Implémentation ADFS OIDC

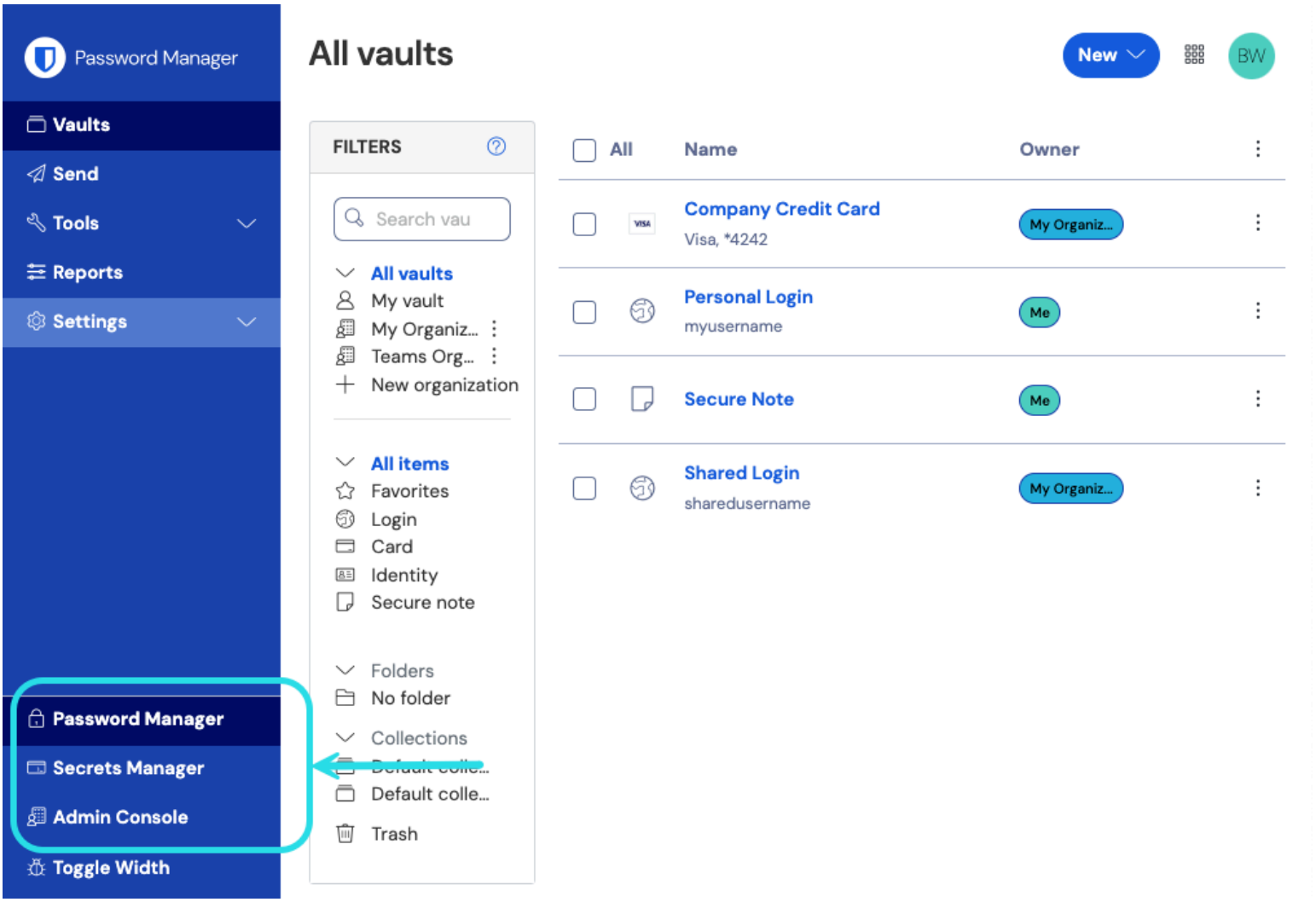
Implémentation ADFS OIDC

Cet article contient de l'aide **spécifique à Active Directory Federation Services (AD FS)** pour configurer l'identifiant avec SSO via OpenID Connect (OIDC). Pour obtenir de l'aide sur la configuration de l'identifiant avec SSO pour un autre IdP OIDC, ou pour configurer AD FS via SAML 2.0, voir Configuration OIDC ou Mise en œuvre ADFS SAML.

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.

Ouvrez SSO dans le coffre web

Connectez-vous à l'application web Bitwarden et ouvrez la console Admin à l'aide du sélecteur de produit (⊞):



commutateur-de-produit

Sélectionnez **Paramètres** → **Authentification unique** depuis la navigation :

Configuration OIDC

Si vous ne l'avez pas déjà fait, créez un **identifiant SSO** unique pour votre organisation. Sinon, vous n'avez pas besoin d'éditer quoi que ce soit sur cet écran pour l'instant, mais gardez-le ouvert pour une référence facile.

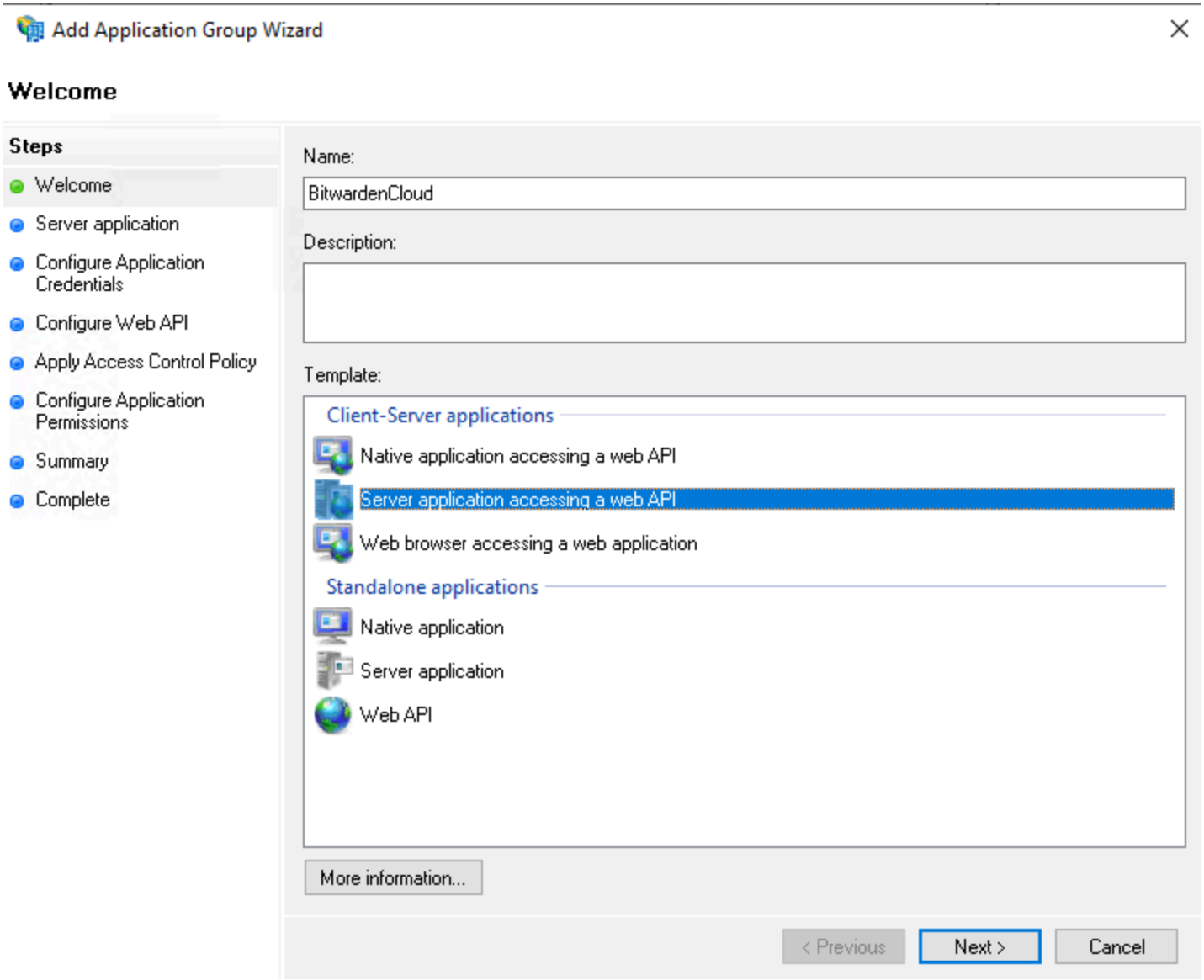
> **Tip**
>
> Il existe des options alternatives de **décryptage des membres**. Apprenez comment commencer à utiliser SSO avec des appareils de confiance ou Key Connector.

Créez un groupe d'application

Dans Gestionnaire de serveur, naviguez jusqu'à **Gestion AD FS** et créez un nouveau groupe d'application :

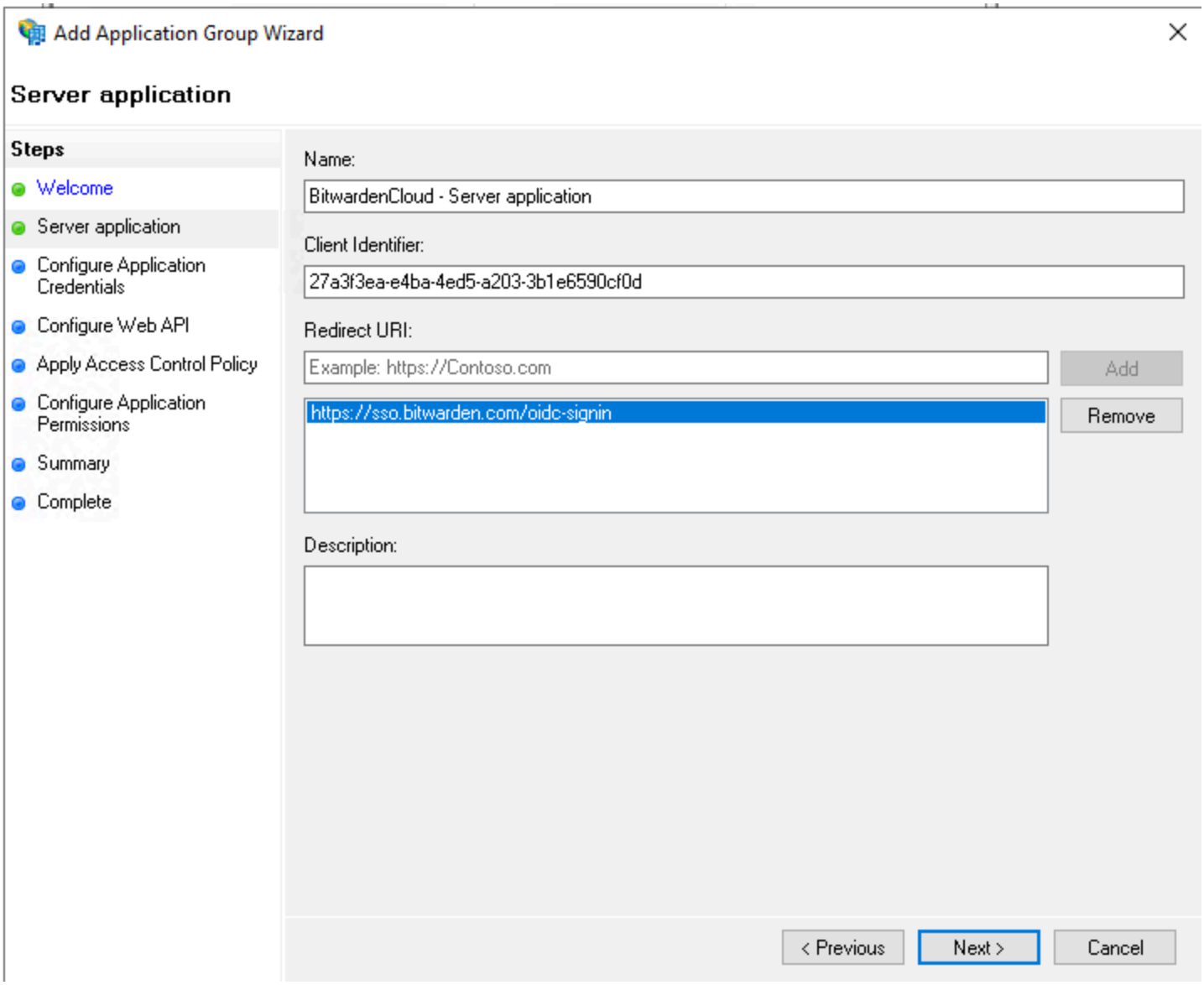
1. Dans l'arborescence de la console, sélectionnez **Groupes d'applications** et choisissez **Ajouter un groupe d'applications** dans la liste des actions.

2. Sur l'écran d'accueil de l'assistant, choisissez le modèle **Application serveur accédant à une API web**.



AD FS Add Application Group

3. Sur l'écran de l'application serveur:

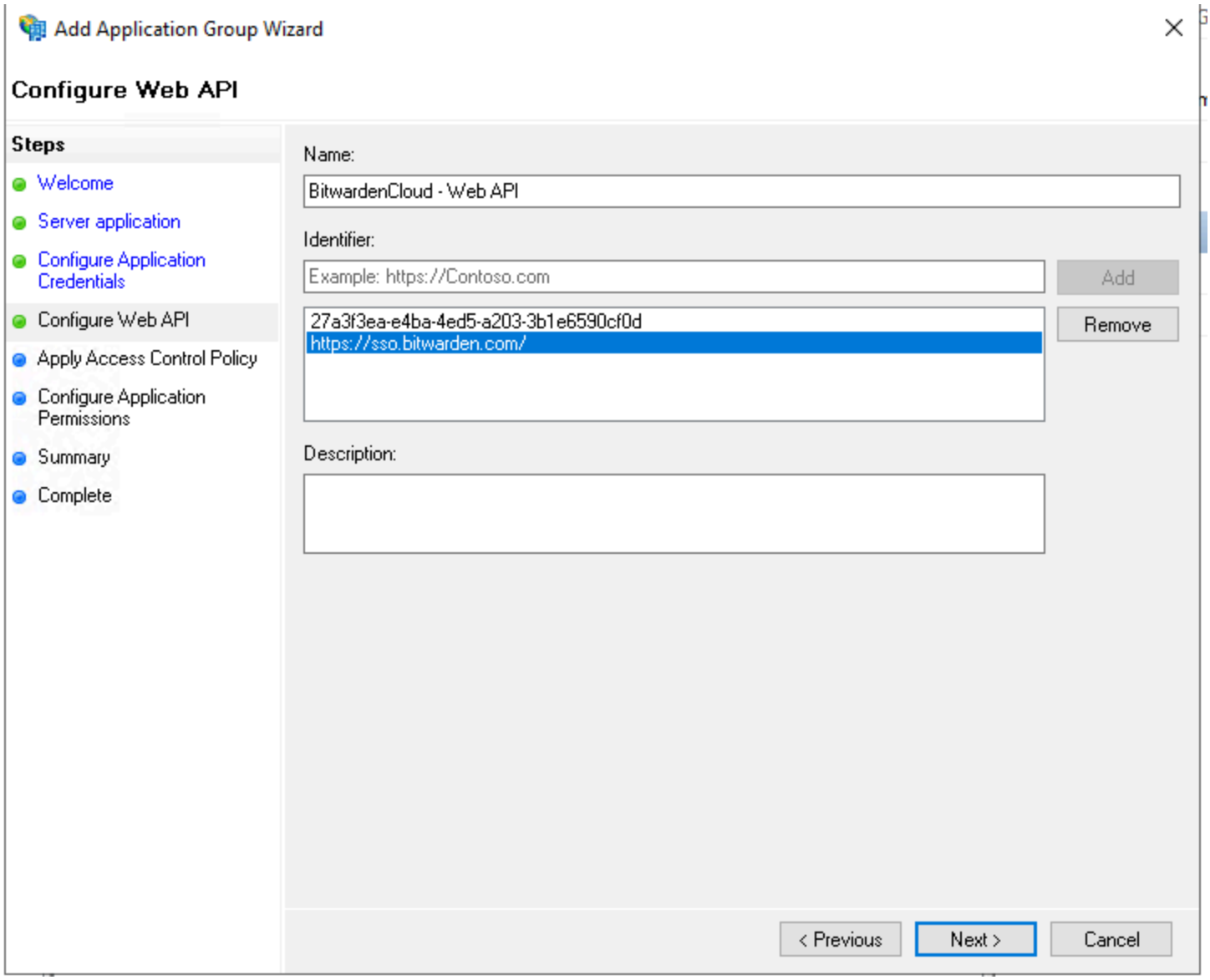


AD FS Server Application screen

- Donnez à l'application serveur un **Nom**.
- Prenez note de l'**Identifiant du client**. Vous aurez besoin de cette valeur dans une étape ultérieure.
- Spécifiez une **URI de redirection**. Pour les clients hébergés dans le cloud, c'est `https://sso.bitwarden.com/oidc-signin` ou `https://sso.bitwarden.eu/oidc-signin`. Pour les instances auto-hébergées, cela est déterminé par votre URL de serveur configurée, par exemple `https://votre.domaine.com/sso/oidc-signin`.

4. Sur l'écran Configurer les identifiants de l'application, prenez note du **Secret du client**. Vous aurez besoin de cette valeur dans une étape ultérieure.

5. Sur l'écran de configuration de l'API Web :

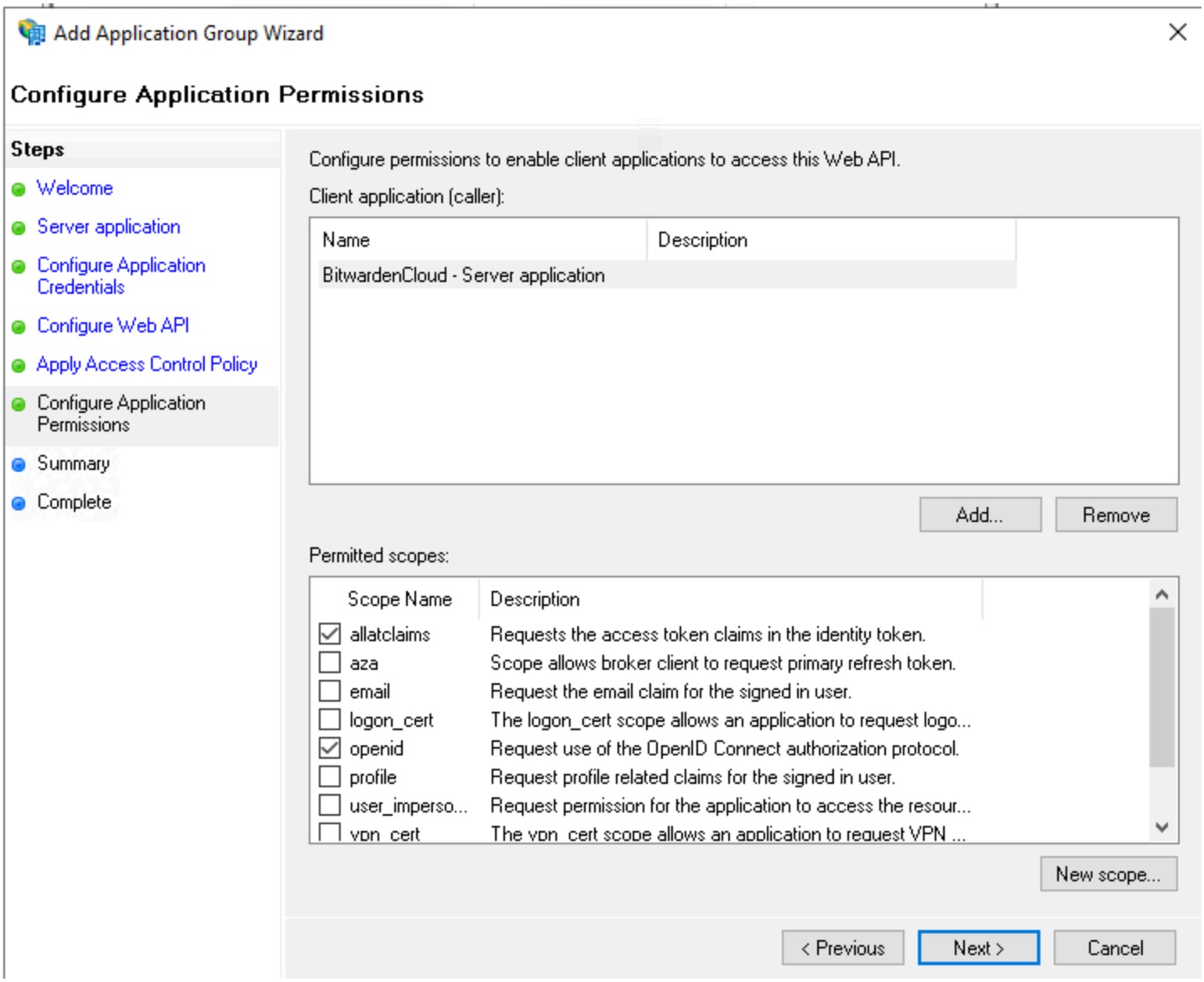


AD FS Configure Web API screen

- Donnez un **Nom** à l'API Web.
- Ajoutez l'**Identifiant du client** et l'**URI de redirection** (voir étape 2B. & C.) à la liste des identifiants.

6. Sur l'écran Appliquer la politique de contrôle d'accès, définissez une politique de contrôle d'accès appropriée pour le groupe d'applications.

7. Sur l'écran de configuration des autorisations d'application, autorisez les portées `allatclaims` et `openid`.



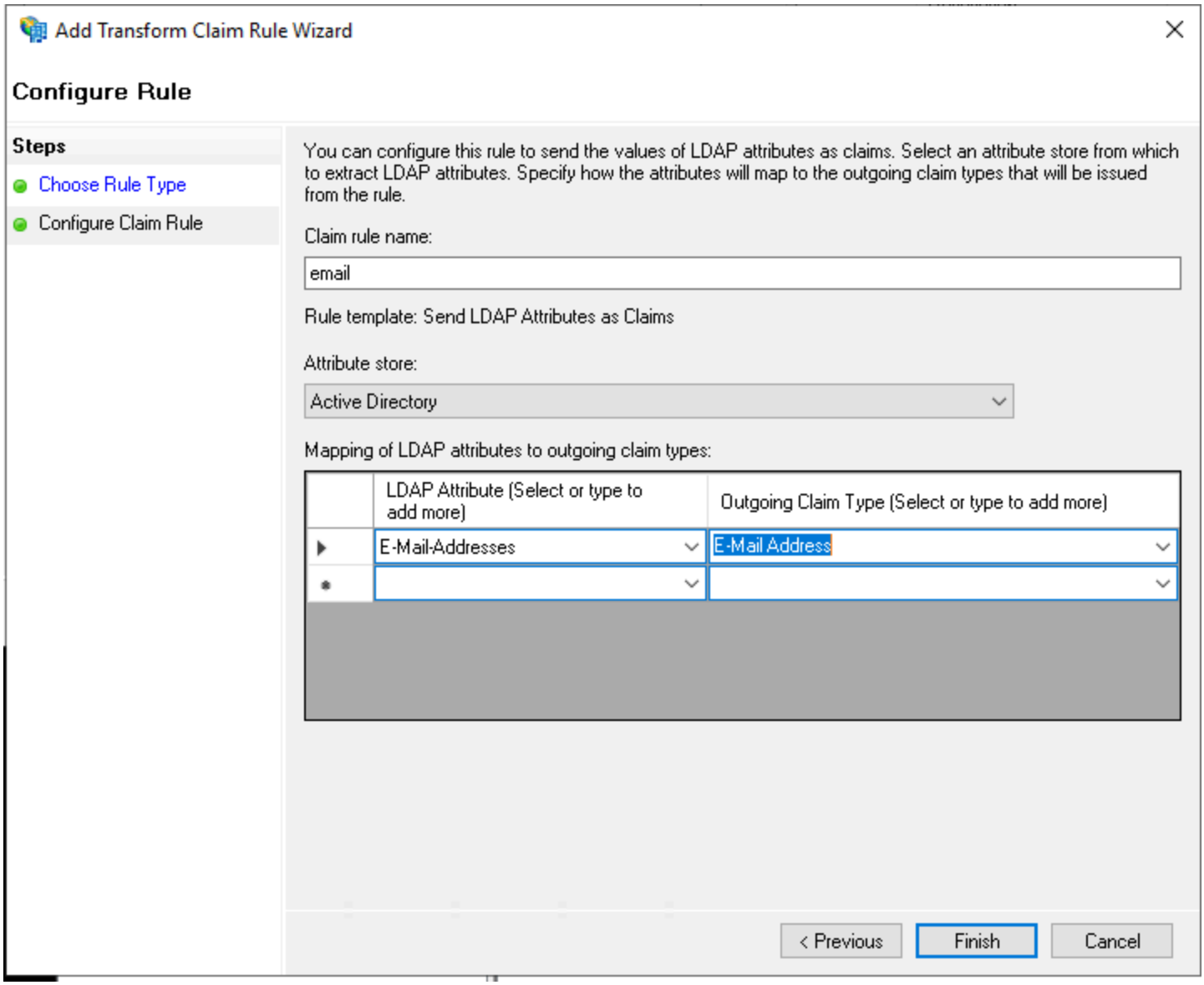
AD FS Configure Application Permissions screen

8. Terminez l'assistant d'ajout de groupe d'applications.

Ajoutez une règle de revendication de transformation

Dans Gestionnaire de serveur, naviguez jusqu'à **Gestion AD FS** et éditez le groupe d'applications créé :

1. Dans l'arborescence de la console, sélectionnez **Groupes d'applications**.
2. Dans la liste des groupes d'applications, faites un clic droit sur le groupe d'applications créé et sélectionnez **Propriétés**.
3. Dans la section Applications, choisissez l'API Web et sélectionnez **Éditer...** .
4. Naviguez vers l'**onglet Règles de Transformation d'Émission** et sélectionnez le bouton **Ajouter une règle...** .
5. Sur l'écran Choisir le type de règle, sélectionnez **Envoyer les attributs LDAP comme revendications.**
6. Sur l'écran Configurer la règle de revendication :



AD FS Configure Claim Rule screen

- Donnez à la règle un **Nom de règle de revendication**.
- Dans le menu déroulant Attribut LDAP, sélectionnez **Adresses E-Mail.**
- Dans le menu déroulant du type de réclamation sortant, sélectionnez **Adresse E-Mail**.

7. Sélectionnez **Terminer.**

Retour à l'application web

À ce stade, vous avez configuré tout ce dont vous avez besoin dans le cadre du gestionnaire de serveur AD FS. Retournez à l'application web Bitwarden pour configurer les champs suivants :

Champ	Description
Autorité	Entrez le nom d'hôte de votre serveur AD FS avec `/adfs` ajouté, par exemple `https://adfs.monentreprise.com/adfs`.
Client ID	Entrez l'ID du client récupéré.
Secret du Client	Entrez le Secret du Client récupéré.
Adresse des métadonnées	Entrez la valeur d'**Autorité** spécifiée avec `/.well-known/openid-configuration` ajouté, par exemple `https://adfs.mybusiness.com/adfs/.well-known/openid-configuration`.
Comportement de redirection OIDC	Sélectionnez **Rediriger GET**.
Récupérer les claims depuis l'endpoint d'informations utilisateur (User Info Endpoint)	Activez cette option si vous recevez des erreurs d'URL trop longues (HTTP 414), des URLS tronquées, et/ou des échecs lors de l'SSO.
Portées personnalisées	Définissez des portées personnalisées à ajouter à la demande (séparées par des virgules).
Types de revendications d'identifiant d'utilisateur client	Définir des clés de type de revendication personnalisées pour l'identification de l'utilisateur (délimitées par des virgules). Lorsqu'ils sont définis, les types de revendications personnalisés sont recherchés avant de se rabattre sur les types standard.
Types de revendications de courriel	Définissez des clés de type de revendication personnalisées pour les adresses de courriel des utilisateurs (délimitées par des virgules). Lorsqu'ils sont définis, les types de revendications personnalisés sont recherchés avant de se rabattre sur les types standard.
Types de revendication de nom personnalisé	Définissez des clés de type de revendication personnalisées pour les noms complets ou les noms d'affichage des utilisateurs (délimités par des virgules). Lorsqu'ils sont définis, les types de revendications personnalisés sont recherchés avant de revenir sur les types standard.

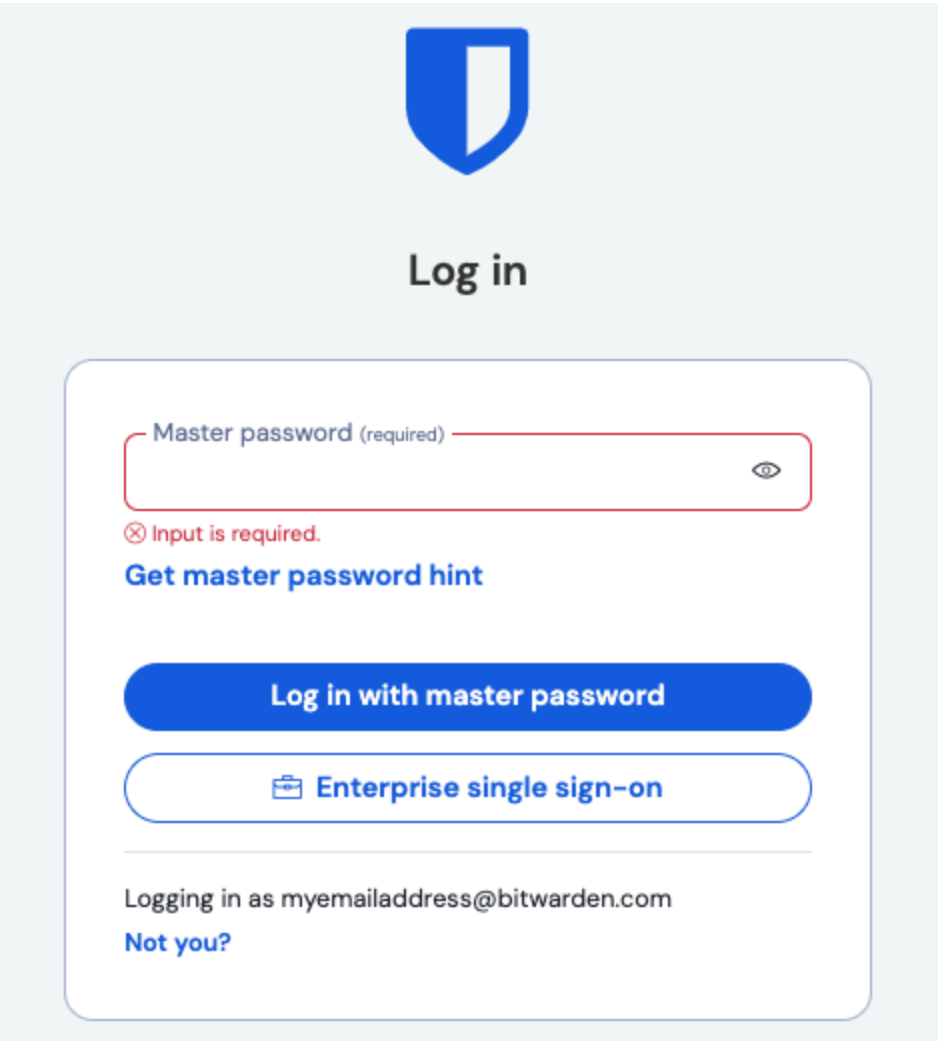
Champ	Description
Valeurs demandées pour les références de classe de contexte d'authentification	Définissez les identifiants de référence de classe de contexte d'authentification (`acr_values`) (séparés par des espaces). Listez `acr_values` dans l'ordre de préférence.
Valeur de revendication "acr" attendue en réponse	Définissez la valeur de revendication `acr` que Bitwarden doit attendre et valider dans la réponse.

Lorsque vous avez terminé de configurer ces champs, **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'ID de l'organisation configurée 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.