

管理者コンソール > SSOでログイン >

ADFS SAMLの実装

ヘルプセンターで表示: https://bitwarden.com/help/saml-adfs/

ADFS SAMLの実装

この記事には、SAML 2.0を介したSSOでのログインを設定するためのActive Directory Federation Services (AD FS)専用のヘルプが含まれています。 別のIdPでSSOを使用したログインの設定についてのヘルプは、SAML 2.0設定を参照してください。

設定は、BitwardenウェブアプリとAD FSサーバー管理マネージャーを同時に操作することを含みます。進行するにあたり、 両方をすぐに利用できる状態にして、記録されている順序で手順を完了することをお勧めします。

∂ Tip

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

Jownload sample ⊥

ウェブアプリでSSOを開く

Bitwardenウェブアプリにログインし、製品スイッチャー(謡)を使用して管理者コンソールを開きます。

Password Manager	All vaults			New \sim	BW BW
🗇 Vaults	FILTERS ⑦		Name	Owner	:
🖉 Send					
\ll Tools \sim	Q Search vau	ASIA	Company Credit Card Visa, *4242	My Organiz	:
₩ Reports	✓ All vaults		Provide the state		
🕸 Settings 🛛 🗸 🗸	 △ My vault △ My Organiz : △ Teams Org 		Personal Login myusername	Me	:
	+ New organization		Secure Note	Me	:
	 ✓ All items ☆ Favorites ③ Login □ Card ☑ Identity □ Secure note 	0 0	Shared Login sharedusername	My Organiz	:
 Password Manager Secrets Manager <i>₫</i> Admin Console <i>☆</i> Toggle Width 	 ✓ Folders ➢ No folder ✓ Collections ➢ Default colle ➢ Default colle ☆ Trash 				

製品-スイッチャー

あなたの組織の設定 → シングルサインオン画面を開きます。

D bit 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.
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.
绺 Groups	SSO identifier (required) unique-organization-identifier
≅ Reporting	Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification
Billing	Member decryption options
Settings	Naster 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 required policy with automatic approximate will turn on when this action is used.
Policies	account recovery administration policy with automatic enroliment 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
SCIM provisioning	
	SAML 2.0 metadata URL
	I have not the time is the bit of

SAML 2.0 設定

まだ作成していない場合は、あなたの組織のためのユニークなSSO識別子を作成し、タイプのドロップダウンからSAMLを選択してください。 この画面を開いたままにして、簡単に参照できるようにしてください。

あなたは、この段階で**ユニークなSPエンティティIDを設定する**オプションをオフにすることができます。これを行うと、 組电IDがSPエンティティID値から削除されますが、ほとんどの場合、このオプションをオンにしておくことをお勧めします。

∂ Tip

代替のメンバー復号化オプションがあります。信頼できるデバイスでのSSOの使い方またはキーコネクターの使い方を学びましょう。

信頼関係パーティーを作成します

AD FSサーバーマネージャーで、**ツール → AD FS管理 → アクション → 信頼するパーティーの信頼を追加**を選択します。ウィザードで、 次の選択を行ってください:

1. ウェルカム画面で、クレーム対応を選択してください。

2. データソース選択画面で、依存パーティについてのデータを手動で入力するを選択してください。

3.「表示名を指定」画面で、Bitwarden専用の表示名を入力してください。

4. URL設定画面で、SAML 2.0 WebSSOプロトコルのサポートを有効にするを選択します。

依存パーティSAML 2.0 SSOサービスURLの入力欄に、アサーションコンシューマーサービス(ACS) URLを入力してください。
 この自動生成された値は、組織の設定 → シングルサインオン画面からコピーでき、設定により異なります。

5. アクセス制御ポリシーを選択画面で、あなたのセキュリティ基準を満たすポリシーを選択してください。

6. 識別子の設定画面で、SPエンティティIDを信頼するパーティの識別子として追加します。この自動生成された値は、組織の設定 → シングルサインオン画面からコピーでき、設定により異なります。

7. アクセス制御ポリシーの選択画面で、希望のポリシーを選択します(デフォルトでは、全員に許可)。

8. 信頼を追加する準備ができました画面で、選択した項目を確認してください。

高度なオプション

信頼するパーティの信頼が作成されると、左側のファイルナビゲータから**信頼するパーティの信頼**を選択し、正しい表示名を選択することで、 その設定をさらに構成することができます。

ハッシュアルゴリズム

セキュアハッシュアルゴリズムを変更するには(デフォルトではSHA-256)、詳細タブに移動します。

翰 AD FS				
翰 File Action View Window Help				
🗢 🄿 🚈 📰 🔢 🖬				
 File Action View Window Help 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 Chime Provider Trusts Application Groups 	Relying Party Trusts Display Name Bitwarden ADFS Test Bitwarden ADFS Test Properties Monitoring Identifiers Encryption Sig Organization Endpoints Specify the secure hash algorithm to use for the Secure hash algorithm: SHA-256	Enabled Typ Yes WS nature Accepted C s Notes Adva is relying party trust.	e Identifier S-T https://sso.bitwarden.com/saml2	Access Control Policy Permit everyone
	OK	Cancel	ply	

Set a Secure Hash Algorithm

エンドポイントバインディング

エンドポイント**バインディング**(デフォルトではPOST)を変更するには、**エンドポイント**タブに移動し、設定されたACS URLを選択します:

翰 AD FS						
翰 File Action View Window Help						
🗢 🄿 🙍 📰 🛛 🖬						
🛅 AD FS	elying Party Trusts					
✓ 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 Prope	erties			×	
Endpoints	Monitoring Identifiers	Encryption Signat	ure Acce	pted Claims		
Scope Descriptions	Organization Endpoints	Proxy Endpoints	Notes	Advanced		
Access Control Policies	Specify the endpoints to use	of or SAML and WS-Fed	erationPassiv	e protocols		
Relying Party Trusts	URL	Index Bin	dina Def	fault Re		
Claims Provider Trusts	SAML Assertion Const	umer Endpoints				
	https://sso.bitwarden.e	com/sa 0 PC	ST Yes	3		
		Edit Endpoint			×	
		Eait Enapoint			^	
		Endpoint type:				
		SAML Assertion Cor	isumer		\sim	
		Binding:				
		POST			~	
		Set the trusted U	RL as defaul	t		
		Index: 0				
	Add SAML					
	Add WS-Federation	https://eeo.bitwarde	n com/eaml?	/3e5d0	42	
		Example: https://sts	contoso.com	/adfs/ls	72	
		Response URL				
		Example: https://sts	.contoso.com	n/logout		
				_		
				L	OK Cancel	
		Edit Endpoir	nt			

請求発行ルールの編集

適切なクレーム、**Name ID**を含む、がBitwardenに渡されることを確認するためのクレーム発行ルールを構築します。 次のタブはサンプルのルールセットを示しています:

⇒Rule 1

翰 AD FS 翰 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

sitwarder	n ADFS Test	Yes	WS-T.	https://sso.bitwarde	en.com/saml2	Permit evervone
				intpos / coordinated		, chine of onjoine
Edit Clai	m Issuance Policy for Bitwarden A	ADFS Test		×		
Issuance	e Transform Rules					
The to	liowing transform rules specify the cla	ims that will be sent t	o the relyin	g party.		
Orde	er Rule Name	Issued C	laims			
1	Bitwarden	E-Mail A	ddress,Nam	ne,Giv		
2	UPN	UPN				
3	Transform Name ID	Name IE)			
Edit Rule	e - Bitwarden				×	
You can	configure this rule to send the values	of LDAP attributes a	as claims. S	elect an attribute store	e from which	
from the	rule.	induites will map to in	ie outgoing	claim types that will b	eissued	
Claim nuk	o oomo:					
	e name.					
Bitwarde	en					
Rule tem	nplate: Send LDAP Attributes as Claim	IS				
riche com						
Au d a						
Attribute	store:					
Attribute Active [store: Directory			~		
Attribute Active [Mapping	store: Directory of LDAP attributes to outgoing claim	types:		~		
Attribute Active [Mapping	store: Directory of LDAP attributes to outgoing claim	types:		~		
Attribute Active [Mapping	store: Directory of LDAP attributes to outgoing claim LDAP Attribute (Select or type to add more)	types: Outgoing Cla	im Type (Se		ore)	
Attribute Active [Mapping	store: Directory of LDAP attributes to outgoing claim LDAP Attribute (Select or type to add more) E-Mail-Addresses	types: Outgoing Cla	im Type (Se		ire)	
Attribute Active [Mapping	store: Directory of LDAP attributes to outgoing claim LDAP Attribute (Select or type to add more) E-Mail-Addresses Display-Name	types: Outgoing Cla V E-Mail Addres V Name	im Type (Se s	elect or type to add model	ore) ~ ~	
Attribute Active [Mapping	store: Directory of LDAP attributes to outgoing claim LDAP Attribute (Select or type to add more) E-Mail-Addresses Display-Name Given-Name	types: Outgoing Cla Classical Addres Name Given Name	im Type (Se s	elect or type to add mo	ne) ~ ~ ~	
Attribute Active [Mapping	store: Directory of LDAP attributes to outgoing claim LDAP Attribute (Select or type to add more) E-Mail-Addresses Display-Name Given-Name Sumame	types: Outgoing Cla C E-Mail Addres Name Given Name Given Name Surname	im Type (Se s	elect or type to add mo	ore) ~ ~ ~ ~	
Attribute Active [Mapping	store: Directory of LDAP attributes to outgoing claim LDAP Attribute (Select or type to add more) E-Mail-Addresses Display-Name Given-Name Sumame	types: Outgoing Cla C E-Mail Addres Name Given Name Given Name Sumame	im Type (Se s	elect or type to add mo	vre) ~ ~ ~ ~ ~	
Attribute Active [Mapping	store: Directory of LDAP attributes to outgoing claim LDAP Attribute (Select or type to add more) E-Mail-Addresses Display-Name Given-Name Surname	types: Outgoing Cla C E-Mail Addres Name Given Name Given Name Surname Surname	im Type (Se s	elect or type to add mo	vre) ~ ~ ~ ~ ~	
Attribute Active [Mapping	store: Directory of LDAP attributes to outgoing claim LDAP Attribute (Select or type to add more) E-Mail-Addresses Display-Name Given-Name Sumame	types: Outgoing Cla C E-Mail Addres Name Given Name Given Name Sumame Sumame	im Type (Se s	elect or type to add mo	ne) ~ ~ ~ ~ ~	
Attribute Active [Mapping	store: Directory of LDAP attributes to outgoing claim LDAP Attribute (Select or type to add more) E-Mail-Addresses Display-Name Given-Name Sumame	types: Outgoing Cla C E-Mail Addres Name Given Name Given Name Sumame Sumame	im Type (Se s	elect or type to add mo	ne) ~ ~ ~ ~ ~	
Attribute Active I Mapping	store: Directory of LDAP attributes to outgoing claim LDAP Attribute (Select or type to add more) E-Mail-Addresses Display-Name Given-Name Sumame	types: Outgoing Cla C E-Mail Addres Name Given Name Given Name Sumame Sumame	im Type (Se s	elect or type to add mo	ne) ~ ~ ~ ~ ~	
Attribute Active I Mapping	store: Directory of LDAP attributes to outgoing claim LDAP Attribute (Select or type to add more) E-Mail-Addresses Display-Name Given-Name Sumame	types: Outgoing Cla C E-Mail Addres Name Given Name Given Name Surname	im Type (Se	elect or type to add mo	ne) ~ ~ ~ ~ ~	
Attribute Active I Mapping	store: Directory of LDAP attributes to outgoing claim LDAP Attribute (Select or type to add more) E-Mail-Addresses Display-Name Given-Name Surname	types: Outgoing Cla Certail Addres Name Given Name Given Name Surname Surname	im Type (Se s	elect or type to add mo	ne) ~ ~ ~ ~ ~	
Attribute Active I Mapping	store: Directory of LDAP attributes to outgoing claim LDAP Attribute (Select or type to add more) E-Mail-Addresses Display-Name Given-Name Surname	types: Outgoing Cla C E-Mail Addres Name Given Name Surname Surname	im Type (Se	elect or type to add mo	ne) ~ ~ ~ ~ ~	
Attribute Active I Mapping	store: Directory of LDAP attributes to outgoing claim LDAP Attribute (Select or type to add more) E-Mail-Addresses Display-Name Given-Name Surname	types: Outgoing Cla E-Mail Addres Name Given Name Surname Surname	im Type (Se	elect or type to add mo	ne) ~ ~ ~ ~ ~	
Attribute Active I Mapping	store: Directory of LDAP attributes to outgoing claim LDAP Attribute (Select or type to add more) E-Mail-Addresses Display-Name Given-Name Surname	types: Outgoing Cla E-Mail Addres Name Given Name Surname Surname	im Type (Se s	elect or type to add mo	ne) ~ ~ ~ ~ ~	
Attribute Active I Mapping	store: Directory of LDAP attributes to outgoing claim LDAP Attribute (Select or type to add more) E-Mail-Addresses Display-Name Given-Name Surname	types: Outgoing Cla E-Mail Addres Name Given Name Surname Surname	im Type (Se	elect or type to add mo	ne) ~ ~ ~ ~	

ADFS Rule 1

⇒Rule 2

翰 AD FS 翰 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

Bitwarden	me	Enabled	Туре	Identifier	Access Control Policy
Sitteratori	ADFS Test	Yes	WS-T	https://sso.bitwarden.com/saml2	Permit everyone
Edit Clain	n Issuance Policy for Bitwarden A	DFS Test		×	
Issuance	Transform Rules				
The foll	owing transform rules specify the clai	ms that will be sent t	to the relyin	g party.	
Order	Rule Name	Issued C	laims		
1	Bitwarden	E-Mail A	ddress,Nan	ne,Giv	
2	UPN	UPN			
3	Transform Name ID	Name IE)		
Edit Rule	- UPN			×	
You can o	configure this rule to send the values	of LDAP attributes a	as claims. S	elect an attribute store from which	
from the n	lle.	noutes will map to th	ie outgoing	ciain types that will be issued	
Claim rule	name:				
UPN					
Active Di	rectory of LDAP attributes to outgoing claim t	VDes:		~	
	LDAP Attribute (Select or type to add more)	Outgoing Clai	im Type (Se	elect or type to add more)	
•	User-Principal-Name	✓ UPN		~	
*		~		~	
			_		

ADFS Rule 2

⇒Rule 3

🙀 AD FS					
🗌 File Action View Window Help					
🔶 🏟 🔁 📰 🚺					
AD FS	Relying Party Trusts				
Service Attribute Storer	Display Name	Enabled	Type Ide	entifier	Access Control Policy
Authentication Methods	Bitwarden ADFS Test	Yes	WS-T htt	tps://sso.bitwarden.com/saml2	Permit everyone
Certificates				~	
Claim Descriptions	Edit Claim Issuance Policy	for Bitwarden ADFS Test		×	
Endpoints	Issuance Transform Rules				
Scope Descriptions	The following transform rule	es specify the claims that will be sent to	the relying par	rty.	
Web Application Proxy	Orden Bide Name	law and Cl			
Relying Party Trusts	1 Bitwarden	E-Mail Ad	aims Idress Name Giv	iv	
Claims Provider Trusts	2 UPN	UPN	aress, Name, ar		
Application Groups	3 Transform Name	ID Name ID			
	Edit Rule - Transform Nam	e ID		×	
	You can configure this sub t	a man an incoming claim tunc to an ou	tasing claim tur	A an artice you are	
	also map an incoming claim	value to an outgoing claim value. Spec	cify the incoming	ig claim type to map to the	
	Outgoing claim type and whe	ther the claim value should be mapped	d to a new clain	m value.	
	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 val				
	Replace an incoming cla	im value with a different outgoing claim	value		
	Incoming 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			
	Mary Dide Language			OK Carrel	
	view Rule Language			Cancel	
		ADFS Rule 3			

証明書を取得する

左側のファイルナビゲーターで、AD FS → **サービス → 証明書**を選択して、証明書のリストを開きます。**トークン署名**証明書を選択し、 その**詳細**タブに移動し、**ファイルにコピー…**ボタンを選択してBase-64エンコードされたトークン署名証明書をエクスポートします。

🙀 AD FS						
훾 File Action View Window Help						
🔶 🔿 🔝 🔽						
AD FS	Certificates					
✓ Service ☐ Attribute Stores	Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Authentication Methods Certificates Claim Descriptions	CN=bitwarden		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 Claims Provider Trusts	General Details Certificate	on Path)	<	•	
Application Groups	General Details Certification	Value V3 7abebff3b71ed78e42 sha256RSA m sha256 ADFS Signing - bitwar Thursday, September Friday, September 24 ADES Signing - bitwar	24d32a5a dentest 24, 202 b, 2021 8 dentest			
				-		

Get token-signing Certificate

この証明書は後のステップで必要になります。

連盟サービス識別子を取得します

左側のファイルナビゲーターで、AD FSを選択し、右側のオプションメニューから連盟サービスのプロパティを編集を選択します。 連盟サービスプロパティウィンドウで、連盟サービス識別子をコピーします。

🏟 AD FS			— C		\times
翰 File Action View W	lindow Help			-	8 ×
🗢 🔿 📊 🔽 🖬					
🚰 AD FS	AD FS		Actions		
V Service	Federation Service Properties X	FI	AD FS		
Attribute Stores Authentication Me Certificates 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 Federation Service name: bitwardel org Example: Is fabrikam.com Federation Service identifier: http://bitwarde org/adfs/services/trust Example: http://ts tabrikam.com/adfs/services/trust Web SSO lifetime (minutes): 480 🛫 Enable delegation for service administration Delegate name:		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 Plep		

Get Federation Service Identifier

この識別子は後のステップで必要になります。

ウェブアプリに戻る

この時点で、AD FSサーバー管理者のコンテキスト内で必要なすべてを設定しました。設定を完了するためにBitwardenウェブアプリに戻ってください。

シングルサインオン画面は、設定を二つのセクションに分けています:

- SAML サービス プロバイダーの構成によって、 SAML リクエストの形式が決まります。
- SAML IDプロバイダーの設定は、SAMLのレスポンスで期待する形式を決定します。

サービスプロバイダーの設定

サービスプロバイダー設定セクションで、以下のフィールドを設定します:

フィールド	説明
名前ID形式	送信名ID形式 を選択します。これは請求発行ルールを構築する際に選択されます(ルール3 を参照)。
アウトバウンド署名アルゴリズム	BitwardenがSAMLリクエストに署名するために使用するアルゴリズム。
署名行動	SAMLリクエストが署名されるかどうか/いつ署名されるか。
最小入力署名アルゴリズム	デフォルトでは、AD FSはSHA-256で署名します。ドロップダウンから SHA-256 を選択してください。 ただし、異なるアルゴリズムを使用するようにAD FSを設定している場合は除きます。
署名されたアサーションが欲しい	BitwardenがSAMLアサーションに署名されることを期待しているかどうか。
証明書を検証する	あなたのldPから信頼できるCAを通じて信頼性と有効性のある証明書を使用するときは、 このボックスをチェックしてください。自己署名証明書は、 適切な信頼チェーンがBitwardenログインのSSO dockerイメージ内に設定されていない限り、 失敗する可能性があります。

サービスプロバイダーの設定が完了したら、作業を保存してください。

IDプロバイダーの設定

IDプロバイダーの設定では、値を取得するためにAD FSサーバーマネージャーを参照する必要がよくあります。

フィールド	説明
エンティティID	取得したフェデレーションサービス識別子を入力してください。メモしてください、 これは HTTPSを使用しないかもしれません 。 このフィールドは大文字と小文字を区別します。
バインディングタイプ	デフォルトでは、AD FSはHTTP POSTエンドポイントバインディングを使用します。HTTP POST を選択してください、異なる方法を使用するようにAD FSを設定している場合を除きます。
シングルサインオンサービスURL	SSOサービスエンドポイントを入力してください。この値は、 サービス → エンドポイントタブでAD FSマネージャーで管理できます。 エンドポイントURLは SAML2.0/WS-FederationのURLパス として記載されており、 通常はhttps://your-ドメイン/adfs/lsのようなものです。FederationMetadata.

フィールド	説明
	<mark>xml</mark> ドキュメントのSingleSignOnServceの設定キーから正確な値を取得することができます。
	ダウンロードした証明書を貼り付け、削除してください。
	BEGIN CERTIFICATE
X509公開証明書	そして
	証明書終了
	証明書の値は大文字と小文字を区別し、余分なスペース、キャリッジリターン、 およびその他の余分な文字 は認証に失敗する原因となります 。
アウトバウンド署名アルゴリズム	デフォルトでは、AD FSはSHA-256で署名します。ドロップダウンから SHA- 256 を選択してください。ただし、異なるアルゴリズムを使用するようにAD FSを設定している場合は除きます。
アウトバウンドログアウトリクエストを無効にする	現在、SSOでの ログインは SLOをサポートしていません。 このオプションは将来の開発のために計画されています。
認証リクエストに署名が必要です	AD FSがSAMLリクエストの署名を期待するかどうか。
① Note	
X509証明書を完成させるとき、有効期限の日付をメモ	Eしてください。SSOエンドユーザーへのサービスの中断を防ぐために、

証明書を更新する必要があります。証明書が期限切れになった場合でも、 管理者と所有者のアカウントは常にメールアドレスとマスターパスワードでログインできます。

IDプロバイダーの設定が完了したら、保存してください。

⊘ Tip

シングルサインオン認証ポリシーを有効にすることで、ユーザーにSSOでログインすることを要求することができます。メモしてください、 これは単一の組織ポリシーも同時に活性化する必要があります。もっと学ぶ

設定をテストする

設定が完了したら、https://vault.bitwarden.comに移動してテストを行います。メールアドレスを入力し、**続行**を選択し、 エンタープライズシングルオンボタンを選択します:

Log in
Master password (required) Solution is required. Get master password hint
Log in with master password
🖻 Enterprise single sign-on
Logging in as myemailaddress@bitwarden.com Not you?

エンタープライズシングルサインオンとマスターパスワード

設定された組織識別子を入力し、**ログイン**を選択してください。あなたの実装が正常に設定されている場合、AD FS SSOログイン画面にリダイレクトされます。AD FSの資格情報で認証した後、Bitwardenのマスターパスワードを入力して保管庫を復号化してください!

(i) Note

Bitwardenは勝手なレスポンスをサポートしていませんので、あなたのIdPからログインを開始するとエラーが発生します。 SSOログインフローはBitwardenから開始されなければなりません。