bitwarden | Article du Centre d'Aide

CONSOLE ADMIN > IDENTIFIEZ-VOUS AVEC SSO >

Implémentation SAML de Keycloak

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

Implémentation SAML de Keycloak

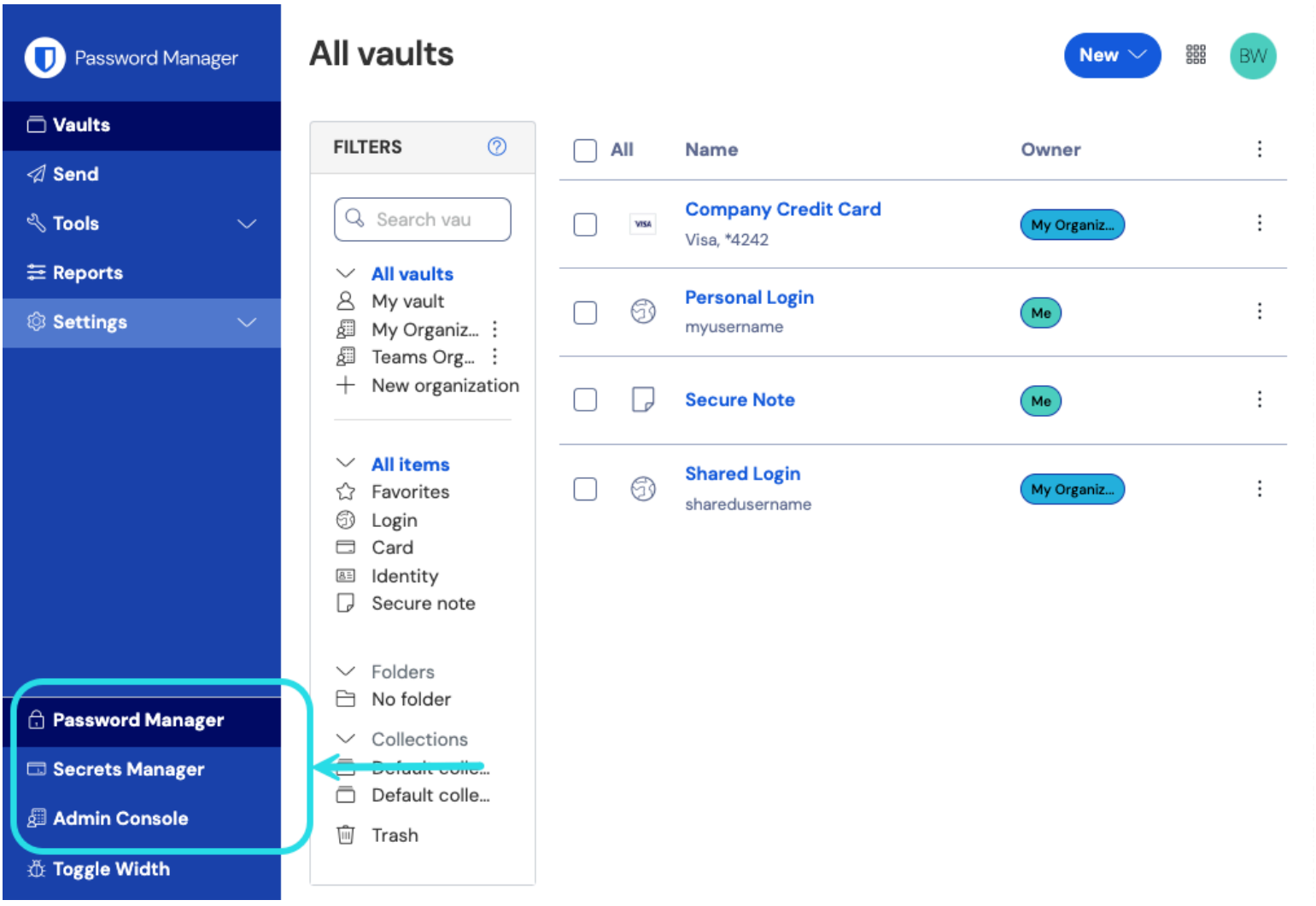
Cet article contient de l'aide **spécifique à Keycloak** pour configurer l'identifiant avec SSO via SAML 2.0. Pour obtenir de l'aide pour configurer l'identifiant avec SSO pour un autre IdP, reportez-vous à Configuration SAML 2.0.

La configuration implique de travailler simultanément avec l'application web Bitwarden et le portail Keycloak. 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

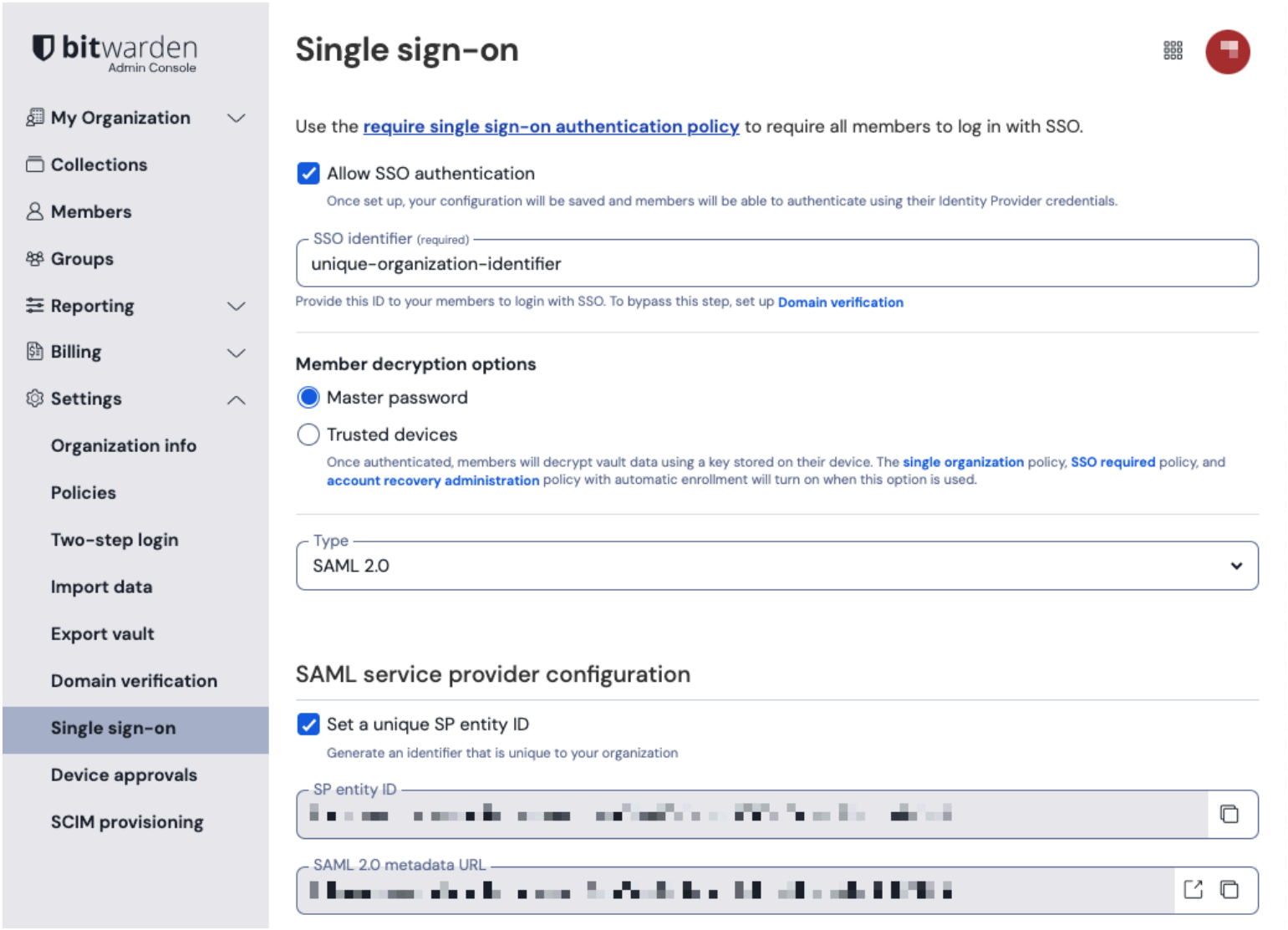
Ouvrez SSO dans l'application web

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 → Authentification unique** de votre organisation :



Configuration SAML 2.0

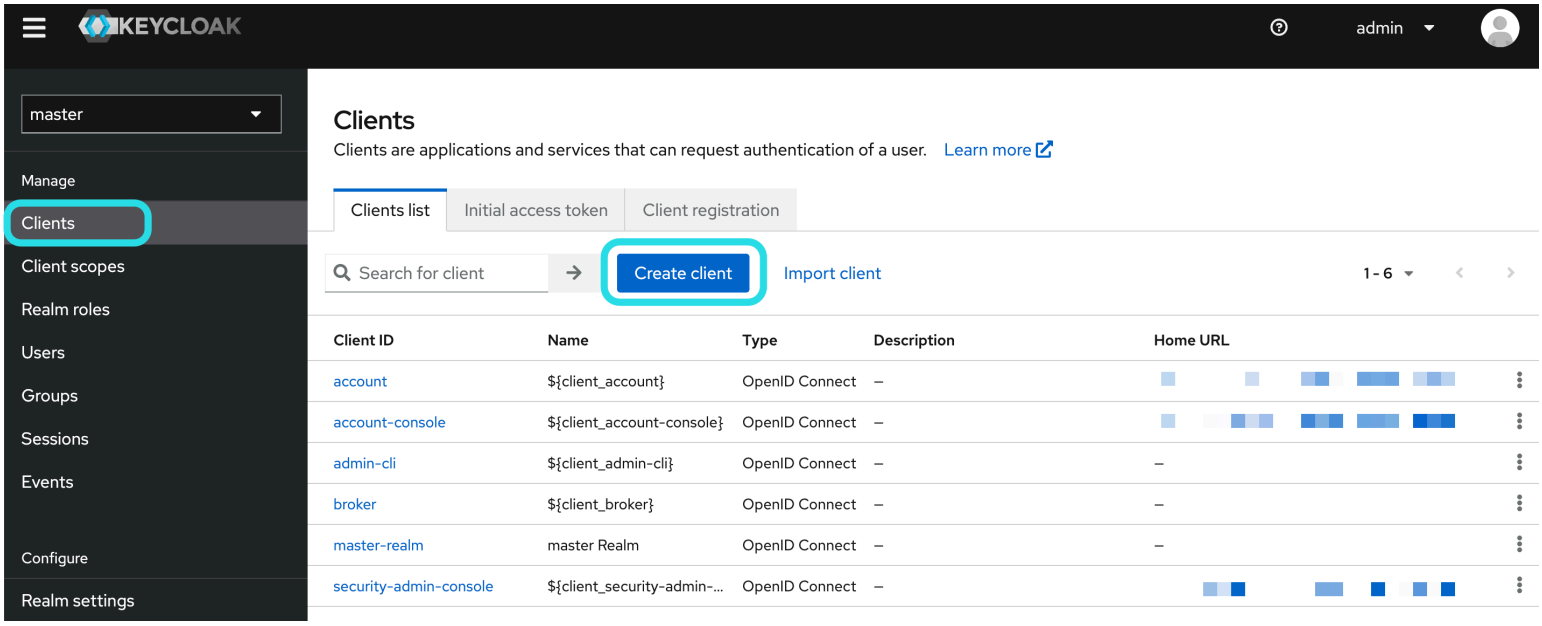
Si vous ne l'avez pas déjà fait, créez un **identifiant SSO** unique pour votre organisation et sélectionnez **SAML** dans le menu déroulant **Saisir**. Gardez cet écran ouvert pour une référence facile.

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.

Configuration de Keycloak

Connectez-vous à Keycloak et sélectionnez **Clients → Créer un client**.



Create a Client

Sur l'écran Créer un client, remplissez les champs suivants :

Champ	Description
Type de client	Sélectionnez SAML.
Client ID	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.
Nom	Entrez un nom de votre choix pour le client Keycloak.

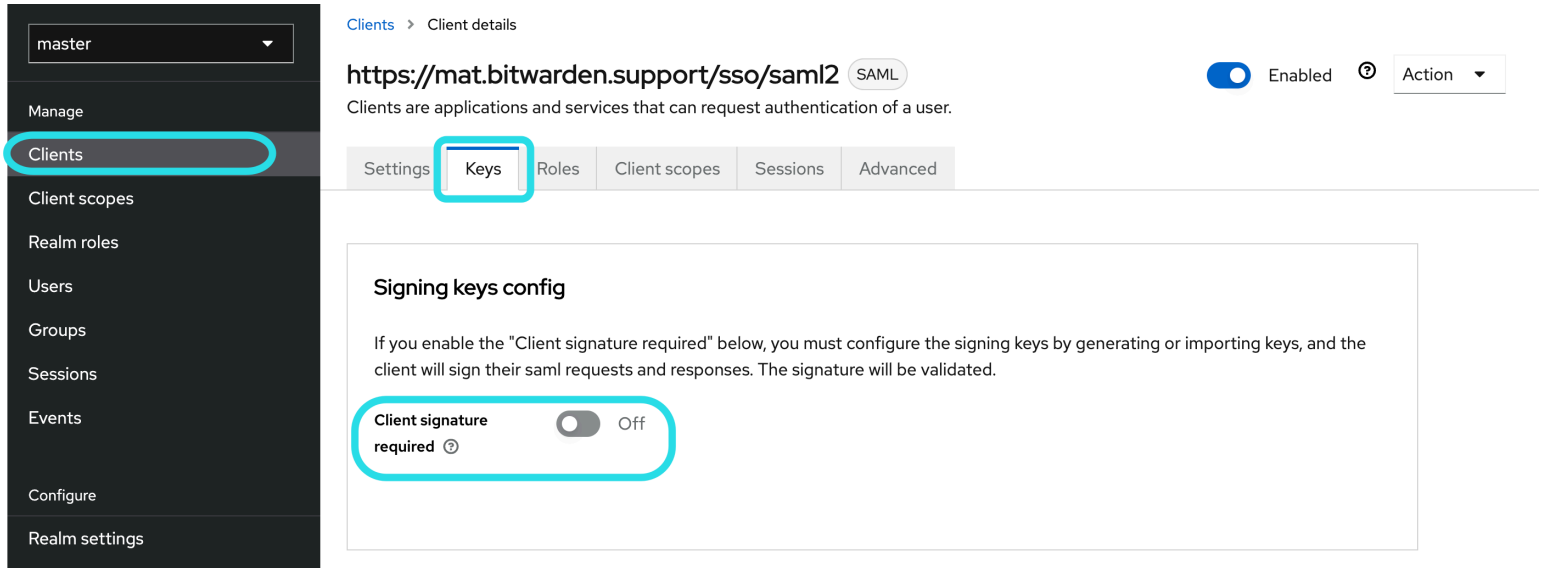
Une fois que vous avez rempli les champs requis sur la page des **Paramètres Généraux**, cliquez sur **Suivant**.

Sur l'écran des **paramètres d'identifiant**, remplissez le champ suivant :

Champ	Description
URIs de redirection valides	Définissez ce champ sur l'URL **du Service de Consommation d'Assertion (ACS)** pré-générée. 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.

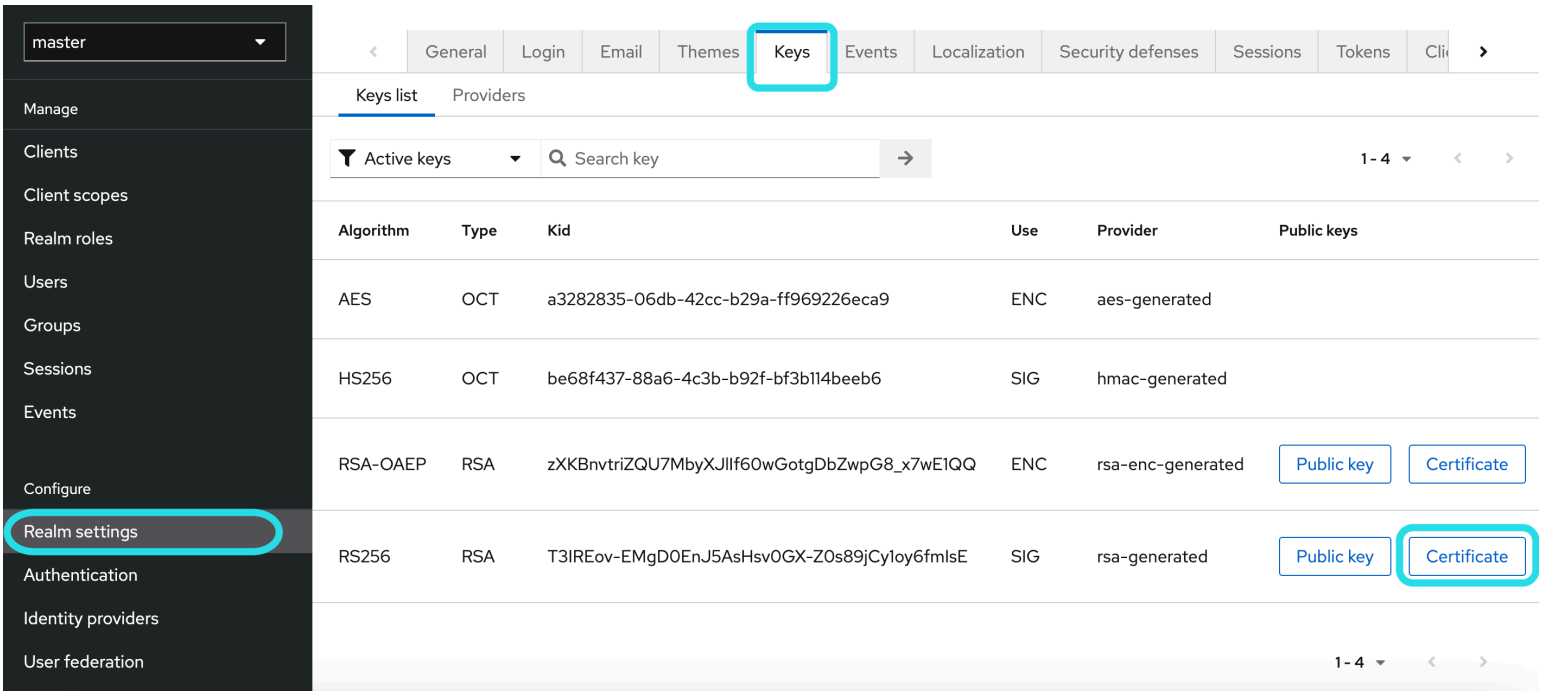
Sélectionnez **Enregistrer**.

Sélectionnez l'onglet Clés et basculez l'option **Signature du client requise** sur **Off**.



Keycloak Keys Config

Enfin, sur la navigation principale de Keycloak, sélectionnez **Paramètres du royaume** puis l'**onglet Clés**. Localisez le certificat **RS256** et sélectionnez **Certificat**.



Keycloak RS256 Certificate

La valeur du certificat sera requise pour la section suivante.

Retour à l'application web

À ce stade, vous avez configuré tout ce dont vous avez besoin dans le contexte du portail Keycloak. Retournez à l'application web Bitwarden et sélectionnez **Paramètres → Connexion unique** depuis la navigation.

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.

Complétez les champs suivants dans la section **Configuration du fournisseur de service SAML** :

Champ	Description
Name ID Format	Sélectionnez **Courriel**.
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.
Algorithme de Signature Minimum Entrant	Sélectionnez l'algorithme que le client Keycloak est configuré pour utiliser pour signer des documents ou des assertions SAML.
Voulez des Assertions Signées	Que Bitwarden s'attend à ce que les assertions SAML soient signées. Si activé, assurez-vous de configurer le client Keycloak pour signer les assertions.
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 avec l'image Docker de l'identifiant Bitwarden avec SSO.

Complétez les champs suivants dans la section **Configuration du fournisseur d'identité SAML** :

Champ	Description
ID de l'entité	Entrez l'URL du royaume Keycloak sur lequel le client a été créé, par exemple `https:///royaumes/`. Ce champ est sensible à la casse.
Type de liaison	Sélectionnez **Rediriger**.
URL du service de connexion unique (SSO)	Entrez votre URL de traitement SAML principal, par exemple `https:///royaumes//protocole/saml`.
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 préconfigurer avec votre **URL de déconnexion** si vous le souhaitez.

Champ	Description
Certificat public X.509	Entrez le **certificat RS256** qui a été copié à l'étape précédente. 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 que le client Keycloak est configuré pour utiliser pour signer des documents ou des assertions SAML.
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 Keycloak 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.

Paramètres supplémentaires de Keycloak

Sur l'**onglet des paramètres du client** Keycloak, des options de configuration supplémentaires sont disponibles :

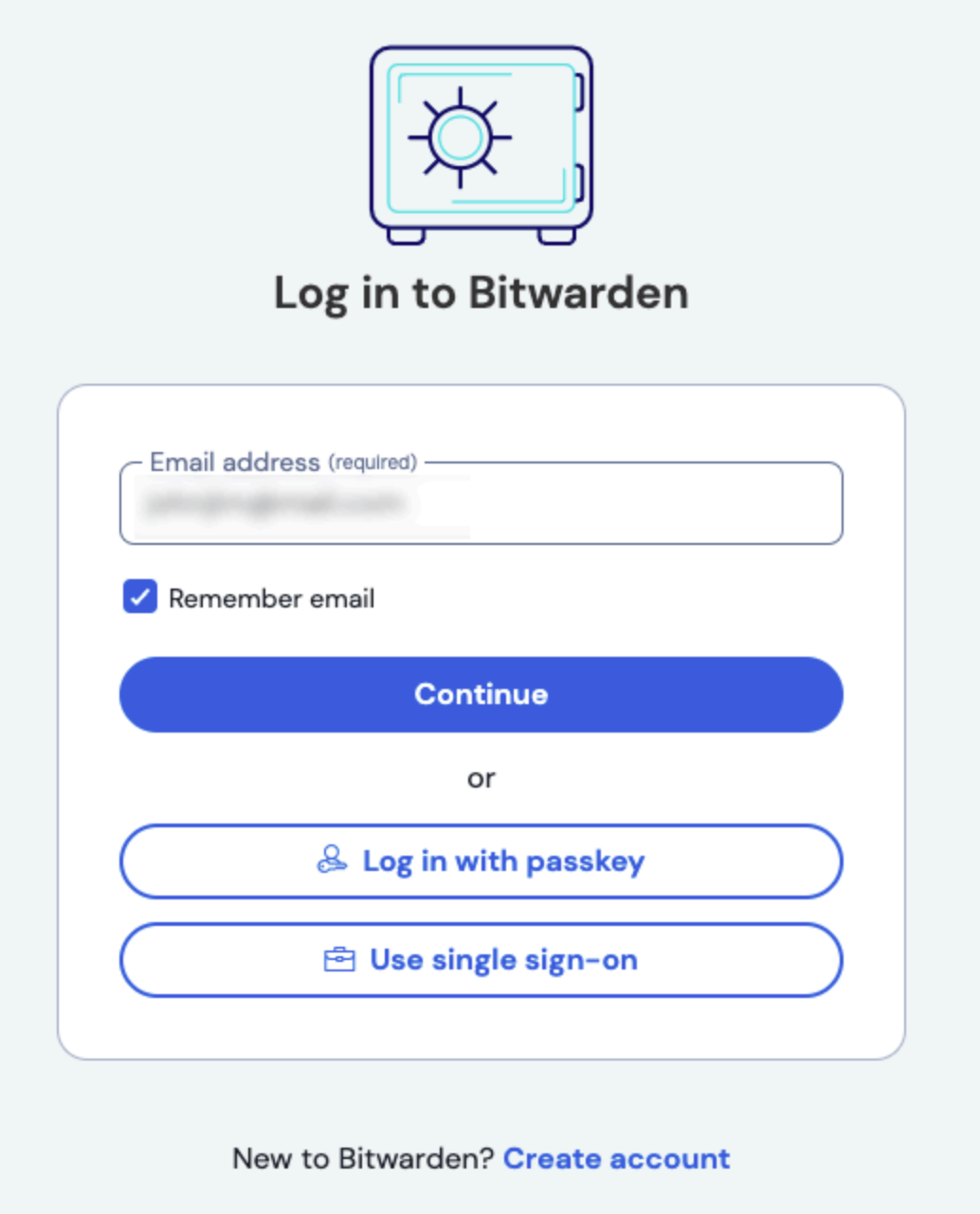
Champ	Description
Signer des documents	Spécifiez si les documents SAML doivent être signés par le royaume Keycloak.
Signer les Assertions	Spécifiez si les assertions SAML doivent être signées par le royaume Keycloak.

Champ	Description
Algorithme de Signature	Si **Sign Assertions** est activé, sélectionnez l'algorithme à utiliser pour signer (`sha-256` par défaut).
Format d'identifiant de nom	Sélectionnez le format d'ID de nom que Keycloak doit utiliser dans les réponses SAML.

Une fois que vous avez terminé le forum, sélectionnez **Enregistrer**.

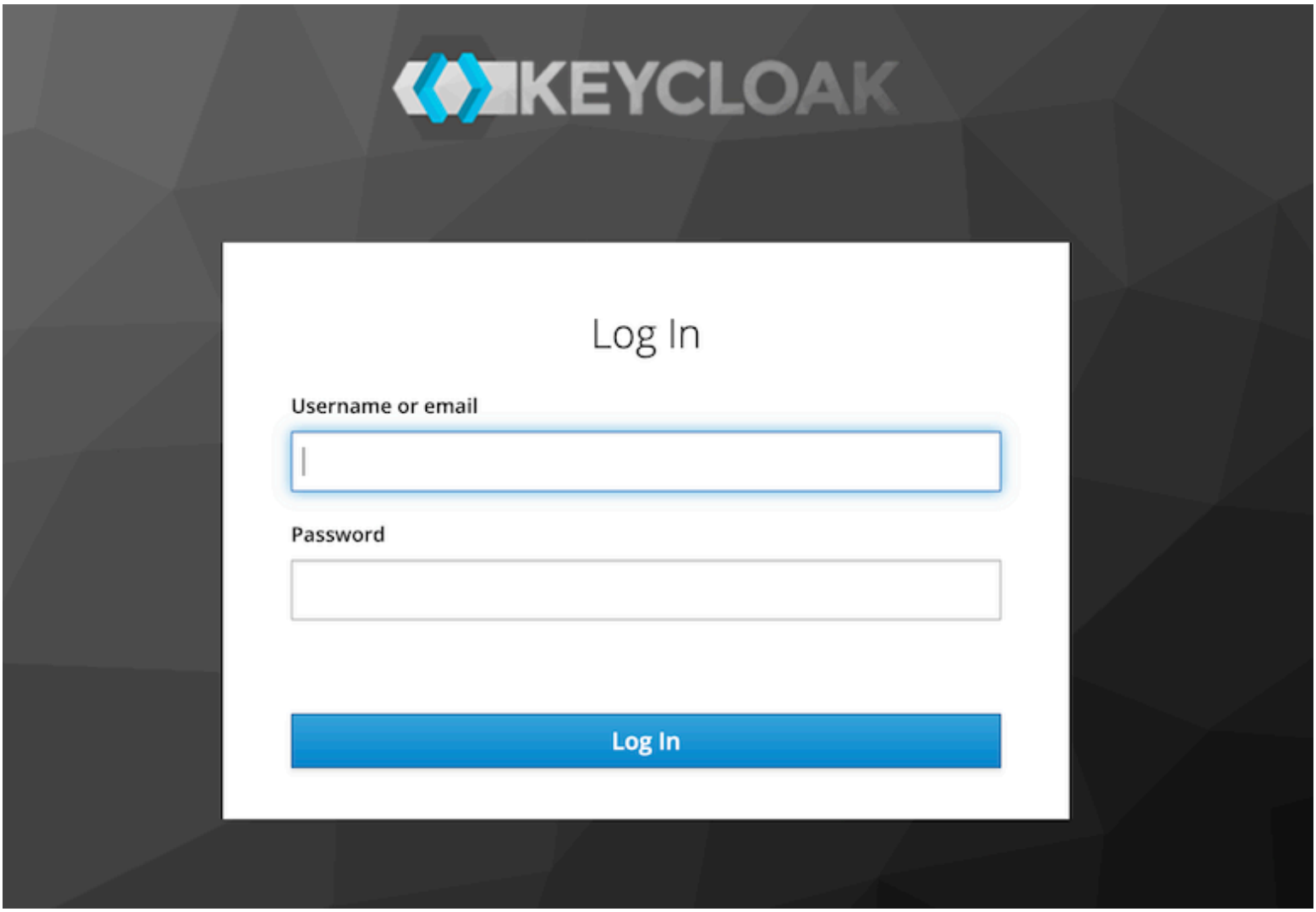
Testez la configuration

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 l'écran d'identifiant Keycloak:



Keycloak Login Screen

Après vous être authentifié avec vos identifiants Keycloak, 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.