Page Title: creating-a-new-user

On this page

Creating a New User

To create a user in Motadata AlOps, a simple but systematic approach involving user creation, role creation, and assigning role to the user is followed. This process ensures efficient management of user access and permissions within the system.

1. Role Creation

â€∢

First, create a role that defines a specific set of permissions and access levels. Roles serve as a convenient way to group users with similar responsibilities or access requirements. For example, if multiple users need the same permissions, such as log management capabilities, you can create a role specifically for log management with the necessary read and write permissions for the log module.

Navigation

â€∢

Go to Menu. Select

Settings

. After that, Go to

User Settings

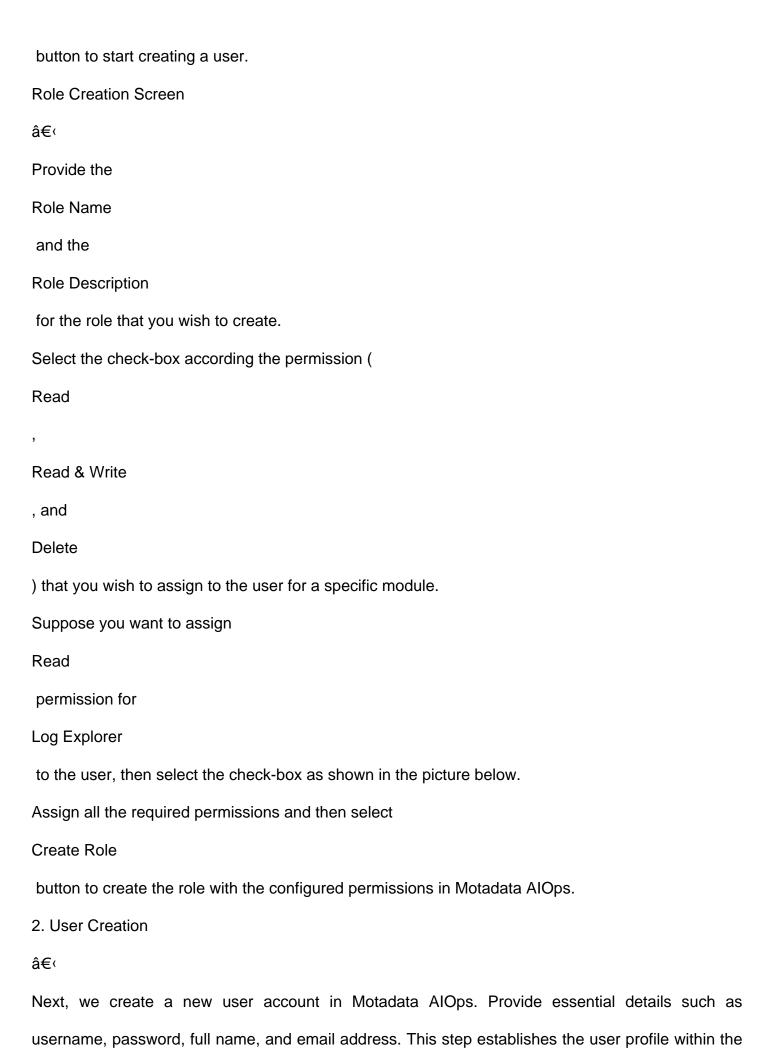
. Select

Role

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

Click on the

Create Role



system.
Navigation
â€⊂
Go to Menu. Select
Settings
. After that, Go to
User Settings
. Select
User
to display the list of all the users in the system.
Click on the
Create User
button to start creating a user.
User Creation Screen
â€⊂
Provide the details for user creation as follows:
Field
Description
First Name
Enter the first name of the user.
Last Name
Enter the last name of the user.
Email Address
Enter the email address of the user.
Mobile Number

Enter the mobile number of the user. **User Name** Set a username for the user you want to create. Password Set a password for the user you want to create. Confirm Password Enter the same password to confirm that the passwords match. Status Use this switch to Disable/Enable the user access. Groups Select the group(s) that you want to assign to the user. The user will be able to access the data from the monitors that fall under the group(s) you select here. Role Select the role from the dropdown that you wish to assign to the user. Select Create User to create the user in the system. Select Reset to erase all the current field values. By assigning roles, you grant users the corresponding permissions and access levels defined within the role. This approach ensures consistency and simplifies user management. For instance, assigning the Log Management role we created in the first step to multiple users responsible for log management saves time and effort, as they inherit the same set of permissions. By assigning groups to a user, you grant users the permission to access monitors that fall under the

same group as the user. You can also create new groups by navigating to

Group

under

User Settings

By following this user creation process, Motadata AlOps enables you to efficiently manage user access and permissions. It provides flexibility in granting appropriate privileges to different users based on their roles and responsibilities. This organized approach streamlines user administration and helps ensure that users have the necessary access to perform their tasks effectively.

Bulk Assign Role and Group to Users

â€∢

Motadata AlOps supports bulk assignment of Roles and Groups to users. This functionality allows you to efficiently assign the necessary access and privileges to multiple users in a single action. This can be beneficial for scenarios where you need to assign the same Roles and Groups to a large number of users.

Select all the users for which you wish to Bulk assign the Role and/or Group.

Click on the

icon in the top right and assign the Role and/or Groups as per your requirements.

Page Title: Idap-server-settings

On this page

LDAP Server Settings

Overview

â€⊂

The LDAP Server Settings screen in Motadata AlOps provides administrators with the ability to

configure and integrate LDAP servers seamlessly. LDAP is a protocol used to access and manage

directory information services, allowing organizations to centralize user authentication and

authorization processes.

With the LDAP Server Settings, administrators can establish a connection between Motadata AlOps

and their LDAP server, enabling user authentication against the LDAP directory. This integration

simplifies user management by leveraging existing LDAP infrastructure and streamlining access

control.

In this section, administrators can define the necessary parameters to establish a connection with

the LDAP server. This includes specifying the LDAP server address, port number, encryption

options, and other authentication settings. By configuring these settings accurately, Motadata AlOps

can communicate with the LDAP server and authenticate user credentials during login.

Integrating an LDAP server with Motadata AlOps offers several benefits, such as centralized user

management, reduced administrative overhead, and enhanced security through consistent

authentication. With LDAP integration, organizations can leverage their existing user directories,

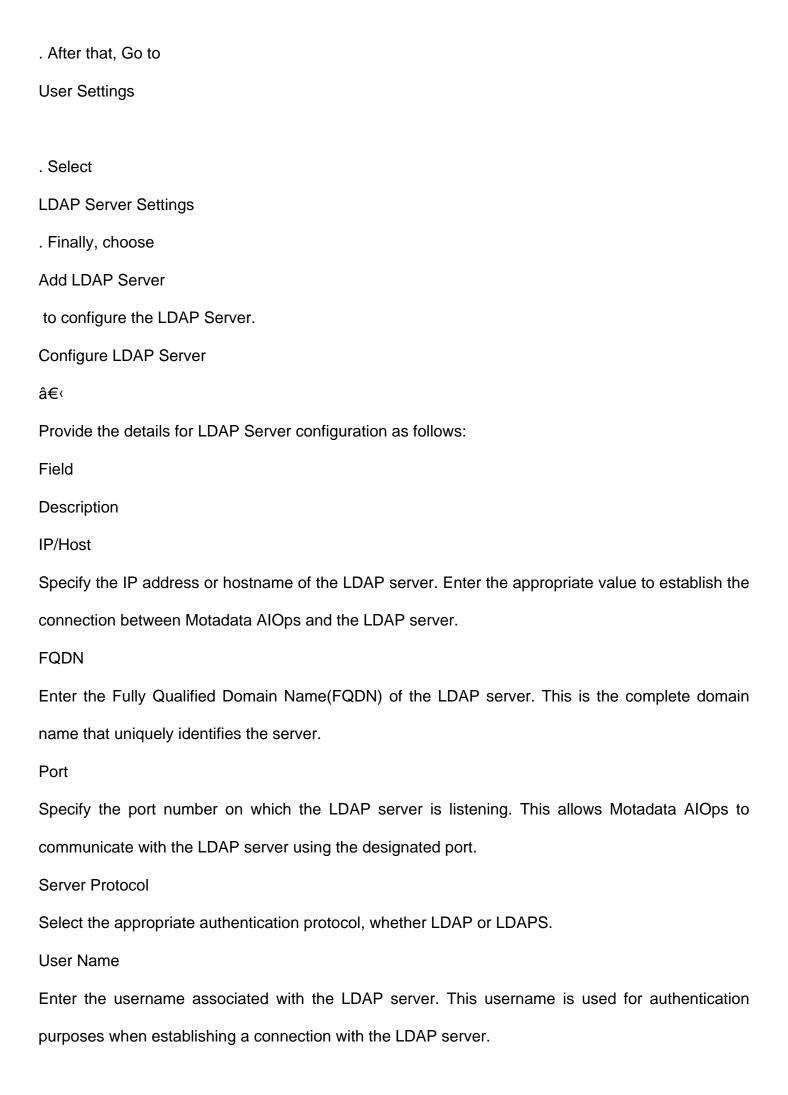
ensuring seamless user authentication and authorization within the Motadata AlOps environment.

Navigation

â€∢

Go to Menu. Select

Settings



Password

Provide the corresponding password for the LDAP server username. This password is used to authenticate the user during the connection establishment process.

Test

This button allows you to verify whether the provided username and password can successfully access the IP or hostname of the LDAP server. This helps ensure the accuracy of the LDAP server configuration.

Import Certificate

This option is only available only when you select the LDAPS protocol in the

Server Protocol

option. Attach the SSL certificate required for LDAPS authentication.

LDAP Authentication

Enable or disable LDAP authentication for user login. When enabled, user credentials are authenticated against the LDAP directory, providing centralized user authentication.

Auto Sync

Enable this feature to allow automatic synchronization of user accounts between Motadata AlOps and the LDAP server. This helps maintain consistency between the two systems, reducing manual effort in managing user accounts.

Sync Every

This option is available only when you select the

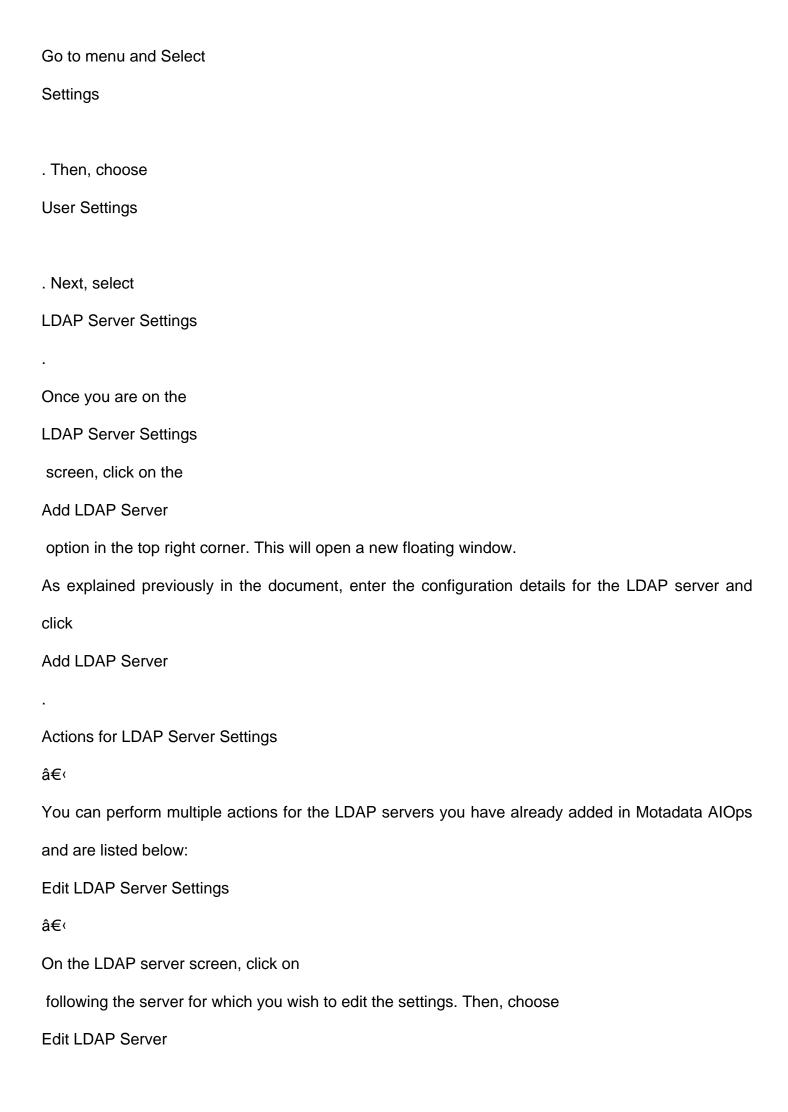
Auto Sync

option. Select the time frame after which you want the synchronisation between Motadata AlOps and the LDAP server to run on a recurrent basis.

Configuring these LDAP Server Settings accurately is crucial to establish a successful connection with the LDAP server and enable user authentication and synchronization within Motadata AlOps.

Add Multiple LDAP Servers

â€∢



to proceed.

All the server configuration options will be visible to you now, make the necessary changes and click

on

Save Changes

.

Force-Sync LDAP Server

â€∢

Even when auto synchronization is enabled for your LDAP server, you can choose to force-sync it.

Keep in mind, this will not have any impact on the auto-sync schedule that you may have defined at

the time of server configuration.

To force-sync LDAP server, click on the icon under the

Sync

column. Moreover, the last sync timestamp is visible right next to it to facilitate informed decision making when running a force-sync.

Delete Existing LDAP Server

â€∢

Click on

for the server you wish to delete. Then, select

Delete LDAP Server

from the list. This action will bring an alert to your screen, click on

Yes

on the alert to confirm deletion.

Page Title: overview

On this page

User Settings

Overview

â€∢

The User Settings screen in Motadata AlOps empowers administrators to manage user accounts, roles, and password policies efficiently. This comprehensive module provides the necessary tools to create users, define roles with specific permissions, and configure password policies to ensure a secure environment. Additionally, it offers the flexibility to configure LDAP (Lightweight Directory Access Protocol) integration for seamless user authentication and authorization.

With the User Settings module, administrators can streamline user management processes, establish appropriate access controls, and enhance overall security within the system. This overview will guide you through the key functionalities and features available in the User Settings screen, enabling you to effectively manage user accounts and access control policies in your Motadata AlOps environment.

Page Title: password-policy

On this page

Configuring Password Policy

unauthorized access.

Overview

â€∢

In Motadata AlOps, administrators have the ability to configure the password policy to enforce security measures and ensure that users create strong and secure passwords. The password policy settings allow administrators to define the minimum requirements for passwords, such as length, complexity, and expiration. By configuring the password policy, organizations can enhance the overall security posture of Motadata AlOps system and protect sensitive information from

With the password policy in place, administrators can establish guidelines for creating passwords that meet specific security standards. This ensures that users adhere to best practices when setting their passwords, reducing the risk of weak or easily guessable passwords that could compromise system security. By implementing a strong password policy, organizations can boost their defense against unauthorized access attempts and strengthen the overall security of their Motadata AlOps environment.

Next, let's look into the details of how administrators can configure the password policy settings in Motadata AlOps, including the specific parameters that can be defined and the impact they have on user password management.

Navigation

â€∢

Go to Menu. Select

Settings

. After that, Go to

User Settings

. Select

Password Settings

to configure the password policy.

Password Settings Screen

â€∢

When configuring the password policy in Motadata AlOps, administrators have the option to define various parameters to enforce password requirements. Here's a description of the fields available in the password policy configuration screen:

Option

Description

Password Expiry

By enabling this setting, administrators can specify a time duration after which user passwords will expire. Users will be prompted to change their passwords periodically to ensure enhanced security. Also, specify the number of days after which the passwords will expire in the blank field besides the Password Expiry

Password Uppercase

Enabling this setting makes it mandatory for passwords to contain at least one uppercase letter.

Users will be required to include uppercase characters in their passwords to meet the password policy requirements.

Password Lowercase

This setting requires passwords to include at least one lowercase letter. Users must include lowercase characters in their passwords to meet the password policy requirements.

Password with Number

Enabling this setting ensures that passwords must contain at least one numerical digit. Users will be

prompted to include numbers in their passwords to comply with the password policy.

Password with Special Character

This field mandates the inclusion of at least one special character in passwords. Special characters include symbols such as !, @, #, \$, etc. Users will need to use special characters to meet the password policy requirements.

Password Length

This setting defines the minimum length required for user passwords. Administrators can specify a minimum number of characters that passwords must contain. Users will need to create passwords with a length that meets or exceeds this number to meet the password policy requirements.

By configuring these fields in the password policy, administrators can establish specific requirements for user passwords, enhancing security and ensuring adherence to best practices for password management.

Page Title: personal-token

On this page

Personal Access Token

Overview

â€∢

Personal Access Token (PAT) is a string of characters that is used in lieu of password to authenticate users when trying to access the Motadata AlOps system. Currently, in context of Motadata AlOps, Personal Access Token (PAT) is used for accessing the data through APIs.

System Administrators can bind the roles and priviliges to a Personal Access Token when creating them. This will allow to fetch and display data according the user privilige and will also prevent unauthorized access to sensitive data.

At a macroscopic level, system administrators will create a Personal Access Token from within the system which will also carry the roles and privileges for the system access. The Personal Access Token will then be passed as a parameter in the API request. Now, whenever the API requests Motadata AlOps to send the data, the generated Personal Access Token will be validated. Only when the Personal Access Token is authenticated, system will send the requested data.

Navigation

â€⊂

Go to Menu. Select

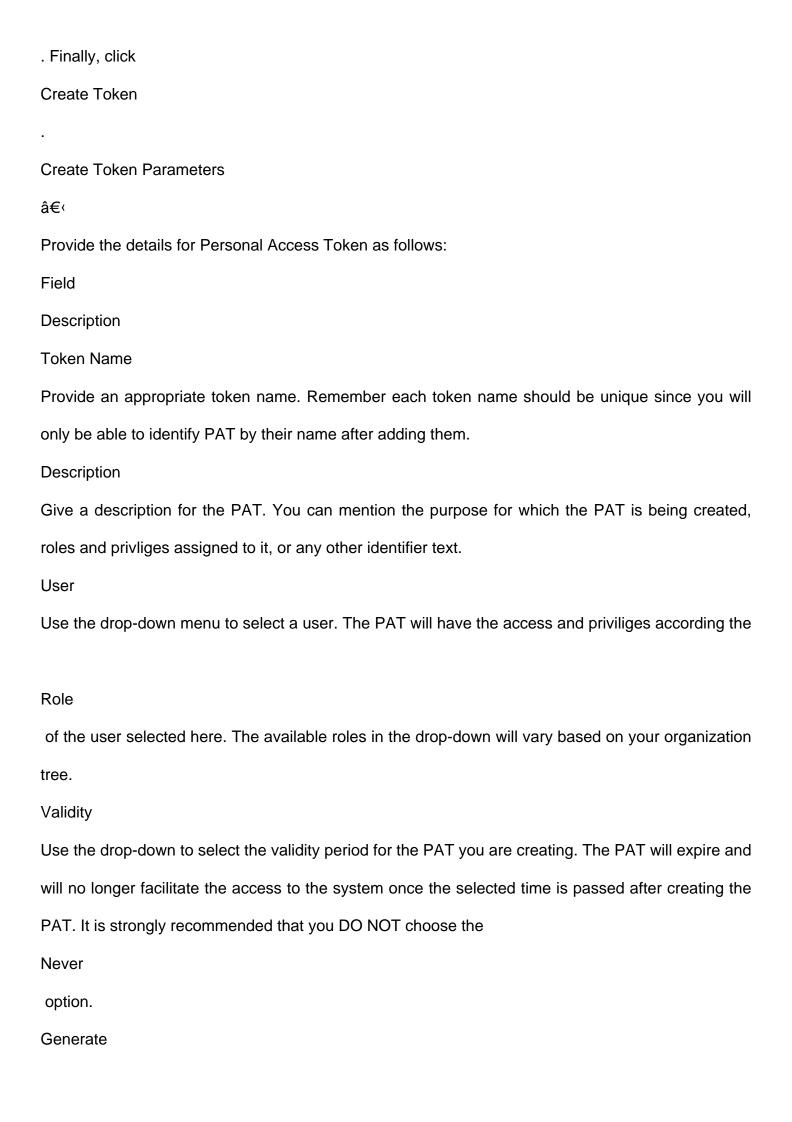
Settings

. After that, Go to

User Settings

. Select

Personal Access Token



Click on the button once you have filled all the details. Personal Access Token After clicking Generate , the PAT will be available in this field. You can view it by clicking on the eye icon. To copy it, click on the copy icon This will be first and last time you will be able to view the Personal Access Token. If the PAT is misplaced, you will have to generate a new PAT again. note Please keep in mind if the LDAP user associated with Personal Access Token is removed, the associated Personal Access Token will be automatically deleted. Select the Reset button to erase all the current field values, if required. Select Create Token to create the token with the information mentioned in all the parameters. Actions for Personal Access Token â€∢ Revoke a Personal Access Token â€∢

In the event of a data breach or when you wish to retire a Personal Access Token from accessing your system, you can revoke its access.

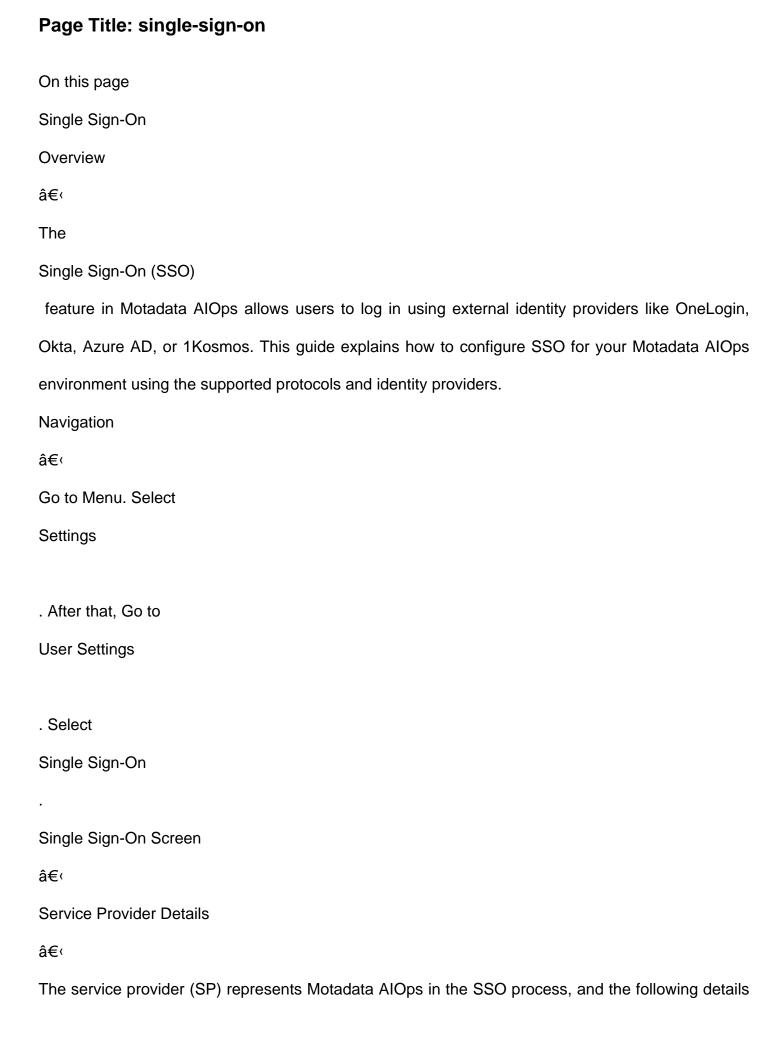
On the Personal Access Token screen, click on and select the

Revoke Access

option. An alert will appear on your screen. Click on

Yes

to confirm your action.



must be configured in your identity provider's platform: Field Description Service Provider Entity ID This is the URL that uniquely identifies Motadata AlOps. For example, this value is mapped to the EntityID in OneLogin. It is set by default but can be edited. The default value is motadata-sp Redirect URL This URL redirects users to the AIOps login page when accessing the domain. It is non-editable. For example, this value is mapped to ACS (Consumer) URL in OneLogin. Service Provider Login URL The URL that Motadata AlOps uses for authentication. This is a non-editable field. For example, this value is mapped to the Login URL in OneLogin. Service Provider Logout URL This URL handles sign-out requests from Motadata AlOps. It is non-editable. For example, this value is mapped to Single Logout URL in OneLogin. **Identity Provider Details** â€∢ Motadata AIOps supports integration with the following identity providers (IdP):

OneLogin, Okta, Azure AD, 1Kosmos

When configuring the identity provider, select either

Upload Metadata File

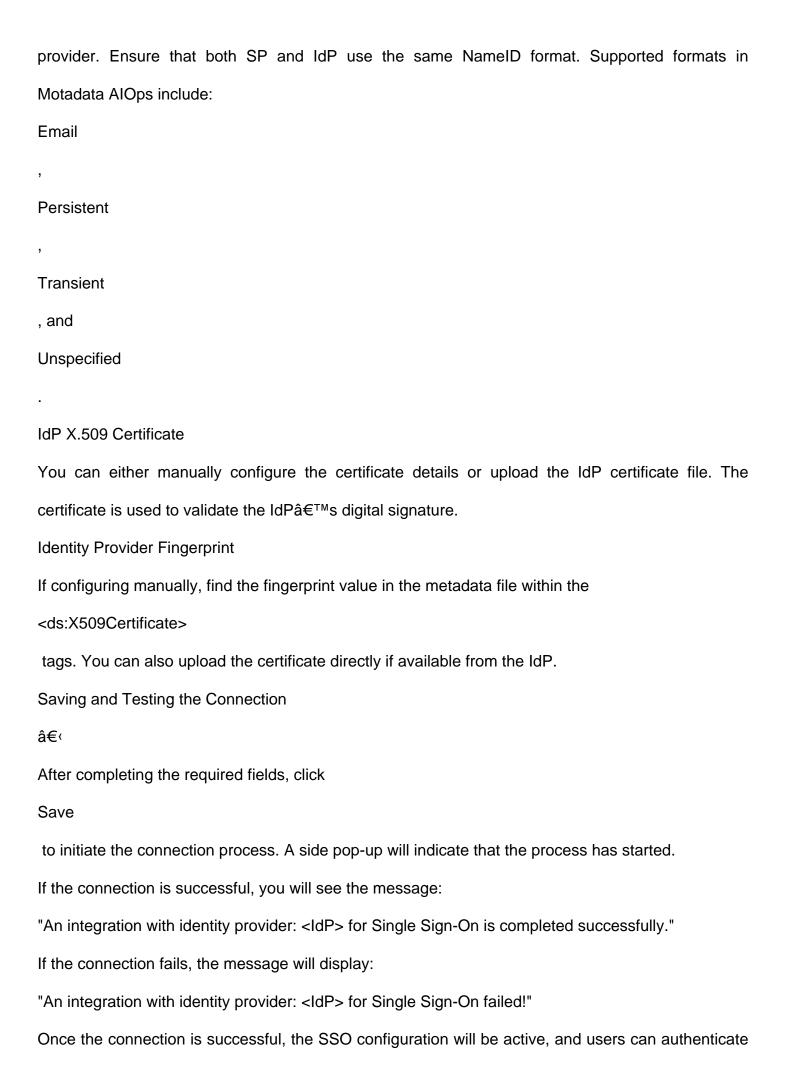
or

Configure Manually

to proceed.
If Uploading Metadata File
â€⊂
Field
Description
Identity Provider Metadata File
Upload the metadata file provided by your identity provider to automatically populate the IdP details.
This option is only available when you select
Upload Metadata File
in the previous field.
If Configuring Manually
â€⊂
When you choose to configure manually, fill in the following fields with the details provided by your
identity provider:
Field
Description
Identity Provider Entity ID
This field is used by Motadata AIOps to verify SAML responses from the identity provider. For
example, This field can be mapped with the 'Issuer URL' provided by OneLogin.
Identity Provider Login URL
It directs users to the IdP login page for authentication. For example, this field can be mapped to the
SAML 2.0 Endpoint (HTTP) provided by OneLogin.
Identity Provider Logout URL
This URL handles logout requests initiated from the service provider. For Example, this field can be
mapped to the 'Single Logout (SLO) Endpoint (HTTP)' provided by OneLogin.

This field defines how the subject (user) is identified between the service provider and identity

NameID Format



through the selected IdP.

This structured guide provides a clear step-by-step approach for configuring SSO in Motadata AlOps, ensuring users understand both automatic and manual configuration methods for their identity providers.

Authentication Process with Single Sign-On

â€⊂

Once a user logs in to Motadata AlOps using Single Sign-On, the system follows a verification sequence:

Initially, the system checks if the user already exists in the

User Settings

within Motadata AlOps.

If the user is not found in

User Settings

, the system then verifies the user with the configured Identity Provider (IdP).

If the user is successfully authenticated through the IdP, they are granted access to Motadata AlOps using SSO. Subsequently, the system adds the user to

User Settings

for future reference.

This process ensures effortless access for users authenticated through SSO, maintaining synchronization between

User Settings

and the configured IdP.