



App registration instructions

Making payroll & HR easy

moorepay
A Zellis Company

Contents

Introduction.....	3
Overview	4
What is the process for enabling SSO?.....	4
Steps	5
Creating an app in Entra.....	5
Enabling single sign-on for your app.....	6
Making your app accessible to users.....	11
Additional app settings	12
Viewing your app in Office 365	14
User login impact.....	15

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)

The screenshot shows the Microsoft Entra 'Create your own application' dialog box. The main window displays the 'Browse Microsoft Entra Gallery' page with a search bar and filters for 'Single Sign-on: All', 'User Account Management: All', and 'Categories: All'. Below the search bar, there are buttons for 'Amazon Web Services (AWS)', 'Google Cloud Platform', and 'Oracle'. The dialog box is open on the right side, titled 'Create your own application'. It includes a 'Got feedback?' link, a description of the gallery, and a form to create a new application. The form has a text input field for the application name, which contains 'Moorepay'. Below the name field, there are three radio button options: '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)', and 'Integrate any other application you don't find in the gallery (Non-gallery)'. The third option is selected.

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**

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

Properties

Name: Moorepay

Application ID: 61a2ea88-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 | Single sign-on

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

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

Moorepay | SAML-based Sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Test this application | 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

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.

- Basic SAML Configuration** Edit

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**

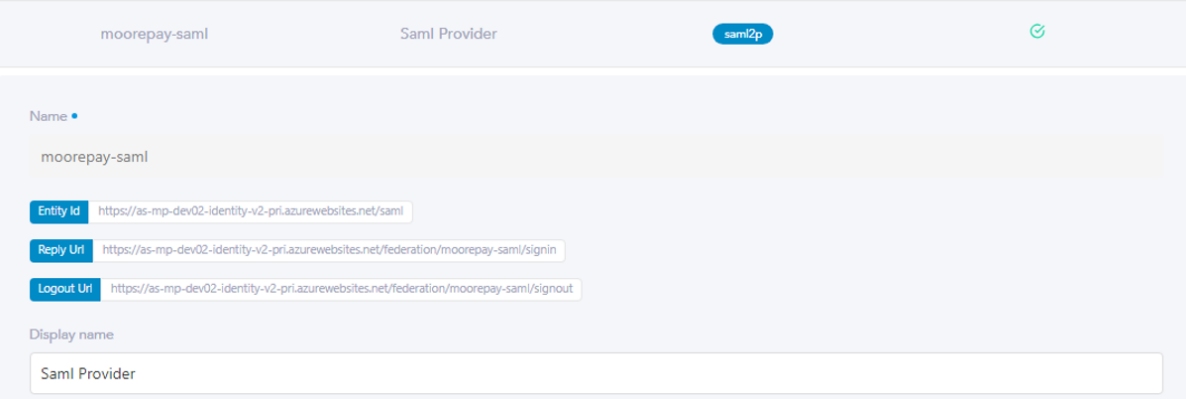
Fill out required fields in Step 1

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- SAML Certificates** Edit

Token signing certificate	
Status	Active
Thumbprint	2F525F28523F8E75DB16736DB1671C35B141C7D
Expiration	11/04/2023, 17:04:26
Notification Email	nearlyheadlessanvie@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:
- Entity ID
<https://app-identity.moorepay.co.uk/saml>
 - Reply URL
<https://app-identity.moorepay.co.uk/federation/<COMPANY NAME>/signin>
 - Logout URL
<https://app-identity.moorepay.co.uk/federation/<COMPANY NAME>/signout>
 - Sign in URL
<https://app.moorepay.co.uk/account/login?idp=<COMPANY NAME>>

Where <COMPANY NAME> 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.



The screenshot shows a configuration page for a SAML Provider. At the top, the name 'moorepay-saml' is displayed, followed by 'Saml Provider' and a 'saml2p' status indicator. Below this, the 'Name' field is set to 'moorepay-saml'. Three fields are listed: 'Entity id' with the URL 'https://as-mp-dev02-identity-v2-pri.azurewebsites.net/saml', 'Reply Url' with 'https://as-mp-dev02-identity-v2-pri.azurewebsites.net/federation/moorepay-saml/signin', and 'Logout Url' with 'https://as-mp-dev02-identity-v2-pri.azurewebsites.net/federation/moorepay-saml/signout'. The 'Display name' field is set to 'Saml Provider'.

- 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.

The screenshot displays the 'Basic SAML Configuration' interface for the Moorepay application. The left sidebar shows the navigation menu with 'Single sign-on' selected. The main content area is divided into three numbered steps:

- Basic SAML Configuration:**
 - Identifier (Entity ID) * **Required**: **Default**
 - Reply URL (Assertion Consumer Service URL) * **Required**: **Index Default**
 - Sign on URL (Optional):
 - Relay State (Optional):
 - Logout Url (Optional):
- Attributes & Claims:**
 - Fill out required fields in Step 1
 - Attributes: givenname, surname, emailaddress, name, Unique User Identifier
 - Claims: user.givenname, user.surname, user.mail, user.userprincipalname, user.userprincipalname
- SAML Certificates:**
 - Token signing certificate: Status (Active), Thumbprint (2f328f28823f8e750bc16736081671c358), Expiration (11/04/2029, 17:04:26), Notification Email (nearlyheadlessarvie@live.com.ph), App Federation Metadata Url (https://login.microsoftonline.com/36a512...), Certificate (Base64), Certificate (Raw), Federation Metadata XML (Download)
 - Verification certificates (optional): Required (No), Active (0)

- 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.

The screenshot shows the Microsoft Azure portal interface for configuring an enterprise application named 'Moorepay'. The left-hand navigation pane includes sections for Overview, Deployment Plan, Diagnose and solve problems, Manage, Properties, Owners, Roles and administrators, Users and groups, Single sign-on (highlighted), Provisioning, Application proxy, Self-service, and Custom security attributes. Below this are Security, Activity, and Troubleshooting + Support.

The main content area displays the configuration steps for 'Moorepay | SAML-based Sign-on'. At the top, there are links for 'Upload metadata file', 'Change single sign-on mode', 'Test this application', and 'Got feedback?'. The configuration is divided into several sections:

- Attributes & Claims:** A table listing attributes and their corresponding claims.

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- SAML Certificates:** A section for managing certificates.
 - Token signing certificate:** Shows a certificate with status 'Active', thumbprint '68E163C7428BCF9EB22C68F998877B7E5D747F', and expiration '01/05/2027, 07:44:16'. The notification email is 'nearly/headlessarvie@live.com.ph'. The App Federation Metadata URL is 'https://login.microsoftonline.com/36a512f2-ae73-...'. There are 'Download' links for the Base64, Raw, and XML versions of the certificate.
 - Verification certificates (optional):** A table showing that Required, Active, and Expired certificates are all set to 'No'.
- Set up Moorepay:** A section where you configure the application to link with Microsoft Entra ID. It lists the Login URL, Microsoft Entra Identifier, and Logout URL, all pointing to the same Microsoft Entra ID endpoint.
- Test single sign-on with Moorepay:** A section with a 'Test' button to verify the configuration.

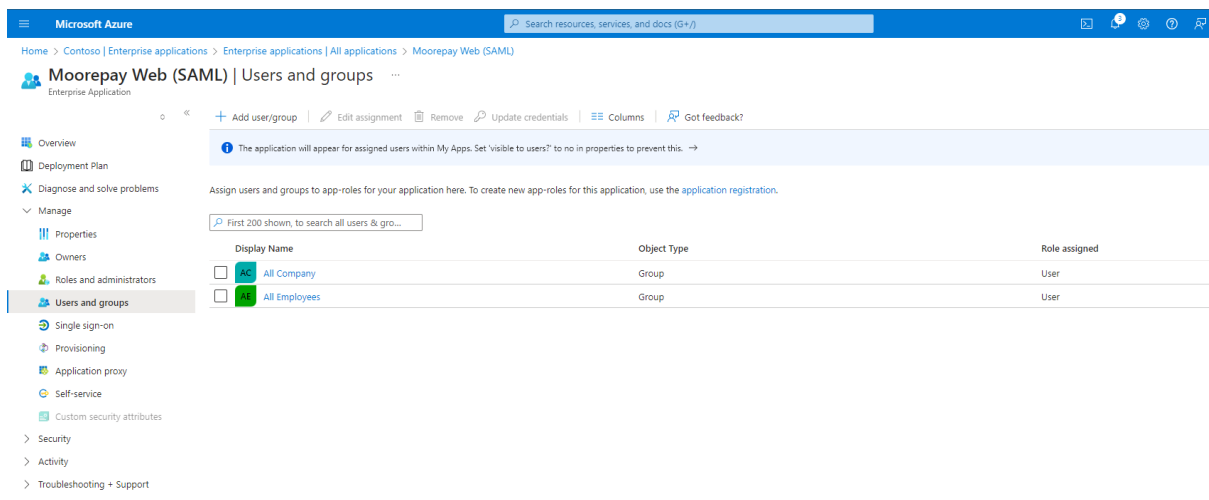
Making your app accessible to users

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.



The screenshot displays the Azure portal interface for the 'Moorepay Web (SAML)' application. The 'Users and groups' section is active, showing a table of assigned users and groups. The table has three columns: 'Display Name', 'Object Type', and 'Role assigned'. Two entries are listed: 'All Company' and 'All Employees', both of type 'Group' and assigned the role 'User'. A search bar is visible above the table, and a message at the top indicates that the application will appear for assigned users within My Apps.

Display Name	Object Type	Role assigned
<input type="checkbox"/> All Company	Group	User
<input type="checkbox"/> All Employees	Group	User

Additional app settings

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

Microsoft Azure

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

Application proxy

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/>

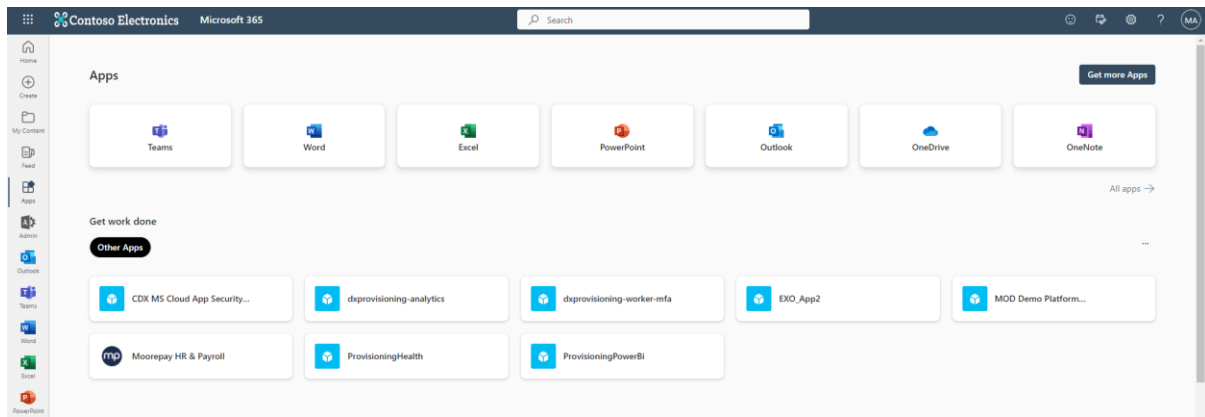
The screenshot displays the 'Branding & properties' configuration page for an application in the Microsoft Azure portal. The breadcrumb trail indicates the path: Home > Contoso | Enterprise applications > Enterprise applications | All applications > Moorepay Web (SAML) | Properties > Moorepay Web (SAML). The page title is 'Moorepay Web (SAML) | Branding & properties'. A search bar and a 'Got feedback?' link are at the top. The left-hand navigation menu includes 'Overview', 'Quickstart', 'Integration assistant', 'Manage', and 'Support + Troubleshooting'. The main content area contains the following fields and sections:

- Name:** Moorepay Web (SAML)
- Logo:** A circular logo with the letters 'mp' in white on a dark blue background.
- Upload new logo:** A button labeled 'Select a file' with a file upload icon.
- 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:** An empty text input field.
- Internal notes:** A text area with the placeholder text 'Add information relevant to the management of this application.'
- Publisher domain:** M365x81832642.onmicrosoft.com. A warning icon indicates that the application's consent screen will show 'Unverified'. A blue 'Update domain' button is present. A link 'Learn more about publisher domain' is also provided.
- Publisher verification:** A section with the text: '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:** A section with the heading 'Add MPN ID to verify publisher' and an information icon. The text below reads: 'The application publisher domain is set to M365x81832642.onmicrosoft.com, but'.

At the bottom of the page, there are two buttons: 'Save' and 'Discard'.

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://app.moorepay.co.uk/account/login?idp=<NAME>> 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.

