

ADMIN CONSOLE > LOGGA IN MED SSO >

# ADFS OIDC Implementation

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

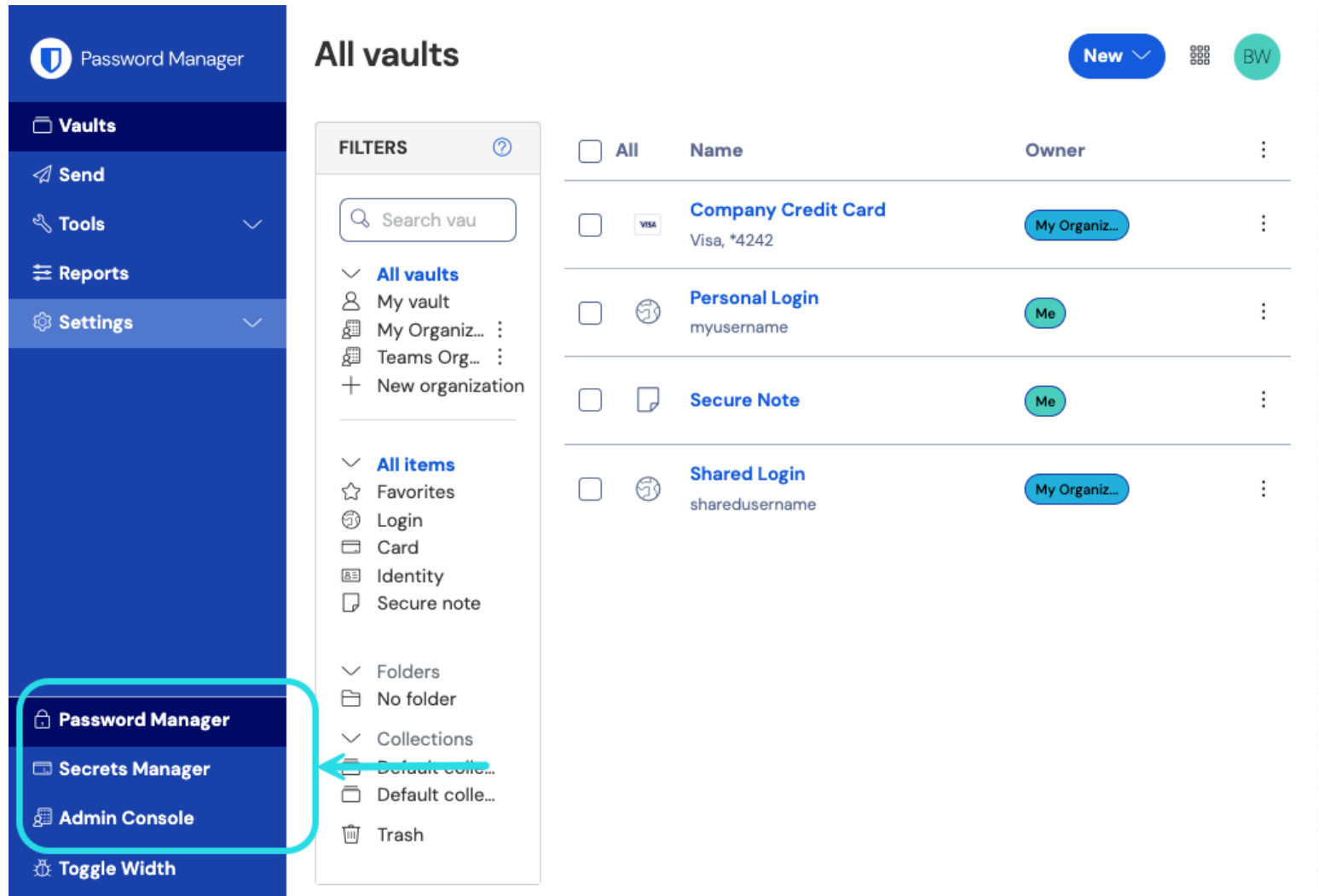
## ADFS OIDC Implementation

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:



The screenshot shows the Bitwarden web app interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, and Settings. The main area is titled 'All vaults' and shows a list of vaults. A red box highlights the 'Password Manager' option in the sidebar, and a red arrow points to the 'Product switcher' button in the top right corner.

	Filters	Product switcher
<ul style="list-style-type: none"> <li>Search vaults</li> <li>All vaults <ul style="list-style-type: none"> <li>My vault</li> <li>My Organiz...</li> <li>Teams Org...</li> <li>New organization</li> </ul> </li> <li>All items <ul style="list-style-type: none"> <li>Favorites</li> <li>Login</li> <li>Card</li> <li>Identity</li> <li>Secure note</li> </ul> </li> <li>Folders <ul style="list-style-type: none"> <li>No folder</li> </ul> </li> <li>Collections <ul style="list-style-type: none"> <li>Default colle...</li> <li>Default colle...</li> </ul> </li> <li>Trash</li> </ul>	<ul style="list-style-type: none"> <li>All</li> <li>Company Credit Card (Visa, *4242)</li> <li>Personal Login (myusername)</li> <li>Secure Note</li> <li>Shared Login (sharedusername)</li> </ul>	<ul style="list-style-type: none"> <li>New</li> <li>BW</li> </ul>

Product switcher

Select **Settings** → **Single sign-on** from the navigation:



- 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)

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.

---

Type

OpenID Connect

---

### OpenID connect configuration

Callback path

Signed out callback path

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.




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.

 Add Application Group Wizard ✕

**Welcome**

**Steps**

- Welcome
- Server application
- Configure Application Credentials
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

Name:  
BitwardenCloud

Description:

Template:

**Client-Server applications**

- Native application accessing a web API
- Server application accessing a web API
- Web browser accessing a web application

**Standalone applications**

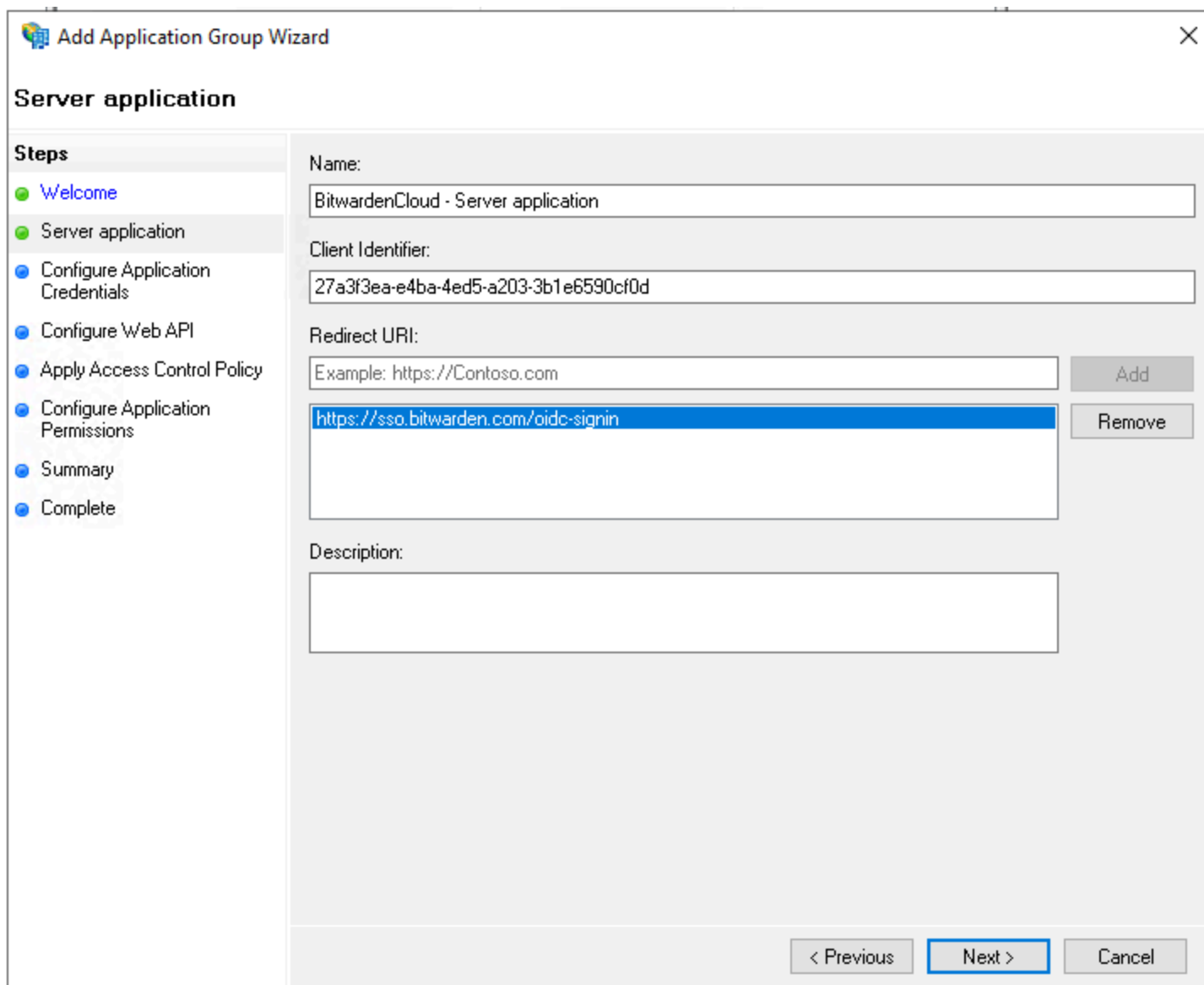
- Native application
- Server application
- Web API

[More information...](#)

< Previous Next > Cancel

AD FS Add Application Group

3. On the Server application screen:



**Add Application Group Wizard**

**Server application**

**Steps**

- Welcome
- Server application
- Configure Application Credentials
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

**Name:**  
BitwardenCloud - Server application

**Client Identifier:**  
27a3f3ea-e4ba-4ed5-a203-3b1e6590cf0d

**Redirect URI:**  
Example: https://Contoso.com Add

https://sso.bitwarden.com/oidc-signin Remove

**Description:**

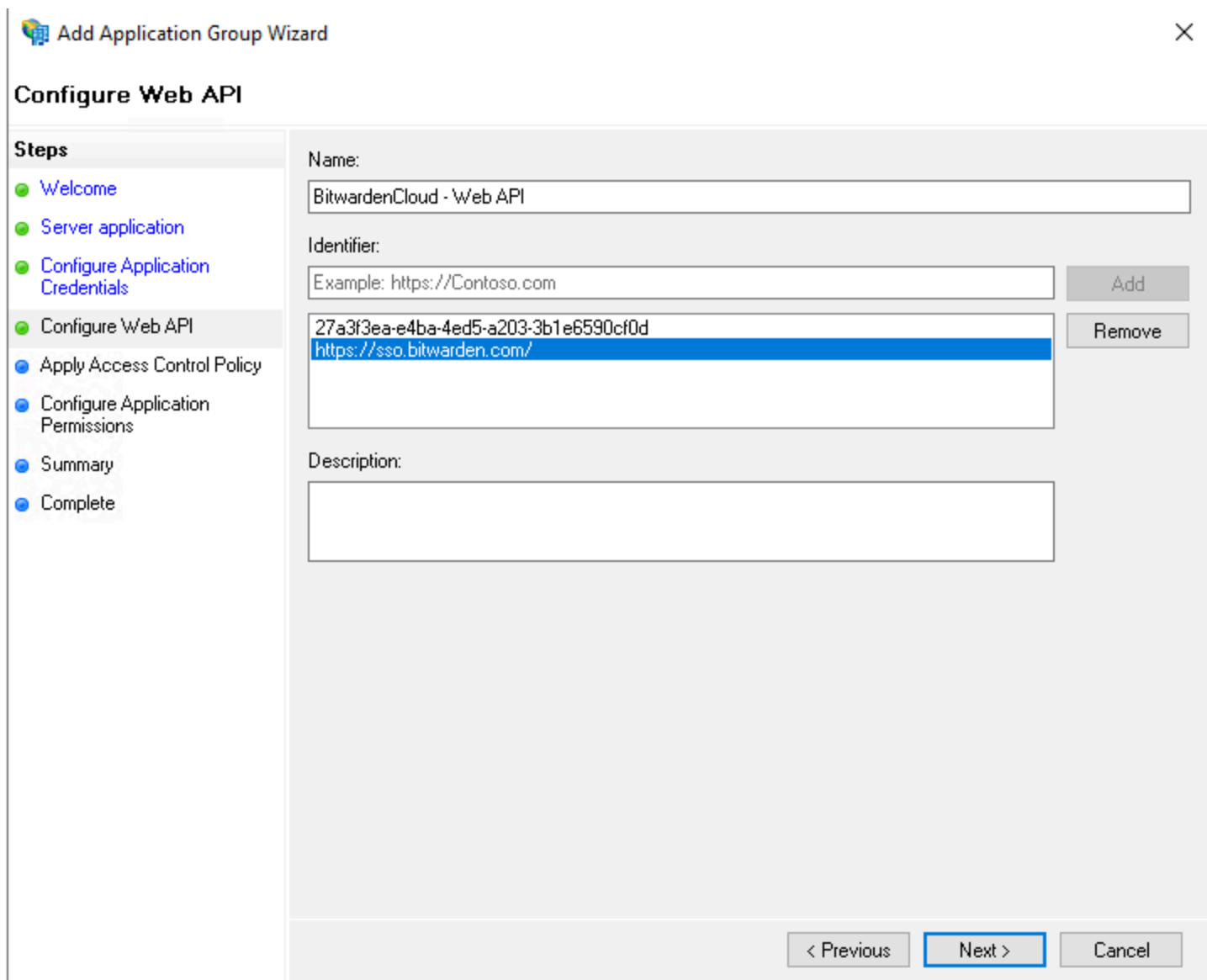
< Previous Next > Cancel

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.bitwarden.eu/oidc-signin>. For self-hosted instances, this is determined by your configured Server URL, for example <https://your.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:

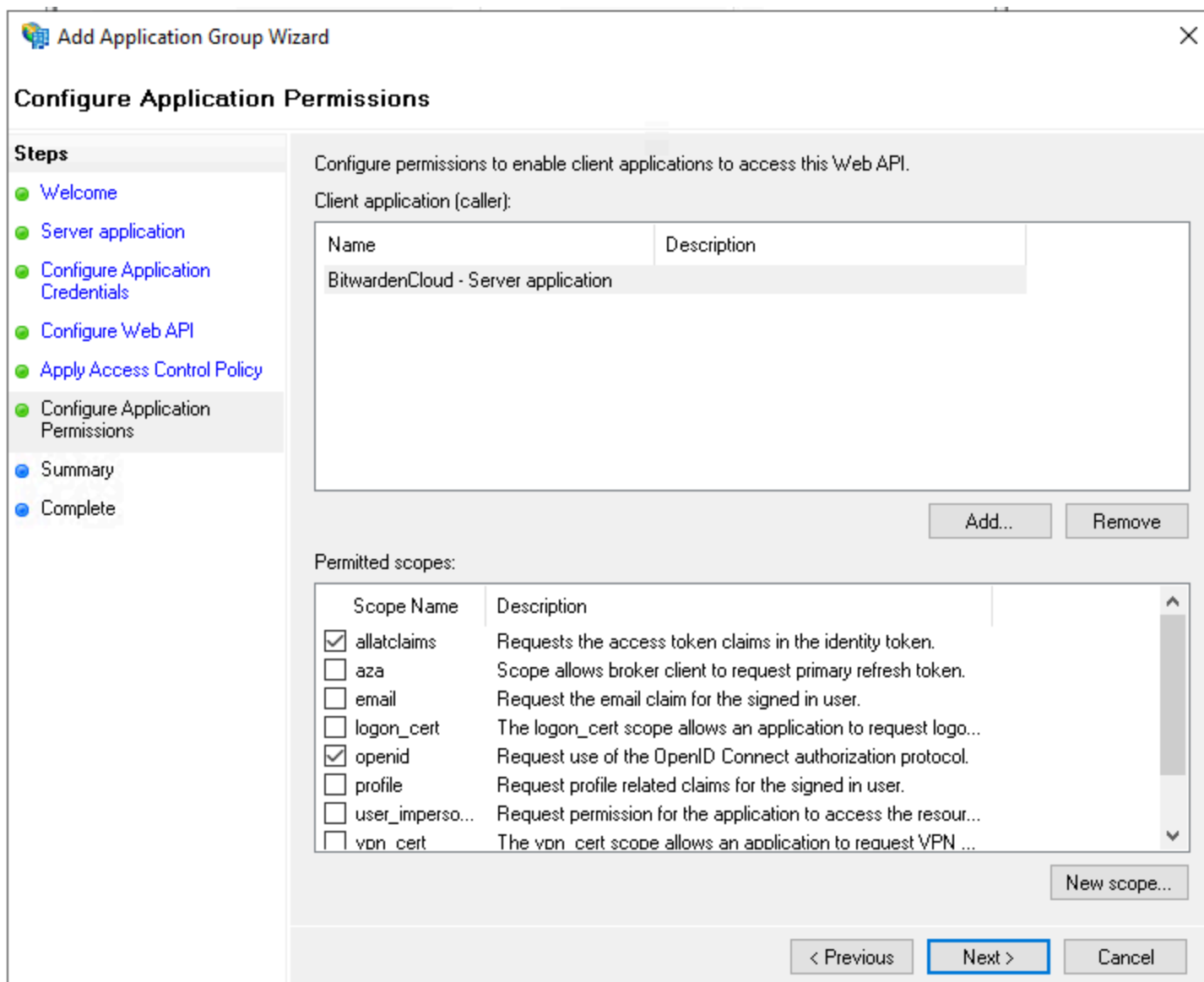


AD FS Configure Web API screen

- 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**.



**Add Application Group Wizard**

**Configure Application Permissions**

Configure permissions to enable client applications to access this Web API.

Client application (caller):

Name	Description
BitwardenCloud - Server application	

Add... Remove

Permitted scopes:

Scope Name	Description
<input checked="" type="checkbox"/> allatclaims	Requests the access token claims in the identity token.
<input type="checkbox"/> aza	Scope allows broker client to request primary refresh token.
<input type="checkbox"/> email	Request the email claim for the signed in user.
<input type="checkbox"/> logon_cert	The logon_cert scope allows an application to request logo...
<input checked="" type="checkbox"/> openid	Request use of the OpenID Connect authorization protocol.
<input type="checkbox"/> profile	Request profile related claims for the signed in user.
<input type="checkbox"/> user_imperso...	Request permission for the application to access the resour...
<input type="checkbox"/> von_cert	The von_cert scope allows an application to request VPN ...

New scope...

< Previous Next > Cancel

AD FS Configure Application Permissions screen

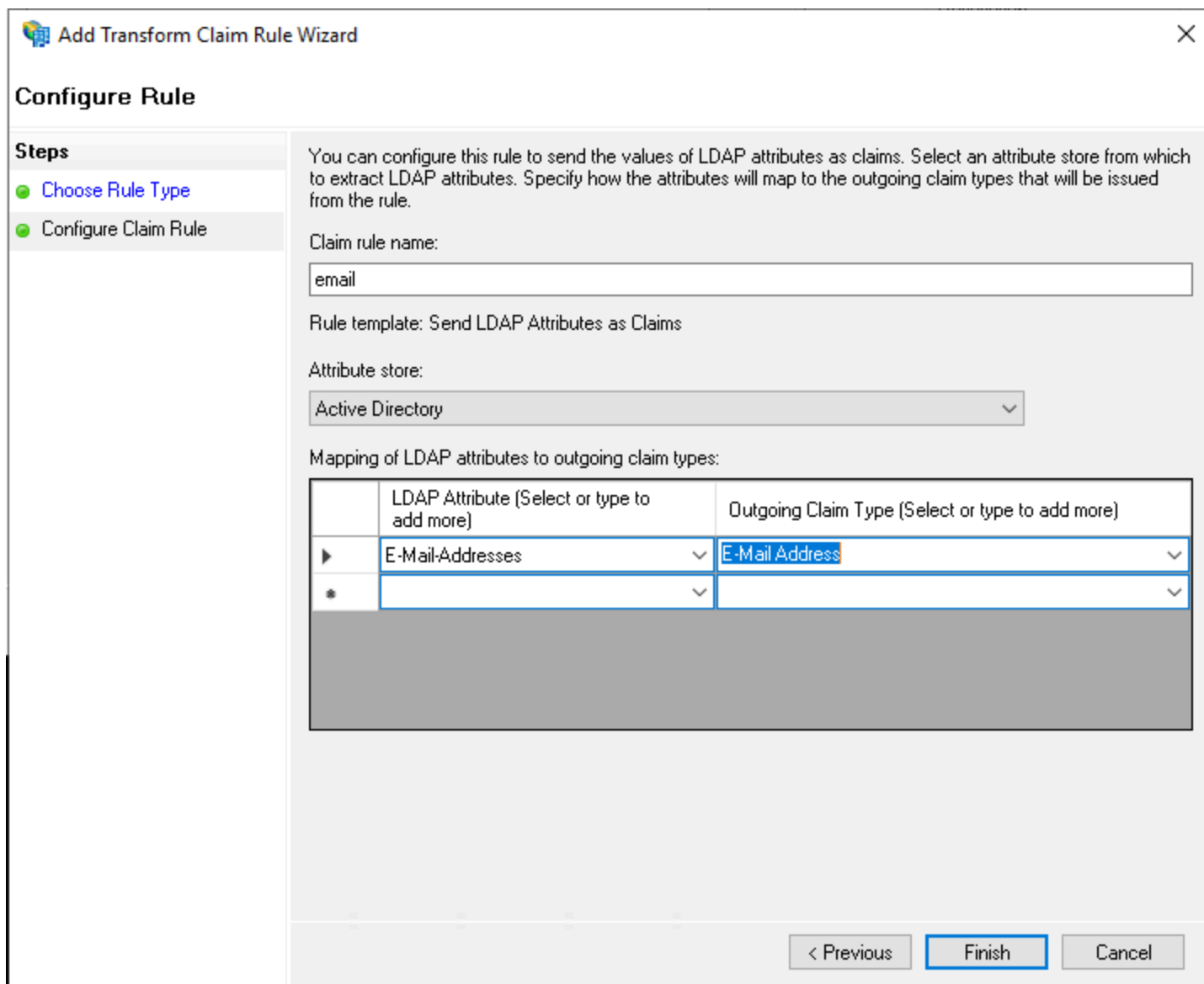
8. Finish the Add Application Group Wizard.

## 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 **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**

**Configure Rule**

**Steps**

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:  
email

Rule template: Send LDAP Attributes as Claims

Attribute store:  
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	E-Mail Address
*		

< 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 context 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 <code>/adfs</code> appended, for example <code>https://adfs.mybusiness.com/adfs</code> .
Client ID	Enter the <code>retrieved</code> Client ID.
Client Secret	Enter the <code>retrieved</code> Client Secret.
Metadata Address	Enter the specified <b>Authority</b> value with <code>/.well-known/openid-configuration</code> appended, for example <code>https://adfs.mybusiness.com/adfs/.well-known/openid-configuration</code> .
OIDC Redirect Behavior	Select <b>Redirect GET</b> .
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.

Field	Description
Requested Authentication Context Class References values	Define Authentication Context Class Reference identifiers ( <b>acr_values</b> ) (space-delimited). List <b>acr_values</b> in preference-order.
Expected "acr" Claim Value In Response	Define the <b>acr</b> 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 to Bitwarden

Email address (required)

☒ Remember email

Continue

or

 Log in with passkey

 Use single sign-on

New to Bitwarden? [Create account](#)

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!

### 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.