管理者コンソール > SSOでログイン >

JumpCloud SAML 実装

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

JumpCloud 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JumpCloud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JumpCloud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(闘)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		Nama	Owner	
🖉 Send			Name	Owner	:
\ll Tools \sim	Q Search vau	VISA	Company Credit Card Visa, *4242	My Organiz	÷
≅ Reports	✓ All vaults		Percent Leste		
🕸 Settings 🛛 🗸 🗸	 ∠ My vault ∅ My Organiz : ∅ Toomo Org 		Personal Login 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 Admin Console [™] 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。

Secure and trusted open source password manager for business

D bit Warden	Single sign-on 🗰 🗧	
	Use the require single sign-on authentication policy to require all members to log in with SSO.	
	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	
$ agreen = ext{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	○ Trusted devices	
Policies	Once authenticated, members will decrypt valit 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	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、 組电IDがSPエンティティID値から削除されますが、ほとんどの場合では、このオプションをオンにしておくことを推奨します。

⊘ 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。

JumpCloud SAMLアプリケーションを作成する

JumpCloudポータルで、メニューからアプリケーションを選択し、開始ボタンを選択します:

Secure and trusted open source password manager for business

n jumpcloud	SSO () & Product Tour Pricing	Alerts	P What's New	Support	i≣ Checklist MM
C Discover GET STARTED					
A Home					
✓ USER MANAGEMENT					
Q Users					
e¶a, User Groups					
- USER AUTHENTICATION		<u>.</u>			
🔂 LDAP		00			
🕑 RADIUS					
Password Manager NEW					
 DEVICE MANAGEMENT 					
C Devices					
& Device Groups					
Policy Management					
Ø Policy Groups					
Commands	Add your first application				
Software Management	Single Sign-On and Identity Management Application Integrations				
	Set up and manage single sign-on or create an identity management integration to				
INTEGRATIONS	import, update, and export users on a regular basis.				
Applications					
Cloud Directories	Get Started				
HR Directories					
	Pro Tip: You can connect nearly any HR Directory or				
Eive Chat	Identity Provider to easily import new users into JumpCloud!				
days left Settings					
Account					
	Create Bitwarden app. Jumpcloud				

検索ボックスにBitwardenを入力し、設定ボタンを選択します:

🔍 bitwarden 🛛 😣			
1 item			
Name 🔺		Supported Functionality	
D bit warden	Bitwarden		configure

⊘ Tip

If you are more comfortable with SAML, or want more control over things like NamelD Format and Signing Algorithms, create a **Custom SAML Application** instead.

一般情報

「一般情報」セクションで、以下の情報を設定してください:

フィールド	説明
ディスプレイラベル	アプリケーションにBitwarden特有の名前を付けてください。

シングルサインオン設定

シングルサインオン設定セクションで、以下の情報を設定します:

Ø An IDP Certificate and Private Key will be generat	ed for this application after activation. Click here to see the Knowledge Base article with details for configuring this application
Service Provider Metadata: 0	
Upload Metadata	
IdP Entity ID: 0	
JumpCloud	
SP Entity ID: 0	
https://sso.bitwarden.com/saml2/	
ACS URL: 0	
https://sso.bitwarden.com/sami2/YOUR_ORG_ID	/Acs/
SP Certificate:	
Upload SP Certificate	
IDP URL:	
https://sso.jumpcloud.com/saml2/ bitwa	rden
Attributes	
If attributes are required by this Service Provider for SSO Service Provider. Learn more.	authentication, they are not editable. Additional attributes may be included in assertions, although support for each attribute will vary for each
USER ATTRIBUTE MAPPING: 0	

Jumpcloud SSO configuration

フィールド	説明
ldPエンティティID	このフィールドを一意で、Bitwarden特有の値に設定します。例えば、 <mark>bitwardensso_yourcompany</mark> 。
SPエンティティID	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。
ACS URL	このフィールドを事前に生成された アサーションコンシューマーサービス(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。

カスタムSAMLアプリのみ

カスタムSAMLアプリケーションを作成した場合、次の**シングルサインオン設定**フィールドも設定する必要があります:

フィールド	説明
SAMLSubject NamelD	JumpCloud属性を指定してください。これはSAMLレスポンスでNamelDとして送信されます。
SAMLSubject NameID形式	SAMLレスポンスで送信されるNamelDの形式を指定してください。
署名アルゴリズム	SAMLアサーションまたはレスポンスに署名するためのアルゴリズムを選択してください。
サインの主張	デフォルトでは、JumpCloudはSAMLレスポンスに署名します。このボックスをチェックして、 SAMLアサーションに署名してください。
ログインURL	あなたのユーザーがSSO経由でBitwardenにログインするURLを指定してください。 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.b itwarden.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/#/ss oなどです。



属性

シングルサインオン設定→属性セクションで、次のSP→IdP属性マッピングを構築します。 JumpCloudでBitwardenアプリケーションを選択した場合、これらはすでに構築されているはずです:

Attributes

If attributes are required by this Service Provider for SSO authentication, they are not editable. Additional attributes may be included in assertions, although support for each attribute will vary for each Service Provider. Learn more.

USER ATTRIBUTE MAPPING: 0

Service Provider Attribute Name	JumpCloud Attribute Name	
email	email	T
uid	username	~
firstname	firstname	Ψ.
lastname	lastname	~
add attribute		

Attribute Mapping

終了したら、アクティベートボタンを選択してください。

証明書をダウンロードしてください

アプリケーションが有効化されたら、作成されたBitwardenアプリケーションを開くために再度SSOメニューオプションを使用してください。 IDP証明書のドロップダウンを選択し、証明書をダウンロードします。

🖚 jumpcloud	SSO		↓ Alerts III Resources 0	D Support	
Home NEW	Featured Applic		Details User Groups		×
 ℜ User Groups ✓ USER AUTHENTICATION G LDAP 	si Sl	Bitwarden	 General Info *Display Label: Bitwarden Login with SSO 		
RADIUS SSO DEVICE MANAGEMENT Devices	Supported functionality SSO JIT Identity Man	Regenerate certificate Download certificate Upload new certificate	Description (Optional) Use the description to add Application specific information that users will see in the User Portal. (For Ex: Indicate how users will authenticate into the Application).		
 Device Groups Configurations (Policies) 	Q Search		Display Option:	_1;	

Download Certificate

ユーザーグループをバインドする

JumpCloudポータルで、メニューから**ユーザーグループ**を選択します。

•1	jumpcloud	Us	er Gro	oups 🛈			\$ Alerts	Resources	③ Supp	ort (s
G	Home NEW										
								ex	pand got	: it	
R	Users										
• #R	User Groups		Q	Search					2 groups	delete	}
			Туре	Group 🔺							
6	LDAP			All Users						>	
C	RADIUS		0	Group of Users							
8	SSO			Bitwarden SSO Group of Users						>	
Ÿ.	Devices										
֎	Device Groups										

User Groups

Bitwarden専用のユーザーグループを作成するか、またはすべてのユーザーのデフォルトユーザーグループを開きます。いずれの場合でも、 アプリケーションタブを選択し、そのユーザーグループの作成したBitwarden SSOアプリケーションへのアクセスを有効にします:

	Det Bitv	t ails Users varden SSO use Search	Device Groups er group is bound to the	Applications following applicatio	RADIUS	Directories	×
$\forall \forall$		Status Nam	e l	Display Label 🔺	Su	pported Functionality	
	•	• UI	bitwarden	Bitwarden Login with	SSO		
Bitwarden SSO							
			Bind App Access	6			

⊘ Tip

Alternatively, you can bind access to user groups directly from the SSO → Bitwarden Application screen.

ウェブアプリに戻る

この時点で、JumpCloud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のウェブ保管庫に戻ってください。

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

次のフィールドを、JumpCloud Portalでアプリ作成中に選択した選択肢に従って設定します:

フィールド	説明
名前ID形式	カスタムSAMLアプリケーションを作成した場合、これを指定されたSAMLSubject NamelDフォーマットに設定します。それ以外の場合は、 未指定 にしてください。
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。

フィールド	説明
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、 JumpCloud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	カスタムSAMLアプリケーションを作成した場合、 選択した署名アルゴリズムにこれを設定してください。それ以外の場合は、rsa-sha256 のままにしてください。
署名付きのアサーションが欲しい	カスタムSAMLアプリケーションを作成した場合、JumpCloudの Sign Assertion オプションを設定した場合は、このボックスをチェックしてください。それ以外の場合は、 チェックを外してください。
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JumpCloud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	JumpCloudの IdPエンティティID を入力してください。 これはJumpCloudのシングルサインオン設定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	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	JumpCloudの IdP URL を入力してください。 これはJumpCloudのシングルサインオン設定画面から取得できます。

フィールド	説明
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。
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 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	カスタムSAMLアプリケーションを作成した場合、 選択した署名アルゴリズムにこれを設定してください。それ以外の場合は、rs a-sha256のままにしてください。
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を希望します	JumpCloud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。

∂ 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、 JumpCloudのログイン画面にリダイレクトされます。

Log in to your application using JumpCloud

Email

User Email Address

Password

Password

SSO Login

Reset User Password

JumpCloud Login

あなたのJumpCloud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。