Implémentation SAML Okta

Implémentation SAML Okta

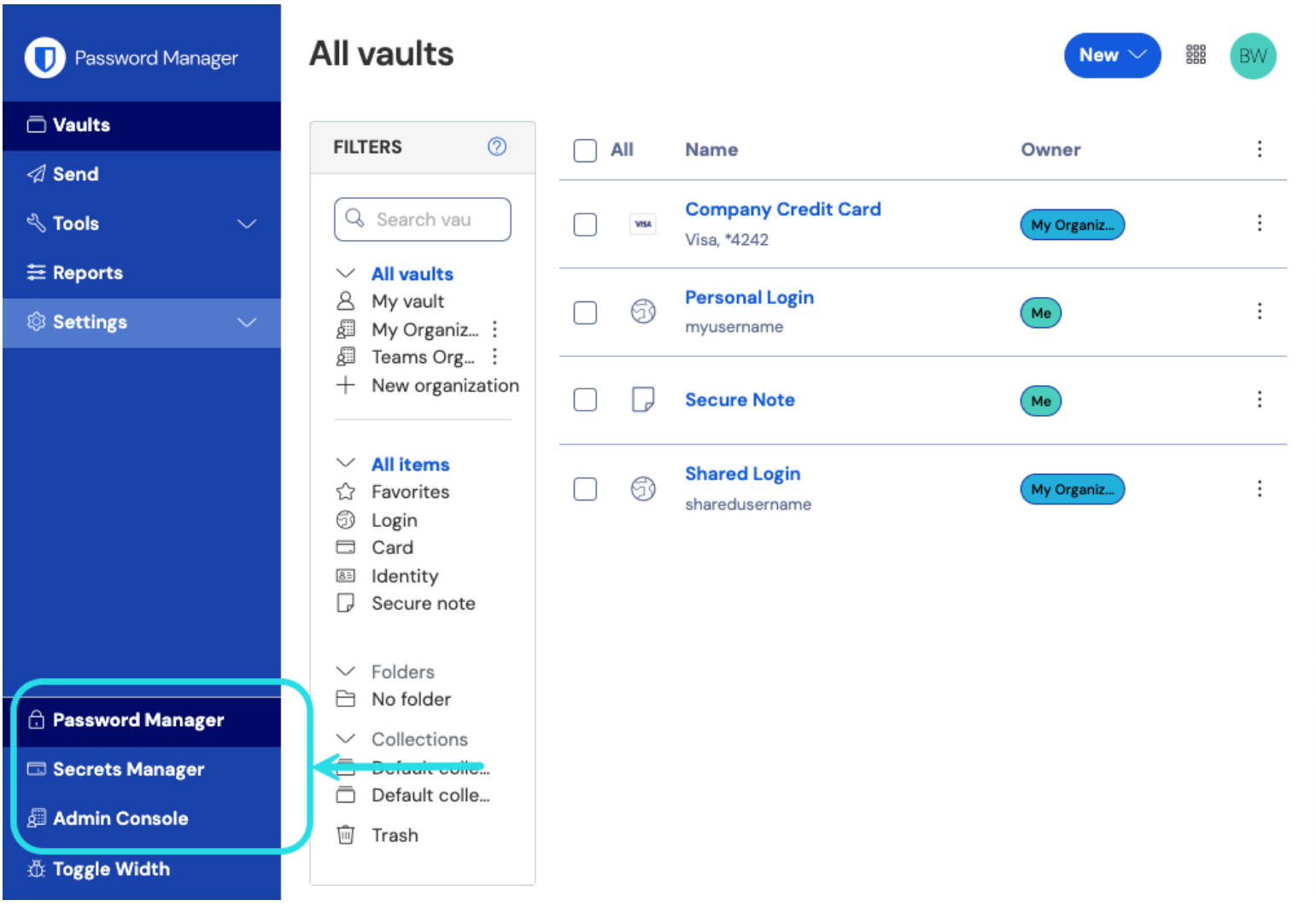
Cet article contient de l'aide **spécifique à Okta** pour configurer l'identifiant avec SSO via SAML 2.0. Pour obtenir de l'aide pour configurer l'identifiant avec SSO pour un autre IdP, reportez-vous à Configuration SAML 2.0.

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

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

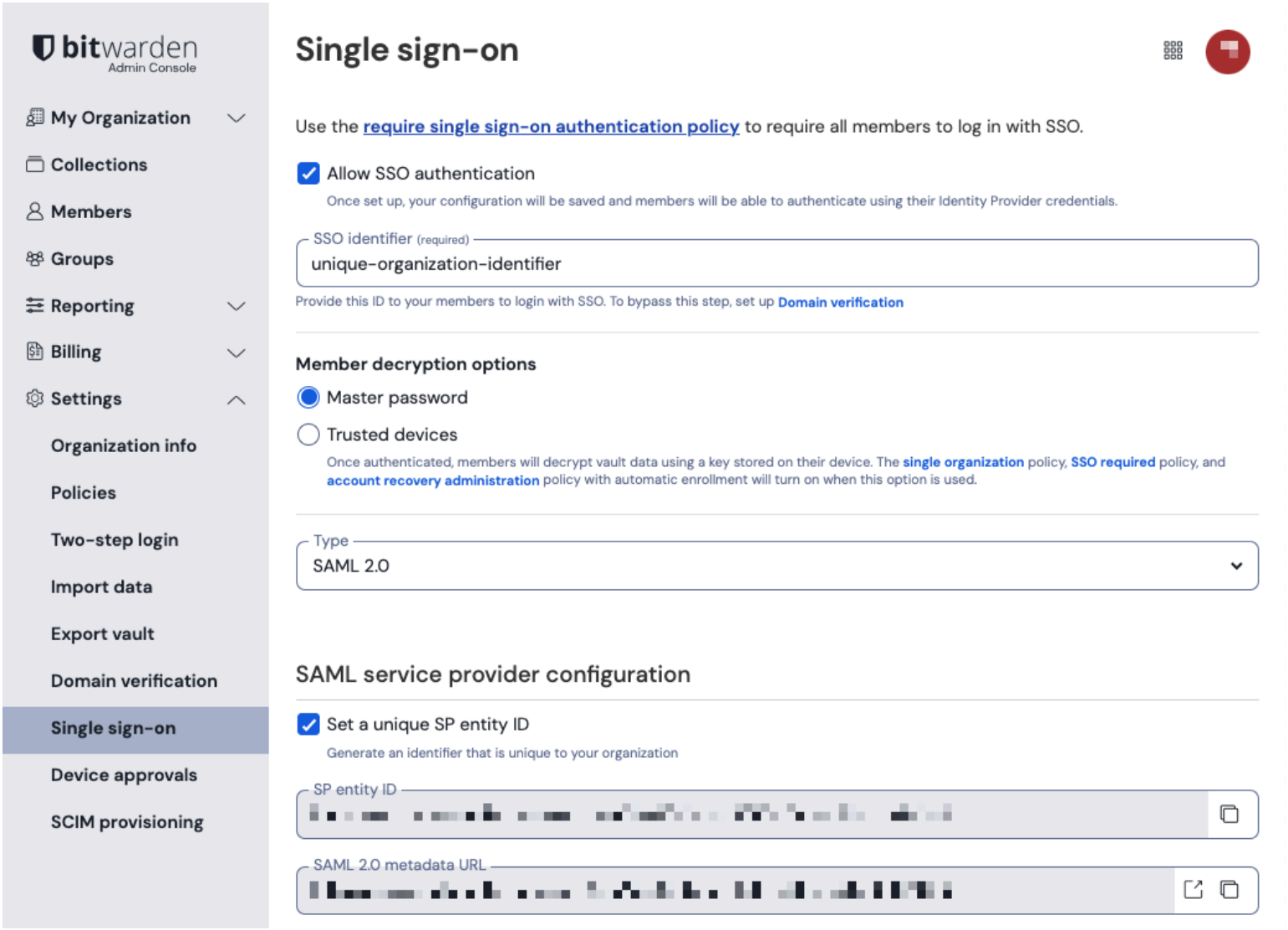
Ouvrez SSO dans l'application web

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

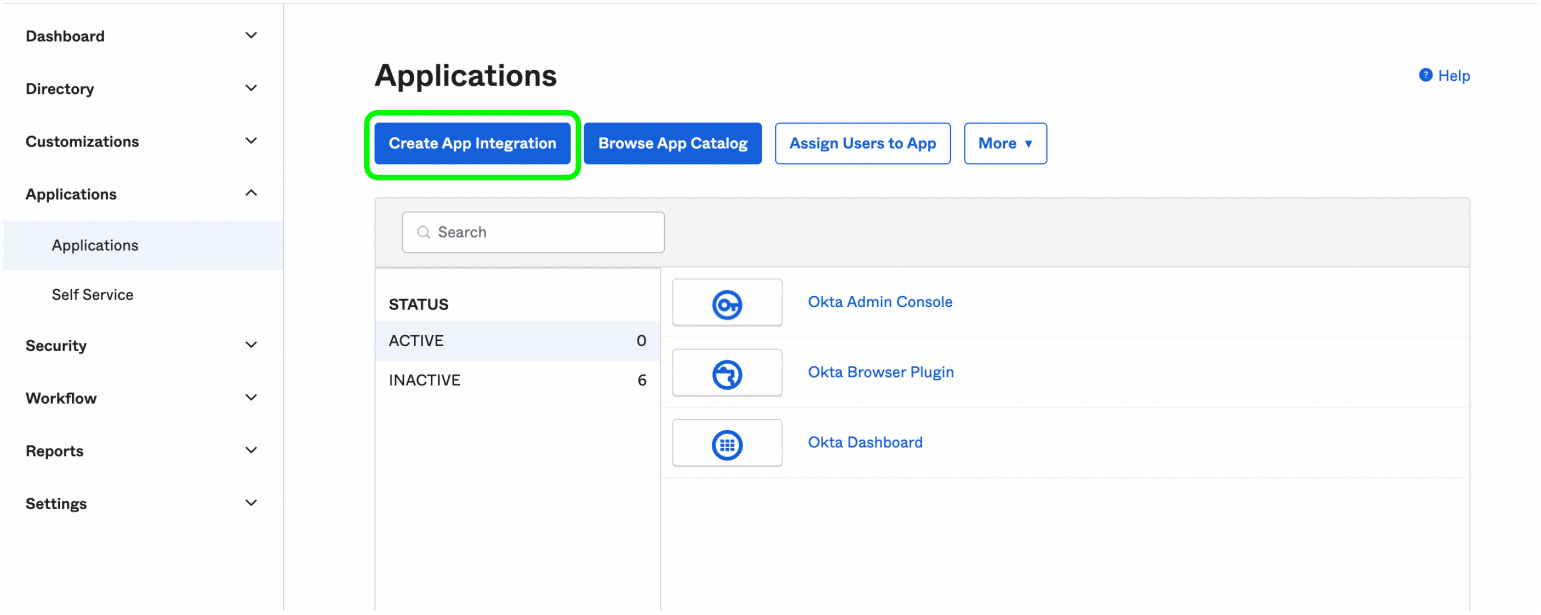
Si vous ne l'avez pas déjà fait, créez un **identifiant SSO** unique pour votre organisation et sélectionnez **SAML** dans le menu déroulant **Saisir** . Gardez cet écran ouvert pour une référence facile.

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.

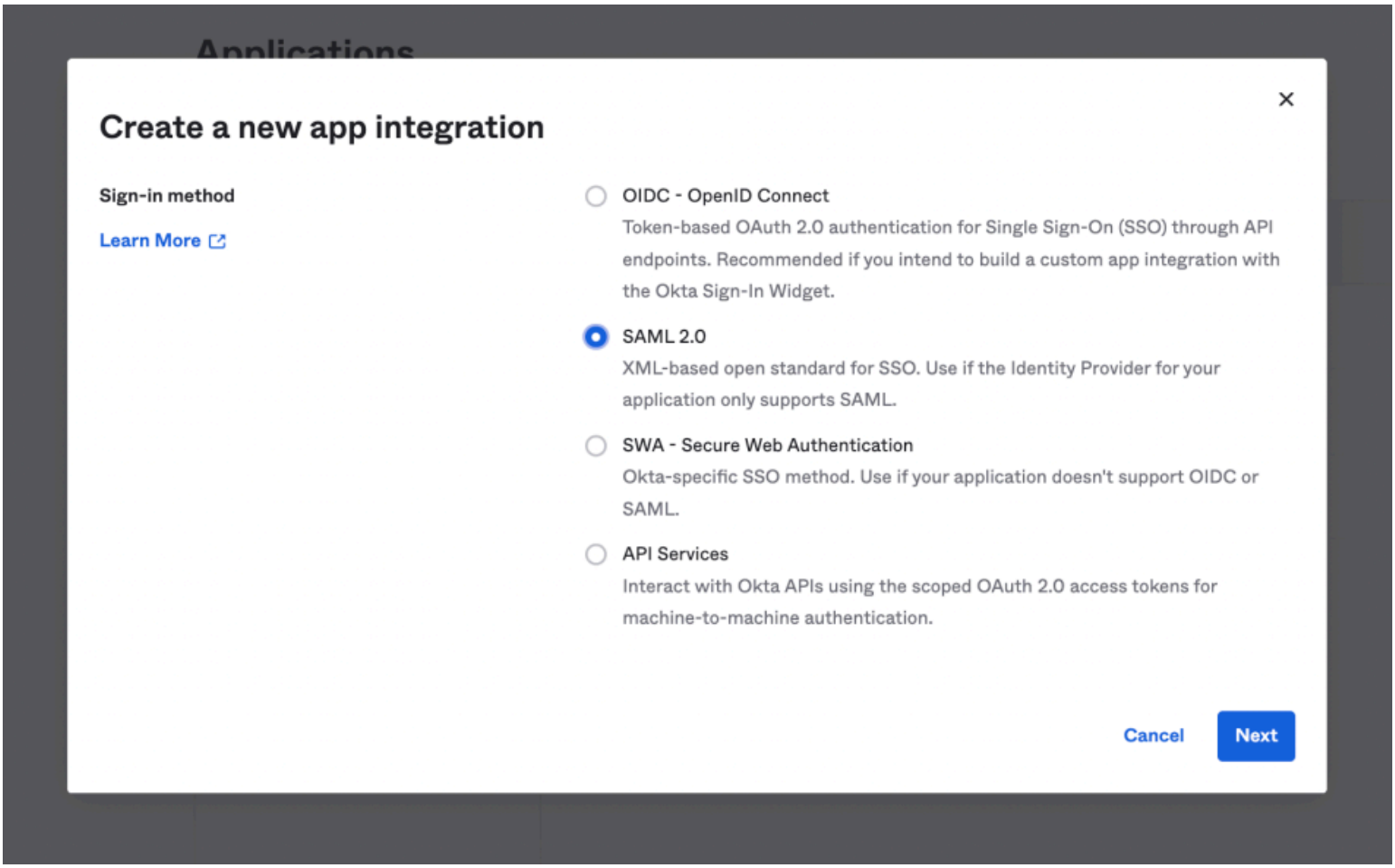
Créez une application Okta

Dans le Portail Admin Okta, sélectionnez **Applications → Applications** à partir de la navigation. Sur l'écran des Applications, sélectionnez le bouton **Créer une Intégration d'Application** :



Okta create app integration

Dans la boîte de dialogue Créer une nouvelle intégration d'application, sélectionnez le bouton radio **SAML 2.0** :



SAML 2.0 radio button

Sélectionnez le bouton **Suivant** pour passer à la configuration.

Paramètres généraux

Sur l'écran des **Paramètres Généraux**, donnez à l'application un nom unique, spécifique à Bitwarden et sélectionnez **Suivant**.

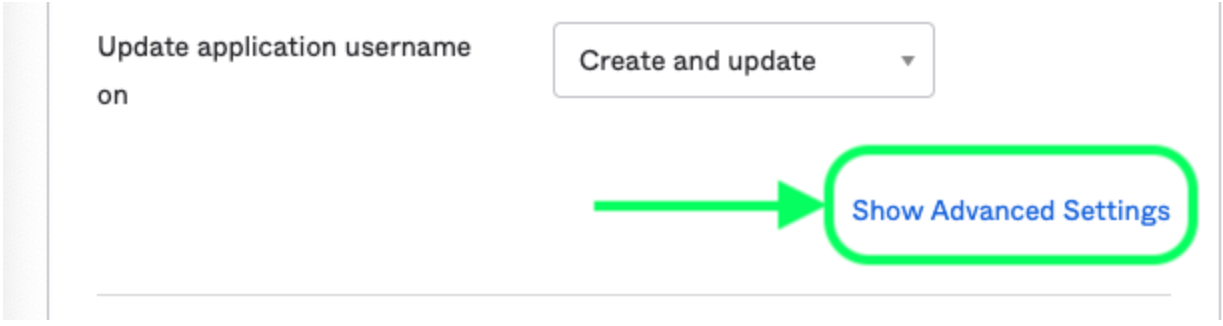
Configurer SAML

Sur l'écran **Configurer SAML**, configurez les champs suivants:

Champ	Description
URL de connexion unique	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.
URI de l'audience (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 votre organisation et variera en fonction de votre configuration.
Name ID Format	Sélectionnez le format SAML NameID à utiliser dans les assertions SAML. Par défaut, **Non spécifié**.
Nom d'utilisateur de l'application	Sélectionnez l'attribut Okta que les utilisateurs utiliseront pour se connecter à Bitwarden avec leur identifiant.

Paramètres avancés

Sélectionnez le lien **Afficher les paramètres avancés** et configurez les champs suivants:

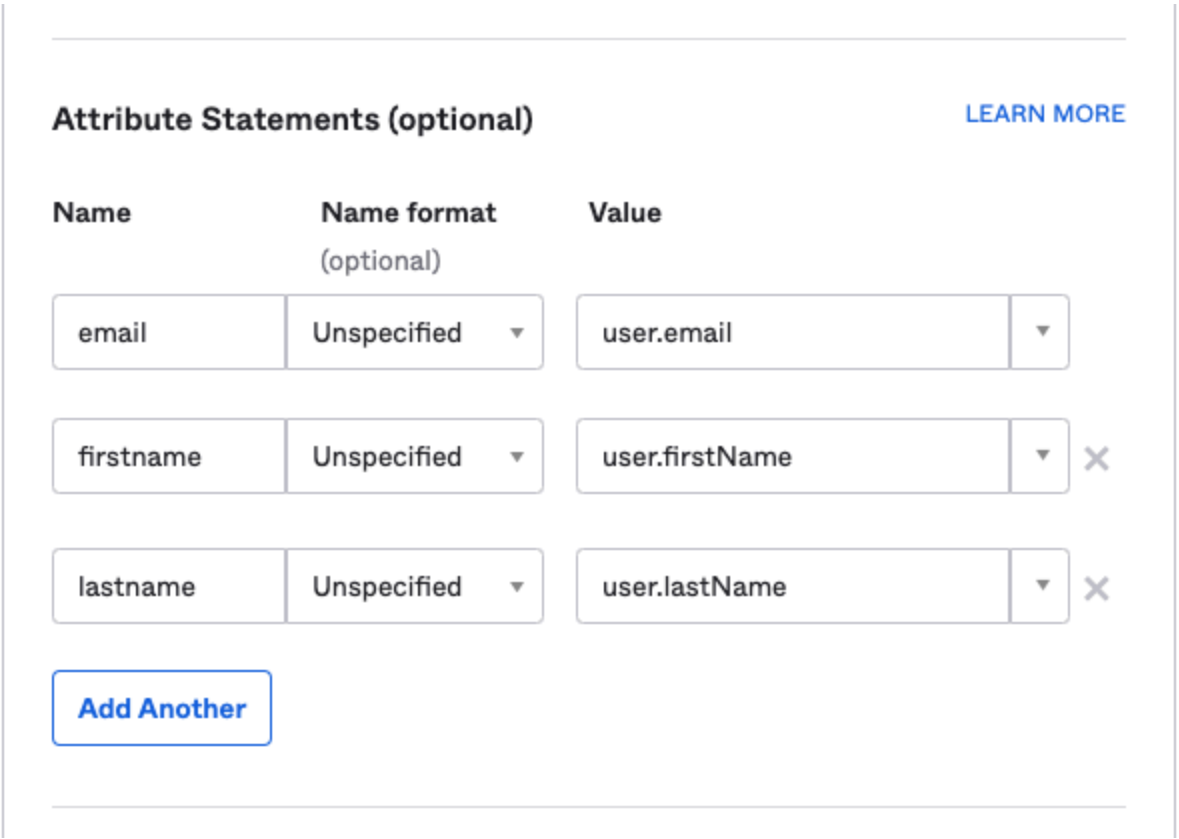


Advanced Settings

Champ	Description
Réponse	Que la réponse SAML soit signée par Okta.
Signature d'Assertion	Que l'assertion SAML soit signée par Okta.
Algorithme de Signature	L'algorithme de signature utilisé pour signer la réponse et/ou l'affirmation, selon ce qui est défini comme **Signé**. Par défaut, `rsa-sha256`.
Algorithme de Digest	L'algorithme de condensat utilisé pour signer la réponse et/ou l'assertion, selon ce qui est défini comme **Signé**. Ce champ doit correspondre à l'**Algorithme de Signature** sélectionné.

Déclarations d'attributs

Dans la section **Déclarations d'Attributs**, construisez les mappages d'attributs suivants SP → IdP :

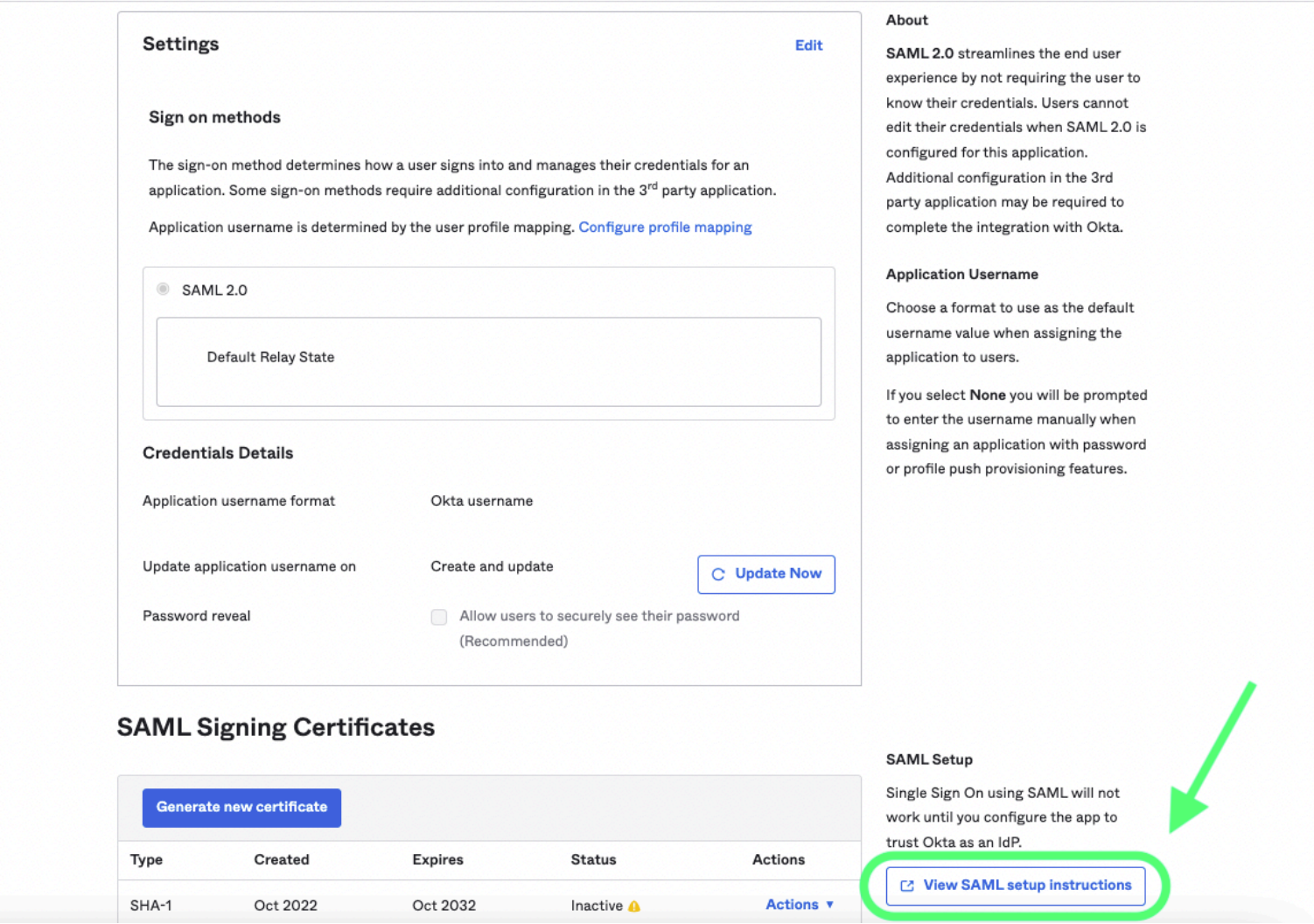


Attribute Statements

Une fois configuré, sélectionnez le bouton **Suivant** pour passer à l'écran **Commentaires** et sélectionnez **Terminer**.

Obtenir les valeurs IdP

Une fois votre application créée, sélectionnez l'onglet **Se connecter** pour l'application et sélectionnez le bouton **Afficher les instructions de configuration** situé sur le côté droit de l'écran:



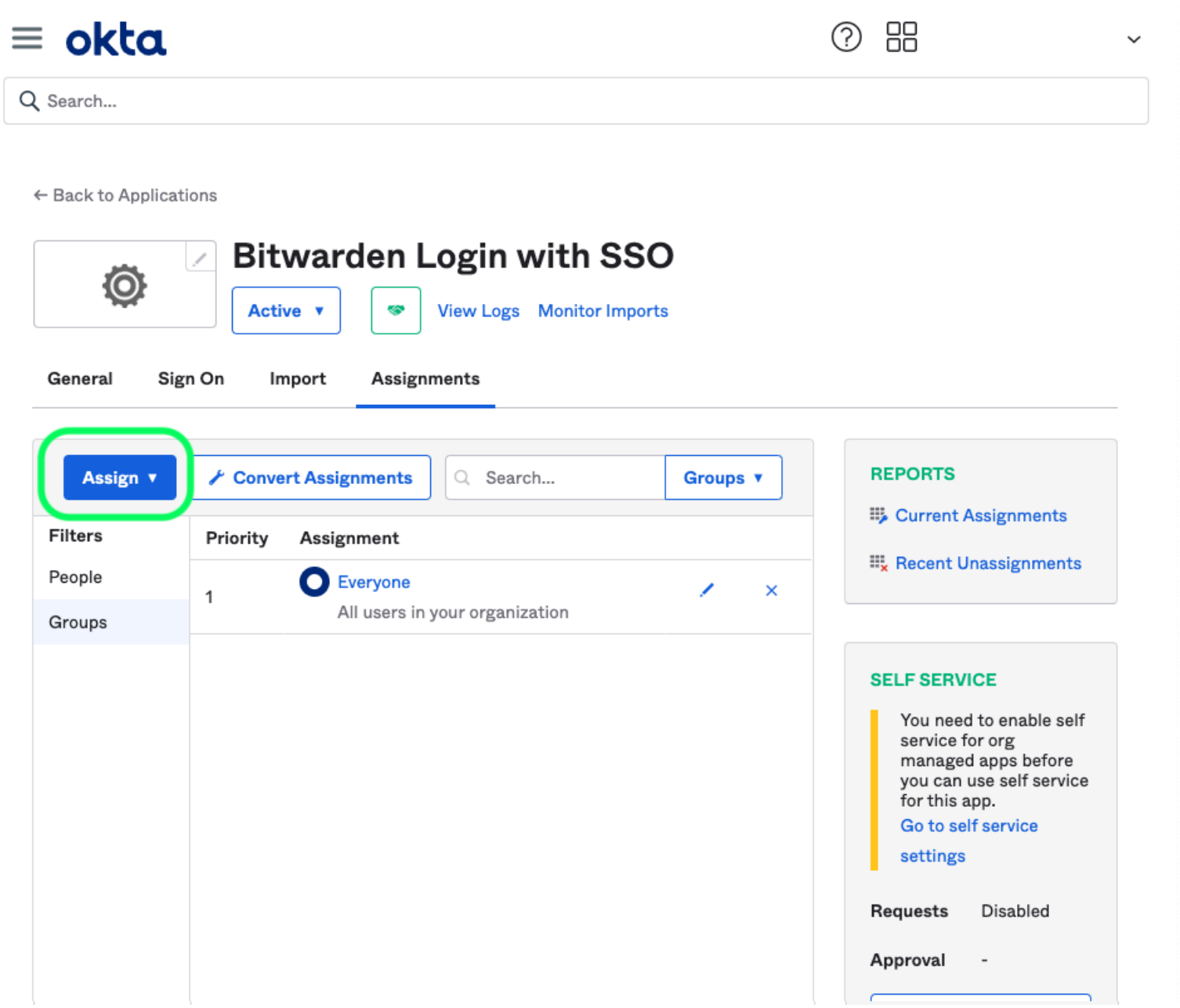
View SAML setup instructions

Laissez cette page ouverte pour une utilisation future, ou copiez l'**URL de connexion unique du fournisseur d'identité** et l'**Émetteur du fournisseur d'identité** et téléchargez le **Certificat X.509** :

IdP Values

Devoirs

Naviguez vers l'**onglet Devoirs** et sélectionnez le bouton **Attribuer** :



Assigning Groups

Vous pouvez attribuer l'accès à l'application sur une base utilisateur par utilisateur en utilisant l'option **Attribuer aux personnes**, ou en masse en utilisant l'option **Attribuer aux groupes**.

Retour à l'application web

À ce stade, vous avez configuré tout ce dont vous avez besoin dans le contexte du Portail Admin Okta. 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 à attendre pour les réponses SAML.

Configuration du fournisseur de services

Configurez les champs suivants en fonction des choix sélectionnés dans le portail admin Okta lors de la création de l'application :

Champ	Description
Format d'identifiant de nom	Définissez ceci sur le format d'ID de nom spécifié dans Okta, sinon laissez **Non spécifié**.
Algorithme de Signature Sortant	L'algorithme que Bitwarden utilisera pour signer les requêtes SAML.
Comportement de signature	Si/quand les demandes SAML seront signées.
Algorithme de Signature Minimum Entrant	Définissez ceci sur l'Algorithme de Signature spécifié dans Okta.
Voulez des Assertions Signées	Cochez cette case si vous avez défini le champ Signature d'Assertion à **Signé** dans Okta.
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 Admin Okta pour récupérer les valeurs de l'application :

Champ	Description
ID de l'entité	Entrez votre **Émetteur du Fournisseur d'Identité**, récupéré depuis l'écran des Paramètres de Connexion Okta en sélectionnant le bouton **Afficher les Instructions de Configuration**. Ce champ est sensible à la casse.
Type de Reliure	Réglé sur **Rediriger**. Okta ne prend actuellement pas en charge HTTP POST.
URL du service de connexion unique	Entrez votre **URL de connexion unique du fournisseur d'Identité**, récupérée depuis l'écran des paramètres de connexion d'Okta.
URL du service de déconnexion unique	L'identification avec SSO ne prend actuellement **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 téléchargé, 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 sélectionné lors de la configuration de l'application Okta. Si vous n'avez pas modifié l'Algorithme de Signature, laissez la valeur par défaut (`rsa-sha256`).
Autoriser les demandes de déconnexion sortantes	La connexion avec SSO ne prend actuellement **pas en charge** SLO.
Voulez-vous que les demandes d'authentification soient signées	Que Okta s'attend à ce que les demandes SAML soient signées.

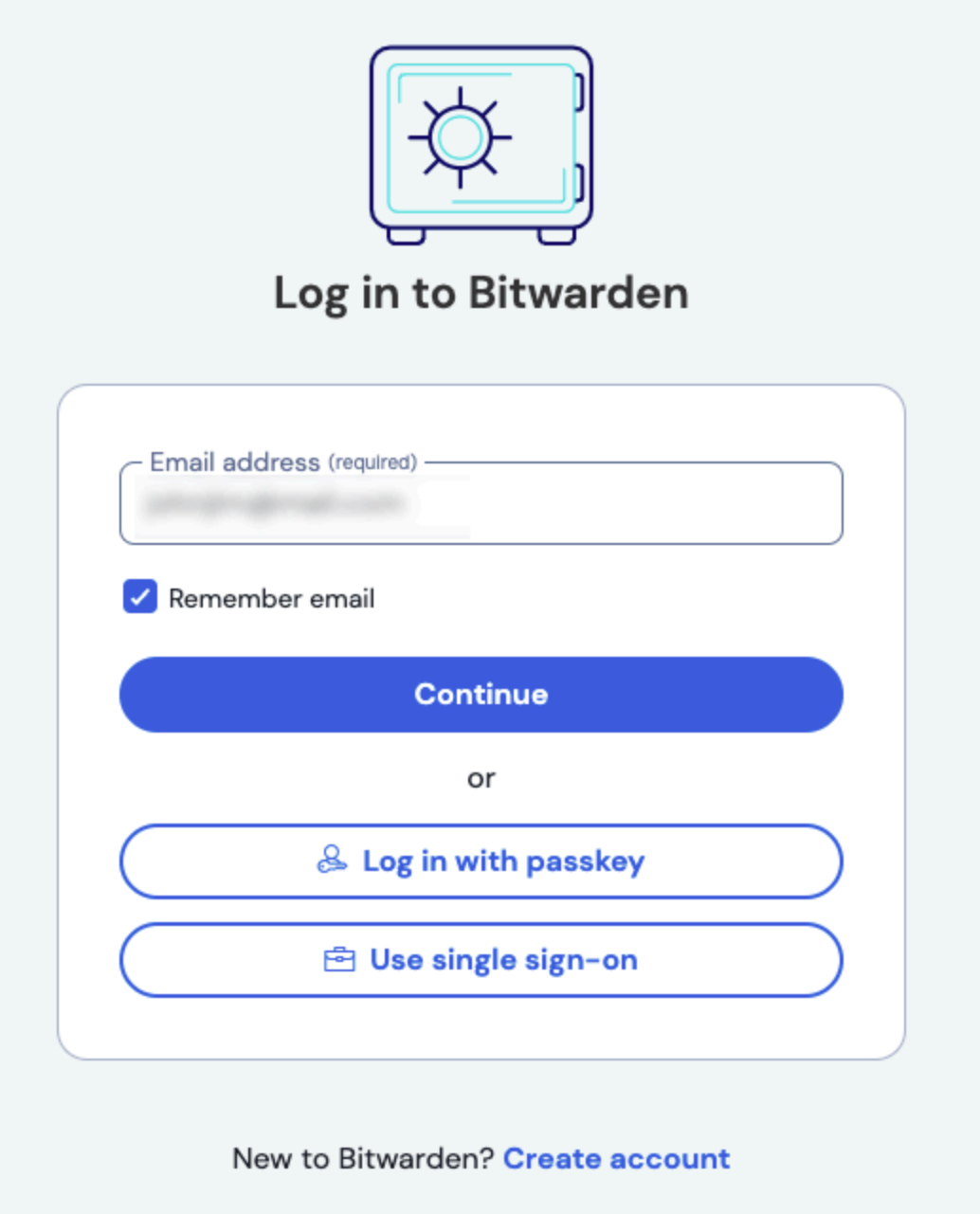
> **Note**
>
> Lors de la complétion du certificat X509, prenez note de la date d'expiration. Les certificats devront être renouvelés afin d'éviter toute interruption de service pour les utilisateurs finaux de SSO. Si un certificat a expiré, les comptes Admin et Propriétaire pourront toujours se connecter 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.

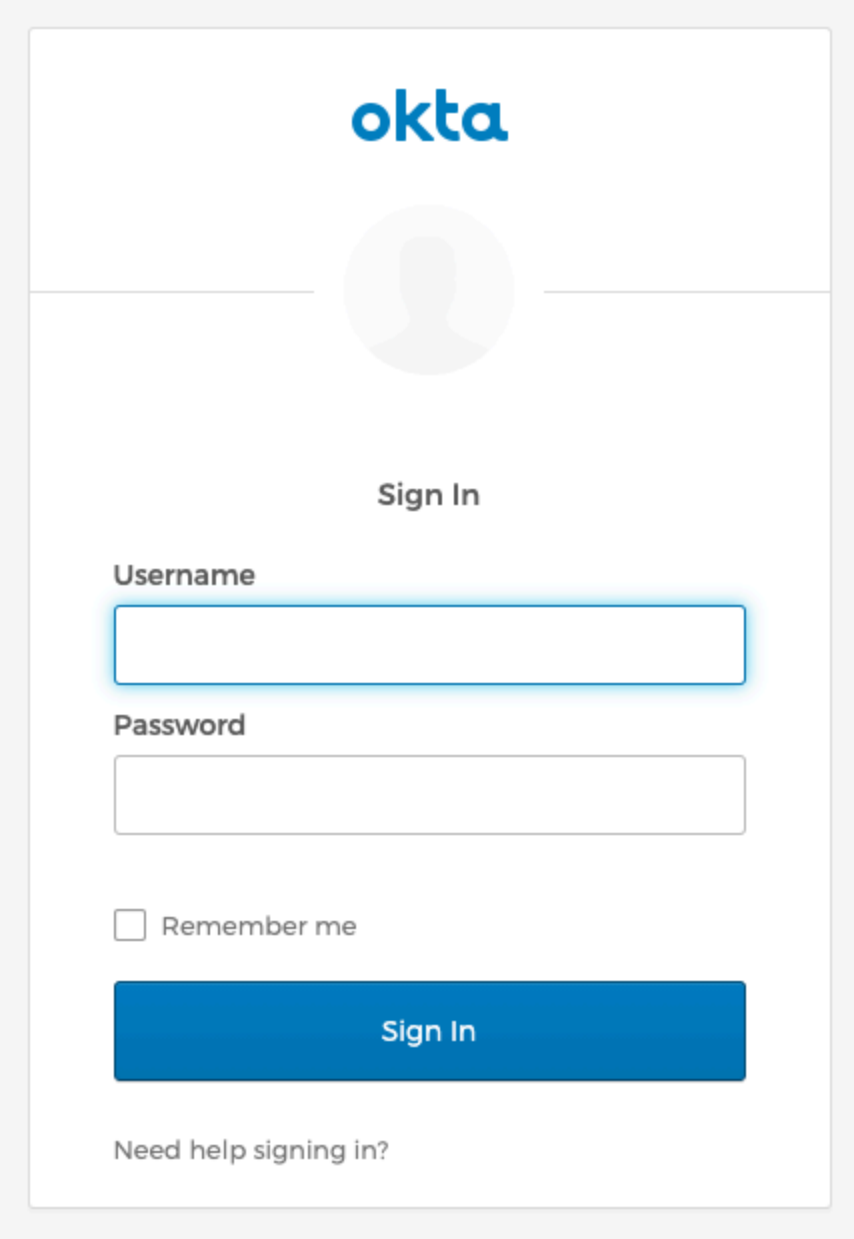
Testez la configuration

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 Okta:



Log in with Okta

Après vous être authentifié avec vos identifiants Okta, entrez votre mot de passe principal Bitwarden pour déchiffrer votre coffre !

Note

Bitwarden does not support unsolicited responses, so initiating login from your IdP will result in an error. The SSO login flow must be initiated from Bitwarden. Okta administrators can create an Okta Bookmark App that will link directly to the Bitwarden web vault login page.

1. As an admin, navigate to the **Applications** drop down located on the main navigation bar and select **Applications**.
2. Click **Browse App Catalog**.
3. Search for **Bookmark App** and click **Add Integration**.
4. Add the following settings to the application:
    1. Give the application a name such as **Bitwarden Login**.
    2. In the **URL** field, provide the URL to your Bitwarden client such as `https://vault.bitwarden.com/#/login` or `your-self-hostedURL.com`.
5. Select **Done** and return to the applications dashboard and edit the newly created app.
6. Assign people and groups to the application. You may also assign a logo to the application for end user recognition. The Bitwarden logo can be obtained here.

Once this process has been completed, assigned people and groups will have a Bitwarden bookmark application on their Okta dashboard that will link them directly to the Bitwarden web vault login page.