Mise en œuvre de SAML par Duo

Mise en œuvre de SAML par Duo

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

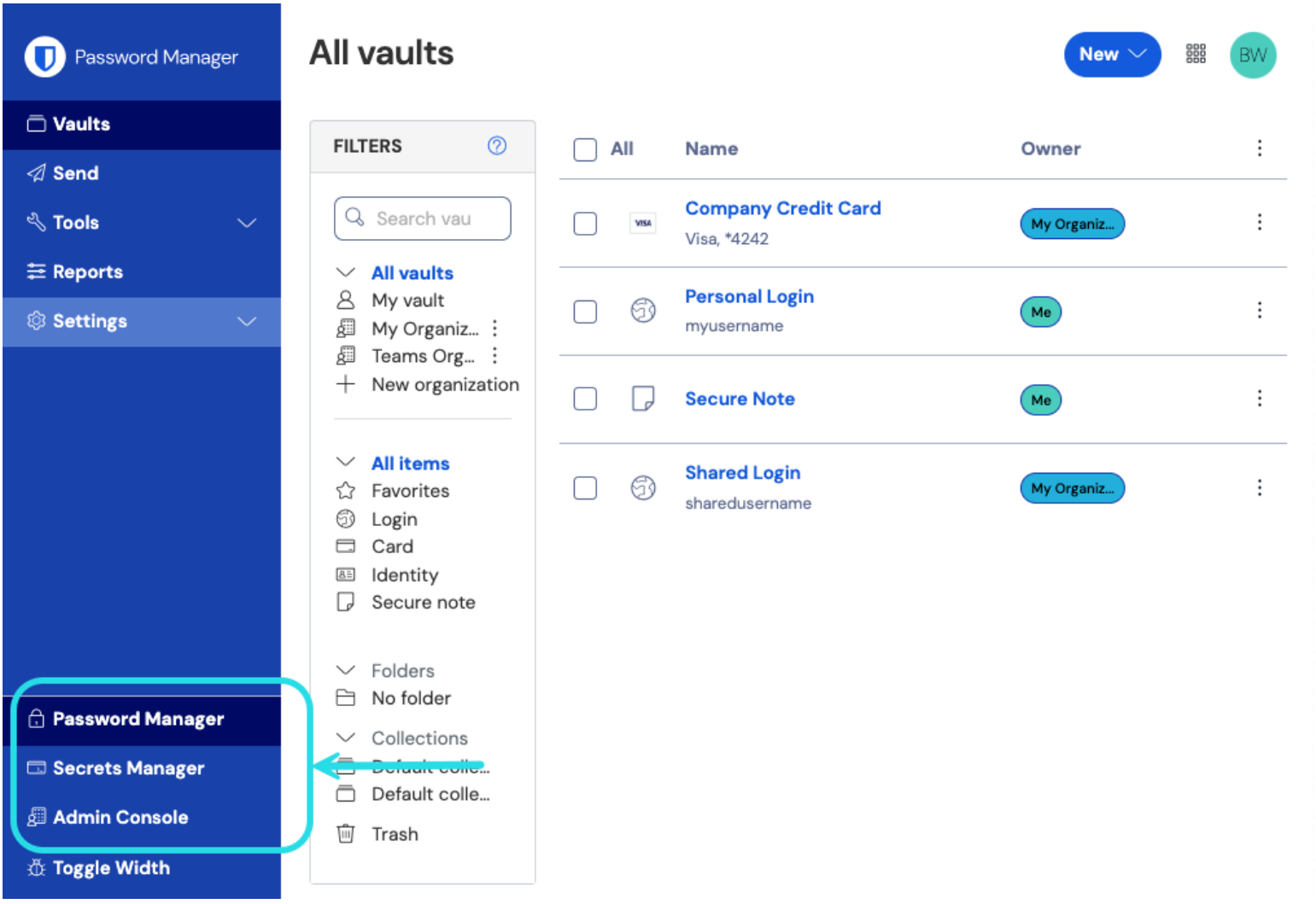
La configuration implique de travailler simultanément entre l'application web Bitwarden et le portail admin de Duo. Au fur et à mesure que vous avancez, nous vous recommandons d'avoir les deux à portée de main et de compléter les étapes dans l'ordre où elles sont documentées.

> **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

> **Warning**
>
> This article assumes that you have already set up Duo with an Identity Provider. If you haven't, see Duo's documentation for details.

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.

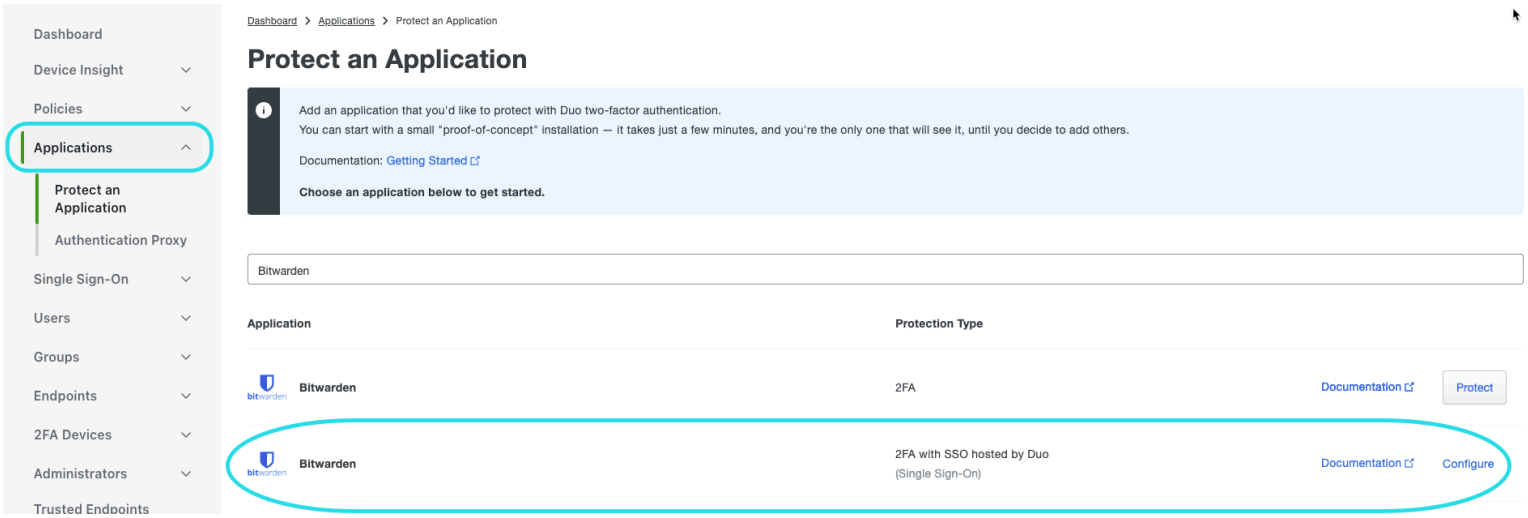
Vous pouvez désactiver l'option **Définir un ID d'entité SP unique** à ce stade si vous le souhaitez. Ce faisant, cela supprimera votre ID d'organisation de la valeur de votre ID d'entité SP, cependant dans presque tous les cas, il est recommandé de laisser cette option activée.

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

Protéger une application

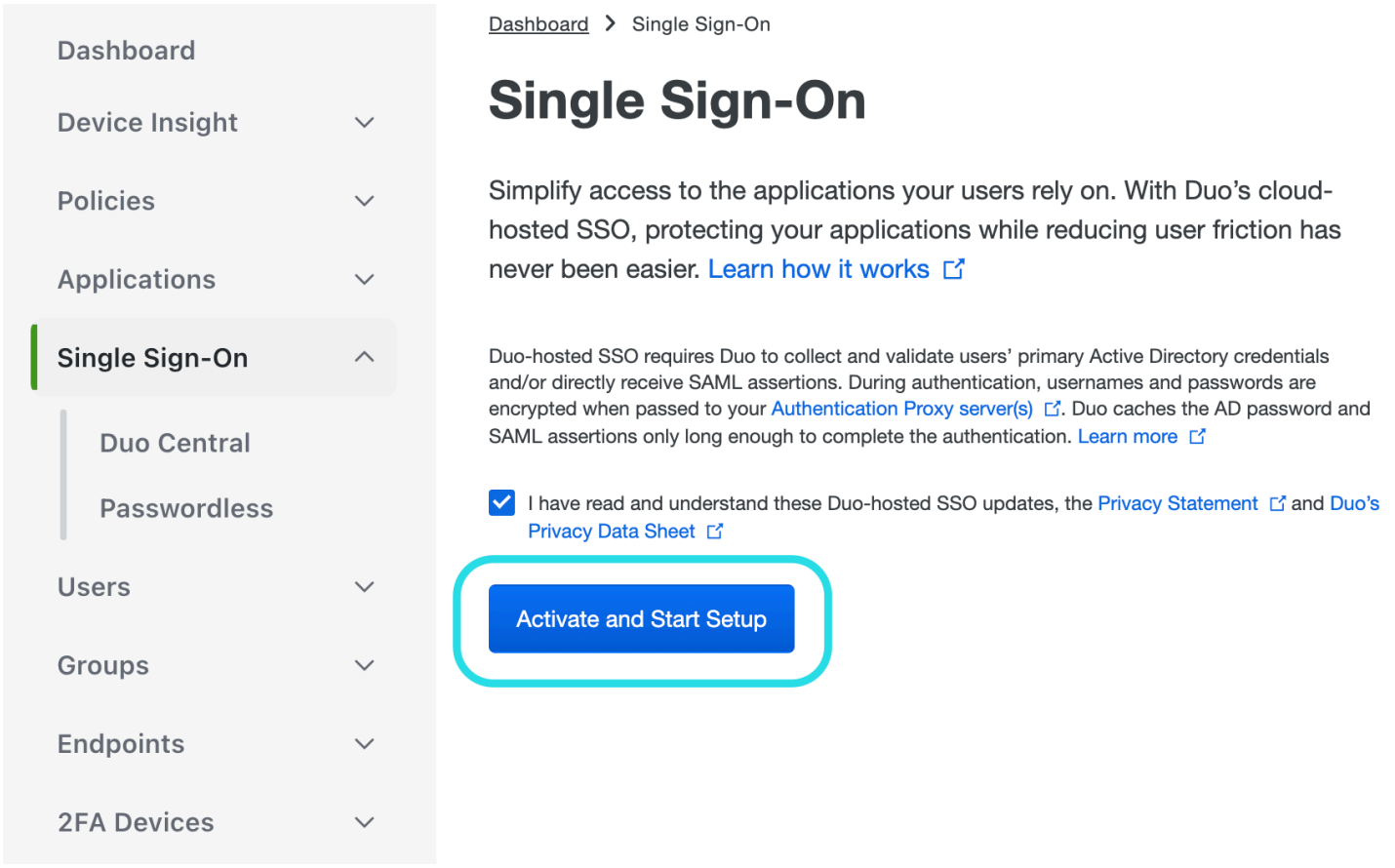
Avant de continuer, veuillez consulter la documentation de Duo pour vérifier que Duo Single Sign-On a été configuré avec votre fournisseur d'identité SAML pour l'authentification.

Dans le Portail Admin de Duo, naviguez vers l'écran **Applications** et sélectionnez **Protéger une Application**. Entrez **Bitwarden** dans la barre de recherche et sélectionnez **Configurer** pour l'application **Bitwarden 2FA avec SSO hébergé par Duo** :



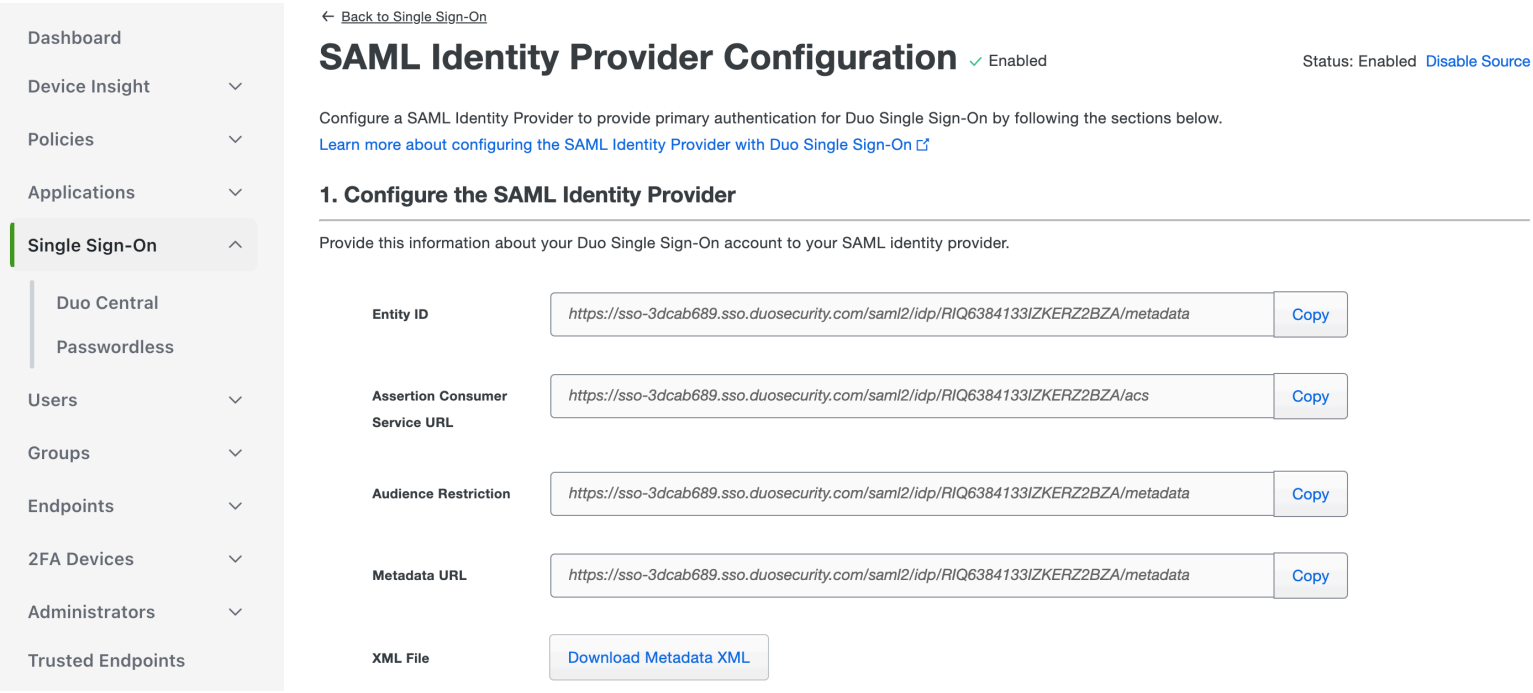
Duo Bitwarden Application

Sélectionnez **Activer et Démarrer la Configuration** pour l'application nouvellement créée:



Duo Activation and Setup

Complétez les étapes et configurations suivantes sur l'écran de configuration de l'application, certaines d'entre elles devront être récupérées depuis l'écran de connexion unique de Bitwarden :



DUO SAML Identity Provider Configuration

Métadonnées

Vous n'avez pas besoin d'éditer quoi que ce soit dans la section **Métadonnées**, mais vous devrez utiliser ces valeurs plus tard :

URLs for Configuration

Téléchargements

Sélectionnez le bouton **Télécharger le certificat** pour télécharger votre certificat X.509, car vous devrez l'utiliser plus tard dans la configuration.

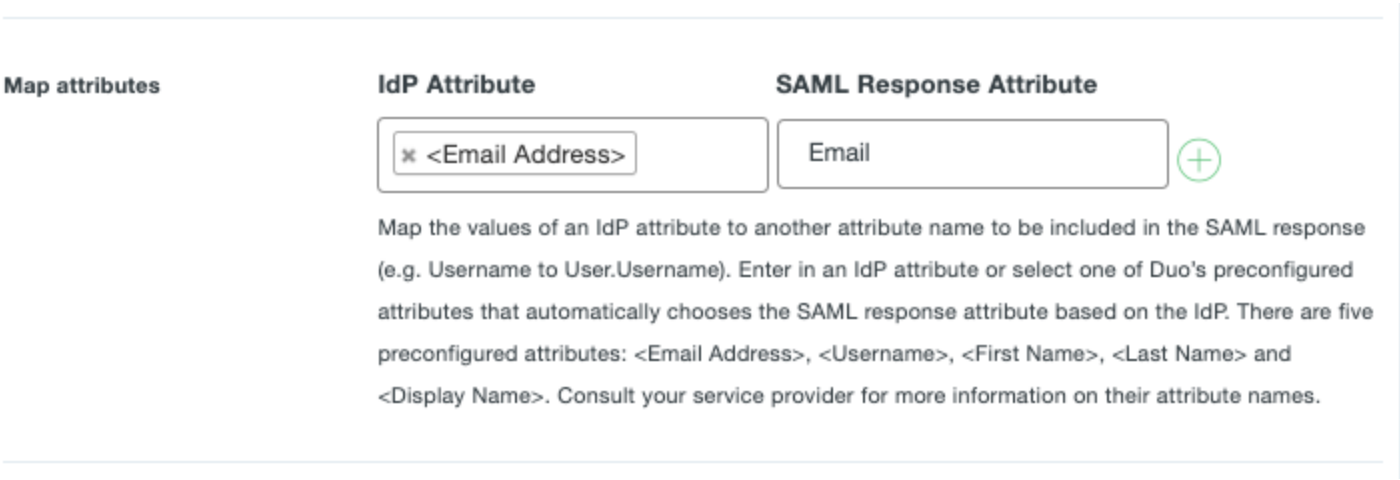
Fournisseur de service

Champ	Description
ID de l'entité	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.

Champ	Description
URL du Service de Consommation d'Assertion (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 l'organisation et variera en fonction de votre configuration.
URL de l'identifiant du fournisseur de services	Définissez ce champ sur l'URL d'identifiant à partir de laquelle les utilisateurs accéderont à Bitwarden. 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`.

Réponse SAML

Champ	Description
Format de l'ID de nom	Définissez ce champ sur le format NameID SAML pour que Duo l'envoie dans les réponses SAML.
Attribut NameID	Définissez ce champ sur l'attribut Duo qui remplira le NameID dans les réponses.
Algorithme de signature	Définissez ce champ sur l'algorithme de chiffrement à utiliser pour les assertions et les réponses SAML.
Options de signature	Sélectionnez si vous souhaitez **Signer la réponse**, **Signer l'affirmation**, ou les deux.
Attributs de carte	Utilisez ces champs pour mapper les attributs IdP aux attributs de réponse SAML. Indépendamment de l'attribut NameID que vous avez configuré, associez l'attribut `Adresse de courriel` de l'IdP à `Courriel`, comme dans la capture d'écran suivante :



Required Attribute Mapping

Une fois que vous avez terminé de configurer ces champs, **Enregistrez** vos modifications.

Retour à l'application web

À ce stade, vous avez configuré tout ce dont vous avez besoin dans le contexte du portail Duo. 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

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

Champ	Description
Format d'identifiant de nom	Format NameID à utiliser dans la requête SAML (`Politique NameID`). Définissez ce champ sur le format NameID sélectionné.
Algorithme de Signature Sortant	Algorithme utilisé pour signer les requêtes SAML, par défaut `rsa-sha256`.
Comportement de signature	Si/quand les demandes SAML seront signées. Par défaut, Duo ne nécessitera pas que les demandes soient signées.

Champ	Description
Algorithme de Signature Minimum Entrant	L'algorithme de signature minimum que Bitwarden acceptera dans les réponses SAML. Par défaut, Duo signera avec `rsa-sha256`, alors choisissez cette option dans le menu déroulant à moins que vous n'ayez sélectionné une option différente.
Voulez des Assertions Signées	Que Bitwarden souhaite des assertions SAML signées. Cochez cette case si vous avez sélectionné l'option de signature Signer l'assertion.
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 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 au Portail Admin de Duo pour récupérer les valeurs de l'application :

Champ	Description
ID de l'entité	Entrez la valeur de l'**ID de l'entité** de votre application Duo, qui peut être récupérée dans la section Métadonnées de l'application Duo. Ce champ est sensible à la casse.
Type de Reliure	Définissez ce champ sur **HTTP Post**.
URL du service de connexion unique	Entrez la valeur de l'**URL de connexion unique** de votre application Duo, qui peut être récupérée dans la section Métadonnées de l'application Duo.
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 pré-configurer avec la valeur de **l'URL de déconnexion unique** de votre application Duo.
Certificat Public X509	Collez le certificat téléchargé, en supprimant `-----DÉBUT DU CERTIFICAT-----`

Champ	Description
	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	Définissez ce champ sur l'algorithme de signature de réponse SAML sélectionné.
Désactiver les demandes de déconnexion sortantes	L'identification 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 Duo attende que les demandes SAML soient signées.

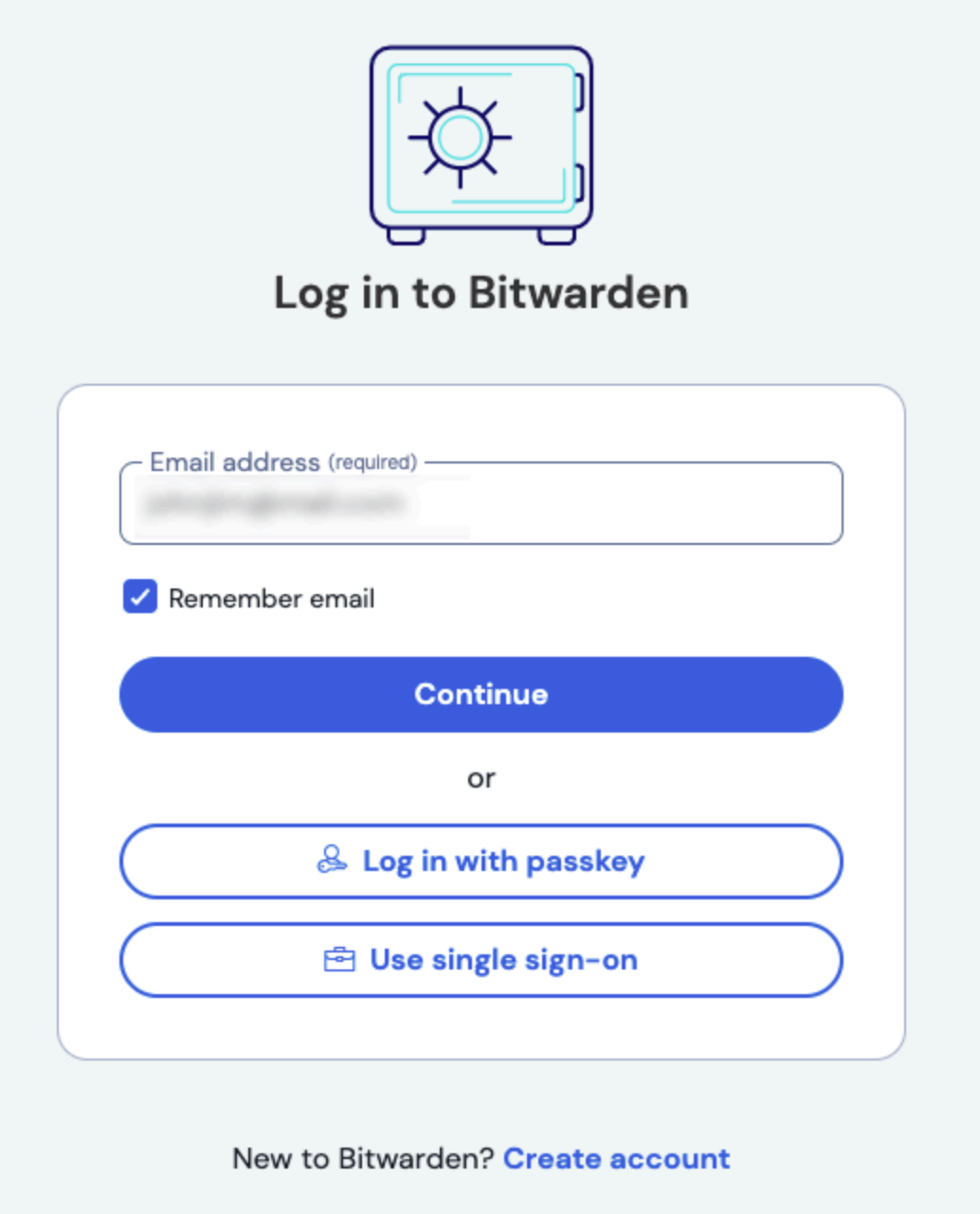
> **Note**
> Lors de la complétion du certificat X509, prenez note de la date d'expiration. Les certificats devront être renouvelés afin d'éviter toute interruption de service pour les utilisateurs finaux de SSO. Si un certificat a expiré, les comptes Admin et Propriétaire pourront toujours se connecter 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 configurée et sélectionnez **Se connecter**. Si votre mise en œuvre est correctement configurée, vous serez redirigé vers l'écran d'identifiant de votre IdP source.

Après vous être authentifié avec votre identifiant IdP et Duo Two-factor, 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.