



erwin Data Intelligence – erwin Data Quality

**User Guide - SSO Configuration for
erwin Data Quality**

Legal Notices

This Documentation, which includes embedded help systems and electronically distributed materials (hereinafter referred to as the Documentation), is for your informational purposes only and is subject to change or withdrawal by Quest Software, Inc and/or its affiliates at any time. This Documentation is proprietary information of Quest Software, Inc and/or its affiliates and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Quest Software, Inc and/or its affiliates.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Quest Software, Inc and/or its affiliates copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Quest Software, Inc and/or its affiliates that all copies and partial copies of the Documentation have been returned to Quest Software, Inc and/or its affiliates or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, QUEST SOFTWARE, INC. PROVIDES THIS DOCUMENTATION AS IS WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL QUEST SOFTWARE, INC. BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF QUEST SOFTWARE, INC. IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is Quest Software, Inc and/or its affiliates Provided with Restricted Rights. Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright© 2025 Quest Software, Inc. and/or its affiliates All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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	1
Overview	1
Steps to Configure SSO in DQLabs	1
ARR Settings for Window	1
Create SAML Configuration URL	3
SAML Configuration Using Microsoft Azure:	4
Login Using SSO	8



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.

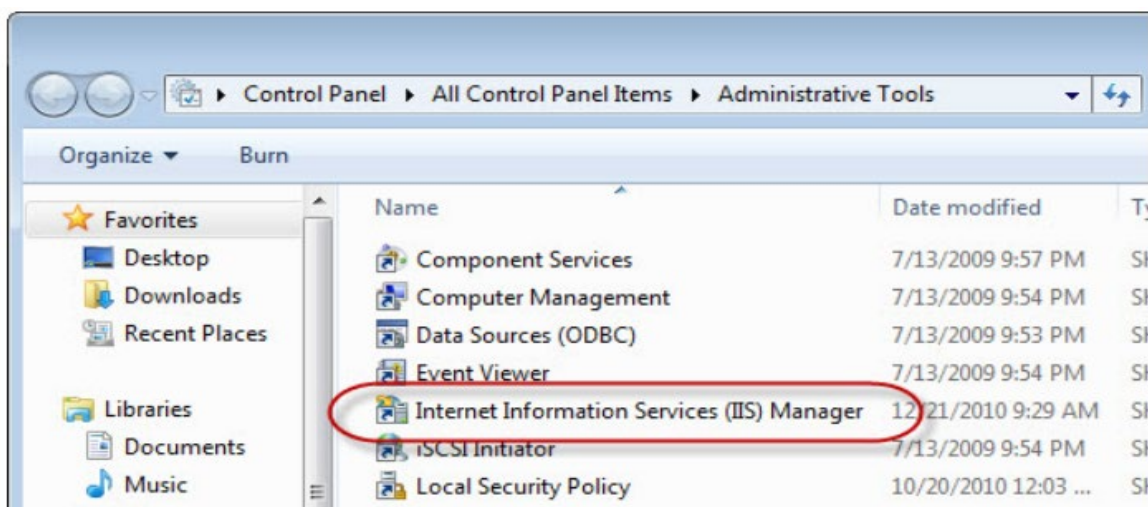
Steps to Configure SSO in DQLabs

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

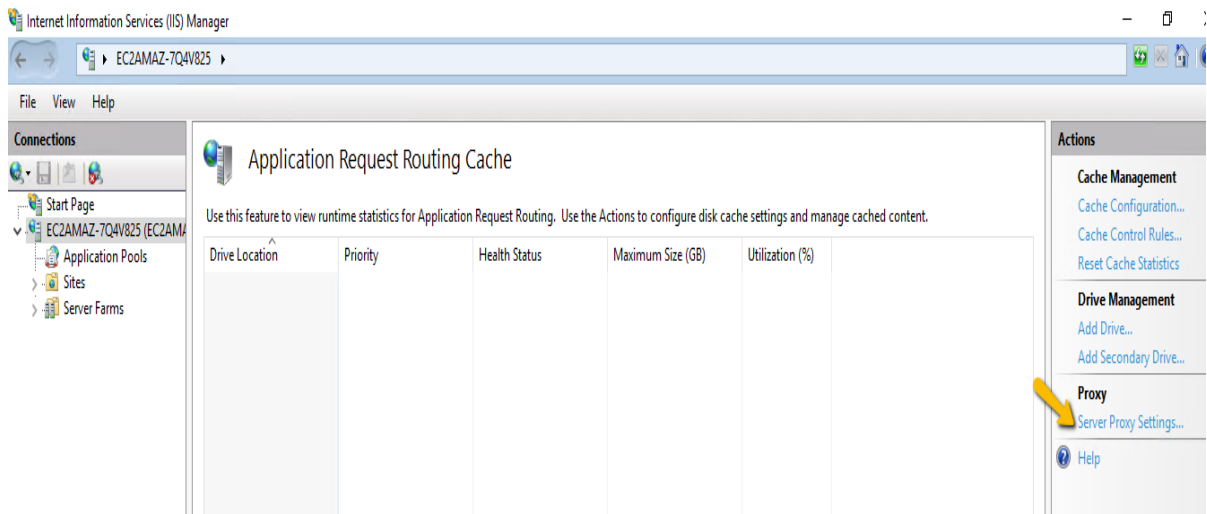
- ARR Settings for windows (Applicable only for windows environment)
- Creation of SAML configuration URL with example
- Logging in using SSO

ARR Settings for Window

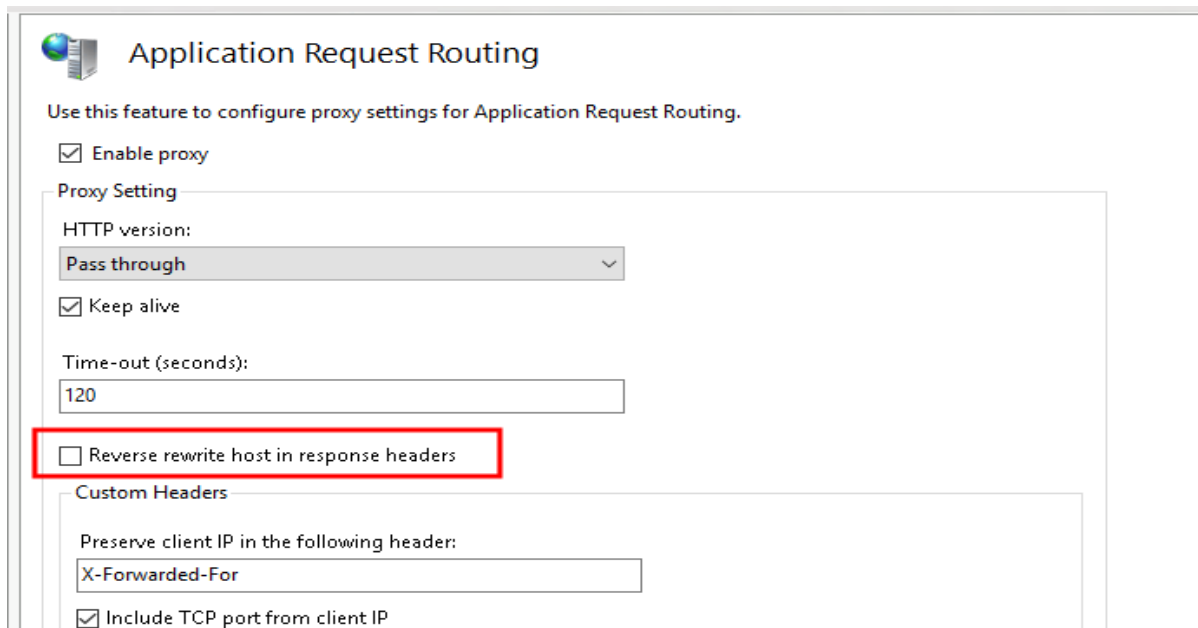
- On the Start screen, click the Control Panel.
- Click System and Security, and then click Administrative Tools.
- In the Administrative Tools window, double-click Internet Information Services (IIS) Manager



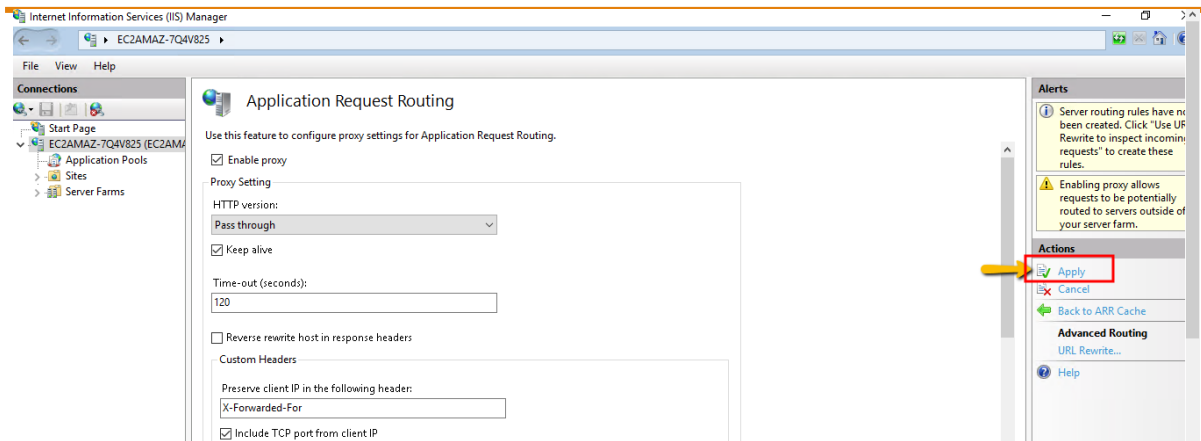
- Now click on server proxy settings under Proxy



- 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.

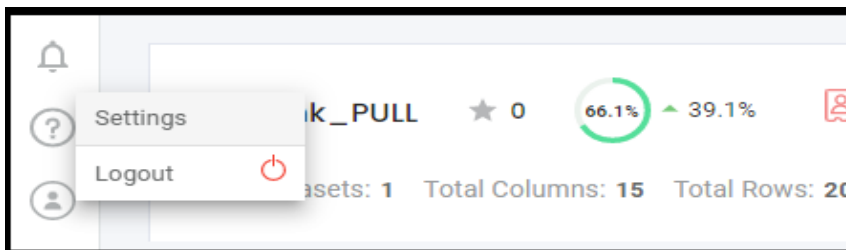


- Click on “Apply” to finish the setting.

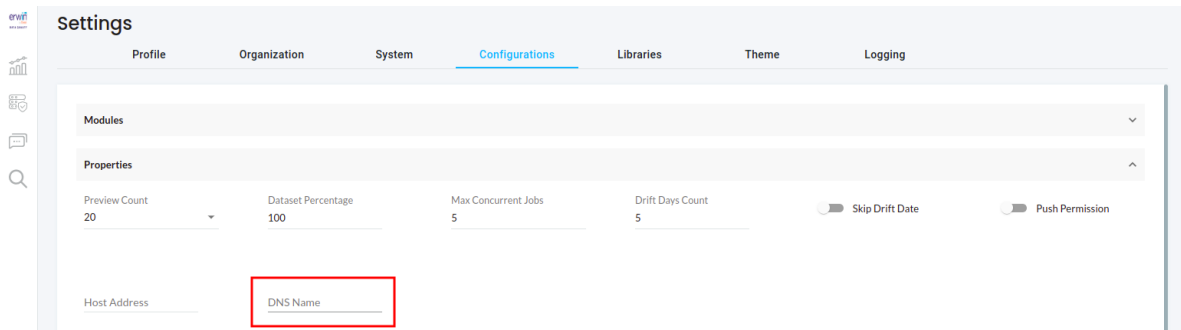


Create SAML Configuration URL

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

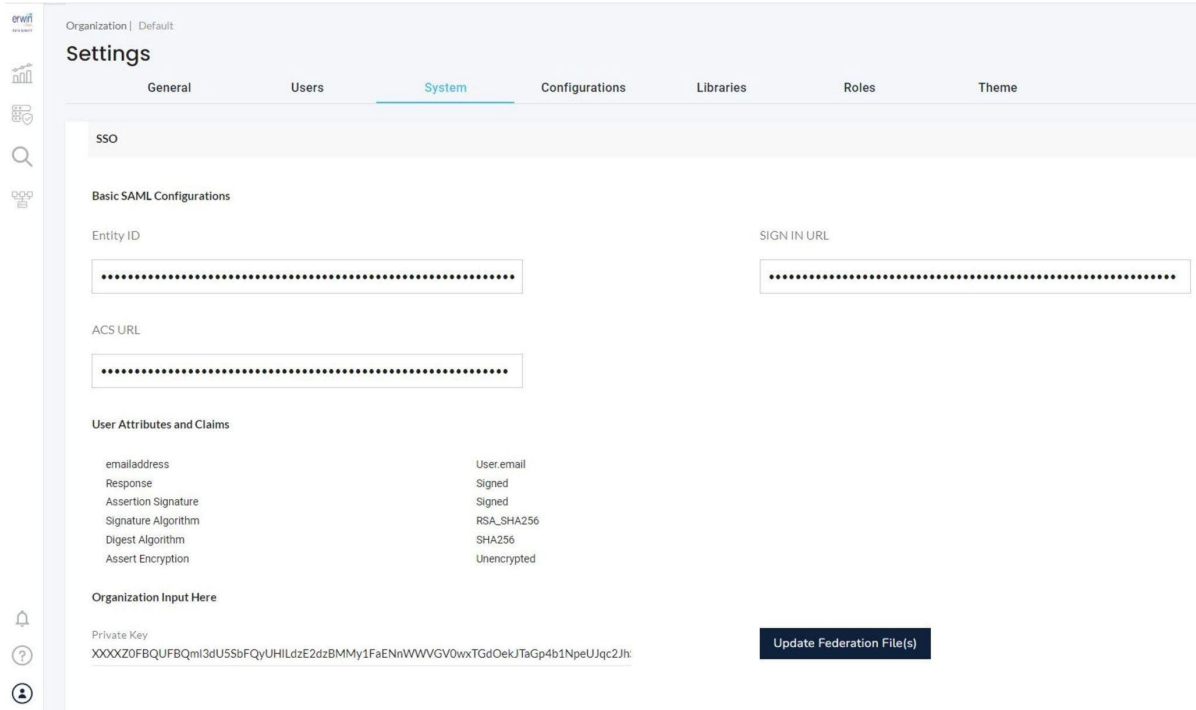


- Provide the Server's DNS Name in the DNS Name input field.



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

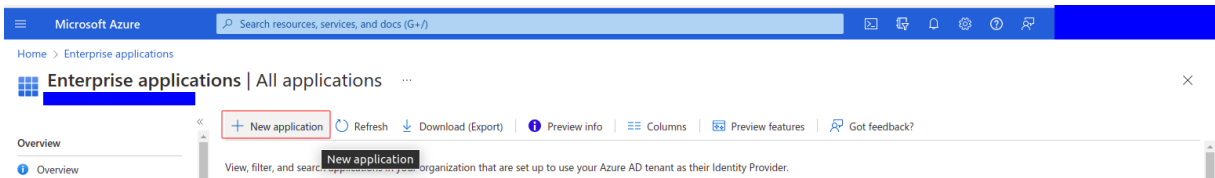
- User can open the organization level Settings by clicking Organization > Edit > System > SSO to get the following details.
 - Entity ID
 - SIGN IN URL
 - ACS URL



- 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.

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Browse Azure AD Gallery' section is visible, with a red box around the '+ Create your own application' button. On the right, the 'Create your own application' dialog box is open. It contains a 'Got feedback?' link, a description of the gallery, and a 'What's the name of your app?' section with an 'Input name' text box highlighted in red. Below this, there are three radio button options: 'Configure Application Proxy for secure remote access to an on-premises application', 'Register an application to integrate with Azure AD (App you're developing)', and 'Integrate any other application you don't find in the gallery (Non-gallery)'. At the bottom right of the dialog, a 'Create' button is highlighted with a red box.

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

The screenshot displays a sequence of five numbered steps for setting up an application in the Azure portal. Step 2, 'Set up single sign on', is highlighted with a grey background. Each step includes an icon, a title, a brief description, and a 'Get started' link.

- 1. Assign users and groups**
Provide specific users and groups access to the applications
[Assign users and groups](#)
- 2. Set up single sign on**
Enable users to sign into their application using their Azure AD credentials
[Get started](#)
- 3. Provision User Accounts**
Automatically create and delete user accounts in the application
[Get started](#)
- 4. Conditional Access**
Secure access to this application with a customizable access policy.
[Create a policy](#)
- 5. Self service**
Enable users to request access to the application using their Azure AD credentials
[Get started](#)

- Click on SAML.

Select a single sign-on method [Help me decide](#)

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in My Apps and/or Office 365 application launcher.

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

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 test1.

1 Basic SAML Configuration Edit

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	<i>Optional</i>
Relay State (Optional)	<i>Optional</i>
Logout Url (Optional)	<i>Optional</i>

Edit basic SAML configuration

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

Microsoft Azure | Search resources, services, and docs (G+)

Home > Enterprise applications > SAML-based Sign-on

Enterprise Application

Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Custom security attributes (preview)
Security
Conditional Access

Basic SAML Configuration

Save | Got feedback?

Want to leave this preview of the SAML Configuration experience? Click here to leave the preview. →

1 Basic SAML Configuration

Identifier (Entity ID) * ⓘ
The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Reply URL (Assertion Consumer Service URL) * ⓘ
The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

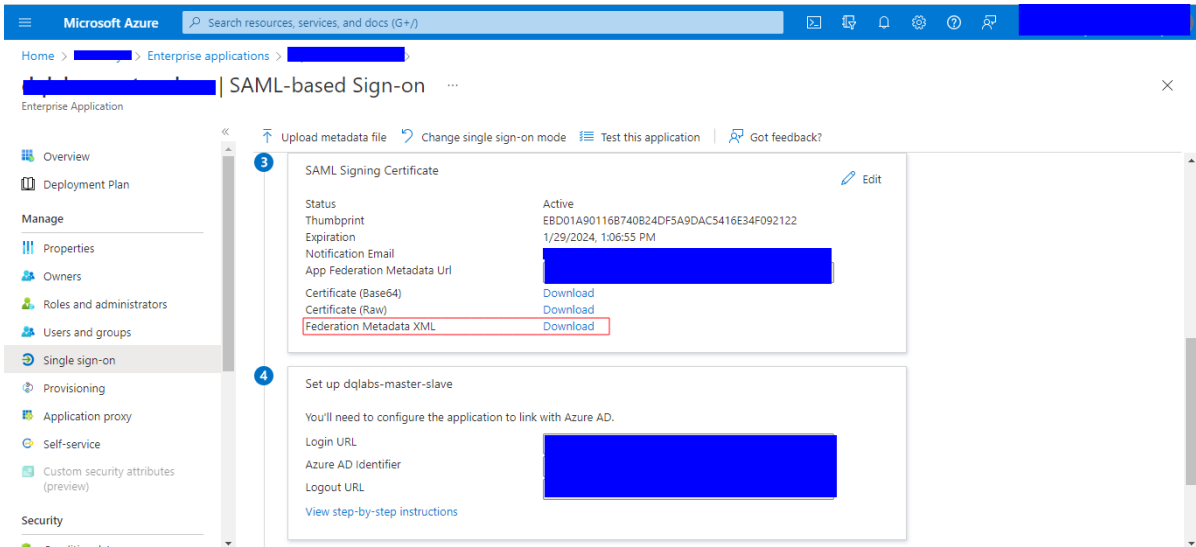
Attributes & Claims

givenname
surname
emailaddress
name
Unique User Identifier

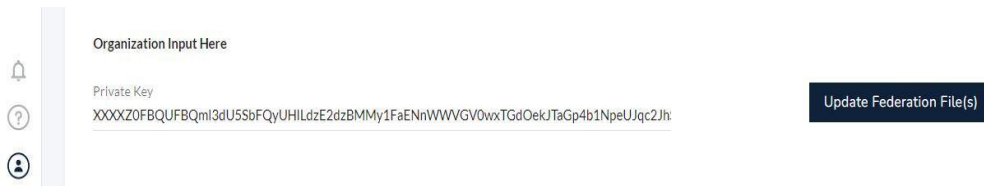
SAML Signing Certificate

Status
Thumbprint

- 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



erwin
by Quest
DATA QUALITY

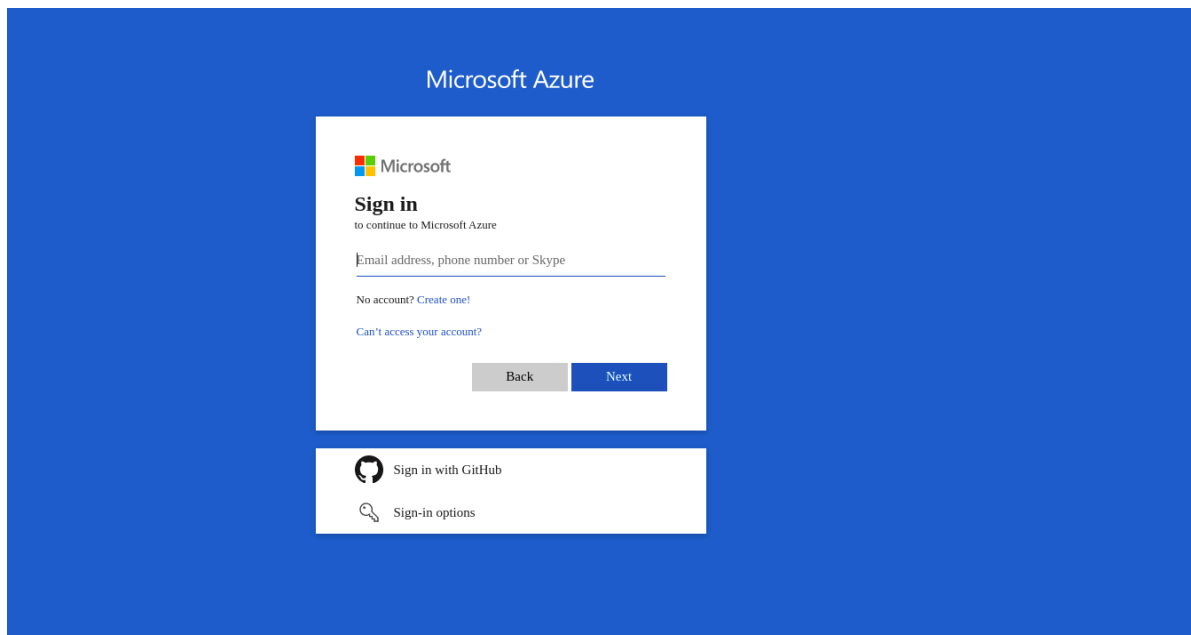
Login

Login

[Forgot Password](#)
[Signin SSO](#)

Licensed to erwin by Quest
Version: 1.4.0(S) 1.4.0(C) 1.4.0(L)
2022-06-27

- 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.

