bitwarden | Article du Centre d'Aide

CONSOLE ADMIN > IDENTIFIEZ-VOUS AVEC SSO

Configuration OIDC

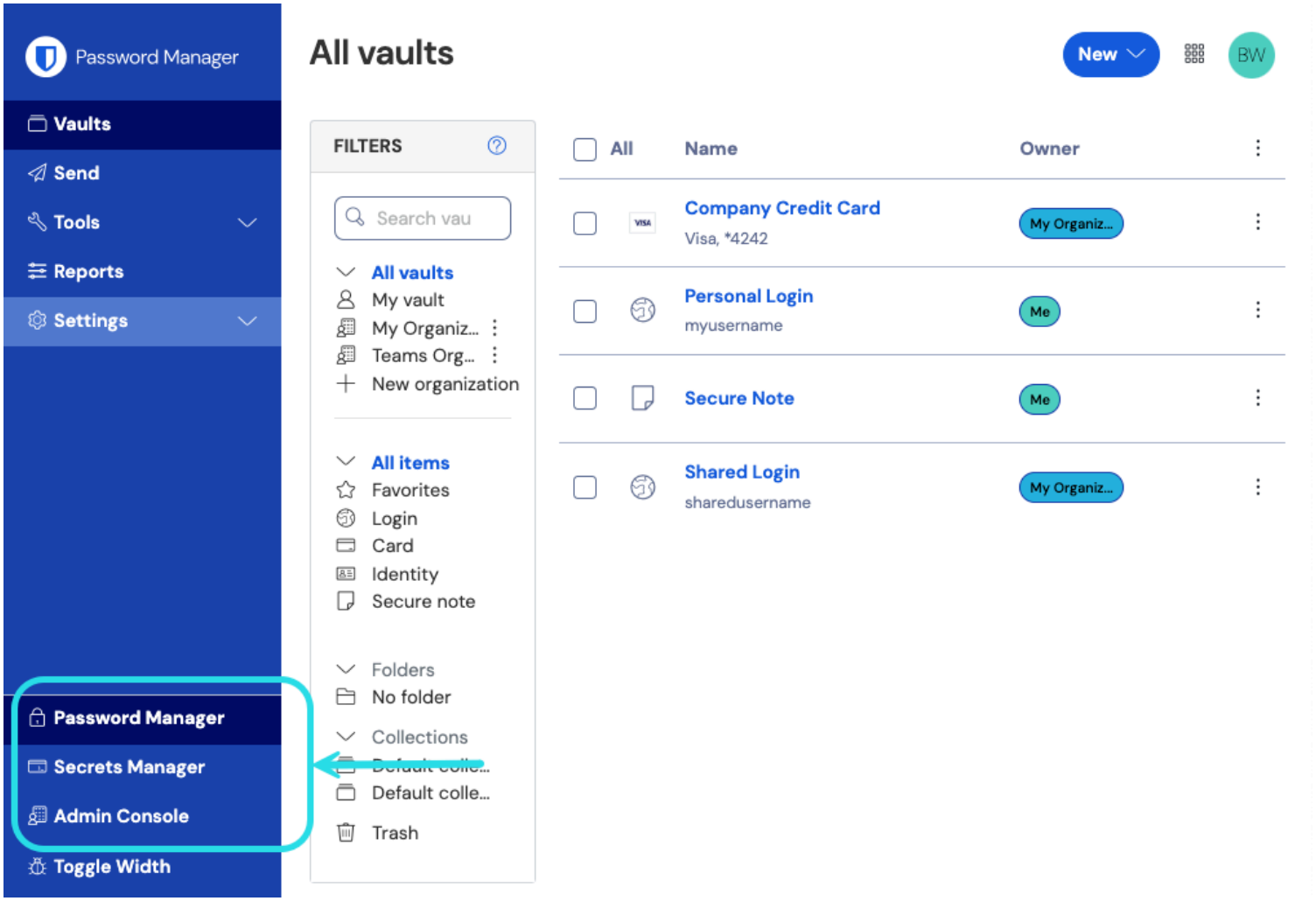
Afficher dans le centre d'aide:
https://bitwarden.com/help/configure-sso-oidc/

Configuration OIDC

Étape 1: Définir un identifiant SSO

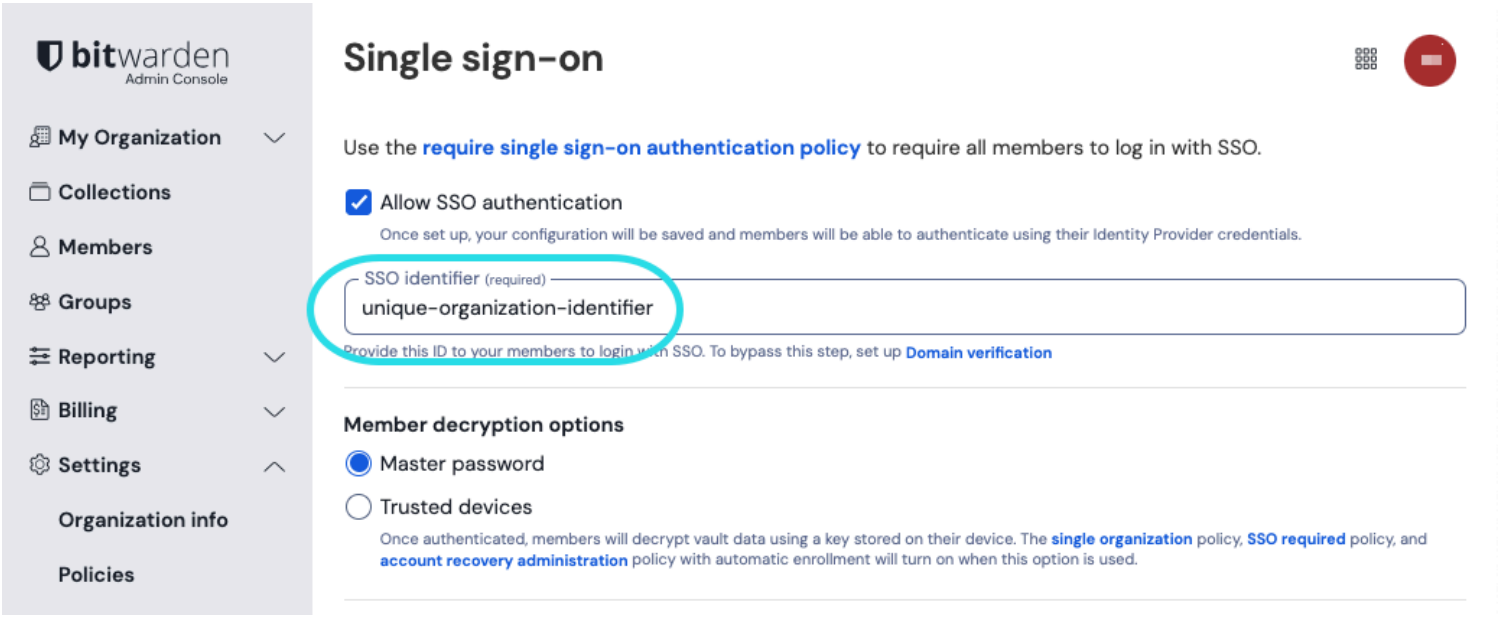
Les utilisateurs qui authentifient leur identité en utilisant SSO devront entrer un **identifiant SSO** qui indique l'organisation (et donc, l'intégration SSO) à authentifier. Pour définir un identifiant SSO unique :

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



commutateur-de-produit

2. Naviguez vers **Paramètres** → **Authentification unique**, et entrez un **Identifiant SSO** unique pour votre organisation :



Entrez un identifiant

3. Passez à **Étape 2: Activer l'identifiant avec SSO**.

> **Tip**
> You will need to share this value with users once the configuration is ready to be used.

Étape 2 : Activer l'identifiant avec SSO

Une fois que vous avez votre identifiant SSO, vous pouvez procéder à l'activation et à la configuration de votre intégration. Pour activer l'identifiant avec SSO :

1. Sur la vue **Paramètres** → **Authentification unique**, cochez la case **Autoriser l'authentification SSO** :

Configuration OIDC

2. Dans le menu déroulant **Saisir**, sélectionnez l'option **OpenID Connect**. Si vous prévoyez d'utiliser SAML à la place, basculez vers le guide de configuration SAML.

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

Étape 3 : Configuration

À partir de ce point, la mise en œuvre variera d'un fournisseur à l'autre. Sautez à l'un de nos **guides d'implémentation** spécifiques pour obtenir de l'aide pour terminer le processus de configuration :

Fournisseur	Guide
Azur	Guide de mise en œuvre Azure

Fournisseur	Guide
Okta	Guide de mise en œuvre Okta

Matériaux de référence de configuration

Les sections suivantes définiront les champs disponibles lors de la configuration de la connexion unique, indépendamment de l'IdP avec lequel vous intégrez. Les champs qui doivent être configurés seront marqués (**obligatoire**).

> **Tip**
>
> **Unless you are comfortable with OpenID Connect**, we recommend using one of the above implementation guides instead of the following generic material.

Champ	Description
Chemin de rappel	(**Généré automatiquement**) L'URL pour la redirection automatique d'authentification. Pour les clients hébergés dans le cloud, c'est `https://sso.bitwarden.com/oidc-signin` ou `https://sso.bitwarden.eu/oidc-signin`. Pour les instances auto-hébergées, cela est déterminé par votre URL de serveur configurée, par exemple `https://votre.domaine.com/sso/oidc-signin`.
Chemin de Rappel de Déconnexion	(**Généré automatiquement**) L'URL pour la redirection automatique de déconnexion. Pour les clients hébergés dans le cloud, c'est `https://sso.bitwarden.com/oidc-signedout` ou `https://sso.bitwarden.eu/oidc-signedout`. Pour les instances auto-hébergées, cela est déterminé par votre URL de serveur configurée, par exemple `https://votre.domaine.com/sso/oidc-signedout`.
Autorité	(**Requis**) L'URL de votre serveur d'autorisation ("Autorité"), contre lequel Bitwarden effectuera l'authentification. Par exemple, `https://your.domain.okta.com/oauth2/default` ou `https://login.microsoft.com//v2.0`.
Client ID	(Un **requis**) Un identifiant pour le client OIDC. Cette valeur est généralement spécifique à une intégration d'application IdP construite, par exemple une inscription d'application Azure ou une application web Okta.

Champ	Description
Secret du Client	(**Obligatoire**) Le secret client utilisé conjointement avec l'ID client pour échanger un jeton d'accès. Cette valeur est généralement spécifique à une intégration d'application IdP construite, par exemple une inscription d'application Azure ou une Application Web Okta.
Adresse des métadonnées	(**Requis si l'Autorité n'est pas valide**) Une URL de métadonnées où Bitwarden peut accéder aux métadonnées du serveur d'autorisation sous forme d'objet JSON. Par exemple, `https://your.domain.okta.com/oauth2/default/.well-known/oauth-authorization-server`
Comportement de redirection OIDC	(**Requis**) Méthode utilisée par l'IdP pour répondre aux demandes d'authentification de Bitwarden. Les options incluent **Form POST** et **Redirect GET**.
Récupérer les claims depuis l'endpoint d'informations utilisateur (User Info Endpoint)	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.
Portées supplémentaires/personnalisées	Définissez des portées personnalisées à ajouter à la demande (séparées par des virgules).
Types de revendications d'identifiant 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 se rabattre sur les types standard.
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 se rabattre sur les types standard.

Champ	Description
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 revenir sur les types standard.
Valeurs Authentication Context Class Reference demandées	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 la revendication `acr` que Bitwarden doit attendre et valider dans la réponse.

Attributs et revendications OIDC

Une **adresse de courriel est requise pour la provision du compte**, qui peut être transmise comme l'un des attributs ou revendications dans le tableau ci-dessous.

Un identifiant utilisateur unique est également fortement recommandé. En cas d'absence, le courriel sera utilisé à sa place pour lier l'utilisateur.

Les attributs/revendications sont listés par ordre de préférence pour la correspondance, y compris les solutions de secours le cas échéant :

Valeur	Revendication/Attribut	Revendication/attribut de secours
ID unique	Configuration des revendications d'identifiant utilisateur personnalisé NameID (quand il n'est pas transitoire) urn:oid:0.9.2342.19200300.100.1.1 Sous IDU UPN NEPP	
Courriel	Revendications de courriel personnalisé configuré Courriel http://schemas.xmlsoap.org/ws/2005/05/identité/claims/emailaddress urn:oid:0.9.2342.19200300.100.1.3 Courrier Adresse électronique	Nom_d'utilisateur_préféré Urn:oid:0.9.2342.19200300.100.1.1 IDU

Valeur	Revendication/Attribut	Revendication/attribut de secours
Nom	Noms de revendications personnalisés configurés Nom http://schemas.xmlsoap.org/ws/2005/05/identité/claims/name urn:oid:2.16.840.1.113730.3.1.241 urn:oid:2.5.4.3 Nom d'affichage CN	Prénom + " " + Nom de famille (voir ci-dessous)
Prénom	urn:oid:2.5.4.42 Prénom Prénom FN Prénom Surnom	
Nom de famille	urn:oid:2.5.4.4 SN Nom de famille Nom de famille	