### BEHEERCONSOLE > INLOGGEN MET SSO >

# **ADFS SAML-implementatie**

Weergeven in het Helpcentrum: https://bitwarden.com/help/saml-adfs/

### **ADFS SAML-implementatie**

Dit artikel bevat **Active Directory Federation Services (AD FS)-specifieke** hulp voor het configureren van aanmelding met SSO via SAML 2.0. Raadpleeg SAML 2.0 Configuratie voor hulp bij het configureren van inloggen met SSO voor een andere IdP.

Bij de configuratie wordt tegelijkertijd gewerkt binnen de Bitwarden webapp en de AD FS Server Manager. We raden u aan om beide documenten bij de hand te hebben en de stappen uit te voeren in de volgorde waarin ze zijn beschreven.

#### **⊘** 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 de webapp**

Log in op de Bitwarden web app en open de Admin Console met behulp van de product switcher ():

Password Manager	All vaults			New 🗸	BW BW
🗇 Vaults			Nama	Owner	
🖉 Send			Name	Owner	•
🖏 Tools 🛛 🗸 🗸	Q Search vau	ASIV	Company Credit Card Visa, *4242	My Organiz	÷
æ Reports	✓ All vaults		Personal Login		
Settings	My vault	0 9	myusername	Me	÷
	ga Teams Org : + New organization		Secure Note	Ме	:
	<ul> <li>✓ All items</li> <li>☆ Favorites</li> <li>③ Login</li> <li>□ Card</li> <li>□ Identity</li> <li>□ Secure note</li> </ul>		Shared Login sharedusername	My Organiz	:
Password Manager	<ul> <li>✓ Folders</li> <li>➡ No folder</li> </ul>				
Secrets Manager					
Admin Console	Default colle				
Admin Console	🔟 Trash				
🛱 Toggle Width					

Product switcher

Open het scherm Instellingen → Eenmalige aanmelding van uw organisatie:

<b>D bit</b> warden	Single sign-on III III III III III III III III III I
🖉 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)
<b>≅</b> Reporting	Provide this ID to your members to login with SSO. To bypass this step, set up <b>Domain verification</b>
🖺 Billing	Member decryption options
Settings	Master password
Organization info	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	Type
Import data	
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	i a com a comunicación de la
	SAML 2.0 metadata URL

SAML 2.0 configuratie

Als je dat nog niet hebt gedaan, maak dan een unieke **SSO-identifier** aan voor je organisatie en selecteer **SAML** in het keuzemenu **Type** . Houd dit scherm open voor gemakkelijke referentie.

U kunt de optie **Een unieke SP entiteit ID instellen** in dit stadium uitschakelen als u dat wilt. Als u dit doet, wordt uw organisatie-ID verwijderd uit uw SP entiteit-ID waarde, maar in bijna alle gevallen is het aan te raden om deze optie aan te laten staan.

#### 🖓 Тір

Er zijn alternatieve **ontcijferingsopties voor leden**. Leer hoe u aan de slag kunt met SSO met vertrouwde apparaten of Key Connector.

#### Een vertrouwensrelatie creëren

Selecteer in de AD FS Server Manager Tools  $\rightarrow$  AD FS Management  $\rightarrow$  Action  $\rightarrow$  Add Relying Party Trust. Maak de volgende selecties in de wizard:

1. Selecteer Claims Aware op het welkomstscherm.

- 2. Selecteer in het scherm Gegevensbron selecteren de optie Gegevens over de betalende partij handmatig invoeren.
- 3. Voer in het scherm Displaynaam opgeven een Bitwarden-specifieke displaynaam in.
- 4. Selecteer in het scherm Configure URL de optie Enable support for SAML 2.0 WebSSO protocol.
  - Voer de URL van de Assertion Consumer Service (ACS) in bij de optie Relying party SAML 2.0 SSO service URL. Deze automatisch gegenereerde waarde kan worden gekopieerd vanuit het Instellingen → Enkelvoudige aanmelding scherm van de organisatie en zal variëren afhankelijk van je instelling.
- 5. Selecteer in het scherm Kies toegangscontrolebeleid het beleid dat voldoet aan uw beveiligingsstandaarden.
- 6. Voeg in het scherm **Configure Identifiers** de SP Entity ID toe als vertrouwensidentificatie voor een betrouwbare partij. Deze automatisch gegenereerde waarde kan worden gekopieerd vanuit het **Instellingen** → **Enkelvoudige aanmelding** scherm van de organisatie en zal variëren afhankelijk van je instelling.
- 7. Selecteer in het scherm Toegangsbeheerbeleid kiezen het gewenste beleid (standaard ledereen toestaan).
- 8. Bekijk uw selecties in het scherm Klaar om vertrouwen toe te voegen.

#### **Geavanceerde opties**

Zodra de relying party trust is aangemaakt, kun je de instellingen verder configureren door **Relying Party Trusts** te selecteren in de linker bestandsnavigator en de juiste weergavenaam te selecteren.

#### Hash-algoritme

Om het veilige hash-algoritme (standaard SHA-256) te wijzigen, navigeer je naar het tabblad Geavanceerd:

翰 AD FS					
훾 File Action View Window Help					
🔶 🧼 🙇 📰 🔢 🗊					
AD FS	Relying Party Trusts				
✓ Service	Display Name	Enabled	Туре	Identifier	Access Control Policy
Authentication Methods	Bitwarden ADFS Test	Yes	WS-T	https://sso.bitwarden.com/saml2	Permit everyone
Certificates					
Claim Descriptions	Bitwarden ADFS Test Properties			×	
Endpoints	Monitoring Identifiers Encryption Si	gnature Acce	pted Claims	3	
Scope Descriptions	Organization Endpoints Proxy Endpoin	ts Notes	Advanced		
Access control Policie	Specify the secure hash algorithm to use for t	his relying party tr	ust.		
Relying Party Trusts	Secure bash algorithm			1	
Claims Provider Trasts					
	ОК	Cancel	Apply		

Set a Secure Hash Algorithm

#### **Eindpunt binding**

Om het eindpunt **Binding** (standaard POST) te wijzigen, navigeer naar het tabblad **Eindpunten** en selecteer de geconfigureerde ACS URL:

File Action View Window Help ADDS Service Service AdDES Service Service Authentication Methods Certificates Certificates Compositions Device Registration Enclosed Device Registration Enclosed Claims Provider Trusts Application Groups Service Service Montoing Identifies Cost of Service Claims Provider Trusts Application Groups Claims Provider Trusts Claims Provider Trusts Application Groups Claims Provider Trusts Application Groups Claims Provider Trusts Claims Provider Trusts Relying Party Trusts Edite Endpoints Claims Provider Trusts Relying Party Trusts Claims Provider Trusts Device Registration Groups Device Registration Gr	AD FS						
A C B C C C C C C C C C C C C C C C C C	🏟 File Action View Window Help						
AD FS         AD FS         Athentication Methods         Cardinizates         Chim Descriptions         Weight Application Proxy         Access Control Policy         Permit everyone         Bitwarden ADFS Text         Yeight Application Proxy         Access Control Policy         Parmit everyone         Bitwarden ADFS Text         Yeight Application Proxy         Access Control Policy         Access Control Policy         Provider Trusts         Application Groups	🗢 🔿 📶 🔽 🖬						
Service Envice Daplay Name Enabled Type Methods Methods Certificates Certificates Certificates Compositions Scope Descriptions Scope Descriptions Monitoring Method ADPS Test Yes WS-T https://sso.bitwarden.com/saml2 Pemit everyone Pemit everyone Bitwarden ADPS Test Yes WS-T https://sso.bitwarden.com/saml2 Pemit everyone Bitwarden ADPS Test Yes WS-T Hitps://sso.bitwarden.com/saml2 Pemit everyone Seckly the endpoints Droy Endpoints New Order Tusts Some Party Trusts Application Groups Https://sso.bitwarden.com/saml2/25500	AD FS	Relving Party Trusts					
Attribute Stores       Display Name       Enabled       type       Memtrice       Access Control Pointy         Bewarden ADFS Test       Yes       WS-T	✓ I Service		-		-	11	A
Authentication Methods Contractes Chain Descriptions Device Registration Endpoints Scope Descriptions We Application Proxy Access Control Policies Claims Provider Trusts Claims Provider Trusts Application Groups We Authentication Groups Beiving Paper Status Application Groups Beiving Provider Trusts Application Groups Beiving Paper Status Application Groups Beiving Paper Status Application Groups Beiving Paper Status Claims Provider Trusts Application Groups Beiving Paper Status Beiving Paper Status Claims Provider Trusts Claims Provider Trusts Clai	Attribute Stores	Display Name	E	nabled	lype	Identifier	Access Control Policy
Certificates Com Descriptions Device Registration Endpoints Web Application Proxy Access Control Policies Pelying Party/Trusts Claims Provider Trusts Application Groups Web Application Groups Web Application Groups Web Application Groups Claims Provider Trusts Application Groups Claims Provider Trusts Application Groups Web Application Groups Web Application Groups Claims Provider Trusts Claims Provider Trusts Clai	Authentication Methods	Bitwarden ADFS Test	Ŷ	es	WS-T	https://sso.bitwarden.com/saml2	Permit everyone
Claim Descriptions   Diverse Registration   Scope Descriptions   Web Application Provy   Access Control Policies   Reging Barly Trusts   Claims Provider Trusts   Application Groups   With Add SAML   URL   Standen Consumer Endpoints   URL as default   Index:   Post   Trusted URL:   Reging Barly Trusts   Application Groups   With Add SAML   Integration Consumer Endpoints   Notes:   Add SAML   Integration Consumer Endpoints   Index:   Post   Trusted URL:   Add SAML   Integration Consumer Endpoints   Integration Consumer Endpoints   Index:   Integration Consumer Endpoints   Integration Consumer Endpoints   Index:   Integration Consumer Endpoints   Integration Consumer Endpoints <td>Certificates</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	Certificates						
Endpoints         Scope Descriptions         WebApplication Proxy         Access Control Policies         Relying Party Trusts         Application Groups             Multiplication Groups	Claim Descriptions	Bitwarden ADFS Test Proper	ties		>	×	
Scope Descriptions Web Application Proxy Access Control Policies Relying Party Trusts Claims Provider Trusts Application Groups Web Application Groups URL INC Mathematication Consumer Endpoints Https://soil.btwarden.com/sail.0 POST Post Federation Post Federation Binding: POST Trusted URL as default Index: 0 Edit Endpoint Mets Policy Federation Post Trusted URL as default Index: 0 Edit Endpoint Post Trusted URL as default Index: 0 Edit Endpoint Post Trusted URL as default Index: 0 Edit Endpoint Post Trusted URL as default Index: 0 Edit Endpoint Mets //soil Ditwarden.com/sail/3/8500 42 Example: https://soil.ctics.com/logout CK Cancel	Endpoints	Marketer Hartford	E	0			
Web Application Proxy         Access Control Policies         Reging Party Trusts         Application Groups             Provider Trusts             Application Groups             Provider Trusts             Application Groups             Provider Trusts             Application Groups             Provider Trusts             Application Groups             Provider Trusts             Application Groups             Provider Trusts             Application Groups             Provider Trusts             Application Groups             Provider Trusts             Application Groups             Provider Trusts             Application Groups             Provider Trusts             Application Groups             Provider Trusts            Application	Scope Descriptions	Organization Endpoints	Provy Endpoints	Accepte	ed Claims dvanced	-	
Access Control Policies Relying Party Trusts Claims Provider Trusts Application Groups URL Index Binding Default Re SAML Assertion Consumer Endpoints Edit Endpoint Findpoint type: SAML Assertion Consumer Binding: POST ves SaML Assertion Consumer Binding: POST ves SaML Assertion Consumer SaML Assertion Consumer Binding: POST ves SaML Assertion Consumer Index: © © Trusted URL: Add WS-Federation Edit Endpoint Trusted URL: Example: https://ss.btwarden.com/saml2/3e5d0 42 Example: https://ss.btwarden.com/saml2/3e5d0 Cancel Example: https://ss.btwarden.com/saml2/3e5d0 Cancel	Web Application Proxy		Free CAML and WC Federa	Notes 70			
Relying Party Trusts Claims Provider Trusts Application Groups	Access Control Policies	Specily the endpoints to use i	IOF SAME and WS-redera	uonrassive	protocois.		
Claims provider Trusts Application Groups SAML Assertion Consumer Endpoints https://sso bitwarden.com/sa 0 POST Yes Edit Endpoint type: SAML Assertion Consumer Binding: POST V Set the trusted URL as default Index: 0 2 Evample: https://sso bitwarden.com/saml2/2e5d0 42 Evample: https://sts.contoso.com/adfa/ts Response URL: Evample: https://sts.contoso.com/dogout CML Cancel	Relying Party Trusts	URL	Index Bindin	g Defau	ult Re		
Appineation Groups     https://sso bitwarden.com/sa     Edit Endpoint     Edit Endpoint     Edit Endpoint     Edit Endpoint     Set the trusted URL:     Add SAML     Trusted URL:     Https://sso bitwarden.com/sami2/3e5d0     Edit Endpoint     Edit Endpoint     Colit Endpoint     Edit Endpoint     Colit Endpoint     Edit Endpoint     Colit Endpoint	Claims Provider Trusts	SAML Assertion Consu	mer Endpoints				
Edit Endpoint     Endpoint type:   SAML Assertion Consumer   Binding:   POST   Binding:   POST     Set the trusted URL as default   Index:   Index:   Index:   Integ://sso.bitwarden.com/sami2/3e5d0   42   Example:   Example:   Integ://sts.contoso.com/logout   OK   Cancel		https://sso.bitwarden.co	om/sa 0 POST	Yes			
Edit Endpoint × Endpoint type: SAML Assertion Consumer Binding: POST POST Trusted URL as default Index: Add SAML Add WS-Federation Trusted URL: Intps://ss.ont/so.com/saml2/3e5d0 42 Example: https://st.contoso.com/adfs/ls Response URL: Example: https://st.contoso.com/logout OK Cancel		r IIII					
Endpoint type:   SAML Assertion Consumer   Binding:   POST   POST   Add SAML   Add SAML   Add WS-Federation   Fitps://sts.contoso.com/adfs/ls   Response URL:   Example: https://sts.contoso.com/logout   OK   Cancel			Edit Endpoint			×	
Induct type:         SAML Assertion Consumer         Binding:         POST         Binding:         POST         Set the trusted URL as default         Index:         Add SAML         Add WS-Federation         Trusted URL:         Integration         Example: https://sts.cont/sos.com/adfs/ls         Response URL:         Example: https://sts.contoso.com/logout         OK         Cancel			Endosint type:				
SAME Assettion Consumer         Binding:         POST         Set the trusted URL as default         Index:       •         Add WS-Federation       •         Trusted URL:       •         https://sts.contoso.com/adfs/ls       42         Example:       •         Example:       •         Intps://sts.contoso.com/adfs/ls       •         Response URL:       •         Example:       •         Cancel       •			CAML Association Commu				
Binding: POST Set the trusted URL as default Index: Add SAML Add WS-Federation Add WS-Federation Fittps://sso.bitwarden.com/sami2/3e5d0 42 Example: https://sts.contoso.com/adfs/ls Response URL: Example: https://sts.contoso.com/logout OK Cancel			SAML Assertion Consu	mer		~	
POST   Set the trusted URL as default Index: 0 : Trusted URL: Add WS-Federation Trusted URL: https://sts.contoso.com/adfs/ls Response URL: Example: https://sts.contoso.com/logout OK Cancel			Binding:				
Image: Set the trusted URL as default         Add SAML         Add WS-Federation         Index:         Image: Trusted URL:         Intps://sso.bitwarden.com/saml2/3e5d0         Example: https://sts.contoso.com/adfs/ls         Response URL:         Image: Example: https://sts.contoso.com/logout         Image: Definition         Image: Definin         Image: Definition<			POST			$\sim$	
Add SAML   Add WS-Federation     Trusted URL:   https://sts.contoso.com/adfs/ls   Response URL:   Example: https://sts.contoso.com/logout     OK   Cancel				1.6 1			
Add SAML   Add WS-Federation   Index:    Index:      Index:   Index:     Index: <td></td> <td>&lt;</td> <td>Set the trusted URL</td> <td>as default</td> <td></td> <td></td> <td></td>		<	Set the trusted URL	as default			
Add WS-Federation       Trusted URL:         https://sts.contoso.com/saml2/3e5d0       42         Example: https://sts.contoso.com/adfs/ls         Response URL:         Example: https://sts.contoso.com/logout         OK       Cancel		Add SAML	Index: 0				
Add WS-Federation       Interest on L.         https://sts.contoso.com/saml2/3e5d0       42         Example: https://sts.contoso.com/adfs/ls         Response URL:         Example: https://sts.contoso.com/logout         OK       Cancel			Trusted LIRL:				
Example: https://sts.contoso.com/adfs/ls Response URL: Example: https://sts.contoso.com/logout OK Cancel		Add WS-Federation	https://eee.httuppdop.g	am /aaml2/2	- 5-10	42	
Example: https://sts.contoso.com/logout  Example: https://sts.contoso.com/logout  Cancel  Edit Ender sint			Filler (1)	. ,	K A	42	
Response URL:         Example: https://sts.contoso.com/logout         OK         Cancel			Example: https://sts.co	ntoso.com/a	acts/is		
Example: https://sts.contoso.com/logout			Response URL:				
Example: https://sts.contoso.com/logout OK Cancel							
OK Cancel			Example: https://sts.co	ntoso.com/lo	ogout		
OK Cancel					_		
						OK Cancel	
Edit Endraint							
			Edit Endpoint				

#### Regels voor claimafgifte bewerken

Stel regels op voor de uitgifte van claims om ervoor te zorgen dat de juiste claims, inclusief **naam-ID**, worden doorgegeven aan Bitwarden. De volgende tabs illustreren een voorbeeld van een regelset:

#### ⇒Rule 1

훾 AD FS					
🗌 File Action View Window Help					
🗢 🄿 📶 🔟 🖬					
📔 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

🙀 AD FS		
훾 File Action View Window Help		
🔶 🧼 🖄 📰 🛛 🖬		
AD FS	Relying Party Trusts	
✓ Service	Display Name Fnabled 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	
Endpoints	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 Relving Party Trusts	Order Rule Name Issued Claims	
Claims Provider Trusts	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:	
	Iranstom Name ID	
	Rule template: Transform an Incoming Claim	
	Incoming claim type: UPN ~	
	Incoming name ID format:	
	Outgoing claim type: Name ID V	
	Outgoing name ID format: Persistent Identifier	
	Pass through all claim values     Data and a state of the state o	
	Replace an incoming claim value with a different outgoing claim value	
	Outgoing claim value: Browse	
	Replace incoming e-mail suffix claims with a new e-mail suffix	
	New e-mail suffix:	
	Example: fabrikam.com	
	View Bula Language	
	View Rule Language	
	ADFS Rule 3	

#### Certificaat krijgen

Selecteer in de linker bestandsnavigator AD FS  $\rightarrow$  Service  $\rightarrow$  Certificaten om de lijst met certificaten te openen. Selecteer het tokenondertekeningscertificaat, navigeer naar het tabblad Details en selecteer de knop Kopieer naar bestand... om het Base-64 gecodeerde tokenondertekeningscertificaat te exporteren:

AD FS						
File Action View Window Help						
AD FS	Certificates					
Attribute Stores	Subject	Issuer	Effective Date	Expiration Date	Status	Primary
<ul> <li>Authentication Methods</li> <li>Certificates</li> <li>Claim Descriptions</li> </ul>	Service communications		9/28/2020	9/26/2030		
Device Registration	CN=ADFS Encryption - bitw	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
<ul> <li>Access Control Policies</li> <li>Relying Party Trusts</li> <li>Claims Provider Trusts</li> <li>Application Groups</li> </ul>	General Details Certification	on Path	>	<	1	
	Show: <all> Field Version Signature algorithm Signature hash algorithm Valid from Valid to Subject</all>	Value V3 7abebff3b71ed78e42 sha256RSA m sha256 ADFS Signing - bitwar Thursday, September Friday, September 24 ADFS Signing - bitwar	Add32a5a dentest t, 2021 8 dentest			

Get token-signing Certificate

Dit certificaat heb je later nodig.

#### Identificatiecode federatieservice ophalen

Selecteer in de linker bestandsnavigator **AD FS** en selecteer in het rechter optiemenu **Edit Federation Service Properties**. Kopieer de **Federation Service Identifier** in het venster Federation Service Properties:

AD 13			
翰 File Action View Window Help			_ 8 ×
AD FS Attribute Stores Attribute Stores Authentication Me Certificates Claim Descriptions Scope Descriptions Web Application P Access Control Policie Relying Party Trusts Claims Provider Trusts Claims Provider Trusts Claims Provider Trusts	ces/trust	Actions         AD FS         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	
Application Groups  Example: http://fs.fabrik.am.com/adfs/servic Web SSO lifetime (minutes): 480 • C Enable delegation for service administrat Delegate name: Allow Local System account for service a Allow Local Administrators group for service Allow Local Administrators group for service	es/trust on Edit administration ce administration OK Cancel Apply	New Window from Here   Refresh     Help	

Get Federation Service Identifier

U hebt deze identificatiecode later nodig.

#### Terug naar de webapp

Op dit punt heb je alles geconfigureerd wat je nodig hebt binnen de context van de AD FS Server Manager. Ga terug naar de Bitwarden web app om de configuratie te voltooien.

Het Single sign-on scherm verdeelt de configuratie in twee secties:

- De configuratie van de SAML-serviceprovider bepaalt het formaat van SAML-verzoeken.
- De configuratie van de SAML identiteitsprovider bepaalt het formaat dat wordt verwacht voor SAML antwoorden.

#### **Configuratie serviceprovider**

Configureer de volgende velden in het gedeelte Serviceproviderconfiguratie:

Veld	Beschrijving
Naam ID Formaat	Selecteer het <b>uitgaande naam-ID-formaat</b> dat is geselecteerd bij het samenstellen van de claimafgifteregels (zie <b>Regel 3</b> ).
Algoritme voor uitgaande ondertekening	Het algoritme dat Bitwarden gebruikt om SAML-verzoeken te ondertekenen.
Ondertekengedrag	Of/wanneer SAML verzoeken ondertekend zullen worden.
Algoritme voor minimale inkomende ondertekening	Standaard ondertekent AD FS met SHA-256. Selecteer <b>SHA-256</b> in de vervolgkeuzelijst tenzij u AD FS hebt geconfigureerd om een ander algoritme te gebruiken.
Ondertekende beweringen	Of Bitwarden verwacht dat SAML-asserties worden ondertekend.
Certificaten valideren	Vink dit vakje aan bij gebruik van vertrouwde en geldige certificaten van je IdP via een vertrouwde CA. Zelfondertekende certificaten kunnen mislukken tenzij de juiste vertrouwensketens zijn geconfigureerd in het Bitwarden login met SSO docker image.

Als je klaar bent met de configuratie van de serviceprovider, sla je je werk **op**.

#### Configuratie identiteitsprovider

Bij het configureren van de identiteitsprovider moet je vaak teruggaan naar de AD FS Server Manager om waarden op te halen:

Veld	Beschrijving
Entiteit ID	Voer de opgehaalde Federation Service Identifier in. Let op, dit <b>mag niet via HTTPS</b> . Dit veld is hoofdlettergevoelig.
Type binding	Standaard gebruikt AD FS HTTP POST endpoint binding. Selecteer <b>HTTP POST</b> tenzij je AD FS hebt geconfigureerd om een andere methode te gebruiken.

Veld	Beschrijving
URL voor service voor eenmalige aanmelding	Voer het eindpunt van de SSO-service in. Deze waarde kan worden geconstrueerd in de <b>Service</b> → Endpoints tab in AD FS Manager. De URL van het eindpunt staat vermeld als <b>URL Path voor</b> SAML2.0/WS-Federation en is meestal zoiets als https://your-domain/adfs/ls. Je kunt de exacte waarde vinden in de configuratiesleutel voor SingleSignOnServce in het FederationMe tadata.xml document.
X509 publiek certificaat	Plak het gedownloade certificaat, verwijderBEGIN CERTIFICAAT enEND CERTIFICAAT De waarde van het certificaat is hoofdlettergevoelig, extra spaties, carriage returns en andere vreemde tekens zorgen <b>ervoor dat de certificering mislukt</b> .
Algoritme voor uitgaande ondertekening	Standaard ondertekent AD FS met SHA-256. Selecteer <b>SHA-256</b> in de vervolgkeuzelijst tenzij u AD FS hebt geconfigureerd om een ander algoritme te gebruiken.
Uitgaande afmeldverzoeken uitschakelen	Inloggen met SSO ondersteunt momenteel <b>geen</b> SLO. Deze optie is gepland voor toekomstige ontwikkeling.
Authenticatieverzoeken ondertekend willen hebben	Of AD FS verwacht dat SAML verzoeken worden ondertekend.

#### (i) Note

Let bij het invullen van het X509-certificaat op de vervaldatum. Certificaten zullen vernieuwd moeten worden om onderbrekingen in de dienstverlening aan SSO eindgebruikers te voorkomen. Als een certificaat is verlopen, kunnen de accounts Admin en Eigenaar altijd inloggen met e-mailadres en hoofdwachtwoord.

Sla uw werk **op** wanneer u klaar bent met de configuratie van de identity provider.

#### **∂** Tip

Je kunt gebruikers verplichten om in te loggen met SSO door het authenticatiebeleid voor eenmalige aanmelding te activeren. Let op, hiervoor moet ook het beleid voor één organisatie worden geactiveerd. Meer informatie.

#### De configuratie testen

Zodra je configuratie voltooid is, kun je deze testen door te navigeren naar https://vault.bitwarden.com, je e-mailadres in te voeren, **Doorgaan** te selecteren en de knop **Enterprise Single-On** te selecteren:

	Log in
Maste	r password (required)
⊗ Input is Get ma	required. ster password hint
	Log in with master password
$\square$	🖶 Enterprise single sign-on
Logging i	n as myemailaddress@bitwarden.com

Enterprise single sign on en hoofdwachtwoord

Voer de geconfigureerde organisatie-ID in en selecteer **Aanmelden**. Als uw implementatie succesvol is geconfigureerd, wordt u doorgestuurd naar het AD FS SSO inlogscherm. Nadat u zich hebt geverifieerd met uw AD FS-gegevens, voert u uw Bitwarden-hoofdwachtwoord in om uw kluis te ontsleutelen!

#### (i) Note

Bitwarden ondersteunt geen ongevraagde antwoorden, dus inloggen vanuit je IdP zal resulteren in een foutmelding. De SSOaanmeldingsstroom moet worden geïnitieerd vanuit Bitwarden.