

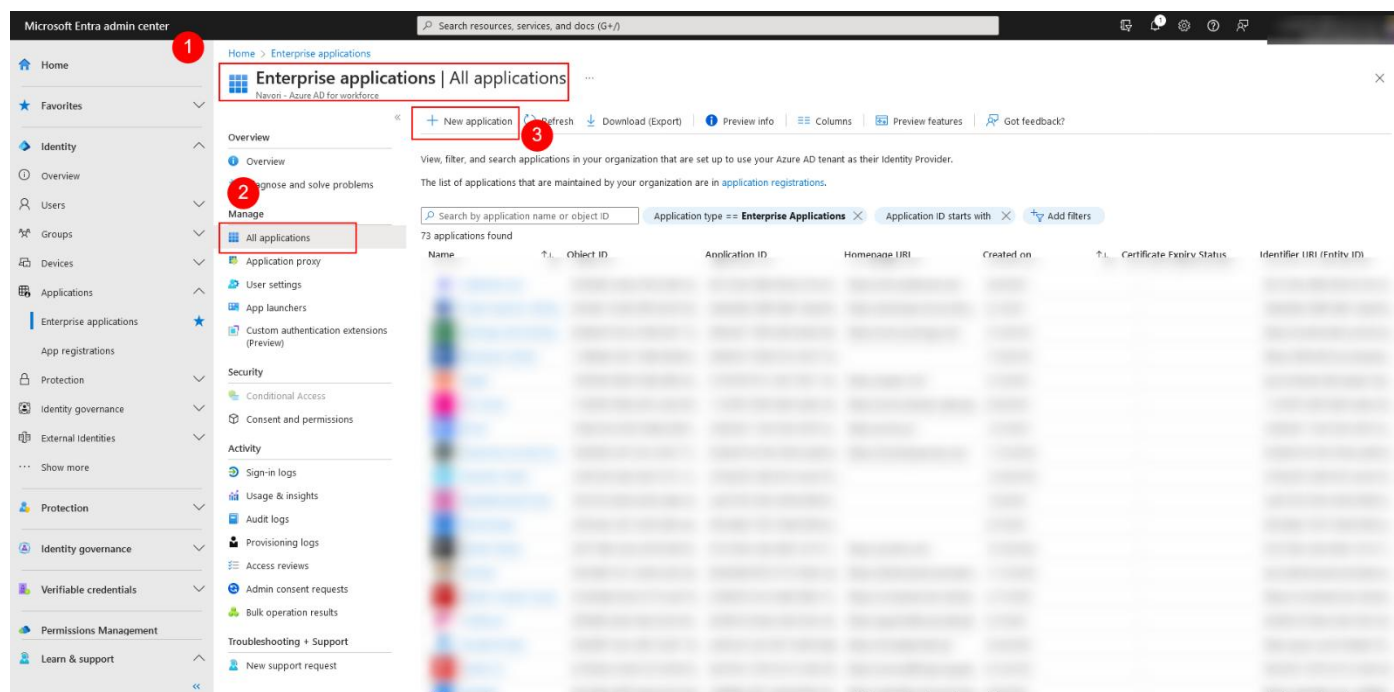
## HOW TO SETUP AZURE AD SSO VS QL MANAGER

For configuring Azure ad SSO vs ql manager there is the below requirement

1. You should have access and privilege of entra.microsoft.com
2. Ql server must be 2.7.5 + version.

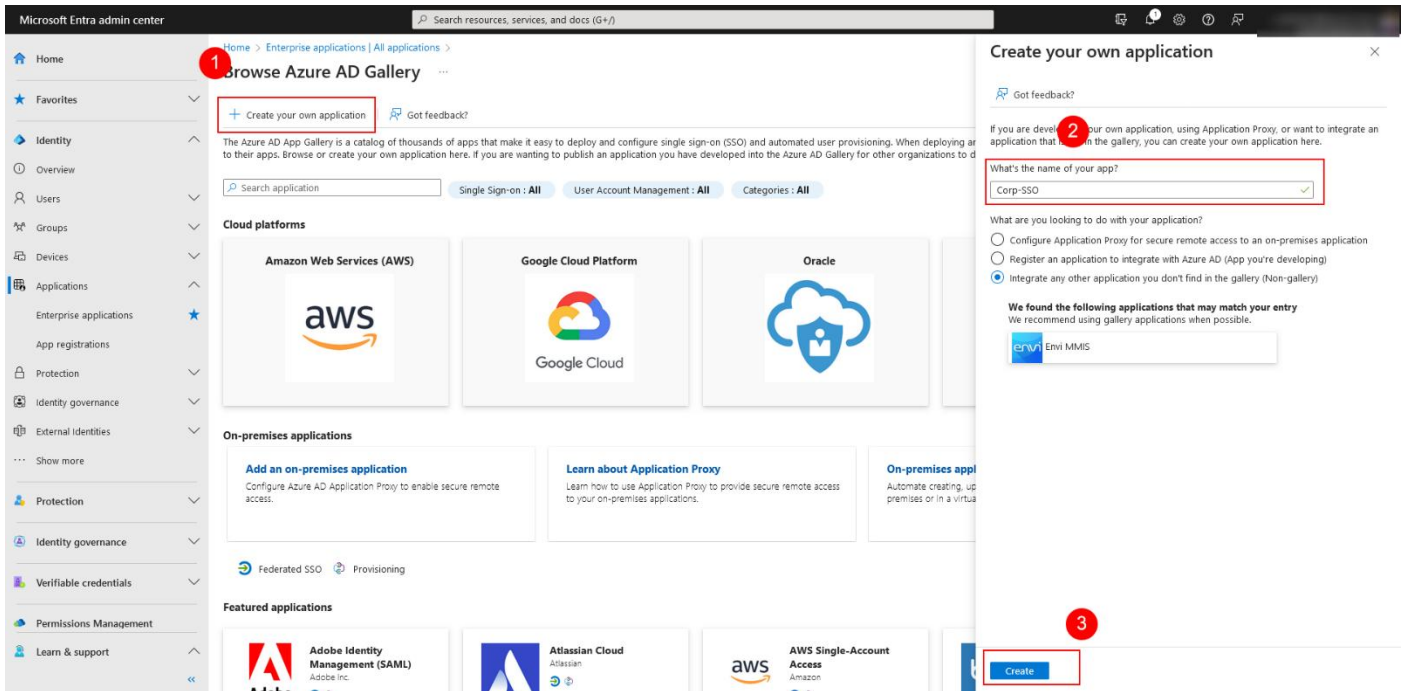
Login to <https://entra.microsoft.com>

1. Click on application >Enterprise application
2. + New application



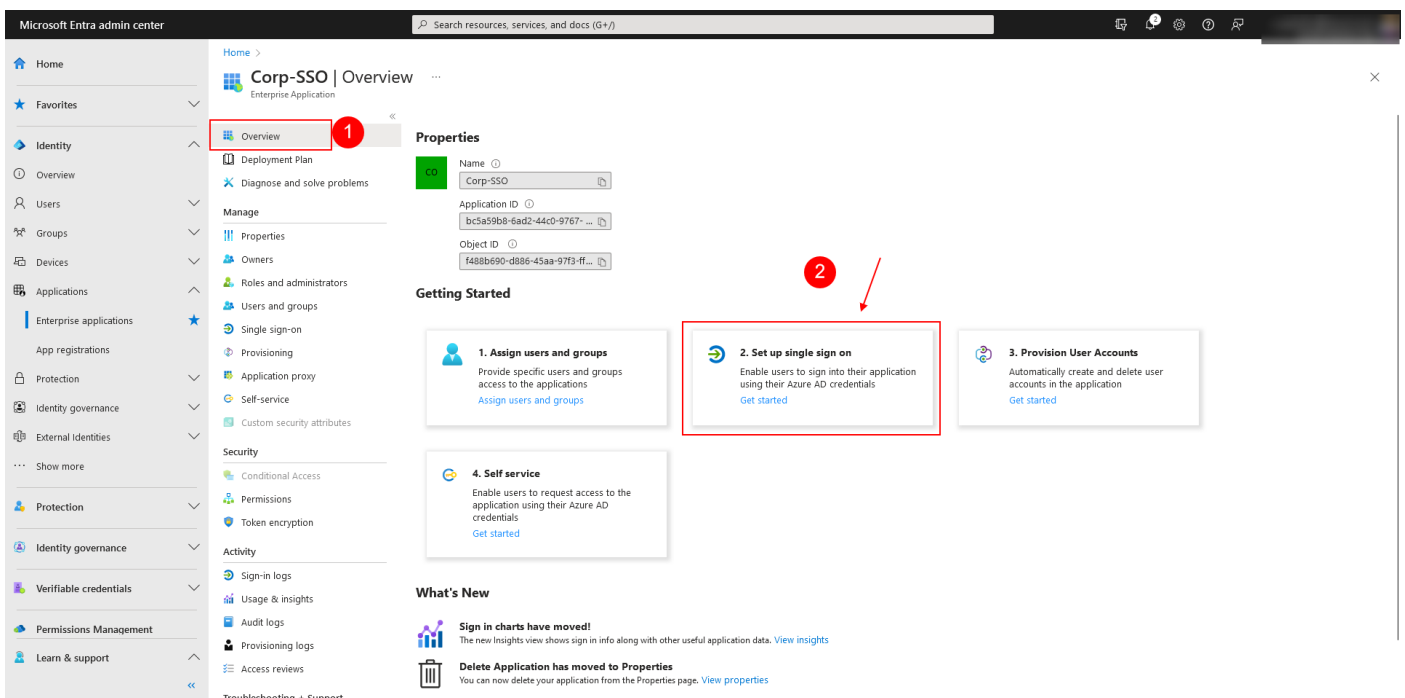
In the next screen Enterprise application > all applications> Browser Azure AD gallery

1. Create your own application.
2. Create your own application put an application name



In application overview.

Click on Setup single sign-on.



JD Molecule Sdn Bhd (844324-V)

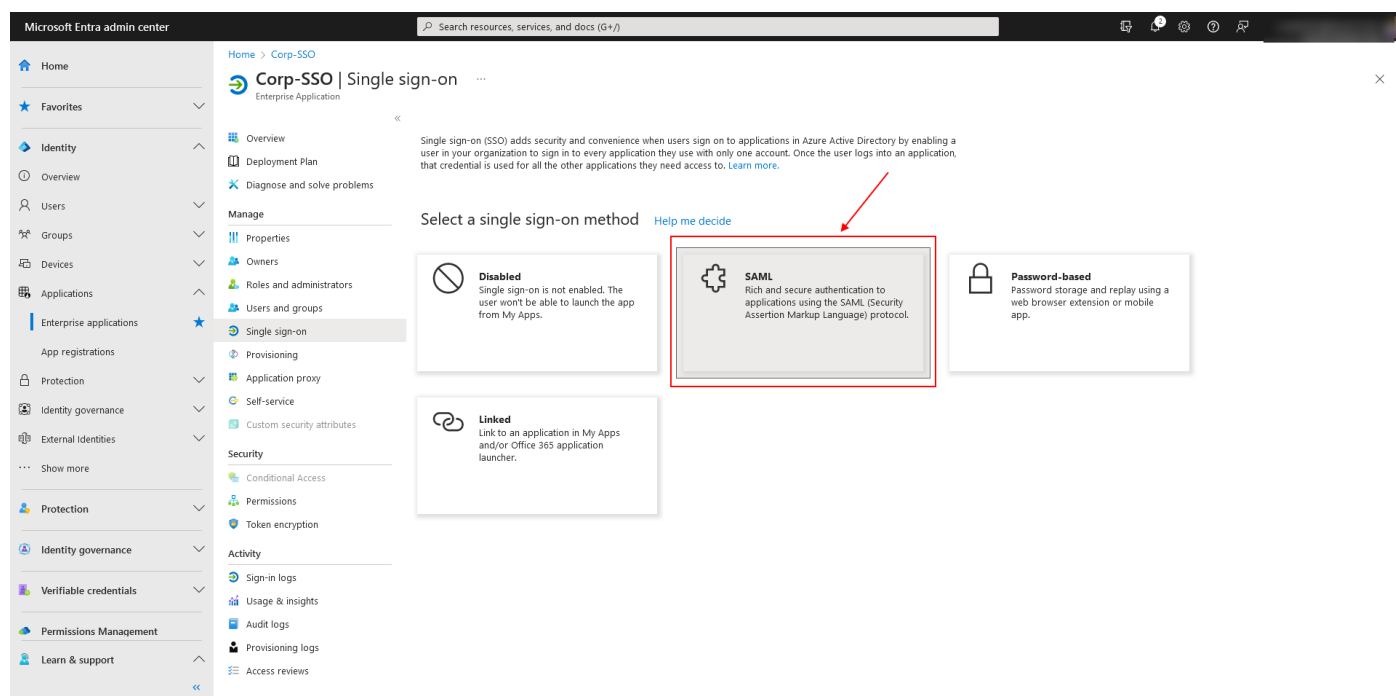
Wisma JDM, 12, Jalan Astaka L, U8/L, Bukit Jelutong Business & Technology Center,  
40150 Shah Alam, Selangor, Malaysia

tel +603.7846.6018  
skype jdmolecule

fax +603.7846.6068  
website www.jdmolecule.com

email outsource@jdmolecule.com

In the next screen single sign On Click on SAML



after clicking on SAML it will show you the next screen look like below.

## Edit Basic SAML configuration

1. Identifier (Entity ID) you need to put a complete URL with your domain name like the below example.

<https://domainname/NavoriService/ADFS.aspx> Replace **domainname** text with your domain name and put it in Identifier (Entity ID) & in Reply URL (Assertion Consumer Service URL)

2. Save

Microsoft Entra admin center

Home > Corp-SSO

Corp-SSO | SAML-based Sign-on

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

Troubleshooting & Support

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating Corp-SSO.

1 Basic SAML Configuration

Identifier (Entity ID)  Required

Reply URL (Assertion Consumer Service URL)  Required

Sign on URL  Optional

Relay State (Optional)  Optional

Logout URL (Optional)  Optional

2 Attributes & Claims

Fill out required fields in Step 1

Attribute	Value
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Certificates

Token signing certificate

Status Active

Thumbprint F8A23743D9CD47B6D1A1FC6

Expiration 10/2/2027, 11:36:49 PM

Notification Email r.vashistha@navori.com

App Federation Metadata URL <https://login.microsoftonline.com/...>

Certificate (Base64)

Certificate (Raw)

Federation Metadata XML

Basic SAML Configuration

Identifier (Entity ID)

Reply URL (Assertion Consumer Service URL)

Sign on URL

Relay State (Optional)

Logout URL (Optional)

The next screen will look like as below

Microsoft Entra admin center

Home > Enterprise applications | All applications > Corp-SSO

Corp-SSO | SAML-based Sign-on

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

Troubleshooting & Support

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating Corp-SSO.

1 Basic SAML Configuration

Identifier (Entity ID)  Edit

Reply URL (Assertion Consumer Service URL)  Edit

Sign on URL  Optional

Relay State (Optional)  Optional

Logout URL (Optional)  Optional

2 Attributes & Claims

Fill out required fields in Step 1

Attribute	Value
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Certificates

Token signing certificate

Status Active

Thumbprint F8A23743D9CD47B6D1A1FC6

Expiration 10/2/2027, 11:36:49 PM

Notification Email r.vashistha@navori.com

App Federation Metadata URL <https://login.microsoftonline.com/...>

Certificate (Base64)

Certificate (Raw)

Federation Metadata XML

Basic SAML Configuration

Identifier (Entity ID)

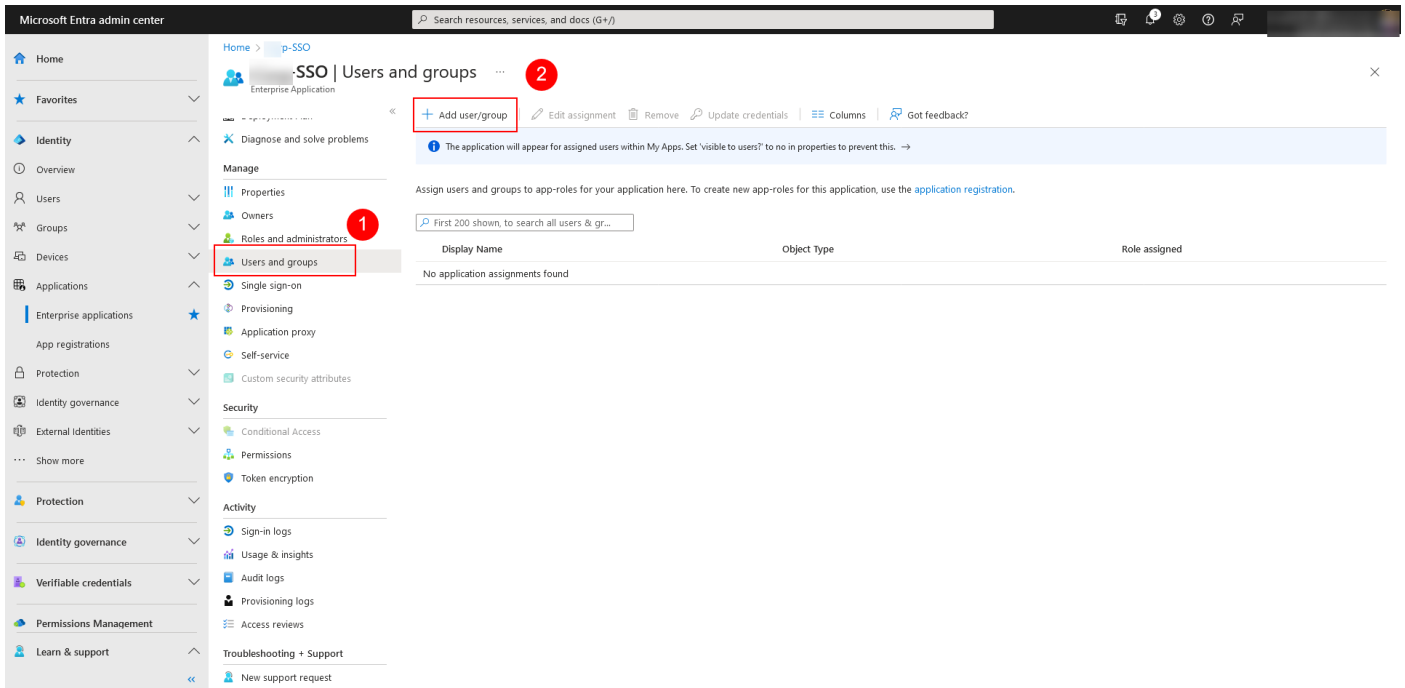
Reply URL (Assertion Consumer Service URL)

Sign on URL

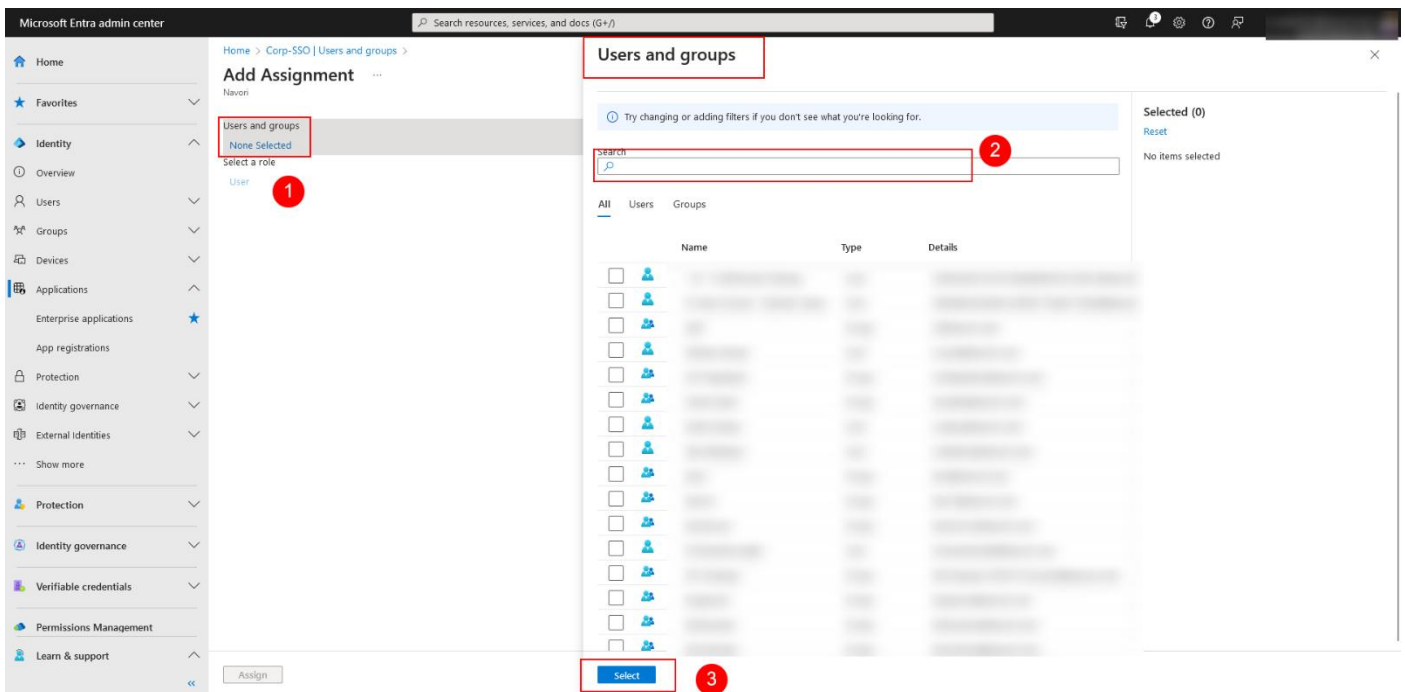
Relay State (Optional)

Logout URL (Optional)

Now there need to provide Application permission to the user for this click on Manage> users and group.



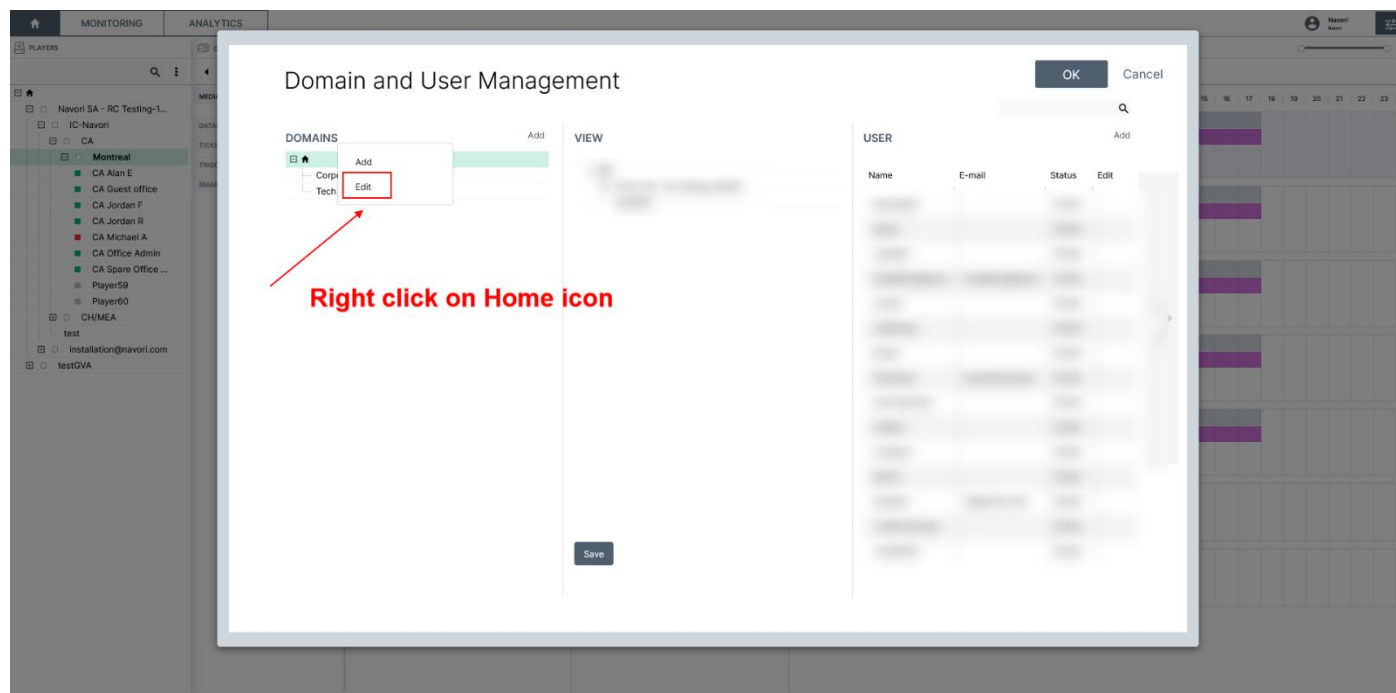
After clicking on users and group next screen look like the below to add assignment > users and group > select users or group which you want to access Qlmanager with Azure AD.



Qlmanager SSO configuration steps:

Login to qlmanager with a root admin account and click on Domain and user management.

In Domain and User management you can see Domain filed now need to click on the Home icon > right click > edit



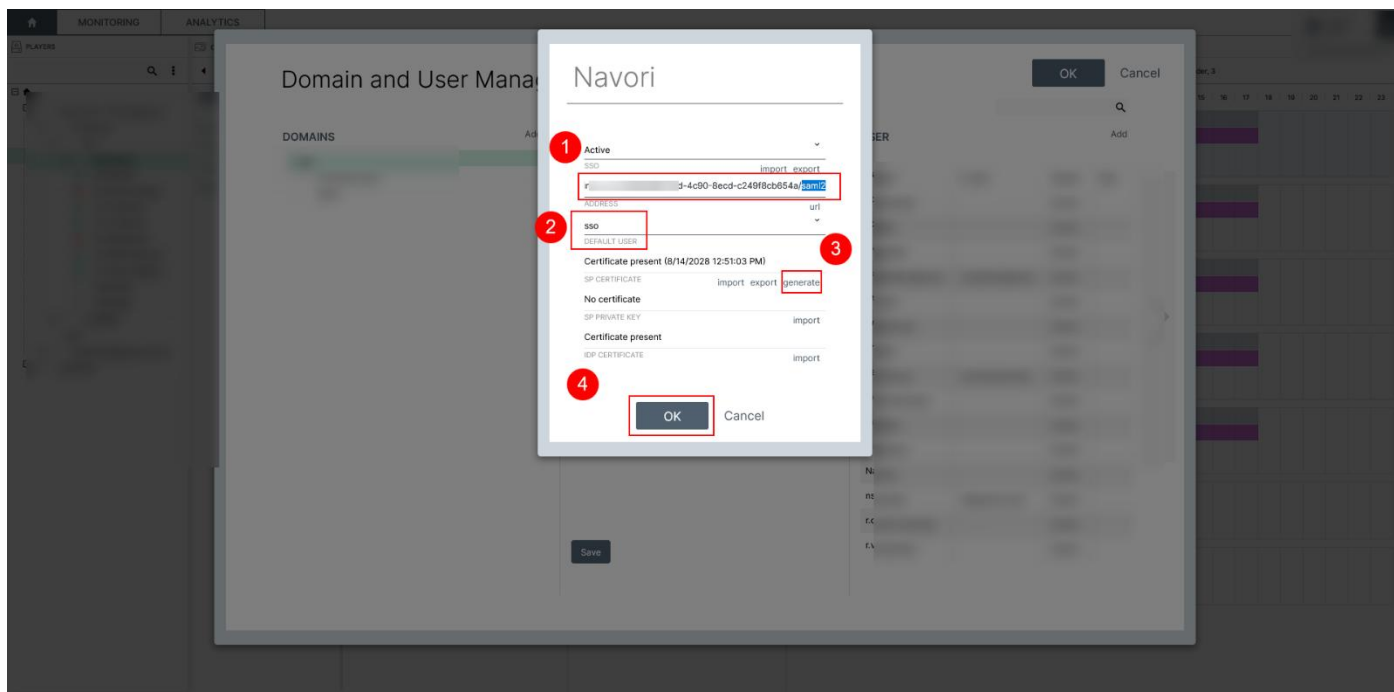
In Domain and User management you can see Domain filed now need to click on the Home icon > right click > edit

it will look like below.

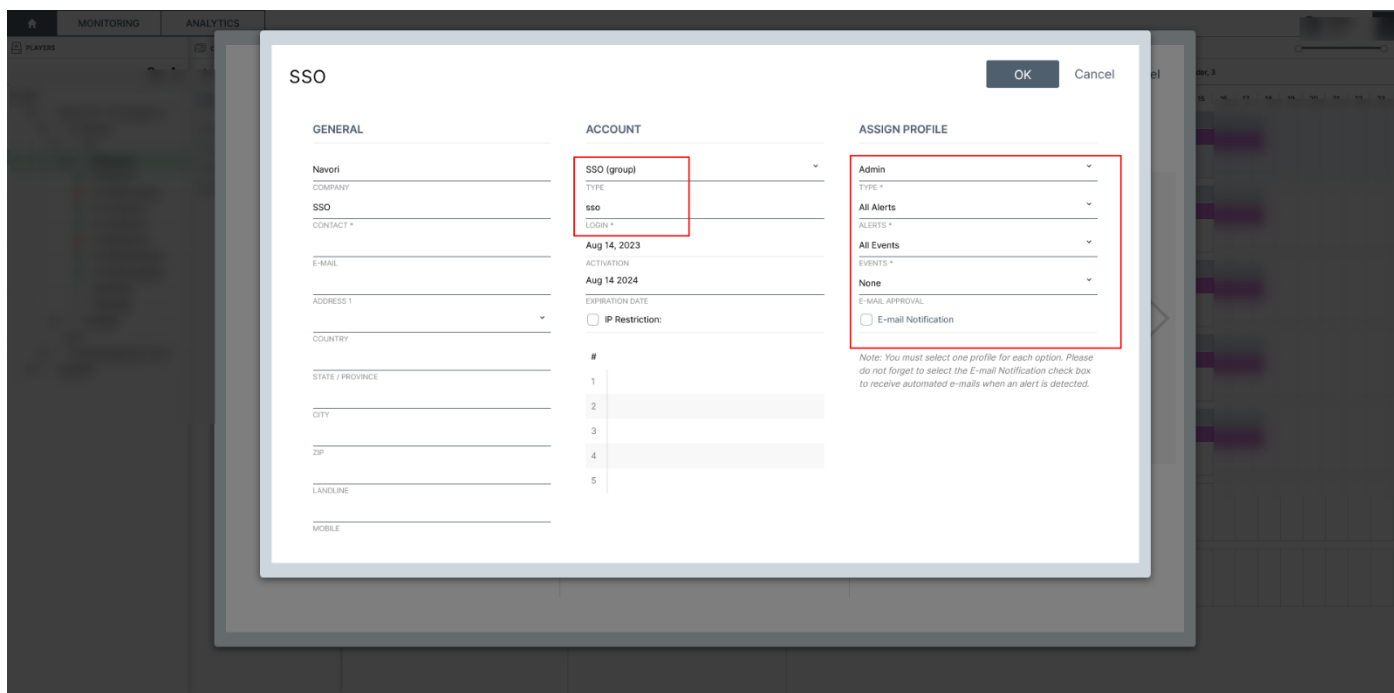
need to create an SSO account for the default user looks in the below next screen.

The status shows below.

1. **SSO> Active**
2. **Address: copy this address from SAML-based Sign-on> Set up ABC-SSO (see in next screen)**
3. **Select sso user as the default user**
4. **Generate certificate**
5. **click on OK**



For this, you need to create an SSO account for the default user looks in the below screen.



Address SAML-based Sign-on> Set up ABC-SSO

Copy this and put it in the Address field in Qlmanager domain and user management.

Microsoft Entra admin center

Home > Enterprise applications > All applications > Corp-SSO

SSO | SAML-based Sign-on

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

Upload metadata file

Change single sign-on mode

Test this application

Got feedback?

Unique User Identifier

user.userprincipalname

SAML Certificates

Token signing certificate

Status

Thumbprint

Expiration

Notification Email

App Federation Metadata Url

Certificate (Base64)

Certificate (Raw)

Federation Metadata XML

Download

Download

Download

Verification certificates (optional)

Required

No

Active

0

Expired

0

Edit

Set up Corp-SSO

You'll need to configure the application to link with Azure AD.

Login URL

https://login.microsoftonline.com/c808b86f-7a9d-4000-b010-000000000000

Azure AD Identifier

Logout URL

Test single sign-on with Corp-SSO

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

Test

Copy this and put in Address field in admin and user management

the configuration is complete .

Test single sign-on with ABC-SSO>Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

also, you can verify to login in to manager >click on SSO authentication > it will redirect you to Microsoft login > put your email id and password > it will redirect to your Qlmanager login

Login

Password

English

Connection

Forgot Password?

Active Directory Authentication

SSO Authentication

Version: 2.8.0, Published on: July 24, 2023 3:36 PM



Please note that for SaaS customers using SSO configuration per tenant, only a single SSO application can be active within the Microsoft Entra ID (Azure AD) environment. This means:

- Each tenant can have only **one SSO application** for the SaaS service.
- A single **Identifier (Entity ID)** is allowed per tenant.
- If an application is already using the identifier <https://saas.navori.com/NavoriService/ADFS.aspx>, a second application **cannot** be registered with the same identifier.

In case facing any issue related to configuration, please open a support ticket!