

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

Microsoft Entra admin center

1. Browse Azure AD Gallery

2. Got feedback?

3. What's the name of your app? Corp-SSO

Create your own application

What are you looking to do with your application?

Configure Application Proxy for secure remote access to an on-premises application

Register an application to integrate with Azure AD (App you're developing)

Integrate any other application you don't find in the gallery (Non-gallery)

We found the following applications that may match your entry. We recommend using gallery applications when possible.

Envi MMIS

In application overview.

Click on Setup single sign-on.

Microsoft Entra admin center

1. Overview

Properties

2. Set up single sign on

3. Create

Getting Started

What's New

Sign in charts have moved!

Delete Application has moved to Properties

In the next screen single sign On Click on SAML

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu is visible with various sections like Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Enterprise applications, Protection, Identity governance, External identities, and more. The 'Enterprise applications' section is expanded, and 'Corp-SSO' is selected. The main content area is titled 'Corp-SSO | Single sign-on' and shows an 'Overview' section with a brief description of SSO. Below this, there's a section titled 'Select a single sign-on method' with three options: 'Disabled' (not enabled), 'SAML' (selected and highlighted with a red box and arrow), and 'Password-based'.

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

The next screen will look like as below

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

Microsoft Entra admin center

Home > p-SSO | Users and groups

Enterprise Application

Manage

Properties

Owners

Roles and administrators

1

Users and groups

2

Add user/group

Edit assignment

Remove

Update credentials

Columns

Got feedback?

The application will appear for assigned users within My Apps. Set 'Visible to users?' to no in properties to prevent this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration.

First 200 shown; to search all users & gr...

Display Name

Object Type

Role assigned

No application assignments found

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.

Microsoft Entra admin center

Home > Corp-SSO | Users and groups > Add Assignment

Users and groups

1

2

3

None Selected

Select a role

User

Search

Selected (0)

Reset

No items selected

All Users Groups

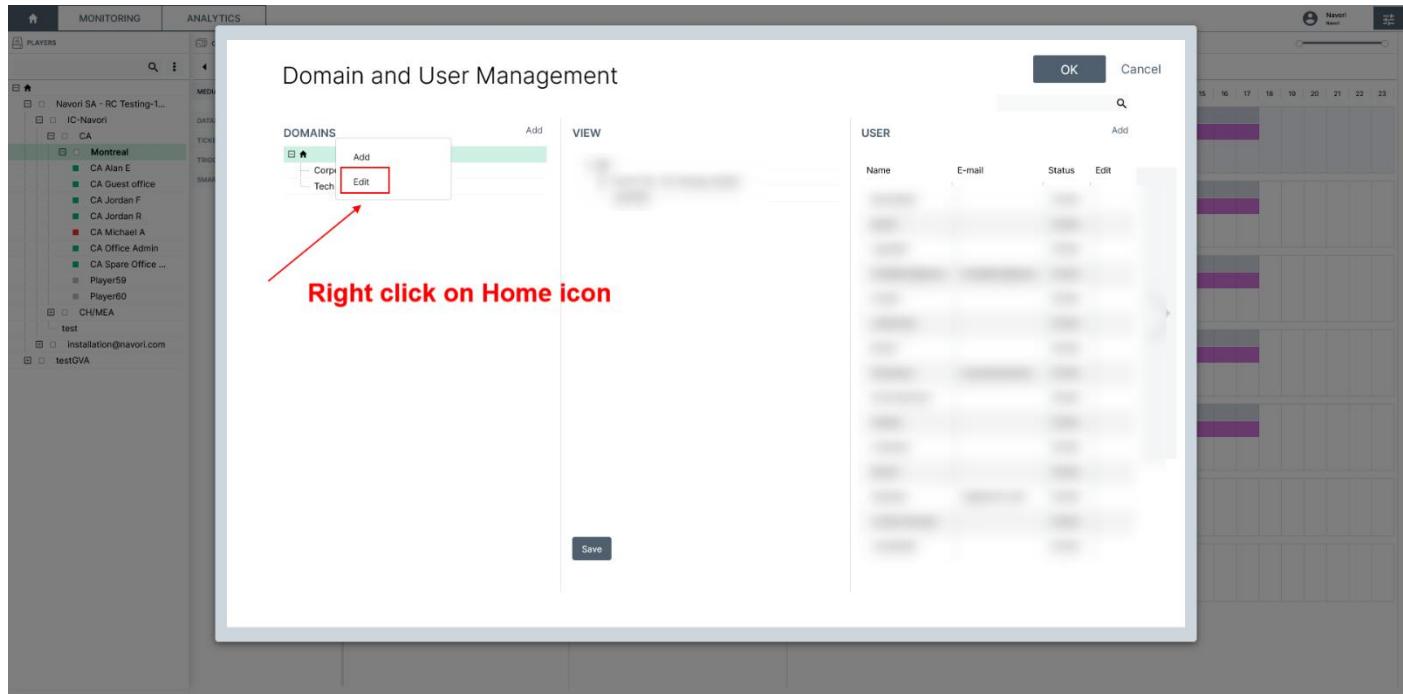
Name Type Details

Select

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



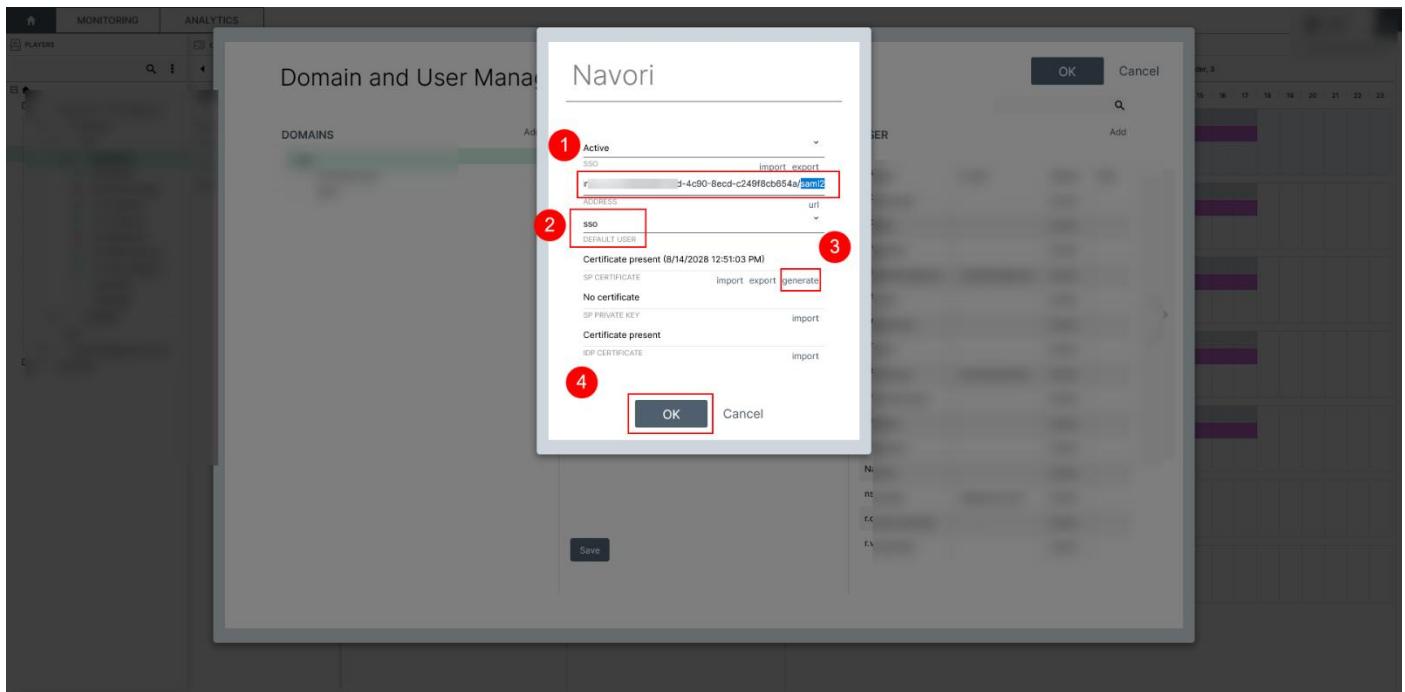
In Domain and User management you can see Domain filed now need to click on the Home icon > right click > edit

it will look like below.

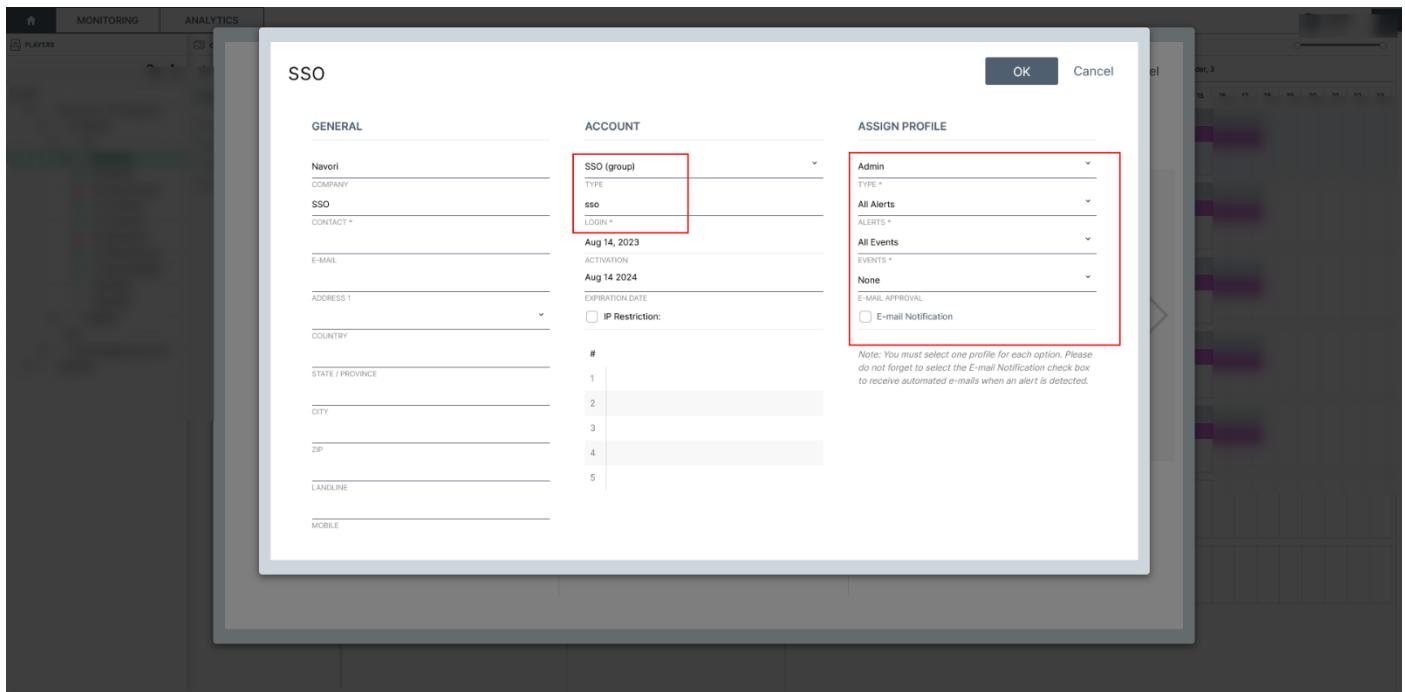
need to create an SSO account for the default user looks in the below next screen.

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.

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

Version: 2.8.0, Published on: July 24, 2023 3:38 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!