管理者コンソール > SSOでログイン >

AuthO SAMLの実装

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

AuthO 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**AuthO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AuthO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.

⊥ 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(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			N	0	
🕼 Send			Name	Owner	:
$ m \stackrel{<}{\sim}$ Tools $~~$ $~~$	Q Search vau	VISA	Company Credit Card Visa, *4242	My Organiz	:
፰ Reports	✓ All vaults		Personal Login		
🕸 Settings 🛛 🗸 🗸	My Vault		myusername	Ме	:
	 Hearing organization Hearing organization 		Secure Note	Ме	:
	 ✓ All items ☆ Favorites ④ Login □ Card □ Identity □ Secure note 		Shared Login sharedusername	My Organiz	÷
Password Manager Secrets Manager	 Folders No folder Collections 				
Admin Console	 Default colle Default colle Trash 				

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。

D bit warden Admin Console	Single sign-on 🗰 🕒
	Use the require single sign-on authentication policy 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.
绺 Groups	SSO identifier (required)
$ \stackrel{\mbox{\tiny \ensuremath{\in}}}{\mbox{\scriptsize =}} \ { m Reporting} \qquad \lor$	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	Trusted devices Once authenticated members will decrypt yoult data using a key stored on their device. The single organization policy. SSO required policy and
Policies	account recovery administration policy with automatic enrollment will turn on when this option is used.
Two-step login	C Type
Import data	SAML 2.0
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
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<mark>SSO識別子</mark>を組織用に作成し、<mark>SAML</mark>を**タイプ**のドロップダウンから選択してください。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、 組电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ーの使い方を学びましょう。

AuthOアプリケーションを作成する

AuthOポータルで、アプリケーションメニューを使用して、**通常のWebアプリケーション**を作成します:

Secure and trusted open source password manager for business

features that are not in t	he Free plan. Like what you're seein	g? Please enter your billing information here.	BILLIN
		G	
Applications			CREATE APPLICAT
Setup a mobile, web or IoT application	ation to use Auth0 for Authenticatio	on. Learn more ►	
Default App			
Default App Generic	Client ID: RM3UeXnRtL8C	CSjPPCg7HiitjInvQs0Be	
Generic	Client ID: RM3UeXnRtL8C	CSjPPCg7HiitjInvQs0Be	





AuthO Settings

AuthO 設定	説明
お名前	アプリケーションにBitwarden特有の名前を付けてください。
ドメイン	この値をメモしてください。それは後のステップで必要になります。
アプリケーションタイプ	通常のウェブアプリケーション を選択してください。
トークンエンドポイント認証方法	投稿(HTTP Post)を選択し、これは後で 設定する 属性にバインディングタイプとしてマッピングされます。
アプリケーションログインURI	このフィールドを事前に生成された SPエンティティID に設定します。 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。
許可されたコールバックURLS	このフィールドを事前に生成された Assertion Consumer Service (ACS) URL に設定します。 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、設定に基づいて異なります。

助成金のタイプ

詳細設定 → 許可タイプセクションで、以下の許可タイプが選択されていることを確認してください(事前に選択されている場合があります):

Application Metadata	Device Settings	OAuth	Grant Types	WS-Federation	Certificates
Grants					
	Authorization Cod	de 🔽	Refresh Token	Client Creder	ntials
Password		Passwordle	ss OTP		

Application Grant Types

証明書

<mark>詳細設定 → 証明書</mark>セクションで、署名証明書をコピーまたはダウンロードしてください。まだそれに何もする必要はありませんが、 後でそれを参照する必要があります。

Advanced Settings					
Application Metadata	Device Settings	OAuth	Grant Types	WS-Federation	Certificates
Signing Certificate	IFICATE				ۍ ۲
MIIDDTCCAfWgAwI BAMTGWRldi1objE MzQxMjIzMTUxMjU	BAgIJdp2+Lsu8IyH xZzJhNi51cy5hdXH xWjAkMSIwIAYDVQ(KcMA0GCSq RoMC5jb20 QDEx1kZXY	GSIb3DQEBCwU wHhcNMjEwNDE taG4xMWcyYTY	AMCQxIjAgBgNV 1MTUxMjUxWhcN udXMuYXV0aDAu	
Y29tMIIBIjANBgk	qhkiG9w0BAQEFAA(RGytTBwJEarqzmg)	DCAQ8AMII MzktBmkU0	BCgKCAQEA2yR BfuzjrtcaQx0	fsSC5LCYkTvuF utRM679AD0PX9	
nCW0wCEE7jkTtdx WZLqwiCErdeKP01	S3/TvqkNkPyf2UE2	27Qo4giJy	6FEUAgsqwTs/	gtX6sxIogeH0N	

AuthO Certificate

エンドポイント

詳細設定 → エンドポイントセクションで何も編集する必要はありませんが、後で参照するためにSAMLエンドポイントが必要になります。

♀ Tip

In smaller windows, the **Endpoints** tab can disappear behind the edge of the browser. If you're having trouble finding it, click the **Certificates** tab and hit the Right Arrow key (\rightarrow).

Certificates Endpoint
G

AuthO Endpoints

AuthOルールを設定する

あなたのアプリケーションのSAMLレスポンスの振る舞いをカスタマイズするためのルールを作成してください。AuthOは数値のオプションを提供していますが、 このセクションではBitwardenのオプションに特にマッピングするものだけに焦点を当てます。カスタムSAML設定ルールセットを作成するには、**認証パイプライン** → **ルール**メニューを使用して十 **ルールを作成**します:

\$	dev-hn11g2a6 Development Q Discuss your needs Docs C Iss
4~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Thank you for purchasing the Free Auth0 plan. You have 21 days left in your trial to experiment with features that are not in the Free plan. Like what you're seeing? Please enter your billing information here.
	Rules Custom Javascript snippets that run in a secure, isolated sandbox in the Auth0 service as part of your authentication pipeline. Learn more ►
א ר מי	TRY ALL RULES WITH Y
× •00	Custom SAML Config
<u> </u>	AuthO Rules

次のいずれかを設定することができます:

+-	説明
署名アルゴ リズム	AuthOがSAMLアサーションまたはレスポンスに署名するために使用するアルゴリズム。デフォルトでは、rsa-sha1 が含まれますが、 この値はrsa-sha256に設定するべきです。 この値を変更する場合、あなたは次のことを行う必要があります: -digestAlgorithm をsha256に設定します。 -Bitwardenの最小入力署名アルゴリズムをrsa-sha256に設定します。
ダイジェス トアルゴリ ズム	SAMLアサーションまたはレスポンスのダイジェストを計算するためのアルゴリズム。デフォルトでは、 <mark>sha-1。signatureAlgorithm</mark> の値も <mark>sha256</mark> に設定する必要があります。
サインレス ポンス	デフォルトでは、AuthOはSAMLアサーションのみに署名します。これを <mark>t rue</mark> に設定して、 アサーションの代わりにSAMLレスポンスに署名します。

*	説明
名前識別子	デフォルトでは、 <mark>urn:oasis:names:tc:SAML:1.1:nameid–format:unspecified。</mark> この値は任意のSAML NamelD形式に設定できます。
形式	もしそうなら、SP 名前ID形式 フィールドを対応するオプションに変更してください(こちらを参照)。

以下のようなスクリプトを使用して、これらのルールを実装してください。ヘルプが必要な場合は、AuthOのドキュメンテーションを参照してください。

Bash
function (upor context collback) (
TUNCTION (USER, CONTEXT, CALLBACK) {
context.samlConfiguration.signatureAlgorithm = "rsa-sha256";
context.samlConfiguration.digestAlgorithm = "sha256";
<pre>context.samlConfiguration.signResponse = "true";</pre>
<pre>context.samlConfiguration.nameIdentifierFormat = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"</pre>
<pre>context.samlConfiguration.binding = "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect";</pre>
callback(null, user, context);
}

ウェブアプリに戻る

この時点で、AuthO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

あなたがカスタムルールを設定していない限り、サービスプロバイダーの設定はすでに完了しているはずです。カスタムルールを設定したり、 実装にさらなる変更を加えたい場合は、関連するフィールドを編集してください。

フィールド	説明
名前ID形式	NamelD形式をSAMLリクエストで指定します(<mark>NameIDPolicy)。</mark> 省略するには、 設定されていません に設定します。
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は、 <mark>rsa–sha256</mark> です。
署名行動	Bitwarden SAMLリクエストが署名されるか/いつ署名されるか。デフォルトでは、 AuthO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	BitwardenがSAMLレスポンスで受け入れる最小の署名アルゴリズム。デフォルトでは、AuthOは <mark>rsa–sha1</mark> で署名します。 ドロップダウンから <mark>rsa–sha256</mark> を選択してください。ただし、カスタム署名ルールを設定している場合は除きます。

フィールド	説明
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を求めるかどうか。デフォルトでは、 AuthOはSAMLアサーションに署名しますので、カスタム署名ルールを設定していない限り、 このボックスをチェックしてください。
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 with 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AuthO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AuthOアプリケーションの ドメイン 値を入力してください(こちらを参照)、接頭辞として <mark>ur</mark> n:を使用します。例えば <mark>urn:bw-help.us.auth0.com</mark> のようになります。 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	あなたのAuthOアプリケーションで指定された トークンエンドポイント認証方法 の値と一致するように、 HTTP POSTを選択してください。
シングルサインオンサービスURL	あなたのAuthOアプリケーションの SAMLプロトコルURL を入力してください (エンドポイントを参照)。例えば、https://bw-help.us.auth0.com/samlp/HcpxD63h7Qzl42 0u8qachPWoZEG0Hho2。
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	取得した署名証明書を貼り付け、削除します BEGIN CERTIFICATE 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、 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、AuthOは <mark>rsa–sha1</mark> で署名します。 <mark>rsa–sha256</mark> を選択してください、 あなたがカスタム署名ルールを設定していない限り。

フィールド	説明
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を希望します	AuthOがSAMLリクエストの署名を期待しているかどうか。
() Note	

🛈 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。

♀ Тір
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。



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、AuthOのログイン画面にリダイレクトされます。



あなたのAuthO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。