bitwarden | Article du Centre d'Aide

CONSOLE ADMIN > IDENTIFIEZ-VOUS AVEC SSO >

Implémentation SAML de OneLogin

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

Implémentation SAML de OneLogin

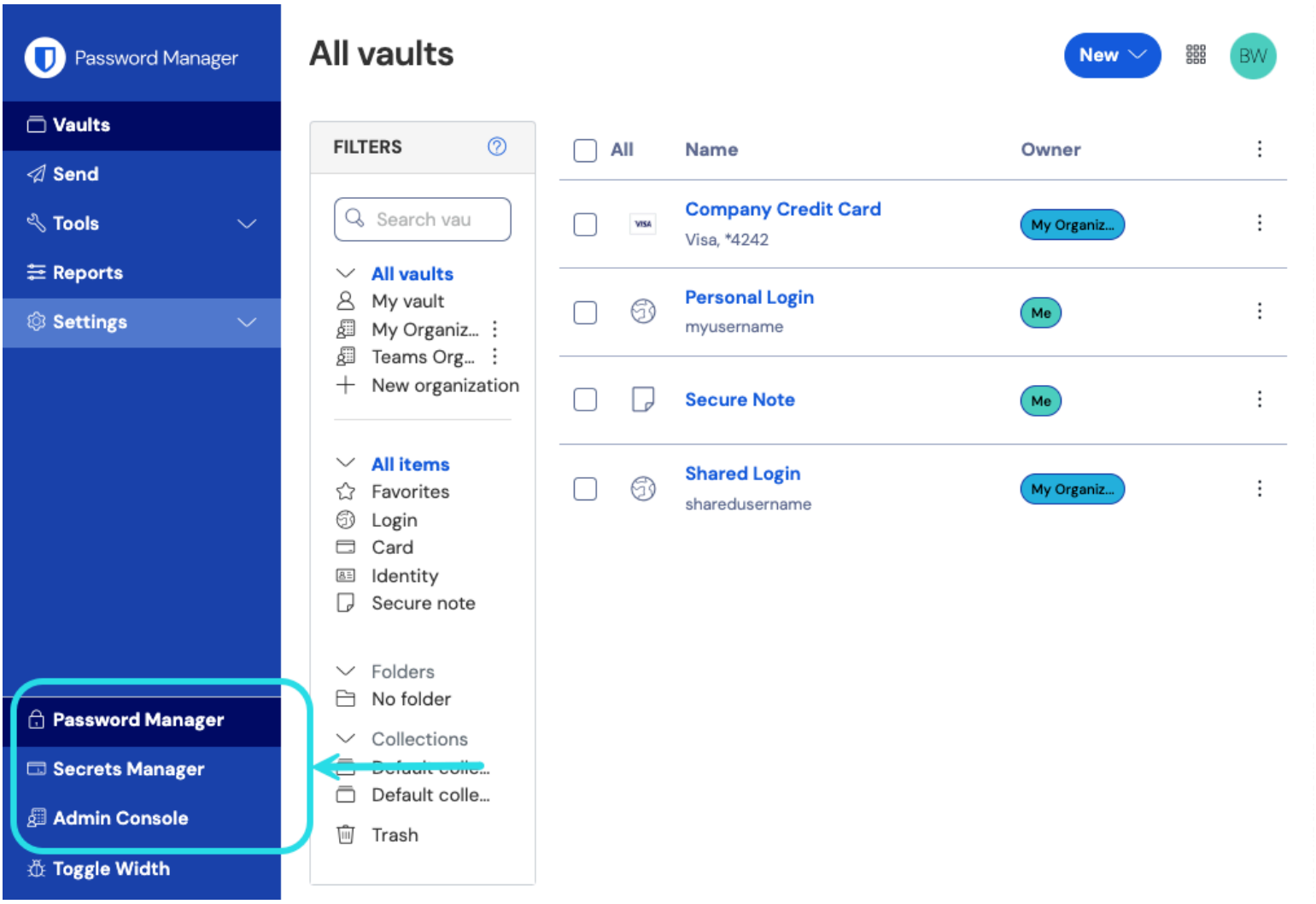
Cet article contient de l'aide spécifique à **OneLogin** pour configurer l'identifiant avec SSO via SAML 2.0. Pour obtenir de l'aide pour configurer l'identifiant avec SSO pour un autre IdP, reportez-vous à Configuration SAML 2.0.

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

> **Tip**
>
> **Already an SSO expert?** Skip the instructions in this article and download screenshots of sample configurations to compare against your own.
>
> Download Sample

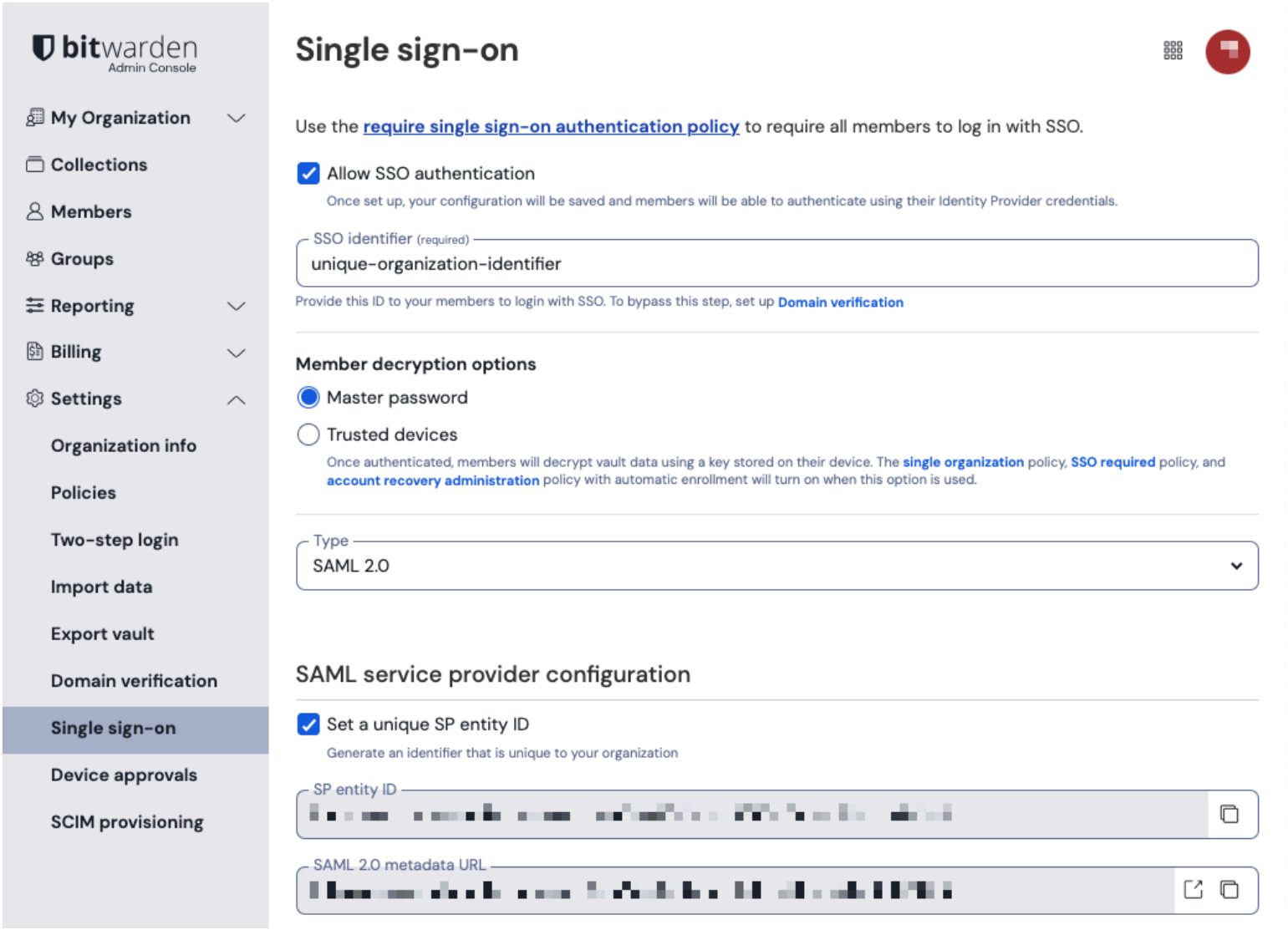
Ouvrez SSO dans l'application web

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

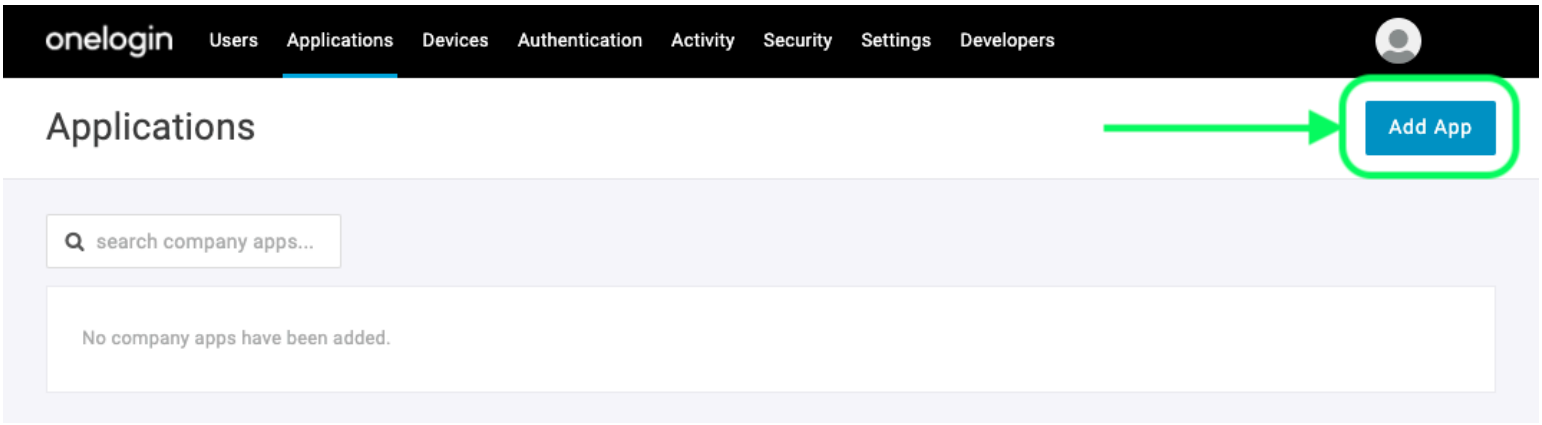
Si vous ne l'avez pas déjà fait, créez un **identifiant SSO** unique pour votre organisation et sélectionnez **SAML** dans le menu déroulant **Saisir**. Gardez cet écran ouvert pour une référence facile.

Vous pouvez désactiver l'option **Définir un ID d'entité SP unique** à ce stade si vous le souhaitez. 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.

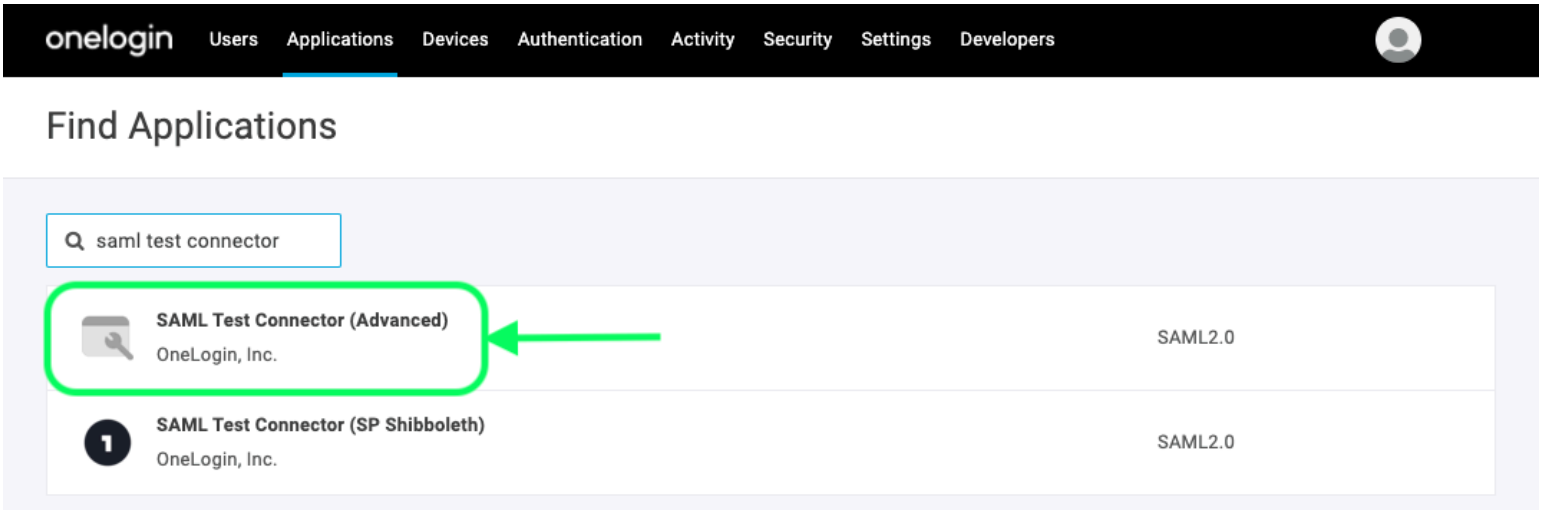
Créez une application OneLogin

Dans le portail OneLogin, naviguez vers l'écran **Applications** et sélectionnez le bouton **Ajouter une application** :



Add an Application

Dans la barre de recherche, saisissez `saml test connector` et sélectionnez l'application **SAML Test Connector (Advanced)** :

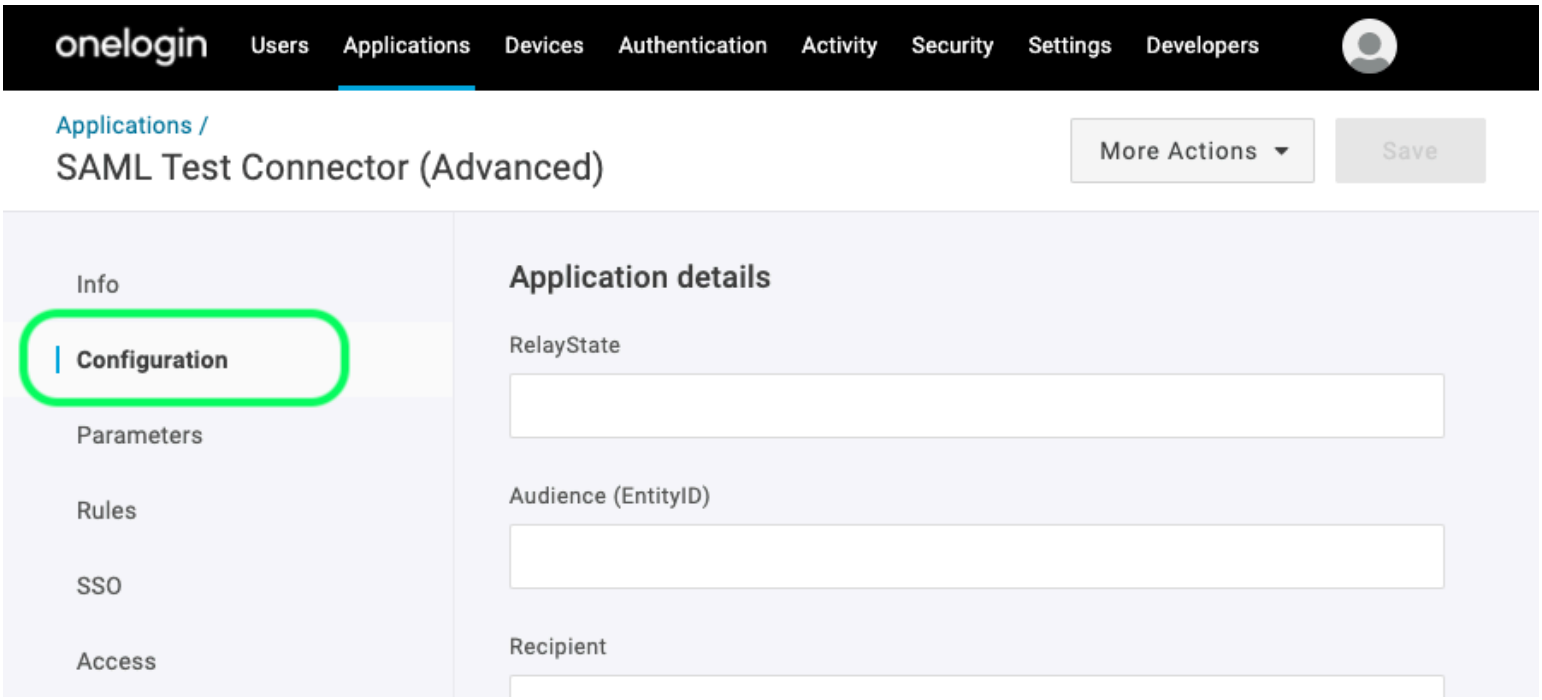


SAML Test Connector App

Donnez à votre application un **Nom d'affichage** spécifique à Bitwarden et sélectionnez le bouton **Enregistrer**.

Configuration

Sélectionnez **Configuration** dans la navigation à gauche et configurez les informations suivantes, dont certaines que vous devrez récupérer à partir de l'écran de connexion unique :



App Configuration

Paramètres de l'application	Description
Audience (EntityID)	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.
Destinataire	Définissez ce champ sur le même **ID d'entité SP** pré-généré utilisé pour le paramètre **Audience (ID d'entité)**.
Validateur d'URL ACS (Consommateur)	Malgré le fait d'être marqué **Requis** par OneLogin, vous n'avez pas réellement besoin de saisir des informations dans ce champ pour intégrer avec Bitwarden. Passez au champ suivant, **URL ACS (Consommateur)**.
URL (Consommateur) ACS	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 votre organisation et variera en fonction de votre configuration.

Paramètres de l'application	Description
Initiateur SAML	Sélectionnez **Fournisseur de Service**. La connexion avec SSO ne prend pas en charge actuellement les assertions SAML initiées par IdP.
Format de nameID SAML	Définissez ce champ sur le Format NameID SAML que vous souhaitez utiliser pour les assertions SAML.
Élément de signature SAML	Par défaut, OneLogin signera la réponse SAML. Vous pouvez régler cela sur **Assertion** ou **Les deux**

Sélectionnez le bouton **Enregistrer** pour terminer vos paramètres de configuration.

Paramètres

Sélectionnez **Paramètres** dans la navigation à gauche et utilisez l'icône + **Ajouter** pour créer les paramètres personnalisés suivants:

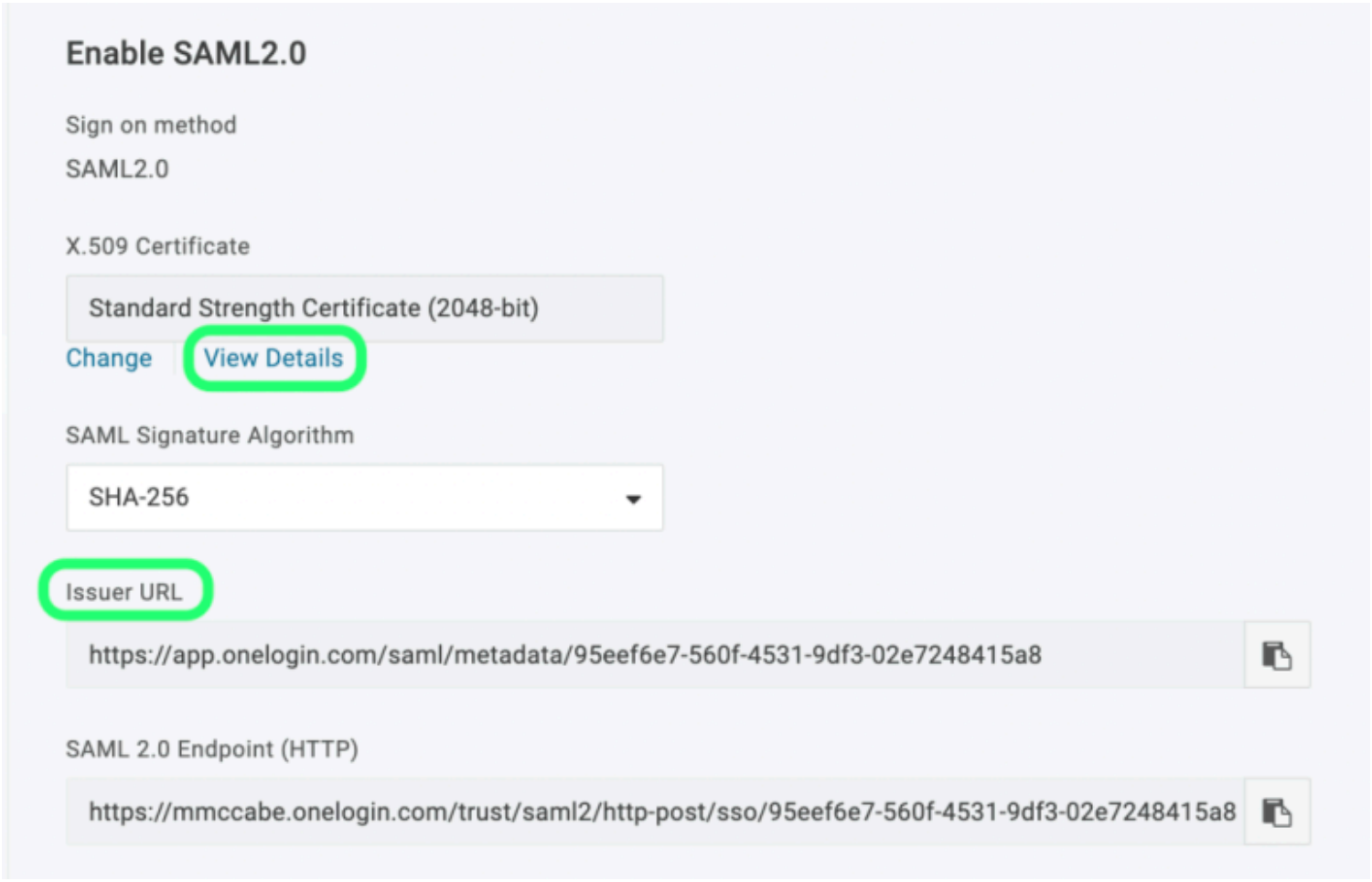
Nom du champ	Valeur
courriel	Courriel
prénom	Prénom
nom de famille	Nom de famille

Sélectionnez le bouton **Enregistrer** pour terminer vos paramètres personnalisés.

SSO

Sélectionnez **SSO** dans la navigation à gauche et complétez ce qui suit:

1. Sélectionnez le lien **Afficher les détails** sous votre certificat X.509 :



View your Cert

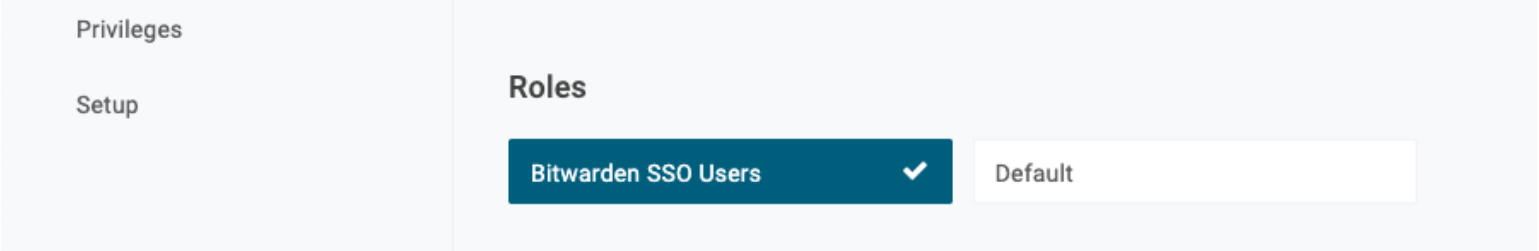
Sur l'écran du Certificat, téléchargez ou copiez votre Certificat X.509 PEM, car vous devrez l'utiliser plus tard. Une fois copié, revenez à l'écran principal de SSO.

2. Définissez votre **Algorithme de Signature SAML**.

3. Prenez note de votre **URL de l'émetteur** et de votre **Point de terminaison SAML 2.0 (HTTP)**. Vous aurez besoin d'utiliser ces valeurs sous peu.

Accès

Sélectionnez **Accès** dans la navigation à gauche. Dans la section **Rôles**, attribuez l'accès à l'application à tous les rôles que vous souhaitez pouvoir utiliser Bitwarden. La plupart des implémentations créent un rôle spécifique à Bitwarden et choisissent plutôt d'attribuer en fonction d'un attrape-tout (par exemple, **Par défaut**) ou en fonction des rôles préexistants.



Role Assignment

Retour à l'application web

À ce stade, vous avez configuré tout ce dont vous avez besoin dans le contexte du portail OneLogin. 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 en fonction des choix sélectionnés dans le portail OneLogin lors de la création de l'application :

Champ	Description
Format d'identifiant de nom	Définissez ce champ sur ce que vous avez sélectionné pour le champ **Format du nomID SAML** de OneLogin lors de la configuration de l'application.
Algorithme de Signature Sortant	Algorithme utilisé pour signer les requêtes SAML, par défaut `sha-256`.
Comportement de signature	Si/quand les demandes SAML seront signées. Par défaut, OneLogin n'exigera pas que les demandes soient signées.
Algorithme de Signature Minimum Entrant	Définissez ce champ sur ce que vous avez sélectionné pour l'**Algorithme de Signature SAML** pendant la configuration de l'application
Voulez-vous des affirmations signées	Cochez cette case si vous avez défini l'élément de signature **SAML** dans OneLogin sur **Assertion** ou **Les deux** pendant la configuration de l'application.
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 dans l'identifiant Bitwarden avec l'image docker 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 nécessitera souvent que vous vous référiez au Portail OneLogin pour récupérer les valeurs de l'application :

Champ	Description
ID de l'entité	Entrez votre **URL de l'émetteur OneLogin**, qui peut être récupérée depuis l'écran SSO de l'application OneLogin. Ce champ est sensible à la casse.
Type de Reliure	Définir sur **HTTP Post** (comme indiqué dans le point de terminaison SAML 2.0 (HTTP)).
URL du service de connexion unique	Entrez votre **Point de terminaison SAML 2.0 (HTTP) OneLogin**, qui peut être récupéré depuis l'écran SSO de l'application OneLogin.
URL du service de déconnexion unique	Connectez-vous avec SSO actuellement **ne prend pas** en charge SLO. Cette option est prévue pour un développement futur, cependant vous pouvez la pré-configurer si vous le souhaitez.

Certificat Public X509	Collez le Certificat X.509 récupéré, 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	Sélectionnez l'algorithme de signature SAML sélectionné dans la section de configuration OneLogin SSO.
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.

Champ	Description
Voulez-vous que les demandes d'authentification soient signées	Que OneLogin 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.

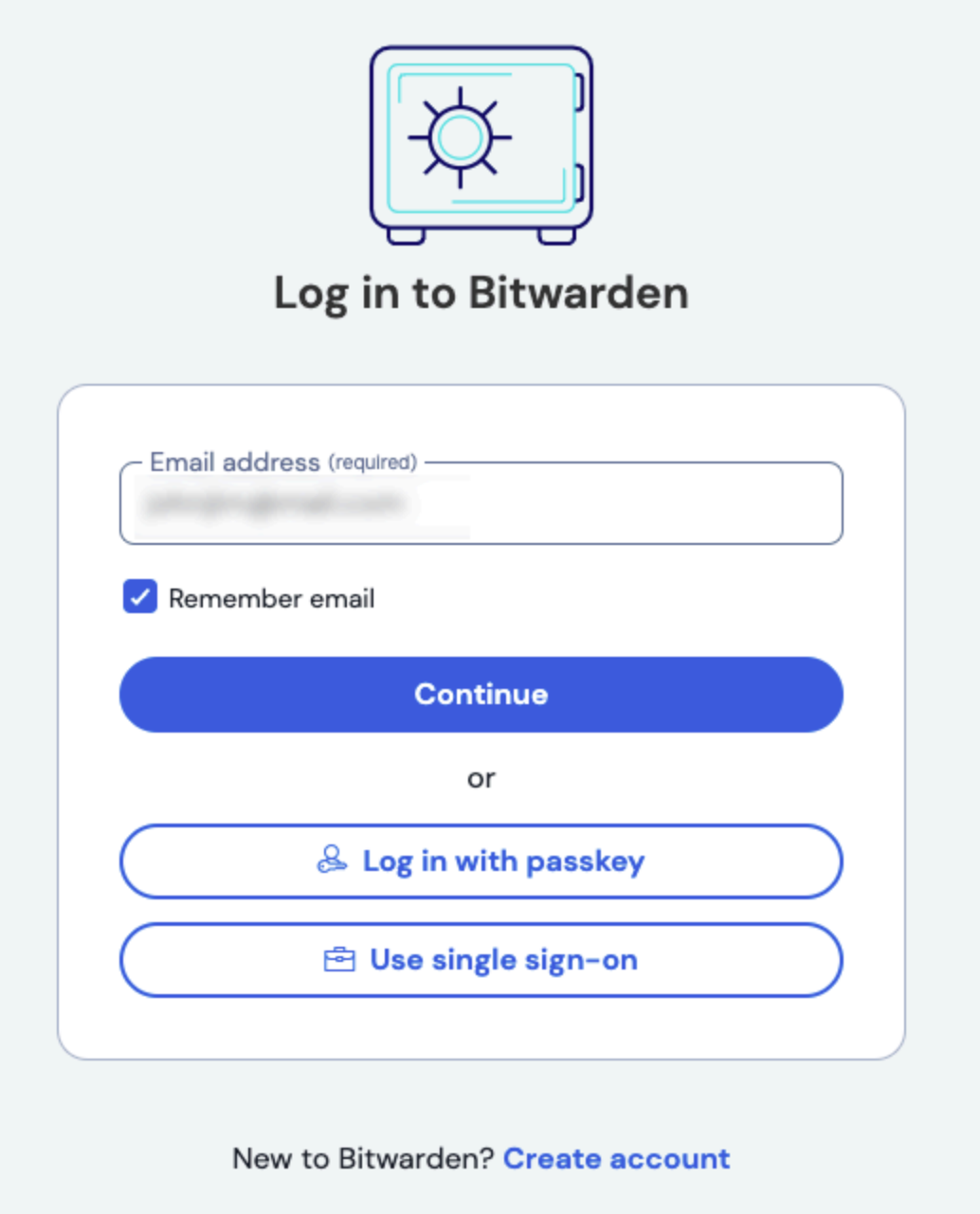
Lorsque vous avez terminé avec la configuration du fournisseur d'identité, **Enregistrez** votre travail.

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.

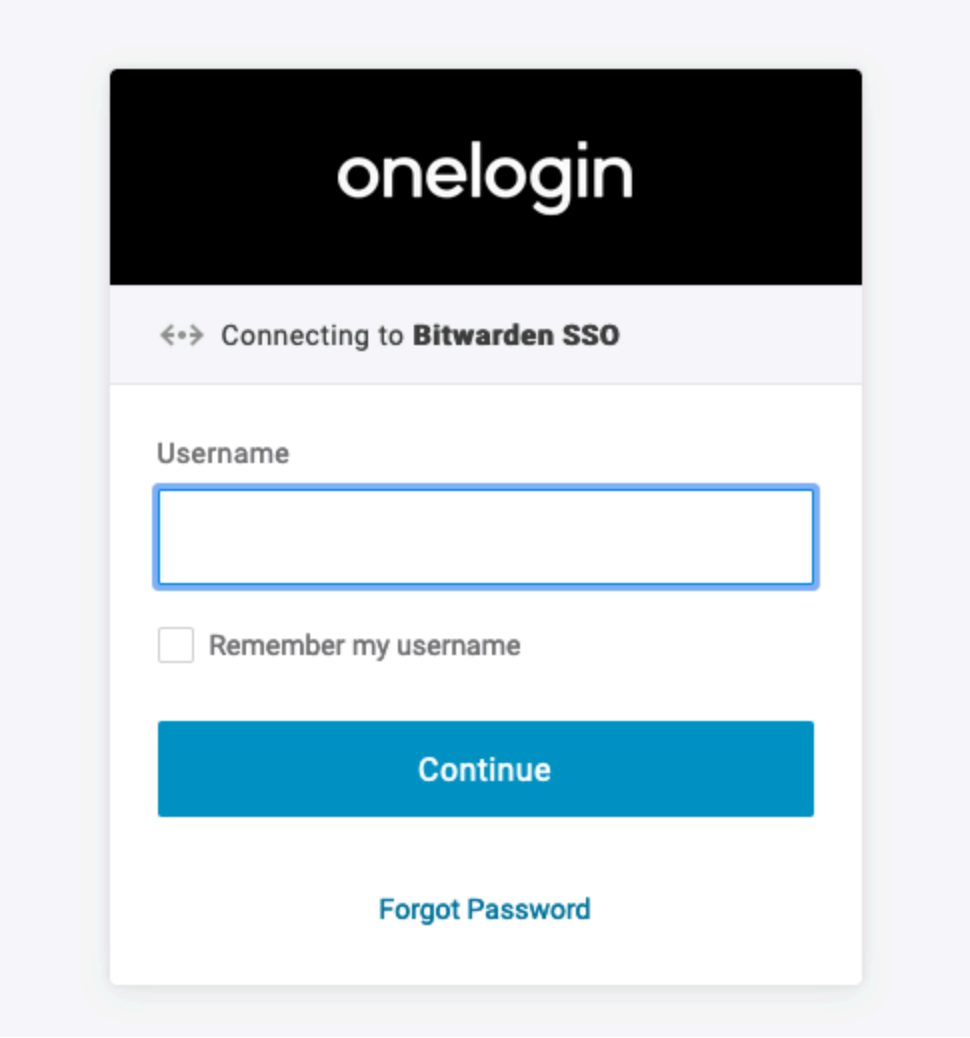
Testez la configuration

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 de l'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 OneLogin :



OneLogin Login

Après vous être authentifié avec vos identifiants OneLogin, 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.