Mise en œuvre du SSO Zero Trust de Cloudflare

Mise en œuvre du SSO Zero Trust de Cloudflare

Cet article contient de l'aide spécifique à **Cloudflare Zero Trust** pour configurer l'identifiant avec SSO. Cloudflare Zero Trust est une plateforme de gestion d'identité et d'accès basée sur le cloud qui peut s'intégrer à plusieurs fournisseurs d'identité (IdPs). Vous pouvez également configurer des passerelles et du tunneling pour un accès sécurisé à la plateforme.

> **Note**
>
> Cloudflare Zero Trust can be configured with any IdP that operates using SAML 2.0 or OIDC SSO configurations. If you are not familiar with these configurations, refer to these articles:
>
> - SAML 2.0 Configuration
> - OIDC Configuration

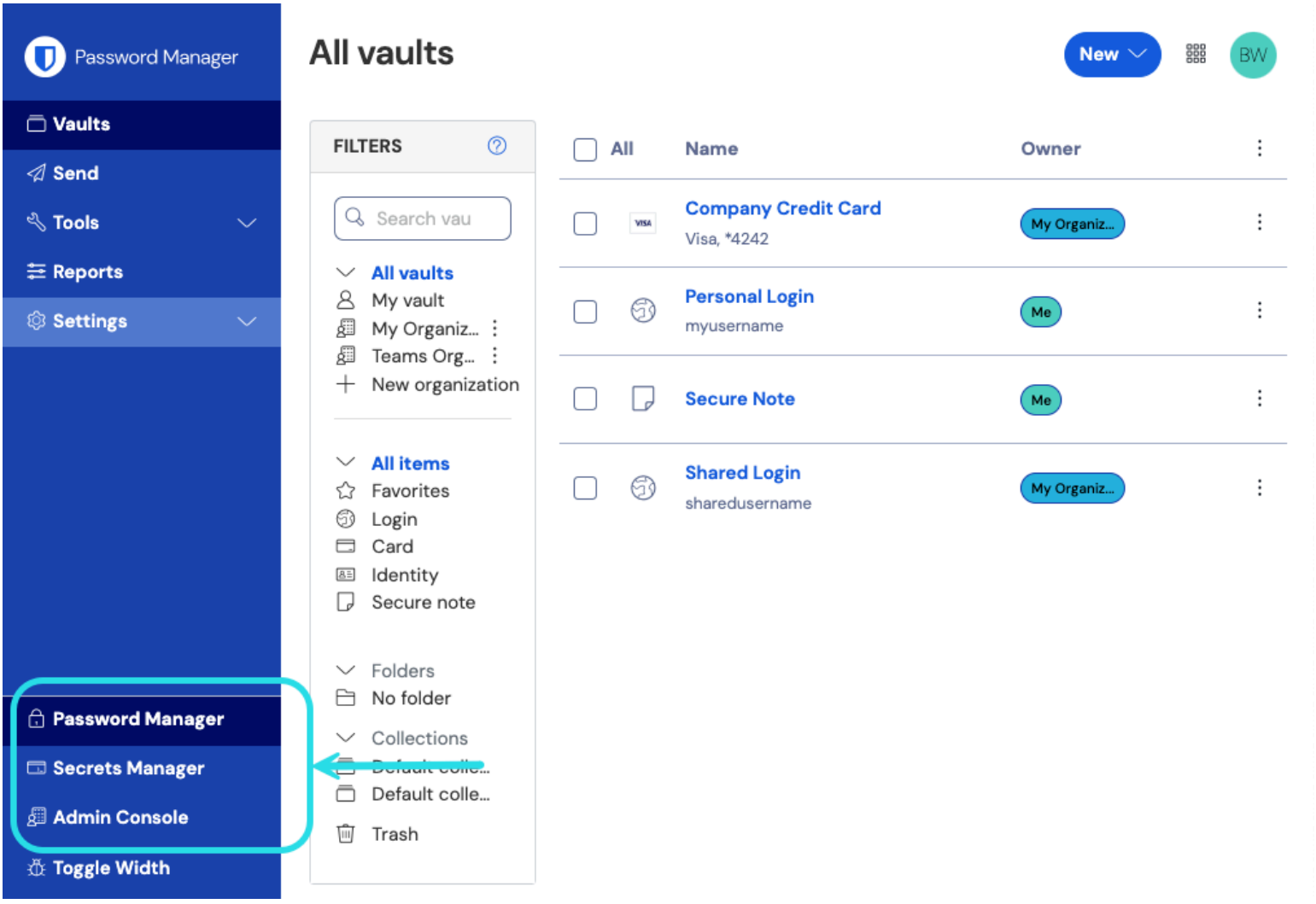
Pourquoi utiliser Cloudflare Zero Trust avec SSO ?

Cloudflare Zero Trust est une plateforme de gestion d'identité et d'accès proxy basée sur le cloud qui peut s'intégrer à plusieurs fournisseurs d'identité (IdPs). L'avantage d'utiliser Cloudflare Zero Trust en plus de votre IdP standard est sa capacité à configurer plusieurs IdP pour l'identifiant. Cloudflare Zero Trust peut fournir un accès SSO à Bitwarden depuis plusieurs organisations distinctes, ou ensembles d'utilisateurs au sein d'une organisation.

Ouvrez SSO dans l'application web

> **Note**
>
> Cloudflare will only support SAML via the Access Application Gateway. This means that the **SAML 2.0** must be selected in the Bitwarden configuration. OIDC authentication can still be configured from the IdP and Cloudflare.

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.

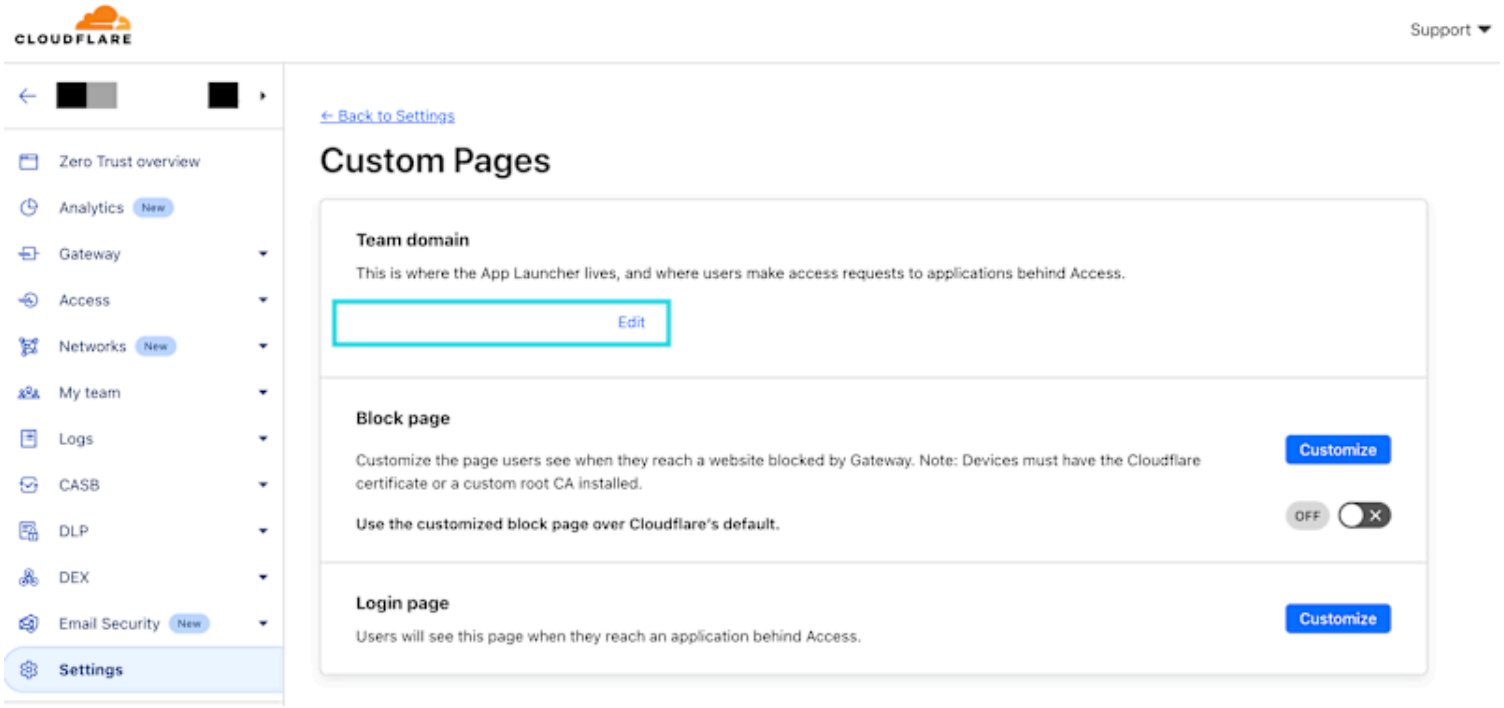
> **Tip**
>
> Il existe des options alternatives de **décryptage des membres**. Apprenez comment commencer à utiliser SSO avec des appareils de confiance ou Key Connector.

Créez une méthode d'identifiant Zero Trust de Cloudflare

Pour créer une méthode d'identifiant Zero Trust Cloufdlare :

1. Naviguez vers Cloudflare Zero Trust et connectez-vous ou créez un compte.

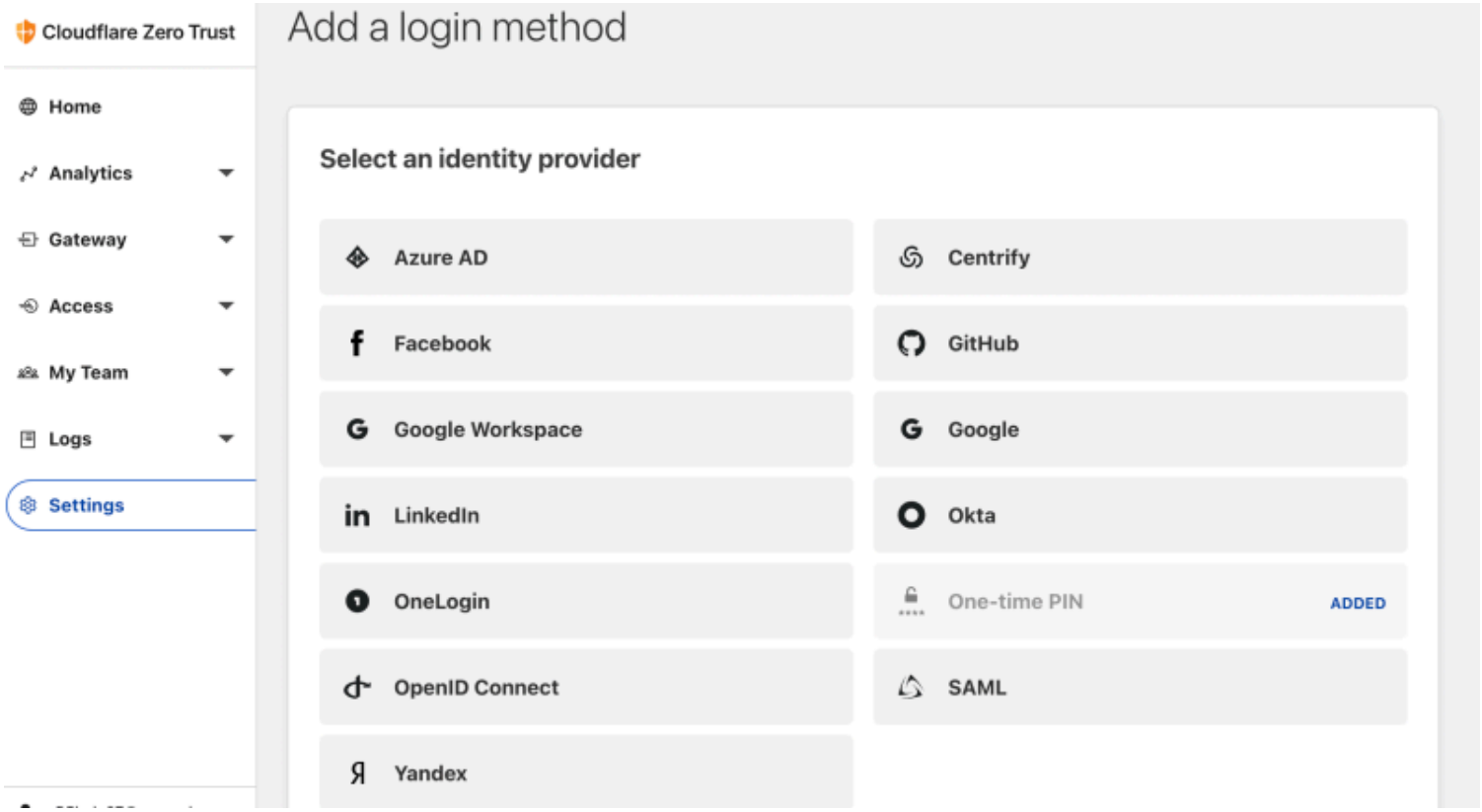
2. Configurez un domaine, qui servira d'URL utilisée par vos utilisateurs pour accéder à vos applications ou à votre **Lanceur d'Applications**, par exemple **https://my-business.cloudflareaccess.com/**. Dans le menu Cloudflare Zero Trust, sélectionnez **Paramètres → Général → Domaine d'équipe**:



Team domain setting

3. Commencez à configurer la première méthode d'identifiant en naviguant vers **Paramètres → Authentification → Ajouter nouveau.**

4. Sélectionnez la méthode d'identifiant pour vous connecter à Cloudflare Zero Trust. Si l'IdP que vous utilisez n'est pas présent sur la liste des IdP, utilisez les options génériques SAML ou OIDC. Dans cet article, Okta sera utilisé comme exemple :



Cloudflare Zero Trust IdP list

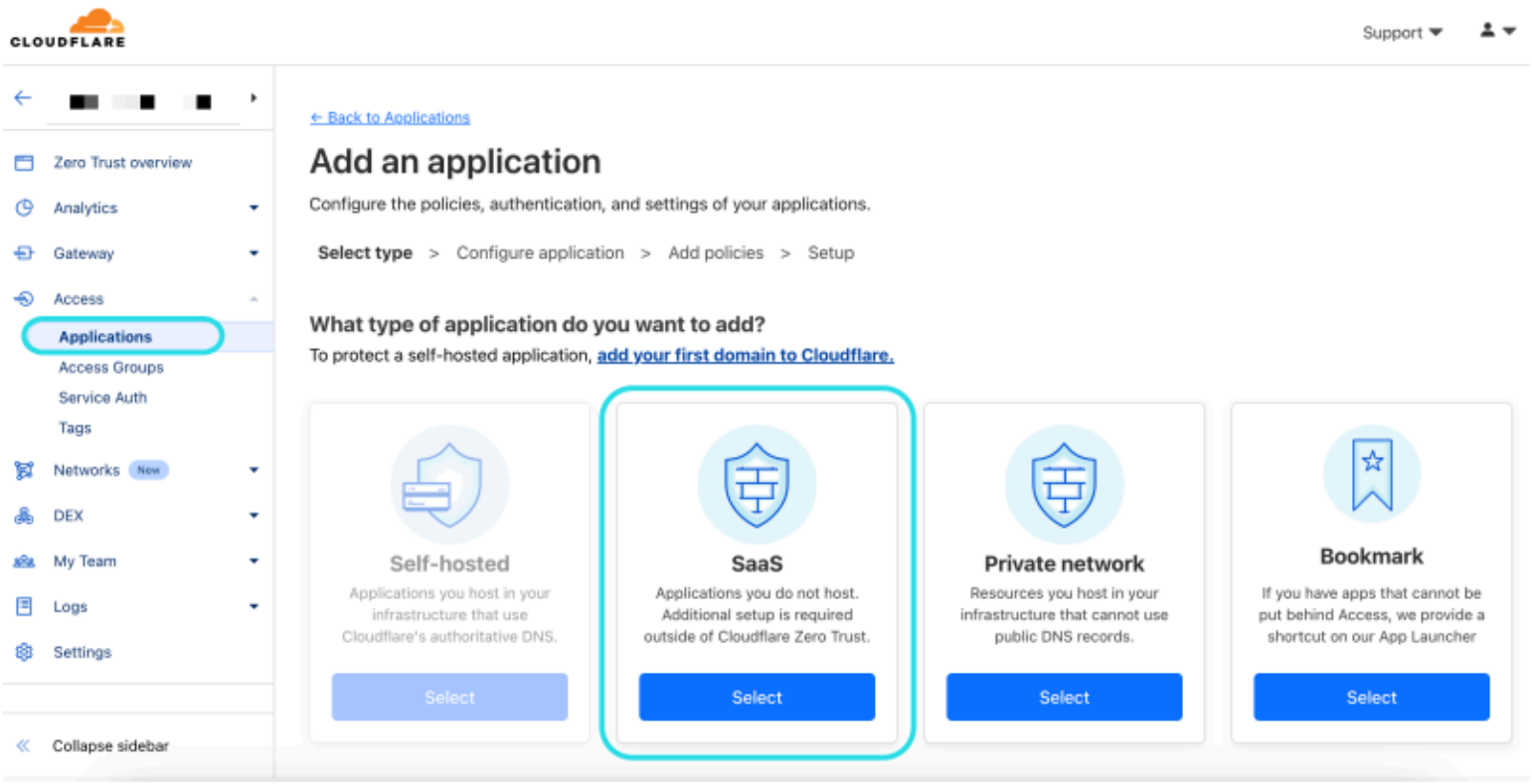
5. Après avoir sélectionné votre méthode d'identifiant IdP choisie, suivez le guide produit fourni par Cloudflare pour intégrer votre IdP.

> **Note**
> If the IdP you are using has a **support groups** feature, this option must be **disabled**. Bitwarden does not support group based claims, enabling this option will result in an XML element error on the Bitwarden end.

Créez une application Cloudflare Zero Trust

Après avoir configuré un IdP, vous devrez créer une application Cloudflare Zero Trust pour Bitwarden. **Dans cet exemple, nous allons créer une application SAML**:

1. Naviguez vers **Accès → Applications → Ajouter une application**.



CFZT add an application

2. Sélectionnez le type **SaaS**.

3. Dans le coffre web de Bitwarden, ouvrez votre organisation et naviguez vers l'écran **Paramètres → Connexion unique**. Utilisez les informations du coffre web pour remplir les informations sur l'écran **Configurer l'application** :

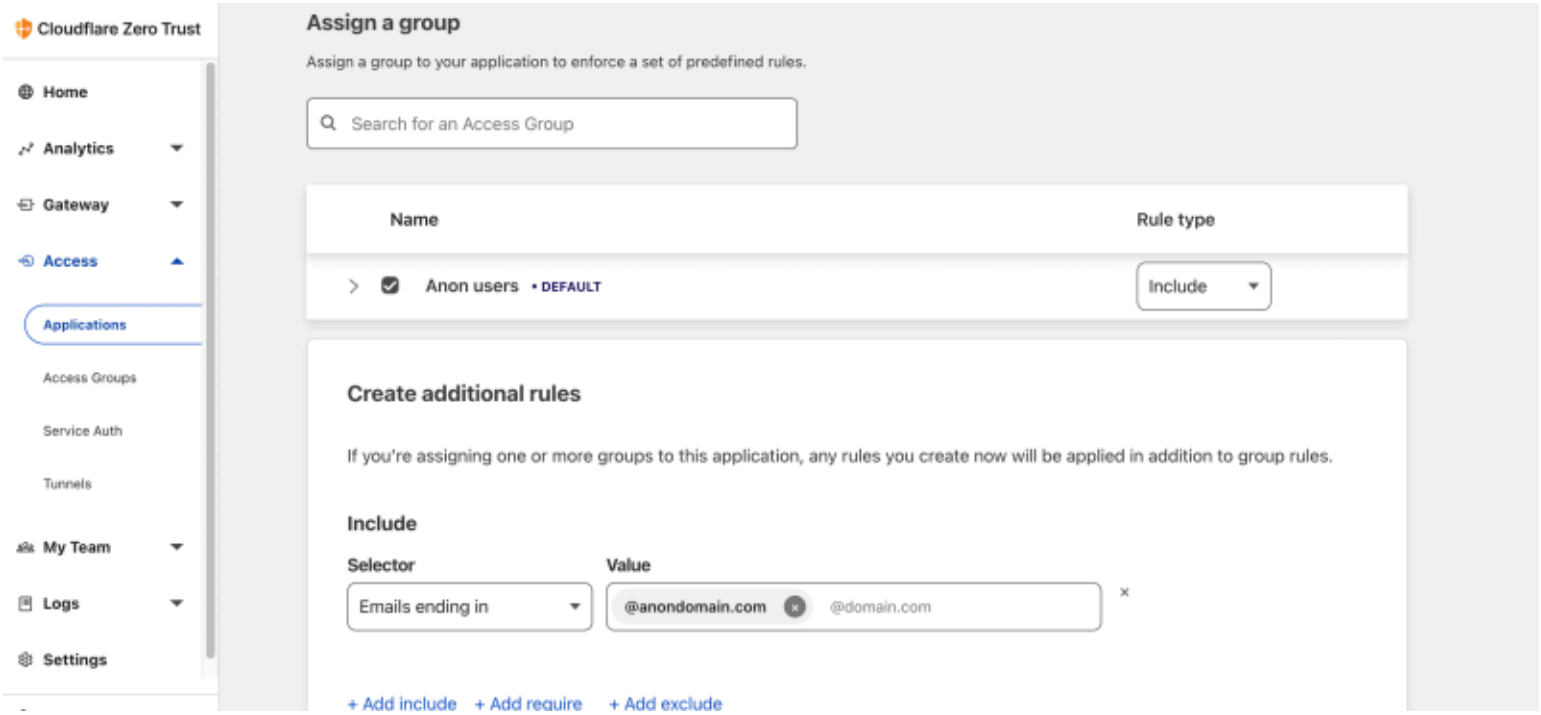
Clé	Description
Application	Entrez `Bitwarden`.
ID de l'entité	Copiez le **ID de l'entité SP** de la page Bitwarden Single Sign-On dans ce champ.
URL du service de consommation d'assertion	Copiez l'**URL du service de consommation d'assertion (ACS)** de la page Bitwarden Single Sign-On dans ce champ.
Format d'identifiant de nom	Sélectionnez **Courriel** dans le menu déroulant.

> **Note**
> For the generic OIDC configuration, the Auth URL, Token URL, and Certificate URL can be located with the well-known URL.

4. Faites défiler jusqu'au menu **Fournisseurs d'Identité**. Sélectionnez le(s) IdP que vous avez configuré(s) dans la section précédente, faites défiler vers le haut et sélectionnez **Suivant.**

5. Ensuite, créez des politiques de sécurité pour l'accès des utilisateurs à l'application. Complétez les champs **Nom de la politique**, **Action**, et **Durée de la session** pour chaque politique de sécurité.

6. Vous pouvez choisir d'attribuer une stratégie de groupe (**Accès → Groupes**) ou des règles de stratégie utilisateur explicites (telles que les e-mails, « e-mails se terminant par », « pays » ou « tout le monde »). Dans l'exemple suivant, le groupe "Anon Users" a été inclus dans la politique de sécurité. Une règle supplémentaire a également été ajoutée pour inclure les courriels se terminant dans le domaine choisi :



CFZT app policy

> **Note**
> You can also apply user access through the **App Launcher** for access to the Bitwarden login with SSO shortcut. This can be managed by navigating to **Authentication → App Launcher → Manage**. The application policies in the above example can be duplicated or generated here.

7. Une fois les politiques de sécurité configurées, faites défiler jusqu'en haut et sélectionnez **Suivant**.

8. Sur l'écran de **Configuration**, copiez les valeurs suivantes et saisissez-les dans leurs champs respectifs sur la page **Single Sign-On** de Bitwarden :

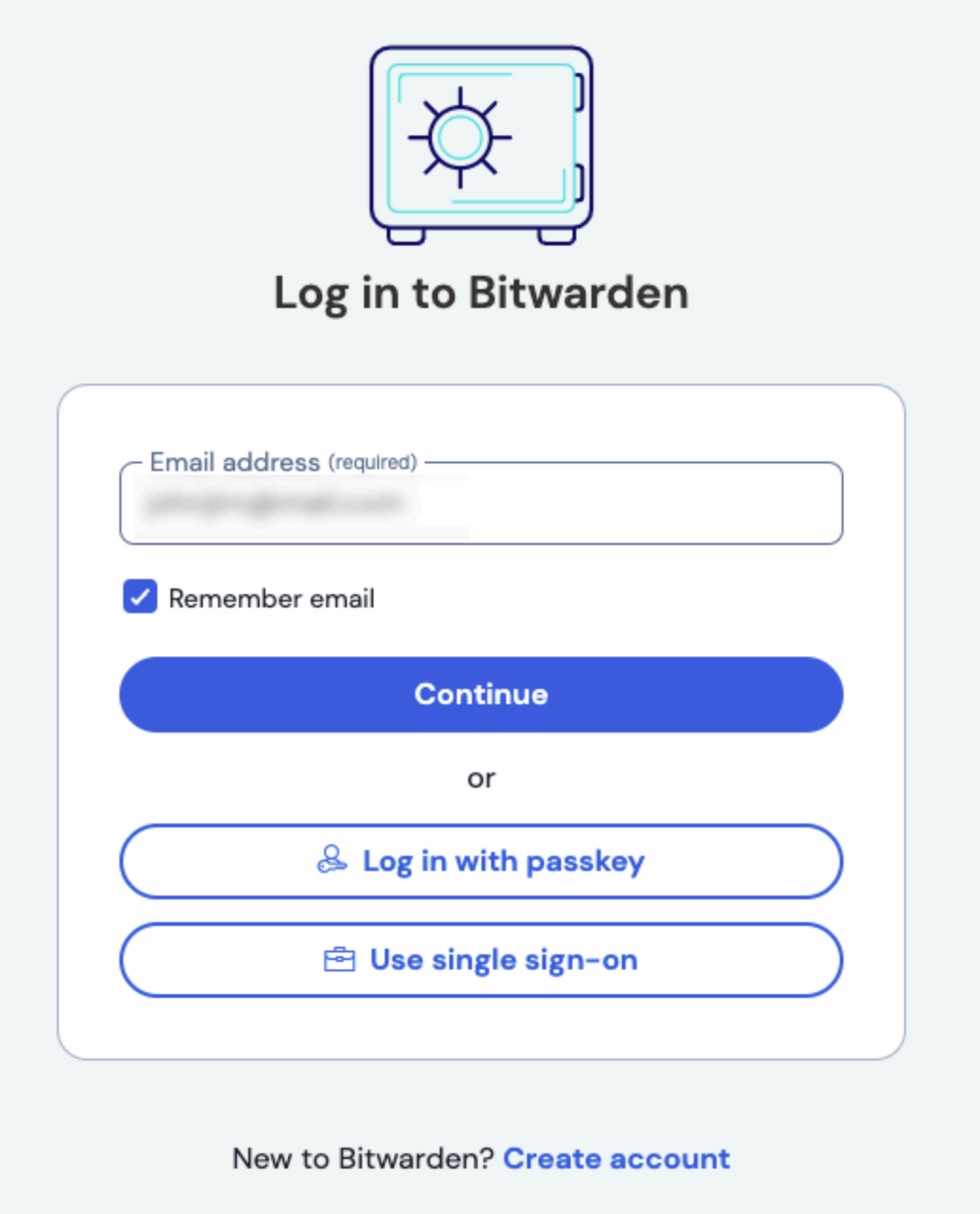
Clé	Description
Point de terminaison SSO	Le point de terminaison SSO indique où votre application SaaS va envoyer les demandes d'identifiant. Cette valeur sera entrée dans le champ **URL du Service de Connexion Unique** dans Bitwarden.
Accéder à l'ID de l'entité ou à l'émetteur	L'ID de l'entité d'accès ou l'émetteur est l'identifiant unique de votre application SaaS. Cette valeur sera entrée dans le champ **ID de l'entité** sur Bitwarden.
Clé publique	La clé publique est le certificat d'accès public qui sera utilisé pour vérifier votre identité. Cette valeur sera entrée dans le champ **Certificat Public X509** sur Bitwarden.

9. Après avoir entré les valeurs dans Bitwarden, sélectionnez **Enregistrer** sur l'écran Bitwarden Single Sign-On et sélectionnez **Terminé** sur la page Cloudflare pour enregistrer l'application.

10. Pour créer un signet vers l'écran d'identifiant Bitwarden avec SSO, sélectionnez **Ajouter une application → Signet**. Vérifiez que le Signet est visible dans le **Lanceur d'application**.

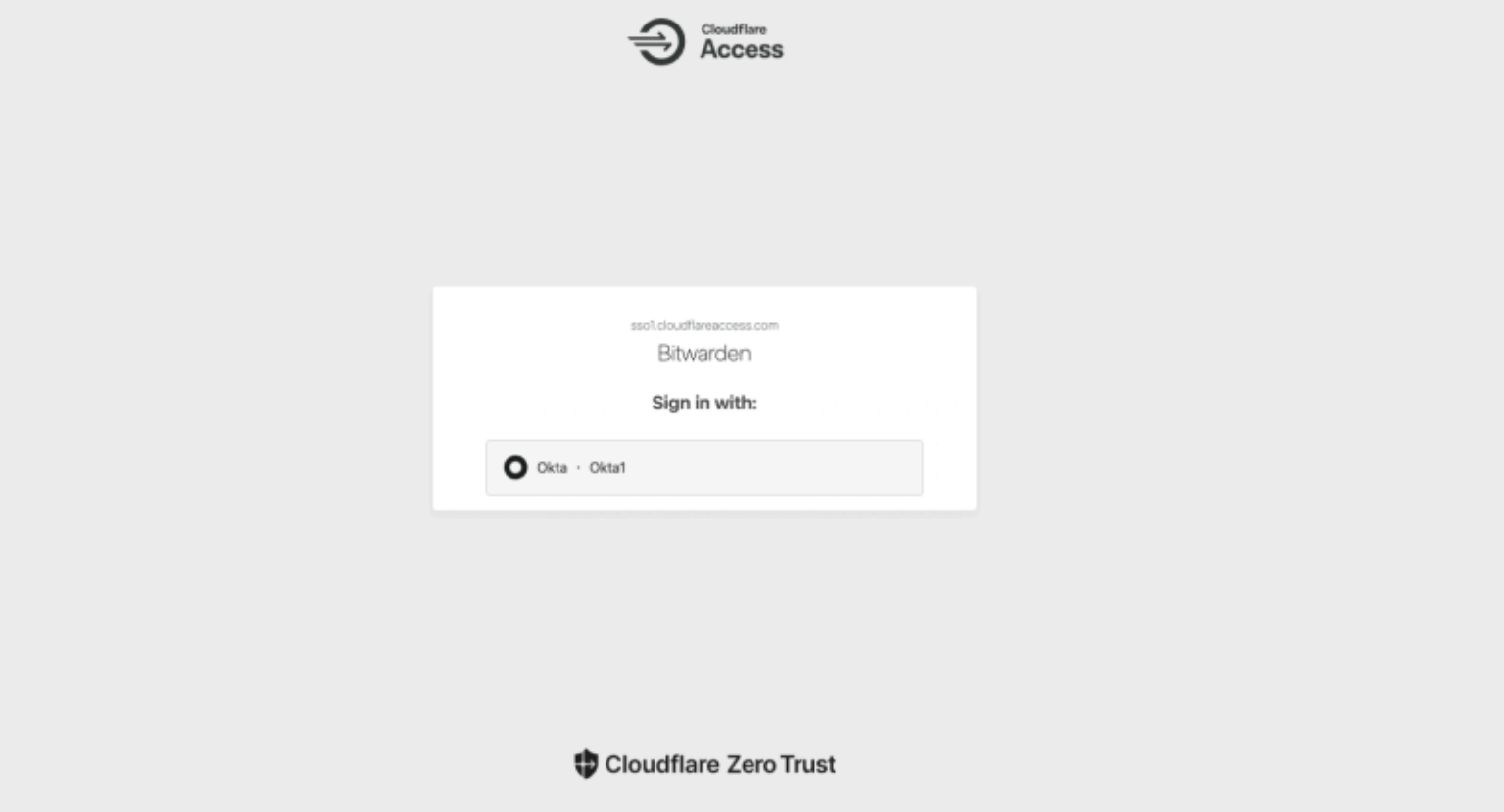
Testez la configuration

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** .



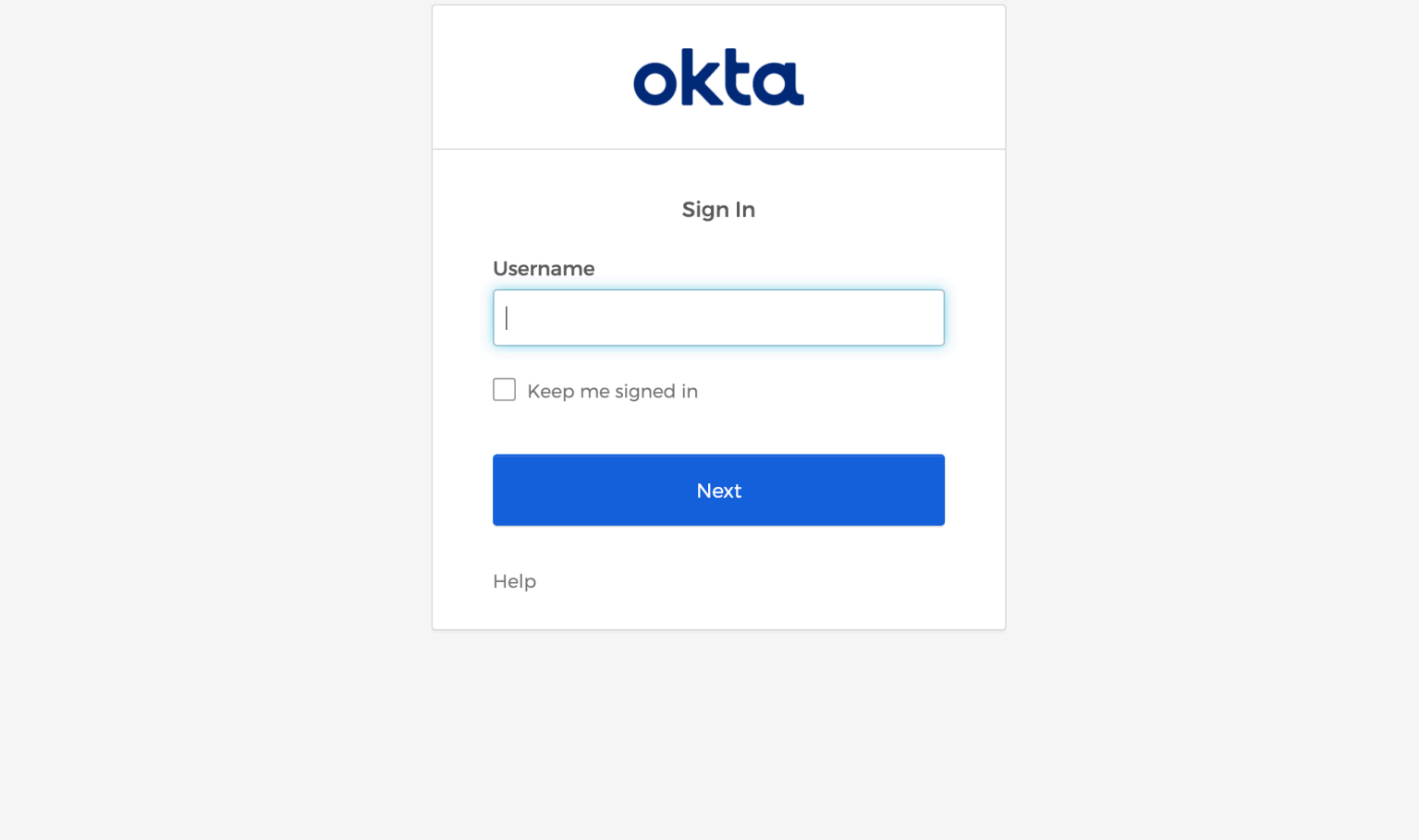
Connexion unique d'entreprise et mot de passe principal

Entrez l'identifiant de l'organisation configurée et sélectionnez **Se connecter**. Si votre mise en œuvre est correctement configurée, vous serez redirigé vers un écran d'accès Cloudflare, où vous pouvez sélectionner l'IdP pour vous connecter avec l'identifiant :



Cloudflare IdP selection

Après avoir sélectionné votre IdP, vous serez dirigé vers la page d'identifiant de votre IdP. Entrez les informations utilisées pour vous connecter via votre IdP :



CFZT IdP login

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