Okta OIDC Implementierung

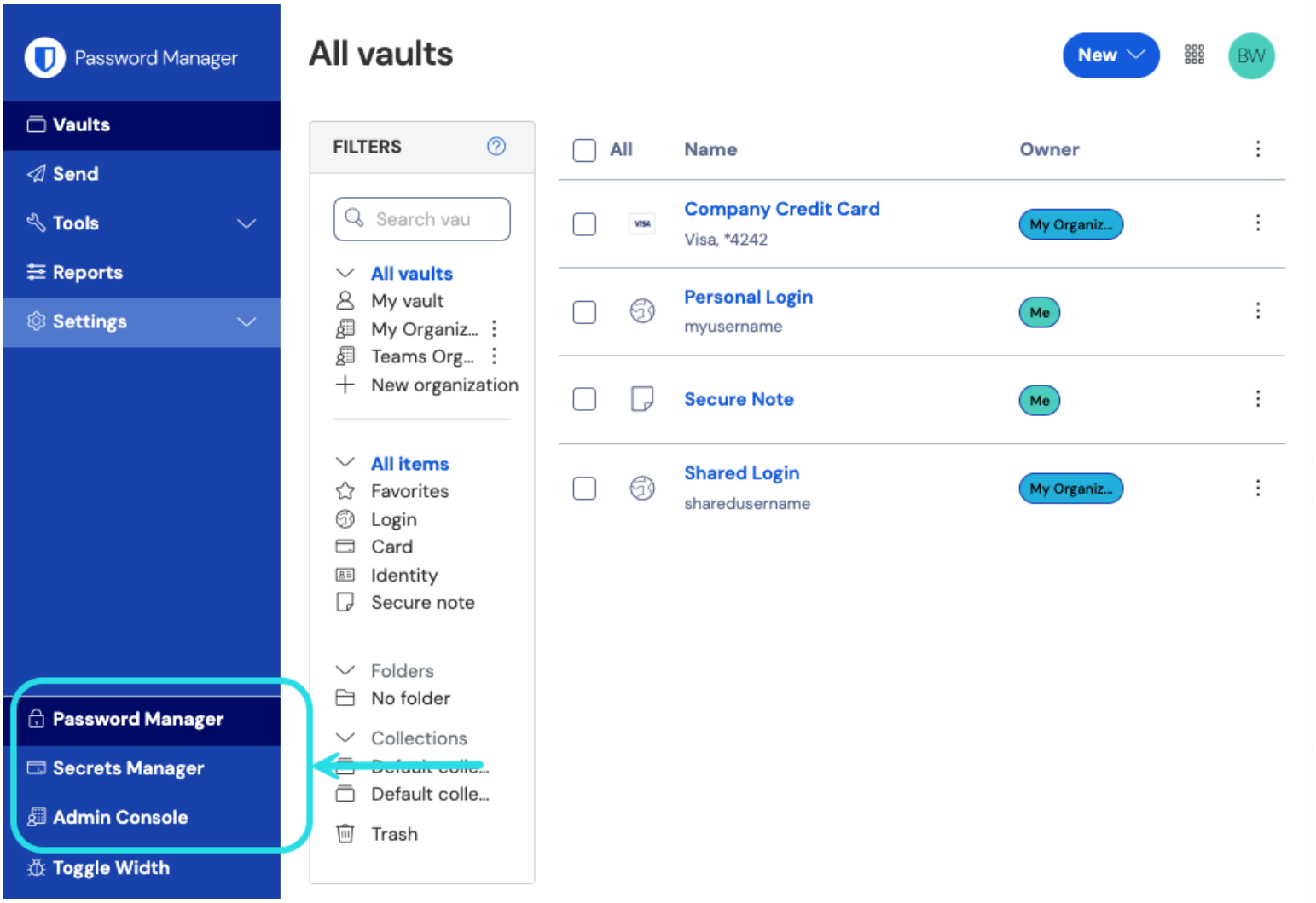
Okta OIDC Implementierung

Dieser Artikel enthält **Okta-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 Okta über SAML 2.0, siehe OIDC Konfiguration oder Okta SAML Implementierung.

Die Konfiguration beinhaltet die gleichzeitige Arbeit innerhalb der Bitwarden-Web-App und des Okta-Administrator-Portals. 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:

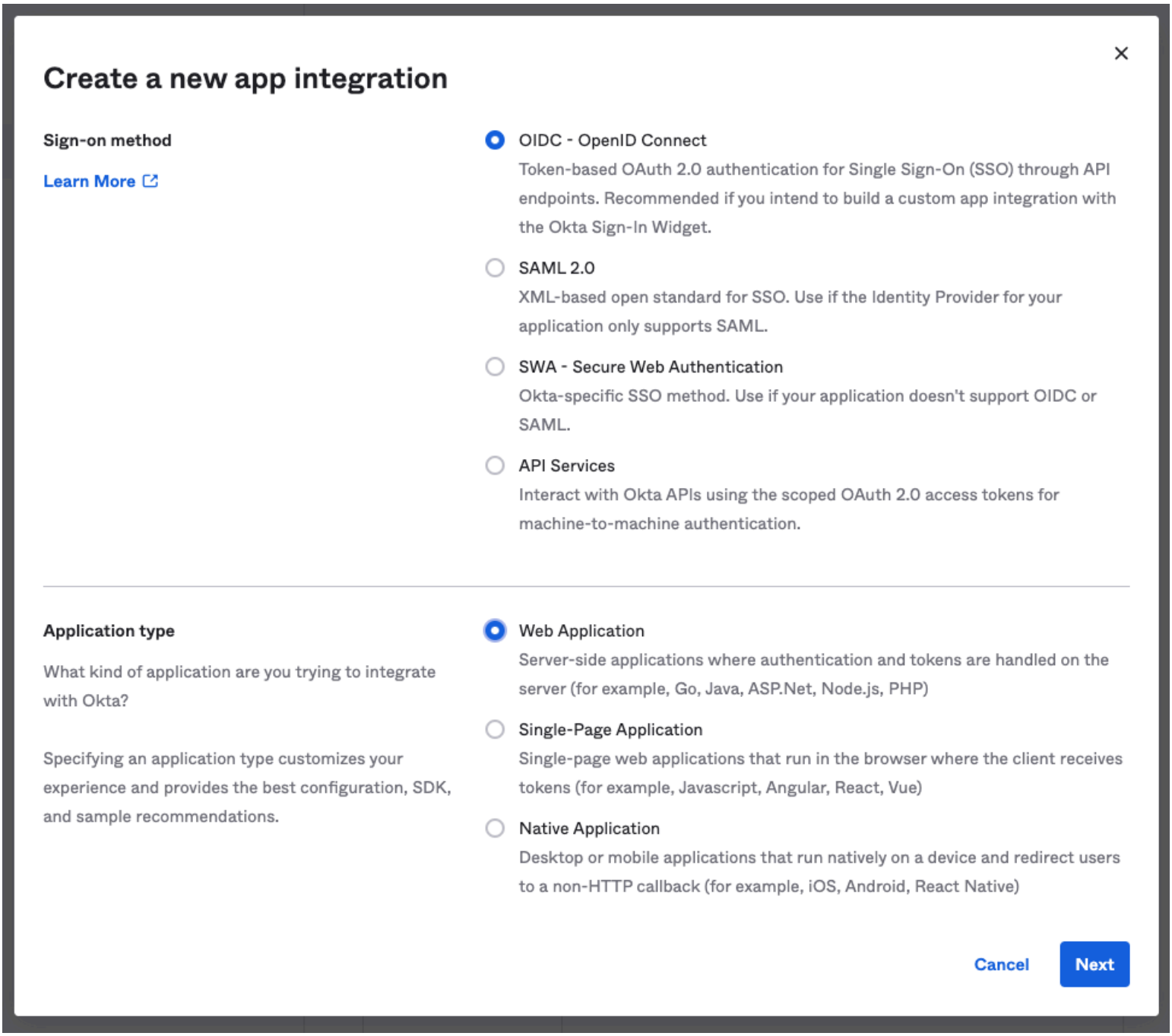
OIDC-Konfiguration

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 Okta-App

Im Okta Administrator Portal wählen Sie **Anwendungen → Anwendungen** aus der Navigation aus. Auf dem Anwendungsbildschirm wählen Sie die Schaltfläche **App-Integration erstellen**. Für die Anmeldemethode wählen Sie **OIDC - OpenID Connect**. Für den Anwendungstyp wählen Sie **Webanwendung**:



Create App Integration

Auf dem Bildschirm für die **Integration der neuen Web-App** konfigurieren Sie die folgenden Felder:

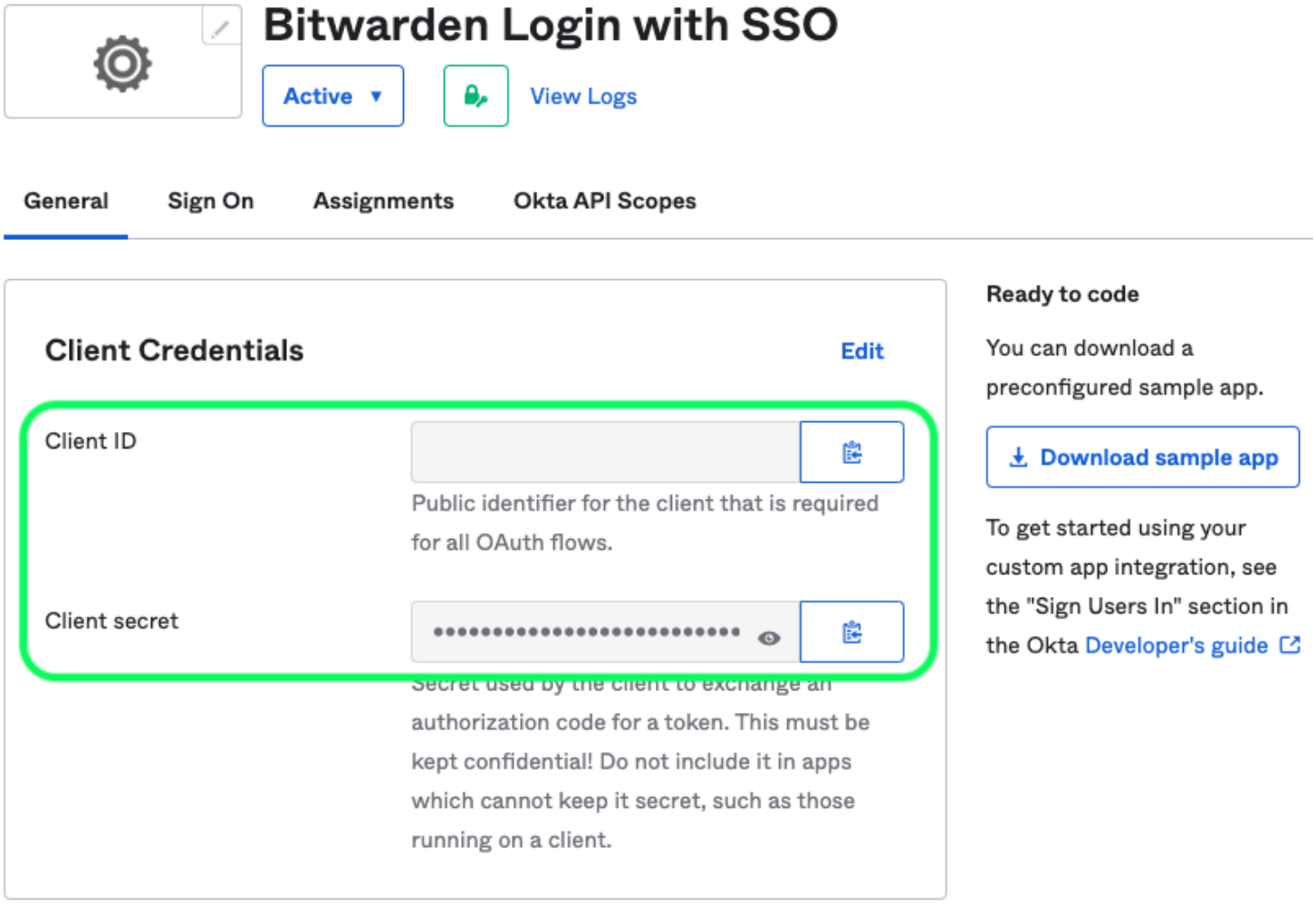
Feld	Beschreibung
Name der App-Integration	Geben Sie der App einen Bitwarden-spezifischen Namen.

Feld	Beschreibung
Zuschusstyp	Aktivieren Sie die folgenden Zulassungs-Typen: - Der Kunde handelt im eigenen Namen → **Anmeldeinformationen des Kunden** - Client handelt im Auftrag eines Benutzers → **Autorisierungscode**
Anmeldeumleitungs-URIs	Setzen Sie dieses Feld auf Ihren **Callback-Pfad**, den Sie vom Bitwarden SSO-Konfigurationsbildschirm abrufen können. 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`.
Abmelde-Umleitungs-URIs	Setzen Sie dieses Feld auf Ihren **Abgemeldet Callback Pfad**, den Sie vom Bitwarden SSO Konfigurationsbildschirm abrufen können.
Aufgaben	Verwenden Sie dieses Feld, um festzulegen, ob alle oder nur ausgewählte Gruppen in der Lage sein werden, Bitwarden Zugangsdaten mit SSO zu verwenden.

Einmal konfiguriert, wählen Sie die **Weiter** Schaltfläche.

Erhalten Sie Client-Anmeldeinformationen

Auf dem Anwendungsbildschirm, kopieren Sie die **Client ID** und **Client Geheimnis** für die neu erstellte Okta-App:

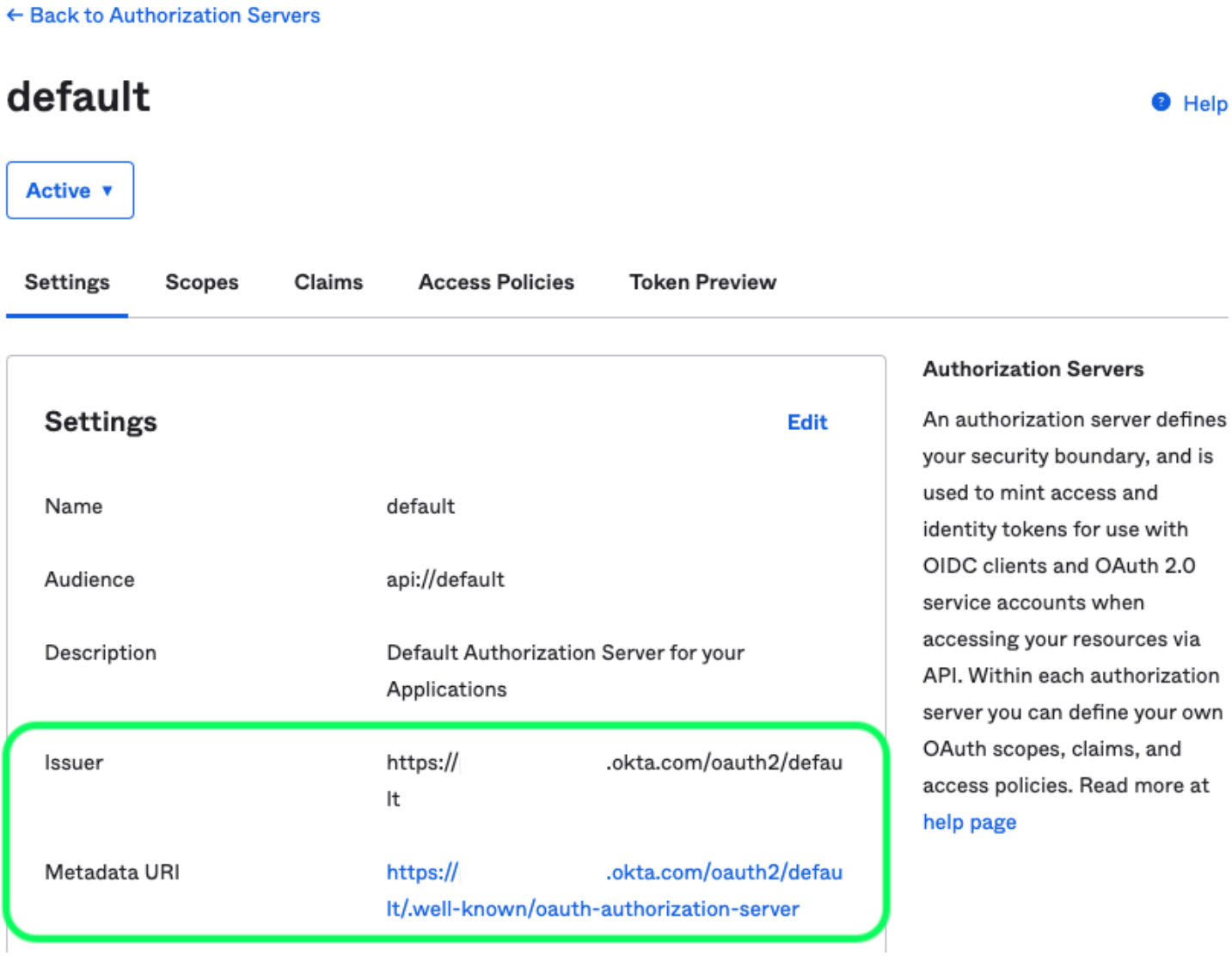


App Client Credentials

Sie werden beide Werte in einem späteren Schritt benötigen.

Erhalten Sie Informationen zum Autorisierungsserver

Wählen Sie **Sicherheit** → **API** aus der Navigation. Aus der Liste der **Autorisierungsserver** wählen Sie den Server aus, den Sie für diese Implementierung verwenden möchten. Auf dem **Einstellungen** Tab für den Server, kopieren Sie die **Aussteller** und **Metadaten URI** Werte:



Okta Authorization Server Settings

Sie müssen beide Werte im nächsten Schritt verwenden.

Zurück zur Web-App

Bis zu diesem Zeitpunkt haben Sie alles konfiguriert, was Sie im Kontext des Okta Administrator Portals benötigen. Kehren Sie zur Bitwarden-Web-App zurück, um die folgenden Felder zu konfigurieren:

Feld	Beschreibung
Zertifizierungsstelle	Geben Sie die abgerufene Aussteller-URI für Ihren Autorisierungsserver ein.
Client-ID	Geben Sie die abgerufene Client-ID für Ihre Okta-App ein.

Feld	Beschreibung
Client-Geheimnis	Geben Sie das abgerufene Client-Geheimnis für Ihre Okta-App ein.
Metadatenadresse	Geben Sie die abgerufene Metadaten-URI für Ihren Autorisierungsserver ein.
OIDC-Umleitungsverhalten	Wählen Sie **GET umleiten**. Okta unterstützt derzeit kein Form POST.
Fordere Ansprüche vom Benutzerinformations-Endpunkt an	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.
Zusätzliche/Individuelle Bereiche	Definieren Sie benutzerdefinierte Bereiche, die der Anfrage hinzugefügt werden sollen (durch Kommas getrennt).
Zusätzliche/Benutzerdefinierte Benutzer-ID-Anspruchs-Typen	Definieren Sie benutzerdefinierte Schlüssel für den Anspruchstyp zur Benutzeridentifikation (durch Kommas getrennt). Wenn definiert, werden benutzerdefinierte Anspruchstypen gesucht, bevor auf Standardtypen zurückgegriffen wird.
Zusätzliche/angepasste 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.
Zusätzliche/angepasste Namensanspruchs-Typen	Definieren Sie benutzerdefinierte Anspruchstypschlüssel 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.

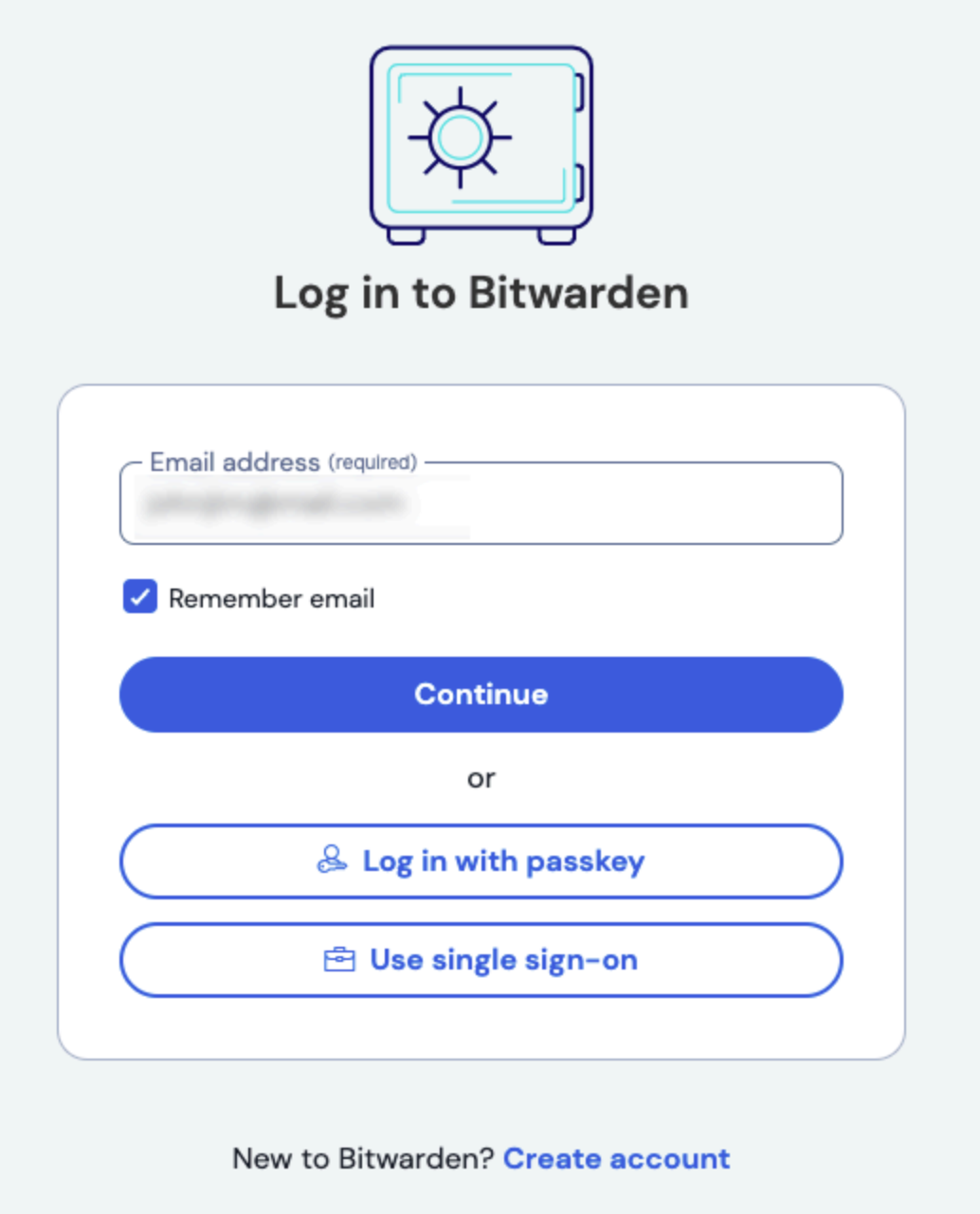
Feld	Beschreibung
Erwarteter "acr" Anspruchswert in der Antwort	Definieren Sie den `acr` Claim-Wert, den Bitwarden in der Antwort erwarten und validieren soll.

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.

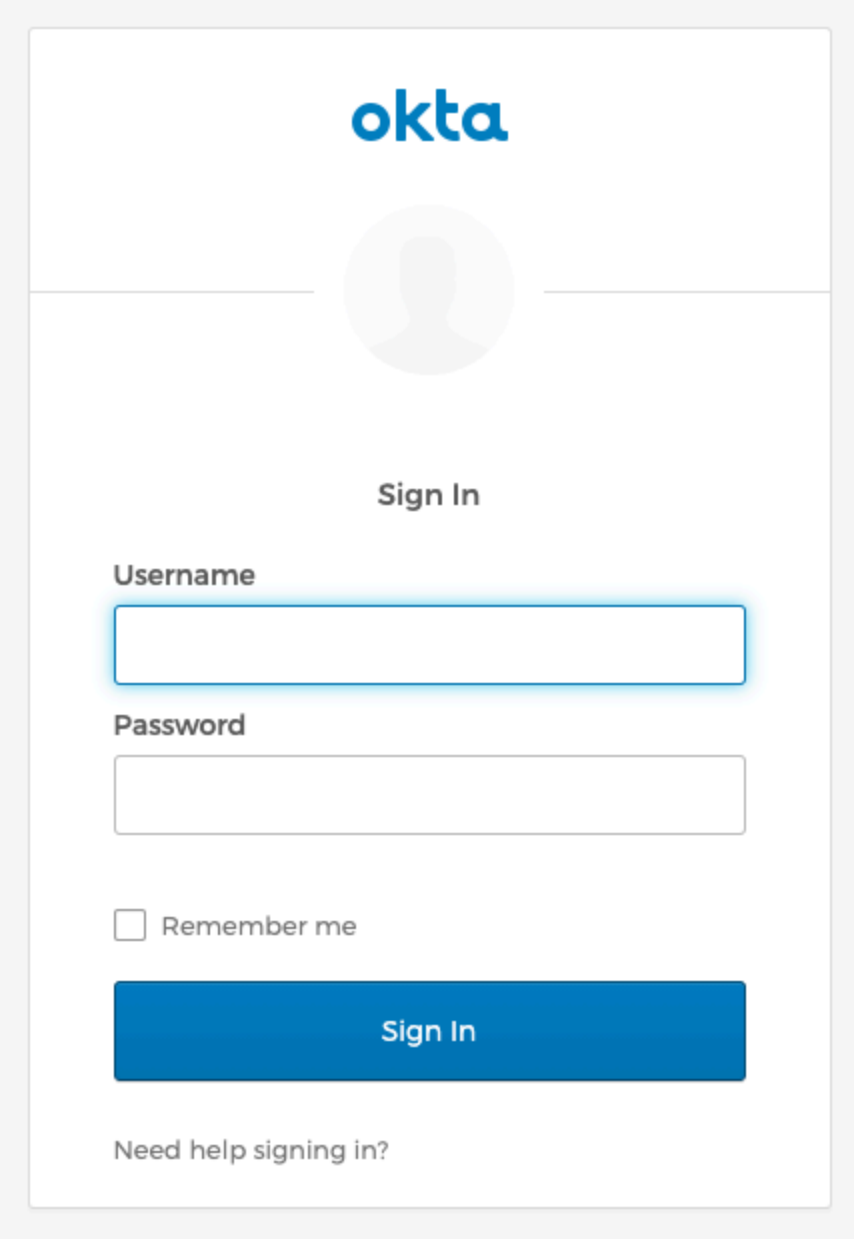
Testen Sie die Konfiguration

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 Organisationskennung ein und wählen Sie **Anmelden**. Wenn Ihre Implementierung erfolgreich konfiguriert ist, werden Sie zur Okta Zugangsdaten Bildschirm weitergeleitet:



Log in with Okta

Nachdem Sie sich mit Ihren Okta-Anmeldeinformationen authentifiziert haben, geben Sie Ihr Bitwarden Master-Passwort ein, um Ihren Tresor zu entschlüsseln!

Note

Bitwarden does not support unsolicited responses, so initiating login from your IdP will result in an error. The SSO login flow must be initiated from Bitwarden. Okta administrators can create an Okta Bookmark App that will link directly to the Bitwarden web vault login page.

1. As an admin, navigate to the **Applications** drop down located on the main navigation bar and select **Applications**.
2. Click **Browse App Catalog**.
3. Search for **Bookmark App** and click **Add Integration**.
4. Add the following settings to the application:
    1. Give the application a name such as **Bitwarden Login**.
    2. In the **URL** field, provide the URL to your Bitwarden client such as `https://vault.bitwarden.com/#/login` or `your-self-hostedURL.com`.
5. Select **Done** and return to the applications dashboard and edit the newly created app.
6. Assign people and groups to the application. You may also assign a logo to the application for end user recognition. The Bitwarden logo can be obtained here.

Once this process has been completed, assigned people and groups will have a Bitwarden bookmark application on their Okta dashboard that will link them directly to the Bitwarden web vault login page.