ADFS OIDC Implementierung

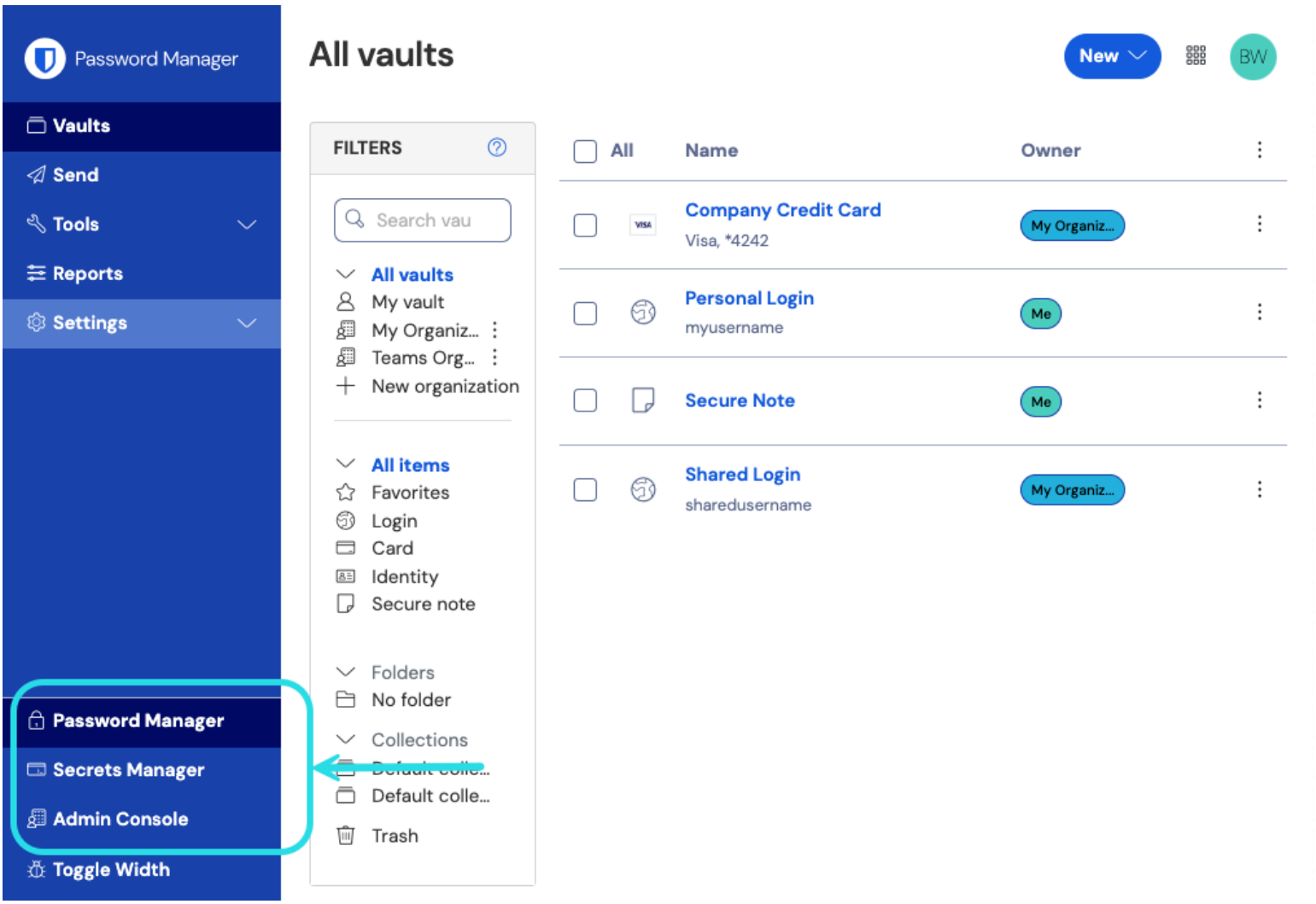
ADFS OIDC Implementierung

Dieser Artikel enthält **Active Directory Federation Services (AD FS)-spezifische** Hilfe zur Konfiguration der Zugangsdaten mit SSO über OpenID Connect (OIDC). Für Hilfe bei der Konfiguration der Zugangsdaten mit SSO für einen anderen OIDC IdP oder bei der Konfiguration von AD FS über SAML 2.0, siehe OIDC Konfiguration oder ADFS SAML Implementierung.

Die Konfiguration beinhaltet das gleichzeitige Arbeiten innerhalb der Bitwarden-Web-App und dem AD FS Server-Manager. Während Sie fortfahren, empfehlen wir, beides griffbereit zu haben und die Schritte in der Reihenfolge durchzuführen, in der sie dokumentiert sind.

Öffnen Sie SSO im Web-Tresor

Melden Sie sich bei der Bitwarden Web-App an und öffnen Sie die Administrator-Konsole mit dem Produktumschalter (▦):



Produktwechsler

Wählen Sie **Einstellungen → Einmaliges Anmelden** aus der Navigation:

OIDC-Konfiguration

Wenn Sie es noch nicht getan haben, erstellen Sie einen einzigartigen **SSO-Identifier** für Ihre Organisation. Andernfalls müssen Sie auf diesem Bildschirm noch nichts bearbeiten, lassen Sie ihn aber offen, um ihn leicht referenzieren zu können.

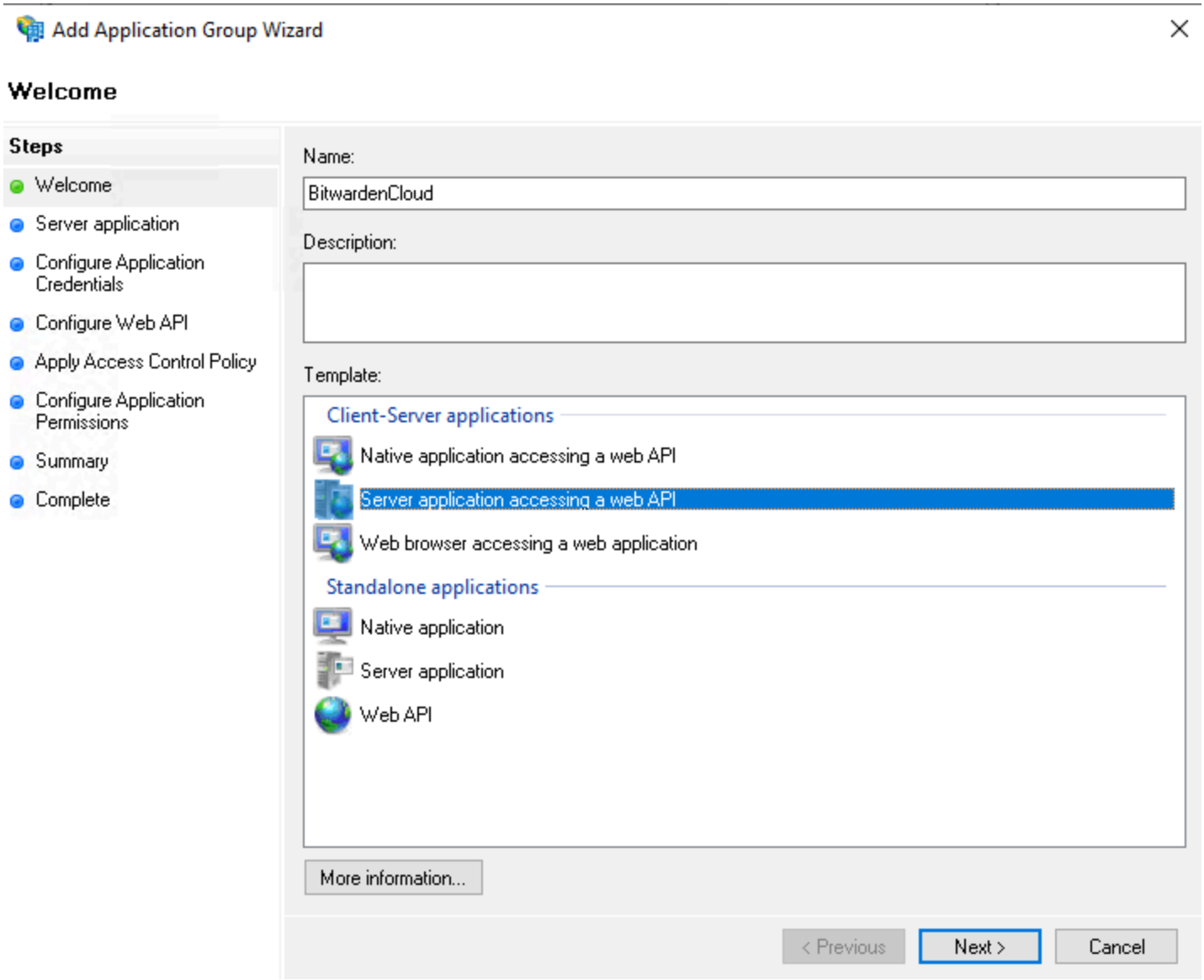
> **Tip**
>
> Es gibt alternative **Mitglied Entschlüsselungsoptionen**. Erfahren Sie, wie Sie mit SSO auf vertrauenswürdigen Geräten oder mit Key Connector beginnen können.

Erstellen Sie eine Anwendungsgruppe

Im Server-Manager navigieren Sie zu **AD FS Verwaltung** und erstellen eine neue Anwendungsgruppe:

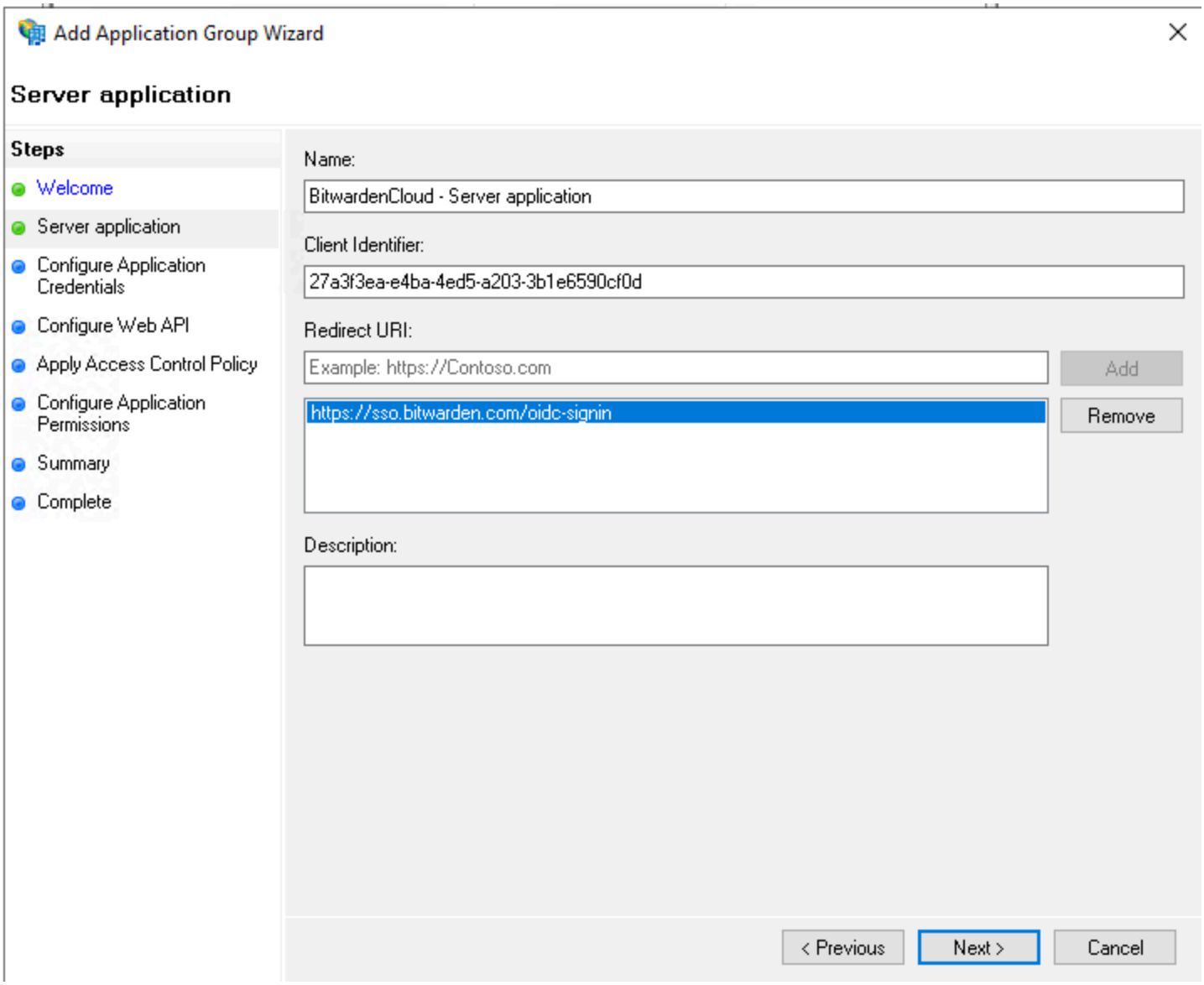
1. Im Konsolenbaum wählen Sie **Anwendungsgruppen** und wählen Sie **Anwendungsgruppe hinzufügen** aus der Aktionsliste.

2. Auf dem Willkommensbildschirm des Assistenten wählen Sie die Vorlage **Serveranwendung, die auf eine Web-API zugreift**.



AD FS Add Application Group

3. Auf dem Serveranwendungs-Bildschirm:

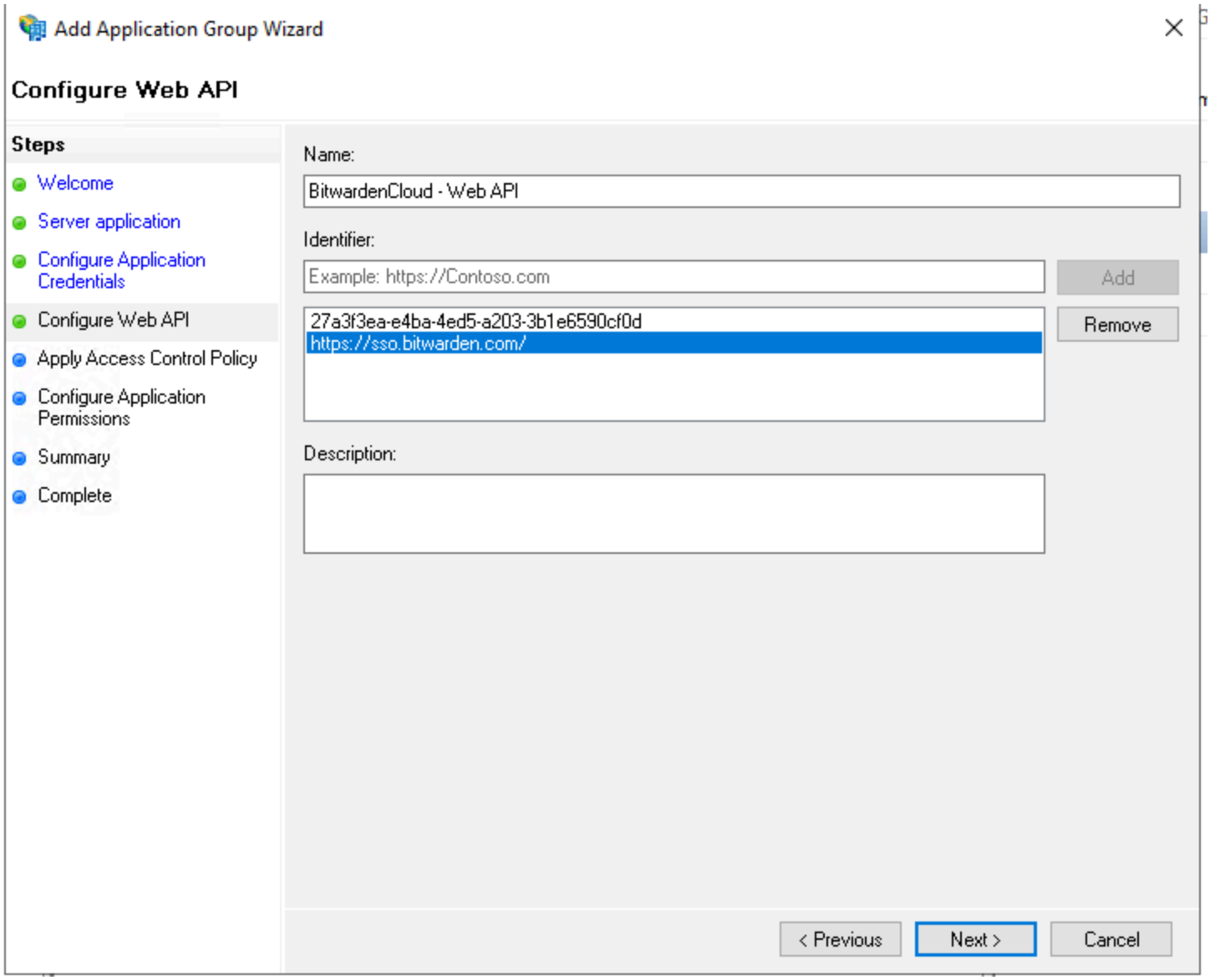


AD FS Server Application screen

- Geben Sie der Serveranwendung einen **Namen**.
- Notieren Sie die **Client-Kennung**. Sie werden diesen Wert in einem nachfolgenden Schritt benötigen.
- Geben Sie eine **Weiterleitungs-URI** an. Für Kunden, die in der Cloud gehostet werden, ist dies `https://sso.bitwarden.com/oidc-signin` oder `https://sso.bitwarden.eu/oidc-signin`. Für selbst gehostete Instanzen wird dies durch Ihre konfigurierte Server-URL bestimmt, zum Beispiel `https://your.domain.com/sso/oidc-signin`.

4. Auf dem Bildschirm zur Konfiguration der Anwendungsdaten, nehmen Sie eine Notiz vom **Client Secret**. Sie werden diesen Wert in einem nachfolgenden Schritt benötigen.

5. Auf dem Konfigurationsbildschirm für die Web-API:

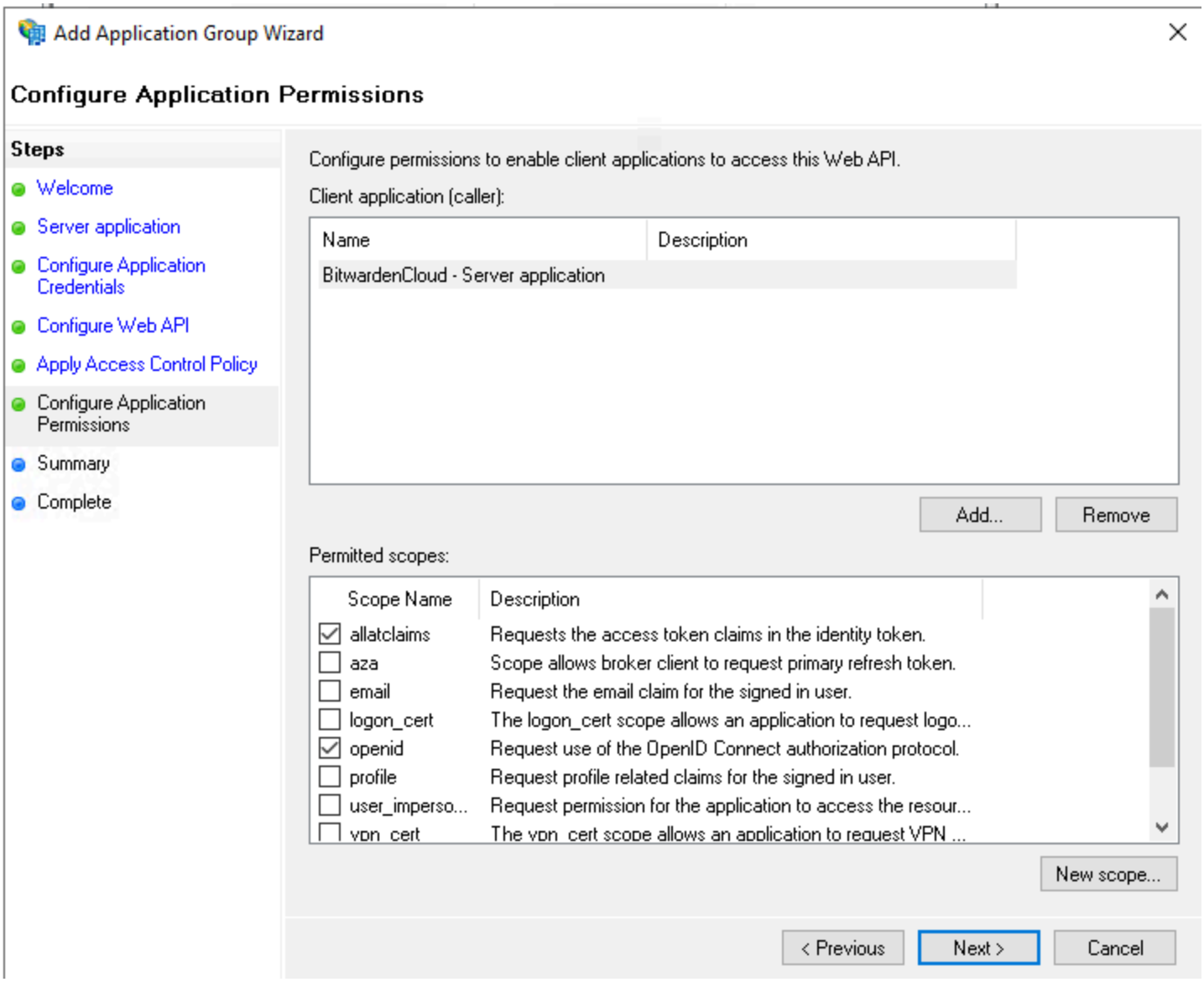


AD FS Configure Web API screen

- Geben Sie der Web-API einen **Namen**.
- Fügen Sie die **Client-Kennung** und die **Weiterleitungs-URI** (siehe Schritt 2B. & C.) zur Kennungsliste hinzu.

6. Auf dem Bildschirm "Zugriffskontrollrichtlinie anwenden" legen Sie eine geeignete Zugriffskontrollrichtlinie für die Anwendungsgruppe fest.

7. Auf dem Bildschirm zur Konfiguration der Anwendungsberechtigungen, erlauben Sie die Bereiche `allatclaims` und `openid`.



AD FS Configure Application Permissions screen

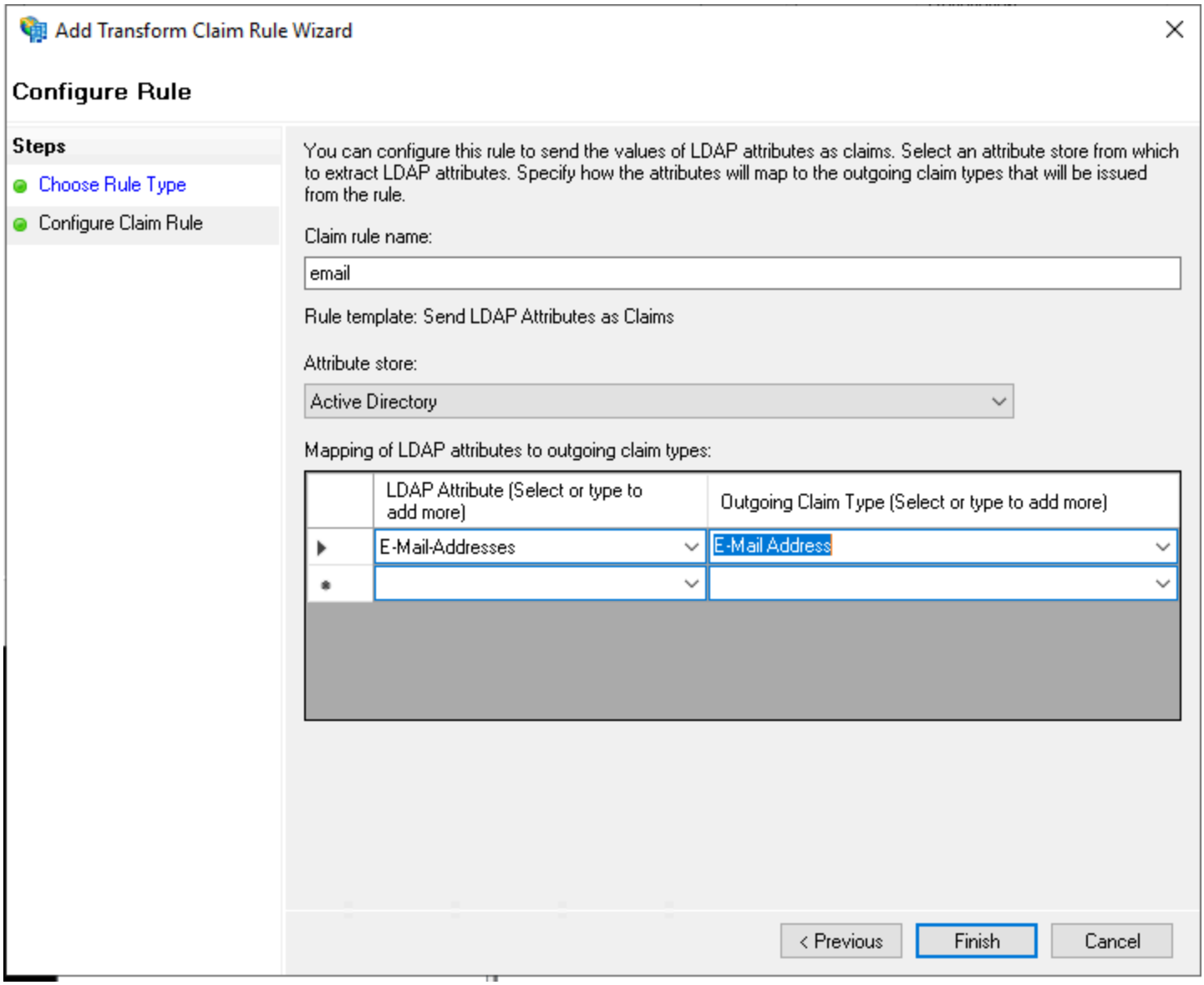
8. Schließen Sie den Assistenten zum Hinzufügen von Anwendungsgruppen ab.

Fügen Sie eine Transformationsanspruch-Regel hinzu

Im Server-Manager navigieren Sie zu **AD FS Verwaltung** und bearbeiten die erstellte Anwendungsgruppe:

1. Im Konsolenbaum wählen Sie **Anwendungsgruppen**.
2. In der Liste der Anwendungsgruppen klicken Sie mit der rechten Maustaste auf die erstellte Anwendungsgruppe und wählen Sie **Eigenschaften** aus.
3. Im Abschnitt Anwendungen wählen Sie die Web API und wählen **Bearbeiten...** .
4. Navigieren Sie zum **Ausgabenumwandlungsregeln** Tab und wählen Sie die **Regel hinzufügen...** Schaltfläche aus.
5. Auf dem Bildschirm Regeltyp auswählen, wählen Sie **Senden Sie LDAP-Attribute als Ansprüche.**

6. Auf dem Bildschirm "Anspruchsregel konfigurieren":



AD FS Configure Claim Rule screen

- Geben Sie der Regel einen **Anspruchsregelnamen**.
- Aus dem LDAP-Attribut-Dropdown wählen Sie **E-Mail-Adressen.**
- Wählen Sie aus dem Dropdown-Menü für den ausgehenden Anspruchstyp **E-Mail-Adresse**.

7. Auswählen **Fertig.**

Zurück zur Web-App

Bis zu diesem Zeitpunkt haben Sie alles, was Sie im Rahmen des AD FS Server Manager benötigen, konfiguriert. Kehren Sie zur Bitwarden-Webanwendung zurück, um die folgenden Felder zu konfigurieren:

Feld	Beschreibung
Zertifizierungsstelle	Geben Sie den Hostnamen Ihres AD FS-Servers mit `/adfs` angehängt ein, zum Beispiel `https://adfs.meinunternehmen.com/adfs`.
Client-ID	Geben Sie die abgerufene Client ID ein.
Clientgeheimnis	Geben Sie das abgerufene Client-Geheimnis ein.
Metadatenadresse	Geben Sie den angegebenen **Authority**-Wert mit `/.well-known/openid-configuration` angehängt ein, zum Beispiel `https://adfs.mybusiness.com/adfs/.well-known/openid-configuration`.
OIDC-Umleitungsverhalten	Wählen Sie **GET umleiten**.
Ansprüche vom Benutzer Info-Endpunkt erhalten	Aktivieren Sie diese Option, wenn Sie Fehlermeldungen erhalten, dass die URL zu lang ist (HTTP 414), abgeschnittene URLs und/oder Fehler während des SSO auftreten.
Benutzerdefinierte Bereiche	Definieren Sie benutzerdefinierte Bereiche, die der Anfrage hinzugefügt werden sollen (durch Kommas getrennt).
Kundennutzer-ID-Anspruchstypen	Definieren Sie benutzerdefinierte Schlüssel für den Anspruchstyp zur Benutzeridentifikation (durch Kommas getrennt). Wenn definiert, werden benutzerdefinierte Anspruchstypen gesucht, bevor auf Standardtypen zurückgegriffen wird.
E-Mail-Adresse Anspruchstypen	Definieren Sie benutzerdefinierte Anspruchstyp-Schlüssel für die E-Mail-Adressen der Benutzer (durch Kommas getrennt). Wenn definiert, werden benutzerdefinierte Anspruchstypen gesucht, bevor auf Standardtypen zurückgegriffen wird.

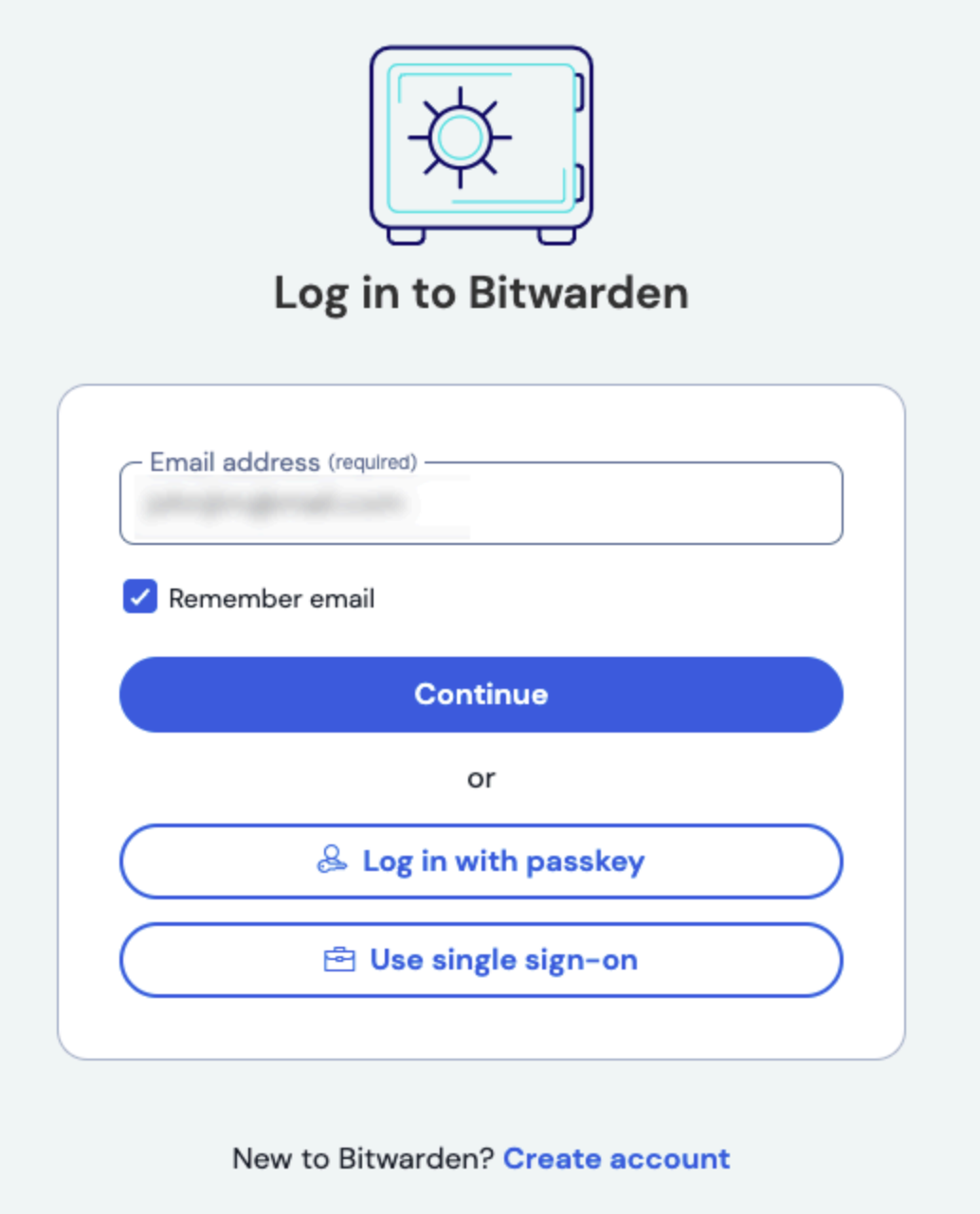
Feld	Beschreibung
Benutzerdefinierte Namensanspruchs-Typen	Definieren Sie benutzerdefinierte Anspruchstyp-Schlüssel für die vollständigen Namen oder Anzeigenamen der Benutzer (durch Kommas getrennt). Wenn definiert, werden benutzerdefinierte Anspruchstypen gesucht, bevor auf Standardtypen zurückgegriffen wird.
Angeforderte Authentifizierungskontextklassenreferenzwerte	Definieren Sie Authentifizierungskontextklassenreferenz-Identifikatoren (`acr_values`) (durch Leerzeichen getrennt). Liste `acr_values` in Präferenzreihenfolge.
Erwarteter "acr" Anspruchswert in der Antwort	Definieren Sie den `acr` Claim-Wert, den Bitwarden in der Antwort erwarten und validieren soll.

Wenn Sie mit der Konfiguration dieser Felder fertig sind, **Speichern** Sie Ihre Arbeit.

> **Tip**
>
> Sie können Benutzer dazu auffordern, sich mit SSO anzumelden, indem Sie die Richtlinie für die Authentifizierung mit Single Sign-On aktivieren. Bitte beachten Sie, dass dies auch die Aktivierung der Einzelorganisation-Richtlinie erfordern wird. Erfahren Sie mehr.

Testen Sie die Konfiguration

Sobald Ihre Konfiguration abgeschlossen ist, testen Sie diese, indem Sie zu https://vault.bitwarden.com navigieren, Ihre E-Mail-Adresse eingeben, **Weiter** auswählen und den **Enterprise Single-On** Button auswählen:



Unternehmens Single Sign On und Master-Passwort

Geben Sie die konfigurierte Organisation ID ein und wählen Sie **Anmelden**. Wenn Ihre Implementierung erfolgreich konfiguriert ist, werden Sie zum AD FS SSO Zugangsdaten-Bildschirm weitergeleitet. Nachdem Sie sich mit Ihren AD FS-Anmeldeinformationen authentifiziert haben, geben Sie Ihr Bitwarden Master-Passwort ein, um Ihren Tresor zu entschlüsseln!

ⓘ Note

Bitwarden unterstützt keine unaufgeforderten Antworten, daher führt das Initiieren von Zugangsdaten von Ihrem IdP zu einem Fehler. Der SSO-Zugangsdaten-Fluss muss von Bitwarden aus initiiert werden.