

## Page Title: configure-the-monitoring-time-period

On this page

Configure the Monitoring Time-period

Overview

â€œ

By default, Motadata is in an active monitoring state 24

\*

7, that is, Motadata carries out data-polling all the time.

But you may not want the monitoring to be done all the time or be notified with alerts outside of your business hours. Motadata takes care of this by allowing you to configure the active monitoring hours in which the data polling is done.

Navigation

â€œ

Go to Menu, Select

Settings

. After that, go to

Monitoring

. Select

Monitoring Hour

. The screen to change the monitoring hours of Motadata AIOps is now displayed.

Click on the

button. The screen asking for your inputs to configure a new monitoring hour is displayed.

Enter the

Monitoring Hour Name

Select the time and days as per the monitoring window you want to configure.

Select the

Reset

button to erase all the current field values, if required.

Select

to create the monitoring hour as per your requirement.

A monitoring hour is now created.

Use-Case

â€œ

Changing the monitoring hour for particular monitor(s):

There might be a case where you want a monitor to be monitored during a specific time period. You can create a monitoring hour accordingly.

The monitoring hour you just created has to be assigned to the monitor using the Edit monitor option from

Device/Cloud/Agent/Service Check Monitor Settings.

Select

Monitoring Hour

to assign the monitor hour to the monitor selected.

Changing the monitoring hour in bulk for multiple devices:

There might be a case where you want multiple monitors to be monitored during a specific time period. You might even want all the monitoring to be done at a time period totally different from the default time. You can create a monitoring hour accordingly.

The monitoring hour you just created has to be assigned to the monitors using the bulk update option. Navigate to

Device/Cloud/Agent/Service Check Monitor Settings

Select all the monitors to which you want to assign the monitoring hour using the check-box in front of the monitor.

Select

Monitoring Hour

to assign the monitor hour in bulk to all the monitors selected.

## Page Title: configuring-a-monitor-maintenance-window

On this page

Configuring a Monitor Maintenance Window

Overview

â€‹

Motadata AIOps is equipped with a feature that allows you to identify if a particular monitor is under maintenance. Once you mark the monitor as under maintenance, the monitor is turned off for further surveillance.

Navigation

â€‹

Go to Menu, Select

Settings

.After that, Go to

Monitoring

. Select

Device\Cloud\Agent\Service Check Monitor Settings

based on the monitor you want to indicate under maintenance.

Navigate to the monitor you want to indicate under maintenance. Under the Actions tab, select to display the dropdown menu as displayed below.

Turning Maintenance ON/OFF

â€‹

Select

On Maintenance

to indicate that maintenance is underway for a monitor. This will change the status of the monitor

from

Enable

to

Maintenance

.

This means the monitor is no longer under surveillance by Motadata AIOps.

Select

Off Maintenance

to indicate that the maintenance is no longer running for a monitor. This will change the status of the monitor from

Maintenance

to

Enable

.

This means the monitor is once again under surveillance by Motadata AIOps.

How to schedule Maintenance window for a monitor?

â€‹

Motadata AIOps allows you to create a maintenance schedule for a monitor which would allow the maintenance to be scheduled as per your custom schedule at specified time intervals in the future.

Navigate to the monitor to schedule its maintenance. Under the

Actions

tab, select

to display the dropdown menu as displayed below.

Select

Schedule Maintenance

to display a scheduler pop-up as shown below.

Fill in the details in the pop-up to create a scheduler. The following parameters are present in the pop-up:

On Maintenance

Field

Description

Start Date

Select the date at which the maintenance is scheduled to start.

Hours

Select the time at which the maintenance is scheduled to start.

Off Maintenance

Field

Description

Start Date

Select the date at which the maintenance is scheduled to end.

Hours

Select the time at which the maintenance is scheduled to end.

Scheduler Type

Option

Description

Once

Select this field to schedule the maintenance only once.

Daily

Select this field to schedule the maintenance to run daily.

Weekly

Select this field to schedule the maintenance to run on a weekly basis:

-

Days:

Select the days of a week when the maintenance will run.

Monthly

Select this field to schedule the maintenance to run on monthly intervals.

-

Months:

Select the months when the maintenance will run in the selected time period.

-

Dates:

Select the dates when the maintenance will run in the selected time period.

Select

Schedule

once all the details are filled out. The Maintenance Schedule is now set up as per the specified parameters.

## Page Title: custom-monitoring-fields

On this page

Custom Monitoring Fields

Overview

â€‹

In our AIOps product, you have the flexibility to add a custom monitoring field with a fixed value to the monitors. This custom field can be used for grouping or tagging purposes to filter out certain monitors as per your requirement.

For example, if you have multiple monitors located at a particular location, you can add a custom field at the monitor level to mention the location of monitors. By creating a custom field with a fixed value, you can assign the field to all the monitors discovered from that particular location. The field will then be available to view against these monitors on the Monitor Screen, as well as the

Device/Agent/Cloud/Service Monitor Settings

Screen.

This feature allows you to customize your monitoring needs and organize your monitors in a more efficient manner.

Navigation

â€‹

Go to Menu, Select

Settings

. After that, go to

Monitoring

. Select

Custom Monitoring Field



. The screen to manage the custom monitoring fields is now displayed.

## Custom Monitoring Field Screen

â€œ

The fields displayed on the screen:

Field

Description

Field Name

The name of the custom field.

Actions

Select

to display permissible actions for the

Custom Monitoring Fields

. The following actions are available:

-

Edit Custom Monitoring Field

: Select this button to edit the custom monitoring field.

You can then add this field against a monitor in the

Device/Agent/Cloud/Service Check Monitor settings

. Select the

Edit

option. After that click on

Add Custom Monitoring Field

to add the custom field to the selected monitor.

## Page Title: file-and-directory-monitoring

On this page

File and Directory Monitoring

Overview

â€‹

Motadata enables you to monitor a file or a directory from a monitor (in this case, the monitor would be a server, whether virtual or non-virtual).

The metrics related to a file or a directory can be made available for monitoring by adding its path to the

File/Directory Monitor Settings

and then running discovery through

Rediscover Settings

.

When you run a

rediscovery for File/Directory

, any paths that you have added in the

File/Directory Settings

section will be discovered and monitored for the selected monitors.

Navigation

â€‹

Go to Menu, Select

Settings

. After that, Go to

Monitoring

. Select

File/Directory Monitor Settings

to display the list of all the processes in the system.

File/Directory List

â€œ

The

File/Directory Monitor Settings

displays the following fields:

Field

Description

Path

The path of the file/directory that can be monitored.

Type

Indicates whether the path belongs to a

File

or a

Directory

.

OS Type

The type of operating system to which the File or the Directory belongs. This is further categorized into the following:

- Windows

- Linux

- IBM AIX

Actions

Select

to display permissible actions on the

## File/Directory

. The following actions are available:

-

### Edit File/Directory

: Select this button to edit the file/directory.

-

### Delete File/Directory

: Select this button to delete the file/directory.

How to add a new File or Directory for monitoring?

â€œ

Select the

button. A new entry is created in the File/Directory list.

Enter the following details to add a File/Directory for monitoring:

Field

Description

Path

Enter the path of the directory or the file that you want to monitor.

Type

Select whether you want to monitor a File or a Directory.

OS Type

Select the operating system of the monitor to which the file or the directory belongs.

Select

to add the path to the list for monitoring.

Select

if you do not wish to add the path to the list for monitoring.

## Page Title: how-to-delete-a-monitor

On this page

How to delete a Monitor?

Overview

â€‹

Motadata AIOps allows you to delete a monitor. Once deleted, the monitor will not be available for further use in the system.

Navigation

â€‹

Go to Menu, Select

Settings

. After that, Go to

Monitoring

. Select

Device\Cloud\Agent\Service Check Monitor Settings

based on the monitor you want to delete.

Navigate to the monitor you want to delete. Under the

Actions

tab, select

to display the dropdown menu as displayed below.

Select

Delete

from the drop-down menu. A pop-up to confirm the deletion of the monitor is displayed as follows:

Select

Yes

to delete the monitor from the system.

Select

No

if you do not wish to delete the monitor from the system.

**Page Title: how-to-edit-monitor-properties**

On this page

Edit Monitor Details

Overview

â€‹

Motadata AIOps allows you to edit certain values of a monitor from the Monitoring Settings console.

Navigation

â€‹

Go to Menu, Select

Settings

. After that, Go to

Monitoring

. Select

Device\Cloud\Agent\Service Check Monitor Settings

based on the monitor you want to edit.

Navigate to the monitor you want to edit. Under the

Actions

tab, select

to display the dropdown menu as displayed below.

How to edit the Monitor details?

â€‹

Select

Edit

from the drop-down menu. A pop-up displaying the details of the monitors is displayed as shown in the picture below.

You can edit the monitor fields as required.

Select the

Reset

button to erase all the current field values, if required.

Select the

Update Monitor

button to save the changes you have made to the monitor fields.



## Page Title: monitor-rediscovery

On this page

Monitor Rediscovery

Overview

â€‹

Motadata AIOps allows you to discover specific instances within monitors for further monitoring by running rediscovery on monitors. Suppose, you have setup a device as monitor in Motadata AIOps. After setting up this device as Monitor, your IT department decides to add a new instance to the device. This instance needs to be configured for monitoring and could be discovered through an execution of a Rediscovery Scheduler.

Types of Instances you can Rediscover in AIOps

â€‹

The following instances are available for Rediscovery:

Application

Cloud

Virtualization

Interface

Process

Service

File/Directory

Hyperconverged Infrastructure (HCI) Cluster

Hyperconverged Infrastructure (HCI) VM

We will look into each of the above instances in detail in a while. Let us first look into how we can configure and schedule a rediscovery run.

Rediscovery Scheduler

â€‹

Let us see how we can schedule a rediscovery. The parameters to configure and schedule a rediscovery for all the type of instances mentioned above are same.

AIOps allows you to schedule the rediscovery for each instance individually so that no new EC2 instances are rediscovered within an AWS monitor if you are only looking to rediscover all the virtual devices within an ESXi. This allows you to have control on the type of instance you need to rediscover.

Navigation

â€‹

Go to the Main Menu, Select

Settings

. After that, Go to

Monitoring

. Select

Rediscover Settings

. The screen to rediscover the instances within a monitor is now displayed.

Here, you can configure a scheduler to run for rediscovery.

Monitor Rediscover Settings Screen

â€‹

The following details for the created schedulers are available on the Rediscover Settings Screen:

Field

Description

Scheduler Type

The frequency at which the scheduler is configured to run.

Start Date

The start date at which the scheduler is configured to run.

## Triggers

The start time at which the scheduler is configured to run.

## Monitors

The monitor for which the scheduler is configured to run.

## Result

The details of the last scheduler run and the discovered instances can be viewed here by clicking on the

View Details

button.

## Actions

The following actions are available to be taken on any scheduler

-

Turn scheduler On/Off

: Select

to toggle the scheduler

On/Off

-

Run scheduler instantly

: Select

to run the scheduler instantly.

-

Edit/Delete scheduler

: Select

to view the options to delete or edit the scheduler.

## How to Schedule a Rediscovery?

â€œ

Select the instance(Application, Cloud, Virtualization etc.) for which you want to schedule a

rediscovery. Now, Select

to schedule a rediscovery.

A pop-up to create the schedule is then displayed.

Enter the following details to create the scheduler:

Field

Description.

Monitors

Select the Monitor for which you want to run the rediscovery. The rediscovery scheduler will run and rediscover new instances on this monitor.

Scheduler Type

Select the frequency at which you want the scheduler to be executed.

Start Date

Select the date when you want the rediscovery to run first.

Hours

Select the time when you want the rediscovery to run. You can even select multiple times as per your requirement.

Notify via Email

Enter the email address of the recipient to be notified after a successful rediscovery run. Once you have entered the email address, click

to save the email address. After saving the email address, you can go ahead and enter more email addresses if needed.

Notify via SMS

Enter the contact number of the recipient to be notified after a successful rediscovery run. Once you have entered the email address, click

to save the email address. After saving the contact number, you can go ahead and enter more email addresses if needed.

Auto-Provision

Check this option if you want to provision all the instances automatically that are discovered after a successful rediscovery run.

Select

Reset

to erase all the current field values, if required.

Select

Create Scheduler

to create the scheduler as per the parameters you entered.

Now, let us look into each instance in detail.

Rediscover Application instances

â€‹

Use-Case

â€‹

Suppose you have provisioned a server as a monitor. Once the monitor is provisioned, you decide to setup a Oracle DB instance on the server. Now, you want to monitor this database instance using AIOps.

Adding the Oracle Database instance as a Monitor

â€‹

This could be done by running a rediscovery from the

Application Scheduler

.

After running the Application rediscovery, you can see the list of all the new applications from all the monitors in the system. This is the list of all the instances that were setup in the devices after they are provisioned as monitors.

note

In case you want to monitor an application from a server that is not setup as a monitor, you first need to setup that server as a monitor. Once that server is setup as a monitor, you can then go

ahead and execute a rediscovery run to monitor the application on that server.

note

In order to rediscover an application present on a Windows server, the corresponding process and service should be available in the

Process Monitor Settings

and

Service Monitor Settings

respectively. In case the corresponding process and service are not already added, you can create a new record of these process and service and then execute a rediscovery run to monitor the application.

Here, you can see that the Oracle Database is available to be discovered on a server. In case Oracle Database is installed on multiple servers and you execute a rediscovery run, you will be able to see multiple instances of Oracle Database on the screen along with the server IP on which it is installed.

Select the

Oracle Database

to rediscover the Oracle DB instance.

A pop-up to set up the discovery profile for the Oracle DB instance is now displayed.

Enter the credential details for the oracle DB and run the discovery.

The following pop-up is displayed once the discovery runs:

Select

Add Instance

to add the database instance for discovery.

The database instance is now added to the system for monitoring and is setup as a monitor. You can view the database instance added to the

Monitors

screen as follows:

Rediscover Cloud instances

â€‹

Use-Case

â€‹

Suppose you have provisioned a AWS device as a monitor. Once the monitor is provisioned, you decide to setup a new EC2 instance on the device. Now, you want to monitor this EC2 instance using AIOps.

Adding the new EC2 instance as a Monitor

â€‹

This could be done by running a rediscovery from the

Cloud Scheduler

.

After running the Cloud rediscovery, you can see the list of all the new instances from all the monitors in the system. This is the list of all the instances that were setup in the devices after they are provisioned as monitors.

Here, you can see that new EC2 instances are available to be discovered on multiple monitors.

Select

from the

Action

column to rediscover the EC2 instance that you need to monitor.

The EC2 instance is now added to the system for monitoring and is setup as a monitor. You can view the EC2 instance added to the

Monitors

screen as follows:

Rediscover Virtualization instances

â€‹

Use-Case

â€‹

Suppose you have provisioned an ESXi as a monitor. Once the monitor is provisioned, you decide to setup new virtual machines on that ESXi. Now, you want to monitor the new virtual machines using AIOps.

Adding the new virtual machines as a Monitor

â€‹

This could be done by running a rediscovery from the  
Virtualization Scheduler

.

After running the Virtualization rediscovery, you can see the list of all the new instances from all the monitors in the system. This is the list of all the instances that were setup in the devices after they are provisioned as monitors.

Here, you can see that new virtual machines are available to be discovered on multiple monitors.

Select

from the

Action

column to rediscover the virtual machines that you need to monitor.

The virtual machine is now added to the system for monitoring and is provisioned as a monitor. You can view the virtual machines added to the

Monitors

screen as follows:

Rediscover Interfaces

â€‹

Use-Case

â€‹

Suppose you have provisioned a switch as a monitor. Suppose there are specific interfaces within the switch that you want to monitor or you want to monitor the interfaces within the VLAN setup in a



switch.

Adding the interfaces as a Monitor

â€œ

This could be done by running a rediscovery from the

Interface Scheduler

.

After running the Interface rediscovery, you can see the list of all the interfaces from all the devices provisioned as monitors in the system.

Here, you can see all the interfaces that are available to be discovered on multiple monitors.

Select

from the

Action

column to rediscover the interfaces that you need to monitor.

The interface is now added to the system for monitoring and is provisioned as a monitor. You can view the interfaces added to the

Monitors

screen as follows:

Rediscover Processes

â€œ

Use-Case

â€œ

Suppose you have provisioned a Windows server as a monitor. Now, there might be specific processes within the server that you want to monitor.

Adding the Process as a Monitor

â€œ

This could be done by running a rediscovery from the

Process Scheduler

.

After running the Interface rediscovery, you can see the list of all the processes from all the Windows server provisioned as monitors in the system.

Here, you can see all the processes that are available to be discovered on multiple monitors.

note

A process can only be discovered if that process is already added to

Process Monitor Settings

. Processes that are most often used are already added in the

Process Monitor Settings

. In case you need to monitor a process that is not already added, you can create a new record of that process in the

Process Monitor Settings

and then execute a rediscovery run to monitor the process.

Select

from the

Action

column to rediscover the interfaces that you need to monitor.

The process is now added to the system for monitoring and is provisioned as a monitor. You can view the processes added to the

Monitors

screen as follows:

Rediscover Services

â€œ

Use-Case

â€œ

Suppose you have provisioned a Windows or a Linux server as a monitor. Now, there might be specific services within the server that you want to monitor.

Adding the service as a Monitor

â€‹

This could be done by running a rediscovery from the

Service Scheduler

.

After running the Interface rediscovery, you can see the list of all the services from all the servers provisioned as monitors in the system. We will provision the service highlighted below.

Here, you can see all the services that are available to be discovered on multiple monitors.

note

A service can only be discovered if that service is already added to

Service Monitor Settings

. Services that are most often used are already added in the

Service Monitor Settings

. In case you need to monitor a service that is not already added, you can create a new record of that service in the

Service Monitor Settings

and then execute a rediscovery run to monitor the service.

Select

from the

Action

column to rediscover the interfaces that you need to monitor.

The service is now added to the system for monitoring and is provisioned as a monitor. You can view these services added to the Monitors screen as follows:

Rediscover File/Directory

â€‹

Use-Case

â€‹

Suppose you have provisioned a Windows or a Linux server as a monitor. Now, there might be specific files or directories within the server that you want to monitor. You might need to make sure that the size of a file does not exceed a certain limit or you might need to monitor the content of a certain file.

Adding the File/Directory as a Monitor

â€“

This could be done by running a rediscovery from the  
File/Directory Scheduler

.

Now, Before you run a rediscovery for file/directory you need to make sure that the file/directory you want to monitor is added to the

File/Folder Monitor Settings

.

Go to the Main Menu, Select  
Settings

. After that, Go to

Monitoring Settings

. Select

File/Folder Monitor Settings

.

Select the

Create File/Directory List

and add the file/directory path that you want to monitor on this screen.

Once the path is added to the

File/Folder Monitor Settings

, you can run the interface resdiscovery for

File/Directory

.

After running the interface rediscovery, you can see the list of all the files/directories added in

File/Folder Monitor Settings

from all the monitors specified in the rediscovery scheduler.

Here, you can see all the files/directories that are available to be discovered on the specified monitors in the scheduler.

Select

from the

Action

column to rediscover the file/directory that you need to monitor.

The file/directory is now added to the system for monitoring and is provisioned as a monitor. You can view the processes added to the Monitors screen.

Rediscover Hyperconverged Infrastructure (HCI) Cluster

â€‹

Use Case

â€‹

Suppose you have provisioned an HCI device (Prism) as a monitor. Now, there could be a specific cluster within that Prism that you wish to add as a monitor.

Adding an HCI Cluster as Monitor

â€‹

This could be done by running a rediscovery from the

HCI scheduler

.

After running the HCI rediscovery, you can see the list of all new clusters for the specific Prism in the system. The list comprises of all the clusters that were set up in the Prism after it was provisioned as

a monitor.

Here, you can see multiple clusters are available to be discovered.

Select

from the

Action

column to rediscover and provision the HCI Cluster that you need to monitor.

The HCI Cluster is now added to the system for monitoring and is setup as a monitor. You can view the HCI Cluster added to the

Monitor

screen.

Rediscover Hyperconverged Infrastructure (HCI) Virtual Machine (VM)

â€œ

Use Case

â€œ

Suppose you have provisioned an HCI AHV (Host) as a monitor. Now, there could be a specific Virtual Machine (VM) within that Host that you wish to add as a monitor.

Adding an HCI VM as a Monitor

â€œ

This could be done by running an rediscovery from the

HCI scheduler

.

After running the HCI rediscovery, you can see the list of all new VMs for the specific Host in the system. This list comprises of all the virtual machines that were set up in AHV (Host) after it was provisioned as a monitor.

Here, you can see multiple clusters are available to be discovered.

Select

from the

## Action

column to rediscover and provision the HCI VM that you need to monitor.

The HCI VM is now added to the system for monitoring and is setup as a monitor. You can view the HCI VM added to the

## Monitor

screen.

## Page Title: monitor-screen

On this page

### Monitoring Your Infrastructure

In the world of IT infrastructure management, having a real-time understanding of the health and performance of your systems is essential. Motadata AIOps introduces the Monitors, a way to provide comprehensive insights into your IT environment, empowering you to proactively manage and optimize your infrastructure.

Monitors play a pivotal role in enabling real-time monitoring and generating insightful performance metrics. With Motadata AIOps, you can monitor a wide range of infrastructure elements, from servers and networks to cloud resources, services, and more. By categorizing monitors based on their infrastructure type, you gain a structured view of your IT landscape.

### Navigation

â€‹

Go to the Main Menu. Select

. The screen to view the monitor details is displayed.

### Monitor Screen

â€‹

Let's explore the Monitors screen in detail, including how monitors are categorized by infrastructure, utilize predefined templates, and harness the power of real-time monitoring insights to maintain a resilient and high-performing IT environment.

### Monitors Categorization Based on Infrastructure

â€‹

In Motadata AIOps, effective monitoring begins with a clear and organized view of your IT infrastructure. The Monitors Categorization Based on Infrastructure allows you to categorize and manage monitors according to different types of infrastructure. This categorization simplifies the process of monitoring and provides quick access to the monitor you need.



Infrastructure Category

Description

Server & Apps

Monitors related to your servers and applications.

Network

Monitors related to your network devices.

Cloud

Monitors related to cloud infrastructure monitoring

Service Check

Monitors for service checks.

Virtualization

Monitoring related to virtualized environments.

Service

Monitors specific to services.

Process

Monitors related to processes.

Interface

Monitors for interfaces.

Other

Additional monitors that may not fit into the above categories.

Actions available on the Monitors Screen

â€‹

For each infrastructure category, you'll find a list of monitors available for monitoring. On each of these screens, you can perform the following actions:

Action

Description

Export

Export the list of monitors in CSV or PDF format for reference.

## Filter

Easily filter the list of monitors based on details such as alert severity and monitor type.

## Set Tag as a Column

Select this option add

key:value based tags

as a column to the monitor details. The Key will be listed as the column name and the value will be available against each monitor under this column based on the value of the tags.

## Reset Column Preference

â€‹

To reset column preference and unhide all hidden columns on the Monitor screen, click on the 'eye' icon and choose the

## Reset Column Preference

option.

## Predefined Templates to View Monitor Details

â€‹

Motadata AIOps offers a range of predefined templates tailored to each infrastructure category and device type. These templates provide you with an instant overview of essential monitoring details.

The goal is to simplify monitoring, ensuring that you have the right information at your fingertips.

When you drill down on a specific monitor, you can view the more details related to that monitor.

The following details are available on the screen

### Metrics Overview

: Get an overview of critical metrics related to the state of each monitor on the pre-defined monitor templates created uniquely based on the infrastructure type to cater to your specific monitoring needs.

### Metric Explorer

: Drill down on a monitor to analyze its metrics using the Metric Explorer tab.

## Active Policies

: See which policies have been created for a particular monitor.

## Actions available for individual monitors

â€‹

When you drill down on a specific monitor, you'll discover a set of actions designed to enhance your monitoring capabilities:

### Poll Now

: Instantly poll metrics related to the monitor.

### SSH Terminal

: Select this option to open an SSH terminal for the monitor. This feature allows you to establish a secure SSH connection to the device directly from the monitor screen, enabling real-time command-line interactions.

### Execute Runbook

: Select this option to execute a Runbook assigned to the selected monitor. The list of all the runbooks assigned to the monitor will be displayed once you click on this button. You can then execute the Runbook that you wish to execute.

### Export

: Export the predefined template as an image in PNG format.

### View More

: Access additional details about the monitor such as the

### Summary

,

### Polling Info

,

### Triggered Policies

, and

### Action History

, tailored to its infrastructure type.

## Dashboard Overview for Each Infrastructure Category

â€‹

Select the

icon to view the dashboard overview screen related to that infrastructure.

The Dashboard overview provides a comprehensive view of each infrastructure category. You can monitor and manage your infrastructure effectively with the following insights available on the dashboard screen:

### Total Monitor Count

: See the total number of monitors present in each infrastructure category on the 'Health Overview' widget.

### Alert Severity

: Check the number of monitors in each alert severity category for each monitor group.

### Highest Severity Alerts

: Drill down on the heat map to view details about the highest severity alerts raised for each monitor.

With Monitors Categorization Based on Infrastructure, Motadata AIOps empowers you to efficiently organize, monitor, and manage your IT infrastructure, ensuring the smooth operation and proactive management of your environment.

## Page Title: monitor-settings

On this page

### Monitor Settings

The Monitor Settings section in Motadata AIOps provides you with comprehensive configuration and management options for monitors, agents, processes, and services that are discovered within the system. This screen serves as a centralized hub for fine-tuning the monitoring settings and optimizing the monitoring experience.

Effectively manage the agents installed on devices for agent-based monitoring. Monitor Settings enables you to view agent status, update existing agents, and more.

Gain granular control over the monitoring of processes and services running on your devices. Configure specific processes and services to be monitored.

Configure scheduled topology scans to maintain an up-to-date visual representation of your network infrastructure. Topology scans provide insights into the relationships and dependencies among devices, enabling better understanding and troubleshooting of network issues.

By leveraging the Monitor Settings in Motadata AIOps, you can fine-tune the monitoring parameters, ensure efficient agent management, monitor critical processes and services, automate rediscovery, and maintain an accurate network topology. These capabilities empower you to proactively manage your IT environment, identify and resolve issues promptly, and optimize the performance and availability of your infrastructure.

### Device Monitor Settings

â€‹

The list of all the Monitors discovered in the system can be viewed under Device Monitor Settings. The monitors can be configured and managed from this screen.

Go to the Main Menu, Select

Settings

. After that, go to

Monitoring Settings

. Select

Device Monitor Settings

. The list of all the monitors that are discovered in the system is now displayed.

The Device Monitor Settings screen displays the following details:

Field

Description

Monitor

The name of the monitor.

IP

The IP address of the monitor.

Host

The hostname of the monitor, if available. The IP address is displayed in case the hostname is not present.

Groups

The group under which the monitor is categorized.

Type

The type of device infrastructure.

Apps

The application detected in a monitor after rediscovery.

Status

The status of the monitor on the following basis:

-

Enable

: The Monitor is switched ON for monitoring.

-

Disable

: The Monitor is switched OFF for monitoring.

-

Maintenance

: The Monitor is under Maintenance and it will not be monitored.

Actions

Select

to display permissible actions for the monitor:

-

Disable

/

Enable

: This button is used to turn

OFF/ON

a monitor.

-

ON/OFF Maintenance

: This button is used to switch the monitor maintenance status to

ON/OFF

.

-

Schedule Maintenance

: This button is used to schedule the maintenance activity of a particular monitor in advance.

-

Metric Settings

: This button is used to configure the metric polling configuration for each monitor.

-

Edit

: This button is used to edit the Monitor details.

-

Delete

: This button is used to delete a particular monitor from the system.

You can also use the bulk update option to make changes to multiple monitors at once.

Agent Monitor Settings

â€‹

The list of all the agents installed in your infrastructure can be viewed under

Agent Monitor Settings

. The agents can be configured and managed from this screen. You can also view the health status of agent on this screen

Go to Menu, Select

Settings

. After that, go to Monitoring . Select

Agent Monitor Settings

. The list of all the agent monitors in the system is now displayed.

The Agent Monitor Settings screen displays the following details:

Field

Description

Monitor

The name of the agent.

IP

The IP address of the agent.

Health



This field provides an at-a-glance indication of the overall health status of the agent. By hovering over individual executable (.exe) files related to metrics, logs, and packet, and Event Log(for Windows) you can obtain specific health information for each category.

#### Groups

The group under which the monitor is categorized.

#### Type

The type of device infrastructure.

#### State

Indicates the connectivity of the agent with Motadata AIOps server.

#### Duration

This field shows the time since which the MotaAgent is in the current

#### Status

#### Status

The status of the monitor on the following basis.

-

#### Enable

: The Monitor is switched ON for monitoring.

-

#### Disable

: The Monitor is switched OFF for monitoring.

-

#### Maintenance

: The Monitor is under Maintenance and it will not be monitored.

#### Version

The version of the MotaAgent.

#### Configuration

Click on

View Details

to configure metric and log polling configuration. You can check more details about this  
here

Actions

Select

to display permissible actions for the monitor

Cloud Monitor Settings

â€‹

The list of all the monitors discovered in the system that belong to a cloud network can be viewed  
under

Cloud Monitor Settings

. The monitors can be configured and managed from this screen.

Go to Menu, Select

Settings

. After that, go to

Monitoring Settings

. Select

Cloud Monitor Settings

. The list of all the monitors that belong to cloud network is now displayed.

The Cloud Monitor settings screen displays the following details:

Field

Description

Monitor

The name of the monitor.

Resource/Region

The region to which the monitor belongs

Account ID

The account ID to which the monitor belongs

Groups

The group under which the monitor is categorized.

Type

The type of device infrastructure.

Status

The status of the monitor on the following basis.

-

Enable

: The Monitor is switched ON for monitoring.

-

Disable

: The Monitor is switched OFF for monitoring.

-

Maintenance

: The Monitor is under Maintenance and it will not be monitored.

Actions

Selecting

displays permissible actions for the monitor :

-

Disable

/

Enable

: This button is used to turn OFF/ON a monitor.

-

## ON/OFF Maintenance

: This button is used to switch the monitor maintenance status to ON/OFF.

-

## Schedule Maintenance

: This button is used to schedule the maintenance activity of a particular monitor in advance.

-

## Metric Settings

: This button is used to configure the metric polling configuration for each monitor.

-

## Edit

: This button is used to edit the Monitor details.

-

## Delete

: This button is used to delete a particular monitor from the Motadata system.

You can also use the bulk update option to make changes to multiple monitors at once.

## Service Check Monitor Settings

â€œ

The list of all the service check monitors can be viewed under Service Check Monitor Settings. The monitors can be configured and managed from this screen.

Go to the Main Menu, Select

Settings

. After that, go to Monitoring

. Select

Service Check Monitor Settings

. The list of all the service check monitors present in the system is now displayed.

The

## Service Check Monitor Settings

screen displays the following details:

### Field

### Description

#### Monitor

The name of the monitor.

#### Type

The type of device infrastructure.

#### Groups

The group under which the monitor is categorized.

#### Target

The specific target for which you created the service check.

#### Status

The status of the monitor on the following basis.

-

#### Enable

: The Monitor is switched ON for monitoring.

-

#### Disable

: The Monitor is switched OFF for monitoring.

-

#### Maintenance

: The Monitor is under Maintenance and it will not be monitored.

#### Actions

#### Selecting

displays permissible actions for the monitor.

-

Disable

/

Enable

: This button is used to turn OFF/ON a monitor.

-

ON/OFF Maintenance

: This button is used to switch the monitor maintenance status to ON/OFF.

-

Schedule Maintenance

: This button is used to schedule the maintenance activity of a particular monitor in advance.

-

Metric Settings

: This button is used to configure the metric polling configuration for each monitor.

-

Edit

: This button is used to edit the Monitor details.

-

Delete

: This button is used to delete a particular monitor from the Motadata system.

You can also use the bulk update option to make changes to multiple monitors at once.

## Page Title: process-monitoring

On this page

Process Monitoring

Overview

â€œ

The

Process Monitoring Settings

is a pre-loaded repository of all the generic processes present in a server (virtual or bare-metal).

This feature allows you to monitor processes and

rediscover

applications easily. When you discover a server, AIOps checks if any of the processes present in this list are active in the server, and if so, these processes are provisioned as monitors.

The pre-loaded list covers most of the well-known processes you need to monitor, making it a comprehensive and efficient solution. However, you can add any specific processes that you want to monitor, giving you complete control over the monitoring process. Once you add a process to the list, you can start monitoring it by executing a rediscovery run.

The list of processes and

services

also helps you rediscover applications. This is a crucial aspect of the monitoring process, as it ensures that you can easily detect and monitor instances within a monitor.

To rediscover an application present on a Windows server, the corresponding process and service should be available in the

Process Monitoring Settings

and

Service Monitoring Settings

, respectively. If they are not already present, you can create a new record for these processes and

services and then execute a rediscovery run to monitor the application.

To rediscover an application present on a Linux server, the corresponding process should be available in the

### Process Monitoring Settings

. If it is not already present, you can create a new record for these processes and then execute a rediscovery run to monitor the application.

Overall, the Process Monitoring feature enables you to monitor your processes and applications effectively, ensuring that your infrastructure is always running smoothly. For more information about rediscovery, please refer to

this guide

.

### Navigation

â€‹

Go to Menu, Select Settings

. After that, Go to

Monitoring

. Select

Process Monitor Settings

to display the list of all the processes that are available in the system.

Process List Screen

â€‹

The Process List screen displays the following fields:

Field

Description

Process

The name of the process that can be monitored.



## Application Type

The type of application to which the process belongs.

## OS Type

The type of operating system to which the process belongs. This is further categorized into the following:

- Windows
- Linux
- IBM AIX

## Actions

### Select

to display permissible actions for the process. The following actions are available for each process:

-

### Edit Process

: Select this button to edit the process name, application type, and OS type of the process.

-

### Delete Process

: Select this button to delete the process from the system.

## How to add a new process for monitoring?

â€œ

Motadata AIOps allows users to add a process to the existing process list in case a certain process that you need to monitor is not already present in the existing process list in the the system.

### Select

present above the list of processes. A new entry is created in the process list.

Enter the following details to create a new process:

### Field

### Description

### Process

Please enter the name of the new process you want to add to Motadata AIOps. This is the name of the process as present in the actual server which is set up as monitor.

Application Type

Select the application type to which this process belongs from the drop down.

OS Type

Select the OS to which this process belongs from the drop down.

Select

to add this process to the process list.

Select

if you do not wish to add this process to the process list.

## Page Title: service-monitoring

On this page

Service Monitor Settings

Overview

â€‹

The

Service Monitoring Settings

is a pre-loaded repository of all the well-known services present in a server (virtual or bare-metal).

This feature allows you to monitor services and

rediscover

applications easily. When you discover a server, AIOps checks if any of the services present in this list are running on the server, and if so, these services are provisioned as monitors.

The pre-loaded list covers most of the well-known services you need to monitor, making it a comprehensive and efficient solution. However, you can add any specific services that you want to monitor, giving you complete control over the monitoring process. Once you add a service to the list, you can start monitoring it by executing a rediscovery run.

The list of services and

processes

also helps you rediscover applications. This is a crucial aspect of the monitoring process, as it ensures that you can easily detect and monitor instances within a monitor.

To rediscover an application present on a Windows server, the corresponding process and service should be available in the

Process Monitoring Settings

and

Service Monitoring Settings

, respectively. If they are not already present, you can create a new record for these processes and

services and then execute a rediscovery run to monitor the application.

To rediscover an application present on a Linux server, the corresponding service should be available in the

### Service Monitoring Settings

. If it is not already present, you can create a new record for these services and then execute a rediscovery run to monitor the application.

Overall, the Service Monitoring feature enables you to monitor your services and applications effectively, ensuring that your infrastructure is always running smoothly. For more information about rediscovery, please refer to

this guide

.

### Navigation

â€‹

Go to Menu, Select

Settings

. After that, Go to

Monitoring

. Select

Service Monitor Settings

to display the list of all the processes that are pre-configured in the system.

Service List

â€‹

The Service List displays the following fields:

Field

Description

## Service

The name of the service that can be monitored.

## Application Type

The type of application to which the service belongs.

## OS Type

The type of operating system to which the service belongs i.e., Windows

## Actions

### Select

to display permissible actions on the service. The following actions are available for each service:

-

### Edit Service

: Select this button to edit the name, application type, and OS type of the service.

-

### Delete Service

: Select this button to delete the service from the system.

## How to add a new service for monitoring?

â€œ

Motadata AIOps allows users to add a service to the existing service list in case a certain service that you need to monitor is not present in the existing service list in the system.

### Select

present above the list of services. A new entry is created in the service list.

Enter the following details to create a new service:

### Field

### Description

### Service

Please enter the name of the new service you want to add to Motadata. This is the name of the service as present in the actual server which is set up as monitor.

### Application Type

Select the application type to which this service belongs from the drop down.

### OS Type

Select the OS to which this service belongs from the drop down.

Select

to add this service to the service list.

Select

if you do not wish to add this service to the service list.

## Page Title: snmp-device-catalog

On this page

SNMP Device Catalog

Overview

â€‹

The SNMP Device Catalog is a critical component in the process of discovering devices from network infrastructure. It is a repository of devices based on their OID, which is used during the discovery of devices in AIOps. When the discovery runs, the OID of the discovered devices is fetched using SNMP walk, and it is checked against the OIDs present in the catalog. Based on the match, a predefined template for monitoring in the monitoring screen and a monitor type are assigned to the discovered device, and it is then displayed in the monitor screen.

The SNMP Device Catalog screen not only contains the OID for the discovered devices, but it also includes the OID for the metrics that need to be monitored for all the network devices in the infrastructure.

Use-Case

â€‹

In some cases, you may want to monitor specific metrics that are not monitored by AIOps by default. This might be new metrics added by the device vendor or even some custom metrics that you might want to create based on certain manipulation of the metric OIDs. In such cases, you can create a new record in the SNMP Device Catalog, where you can map the device OID with the metric OID that you want to poll. This allows AIOps to start polling this metric from the next poll.

Overall, the SNMP Device Catalog screen plays a crucial role in ensuring that your AIOps product can accurately discover and monitor network devices in your environment. By correctly configuring the catalog, you can ensure that your AIOps product provides valuable insights into the health and performance of your infrastructure.

Navigation

â€‹

Go to the Main Menu, Select  
Settings

. After that, go to  
Monitoring Settings

. Select  
SNMP Device Catalog

. The SNMP Device Catalog screen is now displayed.

SNMP Device Catalog Screen

â€‹

Here's an overview of each field in the screen:

Field Name

Description

SNMP Device Catalog Name

This field contains the name of the SNMP device catalog. It is used to uniquely identify the catalog and differentiate it from other SNMP device catalogs.

Vendor

This field specifies the vendor of the device associated with the OID.

Type

This field specifies the type of device that is associated with the OID. For example, it could be a router, switch, firewall, or any other network device.

Used Count

This field indicates the number of times the SNMP device catalog has been used to discover devices in your infrastructure.

System OID



This field contains the system OID for the device associated with the OID. It is a unique identifier used to match the discovered devices during the discovery process.

#### Created By

This field specifies the user who created the SNMP device catalog.

#### Action

This field has three subtypes:

-

#### Edit SNMP Device Catalog

: This action allows you to edit the SNMP device catalog.

-

#### Clone SNMP Device Catalog

: This action allows you to create a new SNMP device catalog by cloning an existing one. You can use this feature to create a new SNMP device catalog with similar settings as an existing one, thereby saving time and effort.

-

#### Assign Monitors

: This action allows you to assign monitors to the SNMP device catalog.

By using the fields on the SNMP Device Catalog screen, you can manage and monitor the devices and metrics in your infrastructure accurately. By correctly configuring the catalog, you can ensure that your AIOps product provides valuable insights into the health and performance of your network infrastructure and helps you detect and resolve any issues proactively.

How to start monitoring a new metric for a device?

â€‹

SNMP Device Catalogs play a vital role in discovering and monitoring devices and metrics in an infrastructure. They contain information such as the device OID, vendor, and type, which is essential for your AIOps product to discover and monitor the devices accurately.

In some cases, a user might need to monitor specific metrics that are not monitored by AIOps. In

such cases, the user can create a new record in the SNMP Device Catalog and map the device OID with the metric OID. Once this is done, the AIOps product will start polling the new metric from the next poll.

Additionally, creating a new SNMP Device Catalog record is also useful when a user needs to monitor devices from a new vendor or type that is not already available in the existing SNMP Device Catalog. By creating a new record, the user can configure the settings specific to the new vendor or type and ensure that the AIOps product can monitor the devices accurately.

Therefore, creating a new SNMP Device Catalog record is a necessary step for users who want to monitor specific metrics or devices that are not already included in the existing SNMP Device Catalog. It allows users to customize and configure the settings as required and ensures that the AIOps product provides accurate insights into the health and performance of their infrastructure.

## Navigation

â€‹

Select

Create SNMP Device Catalog

to create a custom catalog.

Creating a Custom SNMP Device Catalog

â€‹

In Motadata AIOps, you can create a custom SNMP Device Catalog to monitor specific metrics or devices that are not covered by default. To set up a custom catalog, follow the steps below to fill up the necessary details

Field

Description

System OID

Enter the appropriate System OID for the device you want to monitor. The System OID uniquely identifies the device associated with the OID in the catalog.

Name

Provide a meaningful and descriptive name for the SNMP Device Catalog. This name will help you identify the catalog and differentiate it from others in your monitoring setup.

#### Vendor

Specify the vendor of the device associated with the OID. This information helps categorize the devices efficiently for better organization and management.

#### Type

Choose the type of device that is associated with the OID from the available options, such as router, switch, firewall, or other network devices. Selecting the correct device type is essential for accurate device discovery and monitoring.

#### OID Groups

The OID Groups section allows you to categorize the OIDs that need to be monitored.

#### OID Group Name

Each OID Group you create must have a unique name within the catalog. This name will be used to refer to the specific group, making it easier to manage and configure.

#### Scalar/Tabular

Select the appropriate OID type.

- Scalar OIDs represent single, discrete values. These values may include metrics like CPU utilization or memory usage, represented by specific OIDs.
- Tabular OIDs represent sets of related data, presented in a table format. These tables might include information about interfaces, network routes, etc.

#### OID Listing

Under each OID Group, you can list individual OIDs and their corresponding names.

#### OID Name

Assign a descriptive name to each OID, representing the metric or data you want to monitor. For example, you can use "CPU (%)" for CPU utilization.

#### OID

Provide the actual OID (Object Identifier) associated with the metric you want to monitor, e.g.,

1.3.6.1.4.1.9.2.1.58.0 for CPU utilization.

#### Choose OID

If you are unsure about the OID to use, you can utilize the "Choose OID" feature to browse and select from available OIDs supported by the device.

#### Add OID

Select this button to add another OID to the OID group.

Ensure to save your changes after filling up all the required details to create the custom SNMP Device Catalog. This catalog will then be used by Motadata AIOps to discover and monitor devices, along with the specified metrics, providing valuable insights into your network infrastructure's health and performance.

#### Testing the OID

â€œ

After listing all the OIDs and filling up the necessary details in the custom SNMP Device Catalog, it is essential to ensure that the OIDs are correctly configured and can be successfully polled for metrics. Review the listed OIDs to ensure they are accurate and match the metrics you intend to poll.

#### Test OID Group

Once you have verified the OIDs, click on the "Test OID Group" button. A new screen will appear, displaying all the listed OIDs within the OID group you created.

#### Select Parent OID Group

Select the OID that you want to set up as the parent OID for the listed OIDs in the group. The parent OID helps in structuring the OIDs logically, especially when dealing with tabular data or hierarchical metrics.

After selecting the parent OID, click on the

#### Select Parent OID

button.

#### Confirm and Create SNMP Device Catalog

After selecting the parent OID, carefully review all the OID values and their associations. If everything looks correct and validated, proceed to click on the "Create SNMP Device Catalog" button. This will save your custom SNMP Device Catalog with the configured OIDs and their relationships.

By testing the OID values before creating the catalog, you can ensure that the OIDs are functioning correctly and can be polled for the desired metrics. This step is crucial in avoiding potential issues during device discovery and monitoring.

Once the custom SNMP Device Catalog is created, Motadata AIOps will use this catalog to discover and monitor devices based on the specified metrics.

Assign Monitor to the SNMP Device Catalog

â€‹

Once you have successfully created the custom SNMP Device Catalog with the listed OIDs and their associations, the next step is to assign monitors to the catalog. By assigning monitors, you enable Motadata AIOps to start monitoring the new metrics associated with the OIDs in your network infrastructure.

Go back to the SNMP Device Catalog screen and locate the catalog you have just created. Under the

Actions

column of your custom SNMP Device Catalog, click on the

Assign Monitors

option. This action will allow you to specify the monitors that will be associated with the OIDs listed in the catalog.

After clicking on

Assign Monitors

, a list of all available network type monitors will appear.

Carefully review the list of network type monitors and select the ones that are relevant to the metrics you want to monitor. You can choose one or multiple monitors based on your requirements.

Once you have selected the monitors to assign to the SNMP Device Catalog, click on

Assign Monitors

. Motadata AIOps will then associate the chosen monitors with the OIDs in your custom catalog.

With the monitors now assigned to the SNMP Device Catalog, the monitoring process for the new metrics will begin during the next polling cycle. AIOps will collect data from the listed OIDs and provide real-time insights into the performance and health of your devices and network infrastructure.

## **Page Title: topology-scanner**

### Topology Scan

A topology scanner can be used to  
set up the topology maps for network devices  
on the Topology scan.

## Page Title: what-is-a-monitor

What is a Monitor?

A Monitor can be defined as any IT infrastructure component that is discovered and provisioned

within Motadata AIOps for the purpose of comprehensive monitoring. It plays a crucial role in enabling real-time monitoring and generating insightful performance metrics.

In the Motadata AIOps context, a monitor represents an entity that is provisioned by users after executing a discovery. By monitoring the performance metrics at the monitor level, Motadata AIOps gathers and analyzes data for the IT infrastructure. This data polling process forms the foundation for various features such as

Topology

,

Metric Explorer

,

Alerts and Policies

, which leverage the monitor-level metrics to provide valuable insights.

Setting up a monitor in Motadata AIOps involves the following steps:

User creates a credential profile and a discovery profile, and then maps the discovery profile to the credential profile.

User initiates a discovery run, either instantly or a scheduled run to identify devices within the network.

Once the discovery is complete, the user proceeds to provision the discovered devices within Motadata AIOps for monitoring purposes.

These provisioned devices are now referred to as Monitors.

By following this workflow, Motadata AIOps empowers users to effectively monitor the health and performance of their IT infrastructure. The insights gained through the monitoring process enable



informed decision-making and proactive management of the infrastructure.

With monitors in place, users can leverage the robust capabilities of Motadata AIOps to optimize the performance, identify potential issues, and ensure the smooth operation of their IT environment.