



SSO Set-up Instructions



www.hrwize.com

June-July 2025

Contents

SSO Set-up Instructions.....	1
What is the process for enabling SSO?	4
Set-up Process.....	4
Creating an app in Entra	4
Enabling single sign-on for your app.....	5
Making your app accessible to users	9
Additional app settings	9
Viewing your app in Office 365.....	10
User login impact	10

In this guide we'll cover how to create and register a SAML Enterprise App in Microsoft Entra. (Formerly known as Azure Active Directory)

This app is to be used as your private identity provider in HRWize. This will be required as part of Single Sign On. (SSO)

Further information from Microsoft Entra which you may find useful can be [found here](#).



Reduce risk

Reduce the risk that comes along with duplicate data entry. Use HRWize as your single source of truth.



Remove inefficiencies

No more removing and maintaining users across both platforms. Streamline HR processes and improve efficiency.



Improve data security

Maintain records in one system rather than two, improved data security and bank on total compliance.

Overview

What is the process for enabling SSO?

1. Set-up your SAML enterprise app in Microsoft Entra
2. Enable SSO in your SAML enterprise app
3. Input SAML configuration information in the HRWize identity server (IDS)
4. Send your App Federation Metadata to the HRWize team to complete registration
5. Make your application available to all users

Once the above steps have been completed you and your users will be able to utilize SSO to sign-on to the HRWize application.

Note: When using multiple domains, each domain must be whitelisted.

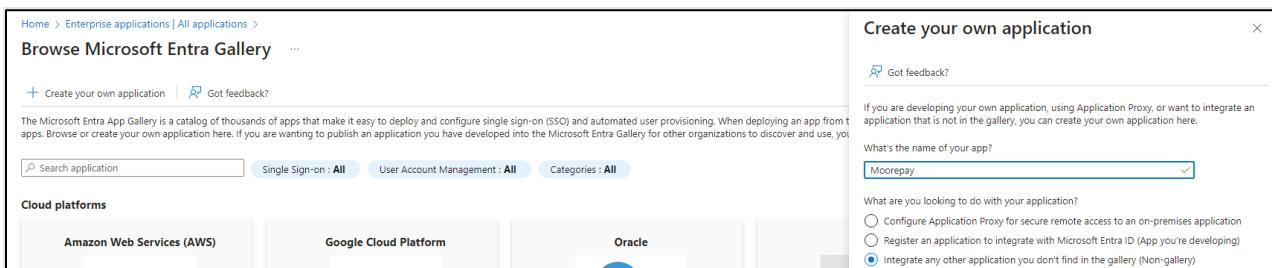
Set-up Process

Creating an app in Entra

1. Login to your [Azure portal](#) and search **enterprise applications** in the top search bar. Click on **new application** and then **create your own application**.

Note: It's important that you create a new application and **do not** simply update your current SSO credentials as this will prevent your users from logging in via your existing SSO.

2. Enter your preferred name for your application, we recommend 'HRWize' for ease of use. Then select **integrate any other application you don't find in the gallery**. (Non-gallery)

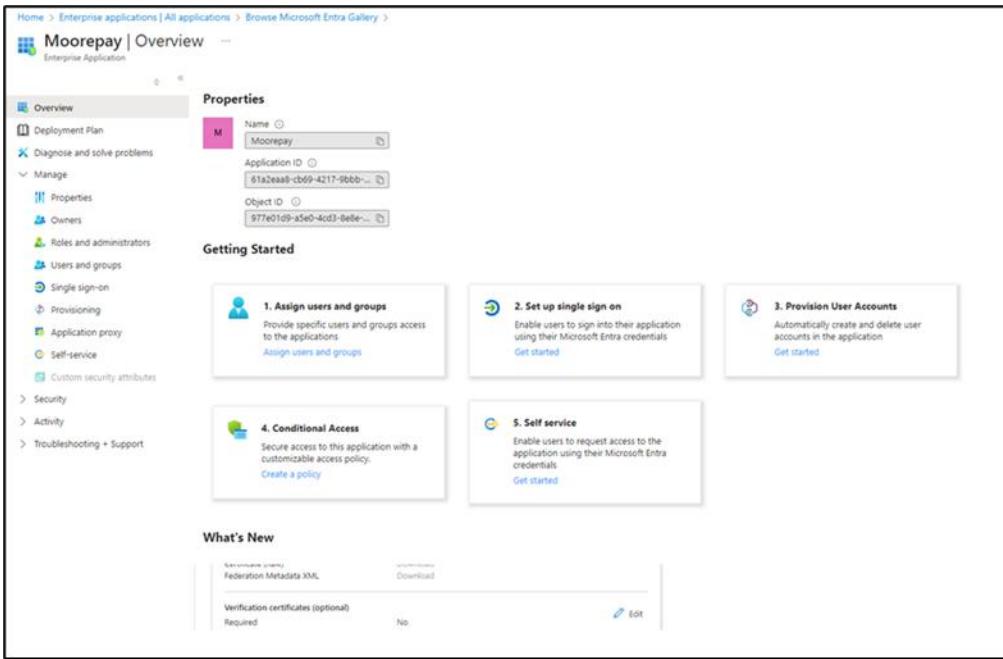


The image shows two side-by-side screenshots. On the left is the Microsoft Entra App Gallery interface, showing a search bar and filters for Single Sign-on, User Account Management, and Categories. Below the search bar are sections for Cloud platforms, including Amazon Web Services (AWS), Google Cloud Platform, and Oracle. On the right is a 'Create your own application' dialog box. It has a 'What's the name of your app?' field containing 'Moorepay', a 'What are you looking to do with your application?' section with a radio button selected for 'Integrate any other application you don't find in the gallery (Non-gallery)', and a note about using Application Proxy or integrating non-gallery apps.

Enabling single sign-on for your app

Once your new application has been set up you should now see it in your dashboard. From here you'll be able to set up single sign-on.

1. In your new application dashboard click on **set up single sign-on**



Moorepay | Overview

Properties

- Name: Moorepay
- Application ID: 61a2eaab-cb69-4217-9bb0-...
- Object ID: 977e01d9-a5e0-4cd3-bb4e-...

Getting Started

1. Assign users and groups
2. Set up single sign on
3. Provision User Accounts
4. Conditional Access
5. Self service

What's New

Federation Metadata XML

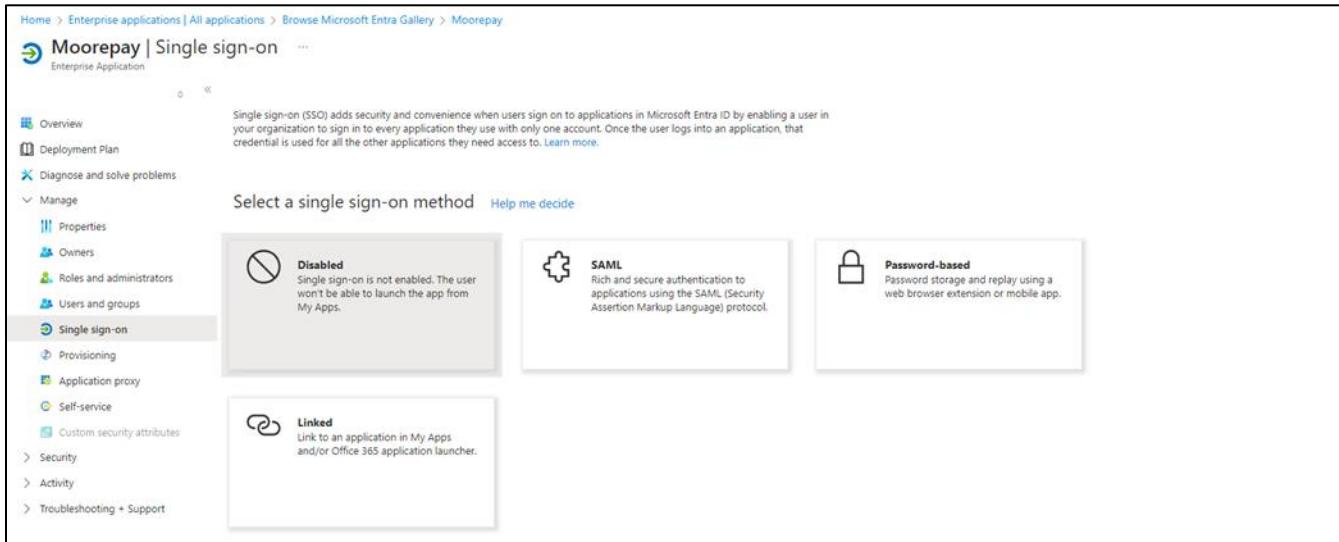
Download

Verification certificates (optional)

Required

No

2. Select SAML



Moorepay | Single sign-on

Select a single sign-on method

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.

Properties

3. In the SAML-based sign-on setup select **edit** in **step 1**

Moorepay | SAML-based Sign-on

Set up Single Sign-On with SAML

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

Attributes & Claims

Fill out required fields in Step 1	
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

SAML Certificates

Token signing certificate	
Status	Active
Thumbprint	2F529F28523F8E750BC167360B1671C35B141C7D
Expiration	11/04/2029, 17:04:26
Notification Email	nearlyheadlesservie@live.com.ph
App Federation Metadata Url	https://login.microsoftonline.com/36a512d2-a873-433a-8a20-1a2a2a2a2a2a
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)

Required
No

Please note {YOUR_ID} = CUSTOMER required below will be provided to you by your consultant. Please reach out to them to receive this ID before starting this process.

For HRWize: Company ID*

4. You will need the following information to complete step 1 of the SAML-based sign-on form:

- Entity ID
<https://identity.hrwize.com/saml>
- Reply URL
<https://identity.hrwize.com/federation/CUSTOMER/signin>
- Logout URL
<https://identity.hrwize.com/federation/CUSTOMER/signout>
- Sign in URL
<https://login.hrwize.com/ids.php?idp=CUSTOMER>

Where 'CUSTOMER' appears, you will need to insert your company name in capitals. If you are unsure what this should be, please contact our support team who will be able to advise.

moorepay-saml

Saml Provider

saml2p

Name •
moorepay-saml

Entity Id: https://as-mp-dev02-identity-v2-pri.azurewebsites.net/saml

Reply Uri: https://as-mp-dev02-identity-v2-pri.azurewebsites.net/federation/moorepay-saml/signin

Logout Uri: https://as-mp-dev02-identity-v2-pri.azurewebsites.net/federation/moorepay-saml/signout

Display name
Saml Provider

5. In the Entra enterprise application basic SAML Configuration screen you'll need to enter Entity ID, Replay URL, Sign on URL and Logout URL as detailed above.

Home > Enterprise applications > All applications > Browse Microsoft Entra Gallery > Moorepay

Moorepay | SAML-based Sign-on

Basic SAML Configuration

Identifier (Entity ID) • Default

Reply URL (Assertion Consumer Service URL) • Index Default

Sign on URL (Optional) Add reply URL

Relay State (Optional) This Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Logout Url (Optional) This URL is used to send the SAML logout response back to the application.

Token signing certificate

Status: Active

Thumbprint: 2F529F28523F8E75D8C16736D81671C35B

Expiration: 11/04/2029, 17:04:26

Notification Email: nearlyheadlesser@live.com.ph

App Federation Metadata Url: <https://login.microsoftonline.com/36a312>

Certificate (Base64)

Certificate (Raw)

Federation Metadata XML

Verification certificates (optional)

Required: No

Active: 0

6. In step 3 of the configuration screen, you'll find the App Federation Metadata URL. You'll need to copy this and keep a copy of this URL secure. The HRWize team will need this URL to complete the registration in HRWize, please share this URL with the HRWize Support team once it is available.

Moorepay | SAML-based Sign-on

Attributes & Claims

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

SAML Certificates

Token signing certificate

Status	Active
Thumbprint	68E163C742BBCBF9EB22C68F998877B7E57D747F
Expiration	01/05/2027, 07:44:16
Notification Email	nearlyheadlesservie@live.com.ph
App Federation Metadata Url	https://login.microsoftonline.com/36a512f2-ae73-408a-89e1-1a2a2a2a2a2a
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)

Required	No
Active	0
Expired	0

Set up Moorepay

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

Login URL	https://login.microsoftonline.com/36a512f2-ae73-408a-89e1-1a2a2a2a2a2a
Microsoft Entra Identifier	https://sts.windows.net/36a512f2-ae73-408a-89e1-1a2a2a2a2a2a
Logout URL	https://login.microsoftonline.com/36a512f2-ae73-408a-89e1-1a2a2a2a2a2a

Test single sign-on with Moorepay

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](#)

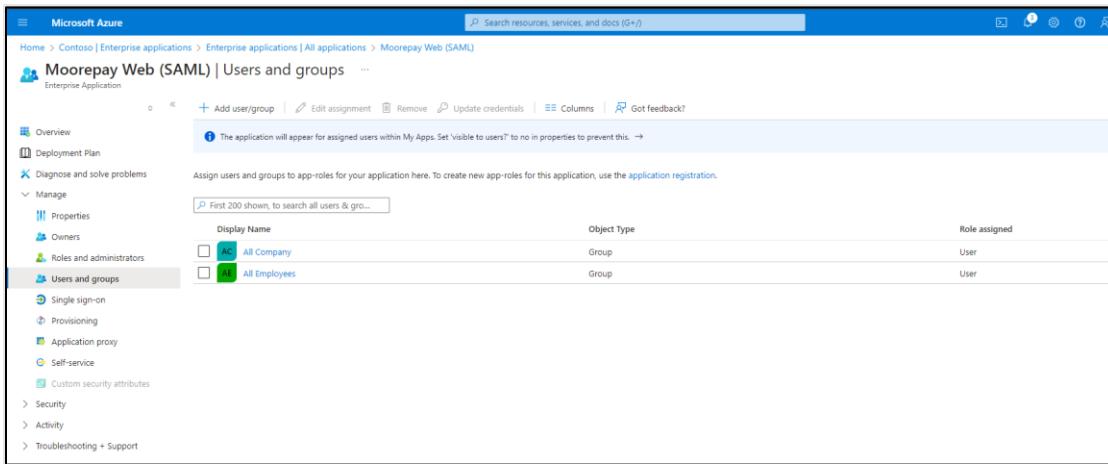
Making your app accessible to users

By default, the Application is inaccessible to any users unless assigned explicitly. That means without assigning your app, employees won't have access.

You can assign it in two ways:

- Depending on your policies as the screenshot below shows
- Toggle off (no) the "Assignment required?" field in the application properties. This will give access to all your users.

Ensure you save whichever method is used.

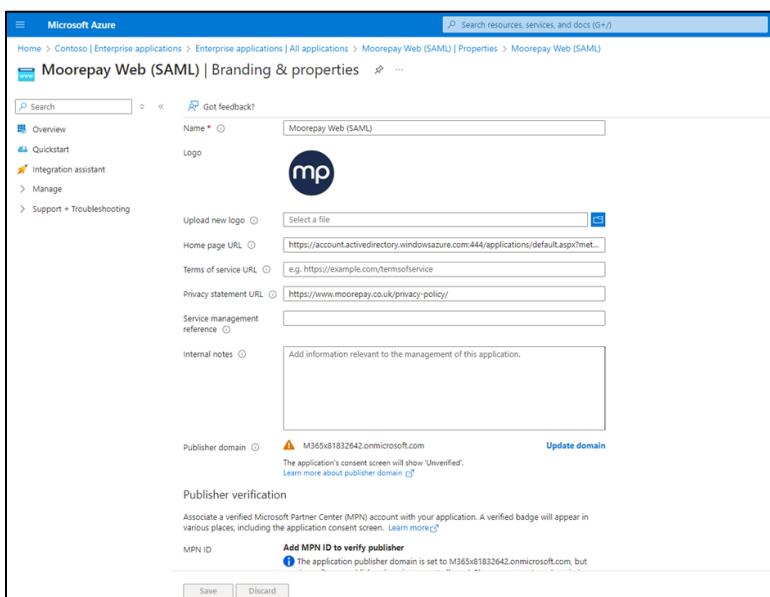


The screenshot shows the 'Users and groups' section of the Azure portal for the 'Moorepay Web (SAML)' application. The left sidebar shows navigation options like Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Application proxy, Self-service, Custom security attributes), Security, Activity, and Troubleshooting + Support. The 'Users and groups' option is selected. The main content area shows a table with two rows:

Display Name	Object Type	Role assigned
All Company	Group	User
All Employees	Group	User

Additional app settings

1. Additional settings can be accessed via **properties** including adding the HRWize logo.



The screenshot shows the 'Branding & properties' section of the Azure portal for the 'Moorepay Web (SAML)' application. The left sidebar shows navigation options like Overview, Quickstart, Integration assistant, Manage, and Support + Troubleshooting. The 'Properties' option is selected. The main content area shows the 'Branding & properties' settings:

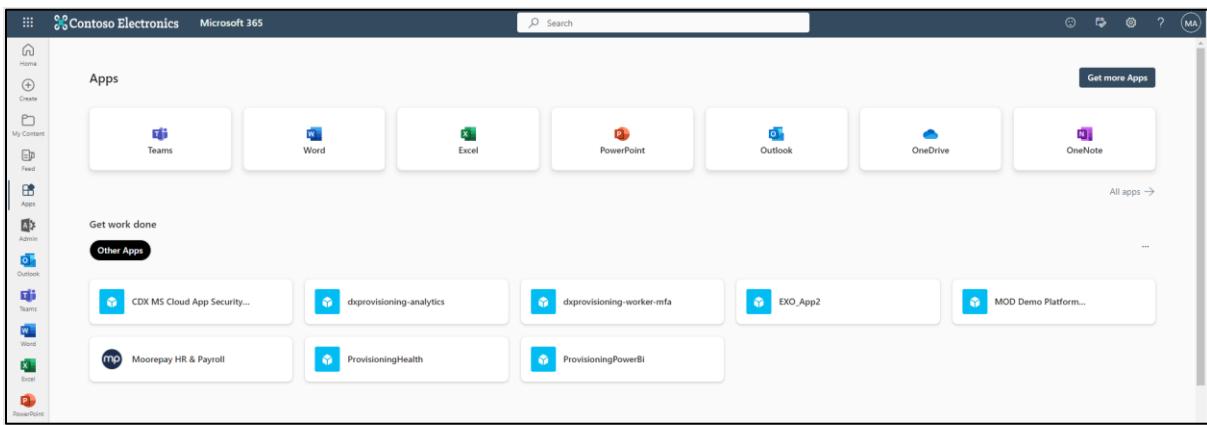
- Logo:** A logo with the letters 'mp' is displayed.
- Upload new logo:** A file input field with the placeholder 'Select a file'.
- Home page URL:** <https://account.activedirectory.windowsazure.com:444/applications/default.aspx?met...>
- Terms of service URL:** [e.g. https://example.com/termsofservice](https://example.com/termsofservice)
- Privacy statement URL:** <https://www.moorepay.co.uk/privacy-policy/>
- Service management reference:** An empty text input field.
- Internal notes:** A text input field for management notes.
- Publisher domain:** M365x@1832642.onmicrosoft.com (with a warning icon: 'The application's consent screen will show 'Unverified'. Learn more about publisher domain')
- Publisher verification:** A section for associating a Microsoft Partner Center (MPN) account.
- MPN ID:** A text input field with the placeholder 'Add MPN ID to verify publisher'.
- Save** and **Discard** buttons at the bottom.

2. Further settings such as the HRWize privacy policy/logo can be set in Application registration.

Please note, the set logo will appear in all Office 365 apps.

Viewing your app in Office 365

Once your app has been set up correctly and SSO has been enabled, HRWize will appear in the list of apps in Microsoft Office 365.



User login impact

If SSO is set-up correctly and the app is visible in Office 365, users will be able to login using the HRWize app or the custom URL <https://login.HRWize.com/ids.php?idp=CUSTOMER> using SSO.

If the username or email in HRWize Identity matches the email address used to login, the system will log straight in. However, if there is no match the user will be prompted to link their HRWize account with their Office 365 account.