

管理者コンソール > SSOでログイン >

# Okta SAMLの実装

ヘルプセンターで表示:

<https://bitwarden.com/help/saml-okta/>

## Okta SAMLの実装

この記事には、SAML 2.0を介したSSOでのOkta特有のログインの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Okta管理者ポータル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ステップ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。

The screenshot shows the Bitwarden web application interface. On the left is a dark blue sidebar with navigation options: Password Manager, Secrets Manager, Admin Console, and Toggle Width. The main content area is titled 'All vaults' and features a 'New' button, a product switcher icon (☰), and a user profile icon (BW). Below the title is a 'FILTERS' section with a search bar and a list of vault categories: All vaults, My vault, My Organiz..., Teams Org..., and New organization. Under 'All items', there are options for Favorites, Login, Card, Identity, Secure note, Folders, No folder, Collections, Default colle..., Default colle..., and Trash. The main vault list has columns for Name and Owner, and includes items like Company Credit Card, Personal Login, Secure Note, and Shared Login. A red circle highlights the 'Password Manager' option in the sidebar, and a red arrow points to the product switcher icon in the top right of the main content area.

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 :



Applications Help

[Create App Integration](#) [Browse App Catalog](#) [Assign Users to App](#) [More](#)

Search

STATUS	ACTIVE	INACTIVE
	0	6

- Okta Admin Console
- Okta Browser Plugin
- Okta Dashboard

Okta create app integration

新しいアプリケーション統合ダイアログで、SAML 2.0ラジオボタンを選択します：

### Create a new app integration

Sign-in method [Learn More](#)

- OIDC - OpenID Connect**  
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**  
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**  
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**  
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

[Cancel](#) [Next](#)

SAML 2.0 radio button

次へボタンを選択して設定に進んでください。

## 一般設定

一般設定画面で、アプリケーションにユニークでBitwarden特有の名前を付け、次へを選択します。

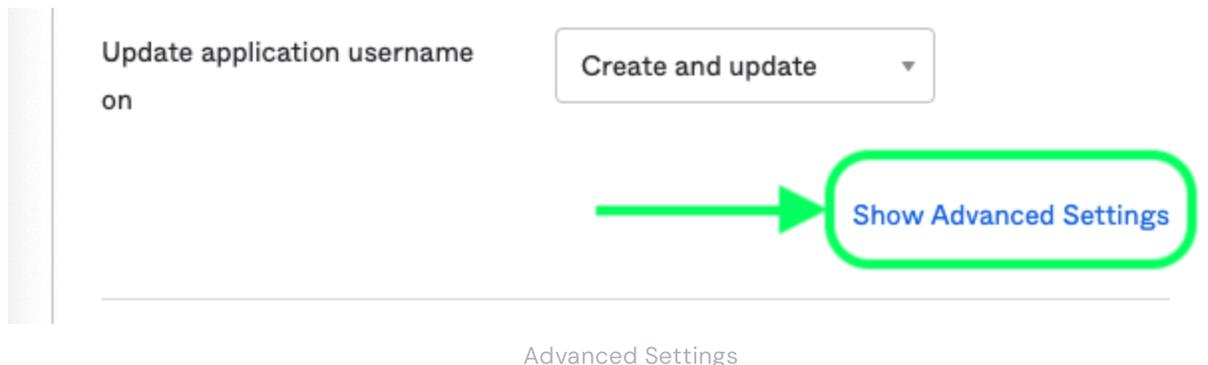
## SAMLを設定する

SAMLの設定画面で、以下のフィールドを設定します:

フィールド	説明
シングルサインオン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 <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。
視聴者のURI (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 <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。
名前IDの形式	SAML NameID形式をSAMLアサーションで使用するために選択します。デフォルトでは、 <b>未指定</b> 。
アプリケーションのユーザー名	Okta属性を選択して、ユーザーがBitwardenにログインするために使用します。

## 高度な設定

詳細設定を表示のリンクを選択し、次のフィールドを設定してください:



フィールド	説明
応答	SAMLレスポンスがOktaによって署名されているかどうか。
主張署名	SAMLアサーションがOktaによって署名されているかどうか。
署名アルゴリズム	応答と/またはアサーションに署名するために使用される署名アルゴリズムは、 <b>署名済み</b> に設定されているものによります。デフォルトでは、 <b>rsa-sha256</b> 。
ダイジェストアルゴリズム	応答と/またはアサーションに署名するために使用されるダイジェストアルゴリズムは、 <b>署名済み</b> に設定されているものによります。このフィールドは、選択された <b>署名アルゴリズム</b> と一致する必要があります。

## 属性ステートメント

属性ステートメントセクションで、以下のSP → IdP属性マッピングを構築します：

**Attribute Statements (optional)** [LEARN MORE](#)

Name	Name format (optional)	Value
email	Unspecified ▼	user.email ▼
firstname	Unspecified ▼	user.firstName ▼ ×
lastname	Unspecified ▼	user.lastName ▼ ×

[Add Another](#)

Attribute Statements

設定が完了したら、次へボタンを選択してフィードバック画面に進み、完了を選択してください。

## IdPの値を取得します

アプリケーションが作成されたら、アプリのサインオンタブを選択し、画面の右側にある設定手順を表示ボタンを選択してください：

### Settings Edit

#### Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3<sup>rd</sup> party application. Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State

#### Credentials Details

Application username format: Okta username

Update application username on: Create and update Update Now

Password reveal:  Allow users to securely see their password (Recommended)

**About**

**SAML 2.0** streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3<sup>rd</sup> party application may be required to complete the integration with Okta.

**Application Username**

Choose a format to use as the default username value when assigning the application to users.

If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

## SAML Signing Certificates

Generate new certificate

Type	Created	Expires	Status	Actions
SHA-1	Oct 2022	Oct 2032	Inactive ⚠	<a href="#">Actions</a>

**SAML Setup**

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

[View SAML setup instructions](#)

[View SAML setup instructions](#)

このページを将来の使用のために開いたままにするか、またはIDプロバイダーのシングルサインオンURLとIDプロバイダーの発行者をコピーして、X.509証明書ダウンロードしてください：

## The following is needed to configure Bitwarden

1 Identity Provider Single Sign-On URL:

```
https://bitwardenhelptest.okta.com/app/bitwardenhelptest_bitwarden_1/exk3fajwkMx07SosA696/sso/saml
```

2 Identity Provider Issuer:

```
http://www.okta.com/exk3fajwkMx07SosA696
```

3 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----  
MIIDjsjCCApqgAwIBAgIGAXw253khMA0GCSqGSIb3DQEBCwUAMIGZMQswCQYDVQQGEwJVUzETMBEG  
A1UECAwKQ2FsaWZvcn5pYTEwMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAAsGA1UECgwET2t0YTEU
```

IdP Values

### 課題

課題タブに移動し、割り当てるボタンを選択します:

← Back to Applications

## Bitwarden Login with SSO

Active ▾
View Logs
Monitor Imports

General   Sign On   Import   **Assignments**

Assign ▾
Convert AssignmentsGroups ▾

Filters	Priority	Assignment
<ul style="list-style-type: none"> <li>People</li> <li style="background-color: #e6f2ff;">Groups</li> </ul>	1	<div style="display: flex; align-items: center;"> <span style="font-weight: bold;">Everyone</span> </div> <p style="font-size: 0.9em; margin: 0;">All users in your organization</p>

**REPORTS**

- [Current Assignments](#)
- [Recent Unassignments](#)

**SELF SERVICE**

You need to enable self service for org managed apps before you can use self service for this app.

[Go to self service settings](#)

**Requests**   Disabled

**Approval**   -

Assigning Groups

アプリケーションへのアクセスは、人々に割り当てるオプションを使用してユーザーごとに、またはグループに割り当てるオプションを使用して一括で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、Okta管理者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。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

次のフィールドを、アプリ作成中にOkta管理者ポータルで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	これをOktaで指定された名前ID形式に設定するか、それ以外の場合は未指定のままにしてください。
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。
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	これをOktaで指定された署名アルゴリズムに設定します。
署名されたアサーションが欲しい	Assertion Signatureフィールドを署名済みのOktaに設定した場合、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Okta管理者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	Oktaのサインオン設定画面から取得した、あなたのIDプロバイダ発行者を入力してください。これは、設定手順を表示ボタンを選択することで取得できます。このフィールドは大文字と小文字を区別します。

フィールド	説明
バインディングタイプ	リダイレクトに設定します。現在、OktaはHTTP POSTをサポートしていません。
シングルサインオンサービスURL	Oktaのサインオン設定画面から取得した、あなたのIDプロバイダーのシングルサインオンURLを入力してください。
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を予定していますが、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	<p>ダウンロードした証明書を貼り付け、削除してください。</p> <p>-----BEGIN CERTIFICATE-----</p> <p>そして</p> <p>-----証明書終了-----</p> <p>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。</p>
アウトバウンド署名アルゴリズム	選択された署名アルゴリズムを選択してください Oktaアプリ設定中に。署名アルゴリズムを変更していない場合は、デフォルトのままにしてください ( rsa-sha256 )。
アウトバウンドログアウト要求を許可する	現在、SSOでのログインはSLOをサポートしていません。
認証リクエストに署名を希望します	Okta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

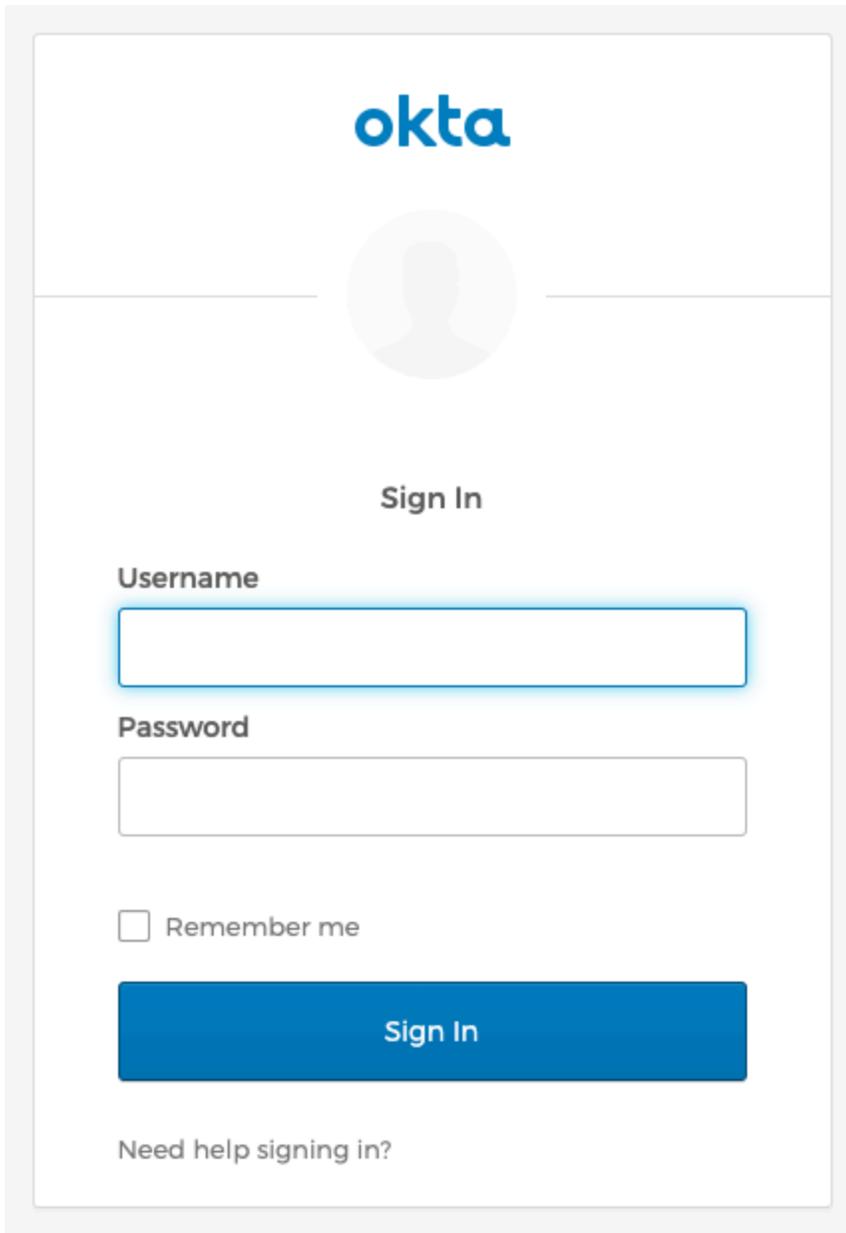
Log in with passkey

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、Oktaのログイン画面にリダイレクトされます。



Log in with Okta

あなたのOkta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 does not support unsolicited responses, so initiating login from your IdP will result in an error. The SSO login flow must be initiated from Bitwarden. Okta administrators can create an [Okta Bookmark App](#) that will link directly to the Bitwarden web vault login page.

1. As an admin, navigate to the **Applications** drop down located on the main navigation bar and select **Applications**.
2. Click **Browse App Catalog**.
3. Search for **Bookmark App** and click **Add Integration**.
4. Add the following settings to the application:
  1. Give the application a name such as **Bitwarden Login**.
  2. In the **URL** field, provide the URL to your Bitwarden client such as <https://vault.bitwarden.com/#/login> or [your-self-hostedURL.com](#).
5. Select **Done** and return to the applications dashboard and edit the newly created app.
6. Assign people and groups to the application. You may also assign a logo to the application for end user recognition. The Bitwarden logo can be obtained [here](#).

Once this process has been completed, assigned people and groups will have a Bitwarden bookmark application on their Okta dashboard that will link them directly to the Bitwarden web vault login page.