

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.

[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 (☰) 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"/>		<b>Company Credit Card</b>	My Organiz...	⋮
<input type="checkbox"/>		Visa, *4242		⋮
<input type="checkbox"/>		<b>Personal Login</b>	Me	⋮
<input type="checkbox"/>		myusername		⋮
<input type="checkbox"/>		<b>Secure Note</b>	Me	⋮
<input type="checkbox"/>		<b>Shared Login</b>	My Organiz...	⋮
<input type="checkbox"/>		sharedusername		⋮

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

[Masked SP entity ID]

SAML 2.0 metadata URL

[Masked 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。

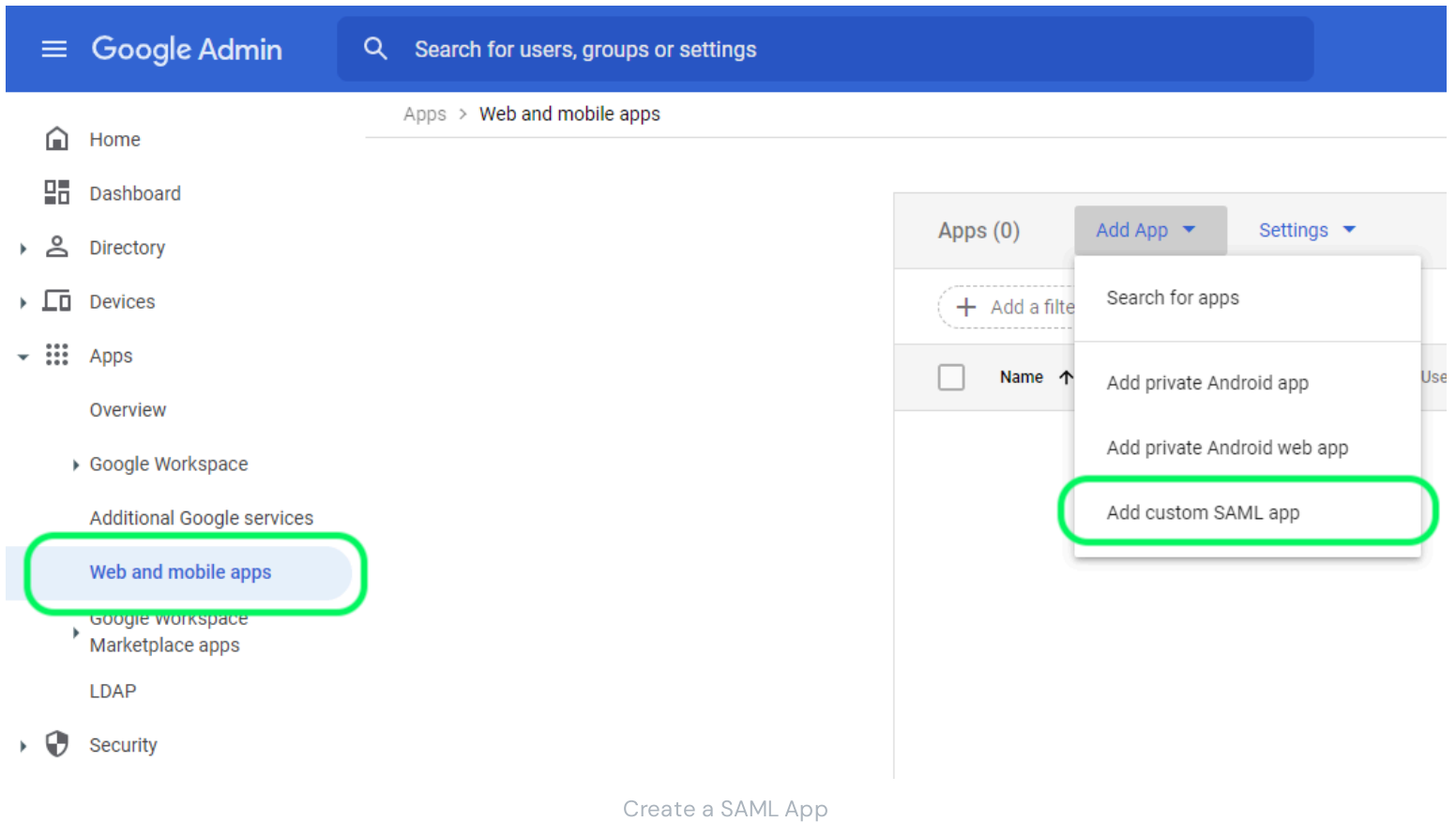
この段階で、必要であれば**ユニークなSPエンティティIDを設定するオプション**をオフにすることができます。これを行うと、あなたのSPエンティティID値から組電IDが削除されますが、ほとんどの場合では、このオプションをオンにしておくことをお勧めします。



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。

## 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。



## 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 custom SAML app

- 1 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



-----BEGIN CERTIFICATE-----

SHA-256 fingerprint



BACK

CANCEL

CONTINUE

IdP Details

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	<p>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。</p> <p>この自動生成された値は、組織の<b>設定</b> → <b>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。</p>
エンティティID	<p>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。</p> <p>この自動生成された値は、組織の<b>設定</b> → <b>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。</p>
開始URL	<p>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。</p> <p>クラウドホストのお客様の場合、これは<a href="https://vault.bitwarden.com/#/sso">https://vault.bitwarden.com/#/sso</a>または<a href="https://vault.bitwarden.eu/#/sso">https://vault.bitwarden.eu/#/sso</a>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<b>設定されたサーバーURL</b>によって決定されます。例えば、<a href="https://your.domain.com/#/sso">https://your.domain.com/#/sso</a>などです。</p>
署名済みの返答	<p>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。</p>
名前IDの形式	<p>このフィールドを<b>Persistent</b>に設定してください。</p>
名前ID	<p>NameID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。</p>

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。

## 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。

SAML

**Bitwarden Login with SSO**

---

[TEST SAML LOGIN](#)

[DOWNLOAD METADATA](#)

[DELETE APP](#)

**User access** ▼

To make the managed app available to select users, choose a group or organizational unit. [Learn more](#)

[View details](#)

OFF for everyone

**Service provider details** ▼

Certificate	ACS URL	Entity ID
Google_2026-5-9-112241_SAML2_0 (Expires May 9, 2026)		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 <b>選択された</b> 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 <b>sha-256</b> 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、 <a href="#">Google IDプロバイダーの詳細セクション</a> 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	<b>HTTP POST</b> 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、 <a href="#">Google IDプロバイダーの詳細セクション</a> 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</b> 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 <b>証明書</b> 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 <b>sha-256</b> 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</b> 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 to Bitwarden

Email address (required)

Remember email

Continue

or

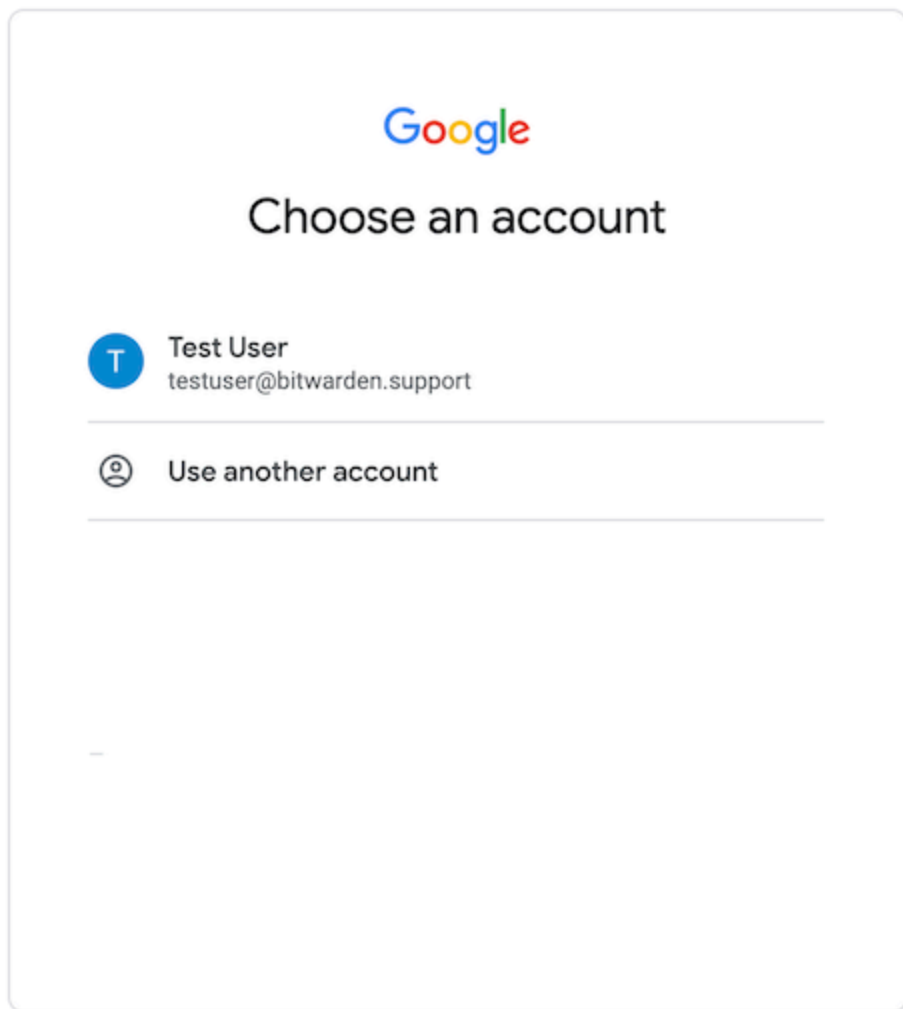
 Log in with passkey

 Use single sign-on

New to Bitwarden? [Create account](#)

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！

**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。