

管理者コンソール > SSOでログイン >

Okta OIDCの実装

ヘルプセンターで表示:

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

Okta OIDCの実装

この記事には、OpenID Connect (OIDC) を介したSSOでの**Okta特有のログイン**を設定するためのヘルプが含まれています。別のOIDC IdPでのSSOを使用したログインの設定、またはSAML 2.0を介したOktaの設定についてのヘルプは、[OIDC設定](#)または[Okta SAML実装](#)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。

ウェブ保管庫でSSOを開く

Bitwardenのウェブアプリにログインし、製品スイッチャー (製品) を使用して管理者コンソールを開きます。

The screenshot displays the Bitwarden web application interface. On the left, a dark blue sidebar contains navigation options: Password Manager, Vaults, Send, Tools, Reports, Settings, Password Manager, Secrets Manager, Admin Console, and Toggle Width. The main content area is titled 'All vaults' and features a 'FILTERS' panel on the left and a list of vaults on the right. The 'FILTERS' panel includes a search bar and sections for 'All vaults', 'All items', 'Folders', 'Collections', and 'Trash'. A red box highlights the 'Password Manager' option in the sidebar, and a red arrow points to the 'Default colle...' option in the 'All items' section. The vaults list includes items like 'Company Credit Card', 'Personal Login', 'Secure Note', and 'Shared Login'.

製品-スイッチャー

ナビゲーションから設定 → シングルサインオンを選択してください。

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
OpenID Connect

OpenID connect configuration

Callback path

Signed out callback path

OIDC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識別子を作成してください。それ以外では、この画面でまだ何も編集する必要はありませんが、簡単に参照できるように開いたままにしておいてください。

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。

Oktaアプリを作成する

Okta管理者ポータルで、アプリケーション → アプリケーションをナビゲーションから選択します。アプリケーション画面で、**アプリ統合を作成**ボタンを選択します。サインオン方法で、**OIDC - OpenID Connect**を選択してください。アプリケーションのタイプで、**ウェブアプリケーション**を選択してください。

×

Create a new app integration

Sign-on 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.

Application type

What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

- Web Application**
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)
- Single-Page Application**
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)
- Native Application**
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

Cancel Next

Create App Integration

新しいWebアプリの統合画面で、以下のフィールドを設定します：

フィールド	説明
アプリ統合名	アプリにBitwarden専用の名前を付けてください。

フィールド	説明
グラントタイプ	<p>以下の許可タイプを有効にしてください：</p> <ul style="list-style-type: none"> - クライアントが自身を代表して行動 → クライアント資格情報 - ユーザーを代表して行動するクライアント → 認証コード
サインインリダイレクトURI	<p>このフィールドをあなたのコールバックパスに設定してください。これはBitwarden SSO設定画面から取得できます。</p> <p>クラウドホストのお客様の場合、これはhttps://sso.bitwarden.com/oidc-signinまたはhttps://sso.bitwarden.eu/oidc-signin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/sso/oidc-signinなどです。</p>
サインアウトリダイレクトURI	<p>このフィールドをあなたのサインアウトコールバックパスに設定してください。これはBitwarden SSO設定画面から取得できます。</p>
課題	<p>このフィールドを使用して、すべてまたは選択したグループのみがBitwarden ログインをSSOで使用できるように指定します。</p>

設定が完了したら、次へボタンを選択してください。

クライアントの資格情報を取得します

アプリケーション画面で、新しく作成されたOktaアプリのクライアントIDとクライアントシークレットをコピーします：



Bitwarden Login with SSO

Active ▾

View Logs

General

Sign On

Assignments

Okta API Scopes

Client Credentials

Edit

Client ID

Public identifier for the client that is required for all OAuth flows.

Client secret

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

Ready to code

You can download a preconfigured sample app.

[Download sample app](#)

To get started using your custom app integration, see the "Sign Users In" section in the Okta [Developer's guide](#)

App Client Credentials

あなたは後のステップで両方の値を使用する必要があります。

認証サーバー情報を取得します

ナビゲーションから **セキュリティ** → **API** を選択します。認証サーバーのリストから、この実装に使用したいサーバーを選択してください。サーバーの設定タブで、**Issuer** と **Metadata URI** の値をコピーします:

[← Back to Authorization Servers](#)

default

[? Help](#)

Active ▾

- Settings**
- Scopes
- Claims
- Access Policies
- Token Preview

Settings		Edit
Name	default	
Audience	api://default	
Description	Default Authorization Server for your Applications	
Issuer	https:// it	.okta.com/oauth2/default
Metadata URI	https:// it/well-known/oauth-authorization-server	.okta.com/oauth2/default

Authorization Servers

An authorization server defines your security boundary, and is used to mint access and identity tokens for use with OIDC clients and OAuth 2.0 service accounts when accessing your resources via API. Within each authorization server you can define your own OAuth scopes, claims, and access policies. Read more at [help page](#)

Okta Authorization Server Settings

次のステップで両方の値を使用する必要があります。

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。次のフィールドを設定するために、Bitwardenウェブアプリに戻ってください：

フィールド	説明
権限	あなたの認証サーバーのための取得した発行者URIを入力してください。
クライアントID	あなたのOktaアプリの取得したクライアントIDを入力してください。

フィールド	説明
クライアントシークレット	あなたのOktaアプリの取得したクライアントシークレットを入力してください。
メタデータアドレス	あなたの認証サーバーのための取得したメタデータURIを入力してください。
OIDCリダイレクトの挙動	リダイレクト GET を選択します。現在、OktaはフォームPOSTをサポートしていません。
ユーザー情報エンドポイントからクレームを取得する	このオプションを有効にすると、URLが長すぎるエラー（HTTP 414）、切り捨てられたURL、および/またはSSO中の失敗が発生した場合に対応します。
追加/カスタムスコープ	リクエストに追加するカスタムスコープを定義します（カンマ区切り）。
追加/カスタムユーザーIDクレームタイプ	ユーザー識別のためのカスタムクレームタイプキーを定義します（カンマ区切り）。定義された場合、カスタムクレームのタイプは、標準のタイプに戻る前に検索されます。
追加/カスタム メールアドレス クレーム タイプ	ユーザーのメールアドレスのためのカスタムクレームタイプキーを定義します（カンマ区切り）。定義された場合、カスタムクレームタイプは、標準タイプに戻る前に検索されます。
追加/カスタム名前クレームタイプ	ユーザーのフルネームまたは表示名のためのカスタムクレームタイプキーを定義します（カンマ区切り）。定義された場合、カスタムクレームのタイプは、標準のタイプに戻る前に検索されます。
要求された認証コンテキストクラス参照値	認証コンテキストクラス参照識別子（ <code>acr_values</code> ）（スペース区切り）を定義してください。リスト <code>acr_values</code> を優先順位で並べてください。
応答で期待される "acr" 請求値	Bitwardenが応答で期待し、検証する <code>acr</code> クレーム値を定義してください。

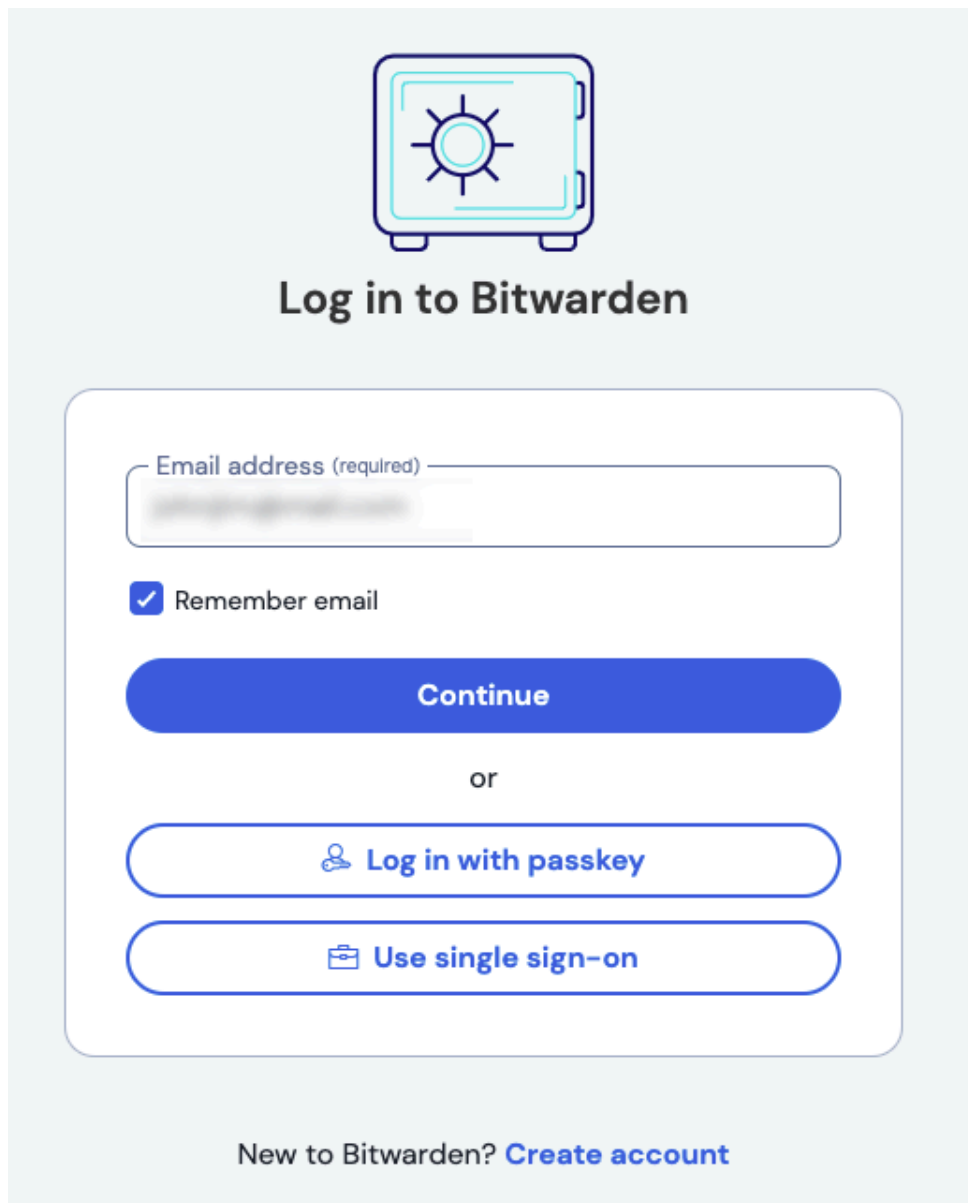
これらのフィールドの設定が完了したら、**保存**してください。

💡 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

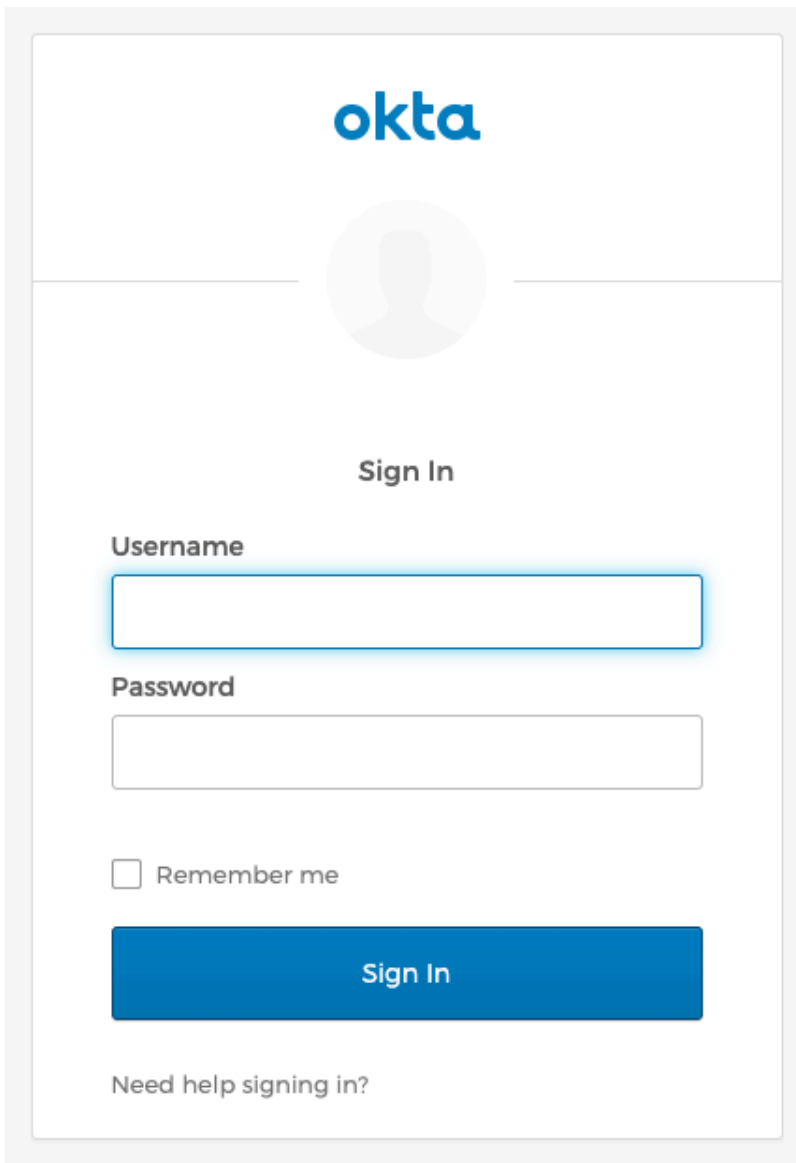
Continue

or

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。



The image shows a screenshot of the Okta Sign In page. At the top, the Okta logo is displayed in blue. Below the logo is a circular placeholder for a user profile picture. Underneath the profile picture, the text "Sign In" is centered. The form contains two input fields: "Username" and "Password". Below the password field is a checkbox labeled "Remember me". At the bottom of the form is a large blue button with the text "Sign In". Below the button, there is a link that says "Need help signing in?".

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！

① 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.