Page Title: flow-configurations

On this page

Configuration to ingest Flow

In this section, we will discuss some of the configuration options available for flow settings in AIOps.

Navigation

â€‹

Go to the Main Menu, Select

Settings

. After that, go to

Flow

. Select

Flow Settings

.

Flow Settings

IP/IP Range Settings

Sample Rate Settings

AS Mapping

IP Mapping

Geolocation Mapping

Protocol Mapping

Application Mapping

Flow Settings

â€‹

In this section, you can configure the flow settings so that AIOps is able to ingest the flow data that

you send to the AIOps server. In order to view flow data of a device in flow explorer, the device must be configured to push the data to Motadata AIOps server.

Flow Settings Screen

â€‹

The following configuration options are available on the screen:

Field

Description

sFlow Port

Specify the port number to which you will send the sFlow data so that AIOps is able to ingest the data and categorise the flow as sFlow in Flow Explorer. This is set to 6343 by default.

Netflow Port

Specify the port number to which you will send the Netflow data so that AIOps is able to ingest the data and categorise the flow as Netflow in Flow Explorer. This is set to 2055 by default

Aggregation Time(Min)

Enter the time period(in Mins) in which the polling values will be aggregated for the metric you select in the

Flow Explorer

tool. This is set to 5 minutes by default.

sFlow v5 Traffic Direction

- Select

Ingress

if the flow that you receive on the sFlow port is Ingress.

- Select

Egress

if the flow that you receive on the sFlow port is Egress.

In this way, you can send flow data to AIOps by configuring the port numbers for flow ingestion and sending the flow data from your devices on these configured ports.

IP/IP Range Settings

â€‹

You can define domain names based on the source of the flow data. This enables you to analyse the flow data related to specific domain name i.e., gain insights into how much bandwidth is being used by a particular IP group/Domain and by which user. You can also use the flow explorer to gain many more insights as per your requirement.

Navigation

â€‹

Go to the Main Menu, Select

Settings

. After that, go to

Flow

. Select

IP/IP Range Settings

.

IP/IP Range Settings Screen

â€‹

Click on the

Create IP/IP Range

button to create a record for mapping an IP/IP Range to a domain name or a group name.

Enter the IP or the IP range in the

IP/IP Range column

and the name that you want to assign to the IP(s) in the

IP Group/Domain Name

column. This creates a mapping of the IP(s) you have specified with the domain name you assigned

to it.

Now, the same domain name will be displayed in the flow diagram instead of simply displaying an IP address whenever flow data comes from the IP(s) specified above.

Sample Rate Settings

â€‹

Once the Flow has been ingested using the configuration settings you applied on the

Flow Settings Screen

, you will find individual listing of each Flow source on this screen.

Typically Motadata AIOps automatically detects Sampling Rate of the ingested Flow. However, in case the ingested Flow is not yet sampled or is undetected, you can easily define a custom sampling rate using the

Custom Sampling Rate

option.

Sample Rate Settings Screen

â€‹

The following configuration options are available on the screen:

Field

Descritpion

Interface Index

Unique identifier of the Flow source interface.

Source

The IP Address of the Flow source.

Interface Name

Interface identifier of the flow source.

Interface Alias

User provided name for the interface of the flow source.

Interface Speed

The total available bandwidth of the interface to transfer Flow data.

Sampling Rate

The Sampling Rate automatically detected by Motadata AIOps is displayed in this field.

Custom Sampling Rate

If you have defined any custom Sampling Rate for a Flow source, it will be displayed here.

Define a Custom Sampling Rate

â€‹

If the Sampling Rate of Flow source is undetected, you can easily adjust the sampling ratio to properly visualize the data.

On the

Sampling Rate Screen

, click on

for the particular Flow source present under the

Actions

column. Then, select

Edit Sampling Rate

.

Next, type the custom sampling ratio value and click on

icon to apply the changes.

AS Mapping

â€‹

You can map the AS numbers with the all the IP sources of an organization to better visualize the Flow data.

You can map AS numbers of organization based on individual IP, IP range, and/or CIDRs using the

AS Mapping

module of Motadata AIOps. This will enable you to efficiently visualize inbound and outbound Flow data with respect to ASNs and help you identify any suspicious flow of traffic.

Navigation

â€‹

Go to the Main Menu, Select

Settings

. After that, go to

Flow

. Select

AS Mapping

.

AS Mapping Screen

â€‹

In this section, you can configure the ASN mapping to efficiently and effectively visualize the Flow data associated with ASNs. You can also view the list of already mapped ASNs.

The following configuration options are available on the screen:

Field

Description

AS Name

Name of the AS that you have mapped with the IP or range of IPs.

AS Number

The unique AS Number provided by IANA.

Organization

Name of the organization associated with the IP addresses.

IP Address Count

Displays the total number of IP address and IP ranges.

To create a new AS mapping, click on the

Create AS Mapping

button.

The following configuration options are available on the screen:

Field

Description

AS Name

Enter the name of the AS that you wish to get displayed.

AS Number

Mentione the unique AS Number provided by IANA.

Organization

Provide the name of the organization associated with the IP addresses.

IP Address/IP Range/CIDR

Enter an IP address, IP range, and or a CIDR here to associate with the mentioned ASN.

Once you have entered all the information required to create the AS Mapping, click on the

Create AS Mapping

button.

Click on the

Reset

button to clear all the fields.

IP Mapping

â€‹

With IP Mapping, Motadata AIOps will help you identify individual users by mapping their system to the IP address. You can either use an Active Directory to import user information or manually upload a CSV file.

Navigation

â€‹

Go to the Main Menu, Select

Settings

. After that, go to

Flow

. Select

IP Mapping

.

IP Mapping Screen

â€‹

The following configuration options are available on the screen:

Field

Description

Profile Name

Name of the profile provided by the user.

Description

Description for the profile.

Source

Source (Manual or Active Directory) will be displayed in this field.

Mapping

Total number of mapped users in the profile.

Last Sync at

Timestamp of the last sync for the profile.

Schedule

Status of the scheduler to perform a sync.

Actions

- Users can manually run the sync by clicking on the

Sync

icon.

- User can edit or delete an existing IP mapping by clicking on the

Ellipsis

icon.

To create a new

IP Mapping

, click on the

Create IP Mapping

button.

Since the configuration process vary for Active Directory and Manual mapping, let's take a look at them individually:

Active Directory

Manual Mapping

Field

Description

Profile Name

Enter the name for the profile you wish to create.

Description

Enter the description for the profile you wish to create.

Source

Select a source from the dropdown.

Domain Name

Mention the domain name for the Active Directory.

Primary Domain Controller

Enter the primary domain controller for the Active Directory.

User Name

Enter the user name for the Active Directory.

Password

Enter the password for the Active Directory.

Field

Description

Profile Name

Enter the name for the profile you wish to create.

Description

Enter the description for the profile you wish to create.

Source

Select a source from the dropdown.

CSV

Upload the CSV containing all user information using the

Upload

button.

Once you have configrued all the fields are per your requirement, click on the

Create IP Mapping

button to create the IP Mapping.

Click on the

Reset

button to clear all the fields.

Geolocation Mapping

â€‹

Geolcation mapping will help you visualize Flow data coming in and out of a particular data center/branch location of your organization. The effectiveness of Geolocation mapping increases multifold when you want to visualize Flow data of multiple branches or data centers of your organization.

Gelocation mapping will help you visualize Flow data coming in and out of your data center/branch location.

Navigation

â€‹

Go to the Main Menu, Select

Settings

. After that, go to

Flow

. Select

Geolocation Mapping

.

Gelocation Mapping Screen

â€‹

The following configuration options are available on the screen:

Field

Description

Profile Name

Name of the geolcation profile.

Description

Description regarding the profile.

Country

Country of the geolocation profile.

City

City of the profile.

IP Address Count

:

Total number of IP address, IP address ranges, or CIDRs associated with the profile.

Actions

Edit

or

Delete

the geolocation profile using the

Ellipsis

icon.

To create a new geolocation mapping, click on the

Create Geolocation Mapping

option.

The following configuration options are available on the screen:

Field

Description

Profile Name

Enter a name of the profile. You can also specify details to identify different branches in the same city.

Description

Provide a description for the profile.

Country

Mention the country where the location of branch/data center is located.

City

Mention the city where the branch/data center resides.

Latitude

Enter Latitude coordinates of the location.

Longitude

Enter Longitude coordinates of the location.

IP Address/IP Range/CIDR

Mention indvidual IP address, IP address ranges, and CIDRs associated with the branch office/data center.

Once you have entered all the information in the appropriate fields, click on

Create Geolacation Mapping

.

To reset all fields, click on

Reset

option.

Protocol Mapping

â€‹

The Protocol Mapping section in Motadata AIOps provides a default mapping between protocols and their corresponding port numbers. This mapping is utilized by the system in the

Flow Explorer

to depict communication via specific ports and protocols.

By associating the correct protocol with the corresponding port number, the Flow Explorer can accurately represent network traffic and help identify the protocols used by different applications.

Navigation

â€‹

Go to Menu. Select

System Settings

. After that, select

Protocol Mapping

. The Protocol Mapping list is now displayed.

Default Protocol Mapping

â€‹

The default protocol mapping in Motadata AIOps includes a comprehensive list of commonly used protocols and their associated port numbers. This mapping is already configured in the system, ensuring that the Flow Explorer accurately depicts the communication protocols.

The default protocol mapping is continuously updated to include new protocols and their corresponding port numbers.

Custom Protocol Mapping

â€‹

Motadata AIOps also provides the flexibility to define custom protocol mapping if required. Users can add new protocols and assign them to specific port numbers using the custom mapping feature.

By defining custom protocol mapping, organizations can accurately represent their unique network architecture and communication protocols in the Flow Explorer.

Please note that modifying the default protocol mapping or defining custom protocol mapping should be done with caution. Ensure that the mapping accurately reflects the protocols and port numbers used in your network environment.

You can also create a new protocol mapping and map a new protocol to a port number as per the network infrastructure setup in your organisation. Click on the

Creat Protocol Mapping

to create a new application mapping.

With the Protocol Mapping feature in Motadata AIOps, you can visualize network traffic in the Flow Explorer with accurate protocol and port representations, allowing for better analysis and understanding of application communication.

Application Mapping

â€‹

The Application Mapping section in Motadata AIOps provides a default mapping between applications and their associated port numbers. This mapping is used by the system to visualize application communication in the

Flow Explorer

.

By associating applications with their respective port numbers, the Flow Explorer can accurately depict how applications communicate over specific ports and protocols.

Navigation

â€‹

Go to Menu. Select

System Settings

. After that, select

Application Mapping

. The Application Mapping list is now displayed.

Default Application Mapping

â€‹

The default application mapping in Motadata AIOps includes a comprehensive list of commonly used applications and their associated port numbers. This mapping is pre-configured in the system to ensure accurate visualization of application communication.

Custom Application Mapping

â€‹

Motadata AIOps also allows users to define custom application mapping if required. With the custom mapping feature, organizations can associate specific applications with their corresponding port numbers, ensuring accurate representation in the Flow Explorer.

By defining custom application mapping, you can tailor the visualization of application communication to match your unique network environment and application landscape.

Please exercise caution when modifying the default application mapping or defining custom application mapping. Ensure that the mapping accurately reflects the applications and port numbers used in your network environment.

You can also create a new application mapping and map a new application to a port number as per the network infrastructure setup in your organisation. Click on the

Create Application Mapping

to create a new application mapping.

With the Application Mapping feature in Motadata AIOps, you can visualize and analyze application communication in the Flow Explorer with accurate representations of applications and their associated port numbers.

Actions Available for Application Mapping

â€‹

You can click on the

Ellipsis

icon available for each mapped application under the

Action

column to access the actions.

Edit Application Mapping

: You can edit an existing mapped application.

Delete Application Mapping

: Delete the particular Application Mapping from the system.

Page Title: flow-explorer

On this page

Flow Explorer

Flow explorer is a tool that enables you to graphically visualize the flow data for all the devices sending flow to Motadata AIOps server. Flow explorer provides consistent visibility into your network allowing you to judge essential infrastructural requirements, make business-driven decisions, and ensure efficient and cost-effective operations based on the network flow data presented to you.

Apart from identifying and troubleshooting of the issues in your network, Flow Explorer also provides network admins with historical data that they can use to improve their IT infrastructure, network health, and performance.

Navigation

â€‹

Go to Menu, Select

Flow Explorer

. After that, Select

Explorer

. The Flow Explorer tool is now displayed.

How to use Flow explorer?

â€‹

Creating the Flow visualisation

â€‹

You will be able to visualise the flow of your network that you have sent to Motadata AIOps on the Flow Explorer.

Now, you can customise the visualisation of the flow of the network based on the counters(metrics) for the flow that you wish to view on the screen.

Option

Description

Counter

Select what you want to see on the flow explorer. Options include things like 'packets', 'volume.bytes', and more. For instance, if you want to see how many packets are moving from one place to another in your network, just choose

packets

.

Aggregation

Select the aggregation function that you want to apply to all the values of the counter that you selected.

Flow Source

Select the devices for which you want to visualise the flow details on the screen. All the devices sending flow to Motadata AIOps server will be available for selection in the dropdown.

Result By

Select up to 4 fields to better visualise and understand the network performnce for the counter you've selected. For example, consider the above diagram where you are visualising the network traffic data. Using Result By, you can see the amount of data (like volume.bytes) based on specific details like where it's coming from (source.ip), which door it used to exit (source.port), where it's going to (destination.ip), and which door it's using to enter (destination.port).

Adjusting the nodes in the Flow Diagram

â€‹

After generating the flow diagram, you have the flexibility to rearrange its components for a personalized view.

To adjust the placement of fields within the diagram, utilize the arrow icons as shown in the image below.

Viewing Field Values

â€‹

For a detailed perspective, you can access a list that displays values for all the fields you've incorporated into the diagram.

Each entry in this list signifies a connection between a source and its corresponding destination in your diagram.

This list is conveniently located beneath the flow diagram, as illustrated in the image below.

Actions available on the Flow Explorer

â€‹

Refresh the flow data

Select

to refresh the flow data.

Take a screenshot of the dashboard

Select

to take a screenshot of the dashboard in its current state.

Change the time period of the flow data

You can change the time period of flow data shown on the flow explorer using the dropdown highlighted in the picture below.

Change the filter

Select

to apply filter conditions for creating the flow diagram.

Change the chart type

You can change the graph used to represent the flow data using the selection higlighted in the picture below.

Save the visualisation as a widget

Select

save the visualisation you created as a

widget

Log to Flow Traffic Feature

â€‹

Motadata AIOps integrates log and flow data through the Log to Traffic feature. By parsing the ingested log data, the platform ensures that this information is also made available as network flow, enabling users to analyze the data as Network flow data within the Flow Explorer.

Page Title: how-to-analyze-the-flow-data

On this page

How to analyze the flow data?

Overview

â€‹

Motadata AIOps provides a powerful tool called Flow Explorer for analyzing network flows. It efficiently processes large amounts of flow data and represents it visually using a Sankey diagram.

To ensure optimal network performance and prevent issues caused by bandwidth hogs and high traffic, it's crucial to proactively identify and resolve them before they cause problems.

Navigation

â€‹

Go to the Menu, Select

Flow Explorer

. The Flow Dashboard screen is now displayed.

Flow Analysis in Motadata AIOps

â€‹

The flow analysis in Motadata AIOps could be done in one of the following ways:

Preset Dashboards

: The flow analytics screen includes multiple inbuilt dashboards that represent important data sets such as Top 5 Conversations and Top 5 Protocols in graphical form.

Flow Explorer

: This tool enables visualizing the flow for all devices sending their flow data to Motadata AIOps, enabling the user to analyze traffic patterns, monitor network bandwidth usage at a granular level, identify the users with maximum bandwidth usage, and trace conversations between internal and external endpoints.

Types of Flow supported in Motadata

â€‹

sFlow (v5/v9)

jFlow

NetFlow

NBAR2

IPFIX (v10)

Page Title: Network-Observability-through-Flow-Analysis

Overview

A major use-case of AIOps is network observability, which involves analyzing the metrics related to a network to understand what is happening inside it, and how the internal state of the network impacts business objectives and the user experience.

One effective way to achieve network observability is by analyzing the flow of your network. This includes monitoring overall network bandwidth usage, identifying users, applications, protocols, and IP address groups that consume the most bandwidth, and analyzing their traffic patterns.

This enhanced visibility into your network's applications, hosts, and conversations enables you to proactively manage your network to reduce outages, solve problems faster, and ensure efficient and cost-effective operations.

Network observability through Flow analysis

Understanding the internal state of networks is an essential component of managing overall performance and reliability of your infrastructure.

As a network administrator, monitoring network traffic is the most efficient way to understand any underlying issues in a network. Motadata AIOps offers a Flow explorer that allows network admins to gain visibility into which server, application, or user is using what amount of bandwidth, and where that bandwidth is being used.

Flow analysis helps align resources to support business results and gain credibility by making data-driven decisions. By studying the flow data of your network, you can:

Monitor network bandwidth usage at a granular level and identify users with maximum bandwidth usage.

Trace the conversations between internal and external endpoints.

Analyze traffic patterns over months, days or minutes by filtering out data for any network element.

Enhance bandwidth capacity before outages occur.

Network observability has assumed even more importance in recent years due to the increase in the

complexity of networking architectures. Modern networks often span multiple data centers and/or clouds, making it challenging to monitor and manage the network effectively.

By providing continuous visibility into networks, and helping teams to map the network state to the organizational business contexts, such as availability and performance guarantees, network observability allows an organization to handle the complexity of modern networks and ensure that their network supports their business expectations.

Page Title: preset-dashboards

On this page

Preset Dashboards

Preset Dashboards in Motadata AIOps provide you with graphical representations of flow datasets, giving you meaningful insights into your network. By default, this screen displays the information for all devices sending their flow to Motadata AIOps.

Actions available on the preset dashboards

â€‹

Select the Event Source

â€‹

To display flow data on the dashboard for a specific event source, follow these steps:

Click on the

Event Source

drop-down at the top of the screen above the dashboard.

A dropdown menu containing a list of all devices sending their flow data to Motadata AIOps will appear.

Select the desired event source(s) from the list to display their data on the dashboard.

Select the Interface

â€‹

To display flow data on the dashboard for a specific interface, follow these steps:

Click on the

Interface

drop-down at the top-right of the screen above the dashboard.

A dropdown menu containing a list of all interfaces for which flow data is being sent to Motadata AIOps will appear.

note

Interfaces are only available in the dropdown if there is flow data moving in or out of that interface, and if the corresponding device is configured as a Monitor.

Select the desired interface(s) from the list to display their data on the dashboard.

Take a screenshot of the dashboard

â€‹

Select

 to take a screenshot of the dashboard.

Change the time period of the flow data

â€‹

Select

 to change the time period for which flow data is shown on the dashboard.