



Instructions de configuration SSO



www.hrwise.com

juin-juillet 2025

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.

Remarque : Lors de l'utilisation de plusieurs domaines, chaque domaine doit être ajouté à la liste blanche.

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 integrate it with your organization's identity provider. If you are wanting to publish an application you have developed into the Microsoft Entra 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

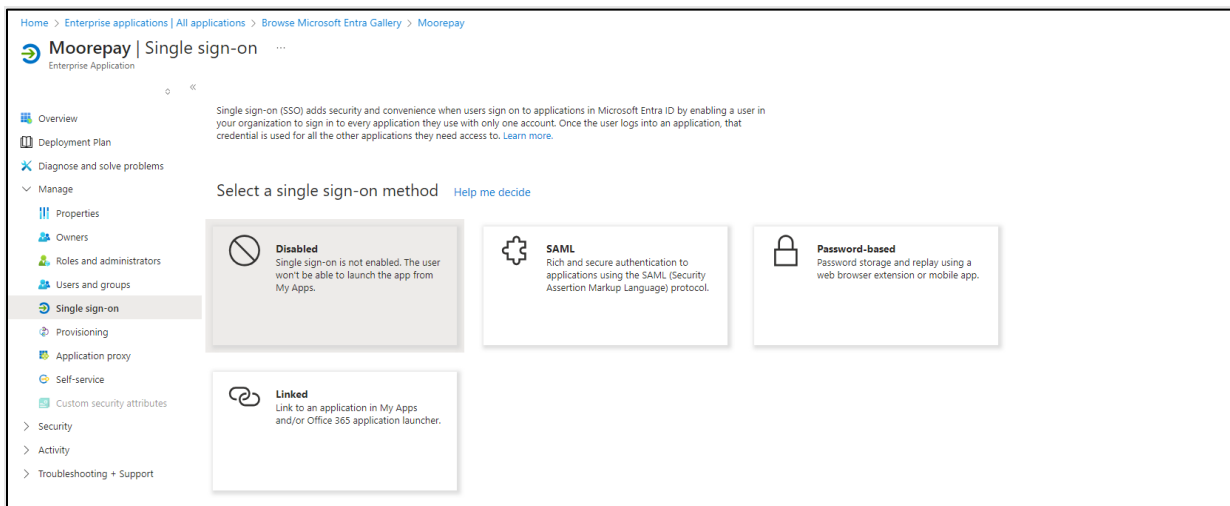
☐ Register an application to integrate with Microsoft Entra ID (App you're developing)

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

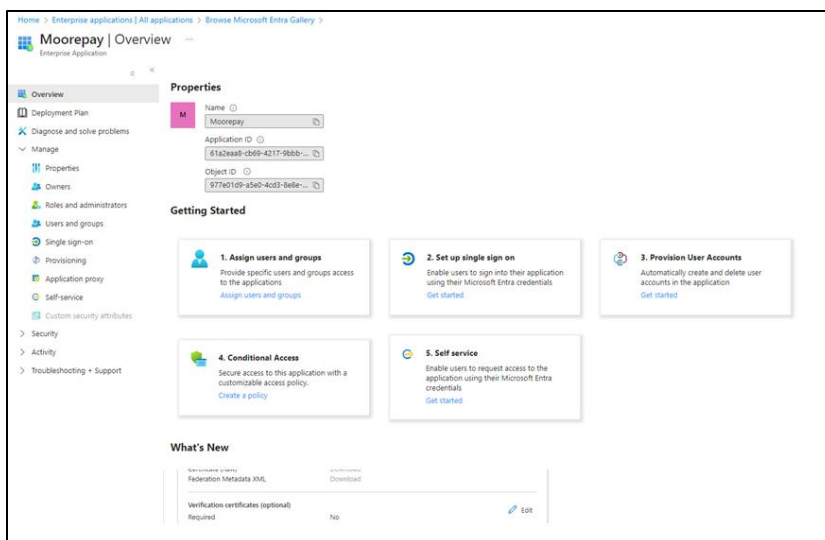
Activer l'authentification unique pour votre application

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.



NB. Veuillez noter que le {Votre_ID} requis ci-dessous vous sera fourni par votre consultant. **Veuillez les contacter** pour recevoir cet identifiant avant de commencer ce processus.

Pour HRWize : ID de l'entreprise

4. Vous aurez besoin des informations suivantes pour remplir l'étape 1 du formulaire de connexion basé sur SAML:
 - a. Identifiant de l'entité
<https://identity.hrwise.com/saml>
 - b. URL de réponse
<https://identity.hrwise.com/federation/CUSTOMER/signin>
 - c. URL de déconnexion
<https://identity.hrwise.com/federation/CUSTOMER/signout>
 - d. 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 'moorepay-saml' under the 'Saml Provider' section. It includes a 'Name' field with the value 'moorepay-saml'. Below it 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 is a 'Display name' field containing '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 for the 'Moorepay | SAML-based Sign-on' application. It contains several sections:

- Identifier (Entity ID):** A text box with the value 'https://as-mp-dev02-identity-v2-pri.azurewebsites.net/saml'.
- Reply URL (Assertion Consumer Service URL):** A text box with the value 'https://as-mp-dev02-identity-v2-pri.azurewebsites.net/federation/moorepay-saml/signin'.
- Sign on URL (Optional):** A text box with the value 'https://login.hrwise.com/ids.php?idp=moorepay-saml'.
- Relay State (Optional):** A text box with the value 'Enter a relay state'.
- Logout Uri (Optional):** A text box with the value 'https://as-mp-dev02-identity-v2-pri.azurewebsites.net/federation/moorepay-saml/signout'.
- Attributes & Claims:** A table showing attributes like 'givenname', 'surname', 'emailaddress', 'name', and 'Unique User Identifier' with their corresponding user attributes.
- SAML Certificates:** A table showing the 'Tokens signing certificate' with details like 'Status', 'Thumbprint', 'Expiration', 'Notification email', and 'App Federation Metadata Uri'.

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 listing attributes and their corresponding claims, such as 'givenname' mapping to 'user.givenname'.
- SAML Certificates:** This section details the 'Token signing certificate', showing its status as 'Active', a thumbprint, an expiration date, and a notification email. It also displays the 'App Federation Metadata URL' with a 'Copy to clipboard' button. Below this, there are links to download the certificate in Base64, Raw, and Federation Metadata XML formats.
- Verification certificates (optional):** A section for managing optional verification certificates, currently showing zero active certificates.
- Set up Moorepay:** This section provides the necessary URLs for linking the application with Microsoft Entra ID, including the Login URL, Microsoft Entra Identifier, and Logout URL.
- Test single sign-on with Moorepay:** A section at the bottom with a 'Test' button to verify the configuration.

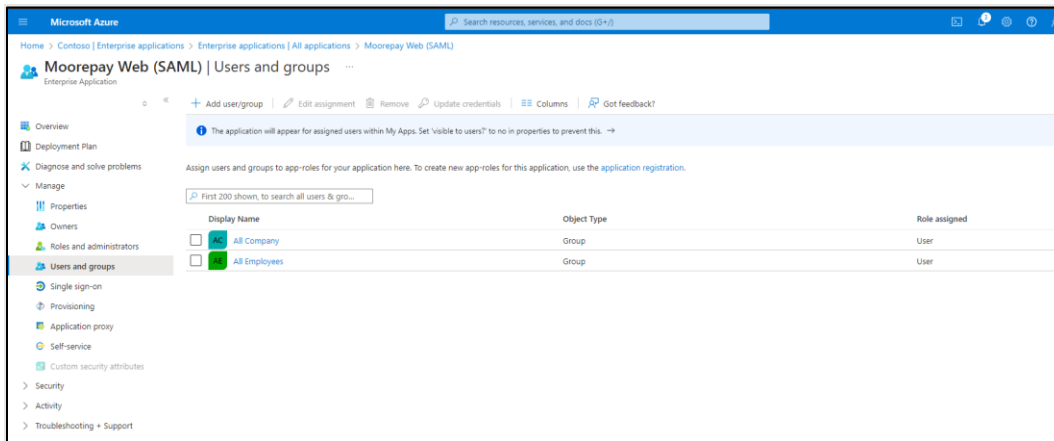
Rendre votre application accessible aux utilisateurs

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 :

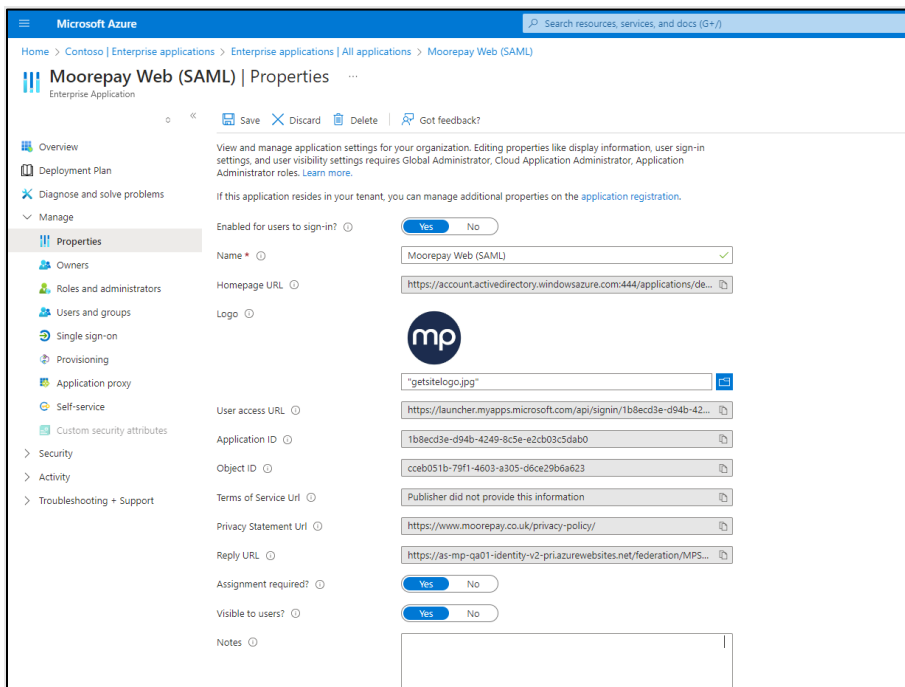
- En fonction de vos politiques, comme le montre la capture d'écran ci-dessous
- Désactivez (non) le champ « *Attribution requise ?* » dans les propriétés de l'application. Cela permettra à tous vos utilisateurs d'y accéder.

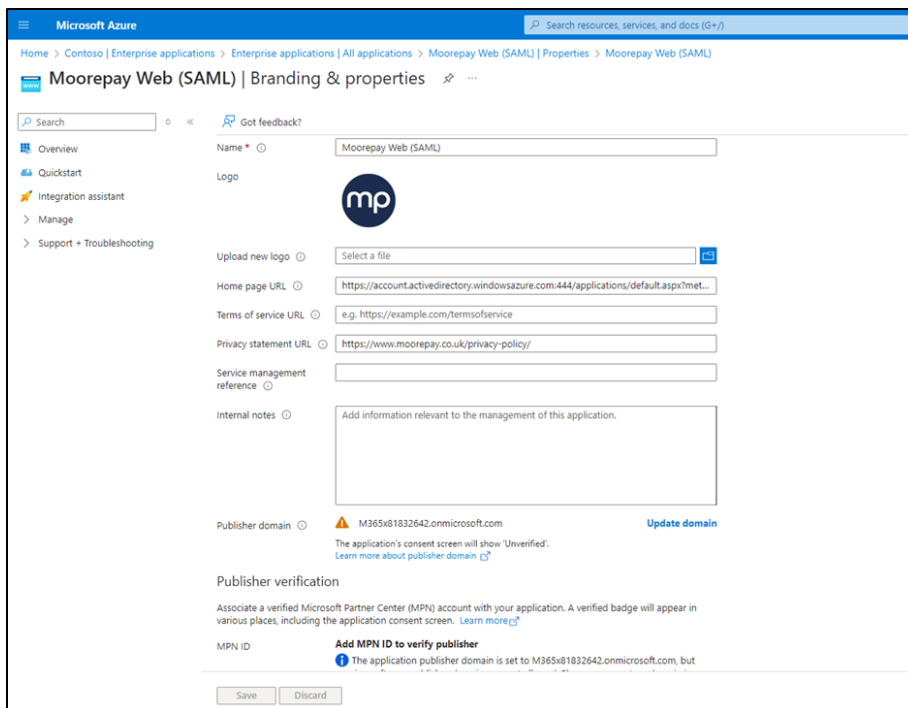
Veillez à enregistrer la méthode utilisée.



Paramètre supplémentaire de l'application

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



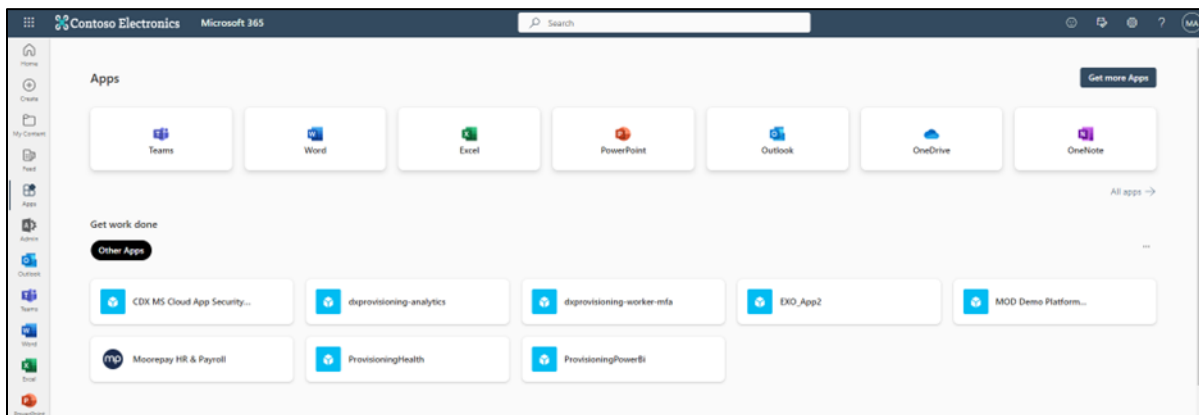


2. D'autres paramètres, tels que la politique de confidentialité/le logo HRWize, peuvent être définis dans l'enregistrement de l'application.

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.