

# Quick Start Guide

Get started in 5 minutes!

This document will give a brief introduction about the product and its installation procedure.

## INTRODUCTION

The role of a network administrator is to manage all the network resources efficiently. This includes monitoring IP addresses and switch ports, detecting rogue devices, and monitoring the performance of end devices. While it is possible to achieve this with several tools available in the market, an integrated solution is recommended for troubleshooting and correlating data between several tools.

OpUtils is an integrated IP address manager, switch port mapper, and rogue device detection solution that helps network admins to perform their tasks efficiently. It also includes tools for network diagnostics, address monitoring, network monitoring, SNMP monitoring, and Cisco monitoring. The tool kit can be used to:

- Manage and monitor IPv4 and IPv6 addresses, subnets, and supernets in real time.
- Scan IP addresses to determine their availability using an advanced IP scanner.
- Create subnet and switch groups using Tree View to track IP addresses and switch ports hassle-free.
- Seamlessly create and manage IP requests using the IP Request tool..
- Monitor DHCP server scopes and resolve DNS.
- Track history of IP addresses and switch ports, and gain insights into IP-MAC change and device change information in switch ports.
- Create custom fields to identify and manage IP addresses and switches easily.
- Gain visibility and control over your IP addresses, switch ports, and other devices with the Active Directory integration.
- Visualize stacked, trunk switch ports, and devices with virtual IP addresses in switch ports.
- Perform end-to-end scanning and mapping of switch ports and view connected device details.
- Define user roles and scopes for your team members using role-based access control (RBAC).
- Configure alerts to stay ahead of IP and switching issues.

## PRE-INSTALLATION

### Software requirements

These are the minimum requirements to run the system.

Software	Evaluation	Production
OS Windows	Windows 10	Windows Server 2022
	Windows	Windows Server 2019
	Server 2012	Windows Server 2016
		Windows Server 2012 R2
		Windows Server 2012
OS Linux to 20.04	Ubuntu 14	Ubuntu 14 to 20.04
	CentOS 7	Red Hat version 7 to 9.1
	Fedora 31	CentOS Stream 8
	Red Hat 7 to 9.1	CentOS 7
	Opensuse 15	
Browsers	Chrome	Chrome preferred
	Firefox	Firefox
	Edge	Edge
Client machines	OpUtils uses a client-side JavaScript-based MVC architecture and it is preferred to view this from a 64-bit laptop for a better viewing experience.	
User privileges	Local administrative privileges required	

### Bandwidth required for OpUtils scanning

If all the tools are scanning simultaneously, the approximate bandwidth utilization would be ~150KBps.

### Hardware requirements

Hardware	Recommended
Processor	Dual Core/ Core 2 Duo or Quad Core
RAM	4GB
Disk Space	Above 10GB

## INSTALLATION:

ManageEngine OpUtils 12 is available for both Windows (64-bit) and Linux (64-bit) and is available in Free and Professional Editions.

- The Free Edition has 17 tools, and it is absolutely free of cost. Important tools included in the Free Edition are Ping, SNMP Ping, MAC Address Resolver, DNS Resolver, Proxy Ping, TCP Reset, and most of the SNMP tools (Community Checker, SNMP Graph, MIB Node Viewer, and MIB Module Viewer).
- The Professional Edition includes all the 34 tools, such as Switch Port Mapper, IP Address Manager, Rogue Detection, and Cisco Tools (Config File Manager, IOS, Flash, IP Routes, Device Monitor, Interfaces, etc.).

## INSTALLING OPUTILS ON WINDOWS

### Steps to install:

1. Download OpUtils from <https://www.manageengine.com/products/oputils/download-free.html>.
2. Execute the downloaded OpUtils.exe to install and follow the instructions in the installation wizard.
3. Click **Next** to begin the installation process. Go through the license agreement and click Yes to proceed to the next step.
4. In the subsequent steps of the wizard, select the OpUtils Edition (30-day trial or Free), the language, and the directory to install OpUtils. Proceed to the next step.
5. Select the Program folder to add the OpUtils shortcuts and click **Next**.
6. Specify the port number to run OpUtils Web Server and click **Next**.
7. Register for technical support by supplying your contact information such as name, email, etc.
8. Verify the installation details and click **Next**.
9. Select the database, then click **Next**. OpUtils supports both PostgreSQL and MSSQL as databases.
10. Click **Finish** to complete the installation process.

## INSTALLING OPUTILS ON LINUX

### Steps to install:

1. Download OpUtils from <https://www.manageengine.com/products/oputils/download-free.html>.
2. Login as root user.
3. Assign the executable permission to the downloaded file using the following command:  
`chmod a+x OpUtils.bin`
4. Execute `./OpUtils.bin` then the installation wizard will pop up.
5. Click **Next** to begin the installation process. Go through the license agreement and proceed to the next step.
6. In the subsequent steps of the wizard, select the OpUtils Edition (Professional or Free), the language, the directory to install OpUtils, and the port number to run OpUtils Web Server. Proceed to the next step.
7. Verify the installation details and click **Next**. Click **Finish** to complete the installation process.

### Note:

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

## POST-INSTALLATION:

### Steps 1:

### ACCESSING OPUTILS:

Default Login Credentials

Username: admin

Password: admin

### Note:

The username and password can be modified later

### Steps 2:

## DISCOVERY:

### IP Address Manager (IPAM)

IPv4 and IPv6 subnets can be added in IP Address Manager both manually and by importing a CSV file. IP Address Manager helps manage and monitor your entire IP address space. Create subnet

groups to add all the subnets based on their usage/location and scan them to get the status of all the IP addresses. Add and monitor supernets, DHCP server scopes, and IPv6 hosts.

## **IP Address Manager > Add > Add IPv4 Subnet / Add Supernet / Add DHCP Server / Add IPv6 Subnet/Site**

### **Switch Port Mapper (SPM)**

The Switch Port Mapper module of OpUtils discovers the devices plugged into each port of a specified switch. The tool is useful for system and network engineers to gain visibility into the IP-MAC status, and availability of switch ports. Since this is real-time discovery you can also view the operational status, port speed, VLAN name, vendor, and connectivity details.

Sub-step 1: Credentials must be added in SPM based on SNMP (v1/v2) and SNMP v3, which helps in the discovery of switches.

## **Switch Port Mapper > Add > Add Switch > Add Credential**

### **Note:**

SNMP v1/v2 requires only the community. However, SNMP V3 requires a username and password

Sub-step 2: Switches can be added in SPM manually by importing a CSV file, or it can be added by discovery of multiple switches.

## **Switch Port Mapper > Add > Add Switch**

### **Rogue device detection**

OpUtils' Rogue Detection feature detects which devices have unauthorized access of your network resources. This is accomplished with the help of the Active Directory integration. Trusted devices' MAC addresses can be imported as a CSV file in OpUtils. OpUtils periodically scans the subnets, switches, gateway servers, and routers to map the MAC-IP data. Whenever a new MAC address is detected in the network, it gets added in the console. The imported MAC address will automatically take the role of a trusted device.

## **Rouge Detection > Import MAC Address Details**

### **Routers**

Discover your routers into OpUtils and start monitoring the router's ARP table entries.

View the collection of MAC-IP data of the network resources by adding routers. The data collected is used in generating the reports and in the tools that use the MAC-IP data.

## **Settings > OpUtils > Routers > Add device**

### Steps 3:

## ADDING SERVERS:

Inclusion of servers and Active Directory is a step that provides greater reliability in monitoring of devices.

### DHCP servers (Microsoft DHCP server, Palo Alto Firewall, Linux Server, Cisco Router, Fortinet Firewall)

OpUtils lets you monitor your DHCP servers to get the list of DHCP Scopes (leased/available IP addresses) in each scope. When you add a DHCP server, it gets scanned automatically to fetch the details. For the data to be accurate and up to date, it is necessary to scan them periodically.

### IP Address Manager > Add > Add DHCP Server

### DNS servers

The most basic function of a DNS server is to translate a domain name into its respective IP address. In other words, DNS servers play a very important role in resolving the DNS name of the IP addresses. DNS servers run special software and communicate with each other using special protocols.

### Settings > OpUtils > IPAM > General > DNS Server Name

### Active Directory

OpUtils is the management interface for IP addresses, switch ports, and rogue device detection. It stores more sensitive information like SNMP read-write community of the switches and routers, which you cannot afford to get hacked. Discover Active Directory in OpUtils to identify trusted devices and weed out unwanted connections.

### Settings > OpUtils > Active Directory > Add AD domain

### Steps 4:

## PERIODIC SCANNING AND EMAIL ALERTS:

Schedule scans and configure alerts for IP Address Manager, Switch Port Mapper, and Rogue Detection. Scan schedules to monitor your IP addresses, switch ports, Active Directory, routers, and DHCP servers. Schedule Wake on LAN to wake up devices periodically. Configure alerts to stay ahead of IP conflicts, switching issues, and ARP spoofing.

### Settings > OpUtils > Scheduler

### Settings > IP Address Manager > Configure Alerts

### Settings > Switch Port Mapper > Configure Alerts

### Note:

You can configure alerts to receive them via email or syslogs.

## Steps 5:

### REPORT GENERATION:

Once OpUtils is configured after all the procedures, it will start to generate reports based on factors like:

- Unused IP addresses
- Reserved Static IP address
- IP Usage Summary
- OS Type Reports
- DHCP Reserved IP Addresses
- Switches by Usage
- Switches by Schedule
- Switches by vendor name
- Switch ports by ifspeed
- Switch ports by iftype
- Device with virtual IP
- Stacked Port details
- Administratively disabled ports
- Port by Operation Status Last Change Time
- Connected IP details
- IP request

### Note:

You can also schedule reports and see who is making what changes in the OpUtils console with Audit.

***Login the ManageEngine web client to view OpUtils Reports.***

**Support:** [oputils-support@manageengine.com](mailto:oputils-support@manageengine.com)

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

**Help Document:** <http://help.oputils.com/>

**Request a Free Demo:** <https://www.manageengine.com/products/oputils/request-demo.html>

**Live Online demo:** <http://demo.oputils.com/>