Page Title: backup-profile

Backup Profile

Refer

Backup and Restore Management

for more details on Backup Profile.

Page Title: collector-settings

On this page

Deployment Settings

The Deployment Settings screen in Motadata AIOps provides a comprehensive overview of the various artefacts configured in your deployment.

Navigation

â€‹

Go to Menu. Select

System Settings

. After that, select

Deployment Settings

. The list of artefacts deployed in Motadata AIOps is now displayed.

Deployment Settings Screen

â€‹

On this screen, you can find the following details related to each artefact installed in your deployment:

Field

Description

Hostname

The hostname of the artefact in your Motadata AIOps deplyment.

Type

The type of the artefact, specifying its role in Motadata AIOps Deployment. The artefact could be a primary application server, secondary application server, primary database, secondary database, observer, or a collector.

Deployment

The type of deployment.

IP

The IP address of the artefact, indicating its location in your network.

Status

The status of the deployment.

Used Count

Displays the total number of entities using the artefact. For example, in case of a collector this value indicates the total number of monitors that are sending data to the collector.

Duration

The duration for which the artefact has been active or running.

Actions

Here, you have the option to edit the deployment settings. This allows you to modify the configuration or parameters as needed. You can also enable the logging option for each artefact using the

Enable Logging

option.

The

Deployment Settings

screen is a central location for managing and monitoring all the artefacts in your Motadata AIOps deployment.

Page Title: data-retention

On this page

Data Retention

Overview

â€‹

Data retention in Motadata AIOps allows you to manage how long historical data is stored in the system. This feature helps you strike a balance between preserving valuable information and automatically cleaning up outdated data.

By configuring data retention settings, you can ensure that the platform retains the data relevant to your operations while efficiently managing storage resources.

Navigation

â€‹

Go to Menu. Select

System Settings

. After that, select

Data Retention

. The configuration page for Data Retention is now displayed.

Data Retention Settings Screen

â€‹

Metric Data Retention

â€‹

Field

Description

Default Duration

Metric raw data will be retained for last

Specifies the duration for retaining raw metric data.

30 days

Metric aggregated data will be retained for last

Specifies the duration for retaining aggregated metric data.

180 days

Log Data Retention

â€‹

Field

Description

Default Duration

Log raw data will be retained for last

Specifies the duration for retaining raw log data.

7 days

Log aggregated data will be retained for last

Specifies the duration for retaining aggregated log data.

180 days

Flow Data Retention

â€‹

Field

Description

Default Duration

Flow raw data will be retained for last

Specifies the duration for retaining raw flow data.

2 days

Flow aggregated data will be retained for last

Specifies the duration for retaining aggregated flow data.

180 days

Trap Data Retention

â€‹

Field

Description

Default Duration

Trap raw data will be retained for last

Specifies the duration for retaining raw trap data.

7 days

Trap aggregated data will be retained for last

Specifies the duration for retaining aggregated trap data.

180 days

System Event Data Retention

â€‹

Field

Description

Default Duration

Notification data will be retained for last

Specifies the duration for retaining notification data.

7 days

Audit data will be retained for last

Specifies the duration for retaining audit data.

30 days

Alert Data Retention

â€‹

Field

Description

Default Duration

Alert Policy data will be retained for last

Specifies the duration for retaining alert policy data.

90 days

NCM Data Retention

â€‹

Field

Description

Default Duration

NCM data will be retained for last

Specifies the duration for retaining NCM versions.

15 version(s)

Select

Save

to apply the changes to the data retention configuration.

Select

Reset

to erase all the current field values, if required.

Update the retention period to align with your organization's data management policies.

By customizing these settings, you can ensure that motadata AIOps optimally manages historical data, meeting both compliance requirements and the unique needs of your operations.

Page Title: mac-address-list

On this page

MAC Address List

Overview

â€‹

The MAC Address List feature in Motadata AIOps allows users to manage a list of MAC addresses associated with devices in their network infrastructure. MAC addresses, also known as Media Access Control addresses, are unique identifiers assigned to network interface controllers (NICs) for communication over a network.

The MAC Address List feature provides a centralized repository for storing and managing MAC addresses

for all the devices discovered in Motadata AIOps.

Navigation

â€‹

Go to Menu. Select

System Settings

. After that, select

MAC Address List

. The MAC Address list is now displayed.

Managing MAC Addresses

â€‹

The MAC Address List screen provides options to add, edit, and delete MAC addresses. Follow the steps below to perform these operations:

Adding MAC Addresses

â€‹

To add a new MAC address to the list, follow these steps:

Click on the

Create MAC Address

 button on the MAC Address List screen.

Enter the MAC address in the provided field. Ensure that the MAC address is entered in the correct format (e.g., 00:1A:2B:3C:4D:5E).

Enter the other required details such as

Device IP Address

,

Interface IP Address

, and

Interface Name

.

Click

 to add the MAC address to the list.

Editing MAC Addresses

â€‹

To edit an existing MAC address in the list, follow these steps:

Locate the MAC address in the list that you want to edit.

Click on the

Edit

 button associated with the MAC address.

Modify the details as required.

Click

 to save the changes.

Deleting MAC Addresses

â€‹

To delete a MAC address from the list, follow these steps:

Locate the MAC address in the list that you want to delete.

Click on the

Delete

button associated with the MAC address.

Confirm the deletion in the prompt that appears.

Please exercise caution when deleting MAC addresses, as it can impact the accuracy of network-related operations and monitoring.

Page Title: mail-server-settings

On this page

Mail Server Settings

Overview

â€‹

Mail server settings allow users to configure the email functionality within Motadata AIOps. By setting up the mail server, users can enable email notifications and alerts, ensuring effective communication and timely response to critical events.

To configure the mail server settings, users need to provide specific details related to their SMTP (Simple Mail Transfer Protocol) server. These details include the SMTP server address, port, email address, security type, authentication requirements, username, and password.

We will provide step-by-step instructions on how to configure the mail server settings in Motadata AIOps. We will cover the necessary details required to ensure successful configuration and usage of this feature.

Navigation

â€‹

Go to Menu. Select

System Settings

. After that, select

Mail Server Settings

. The mail server settings screen is now displayed.

Mail Server Settings Screen

â€‹

The mail server settings screen allows you to enter the required information for configuring the mail server in Motadata AIOps. Let's explore each field:

Option

Description

SMTP Server

Enter the address of your SMTP server. This is the server responsible for sending outgoing emails.

SMTP Server Port

Specify the port number through which the SMTP server communicates. Commonly used port numbers for SMTP include 25, 465, or 587. Check with your email service provider for the correct port to use.

Email

Provide the email address associated with the mail server. This address will be used as the sender's email address for outgoing emails.

Security Type

Choose the appropriate security type for the SMTP server connection. You can select from the following options:

- None: No encryption or security is applied to the connection.
- SSL: Secure Socket Layer encryption is used for the connection.
- TLS: Transport Layer Security encryption is used for the connection.

Ensure that you select the appropriate security type based on your email service provider's requirements.

Authentication Required

Toggle this option to specify whether authentication is required for the SMTP server. If enabled, you need to provide the username and password for authentication.

User Name

If authentication is required, enter the username associated with the mail server.

Password

If authentication is required, provide the password associated with the specified username.

Once you have entered all the necessary details in the respective fields, click on the

Test

button to verify the connection with the SMTP server. A successful connection test ensures that the provided settings are correct and the Motadata AIOps can send emails using the configured mail server.

Finally, click on the

Save Mail Server Settings

button to save the configured mail server settings.

It is important to note that incorrect or incomplete mail server settings may result in unsuccessful email delivery or errors. Ensure that you double-check all the provided details before saving the settings.

With the mail server settings properly configured, you can now leverage the email functionality of Motadata AIOps to receive important notifications, alerts, and reports via email.

Page Title: proxy-server-settings

On this page

Proxy Server Settings

Overview

â€‹

Proxy server settings allow users to configure a proxy server for network communication within Motadata AIOps. A proxy server acts as an intermediary between the Motadata AIOps and the internet, enhancing security, performance, and control over network traffic.

To configure the proxy server settings, users need to provide specific details related to the proxy server, including the proxy server address, port, timeout, proxy type, and authentication requirements.

We will provide step-by-step instructions on how to configure the proxy server settings in the Motadata AIOps. We will cover the necessary details required to ensure successful configuration and usage of this feature.

Navigation

â€‹

Go to Menu. Select

System Settings

. After that, select

Proxy Server Settings

. The proxy server settings screen will now be displayed.

Proxy Server Settings Screen

â€‹

The proxy server settings screen allows you to enter the required information for configuring the proxy server in Motadata AIOps. Below is a summary of the available fields:

Option

Description

Proxy Server Enable

Switch to enable or disable the proxy server in Motadata AIOps.

Proxy Server

Address of the proxy server.

Proxy Server Port

Port number for the proxy server communication.

Timeout (Sec)

Timeout duration in seconds for the connection.

Proxy Type

Type of proxy server being used (HTTP, SOCKS4, SOCKS5).

Authentication Required

Switch to specify if authentication is required.

User Name

Username for proxy server authentication (if required).

Password

Password for proxy server authentication (if required).

Once you have entered all the necessary details in the respective fields, click on the

Test

button to verify the connection with the proxy server. A successful connection test ensures that the provided settings are correct.

Once you have entered all the necessary details in the respective fields, click on the

Save Proxy Server Settings

button to save the configured proxy server settings.

Note that incorrect or incomplete proxy server settings may result in network connection issues. Ensure that you double-check all the provided details before saving the settings.

Page Title: rebranding

On this page

Rebranding

Overview

â€‹

The rebranding feature in Motadata AIOps allows users to customize the appearance of the application to align with their organization's branding. With this feature, users can replace the default Motadata logo on the top left of the screen with their organization's logo. Additionally, users have the option to upload separate logos for the default and dark themes.

To ensure a seamless rebranding experience, the supported image formats for the logo upload are SVG, JPG, and PNG. The recommended size for the logo image is 150 x 150 pixels.

We will cover the necessary details required to customize the application logo according to your organization's branding.

Navigation

â€‹

Go to Menu. Select

System Settings

. After that, select

Rebranding

.

The rebranding settings screen will now be displayed.

Rebranding Settings Screen

â€‹

The rebranding settings screen allows you to upload your organization's logo and customize the application's branding. Follow the steps below to perform the rebranding:

Click on the

Browse Logo

button.

Select the logo file from your local system. Ensure that the file is in one of the supported formats: SVG, JPG, or PNG.

The Motadata logo on the top left of the screen will be replaced with your organization's logo.

Rebranding the application logo helps personalize the user experience and reinforces your organization's identity within Motadata AIOps.

Ensure that the uploaded logo(s) accurately represent your organization and adhere to any branding guidelines or legal requirements.

By customizing the application logo through rebranding, you can create a cohesive and branded experience for your team while using Motadata AIOps.

Page Title: sms-server-settings

On this page

SMS Server Settings

Overview

â€‹

SMS server settings is an important feature of the AIOps that enables users to send SMS notifications to desired recipients. To configure the SMS server settings, users need to provide the SMS gateway URL provided by the service provider their organization uses. This URL must include pre-configured tags for the message and recipient numbers so that AIOps can identify the message to send to the recipient number.

With this feature, users can ensure timely communication of critical issues, incidents, or alerts to stakeholders through SMS notifications. This can help improve the response time of the team and ensure quick resolution of incidents.

In this user guide, we will provide step-by-step instructions on how to configure the SMS server settings in the AIOps product. We will cover the necessary details required to ensure successful configuration and usage of this feature.

Navigation

â€‹

Go to Menu. Select

System Settings

. After that, select

SMS Server Settings

. The SMS server settings screen is now displayed.

SMS Server Settings Screen

â€‹

To configure the SMS gateway URL on the SMS server settings screen, you will need to enter the URL provided by your organization's SMS gateway service provider. This URL typically contains authorization details, message content, language, and recipient numbers.

For example, the gateway URL provided by your service provider may look something like this:

https://www.xyzsmsgateway.com/dev/bulkV2?authorization=YOUR_API_KEY&message=This is test message&language=english&route=q&numbers=9999999999,8888888888,7777777777'

However, to enable the AIOps product to identify the message and recipient numbers, you will need to replace the specific message and number values in the URL with variable tags,

'$$message$$'

and

'$$number$$'

respectively. The updated URL would look like this:

https://www.xyzsmsgateway.com/dev/bulkV2?authorization=YOUR_API_KEY&message=$$message$$&language=english&route=q&numbers=$$number$$'

You will also need to update the API key you have generated by the service provider in the link.

In this updated URL, the variable tag

'$$message$$'

will be replaced with the actual message content entered by the user, and the variable tag

'$$number$$'

will be replaced with the actual recipient numbers entered by the user. This will allow AIOps to understand and use the provided information to send SMS notifications to the desired recipients.

When entering the SMS gateway URL on the SMS server settings screen, it is important to ensure that the URL is entered correctly and all necessary details, including the authorization key, message content, and recipient numbers, are included.

After providing the URL on the field

SMS Gateway URL

, click on the

Test

button. A pop-up asking for a recepient number will be displayed as follows:

Provide the details for the recepient number and message in the pop-up and click on the

Send Test SMS

button. Once the Test SMS is sent successfully, you can then click on the

Save SMS Server Settings

button to save the SMS server settings you just configured.

Page Title: storage-profile

Storage Profile

Refer

Backup and Restore Management

 for more details on Storage Profile.