### 管理者コンソール > SSOでログイン >

# Google SAML 実装

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

### Google SAML 実装

この記事には、SAML 2.0を介したSSOでの**Google Workspace特有の**ログイン設定に関する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Googleワークスペース管理者コンソールを同時に使用する作業を含みます。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。

Password Manager	All vaults			New 🗸	BW
🗇 Vaults	FILTERS		Name	Owner	:
🖉 Send			Name	Owner	•
$\ll$ Tools $\sim$	Q Search vau	VISA	Company Credit Card Visa, *4242	My Organiz	:
<b>≅ Reports</b>	✓ All vaults		Personal Login		
Settings	My vault My Organiz	0 5	myusername	Me	:
	gii Teams Org : + New organization		Secure Note	Me	:
	<ul> <li>✓ All items</li> <li>☆ Favorites</li> <li>④ 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> <li>∅ Admin Console</li> <li>७ Toggle Width</li> </ul>	<ul> <li>Folders</li> <li>No folder</li> <li>Collections</li> <li>Default colle</li> <li>Default colle</li> <li>Trash</li> </ul>				

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 IIII IIII IIII IIII
	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)
	Provide this ID to your members to login with SSO. To bypass this step, set up <b>Domain verification</b>
🕅 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	SAML 2.0
Import data	
Export vault	
Domain verification	SAML service provider configuration
Single sign-on	Set a unique SP entity ID
Device approvals	- 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、必要であれば**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、 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、ほとんどの場合では、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。

#### SAMLアプリを作成します

Google Workspaceの管理者コンソールで、アプリ → ウェブとモバイルアプリをナビゲーションから選択します。 ウェブとモバイルアプリの画面で、アプリを追加 → カスタムSAMLアプリを追加を選択します。

# **U bit**warden

	Google Admin	٩	Search for users, groups or settings			
Ê	) Home		Apps > Web and mobile apps			
	Dashboard					
• 2	Directory			Apps (0)	Add App   Settings	•
• [[	Devices			+ Add a filte	Search for apps	
- :::	Apps			Name 🛧	Add private Android app	Use
	Overview				And private Analoid app	
	Google Workspace				Add private Android web ap	р
	Additional Google services			(	Add custom SAML app	
	Web and mobile apps					
~	Marketplace apps					
	LDAP					
• 0	Security					

#### Create a SAML App

#### アプリの詳細

アプリ詳細画面で、アプリケーションにユニークなBitwarden専用の名前を付け、続けるボタンを選択してください。

#### Google IDプロバイダーの詳細

Google IDプロバイダーの詳細画面で、あなたのSSO URL、エンティティID、 そして**証明書**を後のステップで使用するためにコピーしてください:

× Add cust	tom SAML app			
🖌 App details –	- 2 Google Identity Provider detail: - 3 Service provider details - 4 Attribute mapping			
	To configure single sign-on (SSO) for SAML apps, follow your service provider's instructions. Learn more			
	Option 1: Download IdP metadata			
	DOWNLOAD METADATA			
	OR			
	Option 2: Copy the SSO URL, entity ID, and certificate			
	SSO URL			
	https://accounts.google.com/			
	Entity ID			
	https://accounts.google.com/			
	Certificate			
	Google_ Expires	<u>)</u> ±		
	BEGIN CERTIFICATE			
	SHA-256 fingerprint			
		Ū		
E	ЗАСК СА	NCEL	CONTINUE	



#### 終了したら、**続行**を選択してください。

### サービスプロバイダーの詳細

サービスプロバイダ詳細画面で、以下のフィールドを設定します:

フィールド	説明
ACS URL	このフィールドを事前に生成された <b>Assertion Consumer Service (ACS) URL</b> に設定します。 この自動生成された値は、組織の <b>設定 → シングルサインオン</b> 画面からコピーでき、設定により異なります。
エンティティID	このフィールドを事前に生成された <b>SPエンティティID</b> に設定します。 この自動生成された値は、組織の <b>設定 → シングルサインオン</b> 画面からコピーでき、設定に基づいて異なります。
開始URL	必要に応じて、このフィールドをユーザーがBitwardenにアクセスするためのログインURLに設定します。 クラウドホストのお客様の場合、これはhttps://vault.bitwarden.com/#/ssoまたはhttps://vault.bit warden.eu/#/ssoです。自己ホスト型のインスタンスの場合、 これはあなたの設定されたサーバーURLによって決定されます。例えば、https://your.domain.com/#/sso などです。
署名済みの返答	このボックスをチェックすると、WorkspaceがSAMLレスポンスに署名するようになります。チェックしない場合、 ワークスペースはSAMLアサーションのみに署名します。
名前IDの形式	このフィールドを <b>Persistent</b> に設定してください。
名前ID	NamelDを入力するためのワークスペースユーザー属性を選択してください。

#### 終了したら、**続ける**を選択してください。

#### 属性マッピング

属性マッピング画面で、**マッピングを追加**ボタンを選択し、次のマッピングを構築します:

Googleディレクトリ属性	アプリの属性
プライマリーメールアドレス	メールアドレス

#### **完了**を選択してください。

# **U bit**warden

### アプリを起動してください

デフォルトでは、Workspace SAMLアプリは**全員に対してOFF**になります。SAMLアプリのユーザーアクセスセクションを開き、 **全員に対してON**に設定するか、またはあなたのニーズに応じて特定のグループに設定してください。

TEST SAML LOGIN		~
DOWNLOAD METADATA     Certificate     Google_2026-5-9-112241_SAML2_0     (Expires May 9, 2026)	Entity ID https://sso.bitwarden.com/saml2	

User Access

#### あなたの変更を保存してください。

新しいWorkspaceアプリが既存のユーザーセッションに伝播するまでに最大24時間かかることにメモしてください。

### ウェブアプリに戻る

この時点で、Google Workspace管理者コンソー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のレスポンスで期待するフォーマットを決定します。

#### サービスプロバイダーの設定

次のフィールドを、ワークスペース管理者コンソールで選択した選択肢に従って設定しますセットアップ中に:

フィールド	説明
名前ID形式	このフィールドをWorkspaceで選択された名前ID形式に設定します。
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。

フィールド	説明
最小入力署名アルゴリズム	デフォルトでは、Google WorkspaceはRSA SHA-256で署名します。ドロップダウンから <mark>sha-25</mark> <mark>6</mark> を選択してください。
署名済みアサーションを期待する	BitwardenがSAMLアサーションに署名が必要かどうか。この設定は <b>チェックを外す</b> べきです。
証明書を検証する	あなたのldPから信頼できるCAを通じて信頼性のある有効な証明書を使用するときには、 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 with SSO dockerイメージと一緒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、しばしばワークスペース管理者コンソー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	このフィールドをWorkspaceの <b>エンティティID</b> に設定します。これは、Google IDプロバイダーの詳細セクションから取得するか、 <b>メタデータをダウンロード</b> ボタンを使用して取得します。 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	HTTP POST または <b>リダイレクト</b> に設定します。
シングルサインオンサービスURL	このフィールドをWorkspaceの <b>SSO URL</b> に設定し、Google IDプロバイダーの詳細セクションから取得するか、 <b>メタデータをダウンロード</b> ボタンを使用します。
シングルログアウト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	取得した証明書を貼り付け、削除してください。 BEGIN CERTIFICATE

フィールド	説明
	そして 証明書の終わり 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	デフォルトでは、Google WorkspaceはRSA SHA-256で署名します。 ドロップダウンから <mark>sha-256</mark> 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 <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。
認証リクエストに署名が欲しい	Google WorkspaceがSAMLリクエストの署名を期待しているかどうか。
() 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、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てテストしてください。



	Log in	
Maste © Input is Get ma	er password (required) s required. aster password hint	
	Log in with master password	
	🖻 Enterprise single sign-on	
Logging Not you	in as myemailaddress@bitwarden.com ?	

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、Google Workspaceのログイン画面にリダイレクトされます。



Login

あなたのワークスペースの認証情報で認証した後、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。