bitwarden | Article du Centre d'Aide

CONSOLE ADMIN > IDENTIFIEZ-VOUS AVEC SSO >

Implémentation de SAML ADFS

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

Implémentation de SAML ADFS

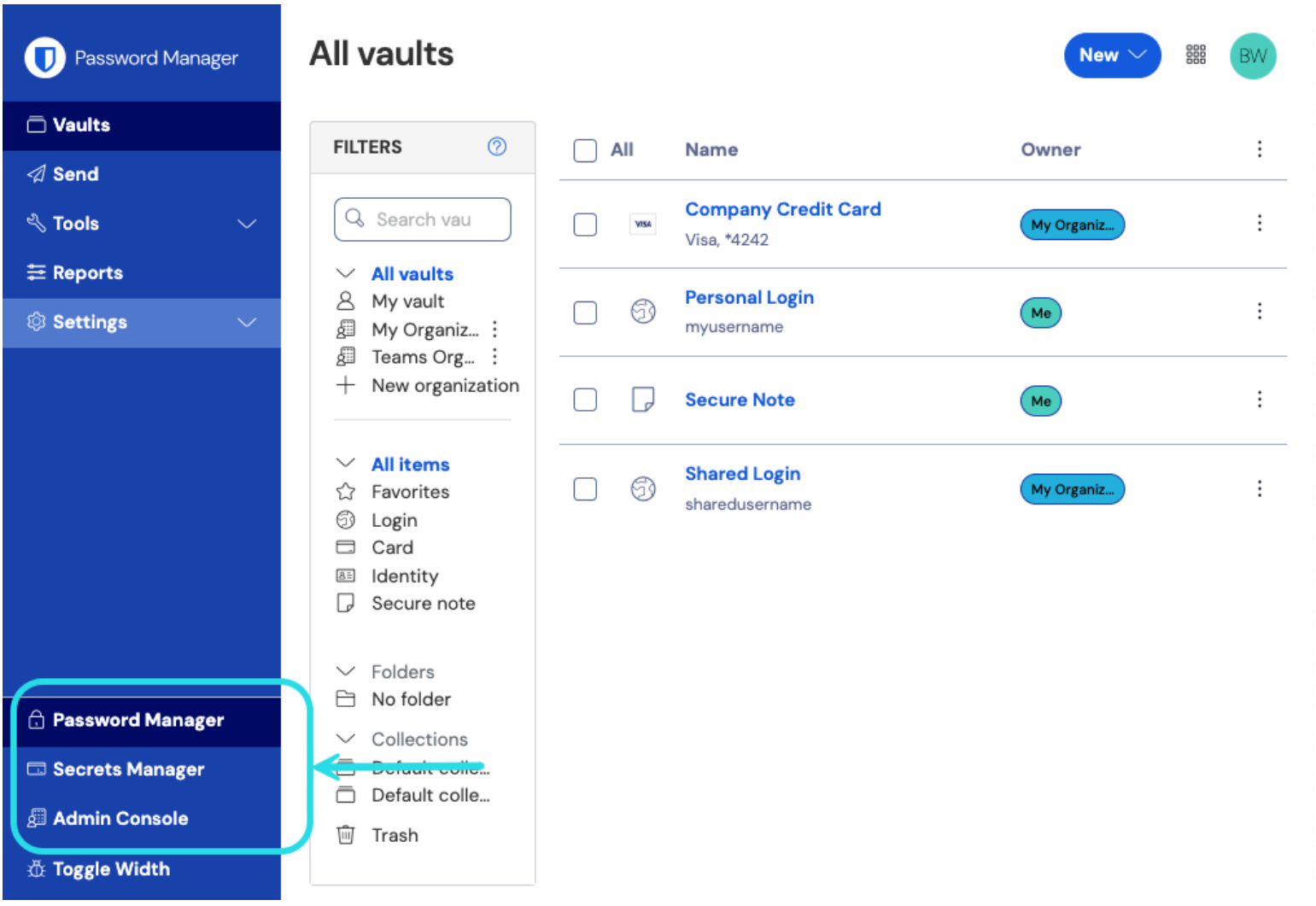
Cet article contient de l'aide **spécifique aux Services de Fédération Active Directory (AD FS)** pour configurer l'identifiant avec SSO via SAML 2.0. Pour obtenir de l'aide pour configurer l'identifiant avec SSO pour un autre IdP, reportez-vous à Configuration SAML 2.0.

La configuration implique de travailler simultanément au sein de l'application web Bitwarden et du Gestionnaire de serveur AD FS. 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**
>
> **Déjà un expert en SSO ?** Ignorez les instructions de cet article et téléchargez des captures d'écran d'exemples de configurations pour les comparer aux vôtres.
>
> saisir: lien-actif id: 5892IOGrU7B9IvBmN0P0xl

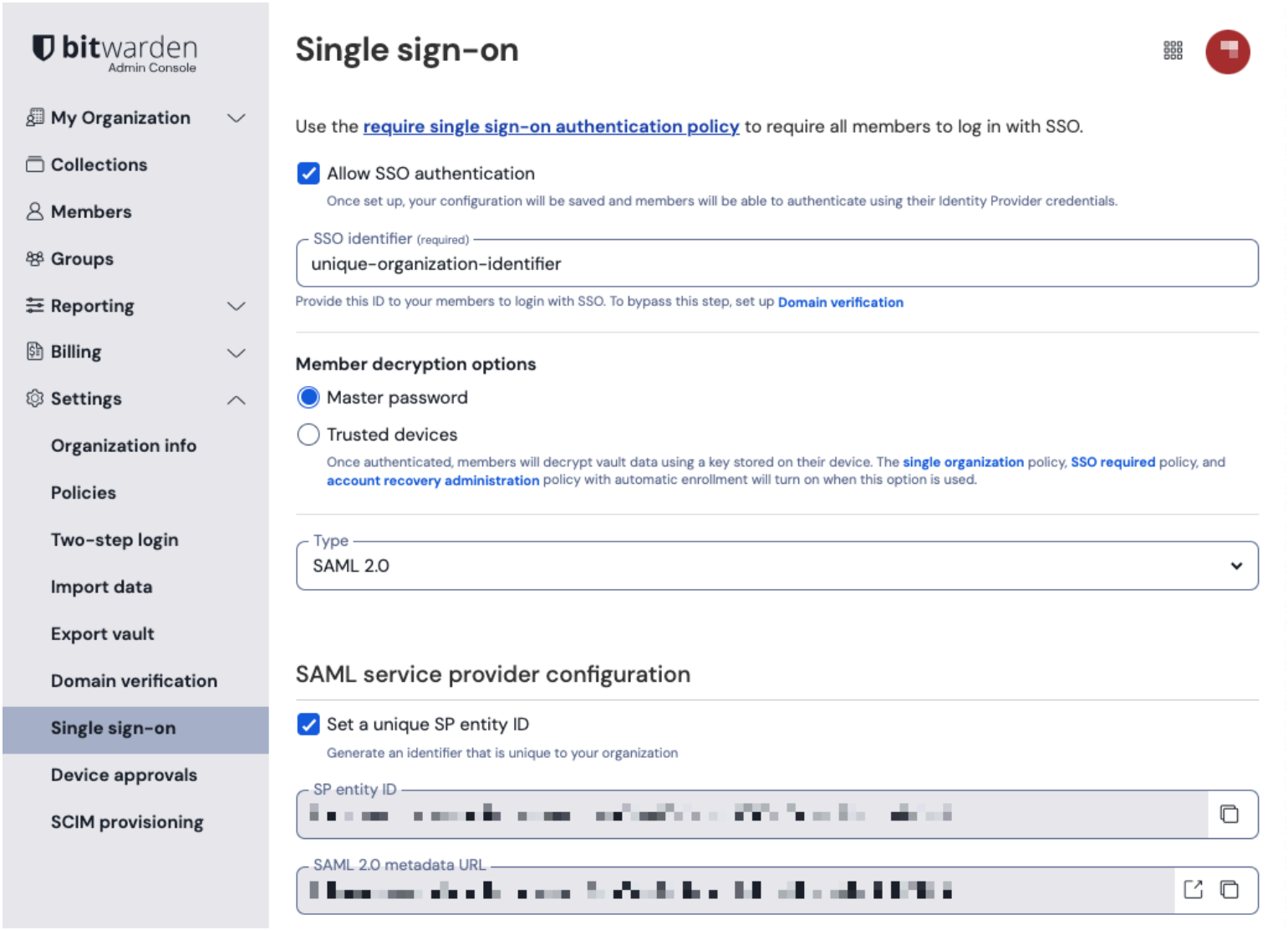
Ouvrez SSO dans l'application web

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. En faisant cela, votre identifiant d'organisation sera supprimé de la valeur de votre identifiant 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.

Créer une relation de confiance avec une partie dépendante

Dans le Gestionnaire de serveur AD FS, sélectionnez **Outils → Gestion AD FS → Action → Ajouter une relation de confiance de partie de confiance**. Dans l'assistant, faites les sélections suivantes :

1. Sur l'écran d'accueil, sélectionnez **Conscient des Réclamations**.

2. Sur l'écran Sélectionner la source de données, sélectionnez **Entrez les données concernant la partie dépendante manuellement**.

3. Sur l'écran Spécifier le nom d'affichage, entrez un nom d'affichage spécifique à Bitwarden.

4. Sur l'écran Configurer l'URL, sélectionnez **Activer le support pour le protocole WebSSO SAML 2.0**.
   - Dans le champ **URL du service SSO SAML 2.0 de la partie de confiance**, entrez l'URL du Service de Consommation d'Assertion (ACS). 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.

5. Sur l'écran **Choisir la politique de contrôle d'accès**, sélectionnez la politique de sécurité qui répond à vos normes de sécurité.

6. Sur l'écran **Configurer les identifiants**, ajoutez l'ID de l'entité SP en tant qu'identifiant de confiance de la partie de confiance. 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.

7. Sur l'écran **Choisir la politique de contrôle d'accès**, sélectionnez la politique souhaitée (par défaut, **Autoriser tout le monde**).

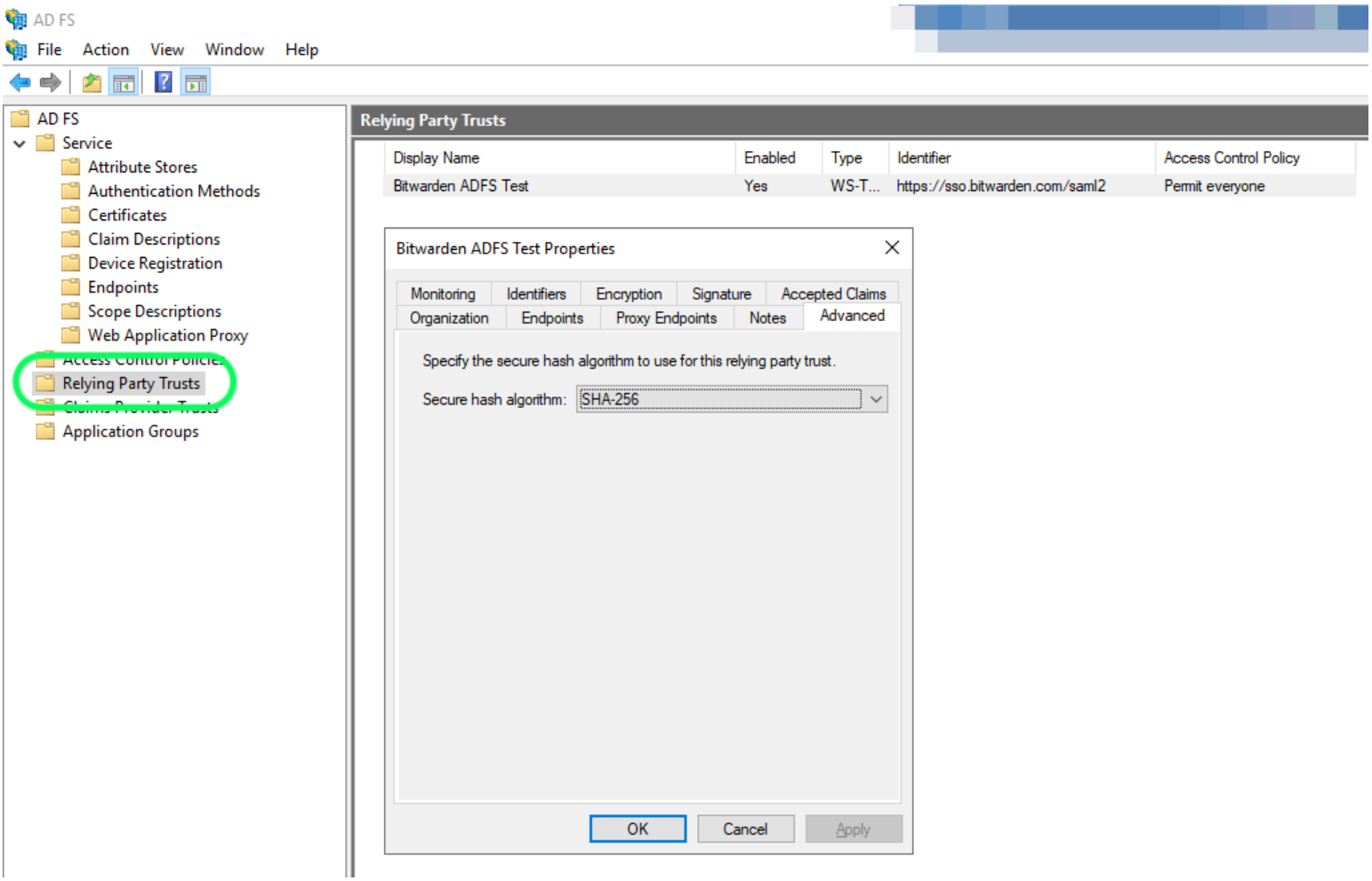
8. Sur l'écran **Prêt à Ajouter Confiance**, vérifiez vos sélections.

Options avancées

Une fois que la confiance de la partie dépendante est créée, vous pouvez configurer davantage ses paramètres en sélectionnant **Confiances de la partie dépendante** à partir du navigateur de fichiers à gauche et en sélectionnant le bon nom d'affichage.

Algorithme de hachage

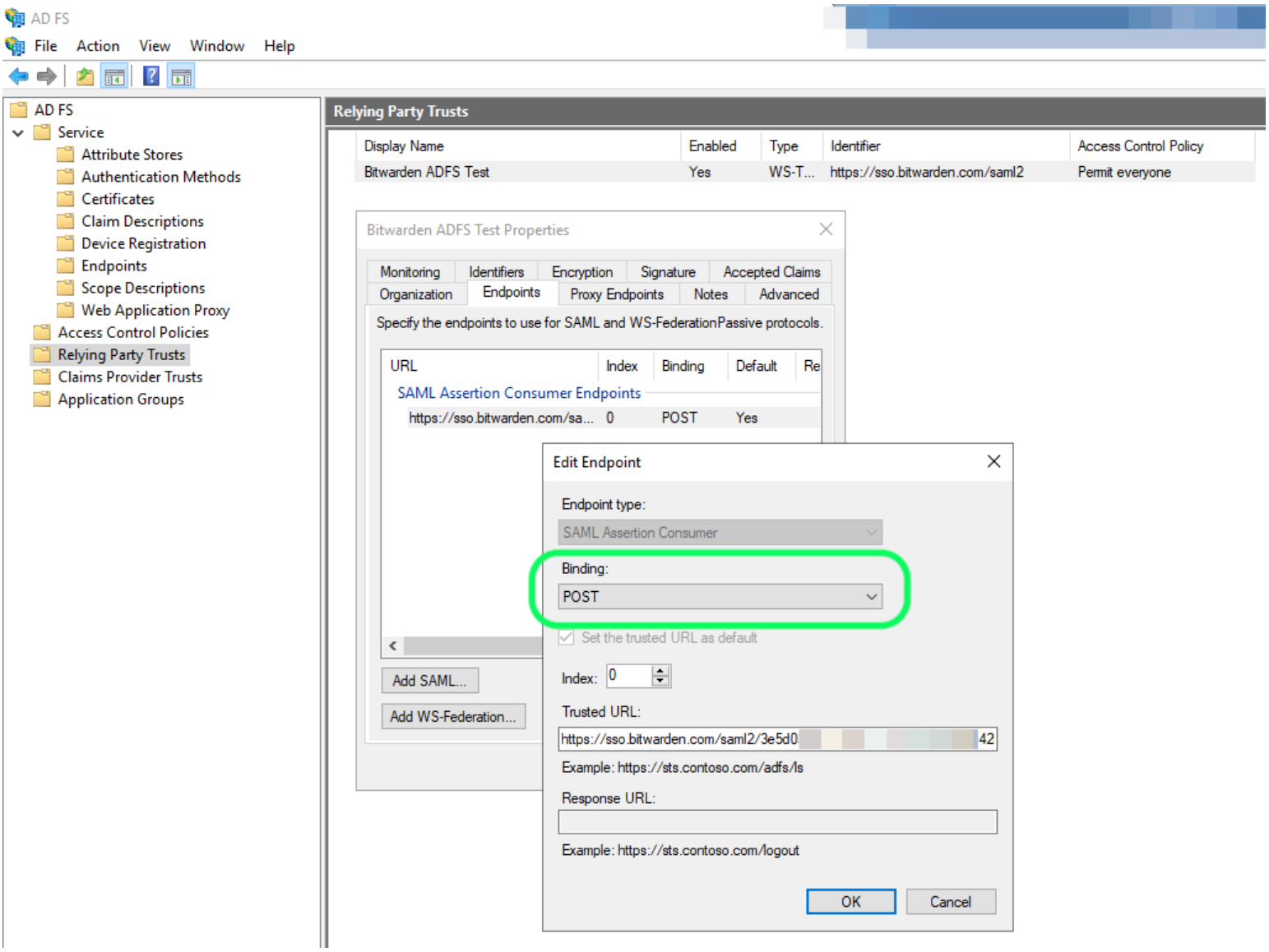
Pour changer l'**Algorithme de hachage sécurisé** (par défaut, SHA-256), naviguez vers l'**onglet Avancé** :



Définir un algorithme de hachage sécurisé

Liaison de point d'extrémité

Pour changer le point de terminaison **Binding** (par défaut, POST), naviguez vers l'**Endpoints** onglet et sélectionnez l'URL ACS configurée :

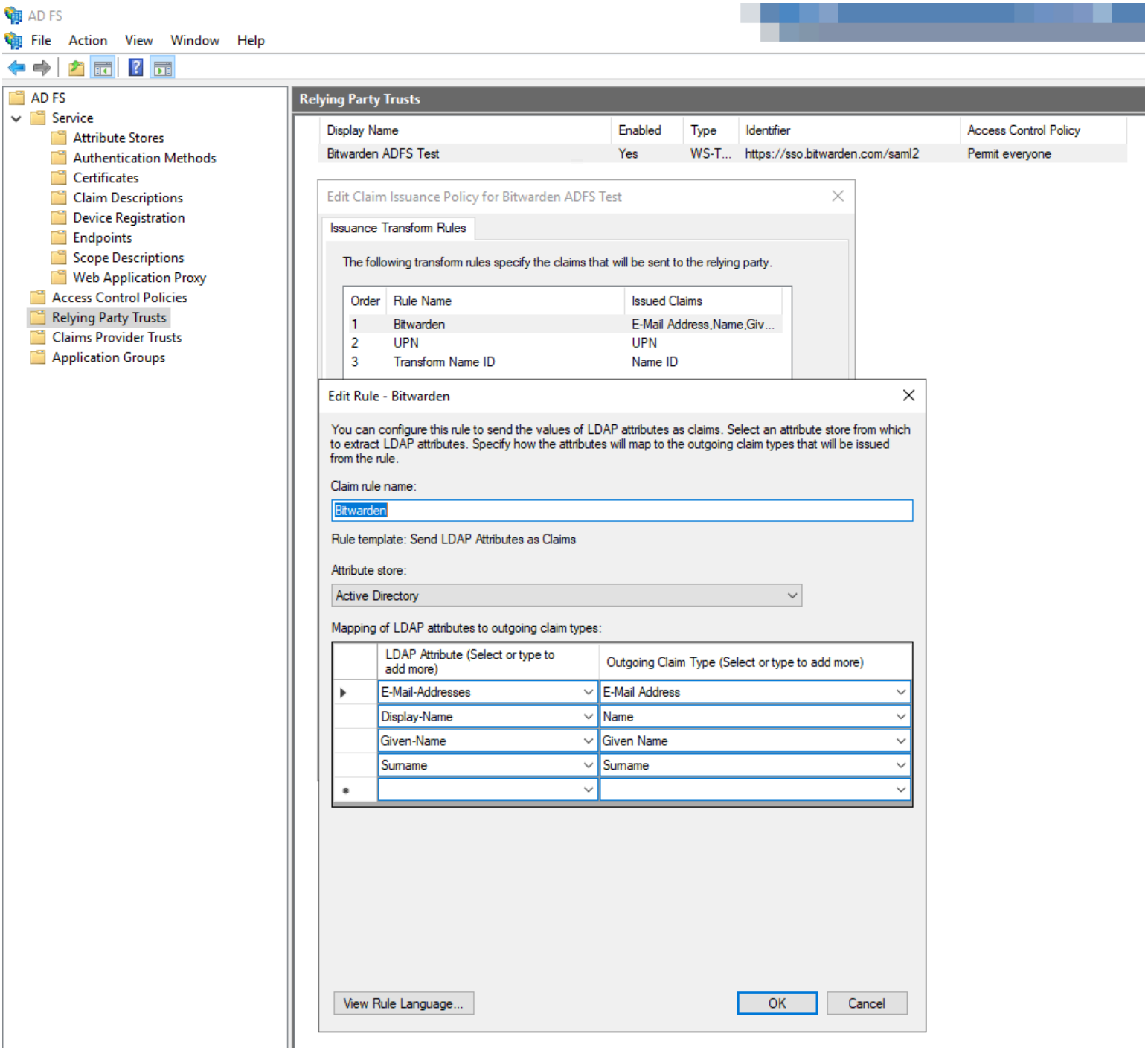


Éditer le Point d'Extrémité

Éditer les règles d'émission de revendications

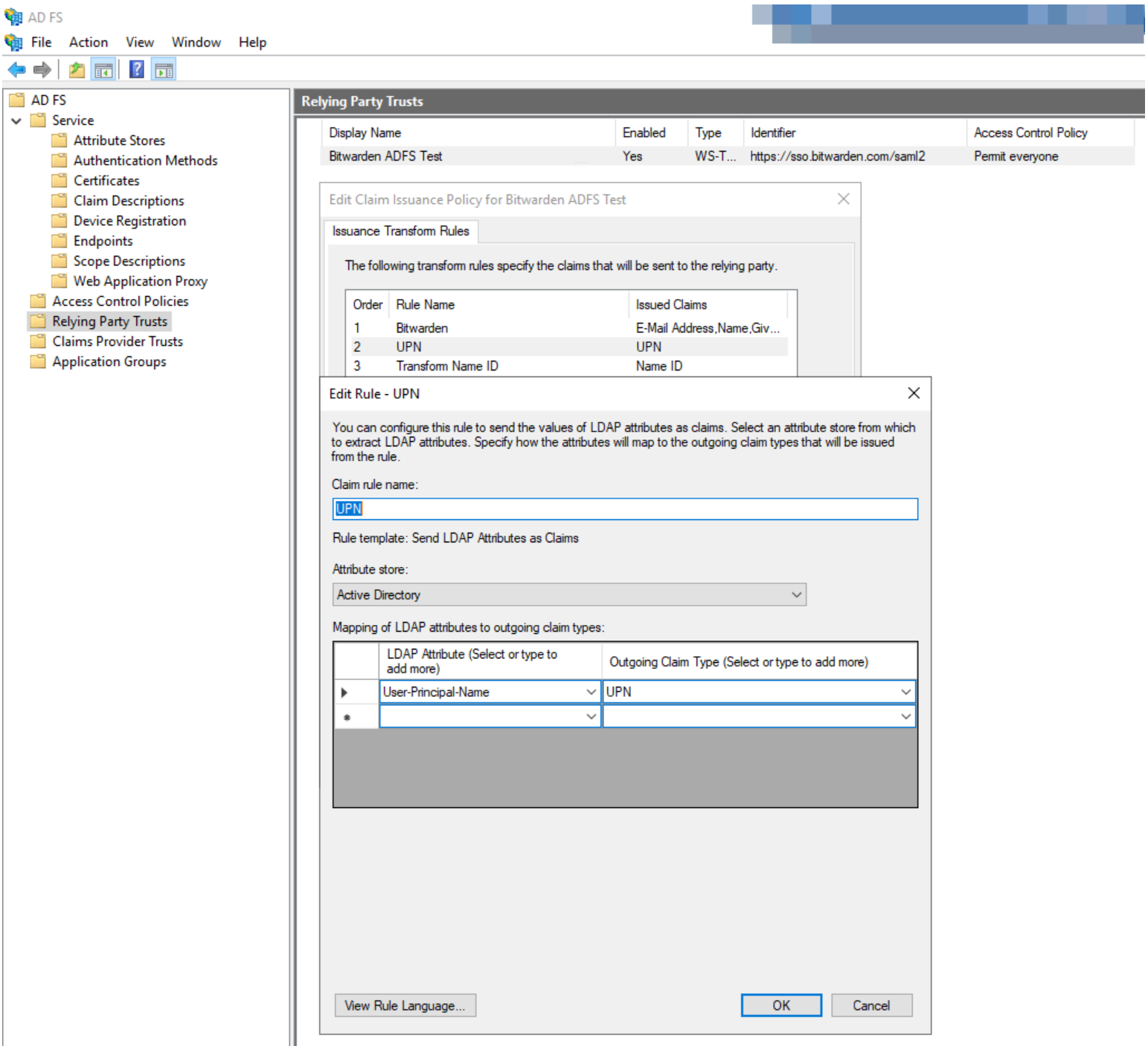
Construisez des règles d'émission de revendications pour garantir que les revendications appropriées, y compris **Name ID**, sont transmises à Bitwarden. Les onglets suivants illustrent un ensemble de règles exemple :

⇒Règle 1



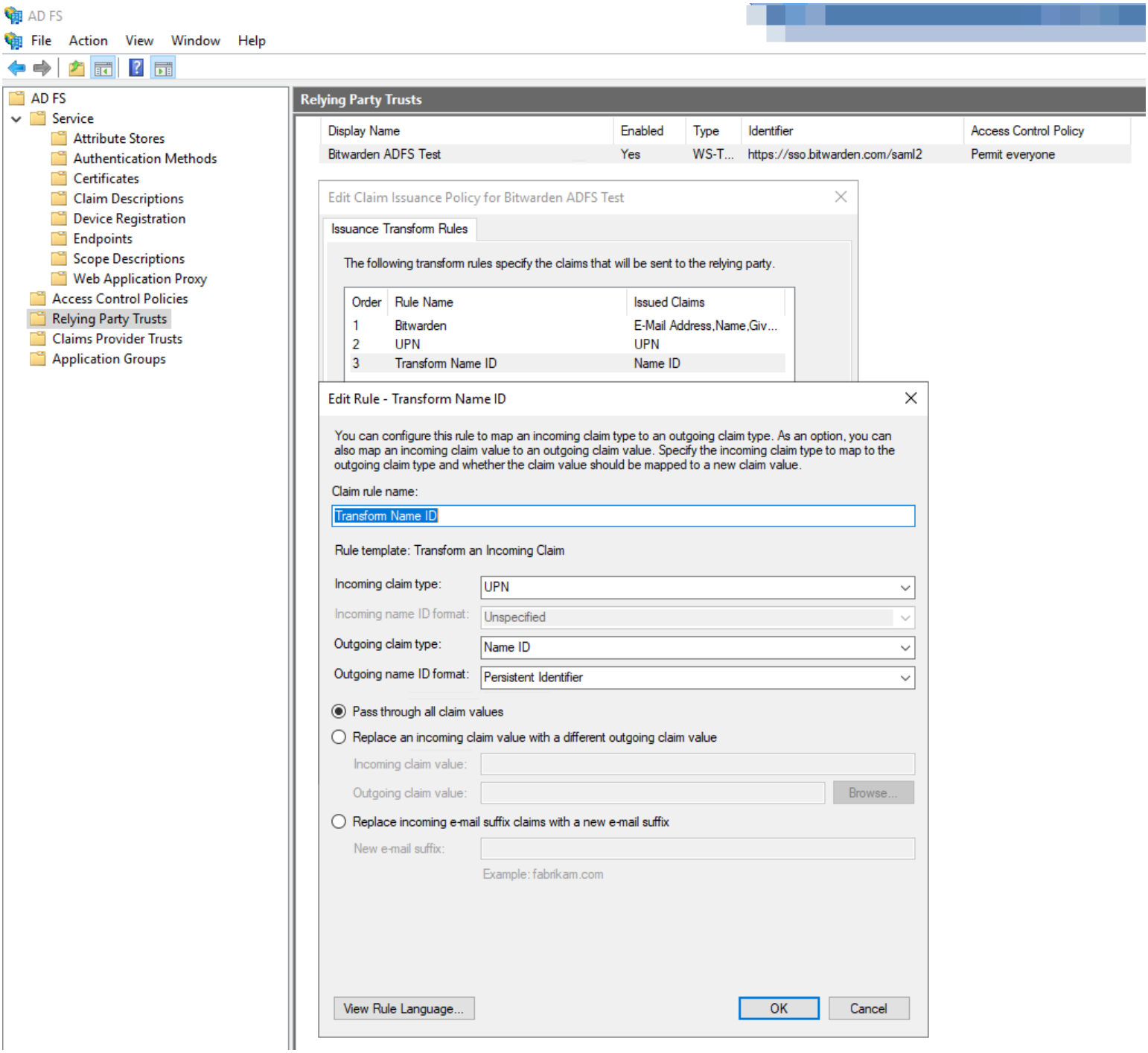
Règle ADFS 1

⇒Règle 2



Règle 2 ADFS

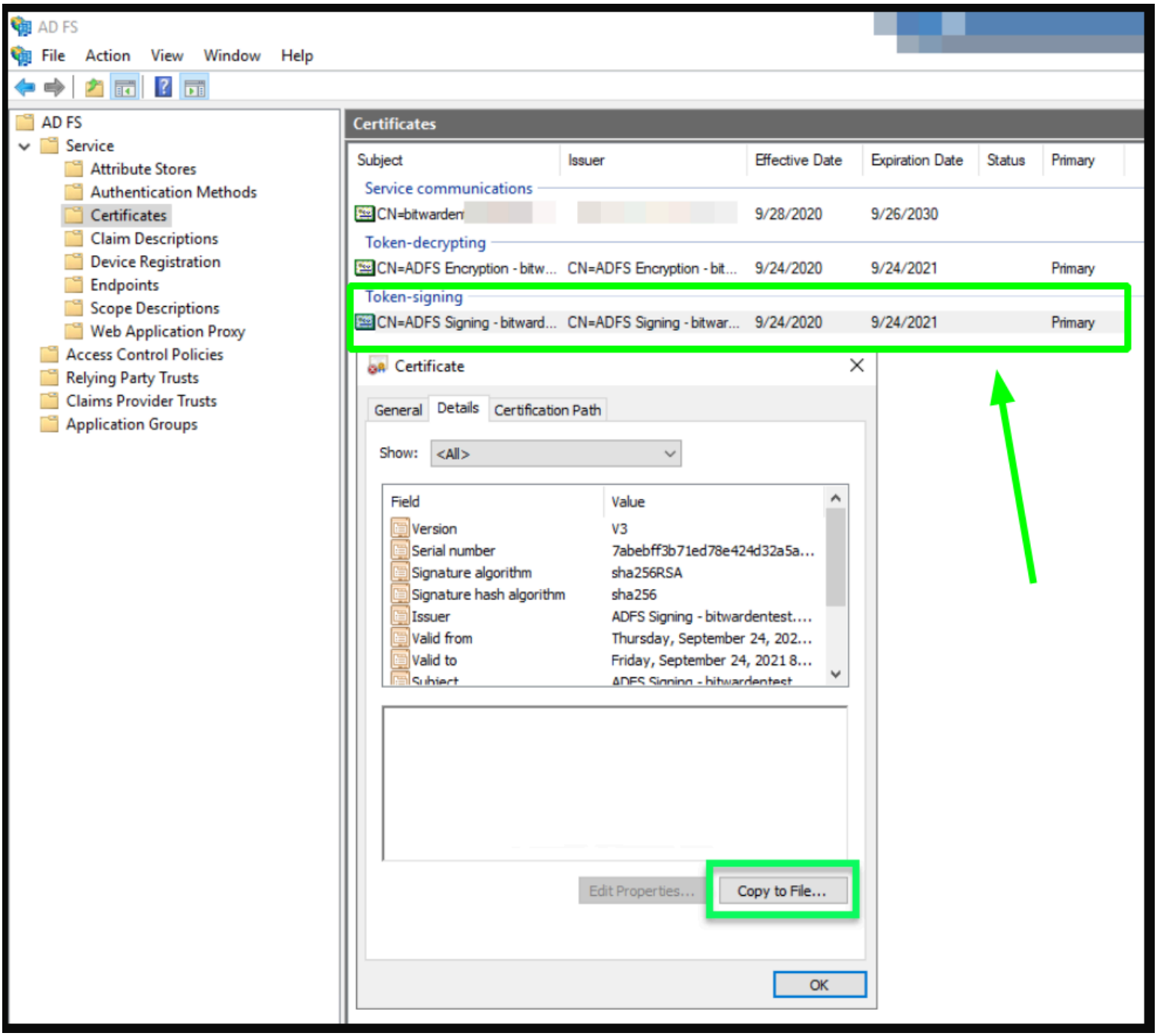
⇒Règle 3



Règle 3 ADFS

Obtenir un certificat

Dans le navigateur de fichiers à gauche, sélectionnez **AD FS → Service → Certificats** pour ouvrir la liste des certificats. Sélectionnez le certificat de **signature de jeton**, naviguez jusqu'à son **onglet Détails**, et sélectionnez le bouton **Copier vers le fichier...** pour exporter le certificat de signature de jeton encodé en Base-64 :

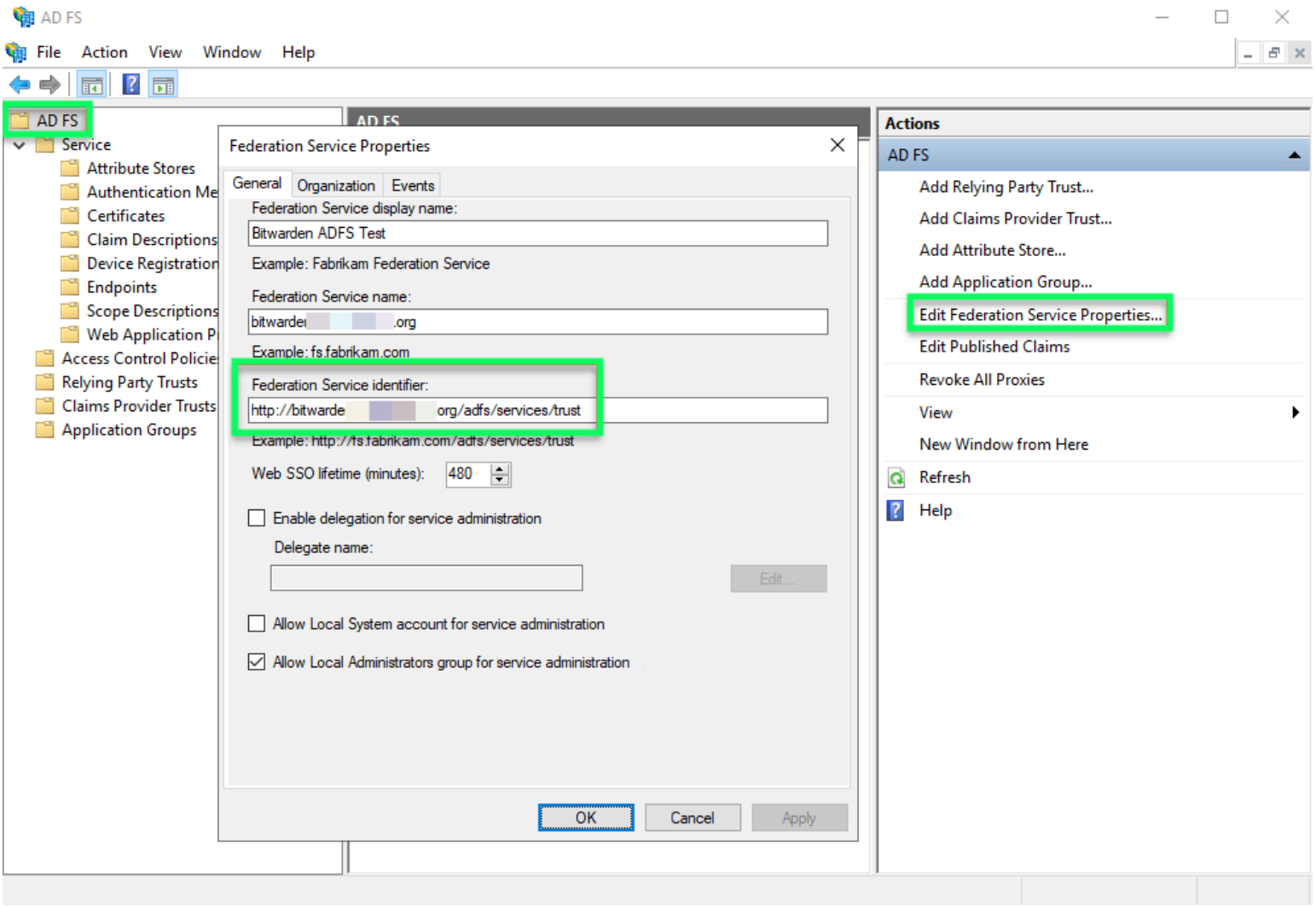


Obtenez le certificat de signature de jeton

Vous aurez besoin de ce certificat lors d'une étape ultérieure.

Obtenez l'identifiant du service de fédération

Dans le navigateur de fichiers à gauche, sélectionnez **AD FS** et dans le menu d'options à droite, sélectionnez **Éditer les propriétés du service de fédération**. Dans la fenêtre des propriétés du service de fédération, copiez l'**Identifiant du Service de Fédération** :



Obtenir l'identifiant du service de fédération

Vous aurez besoin de cet identifiant lors d'une étape ultérieure.

Retour à l'application web

À ce stade, vous avez configuré tout ce dont vous avez besoin dans le contexte du Gestionnaire de serveur AD FS. 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

Dans la section de configuration du fournisseur de services, configurez les champs suivants :

Champ	Description
Format de l'identifiant de nom	Sélectionnez le **Format d'ID de Nom Sortant** choisi lors de la construction des règles d'émission de réclamations (voir **Règle 3**).
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, AD FS signera avec SHA-256. Sélectionnez **SHA-256** dans le menu déroulant à moins que vous n'ayez configuré AD FS pour utiliser un algorithme différent.
Voulez des Assertions Signées	Que Bitwarden s'attend à ce que les assertions SAML soient signées.
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 l'identifiant Bitwarden 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 Gestionnaire de Serveur AD FS pour récupérer des valeurs :

Champ	Description
ID de l'entité	Entrez l'Identifiant du Service Fédération récupéré. Veuillez noter, cela **peut ne pas utiliser HTTPS**. Ce champ est sensible à la casse.

Champ	Description
Type de Reliure	Par défaut, AD FS utilisera la liaison de point de terminaison HTTP POST. Sélectionnez **HTTP POST** sauf si vous avez configuré AD FS pour utiliser une méthode différente.
URL du service de connexion unique	Entrez le point de terminaison du service SSO. Cette valeur peut être construite dans l'**Service → Points de terminaison** onglet dans le gestionnaire AD FS. L'URL de point de terminaison est répertoriée comme **Chemin URL pour SAML2.0/WS-Federation** et est généralement quelque chose comme `https://votre-domaine/adfs/ls`. Vous pouvez obtenir la valeur exacte à partir de la clé de configuration pour SingleSignOnServce dans le document `FederationMetadata.xml`.

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 certification**.

Algorithme de Signature Sortant	Par défaut, AD FS signera avec SHA-256. Sélectionnez **SHA-256** dans le menu déroulant à moins que vous n'ayez configuré AD FS pour utiliser un algorithme différent.
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 AD FS s'attend à ce que les demandes SAML soient signées.

Note

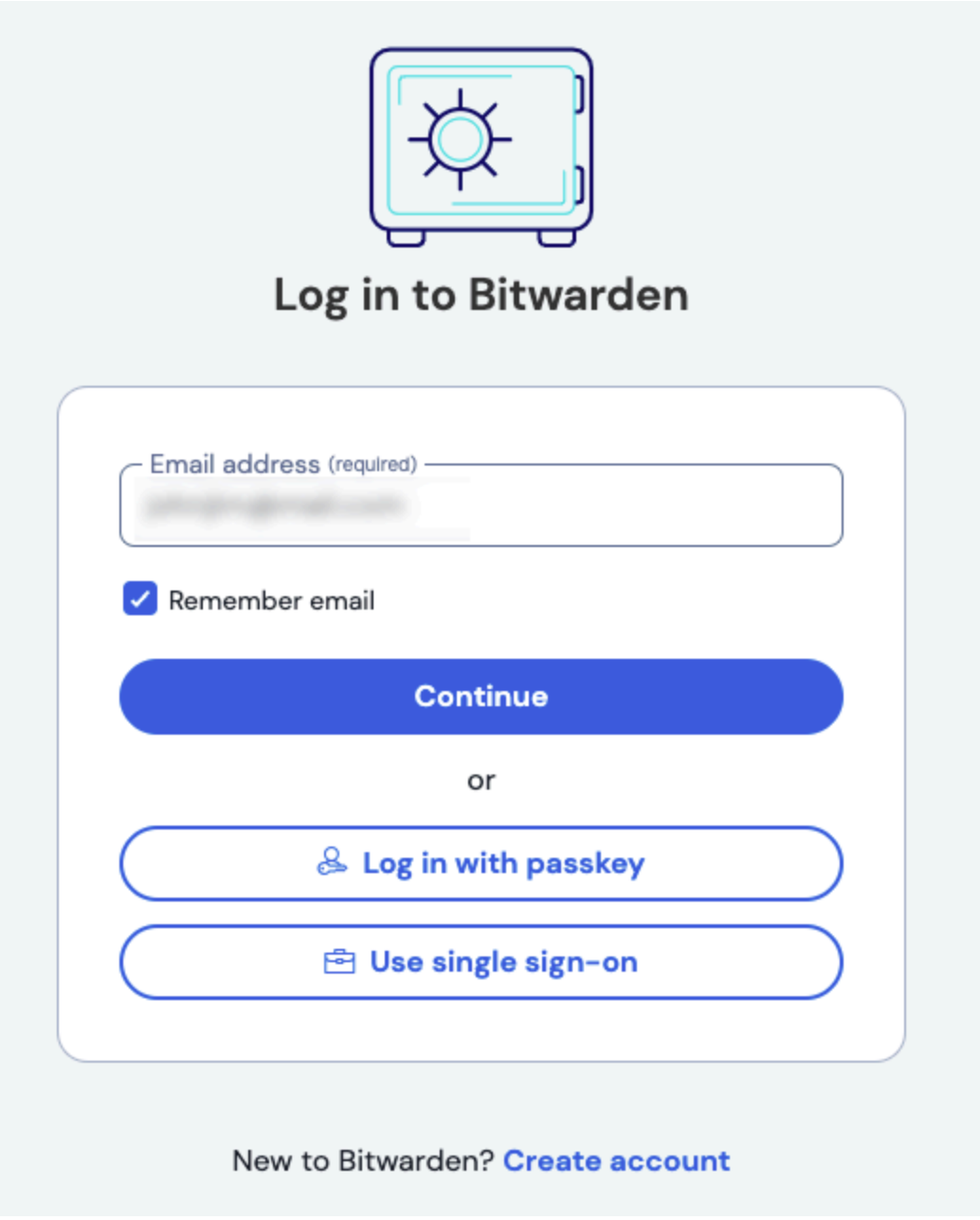
Lors de la complétion du certificat X509, prenez note de la date d'expiration. Les certificats devront être renouvelés afin d'éviter toute interruption de service pour les utilisateurs finaux de SSO. Si un certificat a expiré, les comptes Admin et Propriétaire pourront toujours se connecter avec l'adresse 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 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 correctement configurée, vous serez redirigé vers l'écran d'identifiant SSO AD FS. Après vous être authentifié avec vos identifiants AD FS, 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.