管理者コンソール > SSOでログイン >

AWS SAML 実装

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

AWS SAML 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AWS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AWSコンソー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

すでにSSOの専門家ですか?この記事の指示をスキップして、 自分の設定と比較するためのサンプル設定のスクリーンショットをダウンロードしてください。

▲ タイプ:アセット-ハイパーリンク id:K4Z8nyORzKkHKIJIZ4hh1

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。

U Password Manager	All vaults			New 🗸	BW
🗇 Vaults	FILTERS		Name	Owner	:
🖉 Send			Name	Gwiler	•
🖏 Tools 🛛 🗸 🗸	Q Search vau	VISA	Company Credit Card Visa, *4242	My Organiz	÷
≅ Reports	✓ All vaults		Demonal Login		
🕸 Settings 🛛 🗸 🗸	 ∠ My vault ∠ My Organiz : ∠ Toomo Org 	0 3	myusername	Me	:
	→ New organization		Secure Note	Ме	:
	 ✓ All items ☆ Favorites ④ Login □ Card Identity ↓ Secure note 		Shared Login sharedusername	My Organiz	÷
 Password Manager Secrets Manager ℬ Admin Console Ճ Toggle Width 	 ✓ Folders ➢ No folder ✓ Collections ➢ 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	Single sign-on III III III III IIII IIII IIII IIII
B 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.
卷 Groups	SSO identifier (required)
≅ 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 SAML 2.0
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	i a com a comunicación de la comunicación d
	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SSO識別子を組織用に作成し、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値から組織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。

AWS SSOアプリケーションを作成します

AWSコンソールで、AWS SSOに移動し、ナビゲーションからアプリケーションを選択し、 新しいアプリケーションを追加ボタンを選択します:

aws Services Q	Search	[Option+S] D A ⑦ ◎ N. Virginia ▼
IAM Identity Center	×	IAM Identity Center > Applications
Dashboard Users Groups Settings Multi-account permission AWS accounts Permission sets	s	Applications Administer users and groups for AWS managed or customer managed applications that support identity federation with SAML 2.0 or OAuth 2.0. Learn more Add application AWS managed Customer managed
 Application assignments Applications 		AWS managed applications (0) An AWS managed application is defined by and named for an AWS service, and must be configured from the applicable service console to work with IAM Identity Center.
Related consoles AWS Organizations 🖸 IAM 🕻		Q. Search for an AWS managed application All services ▼ < 1 > ③ Application ▼ Service Owning account ID ▼ Date created ▼ Status ▼ You have not added any applications You have not added any applications
		新しいアプリケーションを追加する

検索バーの下で、カスタムSAML 2.0アプリケーションを追加のオプションを選択します:

AWS SSO Application Catalog

Type the name of an application	1		
 Add a custom SAML 2.0 You can add SSO integrad 	application tion to your custom SAML 2.0-enab	led applications	
10,000 ft	4me ^{**}		 Abstract
10000ft	4me	7Geese	Abstract

カスタムSAMLアプリを追加する

詳細

アプリケーションにユニークでBitwarden特有の表示名を付けてください。

AWS SSOメタデータ

このセクションの情報は、後の設定ステップで必要になります。AWS SSOサインインURLとAWS SSO発行者URLをコピーし、AWS SSO証明書をダウンロードしてください:

aws	Services Q Se	arch	[Option+S] ▷ 수 ⑦ ③ N. Virginia ▼ ■ ■ ■	۰ ۳
≡			IAM Identity Center metadata Your cloud application may require the following certificate and metadata details to recognize IAM Identity Center as the identity provider.	0
			IAM Identity Center SAML metadata file Download IAM Identity Center sign-in URL IAM Identity Center sign-out URL IAM Identity Center sign-out URL	
			IAM Identity Center SAML issuer URL	

AWS SSOメタデータ

アプリケーションのプロパティ

アプリケーション開始URLフィールドに、ユーザーがBitwardenにアクセスするためのログインURLを指定します。 クラウドホストのお客様の場合、これは常にhttps://vault.bitwarden.com/#/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/#/ssoのようなものです。

アプリケーションのメタデータ

アプリケーションのメタデータセクションで、メタデータの値を手動で入力するオプションを選択してください。

Manually type your metadata values O Upload application SAML metadata file Application ACS URL
Application ACS URL

メタデータの値を入力してください

次のフィールドを設定してください:

フィールド	説明
アプリケーションACS URL	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、 設定により異なります。
アプリケーション SAML オーディエンス	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。

終了したら、**変更を保存**を選択してください。

属性マッピング

属性マッピングタブに移動し、次のマッピングを設定します:

aws Services Q Search	[Option+S] D 🗘 ② ③ N. Virginia ▼	
IAM Identity Center $\times \bigotimes_{Y}^{O} c_{Y}$	onfiguration for 'Bitwarden SAML 2.0 application' has been saved. ou must configure attribute mappings for IAM Identity Center to work.	ש
Dashboard Users Groups Settings V Multi-account permissions	AM Identity Center > Applications > Bitwarden SAML 2.0 application Bitwarden SAML 2.0 application	
AWS accounts Permission sets Application assignments Applications	Edit configuration Edit attribute mappings Display name Bitwarden SAML 2.0 application 属性マッピング	
アプリケーション内のユーザー属	性 この 文字列値 またはユーザー 属性をAWS SSOにマップします 形式	
件名	\${user:email} メールアドレ	ス
メールアドレス	<mark>\${user:email</mark> } 特定されてい	ません

割り当てられたユーザー

割り当てられたユーザータブに移動し、ユーザーを割り当てるボタンを選択します:



アプリケーションには個々のレベルでユーザーを割り当てることができますし、グループごとにも割り当てることができます。

ウェブアプリに戻る

この時点で、AWS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2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形式を決定します。

サービスプロバイダーの設定

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が、次のフィールドのいずれかを編集することを選択することができます:

フィールド	説明
名前ID形式	メールアドレス 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。
最小入力署名アルゴリズム	デフォルトでは、AWS SSOはSHA-256で署名します。これを変更していない限り、 ドロップダウンから <mark>sha256</mark> を選択してください。

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されることを期待しているかどうか。
証明書を検証する	あなたのldPから信頼できるCAを通じて信頼された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AWS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	AWS SSO発行者URL を入力してください。これはAWSコンソールのAWS SSOメタデータセクションから取得できます。 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	HTTP POST または リダイレクト に設定します。
シングルサインオンサービスURL	AWS SSOサインインURL を入力してください。これはAWSコンソールのAWS SSOメタデータセクションから取得できます。
シングルログアウトサービスURL	SSOでのログインは現在、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、 AWSコンソールの AWS SSOメタデータ セクションから取得したAWS SSOサインアウトURLで事前に設定することができます。
X5O9公開証明書	ダウンロードした証明書を貼り付け、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、

フィールド	説明
	キャリッジリターン、 その他の余分な文字 は証明書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、AWS SSOは <mark>sha256</mark> で署名します。 これを変更していない限り、ドロップダウンから <mark>sha256</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が欲しい	AWS SSOがSAMLリクエストに署名を期待するかどうか。

(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。

⊘ 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:



	Log in	
Mast © Input	ter password (required)	
	Log in with master password	
\square	🖶 Enterprise single sign-on	
Logging Not yo	g in as myemailaddress@bitwarden.com u?	

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、AWS SSOのログイン画面にリダイレクトされます。

aws		
Sia	a in	
Useri	name	
alic	e, alice@domain.com, DOMAIN\alice	
R	emember username	
	Next	
Ву сої	ntinuing, you agree to the AWS Customer	
Agree	ment or other agreement for AWS services,	
and th	ne Privacy Notice . This site uses essential	
inforn	es, see our Cookie Notice for more nation.	





(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。