

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.

[Download 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 (製品アイコン) を使用して管理者コンソールを開きます。

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login sharedusername	My Organiz...	⋮

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。

bitwarden
Admin Console

My Organization

Collections

Members

Groups

Reporting

Billing

Settings

Organization info

Policies

Two-step login

Import data

Export vault

Domain verification

Single sign-on

Device approvals

SCIM provisioning

Single sign-on



Use the [require single sign-on authentication policy](#) to require all members to log in with SSO.

Allow SSO authentication

Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.

SSO identifier (required)

unique-organization-identifier

Provide this ID to your members to login with SSO. To bypass this step, set up [Domain verification](#)

Member decryption options

Master password

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.

Type

SAML 2.0

SAML service provider configuration

Set a unique SP entity ID

Generate an identifier that is unique to your organization

SP entity ID

[Redacted SP entity ID] [Copy]

SAML 2.0 metadata URL

[Redacted SAML 2.0 metadata URL] [Copy] [Refresh]

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、組電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。

The screenshot shows the AD FS console interface. On the left, the 'Relying Party Trusts' folder is selected. The main pane displays a table of Relying Party Trusts:

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

A 'Bitwarden ADFS Test Properties' dialog box is open, showing the 'Advanced' tab. The 'Secure hash algorithm' dropdown menu is set to 'SHA-256'.

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：

The screenshot shows the AD FS console interface. On the left is a tree view with 'Relying Party Trusts' selected. The main area displays a table of Relying Party Trusts:

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

The 'Bitwarden ADFS Test Properties' dialog box is open, showing the 'Endpoints' tab. It contains a table of endpoints:

URL	Index	Binding	Default	Re
SAML Assertion Consumer Endpoints				
https://sso.bitwarden.com/sa...	0	POST	Yes	

The 'Edit Endpoint' dialog box is also open, showing the 'Binding' dropdown menu set to 'POST', which is highlighted with a green circle. Other fields include 'Endpoint type' (SAML Assertion Consumer), 'Index' (0), 'Trusted URL' (https://sso.bitwarden.com/saml2/3e5d0), and 'Response URL'.

Edit Endpoint

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

The screenshot shows the AD FS console interface. On the left is a navigation tree with 'Relying Party Trusts' selected. The main area displays a table of Relying Party Trusts:

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

An 'Edit Claim Issuance Policy for Bitwarden ADFS Test' dialog is open, showing 'Issuance Transform Rules':

Order	Rule Name	Issued Claims
1	Bitwarden	E-Mail Address, Name, Giv...
2	UPN	UPN
3	Transform Name ID	Name ID

The 'Edit Rule - Bitwarden' dialog is also open, showing configuration details:

- Claim rule name: Bitwarden
- Rule template: Send LDAP Attributes as Claims
- Attribute store: Active Directory
- Mapping of LDAP attributes to outgoing claim types:

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
Surname	Surname
*	

Buttons at the bottom include 'View Rule Language...', 'OK', and 'Cancel'.

ADFS Rule 1

⇒ Rule 2

The screenshot shows the AD FS console interface. On the left is a navigation tree with 'Relying Party Trusts' selected. The main pane displays a table of Relying Party Trusts:

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

Two dialog boxes are open over the console:

- Edit Claim Issuance Policy for Bitwarden ADFS Test**: Shows a table of Issuance Transform Rules:

Order	Rule Name	Issued Claims
1	Bitwarden	E-Mail Address.Name.Giv...
2	UPN	UPN
3	Transform Name ID	Name ID
- Edit Rule - UPN**: A configuration dialog for the UPN rule. It includes:
 - Claim rule name:
 - Rule template: Send LDAP Attributes as Claims
 - Attribute store: Active Directory
 - Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	UPN
*		

ADFS Rule 2

⇒ Rule 3

The screenshot shows the AD FS console interface. On the left is a navigation tree with 'Relying Party Trusts' selected. The main pane shows a table of Relying Party Trusts:

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

An 'Edit Claim Issuance Policy for Bitwarden ADFS Test' dialog is open, showing a table of Issuance Transform Rules:

Order	Rule Name	Issued Claims
1	Bitwarden	E-Mail Address, Name, Giv...
2	UPN	UPN
3	Transform Name ID	Name ID

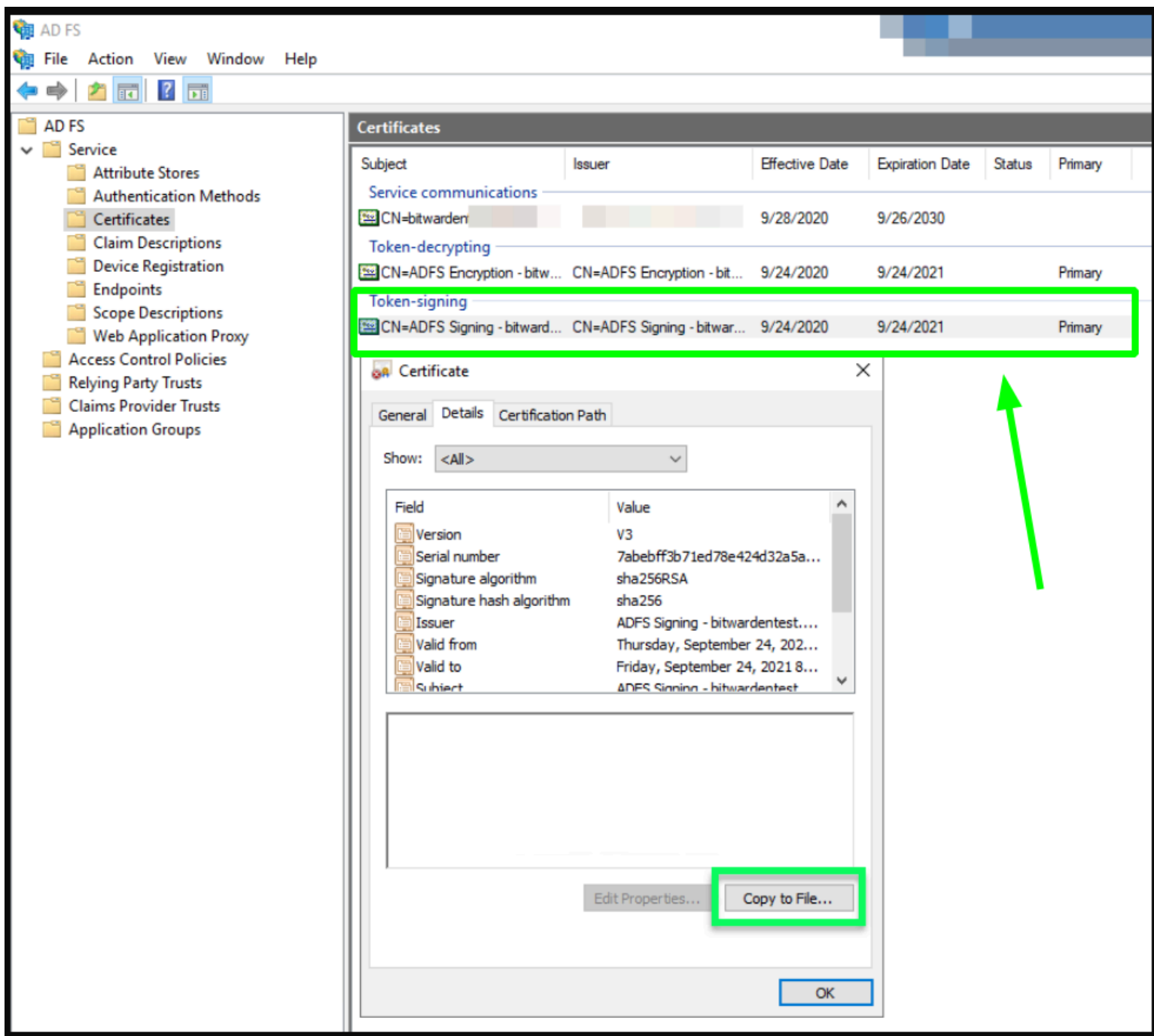
The 'Edit Rule - Transform Name ID' dialog is also open, showing configuration options:

- 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
- Selected option: Pass through all claim values

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。

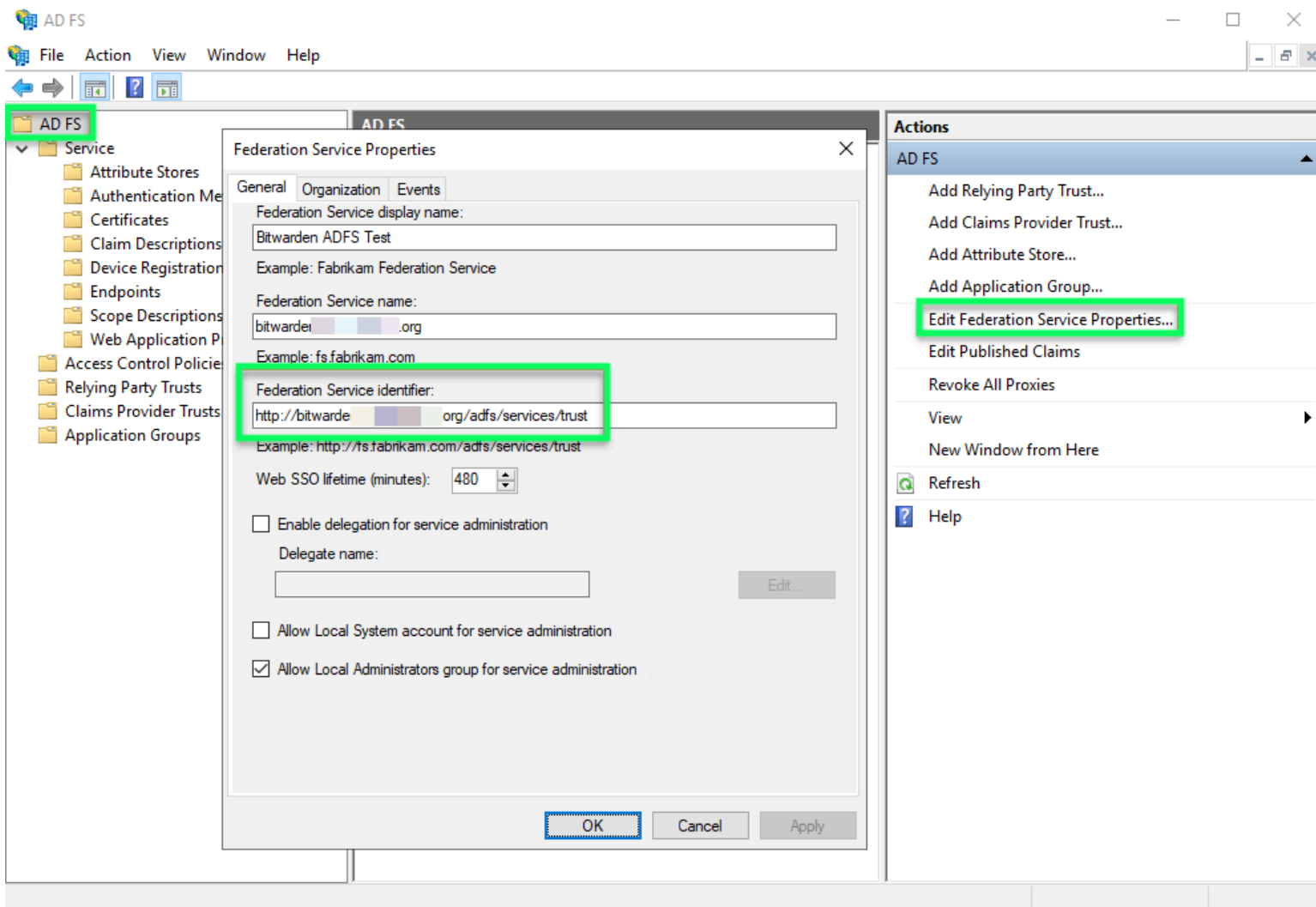


Get token-signing Certificate

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。



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IdP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
X509公開証明書	<p>xml ドキュメントのSingleSignOnServiceの設定キーから正確な値を取得することができます。</p> <hr/> <p>ダウンロードした証明書を貼り付け、削除してください。</p> <p>-----BEGIN CERTIFICATE-----</p> <p>そして</p> <p>-----証明書終了-----</p> <p>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。</p>
アウトバウンド署名アルゴリズム	<p>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。</p>
アウトバウンドログアウトリクエストを無効にする	<p>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。</p>
認証リクエストに署名が必要です	<p>AD FSがSAMLリクエストの署名を期待するかどうか。</p>

📌 Note

X509証明書を完成させるとき、有効期限の日付をメモしてください。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)

⊗ Input 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！

① 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。