bitwarden | Article du Centre d'Aide

CONSOLE ADMIN > IDENTIFIEZ-VOUS AVEC SSO

Configuration SAML 2.0

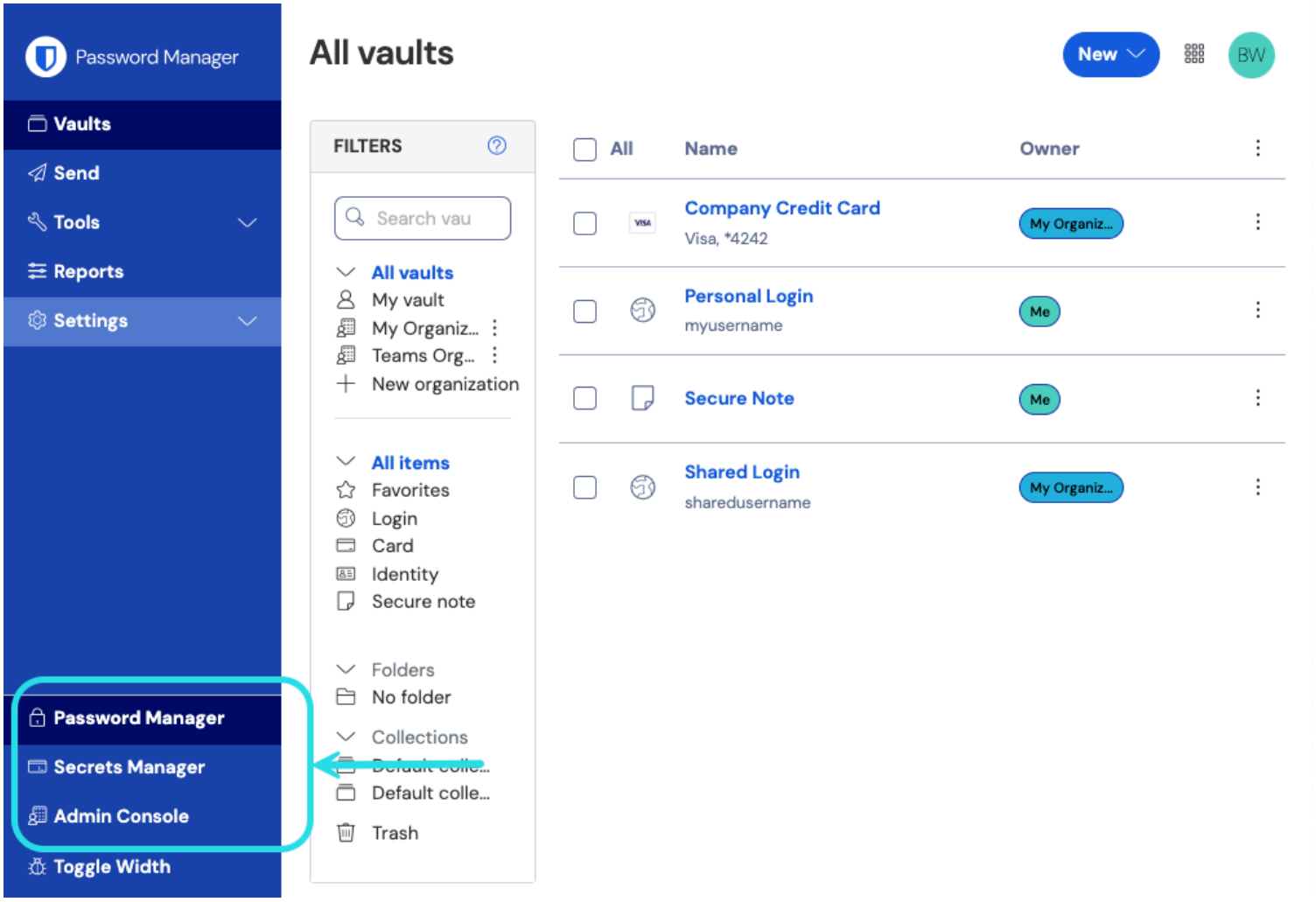
Afficher dans le centre d'aide:
https://bitwarden.com/help/configure-sso-saml/

Configuration SAML 2.0

Étape 1: Définir un identifiant SSO

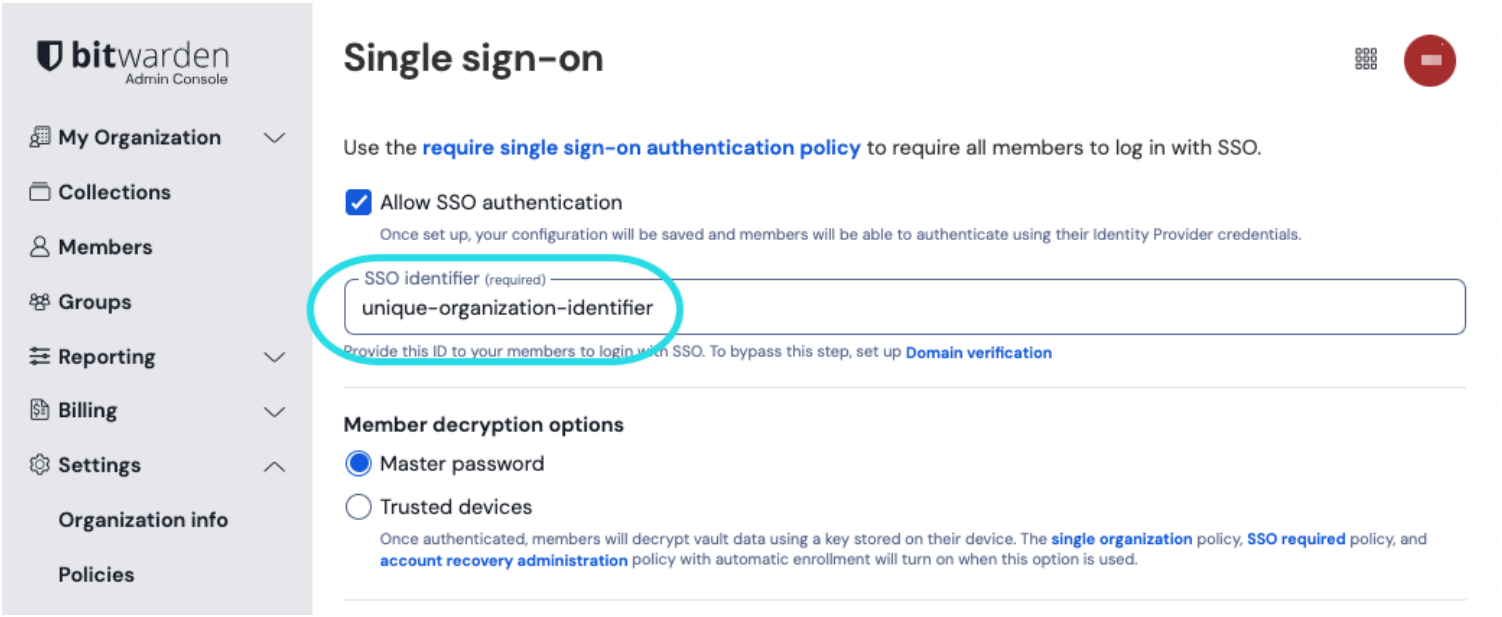
Les utilisateurs qui authentifient leur identité en utilisant SSO devront entrer un **identifiant SSO** qui indique l'organisation (et donc, l'intégration SSO) à authentifier. Pour définir un identifiant SSO unique :

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



commutateur-de-produit

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



Entrez un identifiant

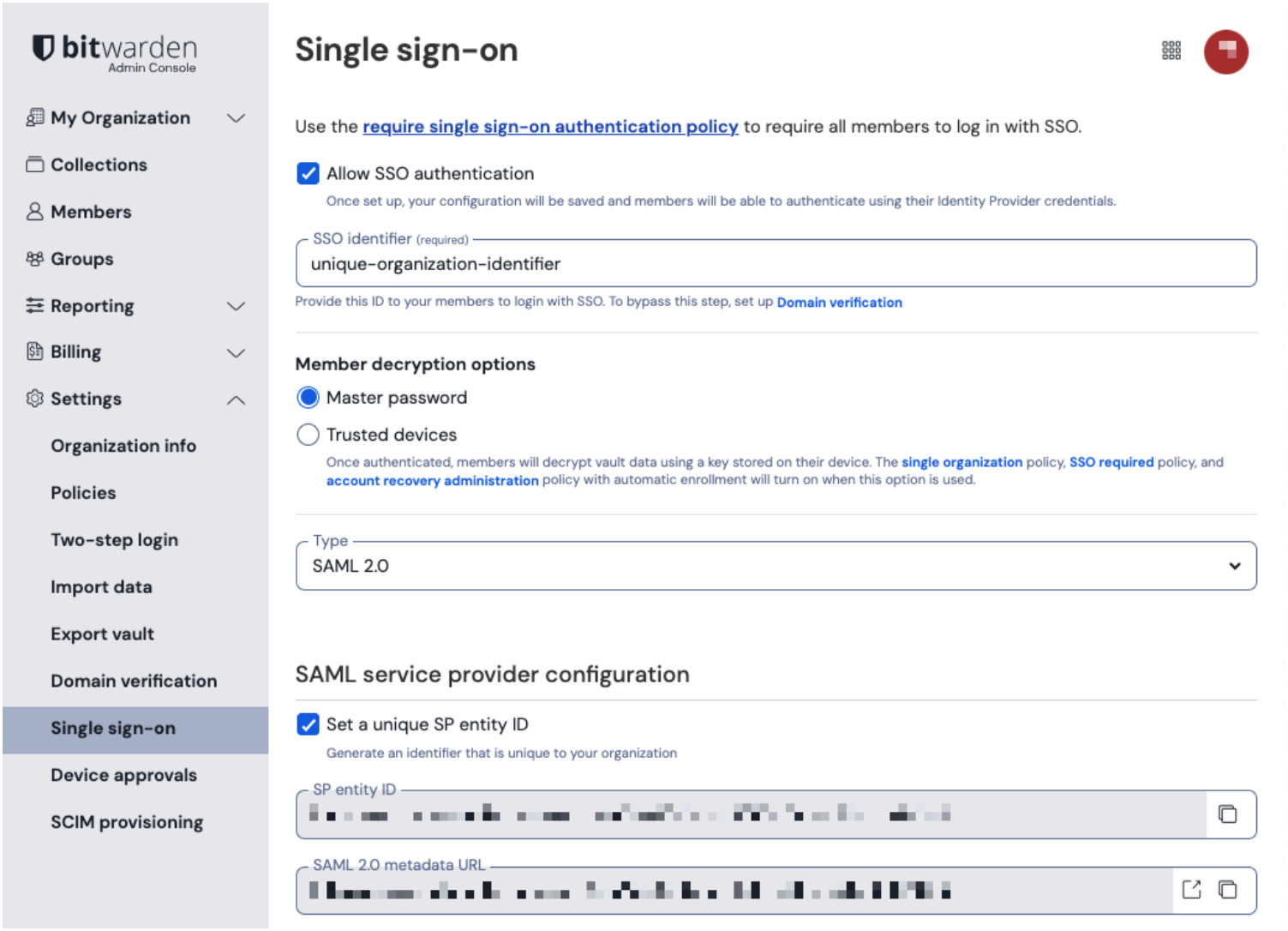
3. Passez à **Étape 2: Activer l'identifiant avec SSO**.

> **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 SAML 2.0

2. Dans le menu déroulant **Saisir**, sélectionnez l'option **SAML 2.0**. Si vous prévoyez d'utiliser OIDC à la place, passez au Guide de Configuration OIDC.

Vous pouvez désactiver l'option **Définir un ID d'entité SP unique** à ce stade si vous le souhaitez. En faisant cela, votre ID d'organisation sera supprimé 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.

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
AD FS	Guide de mise en œuvre AD FS
Auth0	Guide de mise en œuvre Auth0
AWS	Guide de mise en œuvre AWS
Azur	Guide de mise en œuvre Azure
Duo	Guide de mise en œuvre de Duo
Google	Guide de mise en œuvre de Google
JumpCloud	Guide de mise en œuvre de JumpCloud
Keycloak	Guide de mise en œuvre de Keycloak
Okta	Guide de mise en œuvre Okta
OneLogin	Guide de mise en œuvre OneLogin
PingFederate	Guide de mise en œuvre de PingFederate

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 SAML 2.0**, we recommend using one of the above implementation guides instead of the following generic material.

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 à attendre pour les réponses SAML.

Configuration du fournisseur de services

Champ	Description
ID de l'entité SP	(**Généré automatiquement**) Le point de terminaison Bitwarden pour les demandes d'authentification. 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.
URL des métadonnées SAML 2.0	(URL des métadonnées **générées automatiquement**) pour le point d'extrémité Bitwarden. 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 du Service de Consommation d'Assertion (ACS)	(**Généré automatiquement**) Emplacement où l'assertion SAML est envoyée depuis l'IdP. 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.
Format d'identifiant de nom	Format que Bitwarden demandera de l'assertion SAML. Doit être converti en chaîne de caractères. Les options comprennent : -Non spécifié (par défaut) -Adresse de courriel -Nom du sujet X.509 -Nom Qualifié de Domaine Windows -Nom Principal de Kerberos -Identifiant d'entité -Persistant -Éphémère

Champ	Description
Algorithme de Signature Sortant	L'algorithme que Bitwarden utilisera pour signer les requêtes SAML. Les options incluent : - `http://www.w3.org/2001/04/xmldsig-more#rsa-sha256` (par défaut) - `http://www.w3.org/2000/09/xmldsig#rsa-sha1` - `http://www.w3.org/2000/09/xmldsig#rsa-sha384` - `http://www.w3.org/2000/09/xmldsig#rsa-sha512`
Comportement de signature	Si/quand les demandes SAML seront signées. Les options comprennent : -Si IdP veut des demandes d'authentification signées (par défaut) -Toujours -Jamais
Algorithme de Signature Minimum Entrant	Force minimale de l'algorithme que Bitwarden acceptera dans les réponses SAML.
Attendez-vous à des assertions signées	Cochez cette case si Bitwarden doit s'attendre à ce que les réponses de l'IdP soient signées.
Vérifier 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 dans l'image Docker de l'identifiant Bitwarden avec SSO.

Configuration du fournisseur d'Identité

Champ	Description
ID de l'entité	(**Requis**) Adresse ou URL de votre serveur d'identité ou l'Identité de l'IdP Entity ID. Ce champ est sensible à la casse et doit correspondre exactement à la valeur IdP.
Type de Reliure	Méthode utilisée par l'IdP pour répondre aux demandes SAML de Bitwarden. Les options comprennent : -Redirection (recommandée) -HTTP POST

Champ	Description
URL du service de connexion unique	(**Requis si l'ID de l'entité n'est pas une URL**) URL SSO délivrée par votre IdP.
URL du service de déconnexion unique	La connexion avec SSO ne prend actuellement **pas** en charge SLO. Cette option est prévue pour une utilisation future, cependant nous recommandons fortement de pré-configurer ce champ.

Certificat Public X509	(**Requis**) Le corps du certificat encodé en Base-64 X.509. N'incluez pas le
	
	`-----DÉBUT DU CERTIFICAT-----`
	
	et
	
	`-----FIN DU CERTIFICAT-----`
	
	lignes ou portions du certificat au format CER/PEM.
	
	La valeur du certificat est sensible à la casse, les espaces supplémentaires, les retours à la ligne et autres caractères superflus à l'intérieur de ce champ provoqueront une défaillance de la validation du certificat. Copier **seulement** les données du certificat dans ce champ.

Algorithme de Signature Sortant	L'algorithme que votre IdP utilisera pour signer les réponses/affirmations SAML. Les options comprennent : - `http://www.w3.org/2001/04/xmldsig-more#rsa-sha256` (par défaut) - `http://www.w3.org/2000/09/xmldsig#rsa-sha1` - `http://www.w3.org/2000/09/xmldsig#rsa-sha384` - `http://www.w3.org/2000/09/xmldsig#rsa-sha512`
Autoriser les demandes de déconnexion sortantes	La connexion avec SSO ne prend actuellement **pas** en charge SLO. Cette option est prévue pour une utilisation future, cependant nous recommandons fortement de pré-configurer ce champ.
Signer les demandes d'authentification	Cochez cette case si votre IdP doit s'attendre à ce que les demandes SAML de Bitwarden 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.

Attributs SAML & revendications

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 suivant.

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	NameID (quand il n'est pas transitoire) urn:oid:0.9.2342.19200300.100.1.1 Sous IDU UPN NEPP	
Courriel	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
Nom	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	

Valeur	Revendication/Attribut	Revendication/attribut de secours
Nom de famille	urn:oid:2.5.4.4 SN Nom de famille Nom de famille	