

ADMINISTRATOR KONSOLE > MELDEN SIE SICH MIT SSO AN >

# 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 Produktschalter (☰):

The screenshot displays the Bitwarden web interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, Settings, Password Manager, Secrets Manager, Admin Console, and Toggle Width. The main content area is titled 'All vaults' and features a 'New' button, a grid icon, and a 'BW' profile icon. Below the title is a 'FILTERS' panel with a search bar and a list of categories: All vaults, All items, Folders, and Collections. A red box highlights the 'Password Manager' option in the sidebar, and a red arrow points to the 'Default colle...' option in the 'All items' section of the filters. The main vault list includes: Company Credit Card (My Organiz...), Personal Login (Me), Secure Note (Me), and Shared Login (My Organiz...).

Produktwechsler

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

- bitwarden Admin Console
- My Organization
- Collections
- Members
- Groups
- Reporting
- Billing
- Settings
- Organization info
- Policies
- Two-step login
- Import data
- Export vault
- Domain verification
- Single sign-on**
- Device approvals
- SCIM provisioning

## Single sign-on



Use the [require single sign-on authentication policy](#) to require all members to log in with SSO.

Allow SSO authentication

Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.

SSO identifier (required)

Provide this ID to your members to login with SSO. To bypass this step, set up [Domain verification](#)

### Member decryption options

Master password

Trusted devices

Once authenticated, members will decrypt vault data using a key stored on their device. The [single organization](#) policy, [SSO required](#) policy, and [account recovery administration](#) policy with automatic enrollment will turn on when this option is used.

Type

### OpenID connect configuration

Callback path

Signed out callback path

OIDC-Konfiguration

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



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 a new app integration

**Sign-on method**

[Learn More](#) ↗

- OIDC - OpenID Connect**  
 Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**  
 XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**  
 Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**  
 Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

---

**Application type**

What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

- Web Application**  
 Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)
- Single-Page Application**  
 Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)
- Native Application**  
 Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

Cancel Next

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	<p>Aktivieren Sie die folgenden <a href="#">Zulassungs-Typen</a>:</p> <ul style="list-style-type: none"> <li>- Der Kunde handelt im eigenen Namen → <b>Anmeldeinformationen des Kunden</b></li> <li>- Client handelt im Auftrag eines Benutzers → <b>Autorisierungscode</b></li> </ul>
Anmeldeumleitungs-URIs	<p>Setzen Sie dieses Feld auf Ihren <b>Callback-Pfad</b>, den Sie vom Bitwarden SSO-Konfigurationsbildschirm abrufen können.</p> <p>Für Kunden, die in der Cloud gehostet werden, ist dies <a href="https://sso.bitwarden.com/oidc-signin">https://sso.bitwarden.com/oidc-signin</a> oder <a href="https://sso.bitwarden.eu/oidc-signin">https://sso.bitwarden.eu/oidc-signin</a>. Für selbst gehostete Instanzen wird dies durch Ihre <a href="#">konfigurierte Server-URL</a> bestimmt, zum Beispiel <a href="https://your.domain.com/sso/oidc-signin">https://your.domain.com/sso/oidc-signin</a>.</p>
Abmelde-Umleitungs-URIs	<p>Setzen Sie dieses Feld auf Ihren <b>Abgemeldet Callback Pfad</b>, den Sie vom Bitwarden SSO Konfigurationsbildschirm abrufen können.</p>
Aufgaben	<p>Verwenden Sie dieses Feld, um festzulegen, ob alle oder nur ausgewählte Gruppen in der Lage sein werden, Bitwarden Zugangsdaten mit SSO zu verwenden.</p>

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:



# Bitwarden Login with SSO

Active ▾



View Logs

General

Sign On

Assignments

Okta API Scopes

## Client Credentials

Edit

Client ID

Public identifier for the client that is required for all OAuth flows.

Client secret

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

### Ready to code

You can download a preconfigured sample app.

[Download sample app](#)

To get started using your custom app integration, see the "Sign Users In" section in the Okta [Developer's guide](#)

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:

[← Back to Authorization Servers](#)

# default

[Help](#)Active ▾

**Settings** | **Scopes** | **Claims** | **Access Policies** | **Token Preview**

Settings		<a href="#">Edit</a>
Name	default	
Audience	api://default	
Description	Default Authorization Server for your Applications	
Issuer	https:// it	.okta.com/oauth2/default
Metadata URI	https:// it/well-known/oauth-authorization-server	.okta.com/oauth2/default

### Authorization Servers

An authorization server defines your security boundary, and is used to mint access and identity tokens for use with OIDC clients and OAuth 2.0 service accounts when accessing your resources via API. Within each authorization server you can define your own OAuth scopes, claims, and access policies. Read more at [help page](#)

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 <a href="#">abgerufene Aussteller-URI</a> für Ihren Autorisierungsserver ein.
Client-ID	Geben Sie die <a href="#">abgerufene Client-ID</a> für Ihre Okta-App ein.

Feld	Beschreibung
Client-Geheimnis	Geben Sie das <a href="#">abgerufene Client-Geheimnis</a> für Ihre Okta-App ein.
Metadatenadresse	Geben Sie die <a href="#">abgerufene Metadaten-URI</a> für Ihren Autorisierungsserver ein.
OIDC-Umleitungsverhalten	Wählen Sie <b>GET umleiten</b> . 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 ( <b>a cr_values</b> ) (durch Leerzeichen getrennt). Liste <b>acr_values</b> in Präferenzreihenfolge.



Feld	Beschreibung
Erwarteter "acr" Anspruchswert in der Antwort	Definieren Sie den <b>acr</b> 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:



## Log in to Bitwarden

Email address (required)

Remember email

Continue

or

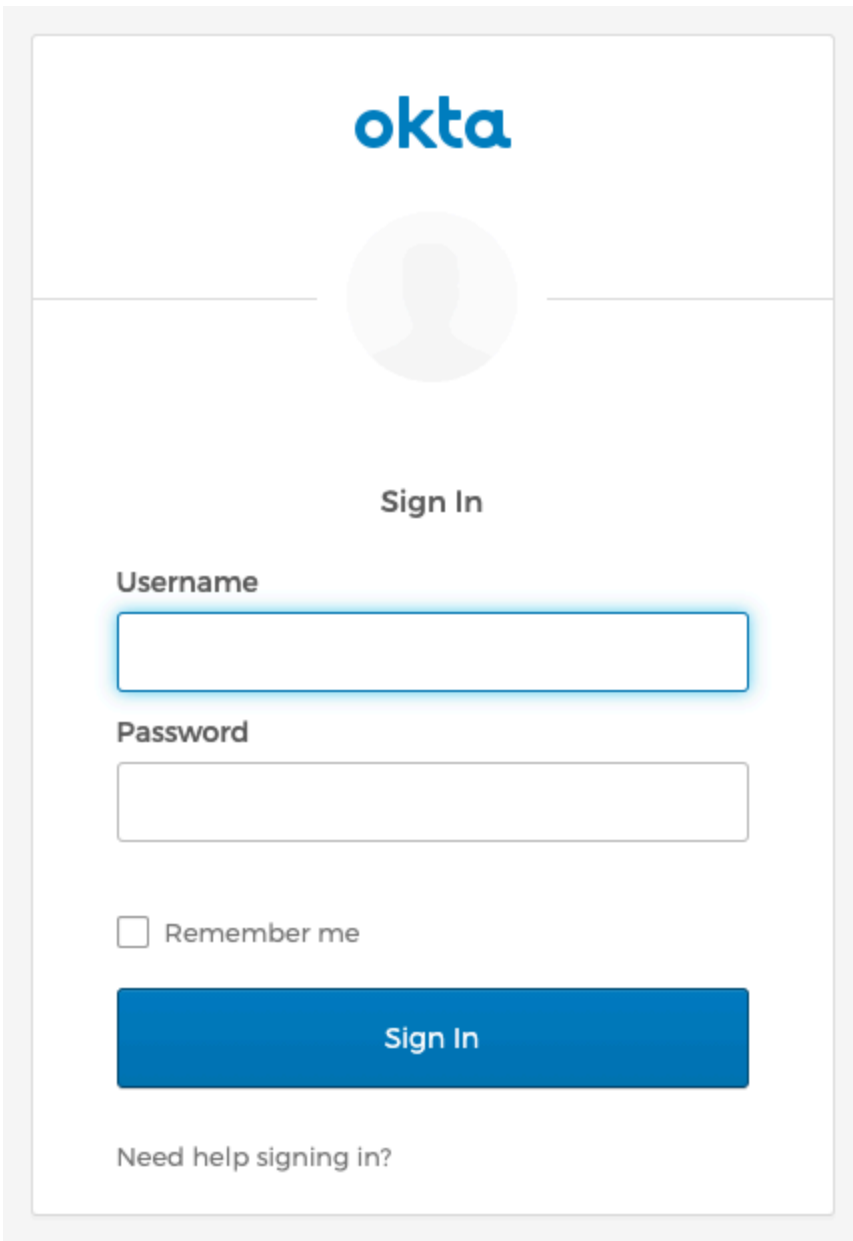
 Log in with passkey

 Use single sign-on

New to Bitwarden? [Create account](#)

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.