bitwarden | Article du Centre d'Aide

CONSOLE ADMIN > IDENTIFIEZ-VOUS AVEC SSO >

Mise en œuvre de l'ID SAML de Microsoft Entra

Afficher dans le centre d'aide:
https://bitwarden.com/help/saml-microsoft-entra-id/

Mise en œuvre de l'ID SAML de Microsoft Entra

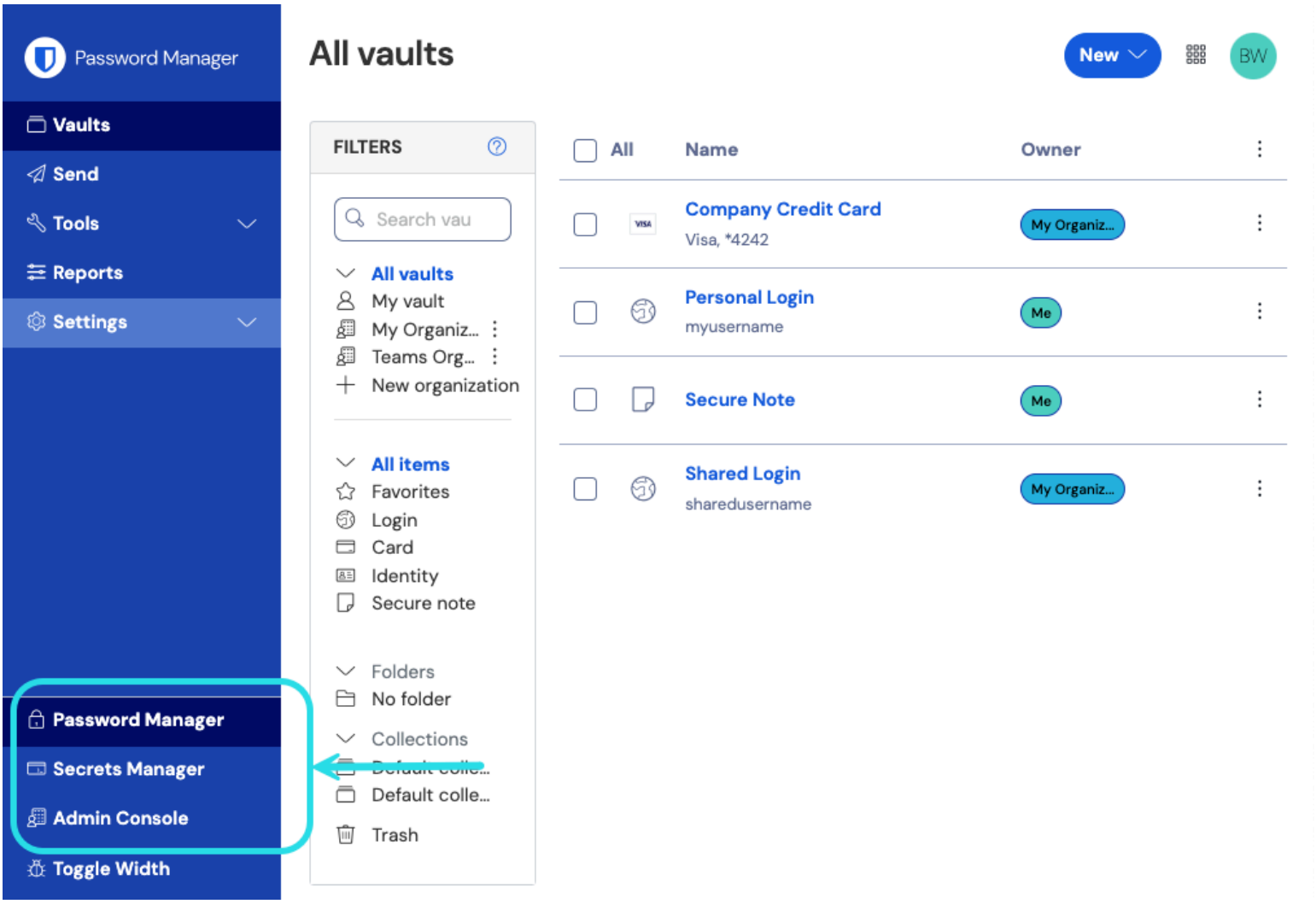
Cet article contient de l'aide **spécifique à Azure** pour configurer l'identifiant avec SSO via SAML 2.0. Pour obtenir de l'aide sur la configuration de l'identifiant avec SSO pour un autre IdP, reportez-vous à Configuration SAML 2.0.

La configuration implique de travailler simultanément avec l'application web Bitwarden et le portail Azure. Au fur et à mesure que vous avancez, nous vous recommandons d'avoir les deux à portée de main et de suivre les étapes dans l'ordre où elles sont documentées.

> **Tip**
>
> **Déjà un expert en SSO ?** Ignorez les instructions de cet article et téléchargez des captures d'écran d'exemples de configurations pour les comparer aux vôtres.
>
> saisir: asset-hyperlink id: 7CKe4TX98FPF86eAimKgak

Ouvrez SSO dans l'application web

Connectez-vous à l'application web Bitwarden et ouvrez la console Admin en utilisant le sélecteur de produit (⊞):



commutateur-de-produit

Ouvrez l'écran **Paramètres → Connexion unique** de votre organisation :

Configuration SAML 2.0

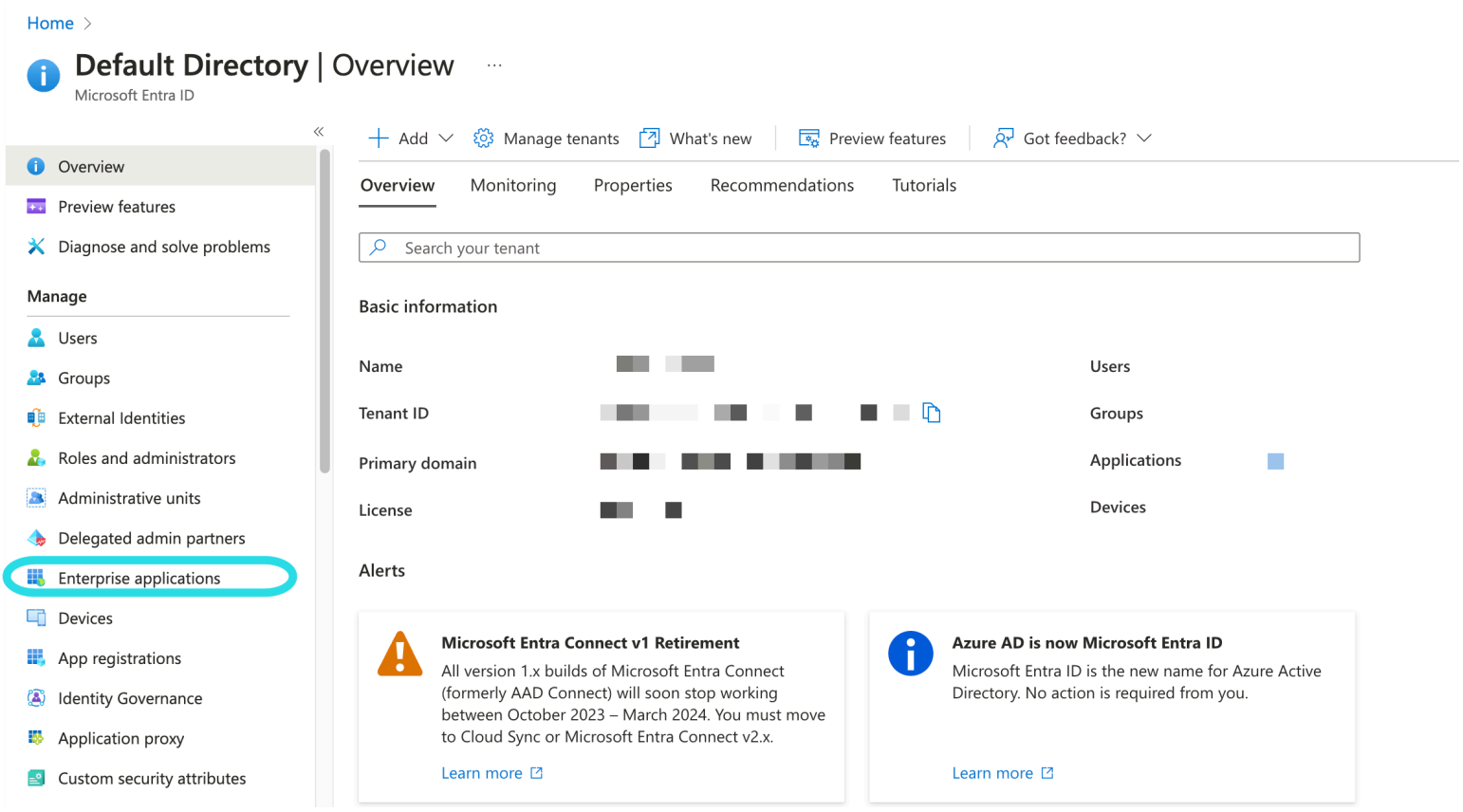
Si vous ne l'avez pas déjà fait, créez un **identifiant SSO** unique pour votre organisation et sélectionnez **SAML** dans le menu déroulant **Saisir**. Gardez cet écran ouvert pour une référence facile.

Vous pouvez désactiver l'option **Définir un ID d'entité SP unique** à ce stade si vous le souhaitez. Ce faisant, cela supprimera votre ID d'organisation de la valeur de votre ID d'entité SP, cependant dans presque tous les cas, il est recommandé de laisser cette option activée.

> **Tip**
>
> Il existe des options alternatives de **décryptage des membres**. Apprenez comment commencer à utiliser SSO avec des appareils de confiance ou Key Connector.

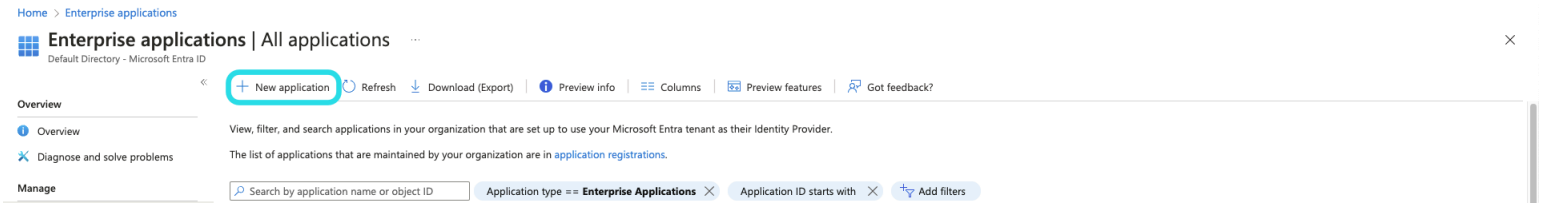
Créez une application d'entreprise

Dans le portail Azure, naviguez jusqu'à **Microsoft Entra ID** et sélectionnez **Applications d'entreprise** dans le menu de navigation :



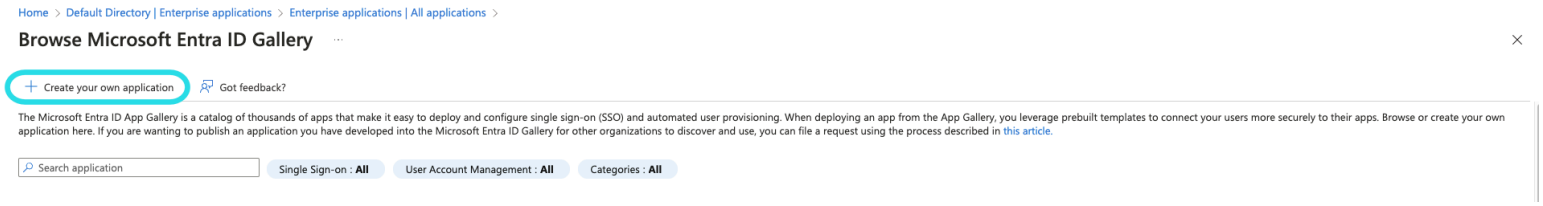
Enterprise applications

Sélectionnez le bouton ＋ **Nouvelle application** :



Create new application

Sur l'écran Parcourir la galerie d'ID Entra de Microsoft, sélectionnez le bouton ＋ **Créez votre propre application** :

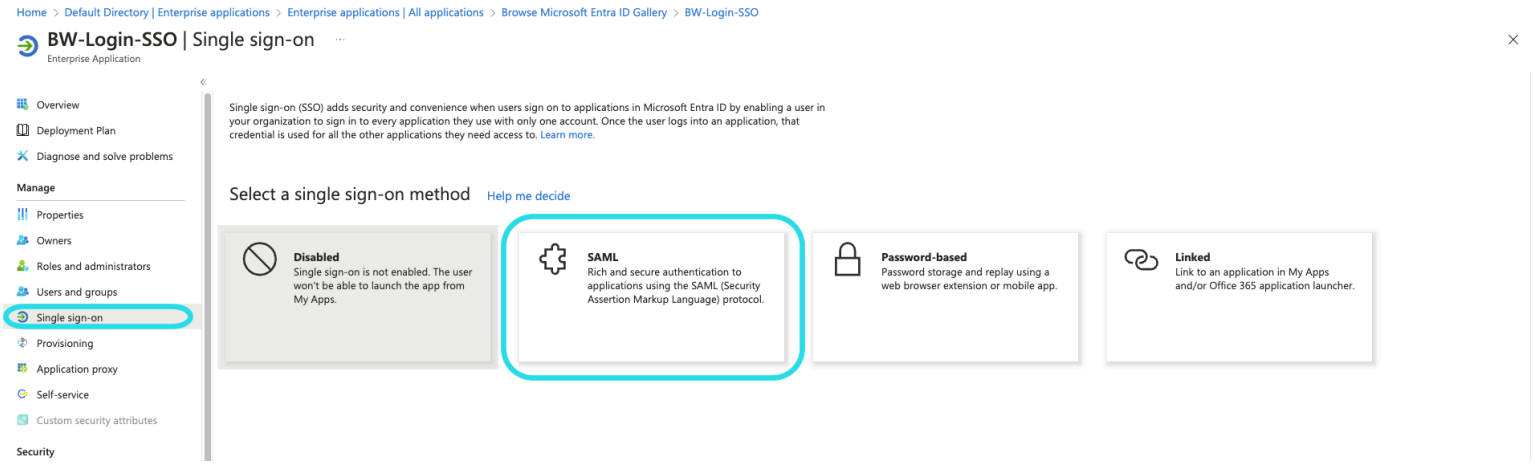


Create your own application

Sur l'écran Créer votre propre application, donnez à l'application un nom unique spécifique à Bitwarden et sélectionnez l'option (Non-galerie). Une fois que vous avez terminé, cliquez sur le bouton **Créer**.

Activer la connexion unique

Depuis l'écran d'aperçu de l'application, sélectionnez **Connexion unique** depuis la navigation :



Configure Single sign-on

Sur l'écran de Single Sign-On, sélectionnez **SAML**.

Configuration SAML

Configuration SAML de base

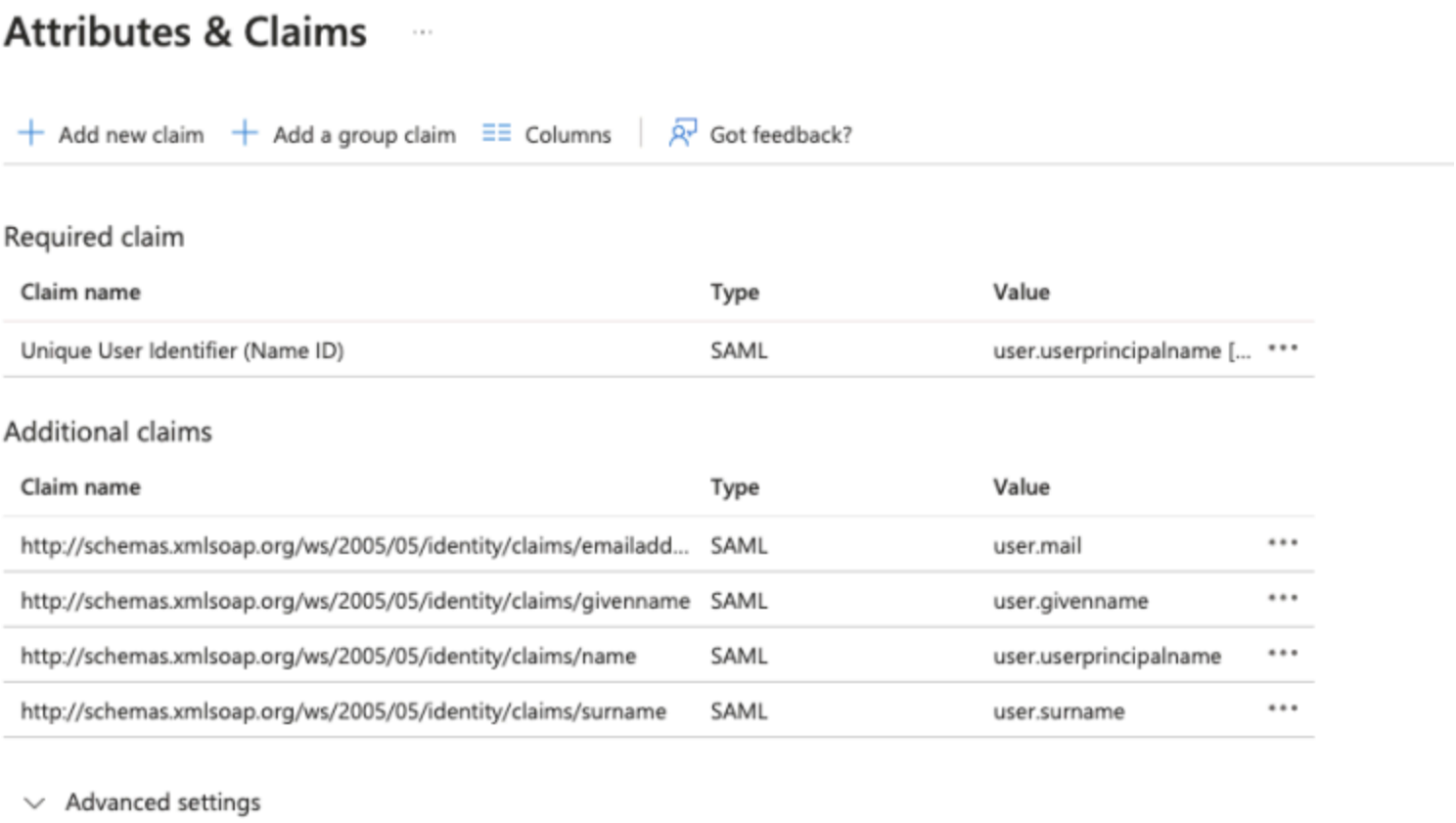
Sélectionnez le bouton **Éditer** et configurez les champs suivants:

Champ	Description
Identifiant (ID d'entité)	Définissez ce champ sur l'**ID d'entité SP** pré-généré. Cette valeur générée automatiquement peut être copiée à partir de l'écran **Paramètres → Connexion unique** de votre organisation et variera en fonction de votre configuration.
URL de réponse (URL du service de consommation d'assertion)	Définissez ce champ sur l'URL du **Service de Consommation d'Assertion (ACS)** pré-généré. Cette valeur générée automatiquement peut être copiée à partir de l'écran **Paramètres → Connexion unique** de l'organisation et variera en fonction de votre configuration.
Se connecter à l'URL	Définissez ce champ sur l'URL d'identifiant à partir de laquelle les utilisateurs accéderont à Bitwarden. Pour les clients hébergés dans le cloud, c'est `https://vault.bitwarden.com/#/sso` ou `https://vault.bitwarden.eu/#/sso`. Pour les instances auto-hébergées, cela est déterminé par vous URL de serveur configuré, par exemple `https://votre-domaine.com/#/sso`.

Attributs de l'utilisateur & revendications

Les revendications par défaut construites par Azure fonctionneront avec l'identifiant avec SSO, cependant vous pouvez optionnellement utiliser cette section pour configurer le format NameID utilisé par Azure dans les réponses SAML.

Sélectionnez le bouton **Éditer** et sélectionnez l'entrée **Identifiant Utilisateur Unique (Nom ID)** pour éditer la revendication de NomID :



Éditer l'identifiant de revendication de nom

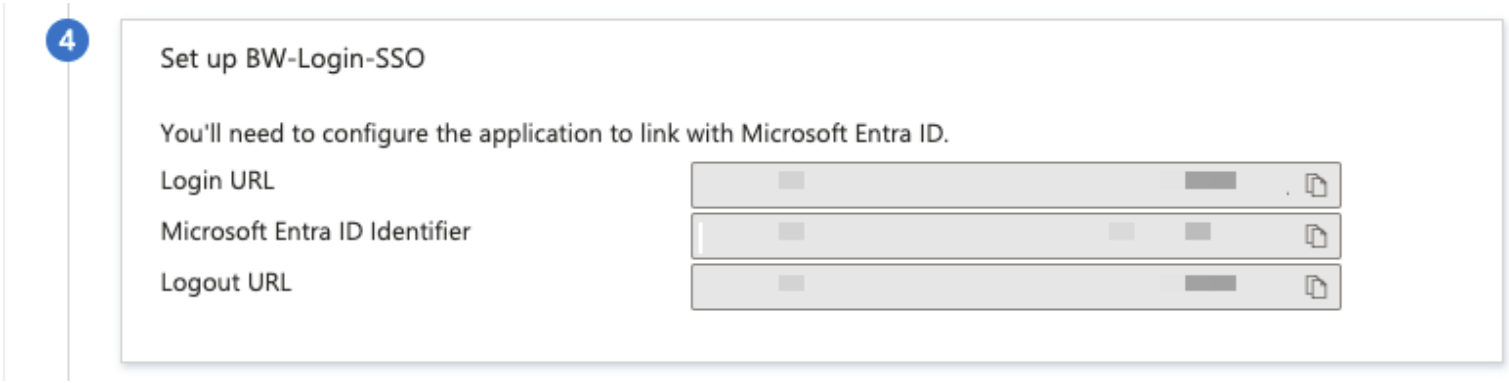
Les options incluent Par défaut, Adresse de courriel, Persistant, Non spécifié, et Nom de domaine qualifié Windows. Pour plus d'informations, reportez-vous à la documentation Microsoft Azure.

Certificat de signature SAML

Téléchargez le Certificat Base64 pour utilisation lors d'une étape ultérieure.

Configurez votre application

Copiez ou prenez note de l'**URL de l'identifiant** et de l'**Identifiant Entra ID de Microsoft** dans cette section pour utilisation lors d'une étape ultérieure :

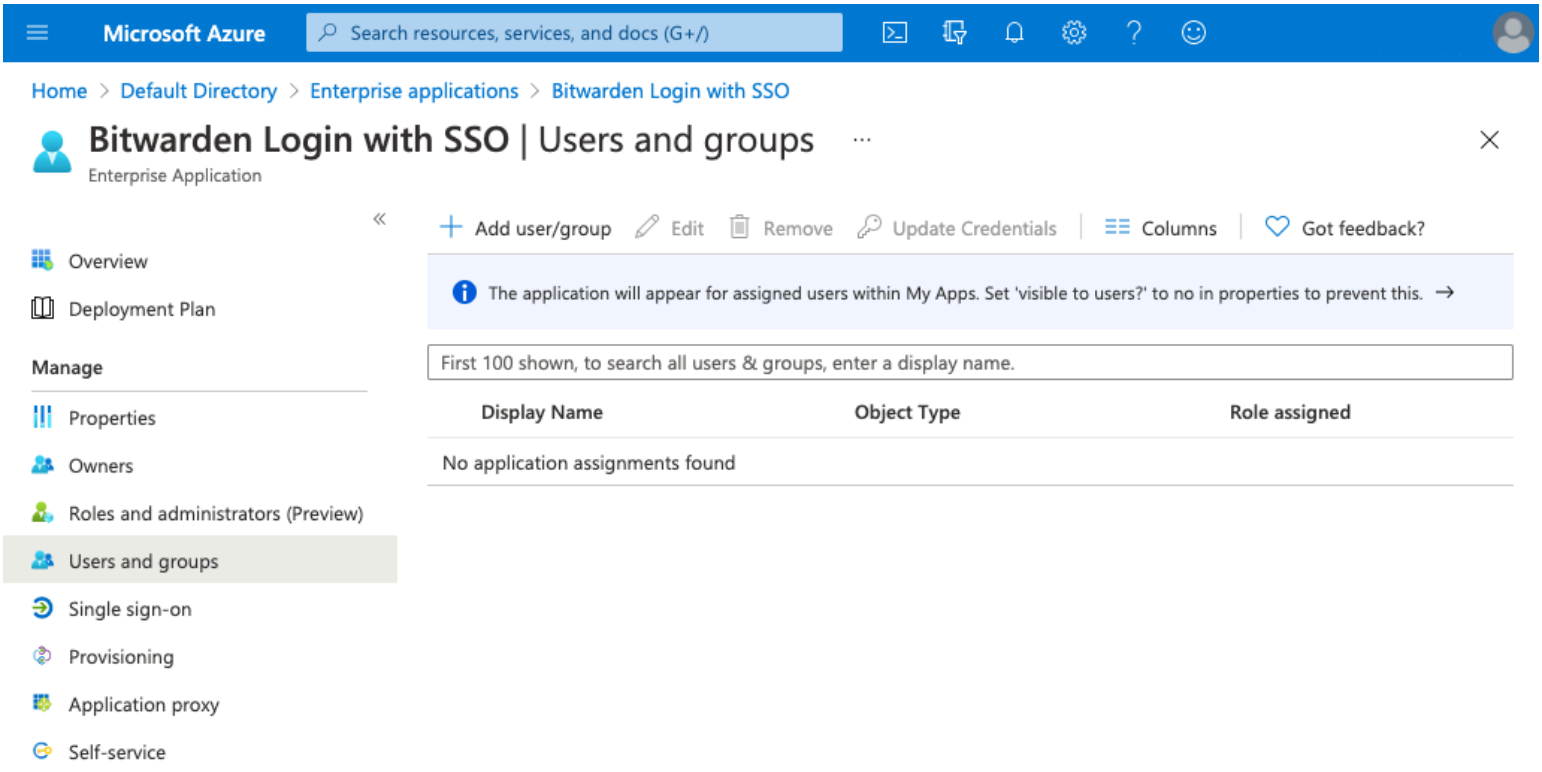


Azure URLs

> **Note**
> If you receive any key errors when logging in via SSO, try copying the X509 certificate information from the Federation Metadata XML file instead.

Utilisateurs et groupes

Sélectionnez **Utilisateurs et groupes** dans la navigation:



Assign users or groups

Sélectionnez le bouton **Ajouter utilisateur/groupe** pour attribuer l'accès à l'identifiant avec l'application SSO à un utilisateur ou à un niveau de groupe.

Retour à l'application web

À ce stade, vous avez configuré tout ce dont vous avez besoin dans le contexte du Portail Azure. Retournez à l'application web Bitwarden pour terminer la configuration.

L'écran de connexion unique sépare la configuration en deux sections :

- **La configuration du fournisseur de services SAML** déterminera le format des requêtes SAML.
- **La configuration du fournisseur d'identité SAML** déterminera le format attendu pour les réponses SAML.

Configuration du fournisseur de services

Configurez les champs suivants :

Champ	Description
Format d'identifiant de nom	Par défaut, Azure utilisera l'adresse de courriel. Si vous avez modifié ce paramètre, sélectionnez la valeur correspondante. Sinon, définissez ce champ sur **Non spécifié** ou **Adresse de courriel**.
Algorithme de Signature Sortant	L'algorithme que Bitwarden utilisera pour signer les requêtes SAML.
Comportement de signature	Si/quand les demandes SAML seront signées.
Algorithme de Signature Minimum Entrant	Par défaut, Azure signera avec RSA SHA-256. Sélectionnez `rsa-sha256` dans le menu déroulant.
Vouloir des Assertions Signées	Que Bitwarden s'attend à ce que les assertions SAML soient signées.
Valider les Certificats	Cochez cette case lorsque vous utilisez des certificats fiables et valides de votre IdP via une CA de confiance. Les certificats auto-signés peuvent échouer à moins que des chaînes de confiance appropriées ne soient configurées avec l'image Docker de l'identifiant Bitwarden avec SSO.

Lorsque vous avez terminé avec la configuration du fournisseur de services, **Enregistrez** votre travail.

Configuration du fournisseur d'Identité

La configuration du fournisseur d'Identité vous demandera souvent de vous référer à nouveau au Portail Azure pour récupérer les valeurs de l'application :

Champ	Description
ID de l'entité	Entrez votre **Identifiant Microsoft Entra ID**, récupéré depuis la section Configurez votre application du portail Azure. Ce champ est sensible à la casse.
Type de Reliure	Définir sur **HTTP POST** ou **Redirection**.
URL du service de connexion unique	Entrez votre **URL d'identifiant**, récupérée depuis la section Configurez votre application du Portail Azure.
URL du service de déconnexion unique	La connexion avec SSO ne prend actuellement **pas** en charge SLO. Cette option est prévue pour un développement futur, cependant vous pouvez la préconfigurer avec votre **URL de déconnexion** si vous le souhaitez.

Certificat Public X509	Collez le certificat téléchargé, en supprimant
	`-----DÉBUT DU CERTIFICAT-----`
	et
	`-----FIN DU CERTIFICAT-----`
	La valeur du certificat est sensible à la casse, les espaces supplémentaires, les retours à la ligne et autres caractères superflus **entraîneront l'échec de la validation du certificat**.

Algorithme de Signature Sortant	Par défaut, Azure signera avec RSA SHA-256. Sélectionnez `rsa-sha256` dans le menu déroulant.
Désactiver les demandes de déconnexion sortantes	La connexion avec SSO ne prend actuellement **pas** en charge SLO. Cette option est prévue pour un développement futur.
Voulez-vous que les demandes d'authentification soient signées	Que Azure s'attend à ce que les demandes SAML soient signées.

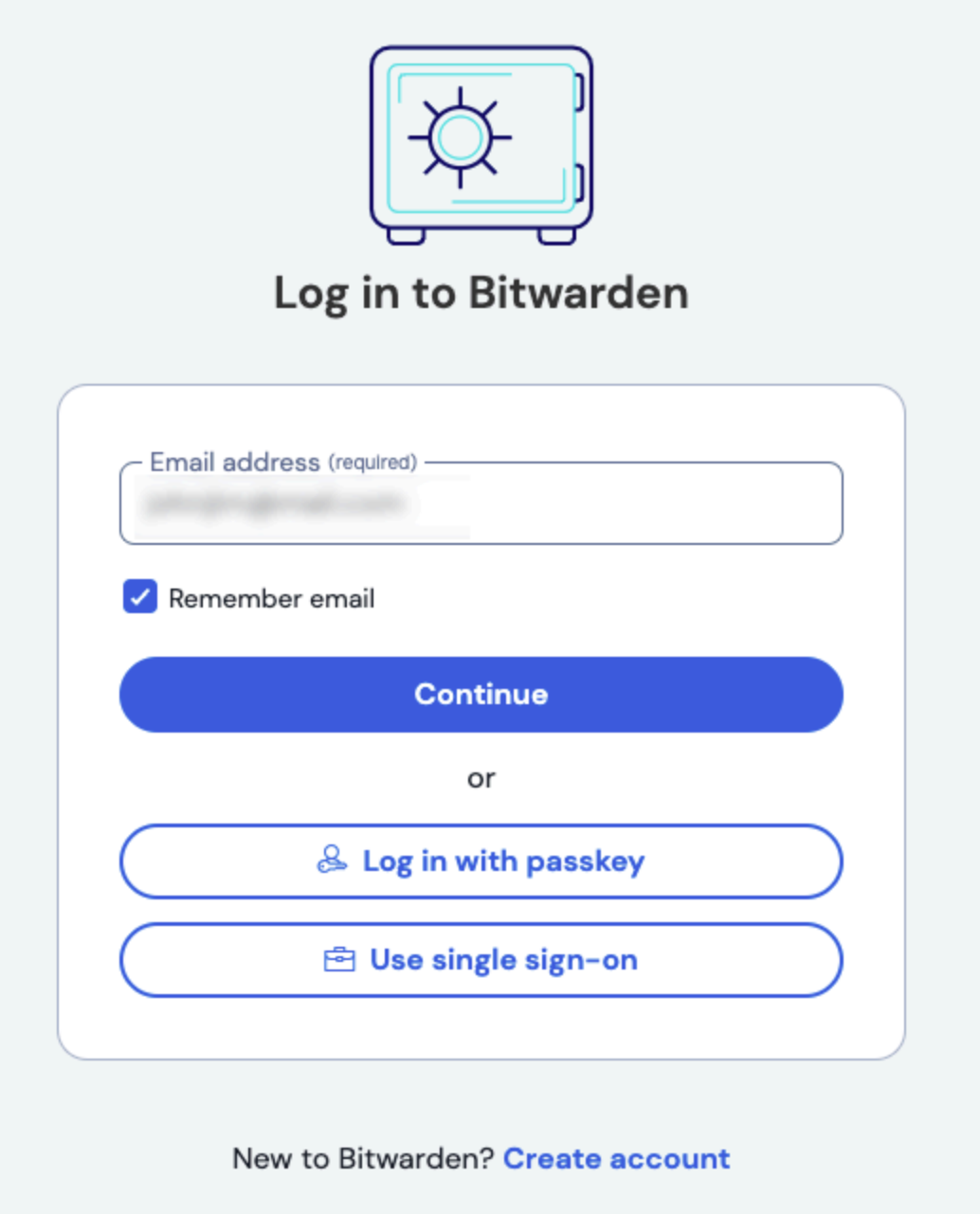
> **Note**
>
> Lors de la complétion du certificat X509, prenez note de la date d'expiration. Les certificats devront être renouvelés afin d'éviter toute interruption de service pour les utilisateurs finaux de SSO. Si un certificat a expiré, les comptes Admin et Propriétaire pourront toujours se connecter avec l'adresse de courriel et le mot de passe principal.

Lorsque vous avez terminé avec la configuration du fournisseur d'identité, **Enregistrez** votre travail.

> **Tip**
>
> Vous pouvez exiger que les utilisateurs se connectent avec SSO en activant la politique d'authentification à connexion unique. Veuillez noter que cela nécessitera également l'activation de la politique de sécurité de l'organisation unique. En savoir plus.

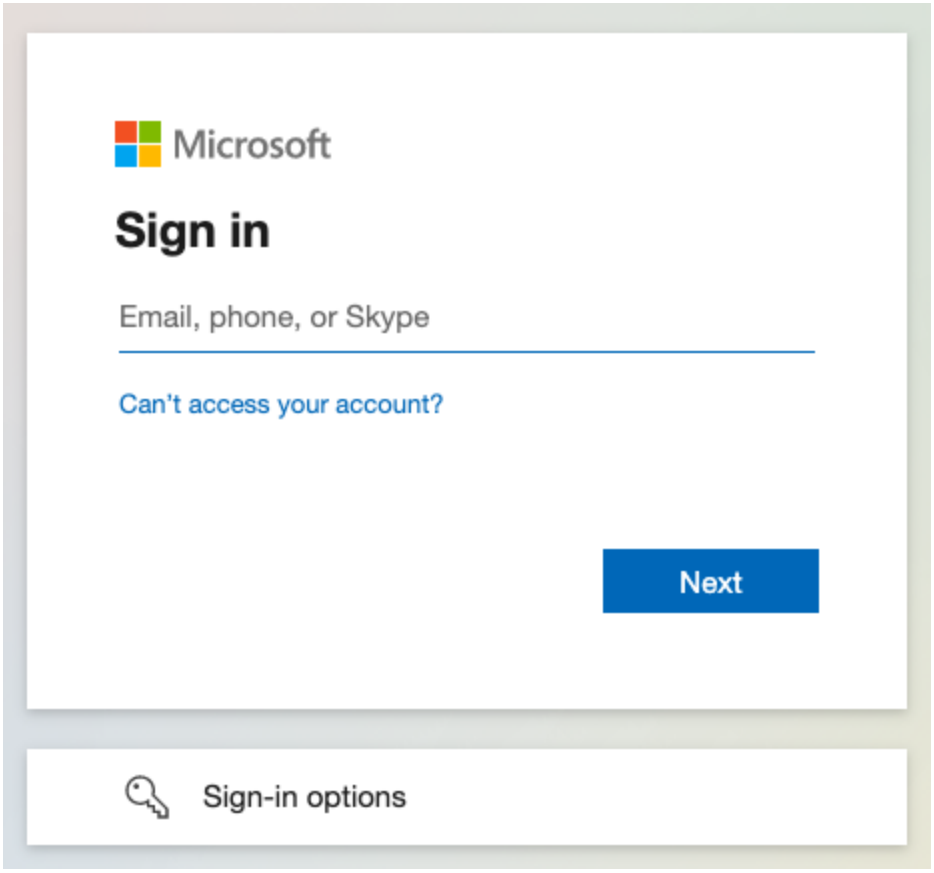
Testez la configuration

Une fois votre configuration terminée, testez-la en vous rendant sur https://vault.bitwarden.com, en entrant votre adresse de courriel, en sélectionnant **Continuer**, et en sélectionnant le bouton **Connexion unique d'Entreprise** :



Connexion unique d'entreprise et mot de passe principal

Entrez l'identifiant de l'organisation configuré et sélectionnez **Se connecter**. Si votre mise en œuvre est correctement configurée, vous serez redirigé vers l'écran d'identifiant Microsoft :



Azure login screen

Après vous être authentifié avec vos identifiants Azure, entrez votre mot de passe principal Bitwarden pour déchiffrer votre coffre !

Note

Bitwarden ne prend pas en charge les réponses non sollicitées, donc l'initiation de l'identifiant à partir de votre IdP entraînera une erreur. Le flux d'identifiant SSO doit être initié à partir de Bitwarden. Les administrateurs SAML Azure peuvent configurer une Inscription d'application pour que les utilisateurs soient dirigés vers la page d'identifiant du coffre web Bitwarden.

1. Désactivez le bouton Bitwarden existant dans la page **Toutes les Applications** en naviguant vers l'application Bitwarden Entreprise actuelle et en sélectionnant les propriétés et réglez l'option **Visible pour les utilisateurs** sur **Non**.

2. Créez l'enregistrement de l'application en naviguant vers **Enregistrements d'application** et en sélectionnant **Nouvel enregistrement**.

3. Fournissez un nom pour l'application comme **Bitwarden SSO**. Ne spécifiez pas une URL de redirection. Sélectionnez **S'inscrire** pour compléter le forum.

4. Une fois l'application créée, naviguez vers **Marque & Propriétés** situé dans le menu de navigation.

5. Ajoutez les paramètres suivants à l'application :

    1. Téléversez un logo pour la reconnaissance de l'utilisateur final. Vous pouvez récupérer le logo Bitwarden ici.

    2. Définissez l'**URL de la page d'accueil** sur votre page d'identifiant client Bitwarden telle que `https://vault.bitwarden.com/#/login` ou `votre-URL-auto-hébergée.com`.

Une fois ce processus terminé, les utilisateurs assignés auront une application Bitwarden qui les liera directement à la page d'identifiant du coffre web Bitwarden.