USER GUIDE

Minder 5.0

mindarray

Contents

1. Installing MindArray Minder

Minder is a composite application that comprises three basic software components:

- Data Store (configuration database) – built in
- Web application (User Interface) – built in
- Data Polling Engines – built in

The application and the Data Store are installed on the same server.

1.1 Supported Platforms

Windows

- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2003 Enterprise x64 Edition
- Windows 7 x64 Edition

Note: If you are running Windows Server 2008, you must upgrade to Windows Server 2008 R2 because Minder 5.0 does not support Windows Server 2008 due to known WMI issues.

Linux

- Fedora
- CentOS
- Ubuntu
- RedHat

1.2 Hardware Requirements

Some desktop-class processors like the Celeron (which has minimal onboard cache) are not suitable for use with Minder. MindArray strongly recommends Pentium 4/M, Xeon, or equivalent processors.

The minimum hardware requirements for MINDER are:

- 2GHz+ CPU on x64 platform
- 4GB RAM
- 20GB disk space (SCSI or fast IDE)

MindArray recommends the following hardware configuration:

- 2 x 3GHz+ Intel Xeon CPU
- 4GB RAM
- 60GB disk space on RAID-5 configuration (SCSI/SATA)

Additional Minder Requirements:

Enterprise-level Minder deployments with the potential for more than 1,000 monitors may need additional computing resources above the standards required for MindArray common components:

1.3 Windows Software Requirements

You must install the following software on Windows platforms:

- Latest Windows Updates
- .NET Framework – Version 3.5, .NET Framework 4.1 is recommended. We also provide it with the setup of Minder.
- Windows operating system management and monitoring tools component.
- Firefox version 30+. (Used for Website monitoring. If you are not planning to monitor Website – ignore this requirement)
- Disable Sleep Mode on Host

1.4 System Security

MindArray strongly recommends that you terminate or disable all unnecessary services and processes on MINDER server (this includes TELNET and FTP).

1.5 SNMP Requirements for Monitored Devices

Minder can monitor the performance of any SNMPv1-, SNMPv2c-, or SNMPv3-enabled device on your network. Consult your device documentation or a technical representative of your device manufacturer to acquire specific instructions for configuring SNMP on your device.

Notes: To properly monitor devices on your network, you must enable SNMP on all devices that are capable of SNMP communications. UNIX based devices should use the configuration of Net-SNMP version 5.5 or higher that is specific to the type of Unix-based operating system in use.

Minder is capable of monitoring VMware ESX and ESXi Servers versions 3.5 and higher with VMware Tools installed. For more information about enabling VMware Tools on your VMware device, consult your VMware documentation or technical representative.

If SNMPv2c is enabled on a device you want to monitor, by default, Minder will attempt to use SNMPv2c to poll the device for performance information. If you only want Minder to poll using SNMPv1, you must disable SNMPv2c on the device to be polled.

2 Using MindArray Minder

This chapter describes how to operate Minder. This chapter assumes that you have installed MindArray Minder.

Minder provides your organization with proactive monitoring, event detection, reporting and problem escalation for mission-critical components of IT infrastructures through an intuitive Web application.

The Minder Web application provides instant Business Visibility by monitoring your critical IT Infrastructure, including but not limited to your network-based services, applications and systems. Current monitoring services include availability, performance, applications, e-commerce, SNMP, port monitoring and custom device/attributes monitoring capability. Minder is designed to be a flexible system where you can set thresholds, test intervals, filters on status views, schedule notifications and generate standard or custom reports based on the privileges you have. Instant Business Visibility provides you access to your data through a Web interface. It saves you time and reduces costs by enabling you to quickly identify and resolve downtime problems without any investment in additional infrastructure or technical expertise.

Read the following sections to learn more about working in the interface and to learn about:

- Network Health Indicator
- Navigate Dashboard
- Search for devices, events and system properties
- Navigate the event console
- Run actions
- Create and use alerts
- Create custom views

2.1 Understanding the Status of Health Indicators

Minder monitors returns the following indicators:

2.1.1. Availability Indicators

Each status reflects the availability state of the Monitor that has been assigned to the system that you are currently viewing. Minder picks up these error codes and triggers an alert or an action. If availability is in a down state, you can acknowledge an alert so that Minder does not generate subsequent notifications.

- Up
  - The availability of Monitor/Device is UP.
- Down
  - The availability of Monitor/Device is down.
- Maintenance
  - The availability of Monitor/Device is in Maintenance State.

- Unknown
  - The availability of Monitor/Device is in Unknown State.
  - The Minder polling engine could not execute the availability monitor.
  - Or The Monitor is disabled.

2.1.2. Performance Health Indicators

Each status reflects the health state of the Monitor that has been assigned to the system that you are currently viewing. Minder picks up these error codes and triggers an alert or an action. If a performance metric health is in a warning or critical state, you can acknowledge an alert so that Minder does not generate subsequent notifications.

- Clear
  - The health of Monitor/Device metrics is Clear/OK.
- Warning
  - The health of Monitor/Device metrics is in Warning state.
  - The attached threshold with performance metrics is in Warning state.
- Critical
  - The health of Monitor/Device metrics is in Critical state.
  - The attached threshold with performance metrics is in Critical state.
- Unreachable
  - The health of Monitor/Device metrics is in Unreachable state.
  - The attached threshold with performance metrics is in Unreachable state.
- Maintenance
  - The health of Monitor/Device metrics is in Maintenance state.
  - The attached threshold with performance metrics is in Maintenance state.
- Unknown
  - The health of Monitor/Device metrics is in Unknown state.
  - Or The Minder polling engine could not execute the performance monitor.
  - Or The Monitor is disabled.
  - Or there is no threshold/policy profile attached to performance metric.
- Not Configured
  - The health of Monitor/Device metrics is in Not Configured state.
  - Or there is no threshold/policy profile attached to performance metric.

2.1.3. Interface and Navigation

After you install Minder and navigate to the interface from your Web browser, the Dashboard appears. The Dashboard provides at-a-glance information about the status of your IT infrastructure. It is the primary window into devices and events that the system enables you to monitor.

The Dashboard can show:

- System information resources and Web pages
- Important error-level device events
- Monitor Group high-level view
- Monitors with “Problems”

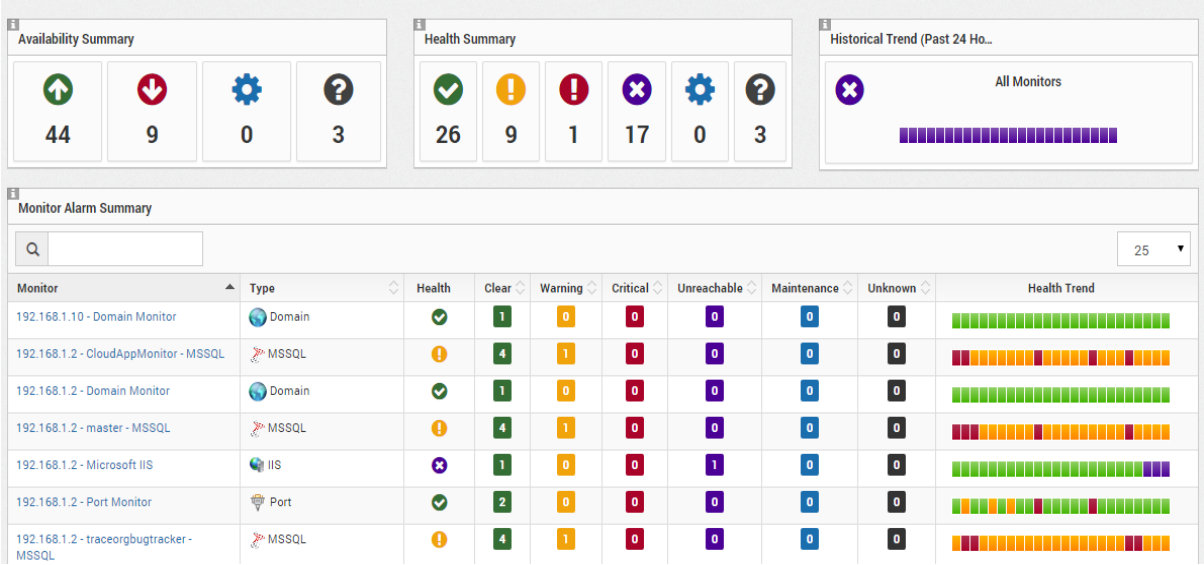


Figure 2.1 Organization Snapshot Dashboard

Key Dashboard and interface areas include:

- Network Health Indicator
- User information area
- Recent Information
- Navigation Bar

2.1.4. Network Health Indicator

The Network Health Indicator provides an instant summary of the status of all devices and events in Minder. The monitor and event count (message as well as threshold violation) is displayed according to different severity. When you click on the icon (shown in the first red box in the following figure), you enable a constant view of network health while using Minder.

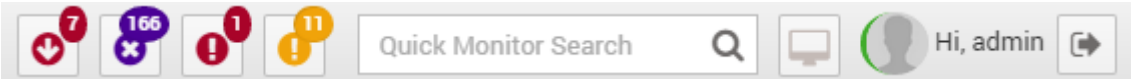


Figure 2.2 Network Health Indicator

Information in the Network Health Indicator gets updated after every 60 seconds by default. The values can be changed from Admin > Global Settings.

Click on any of the colored health indicator boxes to view related information about the monitor or event. For example, clicking on the icon navigates you to the Devices Status Summary page where only monitors with critical health are displayed. Clicking icon navigates you to the live Critical events across all the monitors.

2.1.5. Navigation

The Navigation menu lets you access major system features. In addition to the Dashboard, the menu is divided among several functional areas:

- **Alarms** - Guides you to the event management area, where you can monitor event status, events, history, configuration properties and event transforms. You also can track changes made to events.
- **Business Service/SLA view** - Offers access to network infrastructure, including devices, networks and application monitor views.
- **Reports** - Allows you to view and define reports.
- **Monitors** - Allows you to change monitor properties such as state, credential, department etc.
- **Network Configuration Management** – Allows you to track, manage and replace the configuration of a network device.
- **Flow** – Enables you to monitor IP to IP traffic in your network.
- **Admin** - Provides access to global settings, network discovery and system settings.

2.1.6. User Information Area

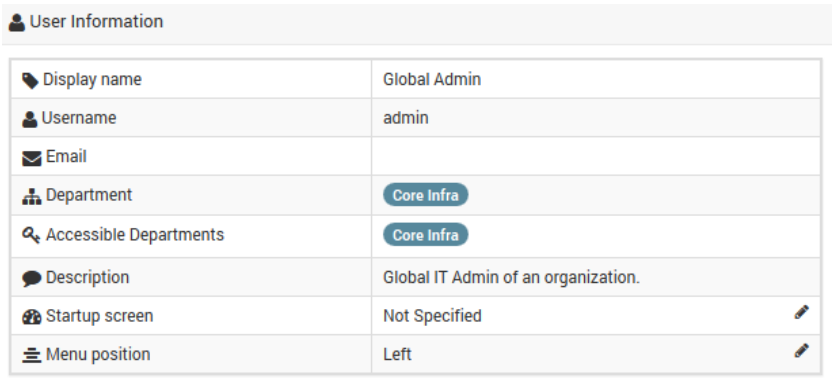


Figure 2.3 User Information Area

The User information area offers information and selections:

- **User Name -** The ID of the user currently logged in appears at the top of this dialog. Click the user edit icon to change user settings, such as menu position on the web console, theme and startup screen.
- **Log Out -** Click to log out of the system.

2.1.7. Viewing Monitor and Health Details

Click on Monitor name in the grid to focus on it. Focusing on a node:

- Open Monitor Page in new tab.
- Hovering monitor name links, shows monitor health as show in the figure below:

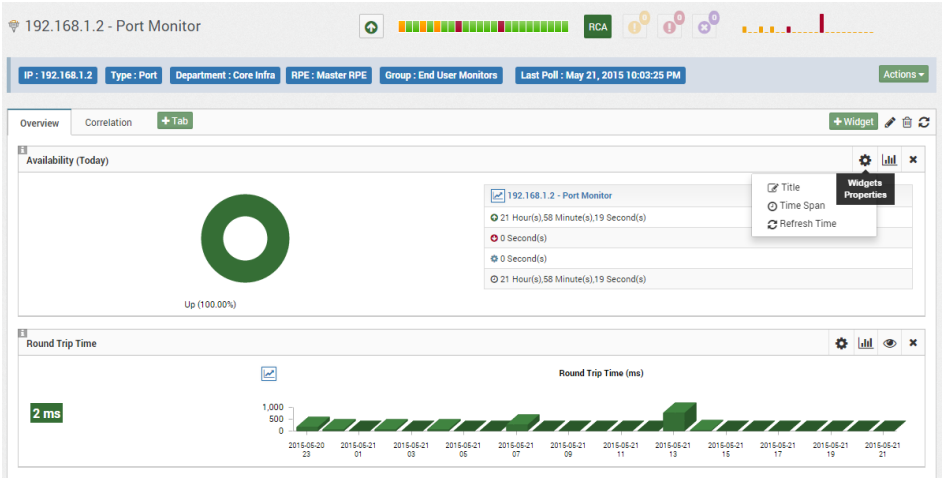


Figure 2.4 Monitor Drill down Page

Alternatively, you can double click on the Health / icon to drill-down on monitor health; this will launch Root-cause analysis details for selected monitor.

2.1.8. Customizing the Dashboard

Through the Real-Time View dashboard feature, Minder allows the creation of custom dashboards to view the performance of services and infrastructure. You can create multiple dashboards, each containing up to twenty components that can display and chart any metrics selected and update in real time. In some type of components, you can click through to view the performance attribute details for containing attributes or attribute summary for devices. Whereas service views let you group attributes and devices according to business-oriented views, the Real-Time View dashboards provide a more abstract way to organize information. For example, you might create a dashboard to monitor bandwidth across your entire network, or a dashboard that reports which devices is at the top resource hogs.

By default, a dashboard is visible only to all other users including who created it.

2.1.9. Customizing Default Dashboard

You can customize the Dashboard by:

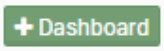
- Selecting the widget you want to monitor
- Arranging widget

You can arrange the widgets that are displayed in all default dashboards. To arrange the widgets, drag and drop them at your desired location. This view will be persisting for each user profiles.

To manage the number of default widget to display, click on add/delete icon towards top right of the dashboard and select the widgets you want to display.

2.1.10. Adding Custom Dashboard

Follow the steps given below to add custom Dashboard by:

1. Navigate to **Dashboards** > Click 

icon to add new dashboard.
2. Dashboard popover appears.
3. Give the **Title** for the dashboard.
4. If you want to keep dashboard accessible to others then choose public.
5. Select the Layout of the Dashboard. Provide description if needed.
6. Click 

icon toward top right corner to add widgets.

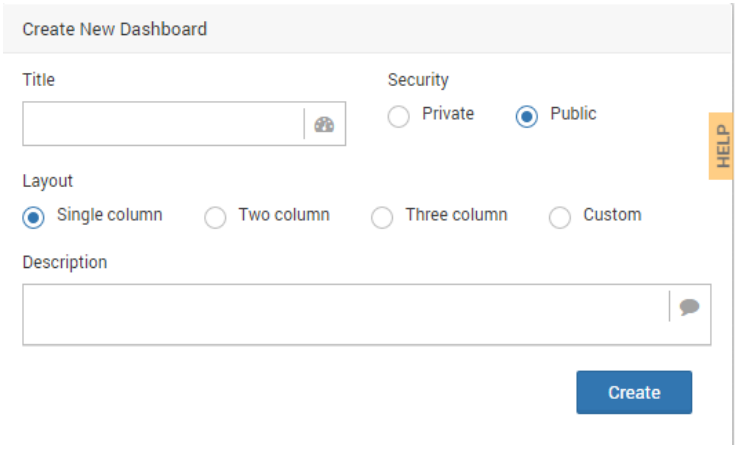


Figure 2.5 Add New Dashboard

Note: Adding widget shows the default and custom created widget created by other users.

Follow the steps to create a new widget:

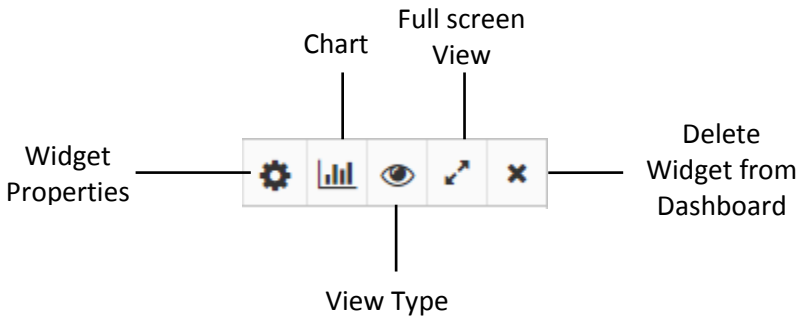
1. Click 

> choose the Widget type from the list in the left.
2. Once Widget has been added > Bind the data source. The system adds widgets to selected dashboard.

For more information on Widgets, **see section 9.15.**

2.1.11. Customizing Widgets

You can customize each widget that appears on the Dashboard. Customization options vary depending on the widget type.



Click , which appears at the top right corner of a widget, to view and customize display options.

Click **Update Settings** to save your selections and then return to main widget content. For creating new Data Widgets see section 9.15.

Click + Widget placed in the top right corner of the widget to select the data source, title of the widget, Time Span, Refresh time and Granularity.

3 Adding and Discovering Devices

Network discovery is a network setting that affects whether your computer can find other computers and devices on the network and whether other computers on the network can find your computer. Discover Network Devices, Serves, Applications, Database, Web Servers, Virtualization Servers, Services, Cloud and Asset with appropriate details to start monitoring them. You need to provide appropriate applicable details:

1. **IP**: You can provide a single IP e.g. 192.168.1.1, an IP range e.g. 192.168.1-200 or import a CSV file with format Monitor Name, IP.
2. **Department**: If you wish to restrict any monitor's access to other departments then you need to select suitable department. Minder will provide Core Infra department by default.
3. **RPE**: If you are implementing distributed monitoring then you need to select the RPE which should poll the information from the monitors of this discovery.
4. **Device Type**: Select all the types which you wish to monitor and can be discovered in the provided range.
   Note: You can select multiple devices in a single discovery with appropriate IP.
5. **Resource Type**: Resources will be populated based on the selection of the devices. E.g. Resource for a Network device is Interface, for a database it is table etc.
6. **Credential Profile**: Appropriate credentials of the user to login into the device each time and get the information.
7. **Device Parameters**: There are default parameters to connect to a device and monitoring data however that can be changed according to your infrastructure.

Minder provides four types of Network Discovery:

- **Device, Server & Apps**
- **Cloud**
- **Services**
- **Asset**

Restrictions of Network Discovery:

1. Minder cannot discover devices that cannot be pinged if **Ping Check Required** option is enabled. If, for example, a firewall blocks echo requests, a device behind it cannot be discovered.
2. If proper credentials are not provided then also minder will not be able to discover y our device.
3. If a device has more than one IP address, it may show up more than once in the discovery results.
4. A few times the added devices may need root credentials and without that, there would be missing information.

3.1 Private Network Discovery

3.1.1. Device, Server & Apps Discovery

Minder can discover multiple device types at a time which can be one of the listed below:

- Network Device (SNMP)
- Server

    - Linux/Unix Host Server (SSH)
    - SNMP Host Server (SNMP)
    - Windows Host Server (WMI)
- Virtualization
    - Citrix Xen Server
    - Hyper-V Server
    - VMware ESX/ESXi Server
- Database Server
    - IBM DB2
    - MSSQL
    - MySQL
    - Oracle
    - PostgresSQL
- Application Server
    - Apache Tomcat
    - GlassFish
    - JBoss
    - Jetty
    - WebLogic
    - WebSphere
- File/Directory Monitor
    - Directory
    - File
- Middleware
    - Active Directory
    - Apache ActiveMQ
    - MSMQ
    - OpenLDAP
    - RabbitMQ
    - WebSphere MQ
- Platform Monitor
    - JVM
    - .NET
- Web Server
    - Apache
    - IIS
    - Nginx

Follow the steps given below to add device by running network discovery:

1. Navigate to **Admin** > **Network Discovery** > **New** > **Device, Server & Apps.**
2. Provide the **Name** for the discovery.
3. Provide IP with one of the three options:
   IP/Host: for single device, **IP Range:** for multiple devices in a range.
   CSV Import: for only a number of selected devices. Directly imports the CSV file when you need all those devices again for discovery or your devices are not in the same range.

Note: Provide hostname and IP address of that host separated by commas in the CSV File

E.g. Mindarray-Host1, 192.168.1.101

Mindarray-Host2, 192.168.1.102

4. Select the **Department** from the list.
5. Select the **RPE** (Remote Polling Engine) from the list.
6. **Ping Check Required** to check if ICMP is enabled. In case you wish to avoid ICMP check e.g. database does not need ping check, then you can disable the option.
7. Select **Device Type** from the list to be discovered. This includes types of devices namely Network Device, Server, Virtualization, Database Server, Application Server, Middleware, Platform and Web Server types

   Discovery Parameters: Also provide the required parameters to make the connection. E.g. Port number and Database instance name in case of Database discovery.
8. Provide the **Resource Type** to be discovered.
9. Provide **Credential Profiles** for selected device type.
10. Click on **Create** to add new discovery.
11. Click on **Run** to run the discovery.
12. Once finished, click on **View Result** to view discovered Devices, resources, applications and virtual machines.
13. Click on **Provision Object** to add selected nodes, resources, applications and virtual machines.

    Note: Discovered Network Device, Servers will be listed under Node tab. Selected Objects should be displayed at top of the pop-up as total number of nodes, resources, applications, virtual machines.

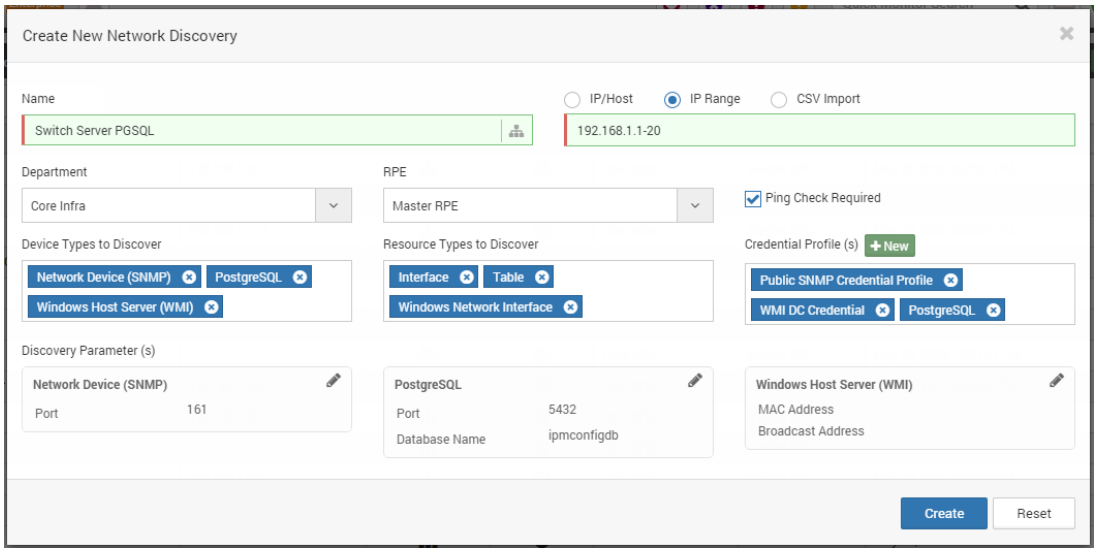


Figure 3.1 Network Discovery > Device, Server & Apps

3.1.2. Cloud Network Discovery

Minder support the discovery and monitoring of below listed cloud platforms:

- Amazon Cloud (AWS)

- Cloud Foundry (CF Cloud)
- Google App Engine (GAE)

Follow the steps given below to add device by running network discovery:

1. Navigate to **Admin** > **Network Discovery** > **New** > **Cloud**.
2. Provide the **Name** for the discovery.
3. Select the **Department** from the list.
4. Select the **RPE** (Remote Polling Engine) from the list.
5. Provide **Credential Profiles** for selected cloud types.
6. Select type of devices from the list to be discovered. This includes types of devices namely Amazon, Cloud Foundry and Google App Engine types.
   Discovery Parameters: Also provide the required parameters to make the connection.
7. Provide the **Cloud Resource Type** to be discovered.
8. Provide appropriate **Discovery Parameters** to discover them successfully.
9. Click on **Create** to add new cloud discovery.
10. Click on **Run** to run the discovery.
11. Once finished, click on **View Result** to view classified Cloud Apps.
12. Click on **Provision Object** to add selected Cloud Apps.
    Note: Discovered Cloud node will be listed under Node tab. Selected Objects should be displayed at top of the pop-up as total number of nodes, resources, applications, virtual machines.

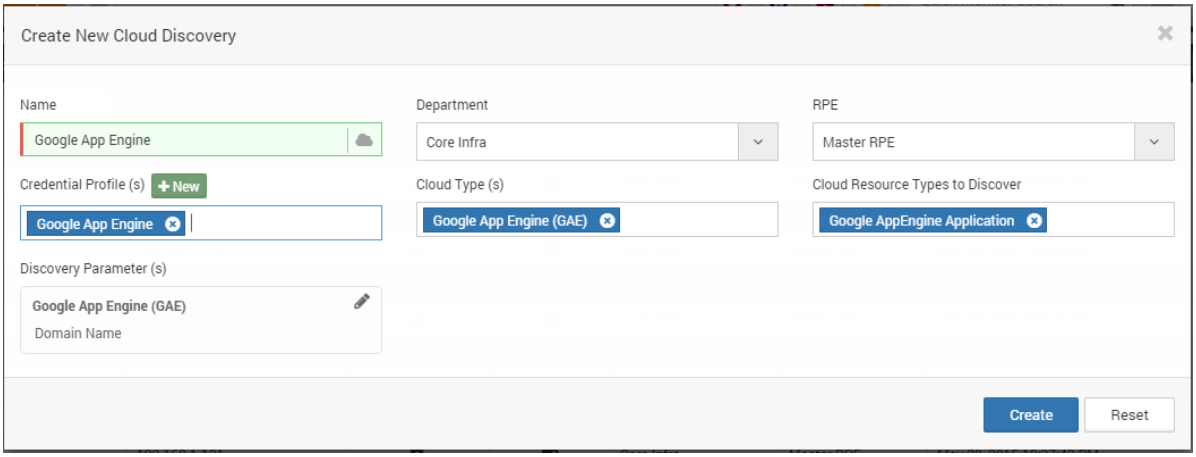


Figure 3.2 Cloud Discovery

3.1.3. Service Discovery

Service monitoring can be enabled "agent less" or by "installing agents" in client locations and configuring your monitors to collect performance data from these agents for monitoring. The service monitors currently supported by Minder include:

- DNS monitor
- FTP monitor
- JDBC Connection monitor
- LDAP server monitor
- Mail Server monitor
- NTP monitor
- Ping monitor
- Radius monitor
- Query monitor
- Script monitor
- Service Port monitor
- URL monitor using Firefox
- URL monitor using Phantom JS

Follow the steps given below to add services by running network discovery:

1. Navigate to **Admin** > **Network Discovery** > **New** > **Service**.
2. Provide the **Name** for the discovery.
3. **IP/Domain/Host/URL:** for single device
   IP Range: for multiple devices.
   CSV Import: for selected multiple devices. When you need all those devices again for discovery, directly import the CSV file.
   Note: Provide hostname and IP address of that host separated by commas in the CSV File
   E.g. Mindarray-Host1, 192.168.1.101
   Mindarray-Host2, 192.168.1.102

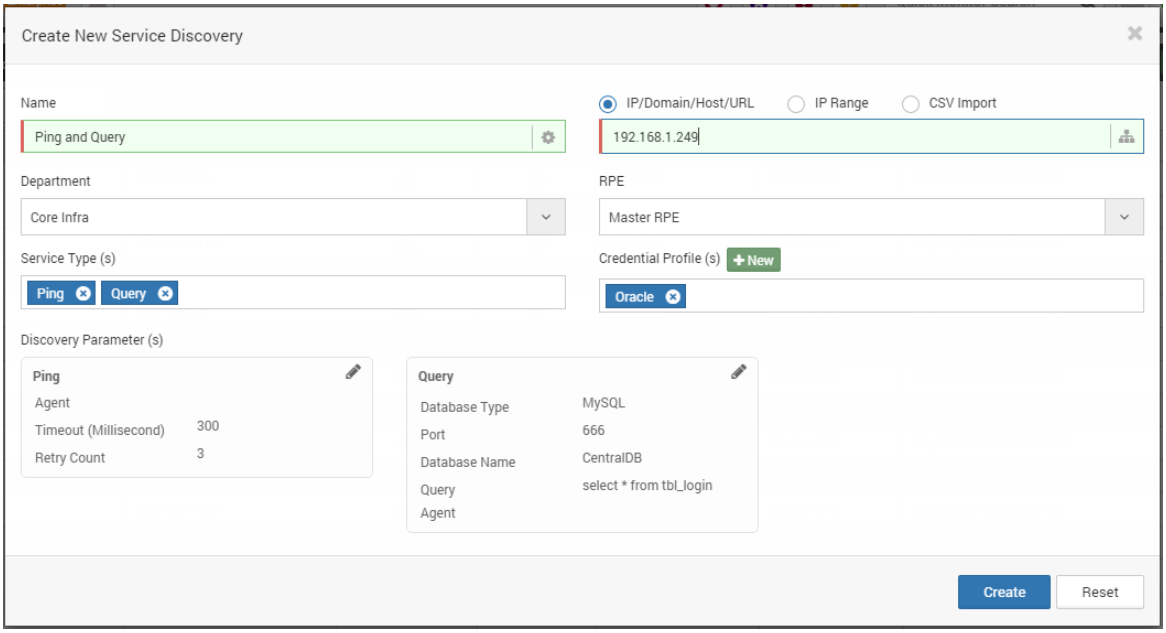


Figure 3.3 Service Discovery

4. Select the **Department** from the list.
5. Select the **RPE** (Remote Polling Engine) from the list.
6. Select **Service Type** from the list to be discovered. This includes types of services such as DNS, Domain, FTP, JDBC, LDAP, Mail, NTP, Ping.
7. Provide **Credential Profile** for selected service type if authentication is required.
8. Click on **Create** to add new Service discovery.
9. Click on **Run** to run the discovery.
10. Once finished, click on **View Result** to view classified Services.
11. Click on **Provision Object** to add selected services.

    Note: Discovered Services will be listed under Node tab. Selected Objects should be displayed at top of the pop-up as total number of nodes, resources, applications, virtual machines.

3.1.4. Asset Discovery

Asset discovery allows you to scan workstation, Desktop and Laptop with Windows or Linux Operating Systems for Software and Hardware inventory tacking. Once Minder starts scanning of software and hardware, you can get alerts and reports about audit changes. Monitoring assets is not calculated based on monitors rather calculated based on number of assets you are monitoring.

In case you have already done Device/Server/App discovery and the host server is provisioned for monitoring then that monitor will be listed under Assets tab. User need to enable the Asset monitoring from here.

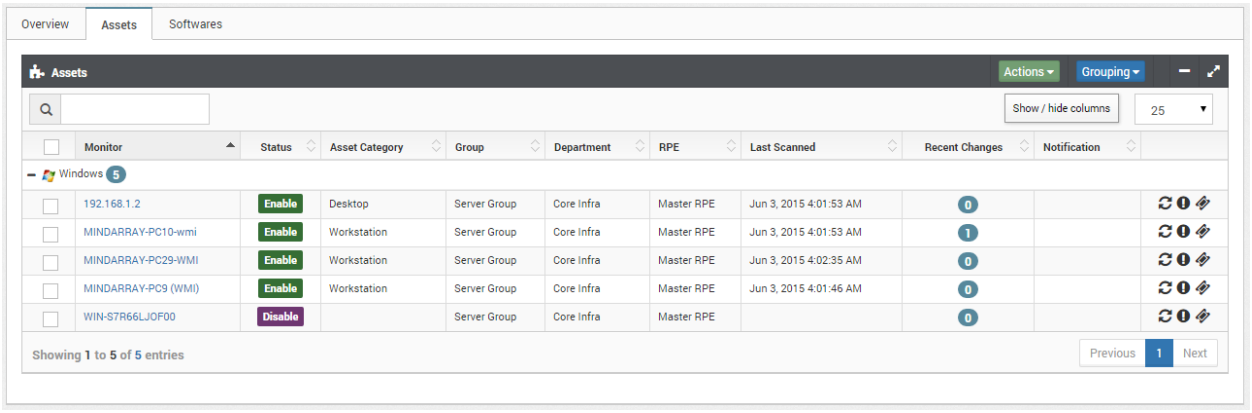


Figure 3.4 Service Discovery

However, if the monitor is not added or listed under Assets tab then follow the steps given below to add asset by running discovery:

1. Navigate to **Admin** > **Network Discovery** > **New** > **Asset**.

2. Provide **Name** for the discovery.
3. **IP/Host:** for single device
   IP Range: for multiple devices.
   CSV Import: for selected multiple devices. When you need all those devices again for discovery, directly import the CSV file.
   Note: Provide hostname and IP address of that host separated by commas in the CSV File.
   E.g. Mindarray-Host1, 192.168.1.101
   Mindarray-Host2, 192.168.1.102
4. Select **Department** from the list.
5. Select **RPE** from the list.
6. Select the **Device type** as Linux/Unix host asset or Windows host asset.
7. Provide the **Credential Profile**.
   Note: In case of Linux/Unix host asset provide SSH credentials and in case of Windows host asset provide WMI credentials.
8. Click on **Create** to add new asset discovery.
9. Click on **Run** to run the discovery.
10. Once finished, click on **View Result** to view classified devices.
11. Click on **Provision Object** to add selected device.

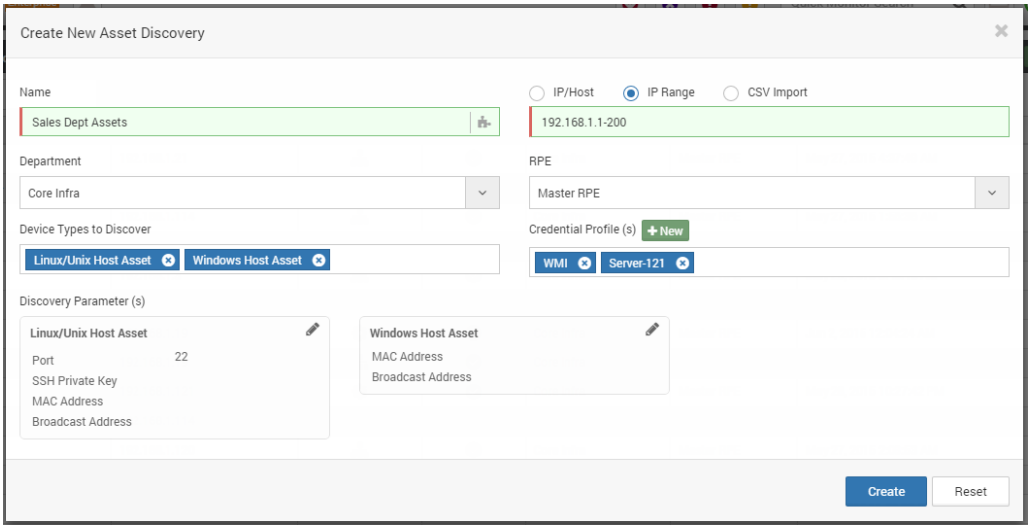


Figure 3.5 Asset Discovery

3.1.5. Example - Adding Hypervisors and Virtual Machines

Follow the steps given below to add hypervisors device by running network discovery:

1. Navigate to **Admin** > **Network Discovery** > **New** > **Device, Server & Apps.**
2. Provide the **Name** for the discovery.
3. **IP:** for single device
   IP Range: for multiple devices.
   CSV Import: for selected multiple devices. When you need all those devices again for discovery,

directly import the CSV file.

Note: Provide hostname and IP address of that host separated by commas in the CSV File.

E.g. Mindarray-Host1, 192.168.1.101

Mindarray-Host2, 192.168.1.102

4. Select the **Department** from the list.
5. Select the **RPE** (Remote Polling Engine) from the list.
6. **Ping Check Required** to check if ICMP is enabled. In case you wish to avoid ICMP check e.g. database does not need ping check, then you can disable the option.
7. Select **Device Type** from the list to be discovered such as Hyper-V Server, Citrix Xen Server, VMware ESX/ ESXi Server.

   Note: In this case also add respective resource type to be discovered - Hyper-V Virtual Machine, Xen Virtual Machine, Xen Network Interface, ESX Virtual Machine etc.
8. Provide **Credential Profile** (VMware/Hyper-V/Citrix).
9. Click on **Create** to create new discovery.
10. Click on **Run** to run the discovery
11. Once finished, click on **View Result** to view classified Hypervisors and Virtual Machines.
12. Click provision object to add selected devices.

    Note: Discovered Hypervisor node will be listed under Node tab, Virtual Machines with in Hypervisor will be listed under Virtual Machine Tab. Selected Objects should be displayed at top of pop-up the as total number of nodes, resources, applications, virtual machines.
13. Click on **Provision Object** add selected objects.

    Note: You can monitor virtual machines at both VM and Host level. To monitor them at host level provide the IP address range in New Discovery and select the device type as Windows\Linux\Unix.

3.1.6. Example - Add Network Device Monitor

To monitor network devices, the system can use:

- SNMP

Follow the steps given below to create Network Device Monitor:

1. Navigate to **Admin** > **Network Discovery** > **New** > **Device, Server & Apps**.
2. Provide the **Name** for the discovery.
3. **IP:** for single device

   IP Range: for multiple devices.

   CSV Import: for selected multiple devices. When you need all those devices again for discovery, directly import the CSV file.

   Note: Provide hostname and IP address of that host separated by commas in the CSV File.

   E.g. Mindarray-Host1, 192.168.1.101

   Mindarray-Host2, 192.168.1.102
4. Select the **Department** from the list.
5. Select the **RPE** (Remote Polling Engine) from the list.

6. Provide IP with one of the three options:
   IP: for single device
   IP Range: for multiple devices in a range.
   CSV Import: for only a number of selected multiple devices. When you need all those devices again for discovery, directly import the CSV file.
   Note: Provide hostname and IP address of that host separated by commas in the CSV File
   E.g. Mindarray-Host1, 192.168.1.101
   Mindarray-Host2, 192.168.1.102
7. Select the **Department** from the list.
8. Select the **RPE** (Remote Polling Engine) from the list.
9. **Ping Check Required** to check if ICMP is enabled. In case you wish to avoid ICMP check e.g. database does not need ping check, then you can disable the option.
10. Select **Device Type** from the list to be discovered. This includes types of devices namely Network Device, Server, Virtualization, Database Server, Application Server, Middleware, Platform and Web Server types
    Discovery Parameters: Also provide the required parameters to make the connection. E.g. Port number and Database instance name in case of Database discovery.
11. Provide the **Resource Type** to be discovered.
12. Provide **Credential Profiles** for SNMP Profile.
13. Click on **Create** to add new discovery.
14. Click on **Run** to run the discovery.
15. Once finished, click on **View Result** to view discovered Network Devices and Interfaces.
16. Click on **Provision Object** to add selected Nodes and Resources.
    Note: Discovered Network Device will be listed under Node tab. Selected Objects should be displayed at top of the pop-up as total number of nodes, resources.

The system starts monitoring for added objects and displays a confirmation message of the action.

3.1.7. Example - Add Server Monitor

To monitor servers, the system can use:

- SNMP
- SSH
- WMI

3.1.7.1. Adding Windows Monitor

MindArray Minder 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, change the associated SNMP polling method to WMI.

Prerequisites to add windows for monitoring

For monitoring the Windows environment using WMI, Minder Windows Service must necessarily be installed on a Windows machine. By default Windows Service is installed if Minder Server is installed on Windows machine. If you have deployed Linux version of Minder then Minder Windows Service must be installed on another Windows machine. For more information on installing Minder Windows Service, please see section: "Installing Windows Service for Linux Deployments". Besides, the device where Minder Windows Service 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.

Microsoft Windows Desktop and Server OS can be monitored using WMI and SNMP polling methods.

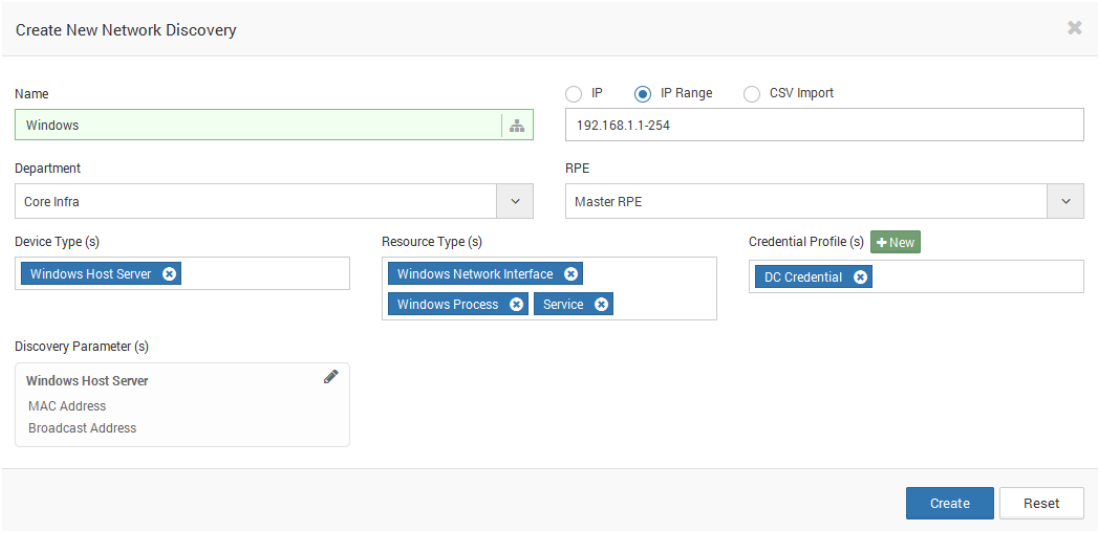


Figure 3.1.7.1 Adding Windows Monitor

Follow the steps given below to create windows server monitor:

1. Navigate to **Admin** > **Network Discovery** > **New** > **Device, Server & Apps.**
2. Provide the **Name** for the discovery.
3. **IP:** for single device

   IP Range: for multiple devices.

   CSV Import: for selected multiple devices. When you need all those devices again for discovery, directly import the CSV file.

   Note: Provide hostname and IP address of that host separated by commas in the CSV File.

   E.g. Mindarray-Host1,

   192.168.1.101

Mindarray-Host2,
192.168.1.102

4. Select the **Department** from the list.
5. Select the **RPE** (Remote Polling Engine) from the list.
6. Allow Ping check or disable the option.
6. Select the **Device Type** as SNMP Host server to monitor server resources using SNMP. For WMI select Windows Host Server
   Discovery Parameters: Also provide the required parameters to make the connection. **E.g.** In case of SNMP Host server Port number (For Server default port is #161).
7. Provide the **Resource Type** to be discovered, E.g. Interface, Process etc.
8. Provide **Credential Profiles** for device types.
9. Click on **Create** to create private network discovery.
10. Click on **Run** to run the network discovery.
11. Once finished, click on **View Result** to view classified devices.
12. Click on **Provision Object** to add selected device.
    Note: Discovered private network node will be listed under Node tab, Selected Objects should be displayed at top of the pop-up as total number of nodes, resources, applications.
13. Click on **Provision Object** to add selected objects.

The system discovers host to start monitoring and displays a confirmation message of the action.

3.1.7.2. Example - Adding Linux/Unix Monitor

Linux/Unix Server OS can be monitored using SHH and SNMP polling methods.

OS supported by MindArray Minder are:

- Linux
- Sun Solaris
- FreeBSD/OpenBSD
- HP UX/Tru64
- IBM AIX
- Mac OS
- Novell
- UnixWare

Follow the steps given below to create any of the above sever monitors:

2. Navigate to **Admin** > **Network Discovery** > **New** > **Device, Server & Apps.**
2. Provide the **Name** for the discovery.
3. **IP:** for single device
   IP Range: for multiple devices.
   CSV Import: for selected multiple devices. When you need all those devices again for discovery, directly import the CSV file.

Note: Provide hostname and IP address of that host separated by commas in the CSV File.
E.g. Mindarray-Host1, 192.168.1.101
Mindarray-Host2, 192.168.1.102

4. Select the **Department** from the list.
5. Select the **RPE** (Remote Polling Engine) from the list.
6. Allow Ping check or disable the option.
6. Select the **Device Type** as SNMP Host server to monitor server resources using SNMP. For SSH select Linux/Unix Host Server
   Discovery Parameters: Also provide the required parameters to make the connection. **E.g.** In case of SNMP Host server Port number (For Server default port is #161) For SSH default is port# 22.
7. Provide the **Resource Type** to be discovered, E.g. Interface, Jobs.
8. Provide **Credential Profile** for device types.
9. Click on **Create** to create network discovery.
10. Click on **Run** the network discovery to start discovery.
11. Once finished, click on **View Result** to view classified devices.
12. Click on **Provision Object** to add selected device.
    Note: Discovered private network node will be listed under Node tab, Selected Objects should be displayed at top of the pop-up as total number of nodes, resources, applications.
13. Click on **Provision Object** to add selected objects.

The system discovers host and displays a confirmation message of the action.

3.1.8. Troubleshoot Unknown Device in Network Discovery

System is not able to recognize the device due to many reasons:

1. Authentication failed.
2. System did not fetch OID.
3. WMI/SNMP services failed.
4. Failing of ping.
5. Port connection failed.
6. Server Error and many other.

Follow the steps given below to know about the reason:

1. Navigate to **Admin** > **Network discovery** > click on **View Result** icon of a particular discovery.

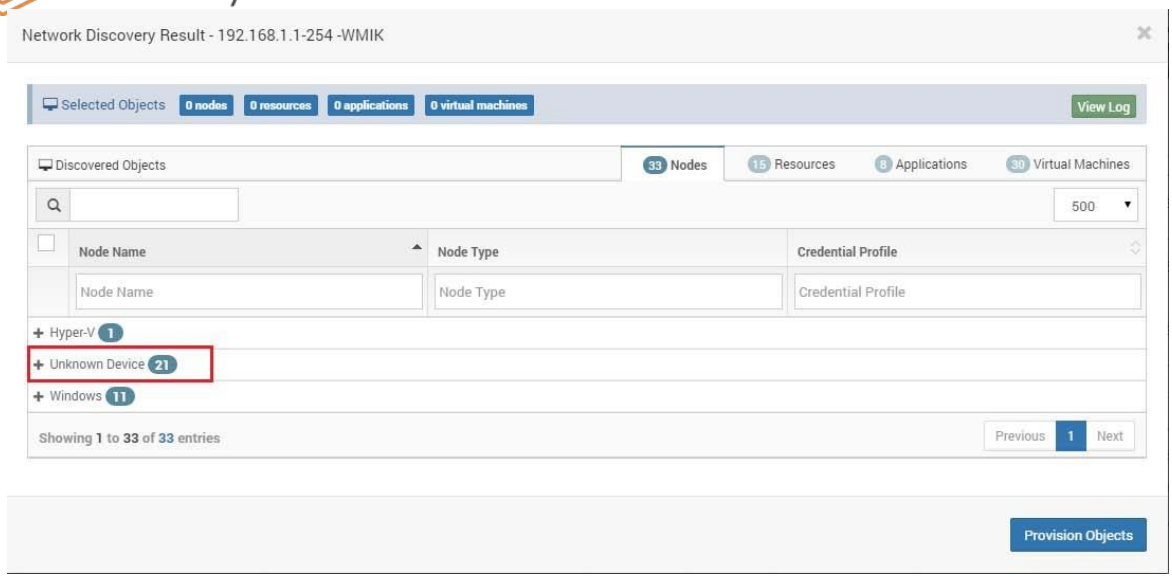


Figure 3.1.8.: Unknown Device

2. Under **Unknown Device** column, click on Click to Troubleshoot.

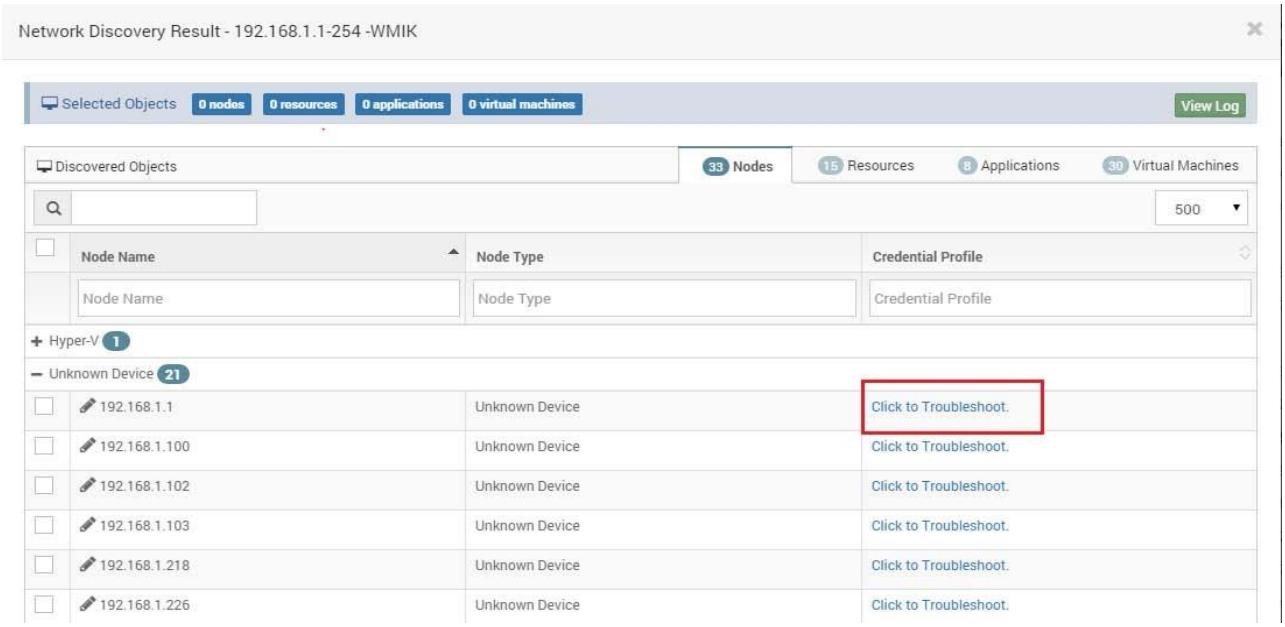


Figure 3.1.8.: Troubleshoot

3. Click on Troubleshoot; reason that why that device is not identified will be displayed.

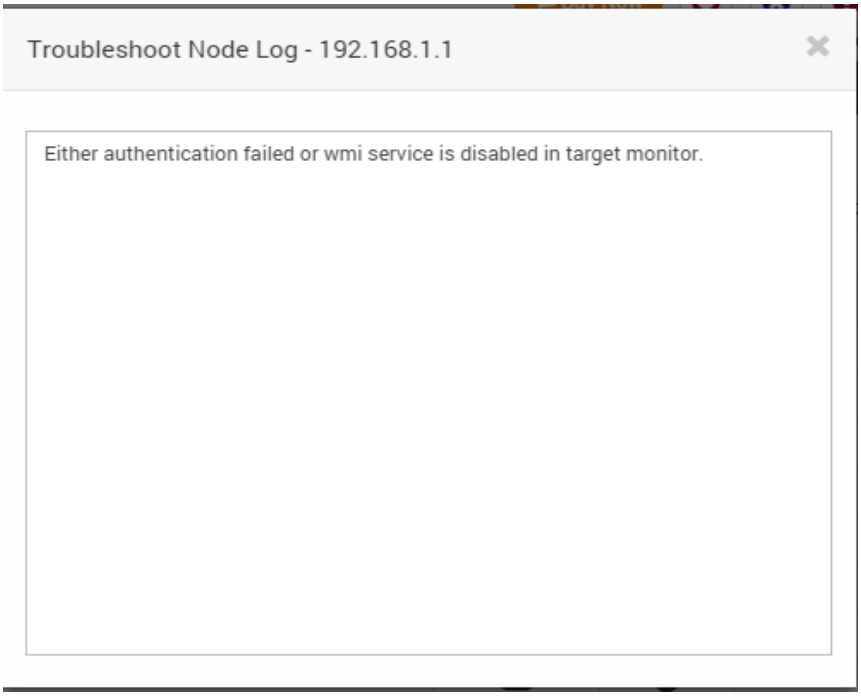


Figure 3.1.8.: Troubleshoot Node Log

Note: To check about Ping fail, port connection and system OID follow **section 6.10.**

3.1.9. Prerequisites to start monitoring

3.1.9.1. Prerequisites for Database Monitor

Database supported by MindArray Minder are:

1. Oracle
2. Microsoft SQL
3. MySQL
4. PostgreSQL
5. IBM DB2

3.1.9.2. Prerequisites for Oracle Database Monitor

In the Oracle database (that you are trying to monitor), ensure that the user name assigned to Minder has the permission to access the Oracle database from the host where Minder is running.

User Privilege: To create a new Oracle database monitor, you should have admin privileges.
Minimum User Privileges -> user with CONNECT and SELECT_CATALOG_ROLE roles.

To discover and add monitors, refer to **section 3.1.**

3.1.9.3. Prerequisites for MySQL Database Monitor

In the MySQL database (that you are trying to monitor), ensure that the user name assigned to Minder has the permission to access the MySQL database from the host where Minder is running. Else, give a relevant user who has the privileges to do the same.

Minimum User Privileges: The user should have privileges to execute SELECT, SHOW DATABASES and REPLICATION commands in the MySQL server. Also, Minder machine should be allowed to access the MySQL database server.

For enabling the privileges, execute the below commands in the remote MySQL Server

```
INSERT INTO user (Host, User) VALUES('<host>','<user>');
GRANT SELECT,SHOW DATABASES,REPLICATION CLIENT ON *.* TO '<user>'@'<host>';
FLUSH PRIVILEGES;
```

To discover and add monitors, refer to **section 3.1.**

3.1.9.4. Prerequisites for MSSQL Database Monitor

In the MSSQL database (that you are trying to monitor), ensure that the user name assigned to Minder has the permission to access the MSSQL database from the host where Minder is running.

Note: Minimum User Privileges required creating a new monitor of MSSQL:
User should be permitted to access MASTER database & MSDB database.
Roles: public + db_datareader should be selected for both MASTER and MSDB databases.

Database Accessed: Master
Permit in Database Role: db_datareader & requires **VIEW SERVER STATE** permission on the server.

To grant **VIEW SERVER STATE**, you can use any of the following methods:

1. Execute the following query

GRANT VIEW SERVER STATE TO username;

2. In SQL management studio for user choose Properties -> Securable -> Click **Add** (under securable) -> choose "**All objects of the Types...**" -> choose **Servers** -> choose **Grant** for "**View server state**" permission.

To discover and add monitors, refer to **section 3.1.**

3.1.9.5. Prerequisites for PostgreSQL Database Monitor

In the MSSQL database (that you are trying to monitor), ensure that the user name assigned to Minder has the permission to access the MSSQL database from the host where Minder is running.

Note: MINDER uses PostgreSQL subsystem statistics collector to monitor PostgreSQL server activity. By default statistics collector is accessible.

Also in **postgresql.conf** file, the parameter "**LISTEN ADDRESS**" has to be '*'.

To discover and add monitors, refer to **section 3.1.**

3.1.9.6. Prerequisites for DB2 Database Monitor

In the DB2 database (that you are trying to monitor), ensure that the user name assigned to Minder has the permission to access the DB2 database from the host where Minder is running.

User Privileged: To create a new DB2 monitor user should be able to access ***SYSPROC*** procedures.

To discover and add monitors, refer to **section 3.1.**

3.1.9.7. Prerequisites - Web Server Monitor

Web Servers supported by MindArray Minder is:

- Apache HTTP Server
- Microsoft IIS Server
- Nginx Server

3.1.9.8. Prerequisites - Apache HTTP Server Monitor

To monitor Apache Web Server the Server status and the Extended-status should be enabled to fetch additional information from Apache server.

Please enable mod_status on the HTTP server to get stats.

To Enable the **Server Status**, follow the steps given below:

1. In Apache's httpd.conf file, locate "Location /server-status" tag.
2. Remove the comment in the Location/Server-status tag, to Enable Set Handler server-status
3. Change the attribute "deny from all" to "Allow from all"

4. Remove the comment in "LoadModule status_module modules/mod_status.so".
5. Save the conf file and restart the Apache Server

To enable the **Extended-status**, follow the steps given below:

1. Locate "Extended Status" Attribute in httpd.conf file.
2. Remove the comment to enable the status.
3. Save the conf file and restart the Apache Server

To discover and add monitors, refer to **section 3.1.**

3.1.9.9. Prerequisites - Microsoft IIS Server Monitor

To monitor IIS server ensure that Minder has permission to access Windows server where IIS is hosted. Make sure Windows host server type is specified to be discovered while running the network discovery and WMI credential profile is provided to make the connection.

3.1.9.10. Prerequisites - Nginx Server Monitor

To monitor Nginx Server the Server Status should be enabled.

To Enable the Nginx Server Status, follow the steps given below:

6. Configure the location /server_status method in **<NGINX_HOME>/conf/nginx.conf** file, to enable server_status.
7. The value of stub_status attribute should be "on".
8. Change the attribute "deny all" to "Allow all".
9. Save the conf file and restart the Nginx Server.

3.1.9.11. Prerequisites - Application Server Monitor

The Application Servers supported by MindArray Minder is:

- JBoss
- Tomcat
- WebSphere
- WebLogic
- GlassFish
- Jetty

3.1.9.12. Prerequisites - JBoss Server Monitor

Note: MINDER uses **JMX** to monitor JBoss server. JMX should be enabled to retrieve the information from JBoss.

If JBoss is hosted on **Windows platform**, then there are two ways you can configure JMX in JBoss:

- Windows Service
- Windows Command Line

Configuring JMX in JBoss (tested on version 6.0)
Windows Service

1. Edit **%JBOSS_HOME%\bin\run.bat** by adding the following lines, where **%JBOSS_HOME%** is the path to your JBoss installation:

   set "JAVA_OPTS=%JAVA_OPTS% -
   Djavax.management.builder.initial=org.jboss.system.server.jmx.M
   BeanServerBuilderImpl"
   set "JAVA_OPTS=%JAVA_OPTS% -Djboss.platform.mbeanserver"
   set "JAVA_OPTS=%JAVA_OPTS% -
   Dcom.sun.management.jmxremote.port=8686"
   set "JAVA_OPTS=%JAVA_OPTS% -
   Dcom.sun.management.jmxremote.ssl=false"
   set "JAVA_OPTS=%JAVA_OPTS% -
   Dcom.sun.management.jmxremote.authenticate=false"
   …
   rem Setup JBoss specific properties
   set JAVA_OPTS=-Dprogram.name=%PROGNAME% %JAVA_OPTS%
   set "JAVA_OPTS=%JAVA_OPTS% -
   Djavax.management.builder.initial=org.jboss.system.server.jmx.M
   BeanServerBuilderImpl"
   set "JAVA_OPTS=%JAVA_OPTS% -Djboss.platform.mbeanserver"
   set "JAVA_OPTS=%JAVA_OPTS% -
   Dcom.sun.management.jmxremote.port=8686"
   set "JAVA_OPTS=%JAVA_OPTS% -
   Dcom.sun.management.jmxremote.ssl=false"
   set "JAVA_OPTS=%JAVA_OPTS% -
   Dcom.sun.management.jmxremote.authenticate=false"
   …
2. Register JBoss as a service by running: %JBOSS_HOME%\bin\service.bat

   Install.

3. Go to the Windows Services console.
4. Right-click JBoss Application Server service.
5. Click **Properties**.
6. Click the Log On tab and then select Log on as this account.
7. Click **Browse**, find the user “Administrator,” and then type the Administrator password twice.
8. Click **Ok**.
9. Start the JBoss service.

Windows Command Line

1. Edit **%JBOSS_HOME%\bin\run.bat** by adding the following lines, where

   %JBOSS_HOME% is the path to your JBoss installation

   ```
   set "JAVA_OPTS=%JAVA_OPTS% -
   Djavax.management.builder.initial=org.jboss.system.server.jmx.M
   BeanServerBuilderImpl"
   set "JAVA_OPTS=%JAVA_OPTS% -Djboss.platform.mbeanserver"
   set "JAVA_OPTS=%JAVA_OPTS% -
   Dcom.sun.management.jmxremote.port=8686"
   set "JAVA_OPTS=%JAVA_OPTS% -
   Dcom.sun.management.jmxremote.ssl=false"
   set "JAVA_OPTS=%JAVA_OPTS% -
   Dcom.sun.management.jmxremote.authenticate=false"
   …
   rem Setup JBoss specific properties
   set JAVA_OPTS=-Dprogram.name=%PROGNAME% %JAVA_OPTS%
   set "JAVA_OPTS=%JAVA_OPTS% -
   Djavax.management.builder.initial=org.jboss.system.server.jmx.M
   BeanServerBuilderImpl"
   set "JAVA_OPTS=%JAVA_OPTS% -Djboss.platform.mbeanserver"
   set "JAVA_OPTS=%JAVA_OPTS% -
   Dcom.sun.management.jmxremote.port=8686"
   set "JAVA_OPTS=%JAVA_OPTS% -
   Dcom.sun.management.jmxremote.ssl=false"
   set "JAVA_OPTS=%JAVA_OPTS% -
   Dcom.sun.management.jmxremote.authenticate=false":
   …
   ```

2. Start JBoss by running **%JBOSS_HOME%\bin\run.bat**.

For **Linux Platform** do the following:

1. Edit **$JBOSS_HOME/bin/run.sh** by adding the following lines, where **$JBOSS_HOME$** is the path to your JBoss installation:

```
JAVA_OPTS="$JAVA_OPTS -
Djavax.management.builder.initial=org.jboss.system.server.jmx.M
BeanServerBuilderImpl"
JAVA_OPTS="$JAVA_OPTS -Djboss.platform.mbeanserver "
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.port=8686"
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.ssl=false"
JAVA_OPTS="$JAVA_OPTS -
Dcom.sun.management.jmxremote.authenticate=false "
…
# Setup JBoss specific properties
JAVA_OPTS="${JAVA_OPTS:+$JAVA_OPTS -Dprogram.name=$PROGNAME}"
JAVA_OPTS="${JAVA_OPTS:--Dprogram.name=$PROGNAME}"
JAVA_OPTS="$JAVA_OPTS -
Djavax.management.builder.initial=org.jboss.system.server.jmx.M
BeanServerBuilderImpl"
JAVA_OPTS="$JAVA_OPTS -Djboss.platform.mbeanserver "
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.port=8686"
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.ssl=false"
JAVA_OPTS="$JAVA_OPTS -
Dcom.sun.management.jmxremote.authenticate=false "
…
```

2. Run JBoss by running **$JBOSS_HOME/bin/run.sh**.

3.1.9.13. Prerequisites - Tomcat Server Monitor

Note: MINDER uses **JMX** to monitor Tomcat server. JMX should be enabled to retrieve the information from Tomcat.

If Tomcat is hosted on **Windows platform**, then there are two ways you can configure JMX in tomcat:

- Windows Service
- Windows Command Line

Configuring Apache Tomcat (tested on version 7.0)
Windows Service

1. Open Tomcat configuration: Start > All Programs > Apache Tomcat > Configure Tomcat.
2. Open the **Java** tab and then add the following lines to the **Java Options** box:

-Dcom.sun.management.jmxremote

-Dcom.sun.management.jmxremote.port=6969

-Dcom.sun.management.jmxremote.ssl=false

-Dcom.sun.management.jmxremote.authenticate=false

3. Click **Apply**.
4. Go to the Windows Services console.
5. Right-click the Apache Tomcat service and then click **Properties**.
6. Click the **Log On** tab and then select Log on as this account.
7. Click **Browse** and find the user “Administrator” and type the Administrator password twice.
8. Click **Ok**.
9. In the Tomcat Configuration window, return to the General tab and then start the service.

Windows Command Line

1. Open the file %TOMCAT_HOME%\bin\catalina.bat and add the following lines into the Debug, Run and Start sections where %TOMCAT_HOME% is the path of your Tomcat installation:

set "JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote"

set "JAVA_OPTS=%JAVA_OPTS% -

Dcom.sun.management.jmxremote.port=8686"

set "JAVA_OPTS=%JAVA_OPTS% -

Dcom.sun.management.jmxremote.ssl=false"

set "JAVA_OPTS=%JAVA_OPTS% -

Dcom.sun.management.jmxremote.authenticate=false"

…

:doDebug

set "JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote"

set "JAVA_OPTS=%JAVA_OPTS% -

Dcom.sun.management.jmxremote.port=8686"

set "JAVA_OPTS=%JAVA_OPTS% -

Dcom.sun.management.jmxremote.ssl=false"

set "JAVA_OPTS=%JAVA_OPTS% -

Dcom.sun.management.jmxremote.authenticate=false"

shift

```
…
:doRun
set "JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote"
set "JAVA_OPTS=%JAVA_OPTS% -
Dcom.sun.management.jmxremote.port=8686"
set "JAVA_OPTS=%JAVA_OPTS% -
Dcom.sun.management.jmxremote.ssl=false"
set "JAVA_OPTS=%JAVA_OPTS% -
Dcom.sun.management.jmxremote.authenticate=false"
shift
…
:doStart
set "JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote"
set "JAVA_OPTS=%JAVA_OPTS% -
Dcom.sun.management.jmxremote.port=8686"
set "JAVA_OPTS=%JAVA_OPTS% -
Dcom.sun.management.jmxremote.ssl=false"
set "JAVA_OPTS=%JAVA_OPTS% -
Dcom.sun.management.jmxremote.authenticate=false"
shift
…
```

2. Run **%TOMCAT_HOME%\bin\startup.bat** to start Tomcat.

For **Linux Platform** do the following:

1. Open **$TOMCAT_HOME/bin/catalina.sh** and then add the following lines into the Debug, Run and Start sections, where **%TOMCAT_HOME%** is the path to your Tomcat installation:

```
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote"
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.port=8686"
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.ssl=false"
JAVA_OPTS="$JAVA_OPTS -
Dcom.sun.management.jmxremote.authenticate=false "
…
```

```
if [ "$1" = "debug" ] ; then
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote"
JAVA_OPTS="$JAVA_OPTS -
Dcom.sun.management.jmxremote.port=8686"
JAVA_OPTS="$JAVA_OPTS -
Dcom.sun.management.jmxremote.ssl=false"
JAVA_OPTS="$JAVA_OPTS -
Dcom.sun.management.jmxremote.authenticate=false "
if $os400; then
…
elif [ "$1" = "run" ]; then
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote"
JAVA_OPTS="$JAVA_OPTS -
Dcom.sun.management.jmxremote.port=8686"
JAVA_OPTS="$JAVA_OPTS -
Dcom.sun.management.jmxremote.ssl=false"
JAVA_OPTS="$JAVA_OPTS -
Dcom.sun.management.jmxremote.authenticate=false "
shift
…
elif [ "$1" = "start" ] ; then
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote"
JAVA_OPTS="$JAVA_OPTS -
Dcom.sun.management.jmxremote.port=8686"
JAVA_OPTS="$JAVA_OPTS -
Dcom.sun.management.jmxremote.ssl=false"
JAVA_OPTS="$JAVA_OPTS -
Dcom.sun.management.jmxremote.authenticate=false "
if [ ! -z "$CATALINA_PID" ]; then
…
```

2. Run the **$TOMCAT_HOME/bin/startup.sh** command to start Tomcat.

3.1.9.14. Prerequisites - WebSphere Server Monitor

Note: Minder uses **Performance Monitoring Infrastructure (PMI)** to monitor WebSphere. PMI should be enabled to retrieve information from WebSphere server.

To enable **PMI** do the following (tested version 7):

1. Check to see if PerfServletApp.ear is in the list
2. In the left pane, click **Monitoring and Tuning** and **Performance Monitoring Infrastructure (PMI)**.
3. Select your server. In the Configuration tab, enable the PMI and set All Statistics.
4. Set All Statistics in the Run time Tab.
5. Save all changes.
6. In the left panel, click Expand Servers and Server types.
7. Click WebSphere Application Servers.
8. In the main window, click your server.
9. In the Server Infrastructure section, expand Java and Process Management.
10. Click Process Definition.
11. In the Additional Properties section, click Java Virtual Machine.
12. In Generic JVM Arguments, add the following:

    -Djavax.management.builder.initial= -

    Dcom.sun.management.jmxremote
13. Save all changes.
14. Go to the Windows Services console.
15. Right –click the IBM WebSphere service.
16. Click Properties.
17. Click the Log On tab and then select Log on as this account.
18. Click Browse, find the user “Administrator,” and then type the Administrator password twice.
19. Click Ok.
20. Restart the IBM WebSphere Application Server.

3.1.9.15. Prerequisites - WebLogic Server Monitor

Prerequisite: To add support for WebLogic server, you need to copy the wlfullclient.jar from WebLogic installation. On your WebLogic host, navigate to the folder where the WebLogic server was installed. It is typically installed at Oracle/Middleware/wlserver_/server/lib.

Locate the wlfullclient.jar library.

For more information, refer to the following article:
http://docs.oracle.com/cd/E12840_01/wls/docs103/client/jarbuilder.html

For WobLog 9.x:
Copy the wlfullclient.jar library from folder *<WebLogic Home>/weblogic92/server/lib* in Remote WebLogic server version 9 to your MindArray Minder server. The target folder for these files is typically C:\Program Files\MindArray Systems\Minder\lib

For WobLog 10.x:
Copy *Weblogic.jar, wlclient.jar, wljmsclient.jar* from folder *<Weblogic Home>/wlserver_10.0/server/lib* in Remote WebLogic server version 10 to your MindArray Minder server. The target folder for these files is typically C:\Program Files\MindArray Systems\Minder\lib

Note: You will need to overwrite the existing files.

MINDER uses **JMX** to monitor WebLogic. JMX should be enabled to retrieve information from WebLogic server. To configure **JMX** do the following (tested version 7):

For Windows platform

1. Edit the following file, where %MIDDLEWARE_HOME% is the path of your WebLogic installation: %MIDDLEWARE_HOME%\C:\Oracle\Middleware\user_projects\domains\<your_domain>\bin\setDomainEnv.cmd

   Add the following lines to the end of the file:

   set "JAVA_OPIONTS=%JAVA_OPTIONS% -

   Dcom.sun.management.jmxremote"

   set "JAVA_OPTIONS=%JAVA_OPTIONS% -

   Dcom.sun.management.jmxremote.port=8686"

   set "JAVA_OPTIONS=%JAVA_OPTIONS% -

   Dcom.sun.management.jmxremote.ssl=false"

   set "JAVA_OPTIONS=%JAVA_OPTIONS% -Dcom.sun.management.jmxremote.authenticate=false"

2. Restart WebLogic Server.

For Linux platform

1. Edit the following file, where %MIDDLEWARE_HOME% is the path of your WebLogic installation: $MIDDLEWARE_HOME/user_projects/domains/<your_domain>/bin/setDomainEnv.sh

Add the following lines to the end of the file:

```
JAVA_OPTIONS="$JAVA_OPTIONS-Dcom.sun.management.jmxremote"
JAVA_OPTIONS="$JAVA_OPTIONS-Dcom.sun.management.jmxremote.port=8686"
JAVA_OPTIONS="$JAVA_OPTIONS-Dcom.sun.management.jmxremote.ssl=false"
JAVA_OPTIONS="$JAVA_OPTIONS  -Dcom.sun.management.jmxremote.authenticate=false"
```

2. Restart the WebLogic Server.

Note: If you are having difficulty configuring WebLogic to work with Java and/or SNMP, the JMX Java options may not be set in the proper place for your setup of WebLogic. Some implementations of WebLogic, under Windows, require the Java JMX options to be placed in a registry key, as opposed to the setDomainEnv.cmd file.

3.1.9.16. Prerequisites - Glassfish Server Monitor

Note: MINDER uses JMX to monitor Glassfish server. JMX should be enabled to retrieve the information from Glassfish.

To enable JMX in Glassfish do the following:

1. Run the Glassfish Application Server.
2. Open a web browser and then navigate to: http://hostname:4848, where hostname is the name of your Glassfish server.
3. In the left panel, click **Configurations: server-config**.
4. In the main window, click **JVM settings**.
5. Click the **JVM Options** tab.
6. Click **Add JVM Option** and then type -

   Djava.rmi.server.hostname=yourhostname.com in the blank field, where yourhostname.com is the hostname of your Glassfish server.
7. Click **Add JVM Option** and then type -

   Dcom.sun.management.jmxremote.ssl=false in the blank field.
8. Click **Add JVM Option** and then type -

   Dcom.sun.management.jmxremote.authenticate=false in the blank field.
9. Click **Save**.
10. Restart the Glassfish server.

By default, Glassfish uses JMX on port 8686. To change the JMX port you should find the “jmx-connector” section in: %GLASSFISH_HOME%\glassfish\domains\<your_domain>\config\domain.xml, where %GLASSFISH_HOME% is the path where Glassfish is installed, then change the port value.

3.1.9.17. Prerequisites - Jetty Server Monitor

Note: MINDER uses JMX to monitor Jetty server. JMX should be enabled to retrieve the information from Jetty.

To enable JMX in Jetty do the following:

1. Edit the JMX-Jetty.xml file located at in etc/jetty-jmx.xml.

```
<New id="ConnectorServer" class="org.eclipse.jetty.jmx.ConnectorServer">
 <Arg>
  <New class="javax.management.remote.JMXServiceURL">
   <Arg type="java.lang.String">rmi</Arg>
   <Arg type="java.lang.String" />
   <Arg type="java.lang.Integer"><SystemProperty name="jetty.jmxrmiport"
default="1099"/></Arg>
  <Arg type="java.lang.String">/jndi/rmi://<SystemProperty name="jetty.jmxrmihost"
default="localhost"/>:<SystemProperty name="jetty.jmxrmiport"
default="1099"/>/jmxrmi</Arg>
  </New>
 </Arg>
 <Arg>org.eclipse.jetty.jmx:name=rmiconnectorserver</Arg>
 <Call name="start" />
</New>
```

2. Edit the Start.ini in installation root, uncomment the following lines.

```
OPTIONS=jmx
jetty.jmxrmihost=localhost
jetty.jmxrmiport=1099
-Dcom.sun.management.jmxremote
etc/jetty-jmx.xml
```

3. Restart the Jetty server.

3.1.9.18. Prerequisites - Middleware Monitor

The Middleware supported by MindArray Minder is:

- Active Directory
- WebSphere Message Queue
- Active Message Queue
- Microsoft Message Queue

- Rabbit Message Queue

3.1.9.19. Prerequisites - Apache Active Message Queue Monitor

Minder uses JMX to monitor Apache Active MQ.
To enable JMX, following java runtime options needs to be added to your application:

Dcom.sun.management.jmxremote.
Dcom.sun.management.jmxremote.port=1111
Dcom.sun.management.jmxremote.ssl=false
Dcom.sun.management.jmxremote.authenticate=false

Note: Replace 1111 with your installation port. 1111 is default port.

3.1.9.20. Prerequisites - Rabbit Message Queue Monitor

Minder uses rabbitmq-management plugin to monitor Rabbit MQ.
The management plugin is included in the RabbitMQ distribution. To enable it, use rabbitmq-plugins:

rabbitmq-plugins enable rabbitmq_management

Note: User must have “Monitoring” level privileges.

4 Working with Monitors

This section provides information and procedures for managing monitors in the system.

4.1 Viewing the Monitor List

The Monitor list under Monitors shows all monitors in the system. From this view, you can search for monitors and perform a range of management tasks on all monitors.

To access the monitor list navigate to **Monitors** > **Monitors**.

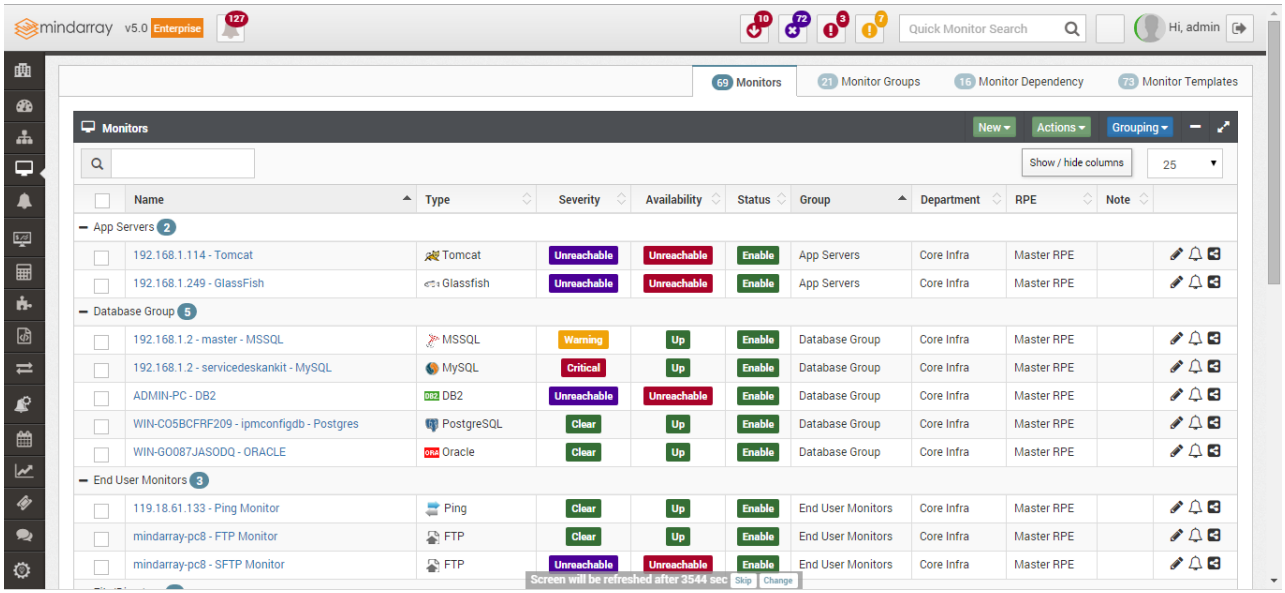


Figure 4.1 Monitor List

4.2 Monitor List

Monitors are organized in the Grid view by:

- Monitor Name
- Monitor Type
- Severity
- Availability
- Status
- Group
- Department
- RPE
- Note
- Edit – Manage Alarms – Shared details

1. Click the **Monitor Name** column header to sort by name.
2. Click **Show/Hide** column button to add/remove columns in the grid.
3. Drag and shift the columns according to your preference..

4.3 Managing Monitors from the Monitor List

You can perform some management tasks for monitor at a time. You can:

- Edit individual monitor. (Change name & polling intervals, Enable/Disable metrics etc.)
- Enable/Disable/Delete Alarms.
- Assign monitors to Departments/Users (Share Monitor).

4.4 Managing Monitor and Performance Attributes

Read the information and procedures in this section to learn about specific monitor management tasks, including

- Renaming monitor
- Enabling performance attributes & polling interval
- Changing monitor credentials
- Changing monitor RPE
- Changing monitor department
- Deleting a monitor
- Disabling a monitor
- Maintenance state

4.5 Renaming Monitor

Because the system uses the manage IP to monitor a device, the device name may be different than its fully qualified domain name (FQDN).

Follow the steps given below to rename a monitor:

1. Navigate to **Monitors** > **Monitors**.
2. Click **Edit** button of Monitor. The Update Monitor page appears in new window.
3. Click **Edit** button of Monitor name. The Update property pop-up appears.
4. Enter the new name for the monitor and then click **Update**.

The system renames the monitor and displays a confirmation message of the action.

4.6 Enabling Performance Metrics (Components)

To enable or disable performance metrics (components) from multiple monitor:

1. Navigate to **Monitors** > **Monitors**.
2. Click on **Action** > **Polling Scheduler** towards the top right corner of the grid.
3. Click **Edit** to enable/disable metrics and their polling time as well.
4. Click **Update**.

To enable or disable performance metrics (components) from single monitor:

1. At the top of the Monitor overview page, navigate to **Actions** > **Polling Scheduler**. The Update Polling Scheduler page appears in new window.
2. Choose **Performance Metrics** to enable/disable.
3. Provide **Polling Time** in seconds.
4. Click **Update.**

The system enables/disables performance attributes for the monitor and displays a confirmation message of the action.

Note: Polling interval must always be multiply by 10. Minimum supported polling interval is 30 seconds for any metric category.

4.7 Changing Monitor Credentials

To change password or to apply new credentials in the system, go to the section titled "Credential Profile."

Note: You can change Monitor profiles attached to monitor but attached polling method cannot be changed. You must create new monitor if you later decide to monitor node using different polling method.

To change applied polling credential profile from monitor:

5. Navigate to **Monitors** > select the **Monitor**.
6. Click **Edit** button of Monitor. The Update Monitor page dialog appears.
7. Click **Edit** button of Credential Profile. The Update property pop-up appears.
8. Change credential profile from the dropdown menu.
9. Click **Update.**

The system updates new credential for the monitor and displays a confirmation message of the action.

4.8 Changing RPE (Remote Polling Engine) of Multiple Monitors

To change/update RPE into multiple monitors:

1. Navigate to **Monitors** > **Monitors** tab.
2. Select monitors from the list.
3. Click **Action** > **Manage RPE**.
4. Select **RPE** you want to apply from the dropdown list.
   Note: To manage RPE navigate to **Admin Panel** > **RPE**.
5. Click **Update.**

The system updates new RPE for selected monitors and displays a confirmation message of the action.

Note: Monitor Location will be inherited from the RPE location.

4.9 Deleting a Monitor

To delete a monitor from the system, follow the steps given below:

1. Navigate to **Monitors** > **Monitor**.
2. Select monitors from the list, click **Delete** button under Actions.
3. Click **Yes.**

The system removes the monitors and associated data from Database and displays a confirmation message of the action.

4.10 Disabling a Monitor

To disable single/multiple monitors from the system, follow the steps given below:

1. Navigate to **Monitors** > **Monitor**.
2. Select monitors from list, navigate to Actions > **Disable**.
3. Click **Yes.**

The system disables the monitors and displays a confirmation message of the action.

Note: Core monitoring and alerting applied to an individual monitor is also disabled.

4.11 Maintenance State

Maintenance state allows scheduled production changes of a monitor or all monitor in a system. You might want to set up a maintenance state, for example, to prevent alerts and warnings while you perform configuration changes or reboot a device.

To change a monitor state from enabled to maintenance on single/multiple monitors follow the steps given below:

1. Navigate to **Monitors** > **Monitor**.
2. Select monitors from the list.
3. Click **Action** > **Maintenance Mode On/Off**.
4. Choose Infinite or scheduled time to turn off maintenance automatically.
5. Click **Update.**

The system changes the monitor state as Maintenance and displays a confirmation message of the action.

Note: Core monitoring and alerting applied to an individual monitor is also disabled and only monitor availability is enabled for this state (Availability will be marked as Maintenance mode).

4.12 Move/Change Department of Single/Multiple Monitors

Warning: Moving a monitor permanently from one department removes the monitor and affects all the SLA, Business Services, Widget and Reports associated with that monitor in source department. In addition, any attached credential profile created by that department's administrator/users is permanently moved to target department. For more information about security see section Security.

To change/update Department into multiple monitors, follow the steps given below:

1. Navigate to the **Monitors** > **Monitors**.
2. Select monitors from the list.
3. Click **Action** > **Move Department**.
4. Select **Department** from the dropdown list to move monitors.
   Note: To manage Department navigate to Admin Panel > Departments.
5. Click **Move.**

The system updates new Department for selected monitors and displays a confirmation message of the action.

4.13 Sharing Monitors to other Departments/Users

Warning: Departments are permission-based entities that comprise the Minder security model. We recommend that you read the review security section ***14*** before making changes to department.

Minder allows you to share monitors to other department with Full-access or Read-Only permission. When a monitor is shared to another department, any new changes done after the share are automatically shared or visible to the target department.

Warning: The credential profile attached to monitor is available to target department if share type is Full-access.

Sharing Entities:

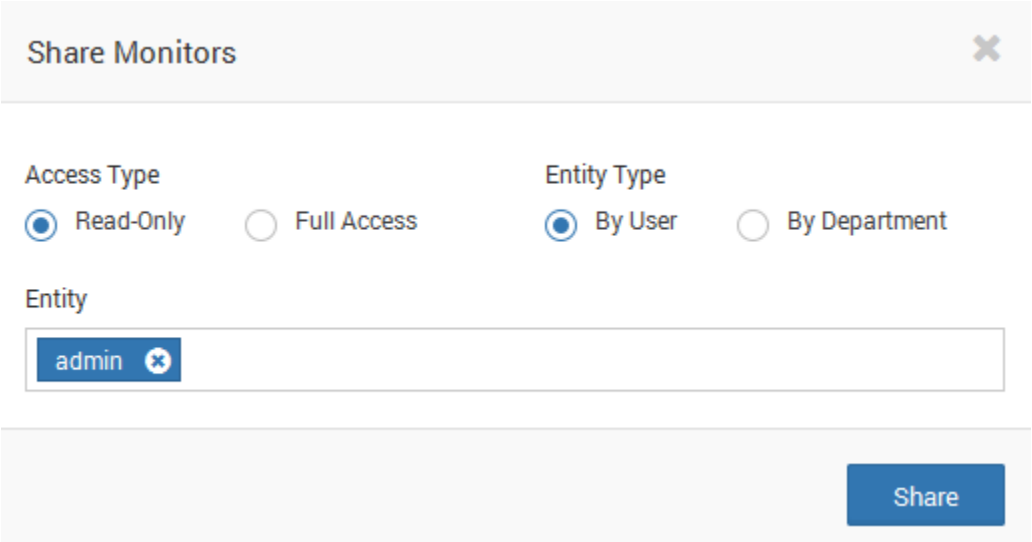


Figure 4.2.Share Monitor to other department/user

Follow the steps given below to share monitor to other department or user:

1. Navigate to **Monitors** > **Monitors**.
2. Select the monitors you want to share.
3. Click **Share** button under Actions menu. Share monitor dialog appears.
4. Choose the **Access** as Read-only or Full-access.
5. Choose whether you want to share to other user of all the user of other department.
6. Click **Share**.

The system now makes the monitor visible to specified department/user and displays confirmation message of the action.

Note: Sharing monitor to other user/department also gives the read-only access to users belong to target department.

4.14 Monitor Groups

To create a Monitor Groups, follow the steps given below:

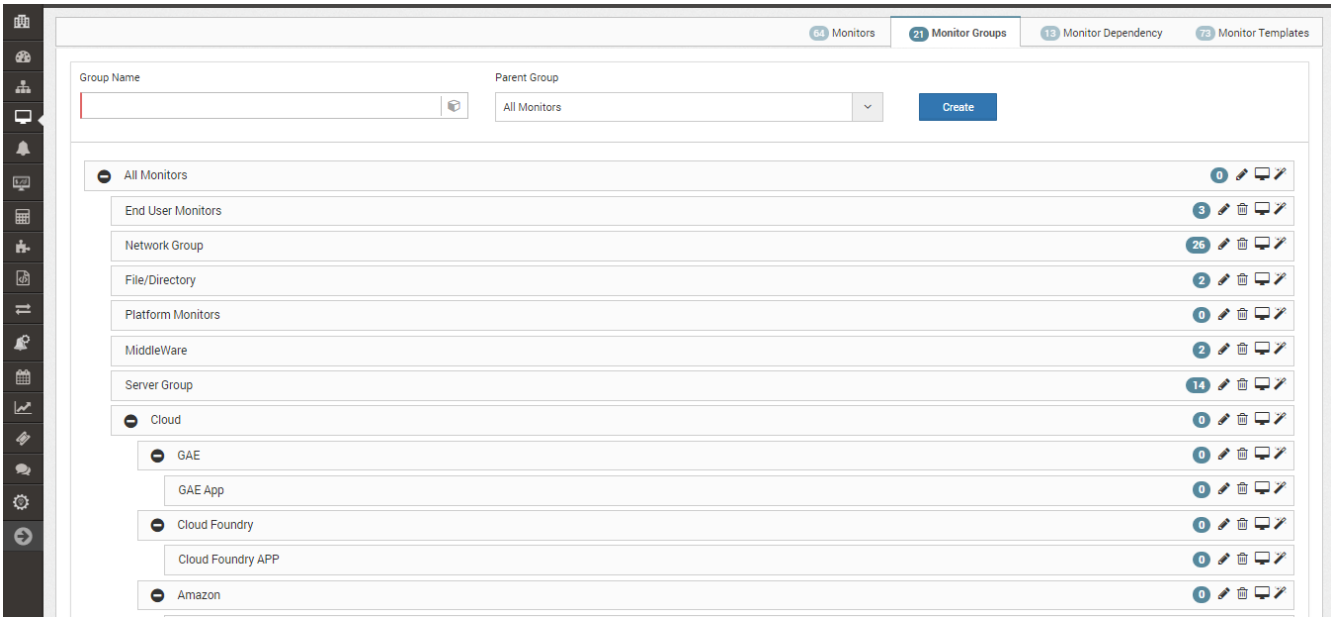


Figure 4.3 Monitor Groups

1. Navigate to **Monitors** > **Monitor Groups**.
2. Provide the Monitor **Group Name**.
3. Select **Parent Group** from the list.
4. Click **Create.**

The system will create Monitor Group and displays confirmation message of the action.

4.15 Assign Monitors Group

Once Monitor group is created, you can set the business rules to automatically assign new monitors to the group.

Follow the steps given below to manually assign monitors to specific group:

1. Navigate to **Monitors** > **Monitor Groups** > Navigate to Group Bar.
2. Click on **Assign Monitors** icon.
3. Select the **Monitors** from the list.
4. Click **Assign Monitors**.

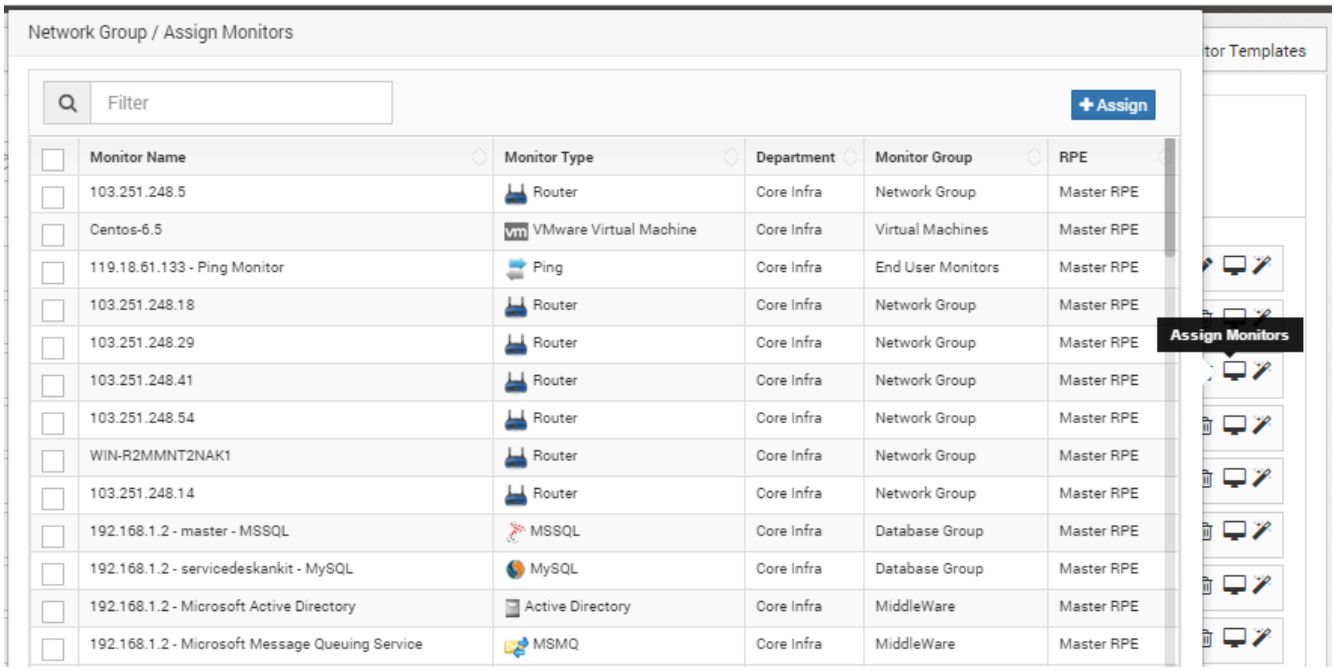


Figure: 4.4 Monitor Group Rules

Follow the steps given below to automatically assign monitors to specific group:

1. Navigate to **Monitors** > **Monitor Groups** > Navigate to Group Bar.
2. Click on **Group Rules** icon. Group Rule dialog appears.
3. Provide the condition to match rule when new monitor is created.
   Note: you can specify multiple rules to match.
4. Click **Update.**

The system will now apply the rules whenever new monitor is created and displays confirmation message of the action.

4.16 Monitor Dependency

Minder automatically creates monitor topology using multiple tools. Dependency is created using multiple technologies such as Switch port mapping, routing table information etc.

Monitor dependency is used to apply correlation and to derive business impact on business service. If you want to map parent child relationship – you should update the Monitor Dependency.

Follow the steps given below to update monitor dependency:

1. Navigate to **Monitors** > **Monitor Dependency** tab.
2. Click on **New** > **Monitor Dependency** dialog appears.
3. Select the monitor from the list. Click on Add button under Dependent monitor grid.
4. Select the dependent monitors.
5. Click **Create.**

The system creates new monitor dependency and displays confirmation message of the action.

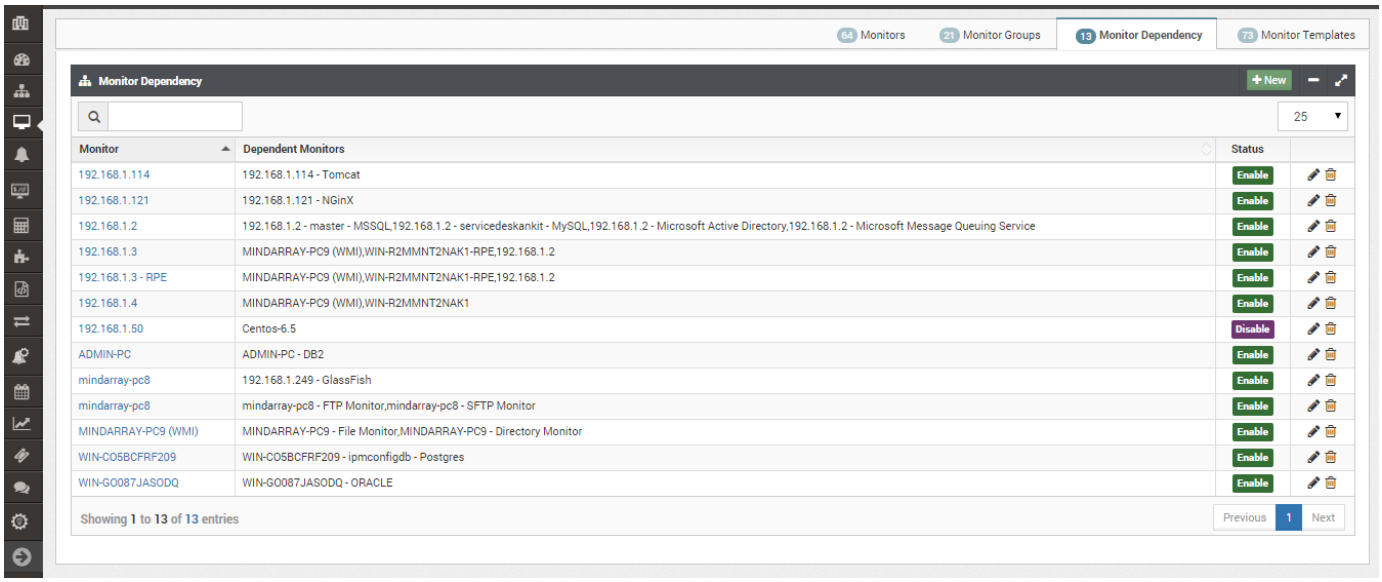


Figure 4.5 Monitor Dependency

4.17 Monitor Templates

Minder supports custom monitoring templates. By default system assigns the default template when new monitor is created. You can customize the default template or create new blank template and customize it based on your needs and then assign it to monitor types.

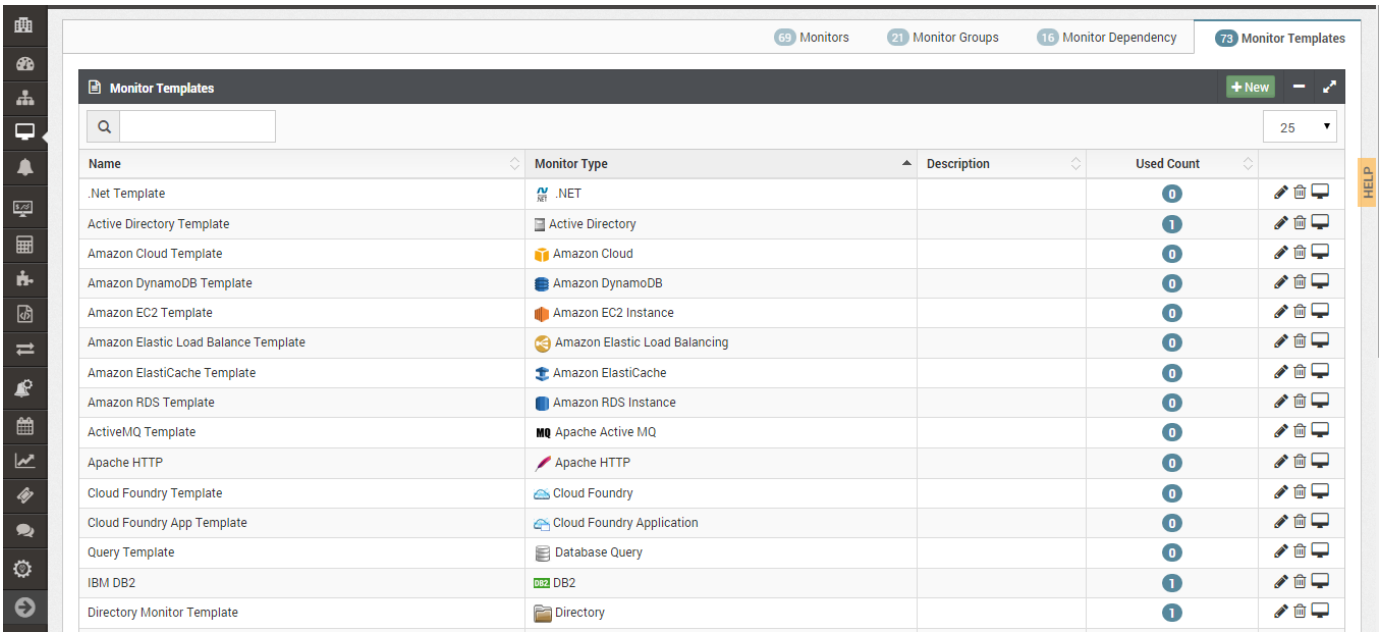


Figure 4.6 Monitor Template

Follow the steps given below to create monitor templates:

1. Navigate to **Monitors** > **Monitor Templates.**
2. Click **Add** to create new blank template. **New Template** dialog appears.
3. Select the monitor type from the list.
4. Click **Create**.

The system will create Monitor Templates and overrides the existing template and displays confirmation message of the action.

Note: Once new template is assigned, navigate to monitor overview page > click on Add widgets to customize it. It will be updated to all the monitors within specific monitor type.

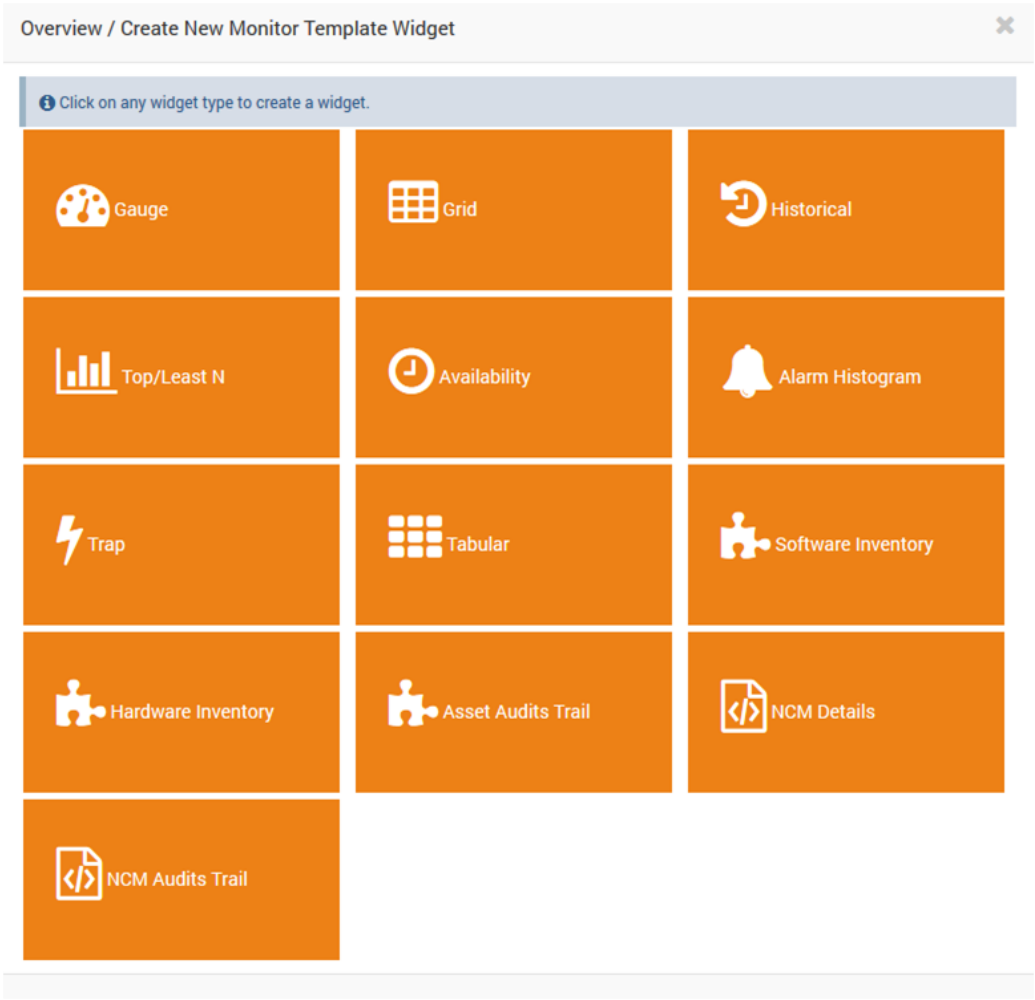


Figure 4.7 Monitor Template Widgets

5 Core Monitoring

Read the following sections for more information about basic and advanced monitoring, including:

- Availability monitoring
- Performance monitoring
- SNMP monitoring
- Monitoring devices remotely through SSH
- Monitoring windows devices
- Inventory Monitoring
- IP-SLA monitoring
- End User monitoring
- Infrastructure monitoring

5.1 Polling scheduler

Minder checks for any information at every specified amount of interval. These intervals can be different for different type of information based on Availability, Disk, CPU, Process, Network, Performance etc. A single metric consists of multiple attributes. For example, Memory Manager consists of Utilized and free memory of different types such as Physical, Virtual and Dynamic Memory.

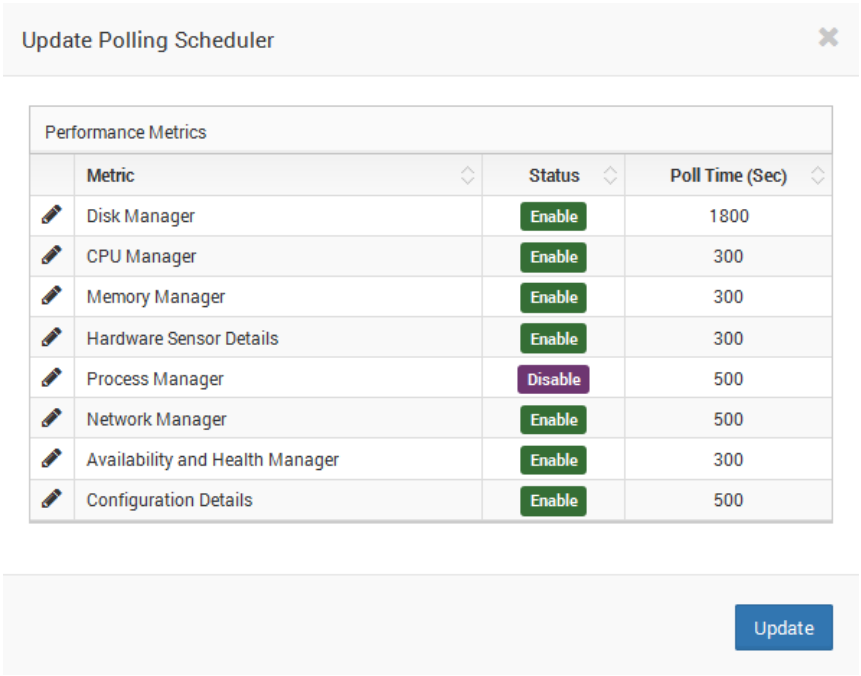


Figure 5.1 Update Performance Metrics

Follow these steps to enable the any metric and modify the polling cycletime.

1. Navigate to **Monitors** > **Monitors**.
2. Select the monitor to enable/disable Availability metric. Navigate to **Actions** > **Polling Scheduler**.
3. Click **Edit** to enable/disable Availability.
4. Select the **polling interval** in seconds.
5. Click **Update.**

The system enables the respective metric monitoring and displays a confirmation message of the action.

5.2 Availability Monitoring

The Availability service lets you manage and monitor devices and system that are running in your network.

You can check your availability from the List of Monitors as shown in the screenshot.

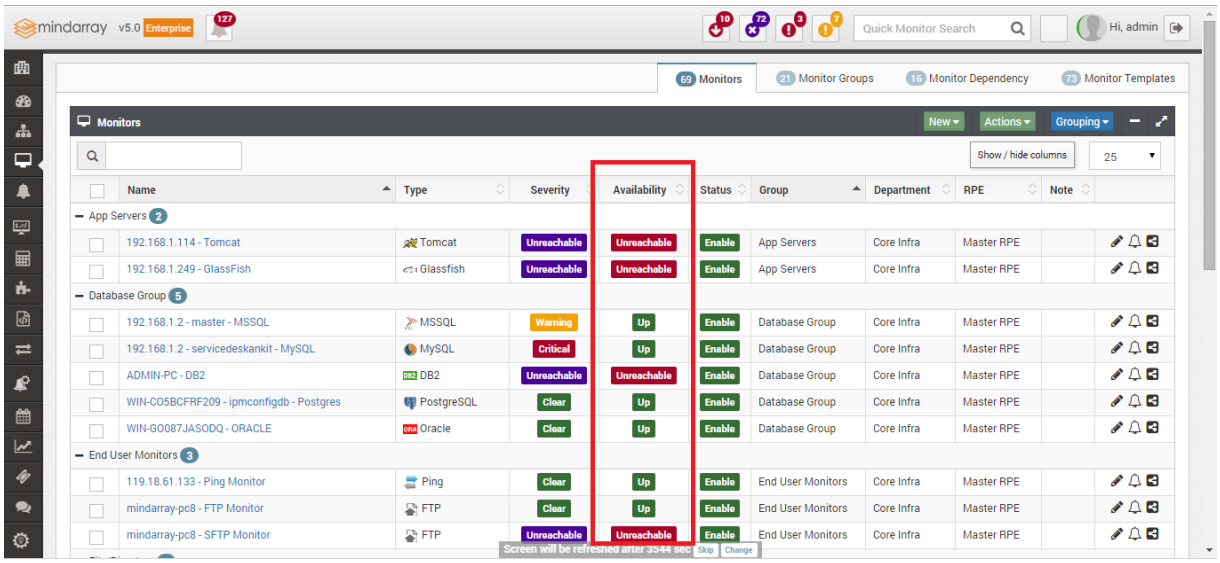


Figure 5.2 Monitor Availability

5.3 Performance Monitoring

Minder uses several methods to monitor performance metrics of monitors and monitor components. These are:

- **Process Manager** - Collects data of added processes through configured polling method from any system correctly configured for Process monitoring.
- **Service Manager (Supports only WMI polling method)** - Allows availability monitoring of Windows services from Windows servers.
- **CPU Manager** - Logs in to devices (by using configured polling method) and collects CPU performance data.

- **Memory Manager** - Logs in to devices (by using configured polling method) and collects Memory performance data.
- **Disk Manager** - Logs in to devices (by using configured polling method) and collects Disk performance data.
- **Network Manager** - Logs in to devices (by using configured polling method) and collects Network performance data.
- **End User Monitoring** - Checks the availability and responsiveness of Web pages, Script, Mail, FTP and others.

Regardless of the monitoring method used, the system stores performance monitoring configuration information in monitoring templates.

5.4 Monitoring Processes

When enabled, the system can monitor the availability and performance attributes of all provisioned processes running on monitor in your network.

Follow the steps to provision the processes and services for monitoring:

1. Navigate to **Monitors** > **Monitors.**
2. Open the monitor for which you want to start monitoring the processes**.**
3. Navigate to **Actions** > **Rediscover**. The Unprovisioned objects would be listed here.
4. Select the unprovisioned objects you wish to monitor and click on Add.

Follow these steps to enable the Process monitoring and modify the polling cycle time:

1. Navigate to **Monitors** > **Monitors.**
2. Select the monitor to enable/disable Process metric. Navigate to **Actions** > **Polling Scheduler.**
3. Click **Edit** to enable/disable Process Metric.
4. Provide the **Poll Time** in seconds.
5. Click **Update.**

The system enables Process monitoring for selected monitor and displays a confirmation message of the action.

5.5 Adding a Process for Availability and Performance Monitoring

To rediscover and add process in process host navigate to Process monitor detail page and follow the steps given below:

1. Navigate to **Monitors** > **Monitors** > select a monitor.
2. Click on **Action** > **Rediscover**.

3. Rediscover dialog appears with list of Provisioned and un-provisioned processes.
4. Select a process to add for monitoring.
5. Click **Add.**

Figure 5.3 Rediscovering the Monitor (Add Process)

The system adds selected Processes for monitoring and displays a confirmation message of the action.

Note: If a process has multiple instances, the system will calculate the average of CPU and memory utilization of instance processes as well as the count of total instances running. However, if the process has only a single instance, CPU utilization and memory usage will be graphed for the single process.

5.6 Monitoring Windows Services

To rediscover and add service in windows host navigate to Windows monitor detail page and follow the steps given below:

1. Make sure the service manager is enabled for the monitor by navigating to **Actions** > **Polling Scheduler**.
2. Once enabled, Navigate to **Actions** > **Rediscover**.
3. The dialog will load the provisioned and un-provisioned service on the host.
4. Select the service to provision for monitoring.
5. System will now add selected service for monitoring and service will load under Service tab once next poll is finished.

The system enables service monitoring for selected monitor and displays a confirmation message of the action.

5.7 Adding a Service for Availability Monitoring

Follow these steps given below to select a service to monitor, or edit monitoring choices for a service:

1. Make sure the Service manager is enabled for the monitor by navigating to **Actions** > **Polling Scheduler**.
2. Once enabled, navigate to **Actions** > **Rediscover**.
3. The dialog will load the provisioned and un-provisioned availability service on the host.
4. Select the availability service to provision for monitoring.
5. System will now add selected availability service for monitoring and service will load under Service tab once next poll is finished.

The system adds selected Services for monitoring and displays a confirmation message of the action.

5.8 Enabling CPU Monitoring

Follow these steps to enable the CPU monitoring and modify the polling cycle time.

1. Navigating to **Monitors** > Select the monitors to enable/disable CPU Monitoring.
2. Navigate to **Actions** > **Polling Scheduler** towards the top right corner of the monitor grid.
3. Click **Edit** to enable/disable CPU Manager, provide the **Poll Time** in seconds.
4. Navigate on **Actions** > **Poll Now** under the monitor overview page to see the latest CPU performance data.

The system enables CPU monitoring for selected monitor and displays a confirmation message of the action.

5.9 Enabling Memory Monitoring

When monitoring a Memory performance data, the Memory manager is selected by default, but you may not want to monitor Memory on some devices. In this case, you can disable its monitoring on those monitors.

Follow these steps to enable the Memory monitoring and modify the polling cycle time.

1. Navigating to **Monitors** > Select the monitors to enable/disable Memory Monitoring.
2. Navigate to **Actions** > **Polling Scheduler** towards the top right corner of the monitor grid.
3. Click **Edit** to enable/disable Memory Manager, provide the **Poll Time** in seconds.
4. Navigate to **Actions** > **Poll Now** under the monitor overview page to see the latest Memory performance data.

The system enables Memory monitoring for selected monitor and displays a confirmation message of the action.

5.10 Enabling Disk Monitoring

When monitoring a Disk performance data, the Disk manager is selected by default, but you may not want to monitor Disk on some devices. In this case, you can disable its monitoring on those monitors. Follow these steps to enable the Disk monitoring and modify the polling cycle time.

1. Navigating to **Monitors** > Select the monitors to enable/disable Disk Monitoring.
2. Navigate to **Actions** > **Polling Scheduler** towards the top right corner of the monitor grid.
3. Click **Edit** to enable/disable Disk Manager, provide the **Poll Time** in seconds.
4. Navigate to **Actions** > **Poll Now** under the monitor overview page to see the latest disk performance data.

The system enables Disk monitoring for selected monitor and displays a confirmation message of the action.

5.11 Monitoring Network Cards and Interfaces

When enabled, the system can monitor the availability and performance data of all interfaces running on monitor in your network.

Follow these steps to enable the Network monitoring and modify the polling cycle time.

1. Navigate to **Monitors** > **Monitors**.
2. Select the monitor to enable/disable Network metric. Navigate to **Actions** > **Polling Scheduler**.
3. Click **Edit** to enable/disable Network Metric.
4. Provide the **Poll Time** in seconds.
5. Click **Update.**

The system enables Network monitoring for selected monitor and displays a confirmation message of the action.

5.12 Adding a Network Interface for Availability and Performance Monitoring

To select a network card and interface to monitor, or edit monitoring choices for a network card and interface, follow these steps:

1. Make sure the Network Interface is enabled for the monitor by navigating to **Actions** > **Polling Scheduler**.
2. Once enabled, navigate to **Actions** > **Rediscover**.
3. The dialog will load the provisioned and un-provisioned Network Interface monitoring on the host.
4. Select the Network Interface to provision for monitoring.

5. System will now add selected Network Interface for monitoring and data will load under Network tab once next poll is finished.

The system adds selected Interfaces for monitoring and displays a confirmation message of the action.

5.13 Real Time Interface Details

For any provisioned interface, you can change the polling time as per your requirements. But, Minder does not allow you to have a polling time of less than 30 seconds. So, instead of waiting for the next poll, Minder allows you to get real time interface details where you can check the current statistics.

Follow the steps given below to check the real time interface details:

1. Navigate to **Monitors** and select any server or network device. You can also search the monitor you want from the **Quick Monitor Search** box available at the top.
2. An overview page for the selected monitor opens.
3. Navigate to **Actions** > **Real Time Interface Details**.
4. **Real Time Interface Details** dialog appears where you can see the statistics graph of the selected interface.
5. You can also **Pause** or change the **Time Interval** for real time viewing.

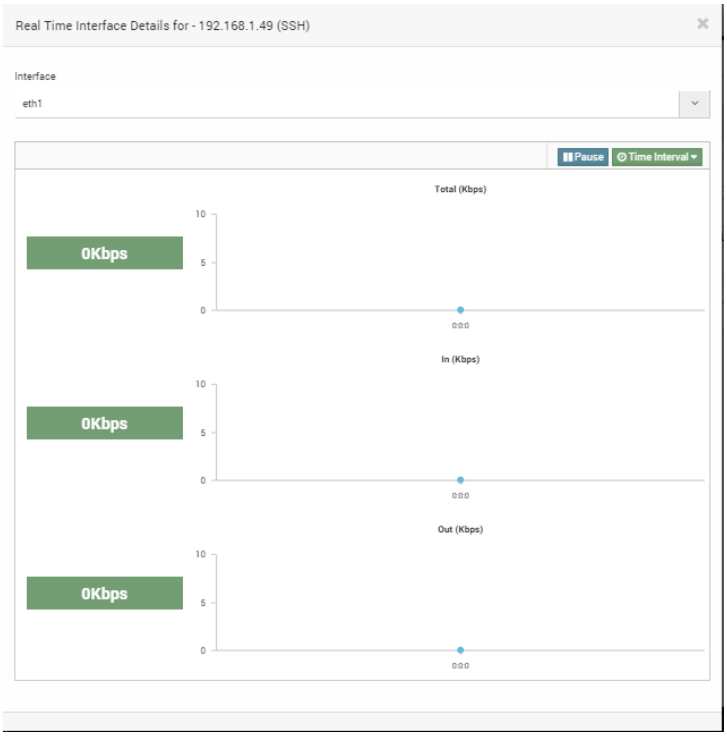


Figure 5.4 Real Time Interface Details

Note: Only the interfaces that you have provisioned will be displayed in the interface drop down list.

5.14 Task Manager

This feature allows you to view all the processes running on a specific Linux or Windows server, along with its CPU and Memory Utilization.

Follow the steps given below to view the task manager:

1. Navigate to **Monitors** and select any server or network device. You can also search the monitor you want from the **Quick Monitor Search** box available at the top.
2. An overview page for the selected server opens.
3. Navigate to **Actions** >**Task Manager**.
4. **Task Manager** Dialog appears where you can see a list of all the processes along with their CPU and Memory Utilization and User for the selected server.
5. You can also **Pause** or change the **Time Interval** for real time viewing.

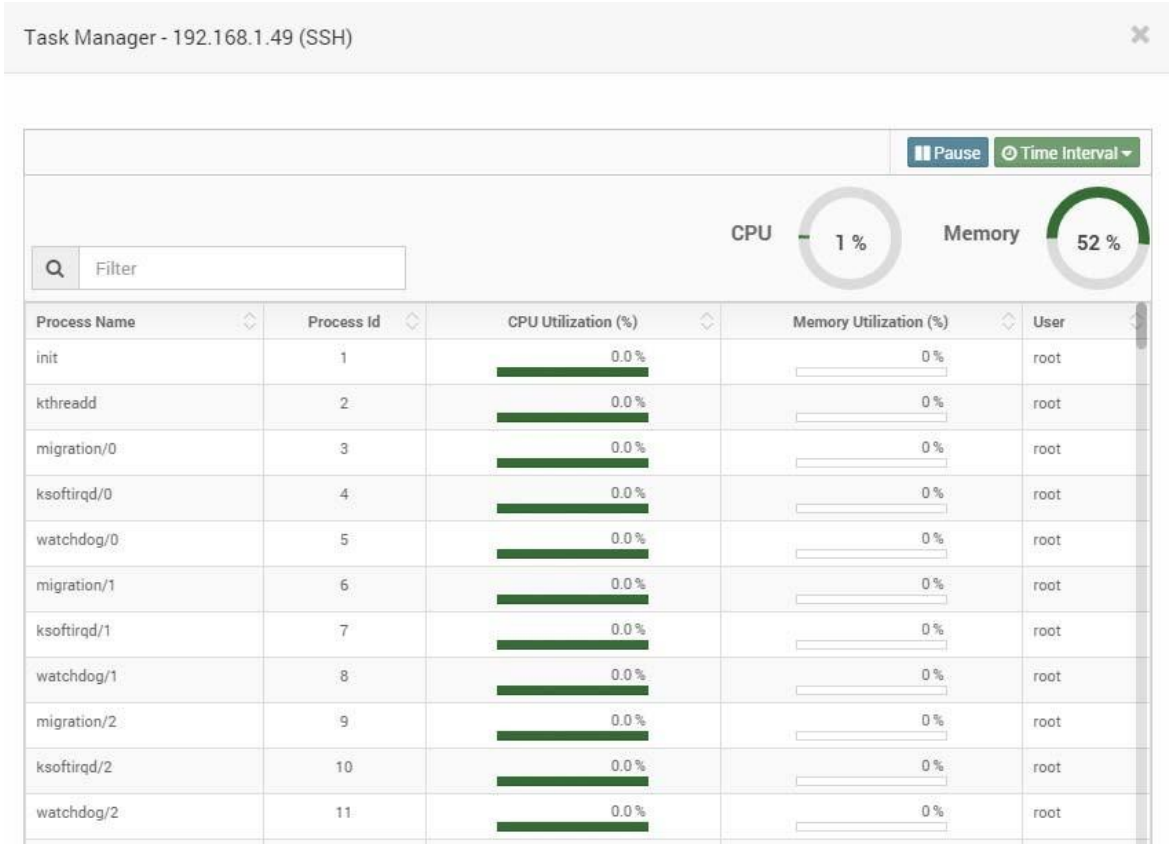


Figure 5.5 Task Manager

5.15 Asset Monitoring

Asset monitoring is one of the features that allow user to monitor software assets as well as hardware

assets. Assets are classified as:

1. Software Assets- software like .Net, Adobe Reader, Skype etc.
2. Hardware Assets- Desktop, laptop, Workstation and Servers

5.16 Software Assets

Minder allows user to get the detail of software installed in different hardware assets.

Follow the steps given below to get the details of software assets.

1. Navigate to **Assets** > **Softwares** Tab.
2. Here you get the list of all the softwares installed in different hardware assets along with the version details in 'Version' column and the number of times the software has been installed in 'Installation Count' column.

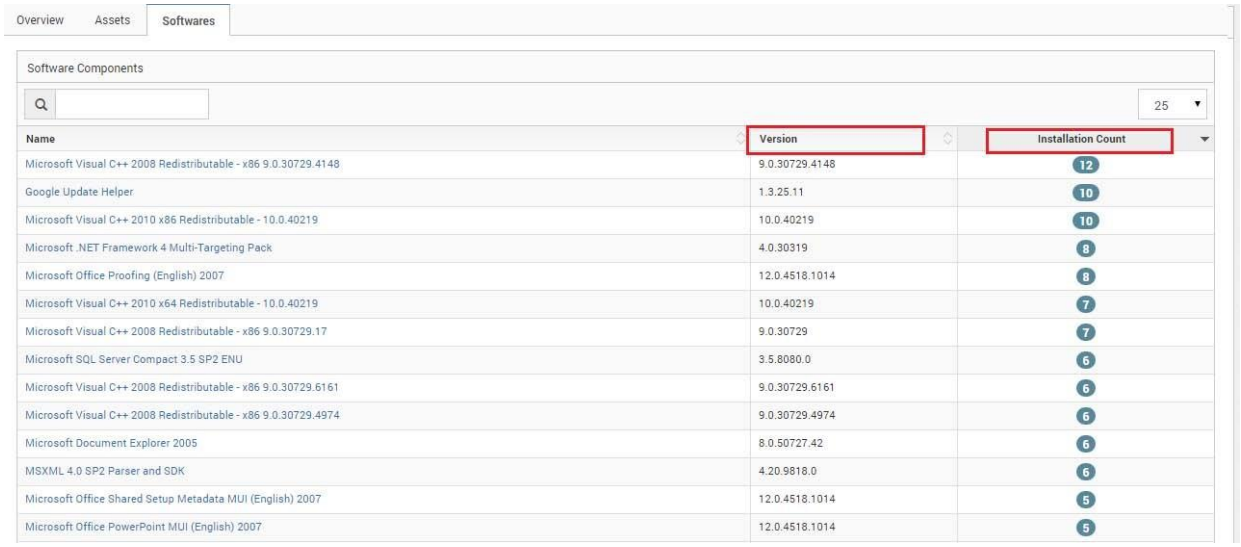


Figure 5.6 List of Softwares

By clicking on the count, you can get the list of the monitors in which that particular software has been installed.

5.17 Getting Software Details of a Particular Monitor

Follow the steps given below to get the software details of a particular monitor:

1. Navigate to **Assets** > Click on **Assets**.
2. Select a monitor.
3. Click on **Scan Now** icon.
4. After scanning is over, click on that monitor > click on **Software**.
5. You get the details of softwares installed on that particular monitor.

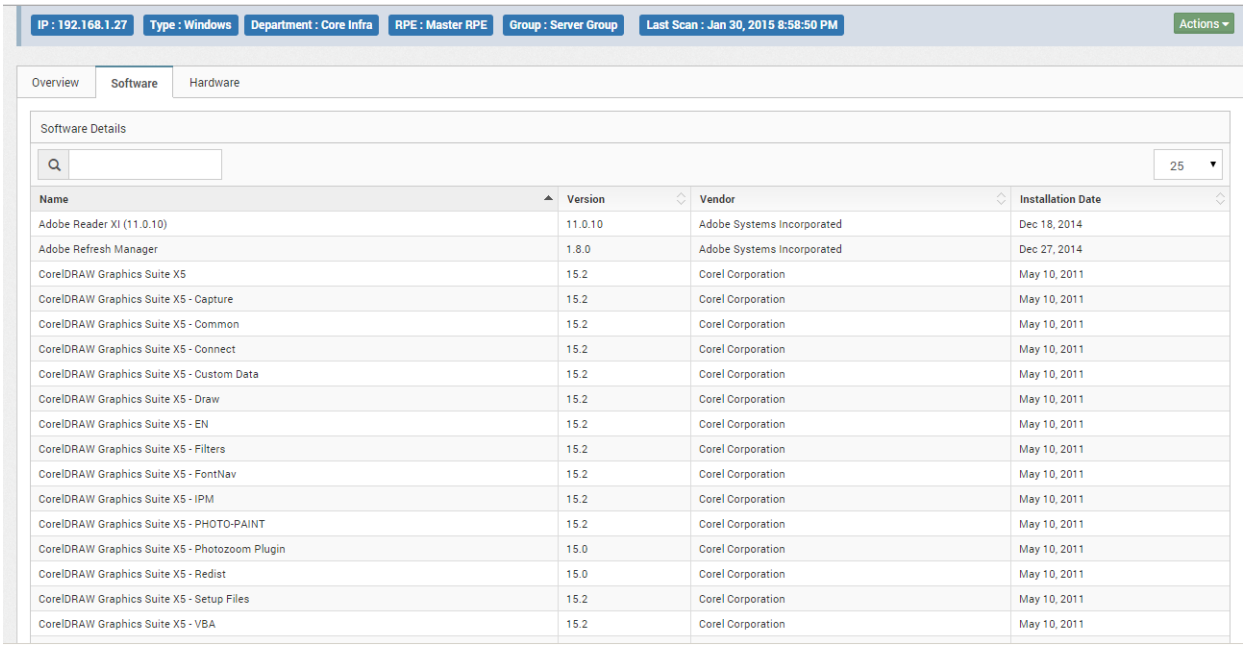


Figure 5.7 Software details of a particular monitor

5.18 Hardware Assets

Minder allows user to get the overview of hardware available in your network.

Follow the steps to get the overview of hardware details:

1. Navigate to **Assets** > **Overview**.
2. Here a graphical representation along with the count of available hardware assets in your network is shown.

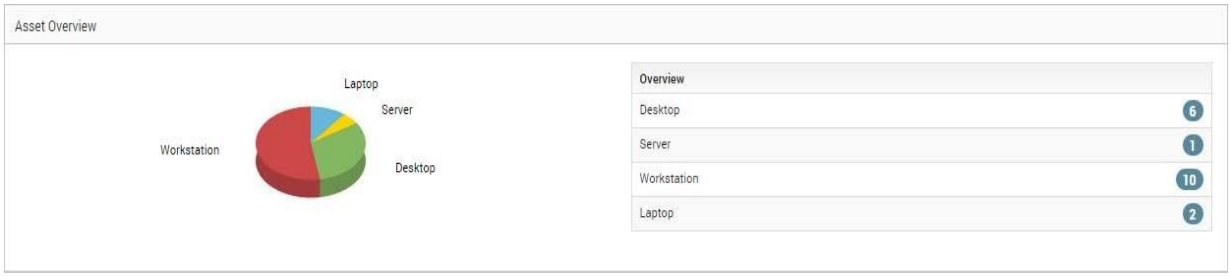


Figure 5.8 Hardware details

By clicking on count, asset name along with asset type can be viewed.

5.19 Getting Hardware Details of a Particular Monitor

Follow the steps given below to get the hardware details of a particular monitor:

1. Navigate to **Assets** > Click on **Assets**.
2. Select a monitor.
3. Click on **Scan Now** icon.
4. After scanning is over, click on that monitor > click on **Hardware**.
5. You get the hardware details of that particular monitor.

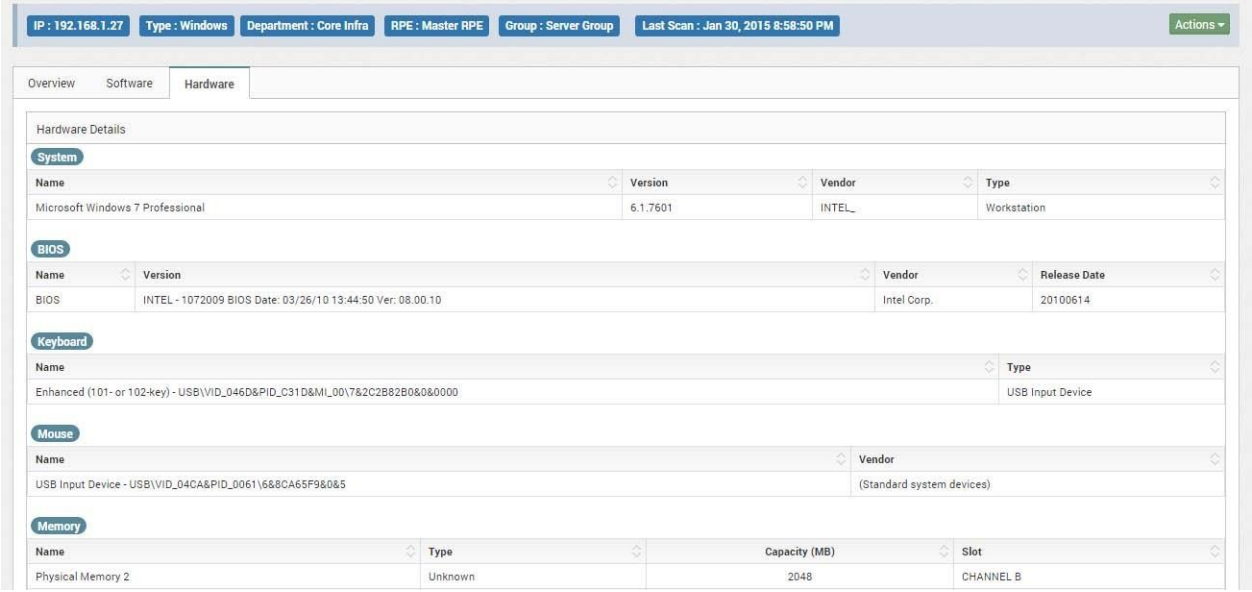


Figure 5.9 Hardware details of a particular monitor

5.20 Monitoring assets along with performance metrics of a particular monitor

Minder allows you to enable asset monitoring. **E.g.** CPU memory on existing monitors which you are already monitoring for performance metrics.

Create a new asset discovery or follow the steps given below:

1. Navigate to **Monitors** > select a monitor.
2. Navigate **Actions** > **Polling scheduler.**
3. Enable Asset manager.

Now it will monitor assets along with metric performance.

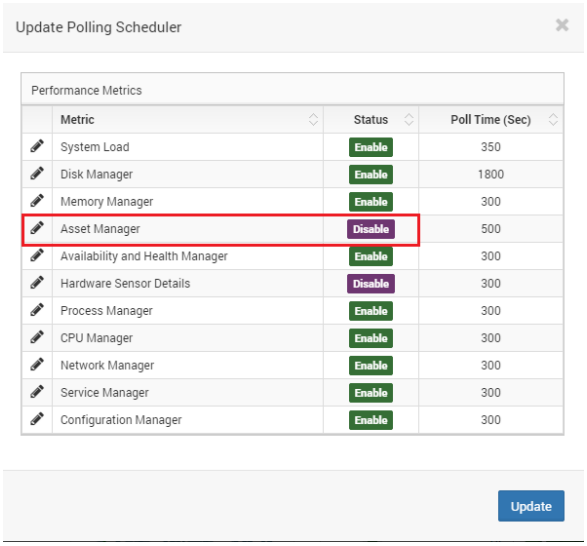


Figure 5.10 Enabling Asset Manager

5.21 Enabling Performance Monitoring on Existing Assets

Minder allows you to enable performance monitoring. **E.g.** CPU, memory monitoring on an existing asset already is being monitored for software and hardware audit.

Follow the steps given below to enable performance metrics along with assets:

1. Navigate to **Monitors** > select a monitor.
2. Navigate **Actions** > **Polling scheduler**.
3. Enable the desired manager that you want to monitor.
4. Now it will monitor assets along with metric performances.
5. Click on **Update**.

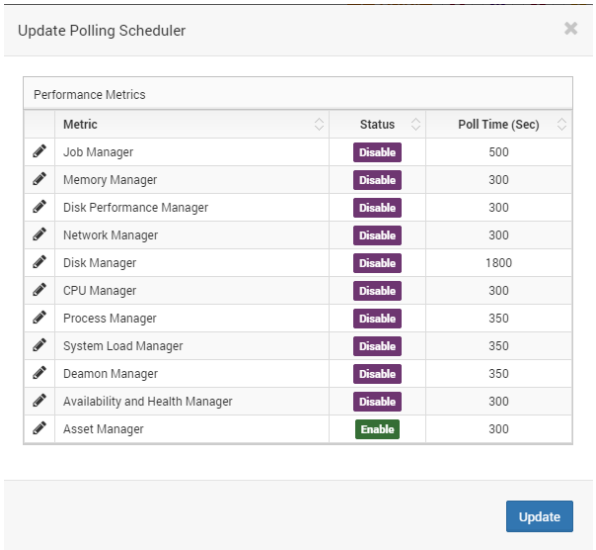
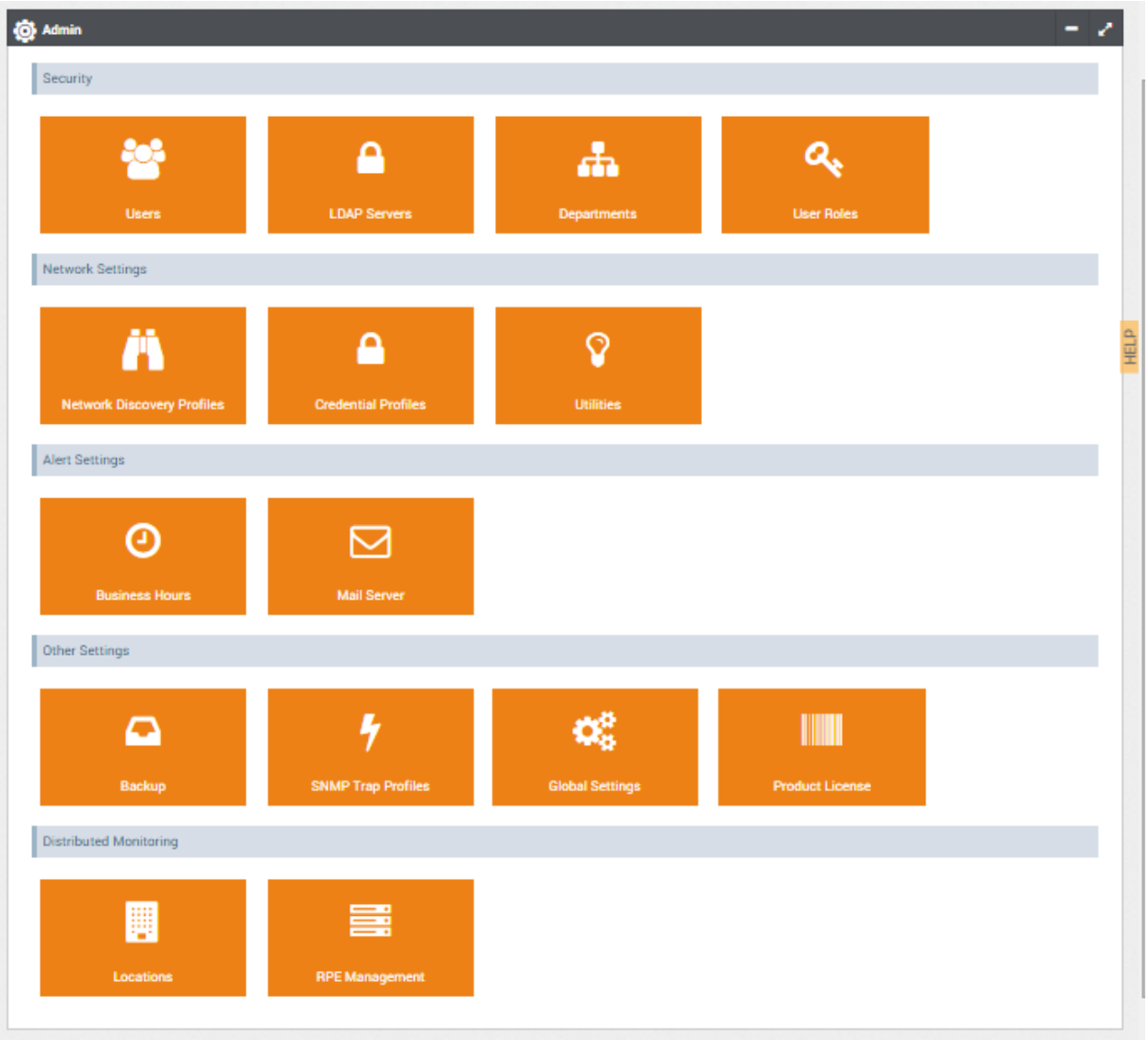


Figure 5.11 Monitoring Performance Metrics

6 Admin Panel

Read the following set of instructions for the following attributes:



- Security
    - Users
    - LDAP Servers
    - Departments
    - User Roles
- Network Settings
    - Network Discovery
    - Credentials Profiles
    - Utilities
- Alarm Settings
    - Business Hours

- Mail Server
- Other Settings
  - Backup
  - SNMP Trap Profiles
  - Global Settings
  - Product License
- Distributed Monitoring
  - Locations
  - RPE Management

6.1. Security

The features and functionality of this is explained in section 13.

6.2. Network Settings

6.2.1. Network Discovery

For information on discovering and adding devices/apps, please refer to section 3.0

6.2.2. Credential Profiles

Pre-configuring a set of credentials in Minder helps applying them to multiple devices at a time, saving a lot of manual effort.

Follow the steps given below to create a credential profile:

1. Navigate to **Admin** > **Credential Profile** > **New**.
2. Provide the name of the profile which you want to configure.
   Note: The credential profiles are used for ease of access to the user. These profiles can be configured here and used globally in the Minder to define the credentials in any other tasks.
3. Select the Credential type as per your requirement.
   Note: The various kinds of profiles available here will be **Server, SNMP Device, Virtualization, Database Server, Application Server, Web Server, Cloud, Middleware, Platform Monitor.**

   For Example:
   SNMP: When you select the SNMP type, you need to provide the SNMP version and the community name for the profile.

1. If selected Credential type is **SNMP**, provide the SNMP **version**.
2. Note: **SNMPv1** and **SNMPv2** are community based security models. Enter the Credential name and description. Configure the correct Read and Write community.
3. If selected SNMP version is **SNMPv3**, provide the SNMP security level.

4. For security level "**No Authentication No Privacy**", enter the name of the user (principal) on behalf of whom the message is being exchanged.
5. For security level "**Authentication No Privacy**", enter the name of the user (principal) on behalf of whom the message is being exchanged.
6. Select any of the authentication protocols as Security Name. Enter the password of authenticated user. MD5 and SHA are processes which are used for generating authentication/privacy keys in SNMPv3 applications.
7. For security level "**Authentication Privacy**", enter the name of the user (principal) on behalf of whom the message is being exchanged.
8. Select any of the authentication protocols as Security Name. Enter the password of authenticated user.
9. Provide the Security Private Password.
10. Select the Department from the list.
11. Create the configurations and the task is done.

The system saves the credential profile and displays a confirmation message of the action.

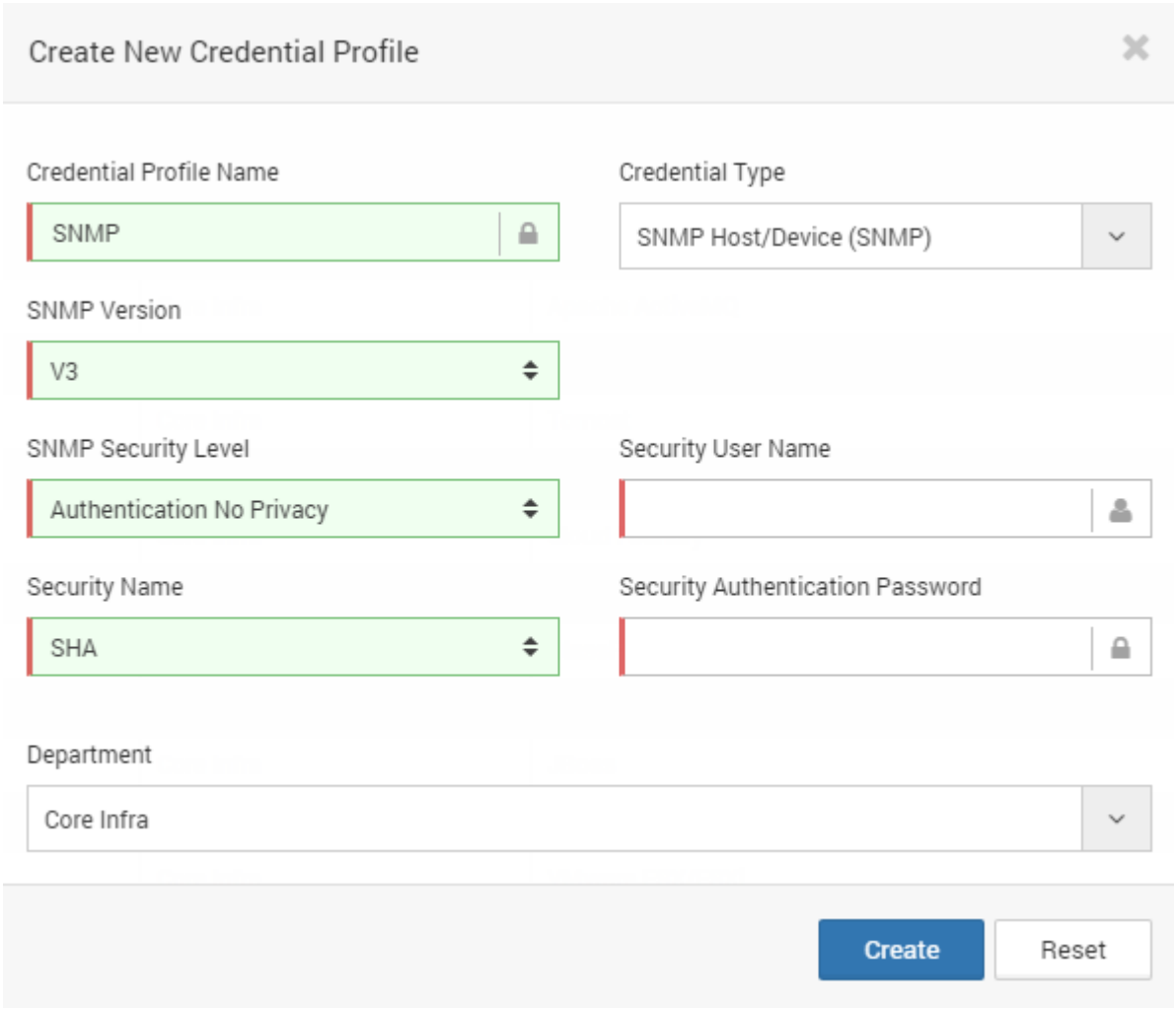


Figure 6.1 Create Credential Profile.

Note: The SNMP credentials created is used during the initial discovery and classifications. Minder uses these credentials to classify and add the devices into Minder.

6.2.3. Utilities

If a monitor is recognized as an unknown device in network discovery, user can check here about what problem has occurred.

Utilities tab provide 3 functionalities to check about the occurred problem:

1. Ping Checker
2. Port Checker
3. System OID Fetcher

6.2.3.1. Ping Checker

User can use ping checker attribute to know whether the ping to a monitor from Minder Server is successful or not. Follow the steps given below to know that monitor has pinged successfully or not:

1. Navigate to **Admin** > **Utilities** > **Ping Checker.**
2. Provide **the IP/Host**
3. Click on **Test**.
4. Result will displayed on top as shown:

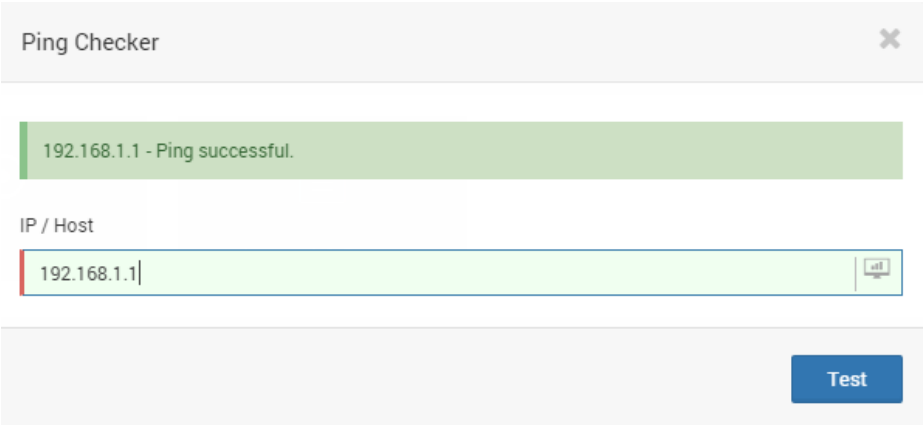


Figure 6.2 Ping Checker

6.2.3.2. Port Checker

User can use port checker attribute to know whether the port of a monitor is connected or not.

Follow the steps given below to know about port connection

1. Navigate to **Admin** > **Utilities** > **Port Checker**.
2. Provide **IP/Host.**
3. Provide **port number.**
4. Click on **Test**.
5. Result will be displayed on top as shown:

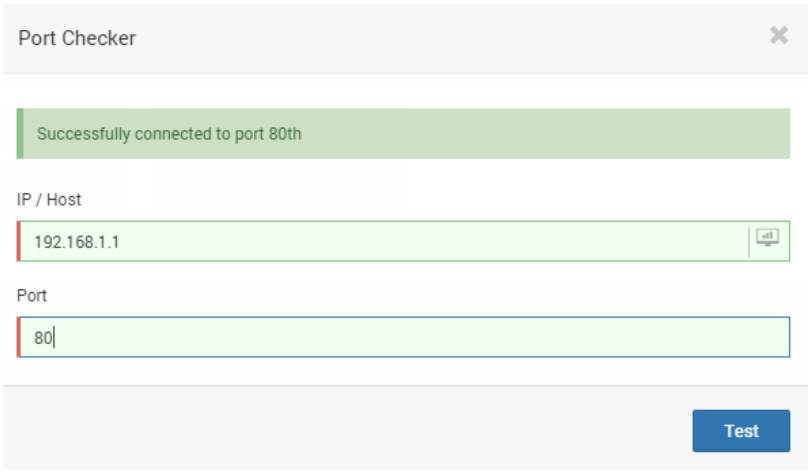


Figure 6.3 Port Checker

6.2.3.3. System OID Fetcher

To know OID of SNMP device, you can use System OID fetcher as only SNMP devices allows you to get the system OID. If the user gets system OID, meaning connection is successful otherwise it will show an error.

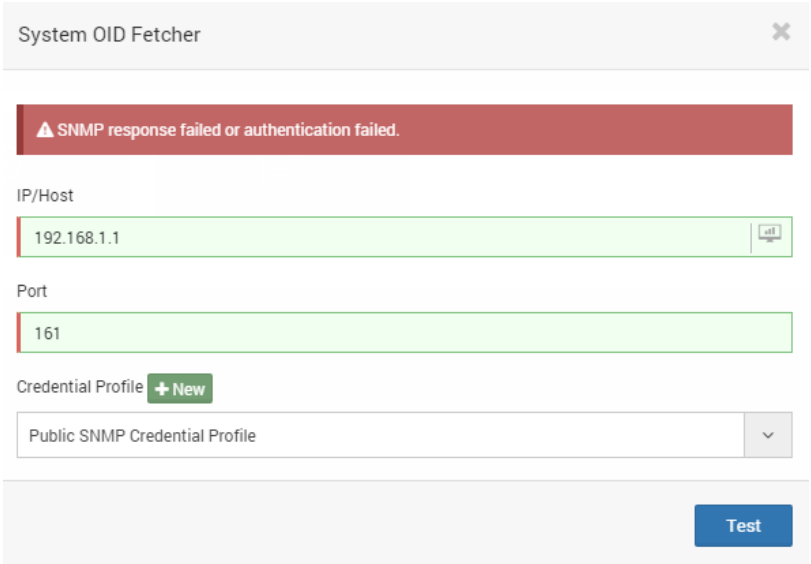


Figure 6.4 System OID Fetcher

Follow the steps given below to get the system OID:

1. Navigate to **Admin** > **Utilities** > **System OID Fetcher.**
2. Provide **IP/Host.**
3. Provide **port number.**
4. Provide **Credential Profile.**
5. Click on **Test**.
6. Result will be displayed on top as shown:

6.3. Alarm Settings

6.3.1. Business Hours

Business Hour is a feature provided by Minder, to control Alarm message Time for any action such as email, SMS, execute script etc. **Example:** You are not bothered if Server's CPU performance slows down after 8:00 PM and don't want alert message in your inbox at that time but if it slows down between 10:00 AM to 8:00 PM you want the alert message right away.

Note: You can also add multiple time slices for each day. Example: You want alert on Monday at 8 am to 12 am and also at 2 pm to 7 pm. You can add multiple entries of same day with respective time slices.

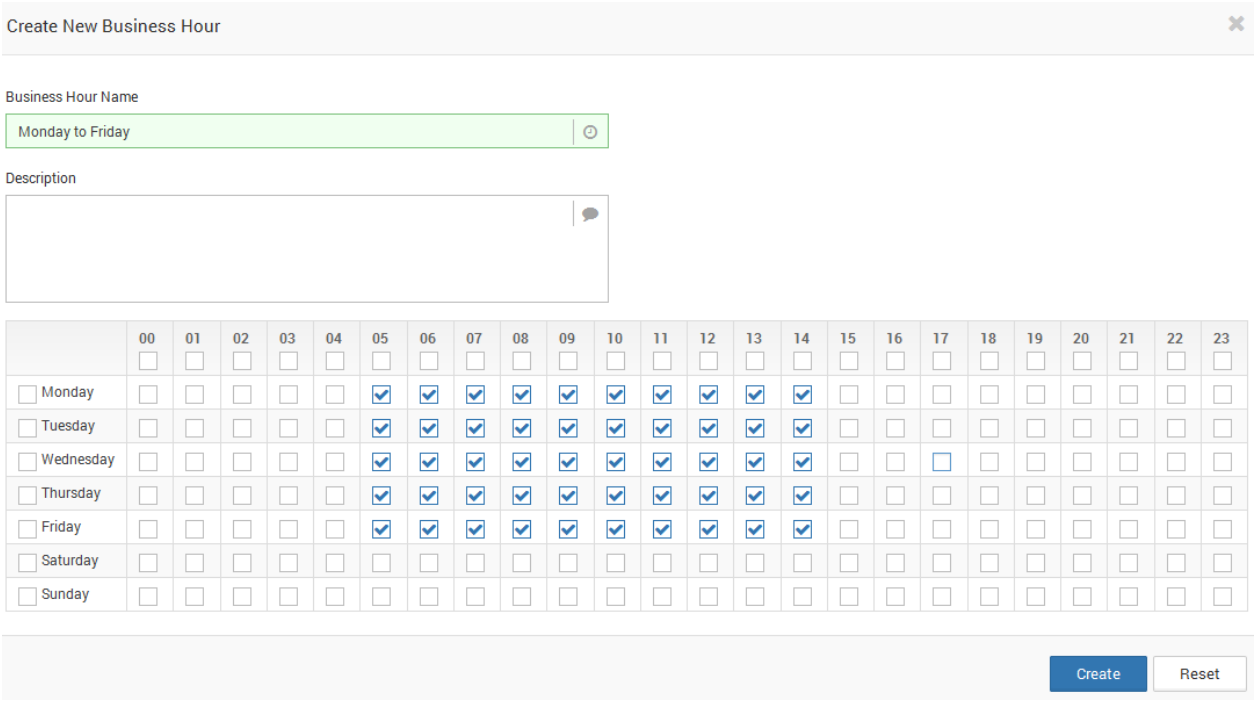


Figure 6.4 Create Business Hours

Navigate to Business hours under the Admin Panel to create or view the business hours. Follow steps given below:

1. Navigate to **Admin** > **Business Hours** > **New**.
2. Provide the **Business Hour name**.
3. Describe the business hour **Description** as per your needs.
4. Provide the time settings.

   Example: Define the specific business hour for each day. Say on Monday you have a working hours from 9:00 to 19:00. During these hours only you would like to receive important notification.
5. Click **Create**.

The system creates new Business Hour profile and displays a confirmation message of the action.

6.3.2. Mail Server

Minder allows you to send alerts to users via email. If you have more than one email server, you can add additional servers with a different configuration. The MINDER console server responsible for sending mail will start with the email server with the primary mail server and if it is unable to reach that server, it will move on to the secondary server on the list until the notification has been sent out successfully. You should make sure that the mail server(s) is configured properly to allow MINDER to relay email to any email address.

Follow the steps given below to configure Mail Server for Notification:

1. Navigate to **Admin** > **Mail Server**.
2. Select **Primary** if configuring the mail server for the first time.
3. Provide **SMTP Server** address.
4. Provide the **SMTP Port** to connect.
5. Provide the **Email** address you want to use as From Address.
6. Select the **security type** from the options. Whether SSL, TLS or no security.
7. If the SMTP server requires authentication - Provide the Username and password for the Mail account.
8. Click on **Configure** and the configurations will be saved. System will automatically send test email to the specified address.

Note: In case Minder is not able to connect to your Gmail server, this is due to some security reasons at mail server side. Check your Google settings and change them if required.

Please refer to the link **https://support.google.com/accounts/answer/6010255** so that you can connect from minder.

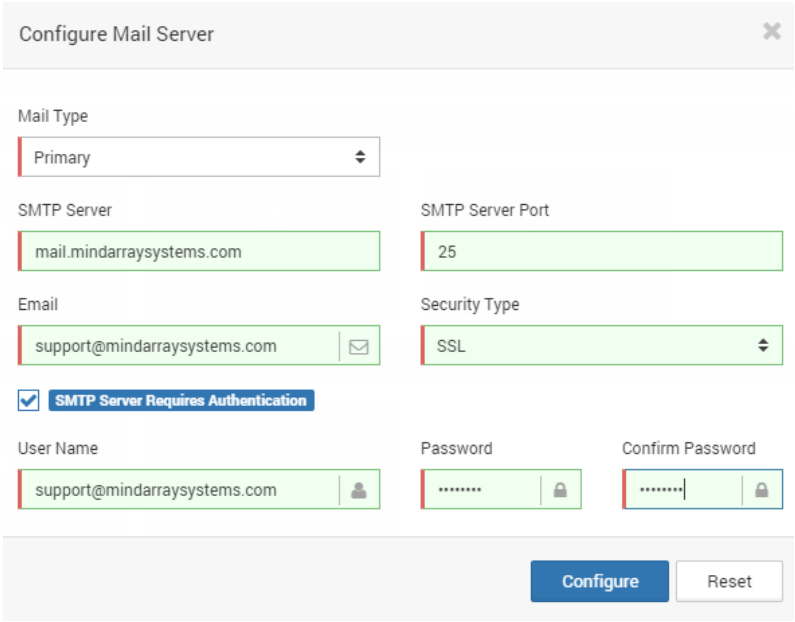
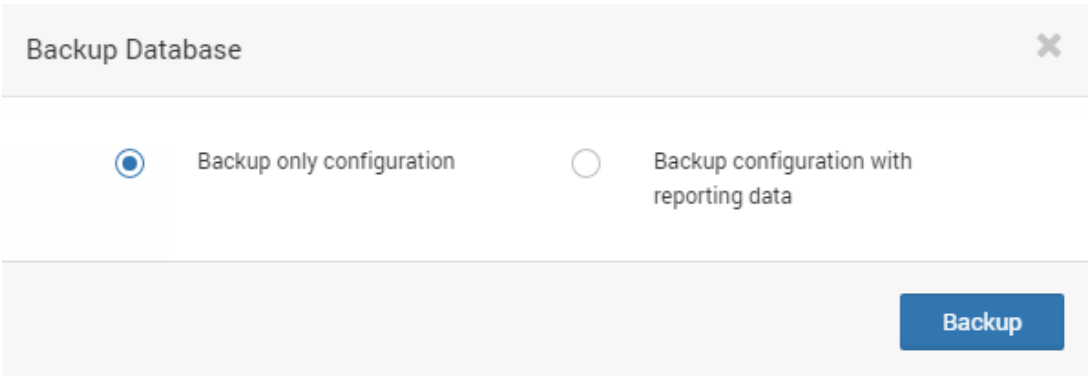


Figure 6.5Configure Mail Server

6.4. Other Settings

6.4.1. Backup

User can backup only the Minder configuration i.e. added servers, network discoveries etc. or chose to select reporting data together with it using this functionality. However, this will only work with licensed version.



There will be a restore utility along with Minder Installation for the Customers of Minder to restore the backup. The backup will be overwritten on the existing Minder configuration.

6.4.2. SNMP Trap Profile(s)

Trap: Asynchronous notification from agent to manager, SNMP traps enable an agent to notify the management station of significant events by way of an unsolicited SNMP message.

Traps are cryptic messages of a fault that occurs in an SNMP device. SNMP traps are alerts generated by agents on a managed device. After the Minder receives the event, the Minder displays it and can choose to take an action based on the event.

Processing SNMP Traps

Minder 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 determine whether a specific trap matches the conditions specified in the Trap Processor. Once a matching Trap is found, an alert is generated.
- Trap Profiles Converts the cryptic message to human-readable alarm.
- The traps that are received by Minder are listed under 'SNMP Trap Dashboard'.

For creating/modifying SNMP traps profile, follow the steps given below:

1. Click on **the SNMP Trap Profile** under **Admin** Section.
2. Click on **New** button, New SNMP Trap Profile dialog appears.
3. Provide the **OID**. The format would be **1.3.6.1.xx** which is without the first '**.**'. By default it is filled when you navigate from SNMP Trap Dashboard.
4. Provide the description.
5. Define the **Severity** level of the trap such as "Clear","Warning", "Critical".
6. Select whether to drop or accept traps as "Enable" or "Disable". In case you wish to get notified then select Disable so that Minder will not filter out the traps.
7. Select Alert/Actions you want to execute whenever you received this trap. All the Email Alert Profiles and Action Profiles can be selected here.
8. Provide the Message you want to replace using variable bindings in SNMP Trap Translator. Variable bindings index start from N to 0 ($0, $1 and so forth). E.g. Interface Ethernet 0/1 is Up can be received from 'Interface $0 is $1'. However, you need to place $0 and $1 accordingly and in relevance with the trap format.
9. Click on **Create**.

The system will create a new SNMP Trap Profile and displays confirmation message of the action. You can add a Trap Widget to get the historical representation of all the received traps in specific Time Span.

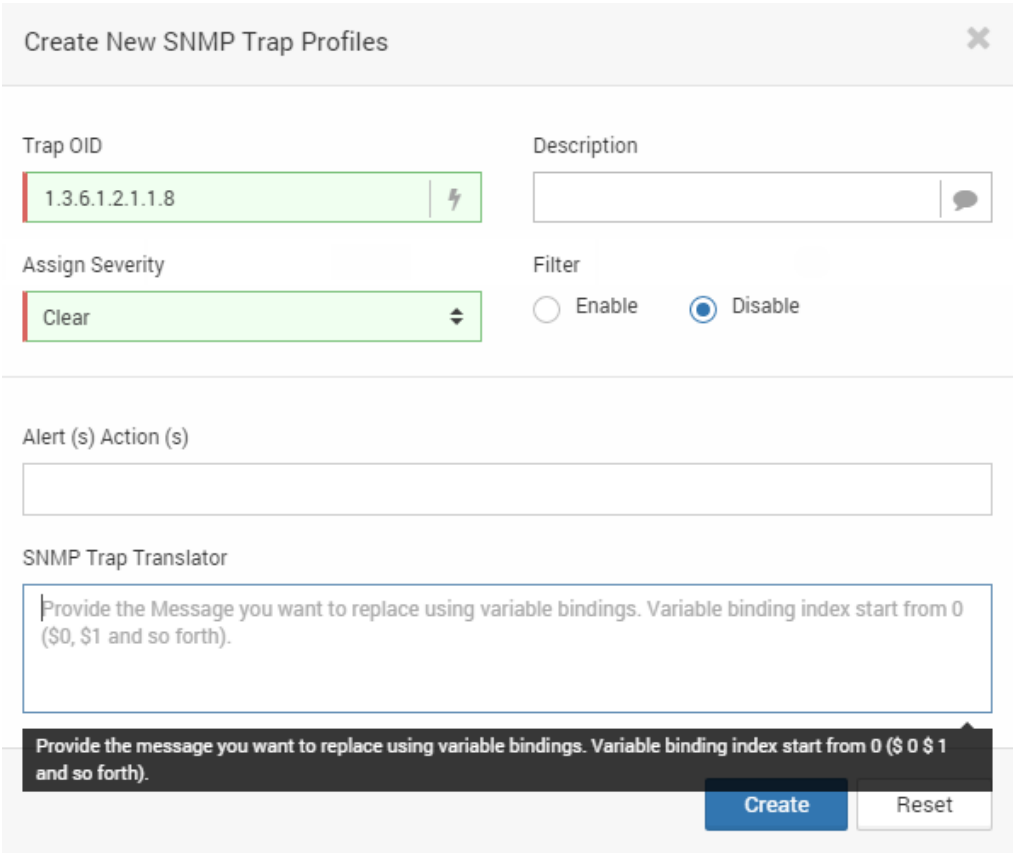


Figure 6.7 Create SNMP Trap

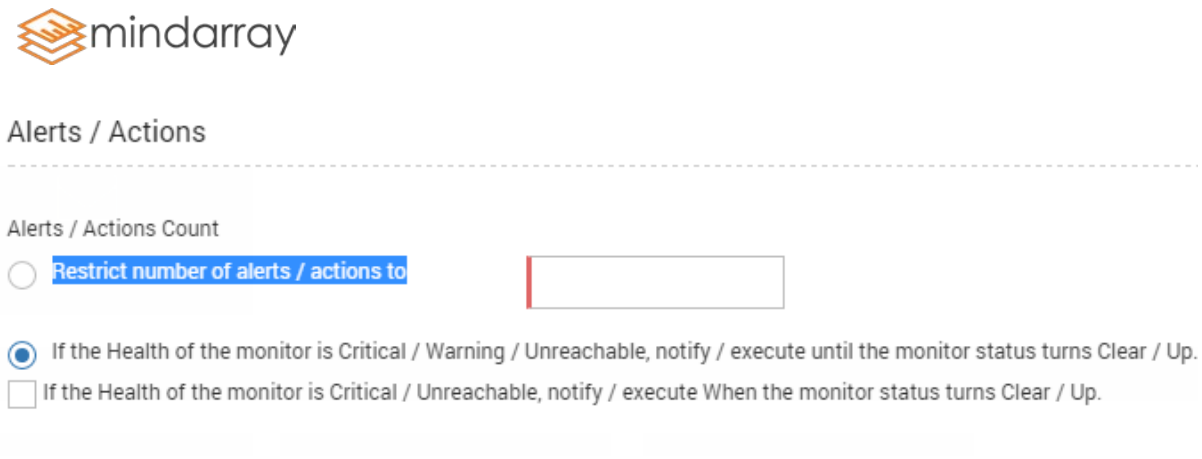
6.4.3. Global Settings

Global setting is the place where it allows you to set the default rules for the monitors created.

Click on the Global setting tab to enter the default values for the various tasks. The details of the value in each filed is explained as under.

6.4.3.1. Alerts/Actions

1. As the name goes, the number of notifications will be sent to specified users in Alert profiles – based on the provided value. This will be applied to all the policies in Minder.
   Example: If the value is set to 2, you will get the notification only 2 times for any alarm triggered until alarm severity is changed.
2. Second option will keep giving you the notifications for all alarms with current severity Critical/Warning/Down until alarm severity changes to Clear state.
3. The last checkbox if enabled will send a single alert when the monitor or its attribute is out of any warning/critical/unknown state.



6.4.3.2. Data Retention

This value defines the days of data to be retained in the database. The retention period counts the days from present day to the number of days defined. The older data will be deleted. For example: data excluding the retention period.

6.4.3.3. LDAP Authentication (Sync Job)

1. Enable LDAP Authentication enables the Authentication against configured LDAP server under Admin > LDAP Servers.
2. This value defines the time period to sync user data with LDAP servers.

If this option is disabled then, Minder will not sync the user from “minder users” or “minder help desk users”.

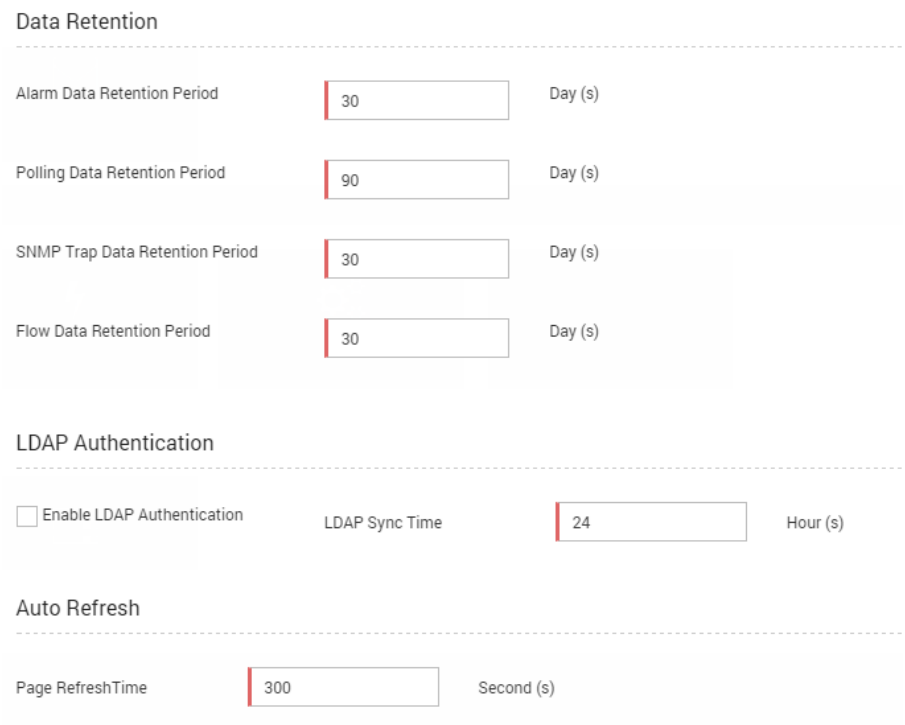


Figure 6.8. Global Settings

6.4.3.4. Auto Refresh

This refreshes the page of Minder at every given interval of seconds. The widgets on a page and all the other details will be refreshed accordingly.

6.4.3.5. Setup Wizard

This pops up the Start up guide for your guidance in Minder. You can know the basic steps and the reason of doing the same.

6.4.3.6. Google Map API Key

Google Map API Key is necessary to create Google Map Widget. . If API is not provided, error page will be displayed as shown below.

Follow the steps given below to get the API key:

1. Create your Google Map API key.
2. Go to https://developers.google.com/maps/documentation/javascript/tutorial.
3. Navigate **Admin** > **Global Settings**.
4. Enter Google Map API Key.
5. Click on **Update**.
6. Finally bind the Data source.

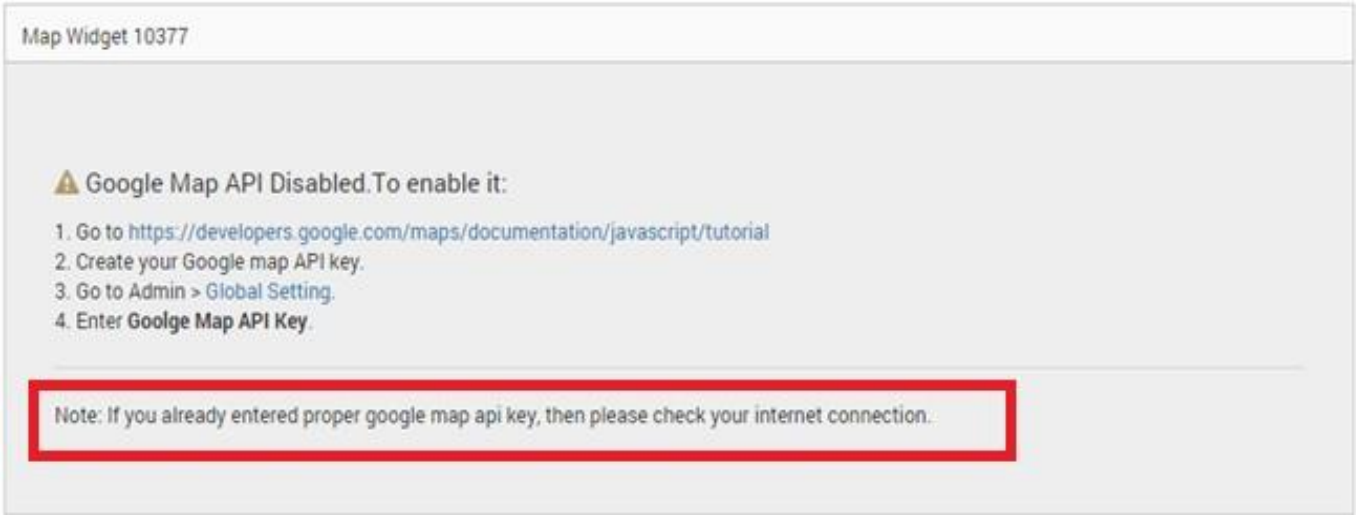


Figure 6.9 Google Map widget error page

6.4.3.7. Ticket Setting

This assigns the default assignee for any new ticket. The user created in Minder will be displayed here.

6.4.3.8. White Labeling

White labeling allows your company to rebrand the product logo to make it appear as your own. Follow the steps given below to set your own logo:

1. Navigate to **Admin** > **Global Settings** > **White Labeling**.
2. **Browse** to set your logo.
3. Click on **Update.**

Figure 6.10 White Labeling

6.4.4. Product License

Here you the detail about the product License such as when the license will expire, monitors used, etc.

The relevant fields shown are as follows.

- **License Issue to**: Show the name of the company to whom the license is sold.
- **License Issue Date**: It will have the details of the date on which the License was issued.
- **License Expiry Date**: It will show the expiry date of the License.
- **License Type**: This indicated the edition of the Minder you are using.
- **Total Monitors**: Show the total number of product monitors.
- **Used Monitors**: Show the number of used monitors in product.
- **Remaining Monitors**: Show the number of remaining monitors.
- **Total Assets**: Show the total number of assets which can be monitored from Minder.
- **Used Assets**: Show the number is used asset monitors.
- **Remaining Assets**: Show the remaining asset monitors.
- **Total RPE**: The number of Remote Polling Engine bought with Minder.
- **Remaining Days**: Show the number of days the before the expiration of the license. After these days you need to purchase the license again.
- **License Status**: This filed shows the status of the license.
- **Add On Modules**: It includes number of modules such as Business Service, Business SLA, Services.

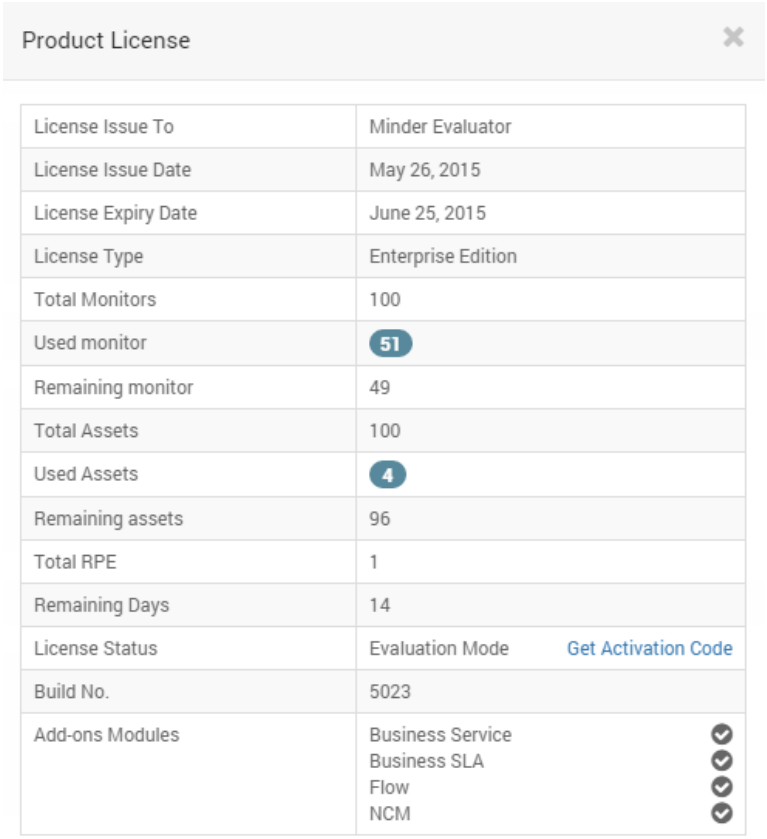


Figure 6.11 Product License

Note: For more information about activating the license contact support@mindarraysystems.com

Generating Activation Code

Generating an offline activation code is one of the best features that enable the user to activate Minder offline.

This is one of the best features by which user can activate minder offline.

Follow the steps given below to activate minder offline:

1. Navigate to **Admin** > **Product License** > **Get activation code**.
2. You will get a code.
3. That code you will have to send it to technical support department and then you will receive a license file which will replace the old file and then offline license is activated

6.5. Distributed Monitoring

6.5.1. Locations

To create the locations follow the steps given below.

1. Navigate to **Admin** > **Locations** > **New**.

2. Provide the Location Name, Description and click over the map to pick up the location.
3. Click on **Create** on the New Location dialog.

The system will create the new Location and display a confirmation message of the action.

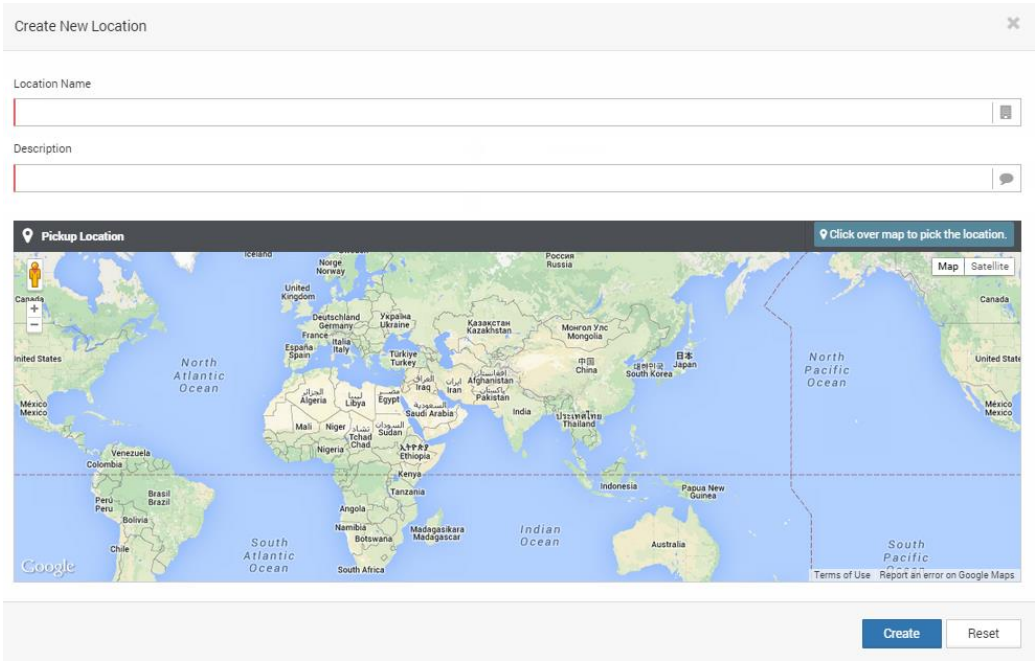


Figure 6.12 Location

6.5.2. RPE Management

Remote Polling Engine allows you to distribute the polling load of the Minder platform installation between multiple servers. It also allows you to poll remote site network locally and push the data to Master server.

To edit a Remote polling engine, follow the steps given below:

1. Navigate to **Admin** > **RPE Management** >  icon.
2. Provide the **Name** for Polling Engine.
3. Select the **Location** to be assigned to the RPE.
4. You cannot change the **Host** and **Port** of the RPE from the Minder Console, but you can change them from minder.conf file.
5. Click on **Update**.

The system will edit the Remote Polling Engine and will display a confirmation message of the action.

7 NCM

MindArray Network Configuration Manager helps you manage, organize and track changes to your network devices, including switches, routers and firewalls. These devices are collectively known as Monitors within MindArray NCM.

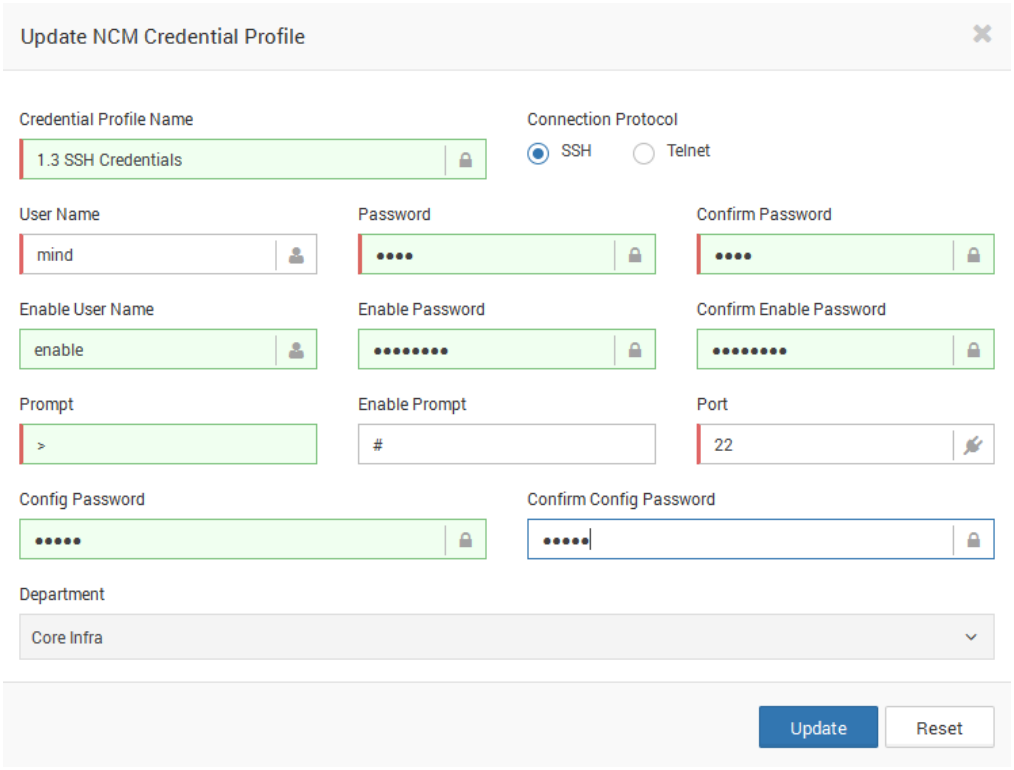
When a Network device is provisioned using SNMP method, that device will be directly imported in the NCM tab.

By default device listed under NCM tab are disabled for configuration management, once you enable device system allows you to apply credentials to the device. To apply credentials you will first have to add device ssh/telnet credentials.

7.1. Adding NCM Credentials

To add new NCM credential profile, follow the steps given below:

1. Navigate to **NCM** > **NCM credential Profile tab**> **New**.
2. Provide a **Name** for this NCM Credential Profile.
3. Provide the **User Name** of the device –which is the value of Login Name provided at the time of establishing a connection with a device.
4. Provide the **Password**.
5. Provide the **Prompt** that appears after successful login. **E.g**. you can prompt as >, #
6. When entering into privileged mode, some devices require User Name to be entered. Provide the **Enable User Name** if prompted; otherwise leave this field empty.
7. **Enabled Password** - This is for entering into privileged mode to perform configuration operations like backup/upload. This parameter is mandatory when Enable User Name is provided.
8. **Enable Prompt** - This is the prompt that will appear after going into enable mode.
9. Provide the SSH **Port**. Default port is #22.
10. Provide **Config Password** and select the **Department**.
11. Click **Create**.



The system will add new NCM credential profile and displays a confirmation message of the action.

7.2. Manually Back up Device Configuration

Once you have successfully applied NCM credentials on the device, System now allows you take back of startup/running configuration of the device and maintain audit/change log of the configuration. System automatically does the versioning of the configuration files whenever new backup done from the device.

Manually taking back of device configuration:

To take the backup of device configuration, follow the steps given below:

1. Navigate to **NCM > NCM tab**.
2. Select the devices for which you want to take configuration backup.
3. Navigate to **Actions** > **Backup running/startup configuration.**

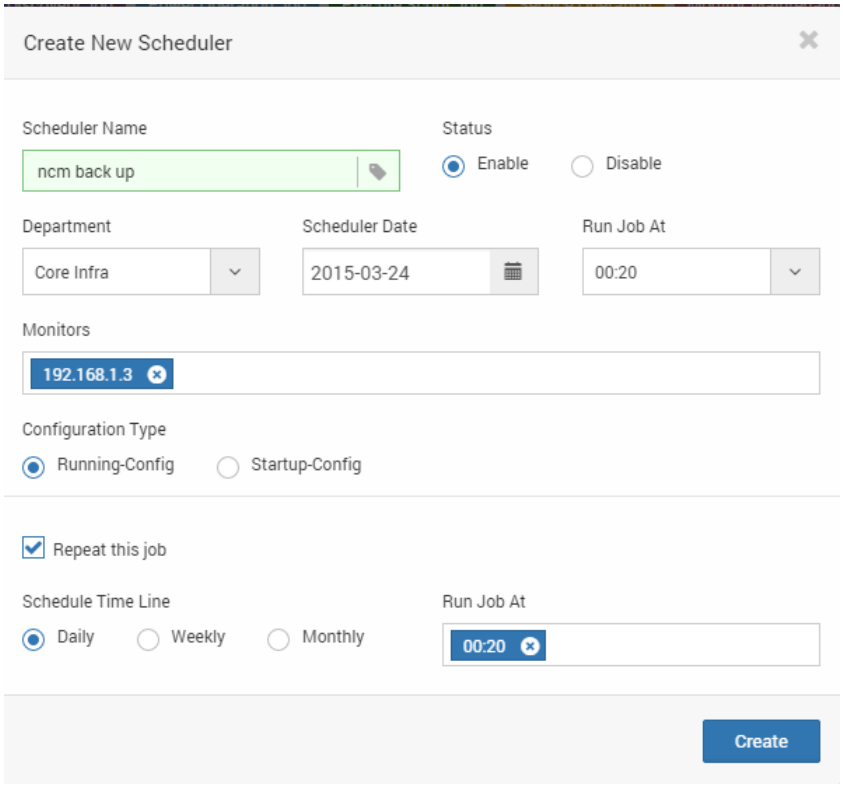
The system takes configuration backup of all the selected devices and displays confirmation message of the action.

7.3. Automatically Back up Device Configuration

System allows you schedule automatic job to back up startup/running configuration from the device.

To schedule NCM backup job, follow the steps given below:

1. Navigate to **Schedulers** > Drag and drop NCM backup job from the top on current or future date.
2. NCM job dialog appears, provide the **Scheduler Name**.
3. Select the **Department** from the list.
4. Provide the **Scheduler date and time** to run the job.
5. Select the **Monitor** for which you want to take back up.
6. Select the **Configuration Type**.
7. If you want to repeat the job, provide the **schedule time** for the operation to repeat daily.
8. If selected schedule time is weekly, provide the day of week and schedule time to run the job.
9. If selected schedule time is monthly, provide the day, month and schedule time to run the job.
10. Click **Create** to finish.



The system will save Scheduled event and displays a confirmation message of the action.

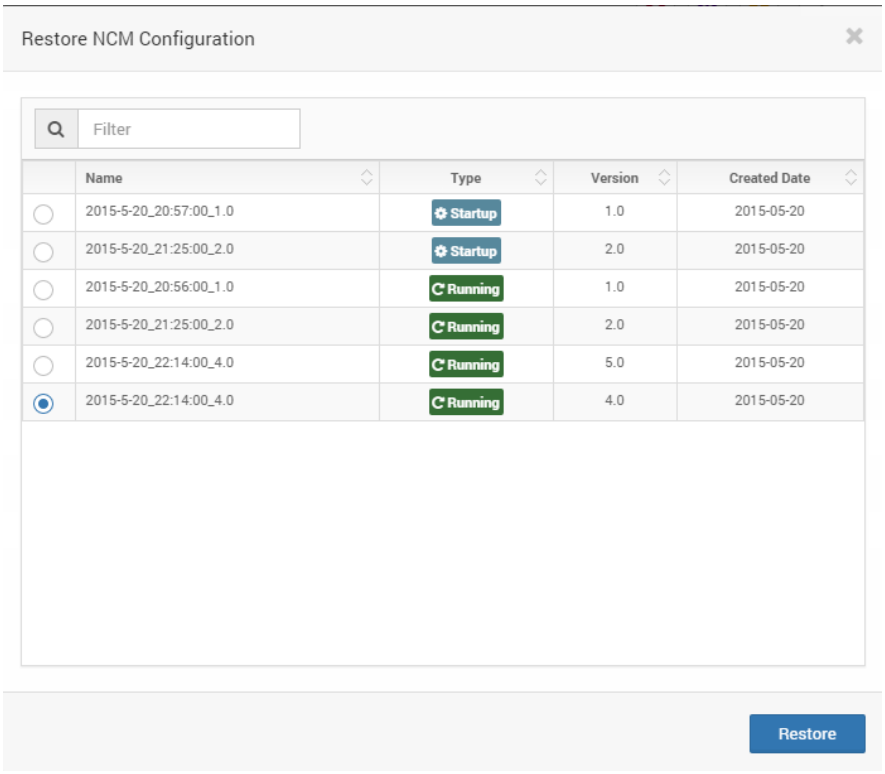
7.4. Restore Device Configuration

To restore previous configuration details in Device, follow the steps given below:

1. Navigate to **NCM > NCM tab**.
2. Select the device for which you want to restore the configuration details.
3. Click **Restore** in the top right Action menu.
4. Select configuration type and select the version to restore.

5. Click **Restore** to finish the action.

The system restores the configuration in Device and displays confirmation message of the action.



7.5. Sync Configuration

Synchronizing the configuration of the device will get your device into startup configuration mode from running configuration.

To sync configuration of a device, follow the steps given below:

1. Navigate to **NCM**.
2. Select the device.
3. Navigate to **Actions** > **Sync Configuration.**

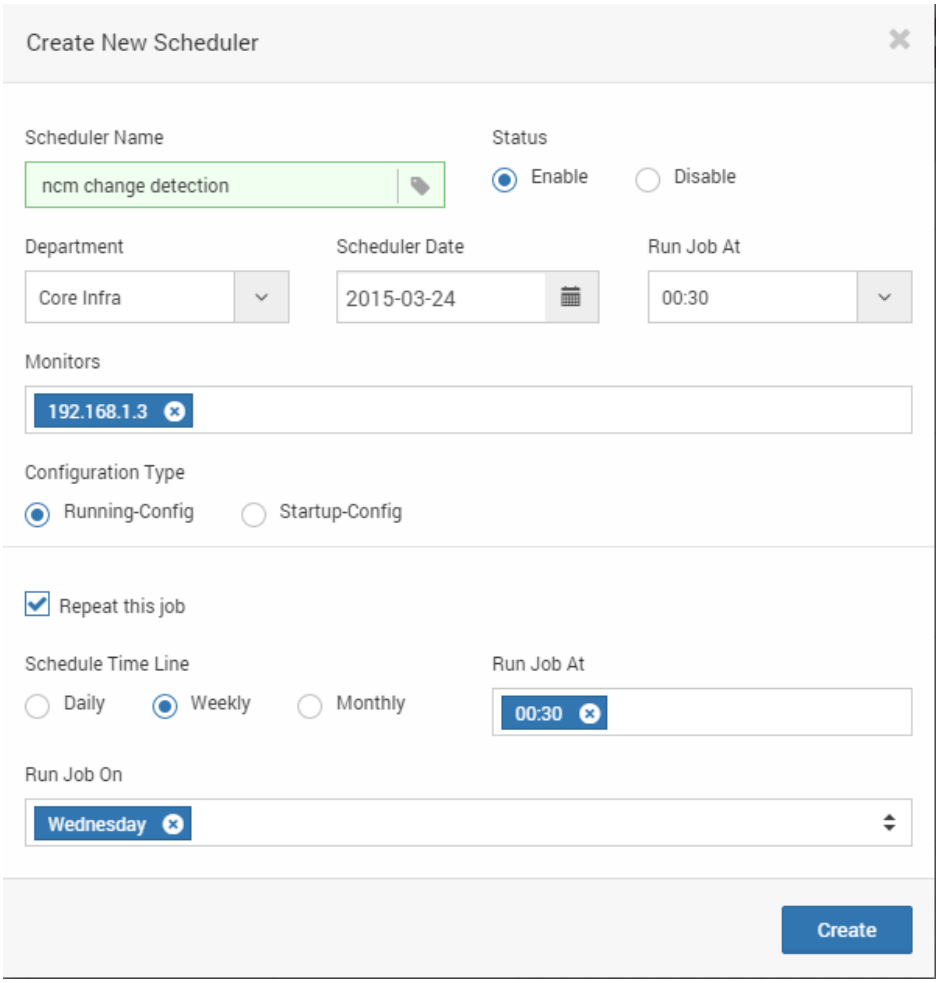
The system applies the startup configuration for device and displays confirmation message of the action.

7.6. NCM Change Detection Job & Notification

NCM change detection job allows you to automatically get notified when a change is detected. You can view the notification in the global notification list towards top left corner of the web console and also send an email to recipients when change is detected.

To detect configuration change and get notified, follow the steps given below:

1. Navigate to **Schedulers** > Click on current or future date > Select **NCM Change Job**.
2. Provide the **Scheduler Name**.
3. Select the **Department** from the list.
4. Provide the **Scheduler date and time** to run the job.
5. Select the **Monitor** for which you want to detect the change.
6. Select the **Configuration Type** you want to compare.
7. Select the recipient to get the change notification.
8. If you want to repeat the job, provide the **schedule time** for the operation to repeat daily.
9. If selected schedule time is weekly, provide the day of week and schedule time to run the job.
10. If selected schedule time is monthly, provide the day, month and schedule time to run the job.
11. Click **Create** to finish.



The system will save Scheduled event and displays a confirmation message of the action.

7.7. NCM widgets

NCM widgets show the NCM overview and Configuration audit log of the device. Two types of NCM widgetsare available:

- **NCM Overview**
- **NCM Audit**

To create NCM widget, follow the steps given below:

1. Navigate to **Dashboard** > Click on widget at the top right corner of the dashboard page > **NCM Widgets**.
2. Click **Add** towards top right corner; Select **NCM Overview/NCM Audit** to represent the data.
3. Once added, navigate to widget in the dashboard.
4. Bind the data source by clicking **Widget Properties** > **Data Source**.
5. Click **Update** to add widget into the system.

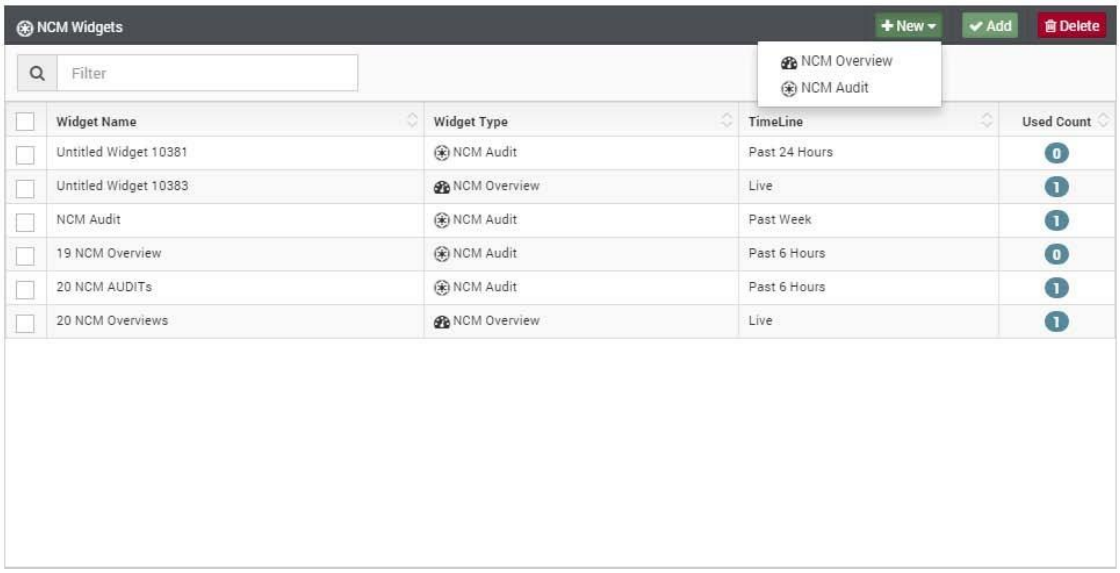


Figure: types of NCM widgets

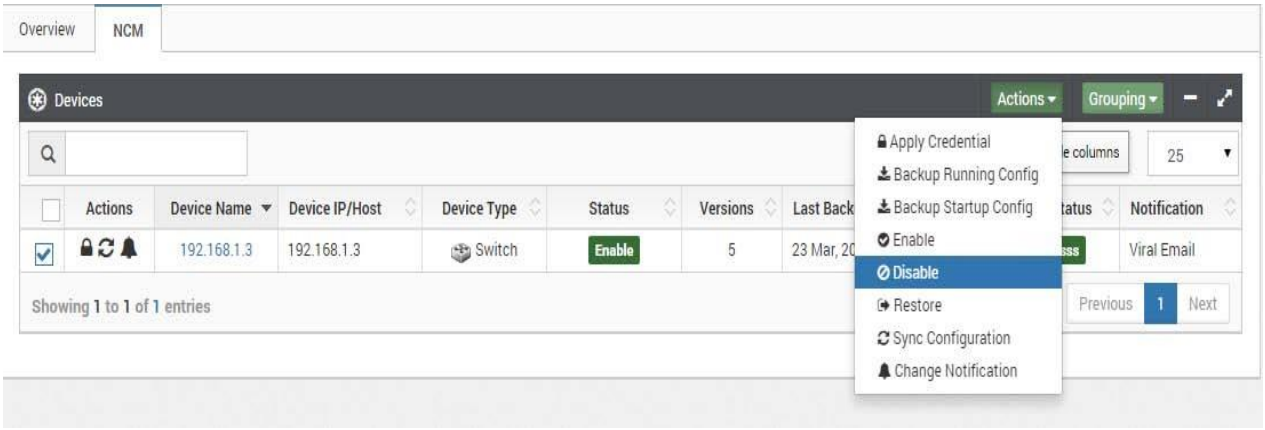
Figure: NCM Audit widget

The system will add the new Widget properties and displays a confirmation message of the action.

7.8. Disabling NCM Monitor

To disable NCM monitor, follow the steps given below:

1. Navigate to **NCM**.
2. Select the devices which you want to disable.
3. Navigate to **Actions** > **Disable.**



The system disables NCM monitor and displays confirmation message of the action.

8 Working with Network Flow

Minder supports has built-in network flow and packet level data collection tools to provide seamless drill-down from system and device level monitoring to troubleshooting and analysis using flow and packet data. This data provides details about the network traffic between hosts, enabling quick identification of impacted services, trouble areas and problem sources.

Network routers and switches can be configured to export conversation records for traffic flowing through them to a "flow collector." These records consist of the source and destination IP address, as well as the source and destination ports. Based on this information, it is possible to find out the total traffic between two hosts and the type of application.

Supported protocols that provide this flow data are NetFlow version 5 and 9, sFlow version 5 and above and IPFix.

8.1. Enabling Export of Flow Records

The network flow analysis engine in Minder relies on collecting network flow data exported by a router or switch, so you need to enable your network equipment to export flow records.

Network flow records are typically exported from the routers to the default TCP port of 9996. Make sure you change the port to 4738.

Note: IPM is set to accept flows at port # 4738.

8.1.1. Enabling Netflow on A Cisco Router (Or Switch Running Ios)

To enable NetFlow on Cisco devices:

1. Telnet or SSH into the router and enter enable mode.
2. Enable Cisco Express Forwarding:
   router(config)# ip cef

3. Enable NetFlow on all physical interfaces that will take part in routing traffic between devices of interest:
   router(config)# interface <interface>
   router(config-if)# ip route-cache flow

   Note: Routers may by default export flow data only for traffic entering the router, so make sure you enable NetFlow on all interfaces for accurate analysis of traffic both into and out of the router.

4. Enable export of NetFlow records:
   router(config)# ip flow-export version 5
   router(config)# ip flow-export destination <Minder_host_ip_address> 4738
   router(config)# ip flow-export source FastEthernet0
   router(config)# ip flow-cache timeout active 1
   router(config)# ip flow-cache timeout inactive 15
   NOTE: The 'ip flow-export source' can be any interface that stays active; a stable or Loopback

interface is preferred.

Save the configuration:
router(config)# end
router# write mem

Go to http://www.cisco.com/en/US/tech/tk812/tsd_technology_support_configure_guide.html for more information about configuring NetFlow on Cisco devices.

8.2. Adding Flow Monitors

You have to add network flow monitors into System to access the Flow received form specific router/device interface.

To add Flow monitor, follow the steps given below:

1. Navigate to **Flow** > **Flow** tab.
2. Click **New** > **New interface** dialog appears.
3. Select the interfaces for flow analysis and click **Add**.
4. Select the Interfaces to enable Flow Analysis. Once selected click **Actions** > **Enable**.

The system enables Flow Analysis on selected interfaces and displays confirmation message of the action.

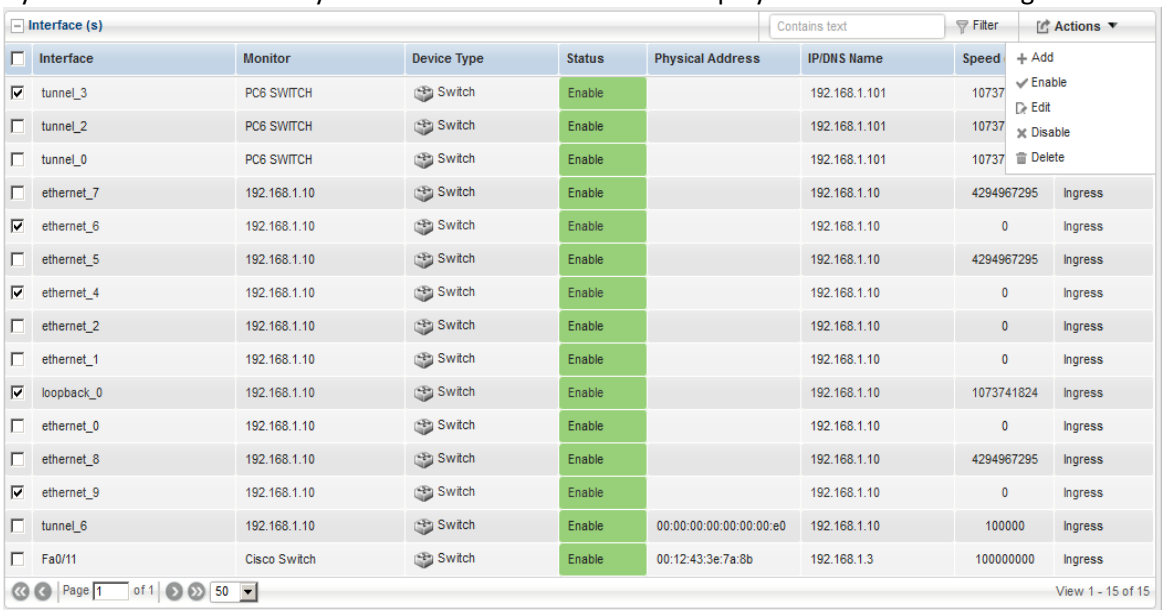


Fig.. Add Flow Monitors

8.3. Creating IP Groups for Classifying Flow Data

Flow analysis engine allows you classify flow data based on specific IP groups. IP groups help you classify traffic stats to particular domain or server having multiple ip addresses.

To create IP groups, follow the steps given below:

1. Navigate to **Flow** > **IP Groups**.
2. Click **New** button, IP group dialog appears.
3. Provide **Name** for the group.
4. Provide IP addresses to associate with the group.
5. Click **Save**.

The system now adds now IP group and displays confirmation message of the action.

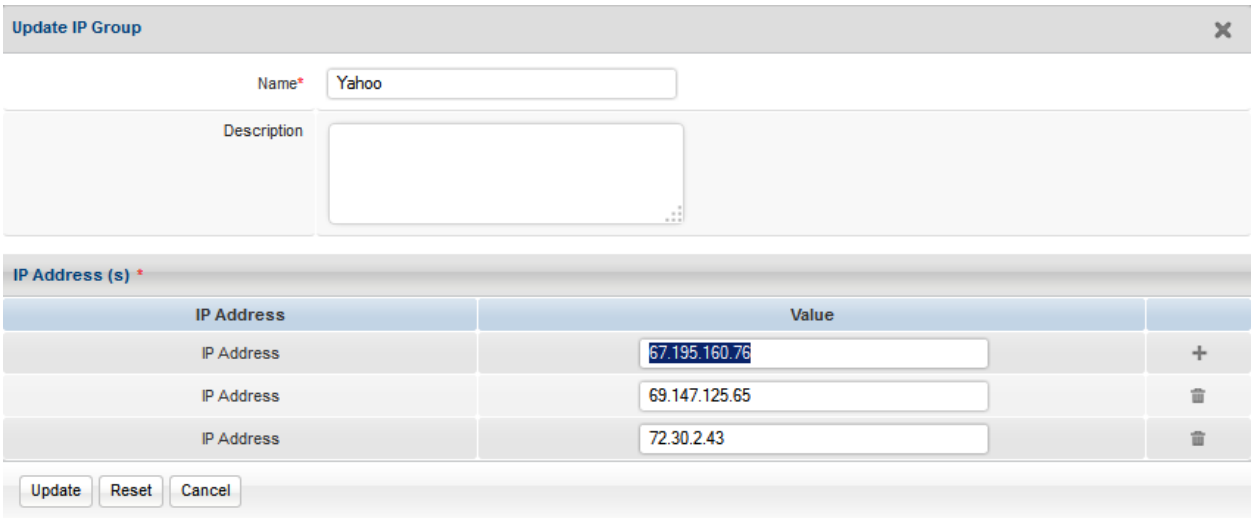


Fig. Creating IP Group to classify traffic flow.

8.4. Viewing Flow Data Analysis by Interface(s)

By default, Minder flow analysis engine gives you data analysis for part 24 hours. You can change the time span by selecting it on the top.

To view flow data analysis of any Interface, follow the steps given below:

1. Navigate to Flow > Overview.
2. Select the appropriate filter from the top to refresh data.
3. You can change the chart type and attributes using the dropdowns on the top.

9 Working with Policy and Alarm (Event)

Policies (Thresholds) define expected bounds for resource values. When the value returned by a resource or component violates a threshold, the system creates an alarm.

Read the following set of instructions for the following attributes:

- Policy Profiles.
- Managing Alarm Events.
- Alarm Annotation.
- Assign/Acknowledge Alarm.
- Suppress Alarm.

9.1. Creating Policy Profile (Alarm)

The New Policy Tab lets you create various thresholds for monitors and their components. Minder allows you to set threshold for different device resources and for different situation

Follow these steps to create new Policy:

1. Navigate to **Policies & Alerts** > **Performance Policy** > **New**.
2. Provide the **Policy Name.**
3. **Flap Count** - Specify consecutive poll count before the system assigns Critical and Warning threshold.
4. Provide desired condition and threshold to evaluate critical and warning threshold.
5. Provide the **Alert**, **Action** and **Escalation Profiles** from the list to invoke when critical or warning threshold triggered.
6. Click **Add** to assign monitor to performance policy profile.
7. Provide **Monitor Type** such as Application Server Monitor, Network device, Server > Select the performance attribute from the list > Click **Search Monitor** to find Monitor having that attribute.
   Note: The system allows you to associate policy with resource attribute values. The returned value of resource attribute is evaluated based on provided threshold values.
8. Click **Add** to selected monitor and their attributes.
9. Click **Create** to associate policy with them.

The system will create Performance Policy and attach it to specified monitor > attributes and displays confirmation message of the action.

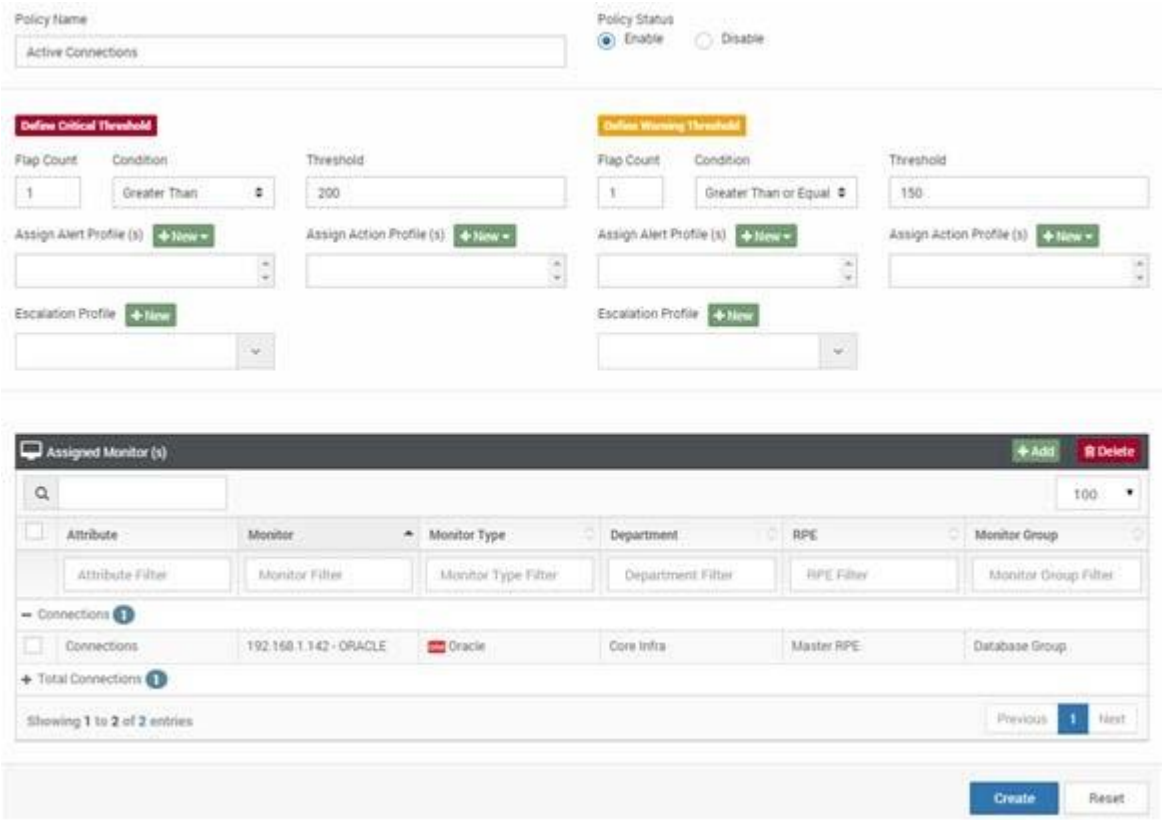


Figure: Performance Policies

Note: Once policy is associated to any attribute of the monitor, system generates an alarm and based on the value returned by a resource system evaluates the threshold and assigns severity to the alarm.

9.2. Viewing Monitor Alarm

Alarms associated to specific monitor are used to determine health of the monitor.

To view the list of associated alarms, follow the steps given below:

1. Navigate to **Monitors** > **Monitor** tab.
2. Click icon to view list of alarms on specific monitor,

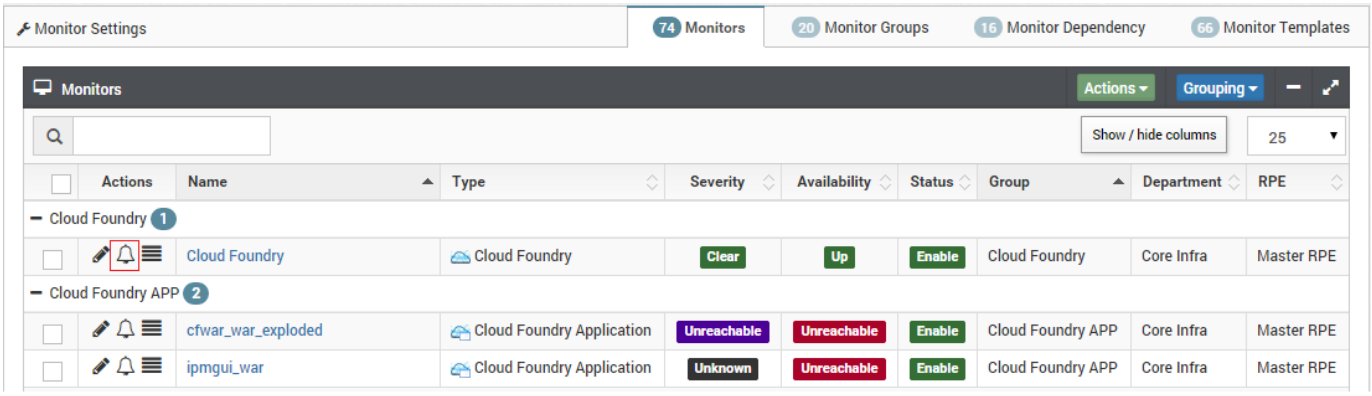


Figure: Viewing alarm

9.3. Delete/Disable Alarm

The system allows you to delete or disable associated policy from resource attribute(s). Removing policy will stop evaluating threshold from attribute value and assigns the unknown severity to attribute values.

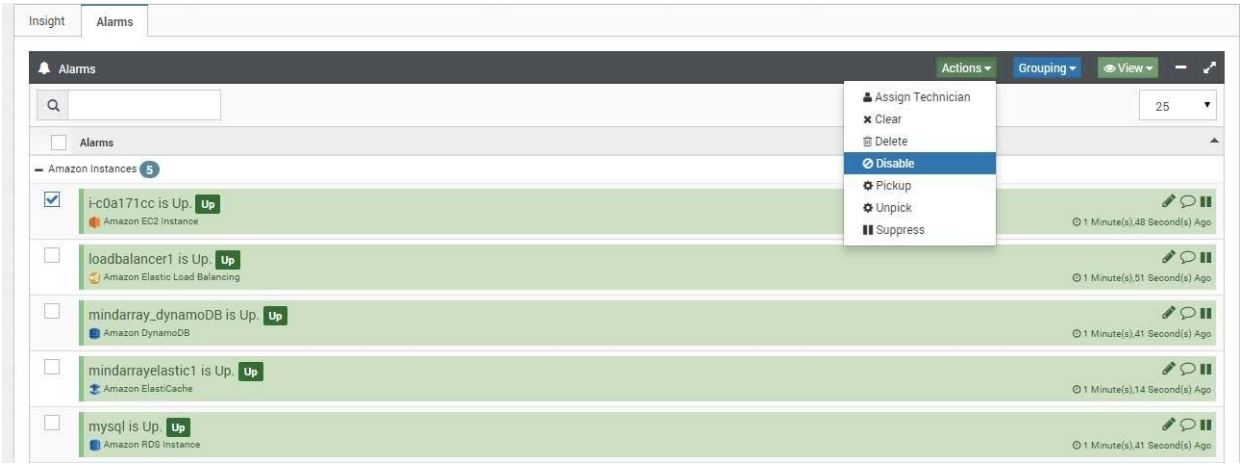


Fig: Delete/Disable Alarm.

Follow the steps given below to disassociate a policy from performance attribute:

1. Navigate to **Alarms** > **Alarms** tab.
2. Alarm page appears. The list displays all the alarms and their respective performance attributes.
3. Select the alarm that you want to disable/delete.
4. Click **Actions** > **Delete/Disable.**

The system disassociates policy from selected Attribute and displays confirmation message of the action.

9.4. Manage Alarm Events

The system allows you to consolidate all the alarm events that are generated from performance attributes and from traps. You can view these events at one central dashboard under Alarms.

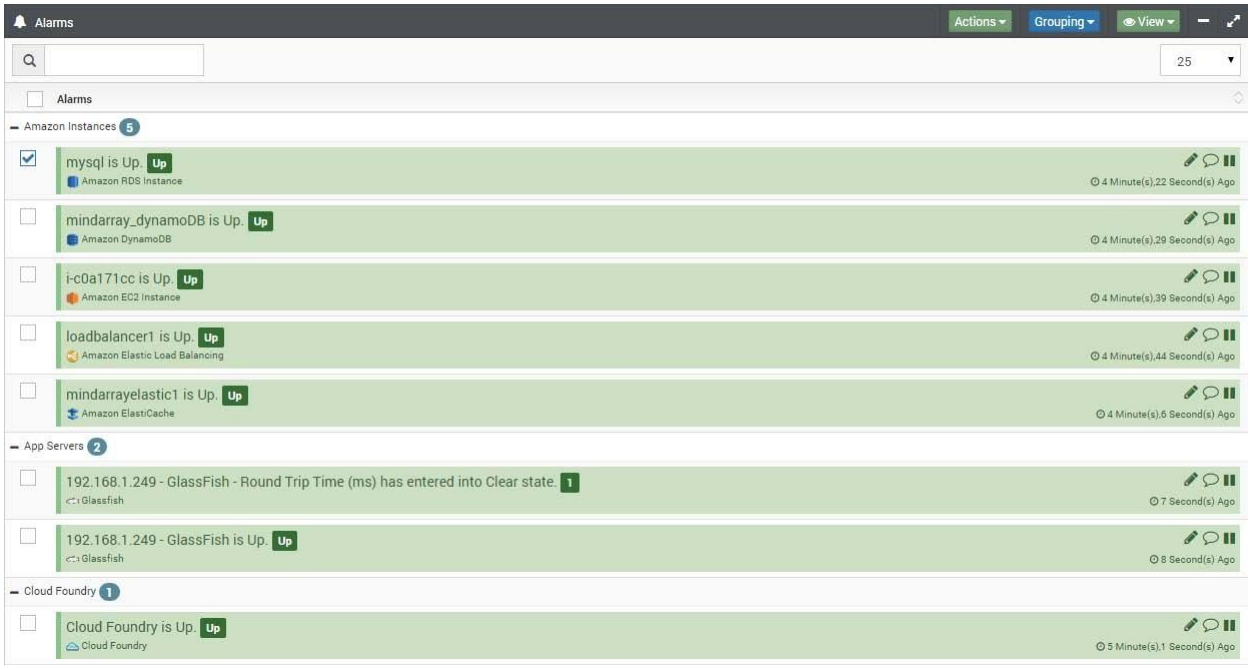


Figure Alarm Dashboard

The system automatically assigns a unique Event ID to each event. By default, the Alarm Dashboard sorts events from newest (top) to oldest (bottom). You can sort alarms in reverse order by clicking the Time Stamp column header. Similarly, you can sort all columns in the Alarm Dashboard by clicking on any column header. You can also add/remove columns from the grid by clicking on Columns on the top.

9.5. Alarm Annotation

Annotation can be done on each alarm by multiple users.

Follow these steps to annotate alarm:

1. Navigate to **Alarms** > **Alarm** tab.
2. Click on **Annotation icon**, Annotation dialog appears.
3. Click on **New** button to add comment.
4. Click **Create**.

Figure: Alarm Annotations

The system will save the added comments and displays confirmation message of the action.

Note: This annotation can be accessed by any users.

9.6. Assign/Acknowledge Alarm

You can quickly acknowledge an alarm event by selecting one or more events and clicking on the **Actions** > **Pickup** Alarm. You can assign alarm events to other users by selecting one or more events and this enables you to pass the events to other users to acknowledge.

Note: In order to acknowledge assigned alarm events, User have to pickup events that are assigned to them.

9.7. Suppress Alarm

You can acknowledge and suppress alarm event until a specific date and time.

Follow the steps given below to acknowledge and suppress events:

1. Navigate to **Alarms** > **Alarms**.
2. Select desired alarm from the list > Click on **Actions** > **Suppress**. Suppression Configuration dialog appears.
3. Provide **Date and time** until which you want to suppress alarm.
4. Click **Update**.

Note: When you acknowledge an alarm event, the state of the monitor also changes on the Monitor Overview Page. MINDER does not use the suppressed alarm to calculate the monitor status (severity) when a performance attribute alarm is in a suppressed state.

9.8. Creating Alarm Escalation Profiles

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 Minder to escalate such unnoticed alarms by sending an e-mail to the person concerned.

To create new alarm escalation profile, follow the steps given below:

1. Navigate to **Policies & Alerts** > **Escalation Profiles**
2. Click on **New** button, Escalation Profile dialog appears.
3. Provide the **Escalation Steps** – By clicking on Add button.
4. Provide the **Alert name** and **Escalation Time (Minutes)**.
5. Repeat the same for Second step. Alert Profile specified in second step will be executed in the specified escalation time after the first steps has been executed.
6. Click **Save**.
7. Assign Escalation profile to any Policy profile to execute.

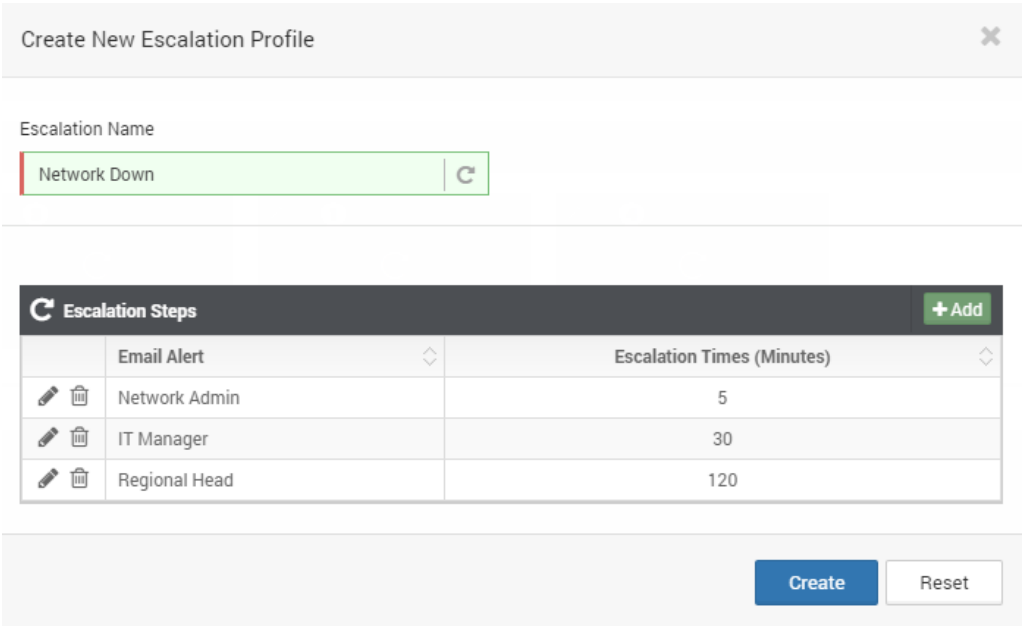


Figure Escalation Profile

10 Working with Alerts & Actions

The Alert & Action tab contains the list of "Actions" that can be configured to be executed when threshold is broken.

Note: To execute Alert & Action profiles, they must be attached to policies. You can configure policies on any performance attributes. For information on Alarm and Policy see section 7 - Working with Policy and Alarm.

Here's the list of Actions that can be configured:

1. **Email Alert (s)**
2. **SMS Alert(s)**
3. **Application Action(s)**
4. **Cloud Auto Scaling(s)**
5. **Log Forward(s)**
6. **Power Action (s)**
7. **Script Action (s)**
8. **Service Action (s)**
9. **SNMP Trap Action (s)**
10. **Virtual Machine Action(s)**
11. **Ticket Action(s)**

10.1. Email Alert(s)

When a threshold is violated in your network you can create alert profiles to notify a user(s) by adding them in your performance policies. To notify a user, provide its email address. You can send an alert to multiple recipients.

Note: You can leave Message subject and body blank to receive default message generated by system or customize the message using following listed macros based on your requirements.

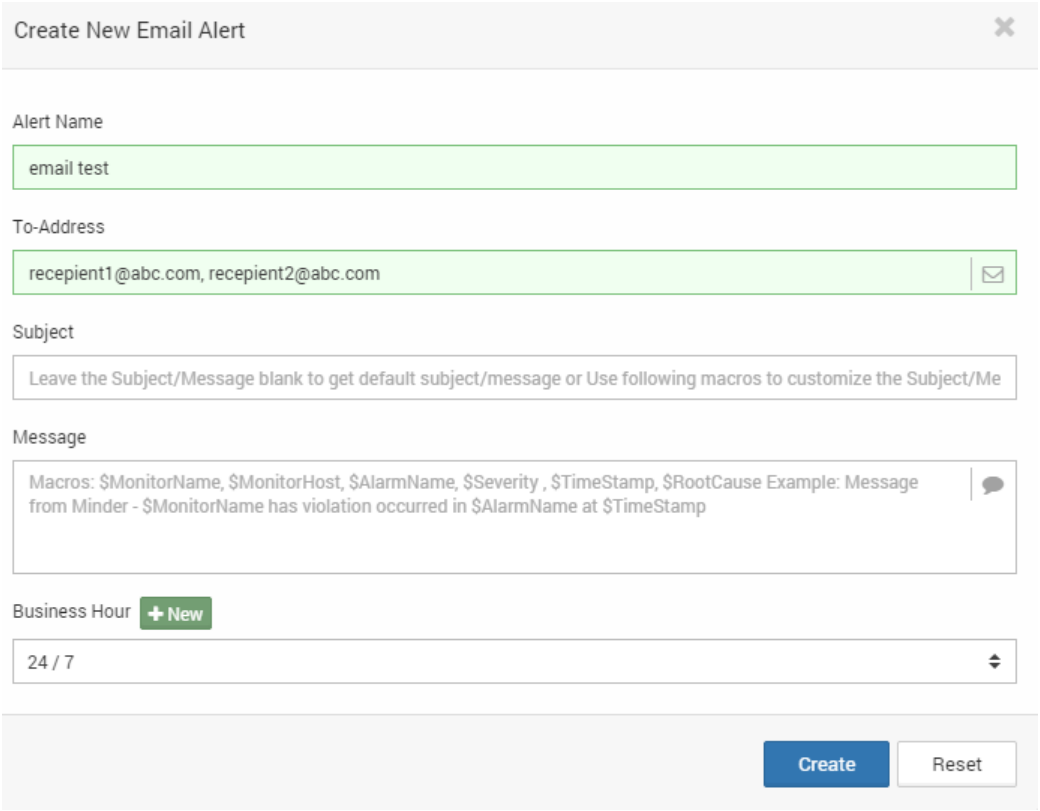
To Configure Send E-Mail follow below steps:

1. Navigate to **Policies and Alerts** > **Alert Profiles** > **Email Alert**.
   Note: These actions will work only after you have configured the Email server under "Configure Mail Server" in "Admin" panel.
2. Provide the **Alert name**.
3. Provide the **Recipient's Address** to send the Emails. You can provide multiple addresses separated by comma.
4. Leave the **Subject** Blank for default message subject or Use following macros to customize the Subject line.
   Macros: $MonitorName

$MonitorHost
$AlarmName
$Severity
$TimeStamp
$RootCause

Example: Message from MINDER - $MonitorName has violation occurred in $AlarmName at $TimeStamp

5. Leave the **Message body** blank to receive default message generated by system or use above macros to customize the Message Body.
6. Select the Business hours when you want to receive the emails. Additional business hours can be added at **Admin Panel** > **Business Hours**.
7. Click **Create**.



The system creates Email Alert action and displays confirmation message of the action.

Note: Mail Server under admin panel must be configured before to create Email Alerts.

Restrict No. of Alerts: You can control the number of alerts to be sent globally (keep sending the alerts until the severity is changed or send only specified number of alerts even if critical state is not changed) when violation occurs. See section 9.6.1 for more information.

10.2. SMS Alert(s)

This feature allows you to deliver alerts and notifications to specified SMS devices in addition to standard email notifications.

Follow the steps given below to configure SMS alert profiles:

1. Navigate to **Policies & Alerts** >**Alert Profiles**>**New**>**SMS Alert**.
2. **Create New SMS Alert** dialog appears.
3. Provide an appropriate **Alert Name**.
4. In **To-Address** field, provide the phone number you want to send the SMS to.
5. Provide an appropriate **URL**.
   E.g.http://login.somegateway.com/api/sms.aspx?user=userName&pwd=password&to={to}&sid=SMS & msg={message}
   Note: Make sure that the "{to}" and "{message}" parameters are mentioned in the URL.
6. If you want to send a customized message, specify it in the **Message** field.
7. Provide a **Business Hour**.

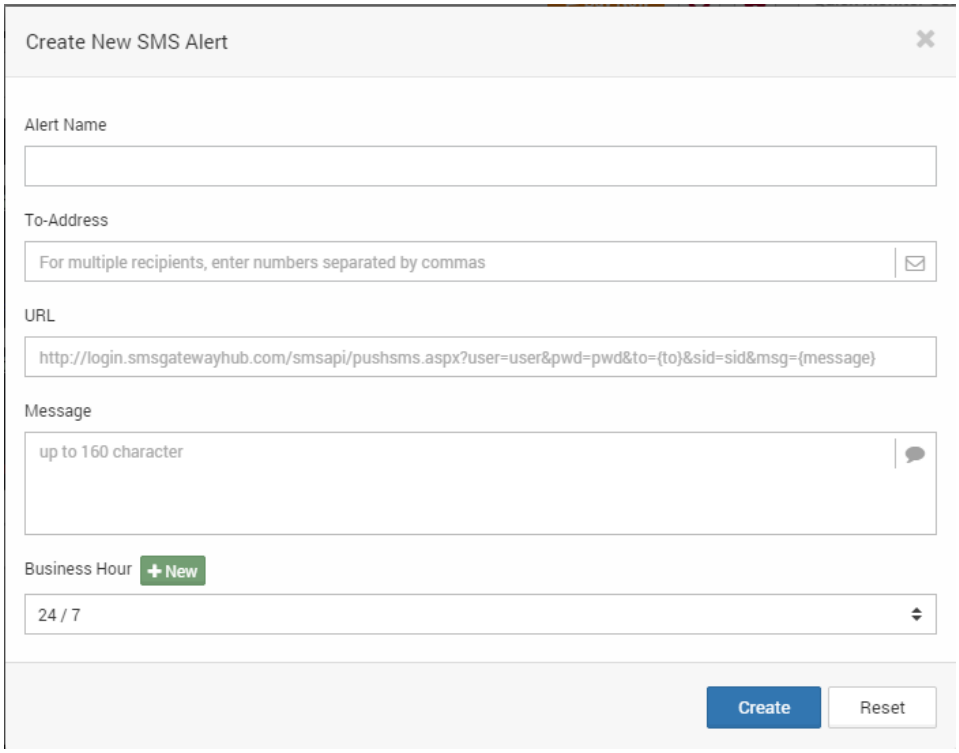


Figure SMS Alert

The system will create the SMS Alert profile and display a conformation message of the action.

You can assign this alert profile to policies, due to which, an SMS with the message specified by you will be sent to the specified phone numbers in case of any threshold violations.

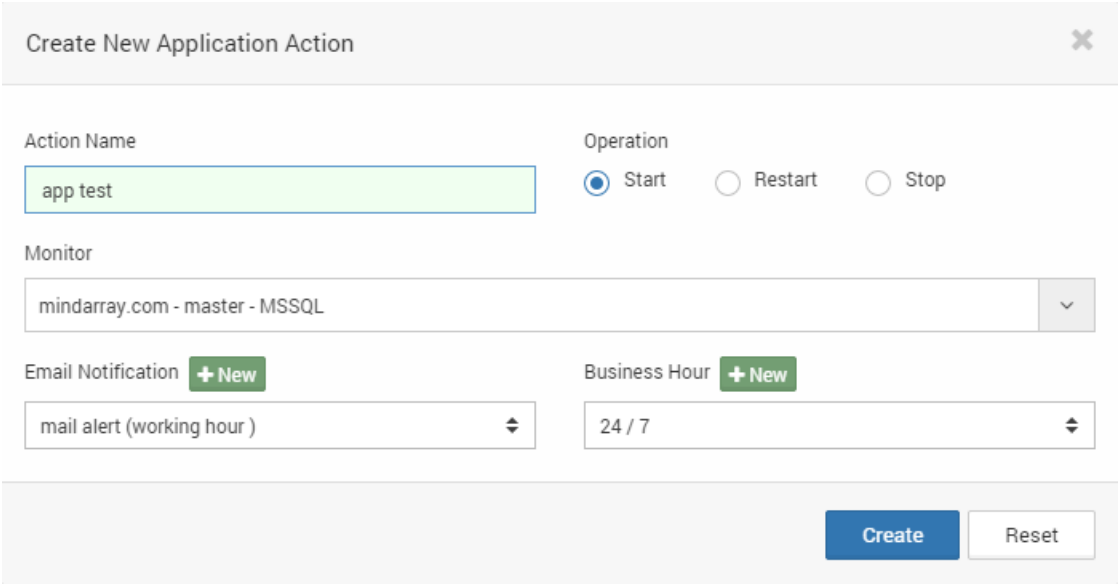
10.3. Application Action(s)

Application action enables you to start/stop/ reboot applications in case of threshold violation. Minder will notify the results to email recipient provided in this action. Minder currently supports these operations only for the following applications:

- **Amazon EC2, Cloud Foundry App applications for cloud**
- **MSSQL application for Database server**
- **Active directory and MSMQ for Middleware**
- **IIS server applications**

Follow below steps to create action to manage Applications:

1. Navigate to **Policies & Alerts** > **Action Profiles** > **New** > **Application**.
2. Provide the **Action Name**.
3. Select **Operation** type.
4. Select the target application **Monitor** from the dropdown.
5. Select **Email alert** profile to get notified about action result.
6. Select the **Business Hours** for action to execute.
7. Click **Create**.



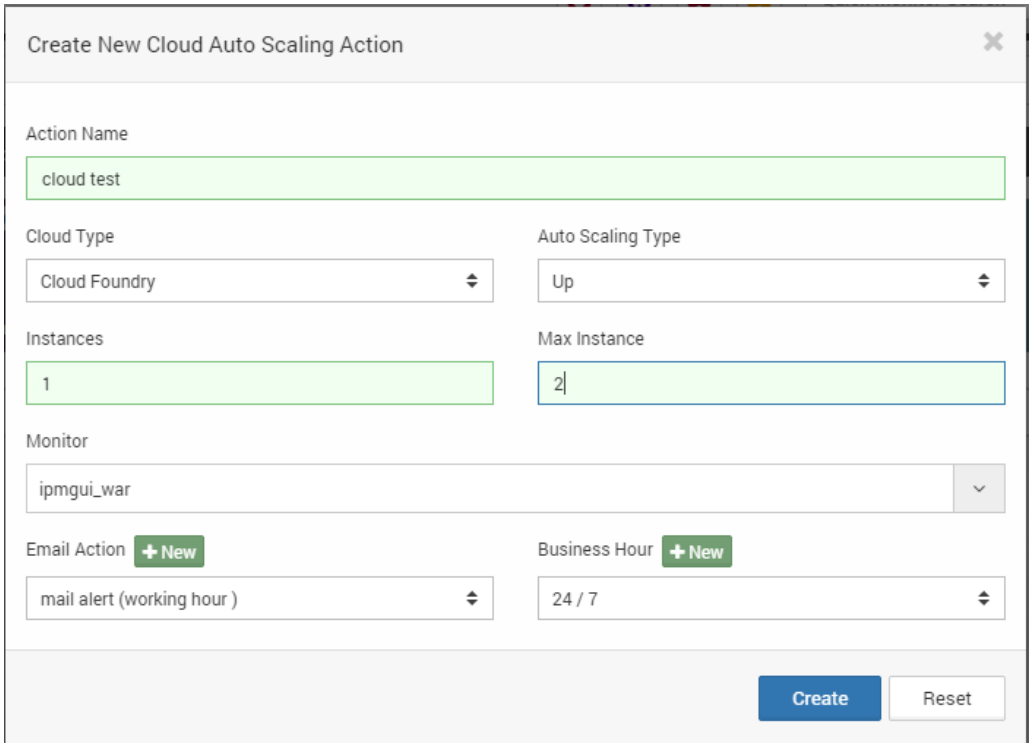
The system creates Application action and displays confirmation message of the action.

10.4. Cloud Auto Scaling(s)

When we use an application on the cloud, it provides us with a default instance. But if there are a large number of requests and one instance can't satisfy all of them, then using auto scaling we can increase or decrease the number of instances as per our requirement. This automatic increase/decrease in the number of instances is called cloud auto scaling.

Follow below steps to create action to manage Cloud Auto Scaling:

1. Navigate to **Policies & Alerts** > **Action Profiles** > **New** > **Cloud Auto Scaling**.
2. Provide the **Action Name.**
3. Select the **Cloud Type** from list.
4. Provide **Auto Scaling Type**.
5. Provide number of instances to be created.
6. Select the target application **Monitor** from the dropdown.
7. Select **Email alert** profile to get notified about action result.
8. Select the **Business Hours** for action to execute.
9. Click **Create**.



The system creates Cloud Auto Scaling action and displays confirmation message of the action.

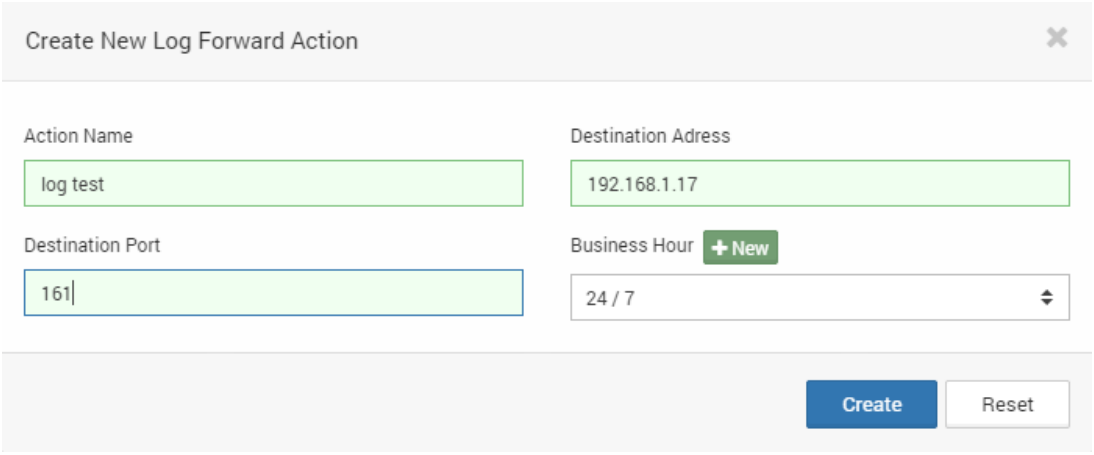
10.5. Log Action(s)

Event Log (Log regarding the policies) generated will be forwarded to the specified IP address at a specific port.

Follow below steps to create action to manage Log:

1. Navigate to **Policies & Alerts** > **Action Profiles** > **New** > **Log Forward.**
2. Provide the **Action name**.
3. Provide the **Destination Address** where you want to receive the logs.

4. Provide the **Destination Port** where you want to listen to the logs sent from here.
5. Select the **Business Hours** for action to execute.
6. Click **Create**.



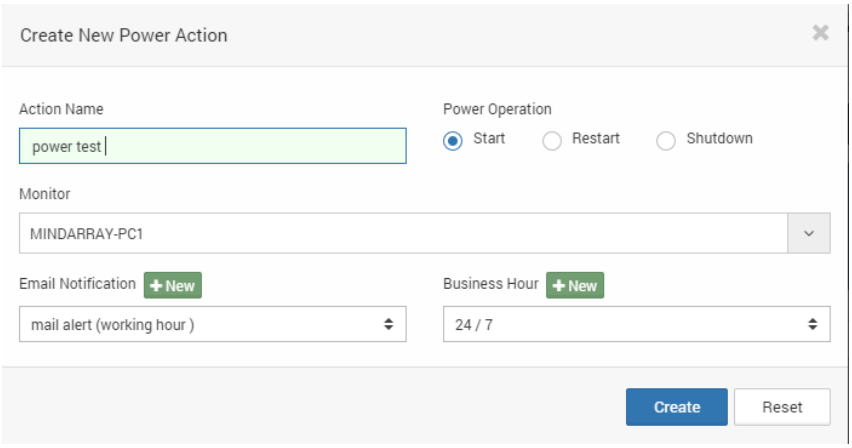
The system creates Log action and displays confirmation message of the action.

10.6. Power Action(s)

You can shutdown/start/restart any system from Minder console. The power actions are very helpful to remotely shutdown or restart a system a certain time. Based on the policies created you can easily avoid outage with the help of power actions.

Follow below steps to create a Power action:

1. Navigate to **Policies & Alerts** > **Action Profiles** > **New** > **Power**.
2. Provide the **Action Name**.
3. Select the **Operation Type**.
   Note: For "Start" operation "monitor MAC address" and "monitor BROADCAST address" are needed to be updated in the relevant monitor.
4. Select the host **Monitor** on which you want to apply the Power Action.
5. Select the Email Alert as defined in the **Email Action** to get the email notification.
6. Select the **Business Hours**.
7. Click **Create**.



The system creates Power action and displays confirmation message of the action.

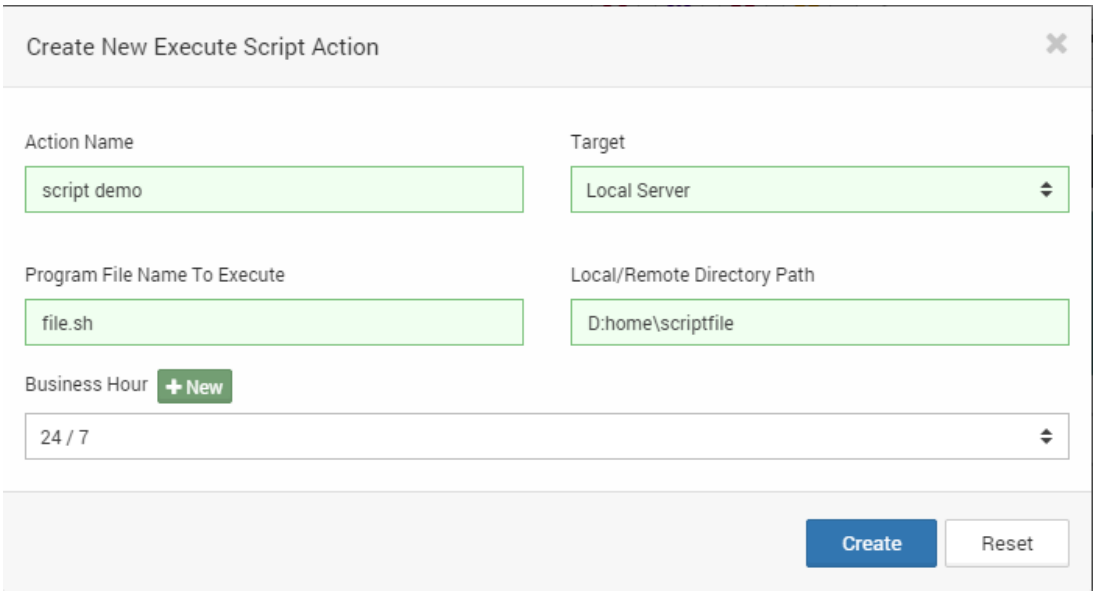
10.7. Script Action(s)

There are several circumstances where you may want to execute a program when a specific network event occurs. Use the Edit Execute Script Action to specify the executable that should be started when the specified alert is triggered or reset, as shown in the following procedure.

Execute your own script, either on local server or on remote server. Provide the path and filename of batch file and rest of the job will be done by the system.

Follow below steps to create action to execute script:

1. Navigate to **Policies and Alerts** > **Action Profiles** > **New** > **Script**.
2. Provide the **Action Name**.
3. Select the **Target** of the script whether you want to execute script locally or remotely.
4. For Remote Target provide select the monitor where you want to execute the script.
5. Provide the **Name of Script file**. E.g. FileName.sh or FileName.bat
6. Provide directory path excluding the filename. For Windows remote target, script should be located on Remote machine.
   Example: D:\foldername\foldername
7. Select the **Business Hours**.
8. Click **Create**.



The system creates Script action and displays confirmation message of the action.

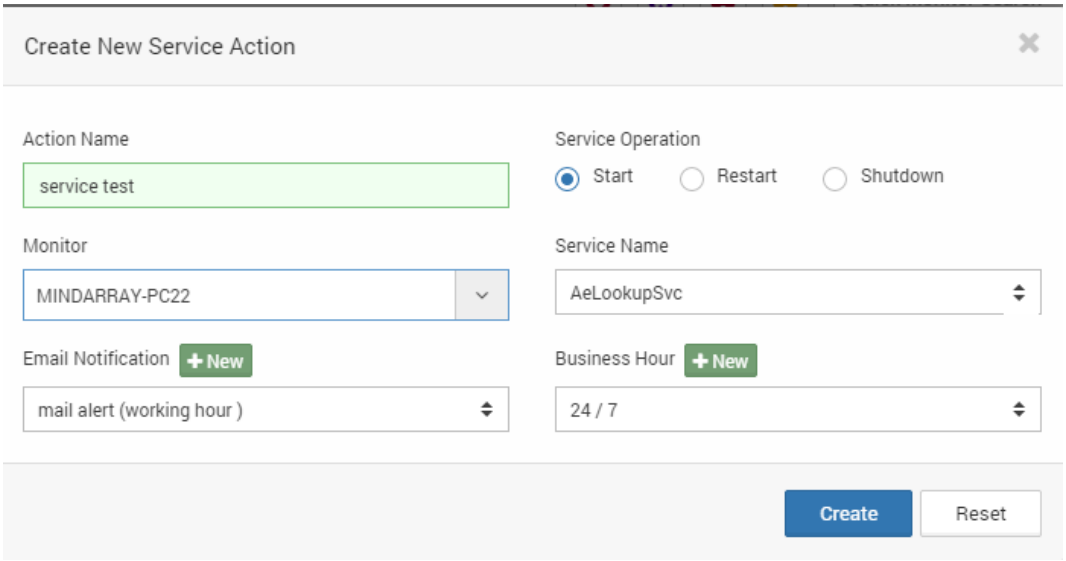
10.8. Service Action(s)

You can shutdown/start/restart any service for the listed monitors from Minder console. The Service actions are very helpful to overcome the stuck process situation for the resources when they violate certain thresholds. So based on the policies created you can easily avoid outage with the help of this Service action.

Note: The monitors in which services are added through Service manager will be listed in the drop down list of monitor.

Follow below steps to create a Service action:

1. Navigate to **Policies & Alerts > Action Profiles > New > Service**.
2. Provide the **Action Name**.
3. Select the **Operation** Type.
   Note: For “Start” operation “monitor MAC address“ and “monitor BROADCAST address” are needed to be updated in the relevant monitor.
4. Select the host **Monitor** on which you want to apply the Service Action.
5. Provide **Email Alert** profile to get the email notification.
6. Select the **Business Hours**.
7. Click **Create** to finish.



The system creates Power action and displays confirmation message of the action.

10.9. SNMP Trap Action(s)

SNMP trap action enables you to send desired message as SNMP trap in case of threshold violation. Minder will notify the listener you have configured in this action.
Follow below steps to create action to send SNMP Trap:

1. Navigate to **Policies & Alerts** > **Action Profiles** > **New** > **SNMP Trap**.
2. Provide the **Action Name**.
3. Provide the **Destination Address** where you want to receive the traps.
4. Provide the **Destination Port** where you want to listen to the traps sent from here.
5. Provide the **Object OID** which you want to bind/display with the trap to be listened.
6. Provide the **Message** to be bound/display to trap to listen.
7. Provide the **Community** for the trap to be listened.
8. Select the **Business Hours** for action to execute.
9. Click **Create** to finish.

The system creates SNMP trap action and displays confirmation message of the action.

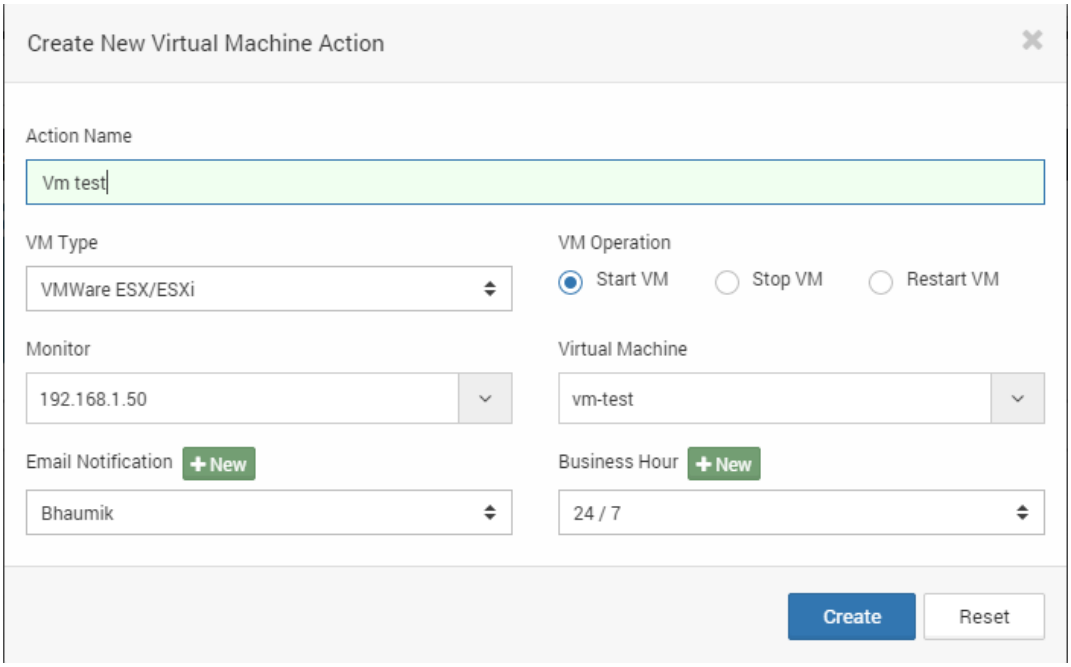
10.10. Virtual Machine Action(s)

Virtual Machine action enables you to start, stop and reboot virtual machines in case of threshold violation. Minder will notify the result to email recipient provided in this action.

Follow below steps to create action to manage Virtual Machines:

1. Navigate to **Policies & Alerts** > **Action Profiles** > **New** > **Virtual Machine**.
2. Provide the **Action Name**..

3. Select the **VM Type** from dropdown whether VMware or Citrix or Hyper-V.
4. Select **Operation Type**.
5. Select the **Host Monitor** from the dropdown (Only provisioned Virtual Machines will be listed).
6. Select target **Virtual Machine** from the dropdown.
7. -Select **Email Alert** profile to get notified about action result.
8. Select the **Business Hours** for action to execute.
9. Click **Create** to finish.



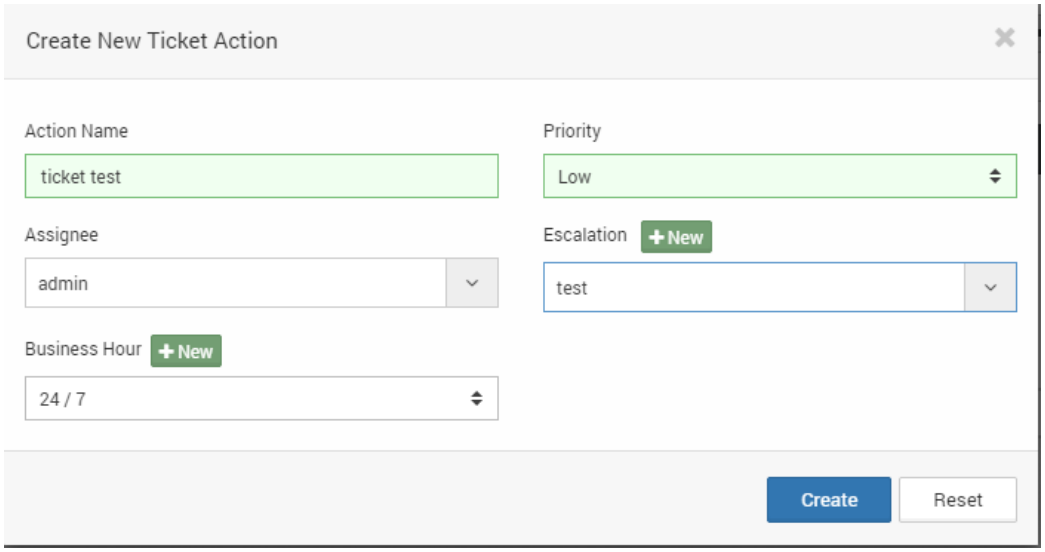
The system creates Virtual Machine action and displays confirmation message of the action.

10.11. Ticket action

You can create a ticket action which you can assign to a performance policy, in which case every time that policy is violated, the ticket will be generated and assigned automatically to the assignee you selected while creating the ticket action.

Follow the steps given below to create a ticket action:

1. Navigate to **Policies & Alerts** >**Action Profiles** >**New** >**Ticket**.
2. Provide the **Action Name**.
3. Select **Priority** for the ticket from the drop down list.
4. Select the **Assignee**.
5. Provide **Escalation profile** from the list or create a new one.
6. Provide the **Business Hour** for the action to execute.
7. Click on **Create**.



The system creates a Ticket action and displays a confirmation message of thesame.

11 Scheduler

Minder provides the ease of use for scheduling different tasks for various categories and generating their reports. Whether it is report generation or monitoring a particular server, you can manage the task at any instance of time.

Minder scheduler allows you to schedule the tasks in different categories namely: generating various reports, managing various monitors' details and network discovery information, power operations, Script execution & Service actions.

We have the following entities based on which the scheduler details and configurations change.

- **Report Job**
- **Network Discovery Job**
- **Power Operation Job**
- **Execute Script Job**
- **Service Operation Job**
- **Monitor Maintenance Job**
- **Alarm Suppression Job**
- **Rediscover Monitor Job**
- **NCM Backup Job**
- **NCM Detection Job**

11.1. Schedule Report Job

Report job allow you to automatically generate reports as per the date and time specified by you.

To schedule the Report Job follow the steps given below:

1. Navigate to **Scheduler** > Click on the date you want to schedule a report.
2. **Report Job dialog** appears, Provide the Scheduler Name.
3. Provide the **Status** as Enable to start scheduler.
4. Provide the **Scheduler date and time** to run the job.
5. Select the **Report Category** you want to send from the various reports listed.
6. Select the **Report Template Name.**
7. Select the **Report Type** you want.
8. Select the **Email Notification** action for the Job.
9. If you want to repeat the job daily/weekly/monthly, provide the schedule time for the operation to repeat daily/weekly/monthly.
10. Click **Create** to finish.

The systems saves Scheduled event and displays a confirmation message of the action.

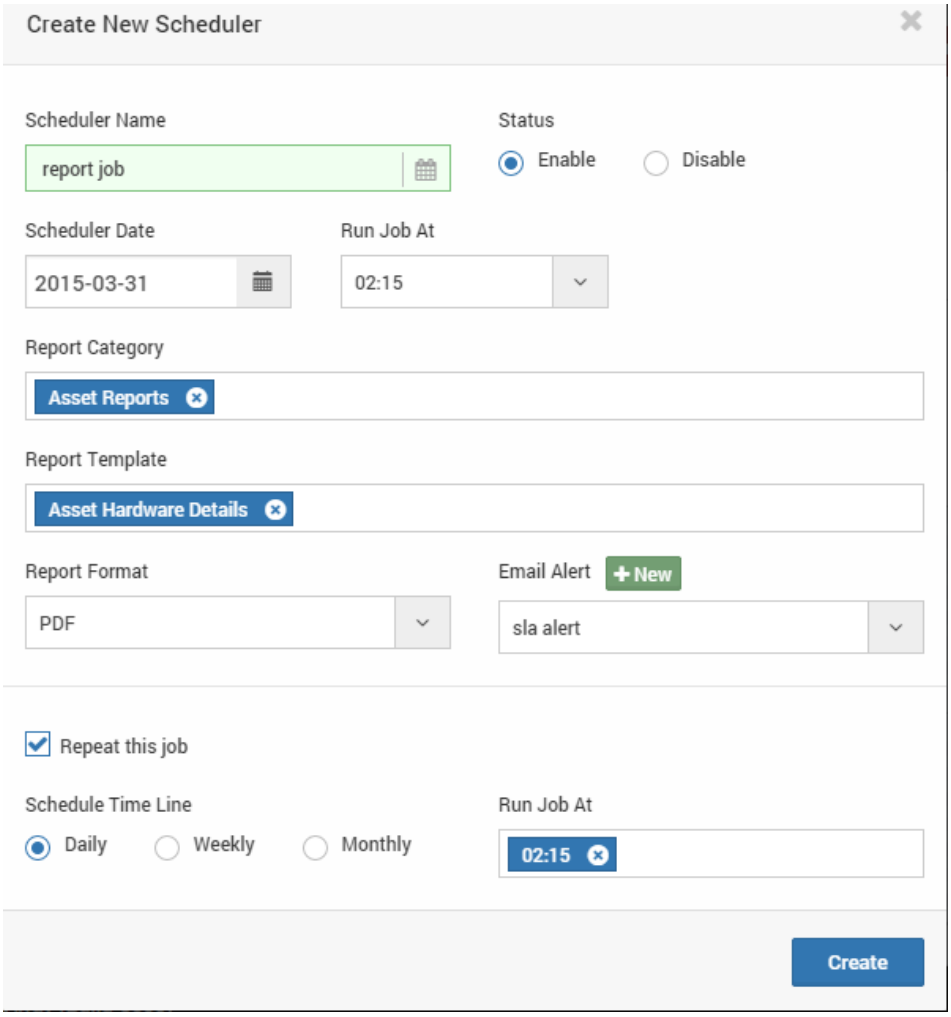


Figure Create scheduled Jobs

11.2. Schedule Network Discovery Job.

Network discovery job allows you scan network on the specified time interval. When this job runs it reports the newly found nodes in the Notification area in the top.

To schedule a Network Discovery job, enter the following details and save the configuration.

1. Navigate to **Scheduler** > Drag and drop Network Discovery job from the top on calendar.
2. **Network Discovery Job dialog** appears, Provide the Scheduler Name.
3. Provide the **Status** as Enable to start scheduler.
4. Provide the **Scheduler date and time** to run the job.
5. Select pre-build network discovery from the list.
6. If you want to repeat the job daily/weekly/monthly, provide the schedule time for the operation to repeat daily/weekly/monthly .
7. Click **Create** to finish.

The systems will save Scheduled event and displays a confirmation message of the action.

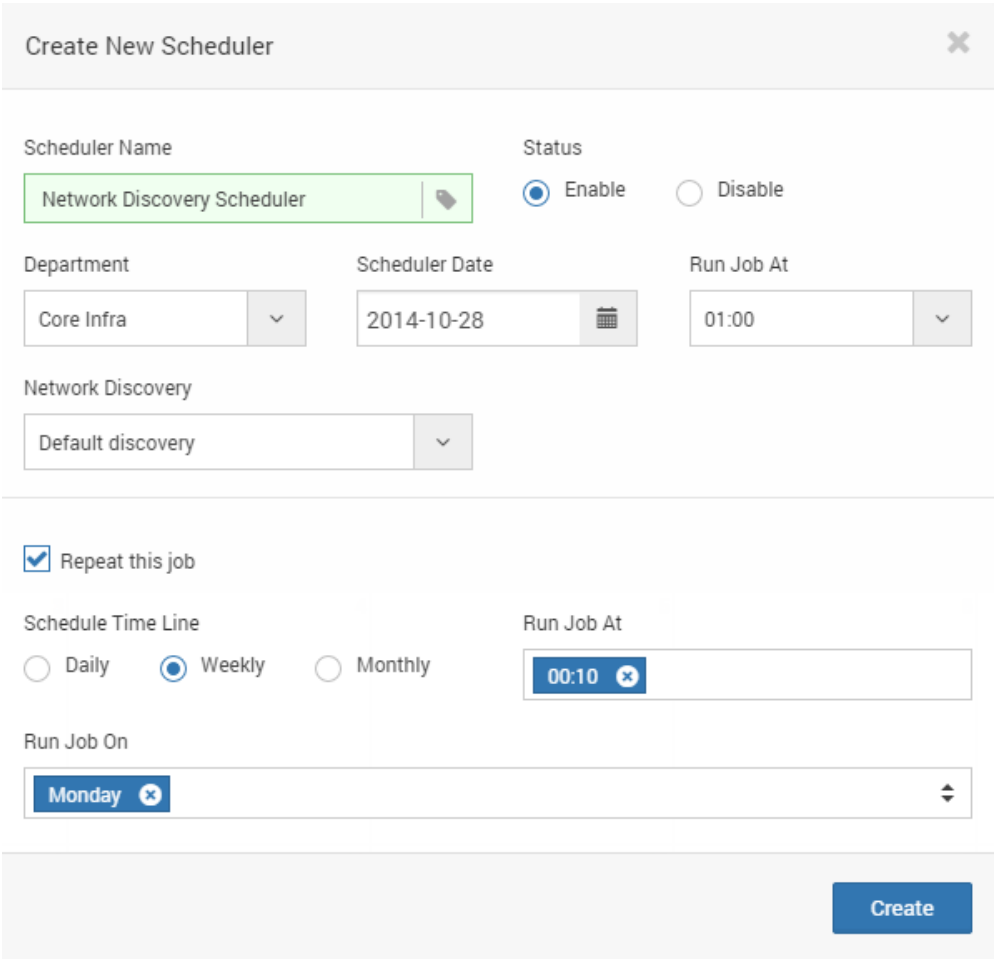


Figure Create network discovery scheduled events

11.3. Power Job

Using Power Job you can schedule start, restart and shutdown operations on any provisioned monitor.

Note: To create power job, you need to have created power action profile. To create scheduled Power job, follow the steps given below:

1. Navigate to **Scheduler** > Drag and drop Power job from the top on calendar.
2. Provide the **Scheduler Name.**
3. Provide the **Status** as Enable to start scheduler.
4. Provide the **Scheduler date and time** to run the job.
5. Select pre-build Power Action from the list to execute which you need to create from **Policies & Alerts > Action Profile.**
6. If you want to **repeat** the job daily/weekly/monthly, provide the schedule time for the operation to repeat daily/weekly/monthly .
7. Click **Create** to finish.

The systems will save Scheduled event and displays a confirmation message of the action.

11.4. Execute Script Job

Script job allows you to schedule the execution of a specific script as per the Execute Script Action Profile.

Note: To create Script job, you need to have created Script action profile.

To create scheduled script job, follow the steps given below:

1. Navigate to **Scheduler** > Drag and drop Script job from the top on calendar.
2. Provide the **Scheduler Name**.
3. Provide the **Status** as Enable to start scheduler.
4. Provide the **Scheduler date and time** to run the job.
5. Select user defined Execute Script Action from the list to execute.
6. If you want to repeat the job daily/weekly/monthly, provide the schedule time for the operation to repeat daily/weekly/monthly .
7. Click **Create** to finish.

The systems will save Scheduled event and displays a confirmation message of the action.

11.5. Windows Service Job

Service job allows you to start, restart or shutdown any specific service of a monitor given in the service action profile on the scheduled date and time.

To create Windows Service job, follow the steps given below:

1. Navigate to **Scheduler** > Drag and drop Network Discovery job from the top on calendar
2. Provide the **Scheduler Name**.
3. Provide the **Status** as Enable to start scheduler.
4. Provide the **Scheduler date and time** to run the job.
5. Select user defined **Service Action** from the list to execute.
6. If you want to repeat the job daily/weekly/monthly, provide the schedule time for the operation to repeat daily/weekly/monthly.
7. Click **Create** to finish.

The systems will save Scheduled event and displays a confirmation message of the action.

11.6. Monitor Maintenance

You can schedule this job to put a monitor in maintenance for a specified/unspecified amount of time.

To create scheduled monitor maintenance job, follow the steps given below:

1. Navigate to **Scheduler** > Drag and drop Maintenance job from the top on calendar.
2. Provide the **Scheduler Name**..
3. Provide the **Status** as Enable to start scheduler.
4. Provide the **Scheduler date and time** to run the job.
5. Select **Target Monitor** from the list.
6. Select **Status** as Enable Maintenance or Disable Maintenance.
7. Provide the **Maintenance Time** along with date and time.
8. If you want to repeat the job daily/weekly/monthly, provide the schedule time for the operation to repeat daily/weekly/monthly .
9. Click **Create** to finish.

The systems will save Scheduled event and displays a confirmation message of the action.

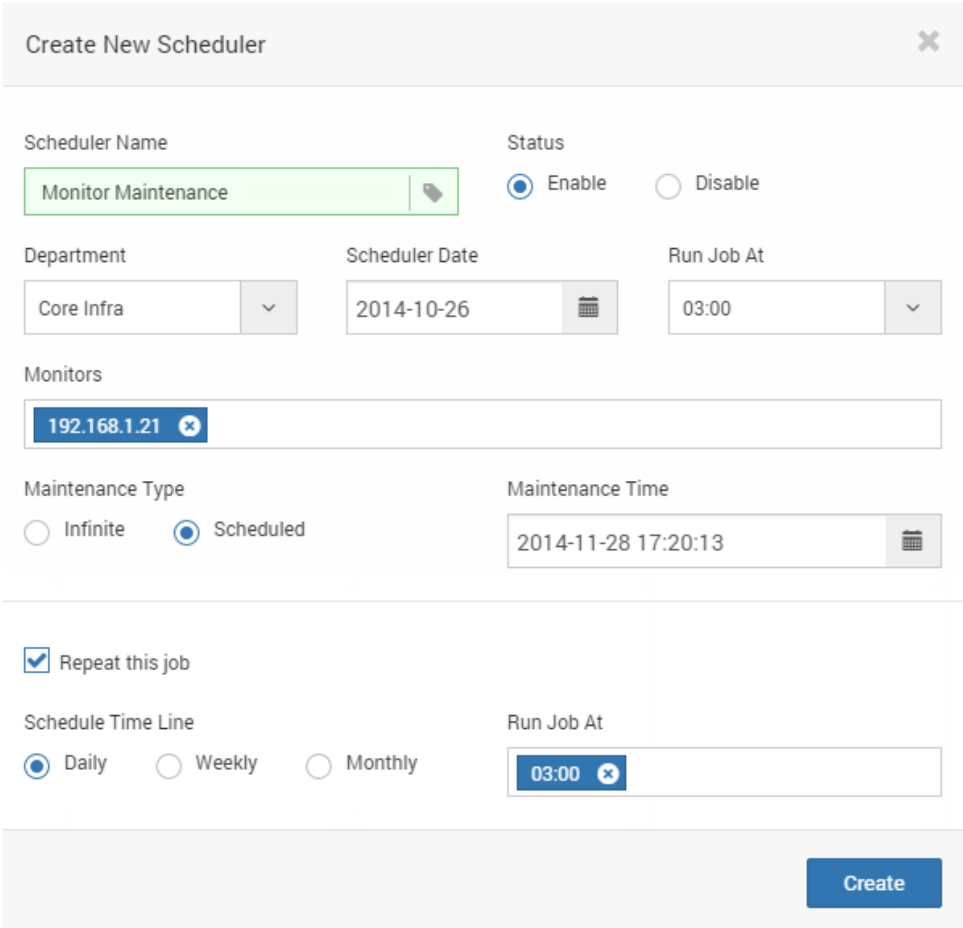


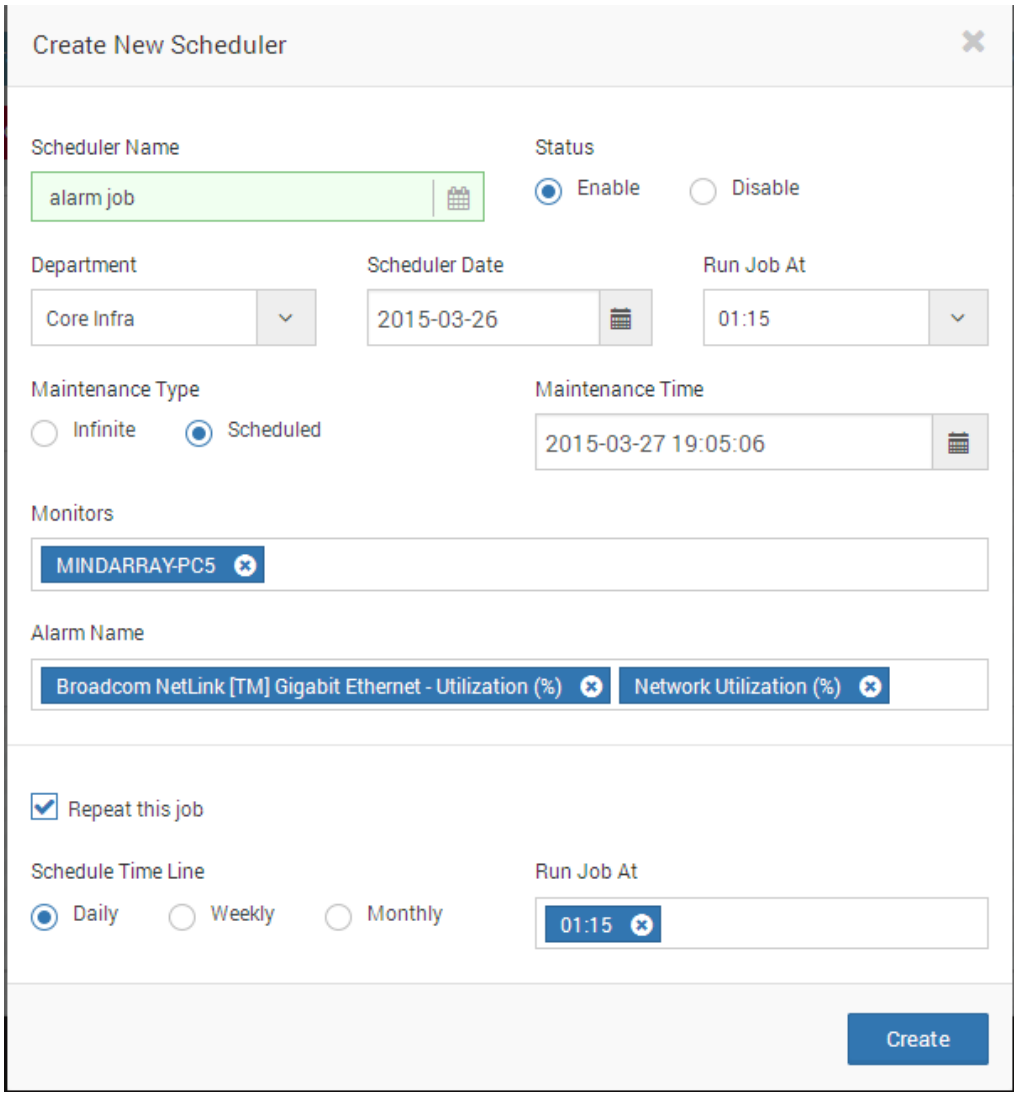
Figure Create monitor maintenance scheduled events

11.7. Alarm Suppression Job

You can temporarily suppress an alarm at a scheduled date and time using alarm suppression job.

To create scheduled Alarm Suppression job, follow the steps given below:

1. Navigate to **Scheduler** > Drag and drop Alarm Suppression job from the top on calendar.
2. Provide the **Scheduler Name**.
3. Provide the **Status** as Enable to start scheduler.
4. Provide the **Scheduler date** and **time** to run the job.
5. Select **status** as Enable Maintenance or Disable Maintenance.
6. Provide the **Maintenance time** along with date and time
7. Select **Target monitor** from the list.
8. Select **Alarm Name** from the list to execute.
9. If you want to repeat the job daily/weekly/monthly, provide the schedule time for the operation to repeat daily/weekly/monthly.
10. Click **Create** to finish.



The system will save Scheduled event and displays a confirmation message of the action.

11.8. Rediscover Monitor

This job is available only for virtualization monitors. It rediscovers the selected the virtualization monitors and automatically provisions all the virtual machines, their process and services.

To create scheduled Rediscover Monitor job, follow the steps given below:

1. Navigate to **Scheduler** > Drag and drop Rediscover Monitor job from the top on calendar.
2. Rediscover Monitor Job dialog appears, provide the **Scheduler Name**.
3. Provide the **Status** as Enable to start scheduler.
4. Provide the **Scheduler data and time** to run the job.
5. Select **Target Monitor** from the list.
6. If you want to repeat the job daily/weekly/monthly, provide the schedule time for the operation to repeat daily/weekly/monthly.
7. Click **Create** to finish.

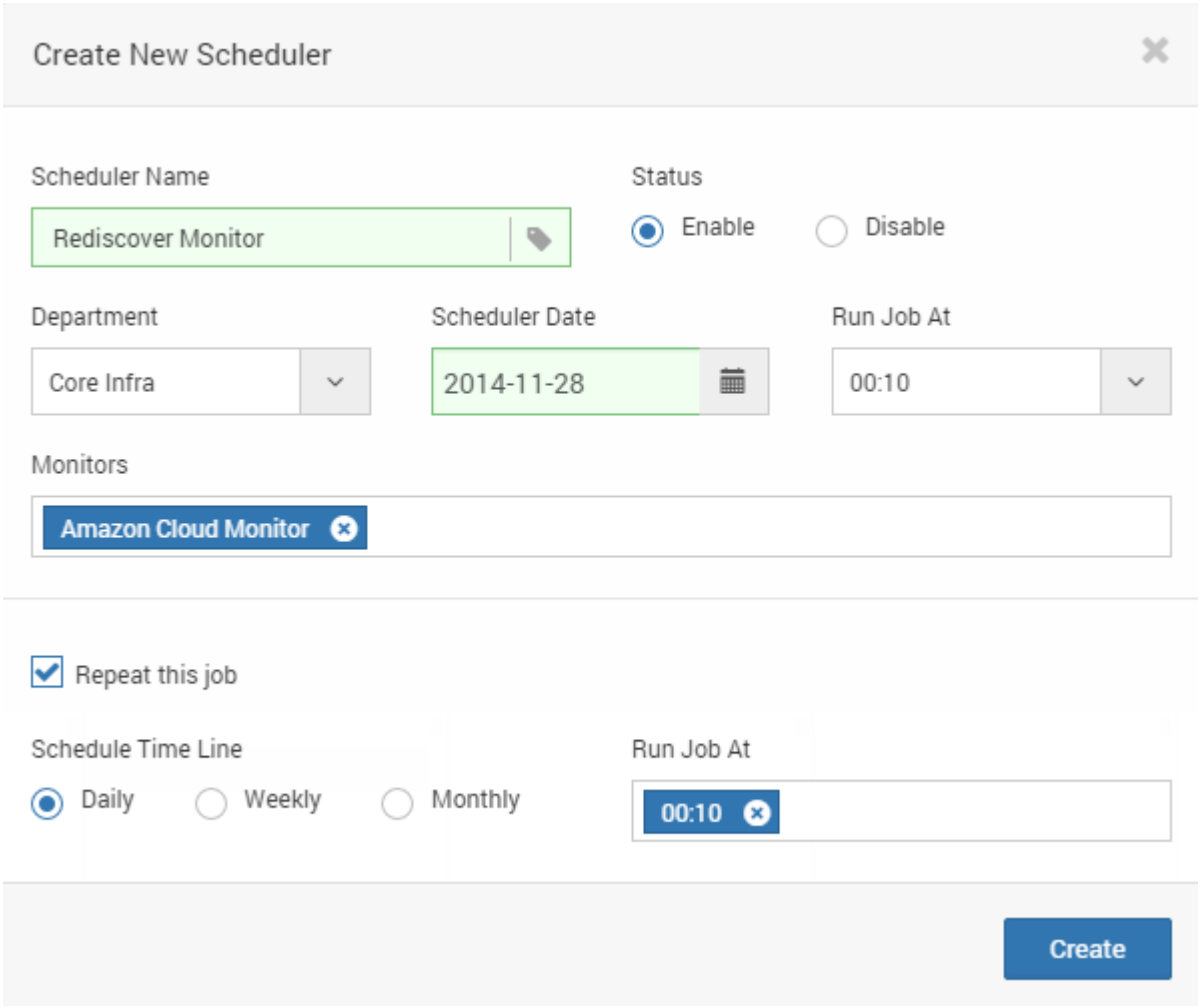


Figure Scheduling rediscover job

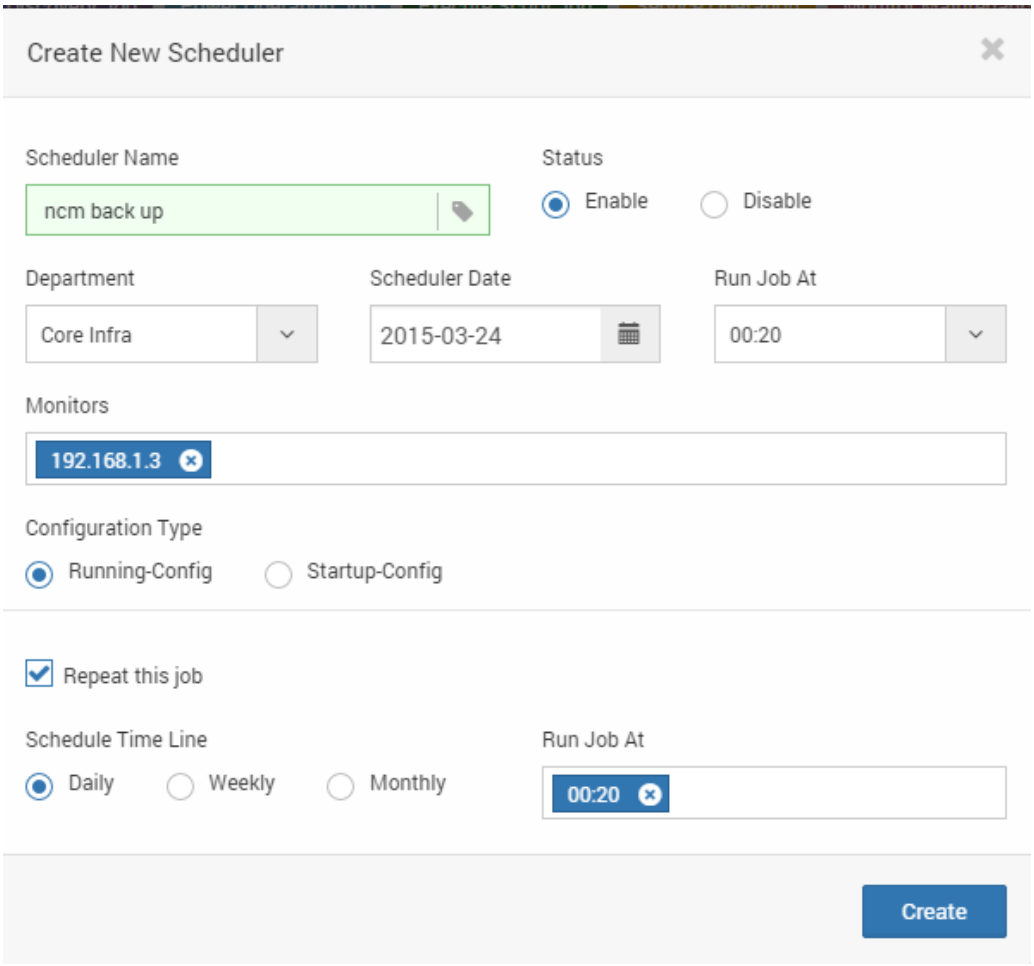
The system will save Scheduled event and displays a confirmation message of the action.

11.9. NCM Backup Job

Taking backup of the data is always the best option, so in case the data is lost due to many problems ranging from computer viruses, hardware failure, etc. You can take the backup at a scheduled date and time using NCM backup job.

To schedule NCM backup job, follow the steps given below:

1. Navigate to **Schedulers** > Drag and drop NCM backup job from the top on calendar.
2. Provide the **Scheduler Name**.
3. Provide the **Scheduler date and time** to run the job.
4. Select the **Monitor** for which you want to take back up.
5. Select the **Configuration Type**.
6. If you want to repeat the job daily/weekly/monthly, provide the schedule time for the operation to repeat daily/weekly/monthly.
7. Click **Create** to finish.

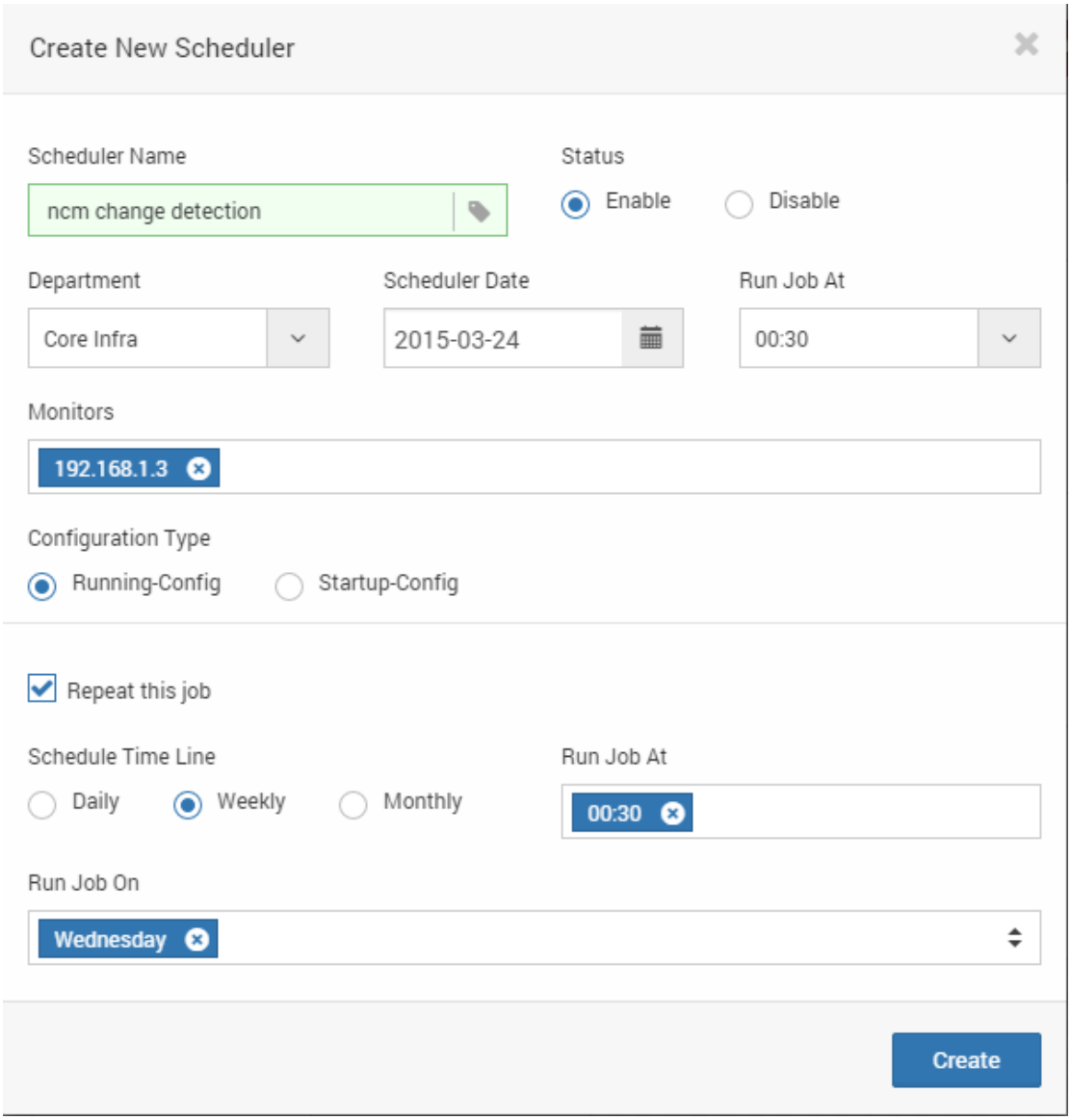


The system will save Scheduled event and displays a confirmation message of the action.

11.10. NCM Change Detection job

To schedule NCM Change Detection job, follow the steps given below:

1. Navigate to **Schedulers** > Drag and drop NCM backup job from the top on calendar.
2. Provide the **Scheduler Name**.
3. Provide the **Scheduler date and time** to run the job.
4. Select the **Monitor** for which you want to take back up.
5. Select the **Configuration Type**.
6. If you want to repeat the job daily/weekly/monthly, provide the schedule time for the operation to repeat daily/weekly/monthly.
7. Click **Create** to finish.



The system will save Scheduled event and displays a confirmation message of the action.

11.11. Off Monitor Maintenance Job

You can schedule this job to get a monitor off maintenance mode at certain user-specified time.

To create scheduled off monitor maintenance job, follow the steps given below:

1. Navigate to **Scheduler** > Drag and drop Off Monitor Maintenance job from the top on calendar. Otherwise, you can just click on the date and click with a plus signed mouse.
2. Provide the **Scheduler Name**..
3. Provide the **Status** as Enable to start scheduler.
4. Provide the **Scheduler date and time** to run the job.
5. Select **Target Monitor** from the list.
6. Provide the **Maintenance Time** along with date and time.
7. If you want to repeat the job daily/weekly/monthly, provide the schedule time for the operation to repeat daily/weekly/monthly.
8. Click **Create** to finish.

The systems will save Scheduled event and displays a confirmation message of the action.

12 Widgets for Custom Dashboard

Widgets are used to create Custom Dashboards and Reports. A dashboard widget is created with the following properties.

- **Component Type**
  The manner in which the information will be presented, chosen from a set of Build-in charts and graph types
- **Title**
  The descriptive title of the component
- **Time Span**
  The historical interval to graph data
- **Granularity**
  The data should be averaged out on hourly/daily/monthly basis or raw data should be shown.
- **Refresh Time**
  The interval at which the component will refresh the information it contains, ranging from 0 to 30 minutes.

12.1. Custom Dashboard

To create new custom dashboard:

1. Navigate to **Dashboards** > Click 

icon to add new dashboard.
2. Dashboard popover appears.
3. Give the **Title** for the dashboard.
4. If you want to keep dashboard accessible to others then choose public.
5. Select the Layout of the Dashboard. Provide description if needed.
6. Click 

icon toward top right corner to add widgets.

The systems will create the new Dashboard and displays a confirmation message of the action.

12.2. Widget Types

Basic reports included in the system are divided among:

- **Alarm Widgets**
- **Availability Widgets**
- **Health Widgets**
- **Performance Widgets**
- **SLA Widgets**
- **Snapshot Widgets**
- **Topology Widgets**
- **Trap Widgets**

- **Map Widgets**
- **Asset Widget**
- **NCM Widgets**

Note: Widgets are used to create custom dashboards and reports. By default all the users except the owner within department has read-only access to widgets.

The following sections provide brief descriptions of widget offered in these categories.

12.3. Adding Default Widgets

System has more than 700+ pre-built widgets to report performance data into custom dashboards.

To add custom Widget follow the steps given below:

1. Navigate to **Dashboards** > Click on + Widget at the top right corner of the dashboard page
2. Select type of widget to add, Widget type represents the type of data that will be presented.
3. Widget grid appears; choose the default widget to be added.
4. Click **Add**.

The systems will add the selected Widget into dashboard and displays a confirmation message of the action.

12.4. Alarm Widget

To create Alarm Widget follow the steps given below:

1. Navigate to **Dashboards** > Click on + Widget at the top right corner of the dashboard page > Alarm Widget.
2. Click **Add** towards top right corner; Select the data manner to represent the data.
3. Once added, navigate to widget in the dashboard.
4. Bind the data source by clicking **Widget Properties** > **Data Source**.
5. Click **Update** to add widget into the system.

The systems will add the new Widget properties and displays a confirmation message of the action.

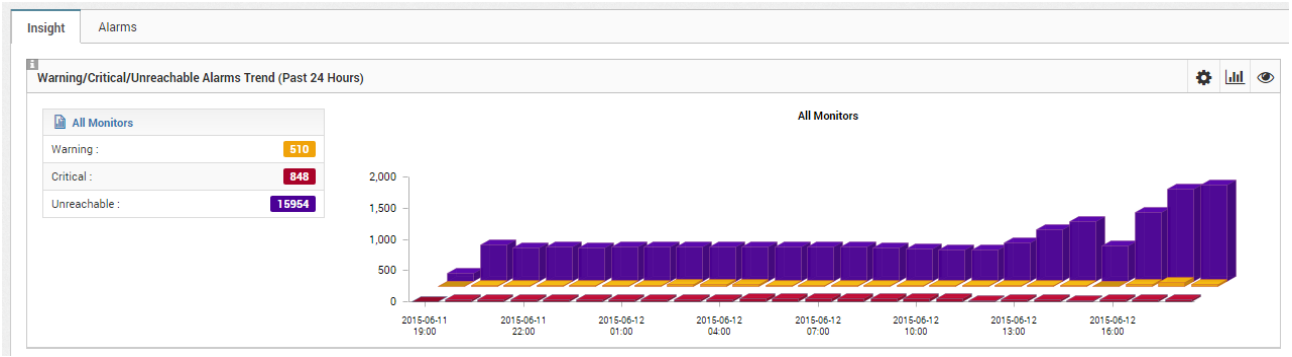


Figure Alarm Widget

12.5. Availability Widget

Availability Widget shows the percentage of time that a monitor or component is considered available. You can filter this report on device, component or monitor group. You also can further limit the time frame for the availability.

The value for a date range is calculated by summing the duration of all availability alarms of a particular monitor with a monitor state of "Enabled" and with a severity state as Clear. This sum is then divided by the duration of the time range and then subtracted from 1 and multiplied by 100 to get the percent available.

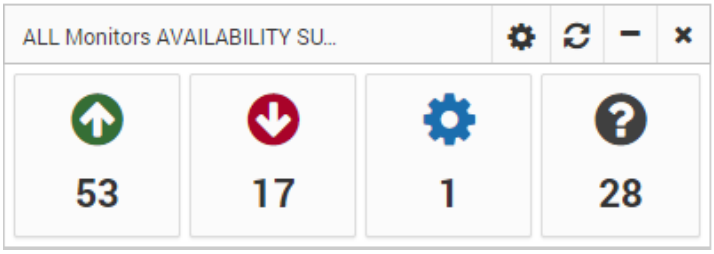


Figure Availability Widget, Widget type – Gauge

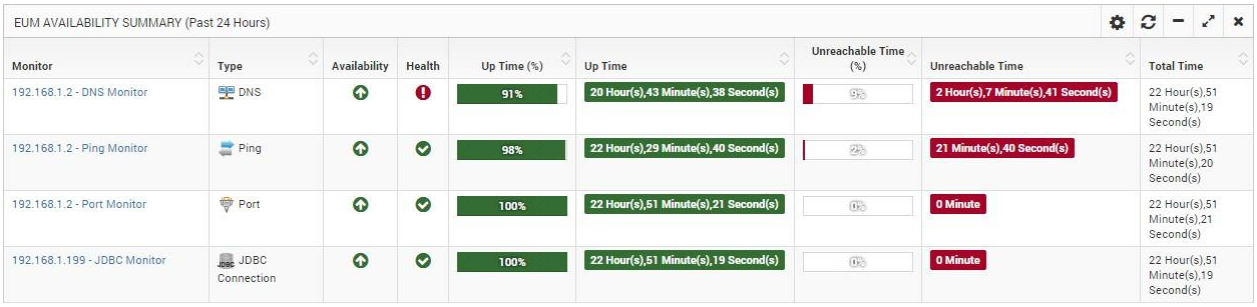


Figure Availability Widget, Widget type – Grid

To create Availability Widget follow the steps given below:

1. Navigate to **Dashboards** > Click on + Widget at the top right corner of the dashboard page and select Availability Widget.
2. Click **Add** towards top right corner; Select the data manner to represent the data.
3. Once added, navigate to **widget** in the dashboard.
4. Bind the data source by clicking **Widget properties** > **Data Source**.
5. Click **Update** to add widget into the system.

The systems will add the new Widget properties and displays a confirmation message of the action.

Note: Alarm events that occur only once are not used in calculating device availability when the associate policy has consecutive poll counts more than one. Specifically, events whose first-time and last-time severity state are the same are not used in the calculation. These could represent an event that

occurs and is subsequently cleared by the next event, or an event that has happened only once in the specified date range.

12.6. Health Widget

Health Widget shows the overall health of a monitor or component. You can filter this report on device, component or monitor group. You also can further limit the time frame with more options.

The health state for a date range is calculated by summing the severity state of all alarms of a particular monitor with a monitor state of "Enabled" and with a severity state as Clear/Warning/Critical.

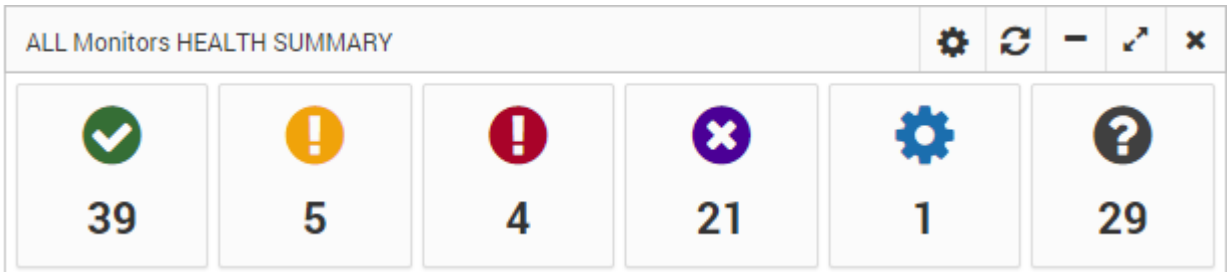


Figure Health Widget, Widget type – Gauge

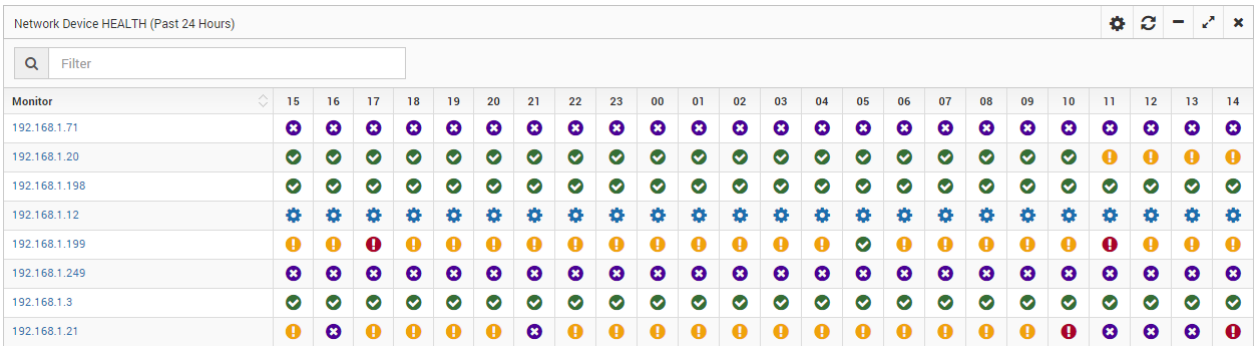


Figure Health Widget, Widget type – Histogram – Last 24 Hours

To create Health Widget follow the steps given below:

1. Navigate to **Dashboards** > Click on + Widget at the top right corner of the dashboard page > **Health Widget.**
2. Click **Add** towards top right corner; Select the data manner to represent the data.
3. Once added, navigate to widget in the dashboard.
4. Bind the data source by clicking **Widget properties > Data Source**
5. Click **Update** to add widget into the system.

The systems will add the new Widget properties and displays a confirmation message of the action.

12.7. Performance Widget

Performance Widget shows monitored interfaces, devices, server and application level performance attributes data. You can customize data manner and summary type (average or Top or Least etc.) to represent the data into widget.

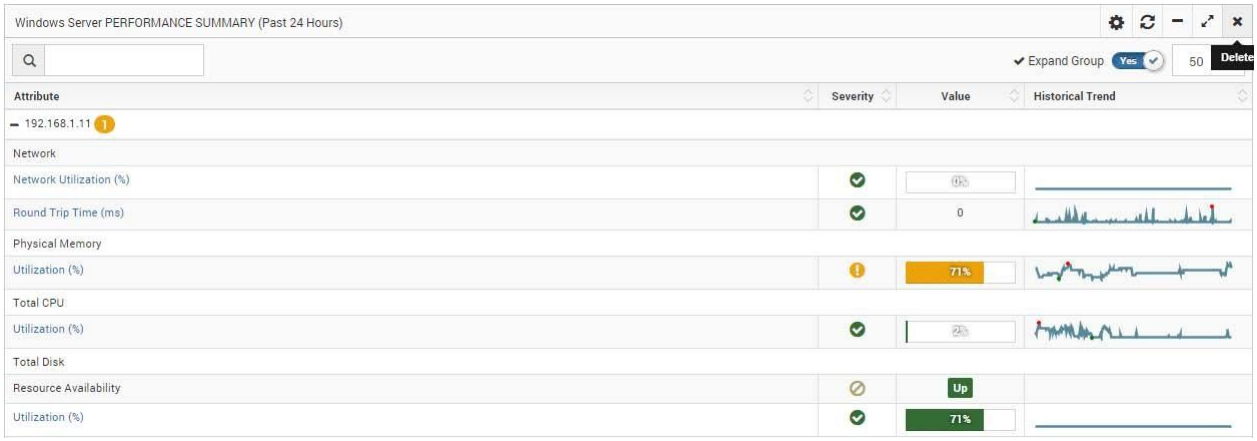


Figure 10.7.1 Performance Widget View Type – Grid

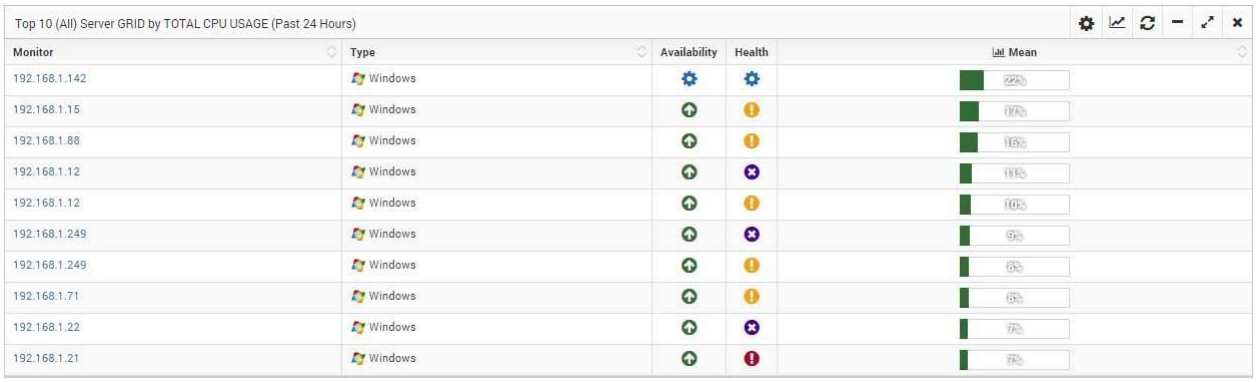


Figure Performance Widget, Widget type – Historical

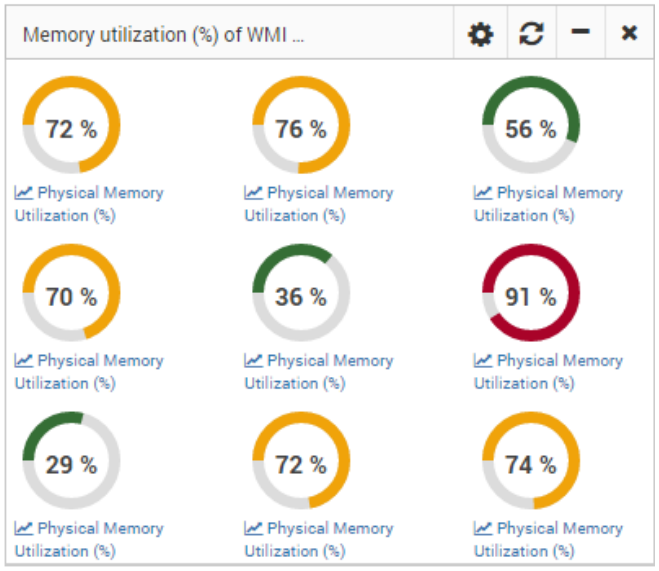


Figure Health Widget, Widget type – Gauge – Live

To create Performance Widget follow the steps given below:

1. Navigate to **Dashboards** > Click on + Widget at the top right corner of the dashboard page > Performance Widget.
2. Click **Add** towards top right corner; Select the data manner to represent the data.
3. Once added, navigate to **widget** in the dashboard.
4. Bind the data source by clicking **Widget properties** > **Data Source**.
5. Click **Update** to add widget into the system.

The systems will create the new Widget properties and displays a confirmation message of the action.

12.8. Map Widget

To create Map Widget follow the steps given below:

1. Navigate to **Dashboards** > Click on + Widget at the top right corner of the dashboard page > **Map Widget**.
2. Click **New** towards the top right corner of the dialog.
3. Select the **Map type** > **Google Map/ Network Map.**
4. Bind the data source by clicking **Widget properties** > **Data Source**.
5. Click **Update** to add widget into the system.

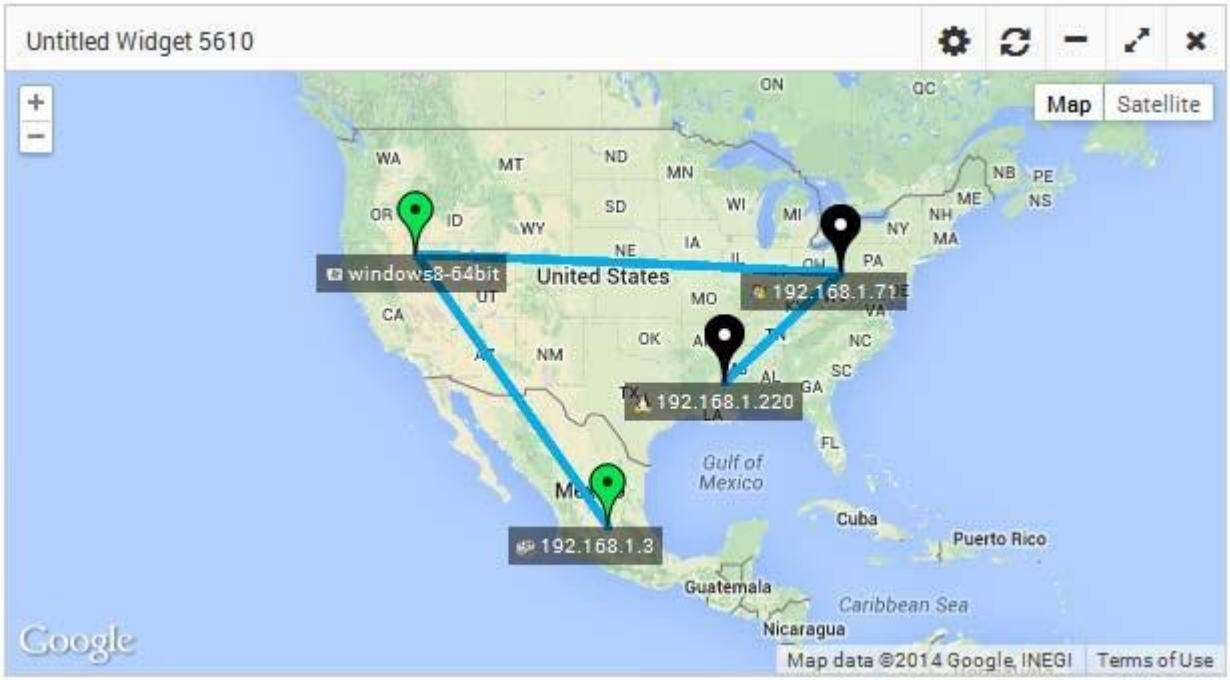


Figure Google Map Widget

The systems will create the new Widget properties and displays a confirmation message of the action.

Google Map API Key

To create Google Map Widget, Google Map API key is necessary. If API is not provided, error page will be displayed like below.

Follow the steps given below to get the API key:

1. Create your Google Map API key.
2. Go to https://developers.google.com/maps/documentation/javascript/tutorial.
3. Navigate to **Admin** > **Global Settings**.
4. Enter Google Map API Key.
5. Click on **Update**.
6. Finally bind the Data source.

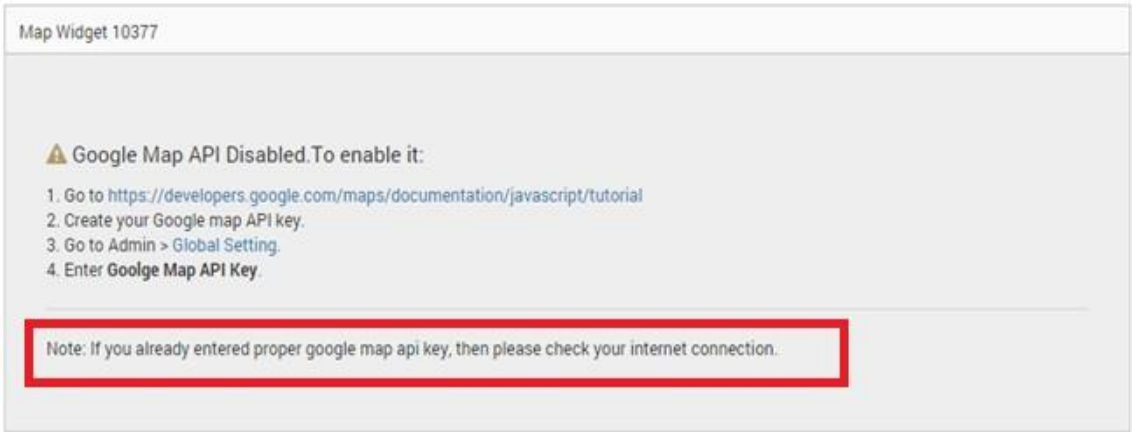


Figure Map widget error page

12.9. Asset Widget

Asset widget shows the asset overview, audit changes, software and hardware details. There are 4 types asset widgets available:

- Asset Overview
- Asset Audit Trail
- Software Usages
- Hardware Inventory

To create Asset Widget follow the steps given below:

1. Navigate to **Dashboards** > Click on + Widget at the top right corner of the dashboard page > **Asset Widget**.
2. Click **New** towards the top right corner of the dialog.
3. Select the **Asset type** > **Asset Overview/Asset Audit Trail/Software Usages/hardware Inventory.**
4. Bind the data source by clicking **Widget properties** > **Data Source**.
5. Click **Update** to add widget into the system.

The systems will create the new Widget properties and displays a confirmation message of the action.

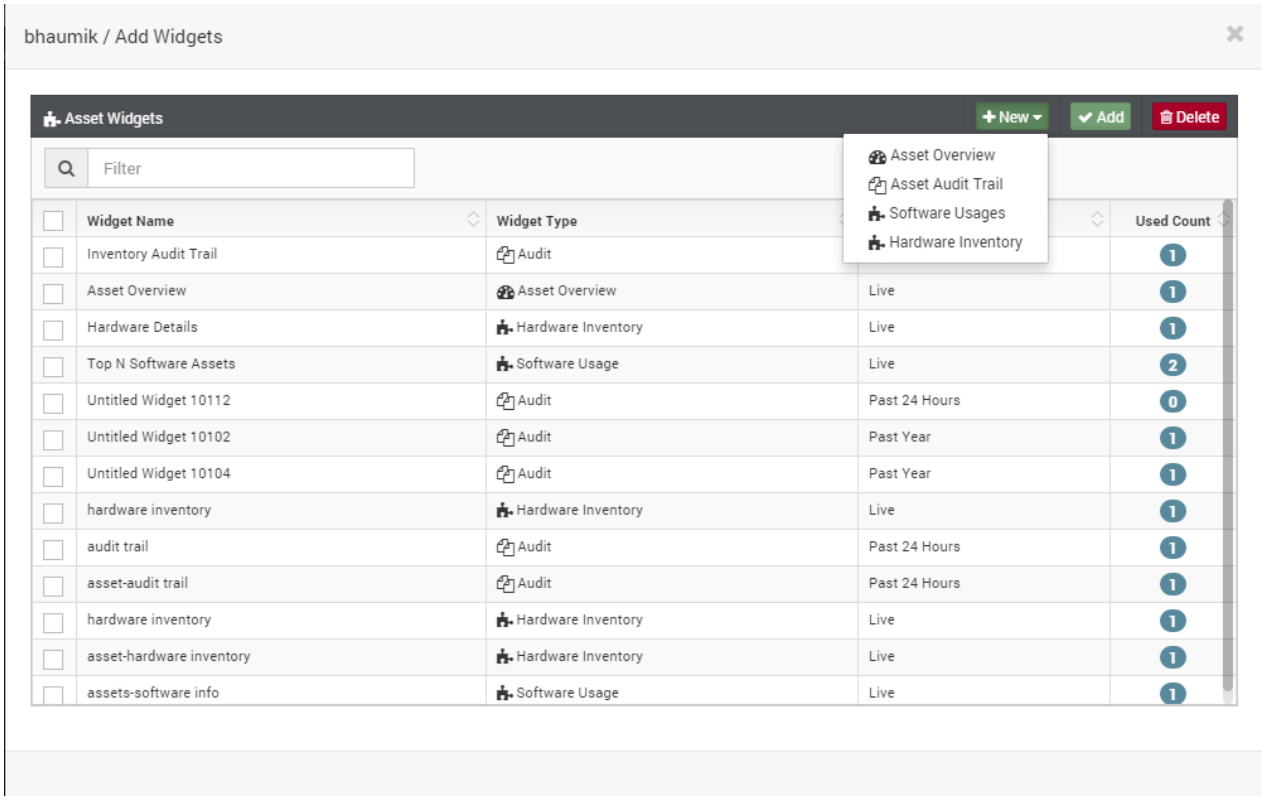


Figure Asset Widget

12.10. NCM Widgets

NCM widgets show the NCM overview and NCM audit log of the device. Two types of NCM widgets are available:

- **NCM Overview**
- **NCM Audit**

To create NCM widget, follow the steps given below:

1. Navigate to **Dashboard** > Click on + Widget at the top right corner of the dashboard page > NCM Widgets.
2. Click **Add** towards top right corner; Select **NCM Overview/NCM Audit** to represent the data.
3. Once added, navigate to widget in the dashboard.
4. Bind the data source by clicking **Widget Properties** > **Data Source**.
5. Click **Update** to add widget into the system.

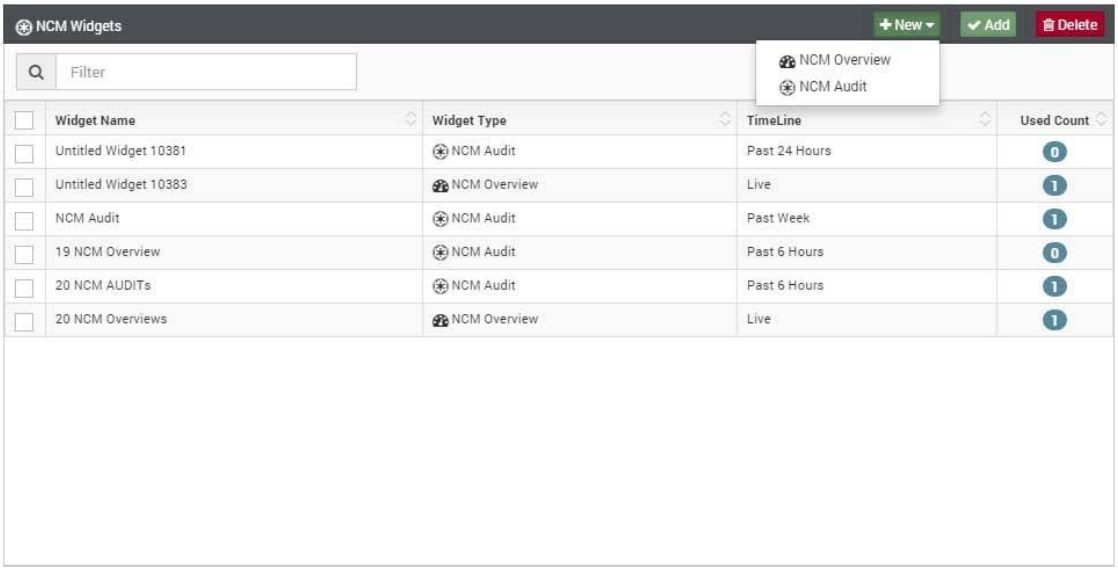


Figure: types of NCM widgets

Figure: NCM Audit widget

The system will add the new Widget properties and displays a confirmation message of the action.

13 Using Service Analytics

13.1. Business Service Monitoring

The Business Service basically creates a group of components to consolidate their KPIs and correlates all the layers of your IT infrastructure to your business service. Business Services lets you monitor infrastructure as a service - group of monitors that are running on your network. This capability provides you greater visibility into the monitor group and behaviors of its components and helps in detecting potential performance problems in network, server or application layer.

Note: To create a business service view, all service components' monitors must be created before and alarm must be configured on desired performance attributes.

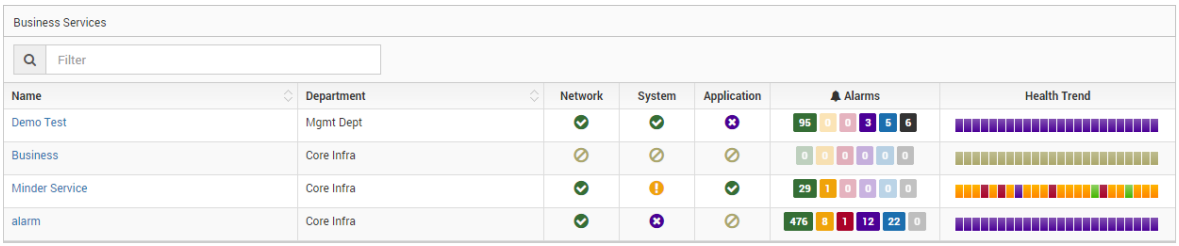


Figure.Business Services Grid

When you create a business service on your end-to-end components, system creates a logical, service- oriented group and start correlating their events as they occur. In addition to that, MindArray consolidates all the events based on infrastructure layers. When issue occurs you can easily pinpoint which layer is actually affected and what's the impact. Clicking on health icon shows the correlated event tree (RAC view) to identify the root-cause of the problem.

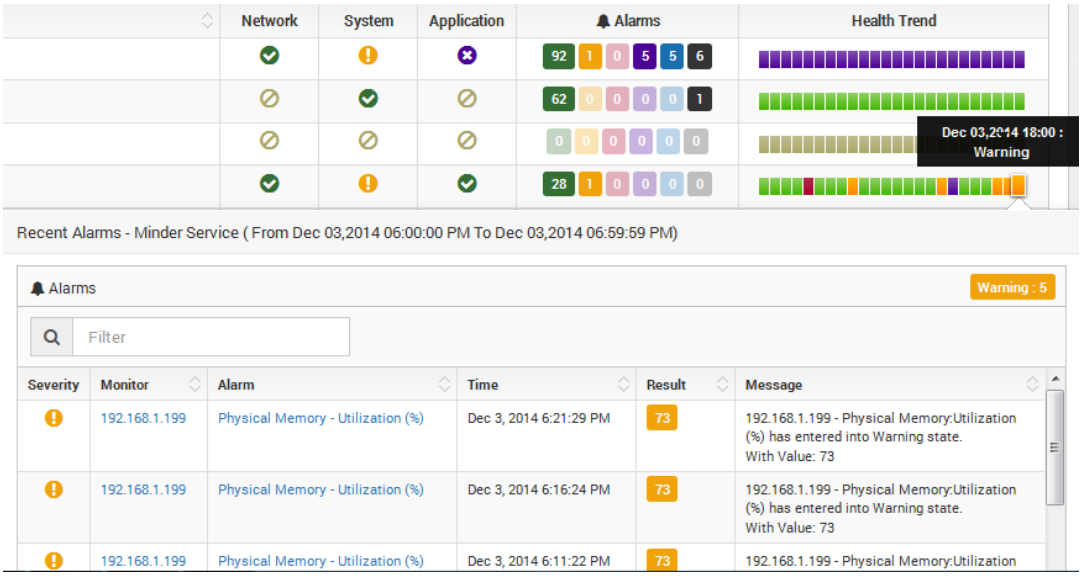


Figure Service Health Dill-Down

13.2. Adding Business Service

Follow the steps given below to create a new business service:

1. Navigate to **Business Services** > **Business Services** tab.
2. **Business Services** page appears. Click on **New** button on the top.
3. Provide **Name** and **Description**.
4. Select **Department** from the list.
5. Click **Create** to add new business service.
6. Once created, Click **Associate monitor icon** to assign monitor into Business Service.
7. Select **Monitor** from the list and click **Assign**.

The system adds Business Service and displays a confirmation message of the action. Navigate to **Business Services** > **Insight** > Click on **Business Service Name** to see drill-down page of the Service.

Note: You can also create nested business service views for more complex business service running in your emprise network. To do that, you should first create low level business service and then add the all the low business service into a new higher level business service.

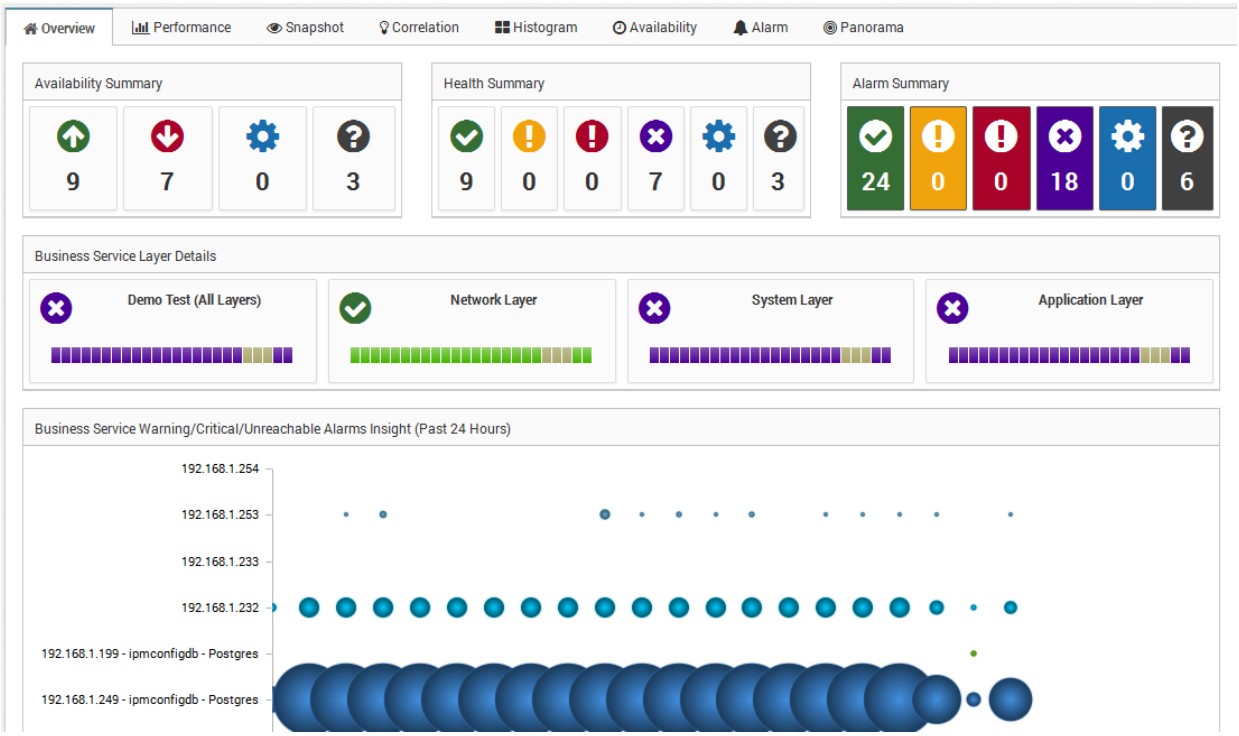


Figure: Business Service Overview

13.3. Adding/Removing Service KPIs - Key Performance Attribute(s)

By default all the attributes that has alarm configured are included into Service Key

Performance Indicator(s) list. If you can't find desired attribute from the containing monitors then navigate to actual monitor and configure an alarm on desired performance attribute.

Additionally, if you create SLA measurement on any business service, these Service Key Performance attributes are included to calculate SLA. For more information on SLA View see section 12.

To add new performance attribute into list, follow the below steps:

1. Navigate to **Business Services** > **Business Services** tab.
2. Click **Business Service Attributes icon** of Business Service, **Service attributes** dialog appears.
3. Select the **Performance Attributes** to add into business service.
   Note: Configure alarm on performance attributes to include attribute that are not listed for any monitor.
4. Click **Update** to apply changes.

The system updates new Performance Attribute(s) and displays a confirmation message of the action.

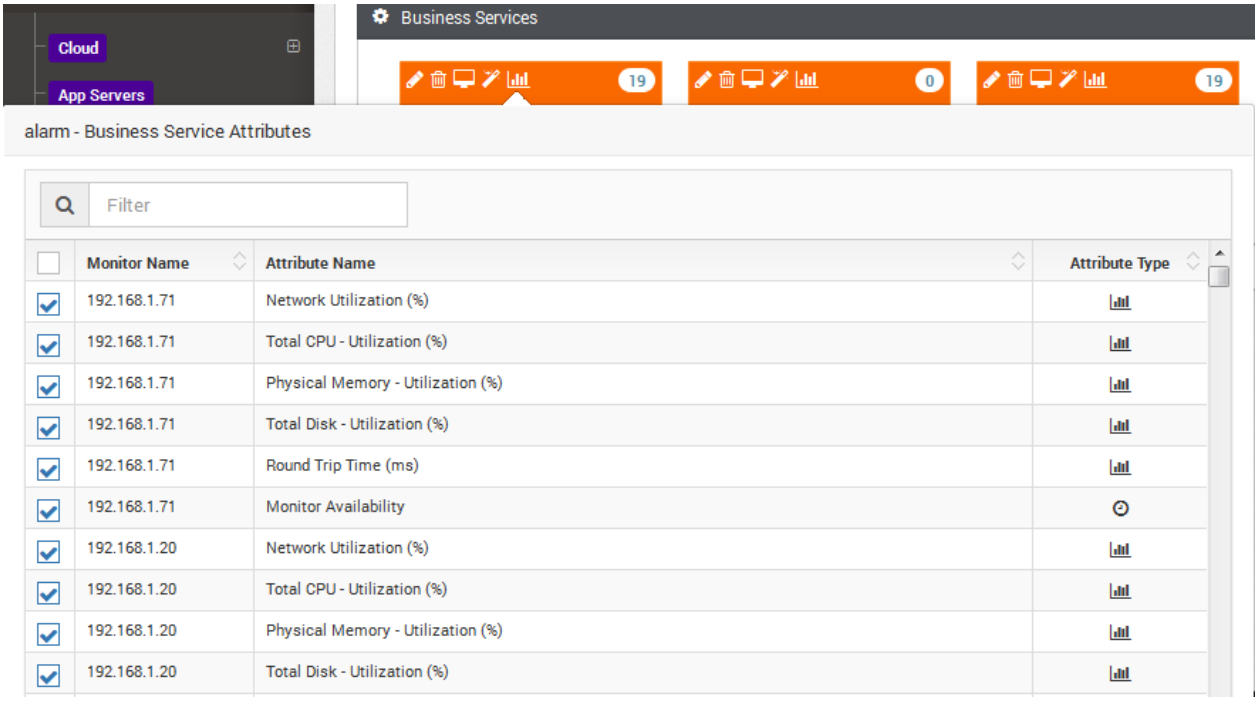


Figure. Adding Business Service Attributes

13.4. Adding Nested Business Services

You can add a low level service into existing business service to track more complex and nested business service. This enables you to create a Master Business Service View with multiple services. You can add N number of services into a Business Service.

Additionally, you can create SLA on Business Service that contains multiple Business Services. When you create a SLA on such business service, System also includes their Service Key Performance Attributes (s) to measure SLA.

Note: To create a nested business service, all service components' monitors must be created before and alarm must be configured on desired performance attributes.

To create a new nested business service, follow these steps:

1. Navigate to **Business Services** > **Business Services** tab.
2. **Business Services** page appears. Click on **New** button on the top.
3. Provide **Name** and **Description**.
4. Select **Department** from the list.
5. Click **Create** to add new business service.
6. Once created, Click Associate monitor icon and select the existing business service and monitors.
7. Click **Assign**.

The system adds new nested Business Service and displays a confirmation message of the action. Navigate to Insight > Business Service Grid to see service drill-down page.

14 Business SLA Manager

Minder has a very flexible SLA Manager for tracking compliance against user-defined Service Level Agreement attributes. These SLA attributes are calculated and displayed on a real-time dashboard. You can configure SLAs for any attributes being monitored in MINDER and specify the following:

- An SLA time period during which the compliance is measured (day, week, or month).
- The SLA threshold specified as a percentage of the time period during which the SLA attributes must be "normal."

If the SLA attributes is in a critical condition for a time period that exceeds this time threshold, then it will be considered a violation of the SLA for that time interval. As an example, you can set up an Service Level Agreement to monitor all the components of an e-commerce service (Web application, network, database) and specify that the SLA requirement is a maximum downtime of 5 minutes each day.

Note: To create SLA measurement on Business Service (Logical Monitor Group), you must create a Business Service before. You can add/remove SLA attributes to calculate SLA in actual Business Service.

14.1. SLA Attributes

These are composite values consisting of one or more device performance attributes and if any of these attributes are in critical state, then the SLA metric is considered to be critical and contributes towards the SLA violation aggregate time.

Each composite SLA attribute can have its own time interval and independent SLA threshold time. You can have an unlimited number of SLA attributes defined in the system. The SLA dashboard displays the amount of time that the attribute is within the SLA threshold and also displays how close the attribute is to violating the SLA requirement.

The underlying device attributes can be assigned to multiple SLA attributes to match complex SLA compliance requirements. As an example, if you want an SLA which stipulates that the database response time will be less than 2 seconds for 95% of the time each day and also that it cannot be slow for more than 3% of the business hours in a 5 day week, you can create two separate SLA and set up different SLA measurements for each of these to meet your requirements..

14.2. Working with Business SLA

To configure Business SLA navigate to Business SLA, displays a list of all the department's configured SLA measurements. Each row contains the SLA measurement name and description. Additionally, there are links for updating each SLA measurement's properties such as assigning/updating attributes, or deleting the measurement.

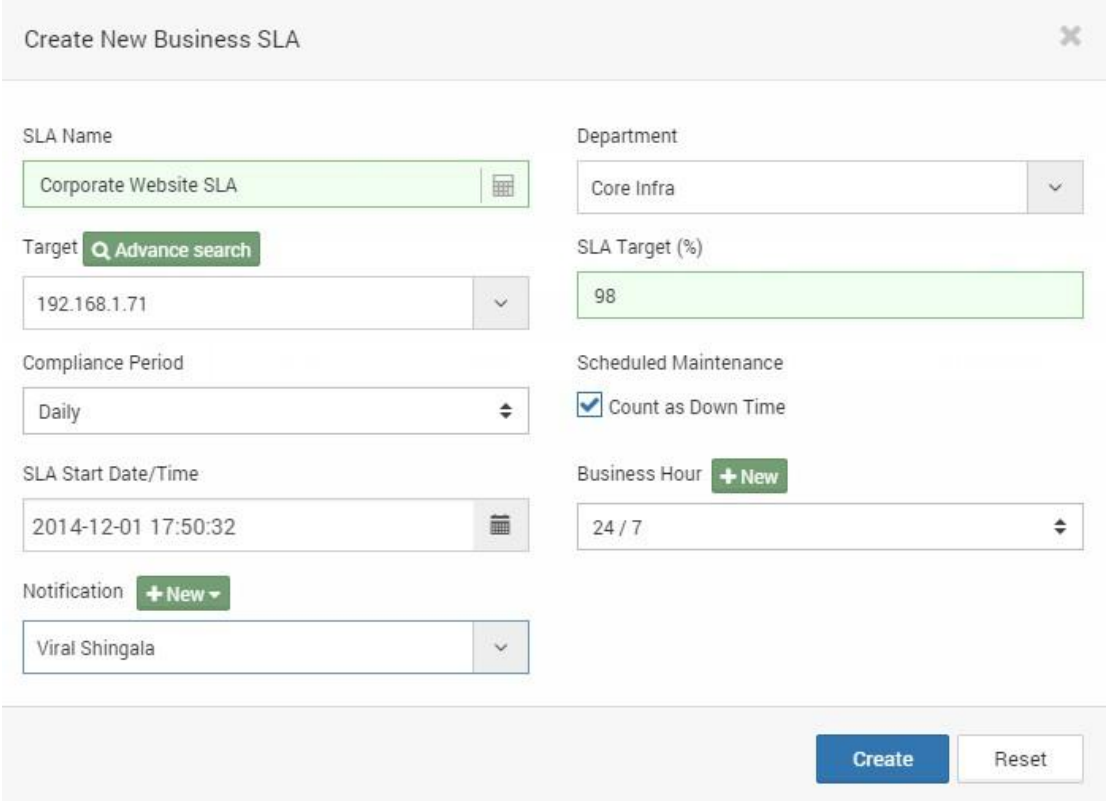


Figure Create Business SLA

To create a new SLA Measurement, follow the below steps:

1. Navigate to **Business SLA** > **Business SLA list** page appears.
2. Click on **New** button on the top.
3. Provide **Name** for Business SLA.
4. Select **Target Monitor** from the dropdown to associate**.**
   Note: To create SLA measurement on Business Service or Group of monitor, you must create a Business Service before. You can add/remove SLA attributes to calculate SLA in actual Business Service.
5. Provide the percentage of the calculation period that the attribute must be in the OK state.
6. Provide **Compliance Period**.
7. Select whether you want to calculate maintenance time of the monitors as down time or ignore it during SLA measurement.
8. Select **Monitoring Period** from the dropdown.
   Note: SLA measurement will run for provided hours only.
9. Select the **Business Hours** for action to execute.
10. Select **Email Alert** profile to get notified about action result.
11. Click **Create**.

The system adds new Business SLA and displays a confirmation message of the action.

Note: Modify Business Service to make any further changes to monitors and performance attributes to include them for SLA Measurement.

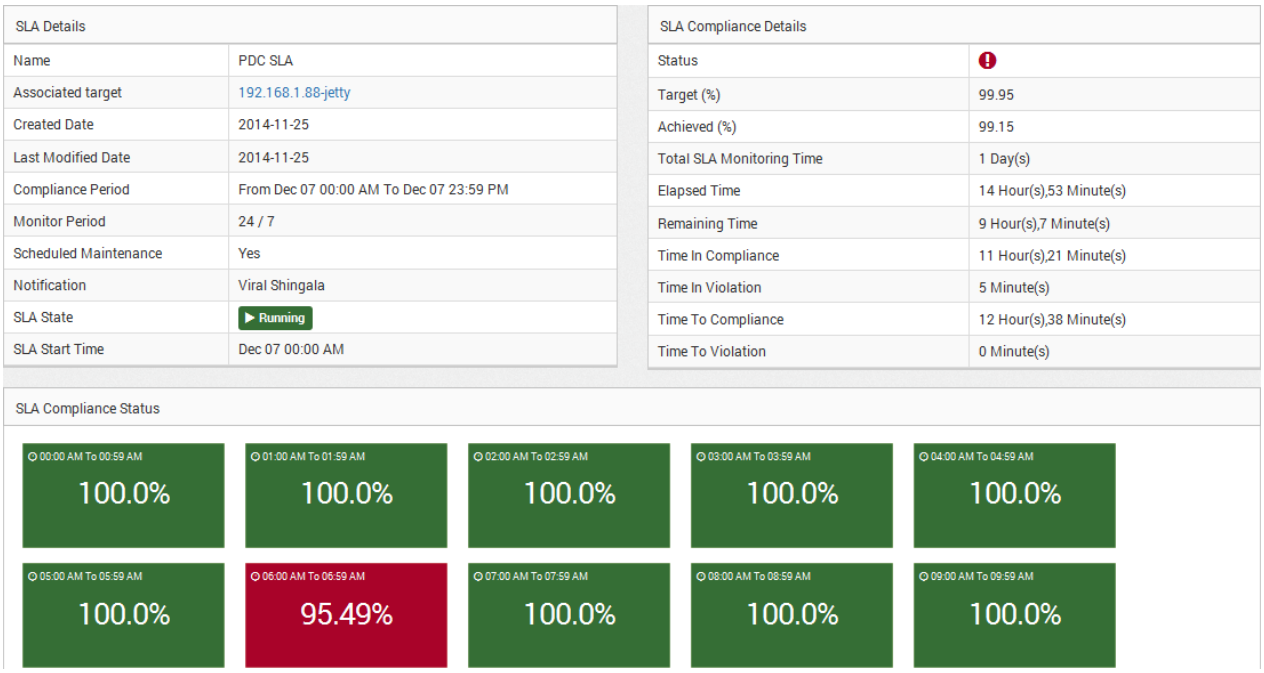


Figure SLA Drill-Down Page

14.3. Modifying Business SLA

To modify SLA View properties:

12. Navigate to **Business SLA** > Click **Edit** button of Business SLA.
13. You can edit SLA View Name, Target Percentage, Compliance Period, Scheduled Maintenance, Monitoring Period, Business Hour and Notification recipients.
14. Click **Update** to apply changes.

The system makes changes to Business SLA and displays a confirmation message of the action.

Note: Changing compliance period, Scheduled Maintenance, Target Percentage will reset the SLA and SLA Measurement will start from newly updated properties. Pervious data of existing Business SLA will also be removed.

14.4. Adding/Removing Performance Attributes from Business SLA

Note: For Business SLA, All performance attributes listed in Business Service > Business

Service attributes(s), are included to measure SLA.

For Monitor Level SLA, by default all the attributes that has alarm configured are included to measure the SLA. If you wish to remove a particular attribute from SLA measurement, you need to disable/delete alarm form that attribute in containing Monitor.

15 Reports

The report panel contains the following set of reports generation options. You can generate the desired type of report based on your requirement.

1. **Pre-Defined Report.**
2. **Custom Report.**

The report template contains the following values.

Search: area to search for Reports.
Favorite: Allows you to add favorite tag to the report.
Edit: Edit the existing report.
Add: To create a report.
Delete: To delete the report from the list.

Let's get started with how to generate above stated reports.

15.1. Predefined Reports

Minder has extensive and flexible reporting at various levels (server, device, performance attributes and business service) as well as of different types (fault, performance, SLA). Most reports are generated in real time by collecting data from the Data-store and then creating the graphs and statistics from the raw data by the reporting engine.

The following historical reports are immediately available with your Minder installation. You can modify reports to suit your Monitoring report requirements. To customize or add a report, you can add widget component into it. For example you can add a historical chart widget and a historical grid widget of same components.

The list of pre-defined reports is as follows:

- Application Reports.
- Cloud Monitor Report.
- Database Report.
- End User Monitor Report.
- File/Directory Monitor.
- Middleware Report.
- Network Device Report.
- Platform Report.
- Server Report.
- Virtualization Report.
- Virtual Machine Report.
- Web Server Report.
- My Favorite

The following sample reports are predefined for reporting current data on your monitored servers and applications.

Current Application and Component Status

- Average Response Time of each Component
- Current CPU Load of each Component
- Current Memory Utilization of each Component
- Current Status of each Application
- Current Status of each Component

Daily Application Availability

- Application Availability – Last Month
- Application Availability – This Month
- Application Availability – This Year

Historical Application CPU and Memory Reports:

- CPU Load for each Application Monitor – Last Month
- CPU Load for each Application Monitor – This Month
- CPU Load for each Application Monitor – This Year
- Memory Load for each Application Monitor – Last Month
- Memory Load for each Application Monitor – This Month
- Memory Load for each Application Monitor – This Year

Historical Reports

- Page File Usage – Last 7 Days
- Page File Usage – Last Month
- Page File Usage – This Month

15.2. Quick Report

The quick reports are available for viewing current and historical data on all monitored components. Minder aggregates and reports, over time, on the data you set it up to monitor. The system provides a range of defined and custom report options in quick reports.

Viewing Quick Reports in the Minder Web Console:

1. Navigate to **Monitor Page/Dashboard.**
2. Click on quick report icon towards top of the widget bar.
3. To change the time range click on 7 & 30 icon on the top right corner.

Note: It is also possible to charge a report chart, guaranty within a web console view. Click on Action menu towards top right corner of the report page.

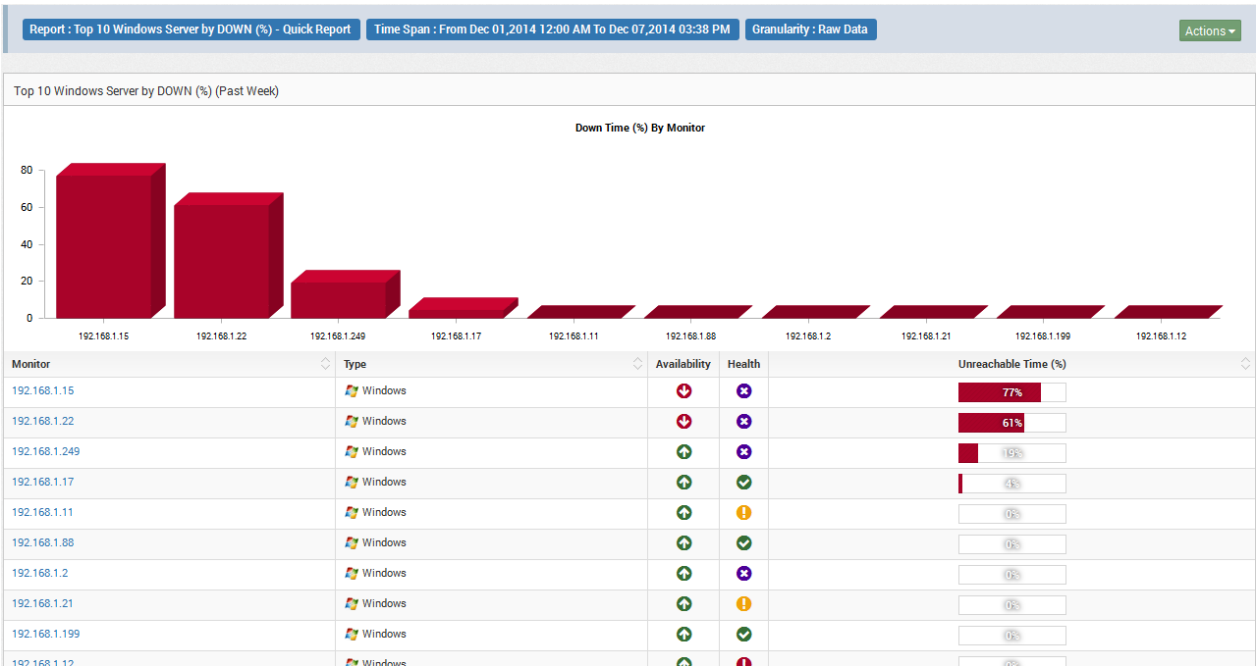


Figure Quick Reports – Top 10 Windows Server by Down Time

15.3. Customizing Default Report

Report generation options are dynamic, all reports includes default widgets. Customizing the default widget require that you select the data to include and decide how that data will be sorted, ordered, filtered and presented. Based upon the type of widget, include widget properties and widget data presentation.

Each report offers different configuration options, so, depending on the report, you can add or remove widgets.

Viewing Quick Reports in the Minder Web Console:

1. Navigate to **Report** > Select Report Category.
2. Select the report, Report drill-down page appears.
3. Click widget properties. Select the options to customize the report – such as Chart type, Time span, Granularity etc.
4. **Update** the widget.

The system updates the widget properties and displays confirmation message of the action.

15.4. Adding Custom Report

In the context of multi-graph reports, report properties are very similar to those in custom dashboard templates. Settings on the widget definition define basic parameters; graph points are added to specify which data should be drawn on report. For more information on creating Widget, see the chapter titled Widgets under Admin Panel.

For Example: To create a report which represents Page File Usage of Process, You must create a widget under performance category that provides this data. When adding performance widget to report, you can select from a list of pre-defined widget and custom widget that are created by admin user.

To generate a new Report, follow steps listed below:

1. Navigate to **Reports** > **Custom Reports.**
2. Click **New**, **Custom Report** dialog appears.
3. Provide **Name** and **Description** for report.
   Click **New** to add more widget. You can select from a list of pre-defined widget and custom widget that are created by users.
   Note: If required data widget is not available, you can add new by click on +New button in the same page. In case of new custom widget – choose the data manner to represent the data.

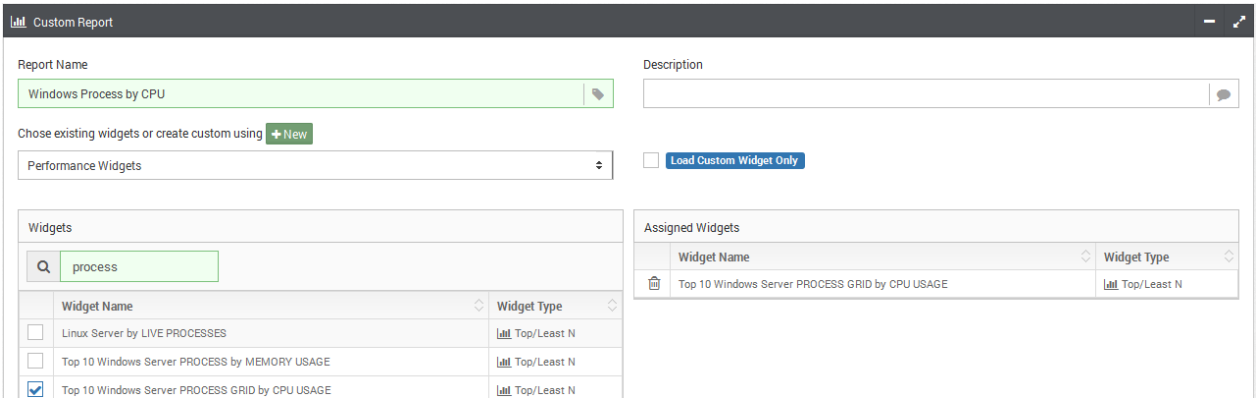


Figure Custom Windows Process Report using default widgets

4. Assign Monitor/Attributes to widget by click in Add button.
5. Create the Report.
6. Report is now listed in Grid. Click on Report Name link to generate report.

The system adds the new Report properties and displays confirmation message of the action.

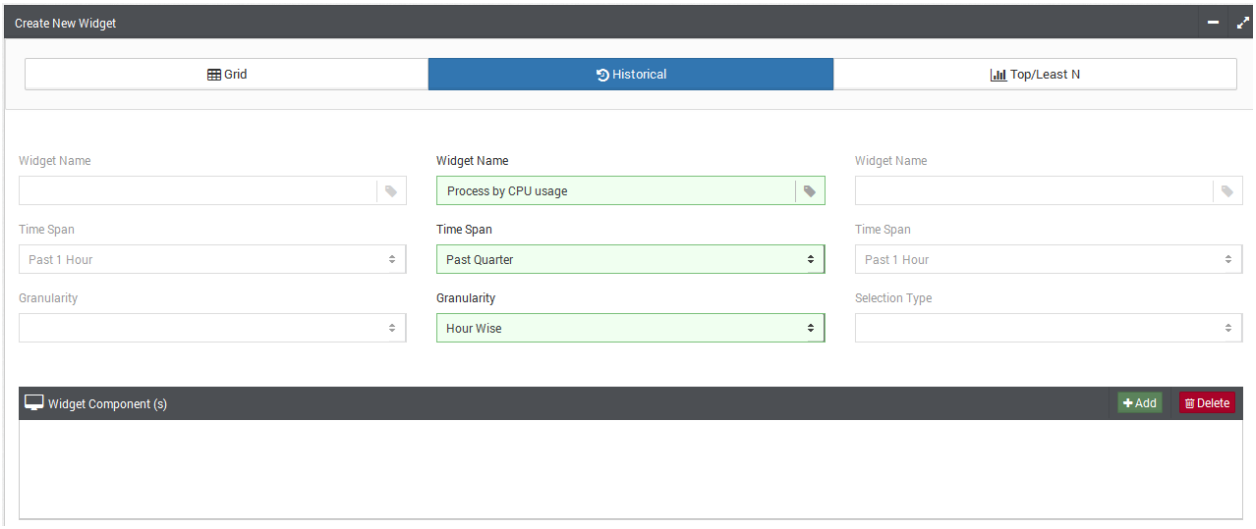


Figure 13.4.2 Creating Custom Data Widget for Windows Process

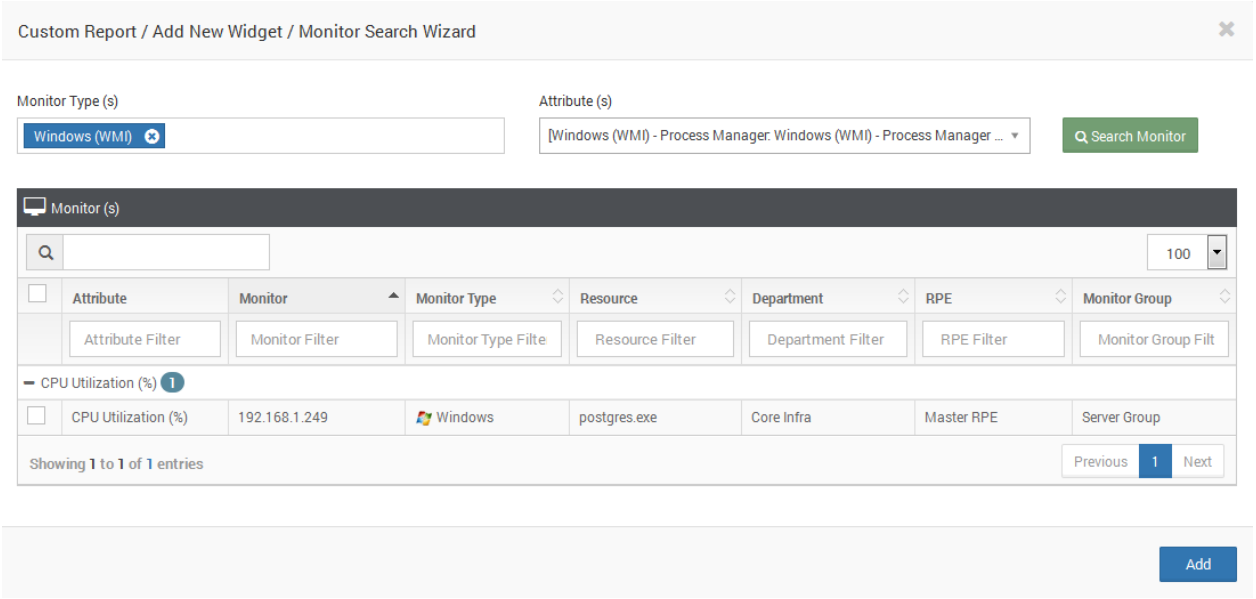


Figure Assign Monitor/Attributes to Data Widgets

15.5. Exporting Report

The following steps required to export an open report from Minder. You can export reports as PDF/EXCEL format and email report to specified email address.

To export report from Minder Web Console:

1. Navigate to **Report**.
2. Click on **PDF/Excel** icons under actions at the top of the page.
3. Use Scheduler action to schedule the report to send to any recipient automatically.

The system exports the Report and displays confirmation message of the action.

15.6. Scheduling Report

The following steps required to schedule an existing report from Minder. You can export reports as PDF format and email PDF version to specified email address.

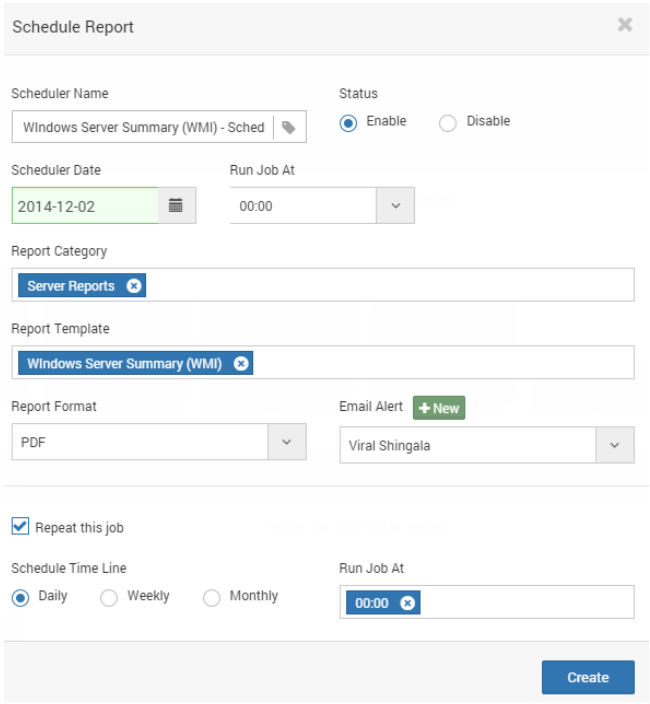


Figure Schedule Report Job

To schedule the Report Job follow the steps given below:

1. Navigate to Scheduler > Drag and drop Report job from the top on calendar.
2. Report Job dialog appears, Provide the Scheduler Name.
3. Provide the Scheduler date and time to run the job.
4. Select the report category you want to send from the various reports listed.
5. Select the report template name.
6. Select the type of the report you want, either in PDF format or CSV format.
7. Select the email notification action for the operation. Report
8. Provide the schedule time for the operation to repeat daily.
9. If selected schedule time is weekly, provide the day of week and schedule time to run the job.
10. If selected schedule time is monthly, provide the day, month and schedule time to run the job.
11. Click Update to finish.

The systems creates Scheduled event and displays a confirmation message of the action.

16 Ticketing

Ticketing feature allows you to assign and escalate ticket of a specific fault scenario to an appropriate technician and also helps to keep the track of the service requests and complaints.

Minder allows you to create two kinds of tickets:

1. Alarm Ticket
2. Help Desk Ticket

Note: All the users will be able to see the created tickets, but only the assignee and the reporter of a ticket will be able to edit the status of that particular ticket.

16.1. Creating Alarm Ticket

16.1.1. From Ticket tab

Follow the steps given below to create alarm tickets from ticket tab:

1. Navigate to **Tickets** > **New** > **Alarm Ticket.**
2. **Create new Ticket** pop up appears.
3. Provide an appropriate **Subject** name for the ticket.
4. Select the **Priority** of your ticket from the list.
5. Select an **Assignee** from the list (technician you want to assign the ticket).
6. Select the name of the **Monitor** and **Alarm** for which you want to create a ticket.
7. Select the required **Status** for the ticket.
8. Provide the **Due Date** to the assignee for the ticket to get resolved.
9. Provide the **Escalation** Profile as per your needs.
10. If the **Email Notification** box is checked then the reporter as well as the assignee will be notified about the status of the ticket.
11. Provide a **Description** if needed.
12. Click on **Create**.

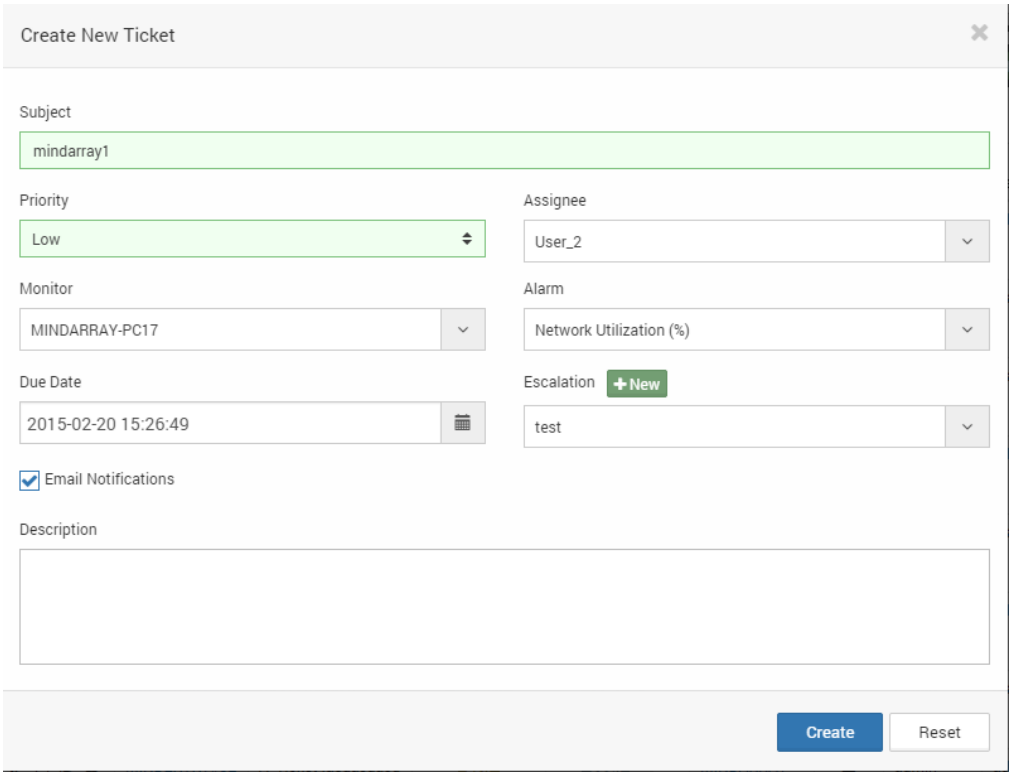


Figure Alarm Ticket

16.1.2. From Alarms

Follow the steps given below to create a ticket using alarms:

1. Navigate to **Alarms** > **Alarms** tab.
2. Click on **Create ticket icon** of the alarm you want to create the ticket for. Create new ticket pop-up appears.
3. Provide an appropriate **Subject** name for the ticket.
4. Select the **Priority** of the ticket from the list.
5. Select an **Assignee** from the list (technician you want to assign the ticket to).
6. Select the **Monitor** and **Alarm** for which you want to create the ticket.
7. Select the required **Status** for the ticket.
8. Provide a **Due date** for the ticket to get resolved.
9. Provide an **Escalation profile** as per your needs.
10. If the **Email notification** box is checked, the reporter and the assignee will get be notified about the status of the ticket.
11. Provide a **Description** if needed.
12. Click on **Create**.

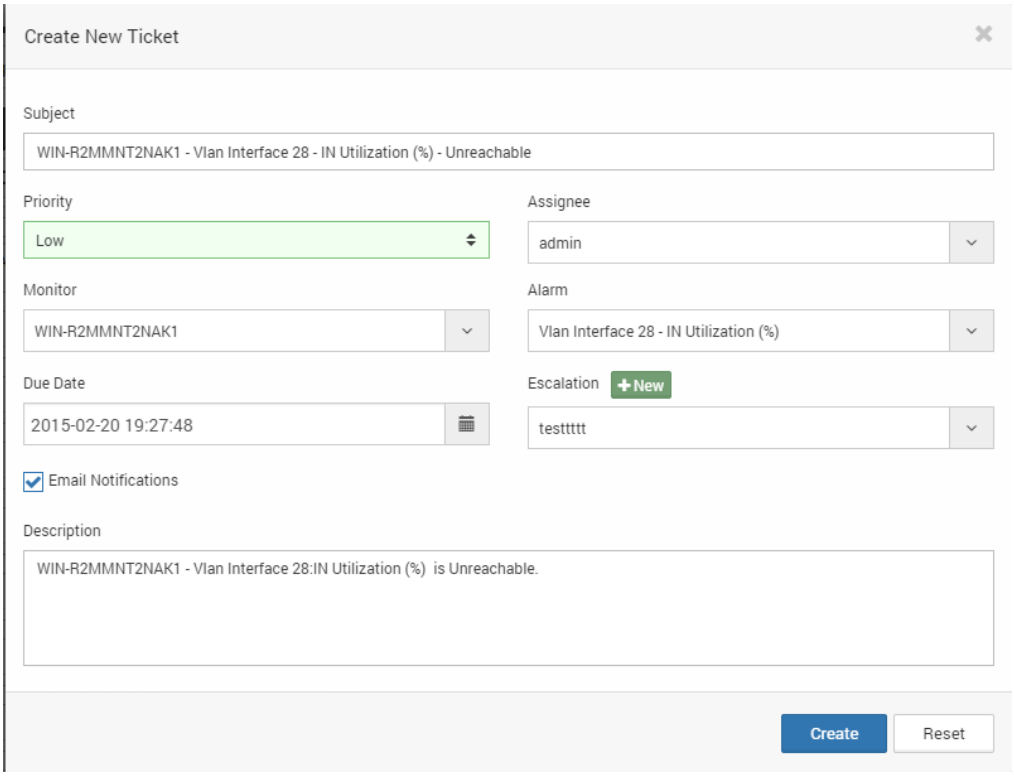


Figure Alarm Ticket

16.2. Creating a Help Desk Ticket

When a fault is detected in assets, user can create a help desk ticket.

16.2.1. From Tickets tab

Follow the steps given below to create a help desk ticket:

1. Navigate to **Tickets** > **New** > **Help desk ticket**.
2. **Create new ticket** pop up appears.
3. Provide an appropriate **Subject** name for the ticket.
4. Select the **Priority** of the ticket from the drop down menu.
5. Select an **Assignee** from the drop down menu (technician you want to assign the ticket to).
6. Select an **Asset** from the drop down list.
7. Select the required **Status** for the ticket.
8. Provide a **Due date** for the ticket to get resolved.
9. Provide an **Escalation** profile as per your needs.
10. If the **Email Notification** box is checked, the reporter and the assignee will get be notified about the status of the ticket.
11. Provide a **Description** if needed.
12. Click on **Create**.

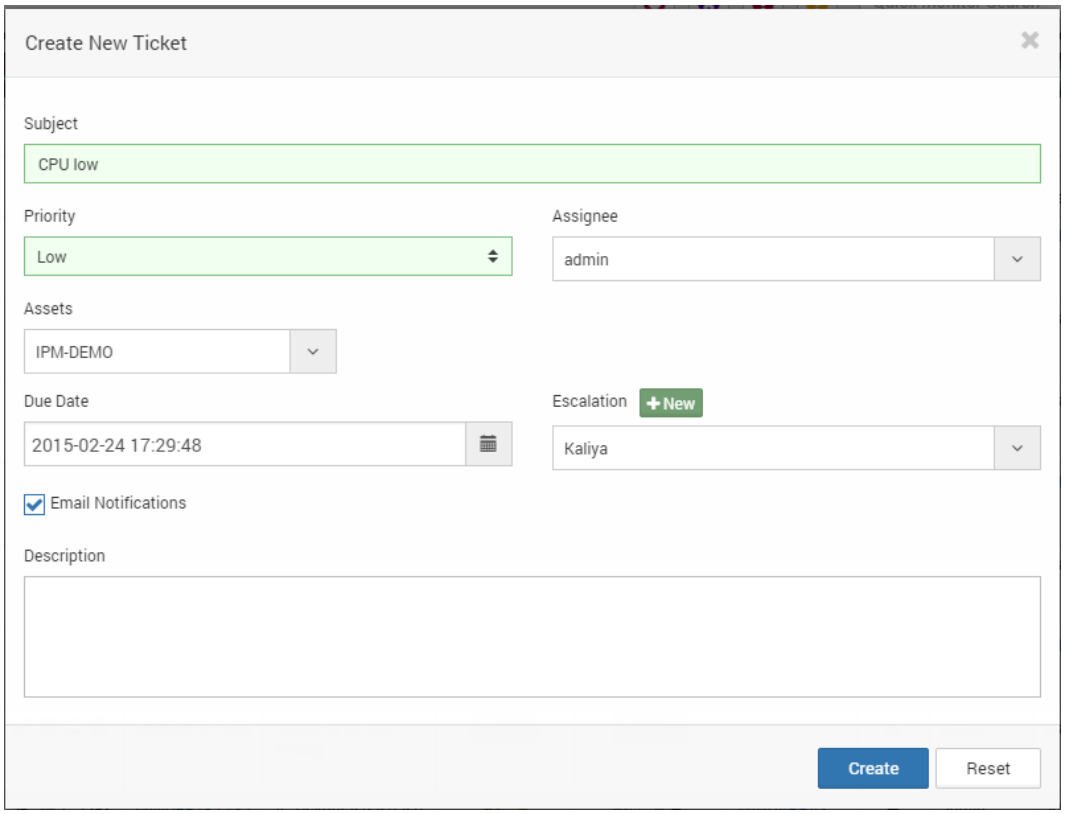


Figure Help Desk Ticket

16.2.2. Creating a Help Desk Ticket by an End User

When users in help desk group of the active directory will log into the Minder, they will only be able to see the help desk ticket page.

Help desk users should follow the steps given below to create a help desk ticket:

1. Log in with the appropriate username and password.
2. **Help desk ticket** page will be displayed.
3. Navigate to **New** > **Help Desk Ticket.**
4. Provide the **Subject** and appropriate **Description**.

Note: The created ticket will be assigned to the pre-configured default assignee.

16.3. Configuring Default Assignee for Help Desk Tickets

When an end user will create a help desk ticket, the ticket will directly be assigned to the user that has been configured here.

Follow the steps given below to assign help desk ticket to default user:

1. Navigate to **Admin** > **Global Settings** > **Ticket Settings**.
2. Select the **Default Assignee**.
3. Click on **Update**.

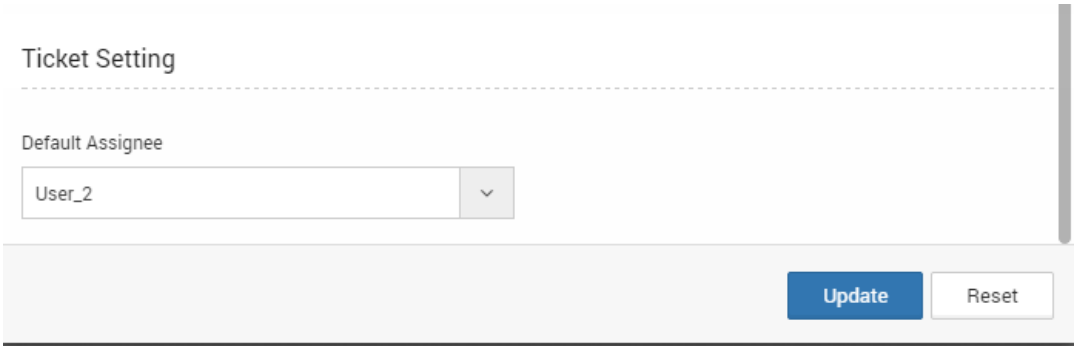


Figure: Configuring Default Assignee

Note: Only admin can change the Default Assignee**.**

16.4. Ticket Escalation

You can provide an escalation profile for when an assignee crosses the due date by which the ticket has to be resolved.

In **Create New Ticket** dialog, you can select escalation profile from the list or you can create a new one. To create a new escalation profile, follow the steps given below:

1. Click on **New** button, **Escalation Profile** dialog appears.
2. Provide the Escalation Steps – By clicking on **Add** button.
3. Provide the **Alert name** and **Escalation Time (in minutes)** to wait until executing the email alert. Click on Add.
4. Repeat the same to add an email alert for Second step. The second email alert will execute in the given time after the first alert has already been executed
5. Click on **Create**.

16.5. Ticket Action

You can create a ticket action which you can assign to a performance policy, in which case every time that policy is violated, the ticket will be generated and assigned automatically to the assignee you selected while creating the ticket action.

Follow the steps given below to create a ticket action:

1. Navigate to **Policies & Alerts** > **Action Profiles** > **New** >**Ticket**.
2. Provide an **Action Name**.
3. Select **Priority** for the ticket from the drop down list.
4. Select the **Assignee**.
5. Provide **Escalation** profile from the list or create a new one.
6. Provide the **Business Hour**.

7. Click on **Create**.

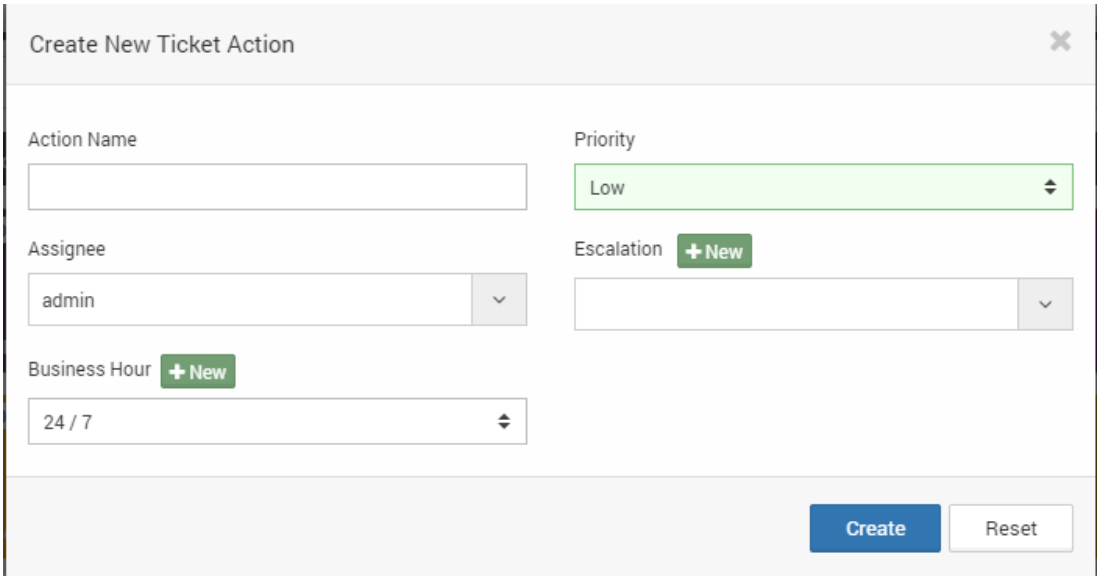


Figure Ticket Action

17 User and Department (Security)

Minder users and departments are permission-based entities that comprise the Minder security model. The multi-tiered administrative hierarchy allows enterprises and service providers to provide each group within the organization or service model the access it needs and no more.

The following are the default roles groups configured with different privileges:

- **Super Admin** - Global access and privileges to all the departments and systems. Super Administrators are members of the Super Admin Role Group.
- **Department Admin** – Regional Admin has access to Specific department and their child departments with full admin privileges. Administrators are members of Department Admin Role, which is associated with department.
- **End User** – End user role users has access to reports on overall system performance and system usage. End users are members of department.

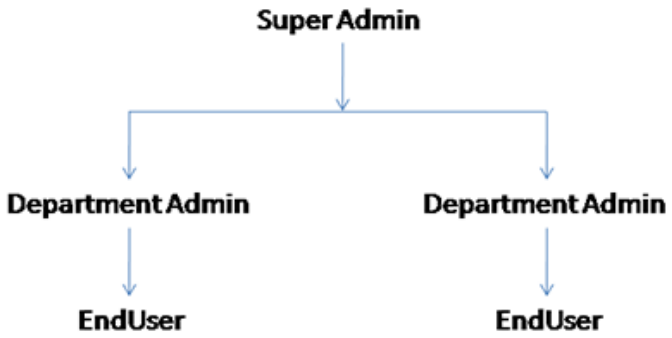
17.1. User and Department Permission

Each department is associated with a single Role Group, which determines what privileges members of the department have. Privileges control which tasks an end user can perform with respect to various Minder properties.

The following are the default roles groups configured with different privileges:

- **Super Admin** - Global access and privileges to all the departments and systems. Super Administrators are members of the Super Admin Role Group.
- **Department Admin** – Regional Admin has access to Specific department and their child departments with full admin privileges. Administrators are members of Department Admin Role, which is associated with department.
- **End User** – End user role users has access to reports on overall system performance and system usage. End users are members of department.

User Hierarchy Diagram



17.2. Working with Departments

Departments can reflect divisions within the company (e.g., Sales, Engineering), locations (e.g., New York), or other meaningful categories. Departments can have multiple child departments.

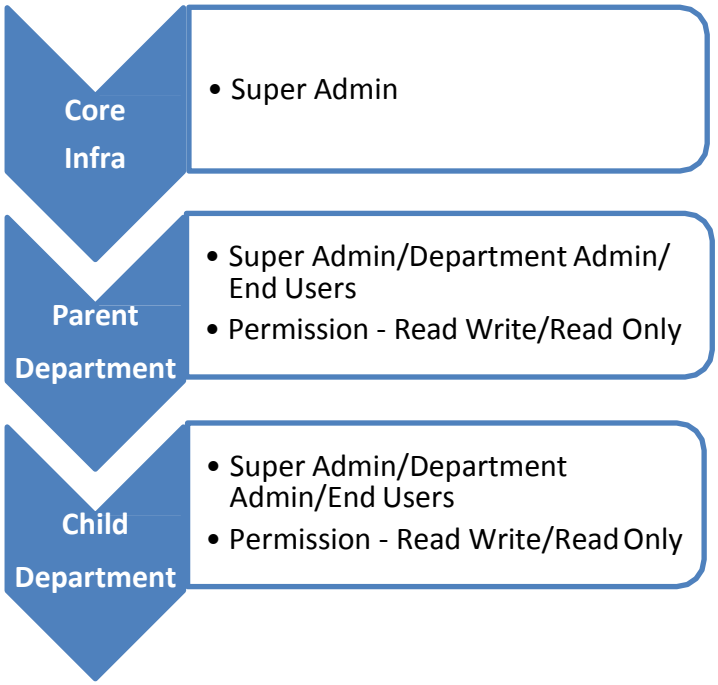
Department Administrators, End users with full permissions can create/delete, read, update and manage devices/monitors, notifications, actions and Log data. Unlike end users, administrators can have visibility across departments.

Administrators, End users from one department cannot view data belonging to another department unless the monitors are shared by the owner (for information on sharing monitors, see Sharing Monitor to Multiple Departments in section 14.2.2.). One monitor cannot be added in multiple departments.

17.3. Adding Department (Parent/Child)

Departments can have a single end user, or multiple child departments and end users. To add a new end user to the system, you need to first create the department and then create an end user. MindArray auto-generates a default department for each parent department created. The name of the auto-generated parent department is "**Core Infra**". All parent departments fall under the Core Infra and only Super Admin has privileges to access it.

Administrative hierarchy:



Service providers can integrate the system with their customer provisioning systems and set up new departments automatically.

To create Parent/Child Department, follow the steps given below:

1. Navigate to **Admin** > **Departments**.
2. Click **New** button, **Create New Department** tab appears.
3. If you are adding child department, select the parent department for child. If you are adding
4. Provide **Department Name**.
5. Click **Create**.

The system adds new department and displays confirmation message of the action.

17.4. User Permission

Each Admin/User is associated with one Role Group, which determines what permission members of the Role Group have. More precisely, permission control which tasks members of a Role Group can perform with respect to entities belonging to the departments associated with specific User.

Role Groups define the following:

- What a user will see when they log in to the Minder web console.
- The items that a user can add, view, edit, or delete when using the web console.

When you create Admin Role Group, consider two factors: The privileges of each set of administrators and how the end users will be administered. To give some administrators limited privileges while others have full privileges, you must create a separate Admin Role Group for each privilege level. Likewise, if two sets of administrators have the same privileges, but each set will administer different end users, you must create discrete Admin Role Group that can be mapped to separate departments.

To create Permission /User Roles, follow the steps given below:

1. Navigate to **Admin** > **User Roles**.
2. Click **New** button, Create New User Role tab appears.
3. Provide **Role Group Name**.
4. Select the **Admin Panel Access** you want to add to this role.
5. Provide the **Description** for user role if you want to.
6. Select the permissions you want to associate with the Role Group.
5. Click **Create**.

The system creates new User Role and displays confirmation message of the action.

Note: By default unchecked boxes provides read-only access to specific functionalities.

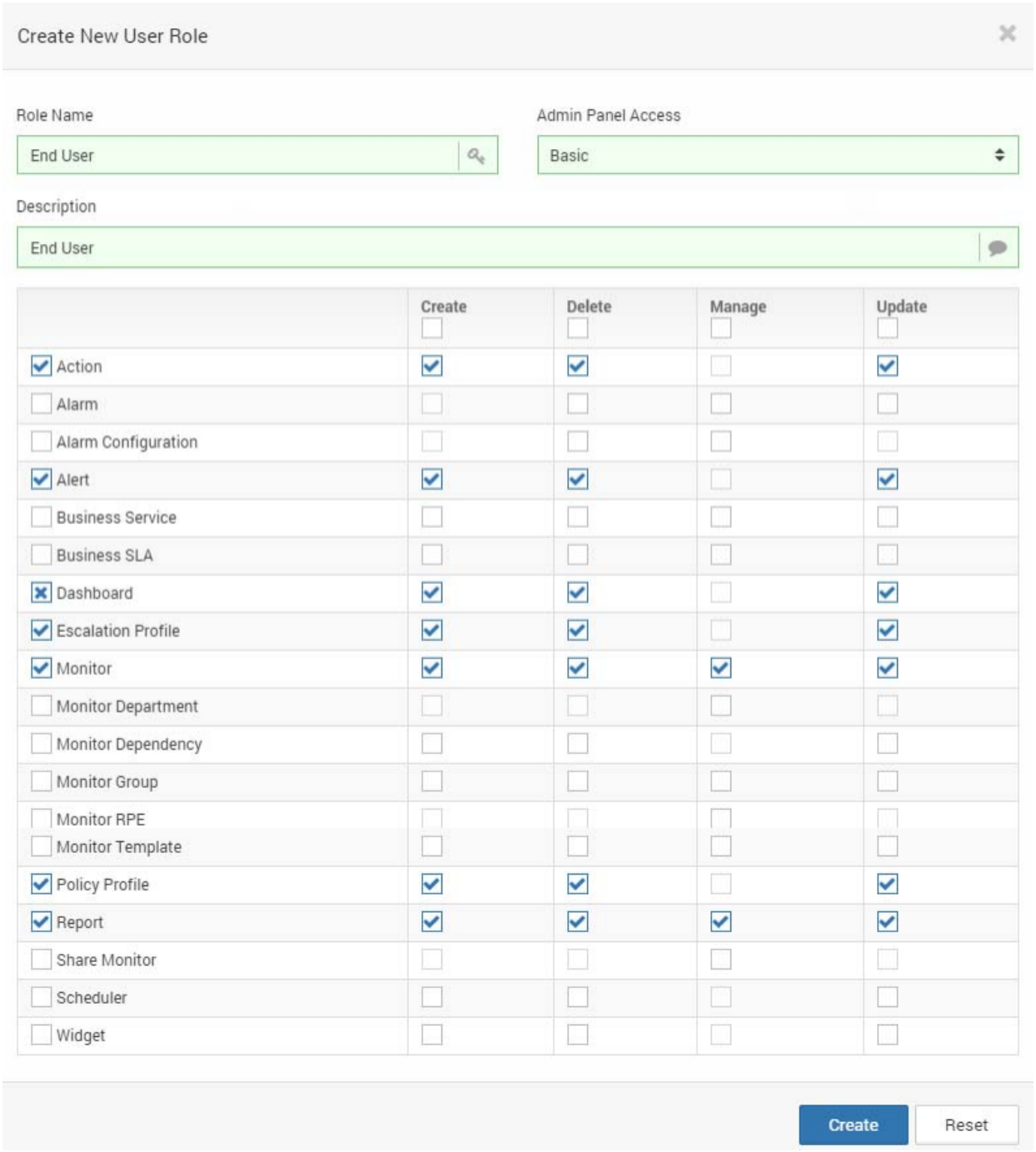


Figure Permission Matrix

17.5. Adding Users

If you are not using AD/LDAP authentication, follow the instruction given below to add MINDER users. For adding AD/LDAP users read the section 16.1.6.

To create MINDER user, follow the steps given below:

1. Navigate to **Admin** > **Users**.
2. Click **New** button, Create New User tab appears.
3. Provide **First Name, Last Name.**
4. Provide the **Username** and **Password**.
5. Provide **Email** address for the user.
6. Select the **Department** of the user.
7. Select the **Role Group** to be assigned to new user.
8. Click **Create**.

The system creates the new user and displays confirmation message of the action.

17.6. Working with AD/LDAP Server

Note: To enable user authentication using AD/LDAP server, navigate to Admin > Global Settings > Enable LDAP Authentication. Also select the Sync interval to sync the user information.

You can import AD/LDAP users in Minder and provide different privileges to them. If you are using Active Directory or an LDAP directory to authenticate the users, you have to create Minder user group in you AD/LDAP server then provide the details of AD/LDAP server to Minder to sync the user's details.

17.7. Adding AD/LDAP Server

Note: You have to create a user group with the name "minder users" or "minder help desk users" to create Helpdesk users specifically in your AD/LDAP and configure LDAP server under Admin > Configure LDAP Server, before adding details into Minder.

Follow the steps given below to create AD/LDAP server:

1. Navigate to **Admin** > **LDAP servers** > **New**.
2. Provide the **Name** for LDAP server configuration.
3. Provide the **LDAP/AD Hostname** or **IP address.**
4. Provide **FQDN**.
5. Provide the **Port Number**. Default Port is 389.
6. Provide Administrator **Username** and **Password**.
7. Click **Create** to finish.

The systems will create LDAP server and displays a confirmation message of the action.

Note: All the users under “Minder users” group will be authenticated using AD/LDAP server. You have to assign role and department to these users. MindArray automatically sync user information based on provided interval under global settings. To manually sync the information, select the LDAP server and click Sync.

17.8. Adding AD/LDAP Users

Once you add the AD/LDAP server details into MINDER, all the users under “Minder users” groups have now access to the Minder web console and they will be authenticated against the provided AD/LDAP server details. You have to assign role and department to these users.

To assign the role and department, follow the steps given below:

1. Navigate to **Admin** > **Users**.
2. Click on **Edit** button of AD/LDAP users, Update user dialog appears.
3. Provide the **Role** and **Department** to user.
4. Click **Update** to finish.

The systems will now configure AD/LDAP user and displays a confirmation message of the action.

17.9. Editing User Information

Follow the steps given below to edit user information:

1. Navigate to **Admin** > **Users**.
2. Click on **Edit** button, Update user dialog appears.
   Note: For AD/LDAP users, you can update their information on AD/LDAP server, MindArray automatically sync their information. To manually sync the information, select the LDAP server and click Sync.
3. Edit the Information.
4. Click **Update** to finish.

The systems will now update user information and displays a confirmation message of the action.

17.10. Sharing Monitors to other Departments/Users

Minder allows you to share monitors to other department with Full-access or Read-Only permission. When a monitor is shared to another department, any new changes done after the share are automatically shared or visible to the target department.

Warning: The credential profile attached to monitor is available to target department if share type is Full-access.

Sharing Entities:

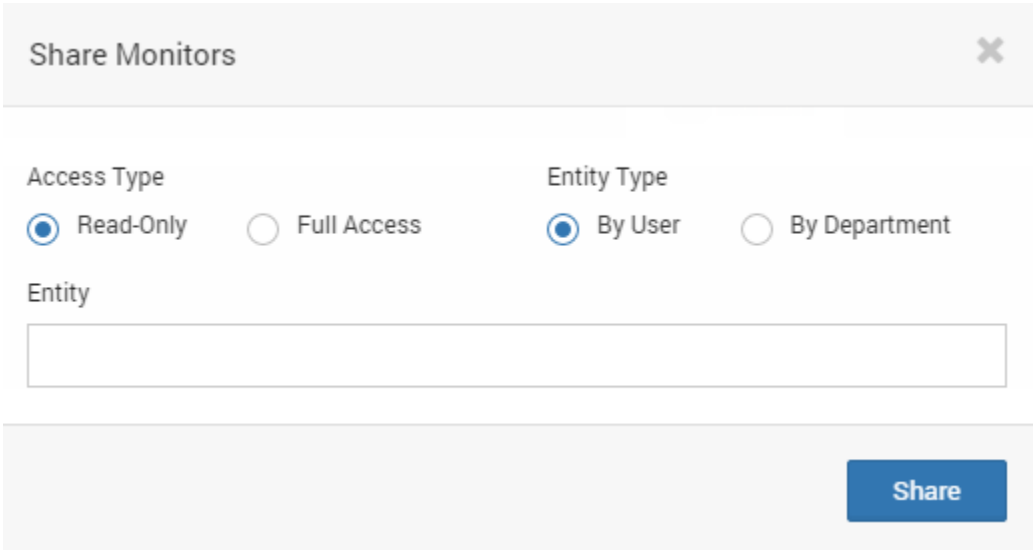


Figure Share Monitor to other department/user

Follow the steps given below to share monitor to other department or user:

1. Navigate to **Monitors** > **Monitors**.
2. Select the monitors you want to share.
3. Click **Actions** > **Share** on the top right corner. Share monitor dialog appears.
4. Choose the access as **Real-only** or **Full-access.**
5. Choose whether you want to share to other user of all the user of other department.
6. Click **Share**.

The system now makes the monitor visible to specified department/user and displays confirmation message of the action.

Note: Sharing monitor to other user/department also gives the read-only access to users belong to target department.

17.11. Move/Change Department of Single/Multiple Monitors

Warning: Moving a monitor permanently from one department removes the monitor and affects all the SLA, Business Services, Widget and Reports associated with that monitor in source department. In addition, any attached credential profile created by that department's administrator/users is permanently moved to target department. For more information about security see section 15.

Follow the steps given below to change/update Department into multiple monitors:

1. Navigate to the **Monitors** > **Monitor**.
2. Select monitors from the list.
3. Click **Action** > **Move**.
4. Select **Department** from the dropdown list to move monitors.
   Note: To manage Department navigate to Admin Panel > Departments.
5. Click **Move.**

The system updates new Department for selected monitors and displays a confirmation message of the action.

Note: You can also change Department of individual monitor from Monitor Overview page.

Glossary

Alarm/Event	Manifestation of important occurrence within the system. Events are generated internally (such as when a threshold is exceeded) or externally (such as through a syslog message or SNMP trap).
Alert/Notification	Email or page sent as a result of an event.
Discovery	Process by which the system gathers detailed information about devices in the Infrastructure. Results of discovery are used to populate the monitors to add.
Monitor Configuration	Property defined on a device or Monitor. Configuration properties control a large part of how monitoring is performed.
Monitoring Template	Description of performance data on a device or device component. Monitoring templates comprise four main elements: collected value, thresholds and graphs.
Performance Attributes	Objects contained by a device. Components include interfaces, OS processes, file systems, CPUs and hard drives.
Policy	Defines a value beyond which a polling value should not go. When a threshold is reached, the system generates an alarm event.