ADMINISTRATOR KONSOLE › MELDEN SIE SICH MIT SSO AN ›

# Okta SAML Implementierung

# Okta SAML Implementierung

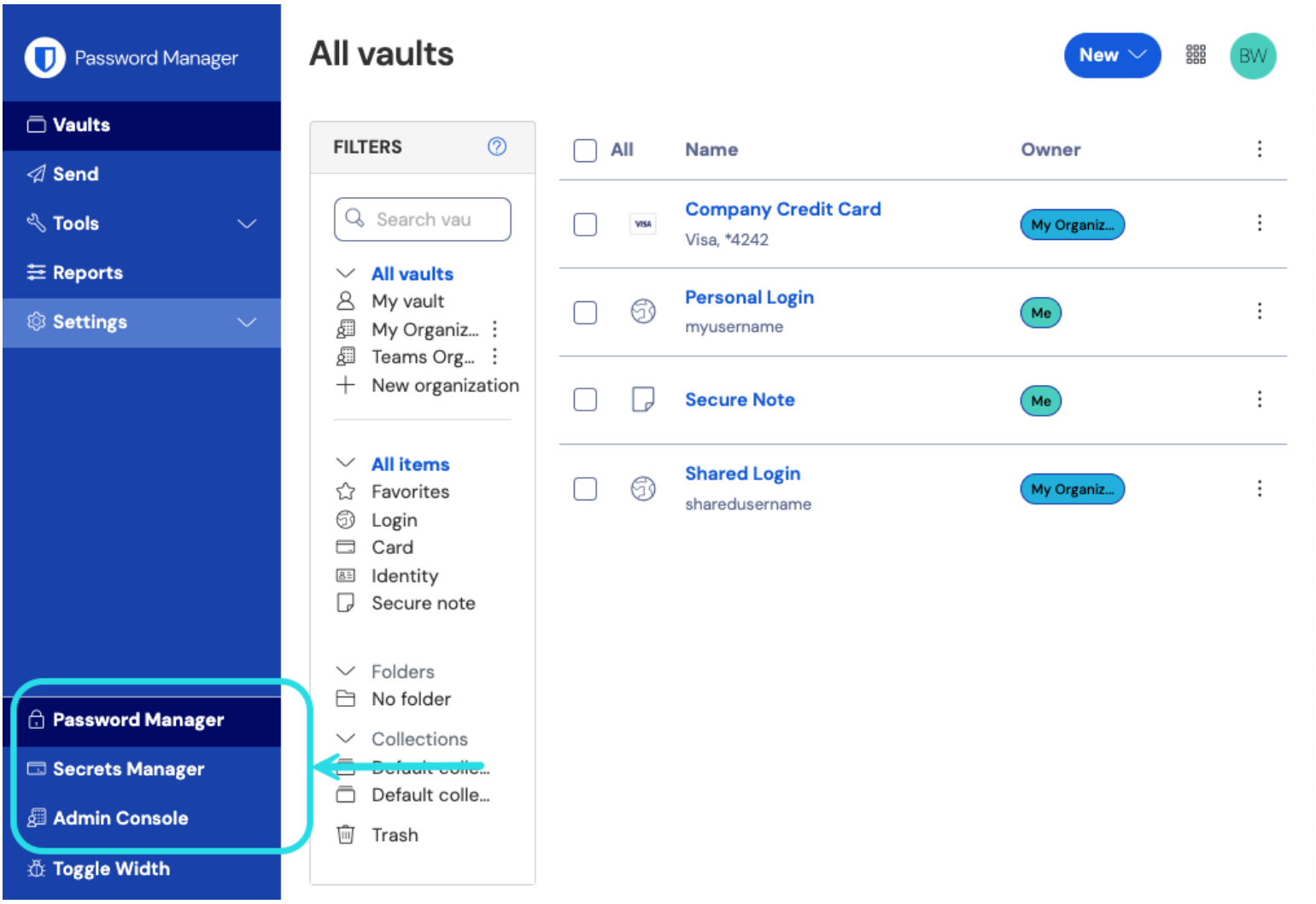
Dieser Artikel enthält **Okta-spezifische** Hilfe zur Konfiguration der Zugangsdaten mit SSO über SAML 2.0. Für Hilfe bei der Konfiguration der Zugangsdaten mit SSO für einen anderen IdP, verweisen Sie auf SAML 2.0 Konfiguration.

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

> **Tip**
>
> **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 Produktumschalter (▦):




Produktwechsler

Öffnen Sie den **Einstellungen → Single sign-on** Bildschirm Ihrer Organisation:


SAML 2.0 Konfiguration

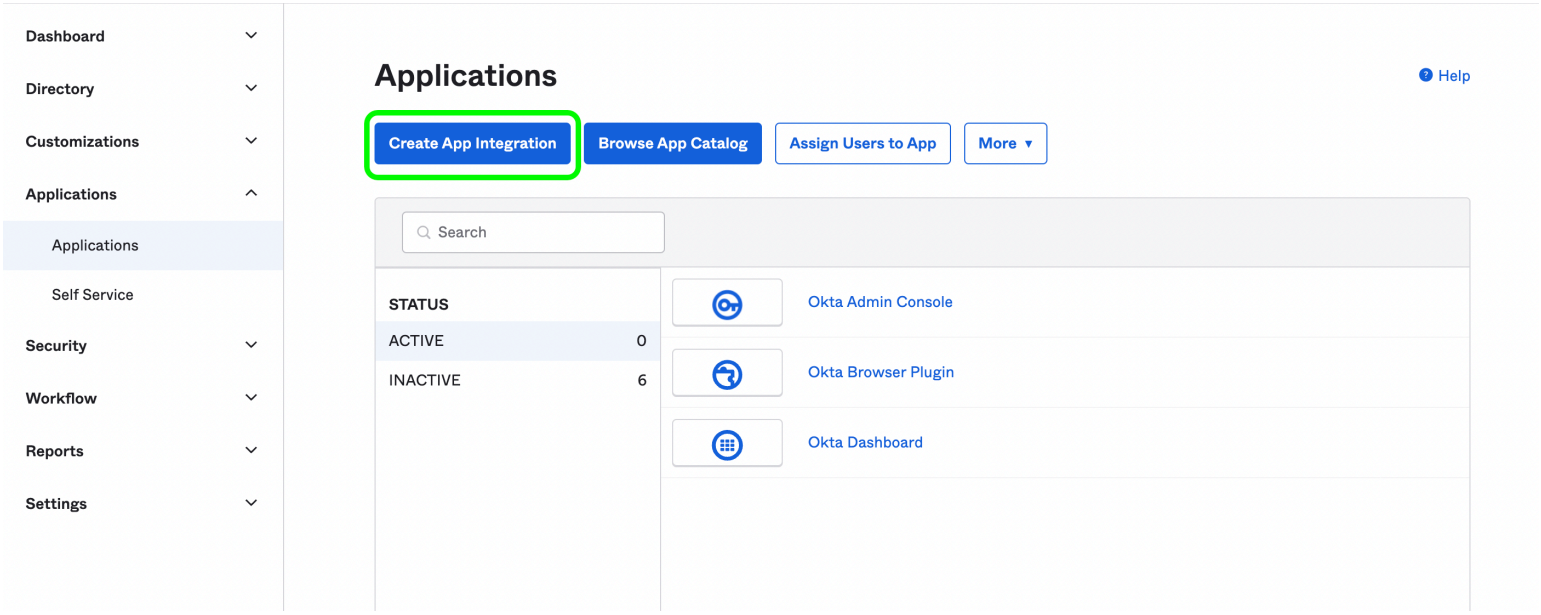
Wenn Sie es noch nicht getan haben, erstellen Sie einen einzigartigen **SSO-Identifikator** für Ihre Organisation und wählen Sie **SAML** aus dem **Typ**-Dropdown aus. Lassen Sie diesen Bildschirm geöffnet, um leicht darauf zugreifen zu können.

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.

> **Tip**
>
> Es gibt alternative **Mitglied Entschlüsselungsoptionen**. Erfahren Sie, wie Sie mit SSO auf vertrauenswürdigen Geräten oder mit Key Connector beginnen können.

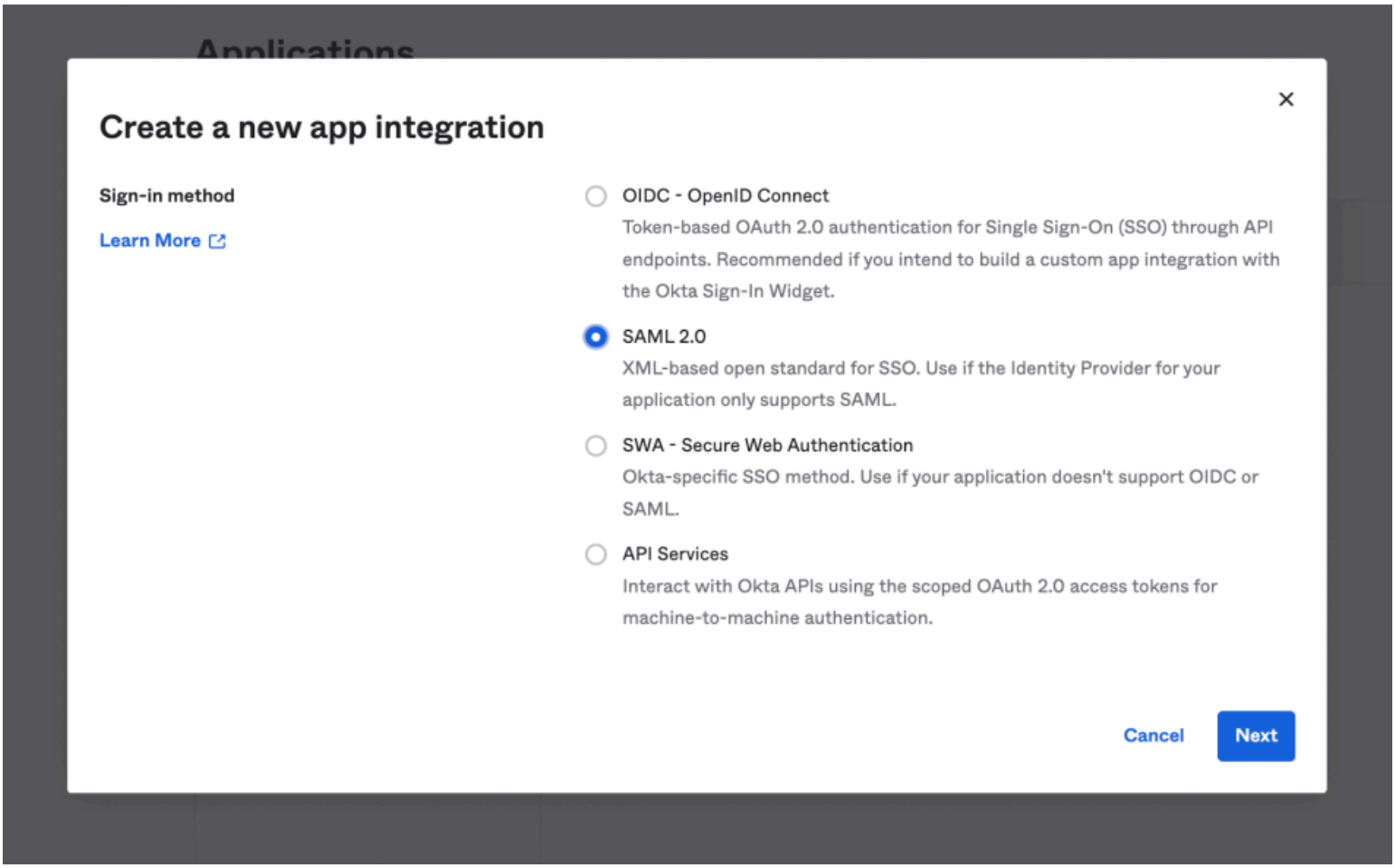
## Erstellen Sie eine Okta-Anwendung

Im Okta Administrator Portal wählen Sie **Anwendungen** → **Anwendungen** aus der Navigation. Auf dem Anwendungsbildschirm wählen Sie die Schaltfläche **App-Integration erstellen**:




Okta create app integration

Im Dialogfenster "Neue Anwendungsintegration erstellen" wählen Sie die Option **SAML 2.0** aus:




SAML 2.0 radio button

Wählen Sie die Schaltfläche **Weiter**, um zur Konfiguration fortzufahren.

## Allgemeine Einstellungen

Auf dem Bildschirm für die **allgemeinen Einstellungen**, geben Sie der Anwendung einen einzigartigen, Bitwarden-spezifischen Namen und wählen Sie **Weiter**.

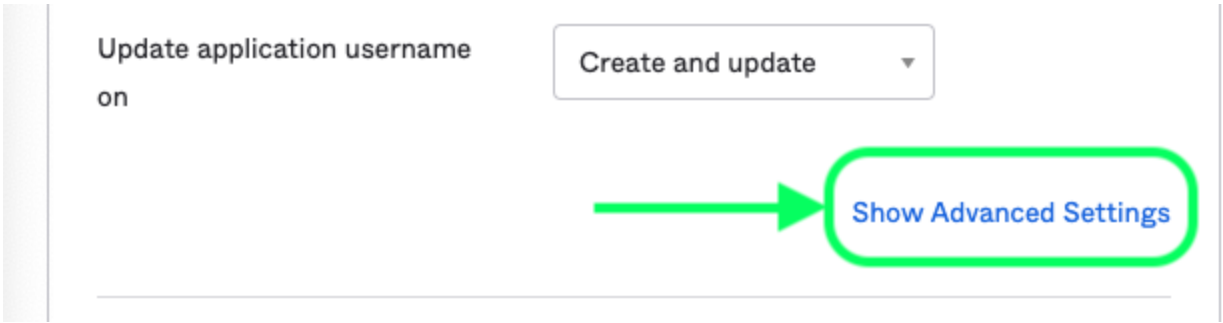
## Konfigurieren Sie SAML

Auf dem **SAML konfigurieren** Bildschirm, konfigurieren Sie die folgenden Felder:

| Feld | Beschreibung |
|---|---|
| Einmalige Anmelde-URL | Setzen Sie dieses Feld auf die vorab generierte **Assertion Consumer Service (ACS) URL**.<br><br>Dieser automatisch generierte Wert kann von der **Einstellungen → Single Sign-On** Bildschirm der Organisation kopiert werden und variiert je nach Ihrer Konfiguration. |
| Publikum URI (SP Entitäts-ID) | Setzen Sie dieses Feld auf die vorab generierte **SP Entity ID**.<br><br>Dieser automatisch generierte Wert kann von der **Einstellungen → Single Sign-On** Bildschirm der Organisation kopiert werden und variiert je nach Ihrer Konfiguration. |
| Namen ID-Format | Wählen Sie das SAML NameID-Format, das in SAML-Behauptungen verwendet werden soll. Standardmäßig, **Nicht spezifiziert**. |
| Anwendungs-Benutzername | Wählen Sie das Okta-Attribut aus, das Benutzer zur Anmeldung bei Bitwarden mit ihren Zugangsdaten verwenden werden. |

## Erweiterte Einstellungen

Wählen Sie den Link **Erweiterte Einstellungen anzeigen** und konfigurieren Sie die folgenden Felder:

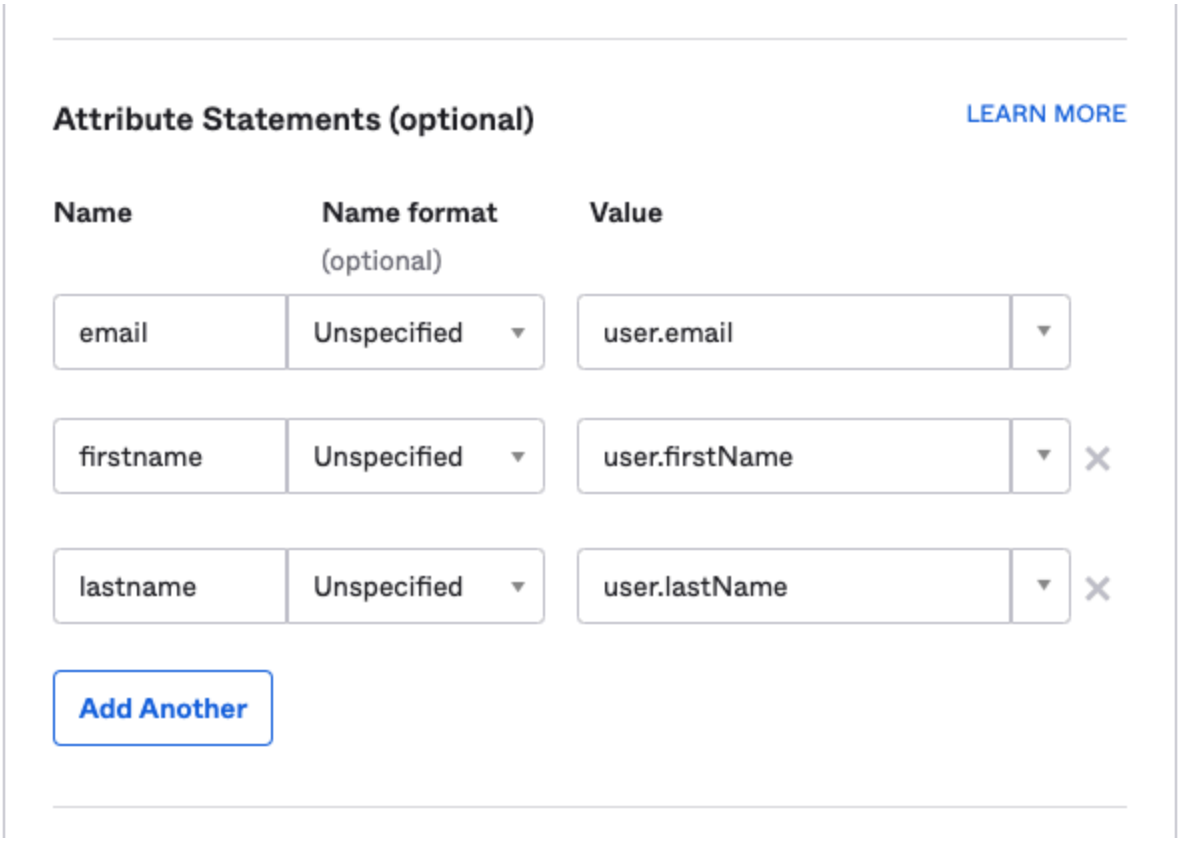



Advanced Settings

| Feld | Beschreibung |
| --- | --- |
| Antwort | Ob die SAML-Antwort von Okta signiert ist. |
| Behauptungsunterschrift | Ob die SAML-Behauptung von Okta signiert ist. |
| Signaturalgorithmus | Der Signaturalgorithmus, der verwendet wird, um die Antwort und/oder Behauptung zu signieren, abhängig davon, welche in den Einstellungen auf **Signiert** gesetzt ist. Standardmäßig, `rsa-sha256`. |
| Verdauungsalgorithmus | Der Digest-Algorithmus, der verwendet wird, um die Antwort und/oder Behauptung zu signieren, abhängig davon, was in den Einstellungen auf **Signiert** gesetzt ist. Dieses Feld muss dem ausgewählten **Signaturalgorithmus** entsprechen. |

### Attribut Aussagen

Im Abschnitt **Attribut Aussagen**, erstellen Sie die folgenden SP → IdP Attributzuordnungen:

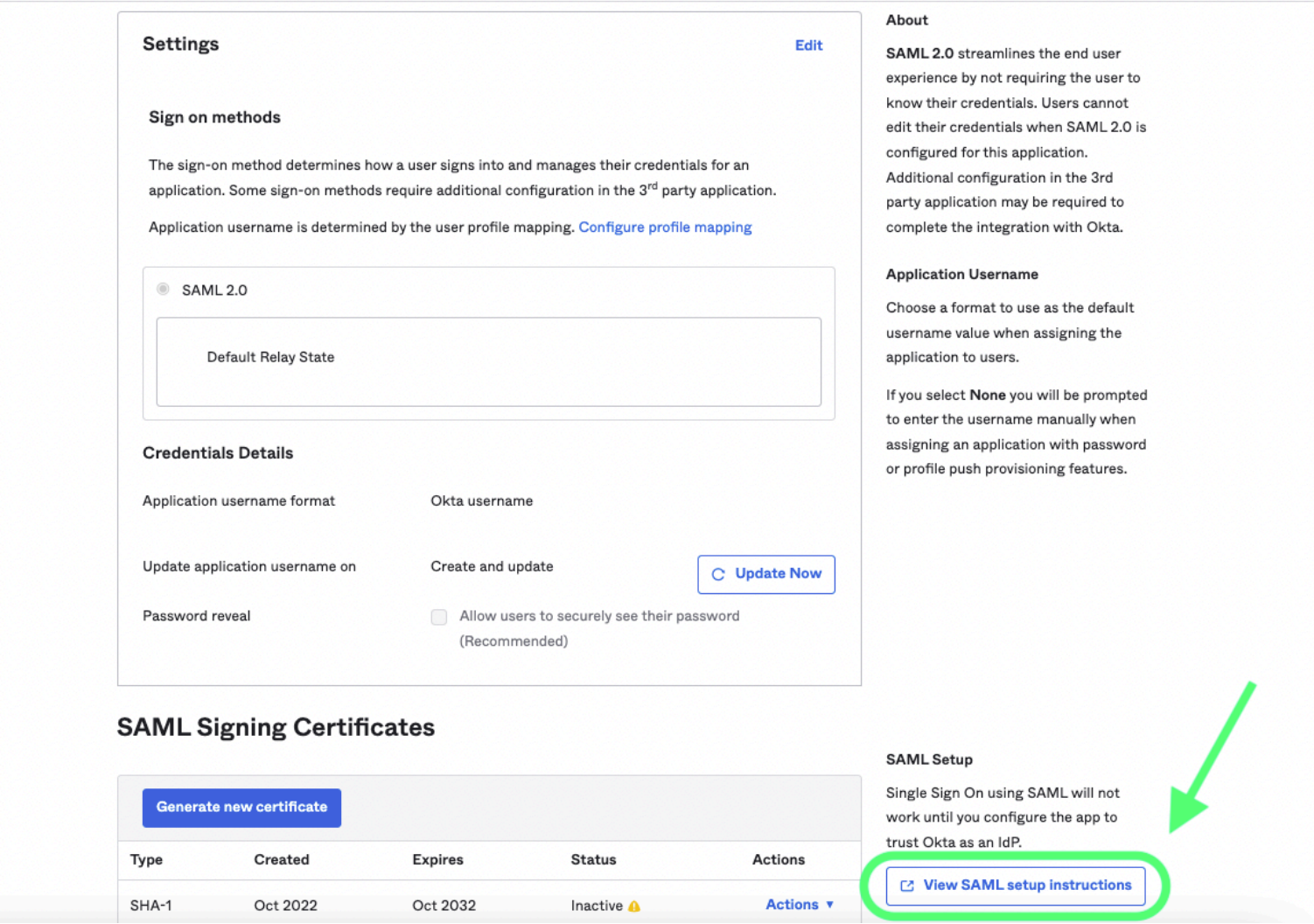



Attribute Statements

Einmal konfiguriert, wählen Sie die **Weiter** Schaltfläche, um zum **Feedback** Bildschirm zu gelangen und wählen Sie **Fertig**.

## Erhalten Sie IdP-Werte

Sobald Ihre Anwendung erstellt ist, wählen Sie den **Anmelden** Tab für die App und wählen Sie die Schaltfläche **Anweisungen einrichten** Ansicht, die sich auf der rechten Seite des Bildschirms befindet:



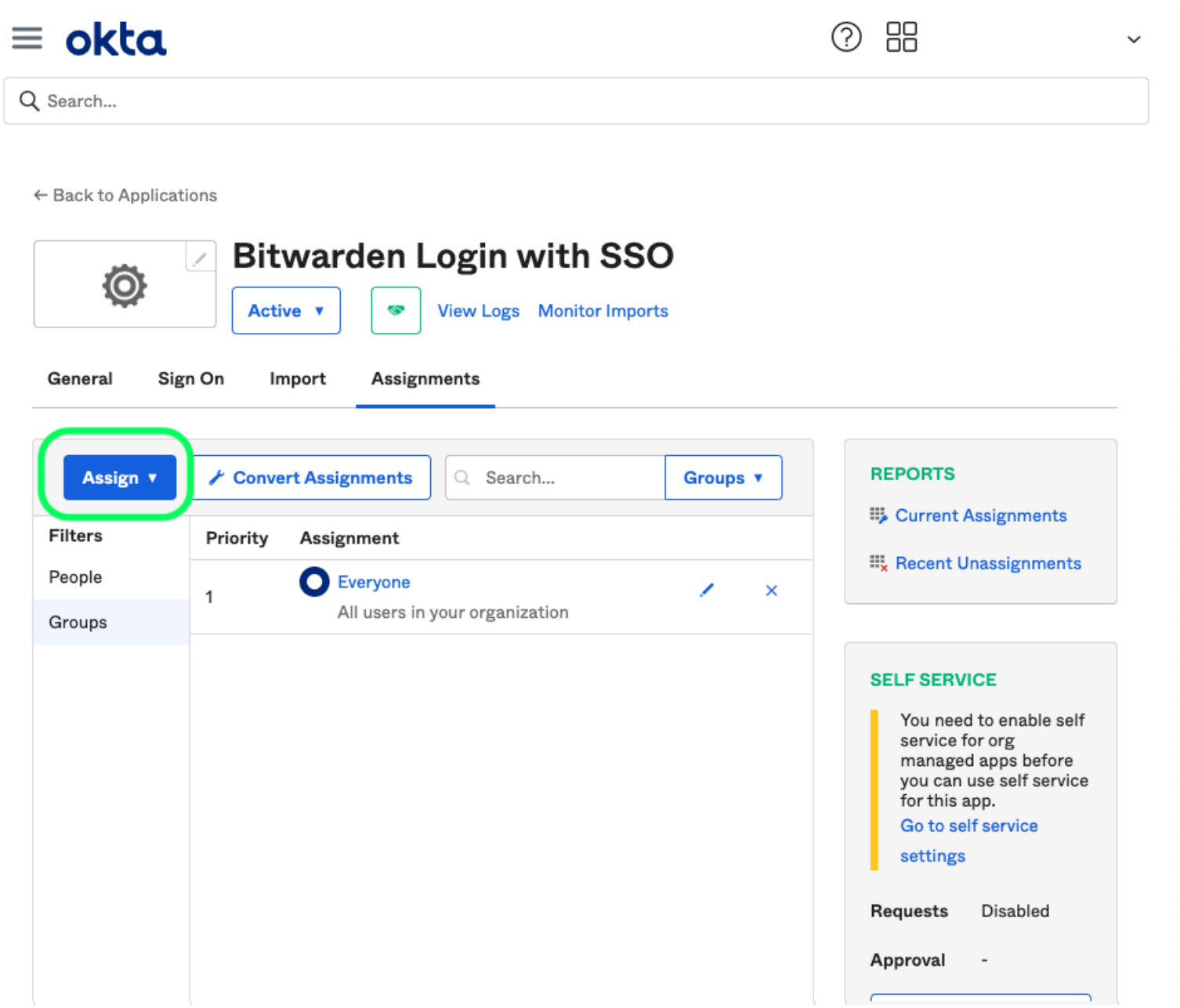

View SAML setup instructions

Lassen Sie diese Seite entweder für die zukünftige Verwendung offen, oder kopieren Sie die **Identität Provider Single Sign-On URL** und den **Identität Provider Aussteller** und laden Sie das **X.509 Zertifikat** herunter:


IdP Values

## Aufgaben

Navigieren Sie zum **Aufgaben** Tab und wählen Sie die **Zuweisen** Schaltfläche:




Assigning Groups

Sie können den Zugriff auf die Anwendung auf Benutzerbasis mithilfe der Option **Zuweisen an Personen** festlegen oder in großen Mengen mithilfe der Option **Zuweisen an Gruppen**.

## Zurück zur Web-App

Bis zu diesem Zeitpunkt haben Sie alles konfiguriert, was Sie im Kontext des Okta Administrator Portals benötigen. 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

Konfigurieren Sie die folgenden Felder entsprechend den in der Okta Administrator Portal während der App-Erstellung getroffenen Auswahlmöglichkeiten:

| Feld | Beschreibung |
|---|---|
| Namens-ID-Format | Stellen Sie dies auf das Namens-ID-Format ein, das in Okta angegeben ist, ansonsten lassen Sie **Unbestimmt**. |
| Ausgehendes Signatur-Algorithmus | Der Algorithmus, den Bitwarden zur Signierung von SAML-Anfragen verwenden wird. |
| Unterzeichnungsverhalten | Ob/wann SAML-Anfragen signiert werden. |
| Mindesteingehendes Signaturalgorithmus | Stellen Sie dies auf den Signaturalgorithmus festgelegt in Okta. |
| Möchte Behauptungen unterschrieben haben | Markieren Sie dieses Kästchen, wenn Sie das Feld für die Behauptungssignatur auf **Unterzeichnet** in Okta in den Einstellungen gesetzt haben. |
| 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, geeignete Vertrauensketten sind innerhalb der Bitwarden Zugangsdaten mit SSO Docker-Image 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 Okta Administrator Portal beziehen, um Anwendungswerte abzurufen:

| Feld | Beschreibung |
| --- | --- |
| Entitäts-ID | Geben Sie Ihren **Identität Provider Aussteller** ein, den Sie vom Okta Anmelden Einstellungen Bildschirm abgerufen haben, indem Sie die **Anleitung einrichten Ansicht** Schaltfläche auswählen. Dieses Feld ist Groß- und Kleinschreibungssensitiv. |
| Bindungsart | Auf **Umleiten** einstellen. Okta unterstützt derzeit HTTP POST nicht. |
| URL des Single Sign On Dienstes | Geben Sie Ihre **Identität Provider Single Sign-On URL** ein, die Sie vom Okta Anmelden Einstellungen Bildschirm abgerufen haben. |
| URL des Einzelabmeldedienstes | 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 heruntergeladene Zertifikat ein und entfernen Sie es.<br><br>`-----BEGIN ZERTIFIKAT-----`<br><br>und<br><br>`-----ENDE ZERTIFIKAT-----`<br><br>Der Zertifikatswert ist Groß- und Kleinschreibungssensitiv, zusätzliche Leerzeichen, Zeilenumbrüche und andere überflüssige Zeichen **werden dazu führen, dass die Zertifikatsvalidierung fehlschlägt**. |
| Ausgehendes Signaturalgorithmus | Wählen Sie den Signaturalgorithmus aus, der während der Okta-App-Konfiguration ausgewählt wurde. Wenn Sie den Signaturalgorithmus nicht geändert haben, lassen Sie den Standard (`rsa-sha256`). |
| Ausgehende Abmeldeanfragen erlauben | Die Anmeldung mit SSO unterstützt derzeit **nicht** SLO. |
| Möchte Authentifizierungsanfragen signiert haben | Ob Okta erwartet, dass SAML-Anfragen signiert werden. |

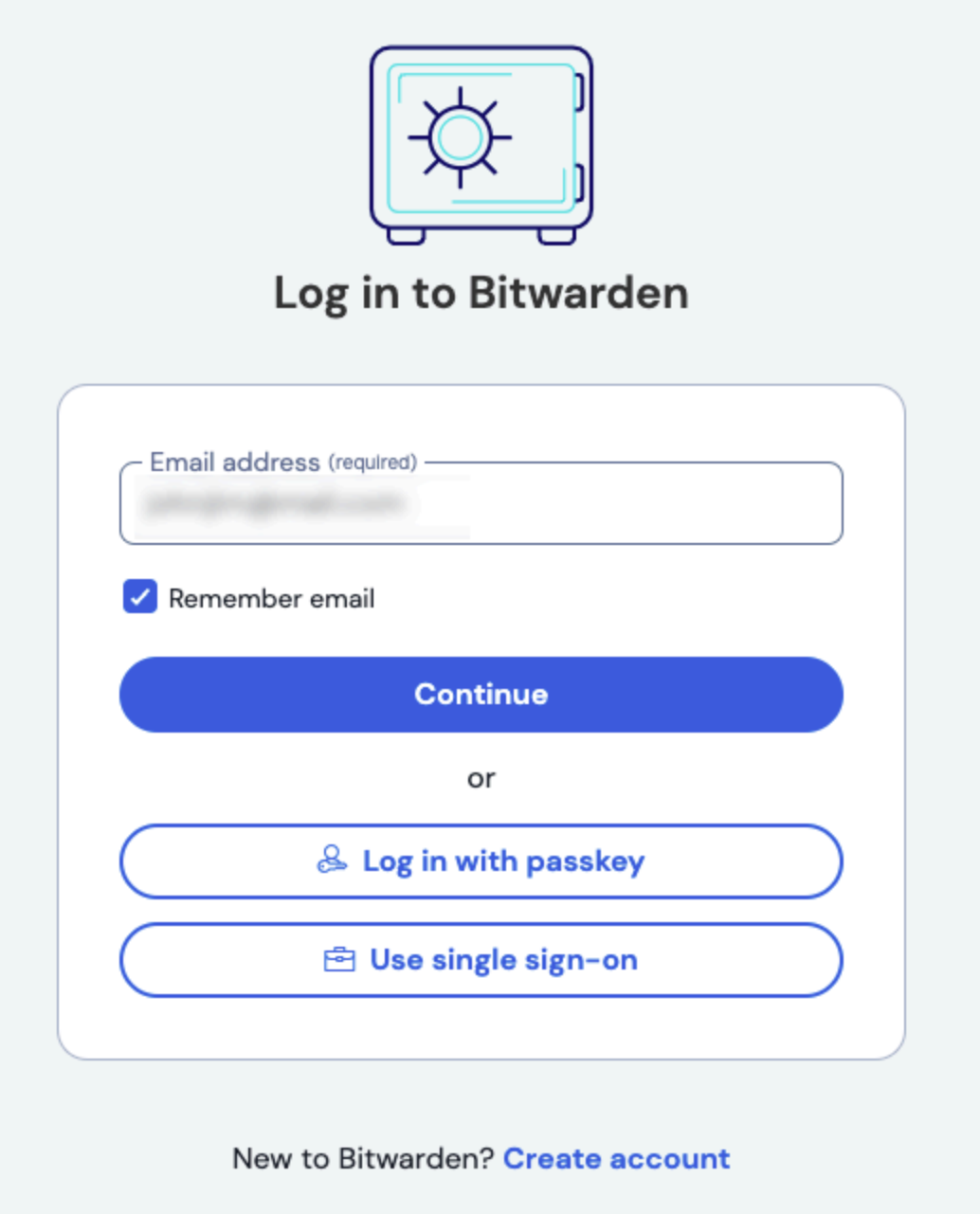
> **Note**
>
> Bei der Ausstellung des X509-Zertifikats, machen Sie eine Notiz vom Ablaufdatum. Zertifikate müssen erneuert werden, um jegliche Unterbrechungen im Dienst für SSO-Endbenutzer zu verhindern. Wenn ein Zertifikat abgelaufen ist, können sich Administrator- und Eigentümer-Konten immer mit E-Mail-Adresse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

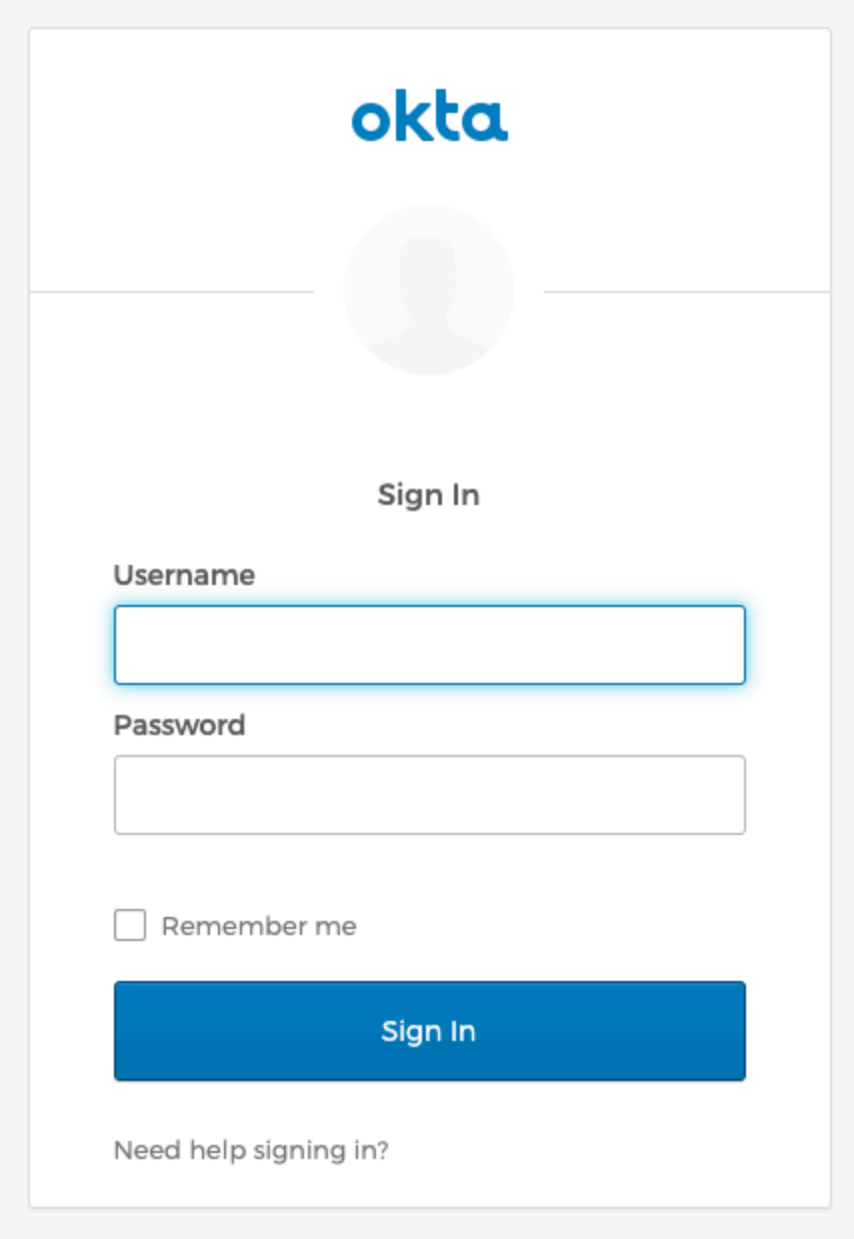
## Testen Sie die Konfiguration

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:




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 zur Okta-Zugangsdaten-Bildschirm weitergeleitet:




Log in with Okta

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

**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.