

OpManager

Best practices guide



Table of Contents

INTRODUCTION	5
LATEST VERSION	6
HARDWARE & SOFTWARE REQUIREMENTS	6
HARDWARE REQUIREMENTS	6
SOFTWARE REQUIREMENTS	7
CONFIGURING OPMANAGER FOR PERFORMANCE	7
DISCOVERY CONFIGURATION	7
PRE-REQUISITES FOR NETWORK DISCOVERY	7
DISCOVER ADD-ON DEVICES	7
<i>a. Enable dedicated 'add-on devices' inventory page</i>	<i>7</i>
<i>b. Push devices to their respective modules when added to OpManager</i>	<i>8</i>
DISCOVERY CRITERIA	8
DISCOVERY FILTER	8
LOGICAL GROUPING	8
SCHEDULE DISCOVERY	8
DISCOVERY RULE ENGINE	9
INTERFACE DISCOVERY	9
LAYER 2 MAP BASED DISCOVERY	9
DEVICE/INTERFACE REDISCOVERY PROPERTIES	9
<i>a. Interface property update scheduler</i>	<i>9</i>
<i>b. Device property update</i>	<i>10</i>
VISUALIZATION FEATURES FOR ENHANCED VISIBILITY	11
BUSINESS VIEW	11

LAYER 2 MAPS_____	11
GOOGLE/ZOHO MAPS_____	12
RACK AND FLOOR VIEW_____	12
DASHBOARD AND NOC VIEW_____	12
MONITORING & DATA-COLLECTION CONFIGURATION_____	12
AVAILABILITY MONITORING_____	12
<i>Device Availability Monitoring Protocol Preference_____</i>	<i>12</i>
<i>Ping preference_____</i>	<i>12</i>
<i>Configuring Ping Parameters_____</i>	<i>12</i>
<i>Disabling Unnecessary Polling During scheduled maintenance_____</i>	<i>13</i>
<i>Device Dependencies_____</i>	<i>13</i>
<i>Monitoring Intervals_____</i>	<i>13</i>
<i>a. Specifying Polling Intervals for Devices_____</i>	<i>13</i>
<i>b. Disabling status polling_____</i>	<i>14</i>
Disabling polling for a device category_____	14
Disable status polling for an interface status_____	14
<i>c. Configuring java heap size_____</i>	<i>14</i>
DATA COLLECTION_____	14
SNMP Data-collection_____	14
WMI Data-collection_____	15
ADDRESSING TIMEOUT ISSUE_____	15
DATABASE CONNECTION POOL_____	16
THRESHOLD SETTINGS_____	16
<i>Specifying Monitoring Intervals for Performance Monitors (CPU, Memory, Disk etc.)_____</i>	<i>17</i>
<i>Specifying Monitoring Intervals for Services (MS SQL, MS Exchange, Telnet etc.)_____</i>	<i>17</i>

IMPLEMENTATION AND PRODUCT STARTUP	17
<i>Security and Authentication Installing and Starting</i>	17
<i>Enabling SSL</i>	17
<i>Securing Admin Account</i>	18
<i>Restricting Users Scope</i>	18
<i>Proxy-settings</i>	18
ALERTING	18
a. <i>SNMP Traps</i>	18
b. <i>Notification Profiles</i>	18
DATABASE TUNING	18
CONFIGURING REMOTE PGSQL PARAMETERS	19
CONFIGURING MSSQL PARAMETERS	19
DISTRIBUTING DATABASE FOR SCALABILITY	19
INCREASING JAVA HEAP SIZE	19
DATABASE MAINTENANCE	19
INTUITIVE REPORTS	20

Introduction

Manageengine OpManager is a network monitoring & management solution that helps monitor your network in a seamless and robust manner. OpManager allows you to monitor various types of network devices such as routers, switches, servers, virtual machines, storage devices etc. and also provides alerts / notifications whenever the devices in your network crosses pre-defined threshold values. This helps avert any network disasters that may otherwise cost your business.

This document lists the best practices for installing and running OpManager to help you get the most out of your network monitoring solution. For further assistance, please feel free to drop an email to opmanager-support@manageengine.com - our support personnel will be more than happy to assist you.

Latest version

The latest version of OpManager (at the time of writing this document (May 2023)) is v12.6. You can download the professional / enterprise edition from [here](#).

Hardware & Software Requirements

The following are the minimum hardware & software requirements that are essential for optimal running of OpManager. Please note that these requirements may increase / decrease based on your network size and usage.

Hardware requirements

Hardware Requirements				
OpManager Standard / Professional	No. of devices	Processor	Memory	Hard Disk
	1 to 250	Intel Xeon 2.0 Ghz 4 Cores/ 4 Threads	4 GB	20 GB minimum
	251 to 500	Intel Xeon 2..5 Ghz 4 Cores/ 8 Threads	8 GB	20 GB minimum
	501 to 1000	Intel Xeon 2..5 Ghz 4 Cores/ 8 Threads or higher	16 GB	40 GB minimum
For add-ons, the memory & hard disk size will increase. A minimum of 40 GB will be required for installing OpManager with add-ons.				
Enterprise edition (Central server)	1000+	Intel Xeon 3.5 Ghz 4 cores/ 8 threads or higher CPUs with a total combined	16 GB or higher	100 GB minimum
Enterprise edition (Probe server)		PassMark score of 7,000 or higher		40 GB minimum

Software requirements

Software	Minimum versions required for evaluation	Version requirements for production
Windows OS	Windows 10 (OR) Windows Server 2012	Windows Server 2022/ 2019/ 2016/ 2012 R2/ 2012
Linux OS	Ubuntu 14 to 20.04/ Cent OS 7/ Fedora 31/ Red Hat 7 to 9.1/ Opensuse 15	Ubuntu 14 to 20.04/ Red Hat version 7 to 9.1/ Opensuse 15/ CentOS Stream 8/ CentOS 7
Browsers	Chrome/ Firefox/ Edge	Chrome(preferred)/ Firefox/ Edge

Configuring OpManager for Performance

Certain parameters can be fine-tuned depending on the environment. While most configurations are exposed via the user interface, few other changes are effected in the configuration files and some database tables manually. Module-wise configurations and recommended values are listed below:

Discovery Configuration

Pre-requisites for Network Discovery

OpManager relies on communication protocols such as SNMP (v1/v2,v3), SSH, CLI, WMI, VMware, Citrix, Nutanix, UCS, and SMI or NetApp for classification and monitoring. So make sure the following configurations are completed before triggering discovery.

- Configure the relevant credentials.
- Define [Device Templates and monitors](#). If your device type is not found in the [supported devices list](#), please reachout to our [support](#).
- Configure [mail server](#) in case of emailing discovery reports.

Note:

- Avoid adding unnecessary monitors to the devices to improve their monitoring efficiency
- Add devices from their dedicated Discovery option. (applicable to Virtual devices, Nutanix, UCS, WLC, Storage)

Discover Add-on Devices

a. Enable dedicated 'add-on devices' inventory page

An add-on is an additional module that enhances OpManager's capabilities by expanding its

scope beyond network monitoring, by offering comprehensive IT management features such as bandwidth and flow monitoring, IP address and switch port management, configuration and change management, and firewall and log management. The add-ons come bundled within the product and do not require any separate installation, but just the suitable licenses for activation.

Devices discovered in OpManager's add-on modules will be added to inventory and listed as 'Unmanaged devices'. This can be prevented by configuring these devices to be listed under "[Discover Add-on Devices page](#)" under Quick Configuration Wizard. To configure this, follow the below steps

1. Stop the OpManager service.
2. Open the **discovery.properties** file from `\conf\OpManager`.
3. Set the value of **DISCOVER_EXTERNAL_NODE** as 'true' and save the file.
4. Start the OpManager service.

b. Push devices to their respective modules when added to OpManager

Devices added to OpManager can be directly pushed to their respective modules. Enable this option from Discovery > Discovery settings > Add to NCM/IPAM

Discovery Criteria

OpManager relies on ICMP/NMap protocol to discover devices and SNMP protocol to discover interfaces. [Device discovery](#) can be performed from one of the multiple discovery criteria such as Device Name/IP, IP Range, CIDR, and CSV File Import. Hasten discovery process by choosing the discovery format that best suits your requirement.

Discovery Filter

During discovery, reduce time consumed by choosing to add or ignore specific devices using the [Discovery filters](#) option.

Logical Grouping

[Create groups](#) to push bulky configurations, set filters in Reports, Widget, Notification Profile, URL Templates, Downtime schedule, Alarm suppression, Device template, Interface template, Test credentials and Workflow.

Note: Business Views can also be treated as a Logical Group and used as a filter, Dashboard and NOC options.

Schedule Discovery

Run [Scheduled Discovery](#) to periodically update your devices and interfaces. Select

rediscovery rule options to customize OpManager's behaviour when a device/interface is newly added or removed.

Discovery Rule Engine

OpManager helps reduce post discovery manual efforts with [Discovery Rule Engine](#). It can be used to configuring activities such as adding monitors, adding devices to business view, associate event log rule, associate notification profile to devices upon successful discovery.

Steps:

- Create new rule from Settings > Discovery > Discovery Rule Engine.
- Select required rule during 'Rules' stage of Discovery process.

Interface Discovery

OpManager allows you to [directly discover interfaces](#) and their properties in bulk by specifying the criteria and condition for devices and their associated interfaces. Go to Settings > Discovery > Interface Discovery. **Note:**

- This is available only on OpManager v12.5.174 and above.
- Using the new interface discovery, discover only the interfaces that you want to monitor and ignore the rest.
- SNMP credential is mandatory to discover interfaces.

Layer 2 Map based Discovery

If the IP range of devices in the network is unknown, Discovery can be initiated with [Layer 2 Maps](#). By using the seed router as reference. OpManager discovers all the devices connected to the seed router and creates a topology Map.

Device/Interface rediscovery properties

a. Interface property update scheduler

Automatically [update Interface properties](#) mentioned in the table by running a scheduler. Please contact our [support team](#) for further assistance on enabling this option and its properties.

Note: Available for versions 12.4.162 and above

Property	Description	Default value
MONITORINGINTERVAL	Period at which the scheduler updates the interface properties.	86400
IFALIAS	An 'alias' name for the interface as specified by the network manager.	TRUE

IFDESCRIPTION	A textual string containing the product name, manufacturer name, and the version of the interface hardware/software.	TRUE
IFNAME	Holds the name of the interface as assigned by the local device	TRUE
DISPLAYNAME	Display name of the interface as shown in the Interface Snapshot page	TRUE
ADMINSTATUS	Admin status (ifAdminStatus) of the interface.	FALSE
OPERATINGSTATUS	The current operational state (ifOperStatus) of the interface.	FALSE
PHYSMEDIA	This variable states the type of this interface as reported by the SNMP agent.	FALSE
HCTTRAFFIC	Enable/Disable the 64-bit Traffic counter.	TRUE
PHYSADDRESS	Represents the media or physical-level address.	FALSE
IPADDRESS	Represents the IP address of the interface.	TRUE
IFSPEED	An estimate of the interface's current bandwidth in bits per second.	FALSE
IFSPEEDIN	The 'In Speed' (Bandwidth) of the Interface.	FALSE
IFSPEEDOUT	The 'Out Speed' (Bandwidth) of the Interface.	FALSE

b. Device property update

When device rediscovery is performed, all parameters are rediscovered. However, certain properties (Device type, Display name, Harddisk size) will not change frequently. So when device rediscovery is performed, you can choose to skip updating said parameters.

Update REDISCOVERYPROPERTIES set PROPVAL = 'true / false' where PROPNAME = <PropertyName>;

PROPNAME	PROPVAL
DEVICETYPE	True
DISPLAYNAME	True
DNSNAME	True
HARDDISKSIZE	True
HARDWAREDETAILS	True
IPADDRESS	True
RAMSIZE	True

Note: All values are set to True by default

Visualization features for enhanced visibility

Visual representation of topology, device dependencies, and network connections help quickly identify health and performance issues. List of visualization features of OpManager are listed below.

Business view

OpManager allows you to [create custom graphical representation](#) of the devices according to the businesses they are catering to. Go to Maps > Business View > Create New. When creating new business views or [infrastructure views](#), it is recommended that Business view names are created without special characters like \$, # etc.

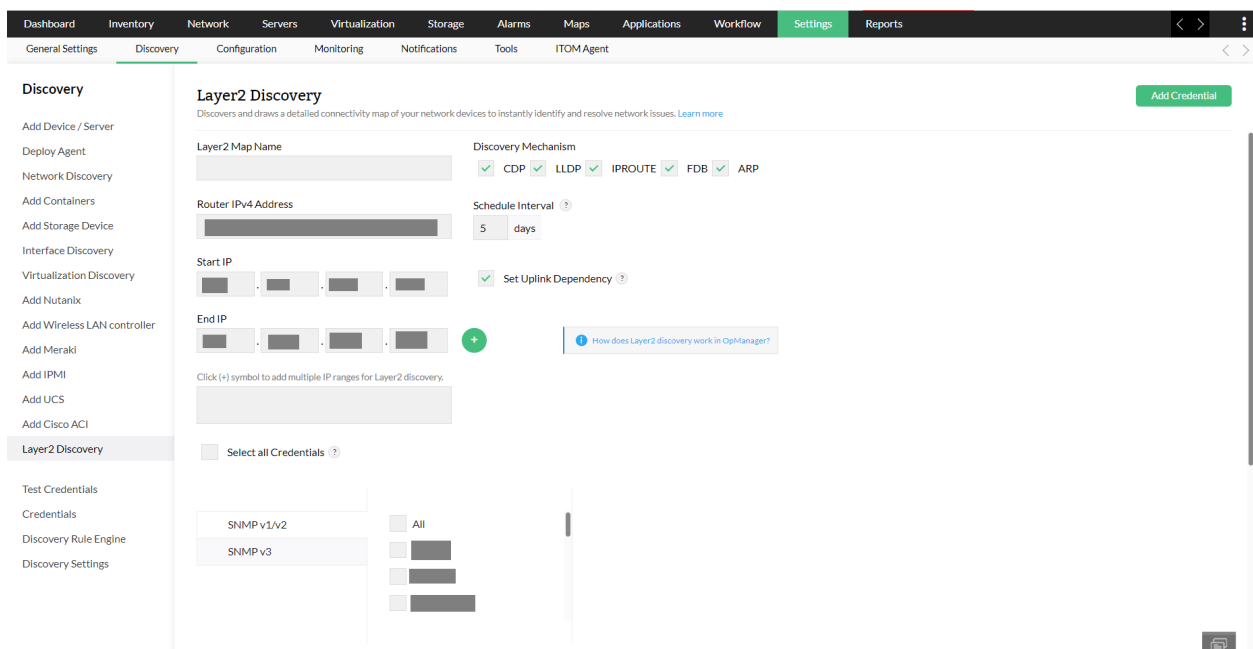
Business views are created to logically group devices such as based on geography, or for assigning to a particular operator/technician. Infrastructure views are created to group devices of a new category, which cannot be ideally classified into the existing infrastructure views.

Example: Environment Sensors, IPPhones etc.

Layer 2 Maps

Layer 2 Maps can be used to draw a [visual representation](#) of the live information of all the devices connected to your seed router. Furthermore, you can [configure the uplink dependencies](#), to optimize the number of alerts. By configuring uplink dependencies, if the seed router is down, the alerts raised for the subsequent child devices will be muted.

Note: Make use of Layer 2 Maps' periodic rediscovery option, to keep your topology map updated.



The screenshot shows the 'Layer2 Discovery' configuration page in the OpManager interface. The page is divided into a left sidebar with navigation links and a main configuration area. The sidebar includes links for 'Discovery', 'Add Device / Server', 'Deploy Agent', 'Network Discovery', 'Add Containers', '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', 'Credentials', 'Discovery Rule Engine', and 'Discovery Settings'. The main configuration area is titled 'Layer2 Discovery' and includes a description: 'Discovers and draws a detailed connectivity map of your network devices to instantly identify and resolve network issues. [Learn more](#)'. It features several input fields and checkboxes: 'Layer2 Map Name' (text input), 'Discovery Mechanism' (checkboxes for CDP, LLDP, IPROUTE, FDB, ARP, all checked), 'Router IPv4 Address' (text input), 'Schedule Interval' (5 days), 'Start IP' and 'End IP' (IP address inputs), 'Set Uplink Dependency' (checked), and 'Select all Credentials' (checkbox). At the bottom, there are sections for 'SNMP v1/v2' and 'SNMP v3' with corresponding checkboxes.

Google/Zoho Maps

OpManager allows both [Google Maps](#) and the free version [Zoho Maps](#) on which you can place your device for better distributed monitoring.

Rack and floor view

Create a [visual representation of your datacenter](#) and monitor their health and availability round the clock.

Dashboard and NOC view

Gain real-time holistic picture of your network devices by placing them on [custom Dashboards](#) and [NOC view](#) and share it with your network management team for quicker issue identification and troubleshooting.

Note: Avoid adding too many real-time widgets. Set their monitoring interval to 5 seconds and above to increase dashboard performance.

Monitoring & Data-collection Configuration:

Availability Monitoring:

Device Availability Monitoring Protocol Preference

OpManager performs availability of devices by using three different protocols - ICMP(default), TCP, and SNMP. If you are present in a ["demilitarised"] zone where ICMP is prohibited, device availability monitoring protocol can be changed to TCP for devices in bulk from Inventory >

Select devices > Menu > monitor via TCP.

Note: SNMP protocol based device availability monitoring can only be configured from individual device snapshot page.

Ping preference

Choose ping preference between Static/Dynamic IP, from Settings > Monitoring > Monitor Settings > Poll Using.

Configuring Ping Parameters

OpManager pings the devices for discovery and further for determining availability, and 4 ping packets are sent by default. If there is network latency, it is possible that some devices are not discovered, or post discovery, they are not polled for status. This can be addressed by configuring few ping parameters.

Steps:

- From /opmanager/conf folder open the file ping.properties.

- Specify the successCount and failureCount. Maximum allowed is 4.
- Uncomment (remove the # symbol) against the timeout parameter and specify the ping timeout depending on the latency.
- Save the changes to the file.
- OpManager service requires a restart when changes are made to this file. So, restart OpManager for the changes to be effected.

Note: The above configuration is recommended only if there is latency. Reducing the number of ping packets will positively impact OpManager's performance.

Disabling Unnecessary Polling During scheduled maintenance

Whenever a maintenance is scheduled in the network for some devices, you can suspend polling for those devices by [scheduling downtime in OpManager](#). This prevents unnecessary requests to network resources resulting in false alerts. There will be improved performance as the devices covered in the scheduled do not use the data poll threads.

Device Dependencies

False alerts are triggered when a set of monitored devices are behind another device (a firewall, router etc). The requests sent to the devices are routed through the firewall or router, and in the event of these dependent devices being down, all devices behind this dependent devices are deemed as down.

[Configuring device dependencies](#) will prevent unnecessary polling to the devices behind the dependent device. (Benefit - prevents a lot of alerts from getting triggered) However, kindly make sure that there aren't any loops while configuring the device dependencies.

Monitoring Intervals

OpManager allows you to set different monitoring intervals for different categories. You can also disable polling for a device category like say, Desktops. Monitoring intervals can be varied for individual devices too.

a. Specifying Polling Intervals for Devices

From Settings > Configuration > Quick Configuration Wizard > Monitoring Intervals, configure a smaller [monitoring interval](#) for critical categories like servers or routers and space out for the other categories like printers etc. The recommended interval for very critical devices is 5 minutes, while you can set a minimum of 1 minute interval also for a very few devices.

In case the polling load is high, kindly check the response time of the particular device. If the response time is too high, kindly check the reason for latency.

b. Disabling status polling:

Disable status polling on the devices and interfaces that are not currently being operational.

Disabling polling for a device category

From Settings > Configuration > Quick Configuration Wizard > Monitoring Intervals, remove selection for the category for which you want to [disable polling](#).

Disable status polling for an interface status

Interface polling can be [disabled both locally and globally](#). Locally by selecting a device from the inventory, on its snapshot page, go to Interface > Menu > Availability Monitoring > Disable status polling. And globally, from Settings > Configuration > Interface template > Interface Types > Select an interface and > Disable status polling.

Configuring java heap size

If the OpManager service is getting slower, you can try increasing OpManager's java heap size. It will be set to 1GB by default. The heap size is the maximum amount of system resources, the OpManager service will consume. The heap size should not be under-allocated to avoid OOM issues, and it must not be over-allocated either to avoid overutilization of system resources. To configure the java heap size, follow the below steps:

1. Click on the support icon at the top right corner of the window.
2. Under the "**Community and details**" section that is found at the bottom of the page, click on the "**Load details**" tab.
3. Here you can edit the value under the "**Configured heap**" field.

Data Collection:

By default, OpManager uses 12 threads for SNMP polling and 12 threads for WMI polling. To know about our common data collection errors, kindly [click here](#).

SNMP Data-collection

The assumption is that each monitored device has a minimum of 10 polleddata (monitored resources such as CPU, memory, incoming traffic, out-going traffic, errors etc). Each Interface object has 11 polleddata which include RxTraffic, TxTraffic, Bandwidth Utilization, Errors, Discards etc. Depending on the number of polleddata, you can increase the number of datapoll threads.

Steps:

- From /opmanager/conf folder, open the filethreads.conf
- Increase the value of datapoll threads from 12 to the required number of threads for SNMP polling.
- Save changes and restart OpManagerService.

Following is a reference table to increase the number of threads:

Number of devices/interface	Hardware	Number of datapoll Threads	Number of SNMP Polled Data	Monitoring Interval
Upto 500 servers / 5000 interfaces	2*3.4GHz, 4GB	12 (default)	Upto 50000	15 mins
Beyond the above numbers	4*3.4GHz, 4GB to 8 GB	13 - 20	More than 50000: Additional 1 thread for every 5000 polleddata	15 mins

WMI Data-collection

(Includes Resource monitors, Windows Service Monitors, AD monitors, MSSQL monitors, Exchange monitors. Assumption is around 50 polleddata per monitored Windows device)

Steps:

In the file /conf/threads.conf, increase the value of WMI_EXEC from 12 to the required number of threads for WMI polling.

Number of devices	Number of Threads	Number of WMI PolledData	Monitoring Interval
100	12	Upto 5000	15
More than 100	13 - 18	Over 5000	15

Addressing Timeout Issue

The default SNMP query timeout to variables in a device is 3 seconds. If there is a delay in the agent response for some devices, you can follow the below steps and configure your suitable

timeout value for SNMP data collection:

Steps:

- Go to "**Settings -> Discovery -> Credentials**"
- Now open the respective credential profile and click on the "**Advanced settings**" option.
- Here, you can configure the timeout value.
- Click on "**Save**".
- The changes will now be updated across all the devices that have been mapped with this particular credential profile.

Database Connection Pool

If the number of PolledData is over 50000, the number of non-transaction connections can be increased in the range of 7 to 10 (default being 6 connections). Here is how you configure:

Steps:

1. From /opmanager/conf folder, open the filedatabase_params.conf.
2. Increase the value of NON_TRANS_CONNECTIONS parameter to the required number.
3. Save changes and restart OpManagerService.

Threshold Settings

OpManager monitors the availability, performance, health, and other critical metrics of the discovered devices with the help of a wide range of monitors. These monitors are configured with threshold values that help OpManager send out alerts when the device violates the specified thresholds. OpManager offers multiple threshold levels such as Attention, trouble, critical, and rearm. The Rearm is the value that determines when the monitor is reverted to 'Normal' status.

[Learn More.](#)

Example: The Warning threshold condition for a memory monitor is selected as greater than [>] and the threshold value is configured as 75. If the value of the monitor oscillates between 72, 80 and 73 for three successive polls, an alert is not raised for the poll with value '80' but the admin might still wish to receive an alert for it.

To avoid this, you can set the Rearm value at a considerably wide interval (say 70 in this situation) to make sure the status returns to 'Normal' only when the value goes below this threshold.

You can also automate the threshold configuration process by using OpManager's "**Adaptive Thresholds**" feature.

By enabling adaptive thresholds, OpManager analyses the device's usage patterns and trends, and sets thresholds automatically. However, OpManager will require three days worth of performance

data for the same. If you are adding devices for the first time, you can manually set thresholds and monitor them during this period. You can later enable Adaptive Thresholds, once you have three days of performance data for OpManager to deal with. [Learn More](#).

NOTE: Kindly note that adaptive thresholds feature is only supported for **CPU utilization, memory utilization, and response time** monitors for the time being.

Specifying Monitoring Intervals for Performance Monitors (CPU, Memory, Disk, and etc)

The resources critical to a device's availability can be [polled more frequently](#), with the minimum configurable interval being 1 minute, while the other resources can be polled less frequently. Reducing the polling frequency will lessen the operating load of OpManager conversely improving performance.

Note: Increase the monitoring interval of less critical devices. Only devices with the highest priority should have a 1 minute monitoring interval.

Specifying Monitoring Intervals for services (MS SQL, MS Exchange, https, telnet, and etc.)

All systems will run a default set of services. However, it is recommended only to poll the necessary services, since, polling services frequently, puts a load on OpManager. Hence, before monitoring a service in a device, kindly make sure that the said service is running in your end-device. [Learn more](#) about monitoring WMI services in OpManager.

Implementation and product startup

Security and Authentication Installing and Starting

The user account with which you install OpManager should have full permission on all folders/sub-folders on the installation directory. Make sure the account has a secure password. Also, you can run OpManager only with the user account with which you installed the application.

Enabling SSL

OpManager supports [enabling SSL for WebClient](#) , securing the web access. Make sure you are on Build No.7010 or higher.

Securing Admin Account

The default user created with full permission is admin with the password also as admin. Make sure you [change the password](#) once you login.

Restricting Users Scope

You can [create user accounts](#) and restrict their scope by assigning full permission or read-only access for all or part of the devices. This is done by creating business views and assigning users with relevant permissions to the users.

Proxy-settings

When monitoring URLs for availability, the requests to the URLs are sent through a proxy. So, this mandates [proxy server settings configuration](#) in OpManager. If the requests to certain URLs are direct and does not require to go through a proxy, the hostnames, or the IP Address of the devices must be specified in the *No Proxy for* field.

Alerting

OpManager sends SNMP, CLI, or WMI queries to devices for monitoring. So, ensure that the monitored devices do not restrict requests coming in from OpManager. If the devices are behind a firewall, the relevant ports must be opened, and also access lists on routing devices must be verified.

a. SNMP Traps

Trap [Processors must be configured](#) for new trap types. These traps are usually marked as unsolicited traps under alarms in OpManager. Once parsers are configured, meaningful alerts are generated from the traps.

b. Notification Profiles

Make sure that correct [mail server details](#) and [sms](#) are configured to enable all email-based and sms based notifications respectively. The secondary mail-server settings must be configured if there is one. It is recommended that when creating [notification profiles](#), the profile names do not contain special characters, space etc.

Database Tuning

OpManager runs on PGSQL and MSSQL. To ensure smooth operation, there should be no connectivity issues between OpManager and the Database server.

Configuring Remote pgSQL Parameters

For versions 12.5 and above (PgSQL 10.10 or above) PGSQL comes bundled with OpManager, however, it can [also be run remotely](#).

Configuring MSSQL Parameters

MSSQL is usually preferred when the database transaction logs will be generated in large numbers. Learn how to [configure OpManager for MSSQL database](#).

Distributing Database for scalability

If the monitored devices are over 500 (or over 5000 interfaces), with more than 50000 polledata, you can consider [migrating the database](#) onto another dedicated server as this promotes load distribution and lag free performance.

Increasing Java Heap Size

OpManager Java Heap Size can be increased based on optimization requirements by editing the value of -Xms/-Xmx parameter in StartOpManagerServer.bat/sh script or by editing the file /opmanager/conf/wrapper.conf (Initial/Maximum Java Heap Size). The recommended JVM Heap Size is:

Hardware	Initial Heap Size (-Xms)	Maximum Heap Size (-Xmx)
1 GB RAM	100	200
2 GB RAM	200	512
4 GB RAM	512	1024

Database maintenance

OpManager collects data from devices at regular intervals. Limit the [Database Maintenance](#) values to its default numbers. Increasing these values will cause a delay in report generation.

Intuitive Reports

OpManager comes with over 100 out-of-the box [Reports](#) that help you quickly assess and report the various metrics of your network. Custom reports can also be created, to access reports, go to Settings > Reports.

To save time on generating reports periodically, they can also be [scheduled ahead of time](#) from Reports > Schedule Reports.

You can also have a comprehensive view of the actions logged in OpManager, the data that has been collected, and the APIs that have been accessed over the time, by going to Reports -> Audit. [Learn More](#).

OpManager's [advanced reports](#) feature helps users ["summarise"] performance across different metrics that spans over different categories such as devices, interfaces, monitors, and etc. This comprehensive reporting feature allows users to gain network insights at a glance, and can even be scheduled at their convenience.

Furthermore, users can even filter out the reports by opening the particular report, and then clicking on the filter icon at the top right corner of the page. Here, users can filter the devices in the report based on the time, category, or business views. The filters in turn, vary based on the type of report used.

Wish you a successful deployment. Feel free to check out our [support forums](#) or [reach out to us](#) for further technical assistance.