bitwarden | Hilfezentrum Artikel

ADMINISTRATOR KONSOLE > MELDEN SIE SICH MIT SSO AN >

# JumpCloud SAML Implementierung

Ansicht im Hilfezentrum:
https://bitwarden.com/help/saml-jumpcloud/

# JumpCloud SAML Implementierung

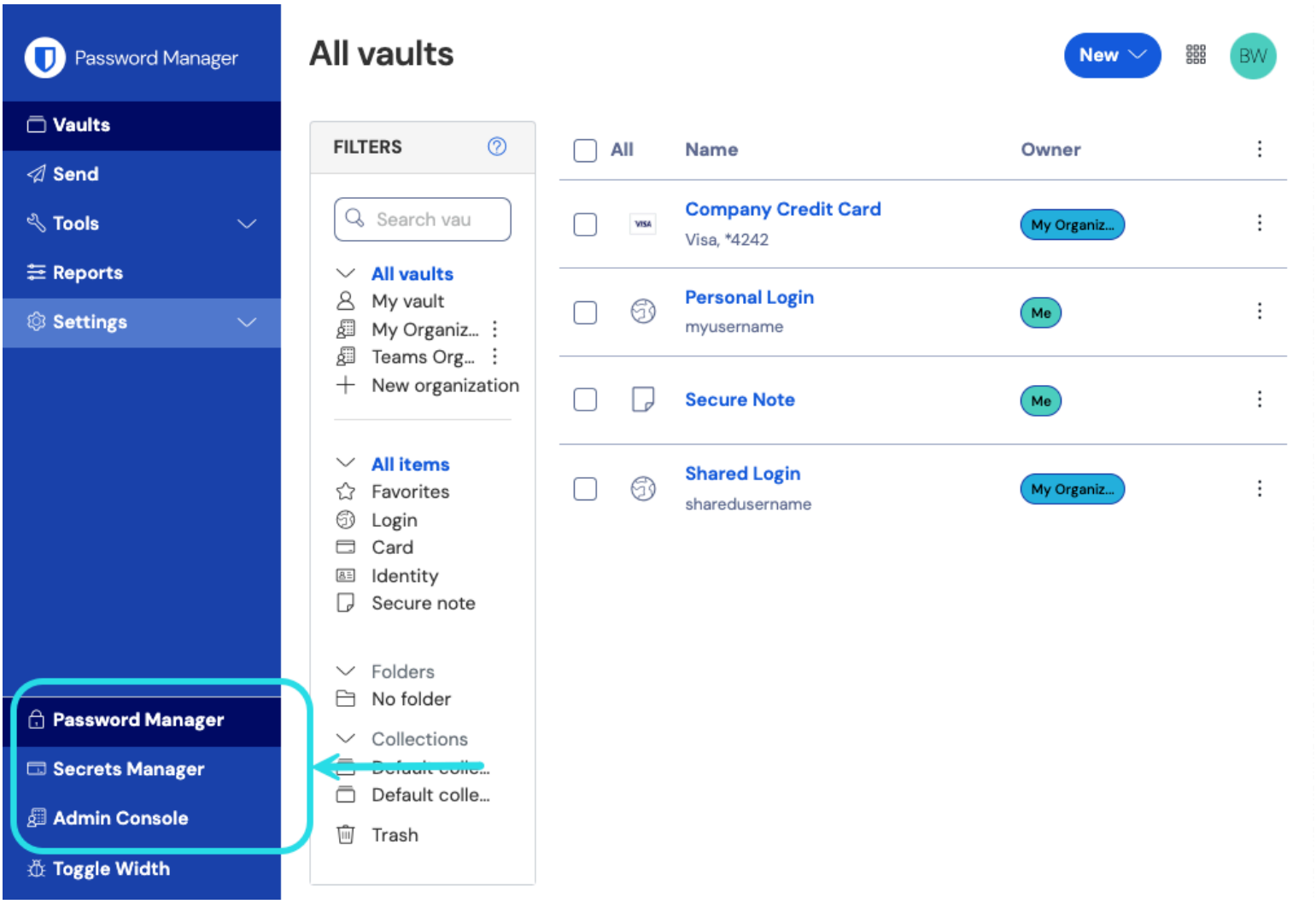
Dieser Artikel enthält **JumpCloud-spezifische** Hilfe zur Konfiguration der Zugangsdaten mit SSO über SAML 2.0. Für Hilfe bei der Konfiguration der Zugangsdaten mit SSO für einen anderen IdP, verweisen Sie auf SAML 2.0 Konfiguration.

Die Konfiguration beinhaltet die gleichzeitige Arbeit innerhalb der Bitwarden-Web-App und des JumpCloud-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

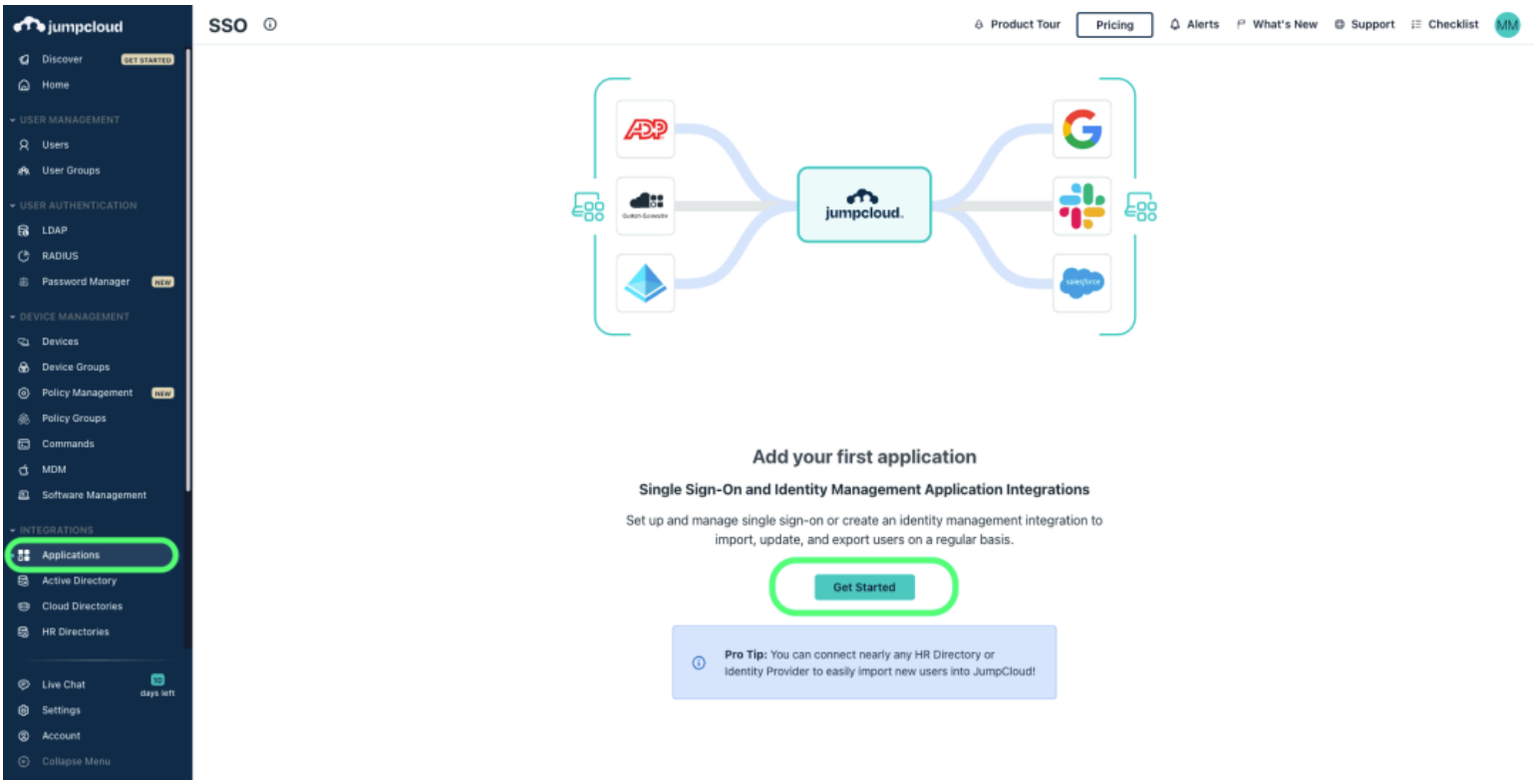
Wenn Sie es noch nicht getan haben, erstellen Sie einen einzigartigen **SSO-Identifikator** für Ihre Organisation und wählen Sie **SAML** aus dem **Typ**-Dropdown aus. Lassen Sie diesen Bildschirm geöffnet, um leicht darauf zugreifen zu können.

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.

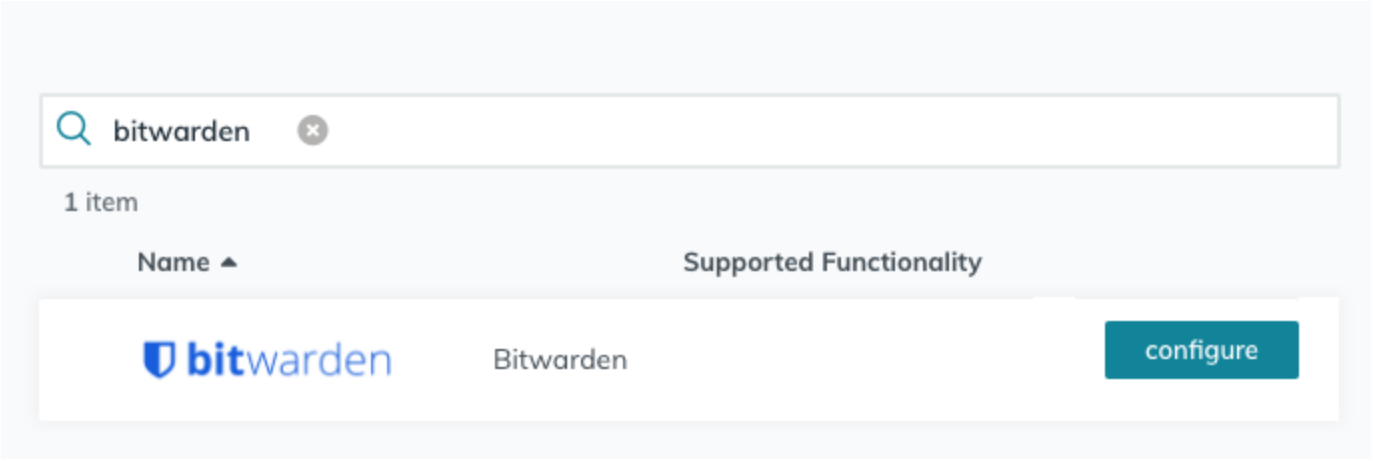
## Erstellen Sie eine JumpCloud SAML-Anwendung

Im JumpCloud Portal wählen Sie **Anwendungen** aus dem Menü und klicken Sie auf die Schaltfläche **Loslegen**:




Create Bitwarden app Jumpcloud

Geben Sie `Bitwarden` in das Suchfeld ein und wählen Sie die **konfigurieren** Schaltfläche:




Configure Bitwarden

> **Tip**
> If you are more comfortable with SAML, or want more control over things like NameID Format and Signing Algorithms, create a **Custom SAML Application** instead.

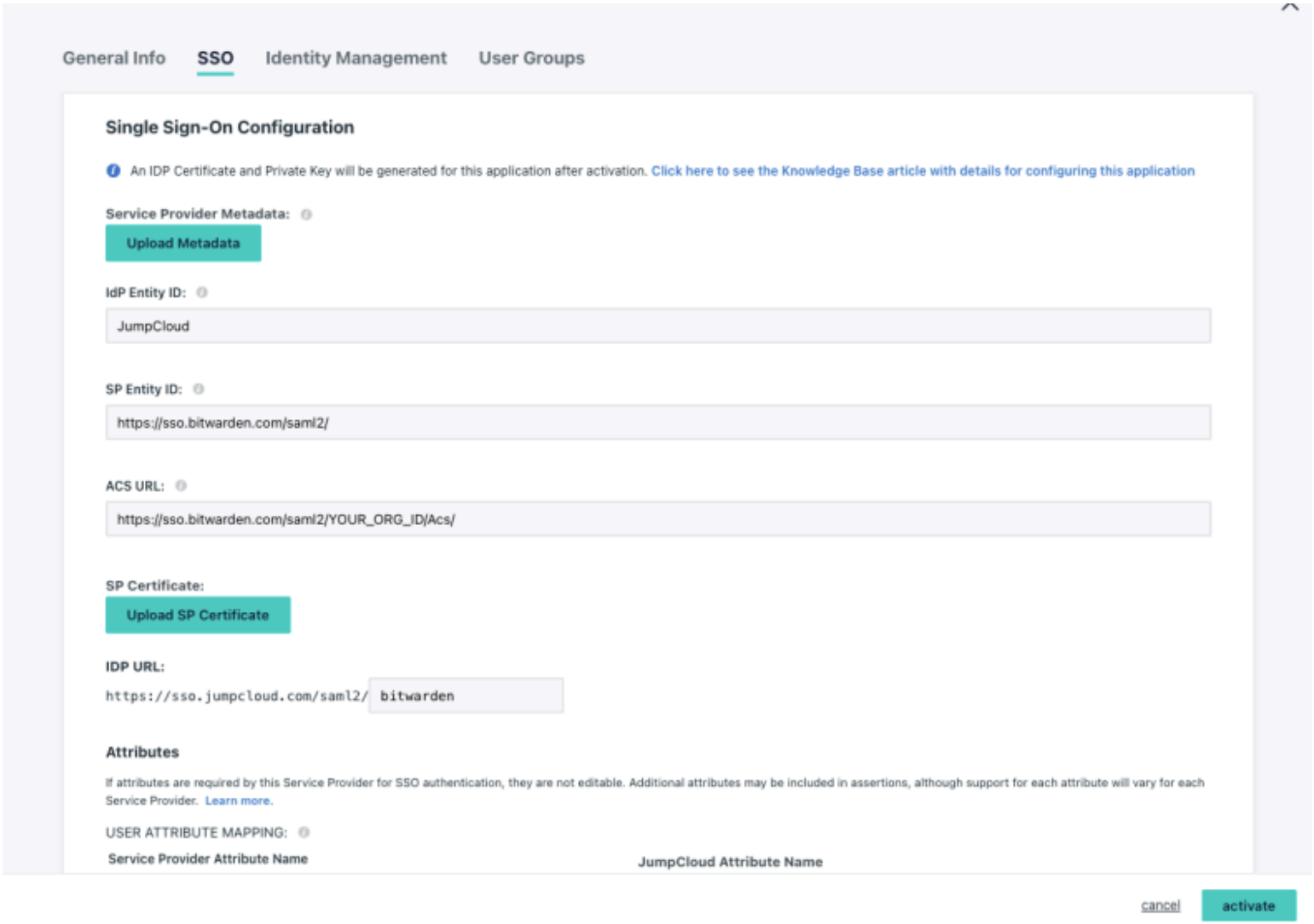
## Allgemeine Informationen

Im Abschnitt **Allgemeine Informationen** konfigurieren Sie die folgenden Informationen:

| Feld | Beschreibung |
| --- | --- |
| Anzeigeetikett | Geben Sie der Anwendung einen Bitwarden-spezifischen Namen. |

## Einmalige Anmeldungs-Konfiguration

Im Abschnitt **Konfiguration für Single Sign-On** konfigurieren Sie die folgenden Informationen:




Jumpcloud SSO configuration

| Feld | Beschreibung |
| --- | --- |
| IdP-Entitäts-ID | Setzen Sie dieses Feld auf einen einzigartigen, Bitwarden-spezifischen Wert, zum Beispiel, `bitwardensso_ihreFirma`. |
| SP-Entitäts-ID | Setzen Sie dieses Feld auf die vorab generierte **SP Entity ID**.<br><br>Dieser automatisch generierte Wert kann aus den **Einstellungen → Single Sign-On** der Organisation kopiert werden und variiert je nach Ihrer Konfiguration. |
| ACS-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. |

### Benutzerdefinierte SAML-App nur

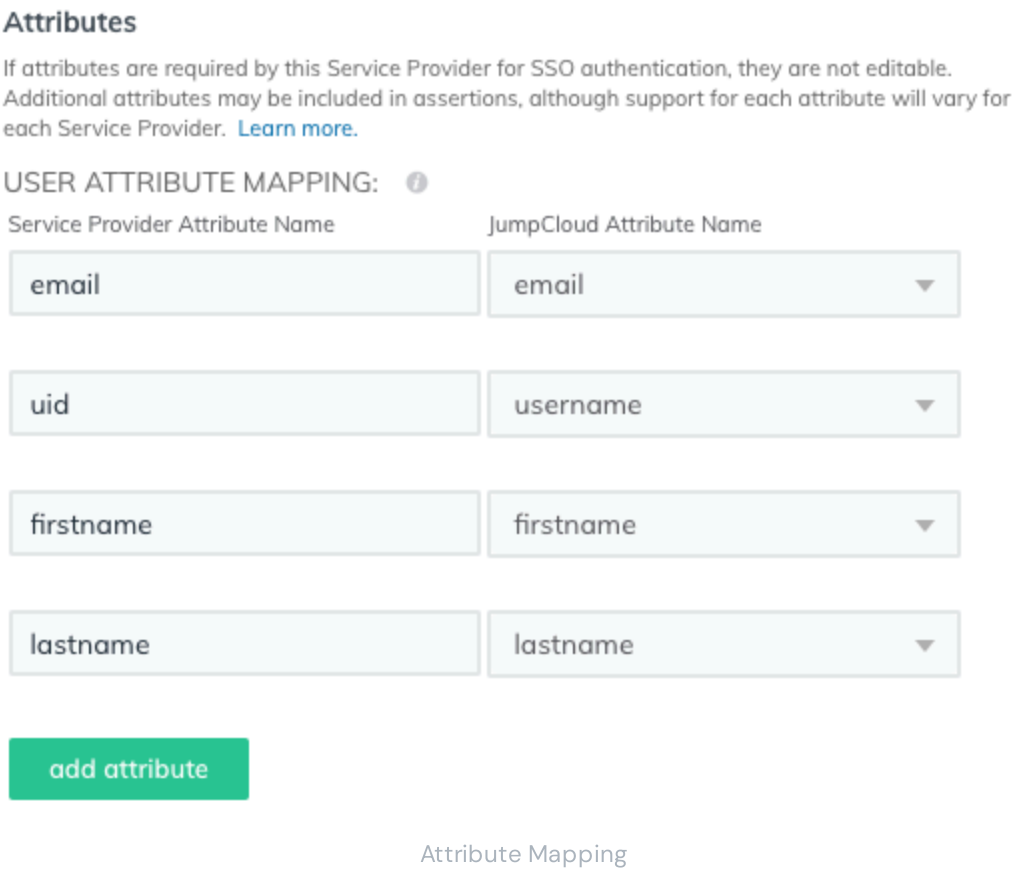
Wenn Sie eine benutzerdefinierte SAML-Anwendung erstellt haben, müssen Sie auch die folgenden Felder für die **Single Sign-On Konfiguration** konfigurieren:

| Feld | Beschreibung |
| --- | --- |
| SAMLSubject NameID | Geben Sie das JumpCloud-Attribut an, das in SAML-Antworten als NameID gesendet wird. |
| SAMLSubject NameID Format | Geben Sie das Format der in SAML-Antworten gesendeten NameID an. |
| Signaturalgorithmus | Wählen Sie den Algorithmus aus, der zum Signieren von SAML-Behauptungen oder Antworten verwendet werden soll. |
| Unterschriftsbehauptung | Standardmäßig wird JumpCloud die SAML-Antwort signieren. Markieren Sie dieses Kästchen, um die SAML-Behauptung zu unterschreiben. |
| URL der Zugangsdaten | Geben Sie die URL an, über die Ihre Benutzer sich über SSO bei Bitwarden mit ihren Zugangsdaten anmelden werden. |

| Feld | Beschreibung |
| --- | --- |
| | Für Kunden, die in der Cloud gehostet werden, ist dies `https://vault.bitwarden.com/#/sso` oder `https://vault.bitwarden.eu/#/sso`. Für selbst gehostete Instanzen wird dies durch Ihre konfigurierte Server-URL bestimmt, zum Beispiel `https://your.domain.com/#/sso`. |

## Eigenschaften

Im Abschnitt **Einmalige Anmeldekonfiguration → Attribute**, erstellen Sie die folgenden SP → IdP Attributzuordnungen. Wenn Sie die Bitwarden-Anwendung in JumpCloud ausgewählt haben, sollten diese bereits erstellt worden sein:

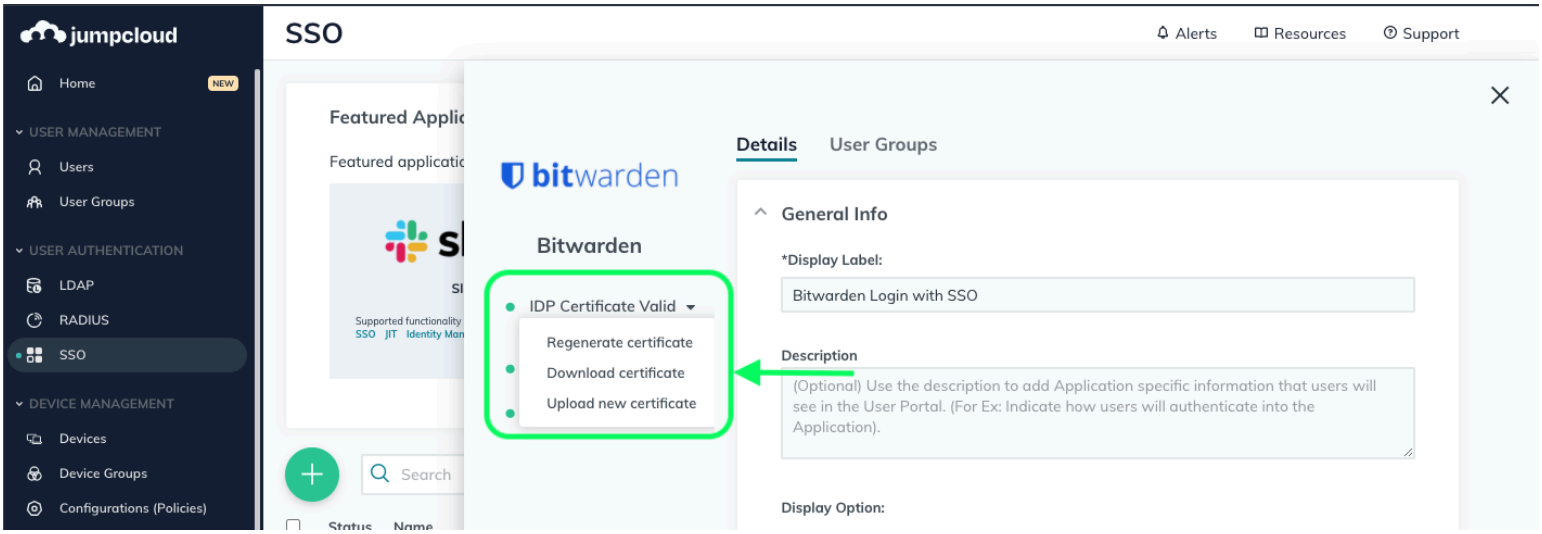



Attribute Mapping

Wenn Sie fertig sind, wählen Sie die **aktivieren** Schaltfläche.

## Laden Sie das Zertifikat herunter

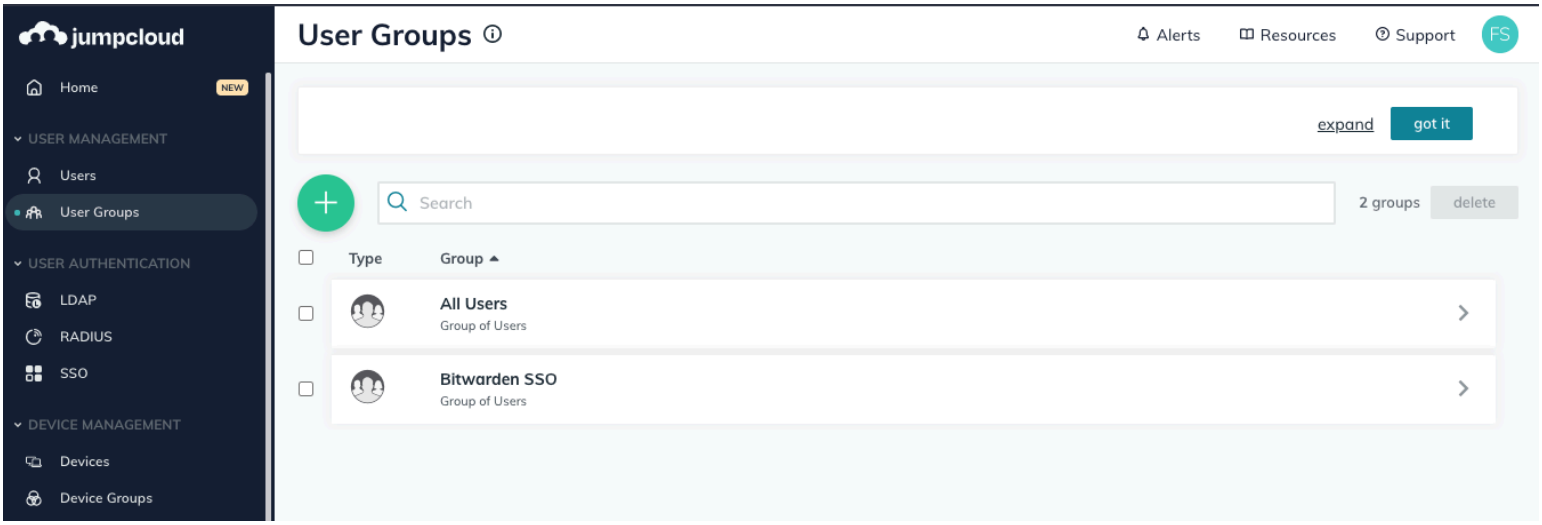
Sobald die Anwendung aktiviert ist, verwenden Sie erneut die **SSO** Menüoption, um die erstellte Bitwarden Anwendung zu öffnen. Wählen Sie das Dropdown-Menü **IDP Zertifikat** und **Zertifikat herunterladen**:




Download Certificate

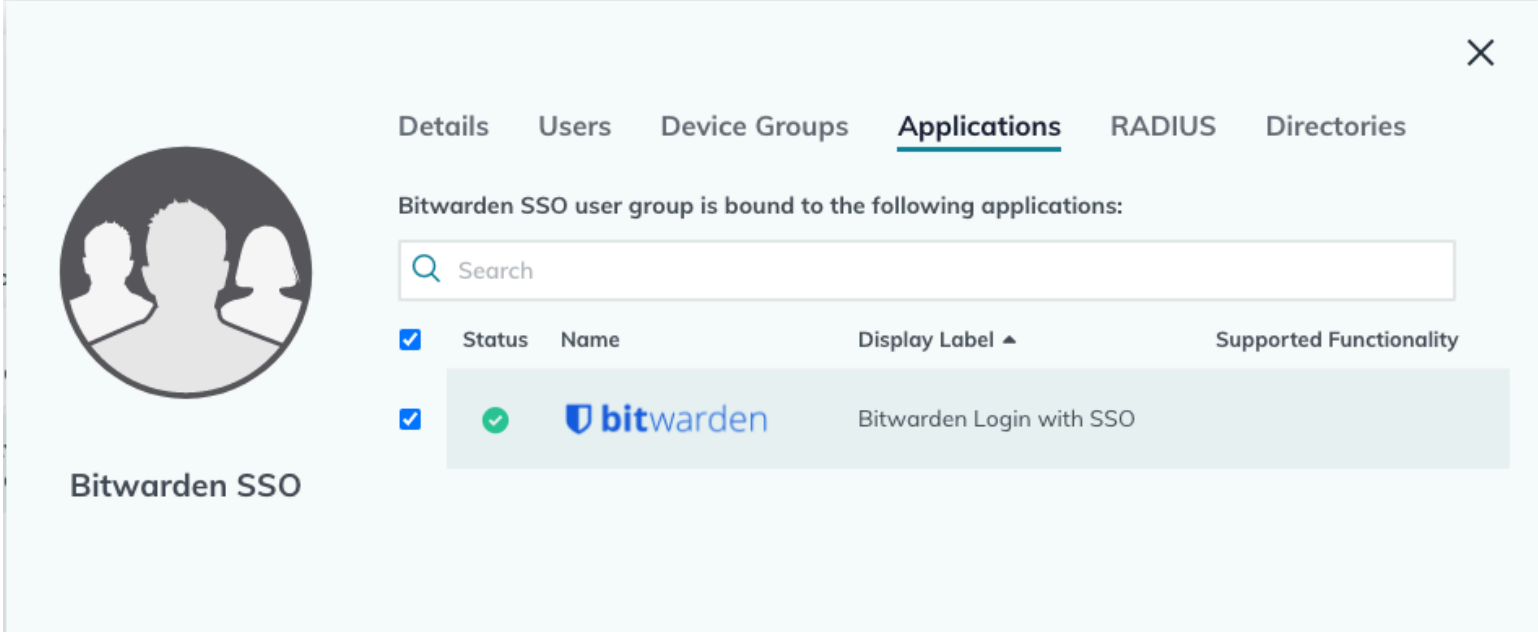
## Benutzergruppen binden

Im JumpCloud Portal wählen Sie **Benutzergruppen** aus dem Menü:




User Groups

Erstellen Sie entweder eine Bitwarden-spezifische Benutzergruppe oder öffnen Sie die standardmäßige Benutzergruppe "Alle Benutzer". In beiden Fällen wählen Sie den Tab **Anwendungen** und aktivieren Sie den Zugriff auf die erstellte Bitwarden SSO-Anwendung für diese Benutzergruppe:




Bind App Access

> **Tip**
> Alternatively, you can bind access to user groups directly from the **SSO → Bitwarden Application** screen.

## Zurück zur Web-App

Bis zu diesem Zeitpunkt haben Sie alles, was Sie im Kontext des JumpCloud Portals benötigen, konfiguriert. Kehren Sie zum Bitwarden Web-Tresor 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 JumpCloud Portal während der App-Erstellung getroffenen Auswahlmöglichkeiten:

| Feld | Beschreibung |
|---|---|
| Namens-ID-Format | Wenn Sie eine benutzerdefinierte SAML-Anwendung erstellt haben, stellen Sie dies auf das angegebene SAMLSubject NameID-Format ein. Andernfalls, lassen Sie **Unspezifiziert**. |

| Feld | Beschreibung |
| --- | --- |
| Ausgehendes Signatur-Algorithmus | Der Algorithmus, den Bitwarden zur Signierung von SAML-Anfragen verwenden wird. |
| Unterzeichnungsverhalten | Ob/wann SAML-Anfragen signiert werden. Standardmäßig erfordert JumpCloud keine signierten Anfragen. |
| Minimales Eingehendes Signatur-Algorithmus | Wenn Sie eine benutzerdefinierte SAML-Anwendung erstellt haben, stellen Sie dies auf den von Ihnen ausgewählten Signaturalgorithmus ein. Andernfalls lassen Sie es als `rsa-sha256`. |
| Möchte Behauptungen unterschrieben haben | Wenn Sie eine benutzerdefinierte SAML-Anwendung erstellt haben, markieren Sie dieses Kästchen, wenn Sie die Option **Sign Assertion** in JumpCloud festgelegt haben. Andernfalls, lassen Sie es ungeprüft. |
| 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 des 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 auf das JumpCloud Portal zurückgreifen, um Anwendungswerte abzurufen:

| Feld | Beschreibung |
| --- | --- |
| Entitäts-ID | Geben Sie Ihre JumpCloud **IdP Entity ID** ein, die Sie vom JumpCloud Single Sign-On Konfigurationsbildschirm abrufen können. Dieses Feld ist Groß- und Kleinschreibungssensitiv. |
| Bindungsart | Auf **Umleiten** einstellen. |

| Feld | Beschreibung |
| --- | --- |
| Einmaliges Anmelden Service URL | Geben Sie Ihre JumpCloud **IdP URL** ein, die Sie vom JumpCloud Single Sign-On Konfigurationsbildschirm abrufen können. |
| URL des Einzelabmeldedienstes | Die Anmeldung mit SSO unterstützt derzeit **nicht** SLO. Diese Option ist für zukünftige Entwicklungen geplant. |
| X509 Öffentliches Zertifikat | Fügen Sie das abgerufene 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 Signatur-Algorithmus | Wenn Sie eine benutzerdefinierte SAML-Anwendung erstellt haben, stellen Sie dies auf den von Ihnen ausgewählten Signaturalgorithmus ein. Andernfalls lassen Sie es als `rsa-sha256`. |
| Deaktivieren Sie ausgehende Abmeldeanfragen | Die Anmeldung mit SSO unterstützt derzeit **nicht** SLO. Diese Option ist für zukünftige Entwicklungen geplant. |
| Möchte Authentifizierungsanfragen signiert haben | Ob JumpCloud erwartet, dass SAML-Anfragen signiert werden. |

**Note**

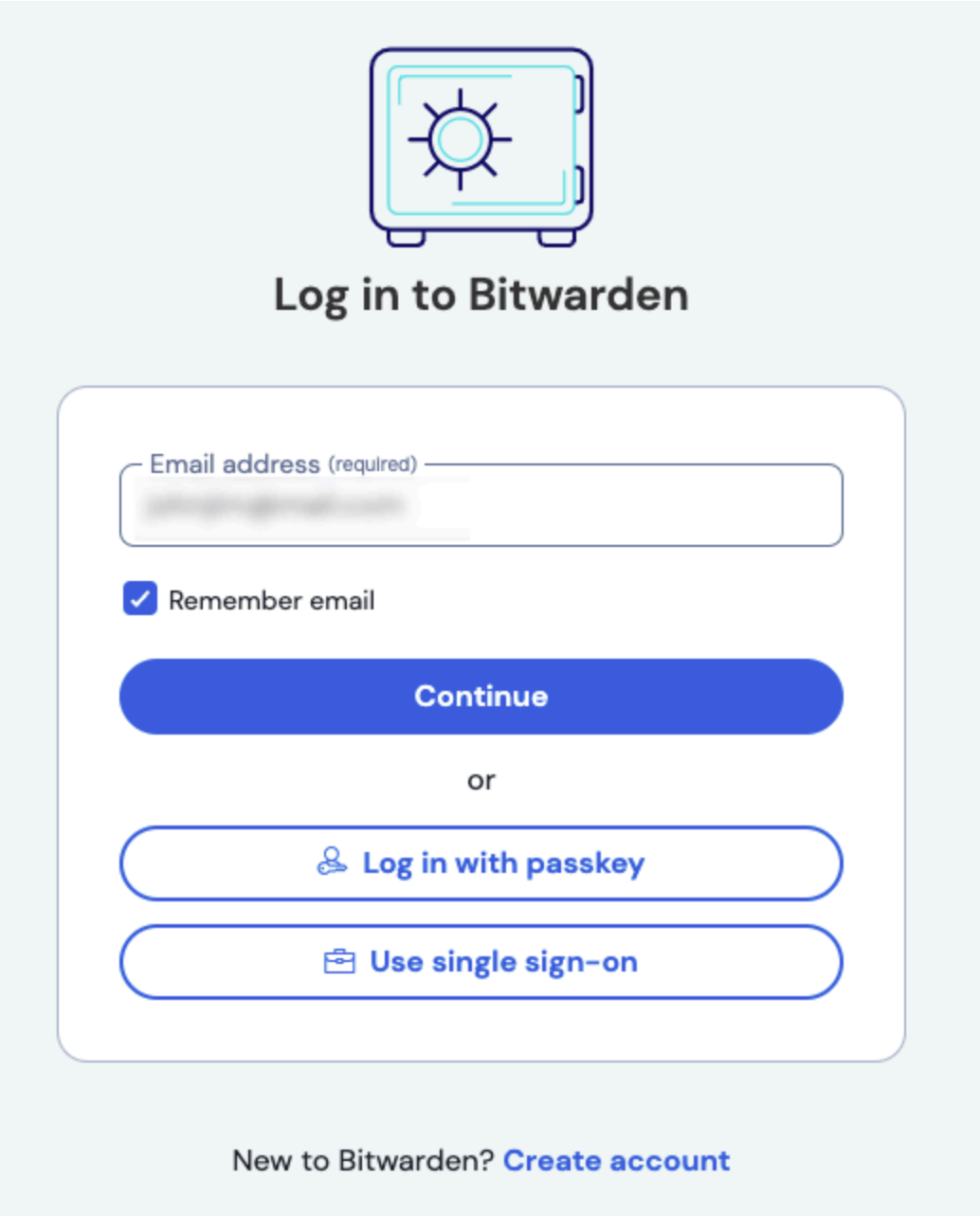
Bei der Ausstellung des X509-Zertifikats, machen Sie eine Notiz vom Ablaufdatum. Zertifikate müssen erneuert werden, um jegliche Unterbrechungen im Dienst für SSO-Endbenutzer zu verhindern. Wenn ein Zertifikat abgelaufen ist, können sich Administrator- und Eigentümer-Konten immer mit E-Mail-Adresse und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

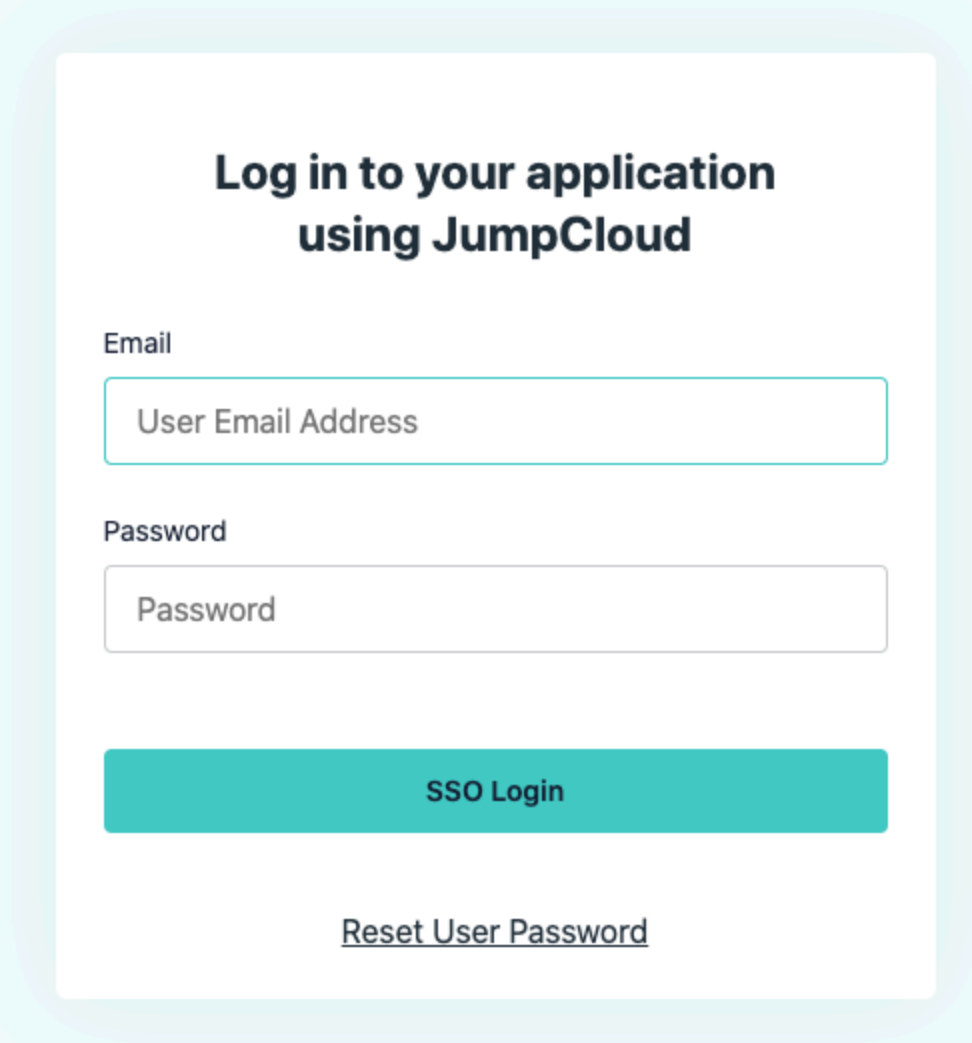
## Testen Sie die Konfiguration

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 zum JumpCloud Zugangsdaten-Bildschirm weitergeleitet:




JumpCloud Login

Nachdem Sie sich mit Ihren JumpCloud-Anmeldedaten 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.