

### ADMINISTRATOR KONSOLE $\rightarrow$ MELDEN SIE SICH MIT SSO AN $\rightarrow$

# **ADFS OIDC Implementierung**

Ansicht im Hilfezentrum: https://bitwarden.com/help/adfs-oidc-implementation/

### **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 (
B):

Password Manager	All vaults			New 🗸	BW
🗇 Vaults	FILTERS ⑦		Name	Owner	:
🖉 Send					
$\ll$ Tools $\qquad \qquad \checkmark$	Q Search vau	ARIV	Company Credit Card Visa, *4242	My Organiz	:
<b>≅</b> Reports	✓ All vaults		Personal Lagin		
🕸 Settings 🛛 🗸 🗸	<ul> <li>∠ My vault</li> <li>∠ My Organiz :</li> <li>∠ Teams Org</li> </ul>	0 3	myusername	Me	:
	+ New organization		Secure Note	Ме	:
	<ul> <li>✓ All items</li> <li>☆ Favorites</li> <li>۞ Login</li> <li>□ Card</li> <li>□ Identity</li> <li>□ Secure note</li> </ul>	D Ø	Shared Login sharedusername	My Organiz	÷
<ul> <li>Password Manager</li> <li>Secrets Manager</li> <li>Admin Console</li> <li> <sup>™</sup> Toggle Width     </li> </ul>	<ul> <li>✓ Folders</li> <li>➢ No folder</li> <li>✓ Collections</li> <li>➢ Default colle</li> <li>➢ Default colle</li> <li>☆ Trash</li> </ul>				

Produktwechsler

Wählen Sie Einstellungen  $\rightarrow$  Einmaliges Anmelden aus der Navigation:

<b>D bit</b> warden	Single sign-on III III III III III III III IIII II
🖉 My Organization 🔍	Use the <b>require single sign-on authentication policy</b> 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.
磐 Groups	SSO identifier (required)
	Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification
🗄 Billing 🗸 🗸	Member decryption options
Settings	Master password
Organization info	O Trusted devices Once authenticated, members will decrypt vault data using a key stored on their device. The single organization policy, SSO required policy, and
Policies	account recovery administration policy with automatic enrollment will turn on when this option is used.
Two-step login	C Type
Import data	OpenID Connect
Export vault	
Domain verification	OpenID connect configuration
Single sign-on	Callback path
Device approvals	- Signed out cellback path
SCIM provisioning	

#### 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.

#### 翰 Add Application Group Wizard

#### Secure and trusted open source password manager for business

 $\times$ 

Weld	come
------	------

Steps	Name:
Welcome	BitwardenCloud
Server application	Description
<ul> <li>Configure Application Credentials</li> </ul>	
Configure Web API	
Apply Access Control Policy	Template:
<ul> <li>Configure Application Permissions</li> </ul>	Client-Server applications
Summary	Native application accessing a web API
Complete	Server application accessing a web API
	Web browser accessing a web application
	Standalone applications
	💷 Native application
	Server application
	More information
	< Previous Next > Cancel
	AD ES Add Application Group

3. Auf dem Serveranwendungs-Bildschirm:

🏟 Add Application Group W	ïzard	×
Server application		
Steps	Name:	
Welcome	BitwardenCloud - Server application	
<ul> <li>Server application</li> </ul>	Client Identifier	
<ul> <li>Configure Application Credentials</li> </ul>	27a3f3ea-e4ba-4ed5-a203-3b1e6590cf0d	
Configure Web API	Redirect URI:	
Apply Access Control Policy	Example: https://Contoso.com	Add
<ul> <li>Configure Application Permissions</li> </ul>	https://sso.bitwarden.com/oidc-signin	Remove
Summary		
Complete		
	Description:	
		7
	< Previous Next >	Cancel

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/oi dc-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:

훾 Add Application Group Wi	zard	×
Configure Web API		ŋ
Steps	Name:	
Welcome	BitwardenCloud - Web API	
Server application	Identifier:	
<ul> <li>Configure Application Credentials</li> </ul>	Example: https://Contoso.com	Add
Configure Web API	27a3f3ea-e4ba-4ed5-a203-3b1e6590cf0d	Remove
Apply Access Control Policy	https://sso.bitwarden.com/	
<ul> <li>Configure Application Permissions</li> </ul>		
Summary	Description:	
Complete		
	< Previous Next >	Cancel

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.

翰 Add Application Group Wi	izard						×
Configure Application I	Permissions						
Steps Welcome	Configure permission Client application (ca	ns to enable client appli aller):	cations to acces	ss this Web API.			
<ul> <li>Server application</li> <li>Configure Application Credentials</li> <li>Configure Web API</li> <li>Apply Access Control Policy</li> <li>Configure Application Permissions</li> </ul>	Name BitwardenCloud - S	erver application	Description				
<ul> <li>Complete</li> </ul>	Permitted scopes:	Description			Add	Remov	ve
	allatclaims aza email logon_cert openid profile user_imperso von_cert	Requests the access Scope allows broker Request the email c The logon_cert scop Request use of the l Request profile relat Request permission The von cert scope	is token claims in r client to reques laim for the signe pe allows an app OpenID Connec red claims for the for the applications allows an appli	the identity toke train user. Sication to reques t authorization pro- signed in user. on to access the cation to request	en. token. st logo otocol. resour VPN	New scor	v
				< Previous	Next >	Cance	el

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  ${\it Bearbeiten...}$  .
- 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":

Madd Transform Claim Rule	Wizard		×
Configure Rule Steps • Choose Rule Type • Configure Claim Rule	You ca to extra from the Claim ru email Rule te Attribut Active	n configure this rule to send the values of LD ct LDAP attributes. Specify how the attribute e rule. ule name: mplate: Send LDAP Attributes as Claims e store: Directory ng of LDAP attributes to outgoing claim types LDAP Attribute (Select or type to add more) E-Mail-Addresses	DAP attributes as claims. Select an attribute store from which es will map to the outgoing claim types that will be issued
			< Previous Finish Cancel

#### 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 <b>Authority</b> -Wert mit /.well-known/openid-c onfiguration angehängt ein, zum Beispiel https://adfs.mybusiness.c om/adfs/.well-known/openid-configuration.
OIDC-Umleitungsverhalten	Wählen Sie <b>GET umleiten</b> .
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.
Benutzerdefinierte Namensanspruchs-Typen	Definieren Sie benutzerdefinierte Anspruchstyp-Schlüssel für die vollständigen Namen oder Anzeigenamen der Benutzer (durch Kommas

Feld	Beschreibung
	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:

	Log in
Maste	er password (required) s required.
	Log in with master password
$\square$	🖶 Enterprise single sign-on
Logging Not you	in as myemailaddress@bitwarden.com ?

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!

#### (i) 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.