# Table of Contents

OpManager v12 ............................................................................................................................................ 1

Installing OpManager ............................................................................................................................. 1
Installing OpManager - EE ..................................................................................................................... 6

User Interface ........................................................................................................................................... 27

Discovery .................................................................................................................................................. 27
  Add Credentials ..................................................................................................................................... 27
  Configure Rule Engine for Discovery ................................................................................................. 30
  Discovering Devices ............................................................................................................................ 33
  Discovering Networks ........................................................................................................................ 34
  Layer 2 Discovery and Mapping ........................................................................................................... 39

Manage Devices ....................................................................................................................................... 40
  Managing and Unmanaging a Device ................................................................................................. 40
  Configure Additional Fields for Devices or Interface ....................................................................... 42
  Configure Device Dependencies .......................................................................................................... 43

Classify and Map the Devices ............................................................................................................... 45
  Using Device Templates ....................................................................................................................... 45
  Using Interface Templates .................................................................................................................... 49
  Categorizing into Default Maps ........................................................................................................... 51
  Add New Infrastructure Views ............................................................................................................ 52
  Different Types of Views ...................................................................................................................... 53

Manage Users ......................................................................................................................................... 55
  Adding Domain ................................................................................................................................. 55
  Creating Users ................................................................................................................................. 56
  Changing Password ............................................................................................................................ 59
  Removing Users ................................................................................................................................. 60
  Pass-through Authentication ............................................................................................................... 61

Manage Network Resources ................................................................................................................. 67
  Monitoring CPU, Memory, Disk Using SNMP .................................................................................... 67
  Monitoring CPU, Memory, Disk Using WMI ..................................................................................... 68
  Monitoring CPU, Memory, Disk Using CLI ....................................................................................... 69
  Adding More Monitors .......................................................................................................................... 70
  Adding Custom Monitors ..................................................................................................................... 71
  Adding WMI-based Custom Monitors ................................................................................................. 72
  Device-specific Monitoring Configuration ............................................................................................ 73
  Configuring Thresholds for monitors .................................................................................................... 74
  Monitoring TCP Services ....................................................................................................................... 75
  Monitoring TCP Services on a Device ................................................................................................. 76
Installing OpManager on Windows

Steps to install:

- Download OpManager for Windows.
- Execute the downloaded OpManager.exe to install and follow the instructions in the installation wizard.

- 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 OpManager Edition (30day trial or Free), language and the directory to install OpManager. Proceed to the next step.
• Select the Program folder to add the OpManager shortcuts and click Next.

- Specify the port number to run OpManager Web Server and click Next.

- Register for technical support by supplying your contact information such as name, email id etc.
Verify the installation details and click Next.

Select the Server Mode i.e., Primary or Standby server and click Next.

- If the Server Mode is selected as Standby, then enter the Primary webserver host, port and login details and complete the installation.

Select the database. OpManager supports both, PostgreSQL and MSSQL as database and click Next.
Installing OpManager on Linux

Prerequisites:

1. If OpManager is installed in Debian machines, make sure that the iputils-ping package is installed.

   This is required because OpManager uses the options of the Ping command provided by the iputils-ping package. Debian OS has two different packages, netkit-ping (installed by default) and iputils-ping. If iputils-ping package is not installed, OpManager will not be able to ping any of the managed devices and also itself and hence reports the status of all devices to be down.

2. Sometimes, you might encounter errors such as database connection not getting established or the server not starting up. To workaround these issues, comment the IPv6 related entries in the etc/hosts file.

3. Check if the DNS resolves properly to the IP Address on the system in which OpManager is installed. Add an entry to etc/host file with ipaddress and host name if there is trouble starting OpManager.

Now, to install OpManager on Linux machines, follow the steps given below:

1. Download OpManager for Linux.

2. Login as root user.

3. Assign the executable permission to the downloaded file using the following command: 

   chmod a+x OpManager.bin

4. Execute ./OpManager.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 OpManager Edition (Professional or Free), language, the directory to install OpManager, and the port number to run OpManager Web Server. Proceed to the next step.
7. Verify the installation details and click Next.
8. Click Finish to complete the installation process.

It is recommended to install OpManager in the opt folder. By default, OpManager is installed in the/opt/ManageEngine/OpManager directory.
Installing OpManager Enterprise Edition

- Configure SQL
- Install Central Server
- Install Probe

Configure SQL

Step 1: Create new login

- Open SQL Management Studio
- Right click on Login
- Select New login
Step 2: Select SQL Server Authentication
Step 3: Click on Server Role. Select Server Roles dbcreator and sysadmin
Step 4: Click on User Mapping. Select Master and db_owner role. Click OK.
Install OpManager Central Server

**Step 1: Download the OpManager Central exe from the below link**

https://www.manageengine.com/cgi-bin/download_exe?id=4883

Run the exe as 'administrator'
Step 2: Click 'Next' to proceed with installation

Step 3: Click 'Yes' to the OpManager License agreement
Step 4: Choose your language for OpManager installation and click 'Next' to proceed

Step 5: Choose the destination folder for OpManager installation and click 'Next' to proceed
Step 6: If you want to change the default web server port for OpManager installation enter the new port number and click 'Next' to proceed.

Step 7: Register your OpManager license with required details to get technical support and click 'Next' to proceed.
Step 8: Select 'Standalone' or 'Primary' server. If you are installing failover, select standby server. First configure standalone or primary for failover installation. Click 'Next' to proceed.

Step 9: Select 'MSSQL' database. Click 'Next' to proceed.
Step 10: Provide MSSQL details like host name, port, database name. Use SA credentials (username and password) created earlier. Click 'Next' to proceed.

Step 11: Search for bcp.exe and bcp.rll in the MSSQL installation directory. Copy these files under OpManagerCentralbin directory. Click 'Next' to proceed.
Step 12: Click on browse and select OpManagerbin\bcp.exe. Click 'Next' to proceed
Step 13: Click ‘Finish’ to complete OpManager Central Server installation

OpManager Central will start now once you click Finish.

Technical support: http://support.opmanager.com

Install OpManager Probe
Step 1: Download the OpManager Probe exe from the below link

https://www.manageengine.com/cgi-bin/download_exe?id=4-887

Run the exe as 'administrator'

Step 2: Click 'Next' to proceed with installation
Step 3: Click 'Yes' to the OpManager License agreement

Step 4: Choose your language for OpManager Probe installation and click 'Next' to proceed
Step 5: Choose the destination folder for OpManager Probe installation and click 'Next' to proceed.

Step 6: If you want to change the default web server, netflow ports for OpManager probe installation enter the new port numbers and click 'Next' to proceed.
Step 7: Enter the details of the proxy server, if the probe is installed behind a proxy server and click 'Next' to proceed

Step 8: Register your OpManager license with required details to get technical support and click 'Next' to proceed
Step 9: Select 'Standalone' or 'Primary' server. If you are installing failover, select standby server. First configure standalone or primary for failover installation. Click 'Next' to proceed.

Step 10: Select 'MSSQL' database. Click 'Next' to proceed.
Step 11: Provide MSSQL details like host name, port, database name. Use SA credentials (username and password) created earlier. Click 'Next' to proceed.

Step 12: Search for bcp.exe and bcp.rll in the MSSQL installation directory. Copy these files under OpManagerCentralbin directory. Click 'Next' to proceed.
Step 13: Click on browse and select OpManagerbinbcp.exe. Click 'Next' to proceed.

Step 14: Provide OpManager Central server details like central server URL, probe name, contact name and contact mail ID. Click 'Register' to proceed.
Step 15: Click ‘Finish’ to complete OpManager Central Server installation.
Add Credentials

OpManager accesses the remote devices using the protocols SNMP, CLI, or WMI. 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.

1. Go to **Settings > Discovery > Credentials**
2. Click **AddCredential**
3. Configure the following parameters and click **Save** to add the credentials:

**Credential Category**: Select the relevant category.
- **Monitor**: Select this if the credential is to monitor a device.
- **Backup**: Select this if the credential is to take backup of device configuration.

**Credential Type**: Select the relevant protocol.

**SNMP v1/SNMPv2**: SNMPv1 and SNMPv2 are community based security models. Enter the Credential name and description. Configure the correct Read and Write community, SNMP Port, SNMP Timeout (in seconds) and SNMP Retries.

**SNMP v3**: SNMPv3 is a user based security model. It provides secure access to the devices by a combination authenticating and encrypting packets over the network. The security features provided in SNMPv3 are Message integrity, Authentication and Encryption. If you select SNMPv3 as the credential type, then configure the following parameters.

1. **Name**: Enter the name of the credential.
2. **Description**: Enter a brief description about the credential.
3. **User Name**: Enter the name of the user (principal) on behalf of whom the message is being exchanged.
4. **Context Name**: An SNMP context name or “context” in short, is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context. An SNMP entity potentially has access to many contexts. In other words, if a management information has been defined under certain context by an SNMPv3 entity, then any management application can access that information by giving that context name. The “context name” is an octet string, which has at least one management information.
5. **Authentication**: Select any of the authentication protocols either MD5 or SHA and enter the password. MD5 and SHA are processes which are used for generating authentication/privacy keys in SNMPv3 applications.
6. **Encryption**: Select any of the encryption protocols either DES or EAS-128 and enter the password. Note: Only after configuring Authentication it is possible to configure Encryption.
7. **SNMP Port**: Enter the SNMP port number.
8. **SNMP Timeout**: Enter the SNMP timeout in seconds.
9. **SNMP Retries**: Enter the SNMP retries.

**WMI**: If you select WMI as the protocol, configure the Domain Name, the User Name, and the Password. Example:- TestDomainTestUser. Also enter the credential name and description.

**Telnet/SSH**: Enter the credential name. Select protocol Telnet or SSH. For Telnet, ensure you configure the correct login prompt, command prompt, and password prompt besides the user name, password, port number and timeout (in seconds) to access the device. For SSH, if you select SSH Key Authentication, ensure you configure the user name and choose the SSH Key using the Browse button, and correct command prompt besides the port number and timeout (in seconds) to access the device.

**VMware**: Enter the credential name. Provide the HTTPS Username and Password of the Host. Enter the HTTPS web service port number and timeout interval for the connection between the Host and OpManager server.
**Citrix**: Enter the credential name. Provide the Username and Password of the Host. Enter the web service port number and timeout interval for the connection between the Host and OpManager server.

**UCS**: Enter the credential name. Provide the UCS Manager Username and Password. Enter the Port, Protocol and Timeout interval for the connection between the UCS and OpManager Server.
Add Credential

Credential Category
- Monitor
- Backup

Credential Type
- SNMP v1/v2

Choose the credential type here.

Name
- SNMP_Main

Description
- SNMP string for all devices.

SNMP Read
- 

SNMP Write
- 

SNMP Port
- 161

SNMP Time Out (sec)
- 10

SNMP Retries
- 0

Click Save once done.
**Rule Engine**

Rule Engine helps you automate the activities such as adding monitors to a device or adding a device to a business view that you carry out after adding the devices to OpManager. This helps you start monitoring the devices straightaway as soon as you add them and avoid repetitive manual effort.

**How does Rule Engine Work?**

The Rule Engine is condition/criteria based. During discovery, devices that satisfy the condition/criteria are associated with the actions specified in the Rule Engine.

**Steps to add a Rule Engine**

1. Go to **Settings > Monitoring > Configuration > Rule Engine -> Add Rule**
2. Enter a **Name** and **Description** for the Rule Engine.
3. Define the **Criteria** and select the **Condition**.
   - Eg. Select Service Name as the Criteria and equals as the Condition, and enter the POP3Svc (POP3Svc is a MSExchange service. This is to verify whether the discovered device is an exchange server or not.)
4. If required you can define multiple criteria, but have to select either AND or OR option.
   - **AND**: Executes the action when all the defined criteria are satisfied.
   - **OR**: Executes the actions when any one of the defined criteria is satisfied.
5. Define the actions
   - Eg. Select Add Service Monitor as the action and select the required service monitors (Exchange server related monitors are added to the devices that satisfy the POP3Svc condition.)
6. Click **Add**. If required you can define multiple actions as well.
7. Click **Save** to save the rule.
Actions with Rule Engine

Following are the actions that can be done on a created rule engine:

- Edit
- Copy As
- Enable/Disable
- Delete

Click the respective icons to carry out these actions on a Rule Engine.

Sample Rule engine which adds Cisco routers to a business view and associates a notification profile automatically upon discovery.
Re-running a Rule

To re-run a rule on demand,

1. Select the rule that you want to re-run.
2. Click on the **Re-run** button.
3. Select the devices on which you want to execute the rule.
4. Click **Run**.
Discover Individual Devices

You might have added more devices to your network and may therefore need to forcefully discover these devices. You can discover such devices on demand by following the steps below:

1. Go to **Settings > Discovery > Add Device**
2. Type either the IP Address or the Device Name of the device to be discovered.
3. Enter the correct Netmask/Network IP. Example: **IPv4**: 255.255.255.0, **IPv6**: fe80::b343:567e:c254:0
4. Select the **discovery credentials**.
5. Click **Add Device** to start discovery

**Note:** If you are unable to add the device, try to ping the device from the OpManager machine and check for response. Search the device using the Device Search box on the top right corner in the WebClient.
Discovering Networks Using OpManager

You can discover devices on a network by either specifying a range or the entire network. OpManager uses ICMP/Nmap to discover the devices on a network.

1. Discovering devices from an IP Range
2. Discovering a complete network
3. Discovering devices by CSV import
4. Discovering Interfaces
5. Scheduled discovery

Discover a Range

To discover devices from a selected range specify the start and end ip address and select the netmask for the devices to be discovered within that range.

1. Go to Settings > Discovery > Discovery - Input
2. Select IP Range: Select this option to specify the range.
3. Start IP: Specify the IP address of the device in the range from where OpManager should start discovery.
4. End IP: Specify the IP address till which OpManager should discover.
5. Netmask: Select the correct netmask.
6. Discovery Credentials: Select the configured Credentials to be used for discovery.
7. Click Discovery for the discovery to start.
Discover a complete network

1. Go to Settings > Discovery > Discovery - Input
2. Select CIDR: Select this option to discover an entire network.
3. Network IP: Specify the Network IP to be discovered.
4. Credentials: Select the credentials and SNMP settings as mentioned above.
5. Click Discovery for the discovery to start.

OpManager supports discovering Hyper-V hosts and VMs using CIDR.

Discover by Importing from a file

You can import a set of IP addresses for discovery from a csv file.

1. Go to Settings > Discovery > Discovery - Input
2. Select CSV File Import
3. Create a csv file (as shown below) with the details of name/paddress of the device, displayname and device type.
4. Browse and select the CSV file from which you want the devices discovered and imported.
5. Provide the correct netmask.
6. Click Discovery for the discovery to start.

**Note**: If you are using DHCP protocol on your network, make sure that both the forward and reverse lookup gets resolved before you add the devices to OpManager.

### Discover Interfaces

1. Go to **Settings > Discovery > Discovery - Interface**
2. Select Category, Devices, Interface Type and Status
3. Click Discover to discover the interfaces
1. We can have Opmanager do a scheduled discovery at specific intervals which sweeps the IP range you entered and adds the devices using the conditions mentioned during the discovery.

2. This can be saved as a profile to be executed per schedule and the report can be e-mailed as well.

3. We can have Discovery reports which gives you information on what device was added and when.
Discovery - Schedule

Email Notification
To Email Address: admin@noc.com

Subject: Discovery report

Message: Please find the attached Network Discovery Report.

Back  Cancel  Next
Layer 2 Mapping

Layer 2 Discovery helps network administrators/ Data center admins to visualize their complete network infrastructure with a live network map. It automatically discovers, maps and reports the complete set of devices (servers, desktops, virtual machines, firewalls etc) present in your infrastructure in less than no time.

It also offers periodical network rediscovery options to keep the map live and up-to-date. You can export these network maps to PDF, take print outs and share it with your peer groups.

Configuration

1. Go to Settings > Discovery > Layer 2 Discovery
2. Layer 2 Map Name > Unique name of Map to be referenced from all the places
3. Router Address > The device must be a Seed Router or an L3 Switch
4. Start IP > Network range starting IP Address
5. End IP > Network range ending IP Address
6. Select the Discovery Mechanism: CDP, LLDP, IPROUTE, FDB, ARP
7. Schedule Interval > Specify the interval (in days) at which the map must be re-drawn
8. Select the respective credential and click Discover to let OpManager draw the map.
Managing and Unmanaging a Device

By default, OpManager manages all the discovered devices. However, there might be some known devices that are under maintenance and hence cannot respond to status polls sent by OpManager. These devices can be set to unmanaged status to avoid unnecessary polling. Once maintenance gets over, they can be set to managed status.

To unmanage a device

1. Go to **Inventory > Devices > Device snapshot** page
2. Under **Actions**, select **Unmanage**.

This stops the status polling and data collection for the device and changes the device status icon to gray.

To start managing an unmanaged device

1. Go to **Inventory > Devices > Device snapshot** page
2. Under **Actions**, select **Manage**.

This resumes the status polling and data collection for the device. The status icon shows the current status of the device.

To Manage or Unmanage devices in **bulk** -

1. Go to **Inventory**
2. Check the devices you wish to manage/unmanage
3. Click on the menu at the top right >> unmanage/unmanage the devices
Configuring Additional Device or Interface Properties

Configure additional properties of a device by adding additional fields. This makes device management easy.

1. Go to Settings > Monitoring > Configuration > Additional Fields. A list of pre-populated fields is shown.
2. Click Add Field button on the top right corner and configure the following values.
   1. Field Name: Configure the name of the additional
   2. Field Type: Select the property type (text, numeric and date)
   3. Field Length: Set the length of the field.
   4. Description: Add a meaningful description for the field.
   5. Click Save

The properties added is applied to all the devices or interfaces.

Device > The additional fields are displayed when you click the Device Notes tab in the device snapshot page.
Interface > The addition fields are displayed when you click the Additional Fields tab in the interface snapshot page.

You can import additional field properties from CSV file. Click Import Field Properties from CSV button. Click Browse button in the Import File field and choose the CSV file containing the additional field properties for device or interface.
Configuring Device Dependencies

The status polling for a device can be controlled based on its dependency on some other device. This prevents the unnecessary status checks made to the dependent nodes.

For instance, many devices will be connected to a switch. If the switch goes down, all the devices connected to it will not be reachable. In this case, it is unnecessary to check the status of the dependent devices.

Configuring dependencies in individual devices

You can configure dependencies for a single device from the device snapshot page. Here are the steps:

1. Go to **Settings > Monitoring > Configuration > Quick Configuration Wizard > Device Dependencies**
2. Select the Category, Devices and click Next
3. Select the dependent Category, Business View and select from the available devices for dependency
4. Click **Save**

OpManager stops monitoring the devices if the dependent device is down. Configuring dependencies prevents false alarms.
### Quick Configuration Wizard

#### Device Dependencies

<table>
<thead>
<tr>
<th>Device Templates</th>
<th>Notification Profiles</th>
<th>Service Monitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event log rules</td>
<td>Device Dependencies</td>
<td>Credentials</td>
</tr>
<tr>
<td>Delete devices</td>
<td>Manage/Unmanage devices</td>
<td>Alarm Suppression</td>
</tr>
</tbody>
</table>

#### Quick Configuration Wizard - Device Dependency

**Category**
- Switch

**Devices**
- CiscoSwitchDevicesExample.com

#### Page 2

Choose the dependency parent device

#### Page 3

**Quick Configuration Wizard - Device Dependency**

- [ ] Assign to all devices in the Category: Switch
- [ ] Assign to all devices in the Business View: RV1
- [ ] Manually group devices

[Cancel] [Next] [Associate]
Classification and Device Templates

During initial discovery, OpManager categorizes the network devices into servers, printers, switches, routers and firewalls. For proper classification, install and start the SNMP agent on all the managed devices.

OpManager comes with over 1150 device templates which carry the initial configurations to classify the devices into the pre-defined categories, and to associate monitors to them. The device templates enables you to effect a configuration once and is applied to several devices at a time whenever there is a change.

The templates carry the information required to classify the devices and to associate relevant monitors. You can define your own templates and modify the existing ones.

Creating/Modifying Device Templates

1. Go to Settings > Monitoring > Configuration > Device Template
2. Click Add Template to define a template for a new device type. Click the Template name to modify an existing one.
3. Configure/Modify the following properties:
   - **Device Template**: Specify the device type.
   - **Vendor Name**: Select the vendor. Click New to add a new vendor, and Save.
   - **Category**: Select the category for the device type. On discovery, the devices are automatically placed in the select Category map.
   - **Monitoring Interval**: Configure the interval at which the device needs monitoring.
   - **Device Image**: Select the image for this device type.
   - **Device Identifier**: Type the sysOID and click Add (or) Click Query Device for OpManager to query the device for the OID.
   - **Add Monitor**: Click this option to select the monitors.
   - **Edit Thresholds**: Click this option to edit thresholds.
   - Click OK button to create the new device template.

To Add a new custom template -

![Device Templates](image)
Add Device Template

Device Template
Windows 10

Vendor Name
Microsoft

Category
Server

Monitoring Interval
15 mins

Device Identifier
.iso.org.dod.internet.private.enterprises.311.1.1.3.1.1

Monitor

Save
To Add a single custom monitor using the MIB:

1. Select the SNMP protocol.
2. Choose the Vendor MIB based on the device type.
3. Enter the required details in the Add Monitor section.
4. Click 'Ok' to save the monitor.

To add several monitors in bulk:

1. Click the 'Add Bulk' tab.
2. Select the appropriate OID and Vendor MIB.
3. Enter the required details for each monitor.
4. Click 'Add' to add each monitor.
The classified devices are placed under different maps for easy management. For proper device classification, make sure you have installed and started SNMP in all the network devices before starting OpManager service.

The default maps include:

- Servers
- Routers
- Desktops
- Switches
- Firewalls
- DomainControllers
- Load Balancer
- WAN Accelerator
- Wireless
- UPS
- PDUs
- Printers
- Virtual Device
- Unknown
- Storage
- URLs
- WAN RTT Monitors
- VoIP Monitors

You can also add your own infrastructure views. Custom infrastructure views can be added to group devices which cannot be classified under the default views provided. For instance, if you would like to monitor some IP Phones, it will not be appropriate to classify them as servers or desktops.

This initial classification may not be accurate if -

- The network devices do not support SNMP.
- some devices have their SNMP settings different from those specified in the Credential Settings.
Classification and Interface Templates

During initial discovery, OpManager categorizes the device interfaces. For proper classification, install and start the SNMP agent on all the managed devices.

OpManager comes with over 230 interface templates which carry the initial configurations to classify the device interfaces into the pre-defined categories, and to associate monitors to them. The interface templates enables you to effect a configuration once and is applied to several devices at a time whenever there is a change.

The Interface templates allows users to apply changes to several interfaces of the same type in one go.

Modifying Interface Templates

1. Go to Settings > Monitoring > Configuration > Interface Template
2. Search for the template you wish to edit and click on it, don’t forget to use the All/Common toggle at the top right to list all type of interfaces.
3. Configure/Modify the following properties:
   - Enable/Disable: Specify the interface monitoring status.
   - Monitoring interval: Select the interval at which this interface type must be polled to fetch data.
   - Utilization: Enter the utilization threshold, if there is a violation of this value an alarm will be raised.
   - Errors: Enter the error rate threshold, if there is a violation of this value an alarm will be raised.
   - Discards: Enter the discard rate threshold, if there is a violation of this value an alarm will be raised.
   - Status poll: Poll the interface for its availability using SNMP (ifAdminStatus & ifOperStatus).

[Diagram showing interface templates with properties to configure]

Alert: Unchecking any value above will stop polling the interface for that parameter.
This initial classification may not be accurate if

- the network devices do not support SNMP.
- some devices have their SNMP settings different from those specified in the Credential Settings.
Categorization into Default Maps

Devices are categorized into the following default maps in OpManager: The classification is done using SNMP and NMAP.

- Servers
- Routers
- Desktops
- Switches
- Firewalls
- DomainControllers
- Load Balancer
- WAN Accelerator
- Wireless
- UPS
- Printers
- PDU
- Virtual Device
- UCS
- Unknown
- Storage
- URLs
- WAN RTT Monitors
- VoIP Monitors

The discovered devices are classified into the above categories based on response to SNMP requests sent by OpManager to the devices. The devices that are not SNMP enabled, and the device types which are not included in the template are incorrectly classified under desktops. You can also add your own infrastructure maps to group your devices according to categories, or create business views to logically group devices, for instance, based on geography.
Adding New Infrastructure Views

You can create more defined groups by adding more custom views. For instance, you might want to group all your Environment Sensors or IP Phones into separate infrastructure views.

Adding New Infrastructure View

1. Go to **Inventory > Sory By Category > Add Category**
2. Specify the category **Name**.
3. Select the category whose properties needs to be inherited for this category
4. Click Add Category

After you create new infrastructure views, you can create device templates for devices of this category. This allows you to define monitors specific to the category and automatically applies the configurations defined in the template to the devices as soon as they are discovered.
Different Types of Views

Heat Maps View
It helps you to visualize your entire network health in real-time from a single page. It uses color codes to communicate the severity of the monitored devices. HeatMap view can be accessed from the Inventory > All Devices, Server, Router, Server, Desktop etc.

Grid View
<table>
<thead>
<tr>
<th>Device Name</th>
<th>Status</th>
<th>IP Address</th>
<th>Device Type</th>
<th>Category</th>
<th>Vendor</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>CiscoRouter.marlab.net</td>
<td>Clear</td>
<td>192.168.49...</td>
<td>Cisco 2900</td>
<td>Router</td>
<td>Cisco</td>
<td>8</td>
</tr>
<tr>
<td>Dell Rack System - G31Z9...</td>
<td>Clear</td>
<td>172.21.10.78</td>
<td>Dell</td>
<td>Server</td>
<td>Dell Inc.</td>
<td>2</td>
</tr>
<tr>
<td>ELA-W52012</td>
<td>Troubleshooting</td>
<td>172.21.146.52</td>
<td>Windows 20...</td>
<td>Server</td>
<td>Microsoft</td>
<td>38</td>
</tr>
<tr>
<td>HP Switch</td>
<td>Clear</td>
<td>192.168.50...</td>
<td>HP Switch J8...</td>
<td>Switch</td>
<td>Hewlett-Pac...</td>
<td>37</td>
</tr>
<tr>
<td>MEJuniper4200</td>
<td>Clear</td>
<td>192.168.49...</td>
<td>Juniper-EX4...</td>
<td>Switch</td>
<td>Juniper</td>
<td>72</td>
</tr>
<tr>
<td>MLCisco1002,MLCisco1002</td>
<td>Clear</td>
<td>192.168.49...</td>
<td>Cisco Device</td>
<td>Router</td>
<td>Cisco</td>
<td>7</td>
</tr>
<tr>
<td>MSP-K8S-64-1</td>
<td>Troubleshooting</td>
<td>172.21.144...</td>
<td>Windows 20...</td>
<td>Server</td>
<td>Microsoft</td>
<td>16</td>
</tr>
<tr>
<td>NPI2DBA13</td>
<td>Clear</td>
<td>192.168.222...</td>
<td>HP-Printer</td>
<td>Printers</td>
<td>Hewlett-Pac...</td>
<td>2</td>
</tr>
<tr>
<td>NPI2DBA17</td>
<td>Clear</td>
<td>192.168.225...</td>
<td>HP-Printer</td>
<td>Printers</td>
<td>Hewlett-Pac...</td>
<td>2</td>
</tr>
<tr>
<td>OPMAN-K8R2S-64-2</td>
<td>Troubleshooting</td>
<td>172.21.146...</td>
<td>Windows 20...</td>
<td>Server</td>
<td>Microsoft</td>
<td>25</td>
</tr>
<tr>
<td>OPMAN-K8R2S-64-6</td>
<td>Troubleshooting</td>
<td>172.21.146...</td>
<td>Windows 20...</td>
<td>Server</td>
<td>Microsoft</td>
<td>24</td>
</tr>
</tbody>
</table>
Add a Domain

To add a domain:

1. Go to Settings > User Management > Windows Domains > Add
2. Enter the Domain Name.
3. Enter the Domain Controller name.
4. Select Enable Auto Login.
   1. Select either All Users or Selected Groups.
      All Users: The auto login will be enabled to all the users. Select the permissions that you want assign - Read Only or Full Control.
      Selected Groups: The auto login will be enabled to the groups you specify. Enter the name of the groups in Read Only and Full Control columns. The access to groups will be enabled accordingly. Note: Configure one Group Name per line. The names are case-sensitive and should be configured as given in your AD
2. Select User Permissions either Read Only or Full Control
5. Select the Social IT Plus Account check box to enable access for the users in Domain for the Social IT Page.
6. Click Add.

A new domain has been successfully added.
Create New Users

You can create users in OpManager and provide required privileges to them. The option to create users is available only for the admin login account or those accounts which have 'Full Control' privilege.

Steps to add a user:

1. Go to Settings > User Management > User > Add User
2. Select user role in Role as Administrator or Operator from the drop down list
3. Select User Type from the drop down list
   - Local Authentication
   - Radius Authentication
   - AD Authentication

Add a local user

1. User Details:
   - Email ID - Email ID for the user
   - Phone Number: the user's phone number
   - Mobile Number: the user's mobile number
   - Password: a password for the above user
   - Re-type Password: retype the password for confirmation
   - Time Zone: time zone of the user location

2. Scope:
   - Monitor - You can provide this user an access to either All Devices, or only Selected Business Views. If All Devices is selected, the user will have access to all the devices of NetFlow, NCM, and Firewall. If Selected Business Views is selected, you can give the access to all business views with Select All option and business views without title with Untitled option
3. Click Add User to add the user according to the scope specified here

Logout and try logging in as the new user and check the privileges.
Add a Radius user

1. **User Details**: 
   - User Name - Name of the AD user to be added
   - Email ID - Email ID for the AD user
   - Phone Number: the user’s phone number
   - Mobile Number: the user’s mobile number
   - Time Zone: time zone of the user location
2. **Scope:**
   
   *Monitor* - You can provide this user an access to either **All Devices**, or only **Selected Business Views**. If All Devices is selected, the user will have access to all the devices of NetFlow, NCM, and Firewall. If Selected Business Views is selected, you can give the access to all business views with Select All option and business views without title with Untitled option.

3. Click **Add User** to add the user according to the scope specified here.

Logout and try logging in as the new user and check the privileges.

---

**Add an AD user**

1. **User Details:**

   - **User Name** - Name of the AD user to be added
   - **Email ID** - Email ID for the AD user
   - **Phone Number** - the user's phone number
   - **Mobile Number** - the user's mobile number
   - **Domain Name** - Select the desired AD domain from the list of available domains or Click **Add Domain** to add a new domain
   - **Time Zone** - time zone of the user location

2. **Scope:**

   *Monitor* - You can provide this user an access to either **All Devices**, or only **Selected Business Views**. If All Devices is selected, the user will have access to all the devices of NetFlow, NCM, and Firewall. If Selected Business Views is selected, you can give the access to all business views with Select All option and business views without title with Untitled option.

3. Click **Add User** to add the user according to the scope specified here.

Logout and try logging in as the new user and check the privileges.
Changing User Passwords

You can change the password for the users. Either the admin user or an user with full control privilege only can change the passwords.

1. Go to Settings User Management.
2. Click the Edit icon against the user name whose password you want changed.
   1. **Password Details:**
      - New Password - a password for the above user
      - Re-type Password - retype the password for confirmation
   2. **Contact Details:**
      - Phone number: the user's phone number
      - Mobile number: the user's mobile number
   3. **Access Details:**
      For users with only partial permission, the business views assigned to that user is displayed. Remove selection for the view if you want to remove the views from the user's purview. For users with full control, this option is not displayed.
Remove Users

You can remove the users.

1. Go to Settings > User Management
2. Click the Delete icon against the user name whose account you want to delete.
3. A confirmation dialog pops up. Click OK. The user account is deleted.
Pass-through Authentication

Pass-through authentication (Single Sign-on) provides the ability to authenticate yourself automatically in OpManager using your currently logged in windows system username and password. You would not need to manually enter your windows credential to log-in to OpManager webclient.

Prerequisites:
- Active directory authentication must have been configured in OpManager for the domain you want enable Pass-through Authentication. [Adding Domain]
- User accounts to whom you want to enable pass-through must have been already available in OpManager. [Create New Users] -> AD User.
- A computer account must be created in the Domain Controller for ensuring secure communication with the Domain Controller by OpManager.
- OpManager webserver must have been added as a trusted site in each browser you will be using to connect OpManager webclient to avoid browser popups asking for credential.

Creating Computer Account:
Run the script NewComputerAccount.vbs present under OpManager_Homeconfapplicationscripts to create a new computer account

cscript NewComputerAccount.vbs account_name /p password /d domain_name

To reset the password for an existing computer account, run the script SetComputerPass.vbs present under OpManager_Homeconfapplicationscripts to create a new computer account

cscript SetComputerPass.vbs account_name /p password /d domain_name

Ensure that the password you give is compliant to the password policy for that domain. Do not use the New Computer Account option present in AD native client which will not allow you to choose password. If you face problem running this script from OpManager server, copy the script to the domain controller machine itself and try running it.

Configuring Trusted Site in Browser:
For Internet Explorer (applicable to Chrome as well):
Open Tools > Internet Options > Security > Local Intranet > Sites > Advanced. Enter OpManager server URL, click Add.

For Firefox:
In URL box enter about:config. Click the button "I'll be careful. I promise", if warning page is displayed. In the resulting page, search for ntlm. Double click the option network.automatic-ntlm-auth.trusted-uris. Enter OpManager server URL in the text box and click OK. (Multiple site entries can be entered separated by comma.)

Configuring in OpManager:
In OpManager webclient, click Settings > User Management > Pass-through. Check Enable

- Domain Name: NETBIOS name of your domain. Example: OPMANHV
- Bind String: DNS Name of your domain Example: opmanhv.com
- DNS Server IP: Primary IP Address of the DNS Server.
- DNS Site: Site under which the Domain Controller is listed.
- Computer Account: Account name of the computer account created. Append $@domain_dns_name with the account name. Example: mytestacc$@OPMANHV.COM
- Password: Password of the computer account
## Pass-through Authentication

<table>
<thead>
<tr>
<th>Enable</th>
<th>Disable</th>
</tr>
</thead>
</table>

### Getting Domain DNS Name and NETBIOS Name:

In the Domain Controller device, open Start -> Administrative Tools -> Active Directory Users and Computers.
Getting DNS Server IP:

Open Command Prompt in OpManager server. Run "ipconfig /all". The first IP Address mentioned beside DNS Servers is the primary DNS Server IP Address.
Getting DNS Site:

In Domain Controller device, open Start -> Administrative Tools -> Active Directory Sites and Services. The Site under which your Domain Controller device name listed is your site name. You can leave the DNS Site field empty in Pass-through configuration form in OpManager, if there is only one site present in your Domain Controller.
Design Limitations:

- Pass-through authentication can be enabled for only one domain, preferably the domain in which OpManager server resides. If pass-through has been configured for a domain other than the one in which OpManager server resides, ensure the other domain will provide logged in user information to a website from different domain.

- Pass-through authentication will work only for the active directory users already been added to OpManager. If you do not want to manually create user account for all the users in your domain, enable auto-login for the domain (Admin->User Manager->Windows Domains). Once auto-login is enabled, you have to manually enter username and password of your account only on the first login and an user account in OpManager will be created automatically, from there on you can simply work without manually entering.

Disable Pass-through Authentication:

In OpManager webclient click on Settings( alt+t ) > User Management > Pass-through. Uncheck "Enable Pass-through Authentication".

(OR)

Connect OpManager database from command line and run the query "delete from JespaConfiguration" and restart OpManager service.

Log File:

If you face any issue with Pass-through Authentication, contact support with the jespa.log file present under OpManager_Homelogs folder.

Troubleshooting:

Case 1:

jespa.log file ends with line getDomainTrusts: Retrieving list of domains and

stderr*.txt contains java.lang.ClassCastException: java.io.PrintStream cannot be cast to java.lang.String
Solution:
Update the log level for jespa log in OpManagerDB

- Connect OpManager database
- Execute the query: `update JespaConfiguration set JESPACONFIG_VALUE='3' where JESPACONFIG_KEY='jespa.log.level'`
- Stop OpManager service
- Delete the file jespa.log under OpManager_Homelogs
- Start OpManager service

Case 2:

jespa.log file contains `jcifs.smb.SmbAuthException: Logon failure: unknown user name or bad password`

Cause:
Password configured for computer account is wrong (or) got expired (or) does not comply to password policy of the domain.

Solution:
Reset password for computer account using SetComputerPass.vbs script and update the value in OpManager.
Monitoring CPU, Memory, Disk Using SNMP

The monitors for CPU, Memory, and Disk Utilization are automatically associated for the devices based on the device template definitions. For instance, for Linux servers, the default template has SNMP-based monitors associated. So, all Linux servers will have SNMP-based resource monitors associated. You will see the dial graphs for these three resources in the device snapshot page if SNMP is enabled.

All the Server templates have the monitors defined for various host resources. By default, the CPU, Memory, and Disk Monitors are associated to the servers. The device snapshot page shows the values of these monitored resources with dial-graphs.

If you do not see these monitors associated to the devices, it could be due to any or all of the following reasons:

- These monitors are not present in the device template.
- SNMP is not enabled on the device. In such case, enable SNMP and add the monitors to the device once again.
- Incorrect SNMP credentials are associated. Check the credential details like the SNMP version, community string etc.

Steps to add the monitors to the device again:

1. From the device snapshot page, select the Monitors tab.
2. From the monitor types, select Performance Monitors.
3. You will see the monitors displayed on the right if associated. Click Add Monitors link on the right.
4. From the list of monitors, select the SNMP monitors for CPU, Memory, and Disk Utilization.
5. You can also add other required monitors like Partition monitors etc.
6. The selected monitors are associated to the device and the resources are monitored.

To check if the SNMP agent in the device returns response, try the following:

- Click the Test Monitor icon against any of the associated monitor names. It does a dynamic query to the device for the value of the selected resource, and show the data.
- Incase the agent does not respond, you see a message to this effect. Refer to the troubleshooting tips to resolve the issue.

As an alternative, you can monitor the non-SNMP Linux servers using CLI (telnet or SSH), or the non-SNMP Windows devices using WMI.
Monitoring Resources Using WMI

OpManager monitors the system resources using SNMP by default. However, in the absence of SNMP on the devices, the non-SNMP windows devices can be monitored using WMI. All the Windows device templates have the resource monitors preconfigured. All you will need to do is, disable the SNMP monitors associated and select the WMI monitors and associate them to the required devices.

Prerequisites
For monitoring the Windows environment, OpManager must necessarily be installed on a Windows machine. Besides, the device where OpManager is installed and the monitored remote Windows devices must have WMI, RPC, and DCOM services enabled on them. Authentication to the remote devices using WMI requires you to login as a domain user with administrator privileges. This is a requirement of the WMI protocol. If the device is in a workgroup, the system user name and password should suffice.

Steps to configure WMI Monitoring
Go to the device snapshot page.
1. From Monitors > Performance Monitors section, remove the SNMP-based monitors if any.
2. Click Add Monitor tab.
3. Now, from the list of resource monitors, select the CPU, Memory, and Disk Utilization monitors which has the protocol name as WMI against the monitor name.
4. Click Add Monitors at the top of the page.

The WMI-based monitors are associated to the device.
Monitoring Resources Using CLI

OpManager monitors the system resources using SNMP by default. However, in the absence of SNMP on the devices, the non-SNMP Linux devices can be monitored using CLI, i.e., Telnet or SSH. All the Unix Servers templates have the resource monitors preconfigured. All you will need to do is disable the SNMP monitors associated and select the CLI monitors and associate them to the required devices.

Prerequisites

For monitoring the unix servers, make sure either Telnet or SSH is enabled on them.

Steps to configure Telnet/SSH Monitoring

Go to the device snapshot page.
1. From Monitors > Performance Monitors section, remove the SNMP-based monitors if any.
2. Click Add Monitor tab.
3. Now, from the list of resource monitors, select the CPU, Memory, and Disk Utilization monitors which has the protocol name as CLI against the monitor name.
4. Click Add Monitors. The monitors are added in the template under the Monitors column.

The CLI-based monitors are associated to the device.
Adding More Monitors

Following are the monitors associated by default for the different device categories:

- **Servers**: CPU, Memory, Disk Utilization
- **Routers**: CPU, Memory, Buffer Hits/Misses, Temperature
- **Switches**: CPU, Memory, BackPlane Utilization
- **Firewalls**: CPU, Memory, and Connection Count.

Similarly, other categories also have few resources monitoring triggered by default. Besides the ones automatically associated, you can monitor more parameters. Here are the steps to configure more monitors:

1. Go to **Settings > Configuration > Device Templates**
2. From the list of templates, select the template for the device type to which you want to associate more monitors. Select the corresponding letter to get to the template quickly.
3. In the device template, from the **Monitors** column, click the **Add** button.
4. All the predefined monitors are listed. Select the required monitors from here and click **OK**
5. Click **OK** and the selected monitors are associated to the devices mapped to the Device Template.
Adding Custom Monitors

In addition to OpManager's default monitors, you can also create your own monitors for the SNMP-enabled devices in your network. The SNMP variable for which you intend configuring a monitor can return either a numeric or a string output when queried.

To add a custom monitor for a resource of a particular device type, the device template must be modified. The new monitor should be defined in the device template so that the monitor is associated for all devices of that type. Here are the steps.

1. Go to Settings > Configuration > Device Templates.
2. Click on the template in which you want to add a new monitor.
3. Example > Linux. Scroll down the template and click Add under Monitors column.
4. Click on the SNMP at the top of this page.
5. Configure the SNMP OID, Monitor Name, Display Name etc and click OK.
6. Click OK.
Adding WMI-based Custom Monitors

In addition to OpManager’s default monitors, you can also create your own monitors for the WMI-enabled devices in your network.

1. Go to Device snap-shot page on which you wish to add a custom WMI monitor
2. Click Monitors > Performance Monitors > Add
3. Select the required WMI monitor
4. Click Add to add the Monitor
Device-specific Monitors

The monitoring configuration may need alteration for specific devices. Doing a bulk-configuration using the device templates, applies the same set of configurations for the devices of the same type. In order to change the configuration for specific devices, here are the steps:

1. Go to the device snapshot page.
2. Click on Monitors > Performance Monitors
3. Click the Edit icon against the monitor name. The Edit Monitor page is displayed.
4. Change the values for the required parameters and click Save.

The changes to the monitor are effected only for that device.
Configuring thresholds for monitors

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 Warning, Trouble and Error for breaking the fault into three stages and taking corrective actions accordingly.

- Attention threshold - low severity
- Trouble threshold - medium severity
- Critical threshold - high severity

You can configure multiple thresholds for the monitors that are associated to a single device, configure from the device template in order to apply across multiple devices.

Configure threshold limits for the monitors associated to a single device

1. Go to the device snapshot page.
2. Click Monitors > Performance Monitor > click on the edit icon corresponding to the monitor for which you want to configure threshold limits. Edit Monitor page opens.
3. Ensure that the monitoring Interval is configured.
4. Specify the unit for the monitored resource in terms of percentage, MB, KB etc (based on how the parameter is measured).
5. Select the condition [>,=, <, or !=] for Warning Threshold, Trouble Threshold & Error Threshold, and enter the value. Alert is raised if the monitored value is greater than, equal to, not equal to, or lesser than (which ever is selected ) the threshold value.
6. Enter the Rearm Value. Rearm value is the value which determines the monitor has restored to normal condition. For instance, the Warning threshold condition for a memory monitor is selected as greater than [>] and the threshold value is configured as 75. The monitored memory value of that device is 80. Now alert is raised and the monitor is in violated condition. At the next poll the monitored value is 72. An alert for returning to normal condition is generated. At the next poll again the monitored value goes to 80. Again a threshold violation alert is generated. In order to avoid this, enter the rearm value. Only if the monitored value reaches the rearm value the monitor goes to the normal condition and a normal alert is raised. Note: If you select the threshold conditions greater, then the rearm value should be lesser than the threshold value and vice versa.
7. In the Consecutive Times field enter the value of how many consecutive times the thresholds (Attention, Trouble and Critical) can be violated to generate the alert.
8. Click on Save

Configure threshold limits for a bulk of devices of same type from their device template page

1. Go to Settings > Configuration > Device Templates > Select the respective template on which you want to configure the threshold.
2. 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.
3. Configure the Attention Threshold, Trouble Threshold, Critical Threshold and Rearm Value and click on OK
4. Click on OK
Monitoring TCP Services

OpManager provides out-of-the-box support for the following services: Web, HTTPS, FTP, IMAP, LDAP, Telnet, MySQL, MS-Exchange, SMTP, POP3, WebLogic, Finger, Echo, DNS, and NTTP. By default, during discovery, OpManager scans the devices for the services: DNS, MSSQL, MySQL, Oracle, SMTP, Web. You can also select other services in the list. When they are found running on their default ports, OpManager starts monitoring the services.

Scanning Services during Discovery

By default, OpManager scans each device on the network for the services that are chosen during discovery. To modify this list, follow the steps given below:

- Go to **Settings > Configuration > Monitors > Services** > Select the service and check "Scan during discovery"

OpManager allows you to change the settings for monitoring these services as per your network needs. You can configure new services that are not available in the list. OpManager can manage services running on standard TCP ports.

**Note:**

- The list contains the service names and the corresponding port numbers. To edit the settings of any of the available services, click on the service name.
- If you do not find the service you want to manage in the list, you can add the service by clicking **Add Service** Adding a New Service.

Viewing Service Status and Response Time

Go to the device snapshot page > **Monitors > Service Monitor** > you will see the list of services managed in the device, if any, with their status and current response time.

- Click the service name to view the historical report on the response time and the availability chart of the service.

Configuring Alerts

By default OpManager raises an alarm if a service is down. If required you can configure OpManager to raise an alarm if the service unavailable for a N number of times consecutively.

- Go to the device snapshot page > **Monitors > Service Monitors** > Click the edit icon against the service on which you wish to configure the threshold or to modify the consecutive time.
To select the services to be monitored in a device, follow the steps given below:

1. Go to Inventory > Click on the Device for which you wish to add a service.
2. Click Monitors > Service Monitors > Add Monitor at the top of the page
3. Select the services to be discovered from the list and click Add Monitor.
Adding New TCP Service Monitors

You can add new TCP services for monitoring.
1. Go to Settings > Monitoring > Configuration > Monitors > Services > Click Add New
2. Specify the name of the TCP service that you want to monitor.
3. Specify the TCP Port number that has to be checked for service availability
4. Specify the timeout interval in seconds for the port-check request.
5. Specify the consecutive time to generate an alarm if the service unavailable for N number of times
6. Click Save

Associating the Service to Devices

To associate a service to a server,
1. Go to Settings > Monitoring > Configuration > Monitors > Services > Associate
2. Select the required TCP service from the dropdown.
3. Select the devices on which you want to monitor the service from the column on the left and move them to the right.
4. Click Associate
Monitoring Windows Services

Certain applications in Windows machine run in the background as services. OpManager discovers and monitors the status of such services using WMI. OpManager generates alarms whenever they fail.

Prerequisites

To monitor Windows services, OpManager should be installed in a Windows machine. OpManager uses WMI to monitor the Windows services and hence you need to provide the login details of a user with administrative privilege to connect to the device. So, make sure you configure a WMI credential so that you can apply this to the Windows devices.

Add Windows Services to a Device

To monitor a Windows service, follow the steps given below:

1. Go to Inventory > Click on the device for which you wish to add a Windows service.
2. Confirm if the correct WMI credential is associated to the device. Else, configure the password details in the device.
3. Click Monitors > Windows Service Monitors. This option will be available only for Windows servers.
4. Click Add Monitor > Select the services to be monitored in the device and click Save.

Associate Windows Service Monitors to several devices

1. Go to Inventory > Click on the device for which you wish to associate Windows service.
2. Click Monitors > Windows Service Monitors > Click Associate at the top of the page.
3. Select the service you wish to associate and click Add Monitors. The selected service monitor is added to the device.

Configuring Alerts

By default OpManager raises an alarm if a Windows service is down. If required you can configure OpManager to raise an alarm if the service unavailable for a N number of times consecutively.

1. Go to the device snapshot page.
2. Monitors > Windows Service Monitors, click on the edit icon corresponding to the Windows service for which you want to configure the alert.
3. Modify the count entered for 'Generate alarm if unavailable for _ consecutive times'. For example if you enter the value as 2, OpManager will raise alarm only if the service is unavailable for 2 consecutive polls.
4. You also have to option to either restart the service or restart the server if the service goes down. Select the check box and appropriate radio button.
5. Click the Save button.
Adding New Windows Service Monitors

In addition to the Windows services monitor supported by OpManager out-of-the-box, you can add monitors for other windows services too.

To add a new Windows service monitor, follow the steps given below:

2. Click Add New > Select the device from the drop-down.
3. Type the domain administrator user name and password for the device in the respective fields and click Next.
4. A list of all the Windows Services available on that machine is displayed. From this select the services that you want to be monitored on the device.
5. Configure the consecutive time for alert.
6. Based on whether or not you want to restart the service or the machine when the service goes down, select the corresponding option.
7. Click Save.
Monitoring Processes on Windows/Unix Servers & Desktops

OpManager provides out-of-the-box support for monitoring the availability of all the processes running on a Windows or Unix system. Windows systems uses WMI and Unix systems uses CLI to monitor the processes that are running on the system.

Here are the steps for configuring Process Monitors:

1. Go to the device snapshot page.
2. Ensure that you have associated the WMI/CLI Credentials to the device.
3. Click Monitors tab > Process Monitors.
4. Click Add Monitors > select the required Process Monitors and Click Add Monitors at the top of the page to get these monitors associated to the device.

Configure Thresholds for Process Monitors

You can set resource thresholds for the Process Monitors. Once a resource (cpu/memory) utilization by a process exceeds the configured threshold, an alert is triggered.

1. Click the Edit icon against the process name.
2. Configure the threshold values for CPU and Memory resources.
3. Configure the number of times you would like to allow threshold violation before being notified. For instance, if you configure the value as 3, OpManager notifies you if the resource threshold is violated 3 consecutive times.
4. Configure the number of the process instances, exceeding which you would like to be notified. For instance, if you would like to be notified if the number of Apache.exe instances on the monitored device exceeds 3, configure the value here as 3 and save the changes.

Alerts are fired based on the above settings.

You can also view active processes on a device and also view the process diagnostics against a system resource.
Viewing Active Processes

OpManager provides you the information on the processes that are currently running on the managed device. You need to have SNMP agent running in the device to view this information.

To view the details, click the device from Inventory and you will see the Active Process widget from the Device snapshot page.
Adding New Process Template

Process templates help you to select the processes that are running on a device, convert each of them into individual templates and apply all of them across multiple devices. To add a new process template,

1. Go to Settings > Monitoring > Configuration > Monitors > Processes > Add New
2. **Device Name**: Select the device which runs the process(es) that needs to be converted into template(s).
3. **Protocol**: Select the relevant protocol to access the device.
4. Select the relevant credential from the drop-down by clicking on the Credential radio button or Click Associated username password to associate the associated credential.
5. Click **Next**. All the processes that are currently running on the device are listed along with their ID, Path and Arguments.
6. Select the required process(es).
7. Click **Save** button at the bottom of the page.

The selected processes are now added and available as templates under Settings > Configuration > Monitors > Processes.
Associating Process Template to Multiple Devices

To associate a process template across multiple devices, follow the steps given below:

1. Go to **Settings > Monitoring > Configuration > Monitors > Processes**
2. Click **Associate**.
3. Select the process template to be associated to multiple devices
4. From the listed devices, select and move the required devices to box seen on the right.
5. Click **Associate**

The selected process template is applied across multiple devices.
Creating Script Monitoring Templates

Script Monitoring templates help you create custom scripts to monitor custom parameters.

Follow the steps given below to add script templates

1. Go to Settings > Monitoring > Configuration > Monitors > Scripts
2. Click Add New and provide a name and description for the template.
3. Configure the Monitoring Interval.
4. Specify the Unit for the monitored parameter.
5. Enter the command to run the script, as if provided in command prompt.

Example:
cscript ${FileName}.vbs
Note that ${FileName} must be followed by script file extension. You may also pass arguments. Argument list may use variable ${DeviceName} which will be replaced with the monitored machine name in run time. Other supported variables are ${UserName} - WMI/CLI username, ${Password} - WMI/CLI password, ${SNMPRead} - SNMP read community string. For example,
cscript ${FileName}.vbs ${DeviceName} ${UserName} ${Password}

Script Output Format
In order to store the result of the script in DB, the output must be in the format given below.

Message:This message will be used as alarm message.
Data:
Instance1           value1
Instance2           value2
...                       ...
InstanceN           valueN

Exit code will be used to set the status of the script monitor. Exit code “0” for up , any other exit code for down. Only numeric values are allowed as statistical data. The instance name and value must be separated by a TAB space(t). Status checking scripts may NOT contain data part. If there is no message in output, a default message will be used for alarm message.

7. Timeout Enter the time to wait for script execution completion.
8. Execute From: Select the machine from which you want to execute the script. Linux scripts can be executed either from the server, where OpManager is running, or from the monitored machine.
9. Executing Directory: Provide the directory path from which you want to execute the script. You may use variables ${TempDir} or ${UserHomeDir} which means OpManager temporary directory and user’s system home directory repectively.
10. Threshold Details: Configure threshold for the script monitor if any.
11. Click on Save button to save the template.

You have successfully created a script monitoring template

Editing Script Templates

To Edit a script template

1. Click on Edit icon corresponding to the script template that you want to edit.
2. Carry out the necessary modifications and Save it.

Importing/Exporting Script Templates

The import/export options allows you to share scripts that are created by you with OpManager community and use the scripts shared by others. Use this form to share the script with OpManager community.

Import scripts

1. Click on Import button that is available in the Script Templates page.
2. Click on Browse button to locate the script (.xml file).
3. Click Import.
The script has been successfully imported to OpManager.

**Export Scripts**
1. Click on Export XML icon corresponding to the script that you want to export.
2. Click on Save to save the script.

**Copying Scripts**
OpManager allows you to save a copy of the script, modify it and use it for other monitoring requirements.
1. Click on Copy As icon that is available in the Script Templates page. The script template opens.
2. Carry out the necessary modifications and Save it.

**Deleting Scripts**
To delete a script, click on the Delete icon corresponding the script template.
Associating Script Monitoring Templates

Script Monitoring templates help you create custom scripts to monitor custom parameters.

Follow the steps given below to add script templates:

1. Go to **Settings > Monitoring > Configuration > Monitors > Scripts**
2. Click **Associate**
3. This will open a page to associate multiple devices to a specific template.
4. Select the required script from the drop-down.
5. Select the devices from left-side box and move it to the right box.
6. Click **Associate**

You have successfully associated script template to multiple devices.
Log File Monitoring

Every application prints status messages, error messages, and other critical information in its log. It is very tedious to skim through all these bulky log files for understanding the application performance. To manage such mission critical applications in real time, monitoring their log files is necessary. OpManager offers agent-based log file monitoring for real-time fault and performance management.

How log file monitoring works?

The log file monitoring agent installed in the end machine, monitors the log files continuously for the required string (It may even be a regex). Once that string is printed, it immediately notifies OpManager server, which in-turn raises the alarm.

Steps to download agent for log file monitoring

Prerequisite: Before installing the agent, add that device in OpManager.

1. Install the agent in the end machine which has the log files.
2. Go to Settings > Monitoring > Configuration > Monitors > Download Agent.

Known Issues:

1. If the file monitoring interval is modified, the match string appeared in the current polling span (old monitoring interval) will be ignored and hence the alert will not be generated. The alert will be raised as usual based on the new monitoring interval from next poll.

Example:

   Consider the file monitoring interval is 5 mins starting at 10.00 AM.
   Search string appears in the monitored log file at 10.02 AM.
   File monitoring interval is modified as 10 mins at 10.03 AM.

   In above case, the agent will ignore the search string which appeared at 10.02 AM. It starts monitoring the log file as fresh from 10.03 AM based on the new monitoring interval (10 mins).
Adding File Monitoring Template

You can now track changes on critical system and user files and be notified if a specific change occurs. For instance, you might want to be notified if the file size increases beyond a defined limit, if some files are missing, log prints etc. Configure meaningful templates in OpManager and apply them to devices on which you want the files monitored. Using the following file monitoring features you can monitor the following parameters:

- **File Content**: Presence of a word/string or in a log file, supports regex as well
- **File size**: Watch for an increase or decrease in the file size
- **Presence of a file**: Check the availability of a file in the specified directory (may have been moved, renamed, or deleted)
- **File age**: Keep track of the age of a file and take actions based on the age
- **File modification**: Be notified if a file has been modified

Steps to configure a file monitoring template

1. Go to **Settings > Monitoring > Configuration > Monitors > Files**
2. Click **New Template**. Add New Template page opens.
3. **Template Name**: Configure a name for the template.
4. **File Path**: Specify the path in which OpManager should locate the file.
5. **Polling Interval**: Configure the interval at which OpManager should monitor the file.
6. **Description**: Provide a brief, meaningful description for the template and click **Save**.

Configuring Alerts for File Monitors

Configure the monitoring criteria based on which you want to be notified:

1. **File Contains**: To monitor the print of a word/string in a log file, you have to install log file monitoring agent in the end server where the application is running. Click on Agent link to download and install the agent. Once you install the agent, it looks for the specified string in the said log file. If the word/string is printed in the log file, OpManager raises alert. If required, you can configure the agent to match the case when searching for the word/string. The notification can be triggered if the alert condition is met the specified number of times.

2. **File Existence**: OpManager looks for the file in the specified path and alerts based on the conditions specified. You can configure to be notified if the file does not exist in the path specified, or be notified if the file exists, or you can choose not to monitor. Also, choose the severity that you would like to assign to this alert. The notification can be triggered if the alert condition is met the specified number of times. That is, OpManager alerts you if a particular file does not exist in a path during two consequetive polls.

3. **File Size**: Configure OpManager to alert you if the file size goes over, or comes below a specified size. Select the relevant threshold for alerting. You can configure the size in terms of bytes, KB, MB, or GB. Choose the severity that you would like to assign to this alert. The alert can be triggered if the threshold is violated a specified number of times.

4. **File Age**: Similarly, you can configure OpManager to alert you based on the age of the file. For instance, you can be notified if a file is over 20 days old.

5. **File Modification**: When a file is modified, the date on which the file is modified is updated. You can configure OpManager to notify you whenever there is a change in the date modified. This option helps you keep track of any changes done in critical files. Choose the severity that you would like to assign to this alert.

Associating the File monitor to devices

Having creating a template with the alert criteria, you can now associate the template to the devices.

1. Go to **Settings > Monitoring > Configuration > Monitors > Files**
2. Click **Associate**
3. Select the required Template from the drop-down
4. Select the devices for which you want to apply this template and move them to the right.
5. Click **Associate** button at the bottom of the column to associate the template to all the selected devices.

The monitor is added to the device and OpManager alerts based on the alert conditions configured.

**Prerequisite:**

- Ensure that device in which you are installing the agent has already been added in OpManager.
- Click on the **Download Agent** link to download the agent.
- Install it on the machine which has the log file. Double-click the exe to begin the installation.
Adding Folder Monitoring Template

Besides monitoring files on the systems, you can also monitor the folders. You can track changes in folders based on the folder size, the number of files in a folder etc. Again, like file monitors, you can be notified if a specific change occurs. For instance, you might want to be notified if the folder size increases beyond a defined limit, if some files in a folder are missing etc. Configure meaningful templates in OpManager and apply them to devices on which you want the folders monitored. Monitor the following parameters on folders:

- Folder size: Watch for an increase or decrease in the file size
- Existence of a file: Check the availability of a file in the specified directory (may have been moved, renamed, or deleted)
- Folder Modification: Keep track of changes (add/remove/ rename) on the files or sub-folders within a folder. However, sub-folder level changes are not monitored.
- File Name: Watch files in a folder by their name.
- File Size/Age: Check the last modified file or all files in a folder for file size and age.
- File count: Keep track of the number of files within a folder.

Steps to configure a file monitoring template

1. Go to Settings > Monitoring > Configuration > Monitors > Folders
3. Template Name: Configure a name for the template.
4. Folder Path: Specify the path in which OpManager should locate the file. You can either provide the local directory (C:) or UNC share path (servernameSharedDirectory).
5. Polling Interval: Configure the interval at which OpManager should monitor the file.
6. Description: Provide a brief, meaningful description for the template and click OK.

Configuring Thresholds for Folder Monitors

Configure the monitoring criteria for Folder/File monitoring conditions based on which you want to be notified:

1. Folder Existence: OpManager looks for the folder in the specified path and alerts based on the conditions specified. You can configure to be notified if the folder does not exist in the path specified, or be notified if the folder exists, or you can choose not to monitor.
2. Folder Size: Configure OpManager to alert you if the folder size goes over, or comes below a specified size. Select the relevant threshold for alerting. You can configure the size in terms of bytes, KB, MB, or GB. Configure the rearm accordingly to reset the alarm.
3. Folder Modification: Select Alert if modified check box to receive alerts when files/sub-folders are added/deleted/renamed in the specified folder.
4. File Filter: By default all the files in the specified folder are monitored. Deselect All files check box and enter the file name or extension (*.pdf,*.txt) of the files alone you want to monitor. You can enter multiple values separated by comma, but no blank space is allowed. You can enter the filename in the following formats:
   - Full file name with extension ‘stdout.doc,stdlog.txt’
   - File name with wild characters ‘*out‘ or ‘std*‘. Files containing the same prefix or suffix name with same/different extension will be monitored
   - File name in date format ‘2011062200001.txt’. Enter the file name in a static format $YYYY$MM$DD*.txt or $YYYY$DD$MM*.txt
5. File Name Contains: OpManager looks for the files in the specified folder and alerts based on the conditions specified. You can configure to be notified if the folder does not contain any file in the specified name, or be notified if the folder contains files in the specified name, or you can choose not to monitor.
6. File Size/Age: OpManager looks either last modified file or all files for file size and age. If the threshold condition for either file size or file age is violated, an alarm is raised. Configure the relevant threshold and rearm conditions.
7. File Count: You can monitor the number of files specified in the File Filter and be alerted if the count changes, or if it violates a count threshold. Configure the rearm accordingly to reset the alarm.
Configuring Alerts for Folder Monitors

Configure the following alerting options:

1. **Severity**: Choose the severity that you would like to assign to this alert.
2. **Consecutive Times**: Specify how many times the threshold can be violated to generate the alert.
3. **Alarm Message Format**: Configure the alarm message. You can include the alarm variables by appending $ to the variable name.

Associating the Folder monitor to devices

Having created a template with the alert criteria, you can now associate the template to the devices.

1. Go to **Settings > Monitoring > Configuration > Monitors > Folders**
2. Click **Associate**
3. Select the required Template from the drop-down
4. Select the devices for which you want to apply this template and move them to the right.
5. Click on **Associate** button at the bottom of the column to associate the template to all the selected devices.

The monitor is added to the device and OpManager alerts based on the alert conditions configured.
Active Directory Monitoring

Active directory monitoring feature takes OpManager a step further in proactive monitoring of Windows environment. The system resources of the Domain Controllers where the Active Directory (AD) database resides, and few critical Active Directory Services are monitored in OpManager.

To make AD monitoring more simple and easily accessible, The Domain Controllers are classified under a separate category under Infrastructure Views. The categorization of the device as a Domain Controller is done automatically if SNMP is enabled. The system resources of the device and the AD services are monitored using WMI.

The snapshot page of the Domain Controller shows a dial graph for AD Store in addition to the dial graphs for CPU, Memory, and Disk Utilization.

The other utilization data displayed in the snapshot page for the Domain Controller are:

- Resource Utilization by LSASS (Local Security Authority Subsystem Service)
- Resource Utilization by NTFRS (NT File Replication Service)
- Ad Store Utilization
- Performance Counters showing information such as the AD Reads, the AD Replication objects etc

Besides these, following are the AD Services monitors associated by default:

- **Windows Time service**: The service synchronizes the time between domain controllers, which prevents time skews from occurring.
- **DNS Client Service**: This service resolves and caches (Domain Name Server) DNS names.
- **File Replication Service**: This service maintains file synchronization of file directory contents among multiple servers.
- **Intersite Messaging Service**: This service is used for mail-based replication between sites. Active Directory includes support for replication between sites by using SMTP over IP transport.
- **Kerberos Key Distribution Center Service**: This service enables users to log on to the network using the Kerberos version 5 authentication protocol.
- **Security Accounts Manager Service**: This service signals other services that the Security Accounts Manager subsystem is ready to accept requests.
- **Server Service**: This service enables the computer to connect to other computers on the network based on the SMB protocol.
- **Workstation Service**: This service provides network connections and communications.
- **Remote Procedure Call (RPC) Service**: This service provides the name services for RPC clients.
- **Net Logon Service**: This service supports pass-through authentication of account logon events for computers in a domain.

You can add more AD Monitors to be monitored by clicking the Add Monitor button.
Exchange Server Monitoring

You can monitor critical MSExchange (2000/2003/2010) Services and parameters using OpManager. Monitoring is done using WMI. Thresholds are pre-configured for critical services. You can also modify or enable thresholds for other services and parameters.

The services monitored are:
- Information Store
- Site Replication Store
- MTA Stacks
- Exchange Management
- SMTP
- POP3
- IMAP4
- System Attendant
- Routing Engine
- Event Service

The Exchange parameters that are monitored can be classified under the following categories:
- Address List Monitors
- POP3 and IMAP Monitors
- Information Store Public Folder Monitors
- Event Service Monitors
- SMTP Monitors
- Information Store Mailbox Monitors
- Message Transfer Agent Monitors
- Directory Service Monitors
- Information Store Monitors

Configuring Exchange Parameters and Services Monitoring

1. Go to the snapshot page of a device that has Exchange running.
2. Click Monitors > Performance Monitors > Add Exchange Monitor
3. Select the Exchange Server version. The monitors of all the Exchange parameters and services are displayed.
4. From this list, select the required Monitors and Click Add to associate it to the Server.

These monitors are associated to the device. Ensure to associate the correct WMI credential to the device. OpManager uses these credentials to connect to the device using WMI.
Monitoring MSSQL Parameters

MSSQL Services and Parameters can be monitored using WMI. OpManager detects the SQL servers by itself and MSSQL related resource metrics are added automatically.

Here are the steps to manually associate the MSSQL monitors to a device:

1. Go to the snapshot page of a device that has MSSQL running.
2. Click on Monitors > Performance Monitors > Add MSSQL Monitor
3. The monitors of all the MSSQL parameters are displayed.
4. From this list, select the required MSSQL Monitors and click Add to associate it to the Server.

These monitors are associated to the device. Ensure to associate the correct WMI credential to the device. OpManager uses these credentials to connect to the device using WMI.
Monitoring Windows Event Logs

The Event Log is a Windows service that logs about program, security, and system events occurring in Windows devices. The events can be related to some application, system or security. You can monitor these events using OpManager and configure to generate alarms when critical events are logged. OpManager uses WMI to fetch the details of these logs and hence you need to provide the log on details of a user with administrative privilege to connect to the Windows machine.

You can view the list of all events monitored by OpManager, Go to Settings > Monitoring > Configuration > Monitors > Event Logs

- Monitoring Windows Events in a Device
- Creating an Event Log Monitor
- Monitoring Custom Event Logs

Monitoring Windows Events in a Device

To monitor Windows events, you need to associate the event log monitors with the device. To do so, follow the steps given below:

1. Go to the device snapshot page.
2. Click Monitors > EventLog Monitors > Add Monitor.
3. Select the event logs to be monitored in the device.
4. Click Associate to add the selected monitors to the device.

Creating an Event Log Monitor

To create an event log monitor, follow the steps given below:

1. Go to Settings > Monitoring > Configuration > Monitors > Event Logs
   In this page, you can see the rules supported by OpManager. They are categorized into Applications, Security, System, DNS Server, File Replication Service, and Directory Service. You can add the event logs that you want to monitor under any of these categories.
2. Click Add New Rule under any one of the categories to add a rule.

   Entries to all the fields except Rule Name are optional. Event ID is a required field to identify the event but can be left empty in few exceptional cases, such as you want to monitor all events that are of the Event Types, say, error or information. Here the filter will be based on the Event Type.

   1. Select the Log File Name.
   2. Type a unique Rule Name.
   3. Enter the Event ID to be monitored. This is the unique identifier for the event logs.
   4. Enter the event Source. This is the name of the software that logs the event.
   5. Enter the event Category. Each event source defines its own categories such as data write error, date read error and so on and will fall under one of these categories.
   6. Type the User name to filter the event log based on the user who has logged on when the event occurred.
   7. Choose the Event Types to filter the event logs based on its type. This will typically be one among Error, Warning, Information, Security audit success and Security audit failure.
   8. Description Match Text : Enter the string to be compared with the log message. This will filter the events that contains this string in the log message.
   9. Generate Alarm if event is raised : By default OpManager raises an alarm if the event occurs. However, you can configure the no. of consecutive times the event can occur within the specified no. of seconds, to raise an alarm.
   10. Choose a severity for the alarm generated in OpManager for this event.

3. Click OK to save the event log rule.

Monitoring Custom Event Logs

You can monitor event logs under a custom category too. Some applications log the events in a new category other than the default System/Applications/Security category. You can now configure rules in OpManager to parse the events in such custom categories and trigger corresponding alerts in OpManager. Here are the steps:

1. Go to Settings > Monitoring > Configuration > Monitors > Event Logs
2. Click **Add Custom Event log**
3. Select a device from the drop-down on which you can query for the event categories.
4. Provide the WMI details **User Name** and **Password** of the device.
5. **List logs that were created in last** Configure the time to list the logs and Click **Query Device**
6. The custom logs in the selected device are listed. Select a log from **Discovered Log Files** and click **OK**

You can now associate the rules (default or custom event logs) to the required devices.
Monitoring URLs for Availability

You can configure OpManager to monitor your Web sites. Many business enterprises require continuous monitoring of their Web sites, as the failure of these sites might have an impact on the business.

You can monitor global URLs, such as www.yahoo.com and www.manageengine.com.com or URLs in a server, such as http://192.168.4.11/index.html, http://web and so on.

You can perform a content match on these URLs and confirm their availability. Further, for pages that require a form submit, such as user name and password, you can provide these details and verify the availability of the next page.

Note: If a proxy server is configured in your network, make sure to provide its details in the Proxy Server Settings page of OpManager. Refer to Configuring Proxy Server Settings for steps to do this. This is required for monitoring any URL in a proxy-enabled LAN.

Configuring a global URL monitor

To configure a global URL monitor, follow the steps given below:

1. Go to Settings > Monitoring > Configuration > Monitors > URLs
2. Click Add New
3. Enter a name to the URL monitor in the URL Monitor name field.
4. Type the URL address to be monitored.
5. Type the Monitoring Interval and the value of Timeout in the respective fields.
6. Generate Alarm if Unavailable for: Enter the number of times the URL can go down consecutively before raising an alert.
7. Match Content: Type the string (max. 250 characters) to be compared with the contents of the monitored Web page in the Match Content field. Click on the Check Now button to instantly verify the correctness of the given details.
8. Select between Get and Post, the methods for any HTTP/HTTPS-based URLs. This is required because certain URLs cannot be accessed using a Get request.
9. Type the request parameters and their values in the form <parameter name>=<value>, if any, to know the actual availability of the URL. Note that you can enter only one parameter in a line.
10. Configure the user name and password for authorization. This will be required in the pages where you need to log-on and test the availability of the host.
11. Select the required notification profile type and click Add button to associate it with this monitor.
12. Click Save to add the URL monitor.

Viewing URL Response Time and Availability

You can get the details about the URL response time and availability in the URL snapshot page.

1. To view the URL snapshot, click the URL link from Settings > Monitoring > Configuration > Monitors > URLs. Then click the URL whose snapshot you want to view.
2. Click the Availability chart to view the availability history and the URL downtime/uptime chart.
**Associating URL Monitors to Servers**

You can add URL monitors to Servers/Domain Controllers to check the availability of the URL from those servers.

1. Go to the device snapshot page.
2. Click **Monitors > URL Monitors**.
3. Click **Add Monitor**
4. [Configure all the values](#) for the URL Monitor and Click **Add Monitor**.

The configured URL is monitored for availability from that Server. You can configure to receive an e-mail or SMS when the URL monitored in a server goes down. For this, you need to create a notification profile for the 'URL is down' criteria and associate it to the server.
Adding Syslog Rules

Syslog is a client/server protocol that sends event notification messages to the syslog receiver. These event notification messages (usually called as syslog messages) help in identifying the authorized and unauthorized activities like installing software, accessing files, illegal logins etc. that take place in the network. In OpManager Syslog rules helps in notifying you if some particular syslog messages such as kernel messages, system daemons, user level messages etc. are sent by the devices.

Apart from the pre-defined syslog rules you can also add any number of syslog rules. Here are the steps to add a syslog rule:

1. Go to Settings > Monitoring > Configuration > Monitors > Syslogs.
2. Click on Add New. Add Syslog Rules page opens.
3. Enter a unique Rule Name.
4. Enter a brief Description about the rule.
5. Select a Facility. Facility refers to the application or the OS that generates the syslog message. By default "Any" is selected.
6. Select the required Severity.
7. Match Text : Enter the text that needs to be verified for matching. Note: Regex is supported for this field.
8. Select the Alarm Severity.
9. Enter the Alarm Message.
10. Click the Advanced button to configure advanced (threshold) rules. This is optional.
    1. Number of Occurrences: Enter the count of the number of consecutive times OpManager can receive syslog message from a device before raising an alert.
    2. Time Interval (seconds): Enter the time interval that should be considered for calculating the number of occurrences.

To clear or rearm the event:
3. Select the Facility Name.
4. Select the Severity.
5. Enter the Matching Text.
6. Click Save
Configuring Syslog Ports

OpManager receives the syslog packets via the default syslog port 514. However, if required you can configure additional ports in OpManager to receive the syslog packets. To configure additional ports, follow the steps given below:

1. Go to Settings > Monitoring > Configuration > Monitors > Syslogs
2. Click on the Syslog Port.
3. Enter the port number(s) separated by a comma.
4. Click Save
Monitoring Syslog Packets

Syslog viewer allows you to ensure whether OpManager receives the syslog packets sent by the devices. Here are the steps to view the list of the devices that send the syslog packets:

1. From Admin tab, click Syslog Rules.
2. Click on the Actions dropdown menu and select Syslog Viewer.

The syslog packets sent by the devices to OpManager are listed. You can also filter the syslog packets by device and port.

Filtering Syslog packets

1. Enter the device's IP address in the Source IP field.
2. Enter the port number via which OpManager receives the syslog packets.
**Viewing Syslog Flow Rate**

To view the flow rate of the syslog packets,
1. Go to **Settings > Monitoring > Configuration > Monitors > Syslogs**
2. Click on the **Flow Rate**.

The flow rate of the Syslog packets are displayed.
Hardware Health Monitoring

Monitor the hardware health of key device parameters such as temperate, voltage, power, fan speed, status of processors, disk arrays, etc. of VMware, HP, Dell and Cisco systems and get alerted if they violate pre-defined thresholds.

Collecting Hardware Health Data

OpManager uses SNMP to monitor and collect the hardware health status of servers, routers & switches. In-case of VMware, the vSphere API is used to collect sensor data.

The hardware health monitors are associated automatically whenever you add a device with proper SNMP credential. If you encounter any problem associating the hardware health monitors, then check for the correct SNMP credentials or contact our support team.

Reporting of Hardware Health:

OpManager provides historical reports on the status of hardware health which can be scheduled based on user needs.
Adding a New VoIP Monitor

Prerequisites

When you want to test a link from your office to another location, you need a Cisco router (IOS version 12.4 or later) at each end.

Steps to set up the monitor

Using OpManager, you can now monitor the voice and video quality of a 'call path'. Call path is the WAN link between the router in your main office and the one in the branch office that you want to monitor.

Step 1: Enable Add (/discover) the router in your LAN to OpManager. And make sure the SNMP read and write community are configured properly, for that router.

Step 2: Enable SLA responder on the destination device you wish to monitor, Steps are detailed below.

1. Open a CLI session on the destination router and enable the EXEC mode as follows:

   `Router>enable`

2. Start the global configuration mode:

   `Router#configure terminal`

3. Enable the IP SLA responder:

   `Router(config)#ip sla responder`
   (or)
   `Router(config)#ip sla monitor responder`

   (Note: Enter any one of the command to enable IP SLA responder as it varies according to the IOS versions.)

4. Repeat the above steps for all the destination routers on which you want to monitor VoIP performance.

Step 3: Creating the VoIP monitor:

1. Go to Inventory -> Select IPSLA from three line menu ->Select VoIP -> Click on + (add symbol) at the top right corner
2. Enter a name for the monitor
3. Select the source router from the list of routers discovered in OpManager, and select the relevant interface.
4. Specify the destination router either by using the 'Search' option to pick from the discovered routers, or use the 'Add' option to specify the IP address of the destination router and submit the details.
5. You will see the summary of the monitor you are about to configure. Now click 'Save' to submit the details to the device. This will take few seconds to configure.

   Refresh the page after few seconds to see the new monitor. The data will be collected every hour, from the time you have configured.

Configuring call settings and threshold template

Defining Call Settings:
Define a template with the required VoIP settings to be used for monitoring performance. The VoIP template comes with pre-populated default values. Incase you would like to effect some changes to the values before initiating monitoring, make the changes as follows:

1. Go to Admin -> Monitoring -> IPSLA -> Call Settings.
2. Configure the following parameters:

**Source Port** - Specify the VoIP UDP port to which VoIP Monitor sends simulated traffic to generate performance metrics. The default port number is set as 16384. You can specify a port in the range of 16384 - 32766.

**Simulated VoIP Codec** - The VoIP jitter codec decides the type of traffic that VoIP Monitor simulates over your network.

**Operation Frequency** - The operation frequency is the frequency with which QoS metrics are collected by the IP SLA agent on your network to determine performance.

**Operation Timeout** - The operation timeout is time to wait for the response from the responder / destination device in msecs.

**Type of service** - The Type of Service octet allows you to set precedence levels for VoIP traffic of the IP SLA operations.

**MOS Advantage Factor** - The advantage factor is a measure, on a scale of 0 to 20, of the willingness of your VoIP network users to trade call quality for convenience.

**Defining Thresholds for the monitored parameters:**

You can define a threshold template so that the VoIP performance parameters can be better suit your company SLA’s (Service Level Agreements). Alerts are triggered based on the thresholds configured so that you can take corrective actions in time. Here are the steps to define a threshold template:

1. Go to Admin -> Monitoring -> IPSLA -> Threshold Template.
2. Configure the following parameters:

**MOS Threshold** : Configure the MOS threshold by specifying the upper and lower MOS range values in the range of 1 to 5.

**Jitter Threshold** : Configure the jitter threshold in msecs with upper and lower threshold limits. The range is from 0 to 6000 msecs.

**Latency Threshold** : Specify the delay allowed in msecs again in the range of 0 to 6000.

**Packet Loss** : Specify the number of packets that can be lost in transit.

**Notification Profile** : Select the required notification profile(s) in order to notify when the any threshold rule is violated.

**Viewing Top 10 Call Paths**

With VoIP Monitor you can view the top 10 call paths by MOS, Packet Loss, Jitter and Latency. This provides you to have a quick view and react proactively. To view the top 10 call paths, follow the steps given below:

1. Go to Inventory-> Select IPSLA from three line menu ->Select VoIP and click on VoIP Monitors.
2. Click on **Top 10**. The top 10 call paths by MOS, Packet Loss, Jitter and Latency are listed.
3. Click on the required call path view its snapshot page.
HyperV Monitoring

Monitoring Hyper-V Host and VMs

OpManager monitors Hyper-V servers via WMI. It provides separate dashboard for Hosts and VMs, to have a quick view on its performance. It also offers a dedicated Snapshot page for the Hyper-V host, which provides comprehensive data such as Health, Inventory, Performance Reports, etc.

Some highlights of monitoring Hyper-V servers with OpManager:

- Monitors effective utilization of critical resources like CPU, Memory, Network and Disk
- Out-of-the-box offers 50 reports on Host and VMs
- Automatically maps the migrated VMs to the corresponding Hosts

Apart from monitoring the Hosts and VMs, OpManager also monitors the Key Performance Indicators (KPIs) of guest OSs. Similar to that of any Windows or Linux server, OpManager monitors the applications, Windows & TCP services, processes running on the VMs using WMI/SNMP.

Discovering Hyper-V Servers in OpManager

To discover the Hyper-V host and VMs, you just need to provide the IP address and WMI credentials of Hyper-V host. The VMs are automatically discovered along with the host.

Steps to discover the Hyper-V host and VMs:

Before proceeding to discover the host and VMs, ensure that you have configured the credentials for both the host and VMs in the credential library. To discover the host and VMs:

1. Go to Admin -> Discovery -> Add Device.
2. Enter the Host Name / IP Address.
3. Enter the correct Netmask and select the appropriate credentials.
4. Click OK button to add the host.

If any of the VMs are already discovered or added, OpManager automatically maps them as Virtual Device.

Note: If the device has been added successfully, but not displayed under the 'Virtualization'. Search for that device. Upon finding the particular device, Go to its snapshot page and look for the device type. If it is mentioned as 'unknown', wrong credentials might have been provided or it is not reachable during discovery. Provide the correct credentials and click on ‘Rediscover Now’ present under three line menu at the top right corner in the snapshot page, to discover it as an Hyper-V host.

Configuring Thresholds for Hyper-V Host and VMs

OpManager out-of-the-box offers monitoring templates for Hyper-V hosts and VMs. The templates help you configure thresholds for multiple hosts and VMs at one shot. The process is similar to that of configuring threshold to monitors available for Windows/Linux servers.

To configure the threshold value and apply the template

1. Go to Admin -> Monitoring -> Device Templates.
2. You can find the HyperV Server and HyperV Virtual Machine templates for the hosts and VMs respectively. Click on the required template.
3. Click on Edit Thresholds button to configure the threshold and rearm value for the required monitors.
4. Click OK.
5. Click **Associate** for the devices to inherit the configurations in the template. While associating the template, click on **Apply & Overwrite** for the devices to remove the old and add the new configurations in the template.

**Note:** To edit the threshold values of a single host, go its snapshot page and click the Monitors tab under Inventory Details. Click on the Edit icon of a monitor to edit its threshold values.

**Managing Hyper-V Alerts**

OpManager monitors Hyper-V host and VM similar to that of any Windows server. Upon clicking the monitors tab in the host snapshot page, the monitors listed for a Windows server is listed here. You can add the required monitors and configure thresholds. If the threshold is violated, OpManager raises an alarm.

**Notifying Hyper-V Alerts**

Notification profiles help you to notify when any alert is raised for virtual devices. The notification can be a sound alert / email alert/ running a script etc. You can associate any of the notification profiles that is already created for the Hyper-V host. Associating notification profile to a Hyper-V host and VM are similar to that of [associating a notification profile to a Windows server](#).
Configuring WAN Monitor

Prerequisites

OpManager primarily relies on Cisco's IP-SLA for monitoring the WAN and the prerequisite therefore is that the device should be a Cisco router and must have IPSLA agent enabled on it. Almost all the routers from Cisco were enabled with IPSLA agent and we support from IOS version 12.3 or later. OpManager uses SNMP to query the Cisco routers for the links' performance data. IPSLA familiarity is not a prerequisite. You just need to tell OpManager which links you want to monitor. OpManager provides an intuitive configuration wizard to help you configure all the IPSLA parameters for monitoring the WAN health.

Steps to set up the WAN Monitor

Using OpManager, you can now monitor the availability and latency of a WAN link / path. A WAN link mentioned here is the path between the router in your main office and the one in the branch office that you wish to monitor.

**Step 1**: Add ( / discover) the router in your LAN to OpManager. And make sure the snmp read and write community are configured properly, for that router.

**Step 2**: Configuring the Router to send traps

Configure the cisco router to send traps to OpManager. Alerts are shown based on the traps received in OpManager. To configure OpManager server as the SNMP Server receiving traps for the routers, telnet the router and type the following command:

```
snmp-server host <opmanager server IP> traps <host community string> rtr
```

For instance, if the OpManager host IP Address is 192.168.18.128, and the community string is private, the command would be:

```
snmp-server host 192.168.18.128 traps private rtr
```

**Step 3**: Creating the WAN Monitor

1. Go to Inventory -> Select IPSLA from three line menu -> Select VoIP -> Click on + (add symbol) at the top right corner
2. Enter a name for the monitor
3. Select the source router from the list of routers discovered in OpManager and then select the relevant interface of the source router
4. Specify the destination IP Address either by using the 'Search' option to pick from the discovered routers, or directly enter the IP Address and click 'Add' and submit the details.
5. You will see the summary of the monitor you are about to configure. Now click ‘Apply to device’ to submit the details to the device. This will take few seconds to configure.

Refresh the page after few seconds to see the new monitor. The data is collected every hour, from the time you have configured.

To edit any of the configuration details, go to the respective template, make the changes and save the details. When you create a new monitor, the updated values take effect. When the configuration is complete, the router starts collecting the data at the specified frequency 60 seconds (default value). OpManager updates this statistics (collected data) every hour and the reports are generated after one hour of configuration.

Configuring Test Parameters and Threshold Template for WAN Monitor

Define a template with the required WAN monitoring settings to be used for monitoring performance. The RTT template comes with pre-populated default values. OpManager uses the configured values to simulate traffic. Incase you would like to effect some changes to the values
before initiating monitoring, make the changes as follows

Configuring Test Parameters

OpManager uses the default settings specified here,

- **Payload**: The default value is 24 kb. Specify an echo payload value in the range of 0 to 16384.
- **Type of Service**: Specify the Echo TOS in the range of 0 to 255, the default being 30.
- **Operation Frequency**: Specify the interval in the range of 0 to 604800 msecs. The default interval is 60. The operation frequency is the frequency with which QoS metrics are collected by the IP SLA agent on your network to determine performance.
- **Operation Timeout**: Specify the timeout in the range of 0 to 604800000, the default being 60 msecs. Make sure that the timeout interval is lesser than the configured operation frequency so that if the operation is not successful, that is, if there is no response from the device, or in the event of a delay, the request is timed out and the subsequent operation is launched at the configured frequency correctly.

Defining Threshold for Round Trip Time

You can define a threshold template so that you are alerted with the WAN monitor violates a specified value. Here are the steps to define a threshold template:

1. Go to Admin -> Monitoring -> IPSLA -> WAN Threshold Template.
2. Configure the upper and lower threshold limits for Round Trip time in msecs, the range being 0 to 60000 msecs. You can also choose various notification profiles configured in OpManager to alert you.

Viewing WAN Monitor Alerts

Go to Inventory-> Select IPSLA from three line menu ->Select VoIP (Select any monitor)-> Alarms (present at the end of the page) to view the alerts raised by WAN Monitor. All the alarms are listed with the Source name, Alarm Message, Status of the Device, Technician, Device category, date and time. Click the alarm message to view the alarm history.
Monitoring VMware ESX/ESXi servers

OpManager monitors your VMware servers for availability and performance using native APIs. The advantage of using native APIs is that it does not require any agent to be installed on your servers. Moreover, it enhances the usability and offers in-depth monitoring capabilities to troubleshoot your Virtual Infrastructure.

Some of the highlights of monitoring VMware Servers with OpManager:

- Supports ESX/ESXi 4.0 to latest version 5.1
- Monitors effective utilization of critical resources like CPU, Memory, Network and Disk
- Supports monitoring of hardware health such as temperature, voltage, power, fan speed, status of processors etc. via API.
- Out-of-the-box 70 plus reports on Host and VMs
- Automatically maps the VMotioned VMs to the corresponding Hosts

Apart from monitoring the Hosts and VMs, OpManager also monitors the Key Performance Indicators (KPIs) of guest OSs. Similar to that of any Windows or Linux server, OpManager monitors the applications, Windows & TCP services, processes running on the VMs using WMI/SNMP.

Pre-requisites for monitoring VMware ESX/ESXi Servers

- HTTPS User Name and Password: As OpManager uses native APIs to monitor the VMware servers, it requires https username and password of the Host server to poll the performance data. Provide the correct https username and password when discovering the Host.
- VMware Tools (optional): We recommend that you install VMware tools on the VMs. In general, VMware tools improve the performance of the Virtual Machine. Moreover, they offer IP address of the VMs, which helps OpManager to automatically discover them. Click here to know the procedures for installing VMware tools.

Discovering VMware ESX/ ESXi servers in OpManager

To discover the host and the VMs, you just need to provide the IP Address and https credentials of the vCenter/Host. When you provide the vCenter credentials, all the host and VMs managed by that particular vCenter will be discovered. In-case of providing the Host credentials, the host along with its VMs are discovered.

Steps to discover the Host and VMs

Before proceeding ensure that you have configured the VMware credentials for the vCenter/Host, and SNMP and WMI credentials for the VMs in the Credential Library. To configure the credentials

1. Go to Admin -> Discovery -> Credential Settings and click Add Credential.
2. Select VMware as the **Credential type** and enter the vCenter/Host Name and its HTTPS Username and Password.

3. Enter the HTTPS web service **port number** and **timeout** interval for the connection between the vCenter/Host and OpManager server.

4. Click **Save** to add the credential.

Similarly, add the credentials for the VMs. Select the Credential Type as WMI for Windows and SNMP for non-Windows OS.

**To discover the vCenter/Host:**

1. Go to **Admin-> Discovery-> Add Device.**

2. Enter the **Device Name / IP Address.**
3. Enter the correct **Netmask** and select the appropriate **credentials**.

4. Click **OK** button to add the vCenter/host.

If any of the VMs are already discovered or added, OpManager automatically maps them as Virtual Device.

Note: If the device has been added successfully, but not displayed under the Virtual Devices, search for that device. Upon finding the particular device, Go to its snapshot page and look for the device type. If it is mentioned as 'unknown', wrong credentials might have been provided or it is not reachable during discovery. Provide the correct credentials and click on ‘Rediscover Now’ present under three line menu at the top right corner in the snapshot page, to discover it as an ESX host.

**Configuring VM IP Address**

OpManager, with the help of installed VMware Tools, identifies the IP address of the VM and maps it to the host. In case the VMware Tools are not installed, OpManager discovers it using VM’s entity name. You can assign the IP address for such VMs in the host snapshot page. Click on the Edit device details present under three line menu icon at the top right.
Manage or Unmanage VMs

You can now choose to monitor only the required VMs on a Host. OpManager discovers all the VMs during the initial discovery and you will find them listed under the inventory in the host snapshot page. Select the relevant icon to monitor the required VMs on the host. OpManager maintains this configuration when a HA, VMotion, or rediscovery happens.

Monitoring VMware ESX servers

All the discovered hosts and VMs are mapped under 'Virtualization' tab in the inventory section. Click on Virtualization ink to access the dashboard page, which provides a quick glance of your critical resources such as CPU, Memory, Network & Disk that are under pressure. Though ideal resource utilization is the key benefit we get from virtualization, it can lead to other problems because it is shared among the servers. Even if a single system has a resource crunch, it hugely affects the performance of the other systems running on the same host. Quickly identifying and fixing the resource utilization problems is therefore vital for a business to run smooth.

OpManager shows the top hosts and VMs by resource utilization and the recent alarms raised. Click on the host or the VM name to see its snapshot page. The Virtual Devices Dashboard page refreshes automatically every 5 minutes to reflect the latest collected statistics.

Listed below are the various types of top resource utilization widgets to quickly identify any over utilized resource. It gives a quick glance on systems which are the top consumers of CPU, Memory, Network, Disk I/O and Disk Space.

<table>
<thead>
<tr>
<th>Top VMs</th>
<th>Top Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Top CPU Consumers</td>
<td>1. Top CPU Consumers</td>
</tr>
<tr>
<td>2. Top CPU Ready Consumers</td>
<td>2. Top Memory Consumers</td>
</tr>
<tr>
<td>3. Top Memory Consumers</td>
<td>3. Top Swap Memory Consumers</td>
</tr>
<tr>
<td>4. Top Swap Memory Consumers</td>
<td>4. Top Network Consumers</td>
</tr>
<tr>
<td>5. Top Disk I/O Consumers</td>
<td>5. Top Disk I/O Consumers</td>
</tr>
<tr>
<td>6. Top Network Consumers</td>
<td>6. Top Disk Space Consumers</td>
</tr>
</tbody>
</table>
Snapshot page of a Host

Snapshot page of Host / VM provides a summary of the current statistics, recent alarms, configuration details such as VMs inventory, resource allocation for each VM, Network Adapters, HBA list and Datastores.

Host Details and Performance Charts

In this section you can find the Host details like IP Address, Vendor of Host, CPU Cores etc. on the left side. The right side gives a quick glance on performance data like CPU Utilization, Memory Utilization, Disk I/O Usage etc., collected during the last poll. These values are collected at an interval of 5 minutes. These data help you determine the current performance of the Host.

Host Heath At-a-Glance

This section provides the last one hour performance chart of the Host. You can view the reports of last 7 or 30 days. Click on 7 or 30 link available on the top right corner to view the last 7 or 30 days performance report respectively.

VM List & Resource Allocation Details
This section lists all the VMs on the Host, resources allotted to each VM, network adapters, storage adapters and datastore details. Any change in the inventory, gets updated automatically. You can also find the monitors that are enabled on the Host and notification profiles associated to it. Click on the respective tab to view its details.

Click on the VM name to see its snapshot page. The snapshot page of the VM is similar to that of any Windows or Linux Server's snapshot page.

**Configuring Thresholds for VMware ESX and VMs**

OpManager out-of-the-box offers monitoring templates for ESX hosts and VMs. The templates help you configure thresholds for multiple ESX hosts and VMs at one shot. For each performance metric you can configure Warning Threshold as well as Error Threshold, and receive proactive alerts if they are violated.

To configure the threshold value and apply the template

1. Go to **Admin -> Monitoring -> Device Templates.**
2. You can find the **VMware ESX/ESXi** and **VMware Virtual Machine** templates for the hosts and VMs respectively. Click on the required template.
3. Click on 'Edit thresholds' to enable or disable the threshold, and to modify Warning Threshold, Error Threshold and Rearm Values.

4. Click **OK**.

5. Click **Associate** for the devices to inherit the configurations in the template. While associating the template, click on **Apply & Overwrite** for the devices to remove the old and add the new configurations in the template.

Note: To edit the threshold values of a single ESX host, go its snapshot page and click the Monitors icon at the top. Click on the Edit icon of a monitor to edit its threshold values.

### Managing VMware Alerts

OpManager fetches events from each ESX Host, similar to SNMP traps. Currently we support important events, and this list is updated every release. Apart from host events, OpManager also monitors threshold for critical performance indicators and raises alerts. The complete list of
Threshold violation alerts and supported events are shown below in Table 1 and Table 2 respectively.

To change the pre-set threshold values for each performance monitor, go to the snapshot page of the host or VM. Check for Monitors-> VM Performance Monitors. All the VM specific performance monitors are grouped under 'VM Performance Monitors'.

Table 1: List of Threshold Monitors for critical performance indicators supported by OpManager

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Threshold Monitors</th>
<th>Virtual Device Type</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Host connection Status</td>
<td>Host</td>
<td>General</td>
</tr>
<tr>
<td>2</td>
<td>Host Data Received (avg)</td>
<td>Host</td>
<td>Network</td>
</tr>
<tr>
<td>3</td>
<td>Host Data Transmission (avg)</td>
<td>Host</td>
<td>Network</td>
</tr>
<tr>
<td>4</td>
<td>Host Network Usage (avg)</td>
<td>Host</td>
<td>Network</td>
</tr>
<tr>
<td>5</td>
<td>Host CPU Utilization (avg)</td>
<td>Host</td>
<td>CPU</td>
</tr>
<tr>
<td>6</td>
<td>Host Memory Utilization (avg)</td>
<td>Host</td>
<td>Memory</td>
</tr>
<tr>
<td>7</td>
<td>Host Disk Read Latency</td>
<td>Host</td>
<td>Disk</td>
</tr>
<tr>
<td>8</td>
<td>Host Disk Write Latency</td>
<td>Host</td>
<td>Disk</td>
</tr>
<tr>
<td>9</td>
<td>Datastore Freespace</td>
<td>Host</td>
<td>Network</td>
</tr>
<tr>
<td>10</td>
<td>VirtualMachine Data Received (avg)</td>
<td>VM</td>
<td>Network</td>
</tr>
<tr>
<td>11</td>
<td>VirtualMachine Data Transmitted (avg)</td>
<td>VM</td>
<td>Network</td>
</tr>
<tr>
<td>12</td>
<td>VirtualMachine Network Usage (avg)</td>
<td>VM</td>
<td>Network</td>
</tr>
<tr>
<td>13</td>
<td>VirtualMachine CPU Usage (avg)</td>
<td>VM</td>
<td>CPU</td>
</tr>
<tr>
<td>14</td>
<td>VirtualMachine Memory Usage (avg)</td>
<td>VM</td>
<td>Memory</td>
</tr>
</tbody>
</table>

Table 2: List of ESX hosts' events supported by OpManager

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Events</th>
<th>Virtual Device Type</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VmFailedToPowerOffEvent</td>
<td>VM</td>
<td>Major (Cleared on event 2 or 3)</td>
</tr>
<tr>
<td>2</td>
<td>VmPoweredOffEvent</td>
<td>VM</td>
<td>Clear</td>
</tr>
<tr>
<td>3</td>
<td>VmPowerOffOnIsolationEvent</td>
<td>VM</td>
<td>Clear</td>
</tr>
<tr>
<td>4</td>
<td>VmFailedToPowerOnEvent</td>
<td>VM</td>
<td>Major (Cleared on event 5)</td>
</tr>
<tr>
<td>5</td>
<td>VmPowerOnEvent</td>
<td>VM</td>
<td>Clear</td>
</tr>
<tr>
<td>6</td>
<td>VmFailedToSuspendEvent</td>
<td>VM</td>
<td>Major (Cleared on event 7)</td>
</tr>
<tr>
<td>7</td>
<td>VmSuspendedEvent</td>
<td>VM</td>
<td>Clear</td>
</tr>
<tr>
<td>8</td>
<td>VmFailedToRebootGuestEvent</td>
<td>VM</td>
<td>Major (Cleared on event 9)</td>
</tr>
<tr>
<td>9</td>
<td>VmGuestRebootEvent</td>
<td>VM</td>
<td>Clear</td>
</tr>
<tr>
<td>10</td>
<td>VmFailoverFailed</td>
<td>VM</td>
<td>Critical (Cleared on event 11)</td>
</tr>
<tr>
<td>11</td>
<td>VmPrimaryFailoverEvent</td>
<td>VM</td>
<td>Clear</td>
</tr>
<tr>
<td>12</td>
<td>VmUpgradeFailedEvent</td>
<td>VM</td>
<td>Major (Cleared on event 13)</td>
</tr>
<tr>
<td>13</td>
<td>VmUpgradeCompleteEvent</td>
<td>VM</td>
<td>Clear</td>
</tr>
<tr>
<td>14</td>
<td>VmDisconnectedEvent</td>
<td>VM</td>
<td>Warning (Cleared on event 15)</td>
</tr>
<tr>
<td>15</td>
<td>VmConnectedEvent</td>
<td>VM</td>
<td>Clear</td>
</tr>
<tr>
<td>16</td>
<td>VmDiskFailedEvent</td>
<td>VM</td>
<td>Major</td>
</tr>
<tr>
<td>17</td>
<td>VmRelocatedEvent</td>
<td>VM</td>
<td>Clear</td>
</tr>
<tr>
<td>18</td>
<td>VmRelocateFailedEvent</td>
<td>VM</td>
<td>Critical (Cleared on event 17)</td>
</tr>
</tbody>
</table>
**Notifying VMware Alerts**

Notification profiles help you to notify when any alert is raised for virtual devices. The notification can be a sound alert / email alert/ running a script etc. You can associate any of the notification profiles that is already created for the ESX host. To associate a notification profile to a virtual device,

1. Go to the snapshot page of the host.
2. Click on **Notification** icon present at the top.
3. If no profiles are associated. Then click on ‘Associate’ to view the list of notification profiles already created.
4. Select the notification profile that you want to associate and click **Associate**.

The notification profile is successfully associated to the host.
Create New Dashboard

Customizing Dashboard feature in OpManager helps you to create your own dashboard and view the desired performance metrics, reports etc at-a-glance. To create a New Dashboard follow the steps given below:

- Click Dashboard > My Dashboard > New Dashboard. Create New Dashboard page opens [screen shots given below].

- **Name**: Enter a unique name for the dashboard.
- **Description**: Brief description about the dashboard.
- Click **Next**.
- Select Widget Category from the drop down list
- Select Widget from the drop down list for the particular widget category
- Click Create button

A new dashboard is created and listed on the My Dashboard page.
Adding New Widgets

To add a new widget to a dashboard follow the steps given below:

1. Go to Dashboard > My Dashboard and click on name of the Dashboard to which you want add widgets.
2. Click on Add Widgets seen at the bottom of the page
3. Select the Widget(s) that you want add to the dashboard.
4. Click Add button to add the selected widget(s) to the dashboard
Editing Widgets

To modify the existing widgets go through the steps given below:
1. Click on the **Edit** against the widget on which you wish to modify the fields.
2. Modify the required fields.
3. Click **Save** to effect the changes.
Deleting Widgets

To delete a widget go through the steps given below:

1. Click on **Delete** icon available on the widget box. A confirmation window pops up.
2. Click **OK** to confirm deleting
Delete Dashboard

To delete a dashboard follow the steps given below:

1. Go to Dashboard > My Dashboard page
2. Click Delete icon of the Dashboard that you want to delete. A confirmation window pops-up.
3. Click OK to confirm deleting.

Note: Default dashboard cannot be deleted. Enterprise Dashboard and System Performance.
Adding New CCTV

CCTV helps you view only the required dashboards repeatedly at required intervals. To add a new CCTV follow the steps given below:

1. Go to Dashboard page and click CCTV Views.
2. Click Create CCTV View. Create CCTV page opens.
3. CCTV Name: Enter a unique CCTV name.
4. Refresh Interval: Select the interval required to switch over to the next dashboard.
5. Description: Enter a brief description about this CCTV.
6. Select the desired dashboards that you want to include in this CCTV.
7. Click Create CCTV View.

A new CCTV has been added.

Viewing CCTV

To view a CCTV view, go to Dashboard page > CCTV Views > Click on the name of the CCTV that you want to view. That particular CCTV opens in a new window.

Editing a CCTV

To edit a CCTV follow the steps given below:

1. Go to Dashboard > CCTV Views > Click on the edit icon against the CCTV name that you want to edit.
2. Make the necessary changes.
3. Click Edit CCTV View to effect the changes.
Client Settings

Change Password

- To change the Login Password, click Client Settings icon > Change Password
- Provide the Current Password
- Provide the New Password
- Provide the new password again in Re-type password
- Click Save

Change Language

OpManager is available in English, Spanish, Chinese Simplified, Japanese, French, German, Korean and Italian languages. The following are the steps to change OpManager from one language to other supported language.

- To change the OpManager language, click Client Settings icon > Language Selector
- Select your preferred language

Keyboard Shortcuts for Quick Navigation

Click Client Settings icon > Keyboard Shortcuts

<table>
<thead>
<tr>
<th>Shortcut</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALT + SPACE</td>
<td>Global Search</td>
</tr>
<tr>
<td>ALT + A</td>
<td>Alarms</td>
</tr>
<tr>
<td>ALT + C</td>
<td>Clear Alarm</td>
</tr>
<tr>
<td>ALT + H</td>
<td>Home Dashboard</td>
</tr>
<tr>
<td>ALT + S</td>
<td>Server Dashboard</td>
</tr>
<tr>
<td>ALT + N</td>
<td>Network Dashboard</td>
</tr>
<tr>
<td>ALT + SHIFT + I</td>
<td>IPAM Dashboard</td>
</tr>
<tr>
<td>ALT + I</td>
<td>Inventory</td>
</tr>
<tr>
<td>ALT + W</td>
<td>Workflow</td>
</tr>
<tr>
<td>ALT + M</td>
<td>Maps</td>
</tr>
<tr>
<td>ALT + V</td>
<td>Virtualization</td>
</tr>
<tr>
<td>ALT + L</td>
<td>Group Chat</td>
</tr>
<tr>
<td>ALT + SHIFT + A</td>
<td>About</td>
</tr>
<tr>
<td>ALT + Q</td>
<td>Submit Query</td>
</tr>
<tr>
<td>CTRL + ALT + 1</td>
<td>View Logs</td>
</tr>
<tr>
<td>ALT + SHIFT + S</td>
<td>Screenshot feedback</td>
</tr>
</tbody>
</table>

ServiceDesk Plus Integration

ServiceDesk Plus software can be integrated with OpManager using this shortcut

- To integrate ServiceDesk Plus with OpManager, click Client Settings icon > ServiceDesk Plus
- Configure all the required parameters
- Click Save

To send a screenshot feedback to OpManager support

- To send a screenshot feedback to OpManager support, click Client Settings icon > Screenshot Feedback
Alternatively, you can use the keyboard shortcut Alt + SHIFT + S

Screenshot of the selected portion of the screen will be taken and a text box will appear on top to add the feedback. Enter the feedback

Click Submit

To sign out as current user from OpManager client

To sign out as current user from OpManager client, click Client Settings icon > Sign Out
Workflow

OpManager’s IT automation workflows are code-free and out-of-the-box offers predefined checks and actions. It includes an agile and flexible drag-n-drop workflow builder. Workflow helps you:

- Initiate IT workflow on network faults or on a routine basis
- Manage Services, Processes, Files and Folders of Windows servers and desktops
- Record the IT workflow procedures as an XML and ensure structured practices across IT

OpManager also offers log reports of executed workflows for future analysis.

Checks and actions available in Workflow

Click here to know the conditions and actions available in Workflow.
Workflow Tasks

Tasks are nothing but checks and actions that help you automate repeated IT actions.

Checks:
Checks are if-else condition based. If the condition is passed/satisfied, the workflow executes the set of actions associated on the success part, executes the other set of actions associated on the failure part. Example: Consider that you have created a workflow with Test a Service, Send Mail, and Start a Service tasks. Send Mail is associated on the success part of Test a Service, and Start a Service is associated on the part. If the service is running, workflow executes Send Mail task to notify the admin that the service is running, else executes Start a Service task to start the service.

Actions:
An action just performs the said activity. Tasks such as start a service, delete file, reboot system are action tasks. If an action task is executed successfully, workflow executes the next successive task. If an action task fails, action task associated on the failure part is executed. Example: Consider that you have created a workflow with 2 action tasks - Start Process and List All Process. List All Process is associated to the success part of the Start Process task. When the workflow is executed, in case if the Start Process task is failed, workflow looks for the task associated on the failure section. If no task is found, executes the task in the success section i.e., List All Process.

Conditions and Actions available in Workflow

<table>
<thead>
<tr>
<th>Device</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Lookup</td>
<td>Executes a DNS lookup command on the end device.</td>
</tr>
<tr>
<td>Ping Device</td>
<td>Sends ICMP packets to the end device.</td>
</tr>
<tr>
<td>Trace Route</td>
<td>Executes a trace route command on the end device.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a Time Delay</td>
<td>Adds a delay to the execution of an action</td>
</tr>
<tr>
<td>Reboot System</td>
<td>Reboots the system</td>
</tr>
<tr>
<td>Shut Down System</td>
<td>Shuts down the system</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Windows Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check</td>
<td>Tests whether a service is running or not.</td>
</tr>
<tr>
<td>Actions</td>
<td>Provides a list of service that are currently running.</td>
</tr>
<tr>
<td>Get Active Services</td>
<td>Pauses a service.</td>
</tr>
<tr>
<td>Pause a Service</td>
<td>Restarts a service.</td>
</tr>
<tr>
<td>Reboot a Service</td>
<td>Resumes a service.</td>
</tr>
<tr>
<td>Start a Service</td>
<td>Starts a service.</td>
</tr>
<tr>
<td>Stop a Service</td>
<td>Stops a service.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check</td>
<td>Test whether a process is running or not.</td>
</tr>
<tr>
<td>Actions</td>
<td>Lists all the processes that currently running.</td>
</tr>
<tr>
<td>Get All Processes</td>
<td>Lists processes by Disk Read.</td>
</tr>
<tr>
<td>Processes by Disk Read</td>
<td>Lists processes by Disk Write.</td>
</tr>
<tr>
<td>Processes by Disk Write</td>
<td>Lists processes by Memory Usage.</td>
</tr>
<tr>
<td>Processes by Memory Usage</td>
<td>Lists processes by CPU usage.</td>
</tr>
<tr>
<td>Processes by CPU Usage</td>
<td>Starts a process.</td>
</tr>
<tr>
<td>Start Process</td>
<td>Stops a process.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HTTP &amp; FTP</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check</td>
<td>Test the availability of a URL.</td>
</tr>
<tr>
<td>Actions</td>
<td>Deletes a file via FTP.</td>
</tr>
<tr>
<td>FTP Delete File</td>
<td>Moves a file within the same remote device via FTP.</td>
</tr>
<tr>
<td>FTP Move File</td>
<td>Renames a file via FTP.</td>
</tr>
<tr>
<td><strong>FTP Upload File</strong></td>
<td>Writes the given content in a file (.txt) and uploads it to the remote device via FTP.</td>
</tr>
<tr>
<td><strong>FTP Post Data/Result</strong></td>
<td>Posts the output received upon querying an URL, in the workflow logs.</td>
</tr>
</tbody>
</table>

### File

| **Checks** |  |
| **Check File** | Checks the availability of a file. |
| **Get File Size** | Gets the size of a file. |

| **Actions** |  |
| **Compress Files** | Files are compressed with Windows Compression. |
| **Compress Older Files** | Files which are not used for a long time are compressed with Windows Compression. You can configure the age of the files. |
| **Copy File** | Copies file to another directory within the same device. |
| **Delete File** | Deletes a file. |
| **Delete Older Files** | Deletes the files which are not used for a long time. Also deletes older files in sub folders. You can configure the age of the files. |
| **Move File** | Moves the files to another directory within the same device. |
| **Move Older Files** | Moves the files which are not used for a long time to another directory within the same device. You can configure the age of the files. |
| **Rename File** | Renames a file. |
| **Uncompress File** | Uncompresses a file. |

### Folder

| **Checks** |  |
| **Check Drive Free Space** | Checks for free space available in a drive. |
| **Get Folder Size** | Gets the size of a folder. |

| **Actions** |  |
| **Compress Folder** | Compresses a folder. |
| **Copy Folder** | Copies the folder to another local directory. |
| **Create Folder** | Creates a folder. |
| **Delete Folder** | Deletes a folder. |
| **List Files** | Lists the files available in a folder. |
| **Move Folder** | Moves a folder to another location. |
| **Rename Folder** | Renames a folder. |
| **Uncompress Folder** | Uncompresses a folder. |

### VMware

| **Actions** |  |
| **Power Off VM** | Turns off the power to a VM. |
| **Power On VM** | Turns on the power to a VM. |
| **Reboot Guest OS** | Restarts a VM. |
| **Refresh Datastore** | Refreshes the datastore. |
| **Reset VM** | Resets a VM abruptly. |
| **Shut Down Guest OS** | Shuts down a VM. |
| **Stand By Guest OS** | Puts a VM in Stand By mode. |
| **Suspend VM** | Suspends a VM. |

### OpManager

| **Check** |  |
| **Check Device Status** | Checks the availability status of a device. |

| **Actions** |  |
| **Acknowledge Alarm** | Acknowledges an alarm. |
| **Add Alarm Note** | Adds a note to an alarm. |
| **Clear Alarm** | Clears an alarm. |
| **Delete Alarm** | Deletes an alarm. |
| **Exit Maintenance** | Moves the device under maintenance mode to normal. |
| **Generate Alarm** | Generates an alarm in OpManager. |
| **Place on Maintenance** | Puts the device on maintenance mode. |
| **Rediscover Device** | RedisCOVERs a device. |
| **Unacknowledge Alarm** | Unacknowledges an alarm. |

### External Actions

| **Actions** |  |
| **Execute Another Workflow** | Executes another workflow as an action. |
| **Execute Linux Script** | Executes a script on the end Linux devices. |
| **Execute Windows Script** | Executes a script on the end Windows devices. |
| **Log a Ticket (Remedy)** | Creates a ticket in BMC Remedy. |
| **Log a Ticket (SDP)** | Creates a ticket in ManageEngine ServiceDesk Plus. |
| **Send Email** | Sends a notification via Email. Ensure that you have configured Mail server settings. |
| **Send Popup Message** | Sends a notification via a pop-up on the end device. At present Workgroup devices alone are supported. |
| **Send SMS** | Sends a notification via SMS. Ensure that you have configured SMS server settings. |
### NCM Actions

<table>
<thead>
<tr>
<th>Actions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup</td>
<td>Takes backup of device configuration files</td>
</tr>
<tr>
<td>Execute Command</td>
<td>Executes a command on the end device</td>
</tr>
<tr>
<td>Execute Template</td>
<td>Executes a template created in NCM Plug-in on the end device</td>
</tr>
<tr>
<td>Get Last N Changes</td>
<td>Fetches the last N configuration changes made</td>
</tr>
</tbody>
</table>

### DNS Lookup:

DNS Lookup executes a DNS lookup command on the end device and provides its status.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select devices icon to select the device. If no device is selected, it will be executed on the device selected in the Info tab.</td>
</tr>
</tbody>
</table>

### Ping Device:

Sends ICMP packets to test whether the device is responding.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device. If no device is selected, it will be executed on the device selected in the Info tab.</td>
</tr>
<tr>
<td>Number of requests</td>
<td>Number of ping requests you want to send.</td>
</tr>
<tr>
<td>Packet Size</td>
<td>Size of the ping packets.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Timeout interval for the ping requests.</td>
</tr>
<tr>
<td>Retries</td>
<td>Number of retries for the ping operation.</td>
</tr>
</tbody>
</table>

### Trace Route:

Executes a trace route command on the end device.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device.</td>
</tr>
</tbody>
</table>

### Add a Time Delay:

Adds a delay to the execution of the subsequent operation.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Duration</td>
<td>Time delay to carry out the subsequent task. You can configure time delay in hours, minutes, and seconds. Select the required one from the dropdown menu.</td>
</tr>
</tbody>
</table>

### Reboot System:

Reboots a remote Windows machine.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device.</td>
</tr>
</tbody>
</table>

### Shut Down System:

Logs off, shuts down, reboots or powers off a remote Windows device forcefully.
### Test a Service
Tests whether a service is running or not.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select devices icon to select the device. You can also log off by selecting the Log Off action from the dropdown.</td>
</tr>
<tr>
<td>Options</td>
<td>Select the action (Log off, Shut down, Reboot or Power off) that you want to carry out on the remote device.</td>
</tr>
</tbody>
</table>

**Service Name**
Name of the service that you want to task whether it is running or not. Use the dropdown menu to select the service. If the service is not listed, use the discover icon to discover the services running the device.

Supported Variable:
- `{Alarm.ServiceName}` - Select this option if you want to retrieve the service name from the alarm entity. If the workflow is triggered from the service down alarm, then this variable is replaced by the servicename from the alarm entity during runtime.
- **Note:** If multiple services down alarm is triggered, this task will be executed for all those services.

### Get Active Services
Provides the list of active services running in the device.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select devices icon to select the device.</td>
</tr>
</tbody>
</table>

### Pause/Restart/Resume/Start/Stop a Service
Pauses/Restarts/Resumes/Starts/ Stops a service.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select devices icon to select the device.</td>
</tr>
<tr>
<td>Service Name</td>
<td>Name of the service that you want to pause/restart/resume/start/stop. Use the dropdown menu to select the service. If the service is not listed, use the discover icon to discover the services running the device.</td>
</tr>
</tbody>
</table>

Supported Variable:
- `{Alarm.ServiceName}` - Select this option if you want to retrieve the service name from the alarm entity. If the workflow is triggered from the service down alarm, then this variable is replaced by the servicename from the alarm entity during runtime.
- **Note:** If multiple services down alarm is triggered, this task will be executed for all those services.

### Test a Process
Tests whether a process is running or not.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select devices icon to select the device.</td>
</tr>
<tr>
<td>Process Name</td>
<td>Name of the process that you want to test. Either you can enter the process name right away (Eg.: <code>mysqld-nt.exe</code>) or you can use the select icon to select the process from the remote devices.</td>
</tr>
<tr>
<td>Path</td>
<td>This field is optional. If you want to match the path also, then check the checkbox near path field and specify the full executable path with process name. Otherwise leave this field empty. (Eg.: <code>C:\Program Files\MySQL\MySQL Server 5.0\bin\mysqld-nt.exe</code>)</td>
</tr>
<tr>
<td>Arguments</td>
<td>This field is also optional. If you want to match the arguments, then check the checkbox near arguments field and specify the arguments. Otherwise leave this field empty. (Eg.: <code>--defaults-file=&quot;my.ini&quot;</code>)</td>
</tr>
</tbody>
</table>
List All Processes/Processes by Disk Read/Processes by Disk Write/Processes by Memory Usage/Processes by CPU Usage

Provides the list of active services, processes by disk read/disk write/Memory usage/CPU usage.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select devices icon to select the device.</td>
</tr>
</tbody>
</table>

Start Process

Starts a process.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select devices icon to select the device.</td>
</tr>
<tr>
<td>Start Directory</td>
<td>The directory from where you want to execute the process.</td>
</tr>
<tr>
<td>Process Command</td>
<td>Command to start the process.</td>
</tr>
</tbody>
</table>

Stop Process

Stops a process running on a device.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select devices icon to select the device.</td>
</tr>
<tr>
<td>Process Name</td>
<td>Name of the process that you want to test. Either you can enter the process name right away (Eg.: mysqld-nt.exe) or you can use the select icon to select the process from the remote devices.</td>
</tr>
<tr>
<td>Path</td>
<td>This field is optional. If you want to match the path while terminating the process, then check the checkbox near path field and specify the full executable path with process name. Otherwise leave this field empty. Ex: C:\Program Files\MySQL\MySQL Server 5.0\bin\mysqld-nt.exe</td>
</tr>
<tr>
<td>Arguments</td>
<td>This field is also optional. If you want to match the arguments when terminating the process, select the checkbox near arguments field and specify the arguments. Otherwise leave this field empty. Ex: --defaults-file=&quot;my.ini&quot;</td>
</tr>
</tbody>
</table>

Check URL

Check whether the URL for its availability.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>URL Address</td>
<td>Address of the HTTP URL that has to be queried.</td>
</tr>
<tr>
<td>Supported Variables:</td>
<td>- $(Alarm.URLAddress) - will retrieve the URLAddress from the alarm entity, if workflow is triggered through alarm. Otherwise nothing will happen.</td>
</tr>
<tr>
<td>Form Method: Get or Post</td>
<td>OpManager tests the URL via Get or Post method. Select the appropriate condition.</td>
</tr>
<tr>
<td>Search and Match Content</td>
<td>The content specified here is verified for its presence in the web page.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Timeout interval for the URL. Default value is 25 seconds. Click on check now button to verify the URL.</td>
</tr>
<tr>
<td>URL Authorization Details</td>
<td>Provide the username and password for URLs that require authentication.</td>
</tr>
<tr>
<td>Check Now</td>
<td>Checks whether the URL is accessible with the entered details.</td>
</tr>
</tbody>
</table>

FTP Delete File

Deletes a file via FTP.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>FTP Server</td>
<td>Name of the FTP Server. You can enter the ftp server name directly or use $(DeviceName)\ variable. $(DeviceName) will be replaced with the name device selected in the Info tab, during the workflow execution.</td>
</tr>
<tr>
<td>FTP Username</td>
<td>Username of the FTP server.</td>
</tr>
</tbody>
</table>
### FTP Password
Password to connect to the FTP server.

### File Name
Name of the file to be deleted. Enter the file name with the path.

### FTP Move File
Move a file to another directory within the same system via FTP.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>FTP Server</td>
<td>Name of the FTP Server. You can enter the ftp server name directly or use ‘${DeviceName}’ variable. ‘${DeviceName}’ will be replaced with the name device selected in the Info tab, during the workflow execution.</td>
</tr>
<tr>
<td>FTP Username</td>
<td>Username of the FTP server.</td>
</tr>
<tr>
<td>FTP Password</td>
<td>Password to connect to the FTP server.</td>
</tr>
<tr>
<td>File Name</td>
<td>Name of the file to be moved. Enter the file name with the path.</td>
</tr>
<tr>
<td>Destination Folder</td>
<td>Destination folder where the file to has to be moved. Enter the path.</td>
</tr>
</tbody>
</table>

### FTP Rename File
Renames a file via FTP.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>FTP Server</td>
<td>Name of the FTP Server. You can enter the ftp server name directly or use ‘${DeviceName}’ variable. ‘${DeviceName}’ will be replaced with the name device selected in the Info tab, during the workflow execution.</td>
</tr>
<tr>
<td>FTP Username</td>
<td>Username of the FTP server.</td>
</tr>
<tr>
<td>FTP Password</td>
<td>Password to connect to the FTP server.</td>
</tr>
<tr>
<td>Source File</td>
<td>Name of the file to be renamed. Enter the file name with the path. Eg.: /root/OpManager/backup/Backup_DB.zip</td>
</tr>
<tr>
<td>New Name</td>
<td>New name for the file. Eg.: Backup_DB_Old.zip</td>
</tr>
</tbody>
</table>

### FTP Upload File
Writes the given content in a file (.txt) and uploads it to the remote device via FTP.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>FTP Server</td>
<td>Name of the FTP Server. You can enter the ftp server name directly or use ‘${DeviceName}’ variable. ‘${DeviceName}’ will be replaced with the name device selected in the Info tab, during the workflow execution.</td>
</tr>
<tr>
<td>FTP Username</td>
<td>Username of the FTP server.</td>
</tr>
<tr>
<td>FTP Password</td>
<td>Password to connect to the FTP server.</td>
</tr>
<tr>
<td>Directory</td>
<td>Directory where the file has to be uploaded.</td>
</tr>
<tr>
<td>Content</td>
<td>Content/value that has to be uploaded.</td>
</tr>
</tbody>
</table>

### HTTP Post Data/Result
Posts the output received upon querying an URL, in the workflow logs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>URL Address</td>
<td>Address of the HTTP URL that has to be queried.</td>
</tr>
<tr>
<td>Supported Variables :</td>
<td></td>
</tr>
<tr>
<td>${Alarm.URLAddress}</td>
<td>will retrieve the URLAddress from the alarm entity, if workflow is triggered through alarm. Otherwise nothing will happen.</td>
</tr>
<tr>
<td>Form Method: Get or Post</td>
<td>OpManager tests the URL via Get or Post method. Select the appropriate condition.</td>
</tr>
<tr>
<td>Search and Match Content</td>
<td>The content specified here is verified for its presence in the web page.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Timeout interval for the URL. Default value is 25 seconds. Click on check now button to verify the URL.</td>
</tr>
<tr>
<td>URL Authorization Details</td>
<td>Provide the username and password for URLs that require authentication.</td>
</tr>
<tr>
<td>Check Now</td>
<td>Checks whether the URL is accessible with the entered details.</td>
</tr>
</tbody>
</table>
Check File
Checks the existence of a file in the specified path.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device or use $(DeviceName) variable. $(DeviceName) will be replaced with the name of the device that is selected in the Info &gt; Devices, during the workflow execution.</td>
</tr>
<tr>
<td>File Name</td>
<td>Name of the file that has to be checked for its existence. Specify the file name with its path.</td>
</tr>
</tbody>
</table>

Get File Size
Checks the file for its size and execute tasks accordingly.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device or use $(DeviceName) variable. $(DeviceName) will be replaced with the name of the device that is selected in the Info &gt; Devices, during the workflow execution.</td>
</tr>
<tr>
<td>File Name</td>
<td>Name of the file that has to be checked for its size. Specify the file name with its path.</td>
</tr>
<tr>
<td>File Size</td>
<td>The size of the file is compared with the value specified here. According to the condition (greater or lesser than) selected the actions are executed.</td>
</tr>
</tbody>
</table>

Compress File/Delete File
Compresses a file with Windows Compression/Deletes a file.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device or use $(DeviceName) variable. $(DeviceName) will be replaced with the name of the device that is selected in the Info &gt; Devices, during the workflow execution.</td>
</tr>
<tr>
<td>File Name</td>
<td>Name of the file that has to be compressed/deleted. Specify the file name with its path.</td>
</tr>
</tbody>
</table>

Compress Older Files/Delete Older Files
Compresses older files with Windows Compression/deletes older files.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device or use $(DeviceName) variable. $(DeviceName) will be replaced with the name of the device that is selected in the Info &gt; Devices, during the workflow execution.</td>
</tr>
<tr>
<td>Folder Name</td>
<td>Folder that contains the old files. Specify the folder path. Note: Delete older files option, deletes the older files in the sub folders also.</td>
</tr>
<tr>
<td>Files Older Than</td>
<td>Files older than the specified number of months/days/hours are compressed/deleted.</td>
</tr>
</tbody>
</table>

Copy File/Move File
 Copies/moves a file from one folder to another within the same computer.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device or use $(DeviceName) variable. $(DeviceName) will be replaced with the name of the device that is selected in the Info &gt; Devices, during the workflow execution.</td>
</tr>
<tr>
<td>File Name</td>
<td>Name of the file that has to be copied/moved to another folder. Specify the file name with its path. You can use the wild card character * (eg.: stderr*.txt) to do the action on all the files. You can also enter multiple files separated by a comma.</td>
</tr>
</tbody>
</table>
### Destination Folder
Name of the folder where the file has to be pasted/moved. Specify the folder path.

### Move Older Files
Moves files that match the age specified to another folder.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device or use <code>${DeviceName}</code> variable. <code>${DeviceName}</code> will be replaced with the name of the device that is selected in the Info-Devices, during the workflow execution.</td>
</tr>
<tr>
<td>Source Folder</td>
<td>Folder that contains the old files. Specify the folder path.</td>
</tr>
<tr>
<td>Destination Folder</td>
<td>Folder to which the old files have to be moved to.</td>
</tr>
<tr>
<td>Files Older Than</td>
<td>Files older than the specified number of months/days/hours are moved.</td>
</tr>
</tbody>
</table>

### Rename File
Renames a file.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device or use <code>${DeviceName}</code> variable. <code>${DeviceName}</code> will be replaced with the name of the device that is selected in the Info-Devices, during the workflow execution.</td>
</tr>
<tr>
<td>Source File Name</td>
<td>Specify the source file name to be renamed</td>
</tr>
<tr>
<td></td>
<td>Eg.: C:\Program Files\OpManager\backup\Backup_DB.zip</td>
</tr>
<tr>
<td>New Name</td>
<td>New name for the file.</td>
</tr>
<tr>
<td></td>
<td>Eg.: Backup_DB_Old.zip</td>
</tr>
</tbody>
</table>

### Uncompresses File
Uncompresses a file that had been compressed with Windows Compression.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device or use <code>${DeviceName}</code> variable. <code>${DeviceName}</code> will be replaced with the name of the device that is selected in the Info-Devices, during the workflow execution.</td>
</tr>
<tr>
<td>File Name</td>
<td>Name of the file that has to be uncompressed. Specify the file name with its path. You can use the wild card character * (eg.: stderr*.txt) to do the action on all the files. You can also enter multiple files separated by a comma.</td>
</tr>
</tbody>
</table>

### Check Drive Free Space
Checks the free space available in a drive.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device or use <code>${DeviceName}</code> variable. <code>${DeviceName}</code> will be replaced with the name of the device that is selected in the Info-Devices, during the workflow execution.</td>
</tr>
<tr>
<td>Drive Name</td>
<td>Name of the drive that has to checked for free space.</td>
</tr>
<tr>
<td>Drive Size</td>
<td>The size of the drive is compared with the value (GB/MB/KB) specified here. According to the condition (greater or lesser than) selected the actions are executed.</td>
</tr>
</tbody>
</table>

### Check Folder Exists
Checks the existence of a folder in the specified path.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device or use <code>${DeviceName}</code> variable. <code>${DeviceName}</code> will be replaced with the name of the device that is selected in the Info-Devices, during the workflow execution.</td>
</tr>
<tr>
<td>File Name</td>
<td>Name of the folder that has to be checked for its existence. Specify the folder path.</td>
</tr>
</tbody>
</table>
Get Folder Size
Checks the free space available in a drive.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device or use $(DeviceName) variable. $(DeviceName) will be replaced with the name of the device that is selected in the Info- Devices, during the workflow execution.</td>
</tr>
<tr>
<td>Folder Name</td>
<td>Name of the folder that has to be checked for its size.</td>
</tr>
<tr>
<td>Folder Size</td>
<td>The size of the drive is compared with the value (GB/MB/KB) specified here. According to the condition (greater or lesser than) selected the actions are executed.</td>
</tr>
</tbody>
</table>

Compress /Uncompress/Delete Folder
Compresses/uncompresses/deletes a folder.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device or use $(DeviceName) variable. $(DeviceName) will be replaced with the name of the device that is selected in the Info- Devices, during the workflow execution.</td>
</tr>
<tr>
<td>Folder Name</td>
<td>Folder that has to be compressed/uncompressed/deleted. Specify the folder path.</td>
</tr>
</tbody>
</table>

Create Folder
Creates a folder in the computer.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device or use $(DeviceName) variable. $(DeviceName) will be replaced with the name of the device that is selected in the Info- Devices, during the workflow execution.</td>
</tr>
<tr>
<td>Folder Name</td>
<td>Name of the folder that has to be created. Specify the folder name with its path.</td>
</tr>
</tbody>
</table>

Copy Folder/Move Folder
Copies/moves a folder to another folder within the same computer.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device or use $(DeviceName) variable. $(DeviceName) will be replaced with the name of the device that is selected in the Info- Devices, during the workflow execution.</td>
</tr>
<tr>
<td>Folder Name</td>
<td>Name of the folder that has to be copied/moved to another folder. Specify the file name with its path.</td>
</tr>
<tr>
<td>Destination Folder</td>
<td>Name of the destination folder where the source folder has to be pasted/moved. Specify the folder path.</td>
</tr>
</tbody>
</table>

List Files
List the files available in a folder.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device or use $(DeviceName) variable. $(DeviceName) will be replaced with the name of the device that is selected in the Info- Devices, during the workflow execution.</td>
</tr>
<tr>
<td>Folder Name</td>
<td>Name of the folder whose files has to be listed. Specify the folder path.</td>
</tr>
</tbody>
</table>

Rename Folder
 Renames a folder.
Add Alarm Note

Adds note to an alarm.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Note</td>
<td>Note that has to be added to the alarm.</td>
</tr>
<tr>
<td></td>
<td>Supported Variables :</td>
</tr>
<tr>
<td></td>
<td>$(Result) - will be replaced with the previously executed task's result.</td>
</tr>
</tbody>
</table>

Generate Alarm

Generates an alarm in OpManager.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>Source</td>
<td>Note that has to be added to the alarm.</td>
</tr>
<tr>
<td></td>
<td>Supported Variables :</td>
</tr>
<tr>
<td></td>
<td>$(Result) - will be replaced with the previously executed task's result.</td>
</tr>
<tr>
<td>Severity</td>
<td>Select the severity of the alarm.</td>
</tr>
<tr>
<td>Message</td>
<td>Message that you want to display in the alarm.</td>
</tr>
<tr>
<td>Alarm Code</td>
<td>Unique string used to trigger the event. Eg.: Threshold-DOWN</td>
</tr>
<tr>
<td>Entity</td>
<td>Uniquely identifies the failure object within the source. Events will be correlated into alarms according to the entity field. Multiple events with the same entity will be grouped as a single alarm.</td>
</tr>
<tr>
<td>Event Type</td>
<td>Description of the event type</td>
</tr>
</tbody>
</table>

Execute Linux Script

Execute script on remote Linux machines and retrieves the output. Depending on the input, this script will either execute from OpManager server or from remote machine. Its success/failure is decided based on its exit code. If the script returns with the exit code 0, then it is considered as success, any other value is considered as failure.

Eg.: For shell script,
    exit(0) -- Success
    exit(1) -- Failure
    exit(-2) -- Failure
Command Line
Specify the command used to execute the script.
Eg.: sh $(FileName) $(DeviceName) arg1
Here, $(FileName) variable is a must to execute the script. OpManager will replace this variable during runtime.
Supported Variables:
$(DeviceName) - will replace the executing devicename during runtime.
$(UserName) - will replace the device username if already given for this device.
$(Password) - will replace the device password if already given for this device.

Script Body
The actual script that has to be executed.

Advanced
Click on Advanced button to configure the following fields.

Execute from Remote Machine
If this option is checked, the script is pushed to remote machine and will be executed. Otherwise it will be executed from OpManager server.

Working Directory
Specify the directory from where you want to execute the script.
Supported Variables:
$(UserHomeDir) - will replace the user's home directory during runtime.
$(TempDir) - will replace device temp directory during runtime. Eg: /tmp

Response Timeout
Time to wait for the script to complete its execution. The default value given here is 60 seconds.

Execute Windows Script
Execute the script on remote Windows machines from OpManager server and retrieves the output. Its success/failure is decided based on its exit code.
If the script returns with the exit code 0, it is considered as success, any other value is considered as a failure.

Eg.: for VBscript:
WScript.Quit(0) -- Success
WScript.Quit(1) -- Failure
WScript.Quit(-2) -- Failure

Parameter | Description
--- | ---
Name | Display name for the task.
Destination Device | Device on which the task has to be executed. Click on the select device icon to select the device or use $(DeviceName) variable. $(DeviceName) will be replaced with the name of the device that is selected in the Info-Devices, during the workflow execution.
Command Line | Specify the command used to execute the script.
Eg.: cscript $(FileName).vbs $(DeviceName) $(UserName) $(Password) arg1
Here, $(FileName) variable is a must to execute the script. OpManager will replace this variable during runtime.
Supported Variables:
$(DeviceName) - will replace the executing devicename during runtime.
$(UserName) - will replace the device username if already given for this device.
$(Password) - will replace the device password if already given for this device.
Script Body | The actual script that has to be executed.
Advanced | Click on Advanced button to configure the following fields.
Working Directory | Specify the directory from where you want to execute the script.
Supported Variables:
$(UserHomeDir) - will replace the user's home directory during runtime.
$(TempDir) - will replace OpManager temporary directory during runtime.
Response Timeout | Timeout interval for the response from the device for the script execution status.

Log a Ticket (Remedy)
Logs a ticket in BMC Remedy.

Parameter | Description
--- | ---
Name | Display name for the ticket.
From Email ID | Email ID of the sender.
Service Desk Mail ID | Email ID of BMC Remedy service desk.
Impact | Select the impact level of the ticket.
Urgency | Select the severity of the ticket.
Summary | Add summary for quick understanding of the issue reported.
Description | Describe the issue.

Log a Ticket (SDP)
Logs a ticket in ManageEngine ServiceDesk Plus. Ensure that ServiceDesk Plus is integrated with OpManager.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the ticket.</td>
</tr>
<tr>
<td>Category</td>
<td>Select the appropriate category for the ticket.</td>
</tr>
<tr>
<td>Sub Category</td>
<td>Select the appropriate sub category.</td>
</tr>
<tr>
<td>Item</td>
<td>Select the appropriate item.</td>
</tr>
<tr>
<td>Priority</td>
<td>Select the priority level of the ticket.</td>
</tr>
<tr>
<td>Group</td>
<td>Select the group.</td>
</tr>
<tr>
<td>Technician</td>
<td>Select the technician to whom you want to assign the ticket.</td>
</tr>
<tr>
<td>Title</td>
<td>Subject of the ticket. You can use variables.</td>
</tr>
<tr>
<td>Description</td>
<td>Describe the issue. You can use variables.</td>
</tr>
</tbody>
</table>

Send Mail
Sends a mail to the email IDs specified. This is useful to notify the result/completion of a task in the workflow.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name for the task.</td>
</tr>
<tr>
<td>From Email ID</td>
<td>Email ID of the sender.</td>
</tr>
<tr>
<td>To Email ID</td>
<td>Email ID of the recipients.</td>
</tr>
<tr>
<td>Mail Format</td>
<td>Email can be sent in plain text or html or in both the formats. Select the required format.</td>
</tr>
<tr>
<td>Subject</td>
<td>Subject of the email. You can use variables.</td>
</tr>
<tr>
<td>Message</td>
<td>Content of the email. You can use variables.</td>
</tr>
</tbody>
</table>

Send Popup Message
Opens a popup window with the given message on remote computers.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info- Devices, during the workflow execution.</td>
</tr>
<tr>
<td>Message</td>
<td>Message that has to be displayed in the popup.</td>
</tr>
</tbody>
</table>

Send SMS
Sends SMS notifications to the mobile number specified. This is useful to notify the result/completion of a task in the workflow.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Device</td>
<td>Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info- Devices, during the workflow execution.</td>
</tr>
<tr>
<td>Message</td>
<td>Message that has to be sent as an SMS. Message should not exceed 160 characters.</td>
</tr>
</tbody>
</table>

Variables:
Variables are used to append dynamic values in a field of a task. Following are the variables:

\${DeviceName} - Name of the device to which workflow has to be associated. Can be used in all fields.
\${WorkflowName} - Name of the Workflow that is to triggered. Can be used in all fields.
\${Result} - Result of previous task.
\${Alarm.ServiceName} - Name of the service for which an alarm is raised.
\${URLAddress} - URL address
\${Alarm.URLAddress} - URL address for which an alarm is raised.
\${UserName} - Username of the device.
\${Password} - Password of the device.
\${Device.DisplayName} - Display name of the device for which an alarm is raised.
\${Alarm.ProcessName} - Name of the process for which an alarm is raised.
Using Variables

Variables can be better understood with an example. Following is the workflow that has to be triggered as an action whenever a service down alarm is raised.

Task 1: ‘Test a service’ task is created to test the service that is down. When the workflow is triggered, the variable \(\text{${Alarm.ServiceName'}\) is replaced with the name of the service that has gone down. \(\text{${DeviceName}}\) is replaced with the name of device.

Task 2: The result of previous task (service up or down) is added as notes to the alarm using \(\text{${Result}}\) variable.
Add Alarm Note

Name: Add Alarm Note

Note: ${Result}
Adding a Workflow

To add a workflow, follow the steps given below:

1. Click on Workflows on the left pane and select New Workflow.
2. Drag and drop the required conditions and actions from the left panel to editor panel.

1. Enter a Name for the condition and actions.
2. To edit or delete a condition or action, click on it and select edit or delete icon.
1. Click **Trigger** at the top of the page.

2. Associate the workflow to the devices.
   a. Click on the **Devices** tab.
   b. Select the devices in Available Devices column and move to Selected devices column. Use the search box to search the devices.
   c. Click **Next**

3. Configure the alarm trigger to trigger a workflow when an alarm is raised or configure schedule trigger if you want to schedule this workflow for periodical execution.
   a. Click on the **Trigger** tab.
   b. Click on the **Alarm Trigger** option. Select the required criteria. Executes this workflow on the associated devices, if any of the criteria is satisfied.
   c. Schedule the workflow execution. Click on the **Schedule Trigger** option. Configure the date and time.
   d. Click **Next**

4. Configure the delayed and recurring triggering of workflow
   a. Enter a **Name**, **Description**, and **Tags** for the workflow.
   b. Define Time: Select either **Apply this profile all time** or **Apply this profile during the below mentioned time window**. Selecting the latter keeps the Workflow active only during the specified days and hours.
   c. Delayed Trigger: If you want the workflow to be triggered at a delay, enter the delay time (in minutes). If you don't want to trigger the workflow if the alarm has been acknowledged in the mean time, you can select the 'Do not trigger if alarm is acknowledged' check box.
   d. Recurring Trigger: This option helps you trigger the workflow at regular intervals, till the alarm is cleared. Enter the trigger interval and number of triggers. If you don't want to trigger the workflow repeatedly if the alarm has been acknowledged, you can select the 'Do not trigger if alarm is acknowledged' check box.
   e. Click **Save**

The workflow has been successfully added. It will be executed on the associated devices at the scheduled time or when any of the criteria selected is satisfied. You can check the output of the workflow in the Workflow Logs.

**Sample Workflow**

Following is a sample workflow which helps gets executed automatically when a device down alarm is raised. This workflow sends ping request, if passed does DNS Lookup and adds the output as notes to the alarm.
Workflow Execution Logs for the sample workflow: Click on **Workflows** from the left pane and select **Workflow Logs**

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Message</th>
<th>Severity</th>
<th>Date &amp; Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping Device</td>
<td>Ping command used was : ping -n 4 -w 1000 -i 32 172.21.153.153</td>
<td>Info</td>
<td>09/02/16 17:41</td>
</tr>
<tr>
<td></td>
<td>Ping output :</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ping: 172.21.153.153 with 32 bytes of data:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reply from 172.21.153.153: bytes=32 time&lt;1ms TTL=128</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reply from 172.21.153.153: bytes=32 time&lt;1ms TTL=128</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reply from 172.21.153.153: bytes=32 time&lt;1ms TTL=128</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ping statistics for 172.21.153.153:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Approximate round trip times in mili-seconds:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Minimum = 0ms, Maximum = 0ms, Average = 0ms</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ping Device</td>
<td>Ping was successful.</td>
<td>Info</td>
<td>09/02/16 17:41</td>
</tr>
<tr>
<td>Add Alarm Note</td>
<td>Task input does not have an alarm entity associated with it.</td>
<td>Error</td>
<td>09/02/16 17:41</td>
</tr>
</tbody>
</table>

**Editing a Workflow**

To edit a workflow, follow the steps given below:

1. Click on **Workflows** from the left pane and click on the respective workflow name to edit.
2. The workflow panel opens. Click **Trigger** button on top to perform the changes you want to do and click **Next**.
3. Modify the name, description, tags, associated devices, schedule, and alarm trigger options if required.
4. Click **Save**
Executing Workflows

Before executing a workflow, ensure that you have associated the workflow to the devices. To execute a workflow:

1. Click on Workflows from the left pane. All the created workflows are listed.
2. Click against the Execute icon on the respective workflow.
3. There is also an option to execute the workflow from the device page. Go to Device page > Workflow > click against the execute icon on the respective workflow.
Workflow Execution Logs

Workflow Logs provide the output of the executed workflows. It provides the result as well the data of each task that had been included in the workflow.

To view Workflow logs

- Click on **Workflows** from the left pane and select **Workflow Logs**. Workflow output for each of the associated device is listed along with the executed date & time and number of tasks.

### Severity

Each task once executed is logged with its severity for understanding its execution status. Following are the severities in Workflow:

- **Info**: Notifies a task has been executed successfully.
- **Error**: Notifies a task has been failed.
- **Warning**: Notifies that a task cannot be performed. Eg.: A delete file action cannot be performed when the directory does not have the specified file. In such cases, the delete file actions is marked as warning.
Alert Actions

You can perform the following alert actions:

**Acknowledge**: This option is useful for the operators to pick up the problem and work on it. When you select an alarm and click on Acknowledge button on top the alarms list, the administrator/operator’s name is populated in the technician's field.

*Note: Alarms that are acknowledged can be excluded from being escalated by configuring accordingly the [alarm escalation rule](#).*

**Unacknowledge**: The assigned technician is removed and the alarm is back in the unassigned list.

**Clear**: You can click this to clear an alarm manually.

**Delete**: You can delete an alarm.

**View History**: Click on the alarm message to view the alarm details and event history.

**Add Notes**: You can add notes to the alarms to explain the steps you have followed to correct the fault or to give tips to the operator who is working on the fault. In the Alarm history page, click the Add Notes option.

**Execute Workflow**: You can execute a workflow to troubleshoot an alarm. Click on Execute Workflow in the Alarm Details page, and select the workflow. The workflow will be executed and the output will be added in the notes.

**Test Actions**: You can notify this alarm via any of the notification profiles created by you. Click on Test Actions in the Alarm Details page, and select the desired notification profile.

**View Availability**: You can view the availability history of the faulty device. Click on More link in Alarm Details page and select Availability.

**Ping**: You can ping the faulty device by clicking on the Ping icon from the top of the Alarm Details page.

**Trace Route**: You can trace route the faulty device by clicking on the Trace Route icon from the top of the Alarm Details page.

**Unmanage**: Alarms created for devices that are under maintenance can be can be avoided by moving the device to unmanaged state. Click Actions> Select Unmanage from Alarm Details page.

**Configure Notifications**: You can configure a notification profile to the faulty devices. Click Actions> Configure Notifications from Alarm Details page.
Configuring Notifications

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.

The different types of notifications available are:

- Email
- SMS
- Run a Program
- Run a System Command
- Log a Ticket (Trouble ticketing in ServiceDesk Plus)

The configured notification settings are available as profiles and these can be associated to different devices for different fault criteria.
**Escalating Alarms**

The alarms of critical devices should not be left unnoticed for a long time. For instance, the mail-servers, web-servers, backup-servers, switches, and routers are so critical that if their faults are not solved within a specified time, the networking functionality will be brought down. You can configure OpManager to escalate such unnoticed alarms by sending an e-mail to the person concerned. However, you have an option to exclude the alarms that are acknowledged from being escalated.

To configure a new alarm escalation rule, follow the steps given below:

1. Click **Settings > Monitoring > Configuration > Alarm Escalation Rules**.
2. Click **Add Rule** to create a rule.
3. Assign a name to the rule in the **Rule Name** field.
4. Select the **Severity** and **Category** of the alarm.
5. Select the **Business View** in order to associate the rule only to the alarms of the devices of the selected business view. If not select None to associate the rule to the alarms of all the devices.
6. Then configure the the interval (**Not Cleared Within**) in either hours or minutes to wait for the alarm to get cleared.
7. In the **Run this check every** box, set the interval in minutes to execute this rule.
8. You can exclude the acknowledged alarms from being escalated by selecting **Exclude Acknowledged Alarms** option.
9. Type the values for the fields under **Notifications** > **Email** to send an e-mail if the alarm is not cleared within the specified interval.
10. Configure the **To Email Address**, **From Email Address**, the **Subject** and the **Message** of the escalation mail.
11. Type the values for the fields under **Notifications** > **SMS** to send a SMS if the alarm is not cleared within the specified interval.
12. Configure the **Mobile Number** and **Message** of the escalation SMS.
13. Click **Save**.

If you configure a new alarm escalation rule, by default it will be enabled. To disable an alarm escalation rule click on Edit icon, deselect the **Enable this rule** option and click on Ok.
Managing Faults in Network

There can various types of faults in a network. With the network health depending on various resources like the system resources, services, network connectivity etc, getting to the root of the problem is simplified when the monitoring solution raises meaningful alarms. OpManager helps you identify the fault quickly with its detailed alarms indicating the resource that is poorly performing in the device. The different types of OpManager alarms include:

- Status-poll Alarms (device, service, interface, port down alarms).
- Threshold-based alarms for host resources, response times etc proactive monitoring.
- Alarms from SNMP Traps.
- Windows event logs based alarms.

OpManager monitors the resources for availability and performance and triggers alarms for all the criteria mentioned above. These alarms can also be sent as email or sms alerts from OpManager.
Processing SNMP Traps into Alarms

- What is SNMP Trap?
- Processing Traps into Alarms
- Tools
- Adding/Modifying Trap Processor
- Loading Trap Parsers from a MIB
- Processing Unsolicited Traps
- Configuring SNMP Traps in Agent

What is SNMP Trap?
Traps are cryptic messages of a fault that occurs in an SNMP device. SNMP traps are alerts generated by agents on a managed device. These traps generate 5 types of data:

- Coldstart or Warmstart: The agent reinitialized its configuration tables.
- Linkup or Linkdown: A network interface card (NIC) on the agent either fails or reinitializes.
- Authentication fails: This happens when an SNMP agent gets a request from an unrecognized community name.
- egpNeighborloss: Agent cannot communicate with its EGP (Exterior Gateway Protocol) peer.
- Enterprise specific: Vendor specific error conditions and error codes.

Processing SNMP Traps into Alarms
OpManager enables you to process the traps from the managed devices.

- When a trap is received from a managed device, the match criteria in the parser determines whether a specific trap matches the conditions specified in the Trap Processor. Once a matching Trap is found, an alert is generated.
- Trap Processor Converts the cryptic message to human-readable alarm.
- Configure OpManager to process the traps that are not processed out-of-the-box and convert them into alarms.
- The traps that are not processed are listed under 'Unsolicited Traps'.

Tools
The following actions can be done by clicking the relevant icon:

- Edit: Edit the Trap
- Enable or disable trap processing: Click to enable/disable trap processing
- Delete processor: Delete the Trap Processor

Adding/Modifying Trap Processor
Go to Settings > Monitoring > Configuration > Monitors > Traps.
Click ‘Add New’ to add a new trap.
Click the TrapParser name/ Edit icon to modify an existing one.
Configure/Modify the following properties:
- Name: Configure a name for the new trap processor.
- Description: Describe the trap.
- Snmp Trap Version: Select the version (SNMP V1/V3).
- SNMP V1 Properties:
  - Generic Type: Cold Start, Link Up, Enterprise, etc. Select the appropriate type for the OID
  - Specific Type: When Generic Type is set to Enterprise a specific trap ID is identified
  - Trap OID: For devices with SNMP v2c version, select the trap oid from the MIB using the Select button.
  - Severity: Select the Alarm severity.
- Failure Component: This option is useful when you deal with a single trap OID that has multiple failure components. The Varbinds containing more details on the trap will
  have information on the failed components (entities like cpu, temperature etc). You can match the entity too by appending the VarBind number in this field to generate
separate alarms for the failed components. For instance, $Source\_trapName\_trap\_v5$.

**Source:** Append the Varbinds to be matched if required. This option is useful if the trap is forwarded from another source.

**Message:** Select the required message variables

**Match Criteria:** Select the appropriate radio button to either match any one or all the conditions that you specify. Select the variable bindings, the condition, and the string to be matched.

**Rearm Criteria:** Similarly, select the appropriate radio button to match the reararm conditions. Select the variable bindings, the condition, and the string to be matched.

**SNMP V3 Properties:**

**Trap OID:** For devices with SNMP v3 version, select the trap oid from the MIB using the Select button.

**Severity:** Select the Alarm severity.

**Failure Component:** This option is useful when you deal with a single trap OID that has multiple failure components. The Varbinds containing more details on the trap will have information on the failed components (entities like cpu, temperature etc). You can match the entity too by appending the VarBind number in this field to generate separate alarms for the failed components. For instance, $Source\_trapName\_trap\_v5$.

**Source:** Append the Varbinds to be matched if required. This option is useful if the trap is forwarded from another source.

**Message:** Select the required message variables.

**Match Criteria:** Select the appropriate radio button to either match any one or all the conditions that you specify. Select the variable bindings, the condition, and the string to be matched.

**Rearm Criteria:** Similarly, select the appropriate radio button to match the rearm conditions. Select the variable bindings, the condition, and the string to be matched.

Click **Save** for the configuration to take effect.

**Loading Trap Parsers from a MIB**

Following are the steps to load the traps from various MIBs

Go to **Settings > Monitoring > Configuration > Monitors > Traps**. All the configured processors are listed here.

Click on **Load Traps From Mibs** at the top of the page.

From the list of MIBs, select the MIB from which you would like to load the trap variable. The traps in that MIB are listed.

Select the required trap variable, and click **Add**.

A Processor for the selected trap is added, and is listed under the **Traps** tab.

**How to process the Unsolicited Traps?**

Go to **Alarms ( ALT+A ) > Click on Unsolicited Traps**.

Click on Create Trap Processor corresponding to the trap message.

Type a name for TrapName.

Make sure that the status is enabled.

Select the Severity.

Click on Add.

**How to configure SNMP Traps in Agent?**

Despite configuring the SNMP Trap Processor in opmanager, you might still not see the alarms based on traps. You might need to check the SNMP agent configuration on the monitored devices.
Receiving SNMP Traps in OpManager

OpManager listens for SNMP traps from devices on the default port 162. So, it automatically acts as a trap receiver and based on the trap processors defined in OpManager, the traps are processed and shown as OpManager alarms.
Alarm Suppression

OpManager provides you the option to suppress the alarms of the devices for a pre-defined time interval. This option will be very useful in cases, where the devices are under maintenance or some known issues exist with them.

Configuring Alarm Suppression for a Single Device

1. Go to the device snapshot page.
2. Click on Actions and select Suppress Alarms.
3. Select the period for which you want to suppress the alarm.

Alarms of this device will be suppressed for the selected period.

To configure the Alarm Suppression in a bulk

1. Go to the respective List View page (Server, Router, Switch etc) > Inventory ( alt+i ) > Sort By Category.
2. Select the devices that you wish to suppress the alarms.
3. Click Actions > Suppress Alarms > Select the period for which you want to suppress the alarm.
Viewing Alerts

The Alarms tab in OpManager shows all the latest alerts. From the list box on the top right corner, you can access the following:

- **All Alarms**: A complete list of alarms is displayed here.
- **Active Alarms**: This view lists only the active alarms that are not yet cleared.
- **Unsolicited Traps**: The unsolicited traps sent by the agents in the managed devices are listed here. These are the traps that are not configured to be processed in OpManager. If you find any of these traps to be critical, you can configure OpManager to process the traps using the information received from the agent. Refer to Creating a Trap Processor for details.
- **EventLog Alarms**: This view lists only the alarms that are triggered from Windows event logs as the source.
- **Syslog Alarms**: This view lists only the alarms logged via syslog.
Configuring Mail Server Settings

OpManager allows you to configure e-mail alerts and SMS alerts to get notified on the fault in your network. By default, OpManager sends the mail to the mail server specified in the e-mail notification profile. To configure the SMTP server settings globally and to provide the secondary mail server settings, follow the steps given below:

1. Go to Settings > Basic Settings, click Mail Server Settings.
2. Enter the SMTP Server name and Port number.
3. Configure the From and To Email ID fields.
4. Enter a Time Out interval.
5. Configure the User name and Password details, if the server requires authentication to send e-mail.
6. For SSL authentication, select the SSL Enabled check-box, browse and select the SSL certificate and key-in the password.
7. Click Save

Verifying Configuration

- To test the settings enter the Email ID and click Test Mail. This e-mail ID will be considered as the default To Email ID while creating Email and SMS notification profiles.
- If you have a secondary mail server in your network, select Add a secondary mail server and provide the details. In case of failure of primary mail server, OpManager uses secondary mail server to send e-mail and SMS.
Configuring Proxy Server Settings

Any business enterprise will have a proxy server to optimize its connectivity to Internet and to filter access to restricted Web sites. In OpManager, to monitor URLs over internet, you need to provide the proxy server details of your enterprise.

To enter the details, follow the steps given below:

1. Go to **Settings > Basic Settings**, click **Proxy Server Settings**.
2. Select the **Enable Proxy** check-box.
3. Enter the Proxy server name, port number in which the Web service is running on the proxy server, and the user name and password to connect to the proxy server.
4. For the devices that do not require to go through a proxy, specify the name or the IP Address of the devices as a comma separated list in the **No Proxy** field.
5. Click **Save** to save the details.
Forwarding Syslog

You can forward the syslog received in OpManager to any NMS.

Steps to forward syslog:

2. Click on Add Destination button.
3. Provide the Name/IP address of the NMS Host to which SysLog has to be forwarded.
4. Provide the SysLog listening port number of the NMS to which SysLog has to be forwarded.
5. Click on Start Forwarder to initiate sending of SysLog to the destination NMS. You can also Stop Forwarder at any desired time.
**Forwarding Traps**

Configure OpManager to notify users over a Trap when there is a specific fault.

Steps to forward Traps:

1. Go to **Settings > Monitoring > Configuration > Monitors > Traps > Forward Trap.**
2. Provide the **Name/IP address** of the host to which notifications has to be sent.
3. Provide the trap listening **port** number of the host to which notifications has to be sent.
4. Click **Save.**
Configuring Email Alerts

You can configure OpManager to send e-mail to network administrators when a fault is detected in the device. You can create separate profiles for each administrator and assign them to devices so that whenever the device has a fault, an e-mail is sent to the technician concerned.

To create an email alert profile, follow the steps given below:

1. Go to Settings > Monitoring > Configuration > Notifications.
2. Click Add.
3. Select the Notification type as Send Email.
4. Provide the To and From Email Address, Subject and Message (select the required alarm variables which is to be displayed on the email subject and message). Click Next.
5. Select the fault criteria for which you need to be notified. For instance, if you want to be notified of threshold violation, select 'Threshold rule is violated'. Additionally notify only when any or all the severity: Critical, Trouble, Attention, Service Down. Click Next.
6. Select the devices either By Category or By Business View or By Devices and click Next.
7. Select the required Time Window, Delayed Trigger and Recurring Trigger and click Next.
8. Give a profile name and Click Test Action to test the email profile or Save to save the profile.

The profile is associated to the selected devices. A notification is sent every time a threshold is violated for a server.

Note: Primary and secondary SMTP server settings can be provided in the Mail Server Settings page in OpManager. Whenever a new email profile is created, the values of the primary SMTP server and the authentication details are retrieved from the Mail Server settings. Refer to Configuring Mail Server Settings for steps to enter the details. If the SMTP server is not available while sending e-mail, secondary mail server is used to send the mail automatically.
Using a Run Program Notification Profile

You can configure OpManager to automatically run a program whenever a fault is detected in the device. For instance, you can configure OpManager to execute a program that corrects the fault or simply produces a sound or that whenever a specific type of an alarm is raised for a device.

To create a profile that executes the specified program, follow the steps given below:

1. Go to Settings > Monitoring > Configuration > Notifications.
2. Click Add.
3. Select the Notification type as Run Program.
4. In the Command Name field, specify the name of the program to be executed with the absolute path. Example C:profilestestprogram.bat.
5. If the program requires some arguments, specify the Program Arguments, Message Variables and click Next.
6. Select the fault criteria for which you need to be notified. For instance, if you want to be notified of threshold violation, select 'Threshold rule is violated'. Additionally notify only when any or all the severity: Critical, Trouble, Attention, Service Down. Click Next.
7. Select the devices either By Category or By Business View or By Devices and click Next.
8. Select the required Time Window, Delayed Trigger and Recurring Trigger and click Next.
9. Give a profile name and Click Test Action to test the email profile or Save to save the profile.

The profile is associated to the selected devices. The program is executed with the specified arguments whenever a fault matching the selected criteria occurs.
Using a Run Command Notification Profile

You can configure OpManager to automatically run a system command whenever a fault is detected in the device. For instance, you can configure OpManager to execute a netsend command to send popup messages to users machines whenever a specific type of an alarm is raised for a device.

To create a profile that executes the specified program, follow the steps given below:

1. Go to **Settings > Monitoring > Configuration > Notifications**.
2. Click **Add**.
3. Select the Notification type as **Run System Command**.
4. In the **Command String** field, specify the command name with additional arguments if any.
5. Select the **Err Append** and **Append** check-boxes to append the output and the error message on executing the command.
6. Select the fault criteria for which you need to be notified. For instance, if you want to be notified of threshold violation, select 'Threshold rule is violated'. Additionally notify only when any or all the severity: Critical, Trouble, Attention, Service Down. Click **Next**.
7. Select the devices either **By Category** or **By Business View** or **By Devices** and click **Next**.
8. Select the required **Time Window, Delayed Trigger** and **Recurring Trigger** and click **Next**.
9. Give a profile name and Click **Test Action** to test the email profile or **Save** to save the profile.

The system command is executed with the specified arguments whenever a fault matching the selected criteria occurs.
Notifications via Traps

Configure OpManager to notify users over a Trap when there is a specific fault.

Steps to configure a trap profile:

1. Go to Settings > Monitoring > Configuration > Notifications.
2. Click Add.
3. Select the Notification type as Trap Profile.
4. Provide the Host Name, Host Port, Version (SNMP version), Community (SNMP read community string) and Varbinds if any. Click Next.
5. Select the fault criteria for which you need to be notified. For instance, if you want to be notified of threshold violation, select 'Threshold rule is violated'. Additionally notify only when any or all the severity: Critical, Trouble, Attention, Service Down. Click Next.
6. Select the devices either By Category or By Business View or By Devices and click Next.
7. Select the required Time Window, Delayed Trigger and Recurring Trigger and click Next.
8. Give a profile name and Click Test Action to test the email profile or Save to save the profile.

You have successfully configured the notification profile.
SysLog Notification Profile

When any fault occurs you can notify users via SysLog.

Steps to configure a SysLog profile:

1. Go to Settings > Monitoring > Configuration > Notifications.
2. Click Add.
3. Select the Notification type as Send SysLog.
4. **Destination Host**: Provide the Name/IP address of the host to which notifications has to be sent.
5. **Destination Port**: Provide the SysLog listening port number of the host to which notifications has to be sent.
6. **Severity**: You can choose any of SysLog severity events to be processed.
7. Select the **Facility** and required **Message Variables**. Click Next
8. Select the fault criteria for which you need to be notified. For instance, if you want to be notified of threshold violation, select 'Threshold rule is violated'. Additionally notify only when any or all the severity: Critical, Trouble, Attention, Service Down. Click Next
9. Select the devices either **By Category** or **By Business View** or **By Devices** and click Next.
10. Select the required **Time Window**, **Delayed Trigger** and **Recurring Trigger** and click Next.
11. Give a profile name and Click **Test Action** to test the email profile or **Save** to save the profile.

You have successfully configured the notification profile.
Modifying and Deleting Notification Profiles

You can modify or remove an existing notification profile. Here are the steps:

1. Go to Settings > Monitoring > Configuration > Notification.
2. All the configured profiles are listed here.
3. Click the Delete icon against the profiles name to delete the profiles.
4. Click on the profiles name to modify the profile properties.

The changes made here are applied for all the devices to which the profile is associated.
About Reports

Intuitive dashboards and detailed reports helps you determine the performance of your network in very less time. OpManager allows you to export the default reports to other file formats such as exporting to PDF or XLS. You can also schedule the reports to be emailed or published. The default reports available in OpManager include:

- **System**: Provides a complete report on all the system related activities of all the devices. This category of reports include All Events, All Down Events, SNMP Trap Log, Windows Event Log, Performance Monitor Log, Notification Profiles Triggered, Downtime Scheduler Log, Schedule Reports Log, All Alerts and All Down Alerts.

- **Health and Performance**: Gives you a detailed report on the health and performance of all/top N devices.

- **Availability and Response**: Gives you a detailed report on the availability and the response time of all/top N devices

- **Inventory**: Inventory reports are available for servers, desktops, all devices, SNMP-enabled devices and non-SNMP devices.

- **My Favourites**: OpManager provides the option to categorize all your important and frequently viewed reports as your favorites.

- **Schedule Reports**: OpManager allows you to schedule a new report and also to schedule a generated report.

- **Custom Report Builder**: custom report builder is the easiest way to generate report using only the data that you want. This stages in four types (Category, Devices, Moinitors, Time Period and Graph or Table view)
Viewing Interface Reports

Interface reports help you to determine the health of the interface by generating detailed reports on In and Out Traffic, In and Out Errors and Discards, Bandwidth & Outage Report, At-a-Glance Report etc. The reports can be exported to PDF format, taken printouts or emailed by clicking the respective icons. To generate the interface reports, follow the steps given below:

1. Go to the snapshot page of the interface whose health report you want to generate.
2. Go to Reports > available on the left pane of the page. All the default reports that can be generated are listed.
3. Click on the name of the required report to generate current day’s report. Click on the 7 or 30 days icon to generate the report for the last 7 or 30 days respectively.
Business View-based Reports

OpManager provides an intuitive Availability Dashboard for your business view. You can track the fault to the root in no time.

To access the business view dashboard, follow the steps below:

1. Go to the required business view.
2. Click on the Dashboard tab. The business view dashboard shows the availability distribution and also the least available devices in that view.
3. Click on the bar indicating a problem to drill down to the actual fault.
4. You can also view the dashboard for various periods like the last 24 hours, or last few days to analyze the trend.
Creating New Reports

Apart from the 100+ available default reports you could also create a new report based on the data that you want. To create a new report follow the steps given below:


2. Enter a unique Name and brief Description.

3. Select the required Report Category. For instance, the report category is selected as Performance Reports.

4. Click Next.
2. Select the **Monitor category**.
3. Select the sub category.
4. Click **Next**.
### Create New Report

<table>
<thead>
<tr>
<th>Input</th>
<th>Metrics</th>
<th>Default Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Input Icon]</td>
<td>![Metrics Icon]</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Business View</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>All Devices</td>
<td></td>
</tr>
<tr>
<td>Show</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Only Top</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Period</td>
<td>Time Window</td>
<td></td>
</tr>
<tr>
<td>Last 30 days</td>
<td>Full 24 hours</td>
<td></td>
</tr>
</tbody>
</table>

6. Select the required **Category**, **Business Views**, **Show All or Top/Bottom N Devices**, **Period** and **Time Window**.

7. Click **Save** to create the new report.

The created report gets saved under the appropriate report category. Go to that category and click on the report to generate the report.
Editing Reports

OpManager allows you to edit a generated report in order to refine for some specific parameters, devices or time periods. To edit a generated report follow the steps given below:

1. Go to Reports > Default Reports > Select the category > Click against the report name that you wish to edit.
2. Click **Edit Report** button available on the top right of the report page.
3. Change the required fields. The various fields that can be altered are Category, Period, Business Views, Time Window.

### Notification Profiles Applied

<table>
<thead>
<tr>
<th>Category</th>
<th>Business View</th>
<th>Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Devices</td>
<td>All Devices</td>
<td></td>
</tr>
</tbody>
</table>

**Time Window** : Generated at : 10/02/16 20:56

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boopathy_Mail_test</td>
<td>1</td>
</tr>
<tr>
<td>ClickATellPF</td>
<td>1</td>
</tr>
<tr>
<td>FILENP</td>
<td>1</td>
</tr>
<tr>
<td>G3</td>
<td>1</td>
</tr>
<tr>
<td>GGG1</td>
<td>1</td>
</tr>
<tr>
<td>GGGGG2</td>
<td>1</td>
</tr>
<tr>
<td>Play Sound</td>
<td>1</td>
</tr>
<tr>
<td>RunSysCmdNF</td>
<td>1</td>
</tr>
</tbody>
</table>
4. After modifying the required fields, click on Show Report to generate the report effecting the changes made.
Copying Reports

OpManager allows you to copy a generated report in order to retain the already configured parameters as template and do some minor changes on them and save as a new report. To copy and save a report follow the steps given below:

1. Click **Copy As** icon available on the top of the report that is generated. A small window opens.

2. Enter a unique **Name** and a brief **Description**.

3. Change the required fields. The various fields that can be altered are Category, Period, Business Views, Time Window and Show all or Top N or Bottom N devices.

4. After modifying the required fields, click **Save** button to save the new report.
Scheduling Reports

OpManager allows you to schedule a new report, schedule a generated report and also to view a scheduled report.

Schedule a new report

1. Go to Reports > Default Reports > Schedule Reports.
2. In the Scheduler Reports Page, click the Add Schedule button on the top right.
3. Configure the following details:
   - **Schedule Name**: Configure a name for the schedule.
   - **Choose Report Type**: All the available reports types can be scheduled (select either one and follow the instructions given below followed by Configuring the Time Settings)

   **Scheduling Device specific Availability reports:**
   - If you have chosen to schedule reports for Device specific 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.
   - Select the **Period** and **Time Window** for which you want to generate the reports.

   **Scheduling Top N Reports / All Devices reports:**
   - If you have selected to schedule the Top N Reports, configure the following details:
   - **Top N Reports**: Select from Top 10/25/50/100/1000 reports.
   - **Period and Time Window**: Choose the Period and Time Window for which you want the report scheduled.
   - **Select Report(s)**: Select the required resource reports to be scheduled.
   - **Generate Availability Report to all devices in this Business View**: Select the relevant check-box and the business view to generate reports specific to the devices in that business view.
4. Click Next
5. **Configuring the Schedule for generating reports**:
   - **Daily**: Select the time at which the reports must be generated every day.
   - **Weekly**: Select the time and also the days on which the reports must be generated.
   - **Monthly**: Select the time, day, and the months for which the reports must be generated.
   - **Report Format Type**: Select either PDF or XLS to receive the report in the respective formats.
   - **Report Delivery**: Select any one of the following options.
     - **Send report as attachment to**: Configure the email ids to which the reports are to be sent as attachments. [or]
     - **Publish the report and send URL alone to**: Configure the url where the reports can be published.
     - **Add Mail Subject and Mail Message**
6. Verify the details of the configured schedule, enter a name for the Schedule and hit Add Schedule for the schedule to take effect.

Scheduling a generated report

1. In the report page that is generated, click Schedule This icon to schedule the report.
2. Enter the **Schedule Name**.
3. Enter the **Email ID** to which the report has to be delivered.
4. Select the **Category** followed by **Business View**.
5. Select the **Period** and **Time Window**.
6. Select the **Report Format** (PDF or XLS).
7. Select the **Report Delivery Type** (Attachment or URL).
9. Click **Save**.

**Viewing the Scheduled Report**

1. Go to Reports > Default Reports > Schedule Reports
2. Click agains the **View** icon on the required report that you wish to see.
3. The list of generated reports for the selected report will appear.
<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Schedule Description</th>
<th>View Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Enabled</td>
<td>All Report - Weekly Schedule</td>
<td></td>
</tr>
<tr>
<td>allalert_rejc</td>
<td>Enabled</td>
<td>All Report - Weekly Schedule</td>
<td></td>
</tr>
<tr>
<td>allalert_rejc</td>
<td>Enabled</td>
<td>All Report - Daily Schedule</td>
<td></td>
</tr>
<tr>
<td>DevSchedul</td>
<td>Enabled</td>
<td>All Report - Weekly Schedule</td>
<td></td>
</tr>
<tr>
<td>devschedul</td>
<td>Enabled</td>
<td>All Report - Weekly Schedule</td>
<td></td>
</tr>
<tr>
<td>devschedul</td>
<td>Enabled</td>
<td>All Report - Weekly Schedule</td>
<td></td>
</tr>
<tr>
<td>WFSch1</td>
<td>Enabled</td>
<td>All Report - Weekly Schedule</td>
<td></td>
</tr>
<tr>
<td>WFSchCop</td>
<td>Enabled</td>
<td>All Report - Daily Schedule</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Favorite Reports

With OpManager you can mark the reports that are frequently viewed as Favorite reports. The reports that are marked as favorite reports are listed under My Favorites report category. To mark a report as your favorite one, follow the steps given below:

1. Generate the report that you want to mark as your favorite.
2. Click the Star icon (Mark a report as Favorite) at the top of the page to mark a report as Favorite.

A message is displayed saying that "This report has been added to your favorite list".
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 the Maps section of OpManager.

Adding a Business View:

1. Go to Maps -> Business Views -> Create New
2. Rename the Business view from ‘Untitled’ on the upper left corner to the desired one.
3. From the available list of devices, drag and drop the devices that has to be grouped, onto the white board.
4. You can customize the view by changing font type, size and color.
5. Choose the required Background (Map) from the preloaded images or upload a new background image and select Apply.
6. Drag and drop devices on the Map based on your requirement.
7. Save the created view.
8. Select Exit to close the view. The created view would be displayed under the Business Views Tab.

Creating Links between devices:

Adding links between devices in business views, helps to represent network diagram on the map. These links can be configured based on user requirements.

To add a link between two devices in a business view,

1. Select the Add link button next to the Background tab. Drag a link from the source to the destination device and click that device. A link properties dialog pops up.
2. Alternatively you can also drag the link button at the top right corner of the source device icon to create a link to the destination device.
3. Configure a display name for the link.

4. In the Get Status from field, select any interface from either the source device or the destination device. The link will inherit the status of the interface that you choose here. For instance, if the source device goes down, and if you have selected an interface from that device, the link also inherits the status of that device. **Note:** You can also select to Get Status from either OpManager or NetFlow. If OpManager is selected, status is got through SNMP. If NetFlow is selected, detailed data like Top Source, Destination, QoS etc., can be obtained.

5. Select the line type and size.

6. Deselect the Show Arrow check box if you don’t want to show the traffic arrows.

7. Click **Apply**.

8. Click **Save** on the left to save the changes.

---

**Modifying Business Views:**

1. To make changes to the existing business views, Access the business view from the **Maps** tab.
2. Click the **Edit** icon to modify the view properties.
3. After modifying the properties like adding/removing links, adding more devices to the view, adding shortcuts on the view, changing background etc, click the **Save** button on the left to save the changes.

**Adding Shortcuts:**

You can add shortcut icons to business views that helps to easily navigate to a view from another view when objects are grouped based on their geographical location.

1. Go to the business view and click the Edit option on right-top corner of the view.
2. Click the Add Shortcut button on the left. A shortcut properties dialog pops up.
3. Configure a name for the shortcut in the Shortcut Name field.
4. From the **Open Submap** list-box, select the map which should be opened when you click the shortcut.
5. Select the icon to be used for the shortcut from the Default Icons or select from the Custom Icon combo-box.
6. Click Apply for the shortcut to be added.

**Note:** You must have created at least two business views to be able to add a shortcut from one view to another.
Google Maps:

OpManager allows you to integrate Google Maps and place the devices on the maps according to the geographic distribution. Please refer google licensing terms and pricing plans before you proceed further.

https://developers.google.com/maps/pricing-and-plans/

To configure Google maps

1. Download this [file](#) to your desktop.
2. Extract the downloaded zip and open maps.html file in any script editor.
3. Update the Google API key as shown below. (Visit this [page](#) generate an API key)
   
   ```html
   <script type='text/javascript' src='//maps.googleapis.com/maps/api/js?sensor=false&language=en&key=YOUR_API_KEY'></script>
   ```
4. Once you update the key, upload the updated maps.html, as shown below

Adding Devices on the Google Map

1. Now, zoom in/out the map and double-click on the location where you want to place a discovered device.
2. A device list box pops up allowing you to select a device to be placed in that location.
3. Select the device and click on Add.
4. Add the required devices on to the map by double-clicking the location.
5. You can also add the devices to the map from the device snapshot page.
6. Go to the device snapshot page.
7. Click on Add to Google Map link in the page to add the device to the map.

Viewing Device Details from Google Map

1. Click on the device balloons on the Google Map to see a popup.
2. Click the device name/IP address on this popup to get into the device snapshot page.
3. The popup also shows the device status.

Deleting Devices from Google Map

1. Click on the device balloons on the Google Map to see a popup.
2. Click the Delete link on this popup to delete the device from the map.
Datacenter Visualization

OpManager helps in creating a virtual replication of Datacenter floors and racks and floors to enable 24x7 monitoring.

3D Rack View:

Virtual Racks can be created with OpManager. These racks display the status of the devices present in them.

To create a Rack View,

1. Under Maps, select the Create New option under Rack Views Tab.
2. Drag and Drop the devices onto the Rack.
3. Click Save on the top right corner.
4. The status and availability of the devices can be seen in the rack created.
3D Floor View:

Floor views can be created in OpManager. The racks are then loaded onto the floor views to create a virtual replica of the Data center.

To create a Floor View,

1. Under Maps, select the Create New option under Floor Views Tab.
2. Select your floor size.
3. Drag and drop paths, aisles and walls as per your Data center.
4. Populate an existing rack view onto the floor map to create your Data center replica.
Layer 2 Maps:

OpManager renders the logical network topology diagram once you discover the networks and network devices. For a better visualization of the physical network connectivity in real networks and the consequences of a failure of a device, network topology map comes handy.

Locating Layer 2 Maps:

OpManager automatically maps L2 devices when Layer 2 discovery is done. The Map can be viewed under the Layer 2 tab of the Maps Section.

Modifying Layer 2 Maps:

To modify the existing Layer 2 Map,

Go to Maps -> Layer 2 Maps Tab.

Select the edit icon on the desired Map.
VMware Maps:

OpManager automatically provides a map of your VMware VCenter, VM's and host machines, once they have been discovered. These Maps can be viewed under the VMware tab under the Maps Section.

**Note**: Either VMware vCenter or Host Based Monitoring is possible in a single Installation. Not both at the same time.

HyperV Maps:

OpManager automatically provides a map of your Hypervisor, guest and Host machines, once they have been discovered. These Maps can be viewed under the HyperV tab under the Maps Section.

Xen Maps:

OpManager automatically provides a map of your Xen hypervisor, guest and host machines, once they have been discovered. These Maps can be viewed under the HyperV tab under the Maps Section.
Cisco UCS Monitoring:

OpManager monitors Cisco UCS System using XML SOAP protocol. Cisco's Unified Computing System integrates computing, networking, virtualization and other datacenter components for cost effective and efficient datacenter management.

UCS Discovery:

UCS discovery in OpManager is similar to the discovery of other devices.

1. Go to **Settings -> Discovery Module**
2. Select the option **Add UCS**
3. Input the **Device Name/IP Address**
4. Select the **Add UCS Credential** to input credential details.
5. Configure credentials by providing the User Name, Password, Port No., Time Out and Protocol details.

Once the device is discovered, it is listed under OpManager's inventory.

Monitoring:

OpManager monitors status and availability of the UCS devices. Detailed information like UCS components, their relationship charts, Chassis information etc., is also monitored by OpManager.

UCS Snapshot Page:

The Snapshot page provides details like IP Address, Monitoring Intervals, Passwords, Status and Response Times of the Device.

OpManager also provides the status of service profiles associated with UCS servers and an overview of UCS components that includes Chassis, Chassis servers, rack mount servers, FEX, ethernet ports etc. These can be viewed in the UCS Snapshot page.
Chassis Information:

OpManager provides a graphical representation of Chassis components that includes Servers, Fan Modules, Power Supply Units, IO Modules etc. This can also be viewed under the snapshot page of the UCS device in OpManager.

Apart from this, OpManager also provides information on the number of chassis, and detailed data on the chassis servers like cores, memory, NICs, operability, Power and association State.
Rack Mounts:

Rack mounts are frames where the servers are enclosed. Several servers can be mounted on the rack as per requirement.

OpManager monitors

- Cores
- Adaptors
- NICs
- Operability
- Associated State

Fabric Interconnectors:

These are a part of UCS devices that acts as a switch, and helps in connecting servers to networks or storage networks.

OpManager monitors

- Fans
- Power Supply Units
- IO Modules
Other UCS Components:

OpManager also monitors and provides detailed information on the other UCS device components such as,

1. Fan Modules
2. Ethernet Ports
3. IO Modules
4. FEX
5. Adaptor Unit
6. Processor Unit
### IO Modules (4)

<table>
<thead>
<tr>
<th>Name</th>
<th>Equipment</th>
<th>model</th>
<th>Vendor</th>
<th>Presence</th>
<th>Overall Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module 1</td>
<td>Chassis 1</td>
<td>UCS-6308-2100P</td>
<td>Cisco Systems Inc</td>
<td>equpped</td>
<td>operable</td>
</tr>
<tr>
<td>Module 2</td>
<td>Chassis 1</td>
<td>UCS-6308-2100P</td>
<td>Cisco Systems Inc</td>
<td>equpped</td>
<td>operable</td>
</tr>
<tr>
<td>Module 3</td>
<td>FEX 2</td>
<td>N2H-C2232PP-18GC</td>
<td>Cisco Systems</td>
<td>equpped</td>
<td>operable</td>
</tr>
<tr>
<td>Module 4</td>
<td>FEX 3</td>
<td>N2H-C2232PP-18GC</td>
<td>Cisco Systems</td>
<td>equpped</td>
<td>operable</td>
</tr>
</tbody>
</table>

### FEX (2)

<table>
<thead>
<tr>
<th>Name</th>
<th>Equipment</th>
<th>model</th>
<th>Vendor</th>
<th>Presence</th>
<th>Overall Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEX 1</td>
<td>sxrBox-2</td>
<td>N2H-C2232PP-18GC</td>
<td>Cisco Systems</td>
<td></td>
<td>operable</td>
</tr>
<tr>
<td>FEX 2</td>
<td>sxrBox-3</td>
<td>N2H-C2232PP-18GC</td>
<td>Cisco Systems</td>
<td></td>
<td>operable</td>
</tr>
</tbody>
</table>

### Adaptor Unit (11)

<table>
<thead>
<tr>
<th>Name</th>
<th>Equipment</th>
<th>Serial</th>
<th>model</th>
<th>Vendor</th>
<th>Thermal</th>
<th>Overall Status</th>
<th>Operability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapter 1</td>
<td>Chassis 1</td>
<td>Q1212019512G</td>
<td>N2O-AX0002</td>
<td>Cisco Systems Inc</td>
<td>Unknown</td>
<td>Operable</td>
<td>Operable</td>
</tr>
<tr>
<td>Adapter 2</td>
<td>Chassis 1</td>
<td>Q1212019513G</td>
<td>N2O-AX0002</td>
<td>Cisco Systems Inc</td>
<td>Unknown</td>
<td>Operable</td>
<td>Operable</td>
</tr>
<tr>
<td>Adapter 3</td>
<td>Chassis 1</td>
<td>Q1212019514G</td>
<td>N2O-AX0002</td>
<td>Cisco Systems Inc</td>
<td>Unknown</td>
<td>Operable</td>
<td>Operable</td>
</tr>
<tr>
<td>Adapter 4</td>
<td>Chassis 1</td>
<td>Q1212019515G</td>
<td>N2O-AX0002</td>
<td>Cisco Systems Inc</td>
<td>Unknown</td>
<td>Operable</td>
<td>Operable</td>
</tr>
<tr>
<td>Adapter 5</td>
<td>Chassis 1</td>
<td>Q1212019516G</td>
<td>N2O-AX0002</td>
<td>Cisco Systems Inc</td>
<td>Unknown</td>
<td>Operable</td>
<td>Operable</td>
</tr>
<tr>
<td>Adapter 6</td>
<td>Chassis 1</td>
<td>Q1212019517G</td>
<td>N2O-AX0002</td>
<td>Cisco Systems Inc</td>
<td>Unknown</td>
<td>Operable</td>
<td>Operable</td>
</tr>
<tr>
<td>Adapter 7</td>
<td>Chassis 1</td>
<td>Q1212019518G</td>
<td>N2O-AX0002</td>
<td>Cisco Systems Inc</td>
<td>Unknown</td>
<td>Operable</td>
<td>Operable</td>
</tr>
<tr>
<td>Adapter 8</td>
<td>Chassis 1</td>
<td>Q1212019519G</td>
<td>N2O-AX0002</td>
<td>Cisco Systems Inc</td>
<td>Unknown</td>
<td>Operable</td>
<td>Operable</td>
</tr>
<tr>
<td>Adapter 9</td>
<td>Chassis 1</td>
<td>Q1212019520G</td>
<td>N2O-AX0002</td>
<td>Cisco Systems Inc</td>
<td>Unknown</td>
<td>Operable</td>
<td>Operable</td>
</tr>
<tr>
<td>Adapter 10</td>
<td>Chassis 1</td>
<td>Q1212019521G</td>
<td>N2O-AX0002</td>
<td>Cisco Systems Inc</td>
<td>Unknown</td>
<td>Operable</td>
<td>Operable</td>
</tr>
<tr>
<td>Adapter 11</td>
<td>Chassis 1</td>
<td>Q1212019522G</td>
<td>N2O-AX0002</td>
<td>Cisco Systems Inc</td>
<td>Unknown</td>
<td>Operable</td>
<td>Operable</td>
</tr>
</tbody>
</table>

### Processor Unit (18)

<table>
<thead>
<tr>
<th>Name</th>
<th>Equipment</th>
<th>model</th>
<th>Thermal</th>
<th>Speed</th>
<th>Cores Enabled</th>
<th>Cores</th>
<th>Overall Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor 1</td>
<td>Chassis 1</td>
<td>Intel(R) Xeon(R) CPU X5370 @ 2.93GHz</td>
<td>Unknown</td>
<td>2.93</td>
<td>4</td>
<td>4</td>
<td>Operable</td>
</tr>
<tr>
<td>Processor 2</td>
<td>Chassis 1</td>
<td>Intel(R) Xeon(R) CPU X5370 @ 2.93GHz</td>
<td>Unknown</td>
<td>2.93</td>
<td>4</td>
<td>4</td>
<td>Operable</td>
</tr>
<tr>
<td>Processor 3</td>
<td>Chassis 1</td>
<td>Intel(R) Xeon(R) CPU X5370 @ 2.93GHz</td>
<td>Unknown</td>
<td>2.93</td>
<td>4</td>
<td>4</td>
<td>Operable</td>
</tr>
<tr>
<td>Processor 4</td>
<td>Chassis 1</td>
<td>Intel(R) Xeon(R) CPU X5370 @ 2.93GHz</td>
<td>Unknown</td>
<td>2.93</td>
<td>4</td>
<td>4</td>
<td>Operable</td>
</tr>
<tr>
<td>Processor 5</td>
<td>Chassis 1</td>
<td>Intel(R) Xeon(R) CPU X5370 @ 2.93GHz</td>
<td>Unknown</td>
<td>2.93</td>
<td>4</td>
<td>4</td>
<td>Operable</td>
</tr>
<tr>
<td>Processor 6</td>
<td>Chassis 1</td>
<td>Intel(R) Xeon(R) CPU X5370 @ 2.93GHz</td>
<td>Unknown</td>
<td>2.93</td>
<td>4</td>
<td>4</td>
<td>Operable</td>
</tr>
<tr>
<td>Processor 7</td>
<td>Chassis 1</td>
<td>Intel(R) Xeon(R) CPU X5370 @ 2.93GHz</td>
<td>Unknown</td>
<td>2.93</td>
<td>4</td>
<td>4</td>
<td>Operable</td>
</tr>
<tr>
<td>Processor 8</td>
<td>Chassis 1</td>
<td>Intel(R) Xeon(R) CPU X5370 @ 2.93GHz</td>
<td>Unknown</td>
<td>2.93</td>
<td>4</td>
<td>4</td>
<td>Operable</td>
</tr>
<tr>
<td>Processor 9</td>
<td>Chassis 1</td>
<td>Intel(R) Xeon(R) CPU X5370 @ 2.93GHz</td>
<td>Unknown</td>
<td>2.93</td>
<td>4</td>
<td>4</td>
<td>Operable</td>
</tr>
<tr>
<td>Processor 10</td>
<td>Chassis 1</td>
<td>Intel(R) Xeon(R) CPU X5370 @ 2.93GHz</td>
<td>Unknown</td>
<td>2.93</td>
<td>4</td>
<td>4</td>
<td>Operable</td>
</tr>
<tr>
<td>Processor 11</td>
<td>Chassis 1</td>
<td>Intel(R) Xeon(R) CPU X5370 @ 2.93GHz</td>
<td>Unknown</td>
<td>2.93</td>
<td>4</td>
<td>4</td>
<td>Operable</td>
</tr>
<tr>
<td>Processor 12</td>
<td>Chassis 1</td>
<td>Intel(R) Xeon(R) CPU X5370 @ 2.93GHz</td>
<td>Unknown</td>
<td>2.93</td>
<td>4</td>
<td>4</td>
<td>Operable</td>
</tr>
<tr>
<td>Processor 13</td>
<td>Chassis 1</td>
<td>Intel(R) Xeon(R) CPU X5370 @ 2.93GHz</td>
<td>Unknown</td>
<td>2.93</td>
<td>4</td>
<td>4</td>
<td>Operable</td>
</tr>
<tr>
<td>Processor 14</td>
<td>Chassis 1</td>
<td>Intel(R) Xeon(R) CPU X5370 @ 2.93GHz</td>
<td>Unknown</td>
<td>2.93</td>
<td>4</td>
<td>4</td>
<td>Operable</td>
</tr>
<tr>
<td>Processor 15</td>
<td>Chassis 1</td>
<td>Intel(R) Xeon(R) CPU X5370 @ 2.93GHz</td>
<td>Unknown</td>
<td>2.93</td>
<td>4</td>
<td>4</td>
<td>Operable</td>
</tr>
<tr>
<td>Processor 16</td>
<td>Chassis 1</td>
<td>Intel(R) Xeon(R) CPU X5370 @ 2.93GHz</td>
<td>Unknown</td>
<td>2.93</td>
<td>4</td>
<td>4</td>
<td>Operable</td>
</tr>
<tr>
<td>Processor 17</td>
<td>Chassis 1</td>
<td>Intel(R) Xeon(R) CPU X5370 @ 2.93GHz</td>
<td>Unknown</td>
<td>2.93</td>
<td>4</td>
<td>4</td>
<td>Operable</td>
</tr>
<tr>
<td>Processor 18</td>
<td>Chassis 1</td>
<td>Intel(R) Xeon(R) CPU X5370 @ 2.93GHz</td>
<td>Unknown</td>
<td>2.93</td>
<td>4</td>
<td>4</td>
<td>Operable</td>
</tr>
</tbody>
</table>
Performance Monitors:

Whenever OpManager discovers UCS devices, UCS performance monitors are automatically associated with it. Thresholds can be set to receive alarms, when breached.

To set thresholds for a performance monitor,

1. Navigate to Inventory -> Category -> UCS and go to the Snapshot Page of the device.
2. Go to Monitors. Performance monitors would already have been added to the device.
3. Select the monitor that you wish to edit.
4. Configure Monitoring Interval, Units, Threshold Details and click on Save.

OpManager sends alarms if the threshold levels are breached.

To add performance monitors for more than one UCS device,
1. Navigate to **Settings -> Monitoring -> Device Templates**
2. Locate **UCS** device template
3. Input the **Device Identifier** (sysOID), query the device and add them
4. Add the required monitor and configure threshold details.
What is Deep Packet Inspection?

Deep Packet Inspection (DPI) is a process to know what is been received and transmitted by a network device. It is the most accurate technique to monitor and analyze the application problems and regulate traffic in best suitable way. With DPI’s packet level analysis, it is easy to make decisions on capacity planning and achieve better network performance and management. DPI helps determine the root cause for performance related issues with the complete traffic picture (both network and application) in a single view.

Opmanager’s Deep Packet Inspection allows you to capture network packets and analyzes packet capture (PCAP) files. The DPI capabilities rely on packet-level analysis to determine whether the network or an application is at fault and react quickly to the issues before they impact users. It gives clear visibility to network administrators about the volumes, application and network performances of application traffic for their enterprise network and helps them to diagnose application performance problems with response time details and drill even further to the root cause of performance degradation issues.

With DPI you can:

- Pinpoint whether the delay is on the network side or application side comparing NRT vs. ART
- Pull the list of affected users for slow apps and communicate them in advance
- Increase application availability and meet SLAs
- Know who is using your bandwidth and regulate them using traffic shaping
- Pull reports on historic data and perform forensics
Understanding DPI in OpManager

Traffic packets passing through the network device, can be mirrored to a port of the same device for inspection. Also multiple (WAN/LAN/Uplink) ports traffic can be mirrored and set for inspection. In case if you wish to inspect packets from multiple devices, all the mirrored ports can be connected to a L2 switch on which OpManager is connected to.

In the above diagram, consider 4 uplink ports are mirrored for monitoring to the last port of individual switches 1, 2, 3 & 4. Here all the mirrored network packets reaches the OpManager installed server through mirroring on Switch 4. Port mirroring commands vary from vendor to vendor, you can check with the respective device vendor for commands.

Below is an example for port mirroring on a HP Switch

```
HPSwitch# config terminal
HPSwitch(config)# mirror 1 port a24
HPSwitch(config)# interface a1-a23
HPSwitch(eth-A1-A23)# monitor all
    Monitor all traffic.
<cr>
HPSwitch(eth-A1-A23)# mirror all
    Monitor all inbound traffic
in
    Monitor all outbound traffic
out
    Monitor all inbound and outbound traffic
both
HPSwitch(eth-A1-A23)# mirror all both
    Mirror destination.
HPSwitch(eth-A1-A23)# mirror all both mirror
    Mirror destination number.
<1-4>
HPSwitch(eth-A1-A23)# mirror all both mirror 1
    Don't add VLAN tag for this untagged-port
no-tag-added
<1-4>
    Mirror destination number.
<cr>
HPSwitch(eth-A1-A23)# mirror all both mirror 1
```
With these received network packets Manageengine will analyze the captured packets and generate reports.

TCP analysis.
As Initial phase Manageengine has introduced analysis for TCP packets even though it captures all packets. Rest will be supported in future. Using the DPI feature, we can calculate application response time (ART), network response time (NRT), url's used and traffic utilization (productivenon-productive).
With these reports a network administrator can have a clear picture of what is consuming the bandwidth at what time and so, he can regulate it cost efficiently.

In DPI we get information about ART,NRT and URL's
NRT : NetWork Response Time. It is the time difference between TCP_SYN packet and its ACK (acknowledgement)
ART : Application Response Time is the time difference between TCP_DATA packet and its ACK (acknowledgement flag)
URL : URL details contained in data packets.
In Opmanager DPI works with winPcap and High performance reporting engine add-on. To configure DPI, follow the steps and screenshots below to enable DPI.

1. For Windows machine, download and install winpcap packages from the below link: https://www.winpcap.org/install/, skip this step for linux OS.

2. Download and install HighPerformance reporting engine under More downloads from the link https://www.manageengine.com/products/netflow/2028821/ME_NFA_HighPerf_Add-On_64bit.exe

3. Navigate to Settings > DPI, Enable DataCollection, select the ethernet card, select the data retention period and save.

Note: To find the respective Network card (in windows), open regedit, navigate to HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindows NTCurrentVersionNetworkCards. Here you can find the respective name of network card in readable format.

4. To Verify navigate to <Opmanager>DPIPcapFilesTemp and check if new file is generated.
<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>temp_035706373</td>
<td>18-06-2017 11:26</td>
<td>Wireshark capture...</td>
<td>0 KB</td>
</tr>
<tr>
<td>temp_770944070</td>
<td>15-06-2017 10:25</td>
<td>Wireshark capture...</td>
<td>10.459 KB</td>
</tr>
</tbody>
</table>
Once Packet capture is started, the high perf database stores the information of URL's, applications, sources, destinations and conversation. To access the information, you can navigate to Inventory > Packet Analysis. Here you can see the URL wise response time where you can drill down to any URL and see who/what caused this traffic.

Statistics can be viewed with respect to any below mentioned criteria.

URL Drill down:
Searching a URL:
Application Drill down:
<table>
<thead>
<tr>
<th>Name</th>
<th>Average RTT</th>
<th>Average AWT</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>cadbms</td>
<td>1080 ms</td>
<td>5967 ms</td>
<td>4.37 KB</td>
</tr>
<tr>
<td>dcsyntesis</td>
<td>1097 ms</td>
<td>5189 ms</td>
<td>3.79 KB</td>
</tr>
<tr>
<td>dplaq</td>
<td>1094 ms</td>
<td>1481 ms</td>
<td>3.63 KB</td>
</tr>
<tr>
<td>dresv</td>
<td>1094 ms</td>
<td>1885 ms</td>
<td>3.63 KB</td>
</tr>
<tr>
<td>dtp</td>
<td>1088 ms</td>
<td>1463 ms</td>
<td>4.14 KB</td>
</tr>
<tr>
<td>dx406</td>
<td>1040 ms</td>
<td>1576 ms</td>
<td>3.72 KB</td>
</tr>
<tr>
<td>dx406f</td>
<td>25182 ms</td>
<td>25160 ms</td>
<td>34.08 MB</td>
</tr>
<tr>
<td>dtx406f</td>
<td>25182 ms</td>
<td>25160 ms</td>
<td>35.21 MB</td>
</tr>
<tr>
<td>dtx406f</td>
<td>41361 ms</td>
<td>40469 ms</td>
<td>191.29 MB</td>
</tr>
<tr>
<td>dxt406f</td>
<td>41361 ms</td>
<td>40469 ms</td>
<td>3.63 KB</td>
</tr>
<tr>
<td>dxt406f</td>
<td>6995 ms</td>
<td>1452 ms</td>
<td>3.63 KB</td>
</tr>
<tr>
<td>dxt406f</td>
<td>6995 ms</td>
<td>1452 ms</td>
<td>3.63 KB</td>
</tr>
<tr>
<td>dxt406f</td>
<td>6996 ms</td>
<td>1452 ms</td>
<td>4.16 KB</td>
</tr>
<tr>
<td>dxt406f</td>
<td>6996 ms</td>
<td>1452 ms</td>
<td>3.63 KB</td>
</tr>
<tr>
<td>dxt406f</td>
<td>6996 ms</td>
<td>1452 ms</td>
<td>1.57 KB</td>
</tr>
<tr>
<td>dxt406f</td>
<td>6996 ms</td>
<td>1452 ms</td>
<td>4.21 KB</td>
</tr>
</tbody>
</table>
Drill down based on Source /Destination IP address:

Source:
Destination:
DPI widgets can be accessed from default dashboard under DPI tab. Custom dashboard can also be created using DPI related widgets.

To access reports from UI, navigate to Reports > DPI. Here we have 2 types, Online/Offline reports. Online reports are generated from embedded in-built database. You can also have the packets captured in PCAP format and generate reports for the same.

Manageengine DPI reports are based on Time and criteria. DPI reports are mainly concentrated on 3 metrics URL, NRT, ART.
Criteria can be **none** or **any** or **multiple** of the list.

Next the time period should be within the DPI data storage time period.

When you generate reports, you can see reports based on Traffic, Application (Layer 4), URL hits, Source,
### Netflow Reports

#### Forensics

**Traffic Between**: 2017-08-17 11:43 To: 2017-08-17 12:43

<table>
<thead>
<tr>
<th>Source</th>
<th>Average RTT</th>
<th>Average NRT</th>
<th>Traffic</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>122.15.156.179</td>
<td>6.506 ms</td>
<td>20.671 ms</td>
<td>11.13 MB</td>
<td>9283</td>
</tr>
<tr>
<td>172.30.93</td>
<td>40.205 ms</td>
<td>85.468 ms</td>
<td>7.1 MB</td>
<td>20113</td>
</tr>
<tr>
<td>42.109.11.94</td>
<td>0.049 ms</td>
<td>15.538 ms</td>
<td>5.68 MB</td>
<td>4229</td>
</tr>
<tr>
<td>122.15.156.191</td>
<td>0.069 ms</td>
<td>20.291 ms</td>
<td>1.89 MB</td>
<td>1772</td>
</tr>
<tr>
<td>98.242.89.39</td>
<td>0.016 ms</td>
<td>1.627 ms</td>
<td>1.68 MB</td>
<td>11675</td>
</tr>
<tr>
<td>116.31.156.157</td>
<td>9.804 ms</td>
<td>0.585 ms</td>
<td>839.19 KB</td>
<td>1245</td>
</tr>
<tr>
<td>212.91.124.334</td>
<td>42.447 ms</td>
<td>1.499 ms</td>
<td>384.01 KB</td>
<td>502</td>
</tr>
<tr>
<td>72.52.254.23</td>
<td>0.074 ms</td>
<td>1.532 ms</td>
<td>340.52 KB</td>
<td>1591</td>
</tr>
<tr>
<td>116.31.156.52</td>
<td>0.076 ms</td>
<td>0.891 ms</td>
<td>214.55 KB</td>
<td>1955</td>
</tr>
<tr>
<td>196.127.246.165</td>
<td>0.073 ms</td>
<td>1.503 ms</td>
<td>305.39 KB</td>
<td>423</td>
</tr>
<tr>
<td>52.188.37</td>
<td>0.075 ms</td>
<td>1.537 ms</td>
<td>52.88 KB</td>
<td>347</td>
</tr>
<tr>
<td>596.163.225.176</td>
<td>0.087 ms</td>
<td>1.599 ms</td>
<td>40.47 KB</td>
<td>569</td>
</tr>
<tr>
<td>229.12.220</td>
<td>0.085 ms</td>
<td>1.505 ms</td>
<td>21.87 KB</td>
<td>529</td>
</tr>
<tr>
<td>201.152.208.7</td>
<td>0.085 ms</td>
<td>1.505 ms</td>
<td>29.97 KB</td>
<td>336</td>
</tr>
<tr>
<td>78.127.125.230</td>
<td>0.089 ms</td>
<td>1.532 ms</td>
<td>28.81 KB</td>
<td>222</td>
</tr>
<tr>
<td>66.951.79.94</td>
<td>0.066 ms</td>
<td>1.504 ms</td>
<td>28.57 KB</td>
<td>508</td>
</tr>
<tr>
<td>122.13.156.143</td>
<td>0.048 ms</td>
<td>77.261 ms</td>
<td>26.07 KB</td>
<td>302</td>
</tr>
</tbody>
</table>

#### Netflow Reports

**Traffic Between**: 2017-08-17 11:43 To: 2017-08-17 12:43

<table>
<thead>
<tr>
<th>Destination</th>
<th>Average RTT</th>
<th>Average NRT</th>
<th>Traffic</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.30.93</td>
<td>6.224 ms</td>
<td>12.803 ms</td>
<td>23.34 MB</td>
<td>45718</td>
</tr>
<tr>
<td>104.48.125.7</td>
<td>1.968 ms</td>
<td>2.267 ms</td>
<td>296.47 KB</td>
<td>122</td>
</tr>
<tr>
<td>52.151.25</td>
<td>64.83 ms</td>
<td>65.137 ms</td>
<td>339.77 KB</td>
<td>804</td>
</tr>
<tr>
<td>172.217.21.34</td>
<td>281.541 ms</td>
<td>168.077 ms</td>
<td>302.87 KB</td>
<td>445</td>
</tr>
<tr>
<td>52.185.302</td>
<td>63.24 ms</td>
<td>63.395 ms</td>
<td>245.81 KB</td>
<td>717</td>
</tr>
<tr>
<td>172.217.21.130</td>
<td>292.628 ms</td>
<td>141.815 ms</td>
<td>212.97 KB</td>
<td>358</td>
</tr>
<tr>
<td>69.372.216.55</td>
<td>1.552 ms</td>
<td>6.124 ms</td>
<td>297.86 KB</td>
<td>244</td>
</tr>
<tr>
<td>104.48.119.24</td>
<td>2.004 ms</td>
<td>2.235 ms</td>
<td>394.01 KB</td>
<td>106</td>
</tr>
<tr>
<td>189.254.161.204</td>
<td>0.21 ms</td>
<td>0.022 ms</td>
<td>151.59 KB</td>
<td>5478</td>
</tr>
<tr>
<td>182.163.13.79</td>
<td>1.479 ms</td>
<td>1.470 ms</td>
<td>148.13 KB</td>
<td>287</td>
</tr>
<tr>
<td>256.18.391.162</td>
<td>1.238 ms</td>
<td>5.035 ms</td>
<td>336.08 KB</td>
<td>454</td>
</tr>
<tr>
<td>69.372.216.56</td>
<td>1.584 ms</td>
<td>6.816 ms</td>
<td>127.2 KB</td>
<td>149</td>
</tr>
<tr>
<td>34.15.71.107</td>
<td>37.427 ms</td>
<td>37.7 ms</td>
<td>124.41 KB</td>
<td>250</td>
</tr>
<tr>
<td>256.18.391.194</td>
<td>1.199 ms</td>
<td>1.499 ms</td>
<td>122.36 KB</td>
<td>365</td>
</tr>
<tr>
<td>172.217.3.34</td>
<td>1.209 ms</td>
<td>20.447 ms</td>
<td>110.48 KB</td>
<td>335</td>
</tr>
<tr>
<td>256.18.391.66</td>
<td>1.3 ms</td>
<td>1.638 ms</td>
<td>90.74 KB</td>
<td>156</td>
</tr>
<tr>
<td>151.30.40.239</td>
<td>1.05 ms</td>
<td>1.695 ms</td>
<td>94.19 KB</td>
<td>630</td>
</tr>
</tbody>
</table>

**Note**: The tables display the average round-trip time (RTT), average network round-trip time (NRT), traffic in megabytes (MB), and packet counts for source and destination IP addresses for the specified time interval.
Offline Reports

Here we also have offline reports where you can save the captured packets (in PCAP format) separately and generate the same above graphs.

![Image of the application interface showing the selection of time between start and end dates for traffic flow analysis]
End User Monitoring in OpManager aims at visualizing the entire bandwidth data of every user in your network. This helps to respond quickly to any performance issues or wireless network congestions that might otherwise affect the quality of user experience.

OpManager correlates the data obtained through NetFlow and Firewall Analyzer add ons, to provide detailed insights on the user’s bandwidth consumption, top accessed sites and Applications and the location of the user.

Adding Users:

To enable end user monitoring, the device details/IP addresses are imported from the Active Directory.

To import Users via Active directory,

1. Go to End User Monitoring Tab.
2. Locate the + icon, and select AD, from the Import Profile Tab, to start importing Users from the Active Directory.
3. Provide the User Name, Password and click on the Import button to get details of devices/IP addresses.

Note: The device details can also be added manually.

To configure manually,

1. Select the Manual Option from the Import Profile Tab
2. Configure the end user details and select the Import button, to add the user.

Once the import is done, the details can be viewed under the People tab of the End User Monitoring module.

User Snapshot:

The user snapshot lists user details. It contains

- Number of devices
- Bandwidth consumed
- Top accessed Applications
- Top accessed URLs

To identify the bandwidth consumed or to identify top accessed Applications and URLs, Netflow data or firewall logs have to be enabled in OpManager.

To enable NetFlow data,

1. Navigate to Settings -> NetFlow
2. Click ON, select the interfaces and click on the Save Button

Connections:

OpManager helps to identify the users connected to your network. It also lists the number of devices, recently connected users and the top 3 Access points.

These user connections can be monitored by fetching details from a wireless controller device(WLC)
To add a WLC device,

1. Go to **Settings** -> **Discovery** -> **Add Device**
2. Provide the Device Name/IP Address of the device.
3. Configure SNMP credentials, and discover the device.

**Note:** OpManager supports Aruba wireless LAN controller at present. More models will be included with further releases.

**Top Users:**

OpManager allows to identify the top users of every application. It lists the amount of data used by the top users of various Applications.

OpManager currently includes around 100 Applications to identify the top user of every application. More Applications would be added in further releases.

```
Top Users by Collaboration Category

- meanatchi-0216: 158.48 MB
- reioe-0162: 3.98 MB
- saravananh-0127: 3.24 MB
- svembu: 0.8 MB
- rnanasekar-0122: 0.6 MB
```

```
Top Users by Youtube

No Data Available
```

**Top Services:**

OpManager allows you to identify top services category wise. It lists the total data used by top Applications.

OpManager includes 25 categories, that helps in listing the top data consuming Applications in the required categories.
Rebranding OpManager

Rebranding option helps you replace OpManager logo that is displayed in the OpManager web client as well as in the reports, with your company's logo. You can also change the product name, company name and copyright details.

To replace OpManager's logo with your Company's logo in the OpManager web client and reports, follow the steps given below

1. Click **Settings > Basic Settings > Rebranding.**
2. Click the Product Name and enter the name. Browse the Report Header Image to replace the image that is displayed in OpManager reports.
3. Browse the OpManager logo and import
4. Click **Save**

Once done with the above changes, restart OpManager.
Configuring Database Maintenance

To plot graphs and generate reports, OpManager collects data from the managed devices at regular intervals. By default, OpManager aggregates the performance data into hourly data at the end of each hour. The hourly data thus calculated will be aggregated into daily data at the end of each day. These aggregated data will be used in graphs and reports.

OpManager allows you to maintain the database with the required data. By default, the detailed data will be maintained for 7 days, the hourly data for 30 days and the daily data for 365 days. After the specified period, the database will be cleaned up automatically.

To configure your own settings for database maintenance, follow the steps given below:

1. Click **Settings > Basic Settings > Database Maintenance**.
2. Specify the values for the following fields:
   a. **Maintain recent alarms in the database** - the maximum number of recent alarms to be maintained must be specified here. For instance, if you want an history of last 500 alarms, specify the value as 500 here.
   b. **Detailed statistics will be maintained for the last _ days** - the detailed data will be maintained for 7 days
   c. **Hourly statistics will be maintained for the last _ days** - the hourly data for 30 days
   d. **Daily statistics will be maintained for the last _ days** - the cleanup interval of the raw data as well as the archived data must be specified here.
3. Click **Save** to apply the changes.

Run Archive
Scheduling Downtime

Maintenance of network devices forms an integral part of network administration. You may want to perform a maintenance of specific device types at specific intervals. If such devices are removed from the network, or rebooted, then you will see alarms indicating that the device, or the applications in the device are unavailable. Since the devices are not available when polled for status during the maintenance period, unnecessary alarms are fired. To prevent the devices from being monitored for status during maintenance, you can schedule a maintenance task for such devices.

Following are the steps:

1. From the Settings tab, select Downtime Scheduler option under Monitoring > Configuration.
2. Click on Add Schedule.
3. In the Add Downtime Schedule form, provide the following details:
   - Schedule Name
   - Schedule Description
   - Select the Status as Enabled, if you want the Scheduled task to take effect immediately. Else select Disabled, so that you can enable it when required.
   - Select the frequency at which the Task has to be scheduled/executed. It can be Once, Every Day, Every Week, and Every Month.
   - Specify the start and end time/day of the task in the corresponding fields.
   - If it is a schedule to be executed every day, then specify the date from which the task must be scheduled.
   - If it is a monthly schedule, select either the date or the day with the time window for the schedule.
   - You can assign the task to only the required devices, or a device category like switches, routers, to a Business view, or to URL Monitors.
4. Click Save

The schedule will be executed as configured.
Schedule Upgrade

Maintenance of network devices forms an integral part of network administration. You may want to perform a maintenance of specific device types at specific intervals. If such devices are removed from the network, or rebooted, then you will see alarms indicating that the device, or the applications in the device are unavailable. Since the devices are not available when polled for status during the maintenance period, unnecessary alarms are fired. To prevent the devices from being monitored for status during maintenance, you can schedule a maintenance task for such devices.

Following are the steps:

1. **Settings > Basic Settings > Schedule Upgrade**

2. In the **Schedule Upgrade Settings**, provide the following details:
   - Select the Status as **Enabled**, if you want the scheduled upgrade to take effect immediately. Else select **Disabled**, so that you can enable it when required.
   - It is scheduled to be **Execute Daily At**, specify the start time in hours, minutes then specify the date from which the task must be scheduled.
   - You can Enable or Disable email notification for the schedule upgrade

Click **Save** to execute the schedule as configured.
Scheduling Reports

OpManager allows you to schedule a new report and also to schedule a generated report.

Schedule a new report
1. From Reports tab, select Schedule Reports
2. In that page, click the Add Schedule button on the top right.
3. Configure the following details:
   - Choose Report Type: All the available reports types can be scheduled.
   - Click Next.

Scheduling Device specific Availability reports:
If you have chosen to schedule reports for device specific availability details, configure the following:
1. Select either a category of devices, or the required business view, or select specific devices manually for generating the availability reports.
2. Select the period and time window for which you want to generate the reports.
3. Click Next.

Scheduling Top N Reports/All Devices reports:
If you have selected to schedule the Top N Reports, configure the following details:
1. Top N Reports: Select from Top 10/25/50/100/1000 reports.
2. Period: Choose the period and time window for which you want the report scheduled.
3. Select Report(s): Select the required resource reports to be scheduled.
4. Business View Reports: Select the relevant check-box and the business view to generate reports specific to the devices in that business view.
5. Click Next.

Configuring the Time Settings for generating reports:
1. Daily: Select the time at which the reports must be generated every day.
2. Weekly: Select the time and also the days on which the reports must be generated.
3. Monthly: Select the time, day, and the months for which the reports must be generated.
4. Report Format Type: Select either PDF or XLS to receive the report in the respective formats.
5. Report Delivery: Select any one of the following options.
   - Configure the email ids to which the reports are to be sent as attachments. [or]
   - Configure the url where the reports can be published.
6. Click Next.

   - Schedule Name: Configure a name for the schedule.
Verify the details of the configured schedule and hit Add Schedule for the schedule to take effect.

Scheduling a generated report
1. In the report page that is generated, click Schedule icon to schedule the report.
2. Enter the schedule name.
3. Enter the email ID to which the report has to be delivered.
4. Select either a category of devices, or the required business view
5. Select the period and time window for which you want to generate the reports.
6. **Report Format Type**: Select either PDF or XLS to receive the report in the respective formats.
7. **Report Delivery**: Select any one of the following options.
   - Send as attachments
   - Send as URL
8. **Daily**: Select the time at which the reports must be generated every day.
9. **Weekly**: Select the time and also the days on which the reports must be generated.
10. **Monthly**: Select the time, day, and the months for which the reports must be generated.
11. Click **Save**.

**Enabling the Configured Schedule**
Once you configure the report schedules, they are listed in the Schedule Reports page (Reports > Schedule Reports page). Select the required schedules and click on the **Enable** button at the bottom of the list. You can also disable or delete a schedule from here.
OpManager 12 System Requirements

Last Updated: March 3, 2017

The system requirements mentioned below are the MINIMUM requirements for all v12 products on the opmanager platform such as NFA 12, NCM 12, Firewall Analyzer 12, and Oputils 12. Based on load the **sizing requirements** may vary for each product.

### Hardware requirements

These are the minimum requirements to run the system. Performance of the system varies based on load.

<table>
<thead>
<tr>
<th>Hardware</th>
<th>OPM50 - OPM250</th>
<th>OPM 500</th>
<th>OPM 1000</th>
<th>OPMPPlus (or opm with addons)</th>
<th>Enterprise Edition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>2GHz</td>
<td>2.5 GHz</td>
<td>Quadcore 2.5 GHz or more</td>
<td>Dual QuadCore 3.5 GHz or higher</td>
<td>Dual Quad Core 3.5 GHz or higher</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB</td>
<td>8 GB</td>
<td>16 GB</td>
<td>32GB</td>
<td>32 GB</td>
</tr>
<tr>
<td>Disc</td>
<td>10GB</td>
<td>10GB</td>
<td>10GB</td>
<td>40GB</td>
<td>40 GB</td>
</tr>
<tr>
<td>VM or dedicated machine</td>
<td>VM</td>
<td>VM</td>
<td>Dedicated</td>
<td>Dedicated</td>
<td>Dedicated</td>
</tr>
</tbody>
</table>

### Software requirements

These are the minimum requirements to run the system.

<table>
<thead>
<tr>
<th>Software</th>
<th>Evaluation</th>
<th>Production</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS - Windows</td>
<td>Windows 10</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td></td>
<td>Windows 8</td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>Windows 7</td>
<td>Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>Windows Vista</td>
<td>Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>Also works with,</td>
<td>Windows Server 2003</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016</td>
<td>Windows Server 2000</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Server 2000</td>
<td></td>
</tr>
<tr>
<td>OS - Linux</td>
<td>Ubuntu</td>
<td>64 bit Linux flavors</td>
</tr>
<tr>
<td></td>
<td>Debian</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Suse</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Red Hat</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Suse</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fedora</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mandrake</td>
<td></td>
</tr>
<tr>
<td>Browsers</td>
<td>Chrome latest</td>
<td>Chrome preferred</td>
</tr>
<tr>
<td></td>
<td>Firefox latest</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IE 11</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edge</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> Do not enable Enterprise Mode option in Internet Explorer. This will make Internet Explorer work as version 7. This is not supported.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client machines</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>User privileges</td>
<td>Local administrative privileges required</td>
<td></td>
</tr>
</tbody>
</table>
Database requirements

These are the minimum requirements to run the system.

<table>
<thead>
<tr>
<th>DB</th>
<th>Essential Edition</th>
<th>Enterprise Edition</th>
</tr>
</thead>
<tbody>
<tr>
<td>PGSQL</td>
<td>Bundled with the product.</td>
<td>For evaluation purpose only. Please use MSSQL for production.</td>
</tr>
</tbody>
</table>

Moving PGSQL to a dedicated server

1. Install PostgreSQL version 9.2.1 on the dedicated server. After successfully installing it,
2. Go to data directory of PostgreSQL installation.
3. By default, under IPv4 local connections, we have the following:
   
   # host all all 127.0.0.1/32 md5/trust - md5/trust or someother is available as last option
   
   1. Change the 127.0.0.1/32 to all

4. By default, under IPv6 local connections, we have the following:
   
   # host all all ::1/128 md5/trust - md5/trust or someother is available as last option
   
   1. Change the ::1/128 to all

5. Save the File.
6. Open Services window and restart the PostgreSQL server running in the machine to effect the changes.

2. Edit the file /opmanager/conf/database_params.conf.
3. Configure the host name and the PostgreSQL port number for the url parameter as given below:
   
   url jdbc:postgresql:// <name of the server where postgresql is installed> : <postgresql port> /OpManagerDB
   
   Example: url jdbc:postgresql://database1-server:5432/OpManagerDB
4. If you wish to enable password, un-comment the password line and set the new password.

SQL

- SQL 2016
- SQL 2014
- SQL 2012
- SQL 2008
- SQL 2005

Important Notices
- For production use 64 bit versions of SQL
- Recovery mode should be set to SIMPLE.
- SQL and opmanager should be in the same LAN. Currently WAN based SQL installations are not supported.
- OpManager supports only SQL server authentication mode.

Processor

- Quad Core
- Dual Quad Core

Dedicated machine or VM

- Dedicated
- Dedicated

Ports required

OpManager opens multiple ports for various needs. Listed below are the basic ones required.

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Port Type</th>
<th>Usage</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>13306</td>
<td>Static</td>
<td>Database Port</td>
<td>Can be changed in conf/database_params.conf file</td>
</tr>
<tr>
<td>31000</td>
<td>Dynamic</td>
<td>Java Wrapper Service Port</td>
<td>Add wrapper.port=22222 parameter in conf/wrapper.conf file to make it static</td>
</tr>
<tr>
<td>22</td>
<td>Static</td>
<td>SSH Port</td>
<td></td>
</tr>
<tr>
<td>80/443</td>
<td>Static</td>
<td>Web Server Port</td>
<td></td>
</tr>
<tr>
<td>2000</td>
<td>Static</td>
<td>Internal Communication Port</td>
<td></td>
</tr>
<tr>
<td>56328</td>
<td>Dynamic</td>
<td>ShutDown Listener Port</td>
<td></td>
</tr>
<tr>
<td>Port Number</td>
<td>Port Type</td>
<td>Usage</td>
<td>Remarks</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>56378</td>
<td>Dynamic</td>
<td>Internal Communication Port</td>
<td>Can be made static by configuring <code>NMS_FE_SECONDARY_PORT</code> parameter in <code>conf/opmanager/conf/server_parameters.conf</code> file</td>
</tr>
<tr>
<td>56469</td>
<td>Dynamic</td>
<td>Internal Communication Port</td>
<td>Can be made static by configuring <code>PORT_TO_LISTEN</code> parameter in <code>conf/opmanager/conf/transportProvider.conf</code> file</td>
</tr>
<tr>
<td>69</td>
<td>Static</td>
<td>TFTP Port</td>
<td></td>
</tr>
<tr>
<td>162</td>
<td>Static</td>
<td>SNMP Receiver Port</td>
<td></td>
</tr>
<tr>
<td>514</td>
<td>Static</td>
<td>SYSLOG Receiver Port</td>
<td></td>
</tr>
<tr>
<td>519</td>
<td>Static</td>
<td>SYSLOG Receiver Port</td>
<td></td>
</tr>
<tr>
<td>1514</td>
<td>Static</td>
<td>Firewall Log Receiver Port</td>
<td></td>
</tr>
<tr>
<td>9996</td>
<td>Static</td>
<td>NetFlow Listener Port</td>
<td></td>
</tr>
</tbody>
</table>

Note: These ports can be changed if not available.

**Threads configured**

OpManager allots a specific number of threads per module. Based on the thread count the job get scheduled in batches (say monitoring or backup or flow processing). Increasing the thread count helps you do more work but at the cost of consuming more hardware resources esp the processor CPU.

**Notice**

It is advisable to change threads after consulting with tech support.

<table>
<thead>
<tr>
<th>Module</th>
<th>Thread Count</th>
<th>Max recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>StatusPoll</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>DataPoll</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>DeepDiscovery</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Config</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>MS</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Network Discovery</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Provisioning</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Datacollection</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>WMI Datacollection</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Realtime Monitoring</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>VMware Monitoring</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Process Monitoring</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Hardware Monitoring</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Hardware Monitoring Disc</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>SavePoll</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>Interface Poll</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Thread Count</td>
<td>Max recommended</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Bulk Data Saver</td>
<td>40</td>
<td></td>
</tr>
</tbody>
</table>
Server Sizing Requirements Guide

Last Updated: April 3, 2017

The table below gives a summary of the maximum load per probe across various modules. Cumulative load per probe will be the sum of category 5, 4, 3, 2 + any one item from category 1. You cannot add more than one item from category 1

<table>
<thead>
<tr>
<th>Category</th>
<th>Max per server (column 1)</th>
<th>Factors that affect column 1</th>
<th>Number of probes required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Monitoring (SNMPv3 Devices)</td>
<td>500</td>
<td>B/C/D/E</td>
</tr>
<tr>
<td>1</td>
<td>Monitoring (SNMPv1,v2 Devices)</td>
<td>1000</td>
<td>B/C/D/E</td>
</tr>
<tr>
<td>1</td>
<td>Monitoring (Server WMI, CLI, VMware)</td>
<td>1000</td>
<td>B/C/D/E</td>
</tr>
<tr>
<td>1</td>
<td>Monitoring (Interfaces)</td>
<td>10,000</td>
<td>B/C/D/E</td>
</tr>
<tr>
<td>2</td>
<td>Netflow (Interfaces)</td>
<td>8000</td>
<td>G/I</td>
</tr>
<tr>
<td>3</td>
<td>NCM (Devices)</td>
<td>5000</td>
<td>K</td>
</tr>
<tr>
<td>4</td>
<td>Firewall (Devices)</td>
<td>50</td>
<td>M</td>
</tr>
<tr>
<td>5</td>
<td>APM Plugin (Monitors)</td>
<td>500</td>
<td>O</td>
</tr>
</tbody>
</table>

Now, let us understand the various aspects of LOAD on an OpManager server.

A. Licensing Unit

A device is a Router/ Switch/Server or any Device that is ping-able through an IP address. OpManager is licensed based on the number of devices it monitors. A single server cannot exceed more than 1000 devices.

**NOTICE**

Interfaces are not licensed. You may monitor interfaces and get them monitored for availability, performance and traffic. But adding lot of interfaces will affect the system performance. A single server cannot handle more than 10,000 SNMP interfaces. If you are monitoring interfaces using ICMP Ping, the number of interfaces per server comes down drastically. Depending on the ping performance and other network factors it might be 2000-5000 interfaces per probe.

B. Monitoring Interval

By default, a server CPU is monitored every 5 mins where as a Disk is monitored every 30 mins. Similarly, interfaces are monitored every 15 mins for certain parameters. The above scalability numbers mentioned in Clause A are based on the default monitoring intervals.

**NOTICE**

Polling the device every 1 Min instead of every 5 Mins increase the load 5 times. If you have 1000 servers which you wish to monitor every 1 Min then you need 5 more Probes instead of just one.

C. Protocol

Monitoring a device through SNMP is different from monitoring the same via WMI. The nature of these protocols make it either easy to monitor in bulk. The above numbers mentioned in Clause A are based on SNMP. For other protocols such as WMI / CLI / VMware API/ Xen API/ UCS API, the numbers are considerably less.
D. Performance Monitors

By default, OpManager collects around 10-15 parameters per network device and around 20-30 parameters per Server/App. The above numbers mentioned in Clause A are for default monitors. If you add more monitors, the performance will be affected and you have to distribute the load by adding more probes.

1000 devices with 10 monitors at 15 Min interval is not equal to 1000 devices with 20 monitors at 15 Min interval. It doubles the load.

E. Traps

OpManager automatically processes traps sent by network devices and servers. If your network sends out tons of traps then it affects the performance. Either you can identify the source of the traps and switch them OFF or if you need these traps, you can add trap processors and convert them into meaningful alarms. The later will require additional Probes to handle the extra load.

1000 devices with occasional one or two traps can be handled in one server. But if 1 device pumps up thousands of traps continuously then OpManager might spend resources in processing the traps that would affect the normal monitoring.

F. Netflow Licensing

Netflow module is licensed based on number of interfaces. Each interface that exports flow to the netflow server is considered as one license. A single NFA Server can handle upto 100k Flows per second with maximum of 5000 interfaces.

When you export flows from the Router/Switch/Firewall to OpManager server, the interfaces will be automatically added in the system. If you don't want some of the interfaces to be processed, you can UNMANAGE them so that those will not be considered in the licensing or delete them if not required.

You can either add more OPM probes with NFA module on it or You can also go with dedicated NFA Distributed Edition with its own Central and Probe model.

G. Flows Per Second (FPS)

A single server can handle upto 100K Flows Per Second. Beyond this you have to add additional Probes.

1000 interfaces with 50 Flows per second equals 50k flows per second at the OpManager end. But if one or two core interfaces pump up 100k flows per second then its better to split the load across multiple probes.

H. RAW DATA Storage

By default, raw data is disabled in OpManager's NetFlow module. This implies that OpManager can handle upto 200K Flows per second. When Raw Data is enabled, OpManager will be able to handle 100K Flows per second, provided that HighPerf add-on is enabled.
I. DNS lookup

By default an ip address is mentioned as it is in the reports and all over the GUI. If you wish to mention their domain name instead of the IPADDRESS then you have to enable ResolveDNS option. But enabling this impacts the performance severely. Every time a flow is processed, the lookup happens. OpManager caches the domain names of the last 50,000 entries but still it is possible that a delay of few seconds can happen.

**NOTICE**

1000 interfaces with 100k flows per second without DNS look up can be handled in one server.
But 1000 interfaces with 100k flows per second WITH DNS lookup which takes 1 second for lookup will have to split into two Probes

J. Network Configuration Manager (NCM) Licensing Unit

NCM is licensed by the number of devices that needs to be backed up or managed. By default a single OpManager server can handle upto 5000 devices. A Switch or a Router or a Load balancer is considered one device irrespective of whether you wish to just to be notified on configuration change, or Backup, or provision them using configlets, or just run compliance reports.

K. NCM Backup interval

By default backup is taken every 24 hours. The number mentioned in Clause I above are based on this interval. If you reduce the interval, it will impact performance and you have to distribute load

**NOTICE**

5000 devices @ 1 day backup is the same as just 200 devices with 1 hour backup. !!!!
So if you have to take backup frequently add more probes and distribute the load

L. Firewall Analyzer Licensing

Each Firewall consumes a License in Firewall Analyzer.

M. Firewall Logs Per Second (LPS)

By default upto 2000 logs per second can be handled in one server. Beyond that you have to add more Probes.

**NOTICE**

50 Firewalls with 40 Logs per second can be handled in one server
but 1 Firewall with 3000 logs cannot be handled. You have to distribute the load.

N. Application Manager Plugin Licensing

APM is licensed based on number of monitors. A server is a monitor. A URL is a monitor. A file or folder is a monitor. A single APM plugin can recommended for 500 monitors on a single install.

**NOTICE**

50 Servers with IIS installed on it will attract 100 monitors if you want to monitor both the OS and the IIS.
Same will attract 150 monitors if you wish to monitor the URLs on all 50 servers.

O. Application Manager Monitoring Interval

Numbers mentioned above in Clause M are applicable only for default monitoring interval. If you wish to collect data more frequently then the number of probes has to be increased

**NOTICE**

You can either choose to install multiple APM plugins (one per probe) or you could also go for separate APM Enterprise Edition
Applications Supported By OpManager Out-of-the-box

**Microsoft Exchange**
- MS Exchange 2000
- MS Exchange 2003
- MS Exchange 2007
- MS Exchange 2010
- MS Exchange 2013
- MS Exchange 2016

**Microsoft SQL**
- MSSQL 2005
- MSSQL 2008
- MSSQL 2008R2
- MSSQL 2012
- MSSQL 2014
- MSSQL 2016

**Microsoft Active Directory**
- Windows 2003
- Windows 2003 R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

**Via Application Monitoring Plugin**

<table>
<thead>
<tr>
<th>Applications Server Monitoring</th>
<th>Database Monitoring</th>
<th>System Management</th>
<th>Virtualization Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft .Net</td>
<td>Oracle Management</td>
<td>Windows Monitoring</td>
<td>VMware Monitoring</td>
</tr>
<tr>
<td>JBoss</td>
<td>MySQL Management</td>
<td>Linux Monitoring</td>
<td>Microsoft Hyper-V Monitor</td>
</tr>
<tr>
<td>Tomcat</td>
<td>DB2 Management</td>
<td>Solaris Monitoring</td>
<td>Virtual Machine Monitor</td>
</tr>
<tr>
<td>Oracle</td>
<td>Sybase Management</td>
<td>AIX Monitoring</td>
<td>Automatic Virtual Resource Provisioning</td>
</tr>
<tr>
<td>JBoss vFabric tc Server</td>
<td>PostgreSQL Monitoring</td>
<td>AS400 Monitoring</td>
<td>Citrix XenServer Monitoring</td>
</tr>
<tr>
<td>BEA WebLogic</td>
<td>Memcached Monitoring</td>
<td>HP-Unix / Tru64 Unix Monitoring</td>
<td></td>
</tr>
<tr>
<td>JBoss vFabric tc Server</td>
<td>Database Query Monitor</td>
<td>FreeBSD Monitoring</td>
<td></td>
</tr>
<tr>
<td>GlassFish Server</td>
<td>MongoDB Monitoring</td>
<td>Novell Monitoring</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cassandra Monitoring</td>
<td>Mac OS Monitoring</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Redis Monitoring</td>
<td>User Defined Custom Monitors</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Event Log Monitoring</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>File System Monitor</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Performance Counters</td>
<td></td>
</tr>
<tr>
<td>ERP Monitoring</td>
<td>Web Server / Web Services</td>
<td>Website Monitoring</td>
<td>Cloud Monitoring</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------</td>
<td>-------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>SAP Monitor</td>
<td>Web Services (SOAP)</td>
<td>URL Monitoring</td>
<td>Amazon EC2 Monitoring</td>
</tr>
<tr>
<td>Oracle E-Business Suite Monitor</td>
<td>Apache Monitoring</td>
<td>Record &amp; Playback HTTP Requests</td>
<td>Amazon RDS Monitoring</td>
</tr>
<tr>
<td></td>
<td>HS Monitoring</td>
<td>URL Content Monitoring</td>
<td>Automated Cloud Resource Management</td>
</tr>
<tr>
<td></td>
<td>Nginx Monitoring</td>
<td>Real Browser Monitor</td>
<td>Windows Azure Monitoring</td>
</tr>
<tr>
<td></td>
<td>PHP Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSL Certificate Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active Directory Monitor</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LDAP Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FTP, SFTP Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other Web Servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Record &amp; Playback HTTP Requests</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL Content Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Real Browser Monitor</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Middleware/Portal Monitoring</td>
<td>Web Transaction Monitoring</td>
<td>End User Monitoring</td>
<td>Custom Monitoring</td>
</tr>
<tr>
<td>WebSphere MQ Monitor</td>
<td>Java Web Transaction Monitoring (APM Insight)</td>
<td>End User Management</td>
<td>RX Consoles</td>
</tr>
<tr>
<td>HS Office SharePoint Monitor</td>
<td>.NET Web Transaction Monitoring</td>
<td>End User Monitoring from branch offices</td>
<td>SNMP Consoles</td>
</tr>
<tr>
<td>WebLogic Integration Monitor</td>
<td>Ruby on Rails Web Transaction Monitoring</td>
<td></td>
<td>File System Monitor</td>
</tr>
<tr>
<td>Microsoft Message Queue (MSMQ)</td>
<td>Java Runtime Monitoring</td>
<td></td>
<td>Windows Performance Counters</td>
</tr>
<tr>
<td>VMware vFabric RabbitMQ</td>
<td>Java Monitoring</td>
<td></td>
<td>Script Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Database Query Monitor</td>
</tr>
</tbody>
</table>
### Third party JavaScript dependency:

Below is the list of third party code and libraries that OpManager makes use of:

<table>
<thead>
<tr>
<th>JS File Name</th>
<th>Version</th>
<th>License Type</th>
<th>License File</th>
</tr>
</thead>
<tbody>
<tr>
<td>calendar.js</td>
<td>1.1.6.1</td>
<td>LGPL</td>
<td>LICENSE_JSCALENDAR.html</td>
</tr>
<tr>
<td>canvg.js</td>
<td></td>
<td>MIT</td>
<td>MIT-LICENSE.txt</td>
</tr>
<tr>
<td>colorpicker.js</td>
<td>1</td>
<td>MIT</td>
<td>LICENSE_COLORPICKER.txt</td>
</tr>
<tr>
<td>cropper.min.js</td>
<td>1</td>
<td>MIT</td>
<td>LICENSE.MD</td>
</tr>
<tr>
<td>d3.min.js</td>
<td>3.4.8</td>
<td>BSD</td>
<td>LICENSE_D3.txt</td>
</tr>
<tr>
<td>d3-tip.v0.6.3.js</td>
<td>0.6.3</td>
<td>MIT</td>
<td>MIT-LICENSE.txt</td>
</tr>
<tr>
<td>ember-shortcuts.js</td>
<td>0.0.3</td>
<td>MIT</td>
<td>LICENSE_SHORTCUTS.txt</td>
</tr>
<tr>
<td>ember.min.js</td>
<td>1.9.1</td>
<td>MIT</td>
<td>LICENSE_EMBERJS.txt</td>
</tr>
<tr>
<td>filesaver.js</td>
<td></td>
<td>MIT</td>
<td>MIT-LICENSE.txt</td>
</tr>
<tr>
<td>Fontello</td>
<td>1</td>
<td>SIL</td>
<td>LICENSE_FONTELLO.txt</td>
</tr>
<tr>
<td>Google Fonts - Bitter-Regular.ttf</td>
<td>1.1</td>
<td>SIL Open Font License 1.1</td>
<td>LICENSE_LATO_GOOGLE_FONTS.txt</td>
</tr>
<tr>
<td>Google Fonts - Lato-Light.ttf, Lato-Regular.ttf, Lato-Bold.ttf</td>
<td>1.1</td>
<td>SIL Open Font License 1.1</td>
<td>LICENSE_LATO_GOOGLE_FONTS.txt</td>
</tr>
<tr>
<td>gridstack.min.js</td>
<td>0.2.5</td>
<td>MIT</td>
<td>GRIDSTACK_LICENSE</td>
</tr>
<tr>
<td>handlebars.min.js</td>
<td>2.0.0</td>
<td>MIT</td>
<td>LICENSE_HANDLEBARS.txt</td>
</tr>
<tr>
<td>html2canvas.js</td>
<td>0.5.0-beta3</td>
<td>MIT</td>
<td>HTML2CANVAS_LICENSE</td>
</tr>
<tr>
<td>intro.js</td>
<td>2.3.0</td>
<td>Commercial</td>
<td>INTROJS_LICENSE.txt</td>
</tr>
<tr>
<td>jquery-1.9.0.min.js</td>
<td>1.9.0</td>
<td>MIT</td>
<td>LICENSE_JQUERY.txt</td>
</tr>
<tr>
<td>jquery-2.1.1.min.js</td>
<td>2.1.1</td>
<td>MIT</td>
<td>LICENSE_JQUERY.txt</td>
</tr>
<tr>
<td>jquery-migrate-1.2.1.min.js</td>
<td>1.2.1</td>
<td>MIT</td>
<td>LICENSE_JQUERY_MIGRATE.txt</td>
</tr>
<tr>
<td>jquery-ui-1.10.1.custom.min.js</td>
<td>1.10.1</td>
<td>MIT</td>
<td>LICENSE_JQUERY_UI_1_5_3.html</td>
</tr>
<tr>
<td>jquery-ui.min.js</td>
<td>2.1.1</td>
<td>MIT</td>
<td>LICENSE_JQUERY_UI.txt</td>
</tr>
<tr>
<td>jquery.cookie.js</td>
<td>1</td>
<td>MIT</td>
<td>cm_license_info.html</td>
</tr>
<tr>
<td>jQuery.dPassword.js</td>
<td>0.1</td>
<td>MIT</td>
<td><a href="http://www.opensource.org/licenses/mit-license.php">http://www.opensource.org/licenses/mit-license.php</a></td>
</tr>
<tr>
<td>jQuery.easing.min.js</td>
<td>1.3</td>
<td>BSD</td>
<td>Query Easing Plugin 1.3 License</td>
</tr>
<tr>
<td>jQuery.elastic-source.js</td>
<td>1.6.11</td>
<td>MIT</td>
<td>LICENSE_JQUERY_ELASTIC.txt</td>
</tr>
<tr>
<td>jQuery.event.drag-2.2.js</td>
<td>2.2</td>
<td>MIT</td>
<td>LICENSE_JQUERY.Elastic.js.txt</td>
</tr>
<tr>
<td>jQuery.event.drag.live-2.2.js</td>
<td>2.2</td>
<td>MIT</td>
<td>LICENSE_JQUERY.Elastic.js.txt</td>
</tr>
<tr>
<td>jQuery.event.drop-2.2.js</td>
<td>2.2</td>
<td>MIT</td>
<td>LICENSE_JQUERY.Elastic.js.txt</td>
</tr>
<tr>
<td>jQuery.event.drop.live-2.2.js</td>
<td>2.2</td>
<td>MIT</td>
<td>LICENSE_JQUERY.Elastic.js.txt</td>
</tr>
<tr>
<td>jQuery.flot.js</td>
<td>0.8.1</td>
<td>MIT</td>
<td>LICENSE_FLOT.txt</td>
</tr>
<tr>
<td>jQuery.flot.pie.js</td>
<td>0.7</td>
<td>MIT</td>
<td>LICENSE_FLOT.txt</td>
</tr>
<tr>
<td>jQuery.flot.tooltip.js</td>
<td>0.6.1</td>
<td>MIT</td>
<td>LICENSE_FLOT.txt</td>
</tr>
<tr>
<td>jQuery.gridster.min.js</td>
<td>0.5.6</td>
<td>MIT</td>
<td>DUCKSBOARD_GRIDSTER_JS_V0_5_6_0_G3140374_LICENSE.txt</td>
</tr>
<tr>
<td>jQuery.inlineStyler.min.js</td>
<td>1.0.1</td>
<td>MIT</td>
<td>QUERY.INLINESTYLER_LICENSE</td>
</tr>
<tr>
<td>jQuery.jsGrid.src.js</td>
<td>4.4.4</td>
<td>MIT</td>
<td>LICENSE.jsGrid.src.js</td>
</tr>
<tr>
<td>jQuery.mCustomScrollbar.min.js</td>
<td>3.15</td>
<td>MIT</td>
<td>LICENSE_CUSTOM_SCROLLBAR_PLUGIN.txt</td>
</tr>
<tr>
<td>jQuery.mentionsInput.js</td>
<td>1.0.2</td>
<td>MIT</td>
<td>LICENSE_JQUERY MENTIONS.INPUT.txt</td>
</tr>
<tr>
<td>jQuery.mousewheel.min.js</td>
<td>3.1.12</td>
<td>MIT</td>
<td>Query Mousewheel 3_1_12%Query Mousewheel 3.1.12 License%txt</td>
</tr>
<tr>
<td>jQuery.qrcode.min.js</td>
<td>1</td>
<td>MIT</td>
<td>QUERY-QRCODE_MIT-LICENSE.TXT</td>
</tr>
<tr>
<td>jQuery.smooth-scroll.min.js</td>
<td>v1.3+</td>
<td>MIT</td>
<td>LICENSE_NMAP.txt</td>
</tr>
<tr>
<td>JColor.js</td>
<td>1.4.0</td>
<td>LGPL</td>
<td>LICENSE_JCOLOR_TYPE.txt</td>
</tr>
<tr>
<td>JSPDF.js</td>
<td>0.9.0</td>
<td>MIT</td>
<td>LICENSE_JSPDF.txt</td>
</tr>
<tr>
<td>JSPDF.plugin.addImage.js</td>
<td>0.9.0</td>
<td>MIT</td>
<td>LICENSE_JSPDF.txt</td>
</tr>
<tr>
<td>JSPDF.plugin.addImage.js</td>
<td>0.9.0</td>
<td>MIT</td>
<td>LICENSE_JSPDF.txt</td>
</tr>
<tr>
<td>jPlumb-1.7.10.js</td>
<td>1.7.10</td>
<td>MIT</td>
<td>LICENSE_JSPDF.plugin.addImage.js</td>
</tr>
<tr>
<td>Jstree.min.js</td>
<td>3.0.8</td>
<td>MIT</td>
<td>STREE_LICENSE-MIT</td>
</tr>
<tr>
<td>Lightbox.js</td>
<td>2.5.1</td>
<td>MIT</td>
<td>LICENSE.Lightbox.js</td>
</tr>
<tr>
<td>moment-timezone-with-data.min.js</td>
<td>0.5.4</td>
<td>MIT</td>
<td>MOMENT_TIMEZONE_LICENSE</td>
</tr>
<tr>
<td>moment.min.js</td>
<td>2.13.0</td>
<td>MIT</td>
<td>LICENSE_TIMEZONE_LICENSE</td>
</tr>
<tr>
<td>morris.js</td>
<td>0.5.0</td>
<td>BSD</td>
<td>MORRIS_LICENSE.txt</td>
</tr>
</tbody>
</table>

**Note:** The details of the license files are not provided in the document, but they are assumed to be located in the specified directories or linked to the respective libraries.
<table>
<thead>
<tr>
<th>File Name</th>
<th>Version</th>
<th>License</th>
<th>License File</th>
</tr>
</thead>
<tbody>
<tr>
<td>PointerLockControls.js</td>
<td>1</td>
<td>MIT</td>
<td>Threejs License.txt</td>
</tr>
<tr>
<td>RadialProgress.js</td>
<td></td>
<td>MIT</td>
<td>LICENSE_RADIALPROGRESS.txt</td>
</tr>
<tr>
<td>Raphael-min.js</td>
<td>2.1.0</td>
<td>MIT</td>
<td>LICENSE_RAPHAEL.txt</td>
</tr>
<tr>
<td>rgbcolor.js</td>
<td>1</td>
<td>MIT</td>
<td>CANVG MIT-LICENSE.TXT</td>
</tr>
<tr>
<td>Rickshaw.js</td>
<td></td>
<td>MIT</td>
<td>LICENSE_RICKSHAW.txt</td>
</tr>
<tr>
<td>Select2.min.js</td>
<td>4.0.3</td>
<td>MIT</td>
<td>Select2 LICENSE.html</td>
</tr>
<tr>
<td>Three.js</td>
<td>Revision 49</td>
<td>MIT</td>
<td>LICENSE_THREE_JS.txt</td>
</tr>
<tr>
<td>Timeline.js</td>
<td>3.3.10</td>
<td>MPL</td>
<td>TIMELINEJS3_3_0_0_LICENSE.html</td>
</tr>
<tr>
<td>Underscore-min.js</td>
<td>1.3.3</td>
<td>MIT</td>
<td>LICENSE_JQUERY_UNDERSCORE.txt</td>
</tr>
<tr>
<td>Vis.min.js</td>
<td>4.16.1</td>
<td>Apache 2.0</td>
<td>VISJS_LICENSE.html</td>
</tr>
</tbody>
</table>
### Third-party Library dependency

Below is the list of code and libraries OpManager makes use of:

<table>
<thead>
<tr>
<th>JAR Name</th>
<th>Version Number</th>
<th>License Type</th>
<th>3rd Party Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java</td>
<td>1.7.0_55-b13</td>
<td>Sun Microsystems, Inc. Binary Code License Agreement</td>
<td>Sun Microsystems, Inc.</td>
</tr>
<tr>
<td>Postgresql</td>
<td>9.2.4</td>
<td>PostgreSQL License</td>
<td>Postgresql</td>
</tr>
<tr>
<td>Apache Tomcat</td>
<td>8.5.13</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>activation.jar</td>
<td>1.0.2</td>
<td>Sun Microsystems, Inc. Binary Code License Agreement</td>
<td>Sun Microsystems, Inc.</td>
</tr>
<tr>
<td>activation.jar</td>
<td>1.0.2</td>
<td>Sun Microsystems, Inc. Binary Code License Agreement</td>
<td>Sun Microsystems Inc.</td>
</tr>
<tr>
<td>annotations-api.jar</td>
<td>0.0.FR</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>Antisamy-1.5.3.jar</td>
<td>1.5.3</td>
<td>The BSD 3-Clause License</td>
<td>The Open Web Application Security Project (OWASP)</td>
</tr>
<tr>
<td>aspectjweaver.jar</td>
<td>1.7.2</td>
<td>EPL 1.0</td>
<td>aspectj.org</td>
</tr>
<tr>
<td>ioxis.jar</td>
<td>1.4</td>
<td>Apache License, Version 2.0</td>
<td>Apache Web Services</td>
</tr>
<tr>
<td>batik-awt-util.jar</td>
<td>1.0</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>batik-css.jar</td>
<td>1.7+r608262</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>batik-dom.jar</td>
<td>1.0</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>batik-swingen.jar</td>
<td>1.0</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>batik-util.jar</td>
<td>1.7+r608262</td>
<td>Apache License, Version 2.0</td>
<td>The Apache Software Foundation</td>
</tr>
<tr>
<td>batik-ui.jar</td>
<td>1.0</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>batik-xml.jar</td>
<td>1.0</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>bcprov-jdk1son-1.52.jar</td>
<td>1.52.0</td>
<td>MIT License</td>
<td>BouncyCastle.org</td>
</tr>
<tr>
<td>bcprov.jar</td>
<td>1.37.0</td>
<td>MIT License</td>
<td>BouncyCastle.org</td>
</tr>
<tr>
<td>catalina-ant.jar</td>
<td>1.5.13</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>catalina-ha.jar</td>
<td>1.5.13</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>catalina-storeconfig.jar</td>
<td>1.5.13</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>catalina-tribes.jar</td>
<td>1.5.13</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>catalina.jar</td>
<td>1.5.13</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>cewolf.jar</td>
<td>1.4.2</td>
<td>LGPLv2</td>
<td>Sun Microsystems, Inc.</td>
</tr>
<tr>
<td>commons-beanutils-1.8.0.jar</td>
<td>1.8.0</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>commons-beanutils.jar</td>
<td>1.6</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>commons-chain-1.2.jar</td>
<td>1.2</td>
<td>Apache License, Version 2.0</td>
<td>The Apache Software Foundation</td>
</tr>
<tr>
<td>commons-collections.jar</td>
<td>1.0</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>commons-digester.jar</td>
<td>1.8</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>commons-fileupload-1.3.1.jar</td>
<td>1.3.1</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>commons-httpclient-3.0.0rc1.jar</td>
<td>3.0-rc1</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>commons-httpclient-3.1.jar</td>
<td>3.1</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>commons-io-1.2.jar</td>
<td>1.2</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>commons-lang-2.0.jar</td>
<td>2.0</td>
<td>Apache Software License, Version 1.1</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>commons-lang-3.1.jar</td>
<td>3.1</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>commons-logging-2.1.jar</td>
<td>2.1</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>commons-logging-2.2.jar</td>
<td>2.1</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>commons-logging.jar</td>
<td>2.1</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>commons-logging-1.1.jar</td>
<td>1.1</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>commons-net-2.0.jar</td>
<td>2.0</td>
<td>Apache License, Version 2.0</td>
<td>The Apache Software Foundation</td>
</tr>
<tr>
<td>commons-net-3.1.jar</td>
<td>3.1</td>
<td>Apache License, Version 2.0</td>
<td>The Apache Software Foundation</td>
</tr>
<tr>
<td>commons-validator-1.3.1.jar</td>
<td>1.3.1</td>
<td>Apache License, Version 2.0</td>
<td>The Apache Software Foundation</td>
</tr>
<tr>
<td>concurrent.jar</td>
<td>1.3</td>
<td>LGPL</td>
<td>osgpwo.edu</td>
</tr>
<tr>
<td>difftutils-1.2.1.jar</td>
<td>1.2.1</td>
<td>Apache License, Version 2.0</td>
<td>difftutils</td>
</tr>
<tr>
<td>groovy-2.0.6.jar</td>
<td>2.0.6</td>
<td>BSD License</td>
<td>grsjava</td>
</tr>
<tr>
<td>groovy-2.0.5.jar</td>
<td>2.0.5</td>
<td>BSD License</td>
<td>grsjava</td>
</tr>
<tr>
<td>jdom-1.6.jar</td>
<td>1.6</td>
<td>BSD</td>
<td>MetaStuff Ltd.</td>
</tr>
<tr>
<td>jdom-1.6.1.jar</td>
<td>1.6.1</td>
<td>BSD</td>
<td>MetaStuff Ltd.</td>
</tr>
<tr>
<td>File</td>
<td>Version</td>
<td>License</td>
<td>Organization</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------</td>
<td>----------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>xmlrpc-client-3.1.2.jar</td>
<td>3.1.2</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>xmlrpc-client-3.1.jar</td>
<td>3.1</td>
<td>Apache License Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>xmlrpc-common-3.1.2.jar</td>
<td>3.1.2</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>xmlrpc-common-3.1.jar</td>
<td>3.1</td>
<td>Apache License Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>xmlrpc-server-3.1.2.jar</td>
<td>3.1.2</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
<tr>
<td>xmlsec-1.4.1.jar</td>
<td>1.4.1</td>
<td>Apache License, Version 2.0</td>
<td>Apache Software Foundation</td>
</tr>
</tbody>
</table>
OpManager Architecture
Add Credentials

OpManager accesses the remote devices using the protocols SNMP, CLI, or WMI. 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.

1. Go to Settings (alt + t) > Credentials > Discovery
2. Click Add New
3. Configure the following parameters and click Add to add the credentials:

**Credential Type:** Select the relevant protocol.

**SNMP v1/SNMPv2:** SNMPv1 and SNMPv2 are community based security models. Enter the Credential name and description. Configure the correct Read and Write community, and the SNMP Port.

**SNMP v3:** SNMPv3 is a user based security model. It provides secure access to the devices by a combination authenticating and encrypting packets over the network. The security features provided in SNMPv3 are Message integrity, Authentication and Encryption. If you select SNMPv3 as the credential type, then configure the following parameters.

1. **Name:** Enter the name of the credential.
2. **Description:** Enter a brief description about the credential.
3. **User Name:** Enter the name of the user (principal) on behalf of whom the message is being exchanged.
4. **Context Name:** An SNMP context name or “context” in short, is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context. An SNMP entity potentially has access to many contexts. In other words, if a management information has been defined under certain context by an SNMPv3 entity, then any management application can access that information by giving that context name. The “context name” is an octet string, which has at least one management information.
5. **SNMP Port:** Enter the SNMP port number.
6. **Authentication:** Select any of the authentication protocols either MD5 or SHA and enter the password. MD5 and SHA are processes which are used for generating authentication/privacy keys in SNMPv3 applications.
7. **Encryption:** Select any of the encryption protocols either DES or EAS-128 and enter the password. Note: Only after configuring Authentication it is possible to configure Encryption.

**WMI:** If you select WMI as the protocol, configure the Domain Name, the user name, and the password. Example:- TestDomainTestUser. Also enter the credential name and description.

**Telnet/SSH:** Enter the credential name and description. For Telnet/SSH, make sure you configure the correct login prompt, command prompt, and password prompt besides the user name and password to access the device.

**VMware:** Provide the HTTPS Username and Password of the Host. Enter the HTTPS web service port number and timeout interval for the connection between the Host and OpManager server.

**UCS:** Provide the UCS Manager Username and Password. Enter the Port, Protocol and Timeout interval for the connection between the UCS and OpManager Server.
Rule Engine

Rule Engine helps you automate the activities such as adding monitors to a device or adding a device to a business view that you carry out after adding the devices to OpManager. This helps you start monitoring the devices straight away as soon as you add them and avoid repetitive manual effort.

How does Rule Engine Work?
The Rule Engine is condition/criteria based. During discovery, devices that satisfy the condition/criteria are associated with the actions specified in the Rule Engine.

Steps to add a Rule Engine
1. Go to Settings(alt+t) > Configuration > Rule Engine > Add New
2. Enter a Name and Description for the Rule Engine.
3. Define the Criteria and select the Condition.
   Eg. Select Service Name as the Criteria and equals as the Condition, and enter the POP3Svc (POP3Svc is a MSExchange service. This is to verify whether the discovered device is an exchange server or not.)
4. If required you can define multiple criteria, but have to select either AND or OR option.
   AND: Executes the action when all the defined criteria are satisfied.
   OR: Executes the actions when any one of the defined criteria is satisfied.
5. Define the actions
   Eg. Select Add Service Monitor as the action and select the required service monitors (Exchange server related monitors are added to the devices that satisfy the POP3Svc condition.)
6. Click Add. If required you can define multiple actions as well.
7. Click Save to save the rule.

Actions with Rule Engine
Following are the actions that be done on a created rule engine

- Edit
- Copy As
- Enable/Disable
- Delete

Click the respective icons to carry out these actions on a Rule Engine.

Re-running a Rule
To re-run a rule on demand,
1. Select the rule that you want to re-run.
2. Click on the Re-run button.
3. Select the devices on which you want to execute the rule.
4. Click OK.
Discover Individual Devices

You might have added more devices to your network and may therefore need to forcefully discover these devices. You can discover such devices on demand by following the steps below:

1. Go to Settings (alt + t) > Discovery > Add Device
2. Type either the IP Address or the Device Name of the device to be discovered.
3. Enter the correct Netmask/Network IP. Example: IPv4-255.255.255.0, IPv6-::b343:567e:c254:0
4. Select the discovery credentials.
5. Click Add Device to start discovery

**Note:** If you are unable to add the device, try to ping the device from the OpManager machine and check for response. Search the device using the Device Search box on the top right corner in the WebClient.
Discovering Networks Using OpManager

You can discover devices on a network by either specifying a range or the entire network. OpManager uses ICMP/Nmap to discover the devices on a network.

1. **Discovering devices from an IP Range**
2. **Discovering a complete network**
3. **Discovering devices by CSV import**
4. **Discovering Interfaces**

**Discover a Range**

To discover devices from a selected range specify the start and end ip address and select the netmask for the devices to be discovered within that range.

1. Go to Settings (alt + t) > Discovery > Add Network
2. Use IP Range: Select this option to specify the range.
3. Start IP: Specify the IP address of the device in the range from where OpManager should start discovery.
4. End IP: Specify the IP address till which OpManager should discover.
5. Netmask: Select the correct netmask.
6. Discovery Credentials: Select the configured Credentials to be used for discovery.
7. Click Discovery for the discovery to start.

**Discover a complete network**

1. Go to Settings (alt + t) > Discovery > Add Network
2. Use CIDR: Select this option to discover an entire network.
3. Network IP: Specify the Network IP to be discovered.
4. Credentials: Select the credentials and SNMP settings as mentioned above.
5. Click Discovery for the discovery to start.

OpManager supports discovering Hyper-V hosts and VMs using CIDR.

**Discover by Importing from a file**

You can import a set of IP addresses for discovery from a csv file.

1. Go to Settings (alt + t) > Discovery > Add Network
2. Select CSV File Import
3. Create a csv file (as shown below) with the details of name/ipaddress of the device, displayname and device type.

<table>
<thead>
<tr>
<th>DeviceName,DisplayName,DeviceType</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.11.5,FengiAliasChris,Windows7</td>
</tr>
<tr>
<td>172.24.1.21,MailServer,Windows 2008</td>
</tr>
<tr>
<td>172.18.2.101,CiscoRouter,Cisco 2500 Series</td>
</tr>
</tbody>
</table>

4. Browse and select the CSV file from which you want the devices discovered and imported.
5. Provide the correct netmask.
6. Click Discovery for the discovery to start.

**Note:** If you are using DHCP protocol on your network, make sure that both the forward and reverse lookup gets resolved before you add the devices to OpManager.
Discover Interfaces

1. Go to Settings (alt + t) > Discovery > Interface Discovery
2. Select Category, Devices, Interface Type and Status
3. Click Discover to discover the interfaces
Layer 2 Mapping

Layer 2 Discovery helps network administrators/ Data center admins to visualize their complete network infrastructure with a live network map. It automatically discovers, maps and reports the complete set of devices (servers, desktops, virtual machines, firewalls etc) present in your infrastructure in less than no time.

It also offers periodical network rediscovery options to keep the map live and up-to-date. You can export these network maps to PDF, take print outs and share it with your peer groups.

<table>
<thead>
<tr>
<th>Layer2 Discovery</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Router Address</strong> : 192.168.49.1</td>
</tr>
<tr>
<td><strong>Start IP</strong> : 192.168.49.1</td>
</tr>
<tr>
<td><strong>End IP</strong> : 192.168.50.250</td>
</tr>
<tr>
<td><strong>NetMask</strong> : 255.255.255.0</td>
</tr>
<tr>
<td><strong>Layer2 Map Name</strong> : MELab</td>
</tr>
<tr>
<td><strong>Schedule Interval (in days)</strong> : 1</td>
</tr>
<tr>
<td><strong>Credentials to use</strong> : Add Credential</td>
</tr>
</tbody>
</table>

**Configuration**

1. Go to Settings (alt + t) > Discovery > Layer 2 Discovery
2. Router Address > The device must be a **Seed Router** or an **L3 Switch**
3. Start IP > Network range starting IP Address
4. End IP > Network range ending IP Address
5. NetMask
6. Layer 2 Map Name > Unique name of Map to be referenced from all the places
7. Schedule Interval > Specify the interval (in days) at which the map must be re-drawn
8. Select the respective credential and click Discover to let OpManager draw the map.
Managing and Unmanaging a Device

By default, OpManager manages all the discovered devices. However, there might be some known devices that are under maintenance and hence cannot respond to status polls sent by OpManager. These devices can be set to unmanaged status to avoid unnecessary polling. Once maintenance gets over, they can be set to managed status.

To unmanage a device
1. Go to the device snapshot page.
2. Under Actions, select Unmanage.

This stops the status polling and data collection for the device and changes the device status icon to gray.

To start managing an unmanaged device
1. Go to the device snapshot page.
2. Under Actions, select Manage.

This resumes the status polling and data collection for the device. The status icon shows the current status of the device.
Device Snapshot

OpManager’s Device Snapshot shows the device health and that of its resources at a glance.

To view the snapshot page of the device, click the device name link in the map, or type the Name or IP of the device in the Search box and hit Enter. Click the device whose snapshot you want to view.

**Summary**  
This tab list Device details, Availability, ResponseTime, Packetloss, CPU, Memory, Disk Utilization etc

**Alerts**  
This tab display the current alarms for the device

**Monitors**  
This tab list different monitors for the device. You can add or remove monitors from performance monitors

**Graphs**  
This tab display the graph of each resource monitor added

**Notifications**  
This tab list all the notification profile associated to the device. You can also add or associate new profile from here

**Workflow**  
This tab list all the Wokrflow associated to the device

**DeviceNotes**  
This tab shows additional device details. You can add additional fields to denote the device details

**Interfaces**  
This tab list all the all the interface or ports associated to the device. Click the interface name link for more details

---

<table>
<thead>
<tr>
<th>Device snap-shot - Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Details</strong></td>
</tr>
<tr>
<td><strong>Click here to change</strong></td>
</tr>
<tr>
<td><strong>Dial or Graph</strong></td>
</tr>
<tr>
<td><strong>Note</strong>: Resource Monitor dial varies according to the category</td>
</tr>
<tr>
<td><strong>Installed Software or Hardware Details</strong></td>
</tr>
<tr>
<td><strong>Active Process</strong></td>
</tr>
</tbody>
</table>
Device snap-shot - Alerts
Device snap-shot - Monitors

Device snap-shot - Graphs
Device snap-shot - Notifications

Device snap-shot - Workflow
Tools: The following actions can be done by clicking the respective icon:

- Ping
- Trace Route
- Browse
- Open a Telnet session [Note: Telnet is not enabled in IE7 in Windows and Firefox in Linux.
- Open Remote desktop connection [Note: RDP is not enabled in IE7 in Windows.

Actions Menu: List of actions that can be performed on the device include:

- Configure IPMI
- Update Status
- Rediscover Now
- Suppress Alarms
- Monitoring
- Delete
- Manage/UnManage
Configuring Additional Device or Interface Properties

Configure additional properties of a device by adding additional fields. This makes device management easy.

1. Go to Settings (alt + t) > Configuration > Additional Fields. A list of pre-populated fields is shown.
2. Click Add a Field button on the top right corner and configure the following values.
   1. Select Category: Select a category (Devices or Interface)
   2. Field Name: Configure the name of the additional
   3. Field Type: Select the property type (text, numeric and date)
   4. Field Length: Set the length of the field.
   5. Description: Add a meaningful description for the field.
   6. Click Save

The properties added is applied to all the devices or interfaces.

Device > The additional fields are displayed when you click the Device Notes tab in the device snapshot page.
Interface > The addition fields are displayed when you click the Additional Fields tab in the interface snapshot page.
Configuring Device Dependencies

The status polling for a device can be controlled based on its dependency on some other device. This prevents the unnecessary status checks made to the dependent nodes.

For instance, many devices will be connected to a switch. If the switch goes down, all the devices connected to it will not be reachable. In this case, it is unnecessary to check the status of the dependent devices.

Configuring dependencies in individual devices

You can configure dependencies for a single device from the device snapshot page. Here are the steps:

1. Go to the device snapshot page.
2. Device details, click edit and configure the Dependency from the drop down.
3. Click Save

OpManager stops monitoring the devices if the dependent device is down. Configuring dependencies prevents false alarms.
Classification and Device Templates

During initial discovery, OpManager categorizes the network devices into servers, printers, switches, routers and firewalls. For proper classification, install and start the SNMP agent on all the managed devices.

OpManager comes with over 780 device templates which carry the initial configurations to classify the devices into the pre-defined categories, and to associate monitors to them. The device templates enables you to effect a configuration once and is applied to several devices at a time whenever there is a change.

The templates carry the information required to classify the devices and to associate relevant monitors. You can define your own templates and modify the existing ones.

Creating/Modifying Device Templates

1. Go to Settings ( alt+t )> Configuration > Device Templates
2. Click Add New to define a template for a new device type. Click the Template name to modify an existing one.
3. Configure/Modify the following properties:
   - **Device Template**: Specify the device type.
   - **Vendor Name**: Select the vendor. Click Add New to add a new vendor, and Save.
   - **Category**: Select the category for the device type. On discovery, the devices are automatically placed in the select Category map.
   - **Monitoring Interval**: Configure the interval at which the device needs monitoring.
   - **Device Image**: Select the image for this device type.
   - **Device Identifier**: Type the sysOID and click Add (or) Click Query Device for OpManager to query the device for the OID.
   - **Add Monitor**: Click this option to select the monitors.
   - **Edit Thresholds**: Click this option to edit thresholds.
   - Click Create button to create the new device template.

The classified devices are placed under different maps for easy management. For proper device classification, make sure you have installed and started SNMP in all the network devices before starting OpManager service.

The default maps include:

- Servers
- Routers
- Desktops
- Switches
- Firewalls
- DomainControllers
- Load Balancer
- WAN Accelerator
- Wireless
- UPS
- PDU
- Printers
- Virtual Device
- Unknown
- Storage
- URLs
- WAN RTT Monitors
- VoIP Monitors
You can also add your own infrastructure views. Custom infrastructure views can be added to group devices which cannot be classified under the default views provided. For instance, if you would like to monitor some IP Phones, it will not be appropriate to classify them as servers or desktops.

This initial classification may not be accurate if

- the network devices do not support SNMP.
- some devices have their SNMP settings different from those specified in the Credential Settings.
Classification and Device Templates

During initial discovery, OpManager categorizes the network devices into servers, printers, switches, routers and firewalls. For proper classification, [install and start the SNMP agent](#) on all the managed devices.

OpManager comes with over 780 device templates which carry the initial configurations to classify the devices into the pre-defined categories, and to associate monitors to them. The device templates enables you to effect a configuration once and is applied to several devices at a time whenever there is a change.

The templates carry the information required to classify the devices and to associate relevant monitors. You can define your own templates and modify the existing ones.

Creating/Modifying Device Templates

1. Go to Settings (alt+t) > Configuration > Device Templates
2. Click Add New to define a template for a new device type. Click the Template name to modify an existing one.
3. Configure/Modify the following properties:
   - **Device Template**: Specify the device type.
   - **Vendor Name**: Select the vendor. Click Add New to add a new vendor, and Save.
   - **Category**: Select the category for the device type. On discovery, the devices are automatically placed in the select Category map.
   - **Monitoring Interval**: Configure the interval at which the device needs monitoring.
   - **Device Image**: Select the image for this device type.
   - **Device Identifier**: Type the sysOID and click Add.
   - **Add Monitor**: Click this option to select the monitors.
   - **Edit Thresholds**: Click this option to edit thresholds.
   - Click Create button to create the new device template.

The classified devices are placed under different maps for easy management. For proper device classification, make sure you have installed and started SNMP in all the network devices before starting OpManager service.

The default maps include:

- Servers
- Routers
- Desktops
- Switches
- Firewalls
- DomainControllers
- Load Balancer
- WAN Accelerator
- Wireless
- UPS
- PDU
- Printers
- Virtual Device
- Unknown
- Storage
- URLs
- WAN RTT Monitors
- VoIP Monitors
You can also [add your own infrastructure views](#). Custom infrastructure views can be added to group devices which cannot be classified under the default views provided. For instance, if you would like to monitor some IP Phones, it will not be appropriate to classify them as servers or desktops.

This initial classification may not be accurate if

- the network devices do not support SNMP.
- some devices have their SNMP settings different from those specified in the [Credential Settings](#).
Categorization into Default Maps

Devices are categorized into the following default maps in OpManager: The classification is done using SNMP and NMAP.

- Servers
- Routers
- Desktops
- Switches
- Firewalls
- DomainControllers
- Load Balancer
- WAN Accelerator
- Wireless
- UPS
- Printers
- PDU
- Virtual Device
- UCS
- Unknown
- Storage
- URLs
- WAN RTT Monitors
- VoIP Monitors

The discovered devices are classified into the above categories based on response to SNMP requests sent by OpManager to the devices. The devices that are not SNMP enabled, and the device types which are not included in the template are incorrectly classified under desktops. You can also add your own infrastructure maps to group your devices according to categories, or create business views to logically group devices, for instance, based on geography.
Adding New Infrastructure Views

You can create more defined groups by adding more custom views. For instance, you might want to group all your Environment Sensors or IP Phones into separate infrastructure views.

Adding New Infrastructure View

1. Go to Inventory ( alt+i ) > Sort By Category > Add Category
2. Specify the category Name.
3. Select the category whose properties need to be inherited for this category
4. Click Add Category

After you create new infrastructure views, you can create device templates for devices of this category. This allows you to define monitors specific to the category and automatically applies the configurations defined in the template to the devices as soon as they are discovered.
Different Types of Views

HeatMaps View
It helps you to visualize your entire network health in real-time from a single page. It uses color codes to communicate the severity of the monitored devices. HeatMap view can be accessed from the Inventory > All Devices, Server, Router, Server, Desktop etc.

Grid View
<table>
<thead>
<tr>
<th>Device Name</th>
<th>Status</th>
<th>IP Address</th>
<th>Device Type</th>
<th>Category</th>
<th>Vendor</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>CiscoRouter.wwnlab.net</td>
<td>Clear</td>
<td>192.168.49...</td>
<td>Cisco 2900 I</td>
<td>Router</td>
<td>Cisco</td>
<td>8</td>
</tr>
<tr>
<td>Dell Rack System - G31Z9...</td>
<td>Clear</td>
<td>172.21.10.78</td>
<td>Dell</td>
<td>Server</td>
<td>Dell Inc.</td>
<td>2</td>
</tr>
<tr>
<td>ELA-W52012</td>
<td>Error</td>
<td>172.21.146.52</td>
<td>Windows 20...</td>
<td>Server</td>
<td>Microsoft</td>
<td>38</td>
</tr>
<tr>
<td>HPSwitch</td>
<td>Clear</td>
<td>192.168.50...</td>
<td>HP Switch J8...</td>
<td>Switch</td>
<td>Hewlett-Pac...</td>
<td>37</td>
</tr>
<tr>
<td>MEJuniper4200</td>
<td>Clear</td>
<td>192.168.49...</td>
<td>Juniper-EX4...</td>
<td>Switch</td>
<td>Juniper</td>
<td>72</td>
</tr>
<tr>
<td>MLcisco1002,MLcisco1002</td>
<td>Clear</td>
<td>192.168.49...</td>
<td>Cisco Device</td>
<td>Router</td>
<td>Cisco</td>
<td>7</td>
</tr>
<tr>
<td>MS-WS-64-1</td>
<td>Error</td>
<td>172.21.144...</td>
<td>Windows 20...</td>
<td>Server</td>
<td>Microsoft</td>
<td>16</td>
</tr>
<tr>
<td>NPI2DBA13</td>
<td>Clear</td>
<td>192.168.222...</td>
<td>HP-Printer</td>
<td>Printers</td>
<td>Hewlett-Pac...</td>
<td>2</td>
</tr>
<tr>
<td>NPI2DBA17</td>
<td>Clear</td>
<td>192.168.225...</td>
<td>HP-Printer</td>
<td>Printers</td>
<td>Hewlett-Pac...</td>
<td>2</td>
</tr>
<tr>
<td>OPMAN-K8R2S-64-2</td>
<td>Error</td>
<td>172.21.146.4</td>
<td>Windows 20...</td>
<td>Server</td>
<td>Microsoft</td>
<td>25</td>
</tr>
<tr>
<td>OPMAN-K8R2S-64-6</td>
<td>Error</td>
<td>172.21.146.5</td>
<td>Windows 20...</td>
<td>Server</td>
<td>Microsoft</td>
<td>24</td>
</tr>
</tbody>
</table>
Adding a Domain

To add a domain:

2. Enter the Domain Name.
3. Enter the Domain Controller name.
4. Select Enable Auto Login.
   1. Select either All Users or Selected Groups.
      All Users: The auto login will be enabled to all the users. Select the permissions that you want assign - Read Only or Full Control.
      Selected Groups: The auto login will be enabled to the groups you specify. Enter the name of the groups in Read Only and Full Control columns. The access to groups will be enabled accordingly. Note: Configure one Group Name per line. The names are case-sensitive and should be configured as given in your AD.

5. Select the Social IT check box to enable acces for the users in Domain for the Social IT Page.
6. Click Add.

A new domain has been successfully added.
Create New Users

You can create users in OpManager and provide required privileges to them. The option to create users is available only for the admin login account or those accounts which have 'Full Control' privilege.

Steps to add a user:

1. Go to Settings (alt+t) > User Management > User > Add User.
2. Select any of the following tab based on the User type
   - Add Local User
   - Add AD User
   - Authorize AD Group Users

Adding a Local user

1. Login Details:
   - Email ID - Email ID for the user
   - Password - a password for the above user
   - Re-type Password - retype the password for confirmation
2. Contact Details:
   - Phone number: the user's phone number
   - Mobile number: the user's mobile number
3. Access Details:
   - User Permission - Select the permission as Full Control to provide complete admin privilege to the user, or select Read-only Access to restrict the scope of the user to only read operations. A user with this permission can only view the details.
   - Has access to - You can provide this user an access to either All Devices, or only specific Business Views, and/or WAN
4. Select the Social IT Plus Account check box to enable the user to access Social IT page
5. Click Add User to add the user according to the scope specified here

Logout and try logging in as the new user and check the privileges.

Adding an AD user

1. Login Details:
   - User Name - Name of the AD user to be added
   - Email ID - Email ID of the AD user
2. Select AD Domain - Select the desired AD domain from the list of available domains or Click Add Domain to add a new domain.
3. Contact Details:
   - Phone number: the user's phone number
   - Mobile number: the user's mobile number
4. Access Details:
   - User Permission - Select the permission as Full Control to provide complete admin privilege to the user, or select Read-only Access to restrict the scope of the user to only read operations. A user with this permission can only view the details.
   - Has access to - You can provide this user an access to either All Devices, or only specific Business Views, and/or WAN
5. Select the Social IT Plus Account check box to enable the user to access Social IT page
6. Click Add User to add the user according to the scope specified here

Logout and try logging in as the new user and check the privileges.

Authorize AD group Users

1. User Group Details:
Select AD Domain: Click on the drop down menu and select the desired AD domain from the list of available domains or Click Add Domain to add a new domain.

**Domain Controller:** Update/provide the name of the AD domain controller. The domain controller name gets loaded automatically, once you select an existing AD domain.

**Enabling auto login:** You can allow "All Users" (or) "Users from Selected Groups" under the chosen AD domain to access OpManager using their AD credentials. If you have chosen Selected Groups, provide the list of group names that require full or read-only access control. In case if the same user exist in both groups with read only and full control user permissions. The user with read only permission gets the preference over the other.

2. **Access Details:**
   - **User Permissions:** Select "Full Control" to provide complete read/write control to the user to monitor resources using OpManager. Select "Read Only Access" if the user is allowed only to view the resources.
   - Select the **Social IT Plus Account** check box to enable the user to access Social IT page

4. Click **Save.**
Changing User Passwords

You can change the password for the users. Either the admin user or an user with full control privilege only can change the passwords.

1. Go to Settings (alt+t) User Management.
2. Click the Edit icon against the user name whose password you want changed.
   1. **Password Details:**
      - New Password- a password for the above user
      - Re-type Password- retype the password for confirmation
   2. **Contact Details:**
      - Phone number: the user's phone number
      - Mobile number: the user's mobile number
   3. **Access Details:**
      - For users with only partial permission, the business views assigned to that user is displayed. Remove selection for the view if you want to remove the views from the user's purview. For users with full control, this option is not displayed.
Removing Users

You can remove the users.

1. Go to Settings ( alt+t ) --> User Management.
2. Click the Delete icon against the user name whose account you want to delete.
3. A confirmation dialog pops up. Click OK. The user account is deleted.
Pass-through Authentication

Pass-through authentication (Single Sign-on) provides the ability to authenticate yourself automatically in OpManager using your currently logged in windows system username and password. You would not need to manually enter your windows credential to log-in to OpManager webclient.

Prerequisites:

- Active directory authentication must have been configured in OpManager for the domain you want enable Pass-through Authentication. [Adding Domain](#).
- User accounts to whom you want to enable pass-through must have been already available in OpManager. [Create New Users](#) -> AD User.
- A computer account must be created in the Domain Controller for ensuring secure communication with the Domain Controller by OpManager.
- OpManager webserver must have been added as a trusted site in each browser you will be using to connect OpManager webclient to avoid browser popups asking for credential.

Creating Computer Account:

Run the script NewComputerAccount.vbs present under OpManager_Homeconfapplicationscripts to create a new computer account

```
cscript NewComputerAccount.vbs account_name /p password /d domain_name
```

To reset the password for an existing computer account, run the script SetComputerPass.vbs present under OpManager_Homeconfapplicationscripts to create a new computer account

```
cscript SetComputerPass.vbs account_name /p password /d domain_name
```

Ensure that the password you give is compliant to the password policy for that domain. Do not use the New Computer Account option present in AD native client which will not allow you to choose password. If you face problem running this script from OpManager server, copy the script to the domain controller machine itself and try running it.

Configuring Trusted Site in Browser:

For Internet Explorer (applicable to Chrome as well):

Open **Tools -> Internet Options -> Security -> Local Intranet -> Sites -> Advanced**. Enter OpManager server URL, click **Add**.

For Firefox:

In URL box enter **about:config**. Click the button "I'll be careful. I promise", if warning page is displayed. In the resulting page, search for **ntlm**. Double click the option **network.automatic-ntlm-auth.trusted-uris**. Enter OpManager server URL in the text box and click OK. (Multiple site entries can be entered separated by comma.)

Configuring in OpManager:

In OpManager webclient, click **Settings ( alt+t ) -> User Management > Pass-through**. Check "Enable Pass-through Authentication".
Domain Name: NETBIOS name of your domain. Example: OPMANHV

Bind String: DNS Name of your domain Example: opmanhv.com

DNS Server IP: Primary IP Address of the DNS Server.

DNS Site: Site under which the Domain Controller is listed.

Computer Account: Account name of the computer account created. Append $@domain_dns_name with the account name. Example: mytestacc$@OPMANHV.COM

Password: Password of the computer account

Getting Domain DNS Name and NETBIOS Name:
In the Domain Controller device, open Start -> Administrative Tools -> Active Directory Users and Computers.
Getting DNS Server IP:
Open Command Prompt in OpManager server. Run "ipconfig /all". The first IP Address mentioned beside DNS Servers is the primary DNS Server IP Address.

Getting DNS Site:
In Domain Controller device, open Start -> Administrative Tools -> Active Directory Sites and Services. The Site under which your Domain Controller device name listed is your site name. You can leave the DNS Site field empty in Pass-through configuration form in OpManager, if there is only one site present in your Domain Controller.
Design Limitations:

- Pass-through authentication can be enabled for only one domain, preferably the domain in which OpManager server resides. If pass-through has been configured for a domain other than the one in which OpManager server resides, ensure the other domain will provide logged in user information to a website from different domain.
- Pass-through authentication will work only for the active directory users already been added to OpManager. If you do not want to manually create user account for all the users in your domain, enable auto-login for the domain (Admin->User Manager->Windows Domains). Once auto-login is enabled, you have to manually enter username and password of your account only on the first login and an user account in OpManager will be created automatically, from there on you can simply work without manually entering.

Disable Pass-through Authentication:
In OpManager webclient click on Settings(alt+t) > User Management > Pass-through. Uncheck "Enable Pass-through Authentication".

(OR)
Connect OpManager database from command line and run the query “delete from JespaConfiguration” and restart OpManager service.

Log File:
If you face any issue with Pass-through Authentication, contact support with the jespa.log file present under OpManager_Homelogs folder.

Troubleshooting:

Case 1:

jespa.log file ends with line getDomainTrusts: Retrieving list of domains and

stderr*.txt contains java.lang.ClassCastException: java.io.PrintStream cannot be cast to java.lang.String
Solution:
Update the log level for jespa log in OpManagerDB
    • Connect OpManager database
    • Execute the query: `update JespaConfiguration set JESPACONFIG_VALUE='3' where JESPACONFIG_KEY='jespa.log.level'
    • Stop OpManager service
    • Delete the file jespa.log under OpManager_Homelogs
    • Start OpManager service

Case 2:

jespa.log file contains `jcifs.smb.SmbAuthException: Logon failure: unknown user name or bad password`

Cause:
Password configured for computer account is wrong (or) got expired (or) does not comply to password policy of the domain.

Solution:
Reset password for computer account using SetComputerPass.vbs script and update the value in OpManager.
Was this information helpful?
Monitoring CPU, Memory, Disk Using SNMP

The monitors for CPU, Memory, and Disk Utilization are automatically associated for the devices based on the device template definitions. For instance, for Linux servers, the default template has SNMP-based monitors associated. So, all Linux servers will have SNMP-based resource monitors associated. You will see the dial graphs for these three resources in the device snapshot page if SNMP is enabled.

All the Server templates have the monitors defined for various host resources. By default, the CPU, Memory, and Disk Monitors are associated to the servers. The device snapshot page shows the values of these monitored resources with dial-graphs.

If you do not see these monitors associated to the devices, it could be due to any or all of the following reasons:

- These monitors are not present in the device template.
- SNMP is not enabled on the device. In such case, enable SNMP and add the monitors to the device once again.
- Incorrect SNMP credentials are associated. Check the credential details like the SNMP version, community string etc.

Steps to add the monitors to the device again:

1. From the device snapshot page, select the Monitors tab.
2. From the monitor types, select Performance Monitors.
3. You will see the monitors displayed on the right if associated. Click Add Monitors link on the right.
4. From the list of monitors, select the SNMP monitors for CPU, Memory, and Disk Utilization.
5. You can also add other required monitors like Partition monitors etc.
6. The selected monitors are associated to the device and the resources are monitored.

To check if the SNMP agent in the device returns response, try the following:

- Click the Test Monitor icon against any of the associated monitor names. It does a dynamic query to the device for the value of the selected resource, and show the data.
- Incase the agent does not respond, you see a message to this effect. Refer to the troubleshooting tips to resolve the issue.

As an alternative, you can monitor the non-SNMP Linux servers using CLI (telnet or SSH), or the non-SNMP Windows devices using WMI.
Monitoring Resources Using WMI

OpManager monitors the system resources using SNMP by default. However, in the absence of SNMP on the devices, the non-SNMP windows devices can be monitored using WMI. All the Windows device templates have the resource monitors preconfigured. All you will need to do is, disable the SNMP monitors associated and select the WMI monitors and associate them to the required devices.

Prerequisites

For monitoring the Windows environment, OpManager must necessarily be installed on a Windows machine. Besides, the device where OpManager is installed and the monitored remote Windows devices must have WMI, RPC, and DCOM services enabled on them. Authentication to the remote devices using WMI requires you to login as a domain user with administrator privileges. This is a requirement of the WMI protocol. If the device is in a workgroup, the system user name and password should suffice.

Steps to configure WMI Monitoring

Go to the device snapshot page.

1. From Monitors > Performance Monitors section, remove the SNMP-based monitors if any.
2. Click Add Monitor tab.
3. Now, from the list of resource monitors, select the CPU, Memory, and Disk Utilization monitors which has the protocol name as WMI against the monitor name.
4. Click Add Monitors at the top of the page.

The WMI-based monitors are associated to the device.
Monitoring Resources Using CLI

OpManager monitors the system resources using SNMP by default. However, in the absence of SNMP on the devices, the non-SNMP Linux devices can be monitored using CLI, i.e., Telnet or SSH. All the Unix Servers templates have the resource monitors preconfigured. All you will need to do is disable the SNMP monitors associated and select the CLI monitors and associate them to the required devices.

Prerequisites

For monitoring the unix servers, make sure either Telnet or SSH is enabled on them.

Steps to configure Telnet/SSH Monitoring

Go to the device snapshot page.

1. From Monitors --> Performance Monitors section, remove the SNMP-based monitors if any.
2. Click Add Monitor tab.
3. Now, from the list of resource monitors, select the CPU, Memory, and Disk Utilization monitors which has the protocol name as CLI against the monitor name.
4. Click Add Monitors. The monitors are added in the template under the Monitors column.

The CLI-based monitors are associated to the device.
Adding More Monitors

Following are the monitors associated by default for the different device categories:

- **Servers**: CPU, Memory, Disk Utilization
- **Routers**: CPU, Memory, Buffer Hits/Misses, Temperature
- **Switches**: CPU, Memory, BackPlane Utilization
- **Firewalls**: CPU, Memory, and Connection Count.

Similarly, other categories also have few resources monitoring triggered by default. Besides the ones automatically associated, you can monitor more parameters. Here are the steps to configure more monitors:

1. Go to Settings (alt+t) > Configuration > Device Templates.
2. From the list of templates, select the template for the device type to which you want to associate more monitors. Select the corresponding letter to get to the template quickly.
3. In the device template, from the Monitors column, click the Add Monitors button.
4. All the predefined monitors are listed. Select the required monitors from here and click Save.
5. Click Update and the selected monitors are associated to the devices mapped to the Device Template.
Adding Custom Monitors

In addition to OpManager's default monitors, you can also create your own monitors for the SNMP-enabled devices in your network. The SNMP variable for which you intend configuring a monitor can return either a numeric or a string output when queried.

To add a custom monitor for a resource of a particular device type, the device template must be modified. The new monitor should be defined in the device template so that the monitor is associated for all devices of that type. Here are the steps.

1. Go to Settings (alt+t) > Configuration > Device Templates.
2. Click on the template in which you want to add a new monitor.
3. Example > Linux. Scroll down the template and click Add Monitors under Monitors column.
4. Click on the SNMP at the top of this page.
5. Configure the SNMP OID, Monitor Name, Display Name etc and click Save.
6. Click Update.
Adding WMI-based Custom Monitors

In addition to OpManager's default monitors, you can also create your own monitors for the WMI-enabled devices in your network.

1. Go to Device snap-shot page on which you wish to add a custom WMI monitor
2. Click Monitors tab > Performance Monitors > Add WMI Monitor
3. Select the required WMI Class from the dropdown
4. Select the required WMI performance counter and Click Add to add the Monitor
Device-specific Monitors

The monitoring configuration may need alteration for specific devices. Doing a bulk-configuration using the device templates, applies the same set of configurations for the devices of the same type. In order to change the configuration for specific devices, here are the steps:

1. Go to the device snapshot page.
2. Click on Monitors tab > Performance Monitors.
3. Click the Edit icon against the monitor name. The Edit Monitor page is displayed.
4. Change the values for the required parameters and and click Save.

The changes to the monitor are effected only for that device.
Configuring thresholds for monitors

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 Warning, Trouble and Error for breaking the fault into three stages and taking corrective actions accordingly.

- Attention threshold - low severity
- Trouble threshold - medium severity
- Critical threshold - high severity

You can configure multiple thresholds for the monitors that are associated to a single device, configure from the device template in order to apply across multiple devices.

Configure threshold limits for the monitors associated to a single device

1. Go to the device snapshot page.
2. Click Monitors tab > Performance Monitor > click on the edit icon corresponding to the monitor for which you want to configure threshold limits. Edit Monitor page opens.
3. Ensure that the monitoring Interval is configured.
4. Specify the unit for the monitored resource in terms of percentage, MB, KB etc (based on how the parameter is measured).
5. Select the condition [>,=, <, or !=] for Warning Threshold, Trouble Threshold & Error Threshold, and enter the value. Alert is raised if the monitored value is greater than, equal to, not equal to, or lesser than (which ever is selected ) the threshold value.
6. Enter the Rearm Value. Rearm value is the value which the determines the monitor has restored to normal condition. For instance, the Warning threshold condition for a memory monitor is selected as greater than [>] and the threshold value is configured as 75. The monitored memory value of that device is 80. Now alert is raised and the monitor is in violated condition. At the next poll the monitored value is 72. An alert for returning to normal condition is generated. At the next poll again the monitored value goes to 80. Again a threshold violation alert is generated. In order to avoid this, enter the rearm value. Only if the monitored value reaches the rearm value the monitor goes to the normal condition and a normal alert is raised. Note: If you select the threshold conditions greater, then the rearm value should be lesser than the threshold value and vice versa.
7. In the Consecutive Times field enter the value of how many consecutive times the thresholds (Attention, Trouble and Critical) can be violated to generate the alert.
8. Click on OK.

Configure threshold limits for a bulk of devices of same type from their device template page

1. Go to Settings ( alt+t )> Configuration> Device Templates> Select the respective template on which you want to configure the threshold.
2. 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 Threshold button. Edit Thresholds page opens.
3. Configure the Attention Threshold, Trouble Threshold, Critical Threshold and Rearm Value and click on Save.
4. Click on Update.
Viewing Process Diagnostics

You can view the top ten processes utilizing the maximum resources. Process statistics is retrieved using Telnet/SSH/WMI, for which the correct credential must be associated to the devices. To be able to view the diagnostics,

1. Configure relevant CLI and WMI credentials.
2. Click the link on top of the dial graphs for CPU and Memory. The top 10 processes are shown.

You can also end the processes from here.
Monitoring Packet Loss for Devices

You can monitor the packet loss percentage on a per device basis and view even the packet loss reports.

1. Go to the device snapshot page.
2. Look at the Today's Packet Loss value shown on the dial.
3. Click the edit icon to configure threshold value in percentage. If the packet loss percentage exceeds the threshold value, a threshold violation alarm is triggered. This alarm can in turn be notified to email or sms.
4. Click the dial to see the packet loss report, select the time-period according to your need.
Monitoring Response Time of Devices

You can monitor the response time on a per device basis and view even the packet loss reports.

1. Go to the device snapshot page.
2. Look at the Response Time value shown on the dial to know the device response time.
3. Click the edit icon to configure threshold value in milliseconds. If the device response time exceeds the threshold value, a threshold violation alarm is triggered. This alarm can in turn be notified.
4. Click the dial to see the response time report, select the time-period according to your need.
Monitoring TCP Services

OpManager provides out-of-the-box support for the following services: Web, HTTPS, FTP, IMAP, LDAP, Telnet, MySQL, MS-Exchange, SMTP, POP3, WebLogic, Finger, Echo, DNS, and NTTP. By default, during discovery, OpManager scans the devices for the services: DNS, MSSQL, MySQL, Oracle, SMTP, Web. You can also select other services in the list. When they are found running on their default ports, OpManager starts monitoring the services.

Scanning Services during Discovery

By default, OpManager scans each device on the network for the services that are chosen during discovery.

To modify this list, follow the steps given below:

1. Go to Settings (alt+t) > Configuration > Monitors > Services > Select the service and check “Scan during discovery”

OpManager allows you to change the settings for monitoring these services as per your network needs. You can configure new services that are not available in the list. OpManager can manage services running on standard TCP ports.

Note:

- The list contains the service names and the corresponding port numbers. To edit the settings of any of the available services, click on the service name.
- If you do not find the service you want to manage in the list, you can add the service by clicking Add Service Adding a New Service.

Viewing Service Status and Response Time

1. Go to the device snapshot page > Monitors > Service Monitor > you will see the list of services managed in the device, if any, with their status and current response time.
   - Click the service name to view the historical report on the response time and the availability chart of the service.

Configuring Alerts

By default OpManager raises an alarm if a service is down. If required you can configure OpManager to raise an alarm if the service unavailable for a N number of times consecutively.

1. Go to the device snapshot page > Monitors > Service Monitors > Click the edit icon against the service on which you wish to configure the threshold or to modify the consecutive time.
Monitoring TCP Services on a Device

To select the services to be monitored in a device, follow the steps given below:

1. Go to Inventory > Click on the Device for which you wish to add a service.
2. Click Monitors > Service Monitors > Add Monitor at the top of the page
3. Select the services to be discovered from the list and click Add Monitor.
Adding New TCP Service Monitors

You can add new TCP services for monitoring.

1. Go to Settings (alt+t) > Configuration > Monitors > Services > Click Add Service
2. Specify the name of the TCP service that you want to monitor.
3. Specify the TCP Port number that has to be checked for service availability
4. Specify the timeout interval in seconds for the port-check request.
5. Specify the consecutive time to generate an alarm if the service unavailable for N number of times.

Associating the Service to Devices

To associate a service to a server,

1. Go to Settings (alt+t) > Configuration > Monitors > Services > Associate
2. Select the required TCP service from the dropdown.
3. Select the devices on which you want to monitor the service from the column on the left and move them to the right.
4. Click Save.
Monitoring Windows Services

Certain applications in Windows machine run in the background as services. OpManager discovers and monitors the status of such services using WMI. OpManager generates alarms whenever they fail.

Prerequisites

To monitor Windows services, OpManager should be installed in a Windows machine. OpManager uses WMI to monitor the Windows services and hence you need to provide the log on details of a user with administrative privilege to connect to the device. So, make sure you configure a WMI credential so that you can apply this to the windows devices.

Add Windows Services to a Device

To monitor a Windows service, follow the steps given below:

1. Go to Inventory> Click on the device for which you wish to add a windows service.
2. Confirm if the correct WMI credential is associated to the device. Else, configure the password details in the device.
3. Click Monitors> Windows Service Monitors. This option will be available only for Windows servers.
4. Click Add Monitor > Select the services to be monitored in the device and click Save.

Associate Windows Service Monitors to several devices

1. Go to Inventory >Click on the device for which you wish to associate windows service.
2. Click Monitors> Windows Service Monitors> Click Associate at the top of the page.
3. Select the service you wish to associate and click Add Monitors. The selected service monitor is added to the device.

Configuring Alerts

By default OpManager raises an alarm if a Windows service is down. If required you can configure OpManager to raise an alarm if the service unavailable for a N number of times consecutively.

1. Go to the device snapshot page.
2. Monitors> Windows Service Monitors, click on the edit icon corresponding to the Windows service for which you want to configure the alert.
3. Modify the count entered for 'Generate alarm if unavailable for _ consecutive times'. For example if you enter the value as 2, OpManager will raise alarm only if the service is unavailable for 2 consecutive polls.
4. You also have to option to either restart the service or restart the server if the service goes down. Select the check box and appropriate radio button.
5. Click the Save button.
Adding New Windows Service Monitors

In addition to the Windows services monitor supported by OpManager out-of-the-box, you can add monitors for other windows services too.

To add a new Windows service monitor, follow the steps given below:

2. Click Add New > Select the device from the drop-down.
3. Type the domain administrator user name password for the device in the respective fields and click Next.
4. A list of all the Windows Services available on that machine is displayed. From this select the services that you want monitored on the device.
5. Configure the consecutive time for alert.
6. Based on whether or not you want to restart the service or the machine when the service goes down, select the corresponding option.
7. Click Save.
OpManager provides out-of-the-box support for monitoring the availability of all the processes running on a Windows or Unix system. Windows systems use WMI and Unix systems use CLI to monitor the processes that are running on the system.

Here are the steps for configuring Process Monitors:

1. Go to the device snapshot page.
2. Make sure you have associated the WMI/CLI Credentials to the device.
3. Click Monitors tab > Process Monitors.
4. Click Add Monitors > select the required Process Monitors and Click Add Monitors at the top of the page to get these monitors associated to the device.

**Configure Thresholds for Process Monitors**

You can set resource thresholds for the Process Monitors. Once a resource (cpu/memory) utilization by a process exceeds the configured threshold, an alert is triggered.

1. Click the Edit icon against the process name.
2. Configure the threshold values for CPU and Memory resources.
3. Configure the number of times you would like to allow threshold violation before being notified. For instance, if you configure the value as 3, OpManager notifies you if the resource threshold is violated 3 consecutive times.
4. Configure the number of the process instances, exceeding which you would like to be notified. For instance, if you would like to be notified if the number of Apache.exe instances on the monitored device exceeds 3, configure the value here as 3 and save the changes.

Alerts are fired based on the above settings.

You can also view active processes on a device and also view the process diagnostics against a system resource.
Viewing Active Processes

OpManager provides you the information on the processes that are currently running on the managed device. You need to have SNMP agent running in the device to view this information.

To view the details, click the device from Inventory and you will see the Active Process widget from the Device snapshot page.
Adding New Process Template

Process templates helps you to select the processes that are running on a device, convert each of them into individual templates and apply all of them across multiple devices. To add a new process template,

1. Go to **Settings (alt+t)** > Configuration > Monitors > Processes > Add New.
2. **Device Name**: Select the device which runs the process(es) that needs to be converted into template(s).
3. **Protocol**: Select the relevant protocol to access the device.
4. Select the relevant credential from the drop-down by clicking on the **Credential** radio button or Click **Associated username password** to associate the associated credential.
5. Click **Next**. All the processes that are currently running on the device are listed along with their ID, Path and Arguments.
6. Select the required process(es).
7. Click **Add** button at the bottom of the page.

The selected processes are now added and available as templates under Settings > Configuration > Monitors > Processes.
Associating Process Template to Multiple Devices

To associate a process template across multiple devices, follow the steps given below:

1. Go to Settings (alt+t) > Monitors > Processes
2. Click Associate.
3. Select the process template to be associated to multiple devices
4. From the listed devices, select and move the required devices to box seen on the right.
5. Click Save.

The selected process template is applied across multiple devices.
Creating Script Monitoring Templates

Script Monitoring templates help you create custom scripts to monitor custom parameters.

Follow the steps given below to add script templates:

Enter the command to run the script, as if provided in command prompt:

Example:
```
cscript ${FileName}.vbs
```

Note that ${FileName} must be followed by script file extension. You may also pass arguments. Argument list may use variable ${DeviceName} which will be replaced with the monitored machine name in run time. Other supported variables are ${UserName} - WMI/CLI username, ${Password} - WMI/CLI password, ${SNMPRead} - SNMP read community string. For example,
```
cscript ${FileName}.vbs ${DeviceName} ${UserName} ${Password}
```

Script Output Format:
In order to store the result of the script in DB, the output must be in the format given below.

- **Message:** This message will be used as alarm message.
- **Data:**
  - Instance1  value1
  - Instance2  value2
  - ...
  - InstanceN  valueN

Exit code will be used to set the status of the script monitor. Exit code "0" for up, any other exit code for down. Only numeric values are allowed as statistical data. The instance name and value must be separated by a TAB space(t). Status checking scripts may NOT contain data part. If there is no message in output, a default message will be used for alarm message.

Add New and provide a name and description for the template.  
Monitoring Interval.  
Unit for the monitored parameter.

Enter complete content of script file.  
Enter the time to wait for script execution completion.  
Select the machine from which you want to execute the script. Linux scripts can be executed either from the server, where OpManager is running, or from the monitored machine.  
Provide the directory path from which you want to execute the script. You may use variables ${TempDir} or ${UserHomeDir} which means OpManager temporary directory and user's system home directory respectively.  
Configure threshold for the script monitor if any.  
Save button to save the template.

You have successfully created a script monitoring template.

Editing Script Templates

To Edit a script template:

1. Click on **Edit** icon corresponding to the script template that you want to edit.
2. Carry out the necessary modifications and **Save** it.

Importing/Exporting Script Templates

The import/export options allows you to share scripts that are created by you with OpManager community and use the scripts shared by others.

Use **this form** to share the script with OpManager community.

**Import scripts**

1. Click on **Import** button that is available in the Script Templates page.
2. Click on **Browse** button to locate the script (.xml file).
3. Click **Import**.
The script has been successfully imported to OpManager.

**Export Scripts**

1. Click on **Export XML** icon corresponding to the script that you want to export.
2. Click on **Save** to save the script.

**Copying Scripts**

OpManager allows you to save a copy of the script, modify it and use it for other monitoring requirements.

1. Click on **Copy As** icon that is available in the Script Templates page. The script template opens.
2. Carry out the necessary modifications and **Save** it.

**Deleting Scripts**

To delete a script, click on the **Delete** icon corresponding the script template.
Associating Script Monitoring Templates

Script Monitoring templates help you create custom scripts to monitor custom parameters.

Follow the steps given below to add script templates:

1. Go to Settings (alt+t) > Configuration > Monitors > Scripts.
2. Click **Associate**
3. This will open a page to associate multiple devices to a specific template.
4. Select the required script from the drop-down.
5. Select the devices from left-side box and move it to the right box.
6. Click **Save**

You have successfully associated script template to multiple devices.
Log File Monitoring

Every application prints status messages, error messages, and other critical information in its log. It is very tedious to skim through all these bulky log files for understanding the application performance. To manage such mission critical applications in real time, monitoring their log files is necessary. OpManager offers agent-based log file monitoring for real-time fault and performance management.

How log file monitoring works?

The log file monitoring agent installed in the end machine, monitors the log files continuously for the required string (It may even be a regex). Once that string is printed, it immediately notifies OpManager server, which in-turn raises the alarm.

Steps to download agent for log file monitoring

Prerequisite: Before installing the agent, add that device in OpManager.

1. Install the agent in the end machine which has the log files.
2. Go to Settings (alt+t )> Configuration> Monitors> Agents> Download Agent.

Known Issues :

1. If the file monitoring interval is modified, the match string appeared in the current polling span (old monitoring interval) will be ignored and hence the alert will not be generated. The alert will be raised as usual based on the new monitoring interval from next poll.

Example:

Consider the file monitoring interval is 5 mins starting at 10.00 AM.

Search string appears in the monitored log file at 10.02 AM.
File monitoring interval is modified as 10 mins at 10.03 AM.

In above case, the agent will ignore the search string which appeared at 10.02 AM. It starts monitoring the log file as fresh from 10.03 AM based on the new monitoring interval (10 mins).
Adding File Monitoring Template

You can now track changes on critical system and user files and be notified if a specific change occurs. For instance, you might want to be notified if the file size increases beyond a defined limit, if some files are missing, log prints etc. Configure meaningful templates in OpManager and apply them to devices on which you want the files monitored. Using the following file monitoring features you can monitor the following parameters:

**File Content:** Presence of a word/string or in a log file, supports regex as well

**File size:** Watch for an increase or decrease in the file size

**Presence of a file:** Check the availability of a file in the specified directory (may have been moved, renamed, or deleted)

**File age:** Keep track of the age of a file and take actions based on the age

**File modification:** Be notified if a file has been modified

Steps to configure a file monitoring template

1. Go to Settings (alt+t) > Configuration > Monitors > Files
2. Click **New Template**. Add New Template page opens.
3. **Template Name:** Configure a name for the template.
4. **File Path:** Specify the path in which OpManager should locate the file.
5. **Polling Interval:** Configure the interval at which OpManager should monitor the file.
6. **Description:** Provide a brief, meaningful description for the template and click **Save**.

Configuring Alerts for File Monitors

Configure the monitoring criteria based on which you want to be notified:

1. **File Contains:** To monitor the print of a word/string in a log file, you have to install log file monitoring agent in the end server where the application is running. Click on Agent link to download and install the agent. Once you install the agent, it looks for the specified string in the said log file. If the word/string is printed in the log file, OpManager raises alert. If required, you can configure the agent to match the case when searching for the word/string. The notification can be triggered if the alert condition is met the specified number of times.

2. **File Existence:** OpManager looks for the file in the specified path and alerts based on the conditions specified. You can configure to be notified if the file does not exist in the path specified, or be notified if the file exists, or you can choose not to monitor. Also, choose the severity that you would like to assign to this alert. The notification can be triggered if the alert condition is met the specified number of times. That is, OpManager alerts you if a particular file does not exist in a path during two consecutive polls.

3. **File Size:** Configure OpManager to alert you if the file size goes over, or comes below a specified size. Select the relevant threshold for alerting. You can configure the size in terms of bytes, KB, MB, or GB. Choose the severity that you would like to assign to this alert. The alert can be triggered if the threshold is violated a specified number of times.
4. **File Age:** Similarly, you can configure OpManager to alert you based on the age of the file. For instance, you can be notified if a file is over 20 days old.

5. **File Modification:** When a file is modified, the date on which the file is modified is updated. You can configure OpManager to notify you whenever there is a change in the date modified. This option helps you keep track of any changes done in critical files. Choose the severity that you would like to assign to this alert.

**Associating the File monitor to devices**

Having creating a template with the alert criteria, you can now associate the template to the devices.

1. Go to Settings (alt+t) > Configuration > Monitors > Files
2. Click **Associate**
3. Select the required Template from the drop-down
4. Select the devices for which you want to apply this template and move them to the right.
5. Click **Save** button at the bottom of the column to associate the template to all the selected devices.

The monitor is added to the device and OpManager alerts based on the alert conditions configured.

**Prerequisite:**
- Ensure that device in which in you are installing the agent has already been added in OpManager.
- Click on the **Download Agent** link to download the agent.
- Install it on the machine which has the log file. Double-click the exe to begin the installation.
Adding Folder Monitoring Template

Besides monitoring files on the systems, you can also monitor the folders. You can track changes in folders based on the folder size, the number of files in a folder etc. Again, like file monitors, you can be notified if a specific change occurs. For instance, you might want to be notified if the folder size increases beyond a defined limit, if some files in a folder are missing etc. Configure meaningful templates in OpManager and apply them to devices on which you want the folders monitored. Monitor the following parameters on folders:

- Folder size: Watch for an increase or decrease in the file size
- Existence of a file: Check the availability of a file in the specified directory (may have been moved, renamed, or deleted)
- Folder Modification: Keep track of changes (add/remove/rename) on the files or sub-folders within a folder. However, sub-folder level changes are not monitored.
- File Name: Watch files in a folder by their name.
- File Size/Age: Check the last modified file or all files in a folder for file size and age.
- File count: Keep track of the number of files within a folder.

Steps to configure a file monitoring template

1. Go to Settings (alt+t) > Configuration > Monitors > Folders
3. Template Name: Configure a name for the template.
4. Folder Path: Specify the path in which OpManager should locate the file. You can either provide the local directory (C:) or UNC share path (servernameSharedDirectory).
5. Polling Interval: Configure the interval at which OpManager should monitor the file.
6. Description: Provide a brief, meaningful description for the template and click OK.

Configuring Thresholds for Folder Monitors

Configure the monitoring criteria for Folder/File monitoring conditions based on which you want to be notified:

1. Folder Existence: OpManager looks for the folder in the specified path and alerts based on the conditions specified. You can configure to be notified if the folder does not exist in the path specified, or be notified if the folder exists, or you can choose not to monitor.
2. Folder Size: Configure OpManager to alert you if the folder size goes over, or comes below a specified size. Select the relevant threshold for alerting. You can configure the size in terms of bytes, KB, MB, or GB. Configure the rearm accordingly to reset the alarm.
3. Folder Modification: Select Alert if modified check box to receive alerts when files/sub-folders are added/deleted/renamed in the specified folder.
4. File Filter: By default all the files in the specified folder are monitored. Deselect All files check box and enter the file name or extension (*.pdf,*.txt) of the files alone you want to monitor. You can enter multiple values separated by comma, but no blank space is allowed. You can enter the filename in the following formats:
   - Full file name with extension ‘stdout.doc, stdlog.txt’
   - File name with wild characters ‘*out’ or ‘std*’. Files containing the same prefix or suffix name with same/different extension will be monitored
   - File name in date format ‘2011062200001.txt’. Enter the file name in a static format $YYYY$MM$DD$.txt or $YYYY$DD$MM*.txt
5. File Name Contains: OpManager looks for the files in the specified folder and alerts based on the conditions specified. You can configure to be notified if the folder does not contain any file in the specified name, or be notified if the folder contains files in the specified name, or you can choose not to monitor.
6. File Size/Age: OpManager looks either last modified file or all files for file size and age. If the threshold condition for either file size or file age is violated, an alarm is raised. Configure the relevant threshold and rearm conditions.
7. **File Count:** You can monitor the number of files specified in the File Filter and be alerted if the count changes, or if it violates a count threshold. Configure the rearm accordingly to reset the alarm.

---

### Configuring Alerts for Folder Monitors

Configure the following alerting options:

1. **Severity:** Choose the severity that you would like to assign to this alert.
2. **Consecutive Times:** Specify how many times the threshold can be violated to generate the alert.
3. **Alarm Message Format:** Configure the alarm message. You can include the alarm variables by appending $ to the variable name.

---

### Associating the Folder monitor to devices

Having creating a template with the alert criteria, you can now associate the template to the devices.

1. Go to Settings (alt+t) > Configuration > Monitors > Folders
2. Click Associate
3. Select the required Template from the drop-down
4. Select the devices for which you want to apply this template and move them to the right.
5. Click on **Save** button at the bottom of the column to associate the template to all the selected devices.

The monitor is added to the device and OpManager alerts based on the alert conditions configured.
Active Directory Monitoring

Active directory monitoring feature takes OpManager a step further in proactive monitoring of Windows environment. The system resources of the Domain Controllers where the Active Directory (AD) database resides, and few critical Active Directory Services are monitored in OpManager.

To make AD monitoring more simple and easily accessible, The Domain Controllers are classified under a separate category under Infrastructure Views. The categorization of the device as a Domain Controller is done automatically if SNMP is enabled. The system resources of the device and the AD services are monitored using WMI.

The snapshot page of the Domain Controller shows a dial graph for AD Store in addition to the dial graphs for CPU, Memory, and Disk Utilization.

The other utilization data displayed in the snapshot page for the Domain Controller are:

- Resource Utilization by LSASS (Local Security Authority Subsystem Service)
- Resource Utilization by NTFRS (NT File Replication Service)
- Ad Store Utilization
- Performance Counters showing information such as the AD Reads, the AD Replication objects etc

Besides these, following are the AD Services monitors associated by default:

- **Windows Time service**: The service synchronizes the time between domain controllers, which prevents time skews from occurring.
- **DNS Client Service**: This service resolves and caches (Domain Name Server) DNS names.
- **File Replication Service**: This service maintains file synchronization of file directory contents among multiple servers.
- **Intersite Messaging Service**: This service is used for mail-based replication between sites. Active Directory includes support for replication between sites by using SMTP over IP transport.
- **Kerberos Key Distribution Center Service**: This service enables users to log on to the network using the Kerberos version 5 authentication protocol.
- **Security Accounts Manager Service**: This service signals other services that the Security Accounts Manager subsystem is ready to accept requests.
- **Server Service**: This service enables the computer to connect to other computers on the network based on the SMB protocol.
- **Workstation Service**: This service provides network connections and communications.
- **Remote Procedure Call (RPC) Service**: This service provides the name services for RPC clients.
- **Net Logon Service**: This service supports pass-through authentication of account logon events for computers in a domain.

You can add more AD Monitors to be monitored by clicking the Add Monitor button.
Exchange Server Monitoring

You can monitor critical MSExchange (2000/2003/2010) Services and parameters using OpManager. Monitoring is done using WMI. Thresholds are pre-configured for critical services. You can also modify or enable thresholds for other services and parameters.

The services monitored are:

- Information Store
- Site Replication Store
- MTA Stacks
- Exchange Management
- SMTP
- POP3
- IMAP4
- System Attendant
- Routing Engine
- Event Service

The Exchange parameters that are monitored can be classified under the following categories:

- Address List Monitors
- POP3 and IMAP Monitors
- Information Store Public Folder Monitors
- Event Service Monitors
- SMTP Monitors
- Information Store Mailbox Monitors
- Message Transfer Agent Monitors
- Directory Service Monitors
- Information Store Monitors

Configuring Exchange Parameters and Services Monitoring

1. Go to the snapshot page of a device that has Exchange running.
2. Click Monitors tab> Performance Monitors> Add Exchange Monitor
3. Select the Exchange Server version. The monitors of all the Exchange parameters and services are displayed.
4. From this list, select the required Monitors and Click Add to associate it to the Server.

These monitors are associated to the device. Ensure to associate the correct WMI credential to the device. OpManager uses these credentials to connect to the device using WMI.
Monitoring MSSQL Parameters

MSSQL Services and Parameters can be monitored using WMI. OpManager detects the SQL servers by itself and MSSQL related resource metrics are added automatically.

Here are the steps to manually associate the MSSQL monitors to a device:

1. Go to the snapshot page of a device that has MSSQL running.
2. Click on Monitors tab> Performance Monitors> Add MSSQL Monitor
3. The monitors of all the MSSQL parameters are displayed.
4. From this list, select the required MSSQL Monitors and click Add to associate it to the Server.

These monitors are associated to the device. Ensure to associate the correct WMI credential to the device. OpManager uses these credentials to connect to the device using WMI.
Monitoring Windows Event Logs

The Event Log is a Windows service that logs about program, security, and system events occurring in Windows devices. The events can be related to some application, system or security. You can monitor these events using OpManager and configure to generate alarms when critical events are logged. OpManager uses WMI to fetch the details of these logs and hence you need to provide the log on details of a user with administrative privilege to connect to the Windows machine.

You can view the list of all events monitored by OpManager, Go to Settings(alt+t)> Configuration> Monitors> Event Logs

- Monitoring Windows Events in a Device
- Creating an Event Log Monitor
- Monitoring Custom Event Logs

Monitoring Windows Events in a Device

To monitor Windows events, you need to associate the event log monitors with the device. To do so, follow the steps given below:
1. Go to the device snapshot page.
2. Click Monitors tab> EventLog Monitors> Add Monitor.
3. Select the event logs to be monitored in the device.
4. Click Associate to add the selected monitors to the device.

Creating an Event Log Monitor

To create an event log monitor, follow the steps given below:
1. Go to Settings(alt+t)> Configuration> Monitors> Event Logs
   In this page, you can see the rules supported by OpManager. They are categorized into Applications, Security, System, DNS Server, File Replication Service, and Directory Service. You can add the event logs that you want to monitor under any of these categories.
2. Click Add New Rule under any one of the categories to add a rule.
   Entries to all the fields except Rule Name are optional. Event ID is a required field to identify the event but can be left empty in few exceptional cases, such as you want to monitor all events that are of the Event Types, say, error or information. Here the filter will be based on the Event Type.
   1. Select the Log File Name.
   2. Type a unique Rule Name.
   3. Enter the Event ID to be monitored. This is the unique identifier for the event logs.
   4. Enter the event Source. This is the name of the software that logs the event.
5. Enter the event **Category**. Each event source defines its own categories such as data write error, date read error and so on and will fall under one of these categories.

6. Type the **User** name to filter the event log based on the user who has logged on when the event occurred.

7. Choose the **Event Types** to filter the event logs based on its type. This will typically be one among Error, Warning, Information, Security audit success and Security audit failure.

8. **Description Match Text**: Enter the string to be compared with the log message. This will filter the events that contains this string in the log message.

9. **Generate Alarm if event is raised**: By default OpManager raises an alarm if the event occurs. However, you can configure the no. of consecutive times the event can occur within the specified no. of seconds, to raise an alarm.

10. Choose a **severity** for the alarm generated in OpManager for this event.

3. Click **OK** to save the event log rule.

### Monitoring Custom Event Logs

You can monitor event logs under a custom category too. Some applications log the events in a new category other than the default System/Applications/Security category. You can now configure rules in OpManager to parse the events in such custom categories and trigger corresponding alerts in OpManager. Here are the steps:

1. Go to Settings( alt+t )> Configuration> Monitors> Event Logs>
2. Click **Add Custom Event log**
3. Select a device from the drop-down on which you can query for the event categories.
4. Provide the WMI details **User Name** and **Password** of the device.
5. **List logs that were created in last** Configure the time to list the logs and Click **Query Device**
6. The custom logs in the selected device are listed. Select a log from **Discovered Log Files** and click **OK**

You can now associate the rules (default or custom event logs) to the required devices.
Monitoring URLs for Availability

You can configure OpManager to monitor your Web sites. Many business enterprises require continuous monitoring of their Web sites, as the failure of these sites might have an impact on the business.

You can monitor global URLs, such as www.yahoo.com and www.manageengine.com.com or URLs in a server, such as http://192.168.4.11/index.html, http://web and so on.

You can perform a content match on these URLs and confirm their availability. Further, for pages that require a form submit, such as user name and password, you can provide these details and verify the availability of the next page.

Note: If a proxy server is configured in your network, make sure to provide its details in the Proxy Server Settings page of OpManager. Refer to Configuring Proxy Server Settings for steps to do this. This is required for monitoring any URL in a proxy-enabled LAN.

Configuring a global URL monitor

To configure a global URL monitor, follow the steps given below:

1. Go to Settings (alt+t )> Configuration> Monitors> URLs
2. Click Add New
3. Enter a name to the URL monitor in the URL Monitor name field.
4. Type the URL address to be monitored.
5. Type the Monitoring Interval and the value of Timeout in the respective fields.
6. Generate Alarm if Unavailable for: Enter the number of times the URL can go down consecutively before raising an alert.
7. Match Content: Type the string (max. 250 characters) to be compared with the contents of the monitored Web page in the Match Content field. Click on the Check Now button to instantly verify the correctness of the given details.
8. Select between Get and Post, the methods for any HTTP/HTTPS-based URLs. This is required because certain URLs cannot be accessed using a Get request.
9. Type the request parameters and their values in the form <parameter name>=<value>, if any, to know the actual availability of the URL. Note that you can enter only one parameter in a line.
10. Configure the user name and password for authorization. This will be required in the pages where you need to log-on and test the availability of the host.
11. Select the required notification profile type and click Add button to associate it with this monitor.
12. Click **Add Monitor** to add the URL monitor.

**Viewing URL Response Time and Availability**

You can get the details about the URL response time and availability in the URL snapshot page.

To view the URL snapshot, click the URL link from **Settings (alt+t) > Configuration > Monitors > URLs**. Then click the URL whose snapshot you want to view.

Click the **Availability chart** to view the availability history and the URL downtime/uptime chart.
Associating URL Monitors to Servers

You can add URL monitors to Servers/Domain Controllers to check the availability of the URL from those servers.

1. Go to the device snapshot page.
2. Click Monitors tab > URL Monitors.
3. Click **Add Monitor**
4. Configure all the values for the URL Monitor and Click **Add Monitor**.

The configured URL is monitored for availability from that Server. You can configure to receive an e-mail or SMS when the URL monitored in a server goes down. For this, you need to create a notification profile for the 'URL is down' criteria and associate it to the server.
Adding Syslog Rules

Syslog is a client/server protocol that sends event notification messages to the syslog receiver. These event notification messages (usually called as syslog messages) help in identifying the authorized and unauthorized activities like installing software, accessing files, illegal logins etc. that take place in the network. In OpManager Syslog rules helps in notifying you if some particular syslog messages such as kernel messages, system daemons, user level messages etc. are sent by the devices.

Apart from the pre-defined syslog rules you can also add any number of syslog rules. Here are the steps to add a syslog rule:

1. Go to Settings (alt+t) > Configuration > Monitors > Syslogs.
2. Click on Add Syslog Rules. Add Syslog Rules page opens.
3. Enter a unique Rule Name.
4. Enter a brief Description about the rule.
5. Select a Facility. Facility refers to the application or the OS that generates the syslog message. By default "Any" is selected.
6. Select the required Severity.
7. Match Text: Enter the text that needs to be verified for matching. Note: Regex is supported for this field.
8. Select the Alarm Severity.
9. Enter the Alarm Message.
10. Click the Advanced button to configure advanced (threshold) rules. This is optional.

   1. Number of Occurrences: Enter the count of the number of consecutive times OpManager can receive syslog message from a device before raising an alert.
   2. Time Interval (seconds): Enter the time interval that should be considered for calculating the number of occurrences.

To clear or rearm the event:
3. Select the Facility Name.
4. Select the Severity.
5. Enter the Matching Text.
6. Click OK.
Configuring Syslog Ports

OpManager receives the syslog packets via the default syslog port 514. However, if required you can configure additional ports in OpManager to receive the syslog packets. To configure additional ports, follow the steps given below:

1. Go to Settings( alt+t ) > Configuration > Monitors > Syslogs
2. Click on the Syslog Port.
3. Enter the port number(s) separated by a comma.
4. Click OK.
Viewing Syslog Flow Rate

To view the flow rate of the syslog packets,

1. Go to Settings (alt+t) > Configuration > Monitors > Syslogs.
2. Click on the **Flow Rate**.

The flow rate of the Syslog packets are displayed.
Hardware Health Monitoring

Monitor the hardware health of key device parameters such as temperate, voltage, power, fan speed, status of processors, disk arrays, etc. of VMware, HP, Dell and Cisco systems and get alerted if they violate pre-defined thresholds.

Collecting Hardware Health Data

OpManager uses SNMP to monitor and collect the hardware health status of servers, routers & switches. In-case of VMware, the vSphere API is used to collect sensor data.

The hardware health monitors are associated automatically whenever you add a device with proper SNMP credential. If you encounter any problem associating the hardware health monitors, then check for the correct SNMP credentials or contact our support team.

Reporting of Hardware Health:

OpManager provides historical reports on the status of hardware health which can be scheduled based on user needs.
Create New Dashboard

Customizing Dashboard feature in OpManager helps you to create your own dashboard and view the desired performance metrics, reports etc at-a-glance. To create a New Dashboard follow the steps given below:

1. Click Dashboard> New Dashboard. Create New Dashboard page opens [screen shot given below].

- **Name**: Enter a unique name for the dashboard.
- **Description**: Brief description about the dashboard.
- **No. of Columns**: Select the number of columns that you want to have in the dashboard. By default the number of columns is 2.
- **Column Width**: Column 1, Column 2, Column 3 & Column 4: Enter the width of the columns in terms of percentage.
- **Widget List**: Select the Widgets that are to be displayed on the dashboard.
- Click **Create** button.

A new dashboard is created and listed on the left pane of the Dashboard home page.
Adding New Widgets

To add a new widget to a dashboard follow the steps given below:

1. Go to Dashboard and click on name of the Dashboard to which you want add widgets.
2. Click on Add Widgets seen at the top right of the page
3. Select the Widget(s) that you want add to the dashboard.
4. Click Add button to add the selected widget(s) to the dashboard.

Editing Widgets

To modify the existing widgets go through the steps given below:

1. Click on the Edit against the widget on which you wish to modify the fields
2. Modify the required fields.
3. Click Save to effect the changes.

Moving Widgets

OpManager allows you to move the widgets to different locations within the dashboard. To move a particular widget to a different location, click on the widget name (without releasing the click) and drag the widget to the required location.
The widget is now moved to the new location. The widget that is near the old location occupies the old location automatically.

**Embedding Widgets**

Embed widgets as iframes in your website and access it without logging into OpManager. To get the iframe snippet code:

1. Click on **Embed** icon available next to delete icon on the widget box.
2. Copy the iframe snippet code and paste it on the required html page.

**Deleting Widgets**

To delete a widget go through the steps given below:

1. Click on **Delete** icon available on the widget box. A confirmation window pops up.
2. Click **OK** to confirm deleting.
Editing Dashboard Layout

To modify the existing dashboard layout follow the steps given below:

1. Go to Dashboard page and select the Dashboard whose layout has to be changed.
2. Click on the Edit Layout icon available at the top of the page.
3. Name: Name of the dashboard cannot be modified.
4. Description: Brief description about the dashboard.
5. No. of Columns: Select the number of columns that you want to have in the dashboard. By default the number of columns is 2.
6. Column 1, Column 2, Column 3 & Column 4: Enter the width of the columns in terms of percentage.
7. Click Save to effect the changes on the dashboard.
Delete Dashboard

To delete a dashboard follow the steps given below:

1. Go to Dashboard page and click on the name of the Dashboard that you want to delete. That particular dashboard opens.
2. Now click Delete button available at the top of the page. A confirmation window pops-up.
3. Click OK to confirm deleting.

Note: Default dashboard cannot be deleted for ex, Network Overview, Overview, Top 10, Network Top 10 and Server Top 10.
Adding New CCTV

CCTV helps you view only the required dashboards repeatedly at required intervals. To add a new CCTV follow the steps given below:

1. Go to Dashboard page and click CCTV Views.
2. Click Add CCTV. Create CCTV page opens.
3. CCTV Name: Enter a unique CCTV name.
4. Refresh Interval: Select the interval required to switch over to the next dashboard.
5. Description: Enter a brief description about this CCTV.
6. Select the desired dashboards that you want to include in this CCTV.
7. Click Save.

A new CCTV has been added.

Viewing CCTV

To view a CCTV, Go to Dashboard page> CCTV Views> Click on the name of the CCTV that you want to view. That particular CCTV opens in a new window.

Editing a CCTV

To edit a CCTV follow the steps given below:

1. Go to Dashboard> CCTV Views> Click on the edit icon against the CCTV name that you want to edit.
2. Make the necessary changes.
3. Click Save to effect the changes.
Client Settings

Changing the Background Image

- To change the Background Image> Go to Settings(alt+t)> Client Settings> **Background Image**.
- You can either select the available image or browse and upload your own image.

Changing Login Background Image

- To change the Login Background> Go to Settings(alt+t)> Client Settings> **Login Background**.
- You can either select the available image or browse and upload your own image.

Changing Theme

- To change the Login Background> Go to Settings(alt+t)> Client Settings> **Themes**.
- Select the required theme.

Changing Password

- To change the Login Background> Go to Settings(alt+t)> Client Settings> **Change Password**
- Provide the **Current Password**
- Provide the **New Password**
- Click **Ok**

Changing Language

OpManager is available in English, Spanish, Chinese Simplified, Japanese, French, German, Korean and Italian languages. The following are the steps to change OpManager from one language to other supported language.

- To change the Login Background> Go to Settings(alt+t)> Client Settings> **Language Selector**
- Select your preferred language
Keyboard Shortcuts for Quick Navigation

Tab Navigation

<table>
<thead>
<tr>
<th>Shortcut</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alt h</td>
<td>Home</td>
</tr>
<tr>
<td>Alt n</td>
<td>Network</td>
</tr>
<tr>
<td>Alt s</td>
<td>Servers</td>
</tr>
<tr>
<td>Alt t</td>
<td>Settings</td>
</tr>
<tr>
<td>Alt a</td>
<td>Alarms</td>
</tr>
<tr>
<td>Alt m</td>
<td>Maps</td>
</tr>
<tr>
<td>Alt w</td>
<td>Workflows</td>
</tr>
<tr>
<td>Alt v</td>
<td>Virtual</td>
</tr>
<tr>
<td>Alt i</td>
<td>Inventory</td>
</tr>
<tr>
<td>Alt r</td>
<td>Reports</td>
</tr>
</tbody>
</table>

Device

<table>
<thead>
<tr>
<th>Shortcut</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;</td>
<td>Navigate to next device</td>
</tr>
<tr>
<td>&lt;</td>
<td>Navigate to prev device</td>
</tr>
<tr>
<td>Alt Shift p</td>
<td>Ping Device</td>
</tr>
<tr>
<td>Alt Shift t</td>
<td>Trace Route</td>
</tr>
</tbody>
</table>

Alarms
Workflow

OpManager’s IT automation workflows are code-free and out-of-the-box offers predefined checks and actions. It includes an agile and flexible drag-n-drop workflow builder. Workflow helps you:

- Initiate IT workflow on network faults or on a routine basis
- Manage Services, Processes, Files and Folders of Windows servers and desktops
- Record the IT workflow procedures as an XML and ensure structured practices across IT

OpManager also offers log reports of executed workflows for future analysis.

Checks and actions available in Workflow

Click here to know the conditions and actions available in Workflow.
Adding a Workflow

To add a workflow, follow the steps given below:

1. Click on **Workflows** on the left pane and select **New Workflow**.
2. Drag and drop the required conditions and actions from the left panel to editor panel.

1. Enter a **Name** for the condition and actions.
2. To edit or delete a condition or action, click on it and select edit or delete icon.
3. Click **Next** at the top of the page.

4. Enter a **Name**, **Description**, and **Tags** for the workflow.

5. Associate the workflow to the devices.
   1. Click on 'Click here to specify devices' link corresponding to Devices tab.
   2. Select the devices in Available Devices column and move to Selected devices column. Use the search box to search the devices.

6. Schedule the workflow execution. This is not required if you want this workflow to be triggered when an alarm is raised (point 7).
   1. Click on 'Click here to specify workflow schedule' link corresponding to Schedule tab.
   2. Configure the date and time.

7. Configure the alarm trigger to trigger a workflow when an alarm is raised. This is not required if you want to schedule this workflow for periodical execution (point 6).
   1. Click on 'Click here to specify alarm trigger' link corresponding to Alarm Trigger tab.
   2. Select the required criteria. Executes this workflow on the associated devices, if any of the criteria is satisfied.
   3. Define Time: Select either **Apply this profile** all time or **Apply this profile during the below mentioned time window**. Selecting the latter keeps the Workflow active only during the specified days and hours.
   4. Delayed Trigger: If you want the workflow to be triggered at a delay, enter the delay time (in minutes). If you don't want to trigger the workflow if the alarm has been acknowledged in the mean time, you can select the 'Do not trigger if alarm is acknowledged' check box.
   5. Recurring Trigger: This option helps you trigger the workflow at regular intervals, till the alarm is cleared. Enter the trigger interval and number of triggers. If you don't want to trigger the workflow repeatedly if the alarm has been acknowledged, you can select the 'Do not trigger if alarm is acknowledged' check box.

8. Click **Save & Finish** available at the top of the page.

The workflow has been successfully added. It will be executed on the associated devices at the scheduled time or when any of the criteria selected is satisfied. You can check the output of the workflow in the Workflow Logs.

**Sample Workflow**

Following is a sample workflow which helps gets executed automatically when a device down alarm is raised. This workflow sends ping request, if passed does DNS Lookup and adds the output as notes to the alarm.
Workflow Execution Logs for the sample workflow: Click on **Workflows** from the left pane and select **Workflow Logs**

**Editing a Workflow**

To edit a workflow, follow the steps given below:

1. Click on **Workflows** from the left pane and select **All workflows** and click on the respective workflow name to edit.
2. The workflow edit panel opens. Perform the changes you want to do and click **Next**.
3. Modify the name, description, tags, associated devices, schedule, and alarm trigger options if required.
4. Click **Save & Finish**.
Executing Workflows

Before executing a Workflow, ensure that you have associated the workflow to the devices. To execute a workflow:

1. Click on Workflows from the left pane and select All workflows. All the created workflows are listed.
2. Click against the Execute icon on the respective workflow.
3. There is also an option to execute the workflow from the device page. Go to Device page > Workflow > click against the execute icon on the respective workflow.
Workflow Execution Logs

Workflow Logs provide the output of the executed workflows. It provides the result as well the data of each task that had been included in the workflow.

To view Workflow logs

1. Click on Workflows from the left pane and select Workflow Logs. Workflow output for each of the associated device is listed along with the executed date & time and number of tasks.

2. Severity

Each task once executed is logged with its severity for understanding its execution status. Following are the severities in Workflow:

- Info: Notifies a task has been executed successfully.
- Error: Notifies a task has been failed.
- Warning: Notifies that a task cannot be performed. Eg.: A delete file action cannot be performed when the directory does not have the specified file. In such cases, the delete file actions is marked as warning.
Alert Actions

You can perform the following alert actions:

**Acknowledge**: This option is useful for the operators to pick up the problem and work on it. When you select an alarm and click on Acknowledge button on top the alarms list, the administrator/operator's name is populated in the technician's field.

*Note*: Alarms that are acknowledged can be excluded from being escalated by configuring accordingly the alarm escalation rule.

**Unacknowledge**: The assigned technician is removed and the alarm is back in the unassigned list.

**Clear**: You can click this to clear an alarm manually.

**Delete**: You can delete an alarm.

**View History**: Click on the alarm message to view the alarm details and event history.

**Add Notes**: You can add notes to the alarms to explain the steps you have followed to correct the fault or to give tips to the operator who is working on the fault. In the Alarm history page, click the Add Notes option.

**Execute Workflow**: You can execute a workflow to troubleshoot an alarm. Click on Execute Workflow in the Alarm Details page, and select the workflow. The workflow will be executed and the output will be added in the notes.

**Test Actions**: You can notify this alarm via any of the notification profiles created by you. Click on Test Actions in the Alarm Details page, and select the desired notification profile.

**View Availability**: You can view the availability history of the faulty device. Click on More link in Alarm Details page and select Availability.

**Ping**: You can ping the faulty device by clicking on the Ping icon from the top of the Alarm Details page.

**Trace Route**: You can trace route the faulty device by clicking on the Trace Route icon from the top of the Alarm Details page.
Unmanage: Alarms created for devices that are under maintenance can be avoided by moving the device to unmanaged state.

Click Actions> Select Unmanage from Alarm Details page.

Configure Notifications: You can configure a notification profile to the faulty devices. Click Actions> Configure Notifications from Alarm Details page.
Configuring Notifications

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.

The different types of notifications available are:

- Email Alerts
- SMS Alerts
- Run a Program
- Run a System Command
- Log a Ticket (Trouble ticketing in ServiceDesk Plus)

The configured notification settings are available as profiles and these can be associated to different devices for different fault criteria.
Escalating Alarms

The alarms of critical devices should not be left unnoticed for a long time. For instance, the mail-servers, web-servers, backup-servers, switches, and routers are so critical that if their faults are not solved within a specified time, the networking functionality will be brought down. You can configure OpManager to escalate such unnoticed alarms by sending an e-mail to the person concerned. However, you have an option to exclude the alarms that are acknowledged from being escalated.

To configure a new alarm escalation rule, follow the steps given below:

1. Click Settings(alt+t) > Configuration > Alarm Escalation Rules.
2. Click Add Rule to create a rule.
3. Assign a name to the rule in the Rule Name field.
4. Select the Severity and Category of the alarm.
5. Select the Business View in order to associate the rule only to the alarms of the devices of the selected business view. If not select None to associate the rule to the alarms of all the devices.
6. Then configure the the interval (Not Cleared Within) in either hours or minutes to wait for the alarm to get cleared.
7. In the Run this check every box, set the interval in minutes to execute this rule.
8. You can exclude the acknowledged alarms from being escalated by selecting Exclude Acknowledged Alarms option.
9. Type the values for the fields under Escalation Email Details to send an e-mail if the alarm is not cleared within the specified interval.
10. Configure the From Email Address, the Subject and the Message of the escalation mail.
11. Click Ok.

If you configure a new alarm escalation rule, by default it will be enabled. To disable an alarm escalation rule click on Edit icon, deselect the Enable this rule option and click on Ok.
Managing Faults in Network

There can various types of faults in a network. With the network health depending on various resources like the system resources, services, network connectivity etc, getting to the root of the problem is simplified when the monitoring solution raises meaningful alarms. OpManager helps you identify the fault quickly with its detailed alarms indicating the resource that is poorly performing in the device. The different types of OpManager alarms include:

- Status-poll Alarms (device, service, interface, port down alarms).
- Threshold-based alarms for host resources, response times etc proactive monitoring.
- Alarms from SNMP Traps.
- Windows event logs based alarms.

OpManager monitors the resources for availability and performance and triggers alarms for all the criteria mentioned above. These alarms can also be sent as email or sms alerts from OpManager.
Processing SNMP Traps into Alarms

- What is SNMP Trap?
- Processing Traps into Alarms
- Tools
- Adding/Modifying Trap Processor
- Loading Trap Parsers from a MIB
- Processing Unsolicited Traps
- Configuring SNMP Traps in Agent

What is SNMP Trap?
Traps are cryptic messages of a fault that occurs in an SNMP device. SNMP traps are alerts generated by agents on a managed device. These traps generate 5 types of data:

- Coldstart or Warmstart: The agent reinitialized its configuration tables.
- Linkup or Linkdown: A network interface card (NIC) on the agent either fails or reinitializes.
- Authentication fails: This happens when an SNMP agent gets a request from an unrecognized community name.
- egpNeighborloss: Agent cannot communicate with its EGP (Exterior Gateway Protocol) peer.
- Enterprise specific: Vendor specific error conditions and error codes.

Processing SNMP Traps into Alarms
OpManager enables you to process the traps from the managed devices.

When a trap is received from a managed device, the match criteria in the parser determines whether a specific trap matches the conditions specified in the Trap Processor. Once a matching Trap is found, an alert is generated.

- Trap Processor: Converts the cryptic message to human-readable alarm.
- Configure OpManager to process the traps that are not processed out-of-the-box and convert them into alarms.
- The traps that are not processed are listed under ‘Unsolicited Traps’.

Tools
The following actions can be done by clicking the relevant icon:

- Edit: Edit the Trap
- Enable or disable trap processing: Click to enable/disable trap processing
- Delete processor: Delete the Trap Processor

Adding/Modifying Trap Processor

Go to Settings (alt+t) > Configuration > Monitors > Traps.
Click ‘Add New’ to add a new trap.
Click the TrapParser name/ Edit icon to modify an existing one.
Configure/Modify the following properties:

- Name: Configure a name for the new trap processor.
- Description: Describe the trap.
**Snmp Trap Version:** Select the version (SNMP V1/V2c).

**SNMP V1 Properties:**
- **Generic Type:** Cold Start, Link Up, Enterprise, etc. Select the appropriate type for the OID.
- **Specific Type:** When Generic Type is set to Enterprise a specific trap ID is identified.

**Enterprise OID:** Corporation or organization from where the trap originated, such as .1.3.6.1.4.1.x SNMP V2C / V3

**SNMP V2 Properties:**
- **Trap OID:** For devices with SNMP v2c version, select the trap oid from the MIB using the Select button.
- **Message:** Select the required message variables.
- **Severity:** Select the Alarm severity.

**Failure Component:** This option is useful when you deal with a single trap OID that has multiple failure components. The Varbinds containing more details on the trap will have information on the failed components (entities like cpu, temperature etc). You can match the entity too by appending the VarBind number in this field to generate separate alarms for the failed components. For instance, $Source_trapName_trap_$v5.

- **Source:** Append the Varbinds to be matched if required. This option is useful if the trap is forwarded from another source.

**Match Criteria:** Select the appropriate radio button to either match any one or all the conditions that you specify. Select the variable bindings, the condition, and the string to be matched.

**Rearm Criteria:** Similarly, select the appropriate radio button to match the rearm conditions. Select the variable bindings, the condition, and the string to be matched.

Click **Save** for the configuration to take effect.

**Loading Trap Parsers from a MIB**

Following are the steps to load the traps from various MIBs.

Go to settings(alt+t)> Configuration> Monitors> Traps. All the configured processors are listed here.

Click on **Load Traps From Mibs** at the top of the page.

From the list of MIBs, select the MIB from which you would like to load the trap variable. The traps in that MIB are listed.

Select the required trap variable, and click **Add**.

A Processor for the selected trap is added, and is listed under the **Traps** tab.

**How to process the Unsolicited Traps?**

Go to Alarms(alt+a)> Click on Unsolicited Traps.

Click on Create Trap Processor corresponding to the trap message.

Type a name for TrapName.

Make sure that the status is enabled.

Select the Severity.

Click on Add.
How to configure SNMP Traps in Agent?
Despite configuring the SNMP Trap Processor in opmanager, you might still not see the alarms based on traps. You might need to check the SNMP agent configuration on the monitored devices.
Receiving SNMP Traps in OpManager

OpManager listens for SNMP traps from devices on the default port 162. So, it automatically acts as a trap receiver and based on the trap processors defined in OpManager, the traps are processed and shown as OpManager alarms.
Alarm Suppression

OpManager provides you the option to suppress the alarms of the devices for a pre-defined time interval. This option will be very useful in cases, where the devices are under maintenance or some known issues exist with them.

Configuring Alarm Suppression for a Single Device

1. Go to the device snapshot page.
2. Click on Actions and select Suppress Alarms.
3. Select the period for which you want to suppress the alarm.

Alarms of this device will be suppressed for the selected period.

To configure the Alarm Suppression in a bulk

1. Go to the respective List view Page(Server, Router, Switch etc)> Inventory(alt+i)> Sort By Category.
2. Select the devices that you wish to suppress the alarms.
3. Click Actions> Suppress Alarms > Select the period for which you want to suppress the alarm.
Viewing Alerts

The Alarms tab in OpManager shows all the latest alerts.

From the list box on the top right corner, you can access the following:

- **All Alarms**: A complete list of alarms is displayed here.
- **Active Alarms**: This view lists only the active alarms that are not yet cleared.
- **Unsolicited Traps**: The unsolicited traps sent by the agents in the managed devices are listed here. These are the traps that are not configured to be processed in OpManager. If you find any of these traps to be critical, you can configure OpManager to process the traps using the information received from the agent. Refer to Creating a Trap Processor for details.
- **EventLog Alarms**: This view lists only the alarms that are triggered from Windows event logs as the source.
- **Syslog Alarms**: This view lists only the alarms logged via syslog.
OpManager allows you to configure e-mail alerts and SMS alerts to get notified on the fault in your network. By default, OpManager sends the mail to the mail server specified in the e-mail notification profile. To configure the SMTP server settings globally and to provide the secondary mail server settings, follow the steps given below:

1. Go to Settings (alt+t) > Basic Settings, click Mail Server Settings.
2. Enter the SMTP Server name and Port number.
3. Configure the From and To Email ID fields.
4. Enter a Time Out interval.
5. Configure the User name and Password details, if the server requires authentication to send e-mail.
6. For SSL authentication, select the SSL Enabled check-box, browse and select the SSL certificate and key-in the password.

Verifying Configuration

- To test the settings enter the Email ID and click Test Mail. This e-mail ID will be considered as the default To Email ID while creating Email and SMS notification profiles.
- If you have a secondary mail server in your network, select Add a secondary mail server and provide the details. In case of failure of primary mail server, OpManager uses secondary mail server to send e-mail and SMS.
Configuring Proxy Server Settings

Any business enterprise will have a proxy server to optimize its connectivity to Internet and to filter access to restricted Web sites. In OpManager, to monitor URLs over internet, you need to provide the proxy server details of your enterprise.

To enter the details, follow the steps given below:

1. Go to Settings (alt+t) > Basic Settings, click **Proxy Server Settings**.
2. Select the **Enable Proxy** check-box.
3. Enter the Proxy server name, port number in which the Web service is running on the proxy server, and the user name and password to connect to the proxy server.
4. For the devices that do no require to go through a proxy, specify the name or the IP Address of the devices as a comma separated list in the **No Proxy** field.
5. Click **Save** to save the details.
Forwarding Syslog

You can forward the syslog received in OpManager to any NMS.

Steps to forward syslog:

1. Go to Settings (alt+t) > Configuration > Monitors > SysLogs > Forward SysLog.
2. Click on Add Destination button.
3. Provide the Name/IP address of the NMS Host to which SysLog has to be forwarded.
4. Provide the SysLog listening port number of the NMS to which SysLog has to be forwarded.
5. Click on Start Forwarder to initiate sending of SysLog to the destination NMS. You can also Stop Forwarder at any desired time.
Forwarding Traps

Configure OpManager to notify users over a Trap when there is a specific fault.

Steps to forward Traps:
1. Go to Settings( alt+t ) > Configuration > Monitors > Traps > Forward Trap.
2. Provide the name/IP address of the host to which notifications has to be sent.
3. Provide the trap listening port number of the host to which notifications has to be sent.
4. Click Save.
**Configuring Email Alerts**

You can configure OpManager to send e-mail to network administrators when a fault is detected in the device. You can create separate profiles for each administrator and assign them to devices so that whenever the device has a fault, an e-mail is sent to the technician concerned.

To create an email alert profile, follow the steps given below:

1. Go to **Settings (alt+t) > Configuration > Notifications.**
2. Click **Add New.**
3. Select the fault criteria for which you need to be notified. For instance, if you want to be notified of threshold violation, select 'Threshold rule is violated'. Click Next.
4. Select the devices either **All Devices in a category** or **Manually choose Devices** and click next.
5. Select the required **Time Window, Delayed Trigger** and **Recurring Trigger** and click next.
6. Select the Notification type as **Send Email.**
7. Provide the **To and From Email Address, Mail Subject** and **Message** (select the required alarm variables which is to be displayed on the email notification) and click next.
8. Give a profile name and Click **Test Action** to test the email profile or **Create** to create the profile.

The profile is associated to the selected devices. A notification is sent every time a threshold is violated for a server.

**Note:** Primary and secondary SMTP server settings can be provided in the Mail Server Settings page in OpManager. Whenever a new email profile is created, the values of the primary SMTP server and the authentication details are retrieved from the Mail Server settings. Refer to **Configuring Mail Server Settings** for steps to enter the details. If the SMTP server is not available while sending e-mail, secondary mail server is used to send the mail automatically.
Using a Run Program Notification Profile

You can configure OpManager to automatically run a program whenever a fault is detected in the device. For instance, you can configure OpManager to execute a program that corrects the fault or simply produces a sound or that whenever a specific type of an alarm is raised for a device.

To create a profile that executes the specified program, follow the steps given below:

1. Go to Settings (alt+t)> Configuration> Notifications.
2. Click Add New.
3. Select the fault criteria for which you need to be notified. For instance, if you want to be notified of threshold violation, select 'Threshold rule is violated'. Click Next.
4. Select the devices either All Devices in a category or Manually choose Devices and click next.
5. Select the required Time Window, Delayed Trigger and Recurring Trigger and click next.
6. Select the Notification type as Run Program.
7. In the Command Name field, specify the name of the program to be executed with the absolute path. Example C:\profilestestprogram.bat.
8. If the program requires some arguments, specify the Program Arguments and click next.
9. Give a profile name and Click Test Action to test the email profile or Create to create the profile.

The profile is associated to the selected devices. The program is executed with the specified arguments whenever a fault matching the selected criteria occurs.
Using a Run Command Notification Profile

You can configure OpManager to automatically run a system command whenever a fault is detected in the device. For instance, you can configure OpManager to execute a netsend command to send popup messages to users machines whenever a specific type of an alarm is raised for a device.

To create a profile that executes the specified program, follow the steps given below:

1. Go to Settings (alt+t)> Configuration > Notifications.
2. Click Add New.
3. Select the fault criteria for which you need to be notified. For instance, if you want to be notified of threshold violation, select ‘Threshold rule is violated’. Click Next.
4. Select the devices either All Devices in a category or Manually choose Devices and click next.
5. Select the required Time Window, Delayed Trigger and Recurring Trigger and click next.
6. Select the Notification type as Run System Command.
7. In the Command String field, specify the command name with additional arguments if any.
8. Select the Err Append and Append check-boxes to append the output and the error message on executing the command.
9. Give a profile name and Click Test Action to test the email profile or Create to create the profile.

The system command is executed with the specified arguments whenever a fault matching the selected criteria occurs.
Notifications via Traps

Configure OpManager to notify users over a Trap when there is a specific fault.

Steps to configure a trap profile:

1. Go to Settings (alt+t) > Configuration > Notifications.
2. Click Add New.
3. Select the fault criteria when any [selected...] SNMP trap is received from the device, click next.
4. Select the devices either All Devices in a category or Manually choose Devices and click next.
5. Select the required Time Window, Delayed Trigger and Recurring Trigger and click next.
6. Select the Notification type as Send Trap.
7. Provide the Host Name, Host Port, Version(snmp version), Community(snmp read community string) and Varbinds if any.
8. Give a profile name and Click Test Action to test the email profile or Create to create the profile.

You have successfully configured the notification profile.
SysLog Notification Profile

When any fault occurs you can notify users via SysLog.

Steps to configure a SysLog profile:
1. Go to Settings (alt+t) > Configuration > Notifications.
2. Click Add New.
3. Select the fault criteria when any [selected…] Syslog Rules generates alarm, click next.
4. Select the devices either All Devices in a category or Manually choose Devices and click next.
5. Select the required Time Window, Delayed Trigger and Recurring Trigger and click next.
6. Select the Notification type as Send SysLog.
7. Destination Host > Provide the Name/IP address of the host to which notifications has to be sent.
8. Destination Port > Provide the SysLog listening port number of the host to which notifications has to be sent.
9. Severity > You can choose any of SysLog severity events to be processed.
10. Select the Facility and required Message Variables.
11. Give a profile name and Click Test Action to test the email profile or Create to create the profile.

You have successfully configured the notification profile.
Modifying and Deleting Notification Profiles

You can modify or remove an existing notification profile. Here are the steps:

1. Go to Settings (alt+t) > Configuration > Notification.
2. All the configured profiles are listed here.
3. Click the Delete icon against the profiles name to delete the profiles.
4. Click the Edit icon against the profiles name to modify the profile properties.

The changes made here are applied for all the devices to which the profile is associated.
Intuitive dashboards and detailed reports help you determine the performance of your network in very less time. OpManager allows you to export the default reports to other file formats such as exporting to PDF or XLS. You can also schedule the reports to be emailed or published.

The default reports available in OpManager include:

- **System**: Provides a complete report on all the system related activities of all the devices. This category of reports include All Events, All Down Events, SNMP Trap Log, Windows Event Log, Performance Monitor Log, Notification Profiles Triggered, Downtime Scheduler Log, Schedule Reports Log, All Alerts and All Down Alerts.

- **Health and Performance**: Gives you a detailed report on the health and performance of all/top N devices.

- **Availability and Response**: Gives you a detailed report on the availability and the response time of all/top N devices.

- **Inventory**: Inventory reports are available for servers, desktops, all devices, SNMP-enabled devices and non-SNMP devices.

- **Virtual Device**: OpManager monitors all the critical parameters of your VMware servers and allows you to generate reports on the collected value. It provides over 70 different reports out-of-the-box, helping you get an insight into the performance trend and top hosts and VMs.

- **My Favourites**: OpManager provides the option to categorize all your important and frequently viewed reports as your favorites.

- **Schedule Reports**: OpManager allows you to schedule a new report and also to schedule a generated report.

- **Custom Report Builder**: Custom report builder is the easiest way to generate reports using only the data that you want. This stages in four types (Category, Devices, Monitors, Time Period and Graph or Table view)
Viewing Interface Reports

Interface reports help you to determine the health of the interface by generating detailed reports on In and Out Traffic, In and Out Errors and Discards, Bandwidth & Outage Report, At-a-Glance Report etc. The reports can be exported to PDF format, taken printouts or emailed by clicking the respective icons. To generate the interface reports, follow the steps given below:

1. Go to the snapshot page of the interface whose health report you want to generate.
2. Go to Reports (alt+r) > available on the left pane of the page. All the default reports that can be generated are listed.
3. Click on the name of the required report to generate current day’s report. Click on the 7 or 30 days icon to generate the report for the last 7 or 30 days respectively.
Creating New Reports

Apart from the 100+ available default reports you could also create a new report based on the data that you want. To create a new report follow the steps given below:

1. Go to Reports(alt+r) > Default Reports > Select any category > Click the **Create New Report** link at the top of the page. Create New Report page opens.

2. Enter a unique **Name** and brief **Description**.

3. Select the required **Report Category**. For instance, the report category is selected as Performance Reports.

4. Click **Next**.
5. Select the **Monitor category**.
6. Select the sub category.
7. Click **Next**.

8. Select the required **Category**, **Business Views**, **Show All or Top/Bottom N Devices**, **Period** and **Time Window**.

9. Click **Finish** to create the new report.

The created report gets saved under the appropriate report category. Go to that category and click on the report to generate the report.
Editing Reports

OpManager allows you to edit a generated report in order to refine for some specific parameters, devices or time periods. To edit a generated report follow the steps given below:

1. Go to Reports( alt+r )> Default Reports> Select the category> Click against the report name that you wish to edit.
2. Click Edit Report button available on the top right of the report page.
3. Change the required fields. The various fields that can be altered are Category, Period, Business Views, Time Window.
4. After modifying the required fields, click on Show Report to generate the report effecting the changes made.
Copying Reports

OpManager allows you to copy a generated report in order to retain the already configured parameters as template and do some minor changes on them and save as a new report. To copy and save a report follow the steps given below:

1. Click **Copy As** icon available on the top of the report that is generated. A small window opens.

2. Enter a unique **Name** and a brief **Description**.

3. Change the required fields. The various fields that can be altered are Category, Period, Business Views, Time Window and Show all or Top N or Bottom N devices.

4. After modifying the required fields, click **Save** button to save the new report.
Scheduling Reports

OpManager allows you schedule a new report, schedule a generated report and also to view a scheduled report.

Schedule a new report

1. Go to Reports(alt+r)> Default Reports> Schedule Reports.
2. In the Scheduler Reports Page, click the Add Schedule button on the top right.
3. Configure the following details:
   1. **Schedule Name**: Configure a name for the schedule.
   2. **Choose Report Type**: All the available reports types can be scheduled (select either one and follow the instructions given below followed by Configuring the Time Settings)

Scheduling Device specific Availability reports:

1. If you have chosen to schedule reports for Device specific 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.
2. Select the **Period** and **Time Window** for which you want to generate the reports.

Scheduling Top N Reports / All Devices reports:

If you have selected to schedule the Top N Reports, configure the following details:

1. **Top N Reports**: Select from Top 10/25/50/100/1000 reports.
2. **Period and Time Window**: Choose the Period and Time Window for which you want the report scheduled.
3. **Select Report(s)**: Select the required resource reports to be scheduled.
4. **Business View Reports**: Select the relevant check-box and the business view to generate reports specific to the devices in that business view.

Configuring the Time Settings for generating reports:

1. **Daily**: Select the time at which the reports must be generated every day.
2. **Weekly**: Select the time and also the days on which the reports must be generated.
3. **Monthly**: Select the time, day, and the months for which the reports must be generated.
4. **Report Format Type**: Select either PDF or XLS to receive the report in the respective formats.
5. **Report Delivery**: Select any one of the following options.
   - Configure the email ids to which the reports are to be sent as attachments. (or)
   - Configure the url where the reports can be published.
   - **Period**: Choose the period for which you want the report scheduled.
   - **Select Report(s)**: Select the required resource reports to be scheduled.

Verify the details of the configured schedule and hit Add Schedule for the schedule to take effect.
Scheduling a generated report

1. In the report page that is generated, click **Schedule This** button to schedule the report.

   1. Enter the **Schedule Name**.
   2. Select the **Category** followed by **Business View**.
   3. Select the **Period** and **Time Window**.
   4. Select the **Report Format** (PDF or XLS).
   5. Select the **Report Delivery Type** (Attachment or URL).
   6. Enter the **Email ID** to which the report has to be delivered.
   8. Click **Save**.

**Viewing the Scheduled Report**

1. Go to Reports(alt+r)> Default Reports> Schedule Reports
2. Click agains the **view** icon on the required report that you wish to see.
3. The list of generated reports for the selected report will appear.
List of generated reports for shedule_availability

- shedule_availability-9_0-October_8_2014
- shedule_availability-9_0-October_7_2014
- shedule_availability-9_0-October_6_2014
- shedule_availability-9_0-October_5_2014
- shedule_availability-9_0-October_4_2014
- shedule_availability-9_0-October_3_2014
- shedule_availability-9_0-October_2_2014
Configuring Favorite Reports

With OpManager you can mark the reports that are frequently viewed as Favorite reports. The reports that are marked as favorite reports are listed under My Favorites report category. To mark a report as your favorite one, follow the steps given below:

1. Generate the report that you want to mark as your favorite.
2. Click the star icon(Mark a report as Favorite) at the top of the page to mark a report as Favorite.

A message is displayed saying that "This report has been added to your favorite list".
About SIEM plug-in

Security Information and Event Management (SIEM) Plug-in complements OpManager's functionality of data center monitoring and provides you complete network security intelligence that ensures security at your data center. The plug-in can centrally collect, normalize, analyze, correlate and archive log data from heterogeneous sources across your network which helps you to detect and react instantly to security breaches, internal security threats, policy violations and more. SIEM plug-in's real-time event response system gives you instant alert notification on any anomalous activity on your data center network thus helping you respond immediately to the security breach.

The plug-in ensures you being compliant to various regulatory mandates such as PCI-DSS, FISMA, ISO 27001, GLBA, HIPAA, SOX and more. The plug-in supports more than 500+ multivendor log data sources. Click here to see the complete list of supported devices.

Installation Platform

SIEM plug-in supports both Windows and Linux installation (both 32-bit and 64-bit architecture)

Database

The plug-in supports comes with the bundled PostgreSQL database. However, it also supports MS SQL database.

Features:

- Supports heterogeneous log data sources.
- Centralized log collection, analysis and archival capability
- Supports both agent based and agent less log collection methods
- Archives log data for customized time period. Archived log data is made tamper proof with encryption
- Secures confidential files/folders with precise integrity details and also triggers alerts upon any critical changes or unauthorized access to those data.
- Enables the detection of network anomalies quickly with its powerful search engine.
- Monitors privileged user activities and gives you a comprehensive user audit trail.
- Sends out instant alert notification upon any network anomalies and triggers remediation script.
• Drill down dashboards and reports help in in-depth log analysis and provides better insights into network security events.

• Integrated compliance management system helps to stay compliant to various regulatory mandates with its out-of-the-box compliance reports.

• Allows to customize the existing compliance report or build a new report to meet the growing needs of regulatory mandates

How SIEM plug-in different from the EventLog monitoring feature available in OpManager?

The event log monitoring feature just monitors Windows events via WMI. Whereas the SIEM plug-in collects, analyzes, and archives logs of all applications & devices for security and compliance.
Installing SIEM plug-in

Download the SIEM plug-in from OpManager website and follow the below procedure to install:

1. Download SIEM plug-in

2. Shut down OpManager service if it is running.

3. Start the installation sheild of SIEM plug-in. Do not change the suggested installation path while installing. By default, SIEM plug-in will be installed in the same path as that of OpManager. In case if you have moved OpManager to a different directory, then provide the changed directory path.

   For Linux installation, you need to provide the directory path where the OpManager is installed.

4. By default SIEM plug-in uses web server port 8400, ensure that you made it free. In case you want to change the default web server port then follow the procedure stated here <link>.

5. Click Finish to complete the installation

Click here to know more on the system requirements.
Setting up SIEM plug-in

Here is a guide on how to set up and run the OpManager - SIEM plug-in

- Prerequisites
- Troubleshooting tips
- FAQs

Prerequisites

1. At the time of SIEM plugin installation, do not run OpManager service. After installation, when OpManager server is started, the SIEM plugin will also automatically started.

2. Do not change the suggested installation path, while installing SIEM plugin. By default, the plugin will be installed in the same directory in which OpManager is installed (Default path: ManageEngine_EventLogAnalyzer_Plugin.exe/bin). In case, if you have moved OpManager installation to a different directory, then provide the changed path for the plugin installation.

3. For Linux installation, you need to provide the directory path of OpManager installation (Default path: /opt/ManageEngine/OpManager)

Note: Click here to know the system requirements of SIEM plug-in

Troubleshooting tips

1. After SIEM plugin has been installed, ensure the working of database by checking the file elaPluginDB.log file in <OpManager_Home>Eventlog

2. If the database creation fails, then you need to recreate the database. To do that, run <OpManager_Home>EventlogTroubleshootingDBRecreation.bat <database name> in the command prompt with administrator privilege.

3. After recreating the database, ensure the database creation by executing elaPluginDB.log file. Once the database is created successful, then start OpManager service.

Note: Provide the database name as an argument to the command. For instance, in the command, 'DBRecreation.bat eventlog', 'eventlog' is the database name

Need further assistance? Contact support
FAQs

1. My Email/SMS setting and users are not synchronized with OpManager. What should I do?

   By default the Email/SMS settings and users will be automatically synchronized. If they are not synchronized, then click on OpManager’s Admin tab> Sync EventLog option to manually synchronize them.

2. How to change from HTTP to HTTPS (secure communication), after installing SIEM plug-in?

   If you want to change the protocol from HTTP to HTTPS after SIEM installation, follow the below procedure:
   - Go to the location <OpManager_Home>EventLog\l8nScript
   - Open the file server.xml and locate the below entry:

   ```xml
   <Connector port="8400" SSLEnabled="true" acceptCount="100" address="0.0.0.0" clientAuth="false"
   compressableMimeType="text/html,text/xml" compression="force" compressionMinSize="1024"
   connectionTimeout="20000" disableUploadTimeout="true" enableLookups="false"
   keystoreFile="<OpManager keystore file location>" keystorePass="<password>" maxSpareThreads="75"
   maxThreads="150" minSpareThreads="25" noCompressionUserAgents="gozilla, traviata"
   protocol="HTTP/1.1" scheme="https" secure="true" ss1Protocol="TLS" URIEncoding="UTF-8"/>
   ```

   - Provide OpManager’s keystroke file location and password for the fields ‘keystoreFile’ and ‘keystorePass’

   **Note:**

   For example in the below lines, `D:/ManageEngine_OP/OpManager_latest/conf/OPMTrans.key` is the keystrokeFile value and `opmanager` is the password.
If the plugin's web server port connection turns out to be untrusted, then you need to handle this exception through 'Tools option' in your web browser. Below is the screenshot on 'Adding Security Exception' to SIEM plugin's web server port in Firefox browser. Carry out this procedure in accordance to your web browser.

![Security Exception](image)

Provide EventLog Analyzer web server port number here as <server name>:<port number>
Eg: https://eventlog:18500
**Note:**

1. Webserver port number of SIEM plugin is available in server.xml file located in `<EventLogAnalyzer_Home>/conf` directory
2. Both OpManager installation and SIEM plug-in should use the same web protocol. If OpManager runs in HTTP then the plug-in should also use HTTP mode.

3. **How to migrate to a different database for SIEM plug-in?**

   The SIEM plugin uses OpManager's database to store the log data. In case you have changed the database of OpManager after SIEM plug-in installation, then follow the below procedure to manually migrate SIEM plugin's database.
Execute the file DBRecreation.bat/sh located in ‘<OpManager_Home>\EventlogTroubleshooting’ in command prompt.

- Provide your database name as the argument in the above command. For instance in the below command, 'eventlog' is the database name.
  - 'DBRecreation.bat/sh eventlog'

- You must take the database backup before migrating the database. To take the back up, follow the below procedure
  - Run the command prompt with administrator privilege
  - Go to <EventLog Analyzer_Home>/tools/backUpDatabase.bat/sh to backup the data available in the current database. Wait until the backup completion
  - By default, backup file will be stored in <EventLog Analyzer_Home>/backup directory in the name:
    - 'backup_eventlog_<Build_Number>_MM_DD_YYYY_hh_mm.data'

- If you are migrating to MS SQL database, then you need to copy the bcp.exe and bcp.rll files from the installted MS SQL Server to <EventLog Analyzer_Home>/mysqlbin folder

**Note:**

If you are copying the above file from SQL (Version 2005 & above) installed in a machine where plugin is not installed, then install the SQL Native Client in the plugin server as per the SQL version and CPU type

**MSSQL 2005 (32 bit)**

**MSSQL 2005 (64 bit)**
http://download.microsoft.com/download/4/4/d/44dbde61-b385-4fc2-a67d-48053b8f9fad/sqlncli_x64.msi

**MSSQL 2008 (32 bit)**
http://go.microsoft.com/fwlink/?LinkId=123717&clcid=0x409

**MSSQL 2008 (64 bit)**
http://go.microsoft.com/fwlink/?LinkId=123718&clcid=0x409

4. **How do I add only specific Windows hosts for monitoring?**

   By default, the plugin synchronizes all the Windows, Syslog hosts monitored by OpManager. If you need to monitor only specific Windows host, then

   i. Set ‘AutoSync OpManager Hosts’ option in Log Analytics Settings > ELA Configurations tab to ‘False’
ii. Select the specific hosts which you want to add to the plugin from Log Analytics Settings > Manage Hosts > Add > OPM Hosts option
5. How do I add a syslog device to the SIEM plug-in?

The SIEM plug-in automatically adds all the syslog devices that are forwarding its logs to OpManager installation. If you want to add only specific syslog devices to SIEM plug-in then contact our support team for the assistance.

6. How do I add a syslog device exclusively for SIEM plug-in alone?

To add a syslog device only to the SIEM plug-in, follow the below procedure:

i. Login as root user and edit the syslog.conf file in the /etc directory.
ii. Append ".<space/tab>@<server_name> at the end, where <server_name> is the name of the machine on which SIEM plug-in is running.
iii. Save the configuration and exit the editor.
iv. Edit the services file in the /etc directory.
v. Change the syslog service port number to 519, which is the default listener port of SIEM plug-in. If you have chosen a different port other than 519 then remember to enter that same port while adding the device to the SIEM plug-in.
vi. Save the file and exit the editor.

Restart the syslog service on the host using the command:

vii. /etc/rc.d/init.d/syslog restart

For configuring syslog-ng daemon in a Linux host, append the following entries

```
destination eventloganalyzer { udp("<server_name>") port(514)); }

log { source(src); destination(eventloganalyzer); }
```

at the end of /etc/syslog-ng/syslog-ng.conf, where <server_name> is the ip address of the machine on which SIEM plug-in is running.
7. What if the default port 519 is preoccupied in my environment? How do I change the default UDP port used by SIEM plug-in?

If SIEM plug-in's default UDP port is preoccupied, then you can change this default UDP port for syslogs by carrying out the following procedure:

- Go to **Admin tab > Syslog** Rules. Click on Actions drop down menu and select forward Syslog option.
- Now in the Destination details window, edit the destination port by clicking on Actions menu.
- Stop OpManager and SIEM plugin's service.
- Edit the file `runsec.bat/sh` which is located `<EventLog Analyzer_Home>/bin` folder.
- Edit (in notepad) the entry `"binSysEvtCol.exe -loglevel 2 -519"` for default port change and remove ports that are not required. For example, if you do not want port 519 as default, the edited line will look like:

  `"binSysEvtCol.exe -loglevel 2 -<your_port_number>"` - where `<your_port_number>` is your chosen port.
- After saving the `runsec.bat/sh`, restart the SIEM plug-in - OpManager service/server for the changes to take effect.

**Note:** If you want to detect the syslog reception, click on **Admin Tab > Syslog rules > Select 'Action' drop down menu > Select 'Syslog Viewer'**. The syslog viewer will show you the syslogs collected in real-time.
About CMDB Plug-in

CMDB plug-in offers in-depth visibility of your assets present in the IT environment. It centralizes information about all Configuration Items, including their attributes and relationships with which you can ensure uptime and service availability. These Configuration Items (CIs) can be hardware, software, documents, business services and also the people in your organization.

With the help of CMDB Plug-in, OpManager keeps track of all Configuration Items (CI) in your IT environment, maps the relationship between the CIs and helps you predict the impact of CIs before performing any change. Visualization map in CMDB provides a detailed view of the CI relationships which helps in identifying the dependencies between CIs and allows you to manage all the IT components based on their business criticality.

Installation Platform:

CMDB plug-in supports only Windows installation as of now.

Supported DB:
CMDB plug-in supports MSSQL and PostgreSQL.

Ports Used:
• Web: 8080

Features:
• Sync OpManager assets with ServiceDesk Plus.
• Automatic asset update
• Asset association to tickets in SDP
• Relationship Map
• Inventory Reports
Installing CMDB Plug-in

Download the CMDB plug-in from OpManager website and follow the procedure given below to install:

1. Download OpManager's CMDB plug-in file to OpManager server.
2. Shutdown OpManager Service.
3. Double click OpManager's CMDB plug-in exe file. (You have to install CMDB plug-in in OpManager server only)
4. Follow the on-screen instructions to complete the installation process.
5. Start the OpManager Service.

After installing the CMDB plugin, Extract this patch under <opmanager-home> and start the server.

**Note:** You should have OpManager 11100 build or later.
Sync Asset details

To Sync Asset details, Go to Add on/Product settings -> **servicedesk settings**, you can find the two options as shown below

1. **Auto Sync** :

   Whenever a device gets added/deleted/undergoes any change in OpManager, the auto sync feature will update the same in ServiceDesk Plus(SDP). This helps to maintain the CMDB inventory up-to-date.

2. **Merge OpManager Asset details with SDP** : (Auto sync should be yes)

   Few cases on choosing option Yes :

   1. If the discovered device is present in OpManager and not present in SDP. Then the same asset will get added in SDP.

   2. If the discovered device is present both in OpManager and SDP. The asset details in SDP will get updated (i.e. merged) with OpManager info.

   3. When a device is deleted in OpManager, then the same asset should be automatically deleted in SDP (Even though the asset is not added via OpManager - since OpManager has overwrite permission)

   4. In-case of any updates(Ram,OS,IP address, type, category) in devices present in OpManager - the same should get updated in SDP

   On choosing Option No :

   1. If the discovered device is present both in OpManager and SDP - The same asset won’t get merged. It will be skipped by default

   2. On any update in devices present in OpManager - the same should get updated in SDP (only if the asset is added via OpManager)

   3. On deleting any device in OpManager, the same asset should get deleted in SDP. (only if the asset is added via OpManager)
On clicking **Sync Now** button, all the devices present in OpManager will get synced to ServiceDesk Plus.
Diagnostics

This option helps the user to identify the server monitors which are not responding across all Servers. Instead of viewing each and every device page, you can have a consolidated view of the problematic monitors and their servers. It can be accessed by clicking Support-->Support. It lists all the available protocols in which the monitors are added. If a protocol is selected, it lists all the servers and their monitors which are not responding. The **Consecutive Time** option lets the user to select the last N numbers of polls these metrics are not responding. If 5 is selected, it lists only the monitors which are not responding for their last 5 polls. You have to wait for 30 minutes once you change the "Consecutive Time" for the updated monitor list to show.

"**Test Credential**" is used to check if the associated credential for the device is passing or not and the "**Test Action**" is to manually check if the monitor is responding or not.

<table>
<thead>
<tr>
<th>Server Health Report</th>
<th>Consecutive Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>SNMP</td>
</tr>
<tr>
<td><strong>dcorouter</strong></td>
<td></td>
</tr>
<tr>
<td>Monitor Name</td>
<td>Date and Time</td>
</tr>
<tr>
<td>CPU Usage (5 mins avg)</td>
<td>6/14/13 4:54 PM</td>
</tr>
<tr>
<td>Cisco Memory Utilization</td>
<td>6/14/13 4:54 PM</td>
</tr>
<tr>
<td><strong>Jayakumar-0446.cse2.zohocorpin.com</strong></td>
<td></td>
</tr>
<tr>
<td>Monitor Name</td>
<td>Date and Time</td>
</tr>
<tr>
<td>testing12a</td>
<td>Not Collected</td>
</tr>
<tr>
<td>UpTime</td>
<td>Not Collected</td>
</tr>
<tr>
<td><strong>Sanjeev-0326.cse2.zohocorpin.com</strong></td>
<td></td>
</tr>
<tr>
<td>Monitor Name</td>
<td>Date and Time</td>
</tr>
<tr>
<td>testing12a</td>
<td>Not Collected</td>
</tr>
<tr>
<td>UpTime</td>
<td>Not Collected</td>
</tr>
</tbody>
</table>

"**Date and Time**" column shows the last polled date/time. If it says "Not collected", it means there was no data since the monitor was added or device was discovered.
OpManager discovers network topology map from the given Router IP and IP range via SNMP using CDP, ARP, IPRoute Table and Bridge-MIB information.

**Layer2 Enhancements:**
- Discovery of non-cisco devices and end nodes (server, desktop) are now supported.
- Now you can also draw the Layer2 Maps for the devices which are not discovered/monitored in OpManager.

**Router Discovery Algorithm**

WebNms algorithm used: Router must have two or more interfaces and ipForwarding of the device must be set to 1.

**Switch Discovery Algorithm:**

WebNms algorithm used: Switch should support bridge mib.

To discover a map, mouse over to Maps tab > Layer2 Topology Map > Layer 2 Discovery and configure the following details and click in Discover.

- **Router Address**: Provide Router or L3 Switch IP address which meets the above algorithm.
- **Network Range**: Provide Network range to discover devices in the specified range and to draw map.
  - Start Ip - Network Range starting IpAddress.
  - End Ip - Network Range ending IpAddress.
- **Net Mask**: Provide subnet mask
- **Layer2 MapName**: Unique Name for Map to be referenced from all the places.
- **Schedule Interval(Days)**: Provided in days for the rediscovery.
- **Credential To Use**: As of now we are supporting SNMP protocol only, add the credential and select the credential.
After discovery a new map will be added.

Clicking on the Map name will show the complete map discovered.
Deleting and rediscovery of Maps:

A map can be deleted or updated using Delete and Update button shown on the top right corner of the page.

Map zooming option:

If the Map contains more number of devices, it may be shown as overlapped with adjacent devices, it can be enlarged or shrunked using Zooming option marked with + and - buttons on top left of the page.

Printing Maps:

Required maps can be printed directly from the Map page using Print option available on top corner of the page.

Troubleshooting:

1) If you get an error "Please enter valid Router or L3 Switch Address" during discovery, need to verify the following:

   Router must have two or more interfaces and IpForwarding of the device must be set to 1.
1) To verify the above, need to go to the Admin > Mib browser > load Bridge mib from select mib option and enter the devicename/IpAddress, provide SNMP string under Community and enter the below OID one by one or browse to the Object Id column and click SNMP get to verify the response.

**BridgeMib:**

*IfIndex Vs Port*

*IfIndex* - .1.3.6.1.2.1.17.1.4.1.1  
*IfName* - .1.3.6.1.2.1.17.1.4.1.2

**dotdTpFdbTable**

*dotdTpFdbAddress* - .1.3.6.1.2.1.17.4.3.1.1  
*dotdTpFdbPort* - .1.3.6.1.2.1.17.4.3.1.2  
*dotdTpFdbStatus* - .1.3.6.1.2.1.17.4.3.1.3
Pass-through Authentication

Pass-through authentication (Single Sign-on) provides the ability to authenticate yourself automatically in OpManager using your currently logged in windows system username and password. You would not need to manually enter your windows credential to log-in to OpManager webclient.

Prerequisites:

- Active directory authentication must have been configured in OpManager for the domain you want enable Pass-through Authentication.  
  Adding Domain.
- User accounts to whom you want to enable pass-through must have been already available in OpManager. Create New Users -> AD User.
- A computer account must be created in the Domain Controller for ensuring secure communication with the Domain Controller by OpManager.
- OpManager webserver must have been added as a trusted site in each browser you will be using to connect OpManager webclient to avoid browser popups asking for credential.

Creating Computer Account:

Run the script NewComputerAccount.vbs present under OpManager_Homeconfapplicationscripts to create a new computer account

```
cscript NewComputerAccount.vbs account_name /p password /d domain_name
```

To reset the password for an existing computer account, run the script SetComputerPass.vbs present under OpManager_Homeconfapplicationscripts to create a new computer account

```
cscript SetComputerPass.vbs account_name /p password /d domain_name
```

Ensure that the password you give is compliant to the password policy for that domain. Do not use the New Computer Account option present in AD native client which will not allow you to choose password. If you face problem running this script from OpManager server, copy the script to the domain controller machine itself and try running it.

Configuring Trusted Site in Browser:

For Internet Explorer (applicable to Chrome as well):

Open Tools -> Internet Options -> Security -> Local Intranet -> Sites -> Advanced. Enter OpManager server URL, click Add.

For Firefox:
In URL box enter `about:config`. Click the button "I'll be careful. I promise", if warning page is displayed. In the resulting page, search for `ntlm`. Double click the option `network.automatic-ntlm-auth.trusted-uris`. Enter OpManager server URL in the text box and click OK. (Multiple site entries can be entered separated by comma.)

**Configuring in OpManager:**

In OpManager webclient, click Admin tab -> User Manager -> Pass-through. Check "Enable Pass-through Authentication".

**User Configuration**

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>OPMANHV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind String</td>
<td>opmanhv.com</td>
</tr>
<tr>
<td>DNS Server IP</td>
<td>172.18.4.63</td>
</tr>
<tr>
<td>Computer Account</td>
<td>testac$@OPMANHV.COM</td>
</tr>
<tr>
<td>Password</td>
<td>**********</td>
</tr>
</tbody>
</table>

Domain Name: NETBIOS name of your domain. Example: OPMANHV

Bind String: DNS Name of your domain Example: opmanhv.com

DNS Server IP: Primary IP Address of the DNS Server.

DNS Site: Site under which the Domain Controller is listed.

Computer Account: Account name of the computer account created. Append `$@domain_dns_name` with the account name. Example: mytestacc$@OPMANHV.COM

Password: Password of the computer account

**Getting Domain DNS Name and NETBIOS Name:**
In the Domain Controller device, open Start -> Administrative Tools -> Active Directory Users and Computers.

Getting DNS Server IP:

Open Command Prompt in OpManager server. Run "ipconfig /all". The first IP Address mentioned again DNS Servers is the primary DNS Server IP Address.
Getting DNS Site:

In Domain Controller device, open Start -> Administrative Tools -> Active Directory Sites and Services. The Site under which your Domain Controller device name listed is your site name. You can leave the DNS Site field empty in Pass-through configuration form in OpManager, if there is only one site present in your Domain Controller.
Design Limitations:

- Pass-through authentication can be enabled for only one domain, preferably the domain in which OpManager server resides. If pass-through has been configured for a domain other than the one in which OpManager server resides, ensure the other domain will provide logged in user information to a website from different domain.
- Pass-through authentication will work only for the active directory users already been added to OpManager. If you do not want to manually create user account for all the users in your domain, enable auto-login for the domain (Admin->User Manager->Windows Domains). Once auto-login is enabled, you have to manually enter username and password of your account only on the first login and an user account in OpManager will be created automatically, from there on you can simply work without manually entering.

Disable Pass-through Authentication:

In OpManager webclient click on Admin tab -> User Manager -> Pass-through. Uncheck “Enable Pass-through Authentication”.

(OR)

Connect OpManager database from command line and run the query “delete from JespaConfiguration” and restart OpManager service.
Log File:

If you face any issue with Pass-through Authentication, contact support with the `jespa.log` file present under `OpManager_Homelogs` folder.

Troubleshooting:

Case 1:

`jespa.log` file ends with line `getDomainTrusts: Retrieving list of domains and` 

`stderr*.txt` contains `java.lang.ClassCastException: java.io.PrintStream cannot be cast to java.lang.String`

Solution:

Update the log level for `jespa log` in `OpManagerDB`

- Connect `OpManager` database
- Execute the query: `update JespaConfiguration set JESPACONFIG_VALUE='3' where JESPACONFIG_KEY='jespa.log.level'
- Stop `OpManager` service
- Delete the file `jespa.log` under `OpManager_Homelogs`
- Start `OpManager` service

Case 2:

`jespa.log` file contains `jcifs.smb.SmbAuthException: Logon failure: unknown user name or bad password`

Cause:

Password configured for computer account is wrong (or) got expired (or) does not comply to password policy of the domain.

Solution:


Reset password for computer account using SetComputerPass.vbs script and update the value in OpManager.
What is Event Flood?
Receiving a huge number of events of the same ID get generated from a machine within a short span of time.

How does OpManager handle Event flood?
A new thread is added in the opmanager to monitor the number of events generated every hour and cross verify it with a predefined value. If a particular event is generated for more number of times and exceeds the predefined value, the process of updating that particular event in the opmanager database is stopped and an critical alert is generated with a message starting with EVENT PROCESSING STOPPED. Critical event indicates that event update process has been stopped due to event flood and will be resumed from the next hour.

Configuring OpManager to handle Event Flood:

1. To configure the limit of events generated:
   - From the opmanager machine, go to <opmanager home>/conf
   - Open serverparameters.conf.
   - Put an entry at the last as 'EVENTS_PER_HOUR 1000', to monitor event generation.
   - Increase the set default value ‘1000’ as per your requirements, but cannot be set below 1000.
   - Save the file and restart the opmanager.

2. To configure the severity of alerts generated:
   - From opmanager machine, go to <opmanager home>/conf
   - Open serverparameters.conf.
   - Put an entry at the last as 'EVENT_FLOOD_SEVERITY Critical', to monitor event process stopped alert.
   - Change the set default severity to 'Attention', 'Trouble', 'Critical', or 'Info'. By default it will be 'Critical'.
   - Save the file and restart the opmanager.

Note: If you set the severity as 'info', you will not get a seperate alert. It will be appended as an event with the particular Trap or Eventlog alert.
**Note:** The one hour limit will start from the time of start of opmanager. So if the opmanager is started at 1pm, it will check the limit from 1pm to 2pm. If it exceeds within 2pm, the event generation will get stopped. Again it will resume from 2pm and will check till 3pm and the process gets repeated. This time interval cannot be configured as of now.

**Type of events currently handled:**

- All types of eventlogs
- All types of traps

The Event flood handling is available as a patch for 11200 build.
**Issues Fixed: Build 12200**

- Issue with Rule engine settings not being saved is fixed.
- Included clear severity for VMWare events.
- Issue with CiscoTemperature Monitor's instance not added is fixed now.
- Issue with not being able to add SNMP monitors for custom Device template with custom category, custom vendor and added monitors for the first time is fixed.
- Issue with alert remaining in acknowledged state even after clearing and raising it again is fixed.
- Issue with the dial information not being completely visible when more custom monitors are enabled to show dials is fixed.
- Issue with the Threshold settings getting changed after saving them is fixed.
- Issue with the Rearm Type and Threshold types being shown wrongly for string monitors is fixed.
- Issue with the Threshold settings not being retained when a template is exported with threshold settings is fixed.
- Issue with the monitors tab being empty when the SQL instance has special characters is fixed.
- Issue with not being able to enter Sys OID without loading any MIBs is fixed.
- Issue with the Interfaces not updating during rediscovery is fixed.
- Under Traps List view, error with Status getting disabled when OpManager language is Non-English has been resolved.
- Error with Business view selection not working in scheduled report has been fixed.
- Interface Widget - Device Snapshot Page - issue during expansion - fixed.
- Issue with Router CPU Utilization reports showing more than 100 percentage is fixed.
- Issue with profile getting deleted, when notification profile is edited has been fixed for customers who had upgraded from v12000 to 12100.
- Error with Thresholds containing "=' not being saved has been resolved - Req #3009354.
- Issue with Interfaces by Traffic Widget supposed to Show percentage Rx and Tx, but showing values, has been fixed.
- A check has been added to display error message when adding URL with existing name.
- Error where Interfaces Bandwidth Utilization widget does not show any units for data like MB, KB or GB is resolved. - Req:3135717.
- Issue where Notification with "Selected" Trapparser behaved like "ALL" has been fixed.
- Error where Windows service Monitor does not appear if a custom category is chosen on a custom template is fixed.
- Issue with Google maps always being loaded with default zoom value instead of previously set zoom has been fixed.
- Error when Mail server password contains "+" not being stored has been resolved.
- IT360 servlet vulnerability.
- Unable to save Interface monitoring interval value.
- Issue with only 10 VoIP monitors being listed in UI even though more than 10 are added, has been fixed.
- Issue with vCenter discovery if password contains ('&', '<', '>') characters is fixed.
- Error due to credential change in vCenter that resulted in AD authentication not working for SDP and SSL certificate import not being saved OOM in data collection, has been fixed.

**Issues Fixed: Build 11500**

- Servlet and SQL vulnerabilities has been fixed.
- Issue with displaying wrong measurement units for process monitor memory usage in CLI device snapshot page is fixed.
- Script error that occurs while loading 3D rack and floor view in Internet Explorer (IE 10 and above) has been fixed.
- Exception while restoring MySql to PgSql backup file is resolved.
- Issue with wrong display of Interface Up/Down alerts in OpManager Spanish installation is fixed now.
- Issue ID: 99558 - A fix has been applied for proper sorting of outage history in device availability page.
- Issue ID: 99768 - Issue with downtime scheduler showing same name in different schedulers due to comma separation in the device displayname is fixed.
- Issue with deleting newly added sysOID in Device Template page (Old Client) is fixed.
• Issue with updating syslog rule in webclient is resolved

• Issue ID: 100652 - NetApp Inventory data not showing for Exe users (11.3 & 11.4 build). A fix has been applied to resolve this issue

• Thread Lock issue that happens due to recurring notification has been fixed. Due to this issue, the users were unable to clear the alarms

• Issue ID: 103164 - Probe mismatch that occurs while adding the same service from Probe 1 and Probe 2 has been fixed now

• Issue with applying notification profile to multiple devices from Quick Configuration Wizard is fixed

• Issue ID: 103155 - Issue with setting thresholds to the monitors in Device Templates is resolved now (Issue ID: 1603213)

• Issue ID: 101717/102552 - Error while loading vCenter and virtual device snapshot pages due to the presence of special characters in VM name is resolved now

• Issue with associating notification profile in ServiceDesk Plus (Log a ticket) has been resolved

• Issue ID: 103166 - Issue with generating SIF due to special character (%) in the URL address of a URL monitor has been fixed

• Garbled string appears in the URL response for content-type with Shift-JIS encoding. This issue has been fixed

• Issue ID: 101026 - Issue with updating central server details in the install shield of standby server has been fixed

• Issue ID: 103159 - Issue with updating configuration changes in ServiceDesk Plus details due to the cache is fixed now

• Issue ID: 101026 - A fix has been provided to successfully configure failover in OpManager 11400. The issue was with updating secondary server with primary server details

• Issue ID: 100852 - Issue with adding AD Domain details in old web client is fixed now

---

**Issues Fixed: Build 11400**

• Vulnerability in Apache Struts has been fixed

• DB Connection refresh failure issue is resolved

• The issue where editing a business view map leads to an error page has been fixed (Issue ID: 1358809)

• Data Truncation issue while taking back-up in Non-English OS is resolved (Issue ID: 1393262)

• A fix has been applied to avoid out of memory errors while performing bulk cleanup of events during startup. (Issue ID: 1578399)

• Issues with standalone to probe migration has been fixed now

• Breakage in alarms colored view and monitors page for other languages is fixed

• Slideshow button in rack viewer page of old-client is working fine now (Issue ID: 1455575)

• The fix has been applied to increase the field limit of workflow execution log messages (Issue ID: 1455382)

• In Linux installation, issue with Central Probe archive data is resolved

• Issue with trap messages showing invalid byte sequence is resolved (Issue ID: 1320110)

• Issues with storing traps in event table due to junk characters have been fixed now (Issue ID: 1320110)

• The bug that enabled automatic deletion of VMware VMs during migration from one host to another has been fixed.

• A fix has been applied to correct the Hyper-V time interval

• Issue with tabs while logging into OpManager through Single sign on authentication is fixed

• Issue with hardware information being shown as NULL for few Cisco devices is resolved

• Issue with adding HyperV VMs due to NPE is resolved

• AD Groups authorization issue has been fixed now (Issue ID: 1459231)

• The users with unlimited workflow license can now add workflows without any error. The fix has been applied (Issue ID: 1387811, 1451979)

• Links to VoIP, WAN RTT & Virtual Devices has been removed for Read Only users

• Issue with NetApp device inventory details is fixed (Issue ID: 1331275)
- The bug that enabled an empty context while exporting Virtual Machine reports has been fixed
- Issue with "Windows services by Availability" widget has been fixed
- String match in URL Monitoring is working fine now. Fix has been applied (Issue ID: 1355182)
- User ID mismatch when restoring the cross-db backup is fixed (Issue ID: 1451052, 1518844)
- Issue in adding host resource disk and Partition monitor has been resolved (Issue ID: 1431159)
- Issue with the NetApp volumes monitor is fixed (Issue ID: 1331275)
- Configuring NAT in OpManager Server will now enable Schedule Reports to update proper download URL in the report e-mails (Issue ID: 1356561)
- Fix has been applied to show the recipient name in the scheduled report email (Issue ID: 1318658)
- Number format exception that occurs while rediscovering the interfaces has been resolved
- Fix has been applied to correct the alarms from SNMP traps widget
- Issue with the WMI CPU utilization where consecutive times was not working properly was fixed (Issue ID: 1420326)

**Issues Fixed: Build 11300**

- In French installation, issue with junk characters appearing in sys description, device display name, interface display name, hardware details is fixed
- Issue with asset details not getting modified while rediscovering the device via workflow is fixed now
- Netflow add-on will now get loaded within OpManager instead of a separate tab
- Issue with RAM details being left out in Service Desk Plus asset details while syncing the asset details to SDP is resolved
- Issue with receiving notification for traps which are not selected in notification profile criteria page has been fixed
- Issue with business view widgets not showing its details properly has been fixed now
- Issue with probes not showing the dashboard information, reports, etc due to the newly added empty custom fields in central is resolved now. (Issue ID: 1257085)
- WMI data collection getting stopped while upgrading from 9410 -> 10200 -> 11100 has been resolved now.
- Issue with trap category not shown in alarm page for IPMI traps is fixed.
- Issue with wrong file age shown in file monitor details is resolved (Issue ID: 1178050)
- DataCollection problem due to the long probe ID’s is fixed (Issue ID: 1190348)
- Issue with the SNMP partition monitors not getting applied via device templates for devices with WMI & SNMP credential is fixed (Issue ID: 1190348)
- Issue with monitoring large size folders (in GB/TB) has been fixed now
- Failure Component related traps’ not being received for IPMI is fixed
- Error page shown while creating unsolicited traps is resolved (Issue ID: 1224396)
- Issue with Disk Utilization data collection for Novell device is fixed
- Issue with generating PDF version of “All Interfaces availability report” while choosing Top/bottom option is fixed
- Issue in displaying Snapshot page/Dials/Reports for French installation is resolved now
- Issue with the discovery failure of ESX host if it does not have a datastore is fixed
- In Dell Hardware Monitoring, disk array removal status has been now associated to “service down” alert category. Previously it was associated to “clear” alert category
- Issue with VM display name getting modified with VM path name due to fake rename events is resolved
- VMware discovery process will now skip the Template VMs part since they are dummy VMs without an IP address
- Issue with editing monitors that has '%' character in their display name is resolved
- Issue with Interface datacollection in Linux OpManager install with Mysql database after 11200 build upgrade is fixed.
Issues Fixed: Build 11100

- All issues with respect to Windows Services monitoring is addressed.
- Downtime Scheduler - The error 'Failed to load from DB' is fixed now
- Improper alignment in the hardware / vcenter snap shot pages in japanese edition is addressed - (Issue Id 95292)
- Issue of data not collected for hardware parameters such as battery, memory, processors is fixed now
- At times hardware data collection is stops, if the sensor name size is fixed
- Interfaces report such as Total bytes transferred in postgres database was incorrect is fixed. (Issue Id 4612390)
- Schedule reports at times is not generated after 10200 build upgrade due to Message column is fixed now (Issue id 4619595)
- Schedule reports are not generated in linux installation is fixed now (Issue id 4624044)
- Email based SMS notification - headers are shown in the text is fixed now
- OpManager license get corrupted at times, when plugins licenses are applied is fixed
- URL Monitors - Issue of Alarm generation, if consecutive times is configured is fixed
- Issue of downtime report not shown in MSSQL database if the device is down for more than 25 days is addressed
- Device availability reports at times throws error is fixed
- Issue of details shown for a user, if business views are associated is fixed
- CPU utilization, Memory Utilization, Disk Utilization real time graphs were not plotted for other languages is fixed now
- Custom fields for devices and interfaces are now shown in sorted order
- Database backup and restoration at times fails is fixed now
- Central failover registration failure case is addressed (Issue 4638492)
- Process specific workflows are not triggered is fixed (Issue id 4638296)
- Vmware discovery / rediscovery fails when data store is in inaccessible state is fixed
- Auto Vaccum parameter set properly for postgres database
- UPS polling parameters such as battery status, link status will not be updated during polling, if the device is first discovered as non snmp device and moved to ups category
- Issue of duplication drives getting added in the case of multiple node graphs ie. used /free / partition monitors (snmp based) if the index changes is resolved
- Issue of data not getting collected for Memory utilization monitor (WMI) if threshold is configured is fixed.
- WMI - Partition values shown wrongly is corrected now
- Negative Value in InterfaceReport LegendValues (Min, Max) and ReportList is shown as 0 , (Issue id:4620827)
- Issue of thresholds getting removed from devices if applied via Templates is resolved. (Issue ID 4639858)
- Issue of OpManager Agent not getting started is fixed now
- At times, support information file generation fails if any of the installation plugins are not running. This is fixed now.
Issues Fixed: Build 10200

1. Test Actions fails if mail server is configured with secured connection details (Issue Id: 94951)
2. Standalone to Probe migration fails due to Postgres database support is fixed (Issue Id: 94922)
3. VMware virtual switch error is rectified (Issue Id: 94903)
4. Issue in monitoring disk array data for Dell servers is fixed (Issue Id: 94862)
5. Out of Memory error occurs due to VCenter bulk host data fetching is fixed now (Issue Id : 94829)
6. Read only users able to view All devices / All Interface details is corrected now (Issue Id: 94811)
7. Issue of status not getting updated for URL monitors at times is fixed (Issue Id: 94780)
8. Syslog severity not changed in Non-English version is fixed (Issue Id: 94755)
9. Devicetype not mapped if the device is added using Rest API is fixed (Issue Id: 94754)
10. Alarms not shown for SNMP V1 traps is fixed (Issue Id: 94752)
11. Device status not updated at times due to timeout is fixed (Issue Id: 94750)
12. Unable to add a non pingable device using Add device option is fixed (Issue Id: 94733)
13. Business view loading page optimized (Issue Id : 94723)
14. Device specific thresholds not shown in workflow criteria page are fixed (Issue Id: 94720)
15. $DisplayName variable supported in Script monitors now (Issue Id: 94643)
16. Database archiving (hourly / daily) triggered automatically during server start up for the previous hour / day if it misses the same.
17. At times, probe registration fails if the probe name length is greater than 25 characters is fixed
18. Issue of 100% CPU due to hardware monitors is fixed now
19. Issue of hardware monitors shown incorrectly in System diagnostics is fixed now
20. Thresholds if modified in Device templates is overwritten for already configured devices, is fixed now
21. Enhancements and fixes made in OpManager Database backup and restore for all databases
22. Issue of NCM database not started if OpManager uses MySQL database is fixed
23. Issue of OpManager web client loading slowly in MySQL database is fixed
24. Stray entries in the database due to interface, service, URL monitors if deleted, is fixed
25. Unable to login to OpManager client, if the user license count is not set correctly in the license file is fixed
26. Process Monitor data collection not done due to NumberOfLogicalProcessor method not present in Windows XP and 2003 machines is fixed now
27. Devices at times missed in business views a device category is changed with immediate rediscovery is fixed
28. New Client API options missed in the earlier build is fixed now
29. API XML Response issue for List Devices is fixed (Issue Id: 4580213)
30. Page navigation issue in Agents List page for MSSQL database is fixed
31. At times, Agent hangs issue is rectified (Issue Id: 45476 71)
32. URL Monitors at times, not monitors due to User-Agent variable is fixed now
33. Issue of multiple racks of the same can be created is fixed (Issue Id: 4581786)
34. Issue of default WMI monitors such as CPU, Memory, Disk not collected for custom windows device templates is fixed now
35. OpManager security vulnerability due to tomcat is addressed now
36. OpManager server - local host device will be discovered by default during fresh installation.
37. Alarms - Category field shows as question mark, for traps if the IP address is null for interface is fixed (Issue Id: 95136)

Issues Fixed: Build 10100

1. If any interface has Null as its IP address the interfaces are not discovered properly and then error page shown when you click on Interfaces tab (Issue Id 94414)
2. SNMP v1/v3 devices responds partially to SNMP v2 and thus throws error when parsing the SNMP response during shallow discovery. (Issue ID 94390)
3. Discovery fails if device display name contains special characters, is fixed (Issue ID 94375)
4. Monitors, Notification Profiles, Interface Tab doesn't show for NetApp Devices is corrected (Issue ID 4554403)
5. NCM fails to connect in https mode is fixed
6. Issue in viewing the Business view if any interface traffic is null is fixed
7. At times, Netapp Storage devices is not categorized correctly is resolved
8. Trap OID Contains matching fails in during SNMP Trap Processing is rectified
9. OutOfMemory error due to Layer 2 polling is fixed
10. Events Summary widget display the event type as Null for the UPS specific alarms is fixed (Issue ID 94206)
11. Unable to view the alarm escalation due to stray entries in the database is fixed (Issue ID 4554674)
12. WMI Monitors will be shown only if the device type name contains 'WIN' is corrected. Hereafter its based on the vendor type
13. Extra slash added in the credential settings page while updating the credentials is fixed
14. If multiple statsdata hourly table is created in a particular day, then all the tables are not considered for the daily table archiving. This is fixed now (Issue ID 4552226)
15. Unable to start OpManager (enterprise edition) in Windows XP is fixed
16. Database restoration fails from mysql to postgres database is fixed now
17. Incorrect values shown for CPU Utilization - Top 3 Process list. This is corrected now.
18. Process Monitor data collection fails for CLI protocol is fixed
19. Incorrect received syslog has unknown string as host name, now host name taken from packet (Issue ID 4567408)
20. Device template will not be applied, if “Show All Devices” option selected. This is fixed (Issue ID 94456)
21. Host snap shot page now shows the Orphaned vm's

**Issues Fixed: Build 10000**

1. MSSQL instance name duplication due to "MSSQLFDLauncher" services is resolved.
2. Issue with backslash character in WMI attributes leading to an error page is fixed now. (Issue ID 93648)
3. Issue with managing URL's due to license check is fixed now. (Issue ID 93539)
4. Now ‘{IPAddress}’ variable can be used in workflows. (Issue ID 93694)
5. Alarms added via ‘Add Event’ API can be cleared with Rest API. (Support Request Id 4542842)
6. Provision to add the AD user in API is supported now
7. Database disconnection at times occurs, which is due to frequent query which is triggered to check the user permission level. This is fixed now
8. Issue with “Execute Windows Script” task not responding while executing workflows is fixed. (Issue ID 93738)
9. New filtering parameters are added in Rest API for listing alarms. (Support Request Id 4498614)
10. In IE, the issue with real-time graphs in device snapshot page not showing up is fixed now. (Support Request Id 4521422)
11. Devices by Packet Loss widget was displaying zero packet loss condition in red bar. Now it has been fixed and changed to green color.
12. Issue with false alert getting generated for windows services is fixed.
13. Issue with configuring username in authentication details of mail server has been resolved.
14. Data truncation issue in SysLog email notification due to the presence of angular brackets (< , >) in SysLog message has been resolved now (Issue Id 93569)
15. SysLog alarms are not getting generated when there is a single syslog rule. This issue is fixed. (Issue Id 93524)
16. Issue with URL monitors not getting updated on consecutive times even when threshold is enabled, is fixed. (Issue Id 93915)
17. Single quote issue in IE while executing windows script in workflows is fixed now.
18. The issue with multiple thresholds configured in newly created Device Template not getting reflected in central & other probes is fixed now.
19. Issue related to recurring notifications is fixed. (Issue Id 93672)
20. The issue with showing an error Message "Router IOS version may be lower than 12.3" shown even though the device is of greater IOS is fixed
21. IPSLA link status getting greyed out i.e. unmanaged is fixed
22. In IPSLA, issue with adding IPSLA in French and editing display names is fixed
24. During Failover, Unwanted Timers that runs when in standby mode is cancelled and stopped.
25. Multiple syslog rule creation caused by refreshing ‘submit’ page of Syslog addition is fixed.
26. Logo was missing in availability reports. Now logo has been added (Issue ID 93449)
27. Icons to display critical and trouble threshold status in List view page have been added.
28. Now you can also Windows Service monitor by using vendor name instead of type.Services, and URL monitors are allowed for categories
29. For users with full control to a business view, adding WMI monitors option was disabled. This issue has been fixed. (Issue Id 93555)
30. Issue with iPhone alarm page navigation issue is fixed (Issue Id 93515)
31. For printers, even though no alerts are configured when it turns to clear state, alerts are getting raised. This issue has been fixed. (Issue Id 93614)
32. Average value is shown in threshold alerts for CPU utilization with multiple instances.
33. When editing any Availability and Response report, certain options were missing. This issue has been fixed.
34. Proper icon was not associated for devices from Dell. This issue has been fixed.
35. The status of the Services shown wrongly in Maps --> details view is corrected now (Issue ID 93875)
36. Test Action at times failies for System Command / Run Program profiles if the Alarm Message contains $ symbol is fixed (Issue Id 94057)
37. Problem Retrieving XML data alert popup while viewing WAN RTT Monitors (Issue Id 93737)
38. Run System Command profile fails for trap, when we select the specific traps in Notification profile. This is fixed now (Support Request Id 4538155)
39. Technician name filter in the alarms page is fixed
40. Unable to start postgres database in german installation is fixed (issue id 93801)
41. Unable to rediscover the interfaces for the devices discovered as non snmp device and then configuring snmp credentials for the same. (Issue Id 92587)

**Issues Fixed: Build 9410**

1. No data getting collected for interfaces when there is partial response for interface OiDs. This has been fixed now.
2. Backup and restore of OpManager database fails at times. This has been fixed now.
3. Database changes happens twice if the PPM is installed both in Primary and Secondary server. This has been fixed now.
4. Unable to login to OpManager web client at times. This has been fixed now.
5. Support of ‘consecutive times’ in services fails due to the service – exchange. This has been handled now.
6. Loading of OpManager web client is slow after 9400 build. This has been fixed now.
7. Unable to share device / script templates after 9400 build. This has been fixed now.
8. Event log alerts are not raised if ‘consecutive times’ is configured. This has been fixed now.

**Issues Fixed: Build 9400**

1. Issue ID: 90727 - Option provided to export 'Bulk credential test' result to Excel spreadsheet.
2. Issue ID: 84460 - The issue while associating Event Log rule from Quick Configuration Wizard for a custom Windows device type is now fixed. (Note: The device type name should with Windows, for e.g. "Microsoft Windows").
3. Issue ID: 84033 - Custom Report showing any one partition details for multiple disk partition utilization report issue is now fixed.
4. Issue ID: 87977 - MIB browser - At times, double clicking "get" button throws error popup issue is fixed now.
6. Issue ID: 90777 - The 'Select all' option is now fixed while associating SNMP Trap processors to devices in 'Notification Criteria' page.
7. Issue ID: 87228 - The missing MAC server device type icon in ....web-clientdevicesimages folder is now added.
8. Customer period availability report issue is now fixed.
9. Issue ID: 90738 - DataAccessException related to Mail Server Settings related is now fixed.
10. False positives issue related to File Modification in File Monitor features is now fixed.
11. Page loading slow issue for MS SQL device snapshot page, if the device has more than 10 database instance is now optimized for quick page loading.
12. Unable to set rearm value same as threshold value issue has been fixed - To avoid future confusion the rearm condition is now changed from '>' to '>='.
13. Issue ID: 91057 - Creating a New custom dashboard goes to error page issue has been fixed.
14. Issue ID: 91067 - Set as default option is now removed in custom dashboards.
15. Issue ID: 90953 - Issue while showing the graph in an embedded real-time graphs widget is now fixed.
16. Issue ID: 90918 - List the devices in a Business View will work in mobile UI.
17. Issue ID: 90910 - Mobile UI login issue is now fixed.
18. Wrong value shown under the Top 3 Memory Utilizing process issue is now fixed.
19. Issue related to 'Consecutive Times' check for threshold based numeric and string monitor is now fixed.
20. CLI related optimization and issues are fixed.
21. Device Template stored details of multiple node graphs, if removed from the templates has been fixed.
22. Options provide in the BackupDB.bat to exclude NetFlow and NCM plugin backups (Command : BackupDB.bat -exclude netflow, ncm).
23. The URL getting truncated after '/' in Check URL action of workflow module issue has been fixed.
24. Global association of process monitor to a device via workflow is done.
25. URL monitoring issue related to long header situation is now handled.
27. Enterprise Edition: A widget is added to list URL alarms count under 'Site widgets' category in Central server web-client.
28. Alarm suppression not working for IP SLA alarms, even when the source device is at unmanaged state is now fixed.
29. In some cases, alarms not getting triggered, when the set threshold is violated in an IP SLA monitor is now been fixed.
30. SysLog Alarm is not generated if the received syslog has its host name in header is now fixed.
31. Health report y-axis label not shown, if the value is less then 1 issue is now fixed.
32. Unable to add event via REST API by giving IP address issue is now fixed.
33. The issue with system setting -> time zone updates not reflecting in the top right of the product UI is now fixed.
34. Issue ID: 91420 - Device Summary widget does not list devices when the display name contains "&" issue is now fixed.
35. Issue ID: 91340 - Last N hours values of a performance monitor widget does not show value for Last 30 days time period issue has been fixed.
36. Devices not getting discovered using nmap command in Linux OS (RHEL) is now fixed.
37. Issue ID: 91435 - Event type "critical" is now added to Admin -> Event Log Rule section.
38. Error page shown while accessing the Notification profile option from the Device Snapshot page issue is now fixed.
39. Option to customization alarm message's length is now introduced.
40. Ability to customize the default set of monitors to be associated to MS SQL monitoring as 'Auto add' column is now provided.
41. Issue ID: 90961 - Distracting alert box in IE saying "12029 Unknown" when viewing real time widgets is now fixed.
42. Issue ID: 90549 - disk.vbs and disk_snapshot.vbs are overwritten during upgrade issues has been fixed.
43. Now it is made possible to associate asset information in ticket details.
44. Option provided to enabled log-in page ad from system settings page, if the ads are permanently closed by the customer.
45. If ServiceDesk plus is configured not to close the tickets without adding a resolution, OpManager will add the alarm clear state as resolution and close the ticket.
46. Partition-wise disk utilization monitor thresholds can now be applied during the device discovery.
47. Issue ID: 90894 - $eventType is added in alarm variable list of notification profile.
48. Slowness while discovering SNMP v3 devices is now fixed.
49. Changes to the SNMPv3 credentials in the snapshot page, doesn't change in few tables as expected. The result lead to data collection stop issue has been fixed.
50. Real time Monitor hangs in widget/CCTV custom dashboard issue is fixed now.
51. The Consecutive Times setting can be set now independently to each service monitor.
52. Services/ Windows Services/ WMI Service (AD/Exchange/MSSQL) monitors status propagation handled for manual alarm clear and delete.
53. No more alerts for removed Service/ Windows Service/ WMI Service(AD/Exchange/MSSQL) monitors.
54. The Virtual Machine information will be invalid when the datastore connectivity is lost with the ESX host, and OpManager trying to sync inventory changes with ESX either during discovery/rediscovery. We have restricted such invalid VM (Unknown) entry getting updated in OpManager database.
55. When datastore is removed from ESX server, all the threshold entries associated for the VMs and V-Host getting removed are now restricted.
56. The ESX and the Virtual Machines data collection getting affected because of any stale data-store related polling entries got merged with valid entries is fixed now.
57. Issue ID: 86772 - Association of VMware credential from the various list views is now taken care.
58. Issue ID: 91046 - VM ESX Host discovery failure due to the VMs with same UUID has been resolved.
59. Issue ID: 91070 - Threshold of VM's getting reset with default template configuration for the vMotioned VM's of ESX server has been fixed.
60. Issue ID: 90987 - The VMware host data collection problem because of DNS name not treated case-insensitive in the cache has been fixed.
61. The event monitoring to identify vMotion or VM inventory changes in ESX and HyperV, which got interrupted and stopped further monitoring on error scenarios are fixed.
62. The Virtual host ESX & HyperV not listed when configuring workflow on selecting Virtual Device category is now fixed.
63. Issue ID: 91133 - Option provide to apply Windows monitoring templates for HyperV hosts.
64. HyperV guest un-mapping issues to the Host inventory is been handled now.
65. Hyper-V 'Disk Read Latency' and 'Disk Write Latency' monitor's Consecutive times related issues are fixed.
66. Issue ID: 90772 - HyperV Host devices are now shown in VMware ESX/ ESXi monitoring template.
67. Issue ID: 89369 - Hyper-V Host Collection/NextPoll time is displayed now in snapshot page.
68. Issue ID: 90717 - Data collection stops for VM performance monitors, if the virtual guest is moved to Domain Controller category is now being fixed.
69. Issue ID: 83815 - All devices are shown in virtual device reports for full control with Business access privileged users.
70. Issue ID: 91178 - If the list views (excluding Virtualization dashboard) of devices contains the virtual devices then stats are now properly shown from VMware tables.
71. Issue ID: 90736 - While importing Device Template, if the category is not present, then they are added automatically as custom category.
72. Issue ID: 90796 - Vendor Sub-category Name, Index, Display column are now supported in Import/Export Device Template option.
73. SMS modem disconnected repeatedly while trying to trigger SMS through workflow module is fixed now.
74. Business View - Fixed shortcut count problem for OpManager with MS SQL back-end.
75. Business View - Handled issues related to cookie problem when Flash viewer didn't loaded properly.
76. Business View - "Label Name & IP Address" are shown for Routers now.
77. Business View - Map Custom Icon is replaced after a new Device Template is applied.
78. Business View - Device Label Name is replaced by Device Display Name issue is now fixed.
79. Business View - For Non-English instance of OpManager, if a newly created business view didn't have a background image, it wasn't loading in the custom dashboard widget. This issue is now fixed.
81. Business View - The Business View names were now listed in ascending order for non-admin users as well.
82. Disk Forecasting - Forecasting report didn't show, when the table split up has been fixed now.
83. Trap - Fixed question marks (????) shown in category field for trap message received from Desktop.
84. Trap - Correct Category didn't show for "$Agent" type in Trap Alert message. It showed the "$Source" device category's Name. Is now fixed.
85. IPSLA - Selected notification profiles in IPSLA Monitor Threshold Template are now showing as selected.
86. IPSLA - Now you can select all alarms in WAN RTT and VoIP monitors tab.
87. IPSLA - NPE during WAN/ VoIP monitors configuration, if the source has the notification profile already associated in Probe setup issue has been fixed now.
88. Issue ID: 91493 - Enterprise Edition - Error page shown while trying to configure notifications for probe down alarms is now fixed.
89. Enterprise Edition - Unable to start probe if DataID.dmp got corrupted issue is now handled in the product.
90. Enterprise Edition - Unable to start probe if there is any pending response from Central [a threadlock situation] is now fixed.
91. Enterprise Edition - Status of probe not getting changed in central, even though the device, alarms are getting updated properly in central is now being handled.
92. Enterprise Edition - Both the primary and standby probes are showing as Up, even though one of them is down is fixed now.
93. Issue ID: 91714 - Fixed the 0kb file issue while exporting (last 60 days or last 90 days) performance reports as spreadsheets.
94. NCM Plugin - Import devices in plugin to show the Display Name instead of IP address
95. Unable to login, on keeping custom tab as first tab - Now login done based on their Type.
96. Display name gets truncated in infrastructure view if the name contains ‘&’ is fixed now.
97. Unable to generate Down time report in MS SQL backend instance of OpManager is been addressed.
98. Unable to delete sample ticket generated by OpManager in ServiceDesk Plus (during start up) is been fixed now.
99. Device availability widget query changed in MS SQL backend instances.
100. Trail popup will be shown at every login with an option to close it permanently to the prospects.
101. Only selected services and windows services will be shown under Notification profile (from device snapshot page) -> Criteria options.
102. Error Handling done for ServiceDesk add on product settings.
103. Now the list view pages across the product has a default pagination of 100.
104. Fail Over - Heart Beat Schedular (which is used to update the LastCount value in the BEFailOver table) will not be started for Standalone server. It will be triggered in the following scenario,
   1. When the Standby server is registered with the Primary server
   2. When the Standby make itself as Primary
   3. When the Primary send a request to the Standby server to perform failover.
105. Mail server timeout value will not be considered, while sending the emails from now on.
106. Device availability query changed for custom time period reports.
107. Fixed the error 'Managed Object not present' when the interface Display Name is configured from the interfaces snapshot page, configure option.
108. Issues related to Interface status polling using ICMP Ping is fixed.
109. Discovery status is not changed for existed network from now on.
110. Archiving query execution time is included in audit description.
111. No data available issue in performance monitor graphs related reports (At a glance report, Custom report) in discontinued device snapshot page.
112. Issue ID: 91892 - FQDN used in embed widget URLs
113. Issue ID: 92120 & 91334 - Allows already existing MS SQL DB name in the installation wizard.
114. Issue ID: 90608 - Allows special character in the password (MS SQL DB panel from the installation wizard)
Issues Fixed: Build 9200

Virtualization (VMware & Hyper-v)
1. Issues with polling happening when a VMware is unmanaged or when a downtime is scheduled is fixed now.
2. Data collection happens properly even when the datastore name is same as the host name.
3. Missing threshold entries in VMware has been fixed.
4. For better visualization, the VM displayname set as the VM name is now fetched from ESX instead of DNS name.
5. You can now enable VM rediscovery from the snapshot page.
6. Status propagation from VM to Host is restricted.
7. The alarm suppression option in VMware is enabled for ESX/Hyper-V hosts.
8. Issue in VM Rename performed through the VMRename event received via API is fixed.
9. Host network usage monitor issue for non-English language installations is now fixed.
10. Host discovery failure on adding hosts that share same name due to misconfiguration is resolved.

Business view
1. You can now save the Business view names starting with any numeric values.
2. The issues concerned with non-English languages, overlapping icons/status position and the Mapnames in export to visio are fixed.
3. Grid option is provided in Business view editor.

Maps
1. In Layer2 Map, infinite looping that happens in CDPCache table is fixed.
2. All Device page loading time has been improved.

Monitors
1. In process monitors the issue with false alerts getting generated, when you make a query to fetch a list of processes times out is fixed.
2. In process monitors the issue with false alerts getting generated, when the device has more than 1000 processes is fixed.
3. The issue with string OID monitors not displaying the values in the widget is fixed now.
4. Attributes are listed for SQLServer:Plan Cache in Custom WMI Monitors.
5. You can edit the mailbox store location of Used Disk Space monitor in Exchange Monitoring.
6. Issue in saving threshold value for Cisco Memory Utilization has been resolved.
7. While deleting the performance monitor, alarms of that monitor get deleted correctly in probe and central now.
8. In Import/Export Device Template, the issues with multiple custom SNMP monitors and custom WMI monitors are fixed.
9. Thread leak/Memory leak issues due to improper closing of sessions in CLI monitoring, is now fixed.

Widgets
1. The real time widgets can be configured to fit to current screen size while looking in different sized screens.
2. Fit to screen option in Business view widgets works fine now.
3. Downtime scheduler
4. Downtime scheduler is configured to allow granular per minute time.
5. Downtime schedule works properly now even when OpManager server is stopped and started when the schedule is on.

Reports
1. Inventory Report in OpManager is now working fine.
2. Security issue showing IPSLA reports of all devices when logging as a business view user has been resolved.
3. Issue with availability showing different values in reports and snapshot page is fixed.
Notifications
1. The data unavailability issue in notification profile report is fixed.
2. AlarmID variables are now provided in notification profile.

Others
1. The 'Forgot Password' option in the login screen works fine. A link to reset password is sent to the configured email ID.
2. It is now possible to disable "Keep me signed in" option in OpManager.
3. OS Ping is supported for non-English language installations.
4. It's now possible to add WMI counters to Server after IP Address change.
5. Response time values are shown for the devices that are down.
6. You can successfully create tickets in SDP with AD Authentication.
7. CPU spike to 100% during archiving is fixed now.
8. Issue concerned with illegal thread state exception during failover has been resolved.
9. In Central Diagnostics, the data comparison doesn't work in HTTPS mode. This is fixed now.
10. Alarm sync and poll using TCP option in Enterprise Edition is working fine.
11. CSV/Network shallow discovery issues are fixed. It does not hang and the discovery happens even when there are two devices with same SNMP sysname.
12. You can now add process templates even if the credential name has & (xml chars) symbol.
13. IP Address is supported as a command line variable in custom scripts.
14. A Windows service is now restarted automatically when the service goes down.
15. Disk Utilization showing as 0 in certain Linux flavors, and in cases where there is permission denied warning message along with the command output is now working fine.
16. Read-only user cannot update the asset details now.
17. The issues of the Add Device button not working when the credential description contains large space, is fixed.

Issues Fixed: Build 9101

1. Data collection issue for CLI based monitors has been fixed
2. Unable to apply the license, if generated with unique id is resolved
3. Blank report generation issue for interface at-a-glance report in PDF format is now fixed.

Issues Fixed: Build 9100

1. NetFlow process now starts properly even if OpManager MSSQL port number is different.
2. Issue in saving the Syslog rules in non-English installation is now fixed.
3. To remove multiple monitors for devices, you can now remove them from the template and re-apply on the devices. This deletes the relevant monitors on the devices too.
4. NT Services ⁄ Services, when removed from the admin settings, still retained an entry in the ProfileCriteria table and resulted in the deleted service being listed in the Profile criteria page. Has been fixed.
5. Exchange servers list now shows VMwares, if they are hosted on one.
6. Process monitors are now added properly, even if there is a space in the credential name.
7. The ‘percentage’ character is now supported in the community field when configuring an SNMP credential.
8. Event Log alarm is now triggered correctly, even if source alone in configured in the Rule.
9. Windows services are now monitored correctly on Hyper-V devices.
10. Bulk delete of monitors from the device snapshot page, works fine now.
11. In addition to other alert variables, $eventType is supported in notification profiles.
12. Process Diagnostics is now shown correctly for the localhost.
13. While associating file, folder, and process templates, HyperV Devices are now listed.
14. In the Probe set up, Devices list will be empty when trying to add a custom WMI monitor is fixed.
15. In log a ticket, sub-category column not updated in SDP ticket is fixed.

**Issues Fixed: Build 9011**

1. SMS server setting configuration does not break now during an upgrade.
2. The custom TCP service monitors are now displayed properly after the upgrade.
3. An issue in creating statsdata–<date> (to store daily raw data) table at times, is now fixed.
4. Notification profiles related DB restoration issue has been fixed now.

**Issues Fixed: Build 9000**

1. Entity name dependency is removed for ESX hosts. Data collection happens even if the VMs are renamed.
2. VM Tools Version is updated in the ‘VMProperties’ table at the time of rediscovery.
3. VMware hosts are now properly discovered and shown even if there are no VMs.
4. The F5 loadbalancers are now discovered with the correct sysOID.
5. Accurate reports are generated now for disk forecast.
6. A device is now properly added and discovered even if an interface with the same IP is already added.
7. The managed/unmanaged state of devices is now correctly shown in the business views.
8. The parentnet is correctly updated even for unnumbered interfaces.
9. The interface IP address is properly updated during rediscovery.
10. Status polling for the interfaces is now done using the IP address.
11. The primary interface IP is properly updated when the device IP address changes.
12. Any changes to the interfaces are now correctly detected and updated during a device or network rediscovery.
13. When a network is deleted, all the children elements too are fully deleted.
14. Interface reports now show the full data without it getting truncated.
15. Interface polling and data collection now happens properly when interfaces are rediscovered when the agent/device is restarted.
16. Data collection happens normally even for monitors with the character “” in the monitor name.
17. Duplication of sub-interfaces during discovery, is fixed.
18. It is now possible to correctly discover an interface even if the IP address is already present for another interface.
19. SNMP V3 credential can now be associated to devices using the Quick Configuration Wizard (in the Probe).
20. Alarm details can be viewed fully in the RSS feed even if an alarm entity has the special character ‘#’.
21. Device displayed name is now updated with the IP address instead of an empty string if the query to sysName returns white space.
22. A category change to and from virtual device to domain controllers will now work without a glitch.
23. Process monitoring is now possible using cscript.
24. The custom WMI monitors added in the device templates are now properly associated to the devices during discovery.
25. Windows 2008 devices are discovered correctly classified as ‘2008”; it was classified as Windows 7 earlier!
26. Restrictions are included to prevent VMware templates getting wrongly applied to physical devices. Similarly, incorrect importing into
this category is also restricted to avoid unnecessary errors.

27. The VMware monitoring license related issues because of a change in node (module) name, is now fixed.

28. Few issues in the OpManager- ServiceDesk Plus integration, have been fixed.

Issues Fixed: Build 8812

1. The error ‘Unable to find ManagedObject’ in the URL Monitors, is now fixed.
2. In MSSQL Monitors, the issue of default instance specific monitors being shown instead of monitors from the named instance, is now fixed.
3. The issue of “Error” page being displayed when the 7/30 days reports is clicked, is now fixed. This happened when archiving was not started.
4. When the device is in “On Hold” or “On Maintenance” state the following monitors are also paused to avert false alarms (File and folder monitors and Syslog alarms)
5. Interface monitoring related issues have been fixed.
6. Issues in Process Diagnostics, like memory utilization not shown for Solaris devices, listing of only two top processes instead of 3 for CLI based monitors are fixed now.
7. A couple of issues with respect to SLA Widget viz. The changed skin not being displayed in the embedded widget and the link from the widget opening in the same window instead of a new one are fixed now.
8. Netflow Plugin related issues like updating mail server & proxy settings, SNMPv3 details have been fixed. In addition, Chinese language support has been extended for the plug-in.
9. The memory utilization data shown while doing a ‘test monitor’ was different from the collected value has been fixed.
10. High memory usage of java due to WMI based monitoring is fixed.
11. The reports of multiple instance monitors (for e.g. CPU) now shows instance name on top of each graph report.
12. Data collection related issues in CLI and SNMP monitors are now fixed.
13. Issues of notification profile not triggered at times, is fixed.
14. MS SQL database connection loss related issues is now fixed.
15. Log a ticket request is now raised in the Help desk even when the Device IP address is empty.
16. Devices are now added for discovery even if the credentials contain an empty space in any of the fields.
17. Issue of schedule report not getting triggered for “At-a-glance” report is fixed.

Issues Fixed: Build 8811

1. Performance / Interface data not getting collected at times, is resolved 
2. When accessing OpManager Web interface from IE 8, an alert is triggered stating that there is no support for the browser. This is now fixed.
3. Spelling mistake in the over-utilization alert is corrected.

Issues Fixed: Build 8810

1. SNMP socket timeout issue which resulted in SNMP data collection failures at times has been fixed.
2. An issue of the dashboard tab not displayed in the maps list view, is fixed now.
3. Notification not sent when certain monitors in Exchange 2007 or Exchange 2010 exceeded the threshold point has been fixed.
4. Downtime scheduler for business view with VoIP monitors is handled.
5. Thresholds related to non-numeric monitors would stop working once the service is restarted – This issue is fixed now.
6. Issue in monitoring non numeric monitors when associated from device templates is handled.
7. Support request with attachment can now be sent from the support page.
8. Issue in listing of ServiceDesk category and sub category details in “Log a ticket” notification profile for non-English environment is handled.
9. Issue when selecting and editing the monitors for Printer, UPSs and Virtual Devices from notification profile is handled.
10. Switch port mapping issues when one or more switches are discovered simultaneously, is handled now.
11. Failover configuration now includes "Retry" option to help customize based on your network.
12. Generic error messages in failover email notification have been replaced with precise messages to troubleshoot faster.
13. Deletion of SNMPv3 devices resulting in stray entries has been handled.
14. Traps sometimes fall under unsolicited category though the trap parsers are created. This issue has been addressed.
15. A dual entry with actual value and zero, leads to wrong monitoring data display. This has been fixed.
16. Partial monitors associated for an interface in certain situations has been handled.
17. When any monitored network device is restarted, a spike in data occurs. This leads to wrong standard metrics values like min, max or average. This issue has been addressed.
18. Real time monitoring often spikes up for 64 bit devices - This issue has been fixed.
19. Values configured in OpManager were not considered in real time monitoring for interfaces. This is now fixed.
20. Errors and Discards data show wrong values for some of the 64 bit devices. This is fixed now.
21. When we modify any 32 to 64 bit network device or vice versa, reports for all the interfaces will not be shown. This issue has been addressed.
22. Interface "display name" and "ifdescr" in the device page is merged for a clear view and to avoid confusion. Options to modify and retain the same are also made available.
23. IE8 and Chrome browser related issues are fixed.

**Issues Fixed: Build 8723**

**Interfaces**
1. Any change such as disabling a particular threshold configuration either from interface template or interface snap shot page was not effected earlier and alerts were triggered based on the default thresholds. This issue is now fixed.
2. There was an issue in the hourly archiving and daily archiving of interface data. This is fixed.
3. The interface/port display name was rendered blank if it had a special character as part of the display name. This is now fixed in Interface specific widgets, Interface–at–a–glance report, Interface template page.

**Reports**
1. The resource utilization graph in the at–a–glance report now plots the graph correctly.
2. The traffic reports when exported to excel format, reflected wrong units. It is now fixed to show the correct units.
3. Reports with Graphs & Values (Traffic reports etc) does not appear when it is converted to PDF format is now corrected.
4. The interface displayname was earlier trimmed in reports. Now we display the full name in the reports and also during mouse–over.
5. The excel reports for Total Bytes transferred, shows correct data for 7 / 30 days.
6. At a glance report of Device, when exported to PDF format, now shows the proper interface details.
7. All interface reports when exported to excel format, show the appropriate units.
Maps
1. Interface symbols were not shown in the map if the interface display name contains special characters when we rediscover the interfaces. This is fixed.
2. The tooltip for interfaces is now shown properly in the Router and Switch maps.
3. A space in the Custom Infrastructure view name resulting in the imports/additions failing. This is now fixed.
4. Issue of deleting an infrastructure view when the list view is set as default is fixed.

Widgets
1. A couple of event-handling scenarios led to showing NULL in the Event summary in the main dashboard. This is now fixed.

Custom WMI Monitoring
1. The issue of not being able to add custom WMI monitors when the wmidatatype is not set, is now fixed.
2. No data getting collected for Custom WMI monitors after device discovery, if the monitors are associated to a particular device template.

Others
1. Service Desk Integration – Any special character in the service desk parameters such as technician, category etc. leads to failure. Now we have fixed to accommodate all special characters.
2. SMS notifications are split up into messages of a maximum of 125 characters per message. You can now configure whether or not to split up the message. The configuration can be made in smsserver.conf file.
3. Discovery failing in Google chrome browser is fixed.
4. Improved the performance of Opmanager webclient especially the device snapshot and dashboard pages.
5. Data collection at times getting stopped due to WMI and CLI monitors is fixed.
6. Issue of unable to add a new custom event log rule, if all the rules are deleted is fixed.
7. Event specific tables are cleaned up properly now.
8. NCM plugin details shown in About page now.
9. Issue of editing the snmp credentials when the credential name contains space, is fixed.
10. False alerts sometimes raised for windows services, process monitors is fixed.
11. Unable to initiate rediscovery of a device, if there are more number of credentials defined is fixed.
12. Issue of interface name not displayed properly during business view creation and edition is resolved.
13. Issue of duplicate entries in wrapper conf file when database configuration is invoked, is fixed.

Issues Fixed: Build 8722

Startup
1. Issue of primary and secondary running as ‘active’ at the same time, is resolved
2. OpManager upgrades are effected smoothly.
3. Mysql database tables getting corrupted at times, if fixed during server start up.
4. OpManager plugins are not be shown for business view users.

Discovery
1. Issue of device not getting added at times, is fixed.
2. CIDR Discovery related issues are fixed.
3. Network view is grayed out even when there are some active devices added, is fixed.
4. CLI Credentials are listed correctly in Add Server Page.
5. Special characters in SNMP community string and WMI Credentials are supported now.
6. Device Type is now set correctly even if the device is removed and rediscovered again.
7. Interfaces are now discovered/rediscovered properly even if the interface count exceeds 1000.

Maps
1. Issue of error page showing up in some scenarios when viewing the Traffic Map, is fixed.
2. Layer 2 maps now show proper color-coding to reflect the Links status.
3. Layer 2 mapping is shown properly even for routers that have sub-interfaces.
4. Issue of OpManager getting crashed at times, due to large number of iprouting entries in BGP router, is fixed.
5. The list view showing duplicate entries for devices with multiple CPU instances, is fixed.
6. Interface/Port symbol is correctly shown in the corresponding map view page.
7. Issue of being unable to access a business view, is now fixed.
8. Custom business view images are included during backup and restoration.

Alarms
1. Alarms are properly generated when the consecutive failure count is configured in the URL monitors.
2. Threshold alarms are now properly generated even if the message contains the $ symbol.
3. Threshold alarms are properly generated for the WMI based monitors.
4. A read-only user for business views can now view alerts only for the devices in that view.
5. Threshold violation alerts not generated if threshold.conf file is corrupted, is fixed now.
6. OpManager no longer crashes when viewing the devices alarms or unsolicited traps!
7. Issue of SMS alerts not sent at times, is fixed.
8. Issue of device down alert not generated, if already an alert of same severity is present, is fixed.

Monitors
1. Custom WMI monitors can now have same monitor name, if the data is polled using different WMI Class.
2. WMI monitors are added correctly even if the monitor name exceeds 255 characters.
3. The issue of Real Time Monitors not shown if the device has had any WMI specific errors, is now fixed.
4. Used disk space monitor (public / mail store) is now listed correctly for Exchange 2000/2003.
5. You can add Exchange Server - store information details even if more than 10 - 15 stores are configured.
6. The calculation of SNMP-based CPU utilization was formerly incorrect. It is fixed to reflect the correct utilization.
7. When both, SNMP and WMI Process Monitors are added, polling is now done for both the monitors.
8. CLI credential options are removed for network devices.

Data Collection
1. Proper data collection now happens for Cisco Temperature monitor.
2. Data collection stops at times in OpManager 64 bit version. This issue is fixed.
3. Data collection is smooth even if monitored partitions have space in their names.
4. Data archiving was not done due to error in dynamic table creation. This is fixed.
5. Interface data is collected properly even if ifspeed is not configured.
6. Device status is updated correctly irrespective of the dependency configuration.
7. Switch Port Mapper data was not shown at times because of snmp timeout. This is fixed.
8. Issue of CLI based CPU, Memory and Disk utilization data not shown for different flavors of Linux / Solaris / AIX devices is rectified now.

Reports
1. Custom Reports display the resource monitors protocol-wise if all the supported protocol monitors are associated to the device.
2. The sorting in the 'All servers disk usage report' is based on the device names instead of disk usage.
3. Windows Service Monitor Availability and Process Monitor Availability reports are rendered properly when exported to PDF or XLS format.
4. Scheduled reports and custom infrastructure reports can now have a space in the report name. Example: December Report.
5. You can edit the custom report for virtual devices.

Others
1. Modifying or assigning a Downtime schedule to an existing or new business view is now possible.
2. Newly added business view not being displayed when editing the Downtime scheduler is fixed now.
3. You can edit and save the changes for Down Services and Down Devices widgets.

Issues Fixed: Build 8721

1. A couple of issues in daily and weekly schedule in Downtime Scheduler when selecting a daytime are fixed.

Notification Profiles
1. The Advanced button in the notification profiles criteria page now works correctly
2. URL Monitors are now listed in the notification criteria when the devices are categorized under Custom Category
3. For servers running Windows applications, notification is triggered for threshold violation only if the parameters in MSSQL/Exchange/
   Domain Controller monitors are explicitly selected from the criteria even if the condition If Any Threshold value is configured is selected

Reports
1. Availability reports are now approximated to 3 decimal places
2. When exporting a monitor with multiple instances to Excel format, all the instances are now correctly exported
3. Custom Report were not rendered properly when the instance name exceeded a particular length. This is now fixed
4. Issue of ‘No Data’ shown in Total Bytes Transferred report, if scheduled, is fixed

VMware devices
1. You can choose to monitor only the required VMs on a host. You can remove or add the instances to be monitored from the host snapshot
   page
2. Discovery related issues have been fixed
3. Following few issues in the Back Up/ Restoration process are fixed:
   4. Build Number Check is included to address incompatibility issues
   5. Users Permission Check is included and an alert is triggered when the user does not have administrator privilege
   6. After the backup and restoration, the device details are now correctly displayed including the custom fields
   7. The HTTPS mode related backup/ restoration issues are fixed

Maps
1. Fixed no show of data in the list view of a business view when the page size is changed
2. Dashboard views shows no data for Network Maps and Business Views. This is fixed

Others
1. When an alarm is deleted from the alarm details page, the page is redirected to the device snapshot page after deletion
2. The authentication encryption issue in NTLM URL monitors is fixed and the data is collected properly
3. When an IPAddress is changed for a device the other polling parameters are now correctly updated with the changed IP and data
   collection is uninterrupted
4. The page loading issue when the interface/port count exceeds 500 is fixed using smaller icons
5. The resource reports in the list view maps earlier showed the average value. It is now fixed to show the data collected in the latest poll.
6. The alarm escalation, when applied to a business view, now shows the devices filtered based on category within the business view.
7. OpManager webclient shortcut (Start -> All programs -> ManageEngine OpManager -> OpManager Web Client) is invoked correctly in the HTTPS mode.
8. OpManager now accepts a blank password when installing with MSSQL database server.
9. An anti virus check is done during OpManager installation.
10. The DomainController snapshot page is enhanced to reflect proper device information if the Domain Controller license is expired.
11. The issue of device not showing up when searched for, is now fixed.
12. The issue of reports not showing any data at times when Database Maintenance is configured is now fixed.
13. The display and alignment of Widgets in the GUI due to the length of the Widget name is now fixed.
14. Trouble Ticket details are now properly updated when creating a 'Log a Ticket' profile.
15. You can now associate Windows monitors to devices in a custom category inheriting server properties.
16. An occasional error when adding the ‘Information Store box’ monitor on an Exchange server is now fixed.

---

**Issues Fixed: Build 8720**

2. Devices falling under a downtime scheduler that is configured to run ‘once’, was getting unmanaged on upgrade to build 8700. This happened only if OpManager had MS SQL as the database.
3. Upgrading to build 8700, disabled "Read only" users to see the “Alarm Notes”; This issue has been fixed.

---

**Issues Fixed: Build 8052**

1. The URL monitors falling in a Downtime Schedule, are managed and monitored correctly once the schedule is complete.
2. When trying to apply a hotfix or upgrade pack, an alert message is displayed to stop OpManager server if it is found running.
3. An alert message is shown during installation if the user does not have administrator privilege or full control permission for the OpManager installation directory.
4. The issue of the progress bar in the UpdateManager stopping at 98% during upgrade, is fixed.
5. Netflow details are now correctly displayed in the OpManager Firewall Snapshot page.
6. There are no false downtime alerts for devices now.
7. The Jump To link to jump from OpManager to ServiceDesk Plus, now logs you into ServiceDesk Plus smoothly.
8. Appropriate message is shown to create a notification profile without any special characters in the profile name.
9. Duplicate entries were found when collecting data for Interfaces. This is fixed.
10. The option to rediscover interfaces now discovers even the interfaces with holes and lists all the interfaces even if admin/operation status is not implemented in the agent.
11. Issue of traffic exceeding inspeed / out speed is resolved.
12. There was an error in calculating the 95th Percentile value. This is now fixed.
13. You can now configure a notification Profile with syslog / event log rule as criteria.
14. RSS Feed option is not available for users with ‘Read-Only’ privilege.
15. You can now schedule reports even for the resources that have a special character in the SNMP OID.
16. The latest log files (the last two days) are zipped in the Support Information File (SIF) if the size of the entire SIF exceeds 50 MB.
17. Upload of MIBs (present under other directories) using OpManager WebClient is now possible.
18. Windows 2008 devices and Windows Vista devices are now classified correctly using WMI.
19. The status of the URL monitors are now properly updated.
**Issues Fixed: Build 8051**

1. Devices are added more quickly for discovery.
2. Upgrade to the latest versions in Linux without glitches. Few users had trouble upgrading to 8050.
3. Improved data collection for the WMI-based monitors in the 64 bit OS installation.
4. Improved helpdesk integration by fetching the correct information from ServiceDesk Plus.
5. Correct time-range is displayed in the Availability dashboard now.
6. Smooth Alarm escalation configuration after fixing the issues reported.

**Issues Fixed: Build 8050**

1. MySQL connection loss issue in build 8030 is fixed
2. Migration issue for customer using MS SQL backend in build 8030 and 8040 releases has been fixed
3. Incorrect data shown for Domain controller CPU Utilization is fixed
4. Custom configured dials disappearing issue has been fixed

**Issues Fixed: Build 8025**

1. Device snap shot page now shows current hour availability details instead of hourly average
2. The MS SQL Dashboard now includes Cache Hit Ratio data for SQL 2005
3. Included new options to exclude monitoring Exchange Public/ Mail store location while adding Exchange monitors
4. Issue on data collection when WMI credentials contain spaces is fixed
5. Intermittent Test Credentials failure is fixed
6. Includes performance enhancements with respect to Windows Event Log monitoring and Events data reports

**Issues Fixed: Build 8024**

1. Intermittent device polling issue is fixed
2. Options to rediscover is disabled for read only users
3. Notification not sent for Threshold violation for some MSSQL/ Exchange/ Domain Controllers monitors are resolved
4. Notification not sent if the Windows service name contains underscore is fixed
5. Unable to view the MSSQL - database instance name, in Weekly/ Monthly reports is resolved
6. Service Level Management Dashboards add on details will be shown in the About Page
7. Option to drop all the events information added
8. Threshold rearm for process monitors fixed
9. Multiple Real-time widget graphs loading issue is fixed
10. Issue in My-sql backup for Non-English version, is resolved
11. Write Community not getting updated during device discovery issue is fixed.
Issues Fixed: Build 8022

1. Issue of status not getting updated for some devices is fixed
2. Fixed the problem in accessing of the Map page for a Read Only User with access to certain business view
3. Issue in showing incorrect source in trap forwarding scenario is resolved. The actual source device of the trap will be shown instead of the forwarded device
4. Error page in switch snap-shot page if Netflow Plugin is started along with OpManager is fixed
5. Issue of health report not shown if all the devices are in the ‘up’ state is fixed
6. Unable to configure 0 as threshold value for process monitors is fixed

Issues Fixed: Build 8021

1. No data on time range-based availability report fixed
2. Notification profile association for Windows NT services fixed
3. Domain Controller Performance data on at-a-glance reports are shown even if the device is moved to a custom category.
4. Error while adding performance monitor to a device, if moved to custom category is fixed
5. Included option to configure notification profile for devices in custom categories viz. Windows Services, Event-Log rules etc...
6. Sort Interfaces by “IfIndex” in the devices snapshot page
7. Custom/ Vendor specific monitors will be added only for managed interfaces
8. Threshold values not getting cleared issue for interface errors & discards is fixed
9. Memory Performance issue for VMware and CLI-based monitoring fixed
10. System idle process is removed from the list of Top 3 Processes
11. Fixed data not available issue from some NTML URLs
12. OpManager’s latest discussions are now shown in Support tab

Issues Fixed: Build 8020

1. Alarm Suppression: Suppress the alarms of a specific device for a pre-defined time interval.
2. Faster Backup and Restore utilities
3. I18N Internationalization issues fixed (For Japanese and Chinese Language)

Issues Fixed: Build 8007

1. The issue of Packet Loss data not being shown when OpManager is installed in Windows 2008/Vista is fixed
2. The issue of the Device not moving to the managed status when the downtime scheduler is completed has been fixed
3. The Utilization graph was not shown in the interface snapshot page even when the data was collected. This is fixed
4. Issue of status polling getting checked if one configures threshold settings from the interface template is fixed.
5. Issue of broken image or images not correctly shown for business views if multiple Business views widgets are created is fixed
6. Custom period data was not shown if one generates an availability report in pdf or excel format. This is fixed
7. Today’s data report used to be generated if one schedules 7days/30 days availability report. This has been fixed
8. Issue of scrambled reports when monitors of type multiple /multiple node is generated is fixed
9. In the Alarms tab, the issue of alarms not getting cleared or deleted if one selects all alarms is fixed
10. Issue of exchange version details not updated is fixed
11. Error "Database disconnected" has been fixed.
12. Unable to add used/free disk space monitors for Netware devices has been fixed

Issues Fixed: Build 8000

Fixed issues related to non-English versions of OpManager

Issues Fixed: Build 7205

1. Support for integrating Service Desk Plus with users imported from Active Directory.
2. Memory Utilization values now shown for ESX Server devices
3. Provision to configure ‘Attention’ severity alarms in Alarm Escalation
4. Deleted default categories were not listed when adding new category. This is fixed.
5. Fixed issues while rediscovering more than 1000 interfaces

Issues Fixed: Build 7204

1. Interface data not displaying in the device snapshot page even though the data is collected.
2. Unable to delete/clear an alarm if it contains any special character.
3. False alarms in windows services.
4. ESX Servers rediscovery issue.
5. Switch Port Mapper not listing all routers and switches.
6. Data not being shown in router availability and response time reports.
7. Issue in monitoring certain parameters, when the device is imported to the domain controller category.
8. Display name not shown in the device snapshot page, if the sysname is not configured.
10. Data display issue in the following reports

- Health Report - Not showing response time data.
- Availability reports for Business Views.
- Router health report - Not showing Cisco temperature data.
Issues Fixed: Build 7202

1. DB corruption issues.
2. IP address not getting updated for the devices in the DHCP environment.
3. Different values being shown for memory utilization when doing a test monitor and normal data collection.
4. Issue in monitoring VMware performance parameters.
5. Issue in loading traps from MIBs.
6. Issue in displaying utilization reports for last the last 7/30 days with MSSQL being the backend database.
7. Asset details not getting displayed (OpManager and ServiceDesk Plus integrated set-up) if the device is not scanned in ServiceDesk Plus.
8. Service monitors not getting properly associated when using the QCW.
10. Not displaying the interface traffic, if speed is not configured.

Issues Fixed: Build 7201

1. Unable to find the ManagedObject' encountering while getting interface data.
2. Email ID fields not accepting '.local' domain name.

Issues Fixed: Build 7200

1. Not displaying the device name in the Router interface reports.
2. Not displaying the customer's new email address when applying for a new license file in the Support Portal.
3. Firewalls Map - Details View is removed and Small View is made as default.
4. Issues in Switch Port Mapper
   a. Rediscovering a switch.
   b. Not displaying the switch port mappings wrt to the selected switch.
5. Mail option not working for some reports wrt interface.
6. Device Change Password screen - Throws error while submitting the page when device specific credential radio button is selected and no values are given for the same.
7. Some UI related and i18n issues.

Issues Fixed: Build 7100

1. Traffic data not getting collected for some devices when the agent does not respond to all the OIDs.
2. Shortcuts' status not getting propagated in business view.
3. Issue with URL match content filter.
4. Issue in changing the monitoring interval for router memory utilization.
5. Enhanced backup and restore functions.
7. Correct CPU usage and upgraded RAM not rediscovered for VMware.
8. Issue in encountering 'unable to find the device' message while searching a device.
10. CLI max connections reaching issue.
11. Alarm message getting truncated if the alarm message contains ‘$’ symbol is static portion of mail.
12. 7100 ppm not getting applied if the UPS category is removed.

**Important Note:** If you are using a build earlier to 6010, then kindly contact OpManager Support to upgrade
OpManager v12.3

Build No - 123044 - December 27, 2017

- General: 4141842 - Restoration failed when instance length exceeded 255 characters in StatsData table. This issue is now fixed.
- General: After expiry, the license can now be applied in the popup that is prompted once OpManager starts, instead of applying at the command prompt.
- General: After applying the license, the state of IPSLAs changed from "unmanaged" to "managed" previously. This issue is now fixed.
- General: Google map was not restored in the backup/restore process previously. This issue is now fixed.
- OpManager: When more than one probe existed, device count was displayed as zero in the probe's license activation page. This is fixed now.
- OpManager: Audit logs were not recorded for some APIs when the REST API was called from external sources. This issue is fixed now.

Build No - 123043 - December 22, 2017

- OpManager: Previously, APM plugin's visible area was too small. This is now moved to Main tabs area, for clearer visibility.
- OpManager: Previously, file monitoring failed when the devices' WMI Credential contained '. This has been fixed now.
- OpManager: For windows servers, adding free/used disk space WMI Monitors and device partition monitors failed due to the parsing problem of credentials with some specific special characters. This has been fixed.
- OpManager: When OpManager web client's local language was changed to Chinese, adding WAN RTT Monitor failed. This issue has been fixed now.
- OpManager: Previously, folder monitoring failed when the devices' WMI credential contained special characters like '*',|. This has been fixed now.
- OpManager: When a credential included the special character |, then script execution failed. This has been fixed now.
- OpManager: While adding new monitors from the device snapshot page, users were unable to receive monitors from the device. Also, the same issue was faced when WMI monitors were being added to Device Templates. This happened if the device had the special character ('') in its credential. This has been fixed now.
- OpManager: In the global Windows Services template page, previously the success message for add operation was displayed as Failure Message indicator. This issue is fixed now.
- OpManager: Displayed success message, even when the addition of WMI Partition Monitors to devices failed. This has been fixed now.
- OpManager: During workflow execution, the Check File/Folder Tasks failed due to the presence of some special characters in the password. This has been fixed now.
- OpManager: In the virtualization inventory page, filter selection for various tabs did not display the device list as per selection, when any operation like delete was done after the selection or when coming from a different page.
- OpManager: In Reports page, language localization was not done for Reports title and the description message for the default virtual server reports. This has been fixed now.
- OpManager: Under URL availability Widgets, the undefined page was displayed when selecting any URL Monitor, instead of displaying the URL snapshot page.
- OpManager: Previously, CLI Credentials were missing in Add VMware vCenter/ESX page specific to vCenter/ESX. This has been fixed now.
- OpManager: Under Data Maintenance page in Basic Settings, RunArchive button did not work when the Daily Archive option was selected. This has been fixed now.
Build No - 123037 - December 21, 2017

- OpManager: Alarm escalation was not working previously when a business view had been renamed. This issue is now fixed.
- OpManager: Previously under reports, the Audit function did not record workflow logs. This issue is fixed now.
- General: Previously when a user takes a tour of OpManager, the message "Move & Resize widgets by drag and drop" was displayed in English, irrespective of other language installations. This issue is now fixed.
- OpManager: Under reports, while creating a new report, "Inventory Reports" field displayed English characters irrespective of other language installations. This issue is now fixed to support I18N.
- OpManager: Under inventory, while generating reports for any monitor, the "search" field did not support I18N. This has been fixed now.
- OpManager: Under reports, the audit function did not record "schedule reports" logs. This issue is now fixed.

Build No - 123036 - December 19, 2017

- OpManager: While deleting an existing Windows service monitor from the device snapshot page, the list scrolls back to top and page navigation details were reset to default values, thus making the user reset the required view and proceed with deletion task. This issue has been fixed now.
- OpManager: Under Add Monitors from device snapshot pages, clicking anywhere on the grid view of the add list led to the de-selection of the selected items in the list. This has been fixed now.
- OpManager: Previously when the CCTV dashboard contained only one widget, the widget size was small. Now, this is displayed in the full-screen size.
- OpManager: Under the "widget Traffic Reports", the interface traffic graphs were displayed. When the user created a NOC view, the graphs in the traffic reports widget had the X-axis cut-off. This issue is now fixed.
- OpManager: Under widgets, users were unable to expand the 'Top N Conversation' widgets. This has been fixed now.
- OpManager: From the Virtualization Inventory view, users were unable to delete the Datastore Entity. This has been fixed now.
- OpManager: A link has been provided now to add virtual servers directly from the Virtualization Inventory Page.
- OpManager: For non-english Italian language servers, undefined results were displayed while fetching the Windows Services for "Add Windows Service" operation from the Device Snapshot page. This has been fixed now.
- OpManager: The discovery completion status specific alarm had no differentiation between the discovery from ESX Server or from vCenter. This has been fixed now.
- OpManager: For some upgraded setups, VM sprawl related dashboards and widgets were missing. This has been handled now.
- OpManager: Under Reports, if any of the CPU Utilization/Memory Utilization/Disk Utilization reports were empty, then the entire Health Reports were displayed as empty. This has been handled and fixed.
- OpManager: Xen data collection was not happening for Xen Servers with version 7 and above. This has been fixed now.
- OpManager: While configuring notification profiles, the IPSLA-specific Clear Alarm criteria based notification mail, was received even though the criteria was not selected. This has been fixed now.
- OpManager: Disk Monitors were not added to the local host monitored device when it contained multiple NICs. This has been fixed now.

Build No - 123035 - December 14, 2017

- NCM: Fixed the reporting options (violated rules only, compliant rules only or all rules) in scheduling compliance report for CSV format.
- NCM: Error message for expired time in 'Once' option for add schedule page.
• NCM: 4025368 - Fixed the EOL Report with no data in OpManager Probe server.
• NCM: 4244879 - Compliance validation issue in exact set criteria rule is fixed.
• NCM: Admin has to give annotation while authorizing/unauthorizing configchanges.
• NCM: System settings page is enabled for NCM.
• NCM: Filter by time option is provided in changes page.
• NCM: Aruba Controller backup failure issue is fixed.
• NCM: Now configure the number of parallel threads for SSH connection.

Build No - 123034 - December 12, 2017

• OpManager: While adding a custom category with existing name (case-insensitive), users were redirected to Empty Import Devices page. This has been fixed now.
• OpManager: Custom category devices were associated with incorrect polling interval. This issue is now fixed.
• OpManager: Previously, custom category was not set for Windows 7 and Windows 2008 devices. This issue is now fixed.
• OpManager: Interface Rx/Tx Traffic and Utilization data was unavailable in reports, when data exceeded big int character length (19 char) in MSSQL. This has been fixed now.
• OpManager: Under add category in API, users were allowed to create a blank or empty category name. This has been fixed now.
• OpManager: Users were unable to navigate to the device snapshot page from Interface bandwidth report. This issue is now fixed.
• OpManager: Under inventory, the Subnets list view page’s UI was broken previously. This has been fixed now.
• OpManager: Under snapshot page, Graphs icon and click on any graphs show tabular data is not sorted from the last polled value. This issue is now fixed.
• OpManager: Previously, operator users were able to edit outage history reason in device availability reports. This has been fixed now.
• OpManager: Previously under credentials page, the retype password field displayed plain text. This issue is fixed now.
• OpManager: Interface alarm messages were not displayed correctly when the message contained "<<>>" in UI. This issue is now fixed.
• OpManager: The SNMPv3 default port of the MIBBrowser is now changed to 161.
• OpManager: Previously users were unable to update IPv6 IP Address in Edit device details. This issue is now fixed.
• OpManager: Interface graphs can now scale automatically to Mbps or Gbps based on the data.
• OpManager: Previously in real-time traffic widget, the Y axis was not scaled automatically. This issue is now fixed.

Build No - 123033 - December 11, 2017

• NetFlow: Added SNMP support for Wireless LAN Controllers to fetch names of Access Points.
• NetFlow: Client MAC based filter is added newly in Inventory and Snapshot under WLC.
• NetFlow: Widget for Client MAC traffic is added in snapshot view of Client IP.
• NetFlow: Overall Report for IP Groups is added in schedule reports.
• NetFlow: Edit option in Alert profile has been fixed.
• NetFlow: Unwanted vectorwise DB operation is removed to avoid loss of raw data.
• NetFlow: Attacks information is now can be viewed for selected device and interface.
• NetFlow: Issue in attacks search filter has been fixed.
• NetFlow: Option to select Ethernet card name is available in DPI settings.
• NetFlow: Promiscuous mode of ethernet cards has been enabled by default for DPI.
Build No - 123032 - December 6, 2017

- OpUtils: Included actions like add, delete, rename group in IPAM tree under Inventory.
- OpUtils: Option to add/edit subnet location, VLAN name has been provided while modifying a subnet.
- OpUtils: A "Check Now" button is included while adding a switch in the SPM page to verify its presence.
- OpUtils: Under “Switch Ports by ifType” Reports, the IF TYPE was missing for few switch ports previously. This is now fixed
- OpUtils: "M" character had been appending in the total device count in the SPM email alert. This is now fixed
- OpUtils: Previously, WMI query tool was not working due to the presence of "" in the Name field. This issue is now fixed.
- OpUtils: Under Settings, Active Directory scanning was not working previously, if the password contained special characters. This issue is now fixed.
- OpUtils: Under Add Subnet option, the Redirect link leading to sample csv format was not working. The redirect link is now replaced with a sample csv file.
- OpUtils: In the Mac address resolver under Settings, the error message occurring when SNMP community field was not filled, is now deleted.
- OpUtils: AD Status Summary in Dashboard & IP Addresses was not updated after completing the subnet scan. This issue is now fixed.

Build No - 123031 - December 1, 2017

Issues Fixed

- The Refresh Datastore Workflow task execution displayed success message even when the execution failed. This issue has been fixed.
- If there was any change in Canonical Path Names for the LUN Multipath associated to ESX Servers, then rediscovery of vCenter failed. This has been fixed now.
- AMS Expiry notification was not shown to users irrespective of their version. This has been fixed now.
- AppManager plugin data was not displayed to Read Only users even though they had access to all the devices. This issue has been fixed to display APM Plugin data to all the non business view users.
- NT Services that has comma (,) in their Service Name or Display Names were not added in OpManager. This has been fixed now.

Enhancement

- Once a VMware Datastore was deleted or had stopped monitoring in OpManager, there was no option to re-start monitoring. This option is included now.

Build No - 123030 - November 28, 2017

- OpManager will now integrate with SDP through rest APIs. OpManager build 123030 and above and ServiceDesk Plus build 9329 and above will support API-based integration. However, old method of integration will also be available to support customers in older version.
Build No - 123029 - November 24, 2017

- NetFlow: Resource type and resource category are set by default to Top N Problems widget in dashboard.
- NetFlow: Default name will get changed based on the category for Top N problem widget in dashboard.
- NetFlow: The mismatch in Row Count for the top source, destination, conversation, application (L4,L7) has been fixed now.
- NetFlow: Direction issue in Dashboard from network-based (Source network, Destination network) widget has been fixed.
- NetFlow: A new column for DSCP has been added to top conversation widget in dashboard.
- NetFlow: Added an option to redirect from meraki device in device summary widget.
- NetFlow: Redirecting to a particular snapshot with the configured timeframe is proper now and has been fixed.
- NetFlow: Redirecting to snapshot from WLC widgets is proper now and has been fixed.
- NetFlow: WAAS Total Volume graph plotting and time zone is proper now and has been fixed.
- NetFlow: TimeZone issue for Line graph has been fixed now.
- NetFlow: Updating interface name when the speed is 0 is possible now.
- NetFlow: Individual Graph feature across product is proper now and has been fixed.
- NetFlow: Device traffic graph data in device Snapshot page showing incorrect value has been fixed now.
- NetFlow: Error in displaying time across product when the user and browser timezone differs has been fixed.
- NetFlow: Drill down conversation in QoS shows only 50 records (pagination) has been fixed now.
- NetFlow: "Invalid Device selected" displayed in Raw Data Settings while clicking on Save button has been fixed now.
- NetFlow: Raw data was getting duplicated in the database. Now it has been fixed.

Build No - 123028 - November 22, 2017

- OpManager: In the device snapshot page, Response Time and Packet loss report was not working when the time period exceeded 30 days. This issue is now fixed.
- OpManager: In the device snapshot page, a new icon has been added to navigate to Google Map. This icon is displayed only if the device has been already added to the map.
- OpManager: Under Google Map, the "Filter by Type" option in Google Map, did not list any device types in Central. This issue is now fixed.
- OpManager: Under Google Map, the unmanaged state of the severity icon was displayed as undefined. This is fixed now.
- OpManager: In Google Map, the map position will be retained if user redirects to other pages.

Build No - 123027 - November 21, 2017

Enhancements:
- The 'Automatic/On-click/No lookup' options of Resolve DNS in global settings synchronized for all widgets
- Two more SMS service Clickatell and AppSMS supported to send SMS notifications for 'Alarms, Configuration changes, and Availability Alerts'

Issues Fixed:
- 123396 - If dashboard data is with "," in its drilldown page data is shown without ",". The issue is resolved to display it properly
- 121669 - When Traffic Conversation Table in Interface drilldown page is expanded, it was displaying only top 10 rows. Issue fixed to display
• In CCTV view, Operator can view unauthorized device's Live Traffic. Issue is fixed by hiding it
• In one of the 'Proxy Reports', when Search icon is clicked, empty page was displayed. Issue fixed to display appropriate page
• 'No Data' message not internationalized in some graphs, issue fixed by internationalizing it.
• In dashboard traffic and security statistics report, when Search icon is clicked, empty page was displayed. Issue fixed to display appropriate page
• 'In' & 'Out' legends in Device Summary graph were not internationalized, issue fixed by internationalizing it.
• Fixed memory handling issue, during user association and manual IP mapping when device is deleted
• Fixed an issue in reimport option of manual IP mapping
• Fixed issues in FWA Availability alert page UI and Disable notification link in the alert notification mail
• Fixed an issue in script error handling, when a schedule is added for Compliance report without selecting any type of standards
• In standard compliance reports, if clicked to drill down the report, the table values are not displayed. Fixed the issue for table value display
• User with '' character could not be added, for 'End Users' reports. Fixed the issue to add user
• There was an UI alignment issue in NetFlow widget populated in OpManager's End Users report. Fixed the issue to align the UI
• In the dashboard, snapshot view of Cloud Users report, fixed the issue of missing 'Expand View' icon
• Fixed the issue in Disable notification option of the change management alert notification mail
• When TLS option was configured in Mail Server settings, mail notifications for alerts were not sent. Fixed the issue to send mails
• Fixed the misalignment issue in Policy Overview report table. This was for MS SQL database
• When a new report type is added with the existing name, 'Success' message is displayed. Fixed the issue to display 'Failed' message
• Fixed the issue to populate rule details of SRX devices, when the configuration file is not having network object details
• In the 'Unused Rules' report of 'Rule Management', the resource criteria is not applied properly. Fixed the issue to apply the resource criteria properly
• In FWA, log entries for unsuccessful console login attempt on Cisco ASA devices are not there. Fixed the issue to get entries
• Issue, in SonicWALL log parsing for protocol, is fixed
• All the IPs are not getting resolved into names, when 'Resolve DNS' is set to 'Automatic'. Fixed the issue to resolve all IPs
• When scheduled PDF report page count is more than 100, the total page count in PDF footer was not proper. Fixed the issue for proper page count
• Fixed the out of memory error generated when change management report was accessed

Build No - 123026 - November 17, 2017

• An option to associate URL templates to multiple devices from the URL template list has been included.
• An option to view the list of URLs monitors associated to devices has been included in the URL monitors page. Select the Device Specific URLs dropdown to view these monitors.

Build No - 123025 - November 16, 2017

• General: 4139091- User Management - Some users were unable to login the web client after upgrading to the latest service pack. This issue has been now fixed.
• General: 3811324 - When user count exceeded 100, issues were encountered while logging in. This has been fixed now.
• OpManager: Under Notification Profile, email notifications were received as html content, even when plain text format was chosen. This
issue is now fixed.

• OpManager: Under Notification Profile, $eventType was not passed in the notification message. This issue is fixed now.
• OpManager: 4099988 - Under notification profile, when html tags were added in the message field, the profile was not saved. This has been fixed now.
• OpManager: 4133567- Under Send Email Notification Profile, while adding special characters in the subject field, the issue where the profile was saved without retaining the special characters or showed errors, has been fixed now.

Build No - 123024 - November 14, 2017

• Under CCTV view, BusinessView did not fit to screen previously. This issue is now fixed.
• Previously, in the device snapshot page, even though the availability of a device was 96%, the dial display was in red color. This issue is now fixed.
• Under Heatmap, device details were not displayed on mouse-over. This issue is now fixed.
• Interface graphs were plotted incorrectly (Graph stack issue, for example, if interface tx is 8 Mbps & Rx is 6 Mbps then we are plotting the graph for 14 Mbps). This has been fixed now.
• The background image was not displayed properly in BusinessViews widget while accessing more than one widget. This issue is now fixed.
• Interface snapshot page, Under Graphs icon -> click on Interface summary graphs -> 95th percentile line was displayed incorrectly. This has been fixed now.
• In business views, LED icons now have a transparent shape instead of a square one.
• 95th percentile min, max, and avg values were missing in the Interface snapshot page. This issue is now fixed.

Build No - 123023 - November 13, 2017

• NCM: Option to clone a device template is provided in GUI.
• NCM: Provided an option to delete existing sysOID in GUI.
• NCM: Schedule actions are removed from device Inventory multi-select actions list and is now added under a new group 'Schedule'.
• NCM: Option to schedule configlets is provided in Configlets list page.
• NCM: 3942442 - Option to retry backup for backup failed devices.
• NCM: 4101225 - Option to add DNS name in reports for application URL instead of IP Address.
• NCM: 4150507 - Search option is provided to select the device in the multi-select box in GUI.
• NCM: Uniform color coding for authorization & unauthorization across the product.
• NCM: Option to edit import devices and values option is provided in the "Configlet Schedule" page.
• NCM: Configuration Change Trend, Compliance Report, Device Audit Report are now provided on the device snapshot page.

Build No - 123022 - November 9, 2017

• OpManager: 3985963 - Multiple Notification Profiles can now be selected and deleted in bulk.
• OpManager: While scheduling a notification profile, the "Do not trigger" option that prevents unnecessary notifications after acknowledging the alarm, can be validated only if the time is set for Delayed Trigger and Trigger Interval.
• OpManager: When configuring notifications from Alarms, the tab that allows the user to select the notification type, was missing previously. This has been fixed now.
• OpManager: Under Device Snapshot page, the notification profiles that have already been associated with the device will be marked as selected, while listing all available notification profiles for association.
• OpManager: A clear error message in the client will be displayed, when a user tries to associate notification profiles without selecting any.
• OpManager: While sending a test mail from the secondary mail server, the primary server message was received, instead of the secondary
server message. This has been fixed now.

- OpManager: While adding a new notification profile, configurations of previously added Notification Profile were shown. This issue has been fixed now.
- OpManager: Under SDP Add-on, the "Auto Sync assets" functionality now works seamlessly.

Build No - 123021 - November 8, 2017

- OpManager: When a report created from report builder or snapshot page, is exported to PDF, the device name or the report itself is not properly displayed. This issue has been fixed.
- OpManager: All the data in a report is printed on a single page and when the same is exported to PDF it is improper to view. Now, this issue has been fixed by printing the report in multiple pages for a better view.
- OpManager: Issue in creating a report when it contains a special character. This has been fixed.
- OpManager: Issue in exporting partition details report to PDF. This has been fixed.
- OpManager: Links available in the report for Top N Errors and Discards for device and interface fail to redirect correctly. This issue has been fixed.

(Note: Builds 123016 to 123020 are reserved for internal purpose.)

Build No - 123015 - Nov 2, 2017

- OpManager: For default virtual inventory reports in virtual server reports page, Schedule Reports and Send Mail option were not working and was sending blank attachment in the mail. This issue has been fixed now.
- OpManager: For default virtual inventory reports in virtual server reports page, Export as PDF/Excel options were not working. This has been fixed now.
- OpManager: On editing virtual server reports, the Period and Time Window fields were not shown. This has been fixed now.
- OpManager: VMware discover/rediscovery was getting failed when HostPortGroup is duplicated and both the duplicated HostPortGroups are mapped to the same VM/Host. This issue has been fixed now.
- OpManager: If more than one proper credentials for vCenter were added in OpManager, with Auto-VM discovery enabled for one and disabled for the other, then after some time the mapped credential to vCenter/ESX in OpManager was automatically getting changed. This has been fixed now.
- OpManager: The periodic update of VMware vCenter/ESX Inventory in OpManager was not getting properly updated as per configured Update Interval parameter during vCenter/ESX discovery. This has been fixed now.

Build No - 123014 - October 31, 2017

- NetFlow: The issue with export to CSV in inventory has been fixed and enhanced.
- NetFlow: Added an option to export to CSV for NetFlow Group Configurations. This option is added under "Group Settings".

Build No - 123013 - October 27, 2017

- OpManager: While associating "Remote Script Templates", OpManager listed all devices instead of displaying only CLI supported devices. This issue has been fixed now.
- OpManager: IE browser can now support Japanese Characters in Script Templates.
- OpManager: On adding a Syslog rule, The Rearm Match Text was not saved previously. This issue has been fixed now.
OpManager: The "Test Script" button is now removed from Script Templates for the Central Server, as the scripts are executed only at the probe. These scripts can be tested at the probe.

OpManager: When a syslog rule was created at the central server, the same was not synced with the probe. This issue is now fixed.

OpManager: 4190299 - After adding APM plugin to OpManager, APM monitors were not displayed in the device snapshot page. This has been fixed now.

OpManager: 4244060 - Mail Server settings were not be saved, when "" was present in UserName field. This issue is fixed now.

Build No - 123012 - October 26, 2017

- OpManager: On editing the threshold of any performance monitors from the device snapshot page, the consecutive times allowed "0" to be given as input. This has been fixed now.
- OpManager: Few build versions of HyperV2016 were not categorized under "HyperV" due to mismatch in the criteria of HyperV related WMI (Win32_OperatingSystem) class. This issue is now fixed.
- OpManager: Too many unnecessary discovery status popups were displayed while receiving VM events from vCenter environment. This led to slowness due to frequently scheduling inventory updates in OpManager. This has been fixed now.
- OpManager: While editing a process monitor from the device snapshot page, when the instance count criteria matched "=" and if the threshold value was set to "0", the Rearm value was automatically set to "0". This issue is now fixed.

Build No - 123011 - October 24, 2017

- Under VLAN snapshot page, the interface list was not displayed previously. This issue is now fixed.
- The privilege of deleting interfaces from device snapshot page is now restricted to only admin users.
- When navigating from Configuration tab to Monitoring tab in Settings, the Add/Associate buttons in the Performance Monitors page were hidden. This issue is now fixed.
- In the device snapshot page, Interface grid data was displayed even after deleting that particular interface. This issue is now fixed.
- Under Basic Settings, when adding a new category, if the name contained other language characters users were unable to delete the custom category. This issue is now fixed.

Build No - 123010 - October 20, 2017

- OpManager: While adding Real-Time Traffic widget from the dashboard, y-axis will now scale to bps, Kbps, Mbps, Gbps automatically based on the data.

Build No - 123009 - October 16, 2017

- NetFlow: The issue with IPv4 address based criteria in Alert Profiles has been fixed for V9/IPFIX/SFlow flow format.
- NetFlow: The issue with Raw Data memory storage when toggle between raw ON and OFF for has been fixed for all databases i.e HighPerf, PGSQL and MS SQL.
• NetFlow: Interface group name was missing in the PDF generated through Schedule Reports. Now, this has been fixed.
• NetFlow: Application drill down & conversation reports from Inventory>>Interface has now mapped required Src and Dst port for application mapping when data fetched from raw data. This issue with port and application mapping has been fixed.
• NetFlow: Now there is an option to send an SMS alert to multiple mobile numbers from "Alert Profiles" tab in Settings.

Build No - 123008 - October 12, 2017

• Firewall: 4180774 -- Device rule configuration using SCP protocol was not functioning in build 12300. Now, this issue is fixed.
• Firewall: 124197 -- Sometimes, SRX marked as unsupported device, if Firewall Analyzer receives unsupported log as the very first record. Now, wait time is added to check more received logs to avoid unparsed error.
• Firewall: 120221 -- Previously, there was no option to view the selected time-period of each dashboard widgets. Now, sub-header details will be shown in each widget with device information along with time-period applied.
• Firewall: 122695 -- System performance and custom dashboard views were missing when logged in for the first time. Now the issue is fixed and the user can view both. Firewall: 122785 -- Inventory Interface snapshot traffic conversation report's last row was not shown properly in UI. Now the issue is fixed and the report loads the data properly.
• Firewall: 122055 -- Graph units option provided in the Inventory LiveReports page was not in proper sequence. This issue is fixed and the units are now shown in proper order like kbps, Mbps, and Gbps.
• Firewall: 123774 -- When the user selects all predefined reports while creating a report profile, received PDF shows all the reports name on the home page without proper alignment. Now, Alert Message added for Report Profile reports selection.
• Firewall: 122683 -- Editing widget "Top N Hosts by Traffic" and selecting Protocol under category makes the widget to show data of protocol-group by traffic. Now, the issue is fixed by showing Protocol-Group instead of Protocol in dashboard widget - edit section.
• Firewall: 123865 -- 'Live Syslog Viewer' status shown as 'undefined' when we do a continuous refresh. Now the status message handling issue is fixed on the server side to show proper status in the UI for a continuous refresh.
• Firewall: 124244 -- Increased the data dumb volume from base table 'Firewall Records' to next level data table for database performance increase.
• NCM: 4094309 -- SSH Vulnerability #1: The SSH server is configured to support Cipher Block Chaining (CBC) encryption, which may allow an attacker to recover plaintext message from the ciphertext. We've now fixed this by providing an option to disable the CBC mode encryption using system property.
• NCM: 4094309 -- SSH Vulnerability #2: The remote server is configured to allow MD5 and 96-bit MAC algorithms, both of which are weak algorithms. We have now fixed this by providing the option to disable these algorithms using system property.
• NCM: 1584237 -- Configuration Analysis and Security Audit Reports are now supported for device templates which were not supported in earlier versions.

Build No - 123007 - October 11, 2017

• OpManager: IPSLA monitors were not getting created when the source device does not contain the same notification profiles available in the WAN Threshold template. Now, this has been fixed.
• OpManager: When two or more hop-by-hop widgets are present in one single dashboard, the widgets either collapse or get misaligned. Now, this issues has been fixed.
• OpManager: Search was not working for "Path" field in IPSLA monitor's inventory page. When searched for values that were present in the middle of a name were not pulled up in the search. Now, this issue has been fixed. Also, now the monitor name is shown upon mouse-hover.
• OpManager: When editing a hop-by-hop widget, instead of highlighting the respective monitor's name, the one that is listed first was selected. Now, this issue has been fixed and the respective monitor name is selected irrespective of the order.
• OpManager: I18N has been done for the word “Get” in Add URL template page by mistake. Now we have removed I18N for the word “Get” because it's a technical term.
OpManager: I18N was not done for the word "Edit" in process monitor page. Now it's been done.

Build No - 123006 - October 9, 2017

- OpManager: 114501/124174 - Option to disable/enable the pop-up that indicates the discovery status.
- OpManager: 122367 - Virtualization related monitors were able to be associated with non-virtual devices also. This issue has been fixed.
- OpManager: 124545 - In the dashboards black color band, "NetFlow" and "transferred" has been misspelled as "Netflow" and "transfered". This has been corrected.
- OpManager: 122340 - Option to configure the polling interval for custom WMI performance monitors was overlooked and because of this, the polling interval time was set to '0' by default. Now we have provided the option to enter the polling interval.
- OpManager: 122294 - When adding a custom SNMP monitor, the "Units" field was still getting displayed even after changing the "Functional exp" filed value to string ("Numeric to string"). This is an issue has been fixed. Now if the value is changed to string, the "Units" field will be hidden.

Build No - 123005 - October 6, 2017

- Under the inventory tab for IP address management, a read-only tree view has been added for easy classification of subnets.
- Under then inventory tab for IP address management, when IP addresses are filtered by the OS category "Unknown", the list was not loaded. This issue has been fixed.
- Under IP address management, the page loading time for showing the inventory of IP Address, Ports, and Rogue has been improved.
- The changes done in General settings under OpUtils->SPM were not saved in the database. This issue has been fixed.
- When a device that doesn't support the Bridge-MIB was added for IP address and switch port management, no error message was displayed. Now, if such devices are added, an error message will be shown in the UI.

Build No - 123004 - October 3, 2017

- CCTV crash occurring while resizing the widgets has been fixed.
- Option to Add/Remove widgets included in default dashboards.
- The customization done in a dashboard & CCTV with respect to widgets position and size will be retained across users and browsers.

Build No - 123003 - September 28, 2017

Issues fixed in OpManager:

- For other language installation, iTextAsian.jar file has to be downloaded by the user. This download message has been enhanced and is displayed clearly in OpManager's UI.
- The display break issue occurring with "Check URL" feature in Workflows, has been fixed
- Issue with sending SNMP traps containing the variable $entity under notification profile, is fixed
- Issue with the WebAlarms widget where no data was available previously due to DB error, is now fixed.
• Issue with the Trap Processor status handling during sorting/navigation under Monitors, is fixed.
• Issue with trap-version while creating trap processor from unsolicited traps, is fixed.
• The period option missing in Availability Reports after upgrading to 12300 build, is included.
• Schedule Reports Top(10,50,100,1000) and bottom(10,50,100,1000) options are now shown properly.

Build No - 123002 - September 20, 2017

Issues fixed in NetFlow module:
• Router display name was not updated while fetching from Router via SNMP has been fixed.
• Search Filter not working in NetFlow inventory has been fixed.

Build No - 123001 - September 7, 2017

Issues fixed in OpManager:
• Google map widget was not loading properly in CCTV and this has been fixed.
• Browser crash issue when CCTV name has a space has been fixed.
• Issue in adding SNMP v1 and v2 credentials in OpUtilis has been fixed.

Build No - 12300

Features and Enhancements in OpManager
• 39,070 Vendor Templates have been added - To avoid devices getting added as “Unknown”, vendor templates have been added. Vendor template also includes monitors such as system up time, the number of Network Interfaces, and IP routing discards.
• Windows 2016 device is now supported.
• Microsoft Exchange 2016 is now supported.
• Microsoft Hyper-V 2016 is now supported.
• Tomcat version has been upgraded to 8.5.13.
• HTTP v1.1 has been changed to HTTP v2 for SSL encrypted servlets.
• When adding credentials, OpManager now asks to retype the password to avoid adding wrong credentials by mistake.
• Web client’s loading speed has been improved.
• Google Maps page has been revamped to group devices available in the same coordinates.
• Snapshot pages are now available for VMware datastores.
• Option to discover VMs through vCenter or ESX has been added.
• Option to carry out administrative tasks on VMware Host/VM from respective snapshot pages has been added.
• Test credentials of devices in bulk and also schedule it.
• Performance graphs have been added for file and folder monitors.
• Associate multiple performance monitors to various devices.
• Add a new device via a trap. [Settings-> System Settings-> Discovery]
• VPN Tunnels widgets have been added for ASA firewalls.
• Export PDF option has been introduced for Availability reports and Interface Bandwidth utilization.

Issues fixed in OpManager:
• The issue in updating the modified threshold values in the devices when reapplying the template has been fixed.
- Data collected during one instance is duplicated to other instances for WMI Free/Used disk space and partition monitors. This issue has been fixed.
- Trap alarm message displays OID instead of varbind key even after loading the MIB file has been fixed.
- Rules in Rule Engine getting applied by mistake even though the rule is not satisfied has been fixed.
- The issue with credential password containing special characters has been fixed.
- Issue with adding Process Monitors using bulk select options is fixed.
- For non-English language installations, File/Folder monitor’s Age/Size had few issues with the threshold and rearm with hour/day option. This has been fixed.
- Issue with monitoring MSSQL if the instance name has special characters ( _ $ # ) characters, has been fixed.
- Issue with View/Update Rack with the different locale for Non-English OS is fixed.
- Issue with the VM Sprawl data not being visible for VMware is fixed and has been included for HyperV VMs as well.
- Issue with not being able to identify Domain Controller with WMI is fixed.
- Issue with Script Monitors not working with other OS apart from Linux is fixed.
- Authorization issues have been fixed.
- Includes Rack/Floor Status updates.
- CLI Discovery (Telnet) issue fixed.
- Issues Fixed: Interface - When Interface speed exceeds bandwidth, an alarm would be raised.
- Virtual Server inventory reports have been introduced.
- Xen Pool Snapshot to view all the Entities List of a Pool in a single snapshot.

**Features and Enhancements in NetFlow**

- DPI-based bandwidth monitoring to measure NRT vs ART
- Cisco Meraki is now supported.
- sFlow support for Huawei is now added.
- Tab View for NetFlow is provided.
- Drill down from Dashboard option is included.
- Multi select options for Inventory list view for configuration and reports are added.
- Search in inventory, reports, and settings have been enhanced.
- Option to assign an NCM device for Operator role in both standalone version and collector is now added.
- Option to store raw data for 1 year in Highperf add-in is now provided.
- The subject of email and SMS alerts can now be customized.
- Tools in settings White List for Attacks Module is included.
- PDF/CSV enhancement in inventory snapshot.
- Windows authentication for MSSQL.
- Pagination for Autonomous View.
- Basic Audit reporting NetFlow.
- Customizable Email/SMS subject handled in Alerts.
- Resolve DNS option available from the Dashboard.
- Option to add device from NFA to NCM from inventory list.
- Bulk SNMP assignment is provided.
- Unique name association across OPM and NetFlow.
- Report Linking from Inventory.
- Auto selection of SNMP in netflow if the same device is already available in OPM with SNMP credential.
- SFlow support with dual sampling pool for IN and OUT separately. ( SFlow negative value )
- QoS drill down from List view
- Clear DNS cache option.
- Option to select the graph type for traffic widget has been included.
Issues fixed in NetFlow module

- SNMP V3/V2 failure issue fixed Alert Mail fails when there is no authentication provided.
- Display Autonomous View issue is fixed.
- Capacity planning issue - Granularity, 97th percentile, on demand bill generation, units, PDF NFA DE - The issue with utilization showing 0 in interface list, is fixed.
- Multiple E-Mail per threshold issue is fixed.
- SFlow parsing handle for PPPOE flows IPGroup with port range data dump handled.
- The issue in updating the modified threshold values in the devices when reapplying the template has been fixed.

Features and Enhancements in NCM module

- Ability to import new Device Templates using XML file.
- Ability to Edit / Delete Device Templates. Real-time notification of Approval requests.
- Real-time GUI update/auto refresh.
- Export options for Custom Template execution result and Custom Reports introduced.
- User specific Retainable filters and column choosers: Option to show/hide columns in list views.
- Schedule option is added for Configuration upload action.
- Ability to create device group by combining more than one device groups and also dynamically create groups based on predefined rules.
- Possible to add / associate / delete flow export configlets in a Template.
- Also, it is possible to add new Device Identifiers (Device SysObjectId) in a Template manually.

Issues fixed in NCM module

- Sysobject Finder SNMPv3 option provided.
- Issues with creating a user with more than 200 devices associated and not able to create a device group when more than 200 devices selected are fixed.
- The issue with viewing configuration change diff with HTML content is fixed.

Features and Enhancements in Firewall module

- Following devices are supported now:
  - TrendMicro IWSVA 6.5
  - PaloAlto VPN logs
  - Fortigate Management logs
  - SRX Management logs
  - SonicWall IPSec VPN logs
- 'Insider Threat' reports - 'End User Monitoring' Add-On.
- Drill-down for all dashboard reports.
- Exclude IP/IP-range/network from reporting feature.
- URL and VPN reports are provided for Inventory report user-drill down.
- Live report for Proxy servers.
- Live report drill-down for device and interfaces from Inventory.
- Interface Live Traffic widgets in Custom-Dashboard.
- End-User widgets in Custom-Dashboard.
- Anomaly-Alerts based on Country.
• User specific reports for Proxy servers.
• Option to export report as CSV on-demand.
• Option to use Management IP address to fetch device configuration.
• Option to configure ‘Row Count’ for on-demand PDF/CSV report export.
• More reports for Rules in Device-snapshot.

Issues fixed in Firewall module
• SRX policy parsing issue fixed for Compliance & Policy Overview report.
• Live Report out-traffic spike based on SNMP fixed.
• Fortigate 5.2.4 Device rule SSH connection issue fixed.
• VPN Usage Trend report issue fixed.
• PDF issue in non-English client side language issue fixed.
• Export to PDF issue fixed for Rule-Reorder recommendation report.
• SNMP V3 configuration issue without community fixed.
• The drill-down issue for Usernames which contains slash in it.

Features and Enhancements in IPAM/SPM module
• Microsoft DHCP Server has been supported. Scheduler scan.
• Custom columns have been added in IPAM & SPM.
• Edit IP details have been added.
• OS Type summary widget has been added in IPAM dashboard.
• NIC Type table has been updated to identify the device vendor.
• Include, Exclude ports pages has been added.

Issues fixed in IPAM/SPM module
• Issue with add switch has been fixed.
• Issue with modify switch has been fixed.
• Issue with IPAM Publish, Scheduler is fixed.
• Issue with viewing configuration change diff with HTML content is fixed.
• Issue with sorting in inventory and search issue is fixed.
• Issue in Tools, TCP reset has been fixed.
• Multiple UI issues have been addressed.

OpManager v12.2  Build No - 12200

Features and Enhancements in OpManager

• Plug-ins such as NetFlow, NCM, and OpUtils are merged with OpManager for unified network management. These plug-ins will now be available as add-ons and no additional download or upgrade is required.
• New API-based web-client that includes integrated dashboards, snapshot pages, alarms, inventory, and reports.
• Support for radius server authentication.
• Enhanced charts and graphs with drill-down and filter options.
• Tomcat has been upgraded to version 8.
• JRE has been upgraded to version 1.7.

**Limitation:**
• Old struts-based web-client will no longer be available with version 12.2

**Features and Enhancements in NetFlow Analyzer**

• SNMP V1/V2 Mapping issue fixed.
• End user bandwidth monitoring for MSSQL Handled.
• No data for Last 24 hour fixed Device blank page issue fixed (Mapping between OPM and NFA fails/ if deleted from OPM/NCM it is handled).
• Inventory view tab blank out issue fixed. Mailserver setting TLS handled.
• SFlow output interface flow processing handled. SNMP default time and retries handled.
• GRE and ESP include/Exclude handled.
• TimeFrame selection in Expanded Widget View Handled properly NetFlow Issue Fixed: Interface Traffic Widget Table data related Changes
• CBQoS Service Policy Tree Map view First Cut provided in Interface Snapshot Page under CBQoS widget. Device ID assignment fixed in Pagination.

**Features and Enhancements in Network Configuration Manager**

• TFTP Path Disclosure(Vulnerability) fix
• PCI- Deleted User Reviews cannot be Reviewed issue is fixed.
• Configlet schedule PDF attachment issue is fixed
• Unable to backup more than 50 devices issue is fixed.
• Compliance - Rules/RuleGroups not listed when the count is more than 50 issue fixed
• Alarms and Workflows not working issue fixed.
• “write mem” command execution showed failed even though the command execution success in the device.

**Features and Enhancements in Firewall Analyzer**

• Inventory - Device drill down - Top 10 widgets - If I expand without refreshing the widgets, scroll down option is missing.
• Check-point device dll & opsec.exe not bundled.
• “View All” option missed in all default Reports.
• URL-Report parsing issue fixed for Palo-Alto
• Cisco-Meraki (Proxy) and FireSight device support
• Administrator/ Operator specific page view issues fixed
• Showing two scroll-bar in Security Audit page.
Features and Enhancements

- Scheduled Discovery: Now network discovery can be scheduled to run periodically. Other enhancements include options to
  - Skip interface discovery
  - Select interface type during discovery
  - Select rule engine
  - Configure discovery reports
  - Add filters and rediscovery rules for actions such as adding, deleting, and un-managing devices or interfaces
- VLAN Discovery now supported.
- Device template for UCS system with 24 new monitors has been added.
- In 3D data center floor view, options to add air aisles, walk paths and walls have been added newly.
- Option to generate QR code for the devices on the rack.
- Now racks and floors can be added in the Business view.
- Connect now feature is added in Business Views to import connections from Layer2 map and draw the connections.
- Option to convert TopoMapper Plus to OpManager free version and vice versa has been added newly.
- Submit Feedback option has been added to capture a screen and submit the feedback to OpManager team for enhancements and bug fixes.
- Bulk edit option for editing thresholds and polling intervals of AD, MSSQL & Exchange monitors.
- XenServer monitoring is now available in OpManager.
- Extensive support for monitoring VMware events.
- Full monitoring support for VMware devices via vCenter. The earlier option available to monitor them via ESXi servers is withdrawn.
- VMware monitoring is supported from version 4.1 only.
- Now OpManager extends showing configuration details of VMware devices to data centers/clusters.
- New dashboards and widgets for virtualization monitoring have been added.
- Option to configure monitoring interval and threshold settings for monitors of virtual servers has been added newly.
- In addition to VM performance monitors for Virtual Servers, full fledged SNMP/WMI/CLI monitors are also supported now.
- OpStor plug-in 9.0 is compatible with 11400 & 11500 only. So Users upgrading from 11500 to 11600, also need to upgrade OpStor plugin to 9.1 version.
- OpStor plug-in 9.1 is compatible with 11600 only. So customers degrading from 11600 also need to degrade to OpStor 9.0 version.

OpManager v11.5 Build No - 11500 (Feb 5th, 2015)

Features and Enhancements

- Schedule Upgrade - Schedule Upgrade helps to stay up-to-date with the latest version of OpManager. Whenever a new version/update gets released, OpManager downloads it and starts upgrading automatically during the time scheduled by you.
- Migration Support: Migration from Enterprise Edition to LEE - OpManager now supports data migration from Enterprise Edition to Large Enterprise Edition. It provides an option to automatically migrate configuration data from OpManager EE (Central server & Probes), and populate in its own DB.
Migration from Standalone To Enterprise Edition - Users running OpManager standalone edition in PostgreSQL database can now seamlessly migrate to enterprise edition (i.e) central - probe architecture. Earlier this migration feature was supported only for MySQL and MSSQL databases.

SMS jar file has been upgraded from version 1.2.1 to 3.5.3. With this version upgrade, two new fields are introduced in the SMS server settings. Users are requested to revisit the SMS server settings in OpManager webclient and set up the configuration once again. To see the list of compatible GSM modems/phones, click here.

Private Groups in Social IT - Private groups in Social IT allows to carryout discussions on a project within the project members. The admin of the group can invite as many people to join the group. Only the group members will have access to view the discussions that happen in these groups.

It is now possible to add custom dials for all the performance monitors listed in device snapshot page.

Support for monitoring Exchange 2013 environment is newly included in OpManager.

Email attachment size limit for schedule reports has been increased up to 3MB.

OpManager 11500 supports monitoring the disk array data hardware status of all the DELL servers.

Interface templates section has been revamped. Earlier there was a single process for applying and associating templates. But now, it's been split into two processes - Apply template and Associate template. Associate template allows you to choose values to associate instead of associating all template values to interfaces.

New SMS Gateway(Clickatell) has been added for receiving SMS alerts.

To make initial configuration easier, more than 350 device templates are newly added in OpManager. IPSLA monitors are newly added to the notification criteria.

OpManager 11500 provides option to select the required discovery mechanisms such as CDP, LLDP, IPROUTE and FDB during Layer 2 discovery. A new widget for Layer 2 maps has been added. Exchange monitors are discovered automatically if WMI credentials are passed.

---

**OpManager v11.4 Build No - 11400 (Oct 1st, 2014)**

1. **UCS Monitoring:**

UCS Monitoring is an add-on that helps you to monitor all the Cisco UCSes and its components, in your data center. It leverages Cisco UCS XML API to monitor the UCS and instantly notifies you in-case of any fault via email & SMS. Apart from this, the UCS monitor also includes a 2D relationship map that helps you to visualize the relationship among the hosts, clusters, and VMs present in the UCS.

1. **Enhancements in network mapping**

Network mapping functionality in OpManager has got exciting enhancements such as

- LLDP Support - Helps to enhance automatic network discovery in multivendor networks
- Multiple Subnet Range support - Allows you to add multiple subnet ranges. This helps you to choose the desired network range and map them together
- Some of the other network mapping features that are newly included in Fluidic webclient are :
  a. SNMP V3 support
  b. Option to change Layout
  c. Export to visio
  d. Multiple Parent support
  e. Options to Edit, Update and Delete a network map
  f. Support for L2 Switch as Seed device

1. **SIEM Plug-in for OpManager (EventLog Analyzer)**
With the help of ELA Plug-in, you can now effortlessly manage terabytes of machine generated logs, monitor file integrity, conduct log forensics analysis, monitor privileged users, comply to different regulatory bodies and instantly generate variety of reports.

It also offers Real-time Event Correlation with over 70+ out-of-the-box correlation rules for proactive threat management and triggers alert notification via E-mail & SMS or Program execution. In-addition you can also set alerts based on specific type of compliance violation for HIPAA, GLBA, PCI-DSS, SOX, FISMA, etc.

1. **OpStor Plug-in (Storage Management)**

OpStor Plug-in enables you to monitor the storage devices like Storage Arrays, Fabric Switches, Tape Libraries, Tape Drives, Host servers and Host Bus Adapters cards from all leading vendors in the industry. It provides a unified view of storage environment along with effective reporting which in-turn increases visibility and reduces the time taken to detect any faults.

Storage Capacity forecasting helps you to predict the future storage needs by analyzing the usage & traffic utilization trends. Further, the OpStor Plug-in also provides topological map, real-time graphs & various reports on resource utilization, device availability and performance trends.

1. Hardware monitoring support is now available for the Domain Controller category

---

**OpManager v11.3  Build No - 11300 (May 19th, 2014)**

1. OpManager now includes the highly productive, faster and API driven user interface by default. The new web client will be the default UI for new installations. However, the existing customers can use the same old client and switch to the new UI anytime.
2. OpManager now includes Social IT- a private social networking medium built exclusively for IT folks. Social IT provides a cascading, Facebook-like wall for threaded discussions enabling real-time collaboration/communication between IT staffers. This Social IT integration is available only in the new API weboclient. [Learn more](#)
3. Now you can configure OpManager to detect event floods and anomalous event rates with predefined rules. [Click here](#) to know more about OpManager’s event flood handling functionality.

---

**OpManager v11.2  Build No - 11200 (Feb 24th, 2014)**

**Device Discovery in Large Enterprise Edition:**

- With the improved Discovery engine, you can now discover up to 20,000 devices in 5 minutes & 1 million interfaces in 1hour
- In Large Enterprise Edition, device discovery will no longer include the discovery of interfaces. For discovering the interfaces, you will have
to use the "Interfaces Discovery" section

API Client Enhancements

- Live popup notifications have been added to instantly alert you about the alarms raised
- Now you can make use of the keyboard shortcuts to traverse between device snapshot pages & alerts. You can also use the shortcut keys to pickup/clear/delete any alerts
- With the help of Heat Map, you can now get the status of all the monitored devices in real-time from a single page
- Virtualization maps for VMware & Hyper-V enable you to view the relationships among hosts, clusters, and virtual machines

REST API Enhancements

- Includes support for more than 330 REST APIs

Layer2 Enhancements:

- Discovery of non cisco devices and end nodes (server, desktop) are now supported
- Now you can also draw the Layer2 Maps for the devices which are not discovered/monitored in OpManager

Other Enhancements:

- Support for iPad App
- ITPulse tab has been removed from the product as it is EOLed

OpManager v11.1  Build No - 11100 (Nov 15th, 2013)

- CMDB Plug-in Support - The Plug-in helps you to get in-depth visibility of your assets present in your IT environment. This allows you to manage all your IT components based on their business criticality and make informed decisions
- Root Cause Analysis - Enterprise IT departments need sophisticated monitoring for each aspect of their operations, from basic infrastructure to bandwidth, applications and change management. However, these sophisticated tools churn out alerts at an alarming rate and volume, making it difficult to manipulate the alerts and find the root cause of the problem. This is now supported in OpManager
- Functional Expression Support - Functional Expression such as Byte to GB, Celsius to Fahrenheit, String to Numeric, Column Min, Column Max, Numeric to String etc are now supported for SNMP based monitors. Option to store or just alert is also provided now.
- Multi language Support - Language selection options such as Chinese, Japanese, French, Korean etc. are provided in the OpManager webclient
- Notification Profile / Alarm Escalation
  - Option to view the latest Polled Value available for recurring notification and escalation mails
  - Alarm Entity parameter is available now for notification
- Pass Through Authentication support is available now
- Security vulnerability in Postgres database is addressed now.
- Reports - A new report to list all the threshold configured devices is available now
- Around 75 device types are newly added
- Alarm Suppression Configuration is audited now
- Regular expression support provided for Event Log description
- Infrastructure Widget - Option not to show a particular category, if there is no devices present is addressed now
OpManager v11  Build No - 11000 (September 30th, 2013)

OpManager Large Enterprise Edition Release:

1. A single OpManager Large Enterprise Edition server can hold up to 50,000 devices or 1 million interfaces in a single box. It is twenty times more scalable than the enterprise edition.
2. Has twenty times faster discovery engine - Discovers 20,000 servers in 5 mins.
3. Integrated Layer2 Discovery with automated dependency to avoid false alarms.
4. New API client released as THEME for opmanager. Completely built with Ember.js and APIs. Works ten times faster with real-time updates.

OpManager v10  Build No - 10200 (July 22nd, 2013)

Widgets

1. In Performance Monitor widget, Sort Column option is added in Top N Monitored Values
2. Business View Summary widget now includes alarm count and list of devices in business view
3. Option to choose a dashboard when creating new tab
4. Embed widget option to hide headers
5. Open CCTV View link from Manage CCTV page
6. Last Polled Value time period option in following widgets
   • Devices by CPU Utilization
   • Devices by Memory Utilization
   • Devices exceeding N % CPU Utilization
   • Devices exceeding N % Memory Utilization
   • Top N Min/Max/Average CPU Utilization
   • Top N Min/Max/Average Memory Utilization

Schedule Reports

Notification subjects and messages can be configured by the user. Default parameters are Scheduler Name, Report Description, Report Period, Report URL etc.

Rule Engine
1. Support for MSSQL monitors & URL Monitors are provided in Rule Engine.
2. Provision to add a URL as templates is available now.

**MSSQL Monitors**

In MSSQL device snapshot page, Delete Option is provided in MSSQL Instances and MSSQL databases.

**Archiving**

Option to Re Run Archiving is newly added in the Database maintenance page. This feature will be useful in-case the hourly or daily archiving is missed due various reasons such as server maintenance shutdown, database disconnection etc.

**Workflows**

NCM Plugin actions such as Backup, Execute command, Execute template, GetLast N Changes are added as Workflows.

**Hardware Monitors**

1. Option to enable/ disable hardware monitors is added
2. Option to suppress alarms for hardware monitors is supported now

**Device Templates**

1. Option to configure Sys Description is added
2. Operators such as Equals, Not Equals, Contains, Not Contains, Ends with, Starts with etc are now supported in device templates
3. Option to export and import device templates with multiple rules is provided.
Tabs

New tab link 'All Devices by Disk Usage' is added under Maps tab, with the filtering option and the option to delete drives

Maps

Option to set the view as default for SLA Dashboard is added

Reports

Interface aggregate data graphs are added in the new Opmanager API Client

OpManager v10 – Build No - 10100 (May 7th, 2013)

1. With OpManager's new 3D Data Center Builder, you can virtually create an exact model of your racks and data centers. You can embed these datacenter designs on your NOC screens and monitor them 24x7 from anywhere, anytime. The 3D data center can also be viewed from iPad and other tablets.
2. A high productive, ultra-fast, responsive, API driven new UI is ready to use. Built completely on a new JavaScript framework it offers you 10x more productivity than the previous one.
3. You can now avail APM plugin in OpManager central webclient also. Previously the plugin was available only in the standalone version.
4. Now you can make use of APC PDU (Series 7800/ 7830 / 8841/8858 / 8858NA3) templates which are newly added to list of OpManager device templates. With the help of these templates, you can monitor parameters such as PDU Phases, PDU Power/Phase Load, PDU Voltage, PDU Bank Load & many more

OpManager v10 – Build No - 10000 (March 18th, 2013)

1. Now OpManager provides support for monitoring IPv6 network devices and servers. After discovery, device templates along with the essential monitors are applied on the IPv6 devices and monitored for performance.
2. Applications Monitoring plugin for in-depth monitoring of applications such as Oracle, SAP, Sharepoint, Websphere and much more has been added now.
3. Get granular insight into your VMware environment, as OpManager now monitors VMware ESX/ESXi and VMs through vCenter via vSphere API.
4. Now OpManager out-of-the-box monitors hardware health such as temperature, voltage, power, fan speed, status of processors, storage, memory, disk arrays, etc. of HP, Dell, Cisco and Juniper devices, via SNMP. OpManager also supports hardware monitoring for ESX hosts via vSphere API.
5. Failover support for OpManager Central server has been added now. Probe already includes support for failover.
6. Now raise a ticket with OpManager support along with the support information file, in a single click (Support-> Request Support).
7. Adding notes to an alarm has been simplified now. In alarms page, now you can add alarm notes by clicking on the "Note addition button" present beside each alarm notification. You can also add alarm notes in bulk by selecting the desired alarm notes and clicking on "Add note" button.
8. In Enterprise Edition, the intelligence to detect build mismatch between Probe and Central has been added.
9. Time Window option has been added in Schedule Reports page (Issue ID 91998)
10. Time out and max hops are now supported in TraceRoute in both RestAPI and Workflows.
11. Search filtering option added in All Devices and All Interfaces page

OpManager v9 – Build No - 9400 (November 29th, 2012)

1. iPhone App for OpManager: Connect to OpManager server and view the performance of all the devices, recent alarms, and business views from your iPhone. [Download the App now]
3. OpManager supports monitoring NetApp storage devices. [Watch Video]
4. Now authorize AD group users with different access privileges to access OpManager web-client with the new AD authentication feature. [Instructions to configure]
5. A seamless integration with ManageEngine ITPulse, the private social network for IT. OpManager will posts event status automatically in ITPulse, when a technician acknowledges, unacknowledges, or clears an alarm in OpManager. You can also view the details of such alarms from ITPulse itself and discuss the troubleshooting steps. [Watch Video]
6. The NCM plugin data and reports can be added as widgets in the dashboard page. Also OpManager now raises alarm for change detection and backup operations done by the plug-in.
7. OpManager now includes option to view config changes, execute backup/commands from the device snapshot and alarm pages itself.
8. New APIs are available for listing the alarms and devices, triggering a notification profile, and more.
9. OpManager provides option to execute notifications and workflow repeatedly until an alarm gets cleared.
10. To avert false positives, the consecutive times check for status polling is now extended to service monitors, Windows service monitors, interface poll and event log monitors.

Virtualization (VMware & Hyper-V)

1. OpManager includes provision to add event log rules on Hyper-V host server.
2. OpManager includes option to create custom WMI monitors form Hyper-V host and Virtual machines from their respective device template page.
3. OpManager now supports changing the category of virtual devices.
4. IT Automation tab with options to view and create workflows has been introduced in ESX & Hyper-V server snapshot page.

API

1. API now supports JSON output in addition to XML format.
2. In ‘Associate device to Notification Profile’ API, an option to provide the list of thresholds has been added.
3. In ‘Add Device’ API, you can now provide the device type and display name in addition to the device name.
4. Support for associating multiple devices has been added in ‘Add device to Business View’ API.
Workflow

1. Workflow supports new actions like creating OpManager alarms and folder. And also provides wildcard support for file related tasks.
2. The admins can now forcefully shutdown/reboot/logoff the remote machine using shutdown task option in Workflow.
3. Delete older files option in Workflows can now check and delete older files in subfolder also.
4. System Settings
5. OpManager now includes options to configure Date/Time format and also enable logging at runtime, under Admin -> System Settings.

Business view

1. In Business view, now you can zoom in/out.
2. Option to enable/disable traffic arrows for the links is provided now.
3. It is now possible to associate a link to multiple devices in a business view.

Others

1. Options have been included to create charts with data points, stacked area chart and to show the threshold value line in the graph.
2. Separate Alarm is raised for Status Poll, Service down and Windows Service down for better clarity and granular notification handling.
3. Now devices notes can be added in bulk via a CSV import.
4. Option provided to bind OpManager to a particular IP address of the server instead of all IP addresses in the machine.
5. Process monitoring feature is now enhanced to monitor, alert and report on absolute value of process memory in addition to percentage utilization.
6. Delete all option provided to purge the Unsolicited Trap.
7. Discovery Rule Engine now has option to manually rerun the rules against a set of devices.
8. Device Templates has been enhanced to provide a custom OID check in addition to SYSOID for classification.
9. Regex support is now provided for String based threshold setting.
10. The traps raised from the IP address can now be mapped to the source server with option to configure the IPMI address for SNMP traps.
11. License changes - Only managed devices are counted for license.
12. WebAlarm link is now included in CCTV view.

OpManager v9 – Build No - 9200 (July 10th, 2012)

1. IPAM Plugin: IP Address Management plugin helps you manage your IP Address. It also includes Switch Port Mapper to identify the switch port to which a device is connected.
2. Discovery Rule Engine: Automate actions such as adding monitors, associating the devices to a business, etc. that you carry out after adding the devices to OpManager.
3. Tab Customization: Customize OpManager web client by creating tabs for frequently visited pages, third-party embeds, reports, etc. and navigate easily in a click. You can also modify and delete existing tabs.
4. Multiple Threshold support: Configure multiple thresholds for the performance monitors. You can now set multi-level performance thresholds for a monitor and alert at different levels.
5. Log File Monitoring*: - Agent based: Monitor log files of mission critical applications such as MSSQL, Oracle, etc. in real-time. The agent constantly monitors the log files for content that may even be a regex.
6. New Audit Report and Enhancements to Monitor Health Report: Get real-time security audit report in OpManager at a mouse click, and also experience some of the high end enhancements made to monitor device health report.
7. You can now forward Traps and Syslog events from OpManager to any other NMS through Trap/Syslog Forwarder from OpManager GUI.
8. The new improved network discovery engine is 5x faster and discovers over 5,000 interfaces in a minute.
9. Faster Discovery Enhancements.
10. Support for VMware UUID & Replicated VM’s.
11. Configurable options are provided in SDP to create new ticket or reopen existing ticket on reoccurrence of an alert.
12. New VMware reports for Datastore Top Read & Write Latency are included.
13. New Workflow action "Refresh Datastore" is added to the list of several workflow actions.
14. Configurable Timeout option is included in Mail Server Settings.
15. Option is provided to enable protocol level logging at runtime in System Settings.
16. More enhanced rebranding changes are made configurable via brandprops.properties file.
17. New Category "Storage" has been added to device category list.
18. New device templates are included for NetApp/Cisco Routers.

OpManager v9 - Build No - 9100 (March 1st, 2012)

1. Major enhancements have gone into the Map Maker which includes curved lines, localized names, customized line thickness, easy drag-drop etc.
2. The long-awaited option to export and import device templates and share them with the community, is now available. The shared device, workflow, and script templates are listed under the RESOURCES tab in our forums. The shared template are validated and approved before displaying them here.
3. Support for Korean language installation is provided.
4. SSH key authentication for monitoring Unix-based devices, can now be given as file inputs., viz. instead of specifying the user name and password in the OpManager credentials GUI, you can store them in a file and give the file as authentication input.
5. Option to provide timeout in CLI credentials added.
6. You can now test the authentication credentials for multiple devices at one go, instead of testing it for each device.
7. Keep a tab on the monitors for which data is not collected for a specified period by accessing Support Diagnostics GUI.
8. The credentials configured are now grouped by the Protocol and listed for easy manageability. For instance, you’ll see the grouping when adding a new device for discovery.
9. A new device template is included for Cisco5508WLC devices.
10. When configuring trap processors, you’ll be able to select up-to the 20 Varbinds as part of the match criteria.
11. New graph Memory Utilization (UCD SNMP MIB) is added by default.

OpManager v9 - Build No - 9011 (January 5th, 2012)

If OpManager detects a DB collation mismatch during PPM upgrade, a system alert is shown to avoid partial upgrades.
OpManager v9 – Build No - 9000

1. IT Automation Workflows to automate 1st and 2nd level administrative tasks. Few pre-built workflows available out-of-the-box, and intuitive drag and drop GUI to create more custom workflows.
2. A hot-standby for Probe to ensure high availability. Seamless failover and failback between the primary and secondary probes and 100% data integrity.
3. REST API support in OpManager to help integrate with third-party help desk, NMS etc; operations supported include adding a device, adding a notification profile etc.
4. Define custom scripts and leverage OpManager's fault management to the fullest. Supported scripts include Powershell, Linux shell script, VBScript, Python & Perl.
5. Virtualization management support now extended to Hyper-V devices in addition to VMwares; monitor over 70 deep metrics!
6. The GUI has got a new face-lift with new tabs organization for easier and intuitive navigation.
7. Quick links are included to access help on how to configure tasks in OpManager and perform first level troubleshooting. These can be enabled/disabled from Admin > System settings.
9. NFA plug-in now supports 64 bit Windows and Linux installation.
10. Dashboards are introduced for Business View users.
11. Configurable color coding is included for Utilization widgets (Red for over 90%, Yellow for over 80%) [ Editable range value (Top 10, 12, 15) for widgets. (Previously it was a drop down box Top 10, 25, 50)]
12. An option to specify the consecutive number of times a device is polled/threshold is violated, is included in the device templates specific to Virtual devices.
13. You can now edit the threshold type/value of resources defined in the Virtual Machine device templates.
14. It is now possible to edit and save the IP address from the ESX Host snapshot page.
15. If you want to configure bulk URL monitors, you can specify the links in a CSV file and bulk-import them into OpManager at one go!
16. The folder monitoring feature enhancement includes wildcard (file filtering) option.
17. Sixteen new templates are included for A10 networks & blackberry devices!
18. An option is included to apply a change made in the interface template to all interfaces.
19. An option to rediscover the interfaces that are deleted from the device, is included.
20. A list-view is now available for Exchange servers with an option to add a server into exchange category directly.
21. The AMS validity is shown in the GUI with a link leading to renewal procedure.
22. New dashboards are included to show top 10 server and top 10 networks.
23. An automatic notification is triggered when the Probe is down (Enterprise edition).
24. A ‘View Associations’ option is included in Admin > Notification Profiles screen to quickly see a summary of the different profiles associated to the monitored devices.
25. A new device down time report is provided. The report also shows the outage history.
26. Localization support is extended to have the Probe name in Japanese or Chinese (in the respective local installations).
27. You can now add Probes in the Google Map.
28. An option is provided to enable/disable the discovery of a VM in a host.
29. For VMs that are also DomainControllers, the snapshot page is enhanced to show the interface details in two different tabs, one for the Virtual NICs and the Interfaces.
30. The performance monitor widgets now show the instance name in addition to the device name.
32. When configuring alarm escalation or when scheduling a report, you can now select the site too (specific to Enterprise edition).

OpManager v8 – Build No - 8812 (August 17, 2011)

1. The Alarm reports page now has option to filter alarms based on its properties; This report can be exported to .pdf, excel formats and can be emailed.
2. Option to escalate alarms via SMS in addition to email, is included. Option to configure URLs in Alarm Escalation is also added.
3. You can now associate any type of notification profile to a particular or to a group of URL Monitor. This functionality is available under the individual URL monitor page and at the "Quick Configuration Wizard" option.
4. You can now edit or update or add new mail store location for Exchange monitors.
5. Google map integration is enhanced now to show the location of the device both in the Google Map as well as in the Google Map widget.
6. Device search option is now extended to search "interfaces" using interface name or IP address and for "URLs".
7. When polling devices using ICMP ping for availability, choose which round-trip-time metric (Minimum/Maximum/Average response time) you want to show as Device Response Time under device availability. By default OpManager shows the average response time and you can change this now by editing Ping.properties file.
8. A new widget is added to show the total bytes transferred.
9. When reports are scheduled and emailed, the users with non-admin privilege can also access and view the reports.
10. Alarm ID is now configurable in the notification profile both, as part of the subject or/and the message.
11. In the device template "list of monitors", a multiple-select check box is provided against each group of monitors. The same option is available while associating monitors from the device snapshot page.

OpManager v8 – Build No - 8810 (May 9, 2011)

1. VMware ESX/ESXi version 4.1 is now supported.
2. View the domain controller dashboard in VM snapshot page.
3. Apply warning and error thresholds across multiple ESX hosts and VMs using Device templates.
4. NFS datastore reports are added for ESX v 4.1. Generate reports such as Disk Read Speed, Disk Write Speed, Write Latency, etc. on datastore.
5. Discover VMs also using the "Add Device" option under the "Admin" tab.
6. Get more meaningful and actionable SNMP Traps by processing every Varbind with intelligent processor.
7. Port/Interface monitoring has been enhanced for better performance.
8. Embed OpManager dashboard widgets as iframes into other sites
9. Network rediscovery now shows split-up of already discovered devices and new devices count.
10. Web client page loading time is now displayed in every page.
11. Options are included to change the Traffic Counter (32/64 bit) at individual interface level.
12. Interface parameter (ifalias) can be updated in OpManager by performing interface rediscovery operation.
13. UTF-8 Unicode is now supported in OpManager.
14. UPS interface details are monitored and shown now.

OpManager v8 – Build No - 8723 (February 15, 2011)

1. Community page enhanced to reflect industry benchmarks for resource performance.
2. An option is included to configure subject for the email-based SMS profile.
3. Provision to add STM files besides .edb in Exchange Mail and public store.
4. A new report to reflect total bytes transferred is included in the Reports tab.
5. You can now specify match criteria for threshold values in the Interface templates.
6. Interface properties/Custom fields for interfaces are added in notification profiles.
7. Interface snapshot page refreshes now based on the refresh interval configured in the 'Personalize' settings.
8. All Interfaces/Utilization reports are enhanced to show the links capacity. Columns are included to show Inspeed and OutSpeed values.
9. A new Widget is included to display tips to troubleshoot and workaround some configurations and tweaks in OpManager.
OpManager v8 – Build No - 8722 (December 27, 2010)

1. Support for adding non ping-able device is included now.
2. Support for scheduling downtime for consecutive days is provided in Monthly Day-wise option.
3. WAN link report has a link to the interface and device snap shot page.
4. Domain Controller category is now listed in URL response widget.
5. Process monitoring - Down alert is generated if the instance count is 0 and ‘consecutive times’ field is configured.
6. Device Templates now have a ‘Copy As’ option to enable saving the same template under a different name.
7. During Failover, email notifications are sent when:
   • The Standby server is not started.
   • Data replication process is not completed during standby server startup.
   • If data replication fails during take over.
   • Appropriate message is shown to the user, if the client is connected to standby server in standby mode.

OpManager v8 – Build No - 8721 (August 30, 2010)

1. The Downtime Scheduler now has an option to schedule a downtime on a monthly basis
2. Monitoring of Exchange 2010 is now supported
3. The notification criteria for the Printer and UPS includes variables like paper jam, low toner, low battery etc.
4. The threshold configuration now allows you to select ‘Not Equals’ as a match condition
5. OpManager Webclient, if invoked before the OpManager server process, reflects the status of OpManager process
6. The reason for a credential failure is shown on clicking the Test Credentials button
7. More time options such as 1, 2, 4, 6 hours have been included in Widgets
8. New widgets are included to show devices and services that are down, and also to show the business view traffic map
9. An email notification is sent when OpManager loses connection to the database
10. If the Syslog port is occupied, a message to this effect is shown in the Syslog Rules page
11. A hyperlink to the alarm details page is added in the notification mail message
12. The About page shows the latest build number available for download on the OpManager website

OpManager v8 – Build No - 8720 (July 16, 2010)

1. Exhaustive ESX VMware Monitoring using VMware APIs. Supports monitoring ESX 3.5, ESX3.5i, ESX4 and ESX4i
2. Automatic Layer 2/ Layer 3 network mapping
3. Supports configuring Mail server with ssl support
5. New set of device templates and monitors included
6. Category ‘Unknown’ has been introduced
8. NCM plugin version 5500 released. Click here to upgrade to the latest NCM plugin release.
OpManager v8 – Build No - 8052 (Apr 27, 2010)

1. A new CLI-based monitor for partition details of a device is included.
2. Alarm Details page has been enhanced to show the name of the log rule that triggered alarms (for Syslogs, Event Logs, and SNMP Trap based alarms). You can also edit the rule from this page.
3. The status of a Downtime Scheduler (in progress or not) is now shown in the schedule listing page.
4. You can now revert a re-branded installation of OpManager to the original settings that will default to OpManager logo and images.

OpManager v8 – Build No - 8051 (Mar 2, 2010)

1. Link to OpManager Community portal is included as a separate tab.

OpManager v8 – Build No - 8050 (Jan 8, 2010)

1. Data is collected every 5 minutes in the WAN RTT Monitor
2. Hop graphs are now shown for every RTT path from source to destination
3. Data is collected every 5 minutes in the VoIP Monitor
4. OpManager now supports 64-bit OS
5. File and folder monitoring for Windows devices
6. Provision to create custom WMI monitors in addition to the already available SNMP-based custom monitors. You can also associate these monitors from the device templates
7. Users can now access the OpManager web client using iPhone or Blackberry user interfaces
8. A new network traffic map to let you quickly identify highly utilized network links
9. OpManager now also alerts via Twitter Direct Messages
10. More device templates included taking the templates count to over 650 device types out-of-the-box
11. Provision to monitor custom event log categories in addition to the default Windows event logs
12. Reports enhanced to include NT Services and Process availability reports
13. Scheduled reports are now available for all reports and monitors
14. Support to export reports as Excel files now extended to all the in-built reports

OpManager v8 – Build No - 8025 (Nov 23, 2009)

1. Alarm Notifications Include alerting through RSS feeds
2. Provision to edit existing user privileges

OpManager v8 – Build No - 8024 (Oct 9, 2009)

1. The tools in the Device Snapshot page now includes SSH/HTTPS options
2. Export of Switch Port Mapper Reports as PDF or Excel files. Option to send the report via email also included.
3. Ability to send SMS if the OpManager server loses network connectivity.

OpManager v8 – Build No - 8022 (Aug 11, 2009)

1. **Notification Profile:** In addition to ‘Custom Fields for Devices’ and ‘Alarm Variables’, ‘Device Properties’ such as Device Type, Device State, RAM, Disk, IPAddress etc. can now be added to all the notification profiles
2. **Notification Profile:** Option to add ‘Custom Fields for Devices’ and ‘Device Properties’ as arguments for Run System /Run Program command
3. Option to select the required Devices is provided in the MIB Browser
4. Provision to set the ‘List View’ as default map view
5. Option to view the current downtime details in the Outage History reports
6. Interface Real time graphs will be shown by default for all the users, irrespective of license applied
7. The Netflow dashboard can now be seen from the OpManager webclient if the Netflow plugin is installed

OpManager v8 –Build No - 8021

1. **Enhanced Alarm actions:** Option to perform Ping, Trace Route, Test Monitor, Actions, Manage/ Unmanage devices, RDP & much more for every alarm.
2. Email Notification will have a link to device snapshot page for faster access to OpManager web-client
3. Ability to add Google maps to Custom Dashboards
4. Option to sort entries in Infrastructure view widget
5. WMI-based partition details are added out-of-the-box

OpManager v8 –Build No - 8020

1. Alarm Suppression: Suppress the alarms of a specific device for a pre-defined time interval.
2. Faster Backup and Restore utilities
3. I18N Internationalization issues fixed (For Japanese and Chinese Language)

OpManager v8 –Build No - 8007

1. Provision to add Telnet/SSH port number for devices discovered/monitored though CLI.
2. A new option to configure the consecutive times when the alarm should be generated has been added for URL monitors
3. Option to view the Real time graphs for the premium license users
4. SLA Dashboard now shows for business views
5. Option to configure Notification for interfaces belonging to Servers and Desktop category has been added
6. In the device snap shot page, instead of average data the latest collected traffic data is now shown
7. Configure tab option added in the interface snap shot page
8. Bar image option added in All servers disk usage report
9. Default monitors added for MGE and TrippLite type UPS
10. Provision to view the “About” and “Register” link is removed for Read only users
11. Interface name with special character are listed in customizable dashboard widgets
12. Option to monitor the cumulative resource usage for VMware server is enabled, even without the add-on license. (Note: VMware Dashboard still requires add-on licensing)

OpManager v8 – Build No - 8000

1. Plug-in for Network Configuration Management (NCCM).
2. Syslog Monitoring.
4. Customizable dashboards.
5. Plasma TV/CCTV View.
6. List view or Bulk configuration view.
7. Real time graphs for performance Monitors (CPU, Memory, Disk & etc.)
8. Real time Traffic and Bandwidth graphs.
9. More Device Tools (RDP, Telnet apart from Weblinks, Trace Route, Ping and etc).
11. Superior Interface Snapshot page.
12. Enhanced Reports.
14. Intro Tab - To facilitate fast deployment of OpManager.

OpManager v7 – Build No - 7204

1. Support for VoIP Monitoring.
3. All new revamped WAN RTT Monitoring (IP SLA based WAN Monitoring).
4. Over 300 new Device templates have been added.
6. Option to configure ICMP ping to the devices using IP Address or DNS Name. (NOTE - The option is provided in ServerParameters.conf file in OpManagerconf folder).
7. Option to select the Exchange server version (2003 or 2007) while configuring the exchange monitors.
8. Provision to add notes on Alarm messages for read only users.
9. Provision to configure the username/password in DBManager, if there is a change in Database credentials.
10. Ability to configure thresholds even for negative value monitors.
11. Support for monitoring OID of type Time-Ticks.

OpManager v7 – Build No - 7202

1. Ability for the devices in the Custom category to inherit the properties of another selected category.
3. Availability Reports showing the uptime/downtime in day-wise, by hours etc.
4. Provision to delete custom monitors.
5. Option to view current day’s data in Active connections / mobile users / temperature monitors in the snapshot page.

OpManager v7 -Build No - 7200

1. SNMPv3 support.
2. String OID monitoring.
4. Schedule the reports and export to Excel format.
5. Availability reports - Displays onhold, parent down, dependent unavailable, on maintenance parameters of the devices.
6. Generate Time based availability reports.
7. Sys OIDs are added for the following series Cisco 2800, Catalyst 3750, Cisco PIX.
8. Enhanced Webclient Performance wrt Mysql Database. Reduced the number of queries to access a device snapshot page.

OpManager v7 -Build No - 7100

1. Add-on for monitoring VMware ESX Servers.
2. Discover devices by importing from a CSV file.
4. Web-alarm enabling users to be notified of a fault.
5. Determining device availability using TCP Port checks.
6. Provision to add a device directly into a category.
7. Provision to add custom links to devices for ready reference.
8. Provision to select a time-window for a notification to be sent.
9. Exporting reports to XLS file format.
10. Alarm escalation policies can be configured for all devices in a business view.
11. Enhanced switch port mapper showing the ports-devices mapping information.
12. URL password is now in encrypted format.
13. Enhanced the min/max values displayed in the interface reports.
14. MSSQL DB password is now in encrypted format.
15. Top 1000 Reports option is included in scheduled reports.
Upgrading OpManager version 10.x and below to version 11.1

Steps to upgrade OpManager

1. Choose your upgrade path
2. Download the appropriate ppm
3. Apply it on OpManager
4. Restart OpManager

Choose the upgrade path

<table>
<thead>
<tr>
<th>Current build</th>
<th>Upgrade path to the latest build</th>
</tr>
</thead>
<tbody>
<tr>
<td>9410 / 9450 / 10000 / 10100/10200</td>
<td>- Install the Service Pack to move to build 11100</td>
</tr>
<tr>
<td>9400</td>
<td>- Install the Service Pack to move to build 9410</td>
</tr>
<tr>
<td>9200</td>
<td>- Download the JRE PPM upgrade pack as instructed</td>
</tr>
<tr>
<td></td>
<td>- Install the Service Pack to move to build 9410 [It is necessary to upgrade NetFlow plug-in, NCM plug-in and IPAM &amp; SPM plug-in to the latest version, after upgrading OpManager to the build 9410.]</td>
</tr>
<tr>
<td>9100 / 9101</td>
<td>- Install the Service Pack for moving to build 9200</td>
</tr>
<tr>
<td>9010 / 9011</td>
<td>- Install the Service Pack to move to build 9100</td>
</tr>
<tr>
<td>8810 / 8811 / 8812 / 9000</td>
<td>- Please fill this form to move to build 9010</td>
</tr>
<tr>
<td>8000 to 8723</td>
<td>- Install the Service Pack to move to build 8810</td>
</tr>
</tbody>
</table>

Note: Customers using builds earlier to 8000, please get in touch with our support team at opmanager-support@manageengine.com, for upgrade assistance. (Find out which Build you are in).

Instructions to download the appropriate OpManager JRE PPM file

We have moved to the JRE version 1.6 from OpManager build 9400 onwards. The following instructions will help you move from the older OpManager JRE version to version 1.6.

To know which OpManager JRE upgrade PPM to download, follow the instructions below:

1. In the Web Client, click the "Support" link on the top right corner of the page and select "Support" from the drop down menu.
2. Look at the OS Name and Version and OpManager Version on which OpManager is installed under the 'Installation & JVM information' pane (screenshot given below).
3. Now download the corresponding OpManager JRE PPM file to the OS Name and the bit version from the below link. For e.g. If you have installed OpManager in a Windows 64 bit OS, download 'JRE - 64 bit' from the 'For Windows' column.
4. Copy the downloaded OpManager JRE Upgrade PPM file under OpManager installation directory ‘/’ folder e.g. C:Program Files (x86)ManageEngineOpManager.
5. Now download and upgrade the Service Pack PPM as usual ([Upgrade path table](#) | Instructions to apply the Service Pack). Do not use JRE PPM file in Update Manager tool. It is enough if you just apply the Service Pack PPM. The Update Manager tool will internally handle the JRM upgrade before applying the Service Pack.

**Instructions to apply the Upgrade Pack/ Service Pack**

**How to Upgrade OpManager**

**- Video Tutorial**

1. Shut down OpManager. (If OpManager is running as a windows service, stop the service from 'Control Panel' > 'Services' window and close the window)
2. Start command prompt as an administrator [cmd > right click --> run as administrator](#) to see the screenshot.
3. Backup database - [click here](#) to know the steps.
4. End the processes: Open the Task Manager and make sure the processes 'java.exe' or 'wrapper.exe' of OpManager and the plug-ins (NetFlow, NCM & IPAM) are terminated. If not, terminate the processes.
5. Backup OpManager folder: Take a copy of ‘<OpManager-home-directory>‘ folder. This step is to back up the product configuration settings and the plug-in data.
6. Launch Update Manager - Go to '<OpManager-home-directory>/bin' folder and run the script 'UpdateManager.bat' (UpdateManager.sh for Linux).
7. Click 'Browse' button to select the Upgrade Pack file (the .ppm file that you’d downloaded) and choose 'Install'.
8. Follow the on-screen instructions to apply the Service/Upgrade Pack.
9. Once the upgrade is complete, start OpManager Service for the changes to take effect.

Remember, if you are applying more than one upgrade pack, you have to follow the above instructions for applying each upgrade pack.

For instance, if you are on build 9010 and have to move to 9200, here is how you should go about it.

- Follow steps 1 to 9 to upgrade to build 9100. Ensure you start OpManager after this upgrade.
• Again stop OpManager and follow steps 1 to 9 to move to build 9200.

It is necessary to upgrade [APM plug-in](#), [NetFlow plug-in](#), [NCM plug-in](#) and [IPAM & SPM plug-in](#) to the latest version, after upgrading OpManager to the build 9410.

How can I find the build number of OpManager?

1. In the Web Client click the "About" link on top right of the page.
2. Search for the 'Build Number' among the product details listed.
3. Check the following image guide to locate the build number.