bitwarden | Article du Centre d'Aide

CONSOLE ADMIN > IDENTIFIEZ-VOUS AVEC SSO >

Mise en œuvre de Microsoft Entra ID OIDC

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

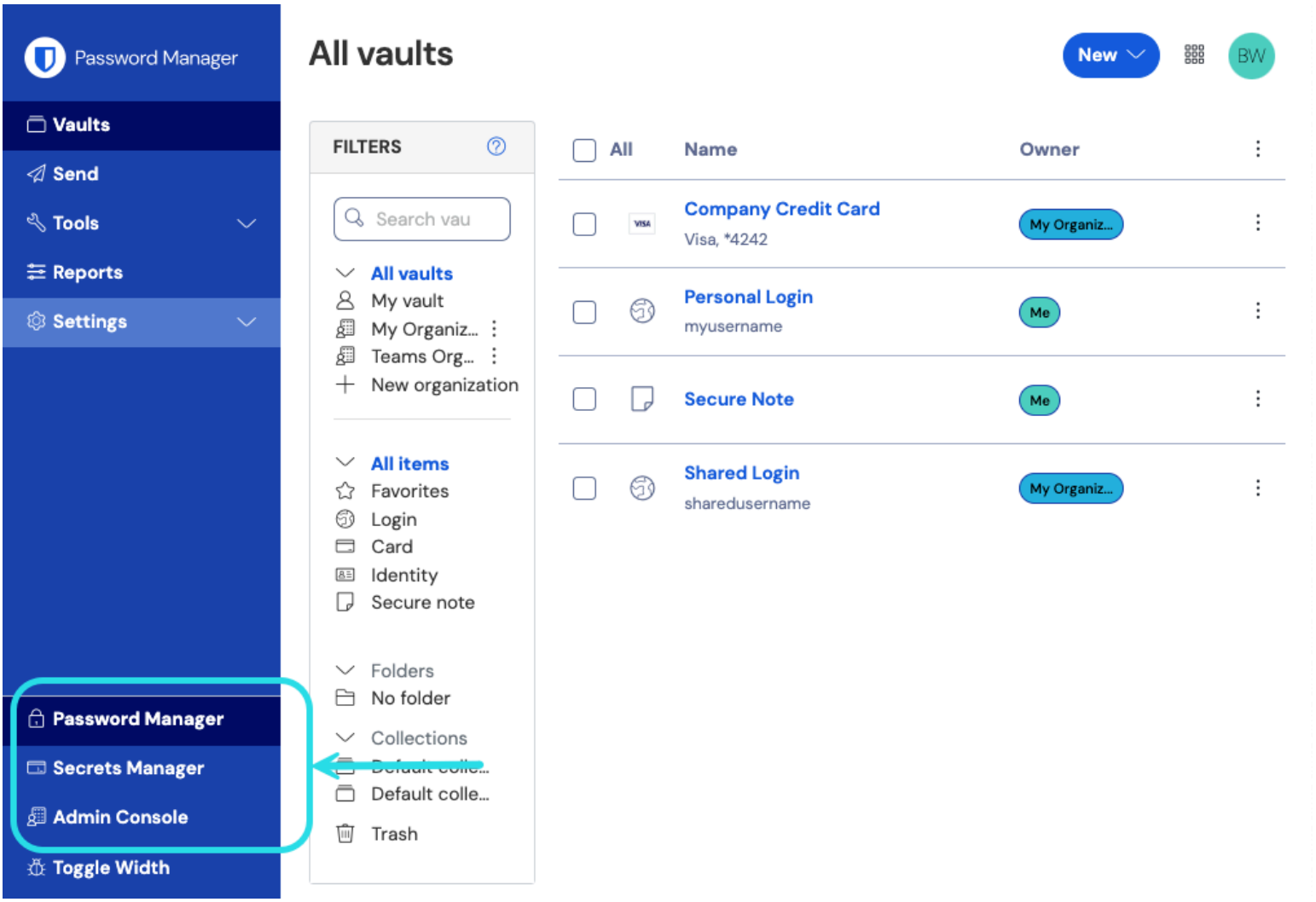
Mise en œuvre de Microsoft Entra ID OIDC

Cet article contient de l'aide **spécifique à Azure** pour configurer l'identifiant avec SSO via OpenID Connect (OIDC). Pour obtenir de l'aide pour configurer l'identifiant avec SSO pour un autre IdP OIDC, ou pour configurer Microsoft Entra ID via SAML 2.0, voir Configuration OIDC ou Implémentation SAML de Microsoft Entra ID.

La configuration implique de travailler simultanément dans 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 compléter les étapes dans l'ordre où elles sont documentées.

Ouvrez SSO dans le coffre web

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



commutateur-de-produit

Sélectionnez **Paramètres → Connexion unique** depuis la navigation :

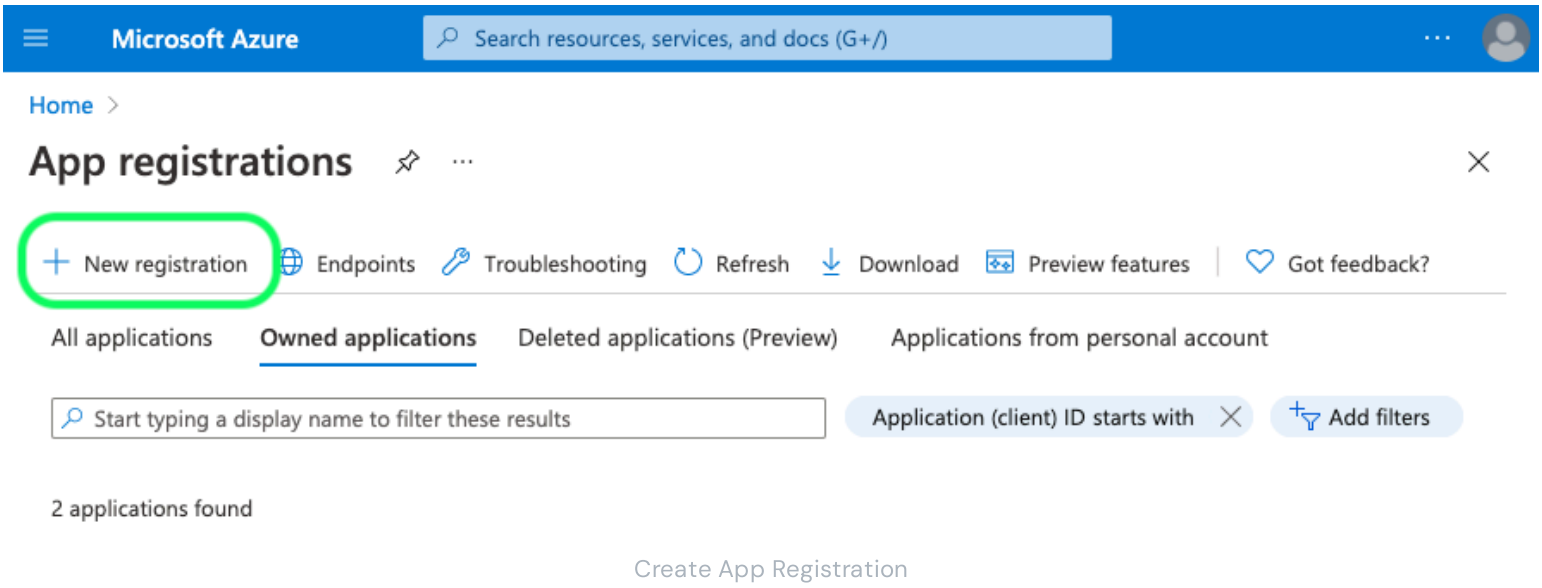
Configuration OIDC

Si vous ne l'avez pas déjà fait, créez un **identifiant SSO** unique pour votre organisation. Sinon, vous n'avez pas besoin d'éditer quoi que ce soit sur cet écran pour l'instant, mais gardez-le ouvert pour une référence facile.

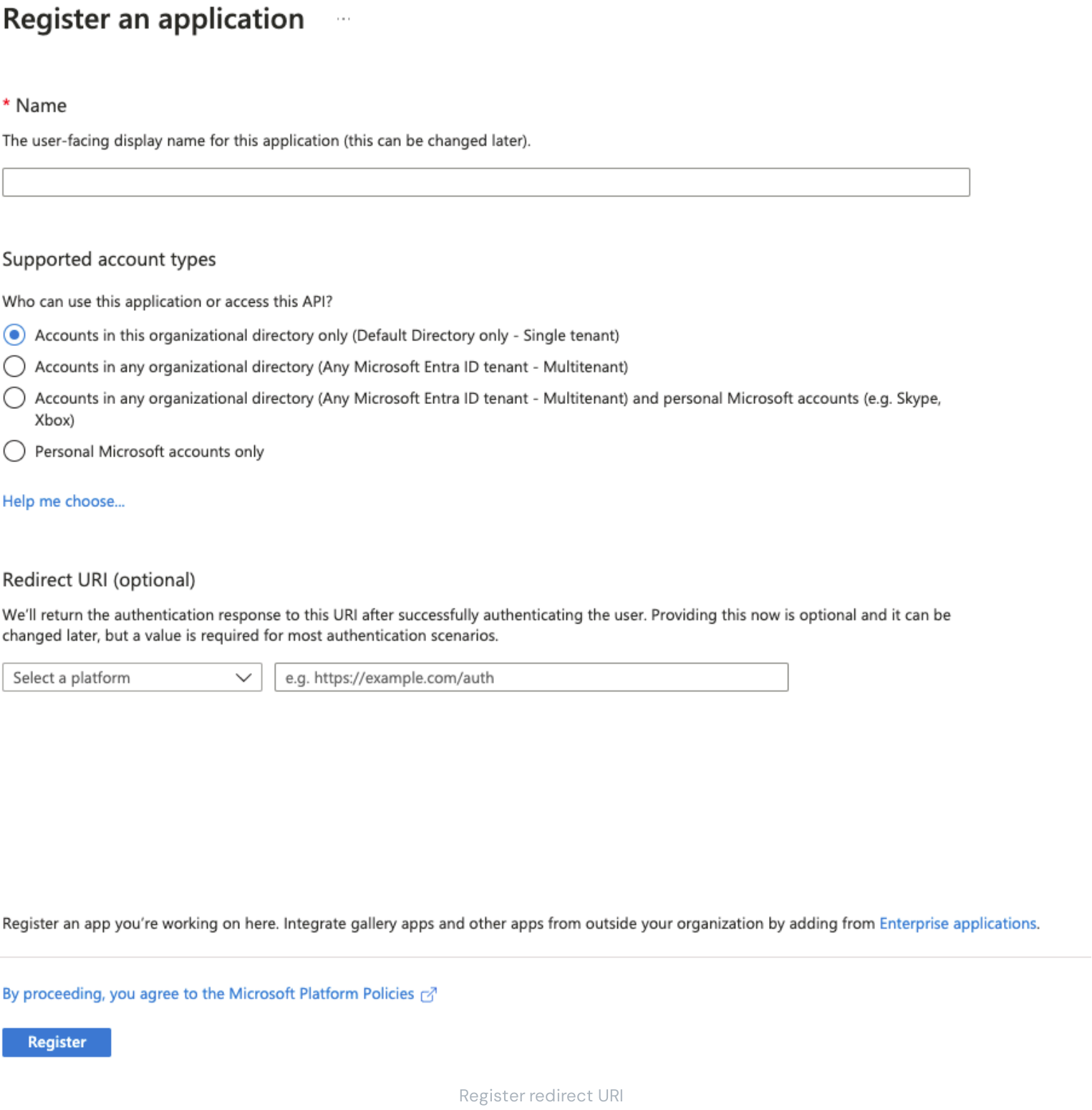
> **Tip**
>
> Il existe des options alternatives de **décryptage des membres**. Apprenez comment commencer à utiliser SSO avec des appareils de confiance ou Key Connector.

Créez une inscription d'application

Dans le portail Azure, naviguez jusqu'à **Microsoft Entra ID** et sélectionnez **Enregistrements d'application.** Pour créer une nouvelle inscription d'application, sélectionnez le bouton **Nouvelle inscription** :



Complétez les champs suivants :



1. Sur l'écran **Enregistrer une application**, donnez à votre application un nom spécifique à Bitwarden et spécifiez quels comptes devraient pouvoir utiliser l'application. Cette sélection déterminera quels utilisateurs peuvent utiliser l'identifiant Bitwarden avec SSO.

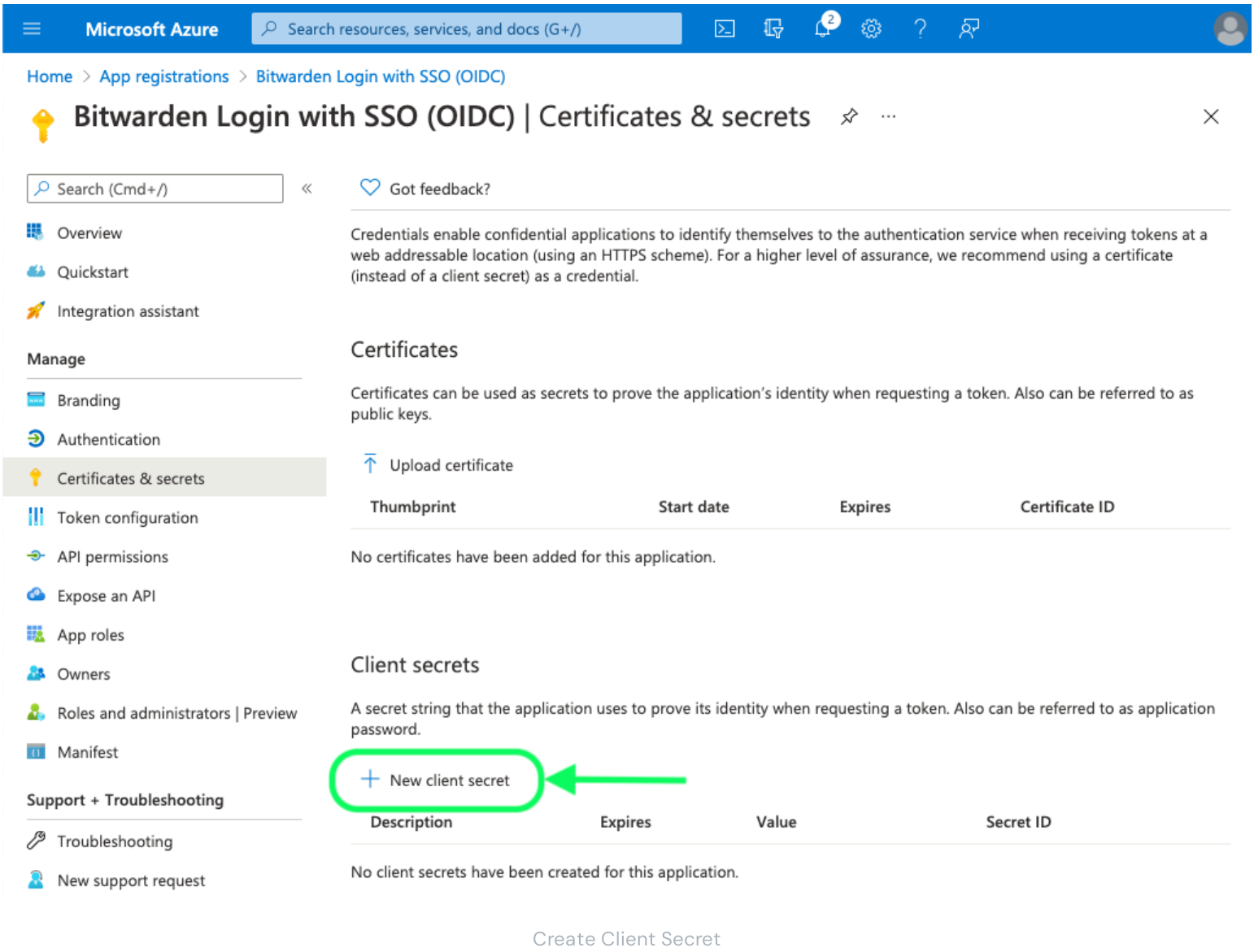
2. Sélectionnez **Authentification** dans la navigation et sélectionnez le bouton **Ajouter une plateforme**.

3. Sélectionnez l'option **Web** sur l'écran de configuration des plateformes et entrez votre **Chemin de Rappel** dans l'entrée des URI de redirection.

> **Note**
>
> Callback Path can be retrieved from the Bitwarden SSO Configuration screen. For cloud-hosted customers, this is `https://sso.bitwarden.com/oidc-signin` or `https://sso.bitwarden.eu/oidc-signin`. For self-hosted instances, this is determined by your configured server URL, for example `https://your.domain.com/sso/oidc-signin`.

Créez un secret de client

Sélectionnez **Certificats & secrets** dans la navigation, et sélectionnez le bouton **Nouveau secret de client** :



Donnez au certificat un nom spécifique à Bitwarden et choisissez une durée d'expiration.

Créer un consentement admin

Sélectionnez **les autorisations API** et cliquez sur ✓ **Accorder l'autorisation admin pour le répertoire par défaut**. La seule autorisation nécessaire est ajoutée par défaut, Microsoft Graph > User.Read.

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 configurer les champs suivants :

Champ	Description
Autorité	Entrez `https://login.microsoft.com//v2.0`, où `TENANT_ID` est la valeur de **l'ID de l'annuaire (locataire)** récupérée sur l'écran d'aperçu de l'enregistrement de l'application.
Client ID	Entrez l'ID de l'application **(client)** de l'enregistrement de l'application, qui peut être récupéré à partir de l'écran d'aperçu.
Secret du Client	Entrez la **Valeur Secrète** du secret de client créé.
Adresse des métadonnées	Pour les mises en œuvre Azure comme documenté, vous pouvez laisser ce champ vide.
Comportement de redirection OIDC	Sélectionnez soit **Form POST** soit **Redirect GET**.
Obtenir des revendications à partir du point de terminaison des informations de l'utilisateur	Activez cette option si vous recevez des erreurs d'URL trop longues (HTTP 414), des URLS tronquées, et/ou des échecs lors de l'SSO.
Scopes supplémentaires/personnalisés	Définissez des portées personnalisées à ajouter à la demande (séparées par des virgules).
Types de revendications d'ID utilisateur supplémentaires/personnalisés	Définissez des clés de type de revendication personnalisées pour l'identification de l'utilisateur (délimitées par des virgules). Lorsqu'ils sont définis, les types de revendications personnalisés sont recherchés avant de revenir sur les types standard.

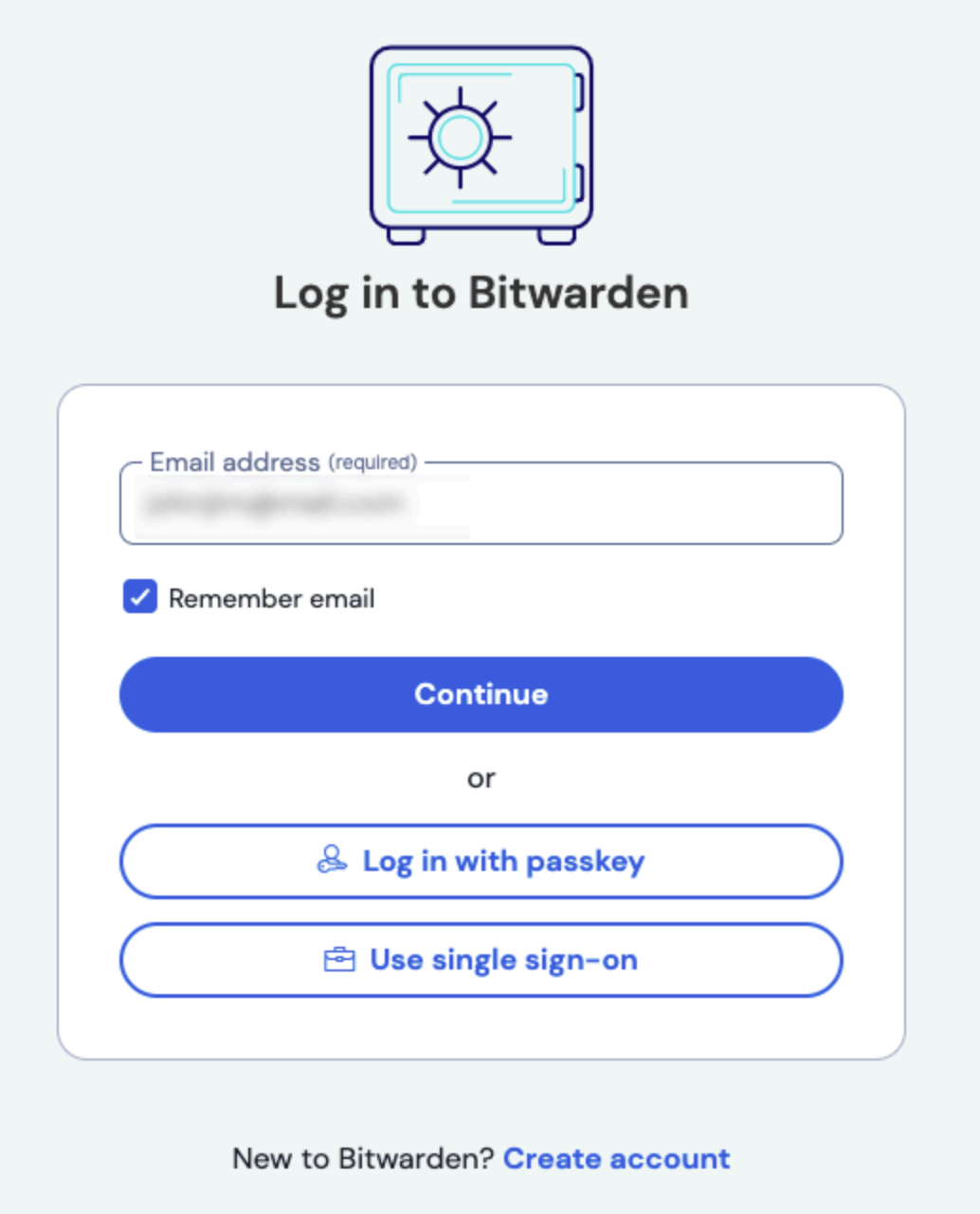
Champ	Description
Types de revendications de courriel supplémentaires/personnalisés	Définissez des clés de type de revendication personnalisées pour les adresses de courriel des utilisateurs (délimitées par des virgules). Lorsqu'ils sont définis, les types de revendications personnalisés sont recherchés avant de revenir sur les types standard.
Types de revendications de noms supplémentaires/personnalisés	Définissez des clés de type de revendication personnalisées pour les noms complets ou les noms d'affichage des utilisateurs (délimités par des virgules). Lorsqu'ils sont définis, les types de revendications personnalisés sont recherchés avant de se rabattre sur les types standard.
Valeurs de référence de la classe de contexte d'authentification demandée	Définissez les identifiants de référence de classe de contexte d'authentification (`acr_values`) (séparés par des espaces). Listez `acr_values` dans l'ordre de préférence.
Valeur de revendication "acr" attendue en réponse	Définissez la valeur de revendication `acr` que Bitwarden doit attendre et valider dans la réponse.

Lorsque vous avez terminé de configurer ces champs, **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.

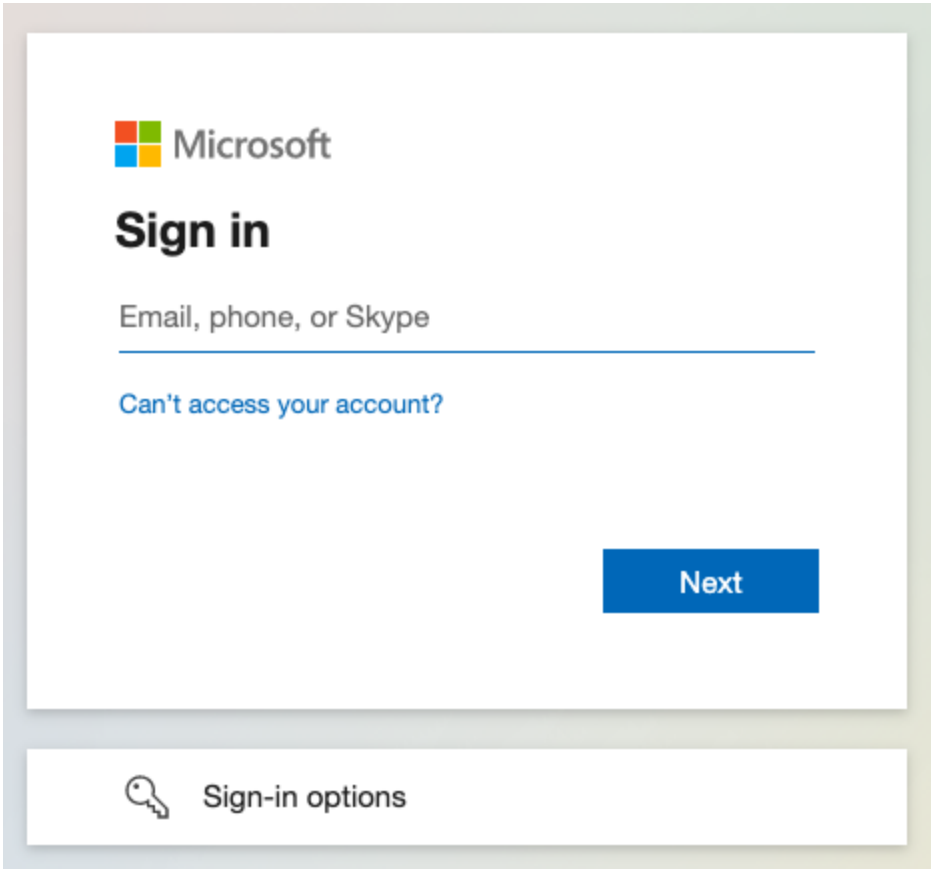
Testez la configuration

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.

Prochaines étapes

1. Éduquez les membres de votre organisation sur comment utiliser l'identifiant avec SSO.