CONSOLE ADMIN > IDENTIFIEZ-VOUS AVEC SSO >

# Implémentation de SAML ADFS

Afficher dans le centre d'aide: https://bitwarden.com/help/saml-adfs/

### Implémentation de SAML ADFS

Cet article contient de l'aide **spécifique aux Services de Fédération Active Directory (AD FS)** pour configurer l'identifiant avec SSO via SAML 2.0. Pour obtenir de l'aide pour configurer l'identifiant avec SSO pour un autre IdP, reportez-vous à Configuration SAML 2.0.

La configuration implique de travailler simultanément au sein de l'application web Bitwarden et du Gestionnaire de serveur AD FS. Au fur et à mesure que vous avancez, nous vous recommandons d'avoir les deux à portée de main et de compléter les étapes dans l'ordre où elles sont documentées.

#### 🖓 Tip

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

Jownload sample ⊥

### **Ouvrez SSO dans l'application web**

Connectez-vous à l'application web Bitwarden et ouvrez la console Admin en utilisant le sélecteur de produit (ﷺ):

Password Manager	All vaults			New 🗸	BW
🗇 Vaults		_ •"	Norma		
🖉 Send			Name	Owner	:
$\ll$ Tools $\sim$	Q Search vau	VISA	Company Credit Card Visa, *4242	My Organiz	:
æ Reports	✓ All vaults		Personal Login		
🕸 Settings 🛛 🗸 🗸	My vault		myusername	Ме	:
	+ New organization		Secure Note	Ме	:
	<ul> <li>✓ All items</li> <li>☆ Favorites</li> <li>④ Login</li> <li>□ Card</li> <li>☑ Identity</li> </ul>		Shared Login sharedusername	My Organiz	:
<ul> <li>Password Manager</li> <li>Secrets Manager</li> <li> <i>B</i> Admin Console <sup>™</sup> Toggle Width         </li> </ul>	<ul> <li>Secure note</li> <li>Folders</li> <li>No folder</li> <li>Collections</li> <li>Default colle</li> <li>Default colle</li> <li>Trash</li> </ul>				
SUCTOBBIE WILLIN					

commutateur-de-produit

#### Ouvrez l'écran **Paramètres** → **Connexion unique** de votre organisation :

<b>D bit</b> warden	Single sign-on 🗰 🕒
🖉 My Organization	Use the <b>require single sign-on authentication policy</b> to require all members to log in with SSO.
Collections	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)
➡ Reporting	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	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.
Policies	
Two-step login	
Import data	SAME 2.0
Export vault	
Domain verification	SAML service provider configuration
Single sign-on	Set a unique SP entity ID
Device approvals	C SP entity ID
SCIM provisioning	
	C SAML 2.0 metadata URL

Configuration SAML 2.0

Si vous ne l'avez pas déjà fait, créez un **identifiant SSO** unique pour votre organisation et sélectionnez **SAML** dans le menu déroulant **Saisir**. Gardez cet écran ouvert pour une référence facile.

Vous pouvez désactiver l'option **Définir un ID d'entité SP unique** à ce stade si vous le souhaitez. En faisant cela, votre identifiant d'organisation sera supprimé de la valeur de votre identifiant d'entité SP, cependant dans presque tous les cas, il est recommandé de laisser cette option activée.

#### **∏ Tip**

Il existe des options alternatives de **décryptage des membres**. Apprenez comment commencer à utiliser SSO avec des appareils de confiance ou Key Connector.

### Créer une relation de confiance avec une partie dépendante

Dans le Gestionnaire de serveur AD FS, sélectionnez **Outils**  $\rightarrow$  **Gestion AD FS**  $\rightarrow$  **Action**  $\rightarrow$  **Ajouter une relation de confiance de partie de confiance**. Dans l'assistant, faites les sélections suivantes :

1. Sur l'écran d'accueil, sélectionnez Conscient des Réclamations.

2. Sur l'écran Sélectionner la source de données, sélectionnez Entrez les données concernant la partie dépendante manuellement.

3. Sur l'écran Spécifier le nom d'affichage, entrez un nom d'affichage spécifique à Bitwarden.

4. Sur l'écran Configurer l'URL, sélectionnez Activer le support pour le protocole WebSSO SAML 2.0.

 Dans le champ URL du service SSO SAML 2.0 de la partie de confiance, entrez l'URL du Service de Consommation d'Assertion (ACS). Cette valeur générée automatiquement peut être copiée à partir de l'écran Paramètres → Connexion unique de l'organisation et variera en fonction de votre configuration.

5. Sur l'écran Choisir la politique de contrôle d'accès, sélectionnez la politique de sécurité qui répond à vos normes de sécurité.

6. Sur l'écran **Configurer les identifiants**, ajoutez l'ID de l'entité SP en tant qu'identifiant de confiance de la partie de confiance. Cette valeur générée automatiquement peut être copiée à partir de l'écran **Paramètres** → **Connexion unique** de l'organisation et variera en fonction de votre configuration.

7. Sur l'écran Choisir la politique de contrôle d'accès, sélectionnez la politique souhaitée (par défaut, Autoriser tout le monde).

8. Sur l'écran Prêt à Ajouter Confiance, vérifiez vos sélections.

#### **Options avancées**

Une fois que la confiance de la partie dépendante est créée, vous pouvez configurer davantage ses paramètres en sélectionnant **Confiances de la partie dépendante** à partir du navigateur de fichiers à gauche et en sélectionnant le bon nom d'affichage.

#### Algorithme de hachage

Pour changer l'Algorithme de hachage sécurisé (par défaut, SHA-256), naviguez vers l'onglet Avancé :

📬 AD FS					
翰 File Action View Window Help					
🔶 🏟 🙍 📰					
AD FS	Relying Party Trusts				
V Service	Display Name	Enabled	Туре	Identifier	Access Control Policy
Attribute Stores	Bitwarden ADFS Test	Yes	WS-T	https://sso.bitwarden.com/saml2	Permit everyone
Certificates					
Claim Descriptions	Bitwarden ADFS Test Properties			×	
Endpoints	Monitoring Identifiers Encryption Sig	nature Acce	pted Claims		
Scope Descriptions	Organization Endpoints Proxy Endpoint	s Notes	Advanced		
Access control Policies	Specify the secure hash algorithm to use for th	is relying party tr	ust.		
📔 Relying Party Trusts	Secure bash algorithm:			1	
Chine Provider Trasts					
	ОК	Cancel	Apply		
		Carloon	Tabled		

Set a Secure Hash Algorithm

#### Liaison de point d'extrémité

Pour changer le point de terminaison Binding (par défaut, POST), naviguez vers l'Endpoints onglet et sélectionnez l'URL ACS configurée :

AD FS	Relying Party Trusts					
<ul> <li>Service</li> <li>Attribute Stores</li> <li>Authentication Methods</li> <li>Certificates</li> <li>Claim Descriptions</li> <li>Device Registration</li> <li>Endpoints</li> <li>Scope Descriptions</li> <li>Web Application Proxy</li> </ul>	Display Name Bitwarden ADFS Test Bitwarden ADFS Test Prope Monitoring Identifiers Organization Endpoints Specify the endpoints to use	erties Encryption Signa Proxy Endpoints e for SAML and WS-Fer	Enabled Yes ture Acce Notes derationPassiv	Type WS-T pted Claims Advanced e protocols	Identifier https://sso.bitwarden.com/saml2	Access Control Policy Permit everyone
<ul> <li>Relying Party Trusts</li> <li>Claims Provider Trusts</li> <li>Application Groups</li> </ul>	URL SAML Assertion Cons https://sso.bitwarden. < Add SAML Add WS-Federation	Index Bi umer Endpoints com/sa 0 Pr Edit Endpoint Endpoint type: SAML Assertion Co Binding: POST Set the trusted Index: 0 🗼 Trusted URL:	nding Def DST Yes Insumer	fault Re		
		Example: https://st Response URL: Example: https://st	s.contoso.con	n/adfs/ls	OK Cancel	

### Éditer les règles d'émission de revendications

Construisez des règles d'émission de revendications pour garantir que les revendications appropriées, y compris **Name ID**, sont transmises à Bitwarden. Les onglets suivants illustrent un ensemble de règles exemple :

### ⇒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

🙀 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	

#### **Obtenir un certificat**

Dans le navigateur de fichiers à gauche, sélectionnez **AD FS**  $\rightarrow$  **Service**  $\rightarrow$  **Certificats** pour ouvrir la liste des certificats. Sélectionnez le certificat de **signature de jeton**, naviguez jusqu'à son **onglet Détails**, et sélectionnez le bouton **Copier vers le fichier...** pour exporter le certificat de signature de jeton encodé en Base-64 :

翰 AD FS								
輸 File	Action View Window	Help						
<>>	2 🖬 🛿 🖬							
AD FS			Certificates					
V Se	rvice Attribute Stores Authentication Methods		Subject Service communications —	lssuer	Effective Date	Expiration Date	Status	Primary
	Certificates Claim Descriptions		CN=bitwarden Token-decrypting		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		Token-signing CN=ADFS Signing - bitward	CN=ADFS Signing - bitwar	9/24/2020	9/24/2021		Primary
I Ac Re Cli Ap	cess Control Policies lying Party Trusts aims Provider Trusts plication Groups		General Details Certificate	on Path	>	<	•	
AF	plication Groups		Show: <all> Field Version Serial number Signature algorithm Signature hash algorithm Issuer Valid from Valid to Subject</all>	Value V3 7abebff3b71ed78e42 sha256RSA m sha256 ADFS Signing - bitwar Thursday, September Friday, September 24 ADES Signing - bitwar	4d32a5a dentest 24, 202 2021 8 dentect			
					OK			

Get token-signing Certificate

Vous aurez besoin de ce certificat lors d'une étape ultérieure.

#### Obtenez l'identifiant du service de fédération

Dans le navigateur de fichiers à gauche, sélectionnez **AD FS** et dans le menu d'options à droite, sélectionnez **Éditer les propriétés du** service de fédération. Dans la fenêtre des propriétés du service de fédération, copiez l'**Identifiant du Service de Fédération** :

翰 File Action View Window Help	_ <i>8</i> ×
AD FS	Actions
Attribute Stores Authentication Me General Organization Events Federation Service display name: Bitwarden ADFS Test Claim Descriptions Cueice Registration Web Application P Descriptions Cueice Registration Relying Party Trusts Claims Provider Trusts Claims Provider Trusts Claims Provider Trusts Claims Provider Trusts Application Groups Claim Service identifier: Claims Provider Trusts Application Groups Claims Provider Trusts Application Groups Claim Service identifier: Claims Provider Trusts Application Groups Claims Provider Trusts Claims Provi	AU 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 New Window from Here Refresh Help

Get Federation Service Identifier

Vous aurez besoin de cet identifiant lors d'une étape ultérieure.

### Retour à l'application web

À ce stade, vous avez configuré tout ce dont vous avez besoin dans le contexte du Gestionnaire de serveur AD FS. Retournez à l'application web Bitwarden pour terminer la configuration.

L'écran de connexion unique sépare la configuration en deux sections :

- La configuration du fournisseur de services SAML déterminera le format des requêtes SAML.
- La configuration du fournisseur d'identité SAML déterminera le format attendu pour les réponses SAML.

#### Configuration du fournisseur de services

Dans la section de configuration du fournisseur de services, configurez les champs suivants :

Champ	Description
Format de l'identifiant de nom	Sélectionnez le <b>Format d'ID de Nom Sortant</b> choisi lors de la construction des règles d'émission de réclamations (voir <b>Règle 3</b> ).
Algorithme de Signature Sortant	L'algorithme que Bitwarden utilisera pour signer les requêtes SAML.
Comportement de signature	Si/quand les demandes SAML seront signées.
Algorithme de Signature Minimum Entrant	Par défaut, AD FS signera avec SHA-256. Sélectionnez <b>SHA-256</b> dans le menu déroulant à moins que vous n'ayez configuré AD FS pour utiliser un algorithme différent.
Voulez des Assertions Signées	Que Bitwarden s'attend à ce que les assertions SAML soient signées.
Valider les Certificats	Cochez cette case lorsque vous utilisez des certificats fiables et valides de votre IdP via une CA de confiance. Les certificats auto-signés peuvent échouer à moins que des chaînes de confiance appropriées ne soient configurées dans l'image Docker de l'identifiant Bitwarden avec SSO.

Lorsque vous avez terminé avec la configuration du fournisseur de services, **Enregistrez** votre travail.

### Configuration du fournisseur d'Identité

La configuration du fournisseur d'Identité nécessitera souvent que vous vous référiez au Gestionnaire de Serveur AD FS pour récupérer des valeurs :

Champ	Description
ID de l'entité	Entrez l'Identifiant du Service Fédération récupéré. Veuillez noter, cela <b>peut ne pas utiliser HTTPS</b> . Ce champ est sensible à la casse.
Type de Reliure	Par défaut, AD FS utilisera la liaison de point de terminaison HTTP POST. Sélectionnez <b>HTTP POST</b> sauf si vous avez configuré AD FS pour utiliser une méthode différente.

Champ	Description
URL du service de connexion unique	Entrez le point de terminaison du service SSO. Cette valeur peut être construite dans l' <b>Service</b> → <b>Points de terminaison</b> onglet dans le gestionnaire AD FS. L'URL de point de terminaison est répertoriée comme <b>Chemin URL pour SAML2.0/WS-Federation</b> et est généralement quelque chose comme https://votre-domaine/adfs/ls. Vous pouvez obtenir la valeur exacte à partir de la clé de configuration pour SingleSignOnServce dans le document FederationMetadata.xml.
Certificat Public X509	Collez le certificat téléchargé, en supprimantDÉBUT DU CERTIFICAT etFIN DU CERTIFICAT La valeur du certificat est sensible à la casse, les espaces supplémentaires, les retours à la ligne et autres caractères superflus entraîneront l'échec de la certification.
Algorithme de Signature Sortant	Par défaut, AD FS signera avec SHA-256. Sélectionnez <b>SHA-256</b> dans le menu déroulant à moins que vous n'ayez configuré AD FS pour utiliser un algorithme différent.
Désactiver les demandes de déconnexion sortantes	L'identification avec SSO ne prend actuellement <b>pas</b> en charge SLO. Cette option est prévue pour un développement futur.
Voulez des Demandes d'Authentification Signées	Que AD FS s'attend à ce que les demandes SAML soient signées.

### (i) Note

Lors de la complétion du certificat X509, prenez note de la date d'expiration. Les certificats devront être renouvelés afin d'éviter toute interruption de service pour les utilisateurs finaux de SSO. Si un certificat a expiré, les comptes Admin et Propriétaire pourront toujours se connecter avec l'adresse de courriel et le mot de passe principal.

Lorsque vous avez terminé avec la configuration du fournisseur d'identité, Enregistrez votre travail.

### **∂** Tip

Vous pouvez exiger que les utilisateurs se connectent avec SSO en activant la politique d'authentification à connexion unique. Veuillez noter que cela nécessitera également l'activation de la politique de sécurité de l'organisation unique. En savoir plus.

### **Testez la configuration**

Une fois votre configuration terminée, testez-la en vous rendant sur https://vault.bitwarden.com, en entrant votre adresse de courriel, en sélectionnant **Continuer**, et en sélectionnant le bouton **Connexion unique d'Entreprise** :

	Log in
- Master	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

Connexion unique d'entreprise et mot de passe principal

Entrez l'identifiant de l'organisation configuré et sélectionnez **Se connecter**. Si votre mise en œuvre est correctement configurée, vous serez redirigé vers l'écran d'identifiant SSO AD FS. Après vous être authentifié avec vos identifiants AD FS, entrez votre mot de passe principal Bitwarden pour déchiffrer votre coffre !

#### (i) Note

Bitwarden ne prend pas en charge les réponses non sollicitées, donc l'initiation de l'identifiant à partir de votre IdP entraînera une erreur. Le flux d'identifiant SSO doit être initié à partir de Bitwarden.