erwin Data Intelligence – erwin Data Quality

User Guide - SSO Configuration for erwin Data Quality

Legal Notices

Contact erwin

Understanding your Support

Review support maintenance programs and offerings.

Registering for Support

Access the erwin support site and click Sign in to register for product support.

Accessing Technical Support

For your convenience, erwin provides easy access to "One Stop" support for erwin Data Intelligence (erwin DI), and includes the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- erwin Support policies and guidelines
- Other helpful resources appropriate for your product

For information about other erwin products, visit http://erwin.com/.

Provide Feedback

If you have comments or questions, or feedback about erwin product documentation, you can send a message to distechpubs@erwin.com.

erwin Data Modeler News and Events

Visit www.erwin.com to get up-to-date news, announcements, and events. View video demos and read up on customer success stories and articles by industry experts.

Contents

Introduction

This document is intended to serve as manual for the integration of SSO using a SAML application in DQLabs. In this document we have provided the steps to integrate with the Octa active directory.

Overview

- Single Sign-on feature in DQLabs is used to login to the portal without manually creating the users.
- DQLabs will support Single sign-on only when the DNS name has the secured protocol.
- DQLabs claim information is Email, so the user cannot be able to login using the username.
- When DQLabs is already installed with the private IP or http. Please redeploy with the domain name.
    - For windows: Redeploy the **DQLabs_Windows_Client_Code_Upgrade** script.
    - For Linux: Linux code update script **DQLabs_Linux_Upgrade** script.

Note: If the environment is Windows, please make sure that the Reverse rewrite host option is disabled in the application settings under IIS. Steps to disable the reverse rewrite option is given below.

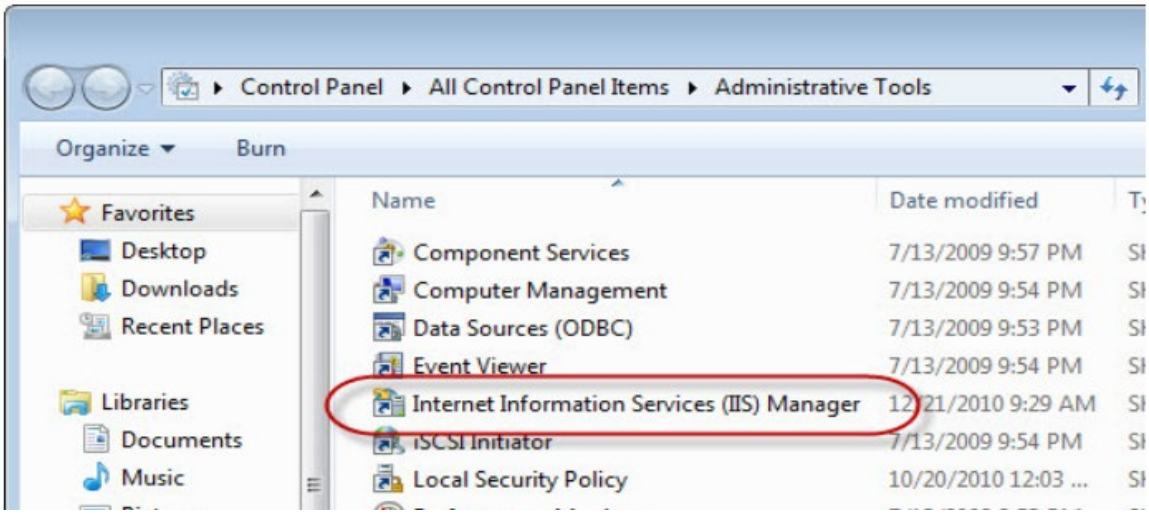
Steps to Configure SSO in DQLabs

The following steps are covered in the configuration of SSO in DQLabs

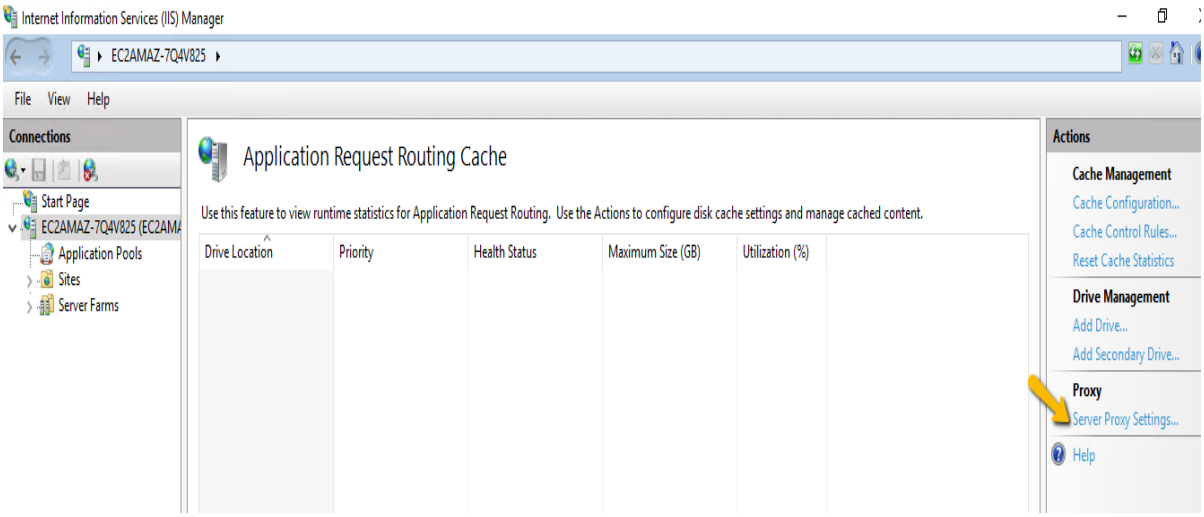
- ARR Settings for windows (Applicable only for windows environment)
- Creation of SAML configuration URL with example
- Logging in using SSO

ARR Settings for Window

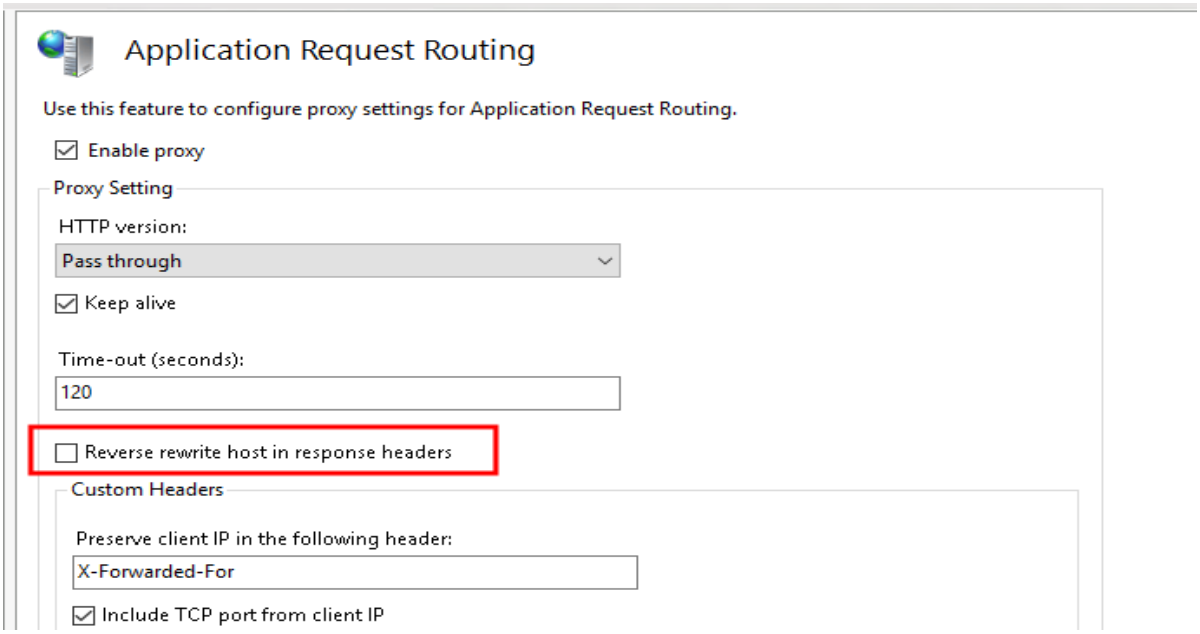
- On the Start screen, click the Control Panel.
- Click System and Security, and then click Administrative Tools.
- In the Administrative Tools window, double-click Internet Information Services (IIS) Manager



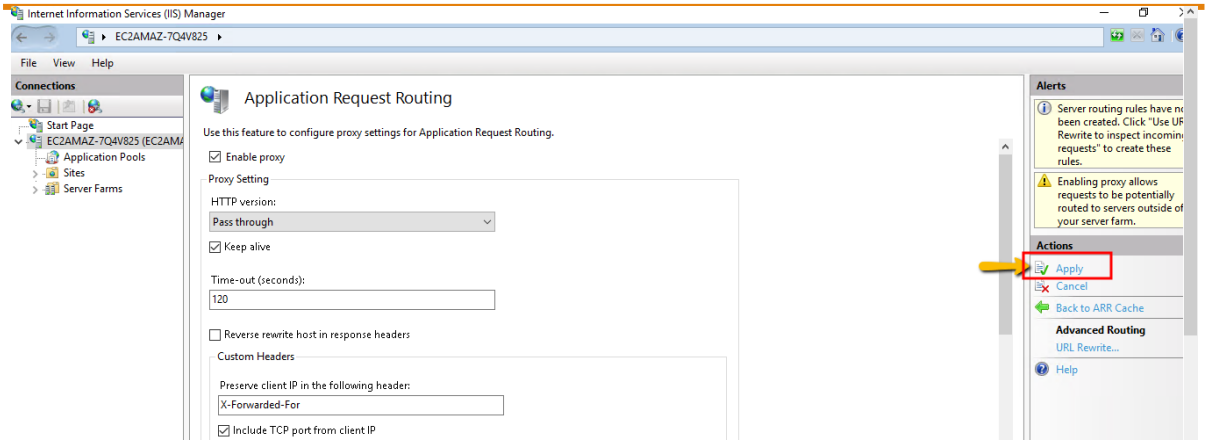
- Now click on server proxy settings under Proxy



- Under Server Proxy Settings, make sure that the Reverse rewrite host in response headers check box is disabled. If not, disable the check box and click Apply.

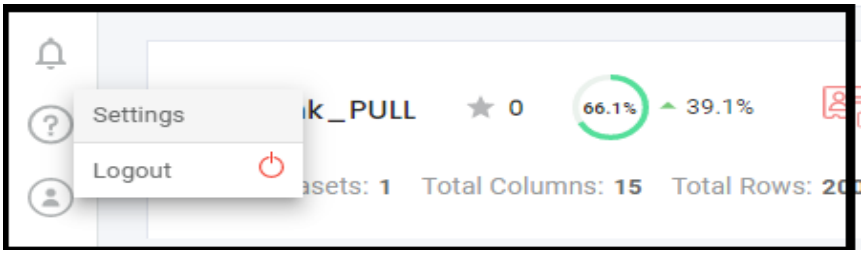


- Click on “Apply” to finish the setting.

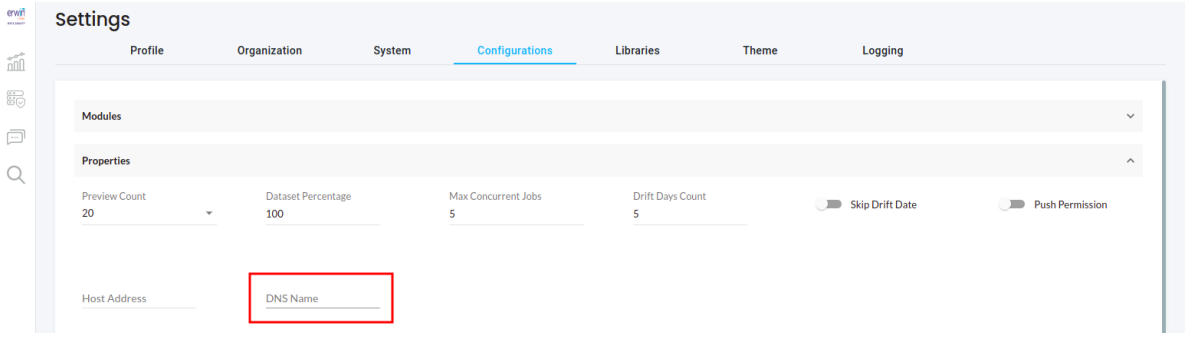


Create SAML Configuration URL

- Login as a superuser.
- Click User > Settings > Configurations tab > Properties.

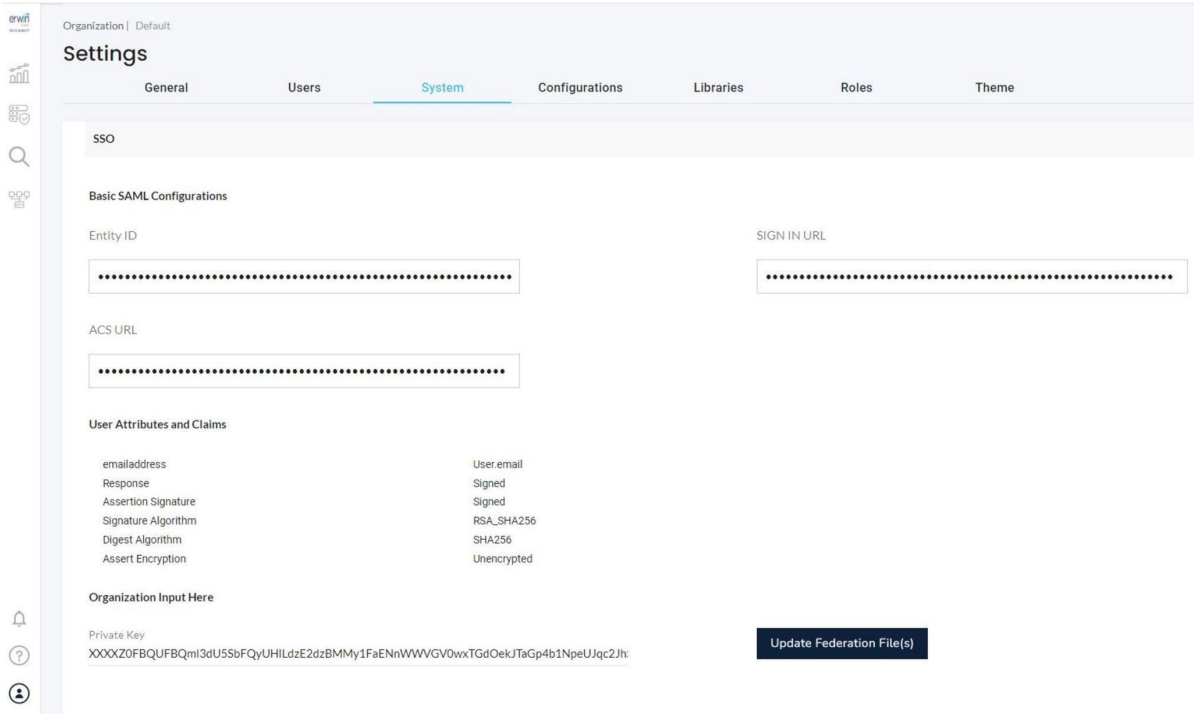


- Provide the Server's DNS Name in the DNS Name input field.



- Once the DNS name got updated the following **Basic SAML Configurations** details will get generated under each organization level settings.

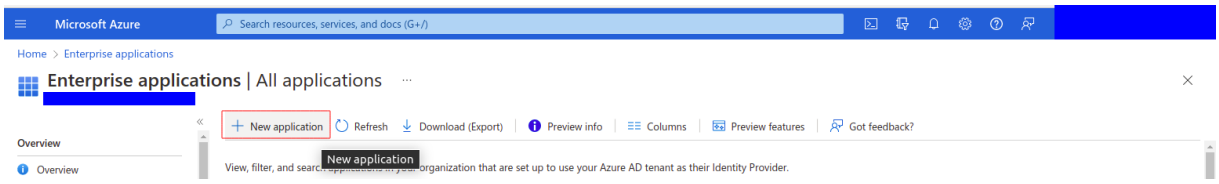
- User can open the organization level Settings by clicking Organization > Edit > System > SSO to get the following details.
    - Entity ID
    - SIGN IN URL
    - ACS URL



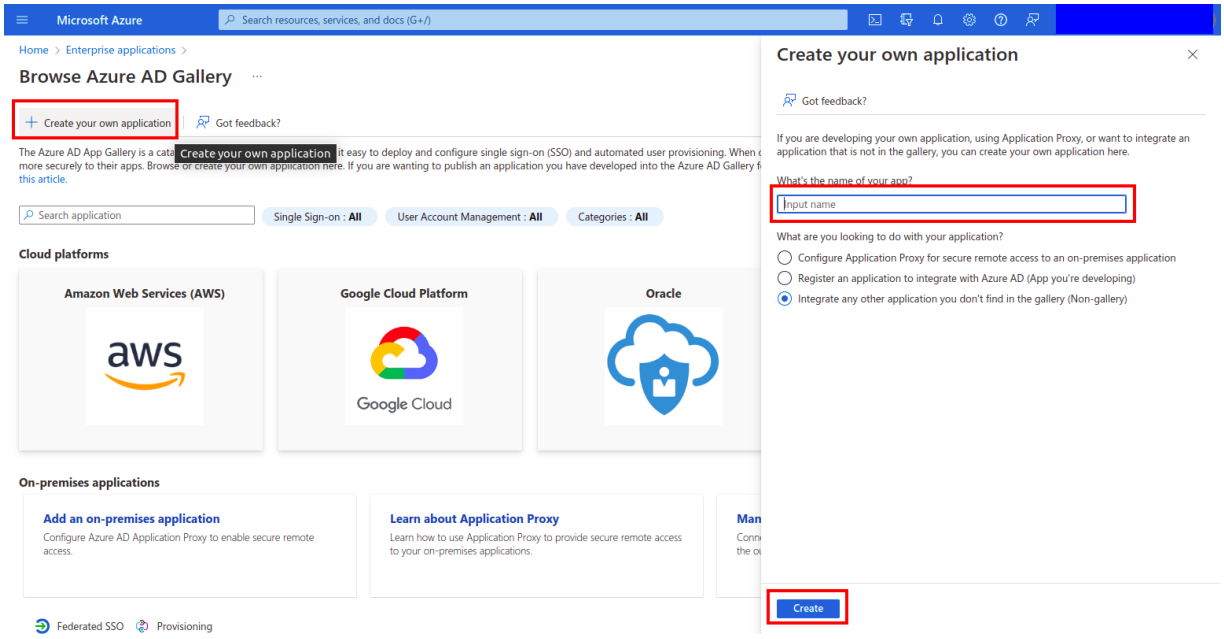
- Using this Basic SAML Configurations, download the federation file in the Active Directory. Please see the following example using Microsoft Azure.
- Add the domain name under the domains field. Same domain should be used while login to the DQLabs application.

SAML Configuration Using Microsoft Azure:

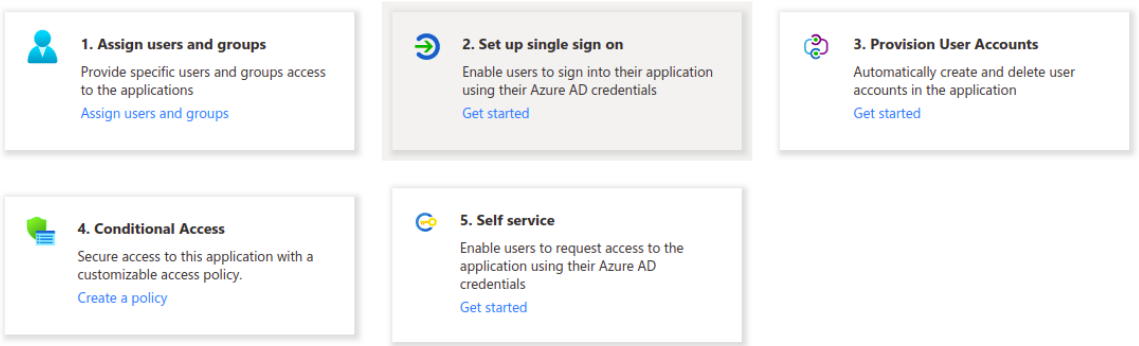
- Open the Microsoft azure application and search for Enterprise applications.
- Click on New application.



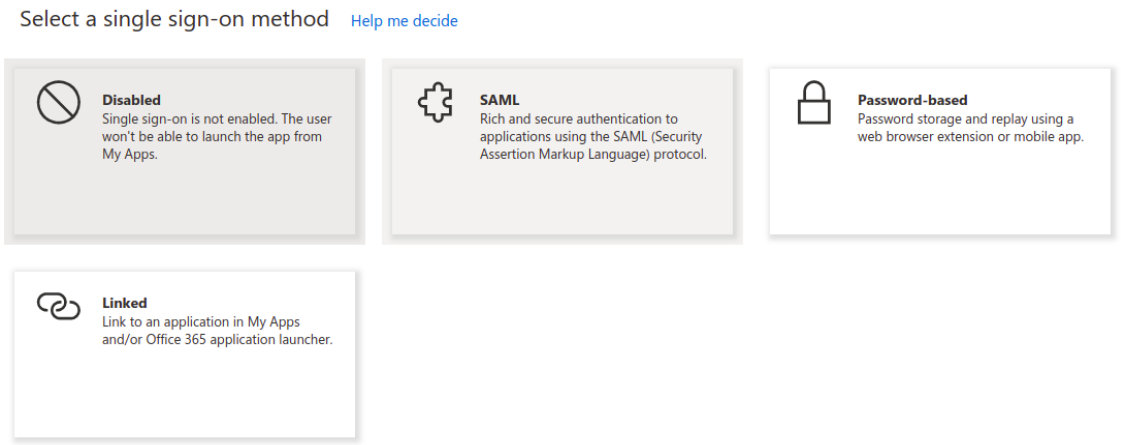
- Click on Create your own application > provide an app name and click Create.



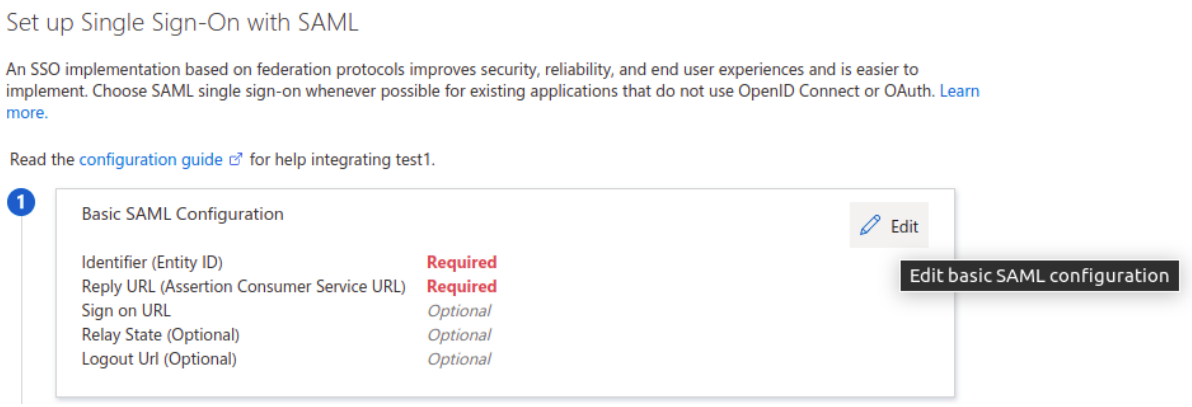
- Once the app created, click on Set up single sign on.



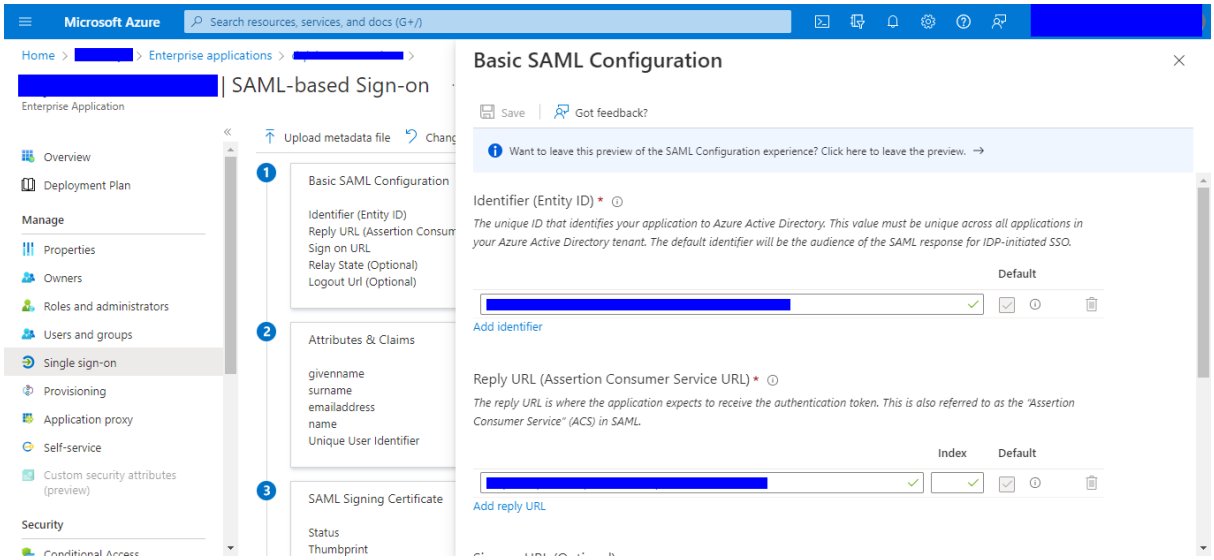
- Click on SAML.



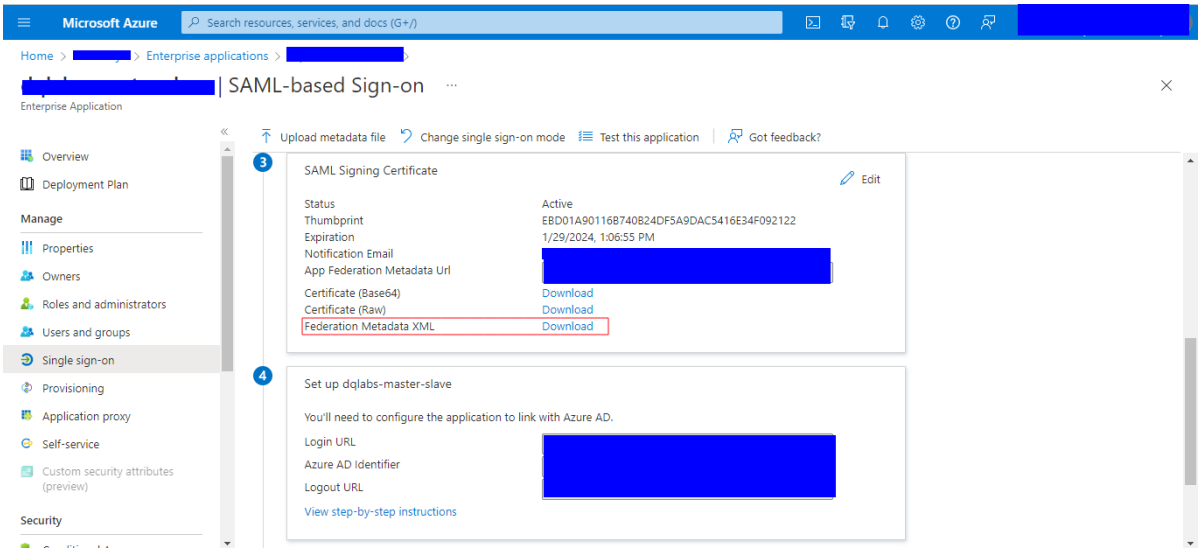
- On the SAML page, click Edit in Basic SAML Configuration.



- Paste the Entity ID, Reply URL(ACS URL) and Sign on URL from the DQLabs portal



- Now user can able to download the Federation Metadata XML in the third step.

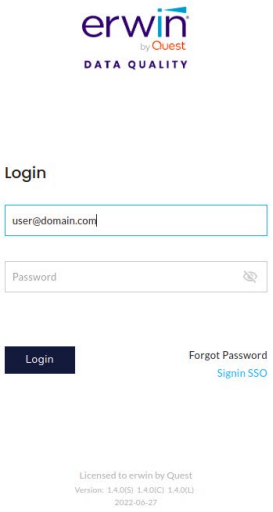


- Insert the private key in the private key input field under the Organization Input Here section in Organisation Settings > System > SSO.
  Private Key- Private key is the same key which used to generate csr to get ssl crt , same private key need to use in our portal

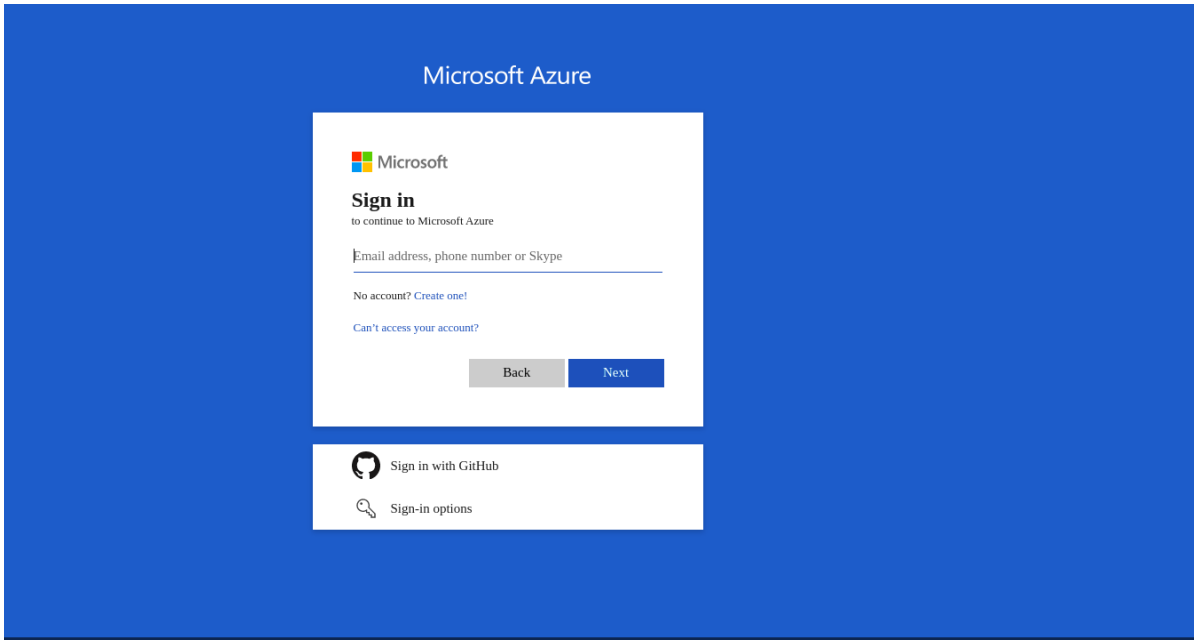
- Once the private key is pasted, upload the downloaded federation file in Update Federation File option will get enabled next to the input field.

Login Using SSO

- Open the portal in the browser and enter the username in the login page.
    - Username must contain valid user name followed by the constant domain name. (Domain name is case sensitive).
      For example: user@domain.com



- Click the SignIn SSO option.
- Now the user will get navigated to the corresponding SSO login page.



- Once the user logged in to the portal successfully, user can verify the user profile and organisation details in Settings > Profile.
  Note: By default, the user's role will be User and this role can be altered.