App registration instructions

Making payroll & HR easy

moorepay
A Zellis Company

Contents

Introduction

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 Moorepay. 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.

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 Moorepay identity server (IDS)
4. Send your App Federation Metadata to the Moorepay team to complete registration
5. Make your application available to all users

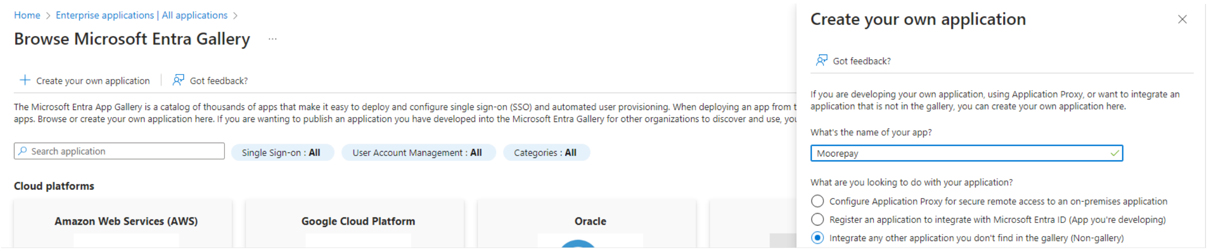
Once the above steps have been completed you and your users will be able to utilise SSO to sign-on to the Moorepay application.

Steps

Creating an app in Entra

1. First head to your Azure portal and search **enterprise applications** in the top search bar. Click on **new application** and then **create your own application**.

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



Home > 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 configure single sign-on (SSO) and automated user provisioning. When deploying an app from t apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discover and use, you

Search application | Single Sign-on : **All** | User Account Management : **All** | Categories : **All**

Cloud platforms

Amazon Web Services (AWS) | **Google Cloud Platform** | **Oracle**

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?

Moorepay ✓

What are you looking to do with your application?

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

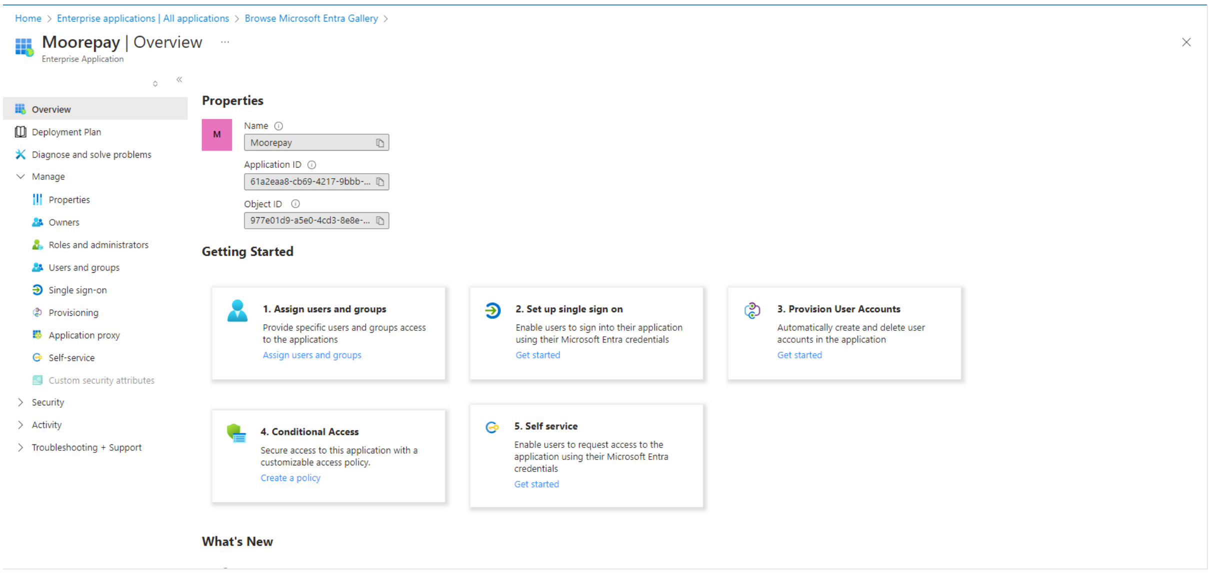
○ Register an application to integrate with Microsoft Entra ID (App you're developing)

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

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**



Properties

Name: Moorepay

Application ID: 61a2eaa8-cb69-4217-9bbb-...

Object ID: 977e01d9-a5e0-4cd3-8e8e-...

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 Microsoft Entra credentials
Get started

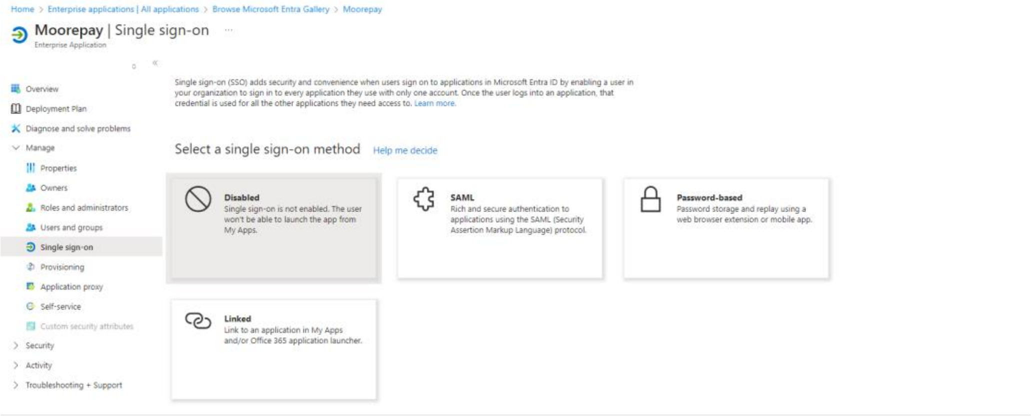
3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

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 Microsoft Entra credentials
Get started

What's New

2. Then select SAML


Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery > Moorepay
Moorepay | Single sign-on ...
Enterprise Application
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
Troubleshooting + Support

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

Select a single sign-on method Help me decide

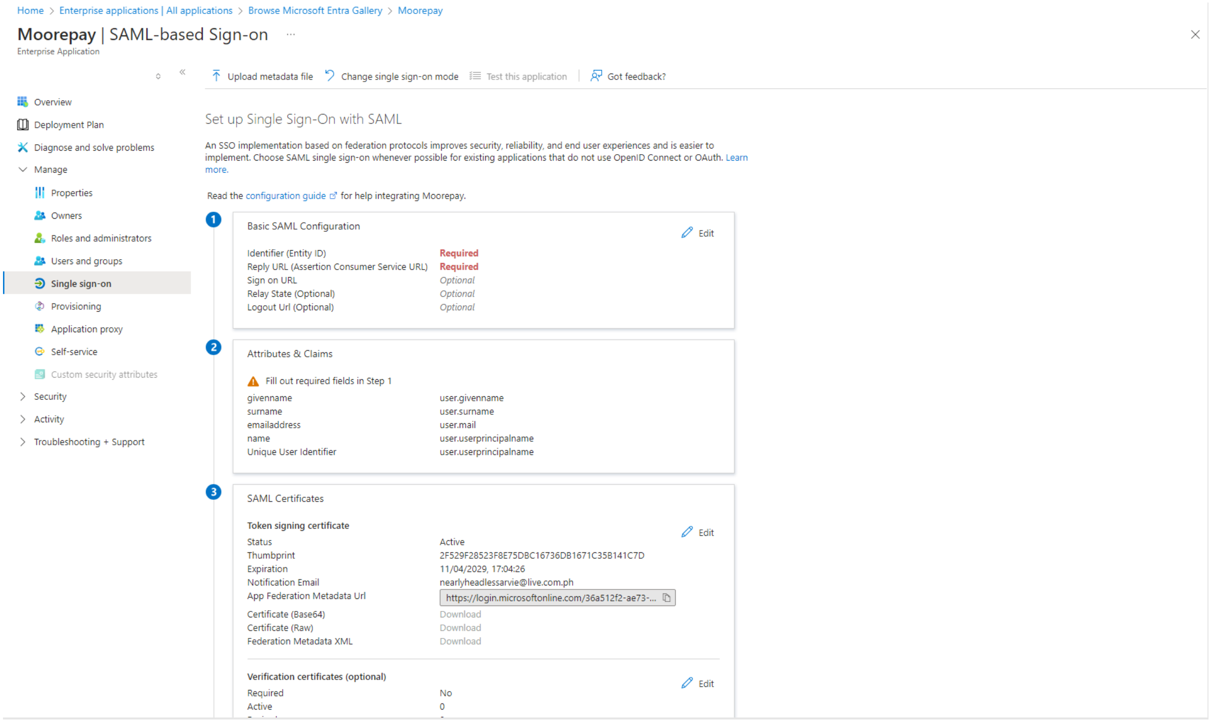
Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

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.

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



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 Moorepay.

1 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*

2 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

3 SAML Certificates

Token signing certificate

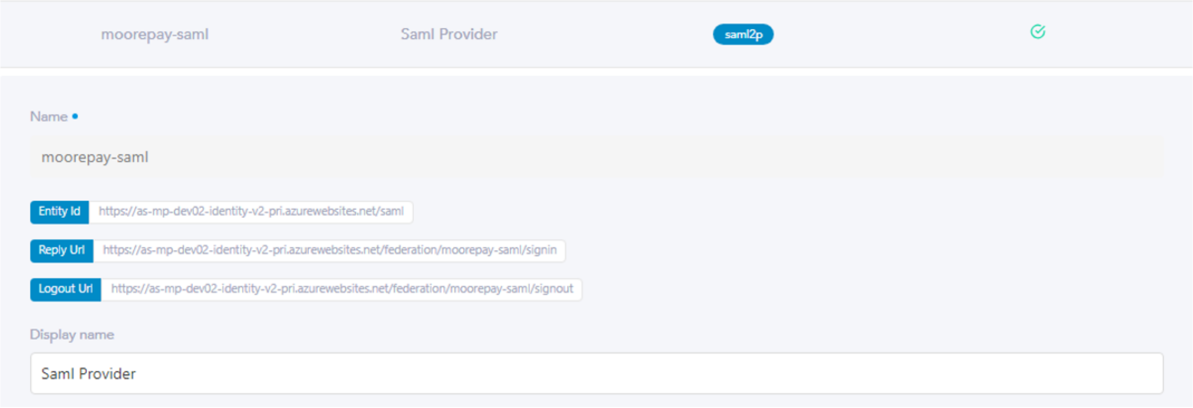
Status	Active
Thumbprint	2F529F28523F8E75DBC16736DB1671C35B141C7D
Expiration	11/04/2029, 17:04:26
Notification Email	nearlyheadlessarvie@live.com.ph
App Federation Metadata Url	https://login.microsoftonline.com/36a512f2-ae73-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)

Required	No
Active	0

4. You will need the following information to complete step 1 of the SAML-based sign-on form:
    a. Entity ID
    https://app-identity.moorepay.co.uk/saml
    b. Reply URL
    https://app-identity.moorepay.co.uk/federation/CUSTOMER/signin
    c. Logout URL
    https://app-identity.moorepay.co.uk/federation/CUSTOMER/signout
    d. Sign in URL
    https://hr.moorepay.co.uk/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

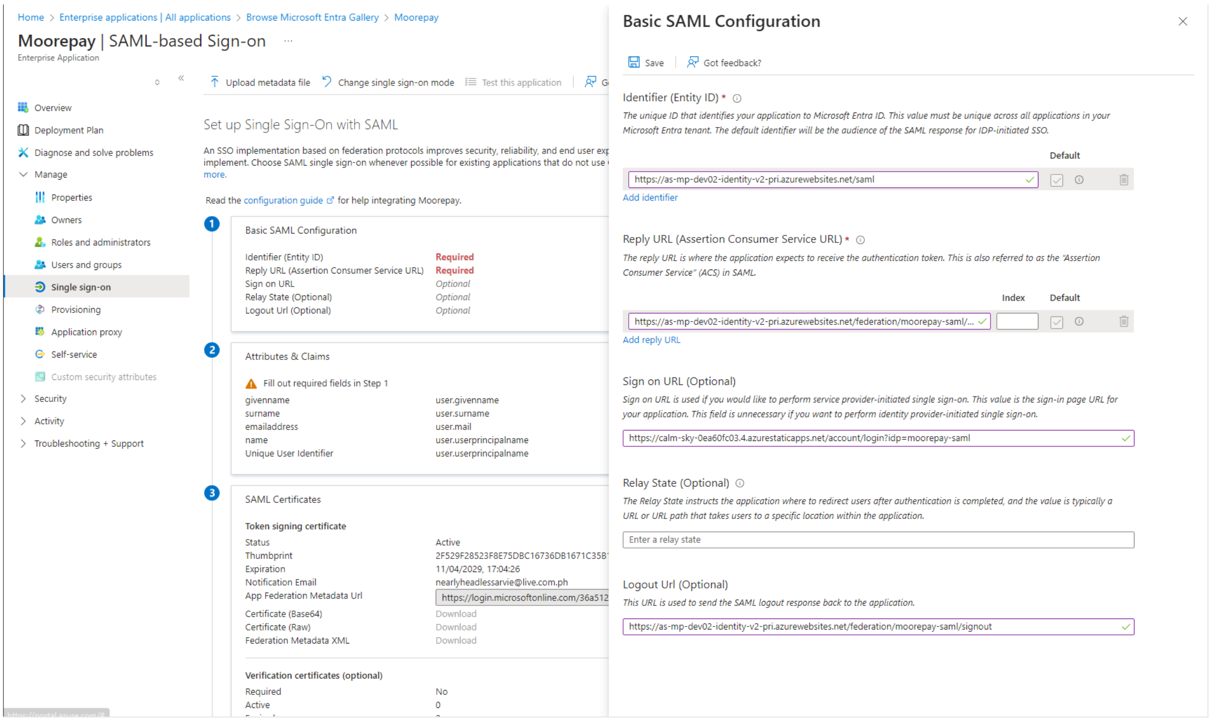
Reply Url: https://as-mp-dev02-identity-v2-pri.azurewebsites.net/federation/moorepay-saml/signin

Logout Url: 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.



Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user exp implement. Choose SAML single sign-on whenever possible for existing applications that do not use more.

Read the configuration guide for help integrating Moorepay.

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	2F529F28523F8E75DBC16736DB1671C35B
Expiration	11/04/2029, 17:04:26
Notification Email	nearlyheadlessarvie@live.com.ph
App Federation Metadata Url	https://login.microsoftonline.com/36a512
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)

Required	No
Active	0

Basic SAML Configuration

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
https://as-mp-dev02-identity-v2-pri.azurewebsites.net/saml ✓	☑

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.

	Index	Default
https://as-mp-dev02-identity-v2-pri.azurewebsites.net/federation/moorepay-saml/... ✓		☑

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

https://calm-sky-0ea60fc03.4.azurestaticapps.net/account/login?idp=moorepay-saml ✓

Relay State (Optional)

The 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.

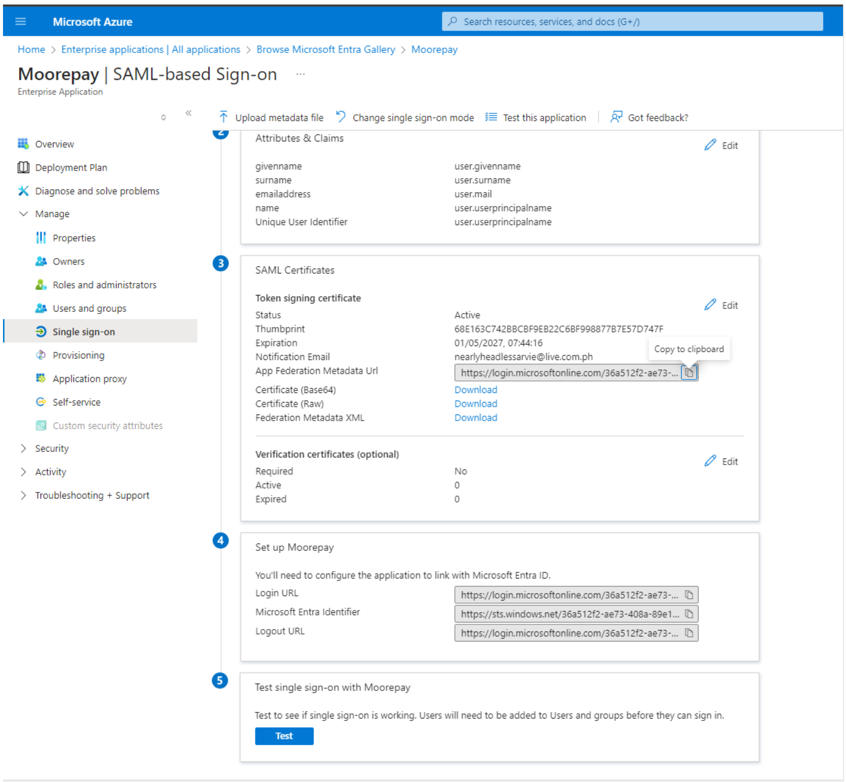
Enter a relay state

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.

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

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 Moorepay team will need this URL to complete the registration in Moorepay, please share this URL with the Moorepay Support team once it is available.



Moorepay | SAML-based Sign-on

Enterprise Application

2 Attributes & Claims

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

3 SAML Certificates

Token signing certificate

Status	Active
Thumbprint	68E163C742BBCBF9EB22C6BF998877B7E57D747F
Expiration	01/05/2027, 07:44:16
Notification Email	nearlyheadlessarvie@live.com.ph
App Federation Metadata Url	https://login.microsoftonline.com/36a512f2-ae73-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)

Required	No
Active	0
Expired	0

4 Set up Moorepay

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

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

5 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.

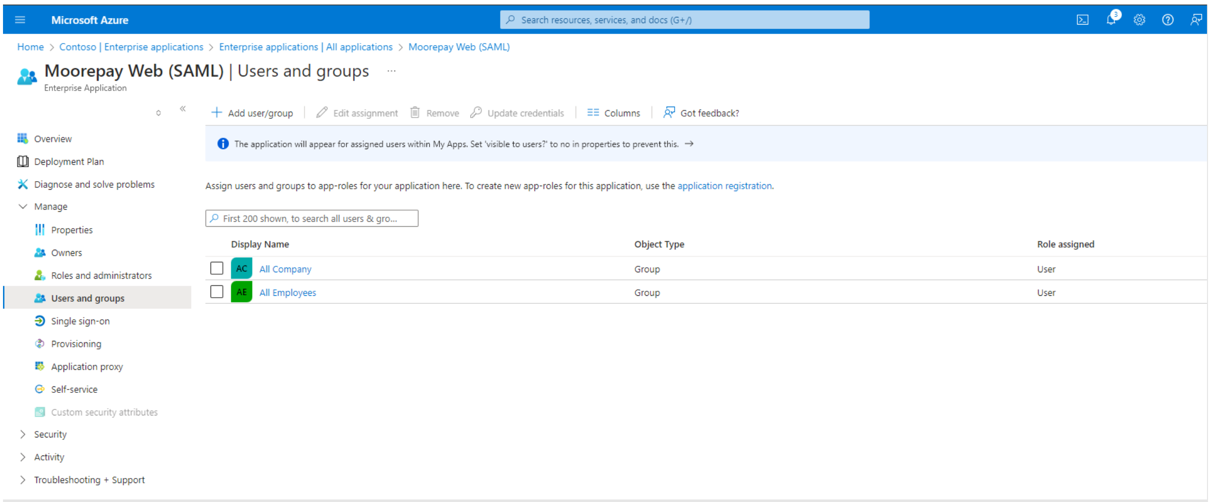
Making your app accessible to users

1. 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.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Contoso | Enterprise applications > Enterprise applications | All applications > Moorepay Web (SAML)

Moorepay Web (SAML) | Users and groups

Enterprise Application

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

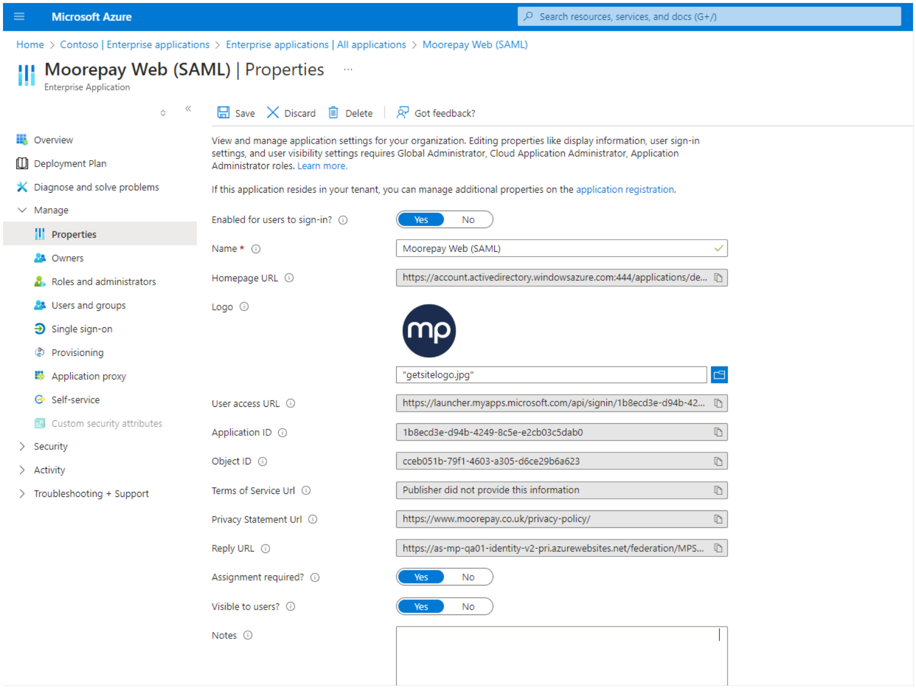
Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration.

First 200 shown, to search all users & gro...

	Display Name	Object Type	Role assigned
□	AC All Company	Group	User
□	AE All Employees	Group	User

Additional app settings

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


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Contoso | Enterprise applications > Enterprise applications | All applications > Moorepay Web (SAML)
Moorepay Web (SAML) | Properties
Enterprise Application
Save
Discard
Delete
Got feedback?
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
Troubleshooting + Support

View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. Learn more.

If this application resides in your tenant, you can manage additional properties on the application registration.

Enabled for users to sign-in? [✓ Yes] No

Name * Moorepay Web (SAML)

Homepage URL https://account.activedirectory.windowsazure.com:444/applications/de...

Logo "getsitelogo.jpg"

User access URL https://launcher.myapps.microsoft.com/api/signin/1b8ecd3e-d94b-42...

Application ID 1b8ecd3e-d94b-4249-8c5e-e2cb03c5dab0

Object ID cceb051b-79f1-4603-a305-d6ce29b6a623

Terms of Service Url Publisher did not provide this information

Privacy Statement Url https://www.moorepay.co.uk/privacy-policy/

Reply URL https://as-mp-qa01-identity-v2-pri.azurewebsites.net/federation/MPS...

Assignment required? [✓ Yes] No

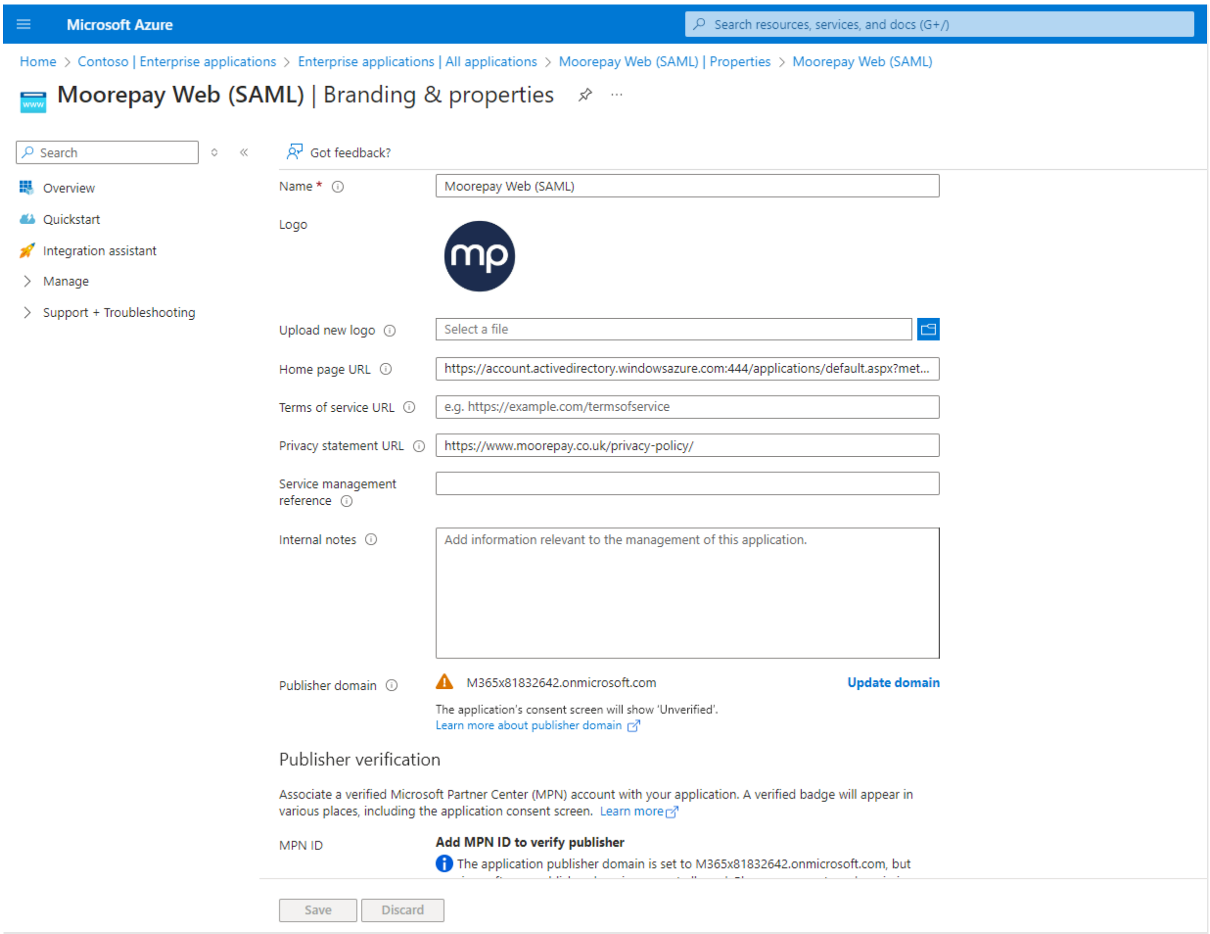
Visible to users? [✓ Yes] No

Notes

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

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

The Moorepay privacy policy, can be found here: https://www.moorepay.co.uk/privacy-policy/



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Contoso | Enterprise applications > Enterprise applications | All applications > Moorepay Web (SAML) | Properties > Moorepay Web (SAML)
Search
Overview
Quickstart
Integration assistant
Manage
Support + Troubleshooting
Got feedback?
mp
Update domain
Save
Discard

Moorepay Web (SAML) | Branding & properties

Name *	Moorepay Web (SAML)
Logo	
Upload new logo	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
Privacy statement URL	https://www.moorepay.co.uk/privacy-policy/
Service management reference	
Internal notes	Add information relevant to the management of this application.
Publisher domain	M365x81832642.onmicrosoft.com The application's consent screen will show 'Unverified'. Learn more about publisher domain

Publisher verification

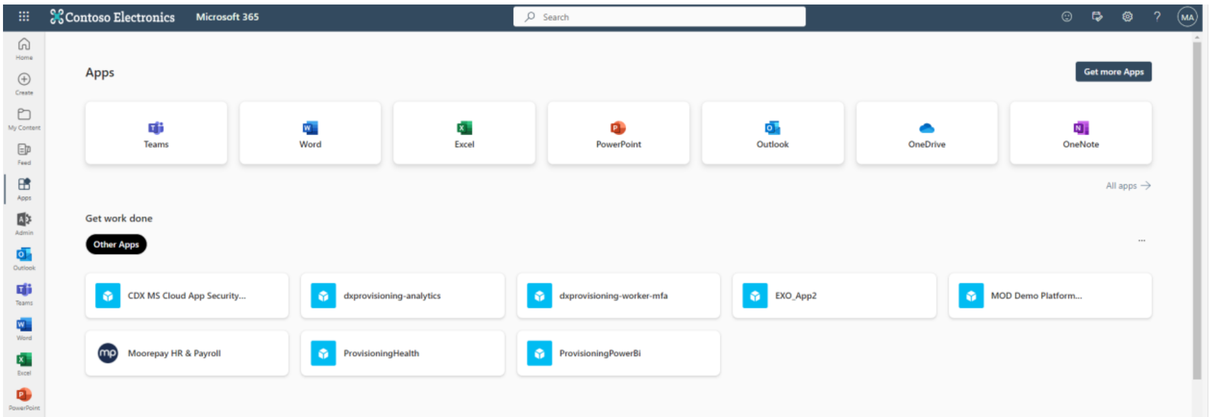
Associate a verified Microsoft Partner Center (MPN) account with your application. A verified badge will appear in various places, including the application consent screen. Learn more

MPN ID: Add MPN ID to verify publisher

The application publisher domain is set to M365x81832642.onmicrosoft.com, but

Viewing your app in Office 365

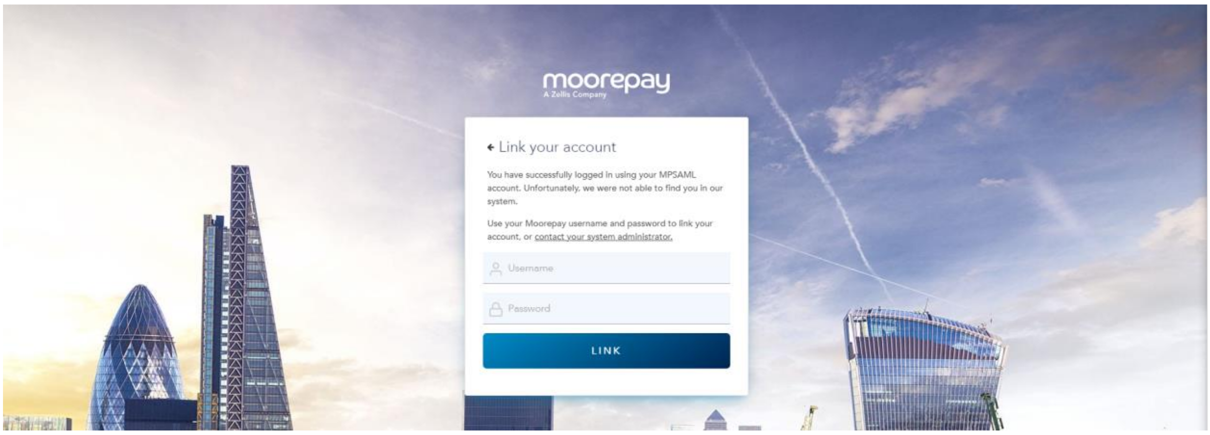
Once your app has been set-up correctly and SSO has been enabled, Moorepay will appear in the list of apps in Microsoft Office 365.



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 Moorepay app or the custom URL https://hr.moorepay.co.uk/ids.php?idp=CUSTOMER using SSO.

If the username or email in Moorepay 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 Moorepay account with their Office 365 account.



Link your account

You have successfully logged in using your MPSAML account. Unfortunately, we were not able to find you in our system.

Use your Moorepay username and password to link your account, or contact your system administrator.