

CONSOLE ADMIN > IDENTIFIEZ-VOUS AVEC SSO >

# Mise en œuvre d'Okta OIDC

## Mise en œuvre d'Okta OIDC

Cet article contient de l'aide **spécifique à Okta** pour configurer l'identifiant avec SSO via OpenID Connect (OIDC). Pour obtenir de l'aide sur la configuration de l'identifiant avec SSO pour un autre IdP OIDC, ou pour configurer Okta via SAML 2.0, voir [Configuration OIDC](#) ou [Implémentation Okta SAML](#).

La configuration implique de travailler simultanément dans l'application web Bitwarden et le portail admin Okta. Au fur et à mesure que vous avancez, nous vous recommandons d'avoir les deux facilement disponibles et de compléter les étapes dans l'ordre où elles sont documentées.

### Ouvrez SSO dans le coffre web

Connectez-vous à l'application web Bitwarden et ouvrez la console Admin à l'aide du sélecteur de produit (☰):

| <input type="checkbox"/> | All | Name                                      | Owner         |   |
|--------------------------|-----|-------------------------------------------|---------------|---|
| <input type="checkbox"/> |     | <b>Company Credit Card</b><br>Visa, *4242 | My Organiz... | ⋮ |
| <input type="checkbox"/> |     | <b>Personal Login</b><br>myusername       | Me            | ⋮ |
| <input type="checkbox"/> |     | <b>Secure Note</b>                        | Me            | ⋮ |
| <input type="checkbox"/> |     | <b>Shared Login</b><br>sharedusername     | My Organiz... | ⋮ |

*commutateur-de-produit*

Sélectionnez **Paramètres** → **Connexion unique** depuis la navigation :

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)

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 configuration

Callback path

Signed out callback path

Configuration OIDC

Si vous ne l'avez pas déjà fait, créez un **identifiant SSO** unique pour votre organisation. Sinon, vous n'avez pas besoin d'éditer quoi que ce soit sur cet écran pour l'instant, mais gardez-le ouvert pour une référence facile.



Il existe des options alternatives de **décryptage des membres**. Apprenez comment commencer à utiliser [SSO avec des appareils de confiance](#) ou [Key Connector](#).

## Créez une application Okta

Dans le Portail Admin Okta, sélectionnez **Applications** → **Applications** depuis la navigation. Sur l'écran des Applications, sélectionnez le bouton **Créer une Intégration d'Application**. Pour la méthode de connexion, sélectionnez **OIDC - OpenID Connect**. Pour le type d'application, sélectionnez **Application Web**:

## 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

Sur l'écran **Intégration de la nouvelle application Web**, configurez les champs suivants :

| Champ                                 | Description                                           |
|---------------------------------------|-------------------------------------------------------|
| Nom de l'intégration de l'application | Donnez à l'application un nom spécifique à Bitwarden. |

| Champ                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type de subvention                 | Activez les <a href="#">types de subventions</a> suivants : <ul style="list-style-type: none"><li>- Client agissant en son propre nom → <b>Identifiants du client</b></li><li>- Client agissant au nom d'un utilisateur → <b>Code d'autorisation</b></li></ul>                                                                                                                                                                                                                                                                                                                                                 |
| URI de redirection de connexion    | Définissez ce champ sur votre <b>Chemin de rappel</b> , qui peut être récupéré à partir de l'écran de configuration SSO de Bitwarden.<br><br>Pour les clients hébergés dans le cloud, c'est <a href="https://sso.bitwarden.com/oidc-signin">https://sso.bitwarden.com/oidc-signin</a> ou <a href="https://sso.bitwarden.eu/oidc-signin">https://sso.bitwarden.eu/oidc-signin</a> . Pour les instances auto-hébergées, cela est déterminé par votre <a href="#">URL de serveur configurée</a> , par exemple <a href="https://votre.domaine.com/sso/oidc-signin">https://votre.domaine.com/sso/oidc-signin</a> . |
| URIs de redirection de déconnexion | Définissez ce champ sur votre <b>Chemin de rappel déconnecté</b> , qui peut être récupéré à partir de l'écran de configuration SSO de Bitwarden.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Devoirs                            | Utilisez ce champ pour désigner si tous ou seulement certains groupes pourront utiliser l'identifiant Bitwarden avec SSO.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

Une fois configuré, sélectionnez le bouton **Suivant**.

## Obtenez les identifiants du client

Sur l'écran de l'Application, copier l'**ID du client** et le **Secret du client** pour l'application Okta nouvellement créée :



# 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

Vous devrez utiliser les deux valeurs lors d'une étape ultérieure.

### Obtenez des informations sur le serveur d'autorisation

Sélectionnez **Sécurité** → **API** dans la navigation. Dans la liste des **Serveurs d'autorisation**, sélectionnez le serveur que vous souhaitez utiliser pour cette mise en œuvre. Sur l'**onglet Paramètres** du serveur, copiez les valeurs **Émetteur** et **URI de Métadonnées** :

[← 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://<br>it                                       | .okta.com/oauth2/default |
| Metadata URI | https://<br>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

Vous devrez utiliser les deux valeurs lors de la prochaine étape.

## Retour à l'application web

À ce stade, vous avez configuré tout ce dont vous avez besoin dans le contexte du Portail Admin Okta. Revenez à l'application web Bitwarden pour configurer les champs suivants :

| Champ     | Description                                                             |
|-----------|-------------------------------------------------------------------------|
| Autorité  | Entrez le URI de l'émetteur récupéré pour votre serveur d'autorisation. |
| Client ID | Entrez l'ID Client récupéré pour votre application Okta.                |

| Champ                                                                                         | Description                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Secret du Client                                                                              | Entrez le <a href="#">secret du client récupéré</a> pour votre application Okta.                                                                                                                                                                                                          |
| Adresse des métadonnées                                                                       | Entrez le <a href="#">URI des métadonnées récupérées</a> pour votre serveur d'autorisation.                                                                                                                                                                                               |
| Comportement de redirection OIDC                                                              | Sélectionnez <b>Rediriger GET</b> . Okta ne prend actuellement pas en charge Form POST.                                                                                                                                                                                                   |
| Obtenir des revendications à partir du point de terminaison des informations de l'utilisateur | Activez cette option si vous recevez des erreurs d'URL trop longues (HTTP 414), des URLs tronquées, et/ou des échecs lors de l'SSO.                                                                                                                                                       |
| Scopes supplémentaires/personnalisés                                                          | Définissez des portées personnalisées à ajouter à la demande (séparées par des virgules).                                                                                                                                                                                                 |
| Types de revendications d'ID utilisateur supplémentaires/personnalisés                        | Définissez des clés de type de revendication personnalisées pour l'identification de l'utilisateur (délimitées par des virgules). Lorsqu'ils sont définis, les types de revendications personnalisés sont recherchés avant de se rabattre sur les types standard.                         |
| Types de revendications de courriel supplémentaires/personnalisées                            | Définissez des clés de type de revendication personnalisées pour les adresses de courriel des utilisateurs (délimitées par des virgules). Lorsqu'ils sont définis, les types de revendications personnalisés sont recherchés avant de se rabattre sur les types standard.                 |
| Types de revendications de noms supplémentaires/personnalisés                                 | Définissez des clés de type de revendication personnalisées pour les noms complets ou les noms d'affichage des utilisateurs (délimités par des virgules). Lorsqu'ils sont définis, les types de revendications personnalisés sont recherchés avant de se rabattre sur les types standard. |
| Valeurs de référence de la classe de contexte d'authentification demandées                    | Définissez les identifiants de référence de classe de contexte d'authentification ( <a href="#">acr_values</a> ) (séparés par des espaces). Listez <a href="#">acr_values</a> dans l'ordre de préférence.                                                                                 |



| Champ                                             | Description                                                                                              |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Valeur de revendication "acr" attendue en réponse | Définissez la valeur de revendication <b>acr</b> que Bitwarden doit attendre et valider dans la réponse. |

Lorsque vous avez terminé de configurer ces champs, **Enregistrez** votre travail.

### 💡 Tip

Vous pouvez exiger que les utilisateurs se connectent avec SSO en activant la politique d'authentification à connexion unique. Veuillez noter que cela nécessitera également l'activation de la politique de sécurité de l'organisation unique. [En savoir plus.](#)

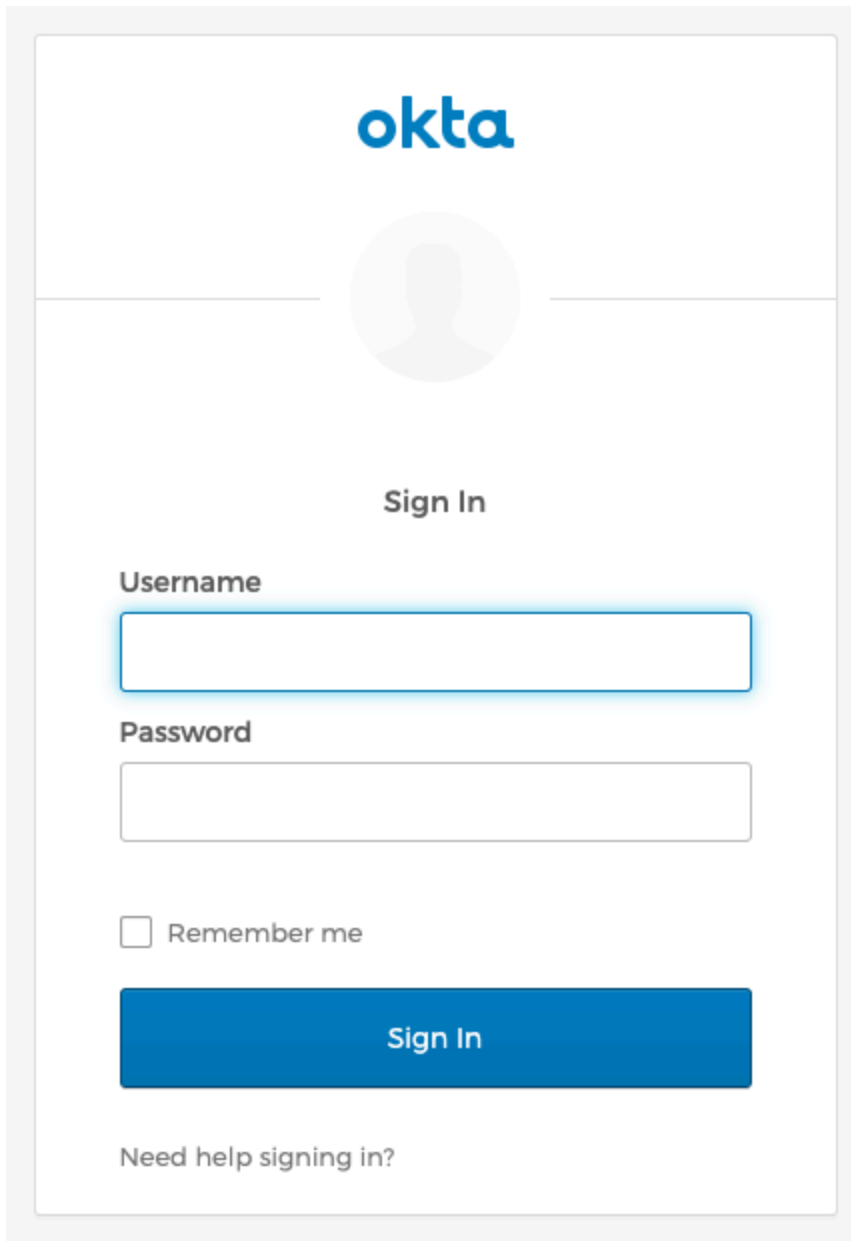
## Testez la configuration

Une fois votre configuration terminée, testez-la en vous rendant sur <https://vault.bitwarden.com>, en entrant votre adresse de courriel, en sélectionnant **Continuer**, et en sélectionnant le bouton **Connexion unique d'Entreprise** :

The screenshot shows the Bitwarden login interface. At the top is the Bitwarden logo and the text "Log in". Below this is a form with a "Master password (required)" input field. The field is empty and has a red border, with a red error message "Input is required." below it. To the right of the input field is an eye icon for toggling visibility. Below the error message is a link "Get master password hint". There are two buttons: a blue "Log in with master password" button and a white "Enterprise single sign-on" button with a briefcase icon. At the bottom, it says "Logging in as myemailaddress@bitwarden.com" and a link "Not you?".

*Connexion unique d'entreprise et mot de passe principal*

Entrez l'identifiant de l'organisation configuré et sélectionnez **Se connecter**. Si votre mise en œuvre est configurée avec succès, vous serez redirigé vers l'écran d'identifiant Okta:



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. There are two input fields: "Username" and "Password". Below the "Password" field is a checkbox labeled "Remember me". At the bottom of the form is a blue button labeled "Sign In". Below the button, the text "Need help signing in?" is visible.

*Log in with Okta*

Après vous être authentifié avec vos identifiants Okta, entrez votre mot de passe principal Bitwarden pour déchiffrer votre coffre !

### 📌 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.