

ADMINISTRATOR KONSOLE > MELDEN SIE SICH MIT SSO AN >

Auth0 SAML Implementierung

Auth0 SAML Implementierung

Dieser Artikel enthält **Auth0-spezifische** Hilfe zur Konfiguration der Zugangsdaten mit SSO über SAML 2.0. Für Hilfe bei der Konfiguration der Zugangsdaten mit SSO für einen anderen IdP, verweisen Sie auf [SAML 2.0 Konfiguration](#).

Die Konfiguration beinhaltet die gleichzeitige Arbeit innerhalb der Bitwarden-Web-App und des Auth0-Portals. Während Sie fortfahren, empfehlen wir, beides griffbereit zu haben und die Schritte in der Reihenfolge durchzuführen, in der sie dokumentiert sind.

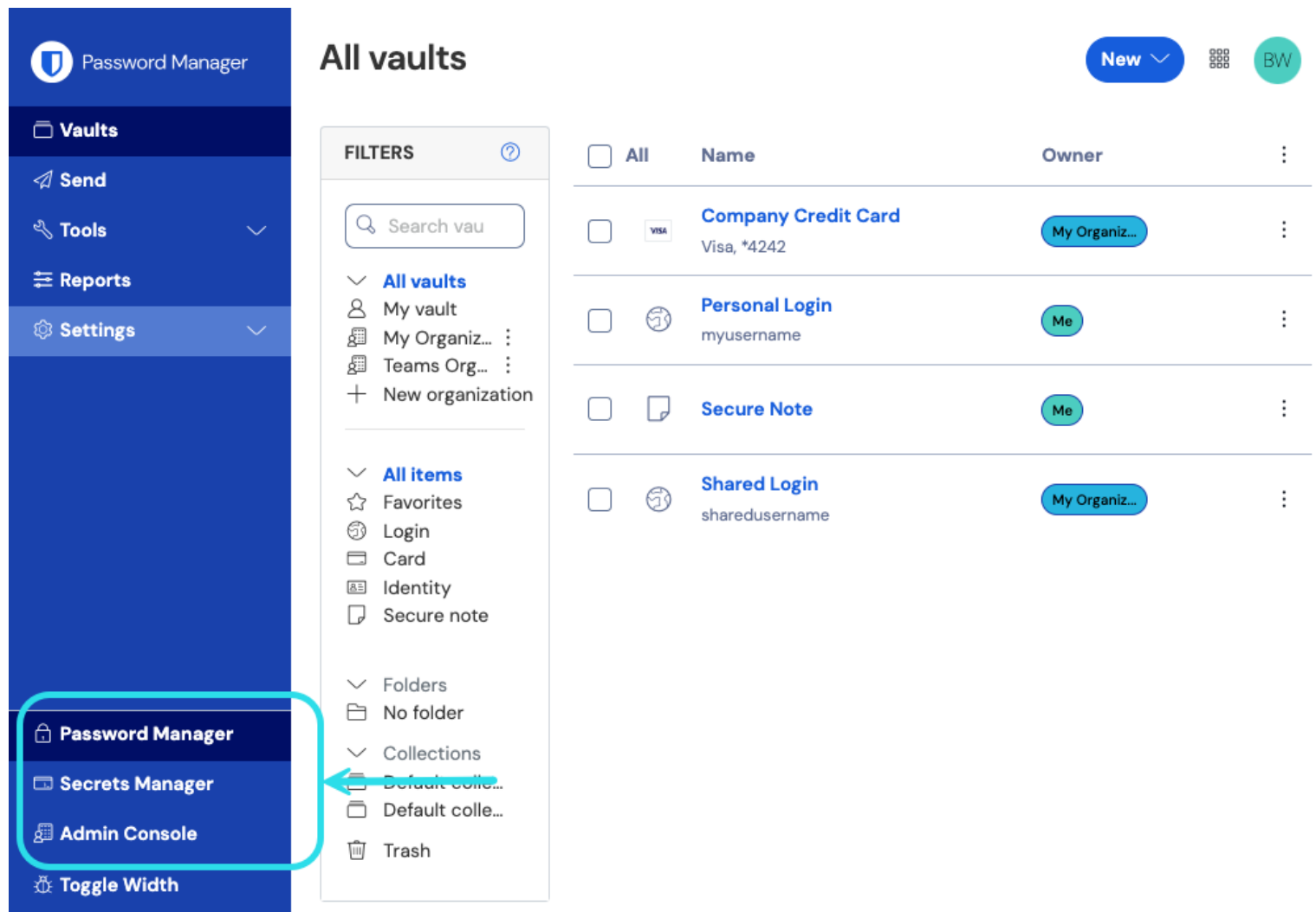


Already an SSO expert? Skip the instructions in this article and download screenshots of sample configurations to compare against your own.

[Download Sample](#)

Öffnen Sie SSO in der Web-App

Melden Sie sich bei der Bitwarden-Web-App an und öffnen Sie die Administrator-Konsole mit dem Produktschalter :



Product switcher

Öffnen Sie die **Einstellungen** Ihrer Organisation → **Einmaliges Anmelden** Bildschirm:



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

SAML 2.0 metadata URL

SAML 2.0 Konfiguration

Wenn Sie es noch nicht getan haben, erstellen Sie einen einzigartigen **SSO-Identifikator** für Ihre Organisation und wählen Sie **SAML** aus dem **Typ**-Dropdown aus. Lassen Sie diesen Bildschirm geöffnet, um leicht darauf zugreifen zu können.

Sie können die Option **Legen Sie eine eindeutige SP-Entitäts-ID fest** in diesem Stadium ausschalten, wenn Sie möchten. Wenn Sie dies tun, wird Ihre Organisations-ID aus Ihrem SP-Entity-ID-Wert entfernt. In fast allen Fällen wird jedoch empfohlen, diese Option aktiviert zu lassen.



Es gibt alternative **Mitglied Entschlüsselungsoptionen**. Erfahren Sie, wie Sie mit [SSO auf vertrauenswürdigen Geräten](#) oder mit [Key Connector](#) beginnen können.

Erstellen Sie eine Auth0-Anwendung

Im Auth0 Portal verwenden Sie das Anwendungen-Menü, um eine **Reguläre Webanwendung** zu erstellen:

 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

Klicken Sie auf den **Einstellungen** Tab und konfigurieren Sie die folgenden Informationen, einige davon müssen Sie vom Bitwarden Single Sign-On Bildschirm abrufen:

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

Auth0 Einstellungen	Beschreibung
Name	Geben Sie der Anwendung einen Bitwarden-spezifischen Namen.
Domain	Nehmen Sie diese Notiz von diesem Wert. Sie werden es in einem späteren Schritt benötigen.
Anwendungstyp	Wählen Sie Reguläre Webanwendung .
Token-Endpunkt-Authentifizierungsmethode	Wählen Sie Post (HTTP Post), das einer Typ Bindung zugeordnet wird, die Sie später konfigurieren werden.

AuthO Einstellungen	Beschreibung
Anwendungs-Zugangsdaten URI	Setzen Sie dieses Feld auf die vorab generierte SP Entity ID. Dieser automatisch generierte Wert kann aus den Einstellungen → Single Sign-On der Organisation kopiert werden und variiert je nach Ihrer Konfiguration.
Erlaubte Callback-URLs	Setzen Sie dieses Feld auf die vorab generierte Assertion Consumer Service (ACS) URL. Dieser automatisch generierte Wert kann von der Einstellungen → Single Sign-On Bildschirm der Organisation kopiert werden und variiert je nach Ihrer Konfiguration.

Zuschusstypen

Im Abschnitt **Erweiterte Einstellungen → Genehmigungsarten**, stellen Sie sicher, dass die folgenden Genehmigungsarten ausgewählt sind (sie könnten bereits vorausgewählt sein):

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

Im Abschnitt **Erweiterte Einstellungen** → **Zertifikate**, kopieren oder laden Sie Ihr Signaturzertifikat hoch. Sie müssen noch nichts damit machen, aber Sie werden es später **referenzieren müssen**.

^

Certificates

Auth0 Certificate

Sie müssen nichts in dem Abschnitt **Erweiterte Einstellungen** → **Endpunkte** bearbeiten, aber Sie werden die SAML-Endpunkte benötigen, um sie **später zu referenzieren**.

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

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

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

Konfigurieren Sie Auth0-Regeln

Erstellen Sie Regeln, um das SAML-Antwortverhalten Ihrer Anwendung anzupassen. Während Auth0 eine [Nummer von Optionen](#) bietet, wird sich dieser Abschnitt nur auf diejenigen konzentrieren, die speziell auf Bitwarden Optionen abgestimmt sind. Um eine benutzerdefinierte SAML-Konfigurationsregelsatz zu erstellen, verwenden Sie das **Auth Pipeline → Regeln** Menü um **+ Regeln zu erstellen**:

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

Sie können eine der folgenden Optionen konfigurieren:

Schlüssel	Beschreibung
Signaturalgorithmus	Algorithmus, den Auth0 zur Signatur der SAML-Behauptung oder Antwort verwenden wird. Standardmäßig wird rsa-sha1 enthalten sein, jedoch sollte dieser Wert auf rsa-sha256 gesetzt werden. Wenn Sie diesen Wert ändern, müssen Sie: -Setzen Sie digestAlgorithm auf sha256. -Stellen Sie (in Bitwarden) den Mindesteingehenden Signaturalgorithmus auf rsa-sha256 ein.
Verdauungsalgorithmus	Algorithmus zur Berechnung des Digests einer SAML-Behauptung oder Antwort. Standardmäßig, sha-1. Der Wert für signatureAlgorithm sollte auch auf sha256 gesetzt werden.
Unterschrift Antwort	Standardmäßig wird Auth0 nur die SAML-Behauptung signieren. Setzen Sie dies auf true , um die SAML-Antwort anstelle der Behauptung zu signieren.

Schlüssel	Beschreibung
NameIdentifierFormat	Standardmäßig, <code>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</code> . Sie können diesen Wert auf jedes SAML NameID Format setzen. Wenn Sie dies tun, ändern Sie das Feld SP Name ID Format auf die entsprechende Option (siehe hier).

Setzen Sie diese Regeln mit einem **Skript** um, wie dem untenstehenden. Für Hilfe, siehe [AuthO's Dokumentation](#).

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);
}
```

Zurück zur Web-App

Bis zu diesem Zeitpunkt haben Sie alles, was Sie im Kontext des AuthO-Portals benötigen, konfiguriert. Kehren Sie zur Bitwarden-Webanwendung zurück, um die Konfiguration abzuschließen.

Der Single-Sign-On-Bildschirm teilt die Konfiguration in zwei Abschnitte auf:

- Die Konfiguration des **SAML-Dienstanbieters** bestimmt das Format der SAML-Anfragen.
- Durch die Konfiguration des SAML-Identitätsanbieters** wird das zu erwartende Format für SAML-Antworten bestimmt.

Konfiguration des Dienstanbieters

Sofern Sie keine [benutzerdefinierten Regeln](#) eingerichtet haben, ist Ihre Dienstanbieter-Konfiguration bereits abgeschlossen. Wenn Sie benutzerdefinierte Regeln konfiguriert haben oder weitere Änderungen an Ihrer Implementierung vornehmen möchten, bearbeiten Sie die relevanten Felder:

Feld	Beschreibung
Namens-ID-Format	NameID Format im SAML-Antrag anzugeben (NameIDPolicy). Zum Überspringen, setzen Sie auf Nicht konfiguriert .

Feld	Beschreibung
Ausgehendes Signatur-Algorithmus	Algorithmus, der zum Signieren von SAML-Anfragen verwendet wird, standardmäßig rsa-sha256 .
Unterzeichnungsverhalten	Ob/wann Bitwarden SAML-Anfragen signiert werden. Standardmäßig erfordert Auth0 keine Signatur für Anfragen.
Mindesteingehtender Signaturalgorithmus	Der Mindestsignaturalgorithmus, den Bitwarden in SAML-Antworten akzeptiert. Standardmäßig wird Auth0 mit rsa-sha1 signieren. Wählen Sie rsa-sha256 aus dem Dropdown-Menü, es sei denn, Sie haben eine benutzerdefinierte Signaturregel konfiguriert.
Möchte Behauptungen unterschrieben haben	Ob Bitwarden SAML-Behauptungen signiert haben möchte. Standardmäßig signiert Auth0 SAML-Behauptungen, also markieren Sie dieses Kästchen, es sei denn, Sie haben eine benutzerdefinierte Signaturregel konfiguriert.
Zertifikate validieren	Markieren Sie dieses Kästchen, wenn Sie vertrauenswürdige und gültige Zertifikate von Ihrem IdP über eine vertrauenswürdige CA verwenden. Selbstsignierte Zertifikate können fehlschlagen, es sei denn, die richtigen Vertrauensketten sind innerhalb des Bitwarden Zugangsdaten mit SSO Docker-Images konfiguriert.

Wenn Sie mit der Konfiguration des Dienstanbieters fertig sind, **speichern** Sie Ihre Arbeit.

Konfiguration des Identitätsanbieters

Die Konfiguration des Identitätsanbieters erfordert oft, dass Sie sich auf das Auth0-Portal beziehen, um Anwendungswerte abzurufen:

Feld	Beschreibung
Entitäts-ID	Geben Sie den Domain -Wert Ihrer Auth0-Anwendung ein (siehe hier), vorangestellt von urn: , zum Beispiel urn:bw-help.us.auth0.com . Dieses Feld ist Groß- und Kleinschreibungssensitiv.
Bindungsart	Wählen Sie HTTP POST , um den Token-Endpunkt-Authentifizierungsmethode Wert zu entsprechen, der in Ihrer Auth0-Anwendung angegeben ist.

Feld	Beschreibung
Einmaliges Anmelden Service URL	Geben Sie die SAML-Protokoll-URL (siehe Endpunkte) Ihrer AuthO-Anwendung ein. Zum Beispiel, https://bw-help.us.auth0.com/samlp/HcpxD63h7Qz1420u8qachPWozEG0Hho2 .
Einzel Abmelden Service URL	Die Anmeldung mit SSO unterstützt derzeit nicht SLO. Diese Option ist für zukünftige Entwicklungen geplant, jedoch können Sie sie vorab konfigurieren, wenn Sie möchten.
X509 Öffentliches Zertifikat	Fügen Sie das abgerufene Signaturzertifikat ein und entfernen Sie es. -----BEGIN ZERTIFIKAT----- und -----ENDE ZERTIFIKAT----- Der Zertifikatswert ist Groß- und Kleinschreibungssensitiv, zusätzliche Leerzeichen, Zeilenumbrüche und andere überflüssige Zeichen werden dazu führen, dass die Zertifikatsvalidierung fehlschlägt.
Ausgehendes Signaturverfahren	Standardmäßig wird AuthO mit rsa-sha1 signieren. Wählen Sie rsa-sha256 aus, es sei denn, Sie haben eine benutzerdefinierte Signaturregel konfiguriert.
Deaktivieren Sie ausgehende Abmeldeanfragen	Die Anmeldung mit SSO unterstützt derzeit nicht SLO. Diese Option ist für zukünftige Entwicklungen geplant.
Möchte Authentifizierungsanfragen signiert haben	Ob AuthO erwartet, dass SAML-Anfragen signiert werden.

Note

Bei der Ausstellung des X509-Zertifikats, machen Sie eine Notiz vom Ablaufdatum. Zertifikate müssen erneuert werden, um jegliche Unterbrechungen im Dienst für SSO-Endbenutzer zu verhindern. Wenn ein Zertifikat abgelaufen ist, können sich Administrator- und Eigentümer-Konten immer mit E-Mail-Adresse und Master-Passwort anmelden.

Wenn Sie mit der Konfiguration des Identitätsanbieters fertig sind, **speichern** Sie Ihre Arbeit.

 Tip

Sie können Benutzer dazu auffordern, sich mit SSO anzumelden, indem Sie die Richtlinie für die Authentifizierung mit Single Sign-On aktivieren. Bitte beachten Sie, dass dies auch die Aktivierung der Einzelorganisation-Richtlinie erfordern wird. [Erfahren Sie mehr.](#)

Testen Sie die Konfiguration

Sobald Ihre Konfiguration abgeschlossen ist, testen Sie diese, indem Sie zu <https://vault.bitwarden.com> navigieren, Ihre E-Mail-Adresse eingeben, **Weiter** auswählen und den **Enterprise Single-On** Button auswählen:



Log in to Bitwarden

Email address (required)

☒ Remember email

Continue

or

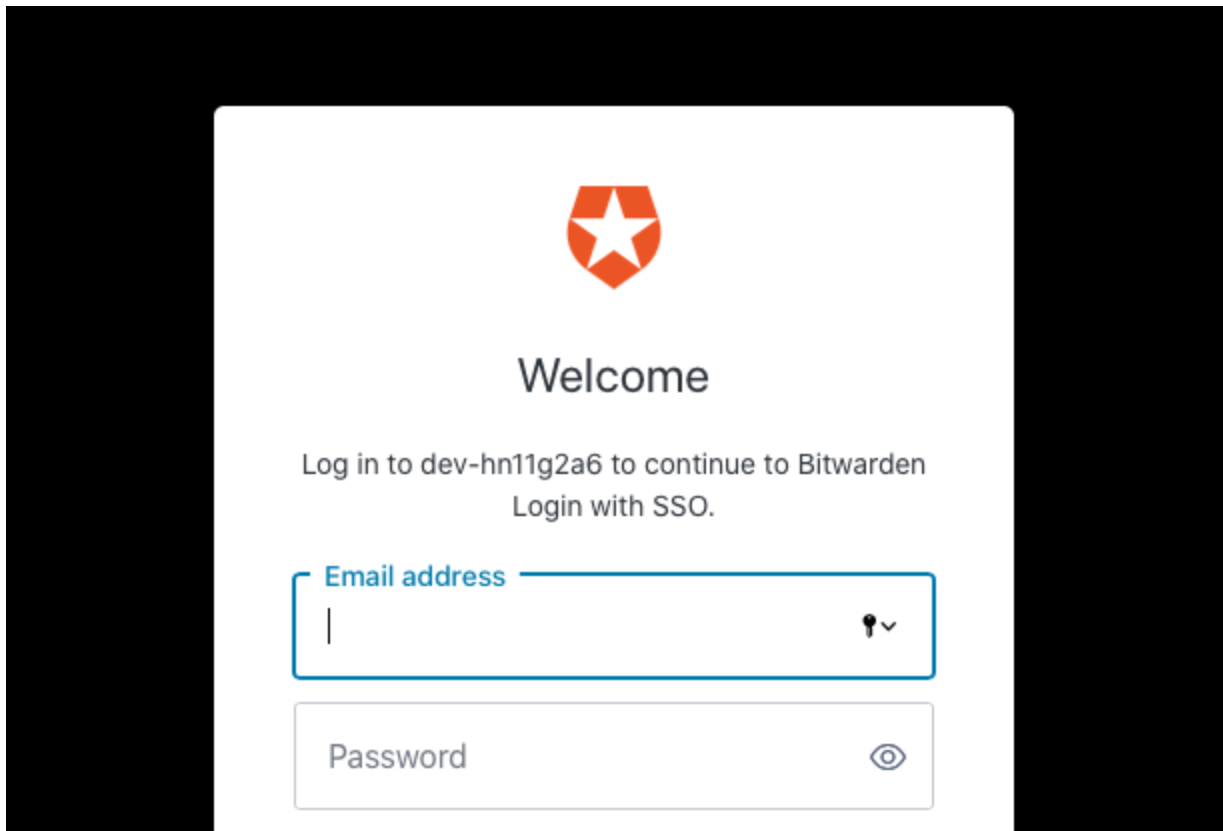
 Log in with passkey

 Use single sign-on

New to Bitwarden? [Create account](#)

Unternehmens Single Sign On und Master-Passwort

Geben Sie die [konfigurierte Organisationskennung](#) ein und wählen Sie **Anmelden**. Wenn Ihre Implementierung erfolgreich konfiguriert ist, werden Sie zum AuthO Zugangsdaten-Bildschirm weitergeleitet:



The image shows a white login card centered on a black background. At the top of the card is the Bitwarden logo (an orange shield with a white star). Below the logo, the word "Welcome" is displayed in a large, dark font. Underneath, the text "Log in to dev-hn11g2a6 to continue to Bitwarden" is shown, followed by "Login with SSO." in a smaller font. There are two input fields: the first is labeled "Email address" in blue text and has a blue border; the second is labeled "Password" in dark text and has a grey border. Both fields contain a vertical cursor. To the right of the "Email address" field is a small icon of a key with a checkmark. To the right of the "Password" field is an eye icon.

AuthO Login

Nachdem Sie sich mit Ihren AuthO-Anmeldeinformationen authentifiziert haben, geben Sie Ihr Bitwarden Master-Passwort ein, um Ihren Tresor zu entschlüsseln!

Note

Bitwarden unterstützt keine unaufgeforderten Antworten, daher führt das Initiieren von Zugangsdaten von Ihrem IdP zu einem Fehler. Der SSO-Zugangsdaten-Fluss muss von Bitwarden aus initiiert werden.