

CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO >

Implementación de ADFS SAML

Ver en el centro de ayuda:

<https://bitwarden.com/help/saml-ads/>

Implementación de ADFS SAML

Este artículo contiene ayuda **específica de Active Directory Federation Services (AD FS)** para configurar el inicio de sesión con SSO a través de SAML 2.0. Para obtener ayuda para configurar el inicio de sesión con SSO para otro IdP, consulte [Configuración de SAML 2.0](#).

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.

Tip

¿Ya eres un experto en SSO? Omite las instrucciones en este artículo y descarga capturas de pantalla de configuraciones de muestra para comparar con las tuyas.

📄 tipo: activo-hipervínculo id: 5892IOGrU7B9lvBmNOPOxl

Abre SSO en la aplicación web

Inicia sesión en la aplicación web de Bitwarden y abre la Consola de Administrador utilizando el conmutador de producto (🏠):

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login sharedusername	My Organiz...	⋮

Selector de producto

Abra la pantalla de **Ajustes** → **Inicio de sesión único** de su organización:

bitwarden Admin Console

- 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
SAML 2.0

SAML service provider configuration

Set a unique SP entity ID

Generate an identifier that is unique to your organization

SP entity ID
[Blurred text]

SAML 2.0 metadata URL
[Blurred text]

Configuración de SAML 2.0

Si aún no lo has hecho, crea un **identificador SSO** único para tu organización y selecciona **SAML** del menú desplegable de **Tipo**. Mantén esta pantalla abierta para fácil referencia.

Puedes desactivar la opción **Establecer una ID de entidad SP única** en esta etapa si lo deseas. Hacerlo eliminará su ID de organización de su valor de ID de entidad SP, sin embargo, en casi todos los casos, se recomienda dejar esta opción activa.



Hay opciones alternativas de **descifrado de miembro**. Aprenda cómo comenzar a usar [SSO con dispositivos de confianza](#) o [Conector de clave](#).

Crear una confianza de parte confiable

En el Administrador de Servidor AD FS, selecciona **Herramientas** → **Gestión de AD FS** → **Acción** → **Agregar Confianza de Parte Dependiente**. En el asistente, haga las siguientes selecciones:

1. En la pantalla de bienvenida, seleccione **Consciente de reclamaciones**.

2. En la pantalla de Selección de Fuente de Datos, seleccione **Ingrese datos sobre la parte confiada manualmente**.
3. En la pantalla de Especificar Nombre de Visualización, ingrese un nombre de visualización específico de Bitwarden.
4. En la pantalla de Configurar URL, seleccione **Habilitar soporte para el protocolo WebSSO SAML 2.0**.
 - En la entrada de **URL del servicio SSO SAML 2.0 de la parte confiable**, ingrese la URL del Servicio de Consumo de Aserciones (ACS). Este valor generado automáticamente se puede copiar desde la pantalla de **Ajustes → Inicio de sesión único** de la organización y variará según su configuración.
5. En la pantalla de **Elegir Política de Control de Acceso**, seleccione la política que cumpla con sus estándares de seguridad.
6. En la pantalla de **Configurar Identificadores**, agregue el ID de la Entidad SP como un identificador de confianza de la parte dependiente. Este valor generado automáticamente se puede copiar desde la pantalla de **Ajustes → Inicio de sesión único** de la organización y variará según su configuración.
7. En la pantalla de **Elegir Política de Control de Acceso**, seleccione la política deseada (por defecto, **Permitir a Todos**).
8. En la pantalla **Listo para Agregar Confianza**, revise sus selecciones.

Opciones avanzadas

Una vez que se crea la confianza de la parte confiada, puedes configurar aún más sus ajustes seleccionando **Confianzas de la Parte Confiada** desde el navegador de archivos de la mano izquierda y seleccionando el nombre de visualización correcto.

Algoritmo hash

Para cambiar el **Algoritmo de hash seguro** (por defecto, SHA-256), navega a la pestaña **Avanzado**:

The screenshot shows the AD FS console with the 'Relying Party Trusts' section selected. A table lists the trust configuration:

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

The 'Bitwarden ADFS Test Properties' dialog box is open, showing the 'Advanced' tab. The 'Secure hash algorithm' is set to 'SHA-256'.

Establecer un Algoritmo de Hash Seguro

Vinculación de punto final

Para cambiar el punto final **Binding** (por defecto, POST), navegue a la pestaña **Endpoints** y seleccione la URL de ACS configurada:

The screenshot shows the AD FS console interface. On the left is a tree view with 'Relying Party Trusts' selected. The main pane shows a table of Relying Party Trusts:

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

The 'Bitwarden ADFS Test Properties' dialog box is open, showing the 'Endpoints' tab. It contains a table of endpoints:

URL	Index	Binding	Default	Re
SAML Assertion Consumer Endpoints				
https://sso.bitwarden.com/sa...	0	POST	Yes	

The 'Edit Endpoint' dialog box is also open, with the 'Binding' dropdown menu highlighted in green. The 'Binding' is set to 'POST'. Other fields include 'Endpoint type' (SAML Assertion Consumer), 'Index' (0), 'Trusted URL' (https://sso.bitwarden.com/saml2/3e5d0), and 'Response URL'.

Editar Punto Final

Editar reglas de emisión de reclamaciones

Construye reglas de emisión de reclamaciones para asegurar que las reclamaciones apropiadas, incluyendo **ID de Nombre**, se pasen a Bitwarden. Las siguientes pestañas ilustran un conjunto de reglas de muestra:

⇒Regla 1

The screenshot shows the Windows AD FS console with the 'Relying Party Trusts' pane open. A table lists the trust configuration:

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

An 'Edit Claim Issuance Policy for Bitwarden ADFS Test' dialog is open, showing 'Issuance Transform Rules' for the trust:

Order	Rule Name	Issued Claims
1	Bitwarden	E-Mail Address, Name, Giv...
2	UPN	UPN
3	Transform Name ID	Name ID

The 'Edit Rule - Bitwarden' dialog is also open, showing configuration details:

- Claim rule name: Bitwarden
- 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
	Display-Name	Name
	Given-Name	Given Name
	Surname	Surname
*		

Buttons at the bottom of the dialog include 'View Rule Language...', 'OK', and 'Cancel'.

Regla 1 de ADFS

⇒Regla 2

AD FS

File Action View Window Help

AD FS

- Service
 - Attribute Stores
 - Authentication Methods
 - Certificates
 - Claim Descriptions
 - Device Registration
 - Endpoints
 - Scope Descriptions
 - Web Application Proxy
 - Access Control Policies
 - Relying Party Trusts**
 - Claims Provider Trusts
 - Application Groups

Relying Party Trusts

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

Edit Claim Issuance Policy for Bitwarden ADFS Test

Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Bitwarden	E-Mail Address, Name, Giv...
2	UPN	UPN
3	Transform Name ID	Name ID

Edit Rule - UPN

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:

Rule template: Send LDAP Attributes as Claims

Attribute store:

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)
▶	User-Principal-Name	UPN
*		

Regla 2 de ADFS

⇒Regla 3

The screenshot shows the AD FS console interface. On the left, the 'Service' folder is expanded to show 'Relying Party Trusts'. The main pane displays a table of Relying Party Trusts:

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

An 'Edit Claim Issuance Policy for Bitwarden ADFS Test' dialog is open, showing a table of Issuance Transform Rules:

Order	Rule Name	Issued Claims
1	Bitwarden	E-Mail Address, Name, Giv...
2	UPN	UPN
3	Transform Name ID	Name ID

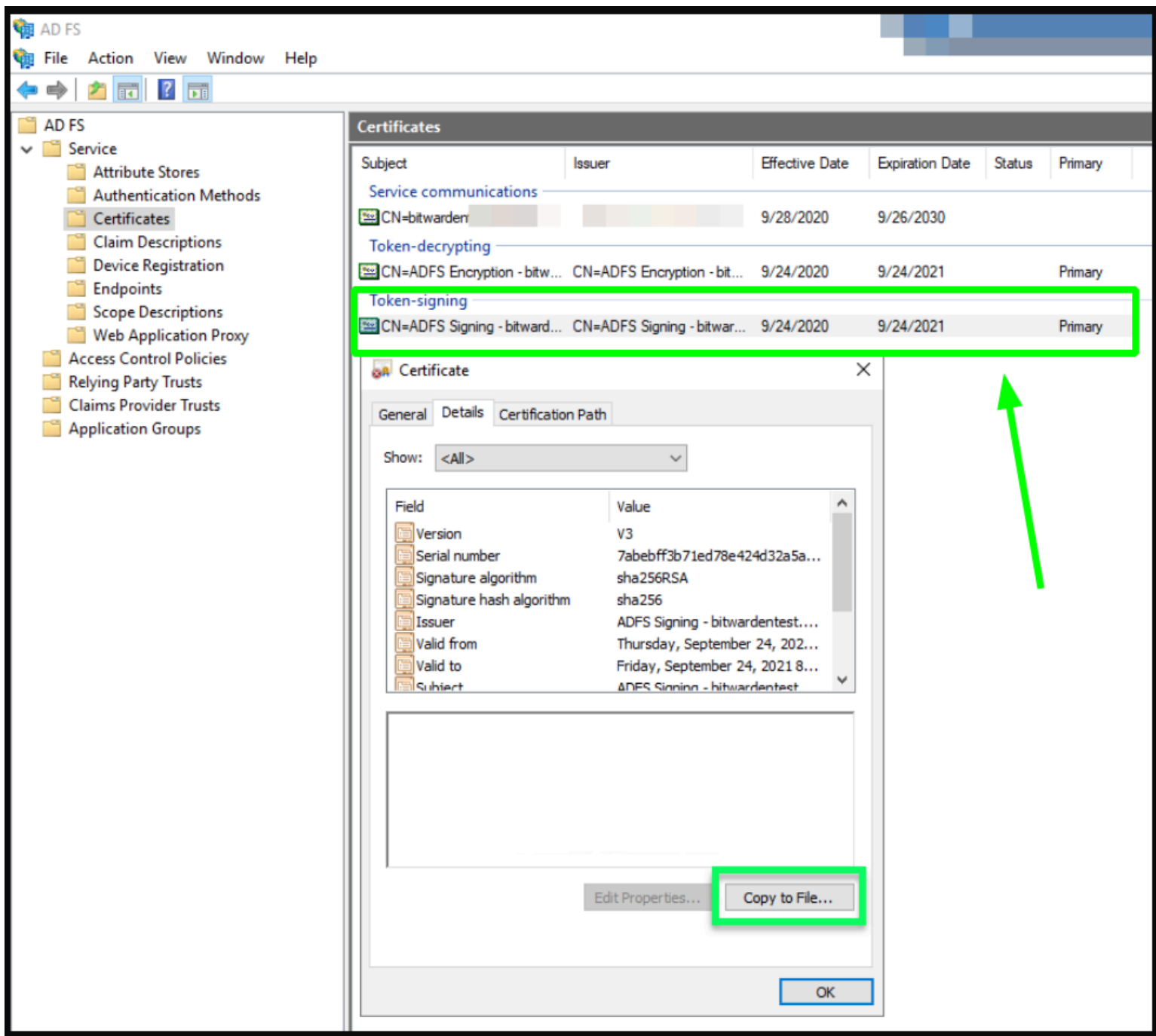
The 'Edit Rule - Transform Name ID' dialog is also open, showing the configuration for this rule:

- Claim rule name: Transform Name ID
- Rule template: Transform an Incoming Claim
- Incoming claim type: UPN
- Incoming name ID format: Unspecified
- Outgoing claim type: Name ID
- Outgoing name ID format: Persistent Identifier
- Selected option: Pass through all claim values

Regla 3 de ADFS

Obtener certificado

En el navegador de archivos de la mano izquierda, seleccione **AD FS** → **Servicio** → **Certificados** para abrir la lista de certificados. Seleccione el certificado de **firma de token**, navegue hasta su pestaña de **Detalles**, y seleccione el botón de **Copiar a Archivo...** para exportar el certificado de firma de token codificado en Base-64:

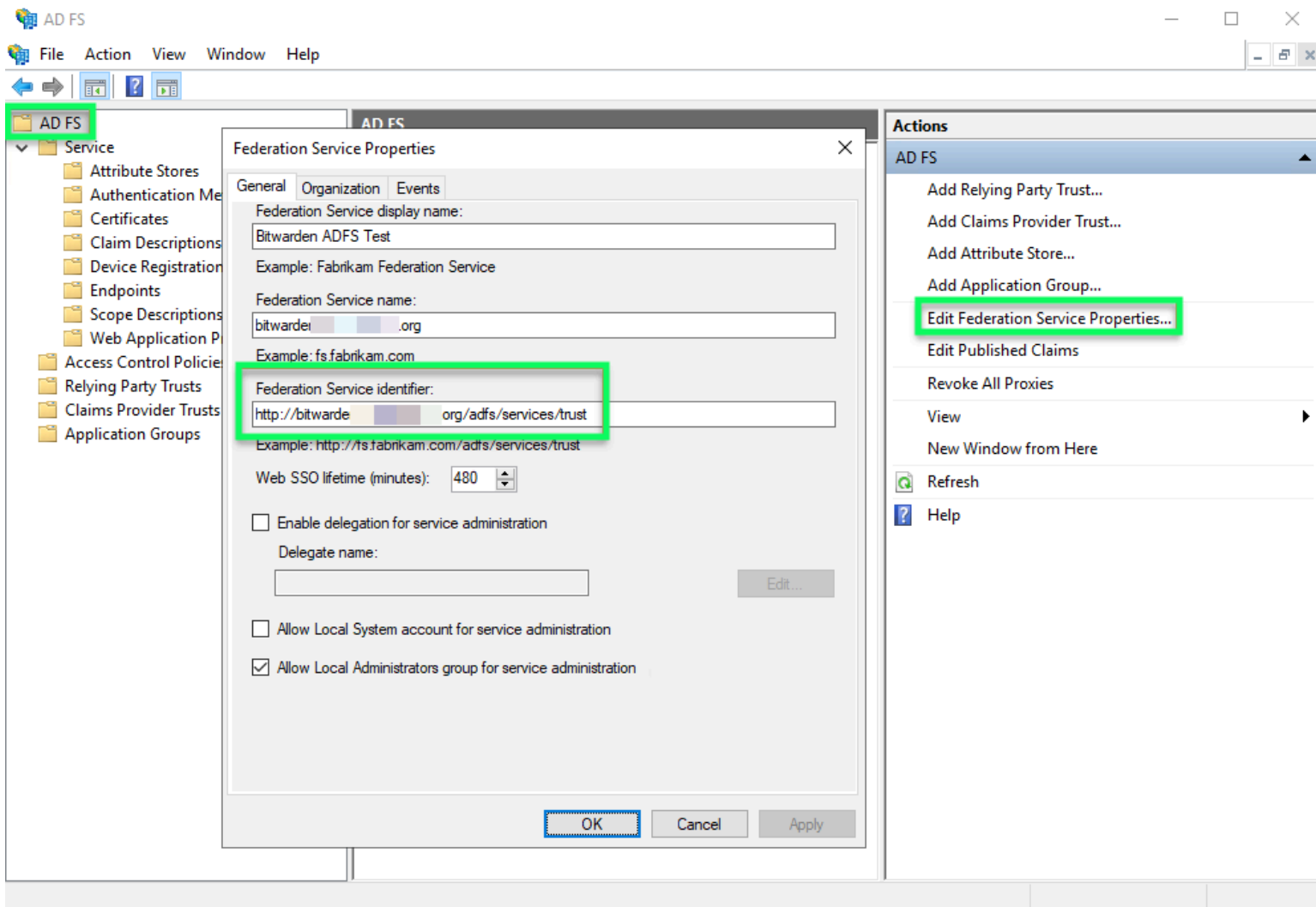


Obtener Certificado de firma de token

Necesitarás este certificado [durante un paso posterior](#).

Obtener el identificador del servicio de federación

En el navegador de archivos de la mano izquierda, selecciona **AD FS** y desde el menú de opciones de la mano derecha selecciona **Editar Propiedades del Servicio de Federación**. En la ventana de Propiedades del Servicio de Federación, copia el **Identificador del Servicio de Federación**:



Obtener Identificador de Servicio de Federación

Necesitarás este identificador durante un paso posterior.

De vuelta a la aplicación web

En este punto, has configurado todo lo que necesitas dentro del contexto del Administrador de Servidor AD FS. Regresa a la aplicación web de Bitwarden para completar la configuración.

La pantalla de inicio de sesión único separa la configuración en dos secciones:

- La configuración del proveedor de servicios SAML determinará el formato de las solicitudes SAML.
- La configuración del proveedor de identidad SAML determinará el formato que se esperará de las respuestas SAML.

Configuración del proveedor de servicios

En la sección de configuración del proveedor de servicios, configure los siguientes campos:

Campo	Descripción
Formato de Identificación de Nombre	Seleccione el Formato de ID de Nombre Saliente seleccionado al construir reglas de emisión de reclamaciones (ver Regla 3).
Algoritmo de Firma de Salida	El algoritmo que Bitwarden utilizará para firmar solicitudes SAML.
Comportamiento de Firma	Si/cuando las solicitudes SAML serán firmadas.
Algoritmo Mínimo de Firma Entrante	Por defecto, AD FS firmará con SHA-256. Seleccione SHA-256 del menú desplegable a menos que haya configurado AD FS para usar un algoritmo diferente .
Quiero Afirmaciones Firmadas	Si Bitwarden espera que las afirmaciones SAML estén firmadas.
Validar Certificados	Marque esta casilla cuando utilice certificados confiables y válidos de su IdP a través de una CA de confianza. Los certificados autofirmados pueden fallar a menos que se configuren cadenas de confianza adecuadas dentro de la imagen de docker de inicio de sesión de Bitwarden con SSO.

Cuando termines con la configuración del proveedor de servicios, **Guarda** tu trabajo.

Configuración del proveedor de Identidad

La configuración del proveedor de Identidad a menudo requerirá que te refieras de nuevo al Administrador del Servidor AD FS para recuperar valores:

Campo	Descripción
ID de la entidad	Ingrese el Identificador del Servicio de Federación recuperado. Por favor, toma nota, esto puede que no use HTTPS . Este campo distingue entre mayúsculas y minúsculas.

Campo	Descripción
Tipo de Encuadernación	Por defecto, AD FS utilizará el enlace de punto final HTTP POST. Seleccione HTTP POST a menos que haya configurado AD FS para usar un método diferente .
URL del Servicio de Inicio de Sesión Único	Ingrese el punto final del servicio SSO. Este valor puede ser construido en la pestaña Servicio → Puntos finales en el gestor de AD FS. La URL del punto final se enumera como Ruta URL para SAML2.O/WS-Federation y generalmente es algo como https://tu-dominio/adfs/ls . Puede obtener el valor exacto de la clave de configuración para SingleSignOnService en el documento FederationMetadata.xml .
Certificado Público X509	Pega el certificado descargado, eliminando -----INICIO CERTIFICADO----- y -----FIN DEL CERTIFICADO----- El valor del certificado es sensible a mayúsculas y minúsculas, espacios extra, retornos de carro y otros caracteres extraneos harán que la certificación falle .
Algoritmo de Firma de Salida	Por defecto, AD FS firmará con SHA-256. Seleccione SHA-256 del menú desplegable a menos que haya configurado AD FS para usar un algoritmo diferente .
Deshabilitar Solicitudes de Cierre de Sesión Salientes	El inicio de sesión con SSO actualmente no admite SLO. Esta opción está planeada para un desarrollo futuro.
Quiere Solicitudes de Autenticación Firmadas	Si AD FS espera que las solicitudes SAML estén firmadas.

Note

Al completar el certificado X509, toma nota de la fecha de vencimiento. Los certificados tendrán que ser renovados para prevenir cualquier interrupción en el servicio a los usuarios finales de SSO. Si un certificado ha caducado, las cuentas de Administrador y Propietario siempre podrán iniciar sesión con la dirección de correo electrónico y la contraseña maestra.

Cuando termines con la configuración del proveedor de identidad, **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 de **Empresa de Inicio de Sesión Único**:



Log in to Bitwarden

Email address (required)

Remember email

Continue

or

Log in with passkey

Use single sign-on

New to Bitwarden? [Create account](#)

Inicio de sesión único empresarial y contraseña maestra

Ingrese el [identificador 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.