QUICK INSTALLATION GUIDE

Minder 4.2

Contents

1. Introducing MindArray Minder

MindArray Minder monitors, manages, and reports data collected form systems, network devices, and applications in a real-time and unified dashboard view.

At the user level, Minder provides all the control and information they may require based on their permission and responsibilities, by continuously monitoring your department level servers, applications, databases and IT resources, and alerts you to problems. Using the information that MindArray Minder gathers, you can solve problems before they impact your business.

Ensuring insight at every stage of interdependent application and services, our unified system helps you quickly identify the slowdown and performance bottlenecks based on key SLA metrics. With much deeper visibility, MindArray gives you comprehensive capabilities to analyze behavior patterns and track resource consumption.

- Get Pro-active notification on service view's containing composite components
- Track operational and performance service levels
- Identify and isolate performance bottlenecks
- Monitor and report on the performance of different performance metrics
- Run the root-cause analysis of a problem in your enterprise network
- Get capacity planning reports.
- Consolidate resources where necessary
- Create logical groups to track critical business service

1.1 Gain Visibility into Server, Application, Virtualization and Network Infrastructure

Enterprise IT environment is now a complex, interconnected and multi-layered system. Without clear visibility to its different aspects, there is a chance that you may be getting less than optimal performance. IT short-sightedness is now a challenge for IT managers that needs to be overcome by a unified infrastructure monitoring platform that would provide reports on real-time.

IT downtime can affect your business by delaying delivering results to your ultimate customers. MindArray monitors everything that is there to be monitored in developing an optimally operating IT infrastructure - maintains logs, applies analytics and insight essential for presenting a clear picture - all these from a unified platform for managing, monitoring and reporting.

1.2. Why Minder?

There are many reasons to choose Minder over any other monitoring product but only a few are listed below:

- 30 Minutes deployment, one touch Resource Aware Network Discovery & Health Status

- No more juggling consoles, Truly Unified IT Monitoring, RCA in 2-minutes, Application & Port level dependencies with multiple views
- No coding, 700+ out-of-the-box Reports & Widgets
- Smart UI & Great User Experience with interactive Flow!
- State-of-the-art Visualization Engine with drag & drop Schedulers

1.3. Key Features of Minder

- **Network Monitoring:**

Complete network management software with configurable discovery rules, extendible monitoring templates. Minder 4.2 also offers visibility into bandwidth usage and network slowdowns in complex environment.

- **Server & Application Monitoring:**

Minder 4.2 can discover and monitor not only System level performance data, but also the host operating system logs and underlying hardware health metrics. Easy-to-use interface gets you up and running quickly.

- **Cloud & virtualization Monitoring:**

Monitors with each component in the cloud and virtual environment, allowing you to identify if they are not delivering the expected service. IT operators need to be assured whether resources will be in place to handle an increasing number of requests.

- **Log (SIEM) Management:**

Minder 4.2 proactively delivers immediate correlation between collected performance data and logs. Minder 4.2 has automatic rules to monitor critical security logs collected from various Event log and Syslog based components.

- **Configuration and Change Management:**

Minder 4.2 provides an integrated solution for automating and controlling the entire life cycle of device configuration management. The efficient backup solution makes change detection, device configuration comparison easier and faster.

- **Flow Monitor**

In-depth visibility into your network traffic, for every device allowing, you to analyze alert and report on network traffic and bandwidth utilization in real-time to ensure quality of service.

2. Installation

2.1. Installation Requirements

The server hosting Minder 4.2 needs the following configuration at minimum:

	Essential Edition 10K interfaces or 500 servers	**Enterprise Edition** 100K interfaces or 5k servers (for both central and probe)	**Large Enterprise Edition** 1000k interfaces or 50k servers
Processor	Intel or AMD 64-bit dual core processor	2 x Intel Xeon Quad Core 3.5 GHz	2 x Intel Xeon Quad Core 3.5 GHz
RAM	4 GB	16 GB	16 GB
OS Windows	2012 R2 / 2012 / 2008 R2 / 2008 / 2003 Server / Vista / v7 / 2000 Professional SP4	2008 R2 64 bit / 2012 R2	2012 R2 / 2008 R2 64 bit (Preferred) 2008 / Win7/8
OS Linux	RedHat 4.x and above, Debian 3.0, Suse, Fedora and Mandrake	CentOS 64 bit or any linux distribution with glibc >= 2.3 and X libraries installed	RedHat 4.x and above, Debian 3.0, Suse, Fedora and Mandrake
Hard Disk	40 GB	320 GB	320 GB
Database	MS SQL 2000, 2005, 2008 and 2012 Or Minder bundled PostgreSQL	MSSQL 2008 and 2012 or Minder bundled PostgreSQL	MSSQL 2008, 2012 or Minder bundled PostgreSQL
Browser	IE 10 or above, Firefox 2.0 or above and Chrome 4.0 or above		

2.2. Installing on Windows

1. Download Minder for your server.
2. Provide your contact details for future email support.
3. Execute the downloaded Minder.exe on a windows server to install and proceed as per the instructions in the installation wizard.
4. Read the license agreement and click yes to start the installation.

5. If C++ is not present in the system then it will ask to install. Click on 'Install' of in Microsoft Visual C++ latest version installation wizard.
6. After the installation of Microsoft Visual C++ wizard is over, Minder will continue its own installation until it is successfully installed.
7. Either turn off your Antivirus software or specify exclusion for Minder in the Antivirus software to allow periodical pings from Minder without restriction.
8. Go to desktop and launch Minder.

Note: Make sure that your date-time settings are set to current date and time before the installation. If your system date is set to a different date then you will not be able to run the Minder server even after successful installation.

2.3. Test Cases

The following test cases help you to make sure the efficient working of Minder post upgrade:

1. Check the version on the login screen to verify that it reflects the same version as the Upgrade.
2. Test a monitor data to verify that Minder polls correct current data.
3. Generate a report for a monitor or any device or refresh a widget.
4. Verify the dashboard data about current alarms and health status.
5. Restart the windows server on which Minder is running and check whether Minder starts up as a service correctly

3. Configuring and setting up the system

3.1. System Startup

Once you successfully install MindArray Minder, Use your web browser to connect to http://your_host:8080/ where your host is the fully qualified host name or IP address of the server that the Minder Web application is running on.

If browser doesn't show the default login screen, then some components did not started or are not operating correctly, check for the following common start-up problems:

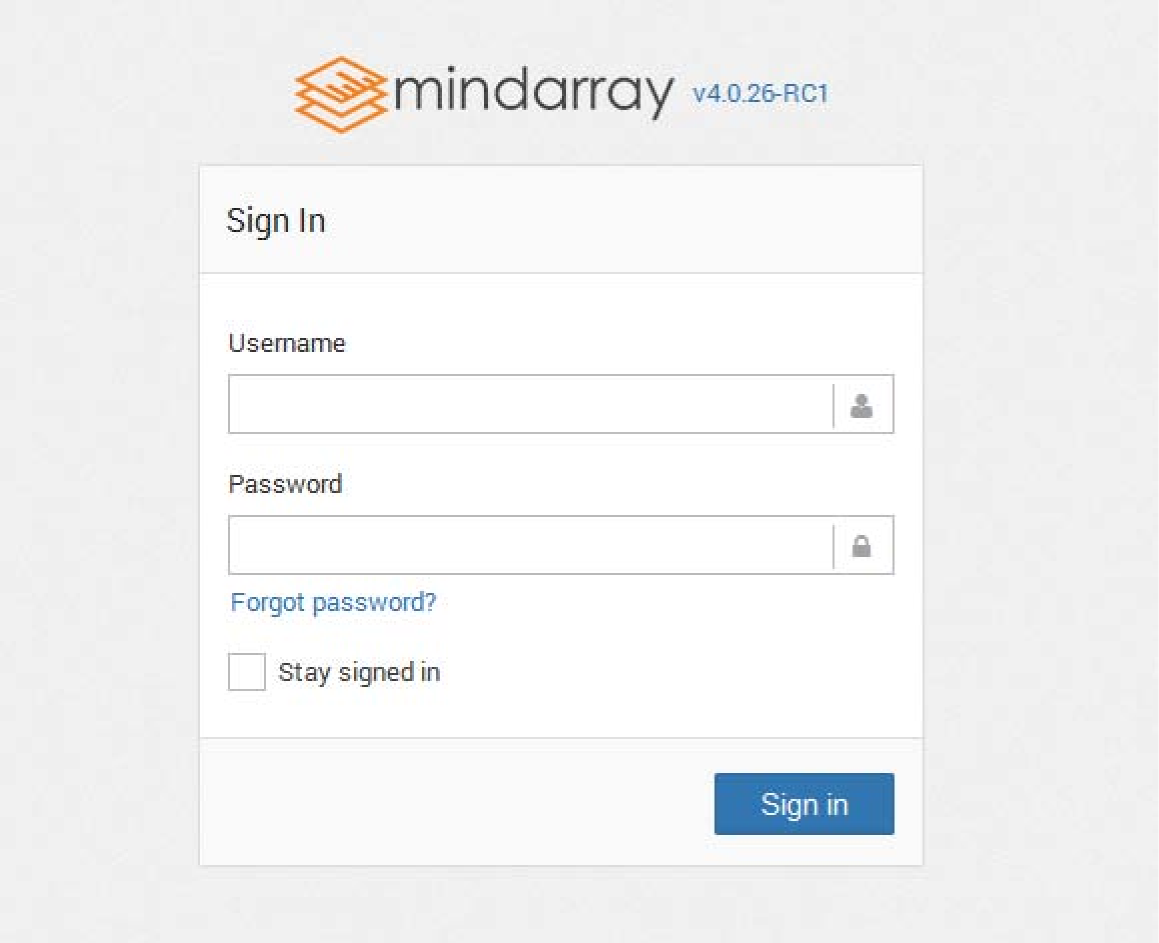
1. Verify that specified port # 8080, 8443 and 5432 are open.
2. MindArray IT Performance Manager Service is running.

3. You can also look for errors in the logs/IPM_KERNEL_INFO.log file in the MindArray Minder directory.

3.2. Logging into MindArray IPM

Use your web browser to connect to http://your_host:8080/ where your host is the fully qualified host name or IP address of the server that the MindArray IPM Web application is running on.

MindArray also configures secured URL to connect to web application using self sign certificate. Use https:// your_host:8443/ where your host is the fully qualified host name or IP address of the server that the MindArray Minder Web application is running on.



1. Use username – **admin** and password – **admin** to logging into system.
2. Navigate to Admin > User to set your user details such as Email, Department, Role Group.
3. Navigate to Admin > Global Settings to set user preferences.

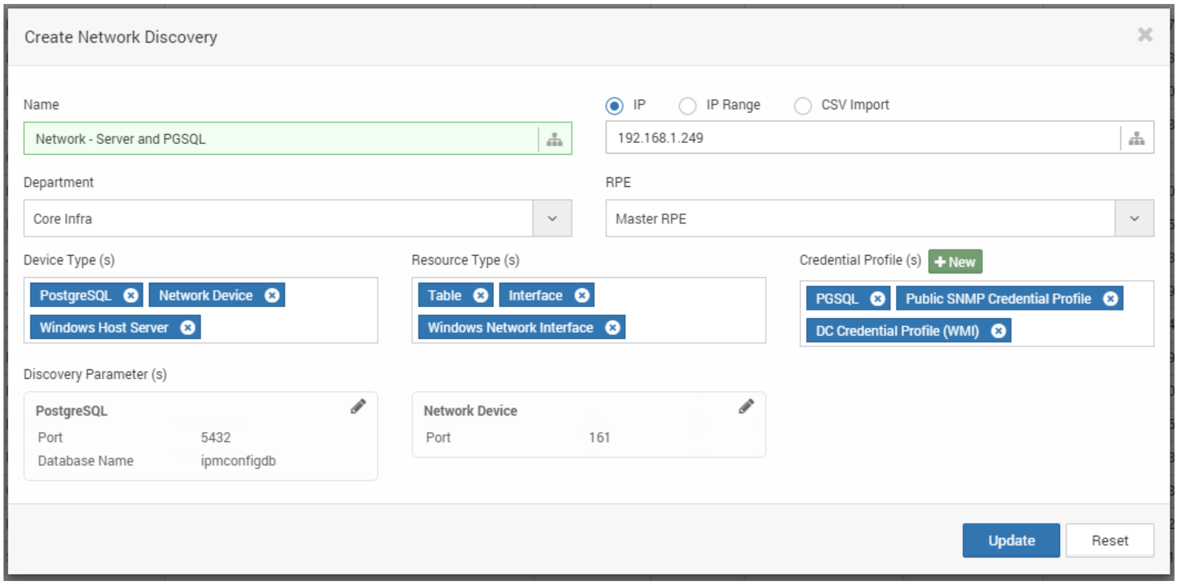
4. Adding Devices (using Network Discovery)

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. Minder provides four types of Network Discovery:

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

4.1. Device, Server & Apps Discovery

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



Create Network Discovery

Name: Network - Server and PGSQL

● IP ○ IP Range ○ CSV Import: 192.168.1.249

Department: Core Infra

RPE: Master RPE

Device Type (s): PostgreSQL, Network Device, Windows Host Server

Resource Type (s): Table, Interface, Windows Network Interface

Credential Profile (s): PGSQL, Public SNMP Credential Profile, DC Credential Profile (WMI)

Discovery Parameter (s)

PostgreSQL
Port 5432
Database Name ipmconfigdb

Network Device
Port 161

Figure 4.1 Network Discovery > Device, Server & Apps

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.

4. Select **Department** from the list.
5. Select **RPE** (Remote Polling Engine) from the list.
6. 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.
7. Provide the **Resource Type** to be discovered, E.g. Process, Service, Interface, Database Tables etc.
8. Provide **Credential profile** 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, Virtual Machines with in Hypervisor will be listed under Virtual Machine Tab. Selected Objects should be displayed at top of the pop-up as total number of nodes, resources, applications, virtual machines.
13. Click on **Provision Object** to add selected objects.

4.2. Cloud Network Discovery

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. **IP:** for single device

   IP Range: for multiple devices.

   CSV Import: for selected multiple devices.
4. Select **Department** from the list.
5. Select **RPE** (Remote Polling Engine) from the list.

6. Select **Device Type** 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 **Resource Type** to be discovered.
8. Provide **Credential profile** for selected cloud types.
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.
13. Click on **Provision Object** to add selected objects.

4.3. Service Discovery

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:** for single device

   IP Range: for multiple devices.

   CSV Import: for selected multiple devices.
4. Select **Department** from the list.
5. Select **RPE** (Remote Polling Engine) from the list.
6. Select **Device 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.

12. Click on **Provision Object** to add selected objects.

4.4. Asset Discovery

Asset discovery allows you to scan workstation, Desktop and Laptop 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.

Follow the steps given below to add asset by running discovery:

1. Navigate to **Admin** > **Network Discovery** > **New** > **Asset**.
2. Provide the **Name** for the discovery.
3. **IP:** for single device

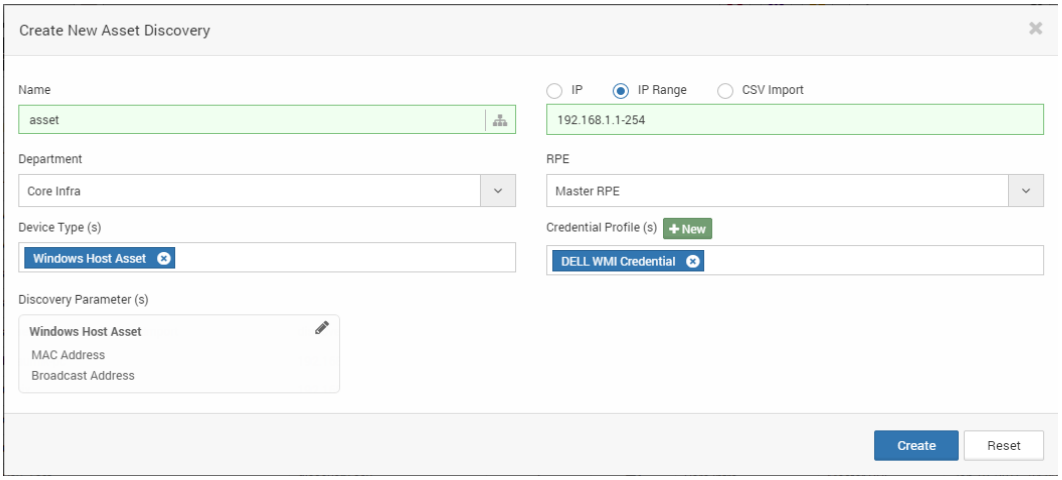
   IP Range: for multiple devices.

   CSV Import: for selected multiple devices.
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.

    Note: Discovered private network 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 the pop-up as total number of nodes, resources, applications, virtual machines.

12. Click on **Provision Object** to add selected objects for monitoring.



Create New Asset Discovery

Name: asset

○ IP ● IP Range ○ CSV Import: 192.168.1.1-254

Department: Core Infra

RPE: Master RPE

Device Type (s): Windows Host Asset

Credential Profile (s): DELL WMI Credential

Discovery Parameter (s)

Windows Host Asset
MAC Address
Broadcast Address

Figure 4.4 Asset Discovery

4.5. 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. Provide IP address range (for multiple devices) or single IP address or import them using CSV file.
4. Select the **Department** from the list.
5. Select the **RPE** (Remote Polling Engine) from the list.
6. 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 Hypervisor resource type to be discovered - Hyper-V Virtual Machine, Xen Virtual Machine, Xen Network Interface, ESX Virtual Machine etc.
7. Provide **Credential Profile** (VMware/Hyper-V/Citrix).
8. Click on **Create** to create new discovery.
9. Click on **Run** to run the discovery
10. Once finished, click on **View Result** to view classified Hypervisors and Virtual Machines.
11. Click on **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.

12. Click on **Provision Object** to 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.

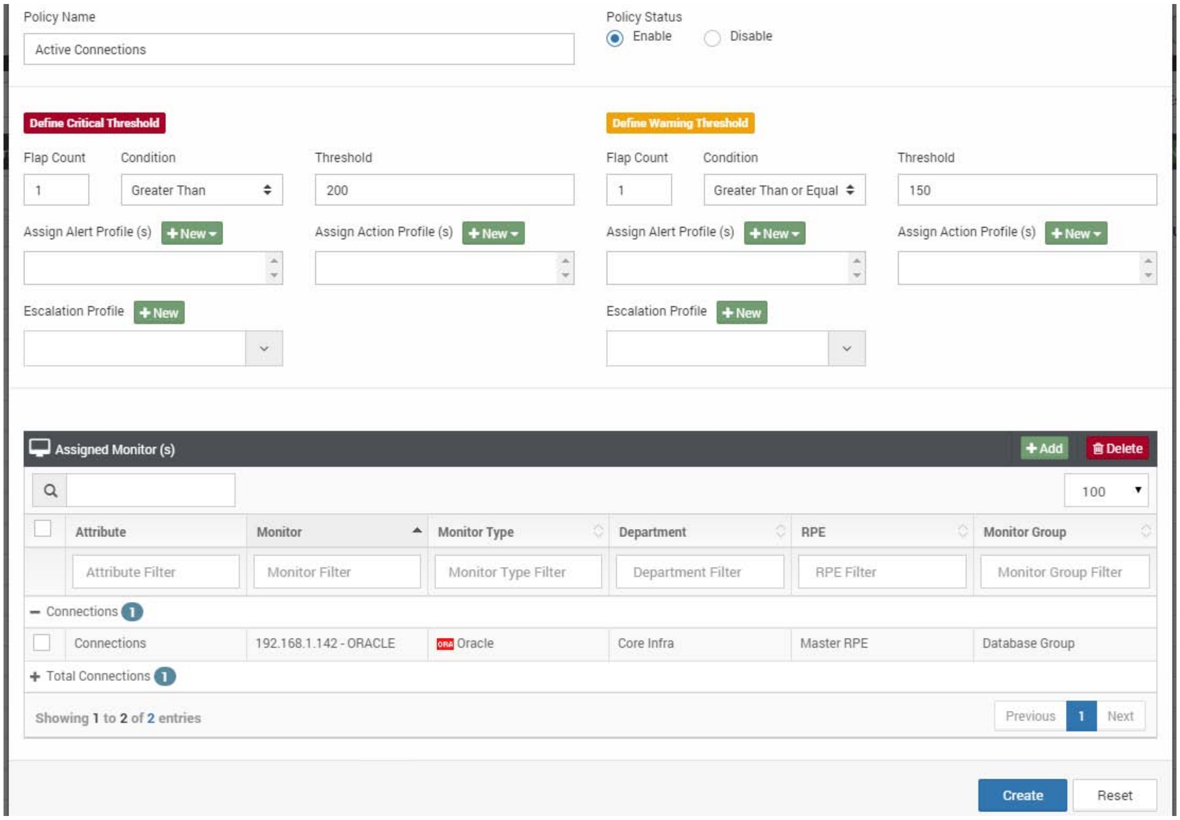
5. Creating Policies and Alerts

Each alert describes an event occurs under certain conditions, and a set of actions defined for it. You must define alerting actions and associate them with particular events.

Actions describe what is to be done when a particular event takes place. An example of an alerting action is emailing a specific user (or group of users) when an event such as ‘Node Down’ takes place on a monitored node.

5.1. Performance Policies

Follow the steps given below to create Performance Policies:



Policy Name: Active Connections

Policy Status: ● Enable ○ Disable

Define Critical Threshold

Flap Count: 1 | Condition: Greater Than | Threshold: 200

Define Warning Threshold

Flap Count: 1 | Condition: Greater Than or Equal | Threshold: 150

Assigned Monitor (s)

□	Attribute	Monitor	Monitor Type	Department	RPE	Monitor Group
	Attribute Filter	Monitor Filter	Monitor Type Filter	Department Filter	RPE Filter	Monitor Group Filter
− Connections 1						
□	Connections	192.168.1.142 - ORACLE	Oracle	Core Infra	Master RPE	Database Group
+ Total Connections 1						

Showing 1 to 2 of 2 entries

Figure 5.1 Performance Policy

1. Navigate to **Policies & Alerts** > **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 on **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 on **Add** to selected monitor and their attributes.
9. Click on **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.

5.2. Viewing Monitor Alarm

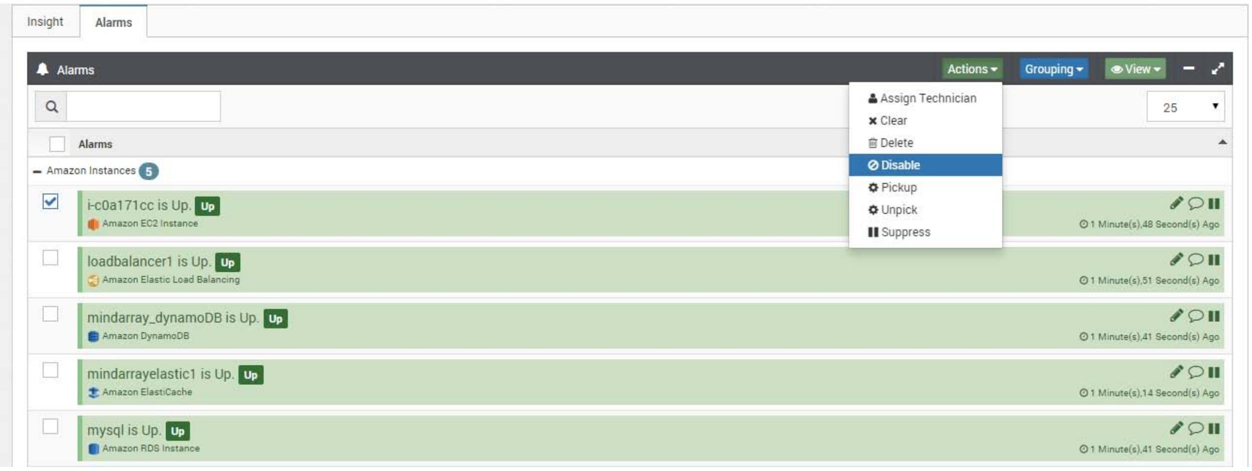
Alarms associated to specific monitor are used to determine health of the monitor.

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

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

5.3. 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.



☑ i-c0a171cc is Up. Up
Amazon EC2 Instance
1 Minute(s),48 Second(s) Ago

□ loadbalancer1 is Up. Up
Amazon Elastic Load Balancing
1 Minute(s),51 Second(s) Ago

□ mindarray_dynamoDB is Up. Up
Amazon DynamoDB
1 Minute(s),41 Second(s) Ago

□ mindarrayelastic1 is Up. Up
Amazon ElastiCache
1 Minute(s),14 Second(s) Ago

□ mysql is Up. Up
Amazon RDS Instance
1 Minute(s),41 Second(s) Ago

Figure 5.3 Delete/Disable Alarm.

To disassociate a policy from performance attribute, follow the steps given below:

1. Navigate to **Alarms** > Click on **Alarms**.
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. Navigate to **Actions** > **Delete/Disable**.

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

5.4. Alert Profiles

Follow the steps given below to create Email alert:

1. Navigate to **Policies & Alerts** > **Alert Profiles** > Click on **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** for the emails action.
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: $Monitor Name
   $Monitor Host
   $Alarm Name
   $Severity
   $Timestamp
   $Root Cause

   Example: Message from IPM - $Monitor Name has violation occurred in $Alarm Name 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 on **Create**.

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

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. To configure number of alters to be sent > Navigate to **Admin** > **Global Settings** > Specify the number of notifications to be sent.

5.5. Creating Action Profile

Follow below steps to create action to send SNMP Trap:

1. Navigate **to Policies & Alerts** > **Action Profiles** > SNMP Trap Actions. Click on **Add** button.
2. Provide the **Action Name** for the SNMP trap action.
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 on **Save** to finish.

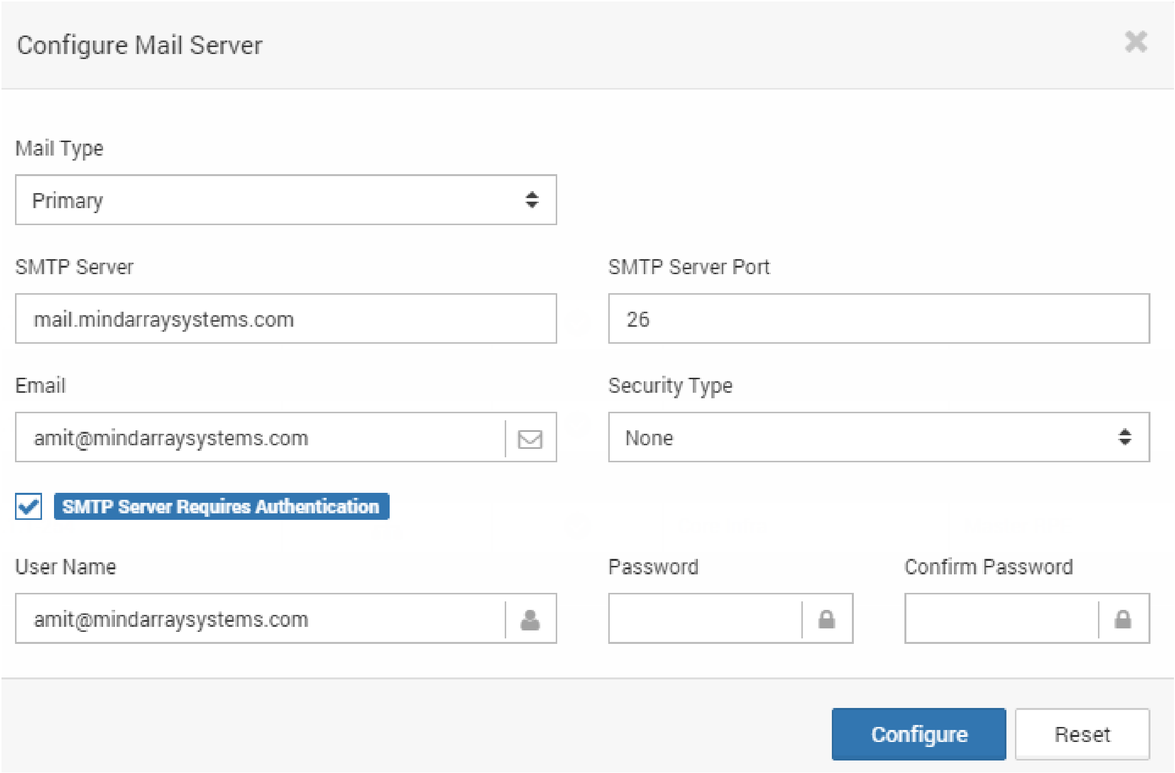
The system saves SNMP trap action, and displays confirmation message of the action.

5.6. Configuring Mail Server

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 Server Port to** connect.
5. Provide the **From Email** address you want to use as FROM.
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.



Mail Type: Primary

SMTP Server: mail.mindarraysystems.com

SMTP Server Port: 26

Email: amit@mindarraysystems.com

Security Type: None

☑ SMTP Server Requires Authentication

User Name: amit@mindarraysystems.com

Password:

Confirm Password:

Figure 5.6 Admin > Configure Mail Server

6. Widgets for Custom Dashboard

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

- **Widget Type**
  Specify the kind of information presented, chosen from the set of features.
- **Component Type**
  Specifies the manner in which the information will be presented, chosen from a set of built-in chart and graph types.
- **Title**
  The descriptive title of the component.
- **Time Span**
  Specifies the duration in which the graph data was observed.
- **Refresh Time**
  The interval at which the component will refresh the information it contains, ranging from 0 to 30 minutes.

6.1. Custom Dashboard

A user may wish to review only a selected number of widgets based on her priority. Interestingly, the custom dashboard provides this facility of only selecting the widgets important in a single context. Also, such custom dashboards can be created multiple times.

To create new custom dashboard:

1. Navigate to **Dashboard** > Click on ✚ icon.
2. Create Dashboard dialog appears. Provide the **Name** of the Dashboard.
3. Select the **Security Type** – If you want to share the dashboard to other team members, choose public.
4. Click on **Create**.

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

6.2. Widget Types

The kind of information which you wish to observe can be selected using Widget types.

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

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

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

6.3. Adding Default Widgets

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

Follow the steps given below to add default Widget:

1. Navigate to **Dashboards** > Click on + 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 you wish to add.
4. Click **Add**.

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

6.4. Adding Custom Widgets

System has more than 700+ pre-built widgets to report performance data into custom dashboards. However, to make a new widget according to your need then you can create your custom widget.

Follow the steps given below to add custom Widget:

1. Navigate to **Dashboards** > Click on + 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; click N**ew** and select the component type.
4. New Untitled Widget will be added in the widget grid. Select it and click on **Add**.
5. After the widget appears on the Dashboard. Click on ⚙ Widget properties and select Data Source.
6. Search, select and update the monitors and their attributes you wish to review in the customized widget.
7. The Time Span, Refresh Time, Width and many other widget properties can be configured from there.

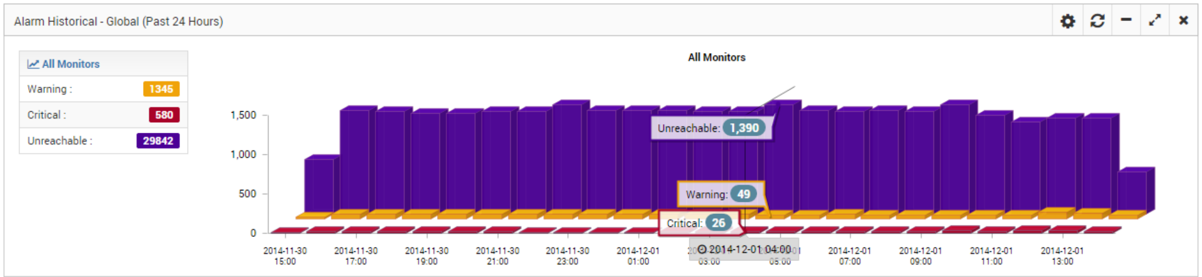
6.5. Alarm Widget

Alarm Widget shows a comprehensive view of the alarms generated in the specified time span in the selected monitors.

Follow the steps given below to create Alarm Widget:

1. Navigate to **Dashboards** > Click on + 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.

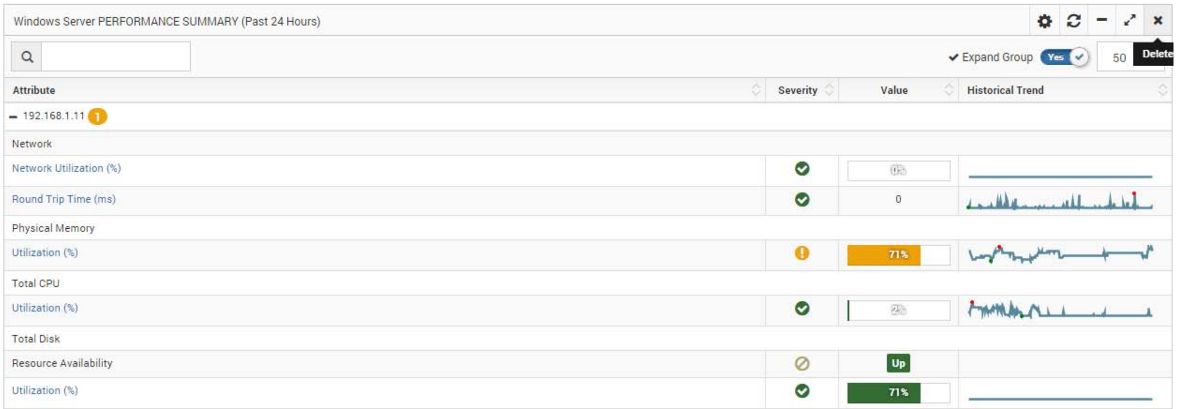

Alarm Historical - Global (Past 24 Hours)

All Monitors	
Warning :	1345
Critical :	580
Unreachable :	29842

Figure 6.5 Alarm Widget

6.6. 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.

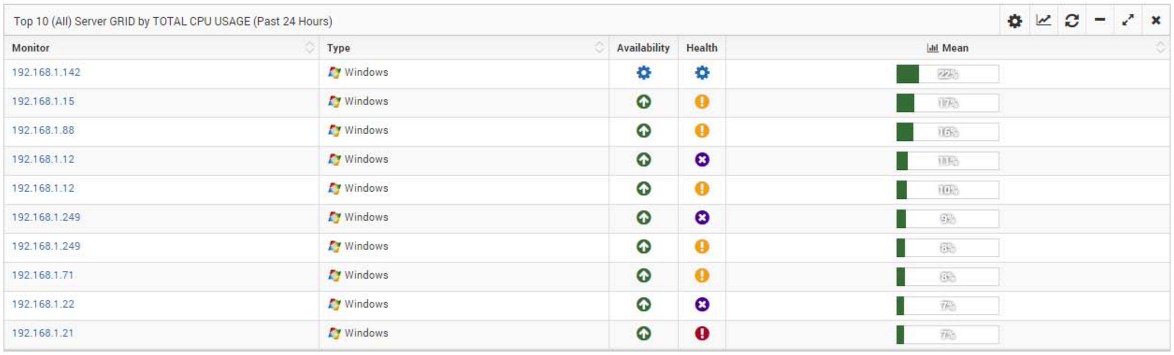


Windows Server PERFORMANCE SUMMARY (Past 24 Hours)

✓ Expand Group Yes 50 Delete

Attribute	Severity	Value	Historical Trend
− 192.168.1.11 1			
Network			
Network Utilization (%)	✓	0%	
Round Trip Time (ms)	✓	0	
Physical Memory			
Utilization (%)	!	71%	
Total CPU			
Utilization (%)	✓	2%	
Total Disk			
Resource Availability	⊘	Up	
Utilization (%)	✓	71%	

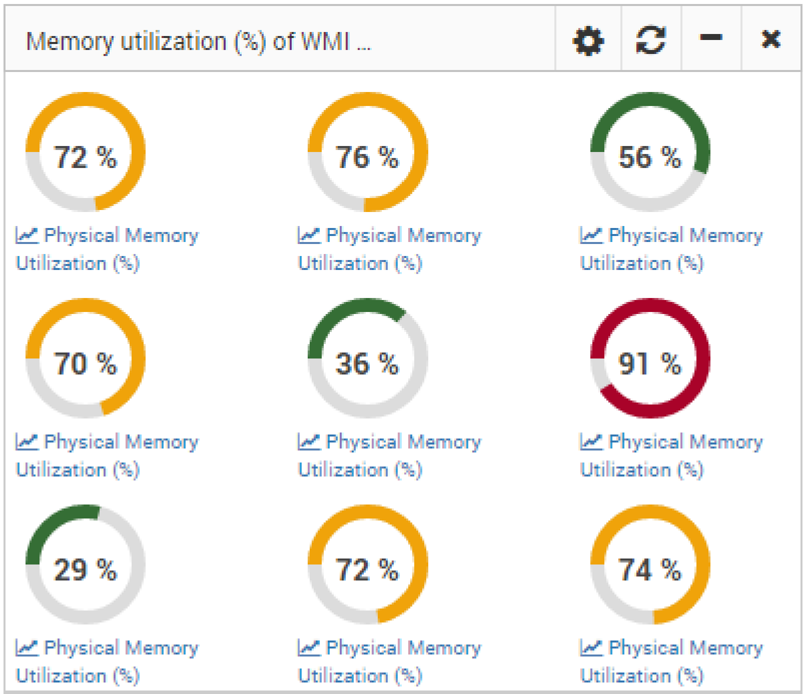
Figure 6.6 Performance Widget View Type – Grid



Top 10 (All) Server GRID by TOTAL CPU USAGE (Past 24 Hours)

Monitor	Type	Availability	Health	Mean
192.168.1.142	Windows	⚙	⚙	22%
192.168.1.15	Windows	↑	!	17%
192.168.1.88	Windows	↑	!	16%
192.168.1.12	Windows	↑	✖	11%
192.168.1.12	Windows	↑	!	10%
192.168.1.249	Windows	↑	✖	9%
192.168.1.249	Windows	↑	!	8%
192.168.1.71	Windows	↑	!	8%
192.168.1.22	Windows	↑	✖	7%
192.168.1.21	Windows	↑	!	7%

Figure 6.6 Performance Widget, Widget type – Historical



Memory utilization (%) of WMI ...

72 % Physical Memory Utilization (%)	76 % Physical Memory Utilization (%)	56 % Physical Memory Utilization (%)
70 % Physical Memory Utilization (%)	36 % Physical Memory Utilization (%)	91 % Physical Memory Utilization (%)
29 % Physical Memory Utilization (%)	72 % Physical Memory Utilization (%)	74 % Physical Memory Utilization (%)

Figure 6.6 Health Widget, Widget type – Gauge – Live

Follow the steps given below to create Performance Widget:

1. Navigate to **Dashboards** > Click on **+** 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.

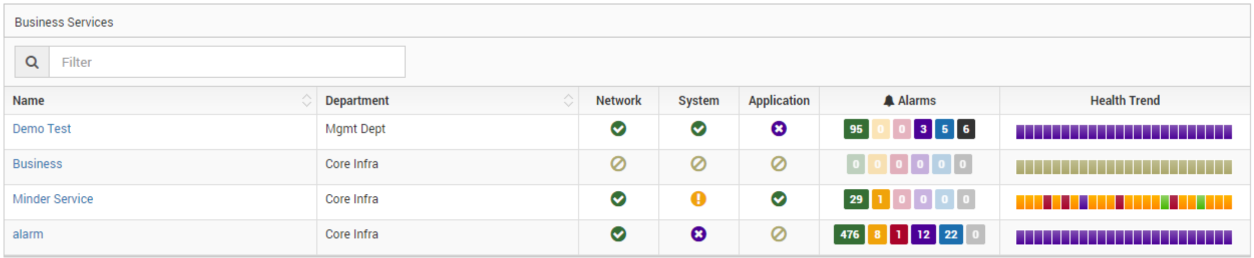
The systems will create the new Widget properties, and displays a confirmation message of the action

7. Using Service Analytics

7.1. 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.



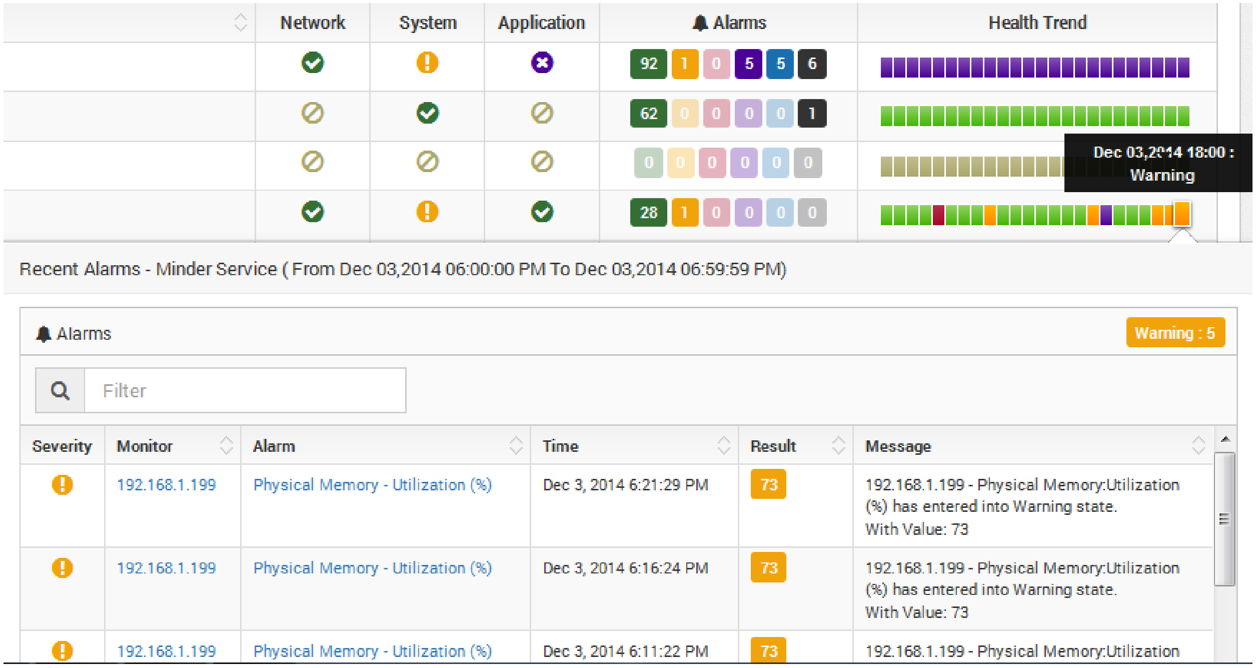
Business Services

Filter

Name	Department	Network	System	Application	Alarms	Health Trend
Demo Test	Mgmt Dept	✓	✓	✖	95 0 0 3 5 6	
Business	Core Infra	⊘	⊘	⊘	0 0 0 0 0 0	
Minder Service	Core Infra	✓	!	✓	29 1 0 0 0 0	
alarm	Core Infra	✓	✖	⊘	476 8 1 12 22 0	

Figure 7.1 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.



	Network	System	Application	Alarms	Health Trend
	✓	!	✖	92 1 0 5 5 6	
	⊘	✓	⊘	62 0 0 0 0 1	
	⊘	⊘	⊘	0 0 0 0 0 0	Dec 03,2014 18:00 : Warning
	✓	!	✓	28 1 0 0 0 0	

Recent Alarms - Minder Service (From Dec 03,2014 06:00:00 PM To Dec 03,2014 06:59:59 PM)

Alarms

Warning : 5

Filter

Severity	Monitor	Alarm	Time	Result	Message
!	192.168.1.199	Physical Memory - Utilization (%)	Dec 3, 2014 6:21:29 PM	73	192.168.1.199 - Physical Memory:Utilization (%) has entered into Warning state. With Value: 73
!	192.168.1.199	Physical Memory - Utilization (%)	Dec 3, 2014 6:16:24 PM	73	192.168.1.199 - Physical Memory:Utilization (%) has entered into Warning state. With Value: 73
!	192.168.1.199	Physical Memory - Utilization (%)	Dec 3, 2014 6:11:22 PM	73	192.168.1.199 - Physical Memory:Utilization

Figure 7.1 Service Health Dill-Down

7.2. Adding Business Service

To create a new business service, follow the steps given below:

1. Navigate **to Business Services** > **Business Services**.
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.

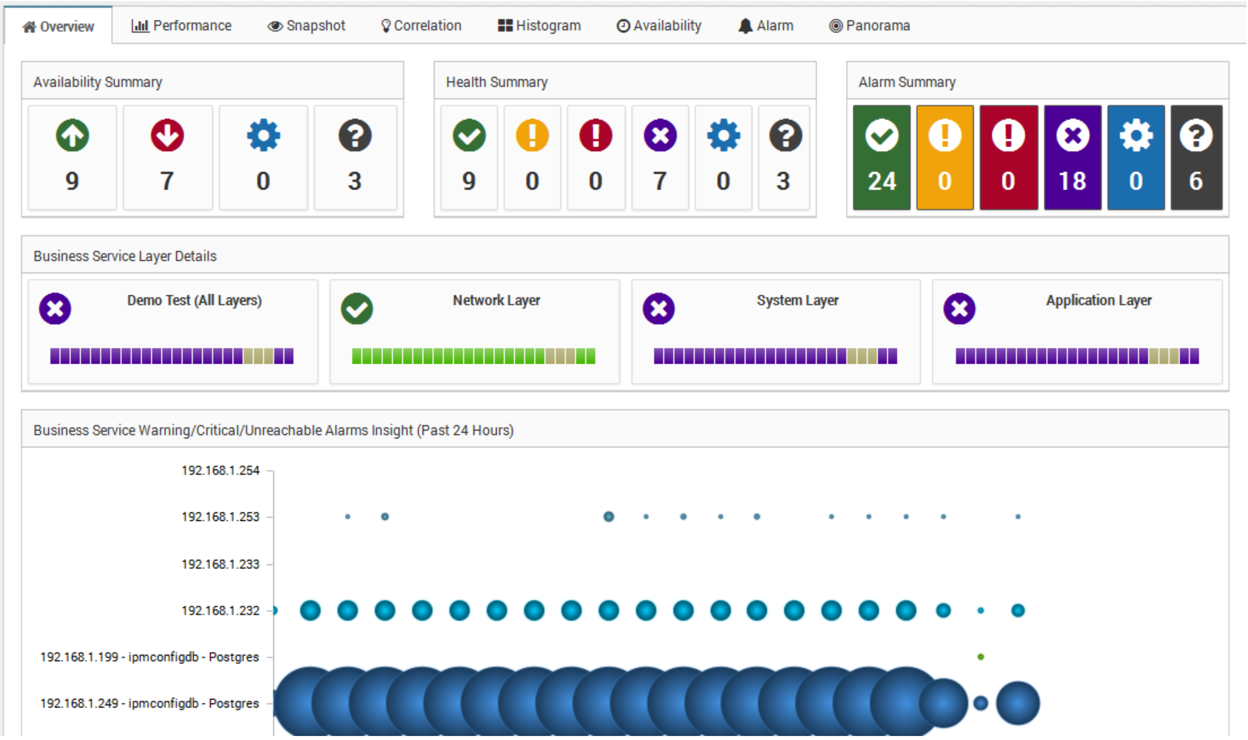
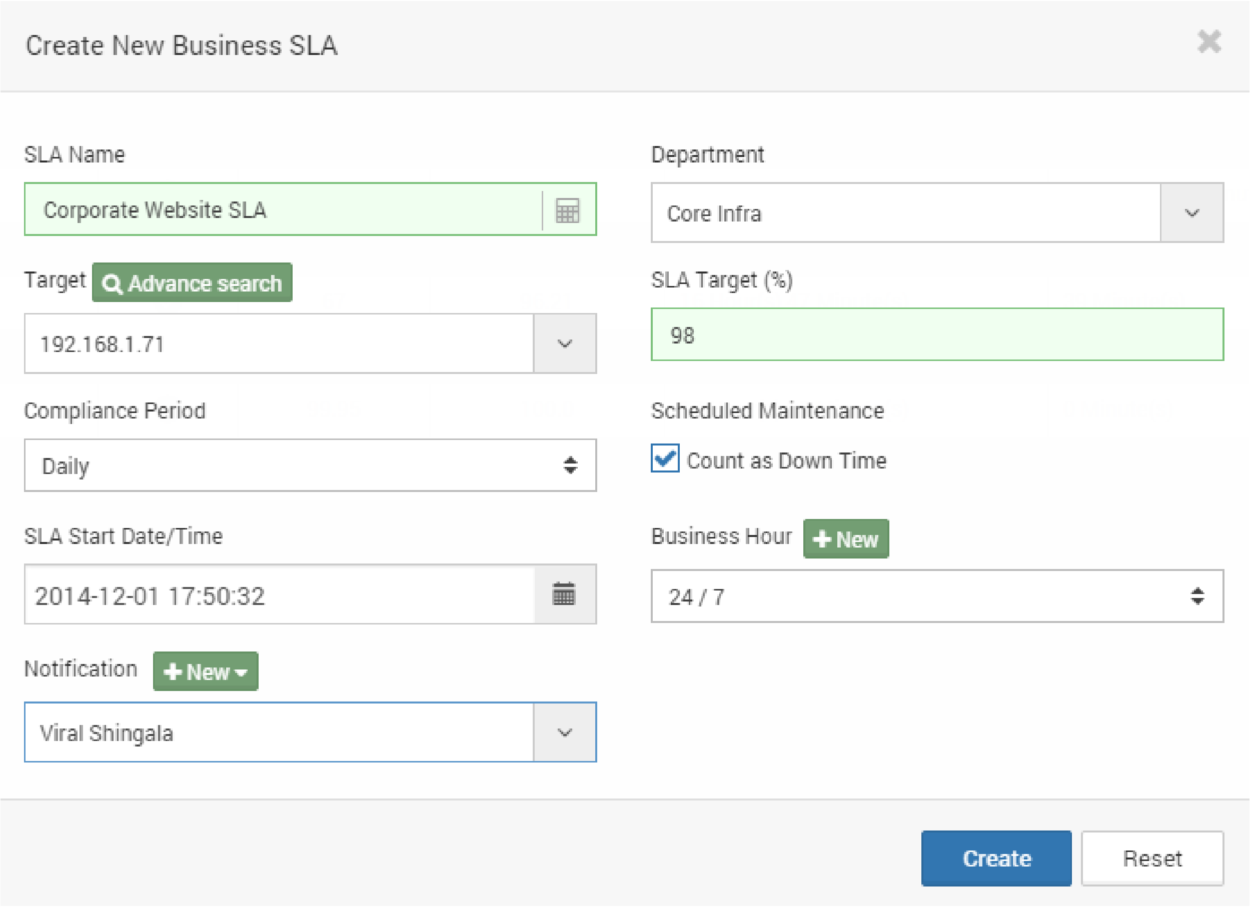


Figure 7.2 Business Service Overview

8. Business SLA

8.1. 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.



SLA Name: Corporate Website SLA

Department: Core Infra

Target: 192.168.1.71

SLA Target (%): 98

Compliance Period: Daily

Scheduled Maintenance: ☑ Count as Down Time

SLA Start Date/Time: 2014-12-01 17:50:32

Business Hour: 24 / 7

Notification: Viral Shingala

Figure 8.1 Create Business SLA

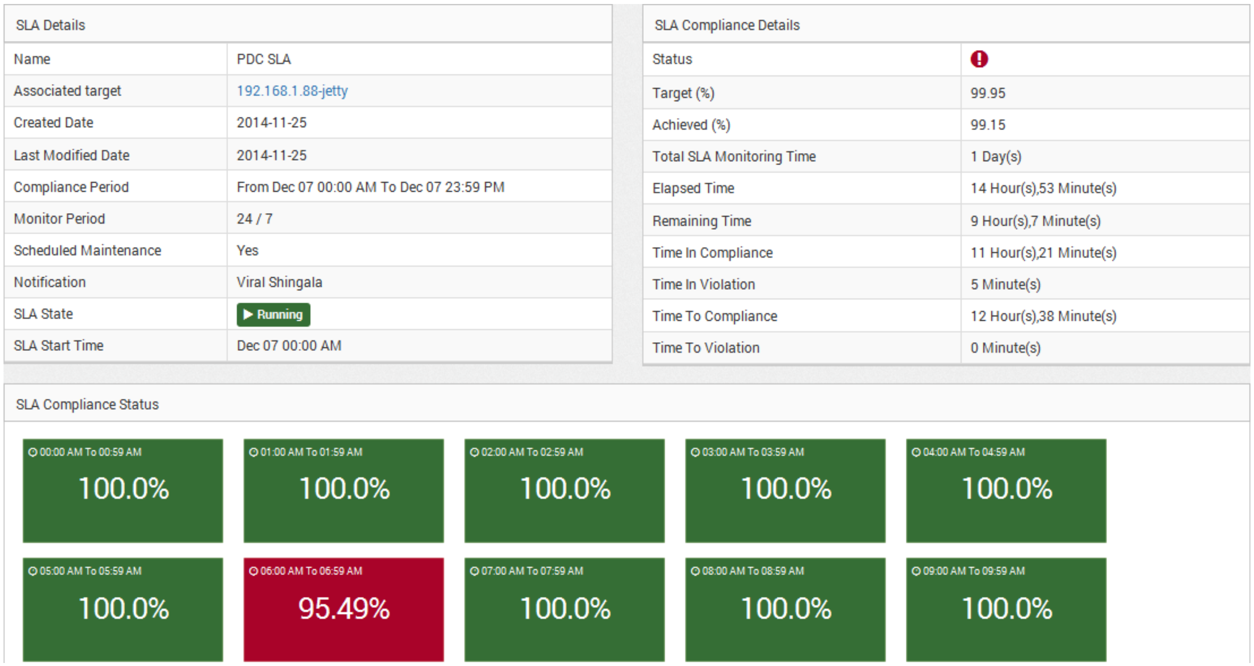
To create a new SLA Measurement, follow the below steps:

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.



SLA Details

Name	PDC SLA
Associated target	192.168.1.88-jetty
Created Date	2014-11-25
Last Modified Date	2014-11-25
Compliance Period	From Dec 07 00:00 AM To Dec 07 23:59 PM
Monitor Period	24 / 7
Scheduled Maintenance	Yes
Notification	Viral Shingala
SLA State	▶ Running
SLA Start Time	Dec 07 00:00 AM

SLA Compliance Details

Status	!
Target (%)	99.95
Achieved (%)	99.15
Total SLA Monitoring Time	1 Day(s)
Elapsed Time	14 Hour(s),53 Minute(s)
Remaining Time	9 Hour(s),7 Minute(s)
Time In Compliance	11 Hour(s),21 Minute(s)
Time In Violation	5 Minute(s)
Time To Compliance	12 Hour(s),38 Minute(s)
Time To Violation	0 Minute(s)

SLA Compliance Status

00:00 AM To 00:59 AM 100.0%	01:00 AM To 01:59 AM 100.0%	02:00 AM To 02:59 AM 100.0%	03:00 AM To 03:59 AM 100.0%	04:00 AM To 04:59 AM 100.0%
05:00 AM To 05:59 AM 100.0%	06:00 AM To 06:59 AM 95.49%	07:00 AM To 07:59 AM 100.0%	08:00 AM To 08:59 AM 100.0%	09:00 AM To 09:59 AM 100.0%

Figure 8.2 SLA Drill-Down Page

9. Reports

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

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

9.1. 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.

Example: Current Device and Component Status

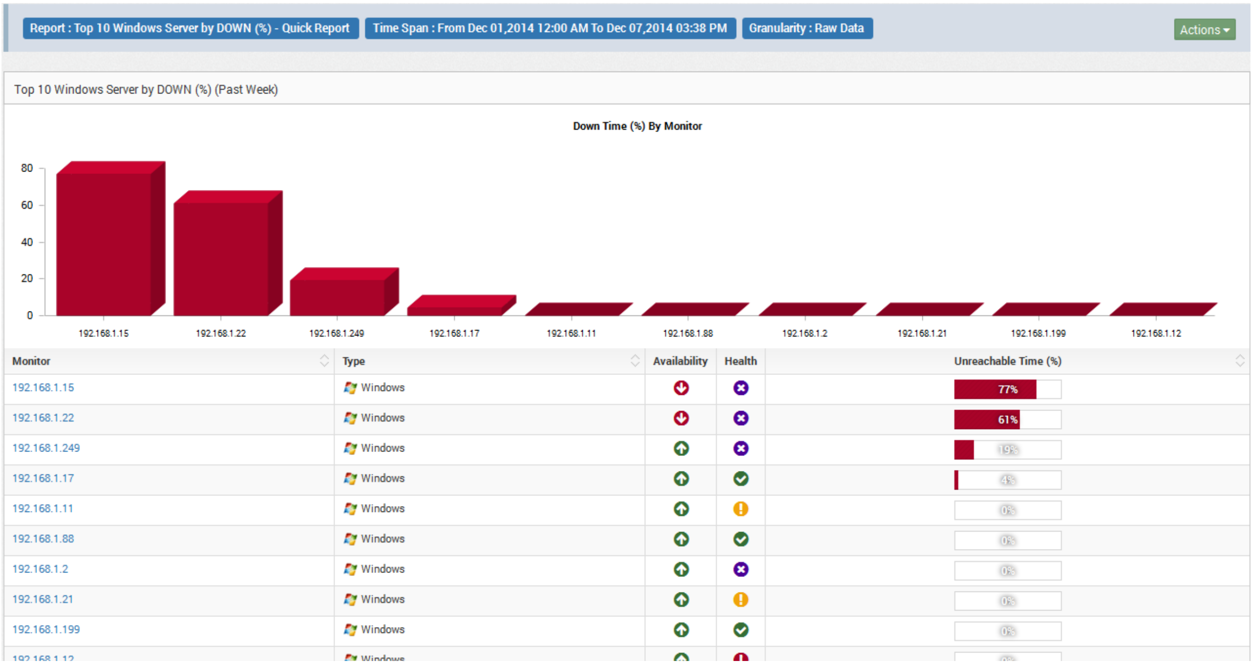
- Average Response Time of each Component
- Current CPU Load of each Component
- Current Memory Utilization of each Component
- Current Status of each Application
- Current Status of each Component

9.2. 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 pre-defined and custom report options in quick reports.

Viewing Quick Reports in the Minder Web Console:

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



Report : Top 10 Windows Server by DOWN (%) - Quick Report | Time Span : From Dec 01,2014 12:00 AM To Dec 07,2014 03:38 PM | Granularity : Raw Data

Top 10 Windows Server by DOWN (%) (Past Week)

Monitor	Type	Availability	Health	Unreachable Time (%)
192.168.1.15	Windows	↓	✖	77%
192.168.1.22	Windows	↓	✖	61%
192.168.1.249	Windows	↑	✖	19%
192.168.1.17	Windows	↑	✓	4%
192.168.1.11	Windows	↑	!	0%
192.168.1.88	Windows	↑	✓	0%
192.168.1.2	Windows	↑	✖	0%
192.168.1.21	Windows	↑	!	0%
192.168.1.199	Windows	↑	✓	0%
192.168.1.12	Windows	↑	!	

Figure 9.2 Quick Report – Top 10 Windows Server by Down Time

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

9.3. 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, therefore, 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 will appear.
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.

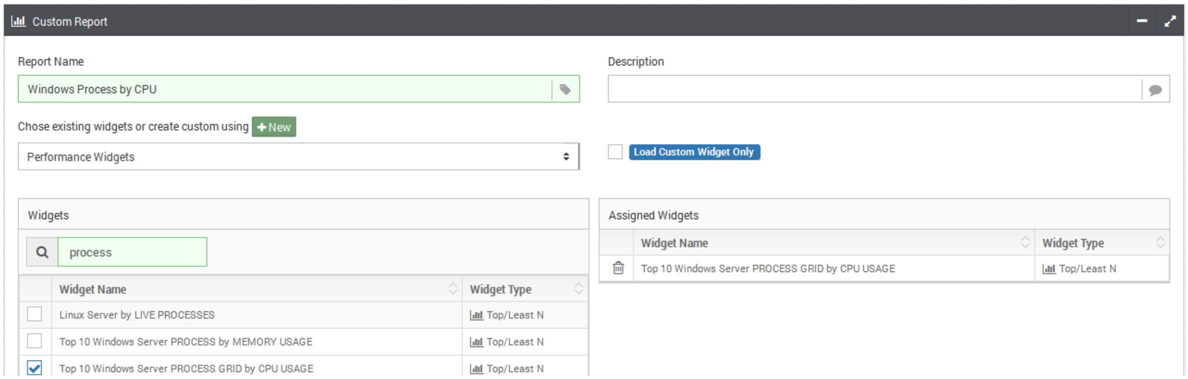
9.4. Adding Custom Report

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.

Follow the steps listed below to generate a new Report:

1. Navigate to Reports > Custom Reports.
2. Click New, Custom Report dialog appears.
3. Provide Name and description for report.
4. Click New to add more widget. You can select from a list of pre-defined widget and custom widget that are created by users.



Custom Report

Report Name: Windows Process by CPU

Description:

Chose existing widgets or create custom using +New

Performance Widgets

□ Load Custom Widget Only

Widgets

process

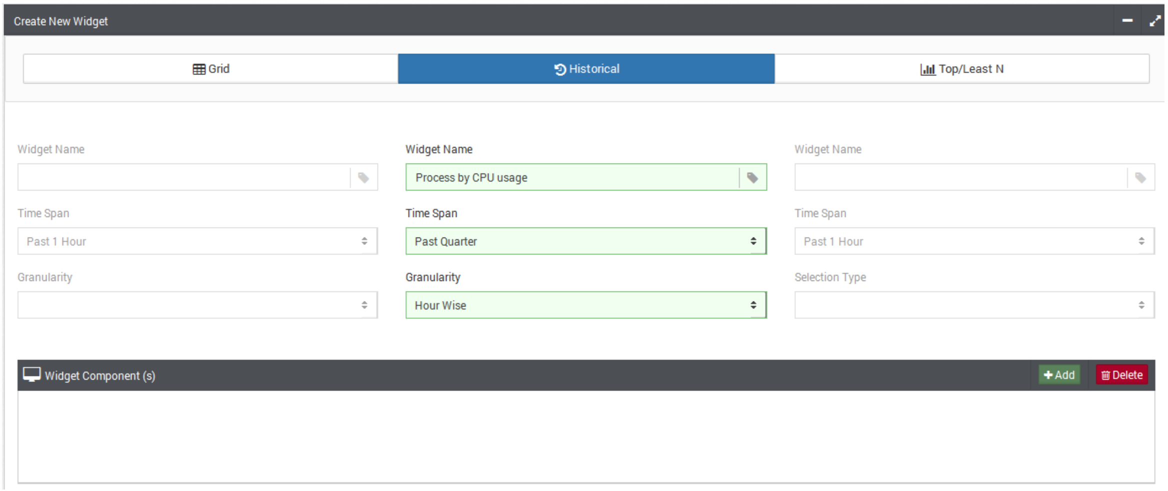
	Widget Name	Widget Type
□	Linux Server by LIVE PROCESSES	Top/Least N
□	Top 10 Windows Server PROCESS by MEMORY USAGE	Top/Least N
☑	Top 10 Windows Server PROCESS GRID by CPU USAGE	Top/Least N

Assigned Widgets

	Widget Name	Widget Type
🗑	Top 10 Windows Server PROCESS GRID by CPU USAGE	Top/Least N

Figure 9.4 Custom Windows Process Report using default widgets

Note: If the required data widget is unavailable, you can add new one by click on +New button in the same page.



Create New Widget

Widget Name:

Time Span: Past 1 Hour

Granularity:

Widget Name: Process by CPU usage

Time Span: Past Quarter

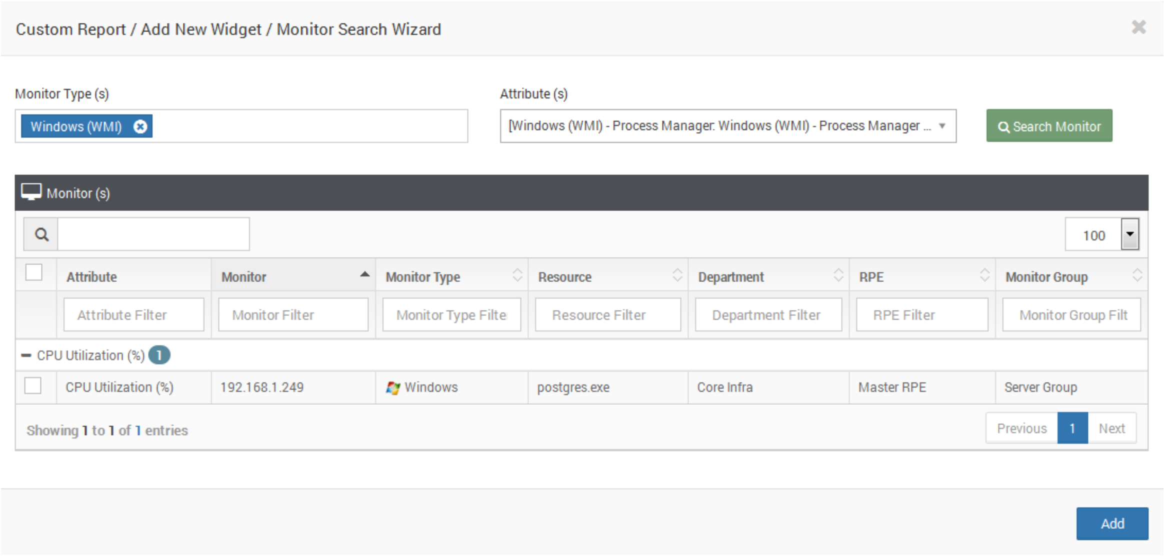
Granularity: Hour Wise

Widget Name:

Time Span: Past 1 Hour

Selection Type:

Figure 9.4 Creating Custom Data Widget for Windows Process



Custom Report / Add New Widget / Monitor Search Wizard

Monitor Type (s): Windows (WMI)

Attribute (s): [Windows (WMI) - Process Manager: Windows (WMI) - Process Manager ...

☐	Attribute	Monitor	Monitor Type	Resource	Department	RPE	Monitor Group
	Attribute Filter	Monitor Filter	Monitor Type Filte	Resource Filter	Department Filter	RPE Filter	Monitor Group Filt
− CPU Utilization (%) 1							
☐	CPU Utilization (%)	192.168.1.249	Windows	postgres.exe	Core Infra	Master RPE	Server Group

Showing 1 to 1 of 1 entries

Fig. 8.4.3 Assign Monitor/Attributes to Data Widgets

5. In case of new custom widget – choose the data manner to represent the data.
6. Assign Monitor/Attributes to widget by click in Add button.
7. Create the Report.
8. 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.

9.5. 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.

10. 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.

To create Alarm Ticket and Help Desk Ticket refer **section 14** in **User Manual**

Contacting MindArray Support Team

Customer Support
Support@mindarraysystems.com