

CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO >

Implementación de ADFS SAML

Ver en el centro de ayuda: https://bitwarden.com/help/saml-adfs/

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

Already an SSO expert? Skip the instructions in this article and download screenshots of sample configurations to compare against your own.

Jownload sample ↓

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 (ﷺ):

Password Manager	All vaults			New 💛	BW BW
🗇 Vaults			Name	0	
🖉 Send			Name	Owner	:
\ll Tools \sim	Q Search vau	ASIV	Company Credit Card Visa, *4242	My Organiz	:
≅ Reports	✓ All vaults		Personal Login		
🕸 Settings 🛛 🗸 🗸	🖄 My Vault 🗐 My Organiz :	0 6	myusername	Me	:
	 Earns Org : + New organization 		Secure Note	Ме	:
	 ✓ All items ☆ Favorites ③ Login □ Card △ Identity □ Secure note 	0 9	Shared Login sharedusername	My Organiz	÷
Password Manager	 ✓ Folders ➡ No folder ✓ Collections 				
🗔 Secrets Manager					
🖉 Admin Console	Default colle				
杰 Toggle Width	🔟 Trash				

Selector de producto

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

D bit warden	Single sign-on III III III III III III III III III I
B My Organization	✓ Use the <u>require single sign-on authentication policy</u> 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.
绺 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 Policies	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.
Two-step login	C Type
Import data	SAML 2.0
Export vault	
Domain verification	SAML service provider configuration
Single sign-on	Set a unique SP entity ID
Device approvals	Generate an identifier that is unique to your organization SP entity ID
SCIM provisioning	
	SAML 2.0 metadata URL

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.

∏ Tip

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 \rightarrow Gestión de AD FS \rightarrow Acción \rightarrow 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:

翰 AD FS					
🎕 File Action View Window Help					
🔶 🄿 🖄 📰 🛛 🗊					
AD FS	Relying Party Trusts				
Service Attribute Stores	Display Name	Enabled	Туре	Identifier	Access Control Policy
Authentication Methods	Bitwarden ADFS Test	Yes	WS-T	https://sso.bitwarden.com/saml2	Permit everyone
Certificates	[
Device Registration	Bitwarden ADFS Test Properties			×	
Endpoints	Monitoring Identifiers Encryption Sig	gnature Acce	pted Claims		
Scope Descriptions	Organization Endpoints Proxy Endpoin	ts Notes	Advanced		
ACCESS CONTION POLICIE	Specify the secure hash algorithm to use for t	nis relying party tr	ust.		
Relying Party Trusts	Secure hash algorithm: SHA-256		~	1	
Application Groups					
		0			
	OK	Cancel	Apply		

Set a Secure Hash Algorithm

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:

File Action View Window Help						
🔿 📶 🛛 🖬						
AD FS	Relying Party Trusts					
Service	Display Name	En	abled	Туре	Identifier	Access Control Policy
Authentication Methods Certificates	Bitwarden ADFS Test	Ye	3	WS-T	https://sso.bitwarden.com/saml2	Permit everyone
Claim Descriptions Device Registration	Bitwarden ADFS Test Proper	ties		2	×	
Endpoints Scope Descriptions	Monitoring Identifiers Organization Endpoints	Encryption Signature Proxy Endpoints No	Accepte otes Ad	ed Claims dvanced		
Web Application Proxy Access Control Policies	Specify the endpoints to use f	or SAML and WS-Federatio	onPassive p	protocols.		
Relying Party Trusts Claims Provider Trusts Application Groups	URL SAML Assertion Consu	Index Binding	Defau	ult Re		
	https://sso.bitwarden.co	om/sa 0 POST	Yes			
		Edit Endpoint			×	
		Endpoint type: SAML Assertion Consum	er		~	
		Binding:				
		POST	e default			
	<	Index: 0				
	Add WS-Federation	Trusted URL:				
		https://sso.bitwarden.com Example: https://sts.com	m/saml2/3e	e5d0 adfs/ls	42	
		Response URL:				
		Example: https://sts.cont	ioso.com/la	ogout		
				Γ	OK Cancel	

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:

⇒Rule 1

훾 AD FS					
🗌 File Action View Window Help					
← ⇒ 2 📰 🔢 🖬					
📔 AD FS	Relying Par	ty Trusts			
V Service	Display	Name	Enabled Type	ldentifier	Access Control Policy
Attribute Stores	Bitwarde	en ADES Test	Yes WS-	T https://sso.bitwarden.com/saml2	Permit everyone
Certificates					
Claim Descriptions	Edit Cla	im Issuance Policy for Bitwarden ADFS	Test	×	
Device Registration	Issuanc	e Transform Rules			
Endpoints					
Scope Descriptions Web Application Proxy	The f	ollowing transform rules specify the claims th	nat will be sent to the re	lying party.	
Access Control Policies	Ord	ler Rule Name	Issued Claims		
📔 Relying Party Trusts	1	Bitwarden	E-Mail Address.	Name.Giv	
Claims Provider Trusts	2	UPN	UPN		
Application Groups	3	Transform Name ID	Name ID		
	Edit Ru	le - Bitwarden		×	
	You ca	n configure this rule to send the values of L	DAP attributes as claim	s. Select an attribute store from which	
	to extra	ct LDAP attributes. Specify how the attribute	es will map to the outgo	bing claim types that will be issued	
	nom une	,			
		lie name:			
	BitWart	len			
	Rule te	mplate: Send LDAP Attributes as Claims			
	Attribut	e store:			
	Active	Directory		\sim	
	Mappin	g of LDAP attributes to outgoing claim types	c		
		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	~	
		Sumame V	Sumame	~	
		~		~	
	10-	Dula Language			
	View	Rule Language		UK Cancel	

ADFS Rule 1

⇒Rule 2



ADFS Rule 2

⇒Rule 3

翰 AD FS		
훾 File Action View Window Help		
🔶 🤿 🗾 📰 🔢 📷		
AD FS	Relying Party Trusts	
✓ Service	Display Name Enabled Type Identifier	Access Control Policy
Attribute Stores	Bitwarden ADFS Test Yes WS-T https://sso.bitwarden.com/saml2	Permit everyone
Certificates		
Claim Descriptions	Edit Claim Issuance Policy for Bitwarden ADFS Test X	
Device Registration	Issuance Transform Rules	
Scope Descriptions	The following transform rules specify the claims that will be sent to the relying party.	
Web Application Proxy		
Access Control Policies Relying Party Trusts	Order Rule Name Issued Claims	
Claims Provider Trusts	1 Bitwarden E-Mail Address,Name,Giv 2 UPN UPN	
Application Groups	3 Transform Name ID Name ID	
	Edit Rule - Transform Name ID X	
	You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the	
	outgoing claim type and whether the claim value should be mapped to a new claim value.	
	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	
	Pass through all claim values	
	Replace an incoming claim value with a different outgoing claim value	
	Incoming claim value:	
	Outgoing claim value: Browse	
	O Replace incoming e-mail suffix claims with a new e-mail suffix	
	New e-mail suffix:	
	Example: fabrikam.com	
	View Rule Language OK Cancel	
	ADFS Rule 3	

Obtener certificado

En el navegador de archivos de la mano izquierda, seleccione AD FS \rightarrow Servicio \rightarrow 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:

🙀 AD FS						
🖬 File Action View Window Help						
AD FS	Certificates					
Service Attribute Stores Authentication Methods	Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Claim Descriptions	CN=bitwarden Token-decorpting		9/28/2020	9/26/2030		
Device Registration Endpoints	CN=ADFS Encryption - bitw	CN=ADFS Encryption - bit	9/24/2020	9/24/2021		Primary
Scope Descriptions Web Application Proxy	CN=ADFS Signing - bitward	. CN=ADFS Signing - bitwar	9/24/2020	9/24/2021		Primary
Access Control Policies Relying Party Trusts	Gertificate		>	×		
Claims Provider Trusts Application Groups	General Details Certification Show: <all> Field Version Serial number Signature algorithm Signature hash algorithm Signature hash algorithm Valid from Valid to Subject</all>	Value V3 7abebff3b71ed78e42 sha256RSA m sha256 ADFS Signing - bitwar Thursday, September 24 ΔDES Signing - bitwar	24d32a5a dentest 24, 202 24, 202 24, 2021 8 24, 2021 8 Copy to File			

Get token-signing Certificate

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**:

1. 1010			
翰 File Action View Wi	ndow Help		_ & ×
🗢 🄿 🗖 🖬			
AD FS Service Attribute Stores Authentication Me Certificates Claim Descriptions Device Registration Endpoints	AD FS Federation Service Properties X General Organization Events Federation Service display name: Bitwarden ADFS Test Example: Fabrikam Federation Service Federation Service name: bitwarden bitwarden .org	Actions AD FS Add Relying Party Trust Add Claims Provider Trust Add Attribute Store Add Application Group Edit Federation Service Properties	•
Web Application P Access Control Policie Relying Party Trusts Claims Provider Trusts Application Groups	Example: fs fabrikam.com Federation Service identifier: http://bitwarde org/adfs/services/trust Example: http://ts fabrikam.com/adfs/services/trust Web SSO lifetime (minutes): 480 🚖	Edit Published Claims Revoke All Proxies View New Window from Here Refresh	•
	 Enable delegation for service administration Delegate name: Edit Allow Local System account for service administration Allow Local Administrators group for service administration 	P Help	
	OK Cancel Apply		

Get Federation Service Identifier

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 SAML2.0/WS-Federation y generalmente es algo como https://tu-dominio/adfs/ls. Puede obtener el valor exacto de la clave de configuración para SingleSignOnServce en el documento Feder ationMetadata.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 extraneous 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.

(i) 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
Maste	r password (required)
⊗ Input i	s required.
Get ma	ister password hint
	Log in with master password

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!

(i) 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.