



# Instructions de configuration SSO



## Table des matières

Instructions de configuration SSO .....	1
Quelle est la procédure à suivre pour activer l'authentification unique (SSO)? .....	4
Créer une application dans Entra .....	4
Activer l'authentification unique pour votre application .....	5
Rendre votre application accessible aux utilisateurs .....	7
Paramètre supplémentaires de l'application.....	8
Afficher votre application dans Office 365 .....	9
Impact de la connexion utilisateur .....	10

Dans ce guide, nous vous expliquons comment créer et enregistrer une application d'entreprise SAML dans Microsoft Entra (anciennement Azure Active Directory).

Cette application doit être utilisée comme fournisseur d'identité privé dans HRWize. Elle est nécessaire dans le cadre de l'authentification unique (SSO).

Vous trouverez de plus amples informations utiles de Microsoft Entra [ici](#).



#### **Réduire le risque**

Réduisez le risque lié à la saisie de données en double. Utilisez HRWize comme source unique de vérité.



#### **Éliminer les inefficacités**

Plus besoin de supprimer et de maintenir des utilisateurs sur les deux plateformes. Simplifiez les processus RH et améliorez l'efficacité.



#### **Améliorer la sécurité des données**

Gestion des dossiers dans un seul système plutôt que deux, amélioration de la sécurité des données et mise en place d'une conformité totale.

## Aperçu

### Quelle est la procédure à suivre pour activer l'authentification unique (SSO)?

1. Configurez votre application d'entreprise SAML dans Microsoft Entra.
2. Activez l'authentification unique (SSO) dans votre application d'entreprise SAML.
3. Saisissez les informations de configuration SAML dans le serveur d'identité HRWize (IDS).
4. Envoyez les métadonnées de fédération d'applications à l'équipe HRWize pour terminer l'enregistrement.
5. Rendez votre application accessible à tous les utilisateurs.

Une fois les étapes ci-dessus terminées, vous et vos utilisateurs pourrez utiliser l'authentification unique (SSO) pour vous connecter à l'application HRWize.

## Processus de configuration

### Créer une application dans Entra

1. Connectez-vous à votre [portail Azure](#) et recherchez « **applications d'entreprise** » dans la barre de recherche supérieure. Cliquez sur « **nouvelle application** », puis sur « **créer votre propre application** ».

**Remarque:** il est important de créer une nouvelle application et de **ne pas** simplement mettre à jour vos informations d'identification SSO actuelles, car cela empêcherait vos utilisateurs de se connecter via votre SSO existant.

2. Entrez le nom que vous souhaitez donner à votre application. Nous vous recommandons « HRWize » pour plus de facilité. Sélectionnez ensuite « Intégrer toute autre application que vous ne trouvez pas dans la galerie ». (Hors galerie)

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 the gallery, you can use the app's configuration to set up SSO and user provisioning. If you are wanting to publish an application you have developed into the Microsoft Entra App Gallery for other organizations to discover and use, you can create your own application here.

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

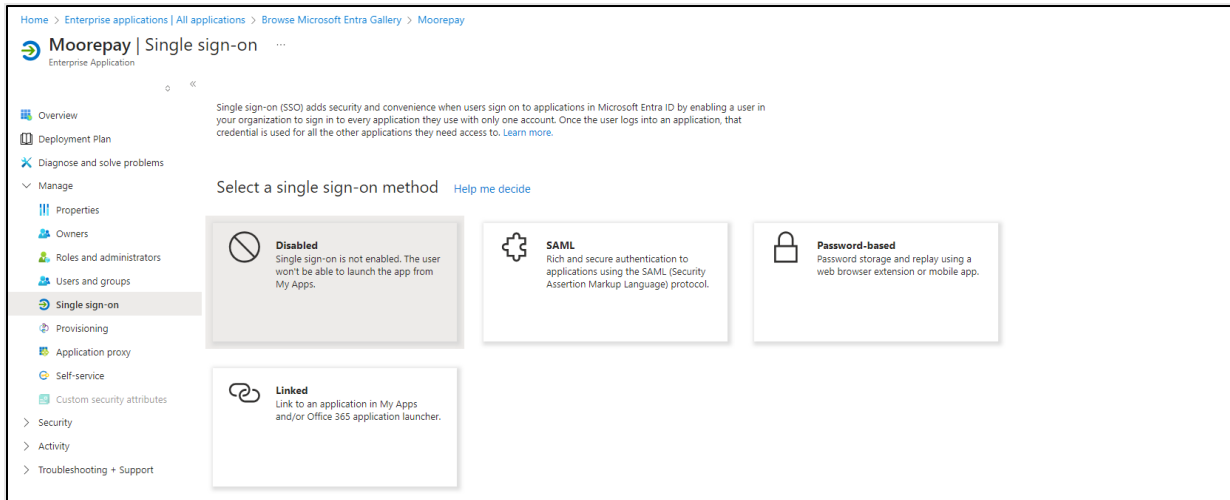
☐ Register an application to integrate with Microsoft Entra ID (App you're developing)

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

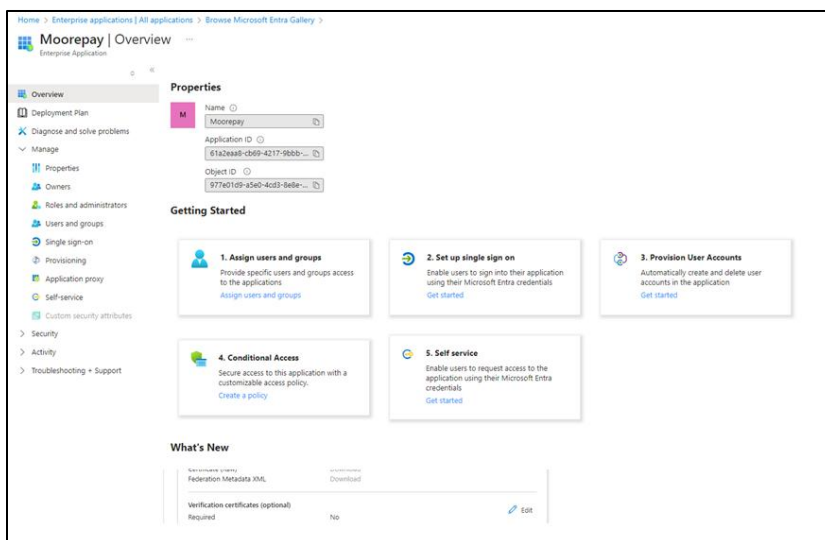
## Activer l'authentification unique pour votre application

Une fois votre nouvelle application configurée, vous devriez la voir apparaître dans votre tableau de bord. À partir de là, vous pourrez configurer l'authentification unique.

1. Dans le tableau de bord de votre nouvelle application, cliquez sur « **Configurer l'authentification unique** ».
2. Sélectionnez SAML.



3. Dans la configuration de connexion basée sur SAML, sélectionnez « Modifier » à l'étape 1.



4. Vous aurez besoin des informations suivantes pour remplir l'étape 1 du formulaire de connexion basé sur SAML:

- Identifiant de l'entité  
<https://identity.hrwise.com/saml>
- URL de réponse  
<https://identity.hrwise.com/federation/CUSTOMER/signin>
- URL de déconnexion  
<https://identity.hrwise.com/federation/CUSTOMER/signout>
- URL de connexion  
<https://login.hrwise.com/ids.php?idp=CUSTOMER>

Là où apparaît « CLIENT », vous devrez insérer le nom de votre entreprise en majuscules. Si vous ne savez pas comment le saisir, veuillez contacter notre équipe d'assistance qui se fera un plaisir de vous aider.

The screenshot shows a configuration page for a SAML provider named 'moorepay-saml'. At the top, there's a header with 'moorepay-saml', 'Saml Provider', and a 'saml2p' button. Below this, there's a 'Name' field with the value 'moorepay-saml'. Underneath, there are three input fields: 'Entity Id' with the value 'https://as-mp-dev02-identity-v2-pri.azurewebsites.net/saml', 'Reply Uri' with 'https://as-mp-dev02-identity-v2-pri.azurewebsites.net/federation/moorepay-saml/signin', and 'Logout Uri' with 'https://as-mp-dev02-identity-v2-pri.azurewebsites.net/federation/moorepay-saml/signout'. At the bottom, there's a 'Display name' field with the value 'Saml Provider'.

5. Dans l'écran Configuration SAML de base de l'application d'entreprise Entra, vous devrez saisir l'ID d'entité, l'URL de relecture, l'URL de connexion et l'URL de déconnexion comme indiqué ci-dessus.

The screenshot shows the 'Basic SAML Configuration' window in the Microsoft Entra admin center. The window is divided into two main sections: 'Set up Single Sign-On with SAML' on the left and 'Basic SAML Configuration' on the right. The left section has a 'Set up Single Sign-On with SAML' heading and a 'Read the configuration guide' link. The right section has a 'Basic SAML Configuration' heading and a 'Save' button. It contains several input fields: 'Identifier (Entity ID)' with the value 'https://as-mp-dev02-identity-v2-pri.azurewebsites.net/saml', 'Reply URL (Assertion Consumer Service URL)' with 'https://as-mp-dev02-identity-v2-pri.azurewebsites.net/federation/moorepay-saml...', 'Sign on URL (Optional)' with 'https://login-hrwise.com/ids.php?idp=moorepay-saml', and 'Logout Uri (Optional)' with 'https://as-mp-dev02-identity-v2-pri.azurewebsites.net/federation/moorepay-saml/signout'. There are also sections for 'Attributes & Claims' and 'SAML Certificates'.

6. À l'étape 3 de l'écran de configuration, vous trouverez l'URL des métadonnées de fédération d'applications. Vous devrez la copier et conserver une copie de cette URL en lieu sûr. L'équipe HRWize aura besoin de cette URL pour terminer l'enregistrement dans HRWize. Veuillez communiquer cette URL à l'équipe d'assistance HRWize dès qu'elle sera disponible.

The screenshot displays the Microsoft Azure portal interface for configuring the Moorepay SAML-based Sign-on application. The left-hand navigation pane lists various management options, with 'Single sign-on' currently selected. The main content area is organized into several sections:

- Attributes & Claims:** A table mapping application attributes to user attributes. For example, 'givenname' maps to 'user.givenname', and 'Unique User Identifier' maps to 'user.userprincipalname'.
- SAML Certificates:** This section contains a 'Token signing certificate' which is 'Active'. It provides details such as the thumbprint (68E163C742B8CBF9E822C68F998877B7E57D747F), expiration date (01/05/2027, 07:44:16), and notification email (nearlyheadlessarvie@live.com.ph). A 'Federation Metadata URL' is also listed, which is the URL that needs to be copied for HRWize. Below this, there are download links for the certificate in Base64, Raw, and Federation Metadata XML formats.
- Verification certificates (optional):** A section for optional verification certificates, currently showing 'Required' as 'No' and 'Active'/'Expired' counts as '0'.
- Set up Moorepay:** This section provides instructions on how to configure the application to link with Microsoft Entra ID. It includes fields for the 'Login URL', 'Microsoft Entra Identifier', and 'Logout URL', each with a corresponding URL provided.
- Test single sign-on with Moorepay:** A section at the bottom with a 'Test' button to verify if the single sign-on is working.

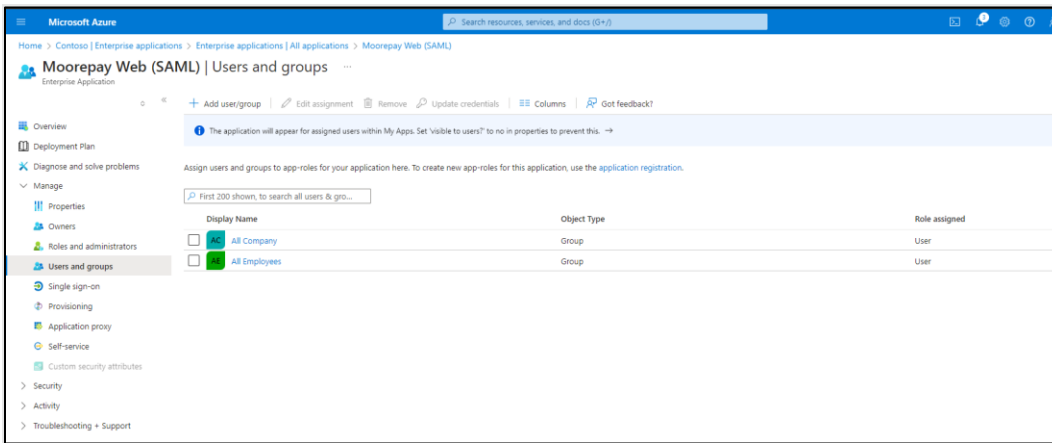
## Rendre votre application accessible aux utilisateurs

Par défaut, l'application est inaccessible à tous les utilisateurs, sauf si elle leur est explicitement attribuée. Cela signifie que sans attribution, vos employés n'y auront pas accès.

### Vous pouvez l'attribuer de deux manières :

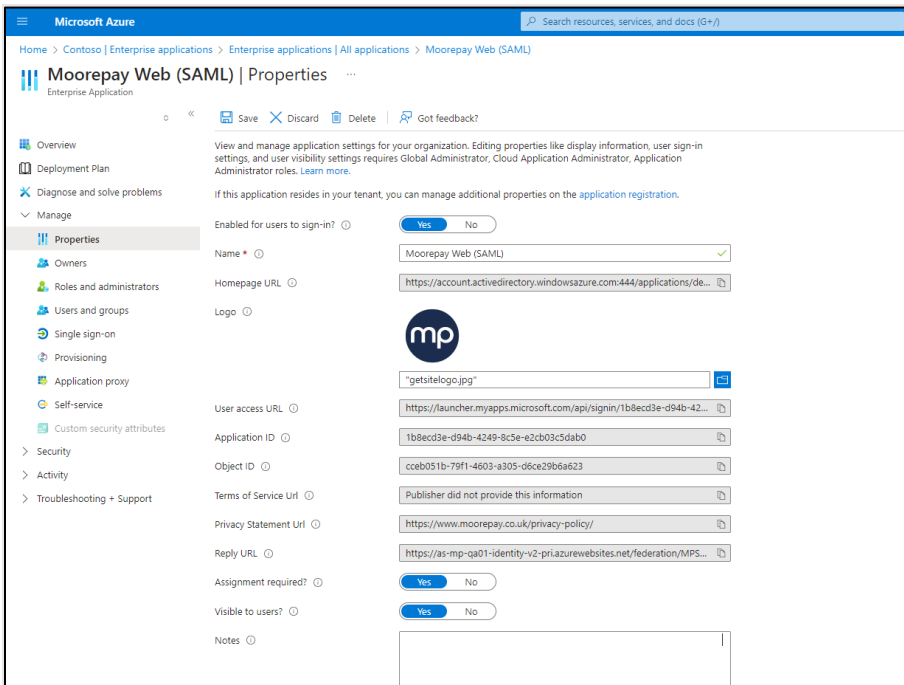
- En fonction de vos politiques, comme le montre la capture d'écran ci-dessous
- Désactivez (non) le champ « *Attribution requise ?* » dans les propriétés de l'application. Cela permettra à tous vos utilisateurs d'y accéder.

Veillez à enregistrer la méthode utilisée.



## Paramètre supplémentaire de l'application

1. Des paramètres supplémentaires sont accessibles via les **propriétés**, notamment l'ajout du logo HRWize.



Microsoft Azure

Home > Contoso > Enterprise applications > Enterprise applications > All applications > Moorepay Web (SAML) > Properties > Moorepay Web (SAML)

Moorepay Web (SAML) | Branding & properties

Search

Overview

Quickstart

Integration assistant

Manage

Support + Troubleshooting

Name \* Moorepay Web (SAML)

Logo

Upload new logo

Home page URL

Terms of service URL

Privacy statement URL

Service management reference

Internal notes

Publisher domain

Publisher verification

MPN ID

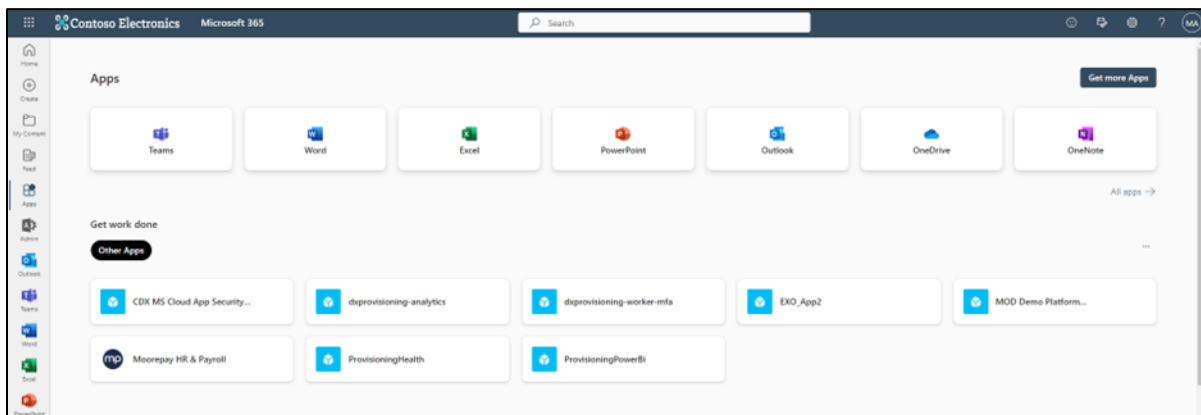
Save Discard

2. D'autres paramètres, tels que la politique de confidentialité/le logo HRWize, peuvent être définis dans l'enregistrement de l'application.

Veuillez noter que le logo défini apparaîtra dans toutes les applications Office 365.

## Afficher votre application dans Office 365

Une fois votre application correctement configurée et l'authentification unique (SSO) activée, HRWize apparaîtra dans la liste des applications dans Microsoft Office 365.



## Impact de la connexion utilisateur

Si l'authentification unique (SSO) est correctement configurée et que l'application est visible dans Office 365, les utilisateurs pourront se connecter à l'aide de l'application HRWize ou de l'URL personnalisée <https://login.HRWize.com/ids.php?idp=CUSTOMER> en utilisant l'authentification unique (SSO).

Si le nom d'utilisateur ou l'adresse courriel dans HRWize Identity correspond à l'adresse courriel utilisée pour se connecter, le système se connectera directement. Toutefois, en cas de non-correspondance, l'utilisateur sera invité à associer son compte HRWize à son compte Office 365.