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-Identifier festzulegen:

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

Password Manager	All vaults		New >> BW
🗇 Vaults			Quantum i
🖉 Send			Owner :
\ll Tools \sim	Q Search vau	Visa, *4242	My Organiz
æ Reports	✓ All vaults	Personal Login	
🕸 Settings 🛛 🗸 🗸	My Vault	myusername	Me
	 Heams Org : New organization 	Secure Note	Me
	 ✓ All items ☆ Favorites ④ Login □ Card Identity □ Secure note 	Shared Login sharedusername	My Organiz
<u></u>	 ✓ Folders ☐ No folder 		
Password Manager	✓ Collections		
🗔 Secrets Manager	Default colle		
🖉 Admin Console	🔟 Trash		
🎂 Toggle Width			
		Produktwechsler	

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

D bit warden		Single sign-on	000	0
B My Organization	\sim	Use the require single sign-on authentication policy to require all members to log in with SSO.		
		Allow SSO authentication		
A Members		Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.		
格 Groups		SSO identifier (required) unique-organization-identifier		
🛱 Reporting	\sim	Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification		
Billing	\sim	Member decryption options		
③ Settings	\sim	Master password		
Organization info Policies		Trusted devices Once authenticated, members will decrypt vault data using a key stored on their device. The single organization policy, SSO require account recovery administration policy with automatic enrollment will turn on when this option is used.	d policy,	and
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-Identifier 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:

D bit warden	Single	sign-on	
🗐 My Organization	✓ Use the requ	uire single sign-on authentication policy to require all members to log in with SSO.	
 □ Collections △ Members ※ Groups ☆ Reporting 	Allow SSG Once set up SSO identifi unique-org Provide this ID to	O authentication b, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials. er (required)	
Billing	Member dec	cryption options	
Settings	🔨 🔵 Master p	assword	
Organization info Policies	Orce authe account rec	devices nticated, members will decrypt vault data using a key stored on their device. The single organization policy, SSO require covery administration policy with automatic enrollment will turn on when this option is used.	ad policy, and
Two-step login	C Type		
Import data	OpenID Co	onnect	*
Export vault			
Domain verificatior	OpenID c	onnect configuration	
Single sign-on	Callback pa	th	
Device approvals	- Signed out		
SCIM provisioning			

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	Azure Implementierungsleitfaden
Okta	Okta Implementierungsleitfaden

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	(Automatisch generiert) Die URL für die automatische Authentifizierungsweiterleitung. Für Kunden, die in der Cloud gehostet werden, ist dies https://sso.bitwarden.co m/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.
Abgemeldet Rückruf Pfad	(Automatisch generiert) Die URL für die automatische Weiterleitung beim Abmelden. Für Kunden, die in der Cloud gehostet werden, ist dies https://sso.bitwarden.co m/oidc-signedout oder https://sso.bitwarden.eu/oidc-signedout. Für selbst gehostete Instanzen wird dies durch Ihre konfigurierte Server-URL bestimmt, zum Beispiel https://your.domain.com/sso/oidc-signedout.
Zertifizierungsstelle	(Erforderlich) Die URL Ihres Autorisierungsservers ("Authority"), gegen den Bitwarden die Authentifizierung durchführen wird. Zum Beispiel, https://your.domain.okta.com/ oauth2/default oder https://login.microsoft.com//v2.0.

Feld	Beschreibung
Client-ID	(Erforderlich) Eine Kennung für den OIDC-Client. Dieser Wert ist typischerweise spezifisch für eine erstellte IdP-App-Integration, zum Beispiel eine Azure-App- Registrierung oder eine Okta-Web-App.
Client-Geheimnis	(Erforderlich) 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 Azure-App-Registrierung oder eine Okta-Web-App.
Metadatenadresse	<pre>(Erforderlich, wenn die Autorität nicht gültig ist) Eine Metadaten-URL, über die Bitwarden auf die Metadaten des Autorisierungsservers als JSON-Objekt zugreifen kann. Zum Beispiel, https://your.domain.okta.com/oauth2/default/.well-known/oauth-author ization-server</pre>
OIDC-Umleitungsverhalten	(Erforderlich) Methode, die vom IdP verwendet wird, um auf Authentifizierungsanfragen von Bitwarden zu antworten. Optionen beinhalten Formular POST und Weiterleitung GET .
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.
Zusätzliche/benutzerdefinierte 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/benutzerdefinierte 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
Zusätzliche/benutzerdefinierte Namensanspruchstypen	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 Authentifizierungskontextklassen Referenzwerte (acr_values)	Definieren Sie Authentifizierungskontextklassenreferenzidentifikatoren (acr_values) (durch Leerzeichen getrennt). Liste acr_values in Präferenzreihenfolge.
Erwarteter "acr" Anspruchswert in der Antwort	Definieren Sie den acr 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 Benutzerkennung 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	

Wert	Anspruch/Eigenschaft	Ausweichanspruch/-attribut
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 Anzeigename CN	Vorname + "" + Nachname (siehe unten)
Vorname	urn:oid:2.5.4.42 Vorname FN Vorname Spitzname	
Nachname	urn:oid:2.5.4.4 SN Nachname Nachname	