

管理者コンソール > SSOでログイン >

Keycloak SAML実装

Keycloak 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**Keycloak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Keycloakポータルを同時に操作することを含みます。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 (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"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login sharedusername	My Organiz...	⋮

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]

SAML 2.0 metadata URL
[Masked]

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、組電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。



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。

Keycloakの設定

Keycloakにログインし、**クライアント** → **クライアントを作成**を選択します。

Clients
Clients are applications and services that can request authentication of a user. [Learn more](#)

Clients list | Initial access token | Client registration

Search for client → **Create client** | Import client

Client ID	Name	Type	Description	Home URL
account	\${client_account}	OpenID Connect	-	
account-console	\${client_account-console}	OpenID Connect	-	
admin-cli	\${client_admin-cli}	OpenID Connect	-	-
broker	\${client_broker}	OpenID Connect	-	-
master-realm	master Realm	OpenID Connect	-	-
security-admin-console	\${client_security-admin-...}	OpenID Connect	-	

[Create a Client](#)

クライアントを作成する画面で、次のフィールドに入力してください：

フィールド	説明
クライアントタイプ	SAMLを選択してください。
クライアント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。
お名前	Keycloakクライアントの名前を自由に入力してください。

必要なフィールドに**一般設定**ページで入力したら、**次へ**をクリックしてください。

ログイン設定画面で、次のフィールドに入力してください：

フィールド	説明
有効なリダイレクトURI	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。

保存を選択してください。

「Keys」タブを選択し、**クライアント署名が必要**オプションを**オフ**に切り替えてください。

master

- Manage
- Clients**
- Client scopes
- Realm roles
- Users
- Groups
- Sessions
- Events
- Configure
- Realm settings

Clients > Client details

https://mat.bitwarden.support/sso/saml2 SAML

Enabled ⓘ Action

Clients are applications and services that can request authentication of a user.

Settings **Keys** Roles Client scopes Sessions Advanced

Signing keys config

If you enable the "Client signature required" below, you must configure the signing keys by generating or importing keys, and the client will sign their saml requests and responses. The signature will be validated.

Client signature required ⓘ Off

Keycloak Keys Config

最後に、Keycloakのメインナビゲーションで、**レルム設定**を選択し、次に**キータブ**を選択します。**RS256証明書**を探して、**証明書**を選択してください。

master

- Manage
- Clients
- Client scopes
- Realm roles
- Users
- Groups
- Sessions
- Events
- Configure
- Realm settings**
- Authentication
- Identity providers
- User federation

< General Login Email Themes **Keys** Events Localization Security defenses Sessions Tokens Cliv >

Keys list Providers

Active keys Search key → 1-4 < >

Algorithm	Type	Kid	Use	Provider	Public keys
AES	OCT	a3282835-06db-42cc-b29a-ff969226eca9	ENC	aes-generated	
HS256	OCT	be68f437-88a6-4c3b-b92f-bf3b114beeb6	SIG	hmac-generated	
RSA-OAEP	RSA	zXKBnvtriZQU7MbyXJlIf60wGotgDbZwpG8_x7wE1QQ	ENC	rsa-enc-generated	Public key Certificate
RS256	RSA	T3IREov-EMgD0EnJ5AsHsv0GX-Z0s89jCyloy6fmlsE	SIG	rsa-generated	Public key Certificate

1-4 < >

Keycloak RS256 Certificate

証明書の値は次のセクションで必要となります。

ウェブアプリに戻る

この時点で、Keycloakポータルコンテキスト内で必要なすべてを設定しました。Bitwardenウェブアプリに戻り、ナビゲーションから**設定**→**シングルサインオン**を選択します。

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の応答に期待する形式を決定します。

次のフィールドを**SAMLサービスプロバイダ設定**セクションで完了してください：

フィールド	説明
名前IDの形式	メールアドレスを選択してください。
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。
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	KeycloakクライアントがSAMLドキュメントまたはアサーションに署名するために使用するよう設定されているアルゴリズムを選択します。
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。トグルがオンの場合、Keycloakクライアントをアサーションに署名するよう設定してください。
証明書を検証する	あなたのIdPから信頼できるCAを通じて信頼でき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ログインの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。

次のフィールドを**SAML IDプロバイダ**設定セクションで完了してください：

フィールド	説明
エンティティID	クライアントが作成されたKeycloakレルムのURLを入力してください。例: https://領域/ 。 このフィールドは大文字と小文字を区別します。
バインディングの種類	リダイレクト を選択します。
シングルサインオンサービス URL	あなたのマスターSAML処理URLを入力してください。例えば、 https://領域//プロトコル/saml 。
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 ログアウトURL で事前に設定することができます。
X509 公開鍵証明書	前のステップでコピーされた RS256証明書 を入力してください。 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 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	KeycloakクライアントがSAMLドキュメントまたはアサーションに署名するために使用するよう設定されているアルゴリズムを選択します。
アウトバウンドログアウトリクエストを無効にする	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。
認証リクエストに署名が欲しい	KeycloakがSAMLリクエストの署名を期待するかどうか。

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、作業を**保存**してください。



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](#)

追加のKeycloak設定

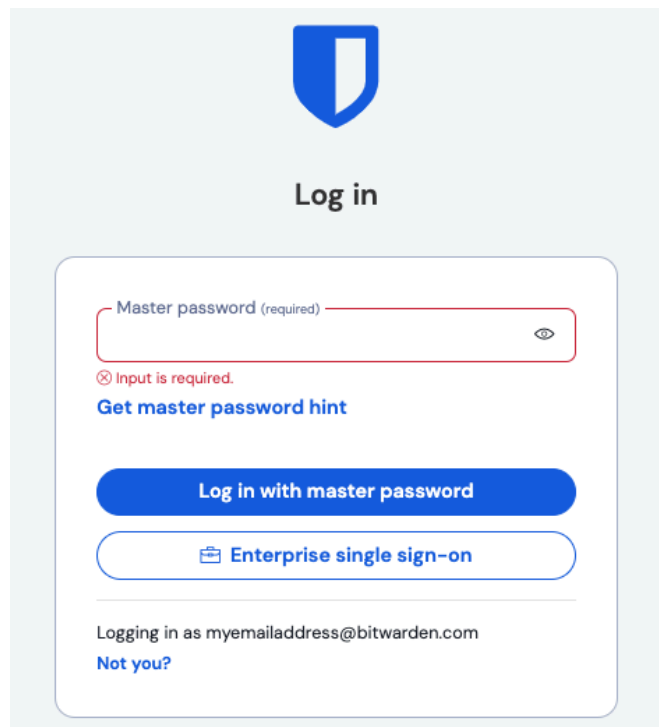
「Keycloakクライアント設定」タブでは、追加の構成オプションを使用できます。

フィールド	説明
書類に署名する	Keycloak領域によってSAMLドキュメントが署名されるべきかどうかを指定してください。
署名アサーション	KeycloakレルムによってSAMLアサーションが署名されるべきかどうかを指定してください。
署名アルゴリズム	署名アサーションが有効になっている場合、署名に使用するアルゴリズムを選択します（デフォルトはsha-256）。
名前ID形式	KeycloakがSAMLレスポンスで使用するName IDフォーマットを選択してください。

フォーラムが完了したら、**保存**を選択してください。

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サインオン**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

設定された組織の識別子を入力し、**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、Keycloakのログイン画面にリダイレクトされます。



Log In

Username or email

Password

Log In

Keycloak Login Screen

あなたのKeycloak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！

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。