Implémentation SAML de JumpCloud

Implémentation SAML de JumpCloud

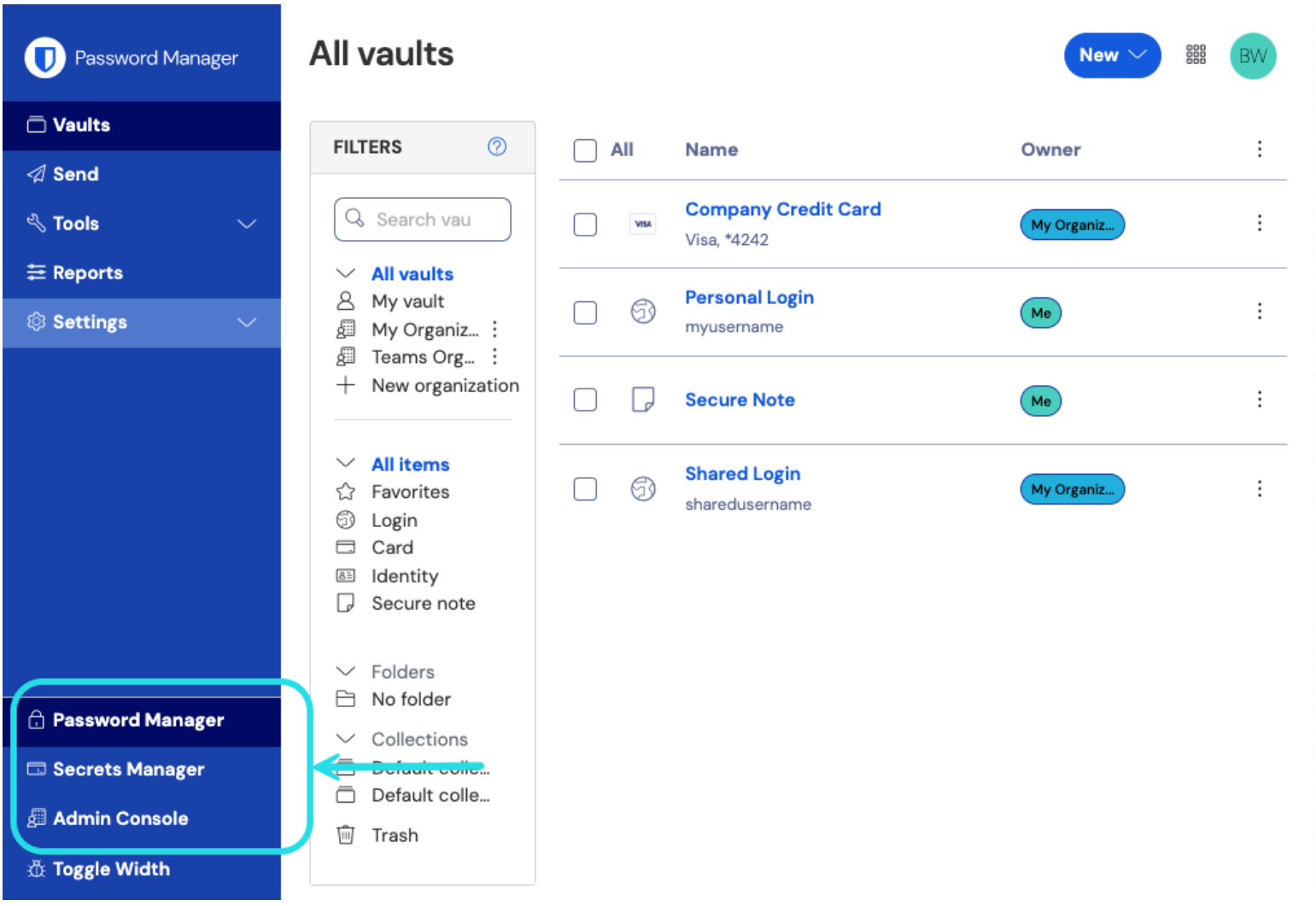
Cet article contient de l'aide **spécifique à JumpCloud** pour configurer l'identifiant avec SSO via SAML 2.0. Pour obtenir de l'aide pour configurer l'identifiant avec SSO pour un autre IdP, reportez-vous à Configuration SAML 2.0.

La configuration implique de travailler simultanément dans l'application web Bitwarden et le portail JumpCloud. 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

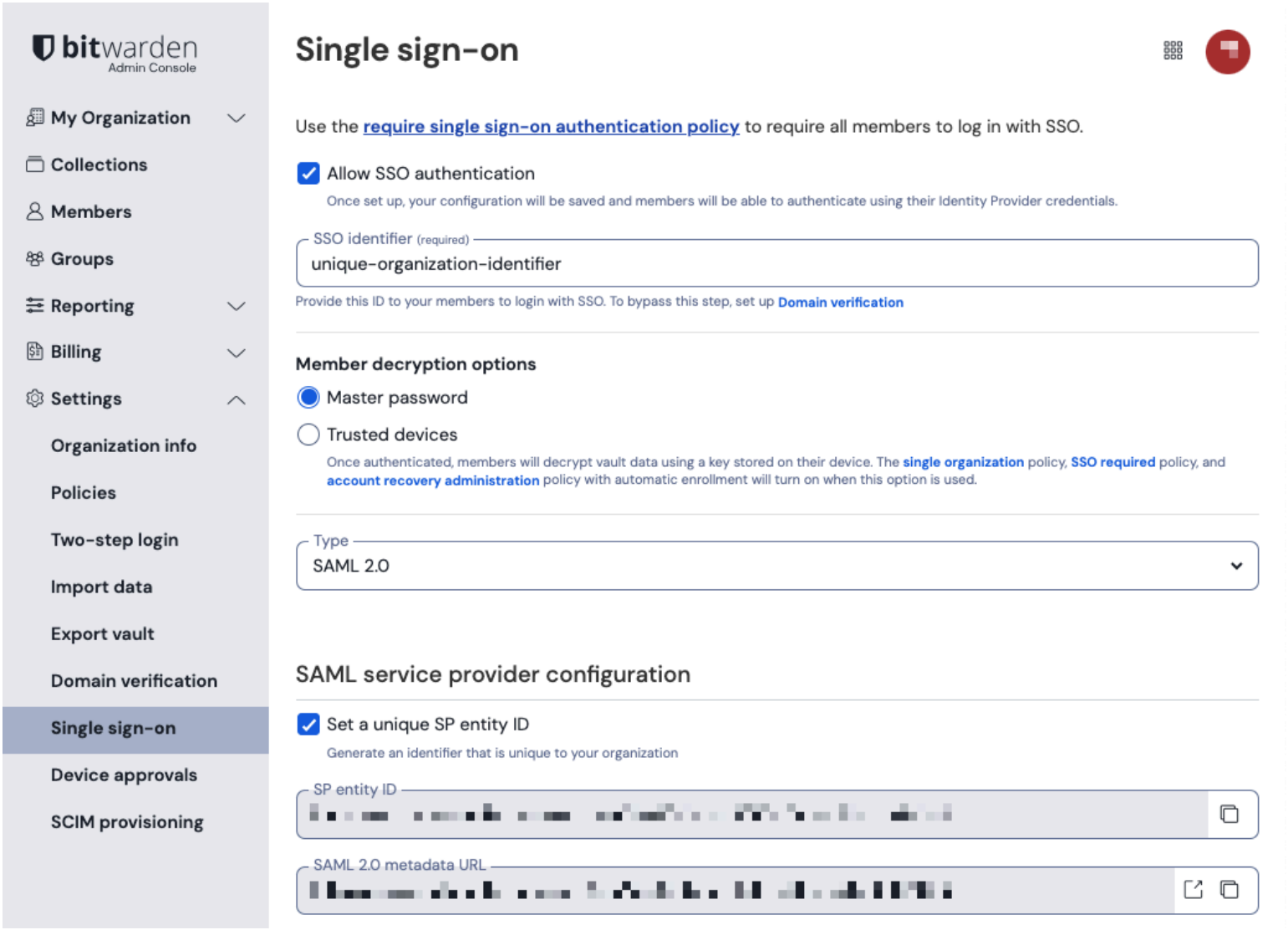
Ouvrez SSO dans l'application web

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

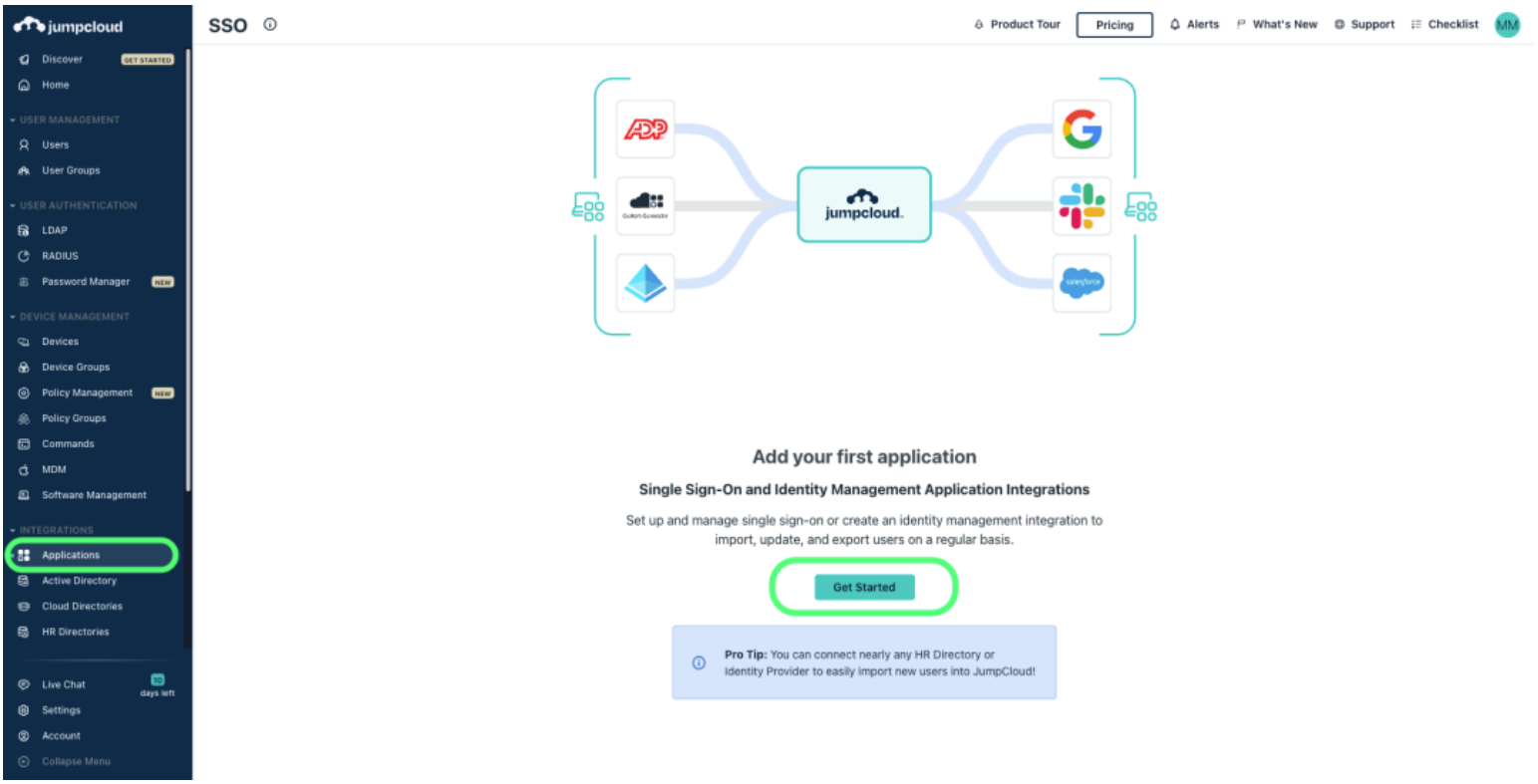
Si vous ne l'avez pas déjà fait, créez un **identifiant SSO** unique pour votre organisation et sélectionnez **SAML** dans le menu déroulant **Saisir** . Gardez cet écran ouvert pour une référence facile.

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.

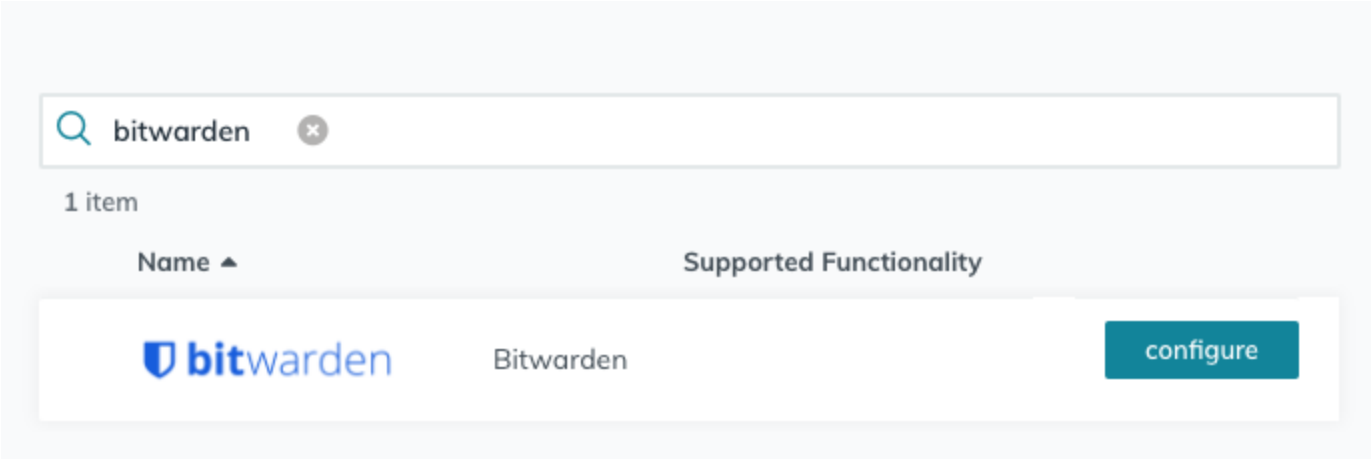
Créez une application SAML JumpCloud

Dans le portail JumpCloud, sélectionnez **Applications** dans le menu et cliquez sur le bouton **Commencer** :



Create Bitwarden app Jumpcloud

Entrez `Bitwarden` dans la boîte de recherche et sélectionnez le bouton **configurer** :



Configure Bitwarden

> **Tip**
>
> If you are more comfortable with SAML, or want more control over things like NameID Format and Signing Algorithms, create a **Custom SAML Application** instead.

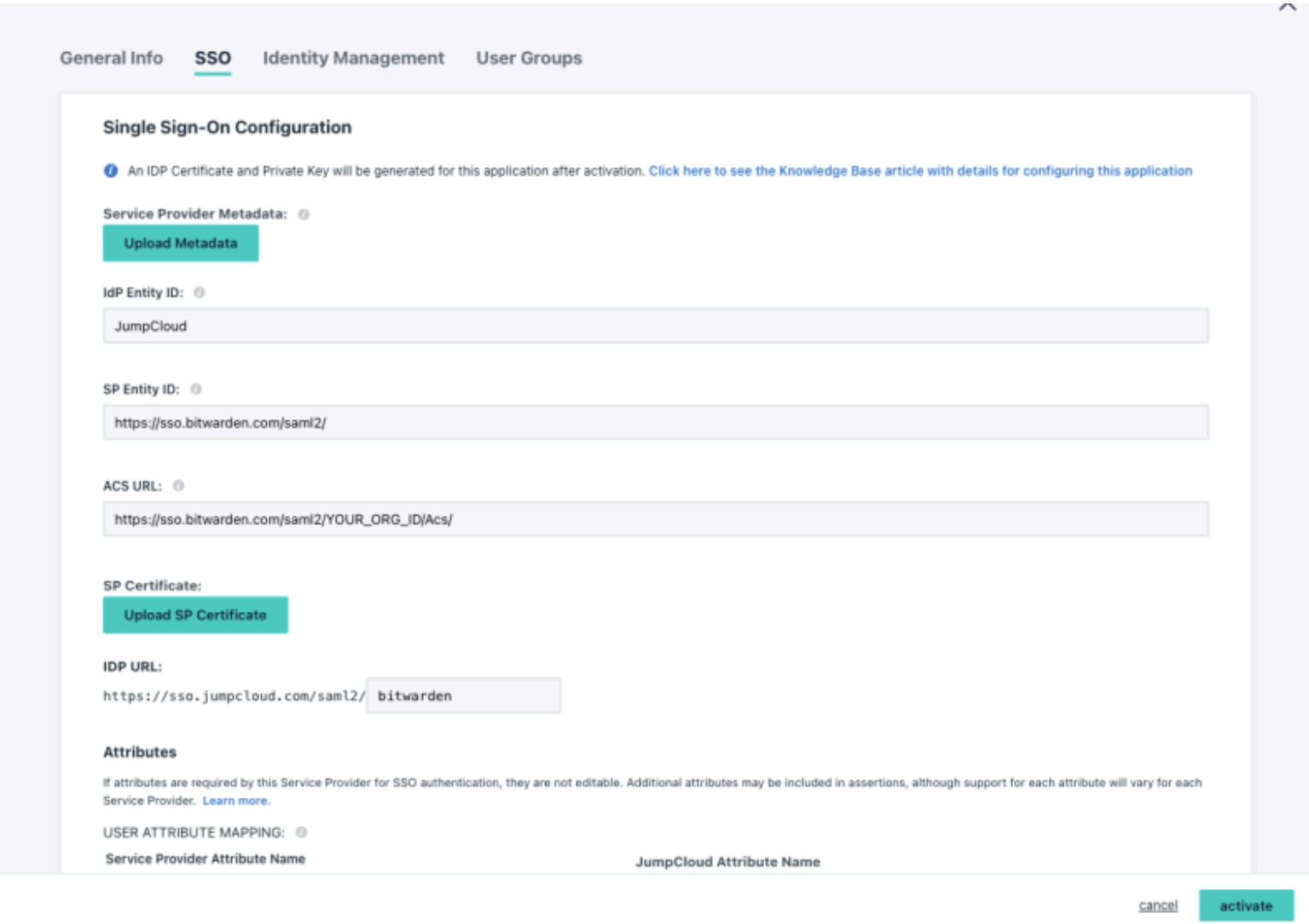
Informations générales

Dans la section **Informations Générales**, configurez les informations suivantes :

Champ	Description
Étiquette d'affichage	Donnez à l'application un nom spécifique à Bitwarden.

Configuration de l'authentification unique

Dans la section **Configuration de la Connexion Unique**, configurez les informations suivantes :



Jumpcloud SSO configuration

Champ	Description
IdP Entity ID	Définissez ce champ sur une valeur unique, spécifique à Bitwarden, par exemple, `bitwardensso_votreentreprise`.
ID de l'entité SP	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 l'organisation et variera en fonction de votre configuration.
URL 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.

Application SAML personnalisée uniquement

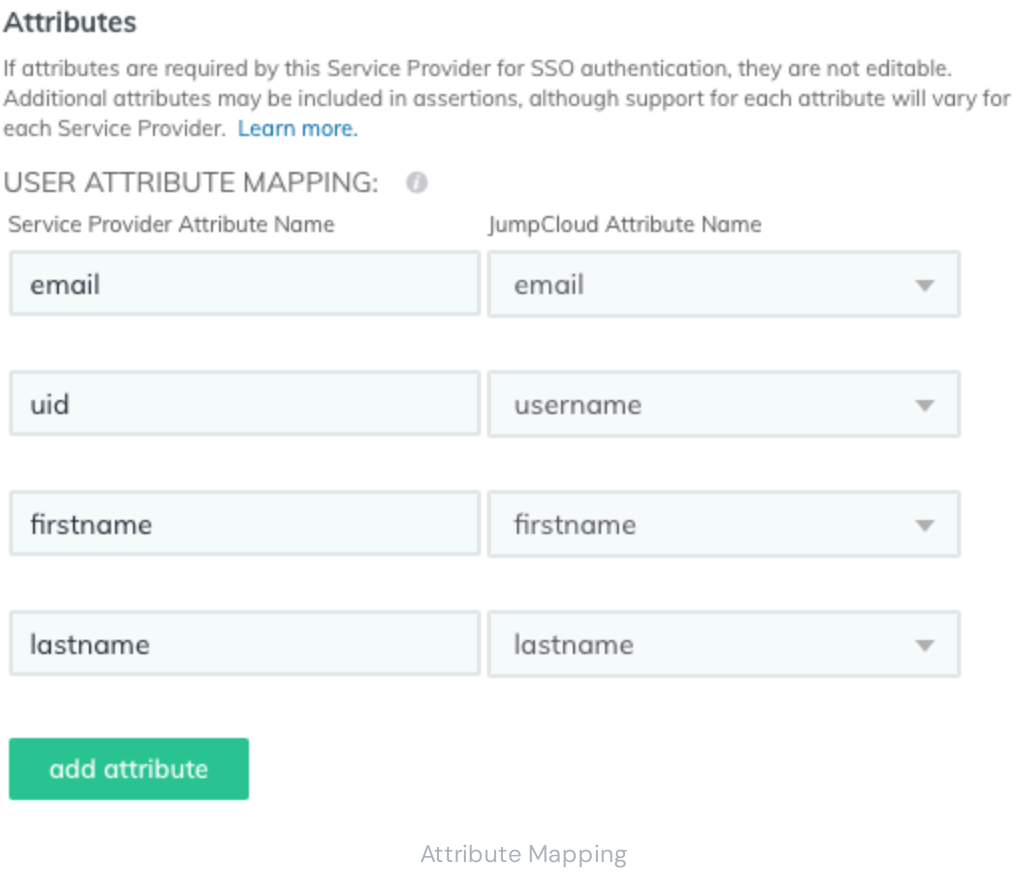
Si vous avez créé une application SAML personnalisée, vous devrez également configurer les champs suivants de la **Configuration de la Connexion Unique** :

Champ	Description
NomID du Sujet SAML	Spécifiez l'attribut JumpCloud qui sera envoyé dans les réponses SAML en tant que NameID.
Format de l'identifiant de nom SAMLSubject	Spécifiez le format du NameID envoyé dans les réponses SAML.
Algorithme de Signature	Sélectionnez l'algorithme à utiliser pour signer les assertions ou les réponses SAML.
Affirmation de signature	Par défaut, JumpCloud signera la réponse SAML. Cochez cette case pour signer l'assertion SAML.
URL de l'identifiant	Spécifiez l'URL à partir de laquelle vos utilisateurs se connecteront à Bitwarden via SSO avec leur identifiant.

Champ	Description
	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 votre URL de serveur configurée, par exemple `https://votre.domaine.com/#/sso`.

Attributs

Dans la section **Configuration du Single Sign-On → Attributs**, construisez les mappages d'attributs suivants SP → IdP. Si vous avez sélectionné l'application Bitwarden dans JumpCloud, celles-ci devraient déjà être construites :

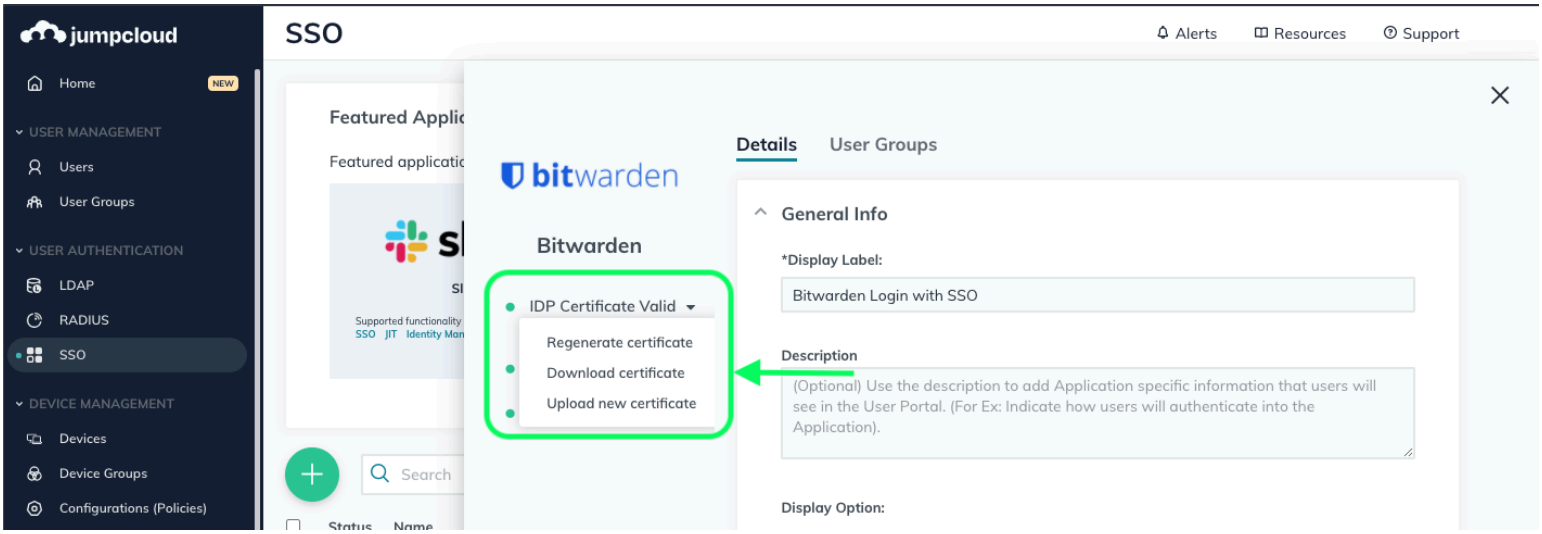


Attribute Mapping

Une fois que vous avez terminé, sélectionnez le bouton **activer**.

Téléchargez le certificat

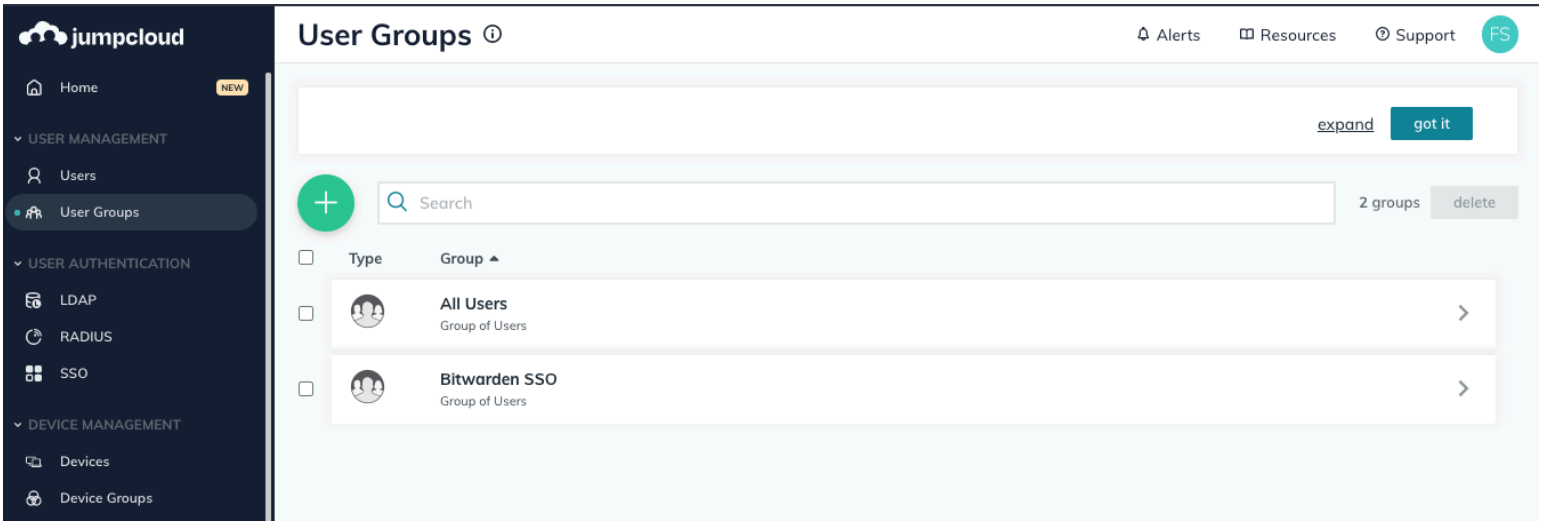
Une fois l'application activée, utilisez à nouveau l'option de menu **SSO** pour ouvrir l'application Bitwarden créée. Sélectionnez le menu déroulant **Certificat IDP** et **Téléchargez le certificat** :



Download Certificate

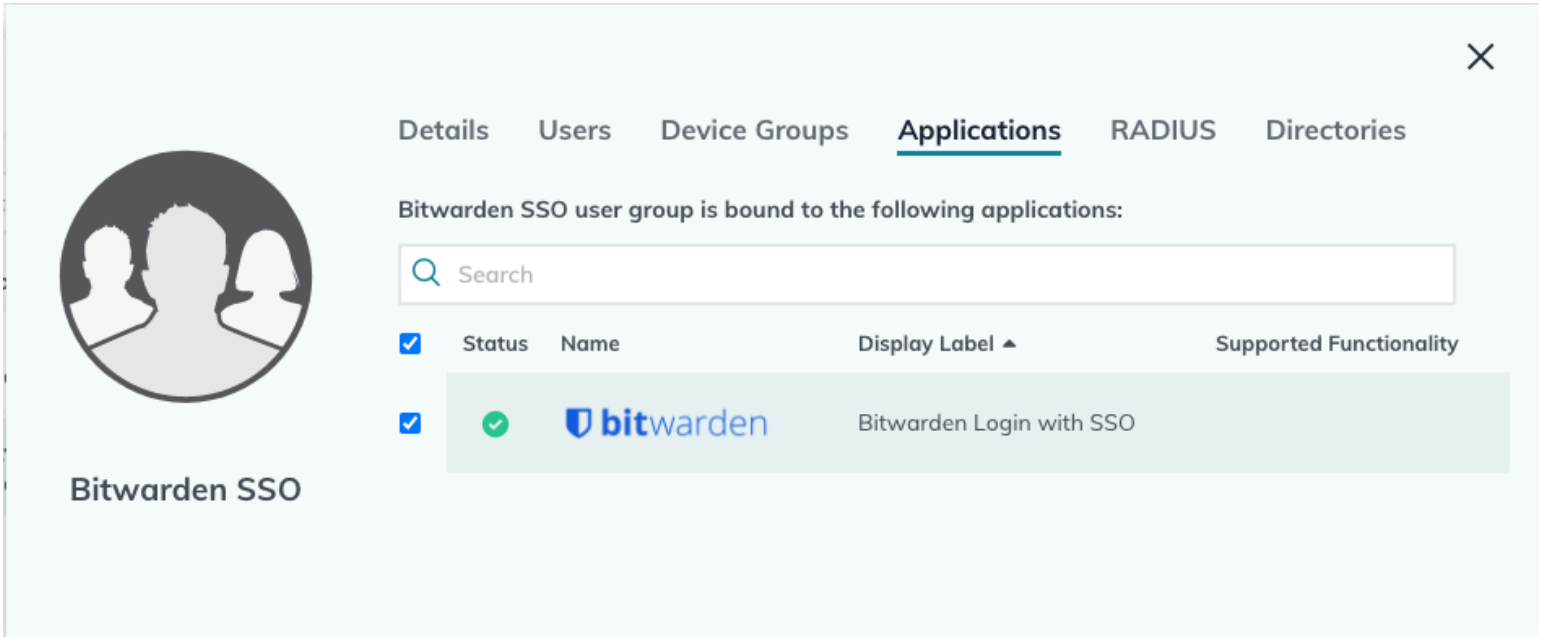
Lier les groupes d'utilisateurs

Dans le portail JumpCloud, sélectionnez **Groupes d'utilisateurs** dans le menu :



User Groups

Créez soit un groupe d'utilisateurs spécifique à Bitwarden, soit ouvrez le groupe d'utilisateurs par défaut Tous les utilisateurs. Dans les deux cas, sélectionnez l'onglet **Applications** et activez l'accès à l'application SSO Bitwarden créée pour ce groupe d'utilisateurs :



Bind App Access

> **Tip**
> Alternatively, you can bind access to user groups directly from the **SSO → Bitwarden Application** screen.

Retour à l'application web

À ce stade, vous avez configuré tout ce dont vous avez besoin dans le contexte du portail JumpCloud. Retournez au coffre 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 JumpCloud lors de la création de l'application :

Champ	Description
Format de l'identifiant de nom	Si vous avez créé une application SAML personnalisée, définissez ceci sur ce que le format NameID SAMLSubject spécifié est dans les paramètres. Sinon, laissez **Non spécifié**.
Algorithme de Signature Sortant	L'algorithme que Bitwarden utilisera pour signer les requêtes SAML.

Champ	Description
Comportement de Signature	Si/quand les demandes SAML seront signées. Par défaut, JumpCloud n'exigera pas que les demandes soient signées.
Algorithme de Signature Minimum Entrant	Si vous avez créé une application SAML personnalisée, réglez ceci sur l'algorithme de signature que vous avez sélectionné dans les paramètres. Sinon, laissez comme `rsa-sha256`.
Voulez des Assertions Signées	Si vous avez créé une application SAML personnalisée, cochez cette case si vous avez défini l'option **Signer l'Assertion** dans JumpCloud. Sinon, laissez décoché.
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'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 nécessitera souvent que vous vous référiez au Portail JumpCloud pour récupérer les valeurs de l'application :

Champ	Description
ID de l'entité	Entrez votre **IdP Entity ID** JumpCloud, qui peut être récupéré à partir de l'écran Configuration de Single Sign-On de JumpCloud. Ce champ est sensible à la casse.
Type de Reliure	Définir sur **Rediriger**.
URL du service de connexion unique	Entrez votre **URL IdP JumpCloud**, qui peut être récupérée depuis l'écran de Configuration de Single Sign-On JumpCloud.
URL du service de déconnexion unique	Se connecter avec SSO ne **supporte pas** actuellement SLO. Cette option est prévue pour un développement futur.

Champ	Description

Certificat Public X509	Collez le certificat 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	Si vous avez créé une application SAML personnalisée, définissez ceci sur l'algorithme de signature que vous avez sélectionné. Sinon, laissez comme `rsa-sha256`.
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 JumpCloud attende 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.

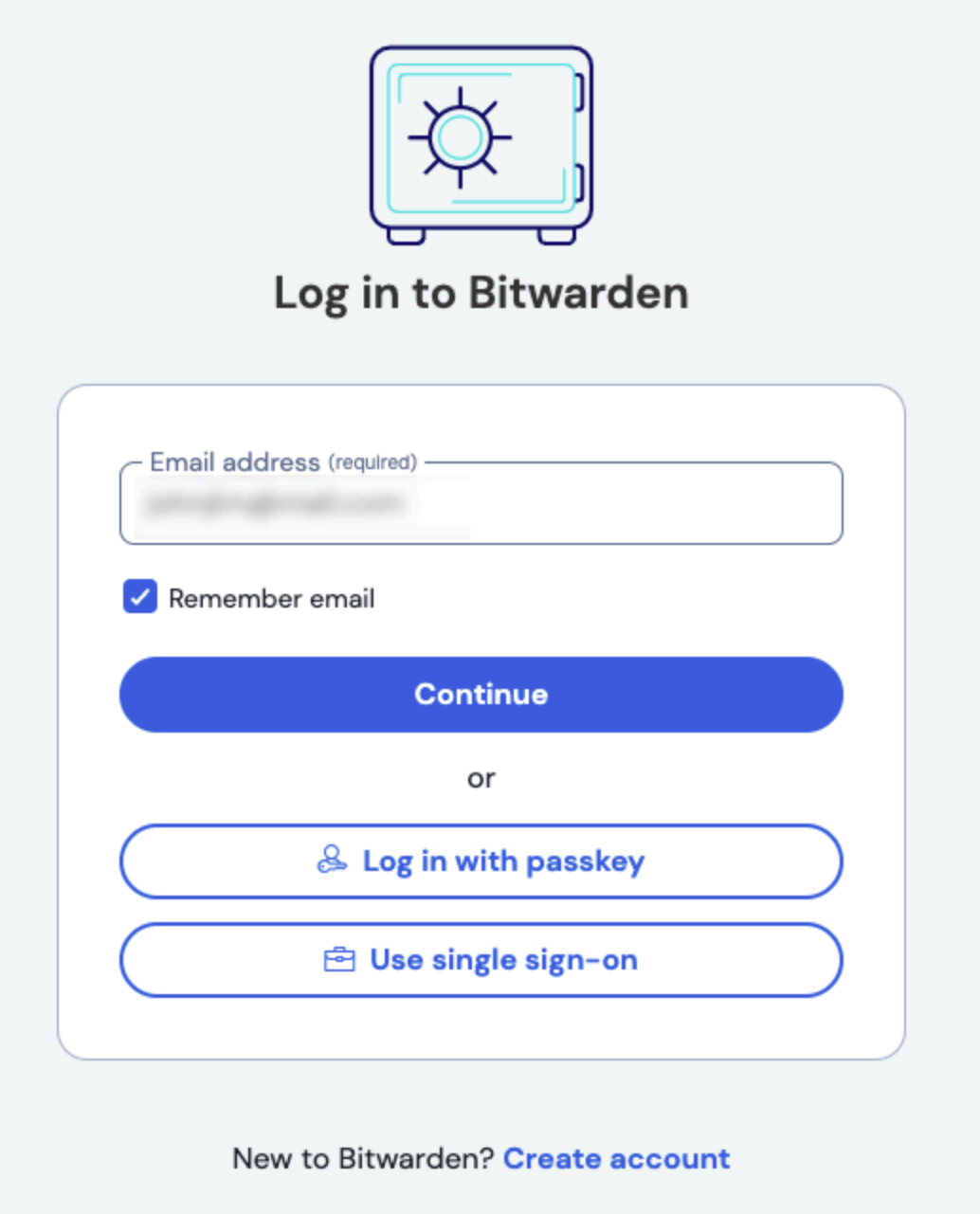
Lorsque vous avez terminé avec la configuration du fournisseur d'identité, **Enregistrez** votre travail.

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.

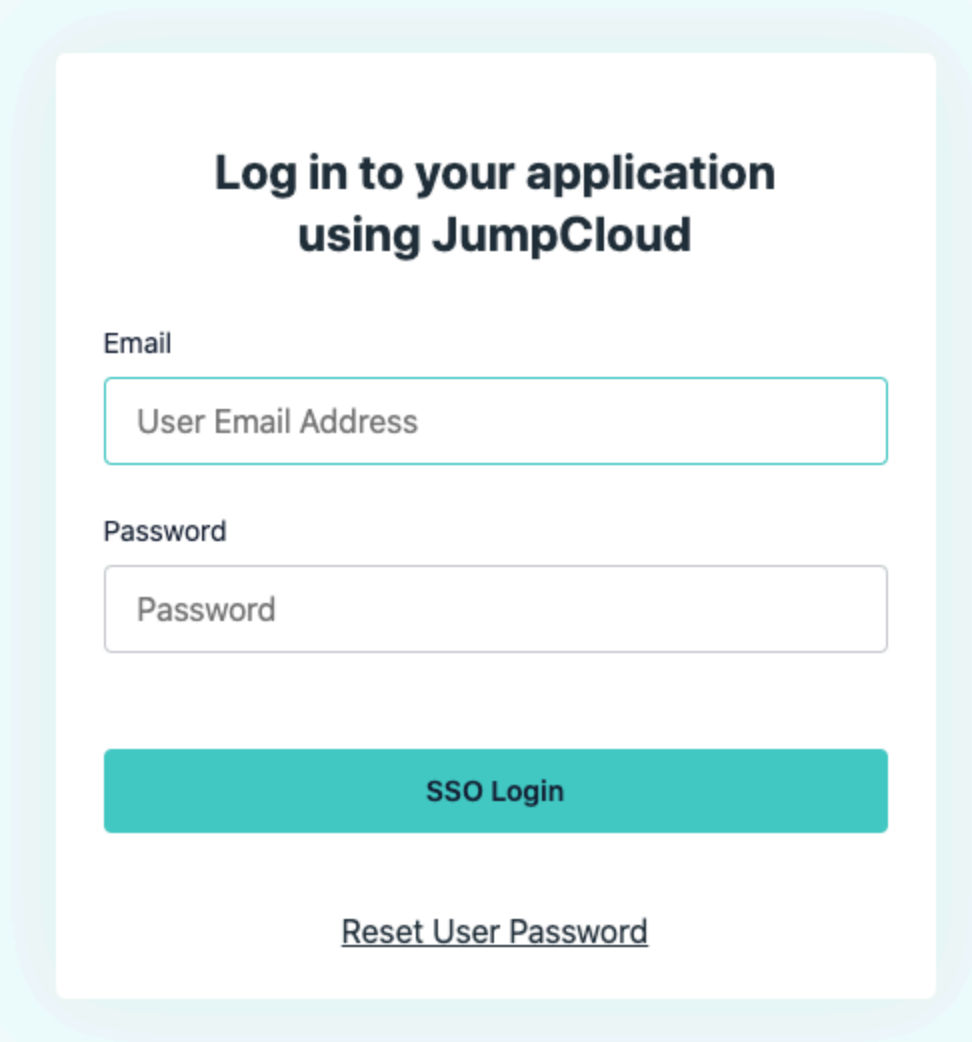
Testez la configuration

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 configurée avec succès, vous serez redirigé vers l'écran d'identifiant JumpCloud :



JumpCloud Login

Après vous être authentifié avec vos identifiants JumpCloud, 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.