

ADMINISTRATOR KONSOLE > MELDEN SIE SICH MIT SSO AN

# OIDC-Konfiguration

Ansicht im Hilfezentrum:

<https://bitwarden.com/help/configure-sso-oidc/>

## OIDC-Konfiguration

### Schritt 1: Legen Sie einen SSO-Identifikator fest

Benutzer, die ihre Identität mit SSO authentifizieren, müssen einen **SSO-Identifikator** eingeben, der die Organisation (und daher die SSO-Integration) zur Authentifizierung angibt. Um einen einzigartigen SSO-Identifizier festzulegen:

1. Melden Sie sich bei der Bitwarden [Web-App](#) an und öffnen Sie die Administrator-Konsole mit dem Produktschalter (☰):

The screenshot displays the Bitwarden Admin Console interface. On the left, a dark blue sidebar contains navigation options: Password Manager, Vaults, Send, Tools, Reports, Settings, Password Manager, Secrets Manager, Admin Console, and Toggle Width. The 'Password Manager' option is circled in red. A red arrow points to the 'Default colle...' option under the 'Collections' section. The main content area is titled 'All vaults' and features a 'New' button and a user profile icon. Below this is a 'FILTERS' section with a search bar and a list of vault categories. The main list shows several vaults:

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		<b>Company Credit Card</b> Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		<b>Personal Login</b> myusername	Me	⋮
<input type="checkbox"/>		<b>Secure Note</b>	Me	⋮
<input type="checkbox"/>		<b>Shared Login</b> sharedusername	My Organiz...	⋮

Produktwechsler

2. Navigieren Sie zu **Einstellungen** → **Einmaliges Anmelden** und geben Sie einen eindeutigen **SSO-Identifizier** für Ihre Organisation ein:

**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)

unique-organization-identifier

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.

*Geben Sie einen Bezeichner ein*

3. Fahren Sie fort zu **Schritt 2: Aktivieren Sie die Zugangsdaten mit SSO**.

#### Tip

You will need to share this value with users once the configuration is ready to be used.

## Schritt 2: Aktivieren Sie die Zugangsdaten mit SSO

Sobald Sie Ihren SSO-Identifizierer haben, können Sie mit der Aktivierung und Konfiguration Ihrer Integration fortfahren. Um die Anmeldung mit SSO zu ermöglichen:

1. Auf der **Einstellungen** → **Single Sign-On** Ansicht, markieren Sie das **SSO-Authentifizierung erlauben** Kontrollkästchen:

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

2. Wählen Sie aus dem Dropdown-Menü **Typ** die Option **OpenID Connect** aus. Wenn Sie stattdessen SAML verwenden möchten, wechseln Sie zum [SAML-Konfigurationshandbuch](#).



#### Tip

Es gibt alternative **Mitglied Entschlüsselungsoptionen**. Erfahren Sie, wie Sie mit [SSO auf vertrauenswürdigen Geräten](#) oder mit [Key Connector](#) beginnen können.

## Schritt 3: Konfiguration

Ab diesem Punkt wird die Umsetzung von Anbieter zu Anbieter variieren. Springen Sie zu einem unserer spezifischen [Implementierungsleitfäden](#) für Hilfe bei der Abschluss des Konfigurationsprozesses:

Anbieter	Leitfaden
Azur	<a href="#">Azure Implementierungsleitfaden</a>

Anbieter	Leitfaden
Okta	<a href="#">Okta Implementierungsleitfaden</a>

## Konfigurationsreferenzmaterialien

Die folgenden Abschnitte definieren die verfügbaren Felder während der Konfiguration des Single Sign-On, unabhängig davon, mit welchem IdP Sie sich integrieren. Felder, die konfiguriert werden müssen, werden markiert (**erforderlich**).



### Tip

Unless you are comfortable with OpenID Connect, we recommend using one of the [above implementation guides](#) instead of the following generic material.

Feld	Beschreibung
Rückrufpfad	( <b>Automatisch generiert</b> ) Die URL für die automatische Authentifizierungsweiterleitung. 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> .
Abgemeldet Rückruf Pfad	( <b>Automatisch generiert</b> ) Die URL für die automatische Weiterleitung beim Abmelden. Für Kunden, die in der Cloud gehostet werden, ist dies <a href="https://sso.bitwarden.com/oidc-signedout">https://sso.bitwarden.com/oidc-signedout</a> oder <a href="https://sso.bitwarden.eu/oidc-signedout">https://sso.bitwarden.eu/oidc-signedout</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-signedout">https://your.domain.com/sso/oidc-signedout</a> .
Zertifizierungsstelle	( <b>Erforderlich</b> ) Die URL Ihres Autorisierungsservers ("Authority"), gegen den Bitwarden die Authentifizierung durchführen wird. Zum Beispiel, <a href="https://your.domain.okta.com/oidc/authorize">https://your.domain.okta.com/oidc/authorize</a> oder <a href="https://login.microsoftonline.com/your-tenant-id/authorize">https://login.microsoftonline.com/your-tenant-id/authorize</a> .
Client-ID	( <b>Erforderlich</b> ) Eine Kennung für den OIDC-Client. Dieser Wert ist typischerweise spezifisch für eine erstellte IdP-App-Integration, zum Beispiel eine <a href="#">Azure-App-Registrierung</a> oder eine <a href="#">Okta-Web-App</a> .

Feld	Beschreibung
Client-Geheimnis	<p><b>(Erforderlich)</b> Das Client-Geheimnis, das in Verbindung mit der Client-ID verwendet wird, um einen Zugriffs-Token zu erhalten. Dieser Wert ist typischerweise spezifisch für eine erstellte IdP-App-Integration, zum Beispiel eine <a href="#">Azure-App-Registrierung</a> oder eine <a href="#">Okta-Web-App</a>.</p>
Metadatenadresse	<p><b>(Erforderlich, wenn die Autorität nicht gültig ist)</b> Eine Metadaten-URL, über die Bitwarden auf die Metadaten des Autorisierungsservers als JSON-Objekt zugreifen kann. Zum Beispiel,</p> <p><a href="https://your.domain.okta.com/oauth2/default/.well-known/oauth-authorization-server">https://your.domain.okta.com/oauth2/default/.well-known/oauth-authorization-server</a></p>
OIDC-Umleitungsverhalten	<p><b>(Erforderlich)</b> Methode, die vom IdP verwendet wird, um auf Authentifizierungsanfragen von Bitwarden zu antworten. Optionen beinhalten <b>Formular POST</b> und <b>Weiterleitung GET</b>.</p>
Ansprüche vom Benutzer Info-Endpunkt erhalten	<p>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.</p>
Zusätzliche/benutzerdefinierte Bereiche	<p>Definieren Sie benutzerdefinierte Bereiche, die der Anfrage hinzugefügt werden sollen (durch Kommas getrennt).</p>
Zusätzliche/benutzerdefinierte Benutzer-ID-Anspruchstypen	<p>Definieren Sie benutzerdefinierte Schlüssel für den Anspruchstyp zur Benutzeridentifikation (durch Kommas getrennt). Wenn definiert, werden benutzerdefinierte Anspruchstypen gesucht, bevor auf Standardtypen zurückgegriffen wird.</p>
Zusätzliche/benutzerdefinierte E-Mail-Adresse Anspruchstypen	<p>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.</p>
Zusätzliche/benutzerdefinierte Namensanspruchstypen	<p>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.</p>

Feld	Beschreibung
Angeforderte Authentifizierungskontextklassen Referenzwerte (acr_values)	Definieren Sie Authentifizierungskontextklassenreferenzidentifikatoren ( <b>acr_values</b> ) (durch Leerzeichen getrennt). Liste <b>acr_values</b> in Präferenzreihenfolge.
Erwarteter "acr" Anspruchswert in der Antwort	Definieren Sie den <b>acr</b> Anspruchswert, den Bitwarden in der Antwort erwarten und validieren soll.

## OIDC Attribute & Ansprüche

Eine **E-Mail-Adresse ist für die Bereitstellung des Kontos erforderlich**, die als eines der Attribute oder Ansprüche in der untenstehenden Tabelle übergeben werden kann.

Eine eindeutige Benutzererkennung wird ebenfalls dringend empfohlen. Wenn abwesend, wird die E-Mail-Adresse stattdessen verwendet, um den Benutzer zu verlinken.

Attribute/Ansprüche sind in der Reihenfolge der Präferenz für die Übereinstimmung aufgelistet, einschließlich Ausweichmöglichkeiten, wo zutreffend.

Wert	Anspruch/Eigenschaft	Ausweichanspruch/-attribut
Eindeutige ID	Konfigurierte benutzerdefinierte Benutzer-ID-Ansprüche NameID (wenn nicht vorübergehend) urn:oid:0.9.2342.19200300.100.1.1 Unter UID UPN EPPN	
E-Mail	Konfigurierte benutzerdefinierte E-Mail-Ansprüche E-Mail http://schemas.xmlsoap.org/ws/2005/05/identität/claims/emailadresse urn:oid:0.9.2342.19200300.100.1.3 Post E-Mail-Adresse	Bevorzugter_Benutzername Urn:oid:0.9.2342.19200300.100.1.1 UID
Name	Konfigurierte benutzerdefinierte Namensansprüche Name http://schemas.xmlsoap.org/ws/2005/05/Identität/claims/name urn:oid:2.16.840.1.113730.3.1.241 urn:oid:2.5.4.3	Vorname + " " + Nachname (siehe unten)

Wert	Anspruch/Eigenschaft	Ausweichanspruch/-attribut
	Anzeigename CN	
Vorname	urn:oid:2.5.4.42 Vorname Vorname FN Vorname Spitzname	
Nachname	urn:oid:2.5.4.4 SN Nachname Nachname	