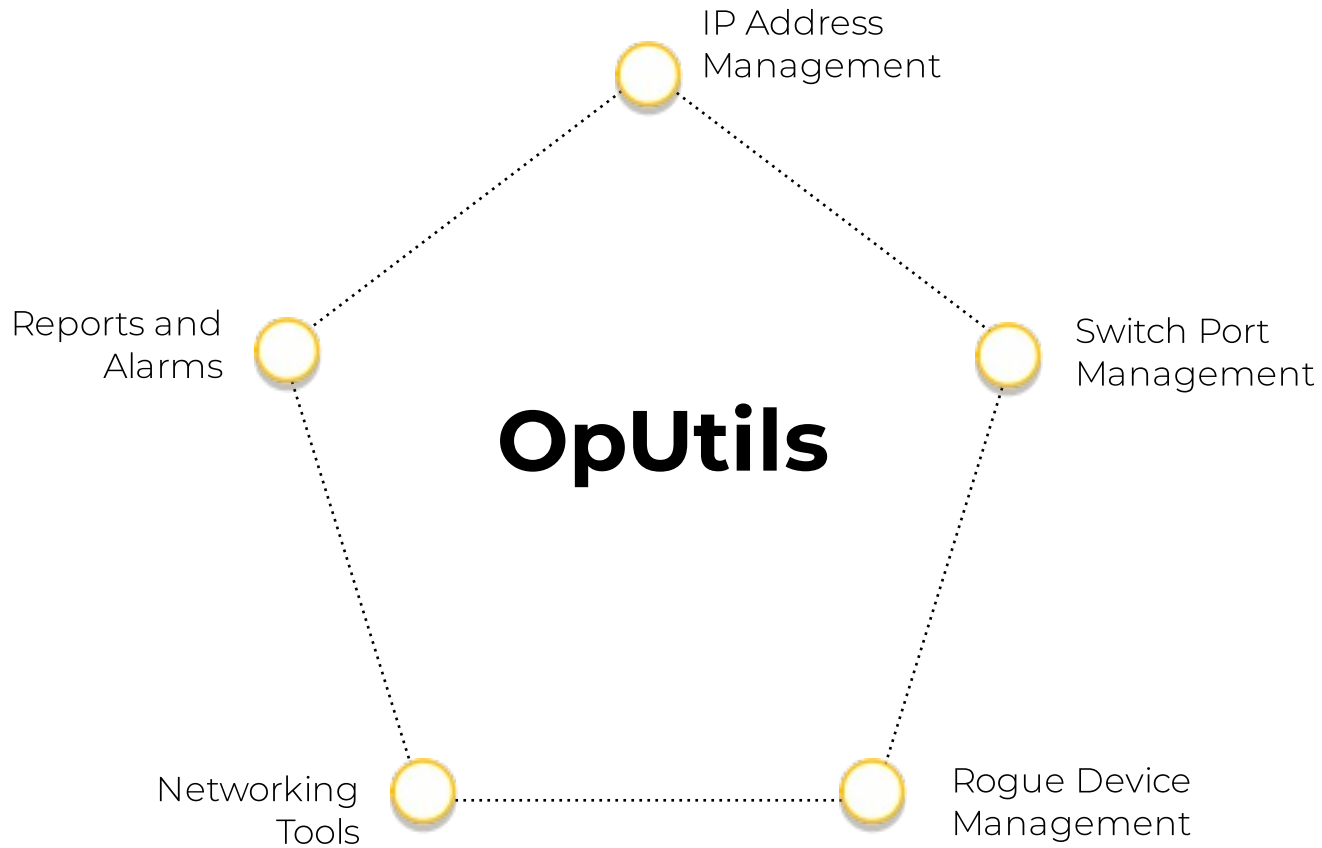


ManageEngine

OpUtils

IP Address & SwitchPort
Management Software

What is OpUtils?



- ManageEngine OpUtils is an efficient IP address and switch port management software that helps network admins to monitor their switches and IP address space with ease.
- This integrated solution aids network admins in effectively detecting rogue device intrusions and blocking them if necessary.
- It's built-in network toolset simplifies day-to-day network tasks such as bandwidth monitoring, configuration backup scheduling, network scanning, and address management.

How can OpUtils help your network?

- Replace spreadsheets for IP address management.
- Eliminate the need for physically tracing cables for switch port mapping.
- Identify, inspect, and block rogue devices.
- Stay ahead of network issues by getting instantly alerted via email, syslog, and in-console.
- Automate reporting on critical IP address and switch port management metrics.
- Simplify network tasks with a centralized network toolset.

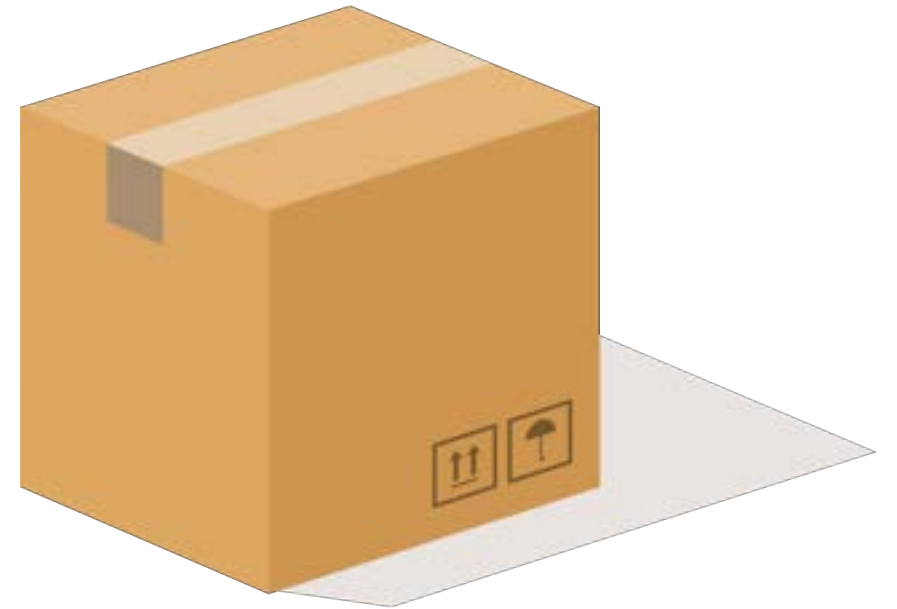


What is the
ManageEngine OpUtils
made of?

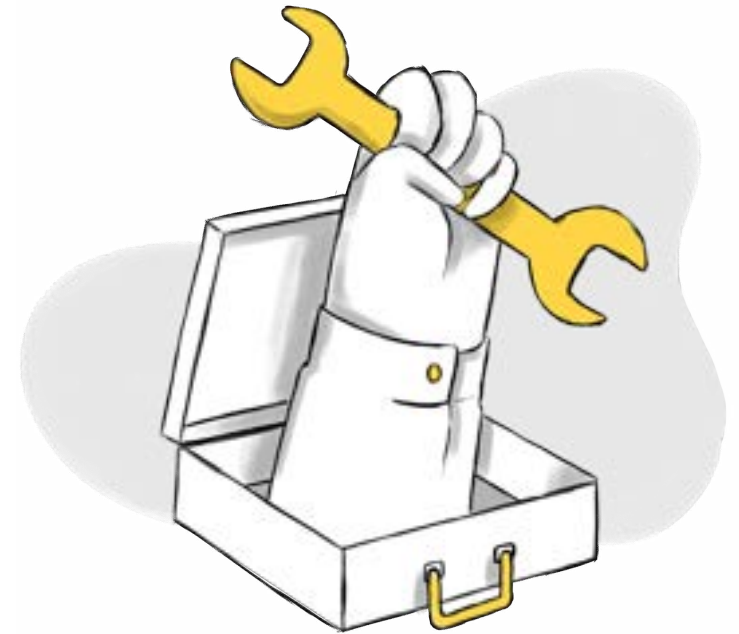


A look into the capabilities that **uncomplicates IT**

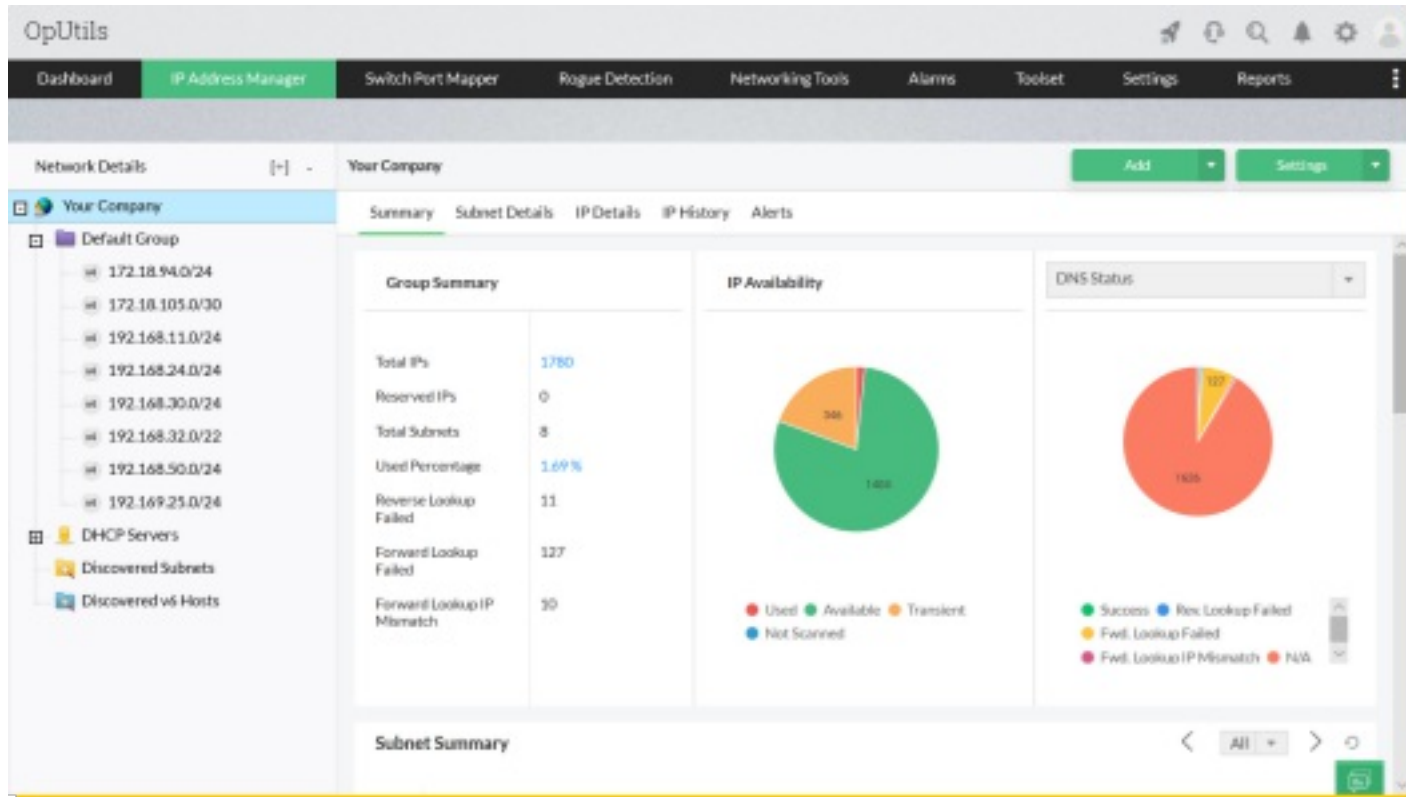
- IP Address Manager
- Switch Port Mapper
- Rogue device detection
- Network tool set
- Schedules, reports, and alarms
- User management



Featured modules



IP Address Management



- Discover and monitor all your IPv4 and IPv6 addresses in tandem.
- Automate advanced IP scanning, IP address tracking, and DHCP scope monitoring across subnets and supernets.
- View historical IP usage logs, and group and manage IPs according to your networking requirements.
- View in-depth insights into monitored IPs with just a click.
- Streamline IP allocation management with built-in with IP Request tool.

Switch Port Management

The screenshot displays the OpUtils Switch Port Mapper interface. At the top, there is a navigation bar with tabs for Dashboard, IP Address Manager, Switch Port Mapper (active), Rogue Detection, Networking Tools, Alarms, Toolset, Settings, and Reports. Below the navigation bar, a yellow banner provides a definition of transient ports: "What is a Transient? These ports are currently not in use. As per the policy, if the ports are inactive for more than 10 continuous days, it will be moved to Available category." Below this, there is a filter section and a table of switch ports.

Switch Name	IPNS Name	Status	Usage	Used Ports	Available
192.168.50.331		Finished	100%	4	0
192.168.50.340		Finished	75%	6	2

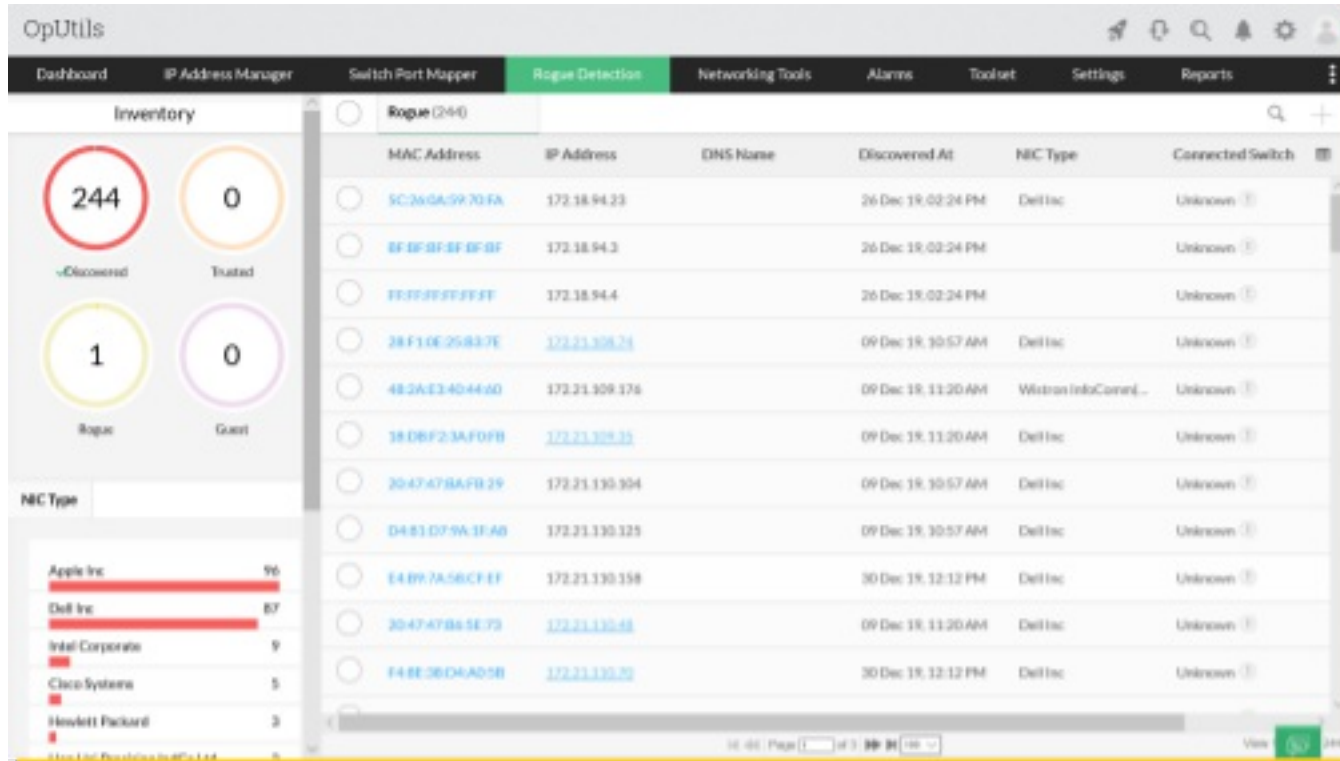
The detailed view for IP 192.168.50.340 shows the following information:

- IP Address:** 192.168.50.340
- System Location:** Cisco/MSR
- System Description:** Cisco 675 Software (2915) Software...
- System Status:** In Progress
- Subnet Address:** 192.168.50.0
- System Name:** Cisco675 (1934)
- OS Name:** Cisco
- Type:** Cisco
- Last Sync Time:** 27 Dec, 19 hours, 3 minutes, 50 sec...
- Last Scan Time:** 24 Jan 20, 06:23 PM
- MAC Address:** 94D3CA2F4DC2
- Comments:** no comments

Below the details, there are three gauges showing port utilization: Used Ports (75%), Transient Ports (0%), and Available Ports (25%). To the right, a "Port View" section shows a visual representation of the switch ports, with some ports highlighted in green to indicate active connections.

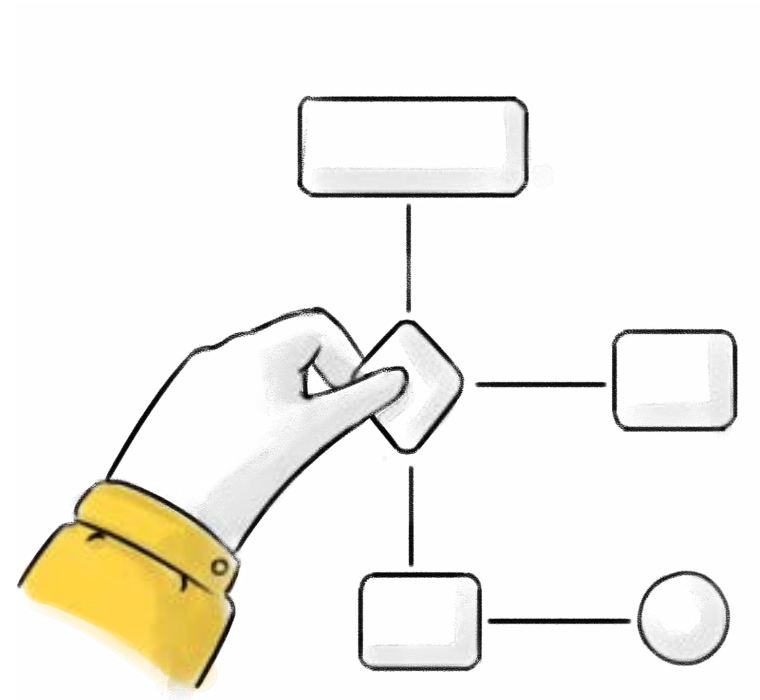
- Discover end-to-end switch port mapping details.
- Inspect ports and connected devices with insights into the IP-MAC details, status, and port speed of each port.
- View the nature of network connection such as if a port is truncated or connected to multiple MAC addresses.
- View historical port utilization logs and alerts.

Rogue device detection & prevention

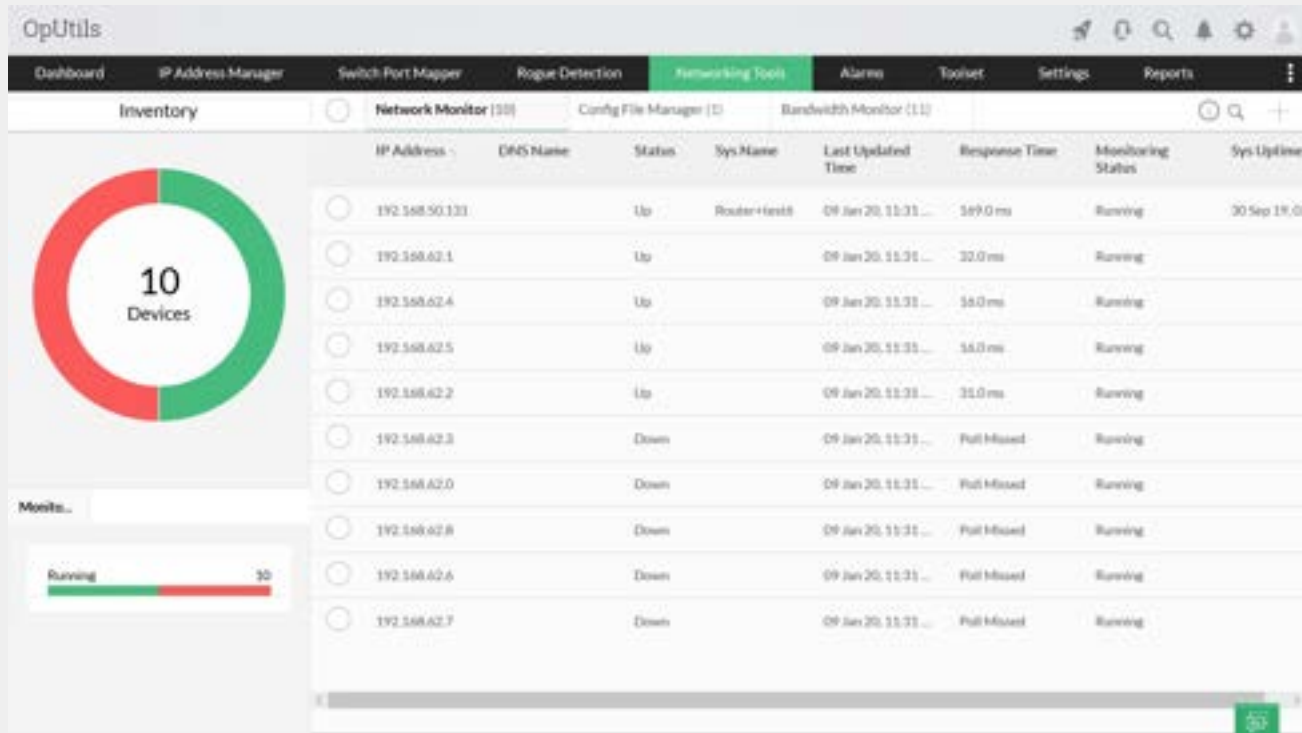


- Periodically scan the routers and subnets to track all new devices entering your network.
- Verify and mark devices as trusted, guest, or rogue, in a click.
- Identify and block switch ports enabling rogue access.
- Stay ahead of ARP spoofing attacks by continually scanning ARP entries

Networking Tools



Network Monitor



- View availability and response time of critical devices.
- Set-up alert escalation rules.
- Set custom polling intervals.

Config File Manager

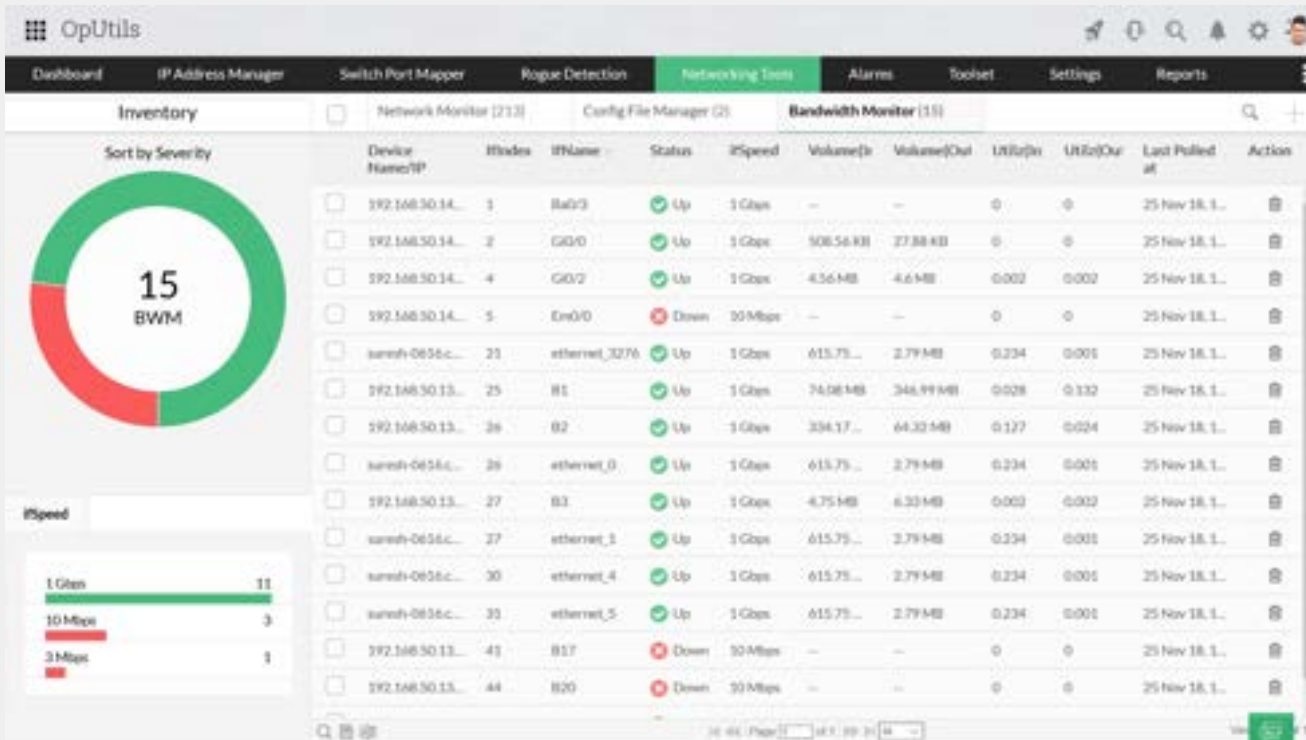
The screenshot displays the OpUtils Config File Manager interface. The top navigation bar includes Dashboard, IP Address Manager, Switch Port Mapper, Rogue Detection, Networking Tools (active), Alarms, Tools, Settings, and Reports. The main content area is divided into three sections: Inventory, Network Monitor (21:3), and Config File Manager (2). The Config File Manager section contains a table with the following data:

IP Address	DNS Name	Config File	Last Updated Time	TFTP/NAT IP	Description	Remarks	Actions
<input type="checkbox"/> 192.168.50.140			22 Jan 20, 09:22 PM	172.21.380		Error retrieving...	
<input type="checkbox"/> 192.168.50.131		No Data	06 Jul 15, 12:14 AM	172.21.380		Error retrieving...	

On the left side, there is a 'Backup Failures' gauge showing a red ring with the number 2 in the center. Below it, a 'Vendor' dropdown is set to 'Cisco/IOS Switch', with a bar chart showing 2 items.

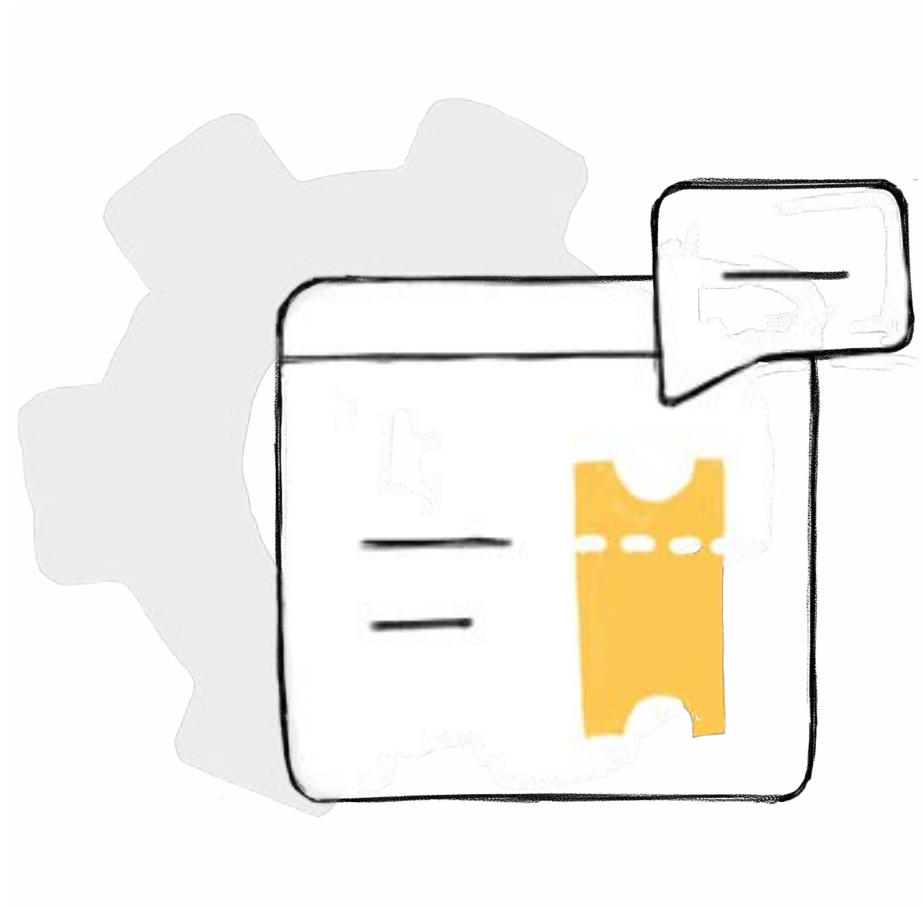
- Real-time Cisco config file change monitoring.
- Compare Cisco config files.
- Upload Cisco config files.
- Scheduled backup for Cisco config files.

Bandwidth Monitor



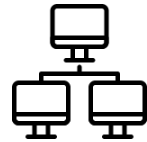
- View the bandwidth usage patterns and network traffic trends.
- Historical bandwidth usage logs.
- Bandwidth Monitoring Reports.

OpUtilsToolset



Ping Tools

Inspect connectivity issues in a LAN environment



Address Monitoring

Resolve MAC address, run DNS lookups, and monitor DHCP scopes



Network Monitoring

Run network scans, system port scans, and view and update system details remotely.



OpUtils Toolset

SNMP Tools

Browse and monitor SNMP MIB's and view configured Traps.



CISCO Tools

Monitor Cisco devices and get in-depth insights.



Others

Various tools to run queries, view syslog, and monitor traps.



Ping Tools


Ping Tools

Ping	SNMP Ping	Proxy Ping	Trace Route	
------	-----------	------------	-------------	--

IP Address/Host Name

Ping

Ping Status


System up and running

Ping Response

- Ping Tool - Ping network nodes to check network connectivity status.
- SNMP Ping - Run ping scans on SNMP-enabled network nodes.
- Proxy Ping - Run ping tests through a remote router to another remote target device.
- Trace Route - Record the route from host to the target destination.

Address Monitoring

Address Monitoring

MAC Address Resolver DNS Resolver DHCP Scope Monitor MAC IP List

IP to MAC MAC to IP

IP Address/Host Name

Community (optional)

Resolve

- MAC Address Resolver - Resolve IP address or host name to the associated MAC address and vice versa.
- DNS Resolver - Translate host name into IP address and vice versa.
- DHCP Scope Monitor - Find the used and available IP addresses in a DHCP Server scope.
- MAC IP List - Displays a list of all monitored IP addresses and their associated MAC address.

Network Monitoring

Network Monitoring

Network Scanner	Port Scanner	System Explorer	TCP Reset	System Details Update	
<input checked="" type="checkbox"/> Ping		<input checked="" type="checkbox"/> SNMP			
<input checked="" type="checkbox"/> MAC Address		<input checked="" type="checkbox"/> DNS			
<input type="button" value="Add IP"/> <input type="button" value="Scan"/> <input type="button" value="Delete"/> <input type="button" value="Search"/>					
<input type="checkbox"/> IP Address	Ping Status	Response Time	SNMP Status	SNMP Response Time	OS Type

Network Scanner - Pings different network nodes to check details including its status, response time, and OS type.

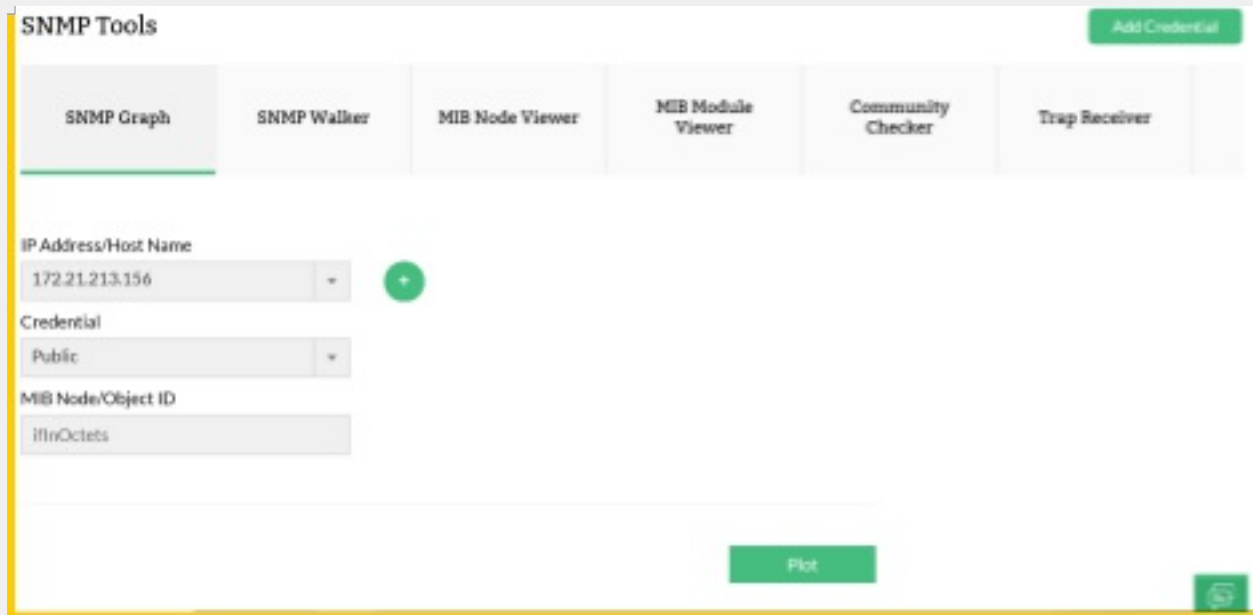
Port Scanner - Runs system port scans to identify open ports and the services running on them.

System Explorer - Get the complete details of a target device including its system snapshot, disk space, CPU usage, processes, and installed software.

TCP Reset - Find and reset the list of TCP connections established in the network.

System Details Update - View and update details such as Name, Location, and Contact of a network device.

SNMP Tools



The screenshot shows the 'SNMP Tools' web interface. At the top, there is a navigation bar with tabs for 'SNMP Graph', 'SNMP Walker', 'MIB Node Viewer', 'MIB Module Viewer', 'Community Checker', and 'Trap Receiver'. The 'SNMP Graph' tab is currently selected. In the top right corner, there is a green button labeled 'Add Credential'. Below the navigation bar, there are three input fields: 'IP Address/Host Name' with the value '172.21.213.156', 'Credential' with the value 'Public', and 'MIB Node/Object ID' with the value 'ifInOctets'. A green plus sign is visible to the right of the IP address field. At the bottom center, there is a green button labeled 'Plot'. In the bottom right corner, there is a small green icon.

- MIB Browser - Load, browse, search, and walk through SNMP MIBs.
- SNMP Graph - Gather data and draw graph for any SNMP device.
- SNMP Walker - Retrieve information on a set of OIDs in a MIB.
- MIB Node Viewer - View the details of a MIB node.
- Trap Receiver - View the configured traps.
- MIB Module Viewer - View the details of a MIB module.
- Community Checker - Read and write community strings.

Cisco Tools

Cisco Tools

Device Scan Device Explorer

Subnet/Network Address

Subnet Mask


Subnet Address


Community


- Device Scan - Scan subnets to collect details of the target Cisco devices.
- Device Explorer - Scan a Cisco device to get details such as device snapshot, chassis details, IOS details, flash memory, interfaces, IP routes, CPU and memory utilization, and access lists.

Other Tools

Others

 WMI Query Tool

 CLI Query Tool

 Forward Trap

 Forward Syslog

 Syslog Viewer

WMI Query Tool - Query remote systems with Device Name, User Name, Password, and Name Space.

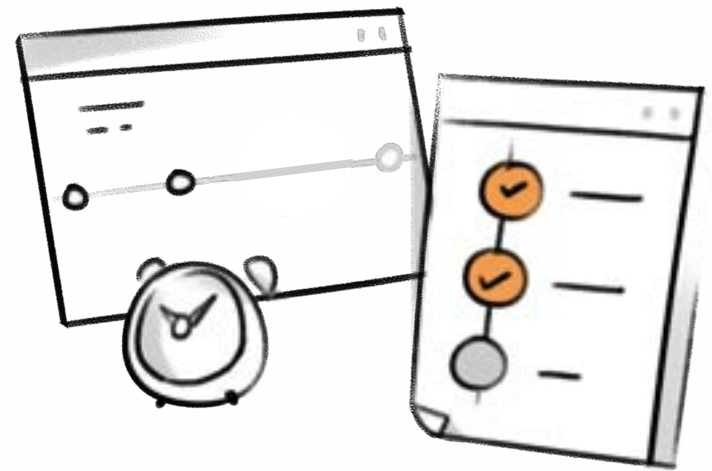
CLI Query Tool - Remotely execute command line queries from your OpUtils console.

Forward Trap - Forward the received traps to configured destinations.



Forward Syslog - Forward the received logs to configured destinations.

Syslog Viewer - View the Source, Facility, Severity, Message, and Response Received Time logged in syslog.

Schedule, configure, and report

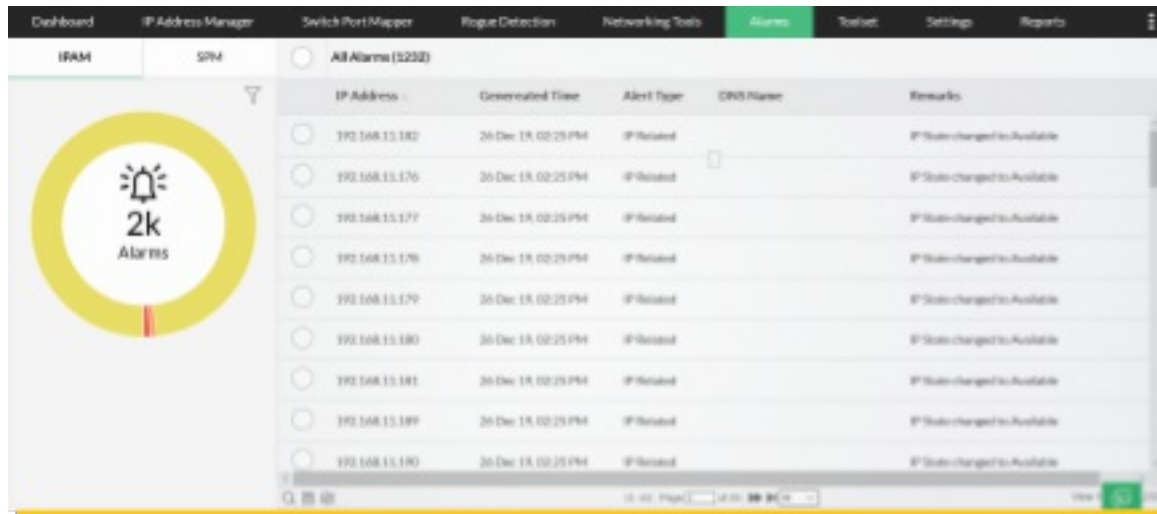


Schedule scans using a Scheduler

General	Scheduler	Configure Alerts	Clean up Policy	Publish	Custom Columns		
Task Name	Type	Subnet Count	Created Time	Last Scan Time	Next Scan Time	Owner	Actions
Default IPv4 Task	IPv4	5			Disabled	admin	
Default IPv6 Task	IPv6	0			Disabled	admin	
test scan	IPv4	2	26 Dec 19, 04:37 PM	23 Jan 20, 01:05 PM	23 Jan 2020, 01:10 PM	admin	
testtasl	IPv4	1	03 Jan 20, 04:55 PM	23 Jan 20, 01:05 PM	23 Jan 2020, 01:10 PM	admin	

- Schedule periodic scanning of monitored subnets, switch ports, and network components with Scheduler.
- Prevent rogue devices from having unrestricted access to your network with continual network scanning.

Configure Alarms



Dashboard | IP Address Manager | Switch Port Mapper | Rogue Detection | Networking Tools | **Alarms** | Toolkit | Settings | Reports

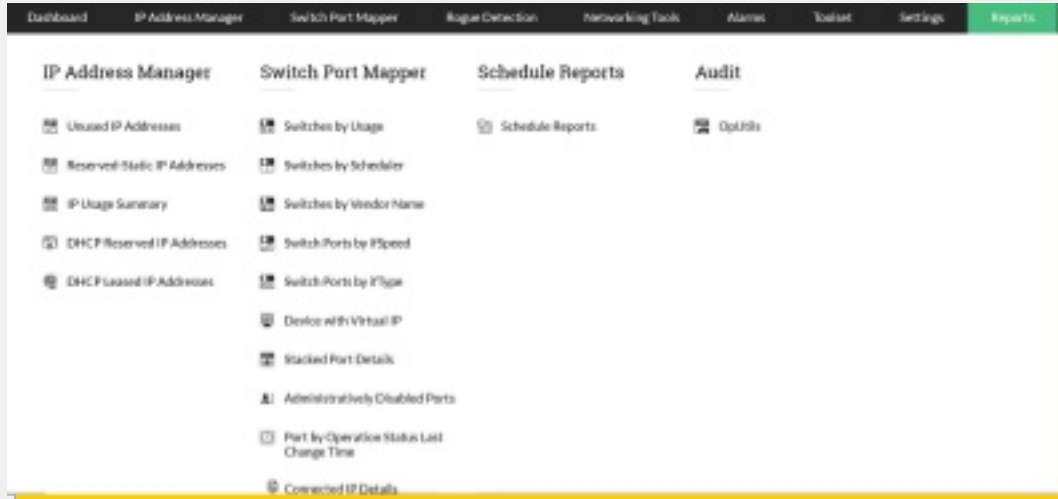
IFAM | SPM | All Alarms (2232)

2k Alarms

IP Address	Generated Time	Alert Type	DNS Name	Remarks
192.168.11.182	20 Dec 18, 02:25 PM	IP Related		IP State changed to Available
192.168.11.176	20 Dec 18, 02:25 PM	IP Related		IP State changed to Available
192.168.11.177	20 Dec 18, 02:25 PM	IP Related		IP State changed to Available
192.168.11.178	20 Dec 18, 02:25 PM	IP Related		IP State changed to Available
192.168.11.179	20 Dec 18, 02:25 PM	IP Related		IP State changed to Available
192.168.11.180	20 Dec 18, 02:25 PM	IP Related		IP State changed to Available
192.168.11.181	20 Dec 18, 02:25 PM	IP Related		IP State changed to Available
192.168.11.189	20 Dec 18, 02:25 PM	IP Related		IP State changed to Available
192.168.11.190	20 Dec 18, 02:25 PM	IP Related		IP State changed to Available

- Proactively monitor your IP address space and network switch ports to identify emerging network issues.
- View all alarms in console or through preferred alert channels.

Generate Reports

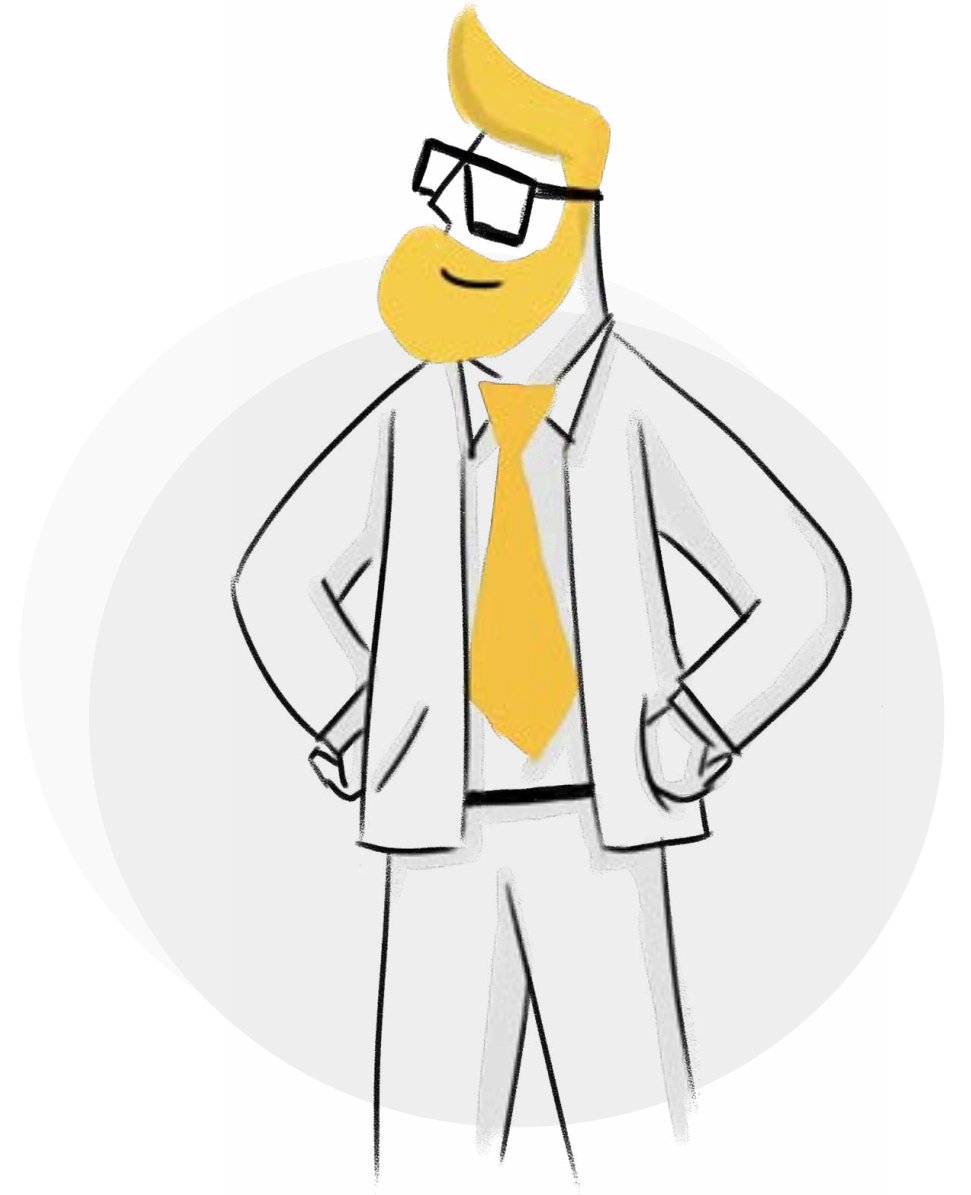


- .Wide variety of reports to track IP and switch port metrics.
- Schedule reports or download on demand.

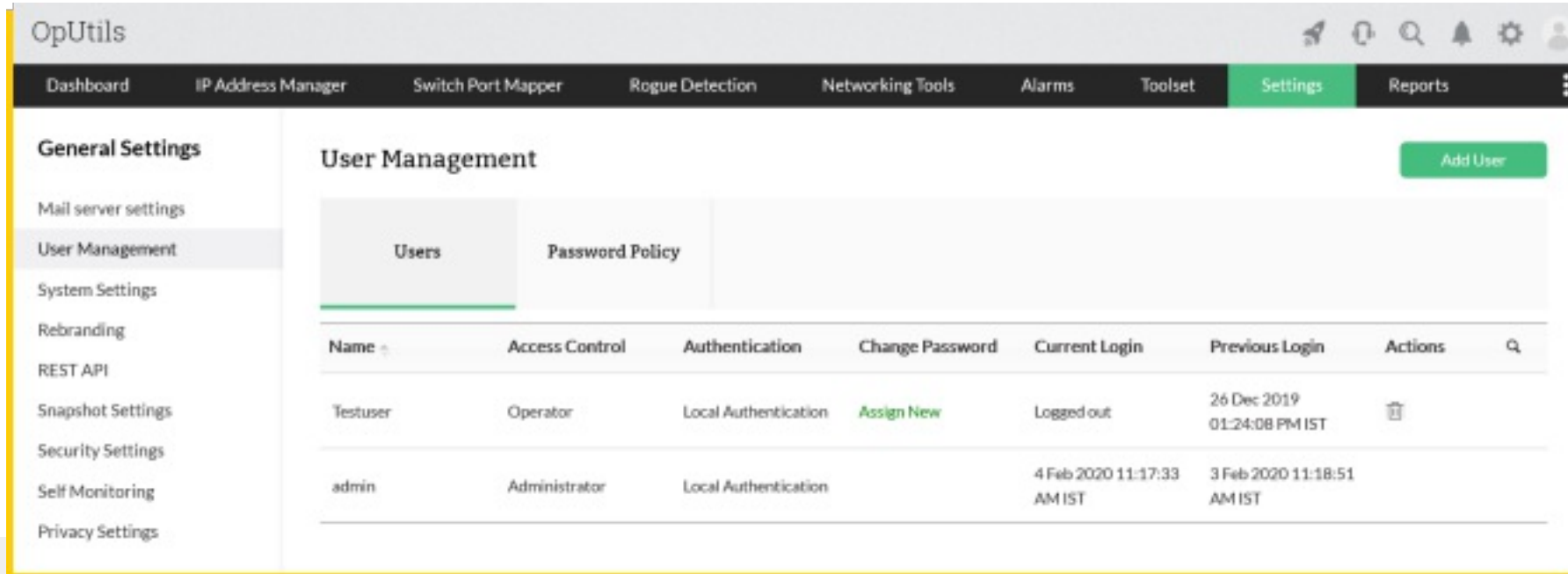
The screenshot shows the 'OpUtils' audit log table. It includes filter options for Tools, Users, Changes, Period, and Action. The table contains five rows of log entries with columns for Tools, Date, User, Action Performed, Changes in, and Description.

Tools	Date	User	Action Performed	Changes in	Description
IP Address Manager	2020-01-03 16:55:30.399	admin	Add	Others	Scheduler 'testcat' has been added. 172.18.305.0 subnet has been moved to this scheduler
Switch Port Mapper	2019-12-27 15:44:08.342	admin	Delete	Others	Scheduler 'Smap' has been deleted and switches (192.168.50.140) in this scheduler has been moved to Default Group
Switch Port Mapper	2019-12-27 15:43:25.843	admin	Add	Others	Scheduler 'Smap' has been added. 192.168.50.140 switch has been moved to this scheduler
Switch Port Mapper	2019-12-27 15:42:43.027	admin	Modify	Others	Scheduler 'Default Group' has been modified
Switch Port Mapper	2019-12-27 15:42:43.958	admin	Modify	Others	Scheduler 'Default Group' has been modified

User management



User management



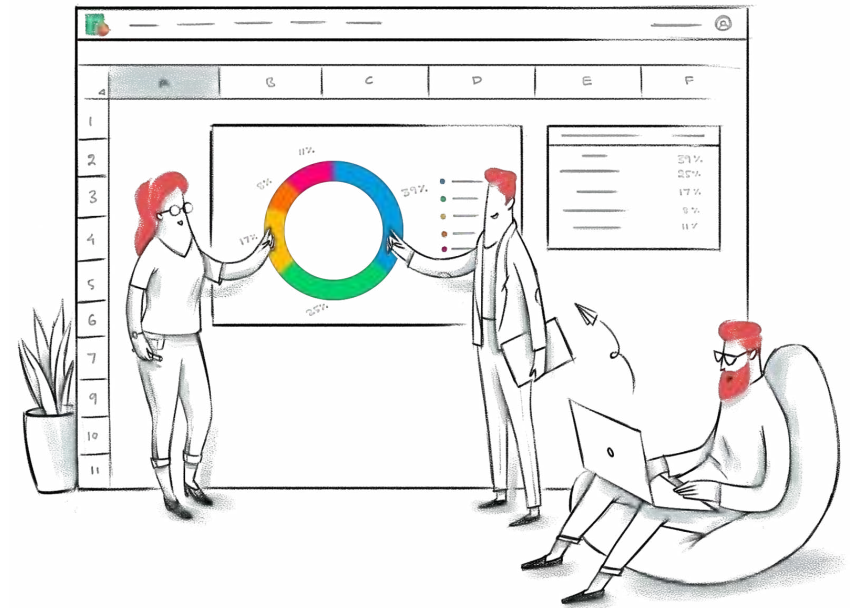
The screenshot displays the OpUtils User Management interface. The top navigation bar includes Dashboard, IP Address Manager, Switch Port Mapper, Rogue Detection, Networking Tools, Alarms, Toolset, Settings (highlighted), and Reports. The left sidebar lists General Settings, Mail server settings, User Management (highlighted), System Settings, Rebranding, REST API, Snapshot Settings, Security Settings, Self Monitoring, and Privacy Settings. The main content area is titled 'User Management' and features an 'Add User' button. Below this, there are two tabs: 'Users' (selected) and 'Password Policy'. The 'Users' tab contains a table with the following data:

Name	Access Control	Authentication	Change Password	Current Login	Previous Login	Actions
Testuser	Operator	Local Authentication	Assign New	Logged out	26 Dec 2019 01:24:08 PM IST	
admin	Administrator	Local Authentication		4 Feb 2020 11:17:33 AM IST	3 Feb 2020 11:18:51 AM IST	

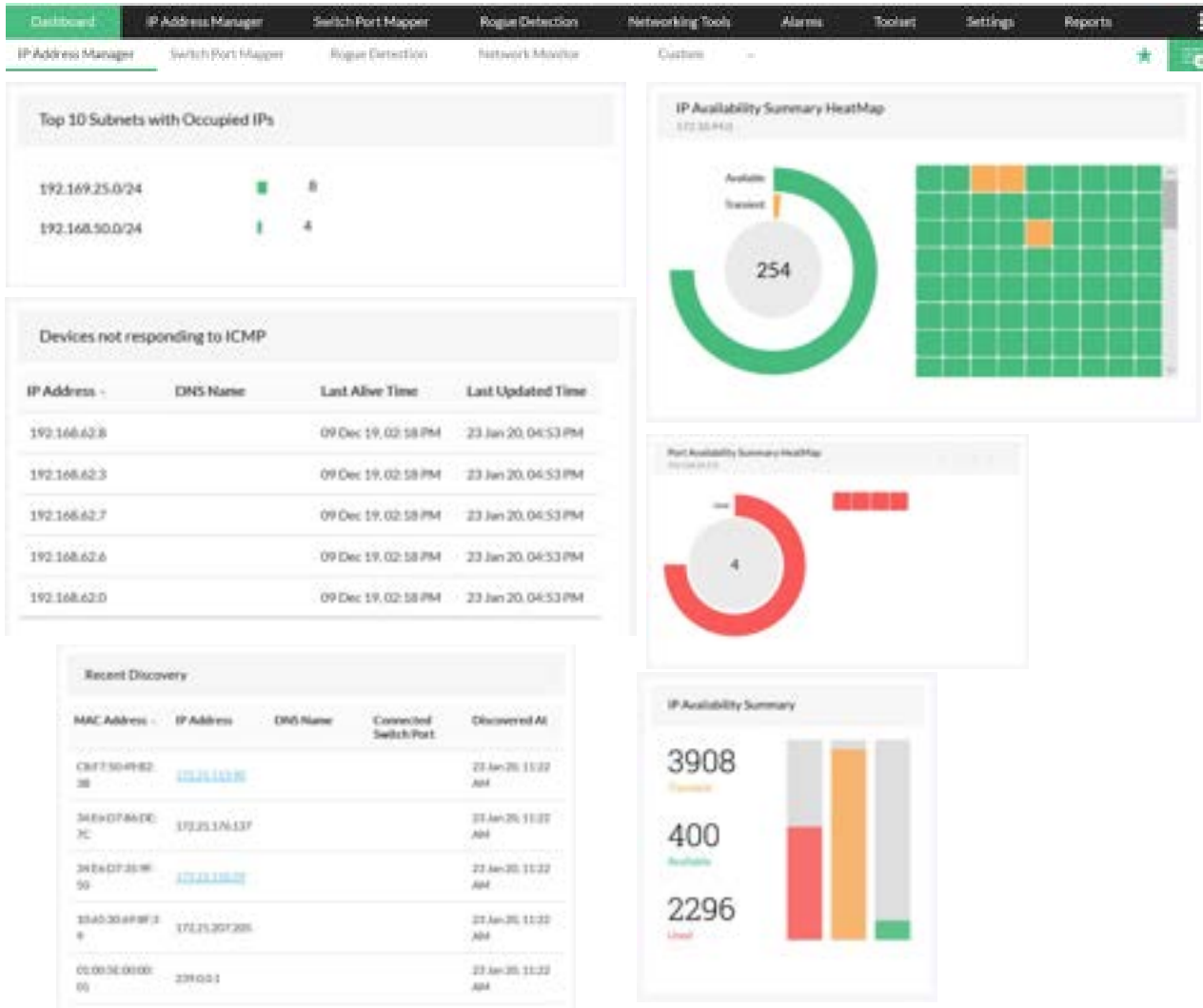
Create multiple user roles along side default administrator and operator roles.

Leverage user scoping capabilities to effectively implement role based access controls (RBAC).

Dashboard and widgets



Dashboard and widgets



- Find out all the operational status of your network with OpUtils' out-of-the-box widgets.
- Create multiple custom dashboards for different users.
- Monitor all the crucial information about your network at a glance.
- Detailed view of the IPs, switch ports and devices in the network.

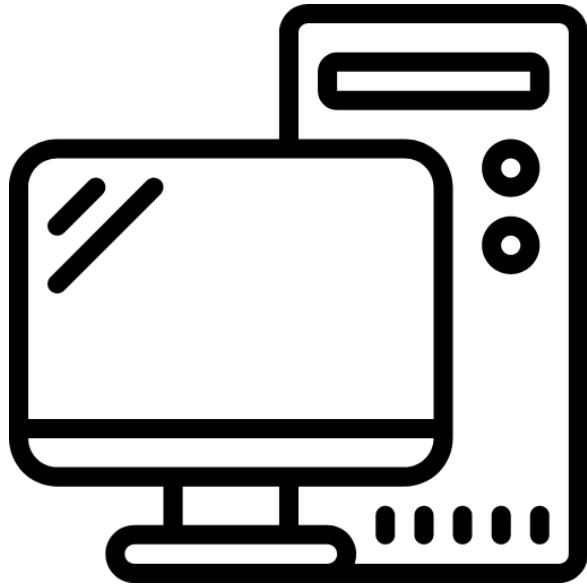
Dashboard and widgets



- Find out all the operational status of your network with OpUtils' out-of-the-box widgets.
- Create multiple custom dashboards for different users.
- Monitor all the crucial information about your network at a glance.
- Detailed view of the IPs, switch ports and devices in the network,.

**What makes OpUtils
standout?**

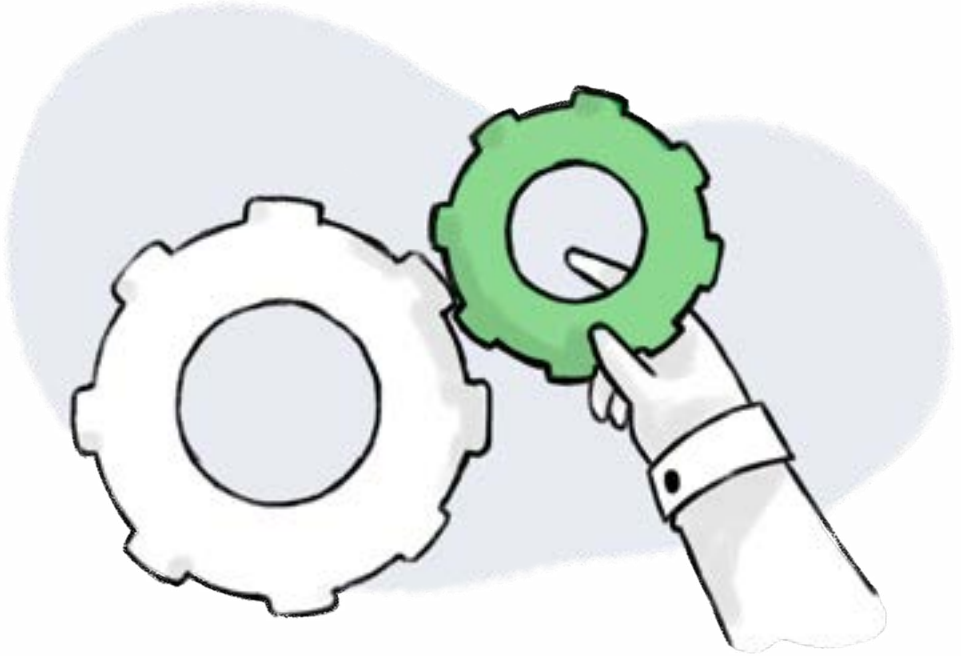




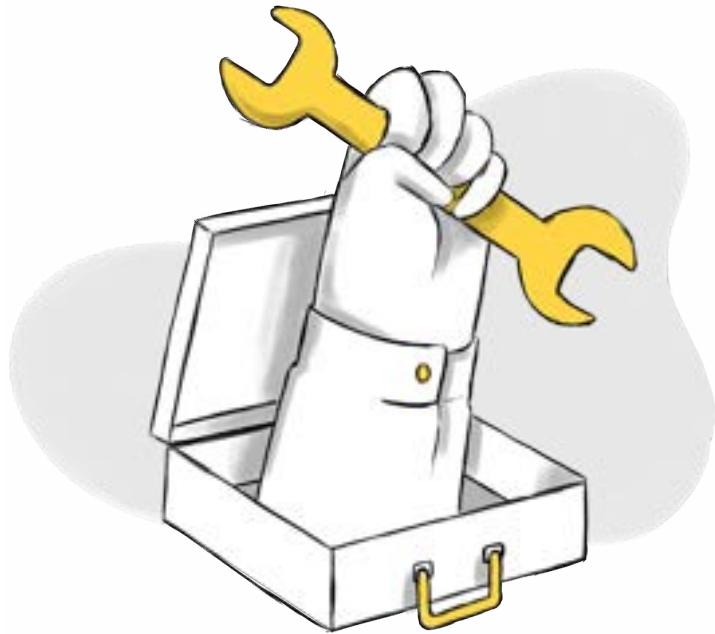
QuickInstallation

InstallOpUtilsin less than 10 minutes.

No additional components required.



**All the tools you'll
ever need!**



No strict defaults! Customize OpUtils as per your IT requirements

- Custom dashboards
- Custom Columns
- Scheduled alerts
- Rebranding option
- Custom NOC views.



All the crucial information at a glance- Visualization

- Easy to use UI
- Graphical depiction of crucial IT metrics
- Top 10 charts.
- All the information you'll ever need is only a few clicks away!



Affordable

Get OpUtils professional edition

starting at **\$345**

Customer Success Story

“OpUtil has provided us a detailed and intuitive interface to easily manage our IP space and switch ports. We can easily find any system on our network through their switch port mapper tool and also quickly identify possible security violations.”

Nichole K. Boscia, CSC

Sr. Network Engineer

NASA Ames Research Center

Advanced Supercomputing Division



Want to know more about OpUtils?



www.oputils.com



https://download.manageengine.com/products/oputils/oputils_brochure.pdf



https://download.manageengine.com/products/oputils/oputils_datasheet.pdf



demo.oputils.com



<https://www.manageengine.com/products/oputils/knowledge-base.html>



<https://pitstop.manageengine.com/portal/community/opmanager/oputils>

THANKYOU

Thankyou

oputils-support@manageengine.com

www.manageengine.com