ADMIN CONSOLE \rightarrow LOGIN WITH SSO \rightarrow

ADFS OIDC Implementation

View in the help center: https://bitwarden.com/help/adfs-oidc-implementation/

U bitwarden

ADFS OIDC Implementation

This article contains **Active Directory Federation Services (AD FS)-specific** help for configuring login with SSO via OpenID Connect (OIDC). For help configuring login with SSO for another OIDC IdP, or for configuring AD FS via SAML 2.0, see OIDC Configuration or ADFS SAML Implementation.

Configuration involves working simultaneously within the Bitwarden web app and the AD FS Server Manager. As you proceed, we recommend having both readily available and completing steps in the order they are documented.

Open SSO in the web vault

Log in to the Bitwarden web app and open the Admin Console using the product switcher:

Password Manager	All vaults			New 🗸	BW
🗇 Vaults	FILTERS 📀		Name	Owner	:
🕼 Send					
\ll Tools \sim	Q Search vau	VISA	Company Credit Card Visa, *4242	My Organiz	:
≢ Reports	✓ All vaults		Personal Login		
🕸 Settings 🛛 🗸 🗸	My Vault		myusername	Me	:
	+ New organization		Secure Note	Ме	:
	 ✓ All items ☆ Favorites ④ Login □ Card Identity ↓ Secure note 		Shared Login sharedusername	My Organiz	÷
 Password Manager Secrets Manager 	 ✓ Folders ➢ No folder ✓ Collections ➢ Default colle ➢ Default colle ☆ Trash 				

Product switcher

Select **Settings** \rightarrow **Single sign-on** from the navigation:

D bit warden	Single sign-on 🗰 🛑)
${\ensuremath{\mathbb B}}$ My Organization $~~ \lor$	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.	
뿅 Groups	SSO identifier (required)	
$\stackrel{\equal}{\rightleftharpoons}$ Reporting \checkmark	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	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.	
Policies		
Two-step login	Type OpenID Connect	٦
Import data		J
Export vault		
Domain verification	OpenID connect configuration	
Single sign-on	Callback path	٦
Device approvals	- Signed out cellback path)
SCIM provisioning)

OIDC configuration

If you haven't already, create a unique **SSO identifier** for your organization. Otherwise, you don't need to edit anything on this screen yet, but keep it open for easy reference.

⊘ Tip

There are alternative Member decryption options. Learn how to get started using SSO with trusted devices or Key Connector.

Create an application group

In Server Manager, navigate to AD FS Management and create a new application group:

1. In the console tree, select Application Groups and choose Add Application Group from the Actions list.

2. On the Welcome screen of the wizard, choose the Server application accessing a web API template.

翰 Add Application Group Wizard

Secure and trusted open source password manager for business

Welcome

Steps	Name:
Welcome	BitwardenCloud
Server application	Description
 Configure Application Credentials 	
Configure Web API	
Apply Access Control Policy	Template:
 Configure Application Permissions 	Client-Server applications
Summary	Native application accessing a web API
 Summary Complete 	Server application accessing a web API Image: Server application accessing a web application Standalone applications Image: Native application Image: Server application Image: Server application Image: Web API Image: Web API
	More information
	< Previous Next > Cancel

AD FS Add Application Group

3. On the Server application screen:

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

AD FS Server Application screen

- Give the server Application a Name.
- Take note of the Client Identifier. You will need this value in a subsequent step.
- Specify a **Redirect URI**. For cloud-hosted customers, this is https://sso.bitwarden.com/oidc-signin or https://sso.bit warden.eu/oidc-signin. For self-hosted instances, this is determined by your configured Server URL, for example https://yo ur.domain.com/sso/oidc-signin.
- 4. On the Configure Application Credentials screen, take note of the Client Secret. You will need this value in a subsequent step.
- 5. On the Configure Web API screen:

🖬 Add Application Group Wizard >			G
Configure Web API			'n
Steps	Name:		
Welcome	BitwardenCloud - Web API		L
Server application	Identifier		l
 Configure Application Credentials 	Example: https://Contoso.com	Add	
Configure Web API	27a3f3ea-e4ba-4ed5-a203-3b1e6590cf0d	Remove	L
Apply Access Control Policy	https://sso.bitwarden.com/		
 Configure Application Permissions 			
Summary	Description:		L
Complete			
			L
			L
			L
			L
			L
			L
			L
			L
			L
		-	
	< Previous Next >	Cancel	

AD FS Configure Web API screen

- Give the Web API a **Name**.
- Add the Client Identifier and Redirect URI (see step 2B. & C.) to the Identifier list.

6. On the Apply Access Control Policy screen, set an appropriate Access Control Policy for the Application Group.

7. On the Configure application permissions screen, permit the scopes allatclaims and openid.

翰 Add Application Group Wi	izard				×
Configure Application I	Permissions				
Steps Welcome	Configure permission Client application (ca	is to enable client applications to aller):	o access this Web API.		
 Server application Configure Application Credentials Configure Web API Apply Access Control Policy Configure Application Permissions Summary 	Name BitwardenCloud - S	Descrip Server application	ition		
Complete	Permitted scopes: Scope Name allatclaims aza email logon_cert openid profile user_imperso von cert	Description Requests the access token of Scope allows broker client to Request the email claim for th The logon_cert scope allows Request use of the OpenID (Request profile related claims Request permission for the a The von cert scope allows a	claims in the identity toke) request primary refresh t he signed in user. s an application to reques Connect authorization pro s for the signed in user. pplication to access the r an application to request ¹	Add n. oken. ti logo ptocol. resour VPN	Remove
			< Previous	Next >	Cancel

AD FS Configure Application Permissions screen

8. Finish the Add Application Group Wizard.

Add a transform claim rule

In Server Manager, navigate to AD FS Management and edit the created application group:

- 1. In the console tree, select **Application Groups**.
- 2. In the Application Groups list, right-click the created application group and select Properties.
- 3. In the Applications section, choose the Web API and select ${\bf Edit...}$.
- 4. Navigate to the Issuance Transform Rules tab and select the Add Rule... button.
- 5. On the Choose Rule Type screen, select **Send LDAP Attributes as Claims.**
- 6. On the Configure Claim Rule screen:

🖬 Add Transform Claim Rule Wizard X				
Configure Rule				
Configure Rule Steps Choose Rule Type Configure Claim Rule	You ca to extra from th Claim r email Rule te Attribut Active	an configure this rule to send the values o act LDAP attributes. Specify how the attrib e rule. ule name: emplate: Send LDAP Attributes as Claims te store: Directory ng of LDAP attributes to outgoing claim ty LDAP Attribute (Select or type to add more) E-Mail-Addresses	f LD bute)AP attributes as claims. Select an attribute store from which as will map to the outgoing claim types that will be issued
				< Previous Finish Cancel

AD FS Configure Claim Rule screen

- Give the rule a **Claim rule name**.
- From the LDAP Attribute dropdown, select **E-Mail-Addresses.**
- From the Outgoing Claim Type dropdown, select E-Mail Address.

7. Select Finish.

Back to the web app

At this point, you have configured everything you need within the contest of the AD FS Server Manager. Return to the Bitwarden web app to configure the following fields:

Field	Description
Authority	Enter the hostname of your AD FS Server with /adfs appended, for example https://adfs.s.mybusiness.com/adfs.
Client ID	Enter the retreived Client ID.
Client Secret	Enter the retrieved Client Secret.
Metadata Address	Enter the specified Authority value with /.well-known/openid-configuration appended, for example https://adfs.mybusiness.com/adfs/.well-known/openid-configuration.
OIDC Redirect Behavior	Select Redirect GET.
Get claims from user info endpoint	Enable this option if you receive URL too long errors (HTTP 414), truncated URLS, and/or failures during SSO.
Custom Scopes	Define custom scopes to be added to the request (comma-delimited).
Customer User ID Claim Types	Define custom claim type keys for user identification (comma-delimited). When defined, custom claim types are searched for before falling back on standard types.
Email Claim Types	Define custom claim type keys for users' email addresses (comma-delimited). When defined, custom claim types are searched for before falling back on standard types.
Custom Name Claim Types	Define custom claim type keys for users' full names or display names (comma-delimited). When defined, custom claim types are searched for before falling back on standard types.
Requested Authentication Context Class References values	Define Authentication Context Class Reference identifiers (acr_values) (space-delimited). List acr_values in preference-order.

Field	Description
Expected "acr" Claim Value In Response	Define the acr Claim Value for Bitwarden to expect and validate in the response.

When you are done configuring these fields, **Save** your work.

∏ Tip

You can require users to log in with SSO by activating the single sign-on authentication policy. Please note, this will require activating the single organization policy as well. Learn more.

Test the configuration

Once your configuration is complete, test it by navigating to https://vault.bitwarden.com, entering your email address, selecting **Continue**, and selecting the **Enterprise Single-On** button:



Log in options screen

Enter the configured Organization ID and select **Log In**. If your implementation is successfully configured, you'll be redirected to the AD FS SSO login screen. After you authenticate with your AD FS credentials, enter your Bitwarden master password to decrypt your vault!

(i) 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.