Implémentation de SAML AWS

Implémentation de SAML AWS

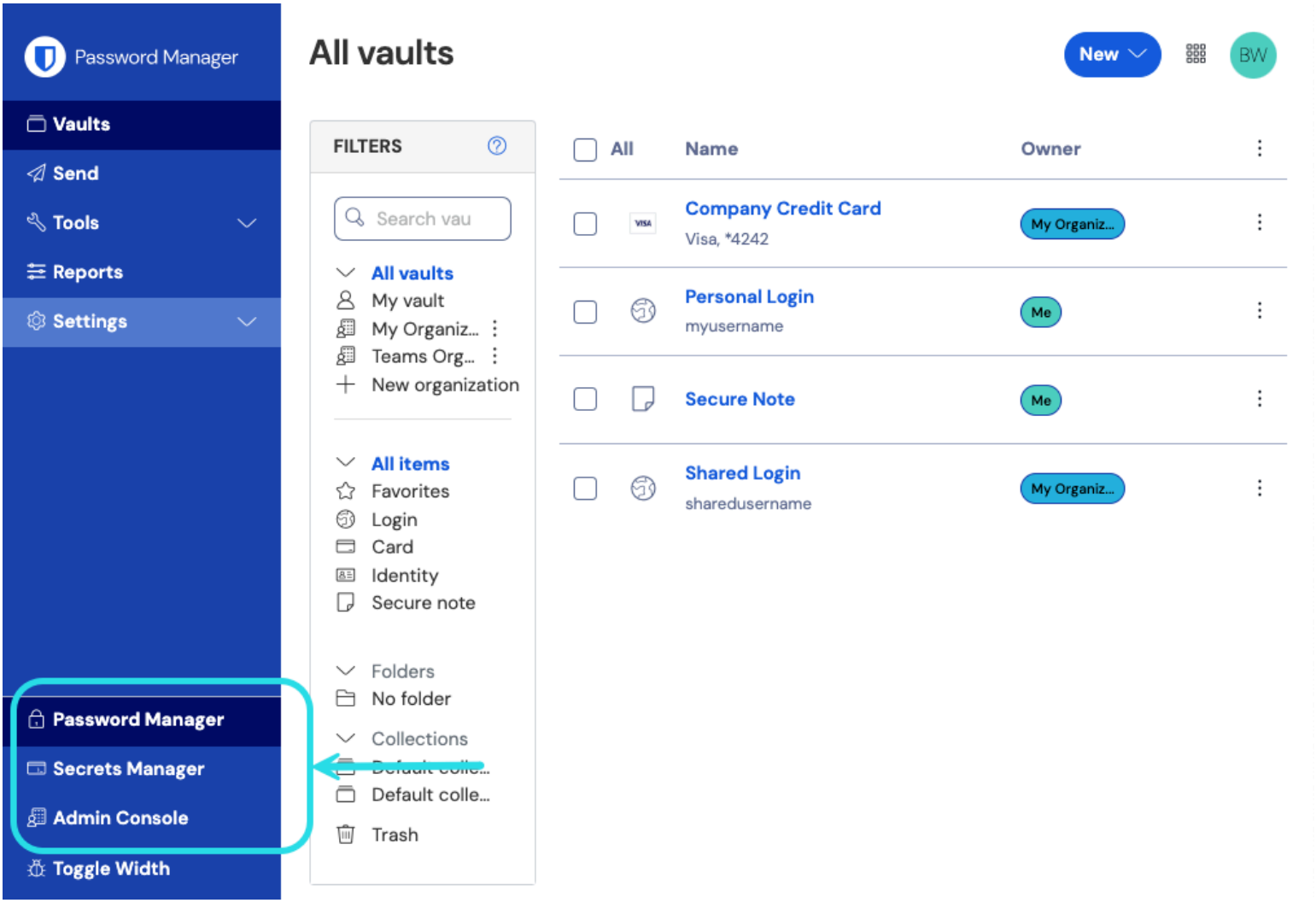
Cet article contient de l'aide **spécifique à AWS** pour configurer l'identifiant avec SSO via SAML 2.0. Pour obtenir de l'aide pour configurer l'identifiant avec SSO pour un autre IdP, reportez-vous à Configuration SAML 2.0.

La configuration implique de travailler simultanément dans l'application web Bitwarden et la console AWS. 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**
>
> **Déjà un expert SSO ?** Ignorez les instructions de cet article et téléchargez des captures d'écran d'exemples de configurations pour les comparer aux vôtres.
>
> saisir: asset-hyperlink id: K4Z8ny0RzKkHKIJlZ4hh1

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

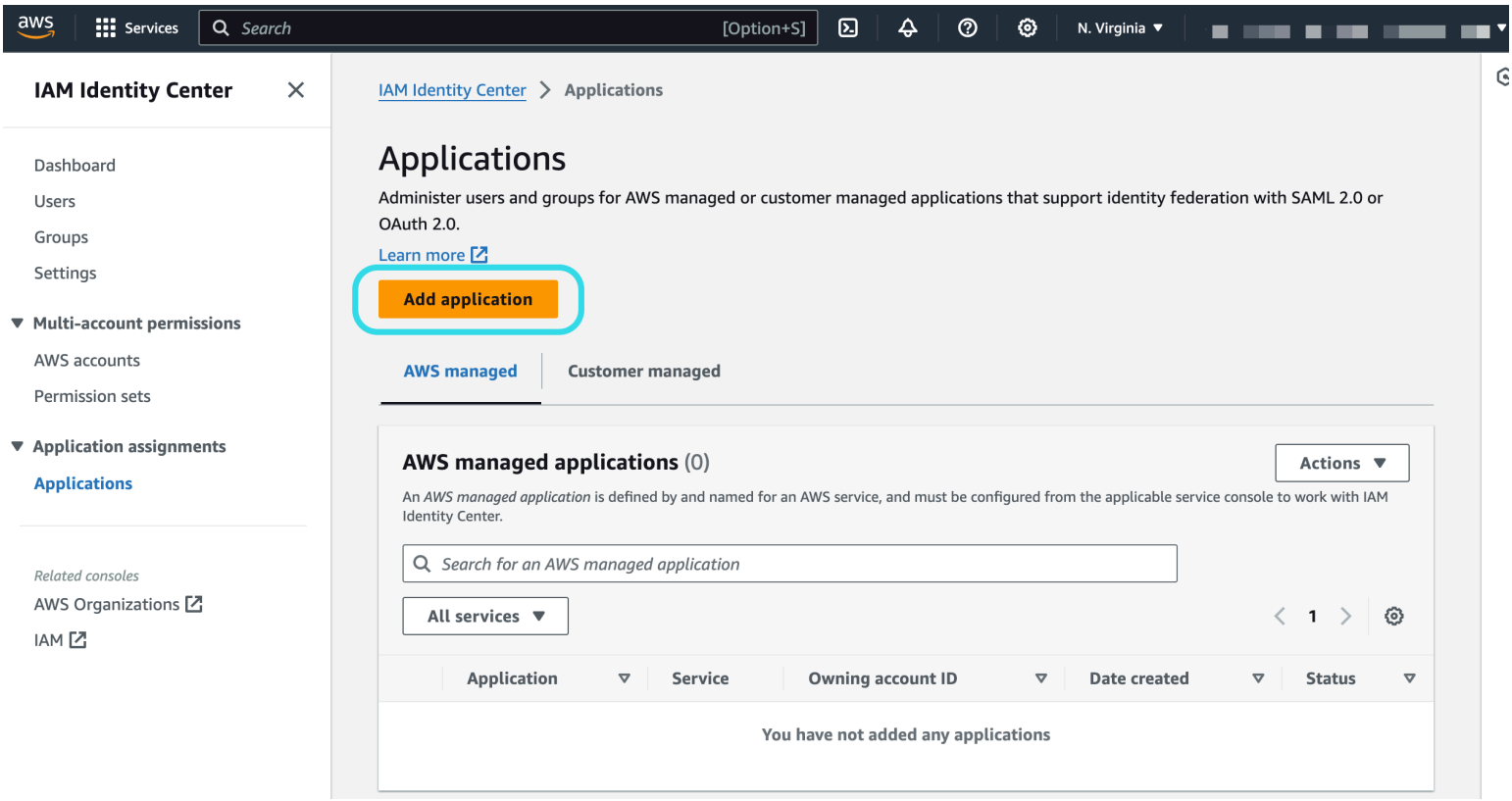
Si vous ne l'avez pas déjà fait, créez un **identifiant SSO** unique pour votre organisation et sélectionnez **SAML** dans le menu déroulant **Saisir** . Gardez cet écran ouvert pour une référence facile.

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.

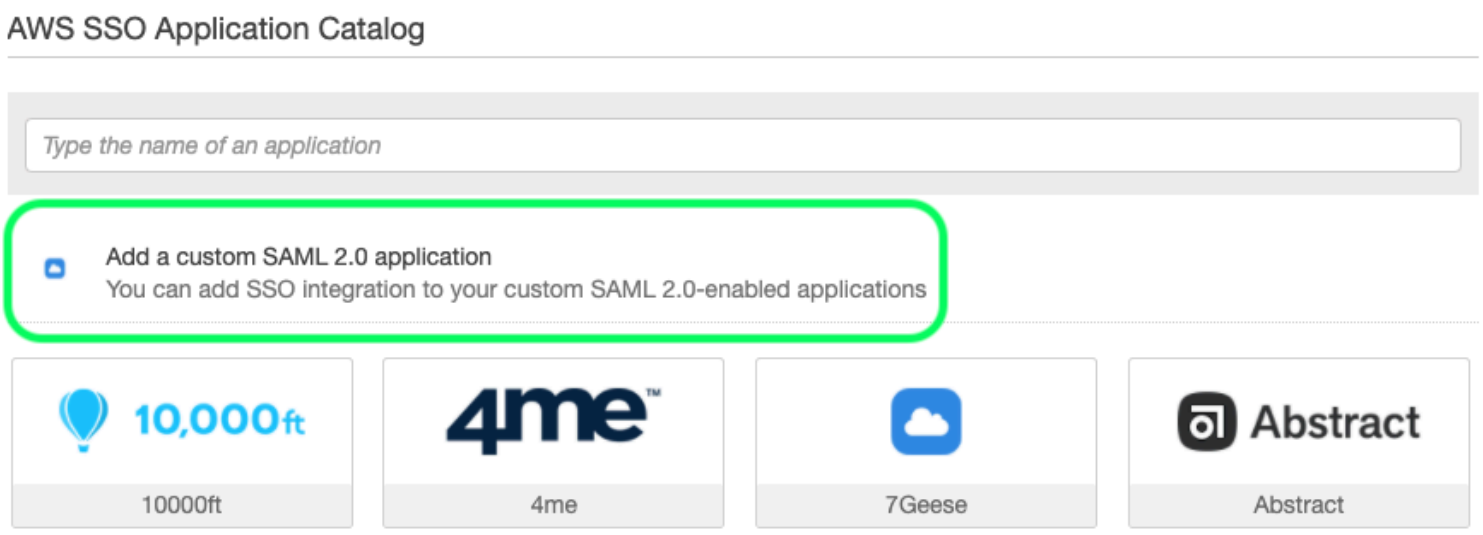
Créez une application AWS SSO

Dans la console AWS, naviguez jusqu'à **AWS SSO**, sélectionnez **Applications** dans la navigation, et sélectionnez le bouton **Ajouter une nouvelle application** :



Ajouter une nouvelle application

Sous la barre de recherche, sélectionnez l'option **Ajouter une application SAML 2.0 personnalisée** :



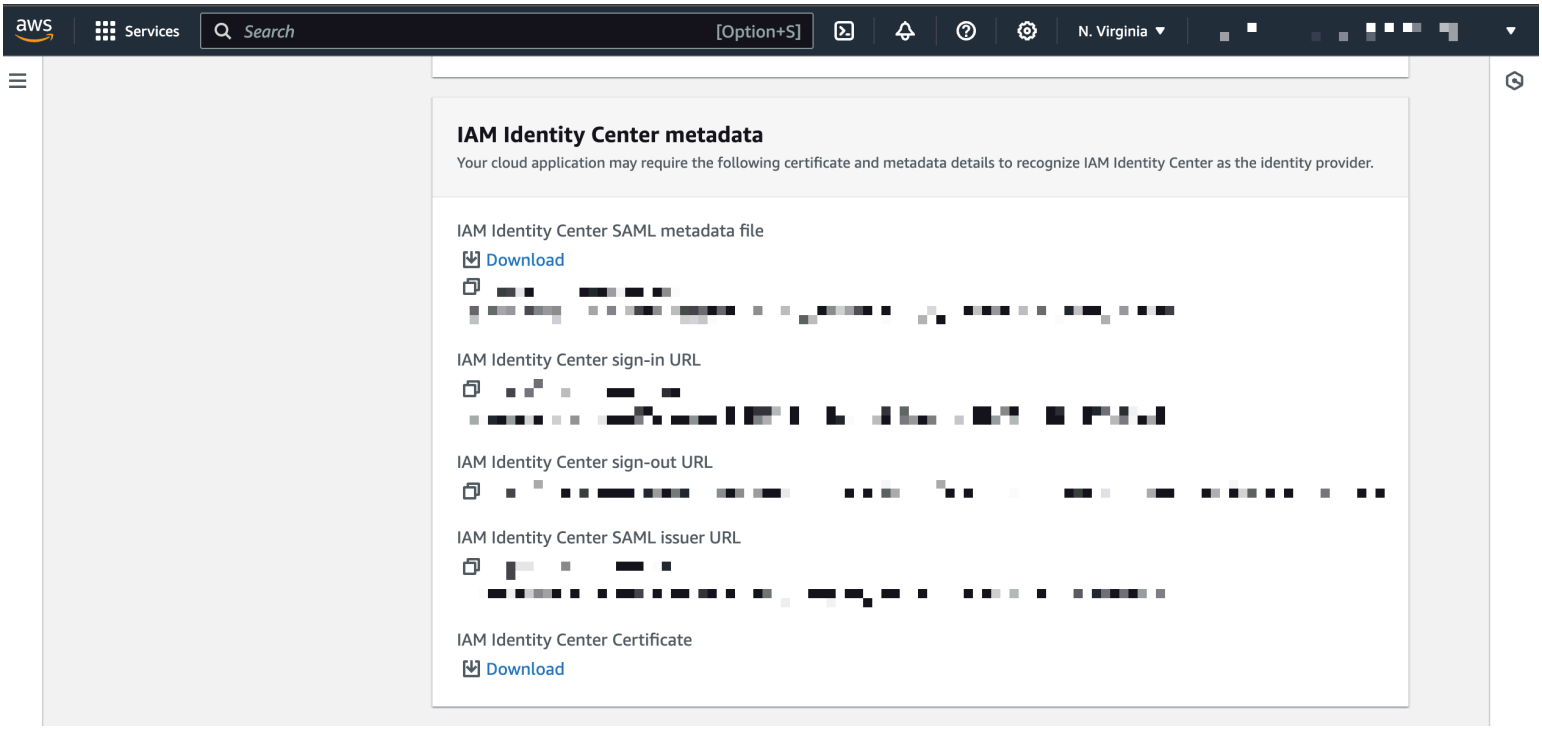
Ajouter une application SAML personnalisée

Détails

Donnez à l'application un **Nom d'affichage** unique et spécifique à Bitwarden.

Métadonnées AWS SSO

Vous aurez besoin des informations de cette section pour une étape de configuration ultérieure. Copiez l'**URL de connexion AWS SSO** et l'**URL de l'émetteur AWS SSO**, et téléchargez le **certificat AWS SSO** :



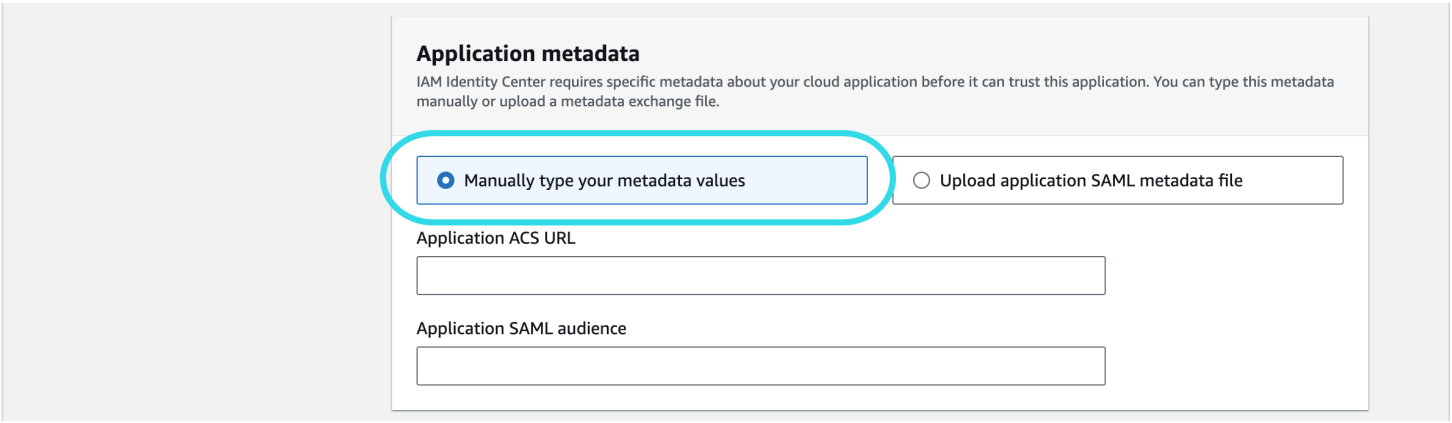
Métadonnées AWS SSO

Propriétés de l'application

Dans le champ **URL de démarrage de l'application**, spécifiez l'URL d'identifiant à partir de laquelle les utilisateurs accéderont à Bitwarden. Pour les clients hébergés dans le cloud, c'est toujours `https://vault.bitwarden.com/#/sso`. Pour les instances auto-hébergées, cela est déterminé par votre URL de serveur configurée, par exemple `https://votre.domaine/#/sso`.

Métadonnées de l'application

Dans la section des métadonnées de l'application, sélectionnez l'option pour entrer manuellement les valeurs des métadonnées :



Entrez les valeurs des métadonnées

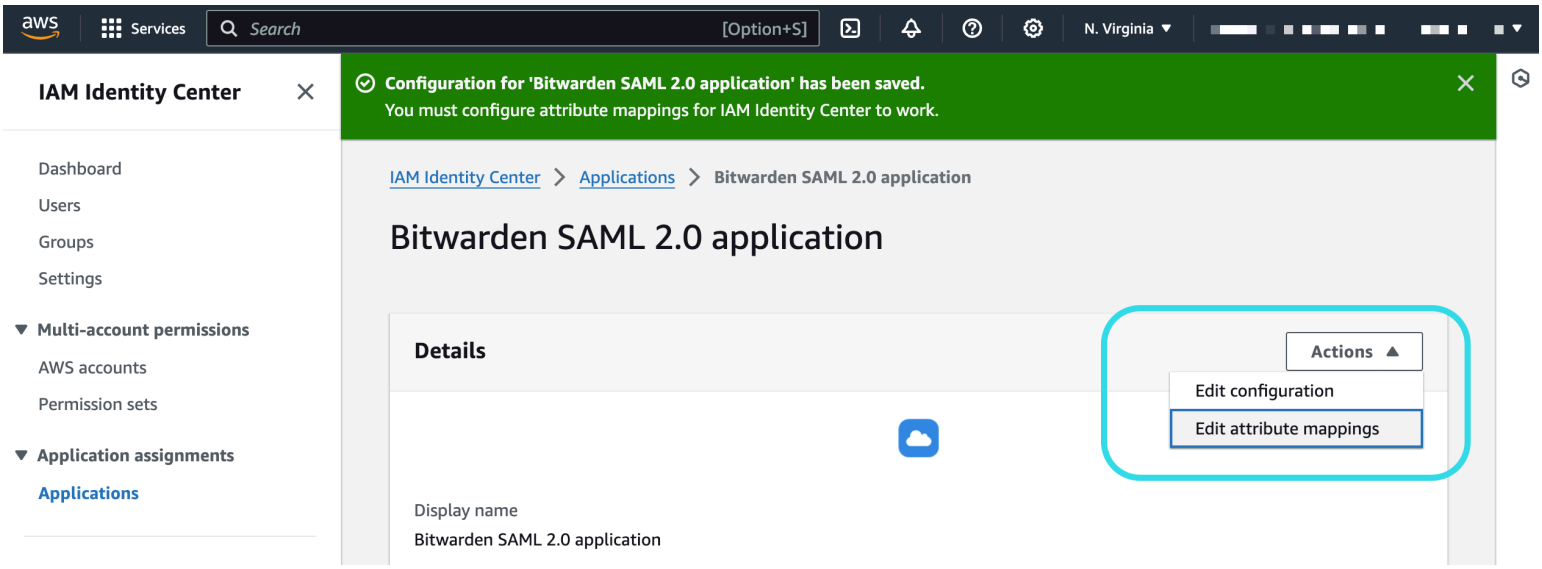
Configurez les champs suivants :

Champ	Description
URL de l'application ACS	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.
Audience de l'application SAML	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.

Lorsque vous avez terminé, sélectionnez **Enregistrer les modifications**.

Mappages d'attributs

Naviguez vers l'onglet **Mappages d'attributs** et configurez les mappages suivants:

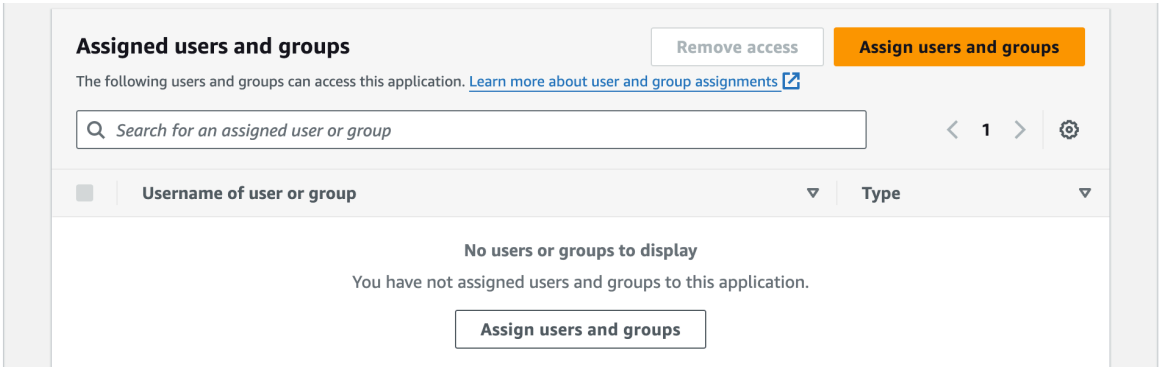


Mappages d'attributs

Attribut d'utilisateur dans l'application	Se traduit par cette valeur de chaîne ou attribut d'utilisateur dans AWS SSO	Format
Sujet	`${user:email}`	adresse électronique
courriel	`${user:email}`	Non spécifié

Utilisateurs assignés

Naviguez vers l'onglet **Utilisateurs assignés** et sélectionnez le bouton **Assigner des utilisateurs** :



Attribuer des utilisateurs

Vous pouvez attribuer des utilisateurs à l'application individuellement, ou par Groupe.

Retour à l'application web

À ce stade, vous avez configuré tout ce dont vous avez besoin dans le contexte de la console AWS. 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

La configuration du fournisseur de services devrait déjà être terminée, cependant, vous pouvez choisir d'éditer l'un des champs suivants :

Champ	Description
Format d'identifiant de nom	Définir sur **Adresse de courriel**.
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	Par défaut, AWS SSO signera avec SHA-256. À moins que vous n'ayez changé cela, sélectionnez `sha256` dans le menu déroulant.
Voulez des Assertions Signées	Que Bitwarden s'attend à ce que les assertions SAML soient signées.
Valider les Certificats	Cochez cette case lorsque vous chantez des certificats de confiance 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 Bitwarden Identifiant 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 à la Console AWS pour récupérer les valeurs de l'application :

Champ	Description
ID de l'entité	Entrez l'**URL de l'émetteur AWS SSO**, récupérée dans la section métadonnées AWS SSO dans la console AWS. Ce champ est sensible à la casse.
Type de Reliure	Définir sur **HTTP POST** ou **Redirection**.
URL du service de connexion unique	Entrez l'**URL de connexion AWS SSO**, récupérée dans la section métadonnées AWS SSO dans la console AWS.
URL du service de déconnexion unique	L'identifiant avec SSO ne prend actuellement **pas en charge** SLO. Cette option est prévue pour un développement futur, cependant vous pouvez la pré-configurer avec l'**URL de déconnexion AWS SSO** récupérée dans la section métadonnées AWS SSO de la console AWS.

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	Par défaut, AWS SSO signera avec `sha256`. À moins que vous n'ayez changé cela, sélectionnez `sha256` dans le menu déroulant.
Désactiver les demandes de déconnexion sortantes	La connexion avec SSO actuellement **ne** supporte pas SLO. Cette option est prévue pour un développement futur.

Champ	Description
Voulez-vous que les demandes d'authentification soient signées	Que AWS SSO s'attend à ce que les demandes SAML soient signées.

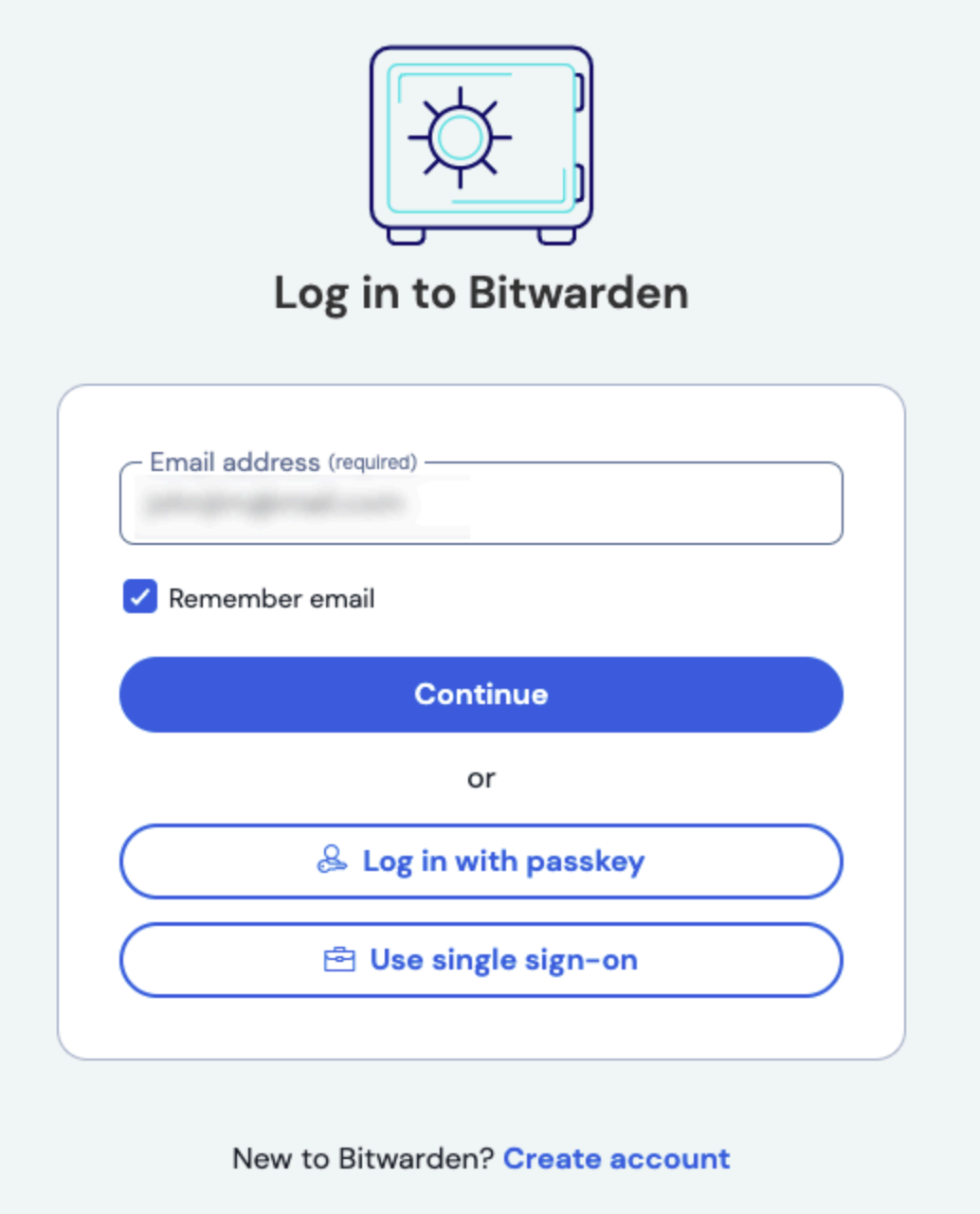
> **Note**
> Lors de la complétion du certificat X509, prenez note de la date d'expiration. Les certificats devront être renouvelés afin d'éviter toute interruption de service pour les utilisateurs finaux de SSO. Si un certificat a expiré, les comptes Admin et Propriétaire pourront toujours se connecter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

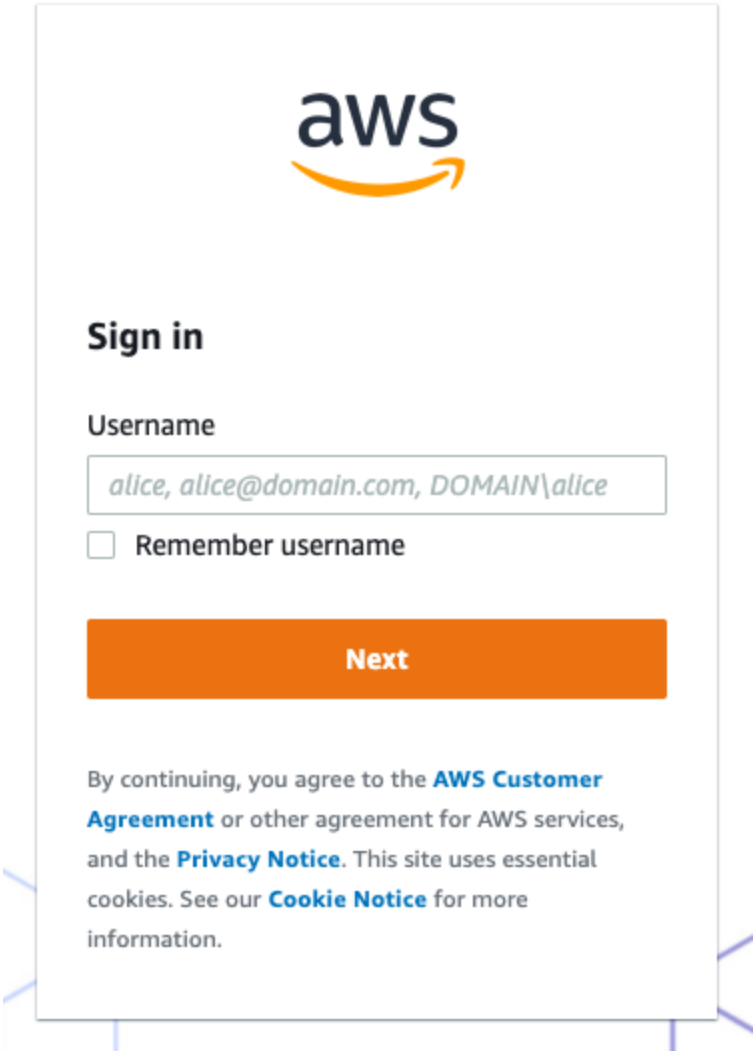
Testez la configuration

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 AWS SSO :



Écran d'identifiant AWS

Après vous être authentifié avec vos identifiants AWS, 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.