ADMIN CONSOLE \rightarrow LOGGA IN MED SSO \rightarrow

ADFS SAML Implementation

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

ADFS SAML Implementation

This article contains **Active Directory Federation Services (AD FS)-specific** help for configuring login with SSO via SAML 2.0. For help configuring login with SSO for another IdP, refer to SAML 2.0 Configuration.

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.

♀ Tip

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

Jownload sample ⊥

Open SSO in the web app

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



U bitwarden

Säker och pålitlig lösenordshanterare med öppen källkod för företag

Open your organization's **Settings** → **Single sign-on** screen:

D bit Warden	Single sign-on 📟	
${\ensuremath{\square}}$ My Organization ${\ensuremath{{\smallsetminus}}}$	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) unique-organization-identifier	
$ agreen arrow ext{Reporting} imes ime$	Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification	
🕅 Billing 🗸 🗸	Member decryption options	
\otimes Settings \wedge	Master password	
Organization info		
Policies	Once authenticated, members will decrypt vault data using a key stored on their device. The single organization policy, SSO required policy, an account recovery administration policy with automatic enrollment will turn on when this option is used.	nd
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	
SCIM provisioning		
	SAML 2.0 metadata URL	
	There are shown in which has been dealed and the first of	

SAML 2.0 configuration

If you haven't already, create a unique **SSO identifier** for your organization and select **SAML** from the the **Type** dropdown. Keep this screen open for easy reference.

You can turn off the **Set a unique SP entity ID** option at this stage if you wish. Doing so will remove your organization ID from your SP entity ID value, however in almost all cases it is recommended to leave this option on.

♀ Tip

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

Create a relying party trust

In the AD FS Server Manager, select Tools \rightarrow AD FS Management \rightarrow Action \rightarrow Add Relying Party Trust. In the wizard, make the following selections:

1. On the Welcome screen, select **Claims Aware**.

2. On the Select Data Source screen, select Enter data about the relying party manually.

3. On the Specify Display Name screen, enter a Bitwarden-specific display name.

4. On the Configure URL screen, select Enable support for SAML 2.0 WebSSO protocol.

• In the **Relying party SAML 2.0 SSO service URL** input, enter the Assertion Consumer Service (ACS) URL. This automaticallygenerated value can be copied from the organization's **Settings** → **Single sign-on** screen and will vary based on your setup.

5. On the **Choose Access Control Policy** screen, select the policy that meets your security standards.

6. On the **Configure Identifiers** screen, add the SP Entity ID as a relying party trust identifier. This automatically-generated value can be copied from the organization's **Settings** → **Single sign-on** screen and will vary based on your setup.

7. On the Choose Access Control Policy screen, select the desired policy (by default, Permit Everyone).

8. On the Ready to Add Trust screen, review your selections.

Advanced options

Once the relying party trust is created, you can further configure its settings by selecting **Relying Party Trusts** from the left-hand file navigator and selecting the correct display name.

Hash algorithm

To change the Secure hash algorithm (by default, SHA-256), navigate to the Advanced tab:

Säker och pålitlig lösenordshanterare med öppen källkod för företag

🙀 AD FS				
🇌 File Action View Window Help				
AD FS	Relying Party Trusts			
V Service	Display Name	Enabled Type	Identifier	Access Control Policy
Authentication Methods	Bitwarden ADFS Test	Yes WS-T	https://sso.bitwarden.com/saml2	Permit everyone
Certificates				
Claim Descriptions				
Device Registration	Bitwarden ADFS Test Properties		~	
Endpoints	Monitoring Identifiers Encryption Signa	ture Accepted Clai	ims	
Scope Descriptions	Organization Endpoints Proxy Endpoints	Notes Advanc	ed	
Web Application Proxy				
Access control Policies	Specify the secure hash algorithm to use for this	relying party trust.		
Relying Party Trusts	Secure hash algorithm: SHA-256		~	
Application Groups				
	ОК	Cancel Apply	/	

Set a Secure Hash Algorithm

Endpoint binding

To change the endpoint **Binding** (by default, POST), navigate to the **Endpoints** tab and select the configured ACS URL:

Säker och pålitlig lösenordshanterare med öppen källkod för företag

D FS Service	Relying Party Trusts		Enabled	Tune	Identifier	Access Central Policy
Attribute Stores Authentication Methods Certificates Claim Descriptions	Bitwarden ADFS Test		Yes	WS-T	https://sso.bitwarden.com/saml2	Permit everyone
Claim Descriptions Device Registration Endpoints Scope Descriptions Web Application Proxy Access Control Policies Relying Party Trusts Claims Provider Trusts Application Groups	Bitwarden ADFS Test Prop Monitoring Identifiers Organization Endpoints Specify the endpoints to use URL SAML Assertion Cons https://sso.bitwarden Add SAML Add WS-Federation	erties Encryption Signatu s Proxy Endpoints e for SAML and WS-Fede Index Bin umer Endpoints com/sa 0 PO Edit Endpoint Endpoint type: SAML Assertion Con Binding: POST V Set the trusted U Index: 0 + Trusted URL: https://sso.bitwarder Example: https://sts.	re Accep Notes aration Passivu ding Def ST Yes sumer RL as default n.com/saml2/ contoso.com	/dgout		

Edit claim issuance rules

Construct claim issuance rules to ensure that the appropriate claims, including **Name ID**, are passed to Bitwarden. The following tabs illustrate a sample ruleset:

⇒Rule 1

File Action View Window Help					
AD FS	Relving 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
Claim Descriptions	Edit Claim Issuance P	olicy for Bitwarden ADFS Test		×	
Device Registration Endpoints	Issuance Transform Ru	les			
Scope Descriptions Web Application Proxy	The following transfo	m rules specify the claims that will be se	nt to the relying p	party.	
Access Control Policies	Order Rule Name	Issue	d Claims		
Claims Provider Trusts	1 Bitwarden	E-Mai	il Address,Name,	,Giv	
Application Groups	3 Transform 1	Name ID Name	• ID		
	Edit Rule - Bitwarden				×
	You can configure this	rule to send the values of LDAP attribute	es as claims. Sele	ect an attribute store from w	which
	to extract LDAP attribut	es. Specify how the attributes will map to	o the outgoing cl	aim types that will be issued	d
	Claim rule name:				
	Bitwarden				
	I Bule template: Send II) AP Attributes as Claims			
	Rule template: Send LL	DAP Attributes as Claims			
	Attribute store:	DAP Attributes as Claims			
	Attribute store:	OAP Attributes as Claims		~	
	Attribute store: Active Directory Mapping of LDAP attrib	DAP Attributes as Claims utes to outgoing claim types:		~	
	Attribute store: Active Directory Mapping of LDAP attribute add more)	DAP Attributes as Claims utes to outgoing claim types: te (Select or type to Outgoing (Claim Type (Sele	ct or type to add more)	
	Attribute store: Active Directory Mapping of LDAP attribu add more) E-Mail-Addres	DAP Attributes as Claims utes to outgoing claim types: te (Select or type to Outgoing (ises V E-Mail Add	Claim Type (Sele ress	ct or type to add more)	~
	Rule template: Send LL Attribute store: Active Directory Mapping of LDAP attribuadd more) E-Mail-Addres Display-Name	DAP Attributes as Claims utes to outgoing claim types: te (Select or type to Outgoing (ses V E-Mail Add Name	Claim Type (Sele ress	ct or type to add more)	~
	Rule template: Send LL Attribute store: Active Directory Mapping of LDAP attribuadd more) E-Mail-Address Display-Name Given-Name 	DAP Attributes as Claims utes to outgoing claim types: te (Select or type to uses V E-Mail Add Given Name Given Name	Claim Type (Sele ress ie	ct or type to add more)	~ ~ ~
	Attribute store: Active Directory Mapping of LDAP attribu- add more) E-Mail-Addres Display-Name Given-Name Surname	DAP Attributes as Claims utes to outgoing claim types: te (Select or type to Outgoing (uses V E-Mail Addu Sea V Rame Given Nam V Sumame	Claim Type (Sele ress e	ct or type to add more)	> > >

ADFS Rule 1

Säker och pålitlig lösenordshanterare med öppen källkod för företag

⇒Rule 2

翰 AD FS				
훾 File Action View Window Help				
🔶 🔿 🗾 🛛 🖬				
📫 AD FS	Relying Party Trusts			
✓	Display Name	Enabled Type	Identifier	Access Control Policy
Attribute Stores	Display Name	Enabled Type	https://www.htwarden.com/com/2	Access Control Folicy
Authentication Methods	bitwarden ADFS Test	1es	https://sso.bitwarden.com/samiz	remii everyone
Certificates	Edit Claim Issuance Policy for Bitward	len ADES Test	×	
Device Registration	Eart claim issuance roney for bitware	ACT ADIO TOSC	~	
Endpoints	Issuance Transform Rules			
Scope Descriptions	The following transform rules specify th	e claims that will be sent to the relyin	ig party.	
Web Application Proxy				
Access Control Policies	Order Rule Name	Issued Claims		
Relying Party Trusts	1 Bitwarden	E-Mail Address,Nar	ne,Giv	
Application Groups	2 UPN	UPN		
	3 Iransform Name ID	Name ID		
	Edit Rule - UPN		×	
	You can configure this rule to send the va	alues of LDAP attributes as claims. S	elect an attribute store from which	
	to extract LDAP attributes. Specify how the	he attributes will map to the outgoing	claim types that will be issued	
	Claim rule name:			
	UPN			
	Rule template: Send LDAP Attributes as (Claims		
	Attribute store:			
	Active Directory		\sim	
	Mapping of LDAP attributes to outgoing of	laim tunes:		
	DAR Attribute (Select extract)	to		
	add more)	Outgoing Claim Type (Se	elect or type to add more)	
	User-Principal-Name	V UPN	~	
	•	~	~	
	View Rule Language		OK Cancel	
1 II				
	AD	FS Rule 2		

⇒Rule 3

翰 AD FS							
输 File Action View Window Help							
🗢 🔿 🚈 🖬							
AD FS R	elying Party Trusts						
✓ Service	Display Name		Enabled	Туре	Identifier	Access Control Po	olicy
Attribute Stores	Bitwarden ADFS Test		Yes	WS-T	https://sso.bitwarden.com/s	aml2 Permit everyone	
Certificates					-		
Claim Descriptions	Edit Claim Issuance Polic	y for Bitwarden ADFS Te	st		×		
Device Registration	Issuance Transform Rules						
Scope Descriptions	The following transform n	les specify the claims that	will be cent to	o the reluin	a patru		
📔 Web Application Proxy		lies specify the claims that	Will De Serie to	o the relying	g party.		
Access Control Policies	Order Rule Name		Issued C	laims			
Claims Provider Trusts	1 Bitwarden		E-Mail Ac	ddress,Nam	ie,Giv		
Application Groups	2 UPN 3 Transform Nam	e ID	Name ID)			
	Edit Rule - Transform Nar	me ID				×	
	You can configure this rule	to map an incoming claim	type to an ou	tgoing clai	m type. As an option, you can		
	also map an incoming claim outgoing claim type and wh	n value to an outgoing clain Nether the claim value shou	n value. Spe Ild be mappe	cify the inc d to a new	oming claim type to map to the claim value.		
	Claim rule name:						
	Transform Name ID						
	Rule template: Transform a	n Incoming Claim					
	Incoming claim type:	UPN				~	
	Incoming name ID format:	Unspecified					
	Outgoing claim type:	Name ID				\sim	
	Outgoing name ID format:	Persistent Identifier					
	Pase through all plaim v	24146					
	Replace an incoming cl	aim value with a different of	outgoing clain	n value			
	Incoming claim value:						
	Outgoing claim value:				Browse		
	Replace incoming e-ma	il suffix claims with a new e	-mail suffix				
	New e-mail suffix:						
		Example: fabrikam.com					
	View Rule Language				OK Cancel		
1 II			0				
		ADES Rule	3				

Get certificate

In the left-hand file navigator, select $ADFS \rightarrow Service \rightarrow Certificates$ to open the list of certificates. Select the Token-signing certificate, navigate to its Details tab, and select the Copy to File... button to export the Base-64 encoded token signing certificate:

🙀 AD FS						
File Action View Window Help						
AD FS	Certificates		_			
Attribute Stores	Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Certificates	Service communications — CN=bitwarden		9/28/2020	9/26/2030		
Claim Descriptions Device Registration Endpoints	Token-decrypting	CN=ADFS Encryption - bit	9/24/2020	9/24/2021		Primary
Scope Descriptions	Token-signing 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	Value V3 7abebff3b71ed78e42 sha256RSA m sha256 ADFS Signing - bitwar Thursday, September Friday, September 24 ADFS Signing - bitwar	24d32a5a rdentest r 24, 202 4, 2021 8 rdentest			
			OK]		

Get token-signing Certificate

You will need this certificate during a later step.

Get federation service identifier

In the left-hand file navigator, select **AD FS** and from the right-hand options menu select **Edit Federation Service Properties**. In the Federation Service Properties window, copy the **Federation Service Identifier**:

Säker och pålitlig lösenordshanterare med öppen källkod för företag

Mad FS			- 🗆 X
翰 File Action View Wi	ndow Help		_ <i>8</i> ×
🔶 🔿 🔲 🖬 🚺			,
📑 AD FS	AD FS	Ī	Actions
V Service	Federation Service Properties X		AD FS
 Authentication Me Certificates Claim Descriptions Device Registration Endpoints Scope Descriptions Web Application P Access Control Policie Relying Party Trusts Claims Provider Trusts Application Groups 	General Organization Events Federation Service display name: Bitwarden ADFS Test Example: Fabrikam Federation Service name: bitwarder .org Example: fs fabrikam.com Federation Service identifier: http://bitwarde org/adfs/services/trust Example: http://ts fabrikam.com/adfs/services/trust Web SSO Ifetime (minutes): 480 Enable delegation for service administration Delegate name: Edit Allow Local Allow Local OK Cancel		Add Relying Party Trust Add Claims Provider Trust Add Attribute Store Add Application Group Edit Federation Service Properties Edit Published Claims Revoke All Proxies View New Window from Here Refresh Help

Get Federation Service Identifier

You will need this identifier during a later step.

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 complete configuration.

The Single sign-on screen separates configuration into two sections:

- SAML service provider configuration will determine the format of SAML requests.
- SAML identity provider configuration will determine the format to expect for SAML responses.

Service provider configuration

In the service provider configuration section, configure the following fields:

Field	Description
Name ID Format	Select the Outgoing Name ID Format selected when constructing claims issuance rules (see Rule 3).
Outbound Signing Algorithm	The algorithm Bitwarden will use to sign SAML requests.
Signing Behavior	Whether/when SAML requests will be signed.
Minimum Incoming Signing Algorithm	By default, AD FS will sign with SHA-256. Select SHA-256 from the dropdown unless you have configured AD FS to use different algorithm.
Want Assertions Signed	Whether Bitwarden expects SAML assertions to be signed.
Validate Certificates	Check this box when using trusted and valid certificates from your IdP through a trusted CA. Self- signed certificates may fail unless proper trust chains are configured within the Bitwarden login with SSO docker image.

When you are done with the service provider configuration, **Save** your work.

Identity provider configuration

Identity provider configuration will often require you to refer back to the AD FS Server Manager to retrieve values:

Field	Description
Entity ID	Enter the retrieved Federation Service Identifier. Please note, this may not use HTTPS . This field is case sensitive.
Binding Type	By default, AD FS with use HTTP POST endpoint binding. Select HTTP POST unless you have configured AD FS to use a different method.

Field	Description
Single Sign On Service URL	Enter the SSO Service Endpoint. This value can be constructed in the Service \rightarrow Endpoints tab in AD FS Manager. The endpoint URL is listed as URL Path for SAML2.0/WS-Federation and is usually something like https://your-domain/adfs/ls. You can obtain the exact value from the configuration key for SingleSignOnServce in the FederationMetadata.xml document.
X509 Public Certificate	Paste the downloaded certificate, removingBEGIN CERTIFICATE andEND CERTIFICATE The certificate value is case sensitive, extra spaces, carriage returns, and other extraneous characters will cause certification to fail.
Outbound Signing Algorithm	By default, AD FS will sign with SHA-256. Select SHA-256 from the dropdown unless you have configured AD FS to use different algorithm.
Disable Outbound Logout Requests	Login with SSO currently does not support SLO. This option is planned for future development.
Want Authentication Requests Signed	Whether AD FS expects SAML requests to be signed.
(i) Note	

When completing the X509 certificate, take note of the expiration date. Certificates will have to be renewed in order to prevent any disruptions in service to SSO end users. If a certificate has expired, Admin and Owner accounts will always be able to log in with email address and master password.

When you are done with the identity provider configuration, **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.

U bitwarden

Test the configuration

Once your configuration is complete, test it by navigating to https://vault.bitwarden.com, entering your email address and selecting the **Use single sign-on** button:

Log in to Bitwarden
Email address (required) Remember email
Continue
or
0
& Log in with passkey
B Log in with passkey B Use single sign-on

Log in options screen

Enter the configured organization identifier and select **Log In**. If your implementation is successfully configured, you will 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.