

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. The administrator has to monitor the health and availability of the devices, check for disk space in critical servers, backup the configuration of routers/switches, monitor the bandwidth, restrict unauthorized network access, identify the devices connected to switch ports, and more. While it is possible to achieve this with several tools available in the market, an integrated solution is the need of the hour when it comes to troubleshooting and correlating data between several tools.

OpUtils with its integrated set of network monitoring tools helps them to perform these tasks efficiently. It includes tools for Network Diagnostics, Address Monitoring, Network Monitoring, SNMP Monitoring, Server Monitoring, and Cisco Monitoring. The tool kit can be used for

- To check the IP Availability using ICMP and to resolve the DNS name of the IP.
- To get the device details using SNMP and to get the device type and hardware details of Windows machines using WMI.
- Troubleshooting connectivity issues in a LAN environment.
- Monitoring the performance, bandwidth and traffic statistics of routers, switches and other networking resources.
- Providing information on IP Addresses, MAC Addresses and DNS names.
- Tracking Desktop information such as system configuration, resource usage and software listing.
- Monitoring Cisco devices and maintaining the devices in good condition
- Browsing MIB's and viewing configured Traps.
- Monitors DHCP Servers(supports only Microsoft) to get the list of DHCP Scopes and the leased/available IP Addresses in each scope.

PRE – INSTALLATION

Software requirements

These are the minimum requirements to run the system.

Software	Evaluation	Production
OS Windows	Windows 10 Windows 8 Windows 7 Windows Vista Also works with, Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 Windows Server 2003 Windows Server 2000	Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 Windows Server 2003 Windows Server 2000
OS Linux	Ubuntu Debian Suse Red Hat Fedora Mandrake	64bit Linux flavors
Browsers	Chorme latest Firefox latest IE 11 Edge Note: Do not enable Enterprise Mode Option in Internet Explorer. This will make Internet Explorer work as version7. this not supported.	Chrome preferred
Client machines	OPManager uses a client side javascript based MVC architecture and it is preferred to view this from a 64 bit laptop for 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 ~150 KBps

Note :

This includes scanning of Switches/Routers ARP tables, IPAM and Bandwidth Monitoring

Hardware Requirements

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

INSTALLATION:

ManageEngine OpUtils12 is available for both windows (32 bit/64 bit) and Linux (32 bit/64 bit) version. ManageEngine OpUtils is available in Free, and Professional Editions.

- The Free Edition has 17 tools, and it is absolutely free of cost. Important tools 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, which includes 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 for Windows](#).
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 (30day trial or Free), 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 id etc.
8. Verify the installation details and click Next.
9. Select the database. OpUtils supports both, PostgreSQL and MSSQL as database and click Next.
10. Click Finish to complete the installation process.

INSTALLING OPUTILS ON LINUX

Steps to install:

1. Download [OpUtils for Linux](#).
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`. The installation wizard pops 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), 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.

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)

Subnets can be added in IPAM both manually and by importing a CSV file. IP Address Management tool helps to keep track of all the IP addresses. It defines a group to add all the subnets based on their usage/location and then scan them to get the current status of each of the IP Addresses.

ManageEngine OpUtils login > Inventory > Subnet/IP address > Add subnet

Switch Port Mapper (SPM)

The Switch Port Mapper utility of OpUtils software 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 ports. Since this is a real-time discovery you can also view the operational status and port speed of each port.

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

ManageEngine OpUtils login > Inventory > Switches/Ports > Add credentials

Note :

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

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

ManageEngine OpUtils login > Inventory > Switches/Ports > Add/Discover Switches

Rogue Device Detection

Rogue Detection is a tool to detect unauthorized access of your network resources. MAC addresses can be imported as CSV file in OpUtils. OpUtils periodically scans the subnets, switches, gateway servers, and routers to collect the MAC IP data. Whenever a new MAC address is detected in the network, it gets added here. The imported MAC address will automatically take the role of a trusted device.

ManageEngine OpUtils login > Inventory > Rogue > Import MAC address details

Routers

The Add Routers screen lets you specify the routers, switches, and gateway servers in your network and schedule scanning. OpUtils, based on the scheduler details, scans the devices to collect the

MAC IP data of the network devices. The data collected is used in arriving the reports and in the tools that uses the MAC IP data. Routers can be added in OpUtils which are Layer 3 Devices that includes switches, gateways, firewalls and printer

ManageEngine OpUtils login > Settings > OpUtils > Routers > Add device

Bandwidth Monitor (BWM)

Bandwidth Monitor tool of OpUtils software provides a real-time network traffic of any SNMP device. It uses SNMP to fetch the bandwidth utilization details of a network interface. The bandwidth utilization of the device displays a comparison of the individual traffic of its interfaces.

ManageEngine OpUtils login > Inventory > BWM > Discover Interfaces

Steps 3:

ADDING SERVERS:

Inclusion of servers and active directory is a step that provides greater reliability in monitoring of devices.

DHCP servers (supports only Microsoft)

OpUtils lets you monitor your DHCP Servers to get the list of DHCP Scopes and the 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.

ManageEngine OpUtils login > Inventory > DHCP > 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 server play a very important role in resolving DNS name of the IP addresses. DNS servers run special software and communicate with each other using special protocols.

ManageEngine OpUtils login > Settings > OpUtils > IPAM > General

Active Directory

OpUtils Web Console is the management interface for various activities like IP Address Management, Switch Port Mapping, etc. It stores more sensitive information like SNMP Write Community of the switches and routers, which you cannot afford to get hacked.

ManageEngine OpUtils login > Settings > OpUtils > Active Directory > Add AD domain

Steps 4:

PERIODICAL SCANNING AND EMAIL ALERT:

IP Address Manager, Switch port mapper, Config file Manager(CFM) and DHCP can create scan profile in order to scan intermittently based on the profile created by the user.

ManageEngine OpUtils login > Settings > OpUtils > IPAM/SPM/DHCP/CFM > Scheduler

MAC - to - IP mapping can also create scan profile in order to scan intermittently based on the profile created by the user.

ManageEngine OpUtils login > Settings > OpUtils > Routers > Scheduler

Note :

Active directory and MAC-to-IP mapping have option to create a scan profile as well as scan individual IP's.

IP Address Manager, Switch port mapper, Rogue, Ping, Bandwidth monitor and DHCP can create alert rule in order to alert the user through emails at necessary conditions.

**ManageEngine OpUtils login > Settings > OpUtils > IPAM/SPM/BWM/Ping/Rogue/DHCP
> Configure Alerts / Alert rule / via email**

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
- ◆ Switches by Usage
- ◆ Switches by Schedule
- ◆ Switches by vendor name
- ◆ Switchports by ifspeed
- ◆ Switchports by iftype
- ◆ Device with virtual IP
- ◆ Stack Port details
- ◆ Administratively disabled ports.
- ◆ Port by Operation Status Last Change Time
- ◆ DHCP reserved IP addresses
- ◆ DHCP leased IP Addresses

ManageEngine OpUtils login > Reports

Login the ManageEngine web client to view OpUtils Reports.

Support: 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/> | **OpUtils Technical Overview Presentation:** <https://www.slideshare.net/opmanagerteam/manageengine-oputils-technical-overview>