CONSOLE ADMIN > IDENTIFIEZ-VOUS AVEC SSO >

Mise en œuvre de SAML par Google

Mise en œuvre de SAML par Google

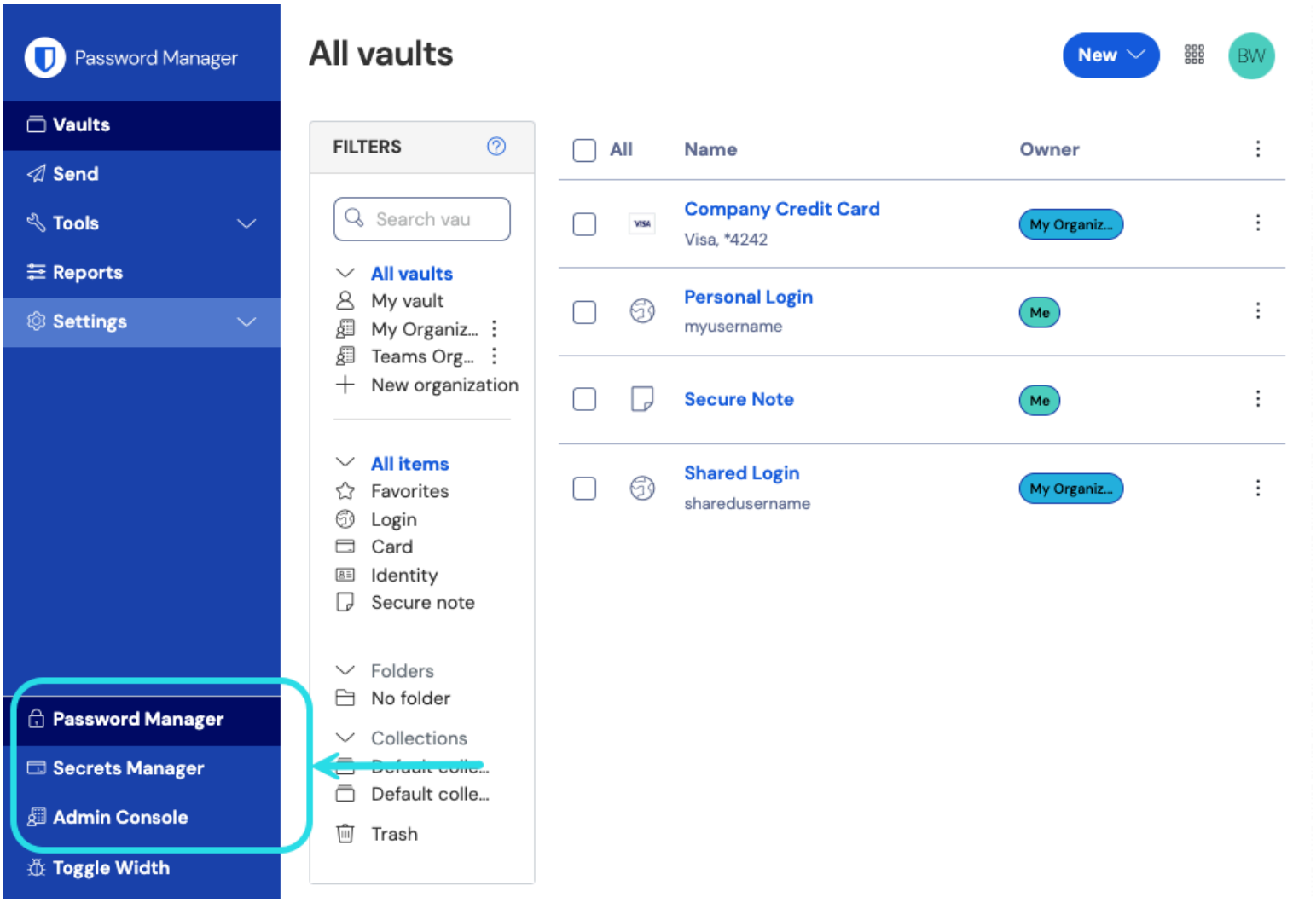
Cet article contient de l'aide **spécifique à Google Workspace** pour configurer l'identifiant avec SSO via SAML 2.0. Pour obtenir de l'aide pour configurer l'identifiant avec SSO pour un autre IdP, reportez-vous à Configuration SAML 2.0.

La configuration implique de travailler simultanément avec l'application web Bitwarden et la console admin de Google Workspace. 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**
>
> **Already an SSO expert?** Skip the instructions in this article and download screenshots of sample configurations to compare against your own.
>
> Download Sample

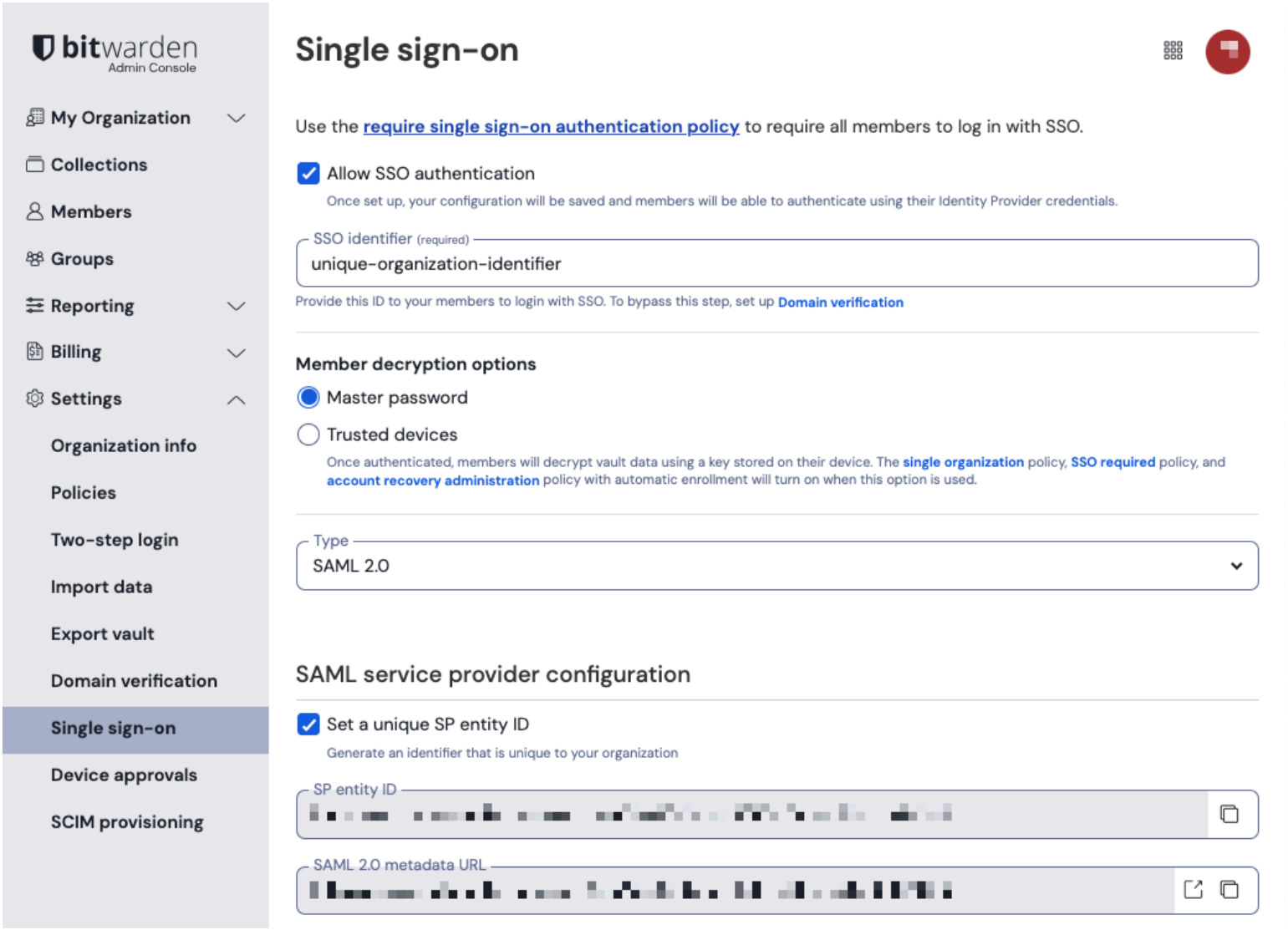
Ouvrez SSO dans l'application web

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

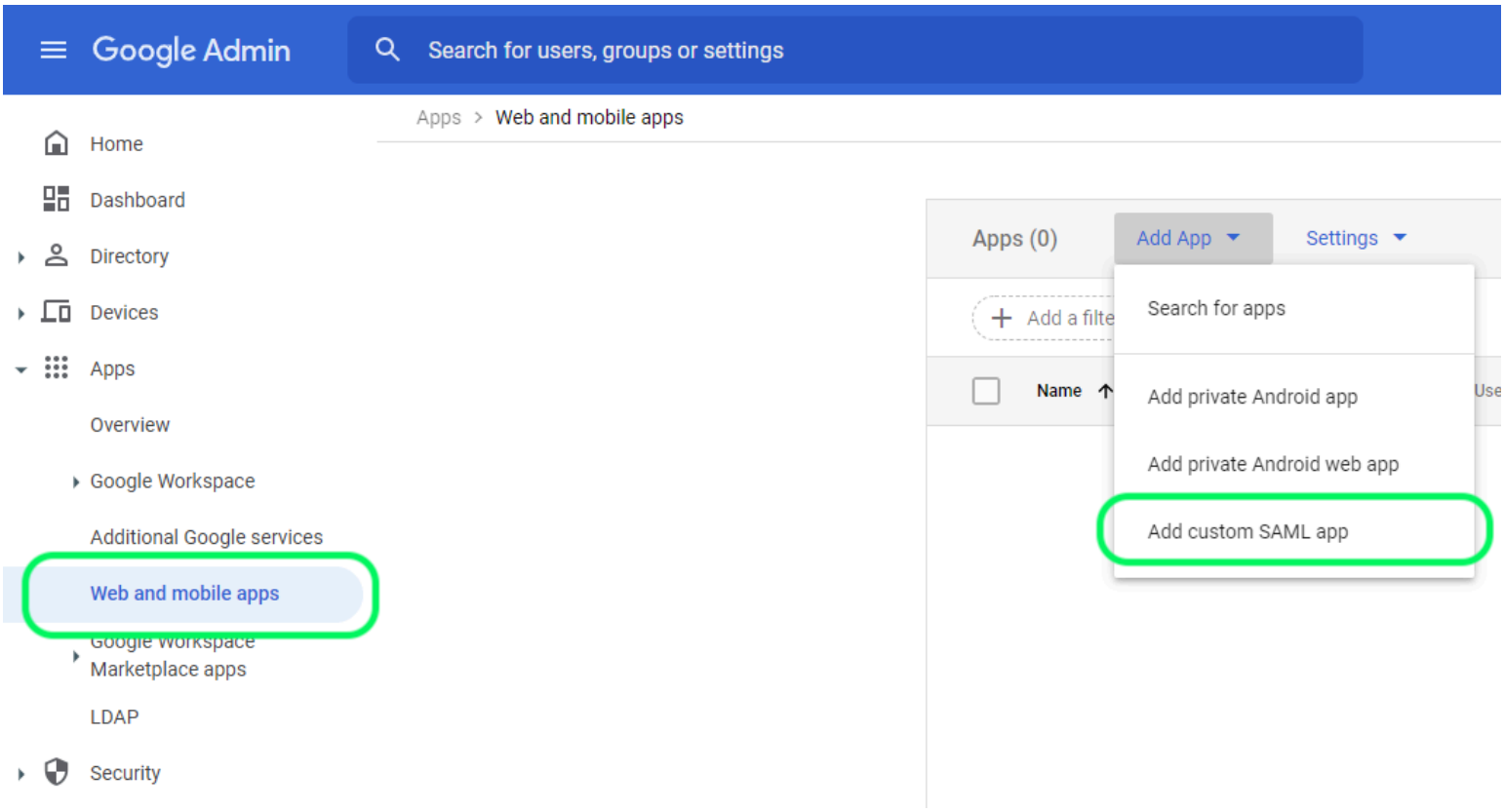
Si vous ne l'avez pas déjà fait, créez un **identifiant SSO** unique pour votre organisation et sélectionnez **SAML** dans le menu déroulant **Saisir**. Gardez cet écran ouvert pour une référence facile.

Vous pouvez désactiver l'option **Définir un ID d'entité SP unique** à ce stade si vous le souhaitez. 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.

Créez une application SAML

Dans la console d'administration de Google Workspace, sélectionnez **Applications** → **Applications Web et mobiles** à partir de la navigation. Sur l'écran Web et applications mobiles, sélectionnez **Ajouter une application** → **Ajouter une application SAML personnalisée** :



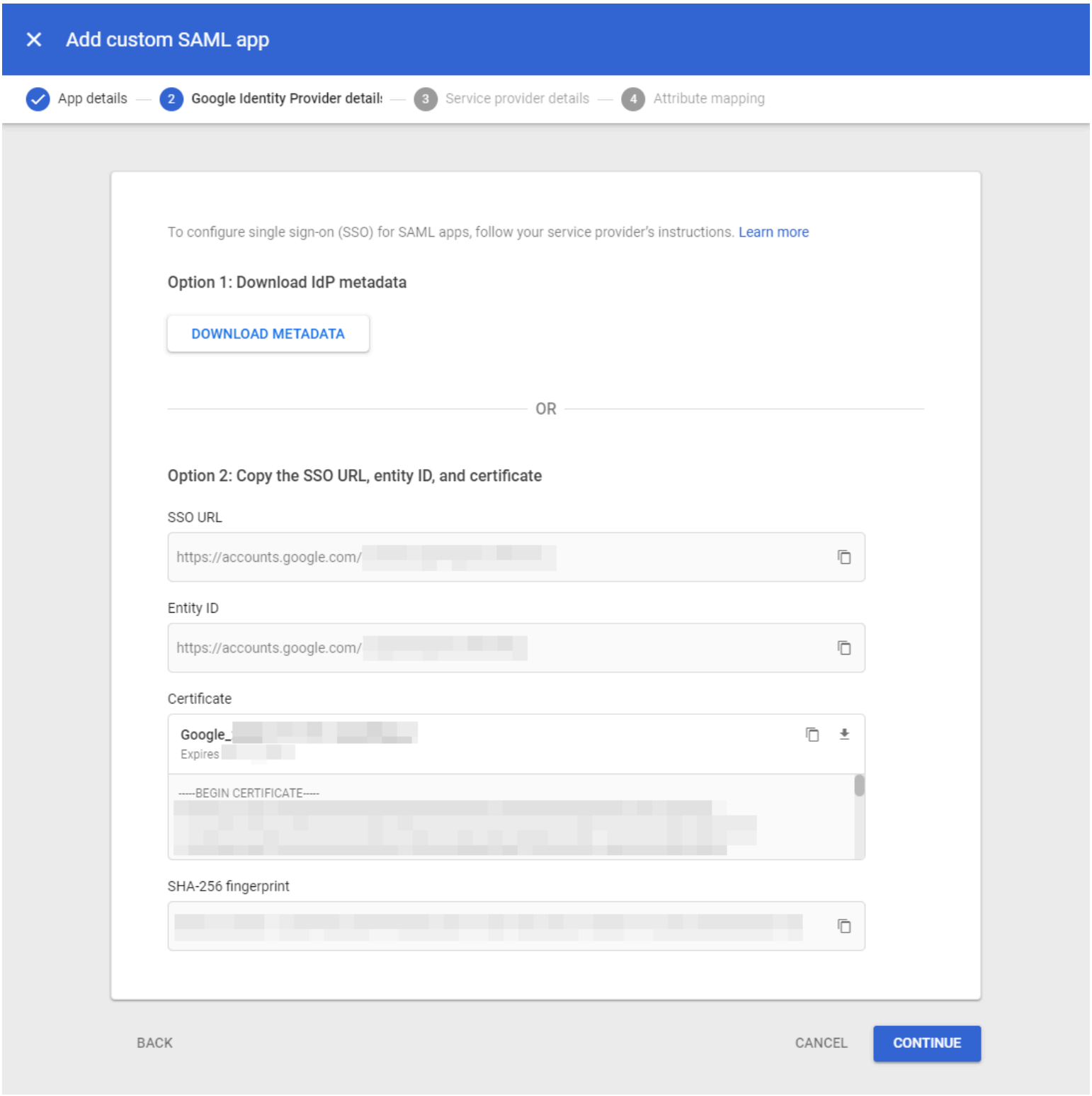
Create a SAML App

Détails de l'application

Sur l'écran de détails de l'application, donnez à l'application un nom spécifique à Bitwarden unique et sélectionnez le bouton **Continuer**.

Détails du fournisseur d'identité Google

Sur l'écran des détails du fournisseur d'identité Google, copiez votre **URL SSO**, **ID d'entité**, et **Certificat** pour utilisation lors d'une étape ultérieure :



IdP Details

Sélectionnez **Continuer** lorsque vous avez terminé.

Détails du fournisseur de services

Sur l'écran des détails du fournisseur de services, configurez les champs suivants :

Champ	Description
URL 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 votre organisation et variera en fonction de votre configuration.
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.
Démarrer l'URL	Facultativement, 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 signée	Cochez cette case si vous souhaitez que Workspace signe les réponses SAML. Si non vérifié, Workspace ne signera que l'assertion SAML.
Name ID Format	Définissez ce champ sur **Persistant**.
Identifiant de nom	Sélectionnez l'attribut utilisateur de l'espace de travail pour peupler NameID.

Sélectionnez **Continuer** lorsque vous avez terminé.

Cartographie des attributs

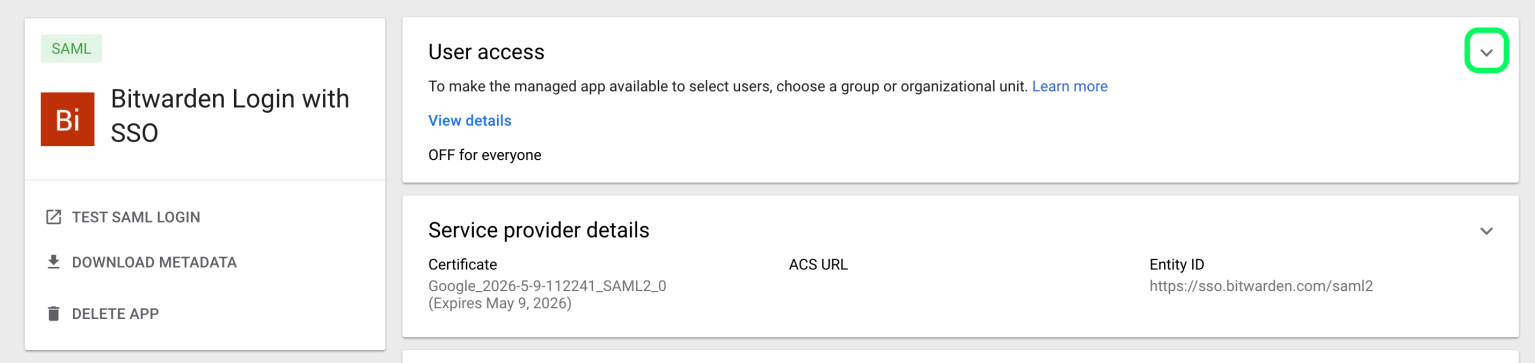
Sur l'écran de mappage des attributs, sélectionnez le bouton **Ajouter un mappage** et construisez le mappage suivant :

Attributs de l'annuaire Google	Attributs de l'application
Courriel principal	courriel

Sélectionnez **Terminer**.

Allumez l'application

Par défaut, les applications SAML de Workspace seront **DÉSACTIVÉES pour tout le monde**. Ouvrez la section Accès utilisateur pour l'application SAML et réglez sur **ON pour tout le monde** ou pour des groupes spécifiques, selon vos besoins :



User Access

Enregistrez vos modifications. Veuillez noter qu'il peut falloir jusqu'à 24 heures pour qu'une nouvelle application Workspace se propage aux sessions existantes des utilisateurs.

Retour à l'application web

À ce stade, vous avez configuré tout ce dont vous avez besoin dans le contexte de la console d'admin de Google Workspace. 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 la console Admin de l'espace de travail pendant la configuration :

Champ	Description
Format d'identifiant de nom	Définissez ce champ sur le format d'ID de nom sélectionné dans l'espace de travail.
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	Par défaut, Google Workspace signera avec RSA SHA-256. Sélectionnez `sha-256` dans le menu déroulant.
Exiger des assertions signées	Que Bitwarden s'attend à ce que les assertions SAML soient signées. Ce paramètre doit être **décoché**.
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 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 vous demandera souvent de vous référer à nouveau à la console Admin de l'espace de travail pour récupérer les valeurs de l'application :

Champ	Description
ID de l'entité	Définissez ce champ sur l'**ID de l'Entité** de l'Espace de travail, récupéré à partir de la section Détails du fournisseur d'Identité Google ou en utilisant le bouton **Télécharger les Métadonnées**. Ce champ est sensible à la casse.
Type de Reliure	Définir sur **HTTP POST** ou **Redirection**.
URL du service de connexion unique	Définissez ce champ sur l'URL SSO de Workspace , récupérée à partir de la section des détails du fournisseur d'Identité Google ou en utilisant le bouton **Télécharger les Métadonnées**.
URL de déconnexion unique	La connexion 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.

Champ	Description

Certificat Public X509	Collez le certificat récupéré, 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, Google Workspace signera avec RSA SHA-256. Sélectionnez `sha-256` dans le menu déroulant.
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 des Demandes d'Authentification Signées	Que Google Workspace attende des demandes SAML à être signées.

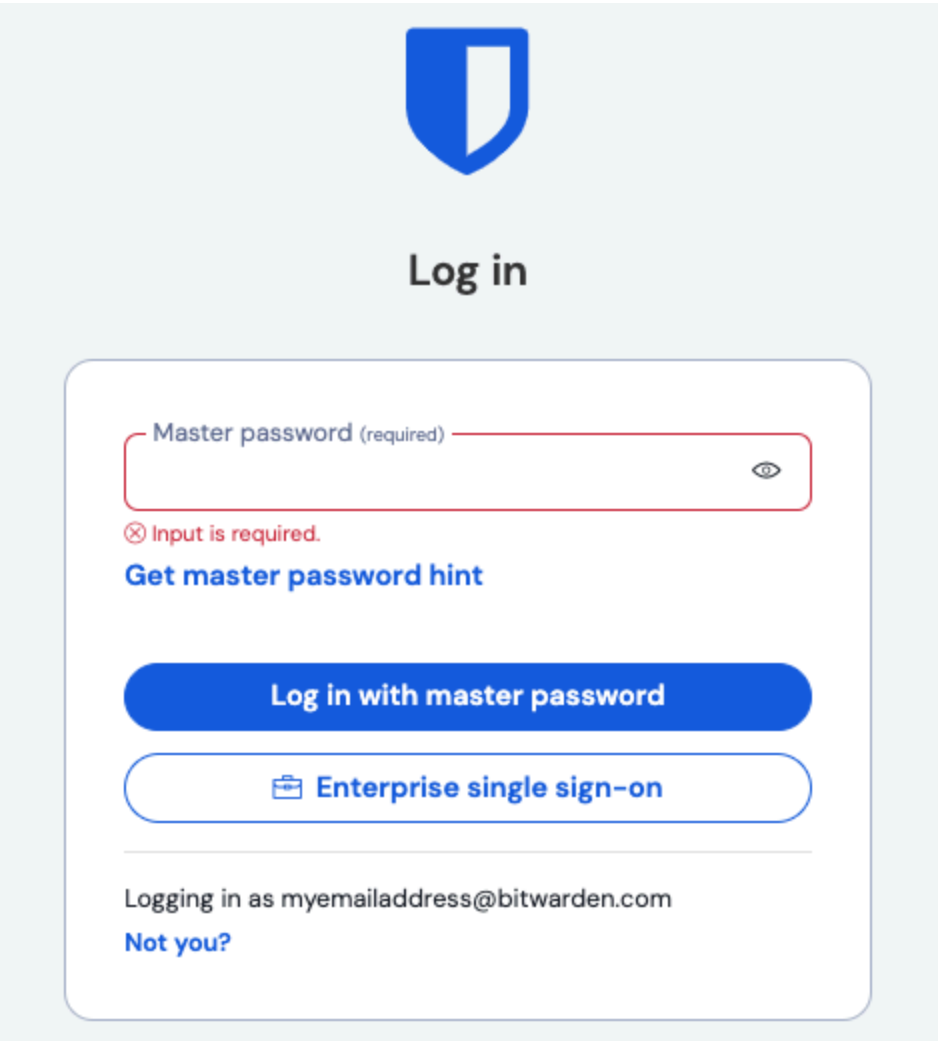
> **Note**
> Lors de la complétion du certificat X509, prenez note de la date d'expiration. Les certificats devront être renouvelés afin d'éviter toute interruption de service pour les utilisateurs finaux de SSO. Si un certificat a expiré, les comptes Admin et Propriétaire pourront toujours se connecter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

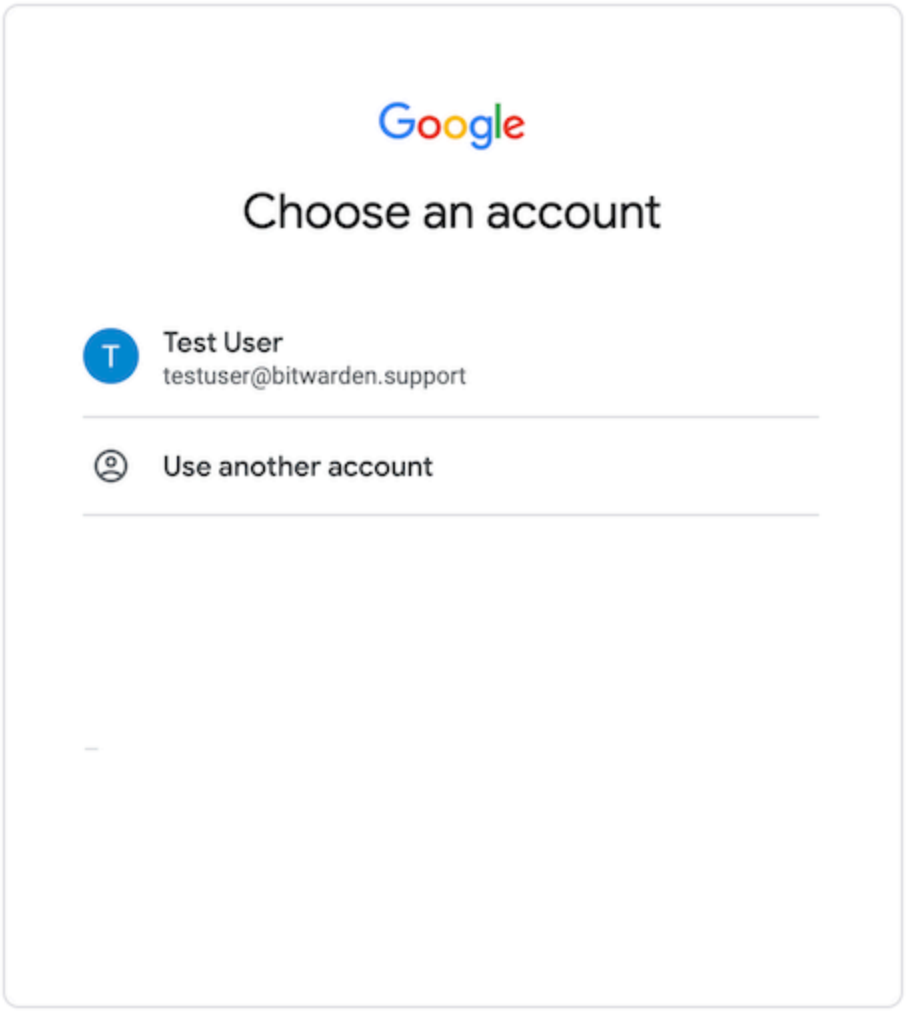
Testez la configuration

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 d'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 configurée avec succès, vous serez redirigé vers l'écran d'identifiant de Google Workspace :



Login

Après vous être authentifié avec vos identifiants de Workspace, 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.