

管理者コンソール > SSOでログイン

SAML 2.0設定

ヘルプセンターで表示:

<https://bitwarden.com/help/configure-ss0-saml/>

SAML 2.0設定

ステップ1：SSO識別子を設定する

SSOを使用してIDを認証するユーザーは、認証に対抗する組織（したがって、SSO統合）を示す**SSO識別子**を入力する必要があります。ユニークなSSO識別子を設定するには：

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

The screenshot shows the Bitwarden web application interface. On the left, there is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, Settings, Password Manager, Secrets Manager, Admin Console, and Toggle Width. A red box highlights the 'Secrets Manager' option, and a red arrow points to it. The main content area is titled 'All vaults' and features a 'FILTERS' sidebar on the left with a search bar and a list of vault categories. The main list displays several vaults:

<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

2. 設定に移動 → シングルサインオン、そしてあなたの組織のためのユニークな**SSO識別子**を入力してください：

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.

識別子を入力してください

3. ステップ2へ進む : SSOでのログインを有効にする。

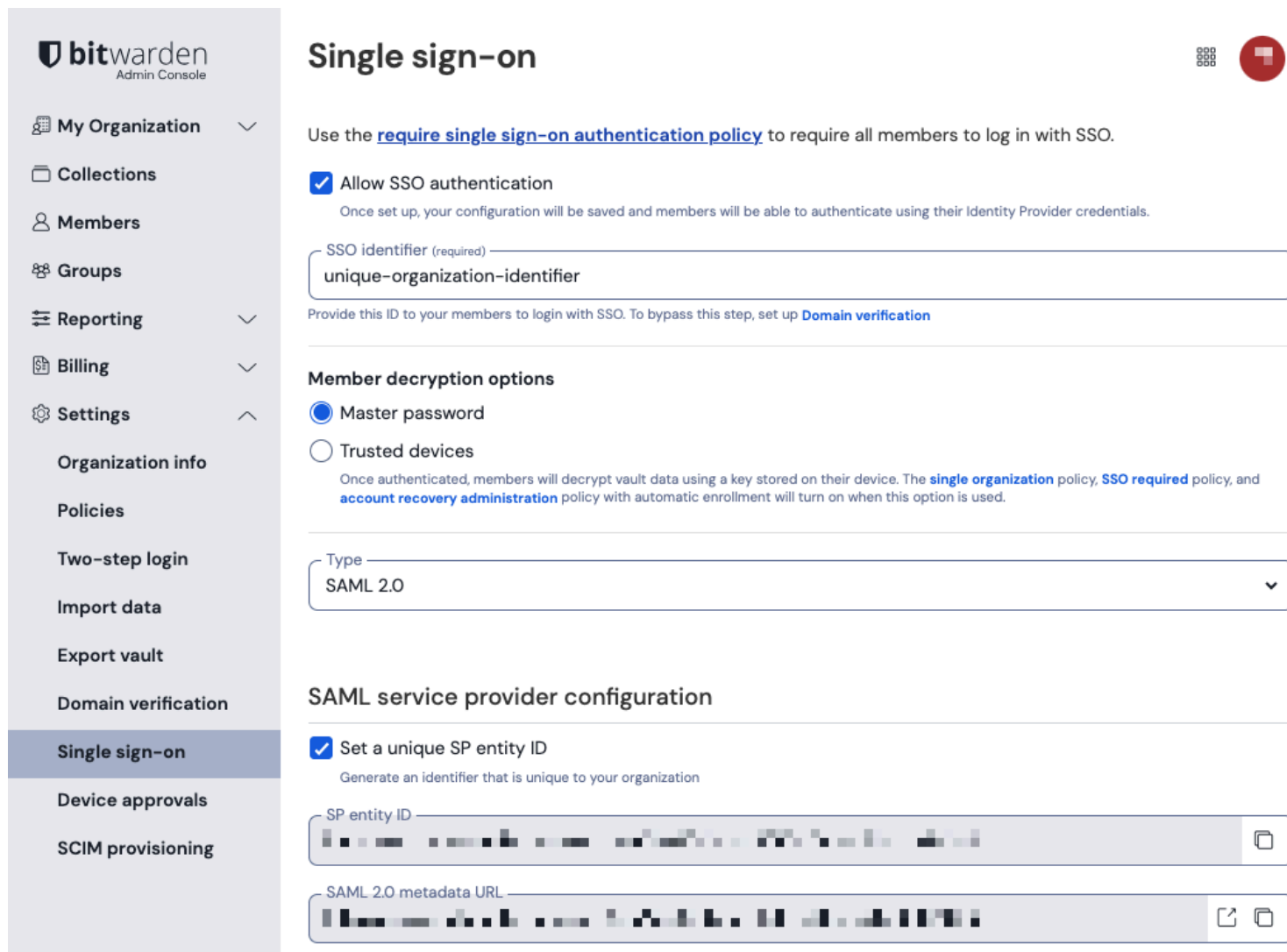


Tip
You will need to share this value with users once the configuration is ready to be used.

ステップ2 : SSOでのログインを有効にする

あなたのSSO識別子を取得したら、あなたの統合を有効化し設定することができます。SSOでのログインを有効にするには :

1. 設定 → シングルサインオン 表示で、SSO認証を許可する チェックボックスを確認してください :



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

SAML 2.0 metadata URL

SAML 2.0設定

2. **タイプ**のドロップダウンメニューから、**SAML 2.0**のオプションを選択してください。もし代わりにOIDCを使用するつもりであれば、[OIDC設定ガイド](#)に切り替えてください。

この段階で、必要に応じて**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。

ステップ3：設定

この時点から、実装はプロバイダーごとに異なります。設定プロセスの完了に役立つ、特定の**実装ガイド**の一つにジャンプしてください：

プロバイダー

AD FS

Auth0

AWS

アズール

デュオ

グーグル

ジャンプクラウド

キークローク

オクタ

ワンログイン

PingFederate

ガイド

[AD FS 実装ガイド](#)

[Auth0 実装ガイド](#)

[AWS 実装ガイド](#)

[Azure 実装ガイド](#)

[Duo 実装ガイド](#)

[Google 実装ガイド](#)

[JumpCloud 実装ガイド](#)

[Keycloak実装ガイド](#)

[Okta 実装ガイド](#)

[OneLogin 実装ガイド](#)

[PingFederate 実装ガイド](#)

設定参考資料

次のセクションでは、どのIdPと統合しているかに関係なく、シングルサインオン設定中に利用可能なフィールドを定義します。設定する必要があるフィールドは、(必須)とマークされます。



Tip

Unless you are comfortable with SAML 2.0, we recommend using one of the [above implementation guides](#) instead of the following generic material.

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プロバイダー設定は、SAMLの応答に期待する形式を決定します。

サービスプロバイダー設定

フィールド	説明
SPエンティティID	<p>(自動生成) 認証リクエスト用の Bitwarden エンドポイント。</p> <p>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。</p>
SAML 2.0 メタデータ URL	<p>(Bitwardenエンドポイントのための自動生成された)メタデータURL。</p> <p>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。</p>
アサーションコンシューマーサービス (ACS) URL	<p>(自動生成) SAMLアサーションがIdPから送信される場所。</p> <p>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。</p>
名前ID形式	<p>BitwardenがSAMLアサーションの形式を要求します。文字列としてキャストする必要があります。オプションには以下のものがあります：</p> <ul style="list-style-type: none"> -未指定 (デフォルト) -メールアドレス -X.509 主体名 - Windows ドメイン修飾名 -ケルベロスプリンシパル名 -エンティティ識別子 -持続的な -一時的な
アウトバウンド署名アルゴリズム	<p>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。オプションには以下のものがあります：</p> <ul style="list-style-type: none"> - http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 (デフォルト) - http://www.w3.org/2000/09/xmldsig#rsa-sha1 - http://www.w3.org/2000/09/xmldsig#rsa-sha384 - http://www.w3.org/2000/09/xmldsig#rsa-sha512
署名行動	<p>SAMLリクエストが署名されるかどうか/いつ署名されるか。オプションには以下のものがあります：</p> <ul style="list-style-type: none"> -IdPが認証リクエストに署名を求める場合 (デフォルト)

フィールド	説明
	-いつも -決して
最小入力署名アルゴリズム	BitwardenがSAMLレスポンスで受け入れるアルゴリズムの最小強度。
署名された主張を期待します	このチェックボックスをチェックすると、BitwardenはIdPからの応答が署名されることを期待します。
証明書を検証する	あなたのIdPから信頼できるCAを通じて信頼性のある有効な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。

IDプロバイダー設定

フィールド	説明
エンティティID	(必須) あなたのIDサーバーのアドレスまたはURL、またはIdPエンティティID。このフィールドは大文字と小文字を区別し、IdPの値と完全に一致する必要があります。
バインディングタイプ	IdPがBitwarden SAMLリクエストに応答するための方法。オプションには以下のものがあります： -リダイレクト (推奨) -HTTP POST
シングルサインオンサービスURL	(エンティティIDがURLでない場合に必要) あなたのIdPによって発行されたSSO URL。
シングルログアウトサービスURL	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使用を計画していますが、このフィールドを事前に設定することを強くお勧めします。
X509公開証明書	(必須) X.509 Base-64エンコードされた証明書本体。含めないでください -----BEGIN CERTIFICATE----- そして -----証明書の終わり-----

フィールド	説明
アウトバウンド署名アルゴリズム	<p>CER/PEM形式の証明書の行または部分。</p> <p>証明書の値は大文字と小文字を区別し、このフィールド内の余分なスペース、キャリッジリターン、およびその他の余分な文字は証明書の検証失敗を引き起こします。このフィールドに証明書のデータのみをコピーしてください。</p> <p>あなたのIdPがSAMLレスポンス/アサーションに署名するために使用するアルゴリズム。オプションには以下のものがあります：</p> <ul style="list-style-type: none"> - http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 (デフォルト) - http://www.w3.org/2000/09/xmldsig#rsa-sha1 - http://www.w3.org/2000/09/xmldsig#rsa-sha384 - http://www.w3.org/2000/09/xmldsig#rsa-sha512
アウトバウンドログアウト要求を許可する	<p>SSOでのログインは現在、SLOをサポートしていません。</p> <p>このオプションは将来の使用を計画していますが、このフィールドを事前に設定することを強くお勧めします。</p>
認証リクエストに署名する	<p>このチェックボックスをチェックすると、あなたのIdPはBitwardenからのSAMLリクエストが署名されることを期待するようになります。</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。

SAML属性&クレーム

アカウントの提供にはメールアドレスが必要です。これは、以下の表の属性またはクレームのいずれかとして渡すことができます。

ユニークなユーザー識別子も非常に推奨されます。不在の場合、ユーザーをリンクするためにメールアドレスが代わりに使用されます。

属性/請求は、適用可能な場合にはフォールバックを含めて、一致のための優先順位でリストされています。

値	請求/属性	フォールバッククレーム/属性
ユニークID	非一時的な場合のNameID urn:oid:0.9.2342.19200300.100.1.1 サブ UID UPN EPPN	

値	請求/属性	フォールバッククレーム/属性
Eメール	<p>Eメール http://schemas.xmlsoap.org/ws/2005/05/ID/claims/emailaddress urn:oid:0.9.2342.19200300.100.1.3 メール メールアドレス</p>	<p>希望のユーザーネーム Urn:oid:0.9.2342.19200300.100.1.1 UID</p>
お名前	<p>お名前 http://schemas.xmlsoap.org/ws/2005/05/ID/claims/name urn:oid:2.16.840.1.113730.3.1.241 urn:oid:2.5.4.3 表示名 CN</p>	<p>名前 + " " + 姓 (下記参照)</p>
名	<p>urn:oid:2.5.4.42 名前 ファーストネーム FN F名 ニックネーム</p>	
姓	<p>urn:oid:2.5.4.4 SN 苗字 苗字</p>	