

CONSOLE ADMIN > IDENTIFIEZ-VOUS AVEC SSO >

Implémentation SAML Auth0

Afficher dans le centre d'aide:
<https://bitwarden.com/help/saml-auth0/>

Implémentation SAML Auth0

Cet article contient de l'aide **spécifique à Auth0** pour configurer l'identifiant avec SSO via SAML 2.0. Pour obtenir de l'aide sur la configuration de l'identifiant avec SSO pour un autre IdP, reportez-vous à [Configuration SAML 2.0](#).

La configuration implique de travailler simultanément dans l'application web Bitwarden et le portail Auth0. Au fur et à mesure que vous avancez, nous vous recommandons d'avoir les deux à portée de main et de compléter les étapes dans l'ordre où elles sont documentées.

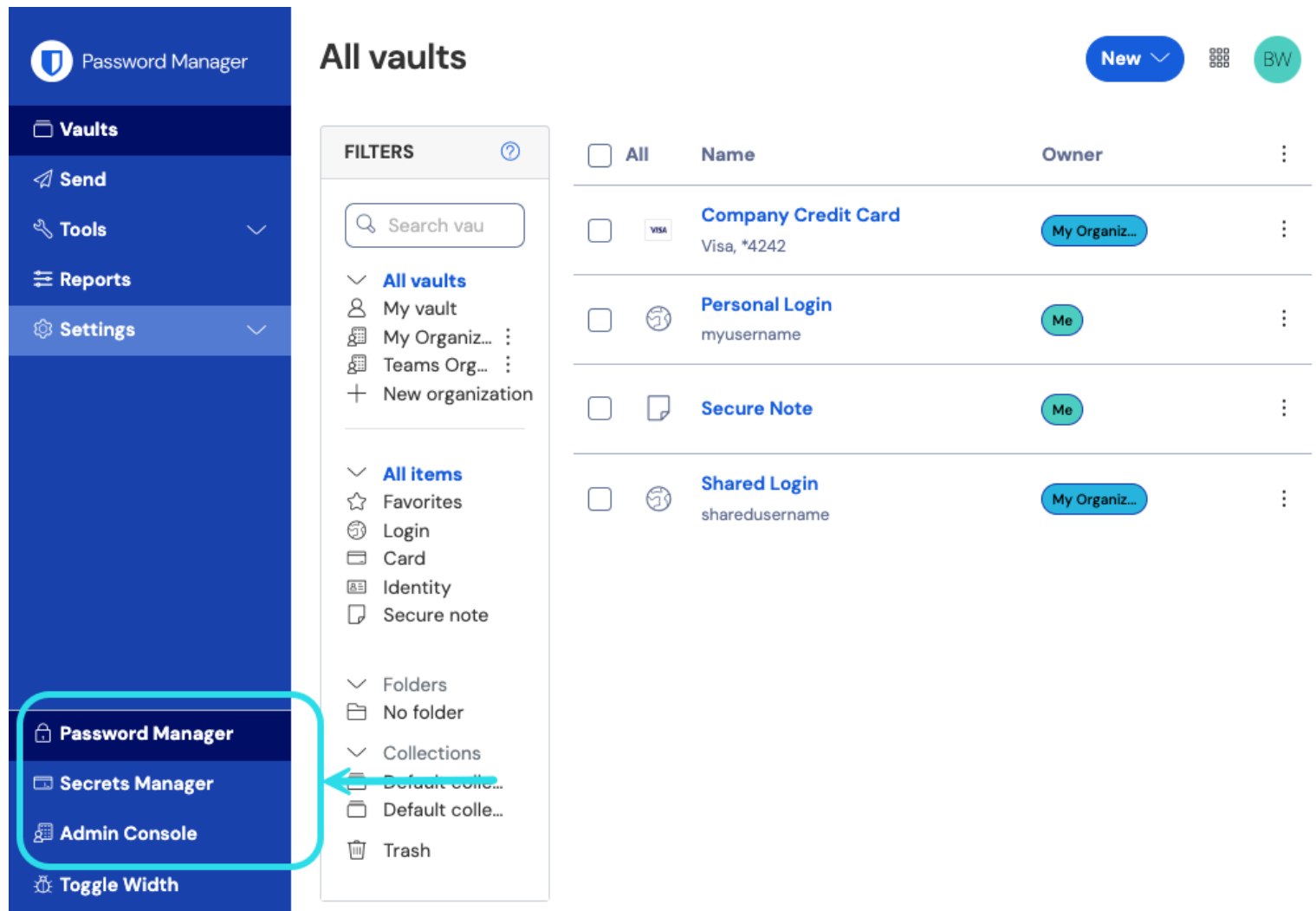


Already an SSO expert? Skip the instructions in this article and download screenshots of sample configurations to compare against your own.

[Download Sample](#)

Ouvrez SSO dans l'application web

Connectez-vous à l'application web Bitwarden et ouvrez la console Admin en utilisant le sélecteur de produit (🔲):



The screenshot shows the Bitwarden web application interface. On the left, there is a sidebar with the following items: Password Manager, Secrets Manager, Admin Console, and Toggle Width. The 'Password Manager' item is highlighted with a red box. In the main area, the 'All vaults' page is displayed. It features a 'FILTERS' section on the left with a search bar and a list of filters: All vaults, My vault, My Organiz..., Teams Org..., New organization, All items, Favorites, Login, Card, Identity, Secure note, Folders, No folder, Collections, Default colle..., Default colle..., and Trash. The main table lists vaults with columns for Name and Owner. The vaults listed are: Company Credit Card (Owner: My Organiz...), Personal Login (Owner: Me), Secure Note (Owner: Me), and Shared Login (Owner: My Organiz...). A red arrow points to the 'Default collection' in the left sidebar.

commutateur-de-produit

Ouvrez l'écran **Paramètres** → **Connexion unique** de votre organisation :



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

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.

☐ 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

SAML 2.0 metadata URL

Configuration SAML 2.0

Si vous ne l'avez pas déjà fait, créez un **identifiant SSO** unique pour votre organisation et sélectionnez **SAML** dans le menu déroulant **Saisir**. Gardez cet écran ouvert pour une référence facile.

Vous pouvez désactiver l'option **Définir un ID d'entité SP unique** à ce stade si vous le souhaitez. Ce faisant, cela supprimera votre ID d'organisation de la valeur de votre ID d'entité SP, cependant dans presque tous les cas, il est recommandé de laisser cette option activée.



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 Auth0

Dans le portail Auth0, utilisez le menu Applications pour créer une **Application Web Régulière** :

 dev-hn11g2a6
Development

Q Discuss your needs Docs  FS



 Thank you for purchasing the Free Auth0 plan. You have 22 days left in your trial to experiment with [features that are not in the Free plan](#). Like what you're seeing? Please enter your [billing information here](#). [BILLING](#)

Applications

Setup a mobile, web or IoT application to use Auth0 for Authentication. [Learn more](#) ▶

 **Default App**
Generic

Client ID: `RM3UeXnRtL8CSjPPCg7HiitjInvQs0Be` 



 [+ CREATE APPLICATION](#)

Auth0 Create Application

Cliquez sur l'**onglet Paramètres** et configurez les informations suivantes, dont certaines que vous devrez récupérer à partir de l'écran de connexion unique Bitwarden :

Basic Information

Name *

Bitwarden Login with SSO

Domain

.us.auth0.com

Client ID

HcoxD53h7Qz1520u8pabhPWozEG0Hho2

Client Secret

.....

The Client Secret is not base64 encoded.

Auth0 Settings

Paramètres Auth0	Description
Nom	Donnez à l'application un nom spécifique à Bitwarden.
Domaine	Prenez note de cette valeur. Vous en aurez besoin lors d'une étape ultérieure.
Type d'application	Sélectionnez Application Web Régulière .
Méthode d'authentification du point de terminaison du jeton	Sélectionnez Post (HTTP Post), qui sera mappé à un attribut de Type de Liaison que vous allez configurer plus tard.

Paramètres Auth0	Description
URI d'identifiant de l'application	Définissez ce champ sur l' ID d'entité SP pré-généré. Cette valeur générée automatiquement peut être copiée à partir de l'écran Paramètres → Connexion unique de votre organisation et variera en fonction de votre configuration.
URLS de rappel autorisés	Définissez ce champ sur l'URL du Service de Consommation d'Assertion (ACS) pré-généré. Cette valeur générée automatiquement peut être copiée à partir de l'écran Paramètres → Connexion unique de votre organisation et variera en fonction de votre configuration.

Types de Subventions

Dans la section **Paramètres Avancés** → **Types de Subventions**, assurez-vous que les types de subventions suivants sont sélectionnés (ils peuvent être pré-sélectionnés):

Advanced Settings

Application Metadata

Device Settings

OAuth

Grant Types

WS-Federation

Certificates

Grants

☒ Implicit

☒ Authorization Code

☒ Refresh Token

☒ Client Credentials

☐ Password

☐ MFA

☐ Passwordless OTP

Application Grant Types

Certificats

Dans la section **Paramètres Avancés** → **Certificats**, copiez ou téléchargez votre certificat de signature. Vous n'aurez pas besoin de faire quoi que ce soit avec pour l'instant, mais vous devrez vous y [référer plus tard](#).

Advanced Settings

[Application Metadata](#)
[Device Settings](#)
[OAuth](#)
[Grant Types](#)
[WS-Federation](#)
[Certificates](#)

Signing Certificate

```
-----BEGIN CERTIFICATE-----
MIIDDTCCAFWgAwIBAgIJdp2+Lsu8IyKcMA0GCSqGSIb3DQEBCwUAMCQxIjAgBgNV
BAMTGWRldi1objExZzZjJhNi51cy5hdXRoMC5jb20wHhcNMjEwMTUxMjUxWhcN
MzQxMjIzMTUxMjUxWjAkMSIwIAYDVQQDExlkZXYtaG4xMWcyYTYudXMUyXV0aDAu
Y29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2yRfsSC5LCYkTvuF
nCW0wCEE7jkTtdxRGytTBwJEaqzmgMzktBmkU0BfuzjrtcaQx0utRM679AD0PX9
WZLqw1CErdeKP01S3/TvqkNkPyf2UE27Qo4giJy6FEUAgsqwTs/gtX6sxIogeH0N
cJ95strc/F+jtw17Tukul1x4nv3TcvK115TZRA38bW/J7Q61QC3MSMS2FG3D/hDi
-----
```



AuthO Certificate

Points finaux

Vous n'avez pas besoin d'éditer quoi que ce soit dans la section **Paramètres Avancés** → **Points de terminaison**, mais vous aurez besoin des points de terminaison SAML pour [référence ultérieure](#).



Tip

In smaller windows, the **Endpoints** tab can disappear behind the edge of the browser. If you're having trouble finding it, click the **Certificates** tab and hit the Right Arrow key (→).

Advanced Settings

MetadataDevice SettingsOAuthGrant TypesWS-FederationCertificatesEndpoints

OAuth

OAuth Authorization URL

https://dev-hn11g2a6.us.auth0.com/authorize

Device Authorization URL

https://dev-hn11g2a6.us.auth0.com/oauth/device/code

Auth0 Endpoints

Configurer les règles Auth0

Créez des règles pour personnaliser le comportement de la réponse SAML de votre application. Bien qu'Auth0 offre [un certain nombre d'options](#), cette section se concentrera uniquement sur celles qui correspondent spécifiquement aux options de Bitwarden. Pour créer un ensemble de règles de configuration SAML personnalisé, utilisez le menu **Pipeline d'Authentification** → **Règles** pour **+ Créer des Règles** :



dev-hn11g2a6

Development



Discuss your needs

 Docs



 FS





Thank you for purchasing the Free Auth0 plan. You have 21 days left in your trial to experiment with [features that are not in the Free plan](#). Like what you're seeing? Please enter your [billing information here](#).

BILLING

Rules

+ CREATE

Custom Javascript snippets that run in a secure, isolated sandbox in the Auth0 service as part of your authentication pipeline. [Learn more](#)

TRY ALL RULES WITH...
REFRESH

Custom SAML Config



Auth0 Rules

Vous pouvez configurer l'un des éléments suivants :

Clé	Description
algorithme de signature	Algorithme que Auth0 utilisera pour signer l'assertion ou la réponse SAML. Par défaut, rsa-sha1 sera inclus, cependant, cette valeur doit être définie sur rsa-sha256. Si vous modifiez cette valeur, vous devez : -Définissez digestAlgorithm sur sha256. -Définissez (dans Bitwarden) l'Algorithme de Signature Entrant Minimum sur rsa-sha256.
algorithme Digest	Algorithme utilisé pour calculer le condensé de l'assertion ou de la réponse SAML. Par défaut, sha-1. La valeur pour signatureAlgorithm, doit également être définie sur sha256.
signeRéponse	Par défaut, Auth0 ne signera que l'assertion SAML. Définissez ceci sur vrai pour signer la réponse SAML au lieu de l'affirmation.

Clé	Description
<code>formatIdentifiantNom</code>	Par défaut, <code>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</code> . Vous pouvez définir cette valeur sur n'importe quel format de NameID SAML. Si vous le faites, changez le champ SP Format d'ID de nom à l'option correspondante (voir ici).

Mettez en œuvre ces règles à l'aide d'un **Script** comme celui ci-dessous. Pour obtenir de l'aide, référez-vous à la [Documentation d'Auth0](#).

Bash

```
function (user, context, callback) {
  context.samlConfiguration.signatureAlgorithm = "rsa-sha256";
  context.samlConfiguration.digestAlgorithm = "sha256";
  context.samlConfiguration.signResponse = "true";
  context.samlConfiguration.nameIdentifierFormat = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress";
  context.samlConfiguration.binding = "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect";
  callback(null, user, context);
}
```

Retour à l'application web

À ce stade, vous avez configuré tout ce dont vous avez besoin dans le contexte du portail Auth0. Retournez à l'application web Bitwarden pour terminer la configuration.

L'écran de connexion unique sépare la configuration en deux sections :

- La configuration du fournisseur de services SAML déterminera le format des requêtes SAML.
- La configuration du fournisseur d'identité SAML déterminera le format à attendre pour les réponses SAML.

Configuration du fournisseur de services

À moins que vous n'ayez configuré des [règles personnalisées](#), la configuration de votre fournisseur de services sera déjà terminée. Si vous avez configuré des règles personnalisées ou souhaitez apporter d'autres modifications à votre mise en œuvre, éditez les champs pertinents :

Champ	Description
Format de l'identifiant de nom	Format NameID à spécifier dans la demande SAML (Politique NameID). Pour omettre, définissez sur Non Configuré .

Champ	Description
Algorithme de Signature Sortant	Algorithme utilisé pour signer les requêtes SAML, par défaut rsa-sha256 .
Comportement de signature	Si/quand les demandes SAML de Bitwarden seront signées. Par défaut, AuthO n'exigera pas que les requêtes soient signées.
Algorithme de Signature Minimum Entrant	L'algorithme de signature minimum que Bitwarden acceptera dans les réponses SAML. Par défaut, AuthO signera avec rsa-sha1 . Sélectionnez rsa-sha256 dans le menu déroulant à moins que vous n'ayez configuré une règle de signature personnalisée .
Voulez-vous des affirmations signées	Que Bitwarden souhaite des assertions SAML signées. Par défaut, AuthO signera les assertions SAML, alors cochez cette case à moins que vous n'ayez configuré une règle de signature personnalisée .
Valider les Certificats	Cochez cette case lorsque vous utilisez des certificats fiables et valides de votre IdP via une CA de confiance. Les certificats auto-signés peuvent échouer à moins que des chaînes de confiance appropriées ne soient configurées dans l'image Docker de Bitwarden Identifiant avec SSO.

Lorsque vous avez terminé avec la configuration du fournisseur de services, **Enregistrez** votre travail.

Configuration du fournisseur d'Identité

La configuration du fournisseur d'Identité nécessitera souvent que vous vous référiez au Portail AuthO pour récupérer les valeurs de l'application :

Champ	Description
ID de l'entité	Entrez la valeur du Domaine de votre application AuthO (voir ici), précédée de urn: , par exemple urn:bw-help.us.auth0.com . Ce champ est sensible à la casse.
Type de Reliure	Sélectionnez HTTP POST pour correspondre à la valeur de la Méthode d'Authentification de l'Endpoint du Jeton spécifiée dans votre application AuthO.

Champ	Description
URL du service de connexion unique	Entrez l' URL du protocole SAML (voir Points de terminaison) de votre application AuthO. Par exemple, https://bw-help.us.auth0.com/samlp/HcpxD63h7Qz1420u8qachPWozEG0Hho2 .
URL du service de déconnexion unique	L'identification avec SSO ne prend actuellement pas en charge SLO. Cette option est prévue pour un développement futur, cependant vous pouvez la pré-configurer si vous le souhaitez.
Certificat Public X509	Collez le certificat de signature récupéré, en supprimant -----DÉBUT DU CERTIFICAT----- et -----FIN DU CERTIFICAT----- La valeur du certificat est sensible à la casse, les espaces supplémentaires, les retours à la ligne et autres caractères superflus entraîneront l'échec de la validation du certificat .
Algorithme de Signature Sortant	Par défaut, AuthO signera avec rsa-sha1 . Sélectionnez rsa-sha256 sauf si vous avez configuré une règle de signature personnalisée .
Désactiver les demandes de déconnexion sortantes	La connexion avec SSO ne prend actuellement pas en charge SLO. Cette option est prévue pour un développement futur.
Voulez-vous que les demandes d'authentification soient signées	Que AuthO s'attend à ce que les demandes SAML soient signées.

Note

Lors de la complétion du certificat X509, prenez note de la date d'expiration. Les certificats devront être renouvelés afin d'éviter toute interruption de service pour les utilisateurs finaux de SSO. Si un certificat a expiré, les comptes Admin et Propriétaire pourront toujours se connecter avec l'adresse de courriel et le mot de passe principal.

Lorsque vous avez terminé avec la configuration du fournisseur d'identité, **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** :



Log in to Bitwarden

Email address (required) ☒ Remember email**Continue**

or



Log in with passkey

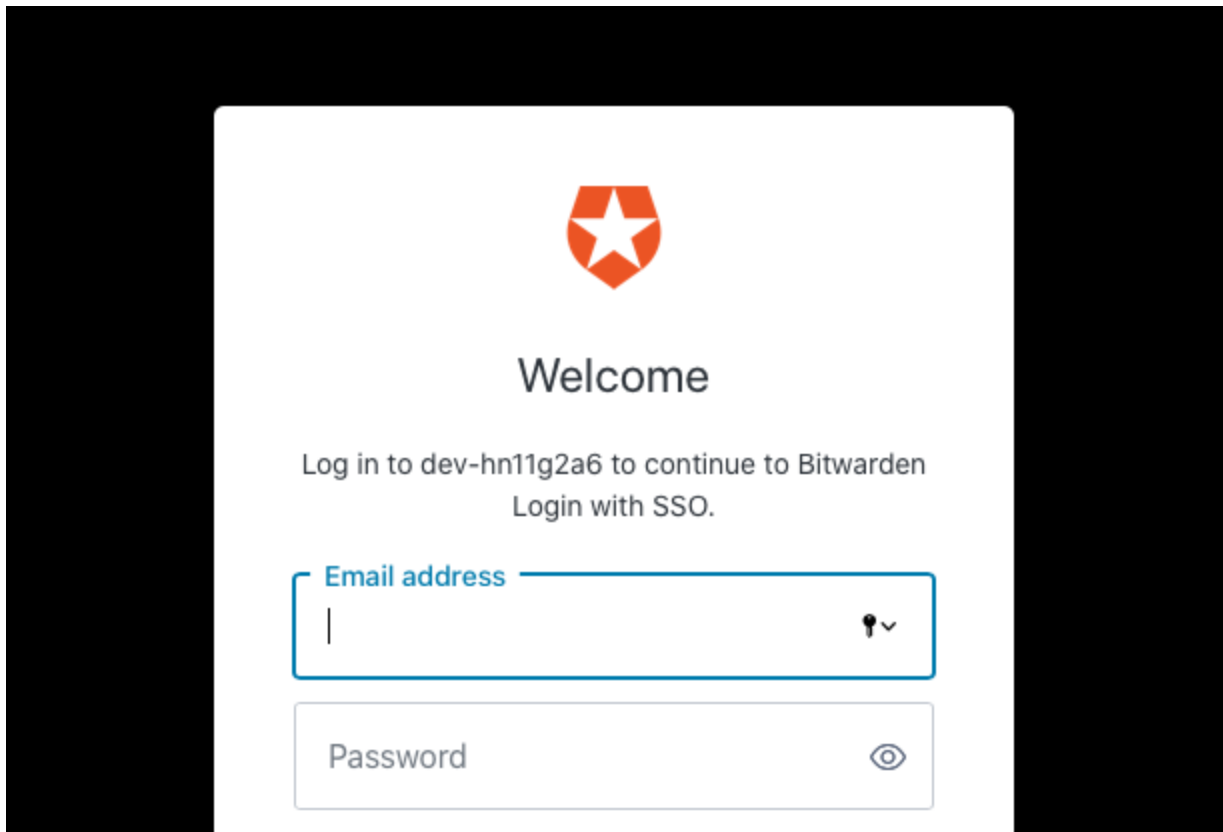


Use single sign-on

New to Bitwarden? [Create account](#)

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 correctement configurée, vous serez redirigé vers l'écran d'identifiant Auth0 :



AuthO Login

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

Note

Bitwarden ne prend pas en charge les réponses non sollicitées, donc l'initiation de l'identifiant à partir de votre IdP entraînera une erreur. Le flux d'identifiant SSO doit être initié à partir de Bitwarden.