管理者コンソール > SSOでログイン >

# OneLogin SAMLの実装

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

# **U bit**warden

### OneLogin 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**OneLogin特有の**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OneLoginポータルの両方で同時に作業を行うことを含みます。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(鼺)を使用して管理者コンソールを開きます。

D Password Manager	All vaults			New 🗸	BW
🗇 Vaults	FILTERS		Nama	Owner	:
🕼 Send			Name	Owner	:
$\ll$ Tools $\sim$	Q Search vau	ASIV	Company Credit Card Visa, *4242	My Organiz	÷
<b>≅ Reports</b>	✓ All vaults		Demonal Login		
Settings $\sim$	<ul> <li>∠ My vault</li> <li>∅ My Organiz :</li> </ul>	0 3	myusername	Me	:
	ġ⊞ Teams Org : + New organization		Secure Note	Me	:
	<ul> <li>✓ All items</li> <li>☆ Favorites</li> <li>⑦ Login</li> <li>□ Card</li> <li>Identity</li> <li>↓ Secure note</li> </ul>		Shared Login sharedusername	My Organiz	÷
<ul> <li>Password Manager</li> <li>Secrets Manager</li> </ul>	<ul> <li>✓ Folders</li> <li>➡ No folder</li> <li>✓ Collections</li> <li>➡ Extract collect.</li> </ul>				
Admin Console	Default colle				
쵸 Toggle Width	in Irasn				

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。

<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.
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) 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	Master password
Organization info Policies	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	
	SAML 2.0 metadata URL

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。

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**のオプションをオフにすることができます。これを行うと、 あなたのSPエンティティID値から組电IDが削除されますが、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。

#### OneLoginアプリを作成します

OneLoginポータルで、アプリケーション画面に移動し、アプリを追加ボタンを選択します:

0	nelogin	Users	Applications	Devices	Authentication	Activity	Security	Settings	Developers	
A	pplicati	ions								Add App
	<b>Q</b> search cor	mpany ap	ops							
	No company	apps hav	re been added.							

Add an Application

#### 検索バーにsaml test connectorとタイプし、SAML Test Connector (Advanced)アプリを選択してください:

<b>jin</b> Users	Applications	Devices	Authentication	Activity	Security	Settings	Developers		
Applicat	ions								
test connecto	r								
SAML Test Co OneLogin, Inc	onnector (Advar	nced)						SAML2.0	
SAML Test Co OneLogin, Inc	onnector (SP Sh :.	nibboleth)						SAML2.0	
	Application I test connector SAML Test CA OneLogin, Inc. SAML Test CA OneLogin, Inc.	Users       Applications         Applications       Applications         I test connector       Itest connector         SAML Test Connector (Advant OneLogin, Inc.       SAML Test Connector (SP SH OneLogin, Inc.	Users       Applications       Devices         Applications       Applications       Applications         I test connector       Applications       Applications         SAML Test Connector (Advanced)       OneLogin, Inc.       Applications         SAML Test Connector (SP Shibboleth)       OneLogin, Inc.       Applications	Openal Devices       Authentication         Applications       Authentication         Applications       Itest connector         Itest connector       Itest Connector (Advanced)         OneLogin, Inc.       SAML Test Connector (SP Shibboleth)         OneLogin, Inc.       Itest Connector (SP Shibboleth)	Open Users       Applications       Devices       Authentication       Activity         Applications       Itest connector       Itest co	Vsers Applications   Devices Authentication   Activity Security   Applications   Itest connector   SAML Test Connector (Advanced)   OneLogin, Inc.     SAML Test Connector (SP Shibboleth)   OneLogin, Inc.	Visers Applications     Applications     Applications     Itest connector     SAML Test Connector (Advanced)     OneLogin, Inc.     SAML Test Connector (SP Shibboleth)     OneLogin, Inc.	Visers Applications     Applications     Applications     Itest connector     SAML Test Connector (Advanced)   OneLogin, Inc.     SAML Test Connector (SP Shibboleth)     OneLogin, Inc.	yin Users Applications     Applications     Itest connector     SAML Test Connector (Advanced)   OneLogin, Inc.     SAML Test Connector (SP Shibboleth)     OneLogin, Inc.     SAML2.0

SAML Test Connector App

#### あなたのアプリケーションにBitwarden特有の表示名を付けて、保存ボタンを選択してください。

#### 設定

左側のナビゲーションから設定を選択し、以下の情報を設定します。これらの一部はシングルサインオン画面から取得する必要があります。

onelogin Users	Applications	Devices Au	uthentication	Activity	Security	Settings	Developers	
Applications / SAML Test Conn	ector (Adv	vanced)				М	ore Actions 🔻	Save
Info Configuration Parameters Rules SSO Access		Application RelayState Audience (En Recipient	ntityID)					
			App Confi	guration				
<b>アプリケーション設定</b> 観客 (エンティティID)	<b>説明</b> このフィ・ この自動: 設定によ	ールドを事前に 生成された値は り異なります。	至生成された <b>S</b> は、組織の <b>設</b> の	Pエンティ ≧ → シング	ティIDに設 `ルサインオ	定します。 ト <b>ン</b> 画面から	らコピーでき、	
受信者	このフィ <sup>-</sup> の設定に(	ールドを、 <b>視聴</b> 使用された同じ	<b>诸(エンティ</b> ジ事前生成され	r <b>ティID)</b> れた <b>SPエン</b>	ティティル	に設定しま	えす。	
ACS (コンシューマー) URL バリデーター	OneLogir このフィ・ 次のフィ・	によって <b>必須</b> る ールドに情報を ールドに進んで	とマークされ <sup>。</sup> 入力する必要 ください、 <b>A</b>	ているにも 要は実際に <b>CS (消費者</b>	かかわらず はありませ <b>;) URL</b> 。	ັ້ ん。Bitwar	denと統合するたと	めには。
ACS(消費者)URL	このフィ・ この自動: 設定によ	ールドを事前に 生成された値は り異なります。	生成された <b>A</b> t、組織の <b>設</b> の	ssertion ( Ĕ → シング	Consumer `ルサインオ	Service (A トン画面から	ACS) URLに設定し らコピーでき、	ます。

アプリケーション設定	説明
SAML イニシエーター	<b>サービスプロバイダー</b> を選択してください。SSOでのログインは現在、 ldPが開始するSAMLアサーションをサポートしていません。
SAML namelD形式	このフィールドを、SAMLアサーションに使用したいSAML NamelDフォーマットに設定します。
SAML署名要素	デフォルトでは、OneLoginはSAMLレスポンスに署名します。 これを <b>アサーション</b> または <b>両方</b> に設定することができます。

設定を完了するには、保存ボタンを選択してください。

#### パラメーター

左側のナビゲーションからパラメータを選択し、十追加アイコンを使用して次のカスタムパラメータを作成します:

フィールド名	值
メールアドレス	Eメール
名前	名
苗字	姓

カスタムパラメータを完了するには、保存ボタンを選択してください。

#### SSO

左側のナビゲーションからSSOを選択し、以下を完了してください:

1. あなたのX.509証明書の下にある詳細を表示リンクを選択してください。

Enable SAML2.0	
Sign on method SAML2.0	
X.509 Certificate	
Standard Strength Certificate (2048-bit)       Change       View Details	
SAML Signature Algorithm	
SHA-256 -	
Issuer URL	
https://app.onelogin.com/saml/metadata/95eef6e7-560f-4531-9df3-02e7248415a8	ß
SAML 2.0 Endpoint (HTTP)	
https://mmccabe.onelogin.com/trust/saml2/http-post/sso/95eef6e7-560f-4531-9df3-02e7248415a8	6
View your Cert	

証明書画面で、X.509 PEM証明書をダウンロードまたはコピーします。後で使用する必要があるためです。コピーしたら、 メインのSSO画面に戻ってください。

- 2. あなたのSAML署名アルゴリズムを設定してください。
- 3. あなたの発行者URLとSAML 2.0エンドポイント(HTTP)をメモしてください。これらの値はすぐに使用する必要があります。

#### アクセス

左側のナビゲーションから**アクセス**を選択してください。**役割**セクションで、 Bitwardenを使用できるようにしたいすべての役割にアプリケーションのアクセスを割り当ててください。ほとんどの実装では、 Bitwarden特有の役割を作成し、代わりにキャッチオール(例えば、**デフォルト**)に基づいて割り当てるか、 既存の役割に基づいて割り当てます。

Privileges				
Setup	Roles			
	Bitwarden SSO Users	~	Default	

Role Assignment

### ウェブアプリに戻る

この時点で、OneLoginポータル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の設定

OneLogin Portalでアプリ作成中に選択した選択肢に従って、以下のフィールドを設定してください:

フィールド	説明
名前ID形式	このフィールドを、 <b>OneLoginのSAML</b> namelDフォーマットフィールドで選択したものに設定します。アプリ設定中に。
アウトバウンド署名アルゴリズム	デフォルトでSAMLリクエストに署名するために使用されるアルゴリズム、 <mark>sha-256</mark> 。
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。デフォルトでは、 OneLoginはリクエストの署名を必要としません。
最小入力署名アルゴリズム	このフィールドを、 <b>SAML署名アルゴリズム</b> アプリ設定中に選択したものに設定してください。
署名されたアサーションが欲しい	このボックスをチェックしてください、 もしOneLoginの <b>SAML署名要素</b> を <b>アサーション</b> または <b>両方</b> にアプリ設定中に設定した場合。
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、アプリケーションの値を取得するために、しばしばOneLoginポータル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	あなたのOneLoginの <b>発行者URL</b> を入力してください。これは、 OneLoginアプリのSSO画面から取得できます。 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	<b>HTTP Post</b> に設定します(SAML 2.0エンドポイント(HTTP) で示されているように)。
シングルサインオンサービスURL	あなたのOneLogin <b>SAML 2.0エンドポイント(HTTP)</b> を入力してください。 これはOneLoginアプリのSSO画面から取得できます。
シングルログアウトサービスURL	現在、SSOでの <b>ログインは</b> 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が、 ご希望であれば事前に設定することができます。
X509公開証明書	取得したX.509証明書を貼り付け、削除してください。 BEGIN CERTIFICATE 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、 その他の余分な文字は認証の検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	OneLogin SSO設定セクションで選択されたSAML署名アルゴリズムを選択してください。
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 <b>サポートしていません</b> 。 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	OneLoginがSAMLリクエストの署名を期待しているかどうか。

#### (i) 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。

#### **∏ ∏ ∏**

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、メールアドレスを入力し、**続ける**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てテストしてください:



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、 OneLoginのログイン画面にリダイレクトされます。

	onelogin	
<∘> Co	nnecting to Bitwarden SSO	
Usernar	me	
Ren	nember my username	
	Continue	
	Forgot Password	

OneLogin Login

OneLogin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。