Implementación de ADFS OIDC

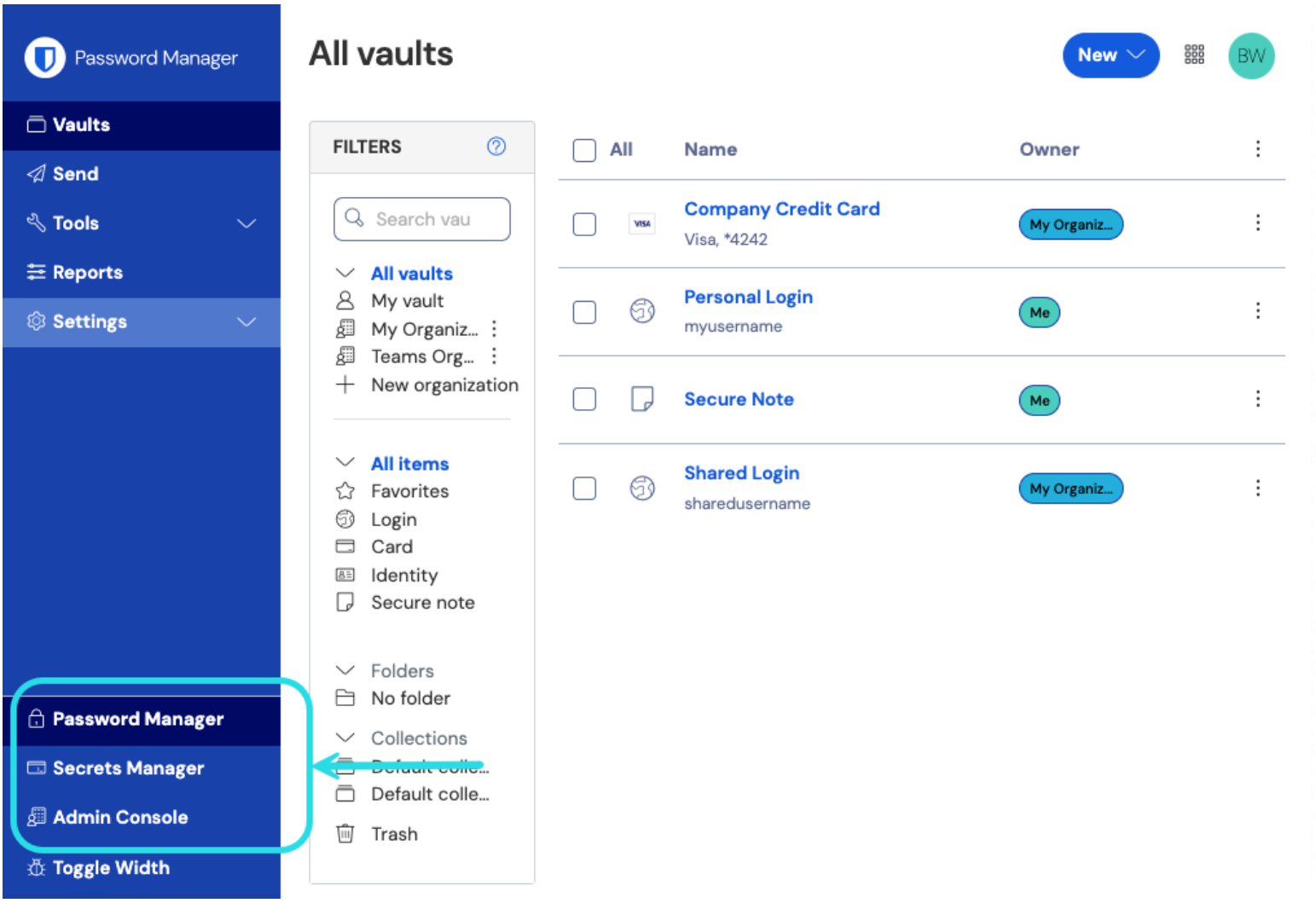
Implementación de ADFS OIDC

Este artículo contiene ayuda **específica de Active Directory Federation Services (AD FS)** para configurar el inicio de sesión con SSO a través de OpenID Connect (OIDC). Para obtener ayuda para configurar el inicio de sesión con SSO para otro IdP OIDC, o para configurar AD FS a través de SAML 2.0, consulte Configuración OIDC o Implementación ADFS SAML.

La configuración implica trabajar simultáneamente dentro de la aplicación web de Bitwarden y el gestor de servidores AD FS. A medida que avanza, recomendamos tener ambos fácilmente disponibles y completar los pasos en el orden en que están documentados.

Abre SSO en la caja fuerte web

Inicia sesión en la aplicación web de Bitwarden y abre la Consola de Administrador usando el cambiador de producto (⊞):



Selector de producto

Seleccione **Ajustes** → **Inicio de sesión único** desde la navegación:

Configuración de OIDC

Si aún no lo has hecho, crea un **identificador SSO** único para tu organización. De lo contrario, no necesitas editar nada en esta pantalla todavía, pero mantenla abierta para una fácil referencia.

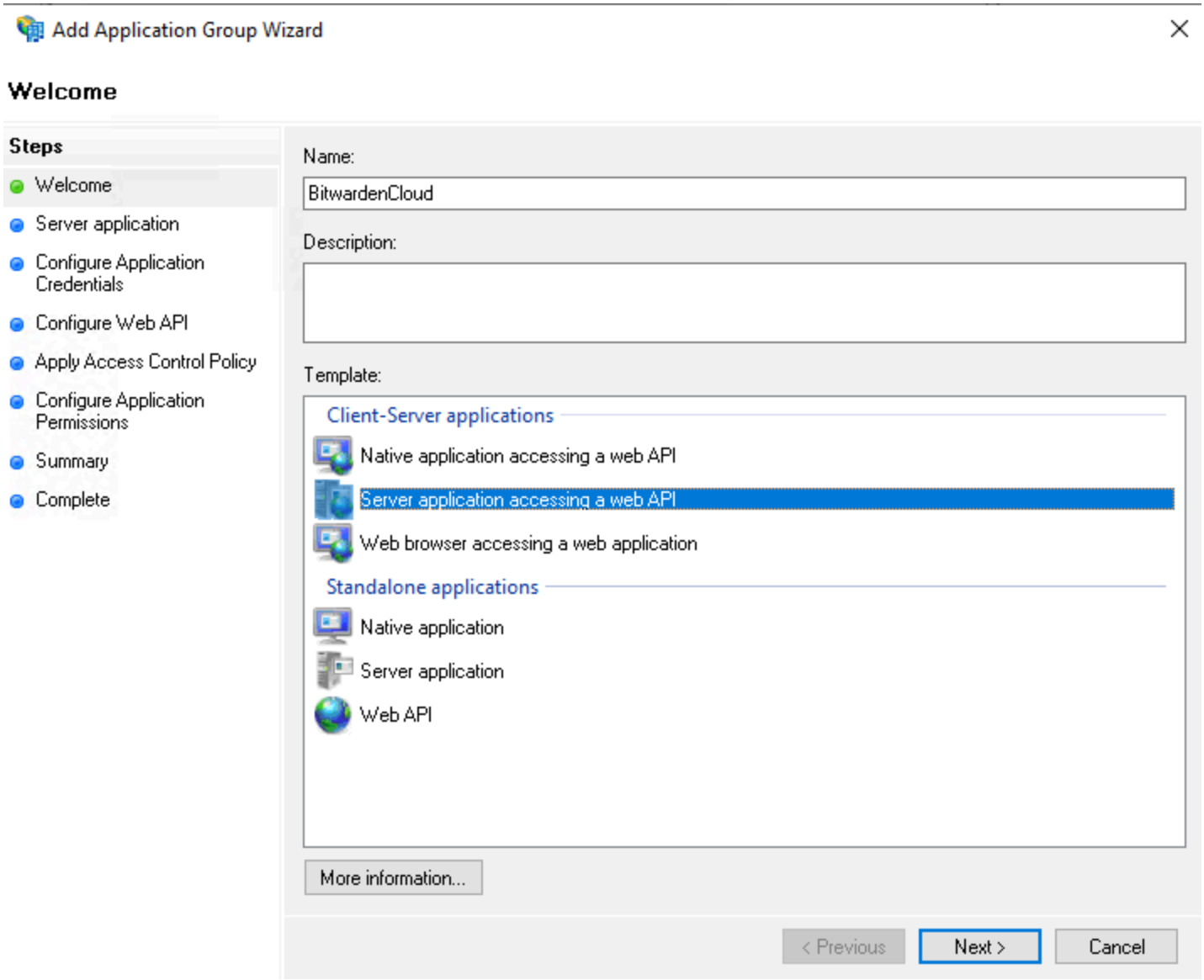
> **Tip**
>
> Hay opciones alternativas de **descifrado de miembro**. Aprenda cómo comenzar a usar SSO con dispositivos de confianza o Conector de clave.

Crea un grupo de aplicación

En el Administrador de Servidor, navega a **Gestión de AD FS** y crea un nuevo grupo de aplicaciones:

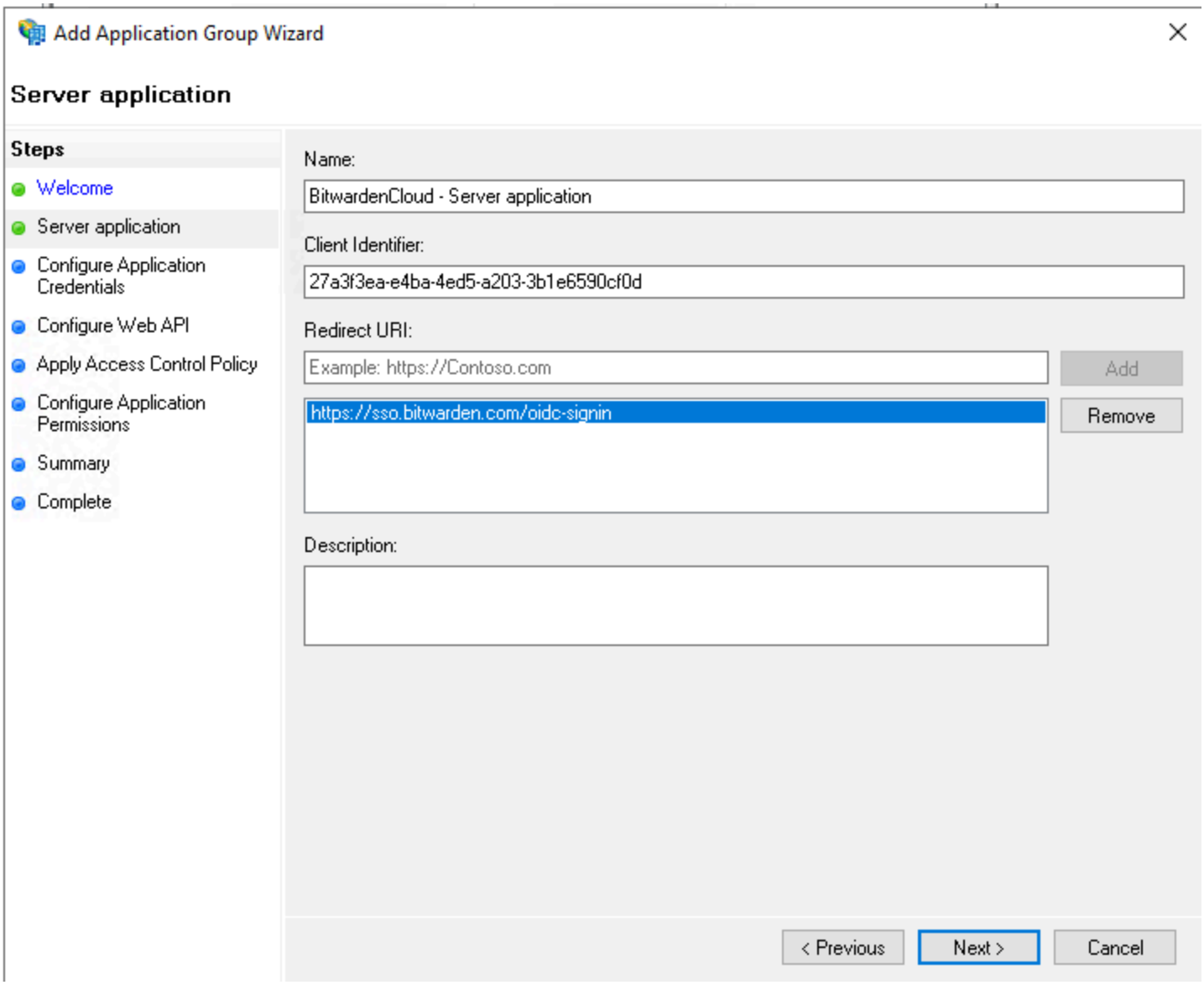
1. En el árbol de la consola, selecciona **Grupos de Aplicaciones** y elige **Agregar Grupo de Aplicaciones** de la lista de Acciones.

2. En la pantalla de bienvenida del asistente, elija la plantilla de **Aplicación de servidor que accede a una API web**.



AD FS Add Application Group

3. En la pantalla de la aplicación del servidor:

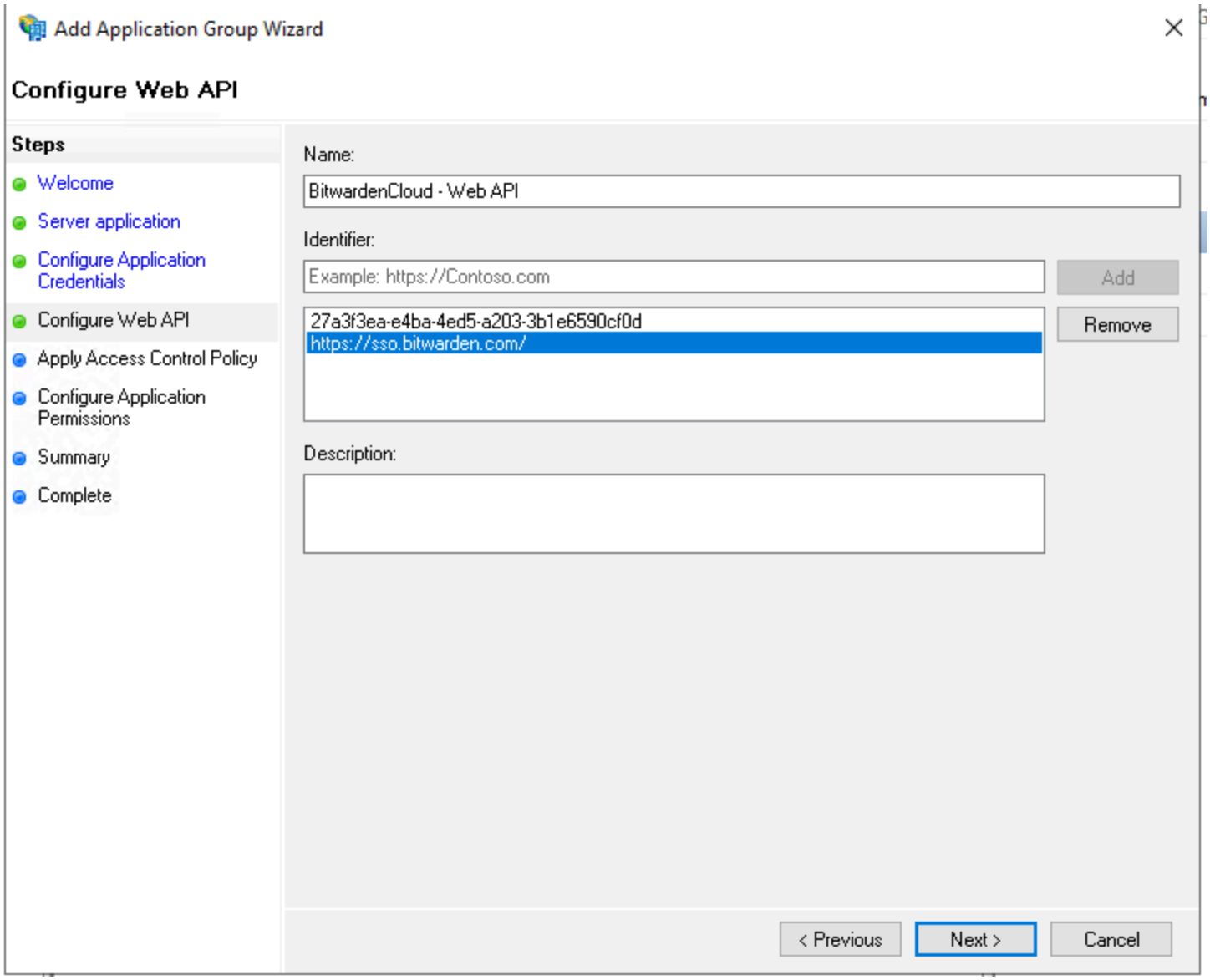


AD FS Server Application screen

- Dale a la aplicación del servidor un **Nombre**.
- Toma nota del **Identificador del Cliente**. Necesitarás este valor en un paso posterior.
- Especifique una **URI de redirección**. Para los clientes alojados en la nube, esto es `https://sso.bitwarden.com/oidc-signin` o `https://sso.bitwarden.eu/oidc-signin`. Para instancias autoalojadas, esto está determinado por la URL de su servidor configurado, por ejemplo `https://your.domain.com/sso/oidc-signin`.

4. En la pantalla de Configurar Credenciales de Aplicación, tome nota del **Secreto del Cliente**. Necesitarás este valor en un paso posterior.

5. En la pantalla de Configuración de la API Web:

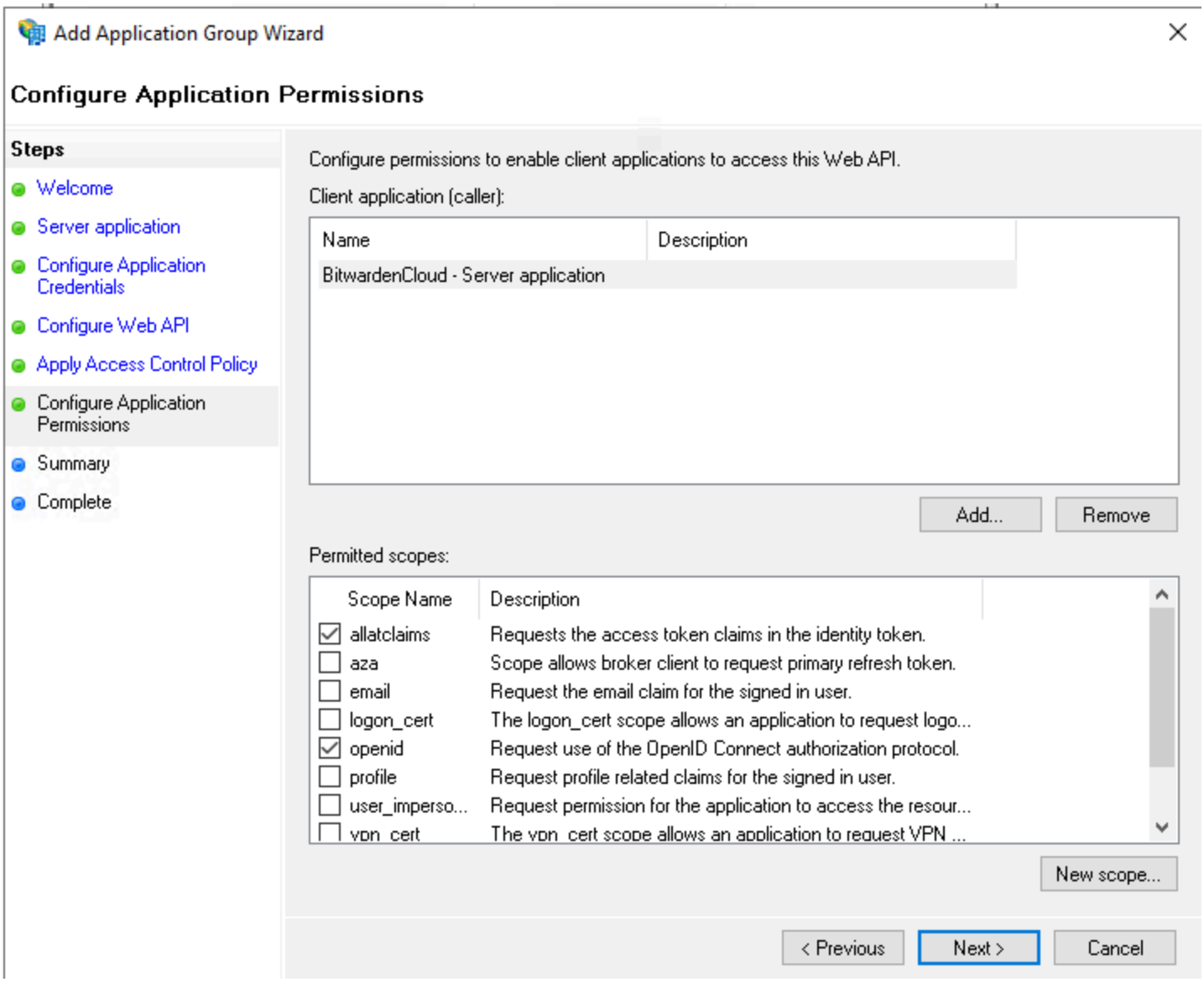


AD FS Configure Web API screen

- Dale a la API web un **Nombre**.
- Agregue el **Identificador del Cliente** y **URI de Redirección** (vea el paso 2B. & C.) a la lista de Identificadores.

6. En la pantalla de Aplicar Política de Control de Acceso, establezca una Política de Control de Acceso apropiada para el Grupo de Aplicaciones.

7. En la pantalla de configuración de permisos de la aplicación, permite los alcances `allatclaims` y `openid`.



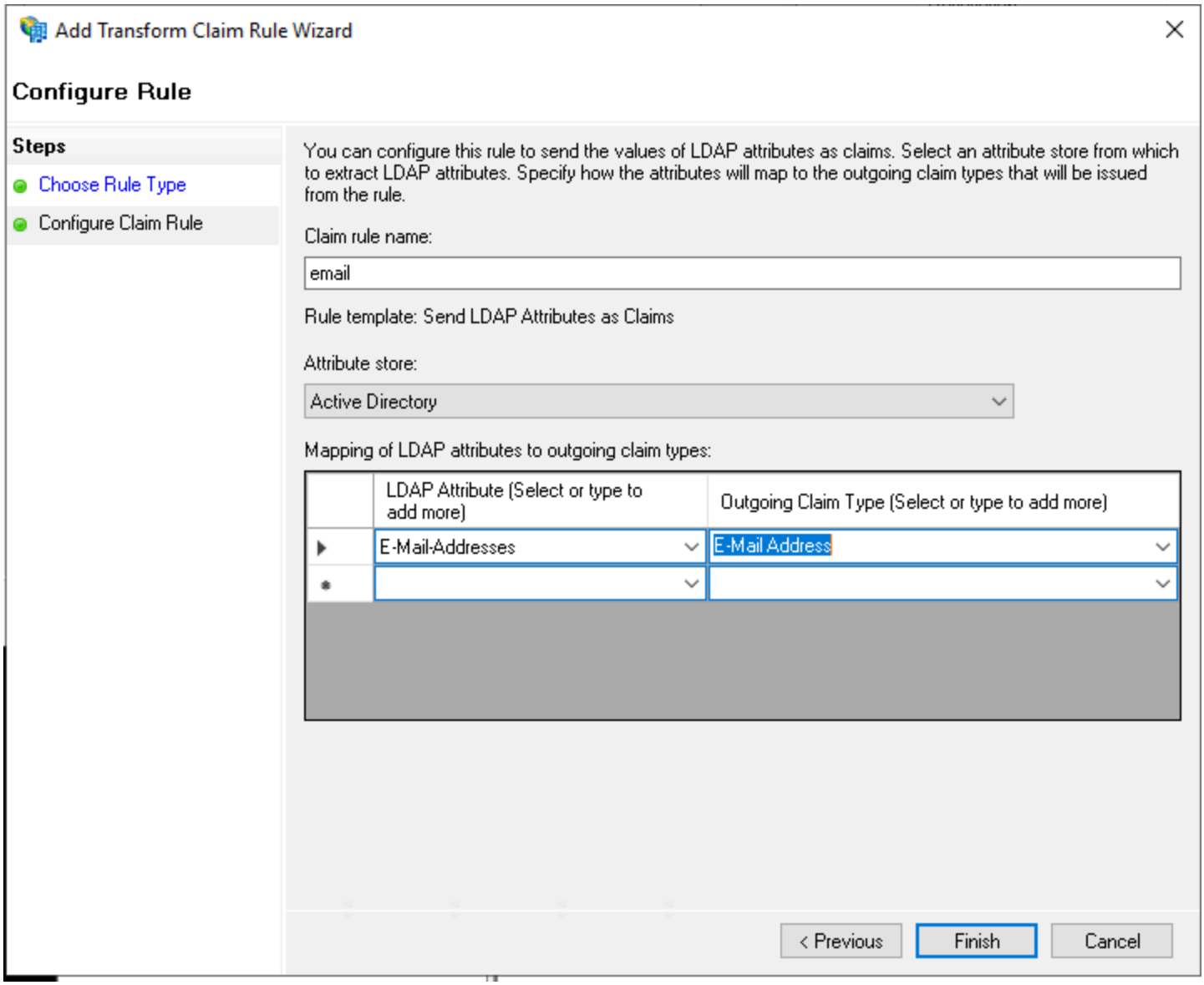
AD FS Configure Application Permissions screen

8. Finaliza el Asistente de Agregar Grupo de Aplicación.

Agrega una regla de reclamación de transformación

En el Administrador de Servidores, navegue a **Gestión de AD FS** y edite el grupo de aplicaciones creado:

1. En el árbol de la consola, selecciona **Grupos de Aplicaciones**.
2. En la lista de Grupos de Aplicaciones, haga clic derecho en el grupo de aplicaciones creado y seleccione **Propiedades**.
3. En la sección de Aplicaciones, elige la API Web y selecciona **Editar...** .
4. Navegue a la pestaña **Reglas de Transformación de Emisión** y seleccione el botón **Agregar Regla...** .
5. En la pantalla de Seleccionar Tipo de Regla, seleccione **Enviar atributos LDAP como reclamaciones.**
6. En la pantalla de Configuración de Regla de Reclamo:



AD FS Configure Claim Rule screen

- Dale a la regla un **Nombre de regla de reclamación**.
- Del menú desplegable de Atributos LDAP, selecciona **Direcciones de correo electrónico.**
- Del menú desplegable de Tipo de Reclamo Saliente, selecciona **Dirección de Correo Electrónico**.

7. Seleccionar **Finalizar.**

De vuelta a la aplicación web

En este punto, has configurado todo lo que necesitas dentro del concurso del Gestor de Servidor AD FS. Regresa a la aplicación web de Bitwarden para configurar los siguientes campos:

Campo	Descripción
Autoridad	Ingrese el nombre de host de su servidor AD FS con `/adfs` añadido, por ejemplo `https://adfs.mybusiness.com/adfs`.
ID de cliente	Ingrese el ID de Cliente recuperado.
Secreto del Cliente	Ingrese el Secreto de Cliente recuperado.
Dirección de Metadatos	Ingrese el valor de **Autoridad** especificado con `/.well-known/openid-configuration` añadido, por ejemplo `https://adfs.mybusiness.com/adfs/.well-known/openid-configuration`.
Comportamiento de Redirección OIDC	Seleccione **Redirigir GET**.
Obtener reclamos del endpoint de información del usuario	Habilite esta opción si recibe errores de URL demasiado larga (HTTP 414), URLS truncadas y/o fallos durante el SSO.
Alcances personalizados	Define los ámbitos personalizados para agregar a la solicitud (delimitados por comas).
Tipos de Reclamaciones de ID de Usuario del Cliente	Defina las claves de tipo de reclamación personalizadas para la identificación del usuario (delimitadas por comas). Cuando se definen, se busca los tipos de reclamaciones personalizadas antes de recurrir a los tipos estándar.
Tipos de Reclamaciones de Correo Electrónico	Defina las claves de tipo de reclamación personalizadas para las direcciones de correo electrónico de los usuarios (delimitadas por comas). Cuando se definen, se busca los tipos de reclamaciones personalizadas antes de recurrir a los tipos estándar.
Tipos de Reclamaciones de Nombres Personalizados	Defina las claves de tipo de reclamación personalizadas para los nombres completos o nombres de visualización de los usuarios (delimitados por comas). Cuando se definen, se busca en los tipos de reclamaciones personalizadas antes de recurrir a los tipos estándar.

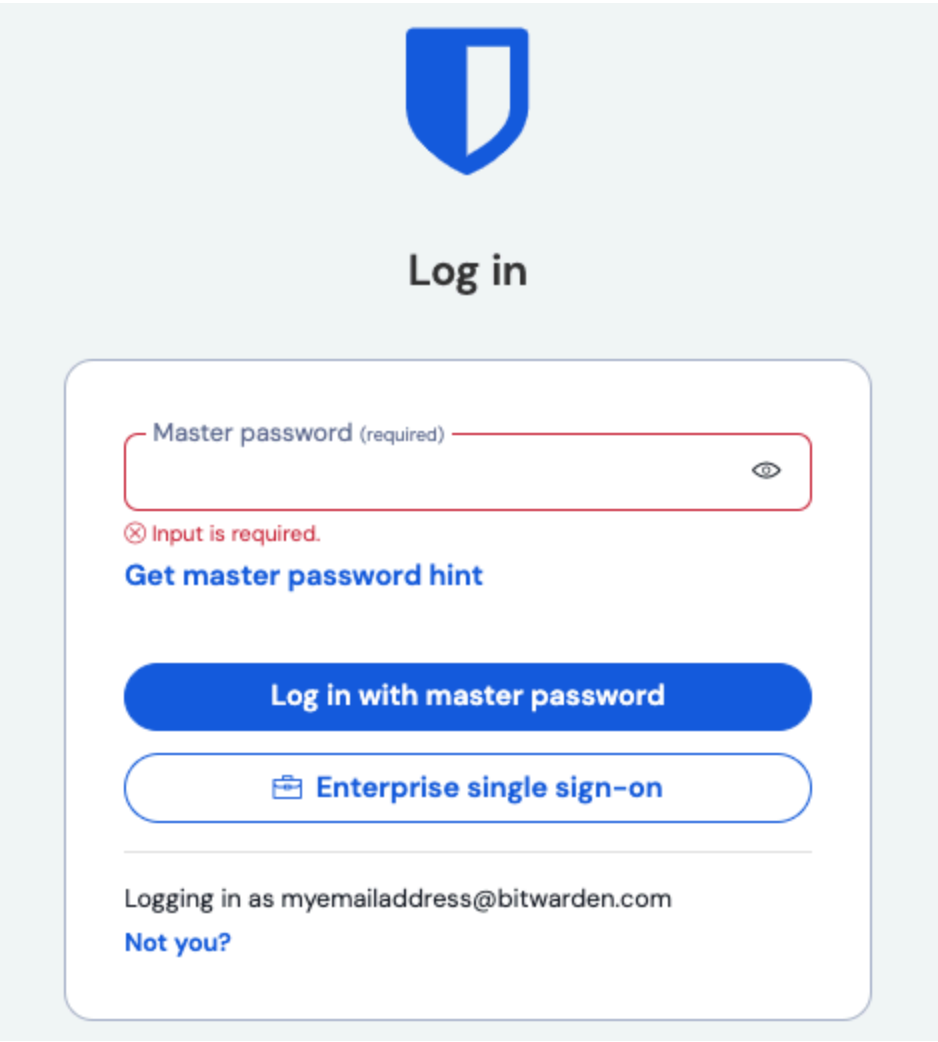
Campo	Descripción
Valores de Referencias de Clase de Contexto de Autenticación Solicitados	Defina los identificadores de referencia de la clase de contexto de autenticación (`acr_values`) (delimitados por espacios). Lista `acr_values` en orden de preferencia.
Valor de reclamación "acr" esperado en respuesta	Define el valor de la reclamación `acr` que Bitwarden espera y valida en la respuesta.

Cuando hayas terminado de configurar estos campos, **Guarda** tu trabajo.

> **Tip**
> Puede requerir que los usuarios inicien sesión con SSO activando la política de autenticación de inicio de sesión único. Por favor, tome nota, esto también requerirá la activación de la política de organización única. Más información.

Prueba la configuración

Una vez que tu configuración esté completa, pruébala navegando a https://vault.bitwarden.com, ingresando tu dirección de correo electrónico, seleccionando **Continuar**, y seleccionando el botón **Empresa Único-Inicio**:



Inicio de sesión único empresarial y contraseña maestra

Ingrese el ID de organización configurado y seleccione **Iniciar sesión**. Si su implementación está configurada con éxito, será redirigido a la pantalla de inicio de sesión de AD FS SSO. ¡Después de autenticarte con tus credenciales de AD FS, ingresa tu contraseña maestra de Bitwarden para descifrar tu caja fuerte!

> **Note**
> Bitwarden no admite respuestas no solicitadas, por lo que iniciar el inicio de sesión desde su IdP resultará en un error. El flujo de inicio de sesión de SSO debe iniciarse desde Bitwarden.