



LinkSquares

SSO Guide for Microsoft Entra ID

SSO Guide for Microsoft Entra ID

This documentation provides a step-by-step guide to setting up Microsoft Entra (formerly known as Azure Active Directory) Single Sign-on (SSO) with LinkSquares.

The guide will cover the following:

- Microsoft Entra ID configuration
- LinkSquares configuration

Contact us at support@linksquares.com for assistance.

Microsoft Entra ID Configuration

The goal of the Microsoft Entra ID implementation for LinkSquares is to enable the user's ability to use a single sign-on account to access the platform.

Here is how it works at a high level:

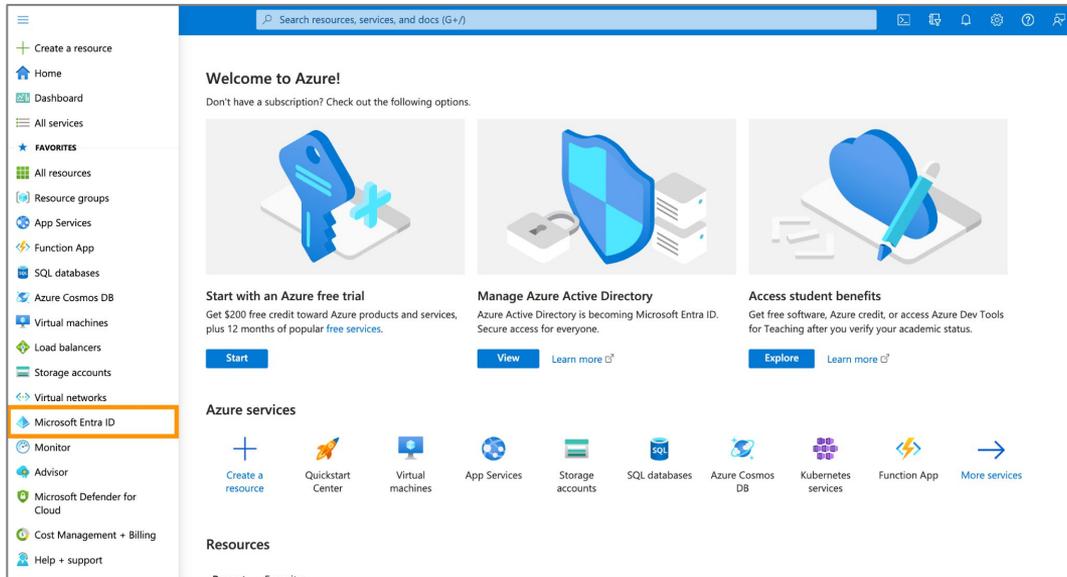


The first step is to configure Microsoft Entra ID to access LinkSquares.

1. Create a Custom Application

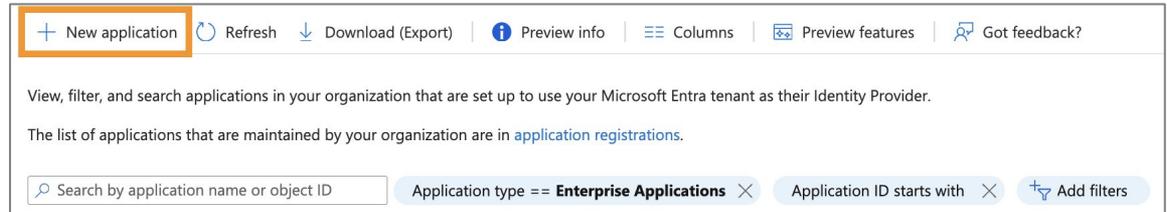
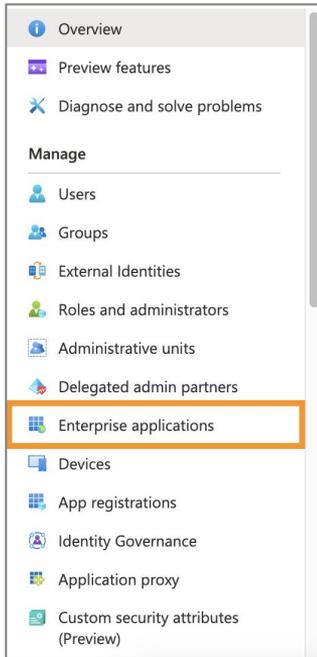
Begin by selecting **Microsoft Entra ID** from the menu within the Azure homepage.

Note: You must be an administrator of your SAML platform to complete these steps.



2. Create a New Enterprise Application

Select **Enterprise applications** from the menu. Next, click **New application** at the top of the page.

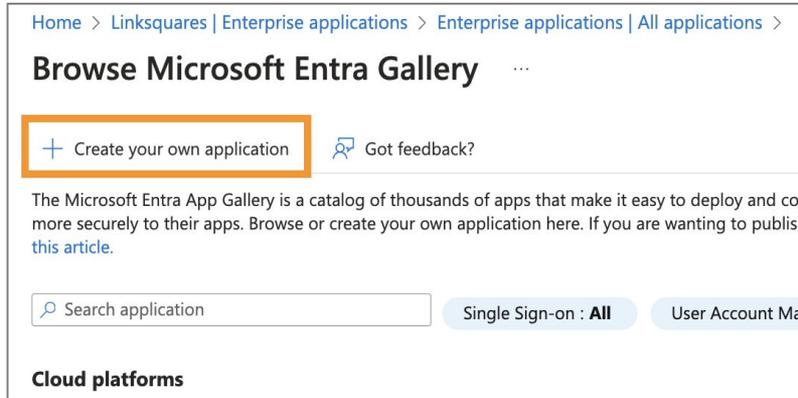


3. Add a Non-Gallery Application

Click **Create your own application** at the top of the page.

Then, set the name. We recommend “LinkSquares.”

Select the non-gallery application option. Click **Create** once complete.



Home > LinkSquares | Enterprise applications > Enterprise applications | All applications >

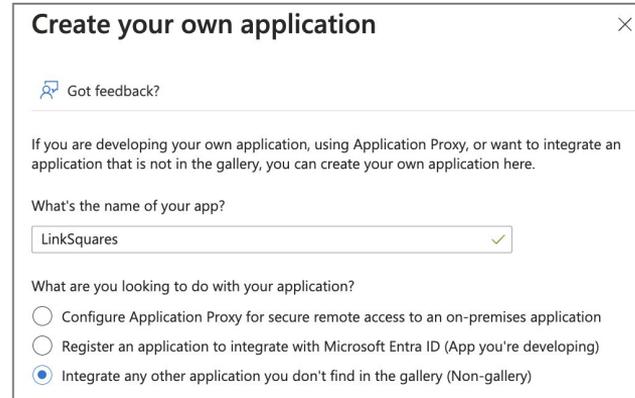
Browse Microsoft Entra Gallery

+ Create your own application  Got feedback?

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and connect more securely to their apps. Browse or create your own application here. If you are wanting to publish [this article](#).

Single Sign-on : **All** User Account Ma

Cloud platforms



Create your own application

 Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

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 Microsoft Entra ID (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)

4. Assign Users and Groups

Begin by assigning users to your LinkSquares group within **Assign users and groups**.

Getting Started

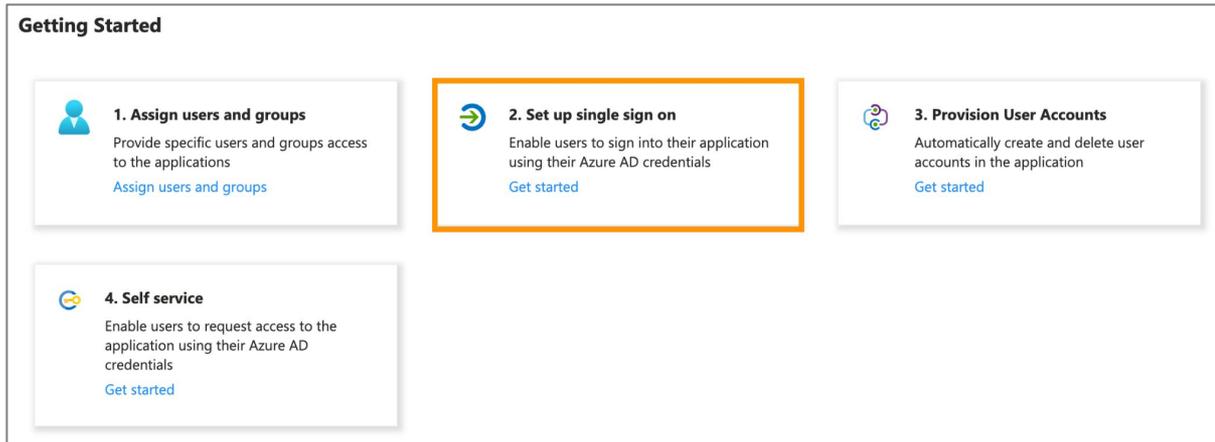
-  **1. Assign users and groups**
Provide specific users and groups access to the applications
[Assign users and groups](#)
-  **2. Set up single sign on**
Enable users to sign into their application using their Azure AD credentials
[Get started](#)
-  **3. Provision User Accounts**
Automatically create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

5. Set Up Single Sign-On

Once you have completed provisioning users, configure SSO within **Set up single sign on**.

Select the **SAML** option.

Getting Started



-  **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. Self service**
Enable users to request access to the application using their Azure AD credentials
[Get started](#)

6. Setting Up Single Sign-On

Within the **Basic SAML Configuration** step, click **Edit** and enter the following information.

Note: Please enter your domain within the URLs.

Identifier (Entity ID)

<https://yourdomain.linksquares.com/saml/metadata>

Reply URL (Assertion Consumer Service URL)

<https://yourdomain.linksquares.com/saml/auth>

Sign on URL

<https://yourdomain.linksquares.com>

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 LinkSquares.

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>

7. Setting Up Single Sign-On

Within the **SAML Certificates** step, click **Download** next to **Certificate (Base64)**.

This will download the file locally. Open the file with a text editor to retrieve and copy the full certificate to enter into LinkSquares during step nine of this guide.

If you are not a LinkSquares Analyze Administrator, email the file to LinkSquares at support@linksquares.com as you will require assistance with the remaining configuration steps.

3 SAML Certificates

Token signing certificate		Edit
Status	Active	
Thumbprint	AD	
Expiration	3/23/2026, 10:33:14 AM	
Notification Email	Notification Email	
App Federation Metadata Url	https://login.microsoftonline.com/2d2f422d-c486-...	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

Verification certificates (optional) (Preview) [Edit](#)

Required	No
Active	0
Expired	0

8. Setting Up Single Sign-On

Within the **Set up LinkSquares** step, copy the information within each field to enter into LinkSquares during step nine of this guide. Click the page icon to quickly copy the fields.

The LinkSquares application requires this information to complete the configuration.

4 Set up LinkSquares

You'll need to configure the application to link with Microsoft Entra ID.

Login URL	https://login.microsoftonline.com/2d2f422d-c486-...
Microsoft Entra Identifier	https://sts.windows.net/2d2f422d-c486-420b-967...
Logout URL	https://login.microsoftonline.com/2d2f422d-c486-...

Setting Up Single Sign-On (cont.)

The following URLs are examples of information that will be copied from these fields.

Login URL

<https://login.microsoftonline.com/e285w989812-p1234-12t31-7pp2-134fg12tq0z5a6/saml>

Microsoft Entra Identifier

<https://sts.windows.net/e285w989812-p1234-12t31-7pp2-134fg12tq0z5a6/>

Logout URL

<https://login.microsoftonline.com/e285w989812-p1234-12t31-7pp2-134fg12tq0z5a6/saml>

Note: The SSO URL will typically be the same as the SLO URL.

Setting Up Single Sign-On (cont.)

These fields will appear as follows within LinkSquares:

Login URL → **Identity Provider SSO URL**

Microsoft Entra Identifier → **Identity Provider SSO Entity ID**

Logout URL → **Identity Provider SLO URL**



A screenshot of a form with four input fields. The fields are labeled as follows:

- Identity Provider SSO Entity ID
- Identity Provider SSO URL
- Identity Provider SLO URL
- Identity Provider Certificate

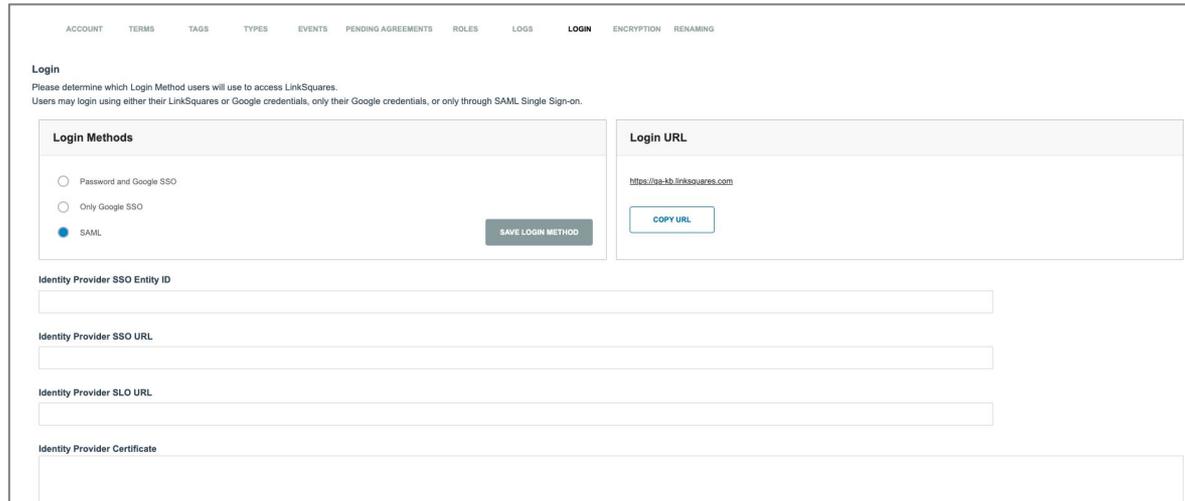
The first three fields are text input boxes, and the fourth is a larger text area. The form is enclosed in a thin black border.

9. LinkSquares Configuration

To complete the configuration, go to **Settings > Analyze App > Login** tab within LinkSquares.

Select the **SAML** option. Then, enter the required information as outlined in the previous slide.

Note: Ensure that you include “BEGIN CERTIFICATE” and “END CERTIFICATE” when pasting the certificate.



The screenshot displays the 'Login' configuration page in LinkSquares. At the top, a navigation menu includes ACCOUNT, TERMS, TAGS, TYPES, EVENTS, PENDING AGREEMENTS, ROLES, LOGS, LOGIN (highlighted), ENCRYPTION, and RENAMING. Below the menu, the 'Login' section contains instructions: 'Please determine which Login Method users will use to access LinkSquares. Users may login using either their LinkSquares or Google credentials, only their Google credentials, or only through SAML Single Sign-on.' The 'Login Methods' section features three radio button options: 'Password and Google SSO', 'Only Google SSO', and 'SAML' (which is selected). A 'SAVE LOGIN METHOD' button is positioned to the right of these options. To the right of the 'Login Methods' section is a 'Login URL' field containing the text 'https://pa-1b.linksquares.com' and a 'COPY URL' button. Below these sections are four text input fields labeled: 'Identity Provider SSO Entity ID', 'Identity Provider SSO URL', 'Identity Provider SLO URL', and 'Identity Provider Certificate'.

10. Success

After clicking **SAVE LOGIN METHOD** within the Login tab, SAML SSO will be successfully enabled.

Your SSO login URL can be found within the Login tab.

Contact us at support@linksquares.com for assistance.

Thank you!