References

Revision 20230904

Denodo Inc.: 525 University Avenue, Suite 31, Palo Alto, CA 94301. USA www.denodo.com

How To Configure Ping Identity for SSO in the Denodo Solution Manager

1 INTRODUCTION

In this document you will learn how to:

- Configure your Ping Identity account to be able to use it as an Identity Provider (IdP) for the Solution Manager.
- Create a user in Ping Identity.
- Create a group.
- Register the Solution Manager as a SAML application.
- Register the Solution Manager as an OpenID application.
- Enable single sign-on (SSO) in the Denodo Solution Manager 8.0, using your Ping Identity account.

This document explains how to register the Solution Manager as a SAML application and as an OpenID application. In a real scenario, you will only do one or the other.

Some organizations are transitioning from Windows Active Directory and Kerberos to “cloud-friendly” Identity Providers (IdP). These IdPs usually provide support for authentication protocols like OpenID and SAML.

Including the roles in the assertion with Oauth is not supported by Ping Identity so we will be explaining this option in this document.

2 SUMMARY OF THE PROCESS

On this document we will follow these steps to configure PingIdentity with Denodo:

- In Ping Identity
  - Create a population.
  - Create a user.
  - Create a group and assign it to the user.
  - Register the Solution Manager as a SAML application or an OpenID application.
- In the Denodo Solution Manager:
  - Enable single sign-on with OpenID or SAML (you cannot enable both).
  - Create a role with the same name as the group you have created in Ping Identity.
  - Grant privileges to this new role.

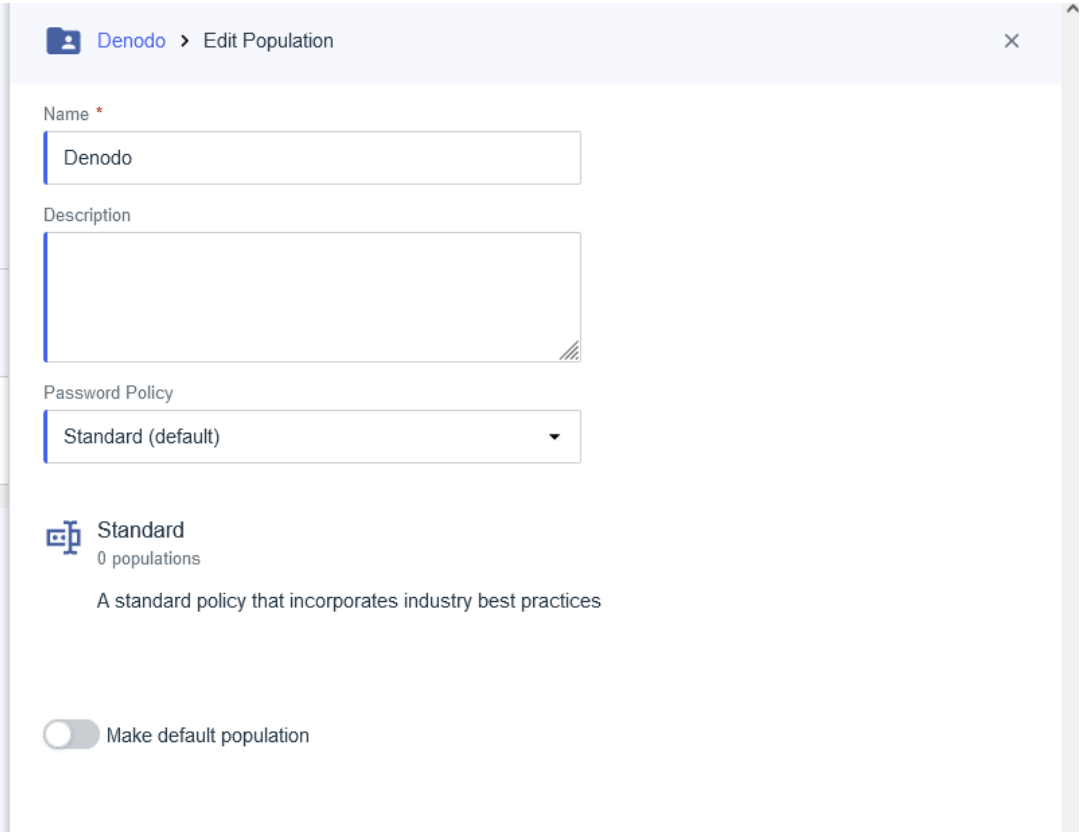
Once this is completed, single sign-on will be enabled on the Solution Manager and users will only have to provide their password in Ping Identity.

An OpenID access token and a SAML assertion usually include the groups to which this user account belongs; that is, the user account associated with this token/assertion. When the Solution Manager receives the token/assertion, it searches the roles defined in Solution Manager that have the same name. The privileges granted to these roles will be the privileges of this user. Note that not all the privileges defined in the token/assertion have to exist in the Solution Manager.

3 PING IDENTITY CONFIGURATION

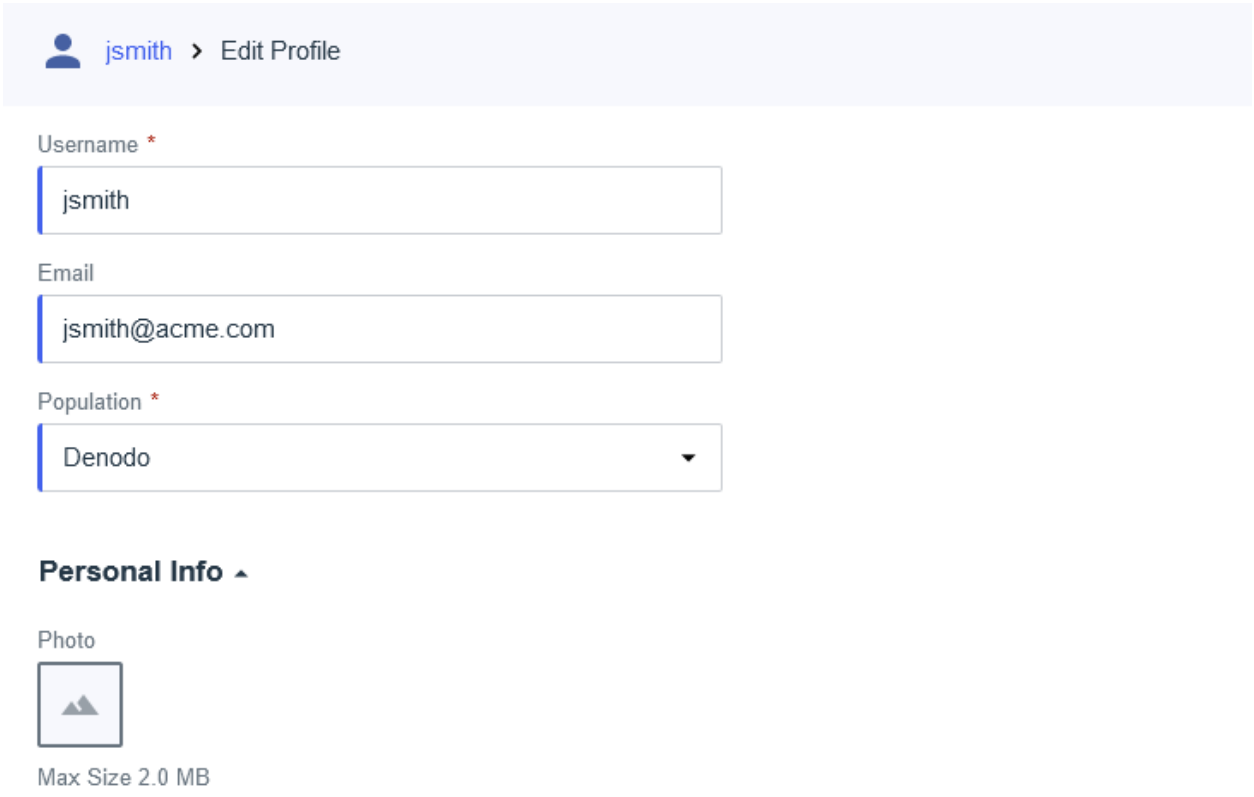
3.1 PING IDENTITY POPULATIONS

A population defines a set of users and can help you make user management simple. Click on `Identity > Populations`. Then click on the Add button and in this form, enter the details of the new population. For example, create the population `Denodo`.



3.2 CREATE A USER IN PING IDENTITY

1. Log in to Ping Identity as the admin user.
2. Click on `Identities > Users`. Then click on the Add User button and in this form, enter the details of the new user. Let's say: `jsmith@acme.com`
3. Set the user population.



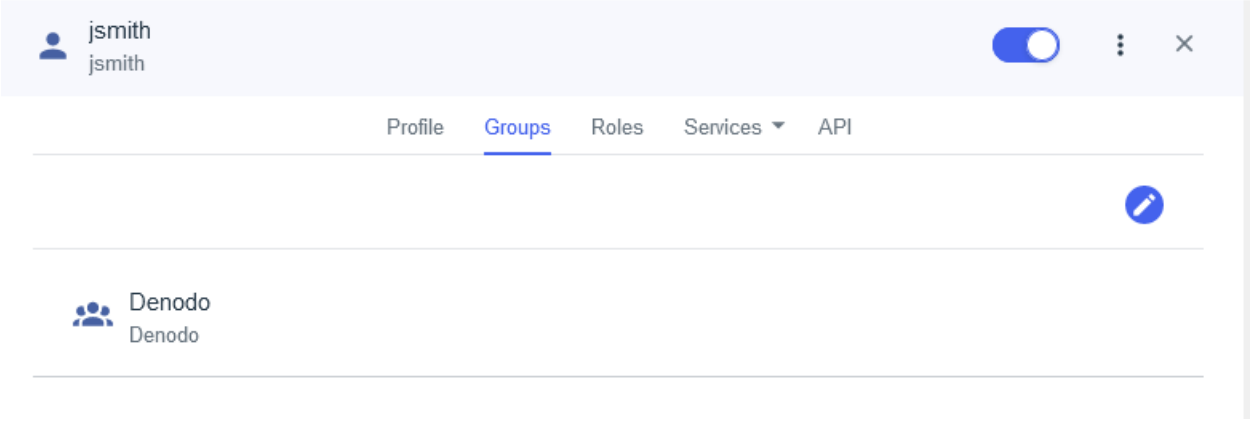
3.3 PING IDENTITY GROUPS

Groups organize a collection of user identities and make it easier to manage access to applications. Click on `Identities > Groups`. Then click on the Add group button and in this form, enter the details of the new group. For example, create the group `Denodo`.

3.4 ASSIGN GROUPS TO A USER

To assign a group to a user, do the following:

1. Click on the user and on the tab Groups. Then, type the name of the group (Denodo) to assign it to the user.

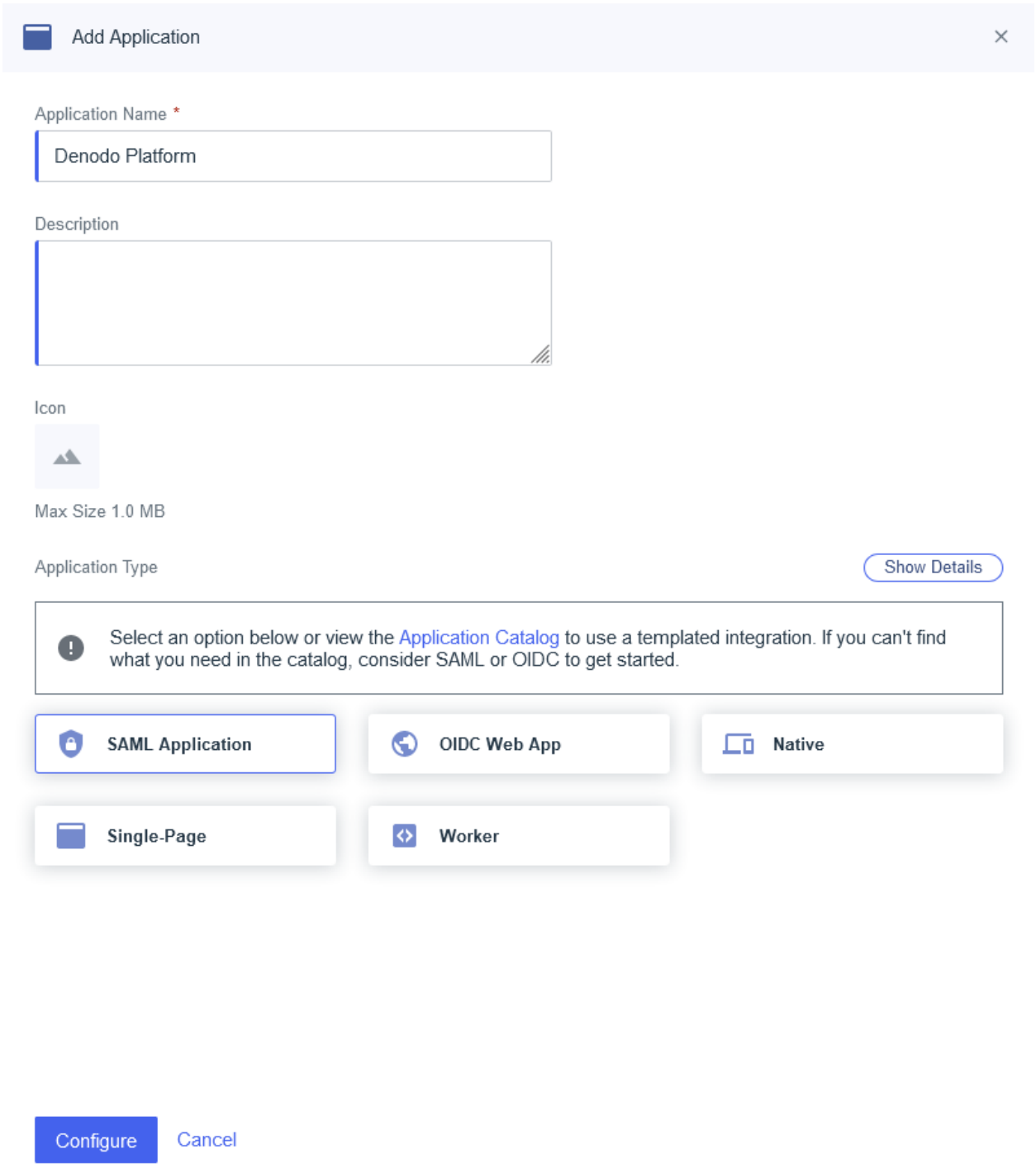


4 SINGLE SIGN-ON WITH SAML

4.1 REGISTER THE SOLUTION MANAGER AS A SAML APPLICATION

Follow the following steps:

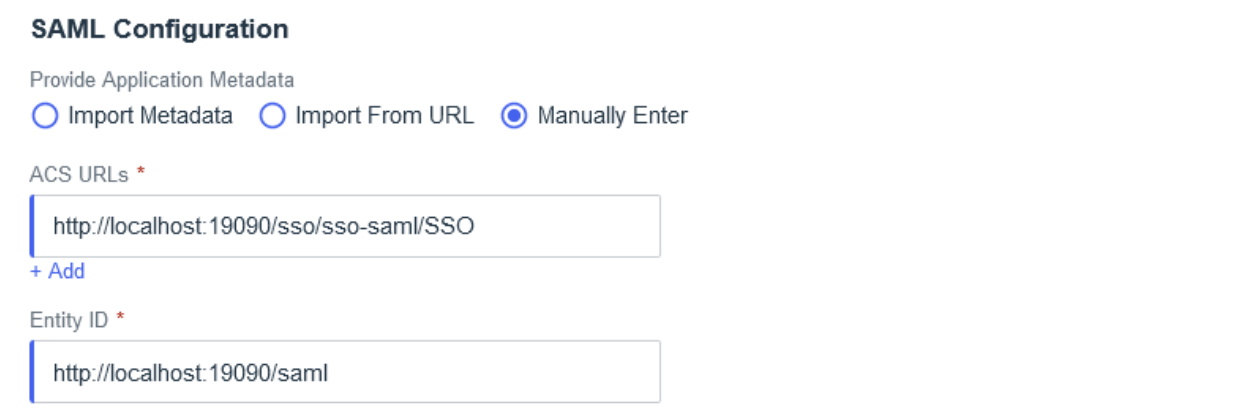
1. Login in Ping Identity as the admin user.
2. Click on `Applications > Add`.
3. Enter a name and select `SAML Application`.



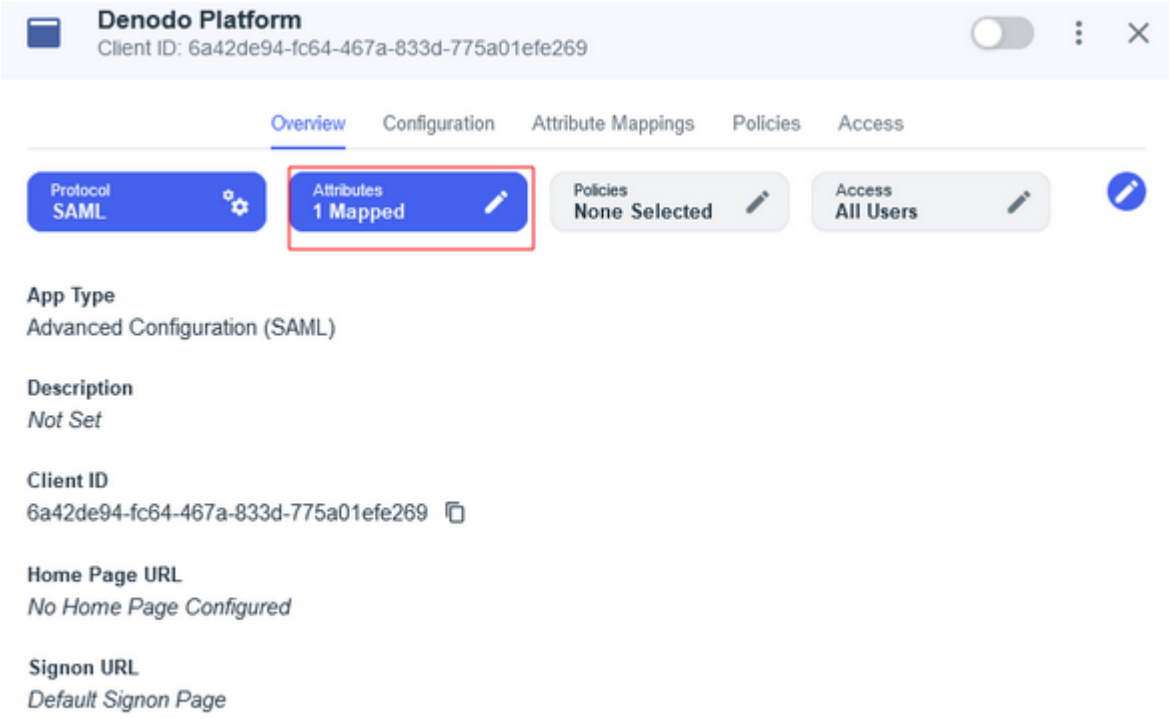
4. Click on `Configure`.
5. Select Manually enter and set:
    - ACS URLs:`http://localhost:19090/sso/sso-saml/SSO`

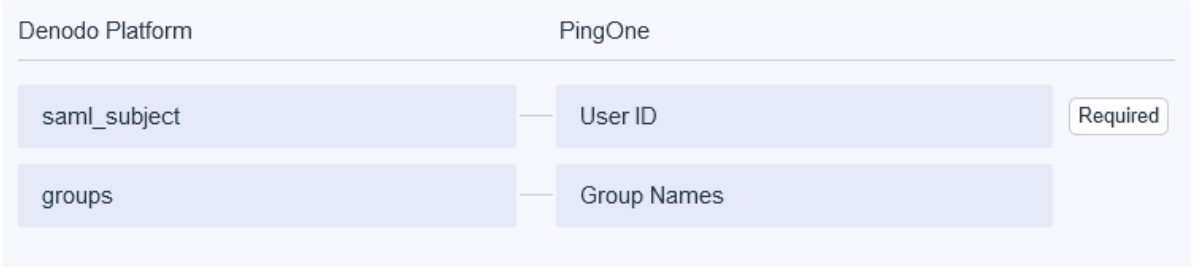
- Entity ID: `http://localhost:19090/saml`

6. Click on Save.

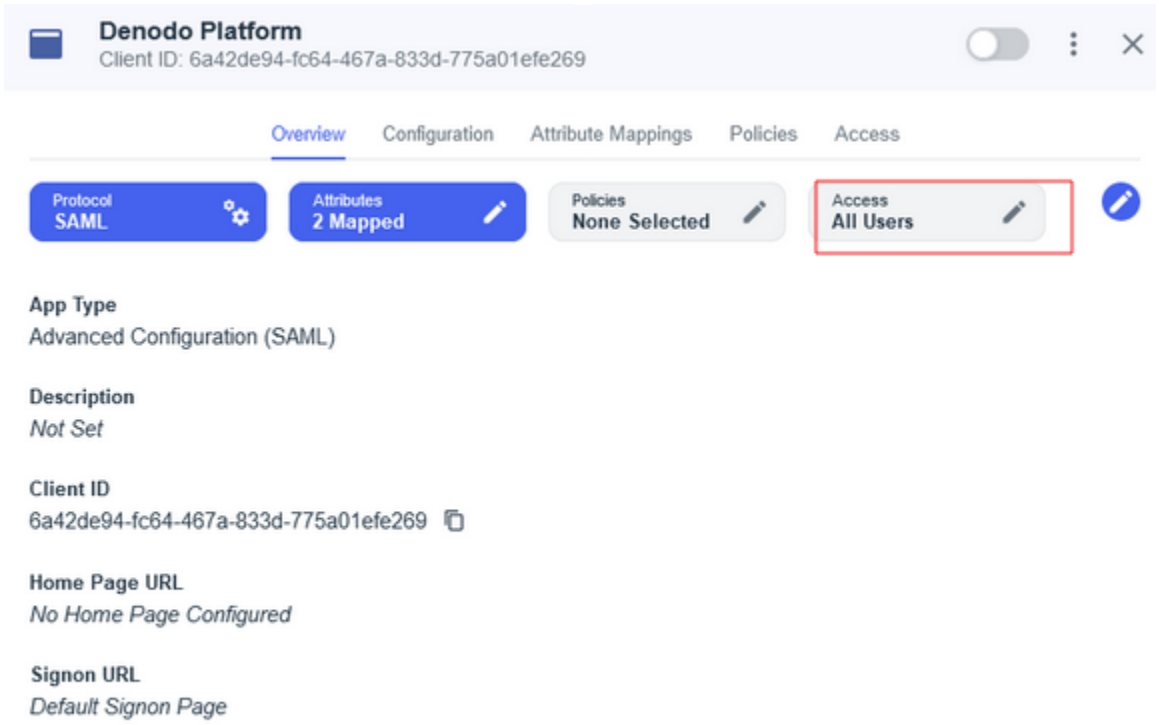


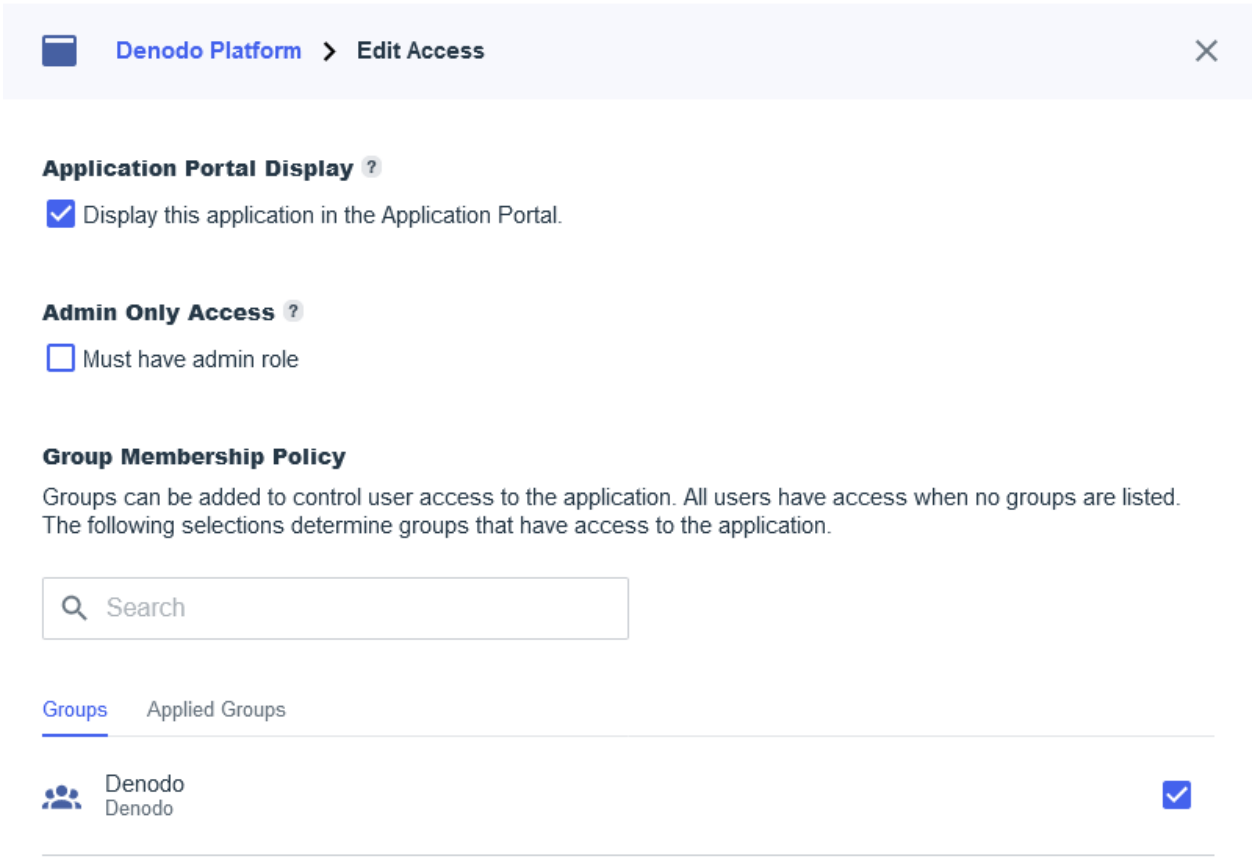
7. Click on the app created and go to the Attributes tab. And add the following attribute: `groups - Group Names`.





8. Now, go to the Access tab and enable The group Denodo.


Denodo Platform
Client ID: 6a42de94-fc64-467a-833d-775a01efe269
Overview
Configuration
Attribute Mappings
Policies
Access
Protocol
SAML
Attributes
2 Mapped
Policies
None Selected
Access
All Users
App Type
Advanced Configuration (SAML)
Description
Not Set
Client ID
6a42de94-fc64-467a-833d-775a01efe269
Home Page URL
No Home Page Configured
Signon URL
Default Signon Page

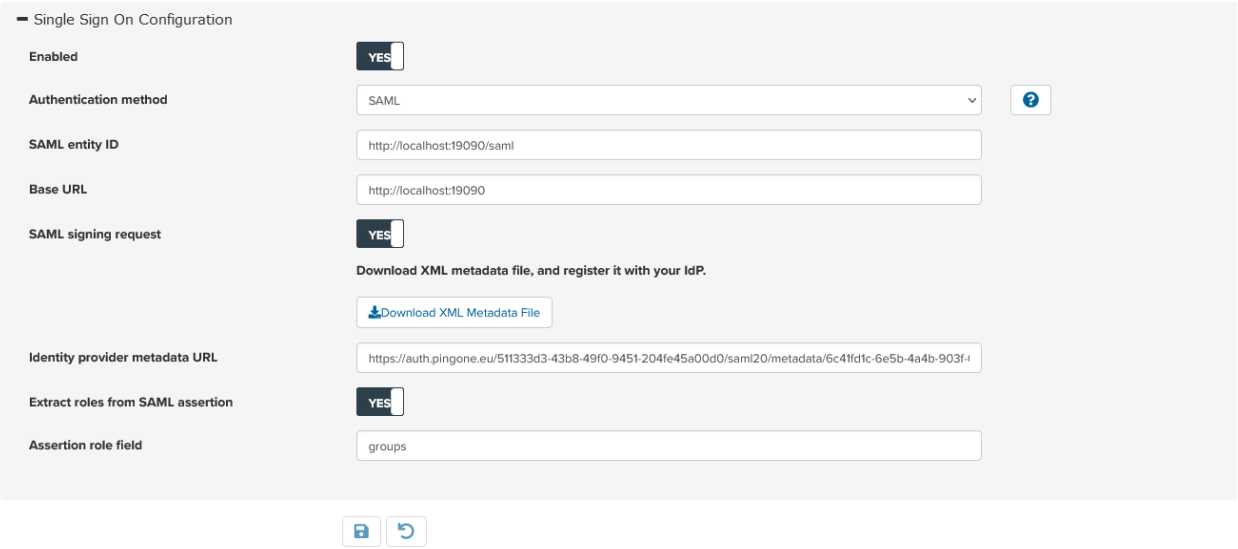


4.2

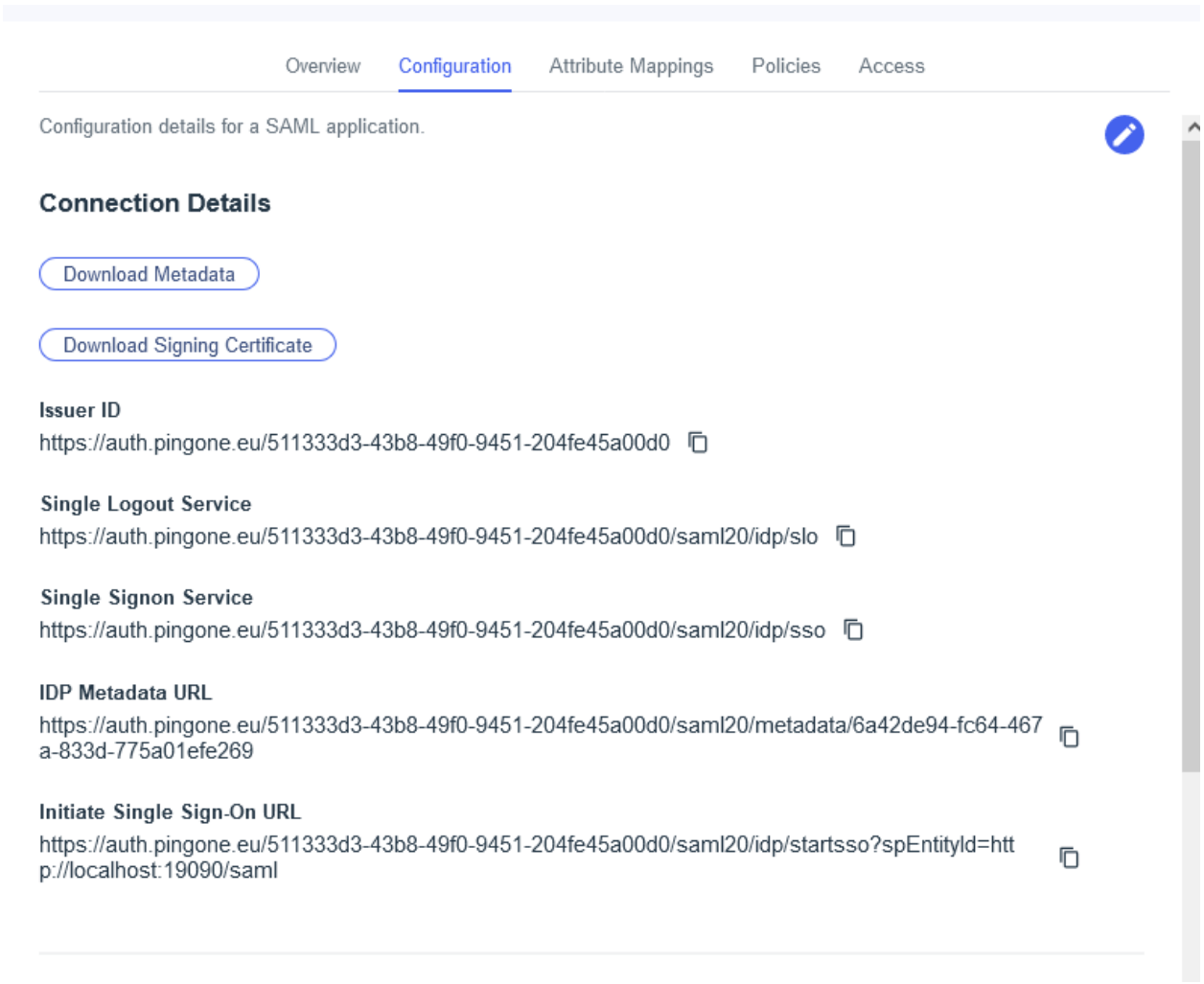
4.3 ENABLING SINGLE SIGN-ON IN SOLUTION MANAGER WITH SAML

Follow these steps:

1. Log in to Solution Manager Web Tool with an administrator user.
2. Click the menu `Configuration > Authentication`.
3. Expand the panel Single Sign On Configuration, enable this feature and select `SAML` as Authentication method.



4. Provide the following:
   - **SAML entity ID**: The entity ID uniquely identifies your Solution Manager installation to the IdP. It must match the Audience URI (SP Entity ID) configured on Ping Identity. For example: `http://localhost:19090/saml`.
   - **Base URL**: The base URL of the web container of the Solution Manager. It will be used as a base URL for Assertion Consumer Service in SAML requests to the IdP. For example: `http://localhost:19090`.
   - **SAML signing request**: if it is enabled, the Solution Manager will sign authorization requests to the IdP.
   - **Identity provider metadata URL**: this is a URL of the configuration file that the IdP (Ping Identity) provides for the application you registered.
     To obtain this URL, go back to Ping Identity, open the details of the application and in the Configuration tab copy the url `IDP Metadata URL`.

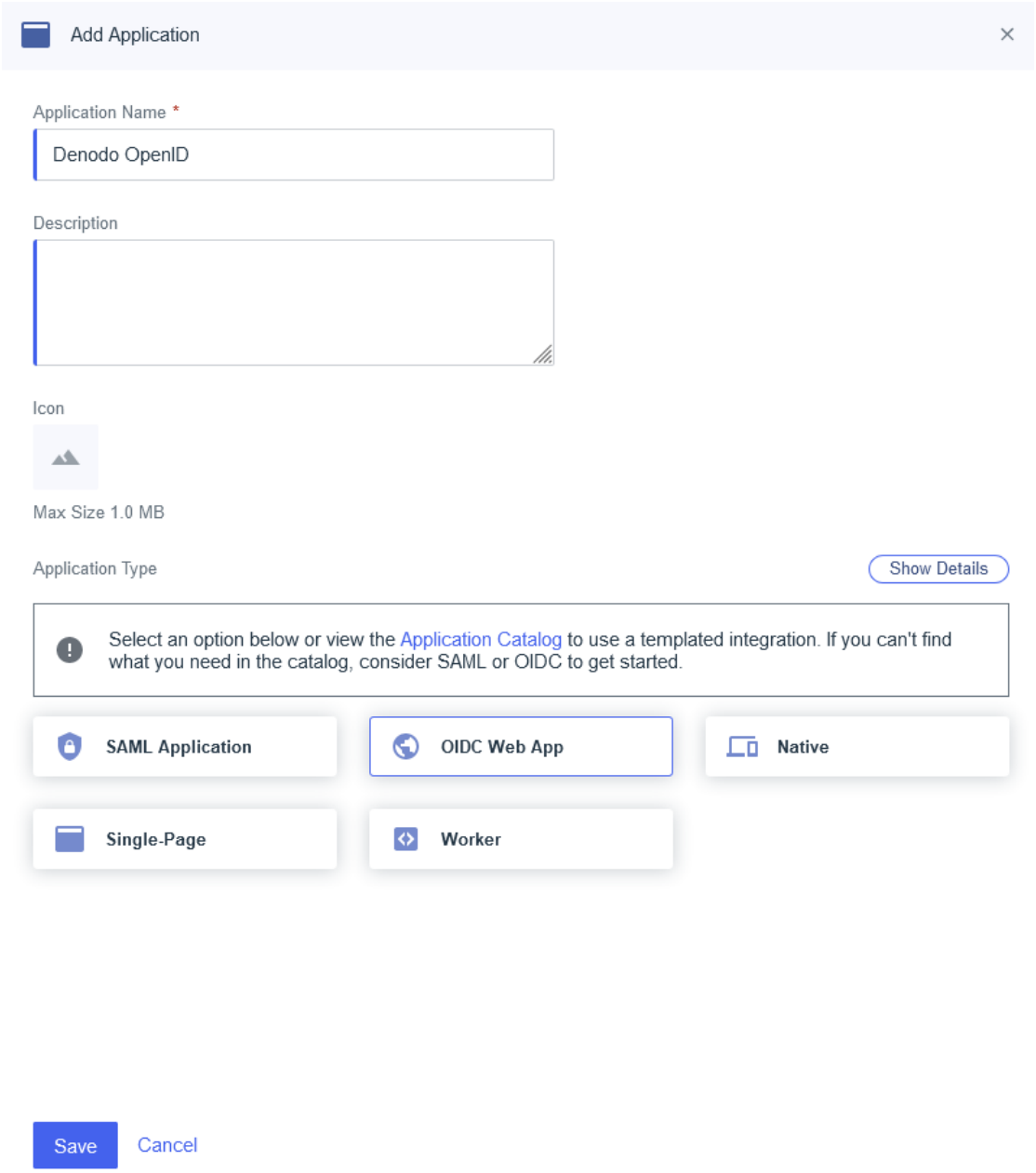


- **Extract roles for SAML assertion**: Enable this. By enabling this option, the Solution Manager will extract the roles of the users that are trying to log in, from the SAML assertion. If this option was disabled, you would have to configure the global LDAP settings of the Solution Manager so the Solution Manager can obtain the roles of the user.
- **Assertion role field**: Fill with the attribute name created for retrieving user groups. For instance: `groups`.

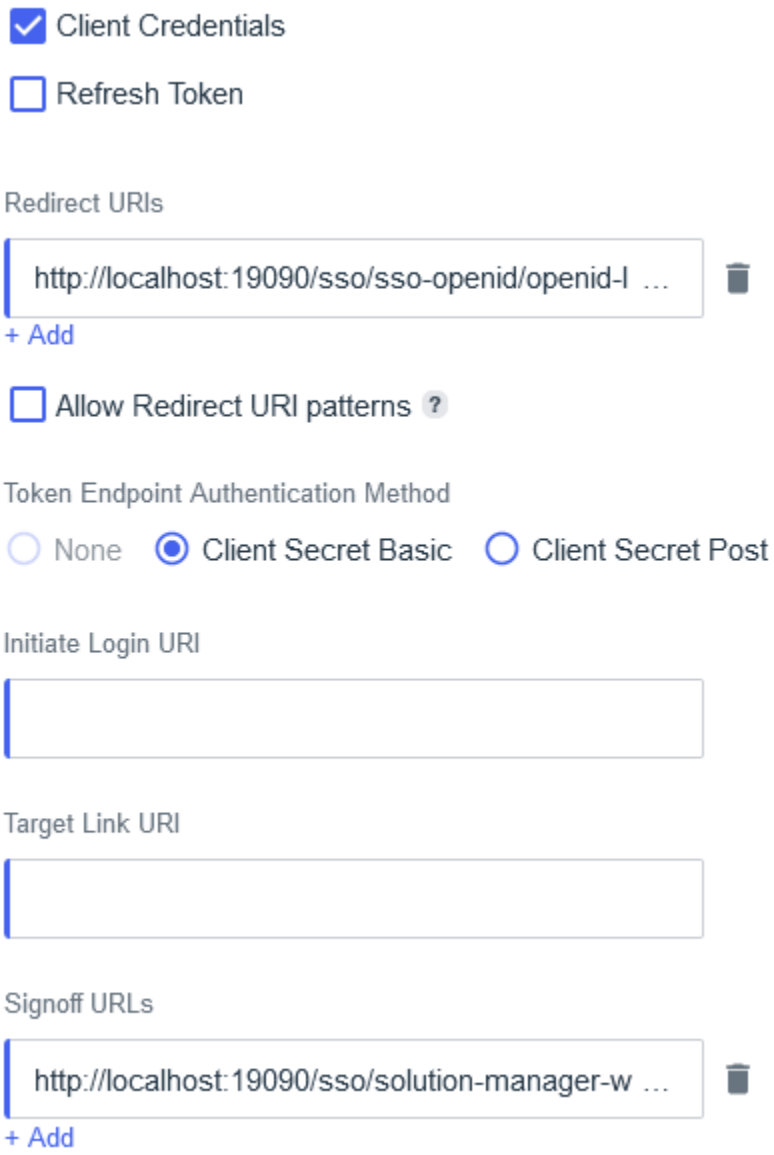
5 SINGLE SIGN-ON WITH OPENID

5.1 REGISTER AN OPENID APPLICATION IN PING IDENTITY

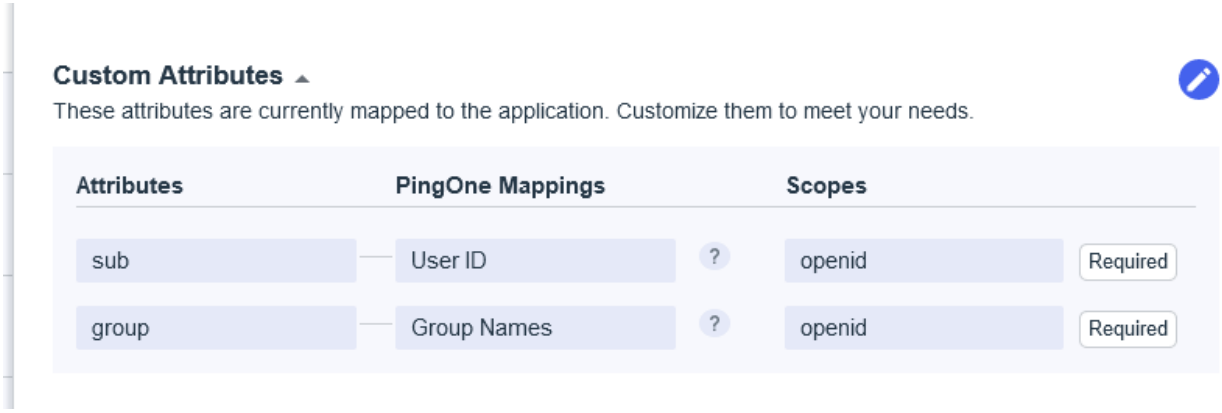
1. Login in Ping Identity as the admin user.
2. Click on `Applications > Add`.
3. Enter a name and select `OIDC Web App Application`.



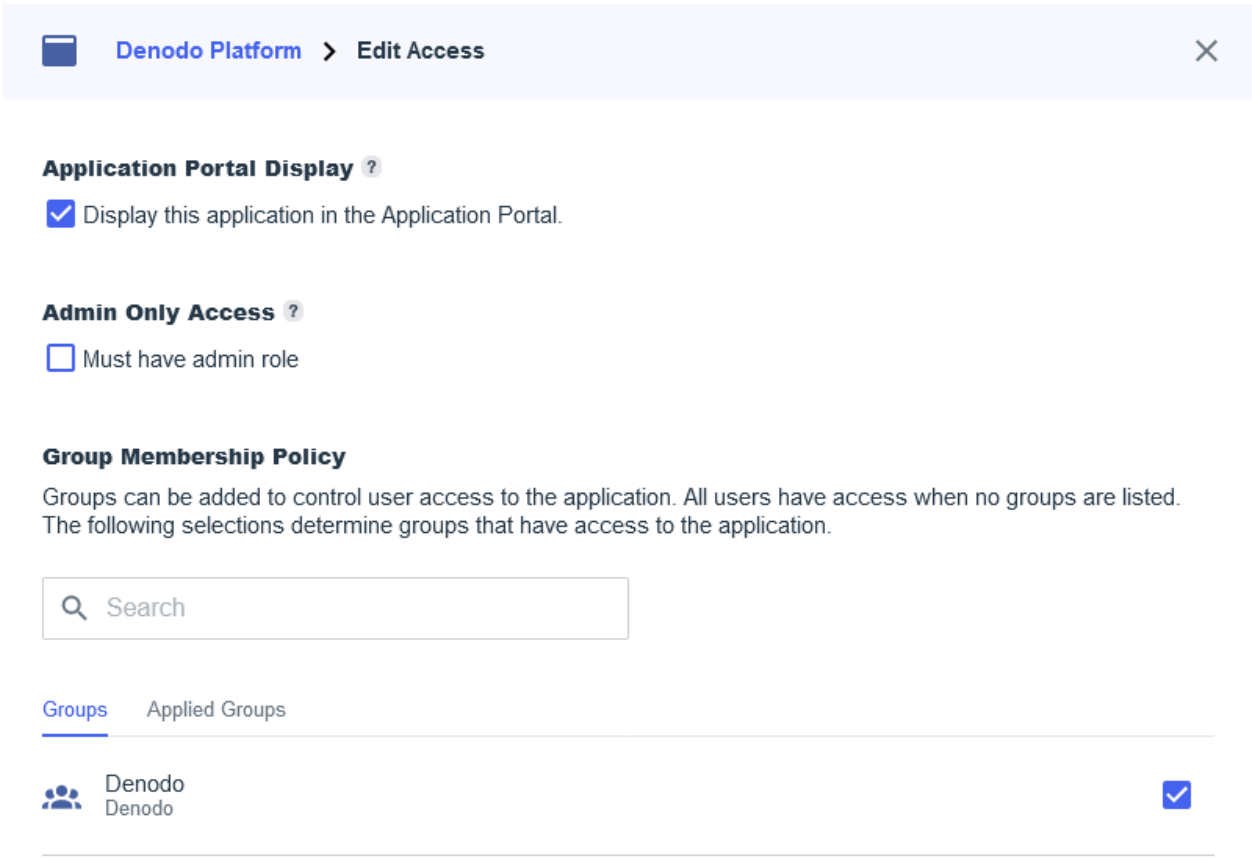
4. Edit the configuration and set the redirect URIs and Signoff URLs. Also, enable `Client Credentials`.
5. Click on Save.



6. Click on the app created and go to the attribute mapping tab. And Set The following attributes: `sub-User ID`, `group - Group Names`.



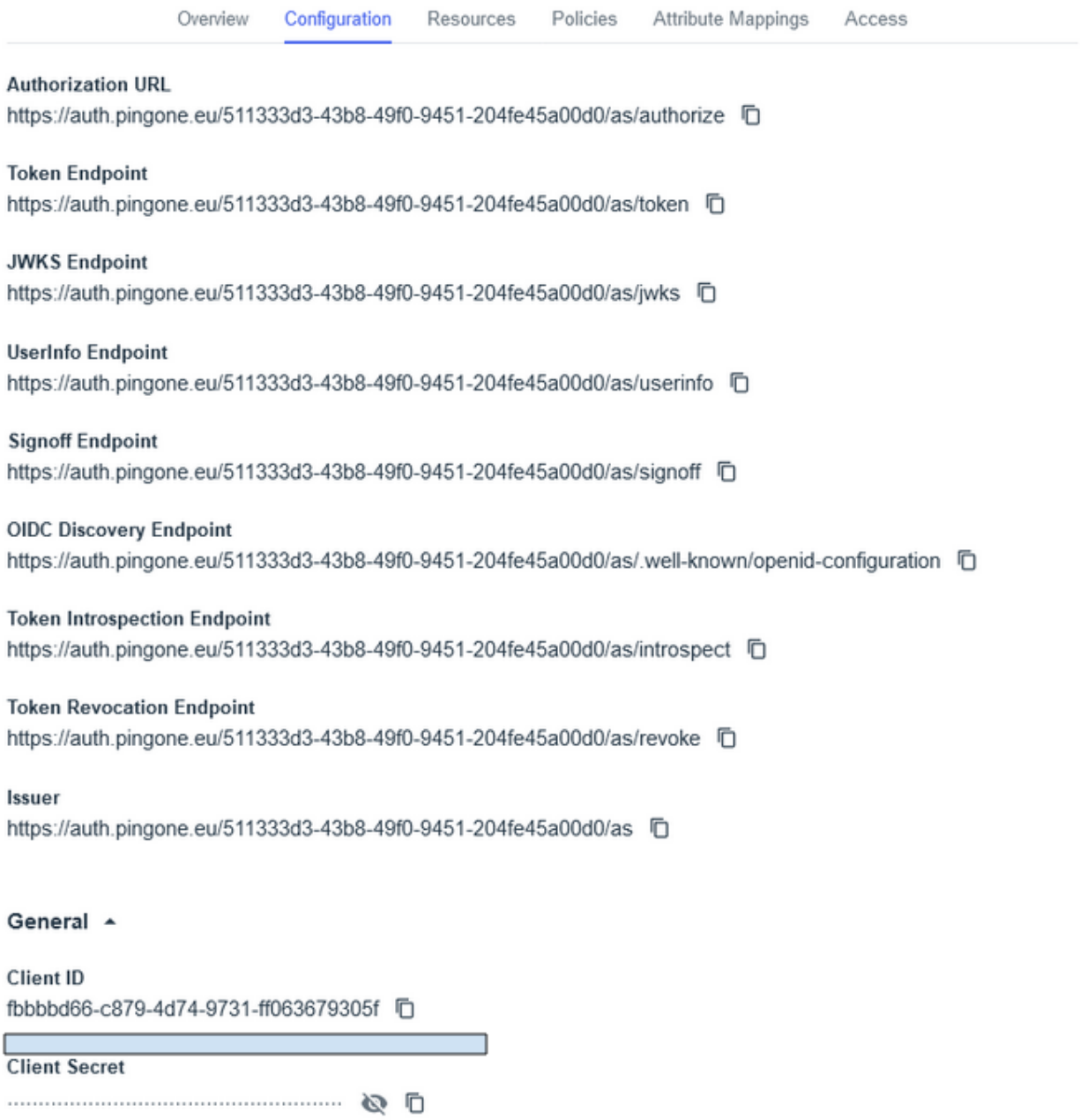
7. Now, go to the Access tab and enable The group `Denodo`.



5.2 ENABLING SINGLE SIGN-ON IN SOLUTION MANAGER WITH OPENID

Follow these steps:

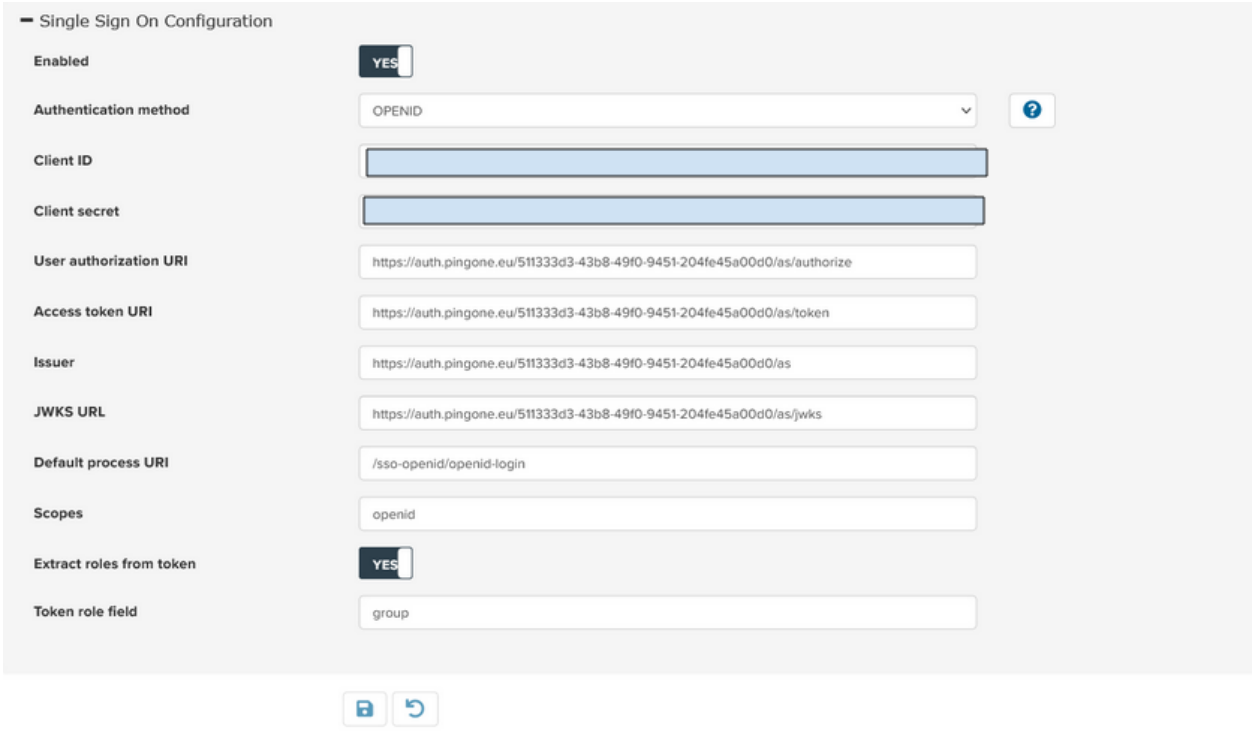
1. Log in to Solution Manager Web Tool with an administrator user.
2. Click the menu `Configuration > Authentication`.
3. Expand the panel Single Sign On Configuration, enable this feature and in the Authentication method, select `openID`.
4. You can obtain the values required in the configuration tab of the application in Ping Identity.



5. Introduce the following configuration:
    - **Client ID**: copy and paste the Client ID of Ping Identity.
    - **Client secret**:copy and paste the Client Secret of Ping Identity.
    - **URI Authoritation URI**: copy and paste the **Authorization URL.**
    - **Access token URI**:copy and paste the **Token Endpoint**.
    - **Issuer**:copy and paste the **Issuer.**
    - **JWKS URL**: copy and paste the **JWKS Endpoint.**

- **Default process URI**: `/sso-openid/openid-login.`
- **Scopes**: `openid.`
- **Token role field**: `group.`

6. Click on Save



5.3 SSO TOKEN CONFIGURATION

Once OpenId is configured, follow these steps to avoid the error: `Could not obtain the username using the claim preferred_username`

- Stop all Solution Manager servers
- Edit `SSOTokenConfiguration.properties` file under `<SOLUTION_MANAGER_HOME>/conf/denodo-sso`
- Add `openid.userNameClaim=sub`
- Start the Solution Manager and the Solution Manager Web Tool again.

5.4 SINGLE SIGN ON

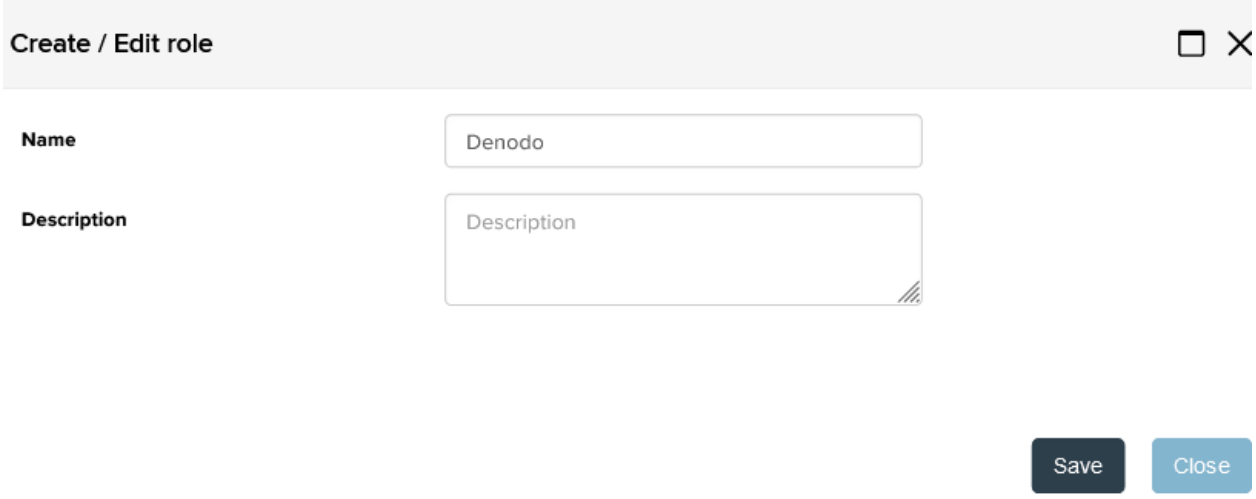
After following these steps the single sign on configuration should be ready.

6 CREATE ROLES IN SOLUTION MANAGER

After enabling SAML or OpenID authentication in Solution Manager, you have to create roles that have the same names as the ones you created in Okta.

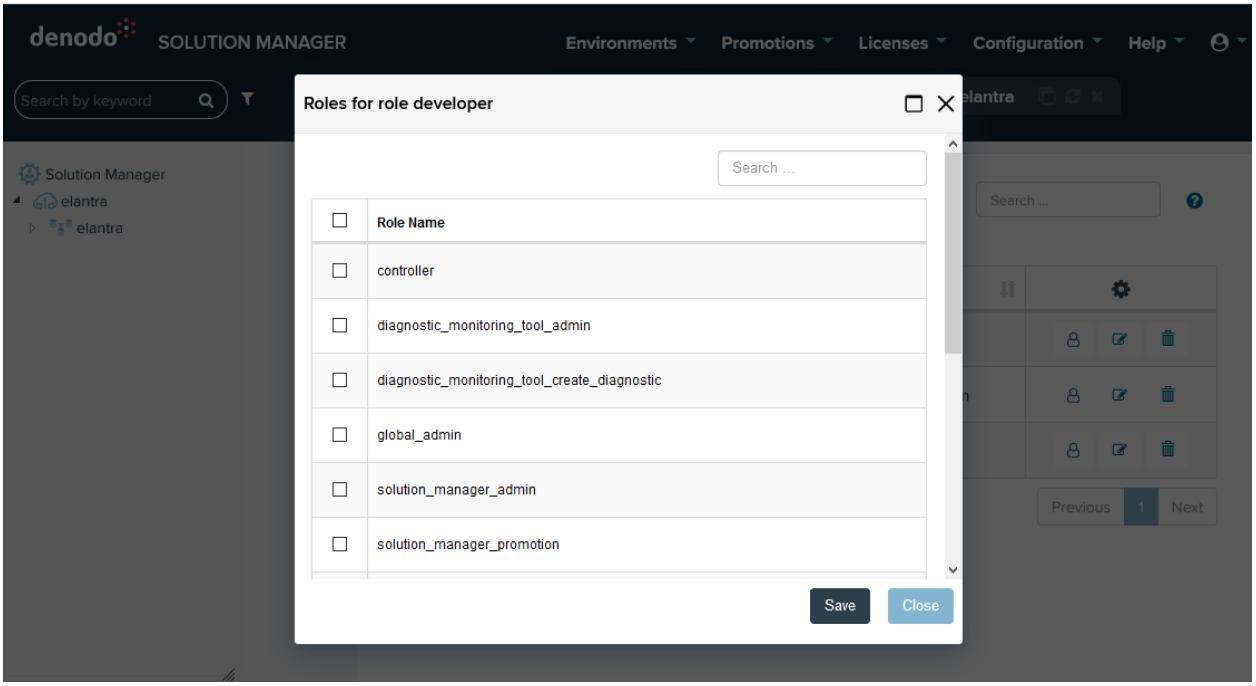
As with LDAP authentication of Virtual DataPort, you do not need to create all the roles that a user of Okta may have; only create the ones you need to.

1. Log in to the Solution Manager with an administrator account.
2. Go to `Configuration > Role management` and click New .



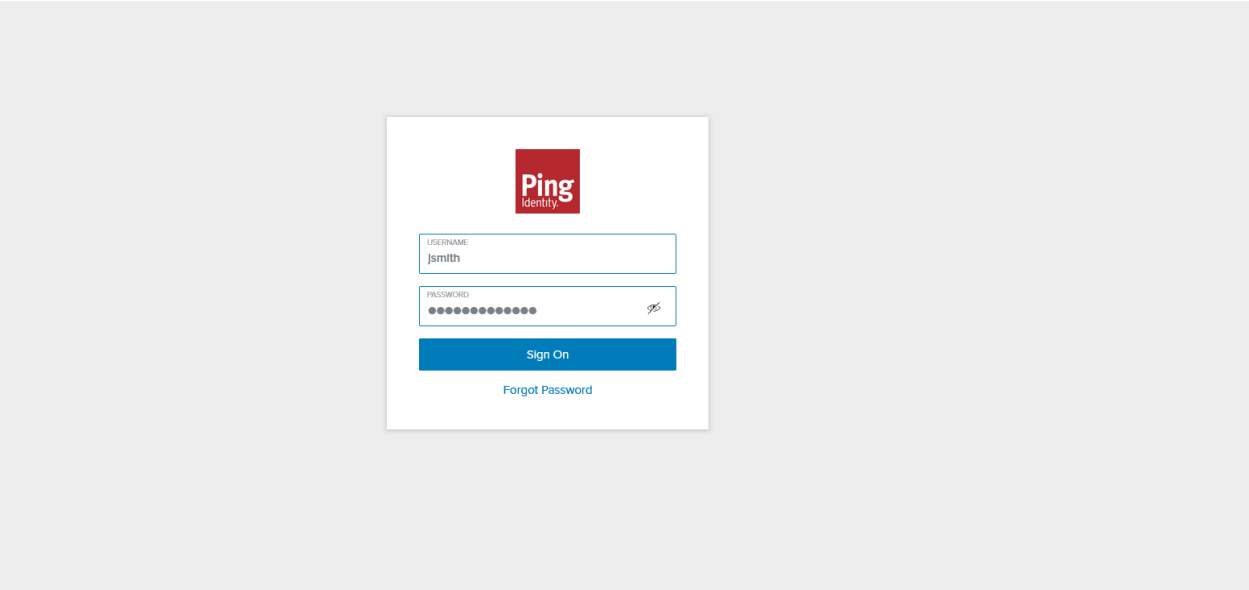
3. Create a role for the roles you have assigned. In this document: `Denodo`.
4. Grant the role `global_admin` to the new role (`Denodo`) (see Authorization details):

   You can grant any other role, this is just an example.



5. At this moment, the single sign-on configuration should be ready. Finally, open a private window in your browser and go to `https:/localhost:19090/solution-manager-web-tool/Login`.

   Click `Single sign-on`. Log in to Ping Identity using the new user account you have created in Ping Identity.



[How To Configure Okta for Single Sign-On in Denodo Solution Manager 8.0
Ping Identity Docs]