUtils DPI Audit Report Settings

NetFlow Reports

Search Report Report Profiles Forensics Favorite Reports Consolidated Report Capacity Planning Report Compare Reports Protocol Distribution Inventory Report Percentile Report LAN WAN Report Geolocation Report Billing Forecast Schedule WAAS Dashboard WAAS Devices List

Consolidated Report

Select Source Interface
Select Device SHCILESTAMP-DR-INT-R2.shdl.com
Select Interface GigabitEthernet0/1
Traffic Type Utilization
Select Top 10
Select Report(s) Application, Source, Destination, QoS, Conversation
Time Period Last hour
Business Hour Filter
Exclude weekends

12

OpManager

Dashboard Inventory Network Servers Virtualization Storage Alarms Maps Workflow Settings Reports

OpManager NetFlow NCM OpUtils DPI Audit Report Settings

NetFlow Reports

Inventory Report Interfaces /

Volume Speed Utilization Last Hour

Router Name	Interface Name	IN						OUT					
		Traffic	Max	Min	Avg	95th Percentile	Link Speed	Traffic	Max	Min	Avg	95th Percentile	Link Speed
ESTAMP-MHDC-INT-R1.softcell.com	GigabitEthernet et0/1	2.851 GB	9.41%	2.26%	3.12%	3.18%	200.000 Mbps	32.438 GB	38.33%	26.52%	35.45%	37.25%	200.000 Mbps
ESTAMP-MHDC-INT-R2.softcell.com	GigabitEthernet et0/1	70.207 KB	0.00%	0.00%	0.00%	0.00%	200.000 Mbps	1.896 MB	0.00%	0.00%	0.00%	0.00%	200.000 Mbps
SHC-CTR-CTRS-R01.softcell.com	20Mbps MTNL	27.585 MB	0.63%	0.01%	0.30%	0.50%	20.000 Mbps	471.767 MB	9.73%	0.01%	5.16%	8.91%	20.000 Mbps
SHC-CTR-CTRS-R02.softcell.com	20Mbps TCL	25.927 KB	0.00%	0.00%	0.00%	0.00%	1.000 Gbps	14.870 KB	0.00%	0.00%	0.00%	0.00%	1.000 Gbps
SHC-CTR-CTRS-R02.softcell.com	GigabitEthernet et0/0/0.2	0.000 Bytes	0.00%	0.00%	0.00%	-	1.000 Gbps	0.000 Bytes	0.00%	0.00%	0.00%	-	1.000 Gbps
SHC-KOL-PTNA-R01.softcell.com	FastEthernet 0/1.2	330.209 MB	104.10%	11.97%	36.09%	77.93%	2.000 Mbps	0.000 Bytes	0.00%	0.00%	0.00%	0.00%	2.000 Mbps

12

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.

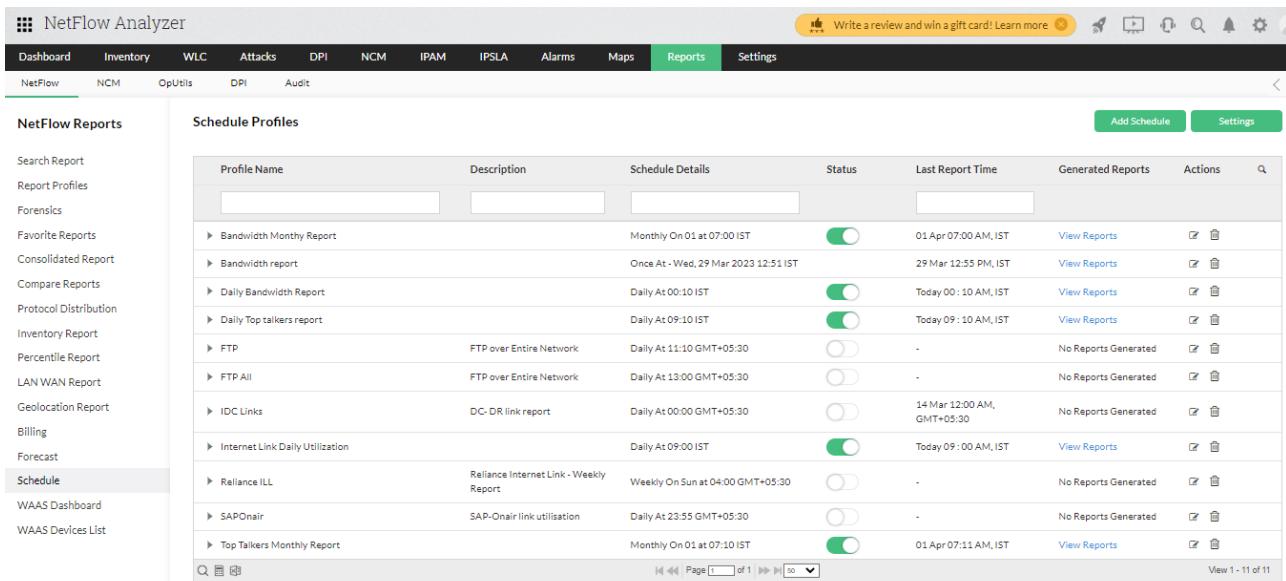
18. Schedule Reports

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.



The screenshot shows the NetFlow Analyzer interface with the 'Reports' tab selected. On the left, a sidebar menu includes 'Schedule' under the 'NetFlow Reports' section. The main content area displays a table titled 'Schedule Profiles' with columns for Profile Name, Description, Schedule Details, Status, Last Report Time, Generated Reports, and Actions. The table lists several scheduled reports, each with a 'View Reports' link and edit/delete icons.

Profile Name	Description	Schedule Details	Status	Last Report Time	Generated Reports	Actions
Bandwidth Monthly Report		Monthly On 01 at 07:00 IST	<input checked="" type="checkbox"/>	01 Apr 07:00 AM, IST	View Reports	 
Bandwidth report		Once At - Wed, 29 Mar 2023 12:51 IST	<input type="checkbox"/>	29 Mar 12:55 PM, IST	View Reports	 
Daily Bandwidth Report		Daily At 00:10 IST	<input checked="" type="checkbox"/>	Today 00:10 AM, IST	View Reports	 
Daily Top talkers report		Daily At 09:10 IST	<input checked="" type="checkbox"/>	Today 09:10 AM, IST	View Reports	 
FTP	FTP over Entire Network	Daily At 11:10 GMT+05:30	<input type="checkbox"/>	-	No Reports Generated	 
FTP All	FTP over Entire Network	Daily At 13:00 GMT+05:30	<input type="checkbox"/>	-	No Reports Generated	 
IDC Links	DC-DR link report	Daily At 00:00 GMT+05:30	<input type="checkbox"/>	14 Mar 12:00 AM, GMT+05:30	No Reports Generated	 
Internet Link Daily Utilization		Daily At 09:00 IST	<input checked="" type="checkbox"/>	Today 09:00 AM, IST	View Reports	 
Reliance ILL	Reliance Internet Link - Weekly Report	Weekly On Sun at 04:00 GMT+05:30	<input type="checkbox"/>	-	No Reports Generated	 
SAPOnair	SAP-Onair link utilisation	Daily At 23:55 GMT+05:30	<input type="checkbox"/>	-	No Reports Generated	 
Top Talkers Monthly Report		Monthly On 01 at 07:10 IST	<input checked="" type="checkbox"/>	01 Apr 07:11 AM, IST	View Reports	 

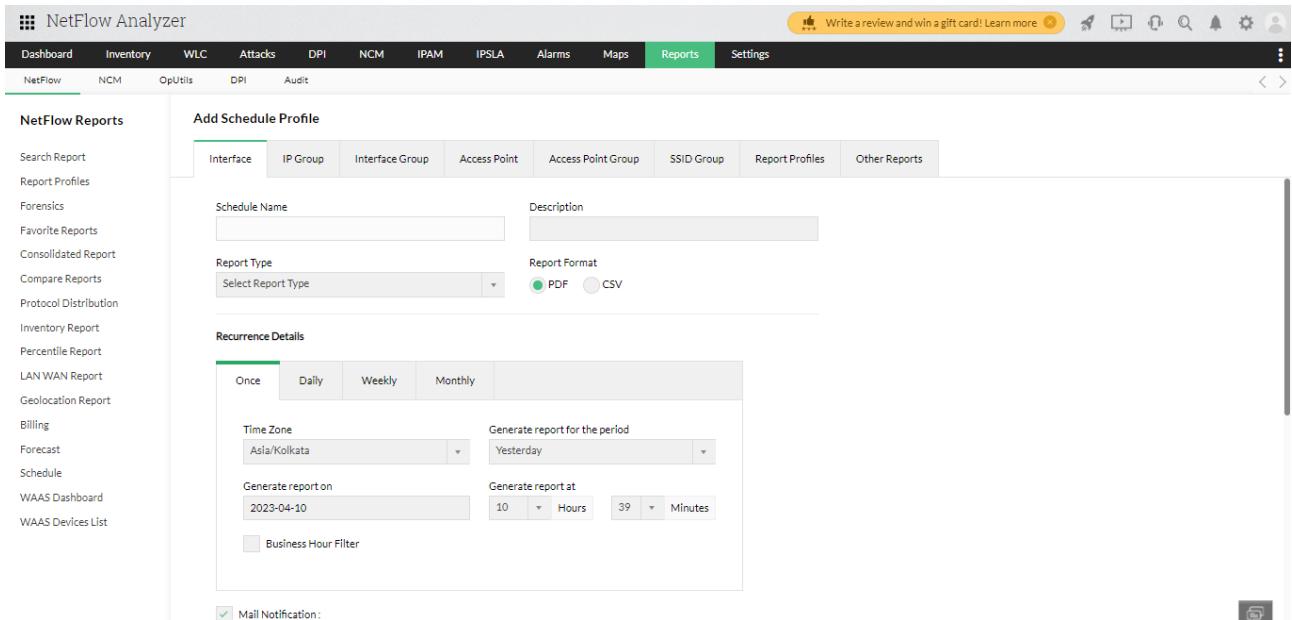
Click on Add Schedule and fill in the necessary details.

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.

