bitwarden | Hilfezentrum Artikel

ADMINISTRATOR KONSOLE › MELDEN SIE SICH MIT SSO AN ›

OneLogin SAML Implementierung

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

OneLogin SAML Implementierung

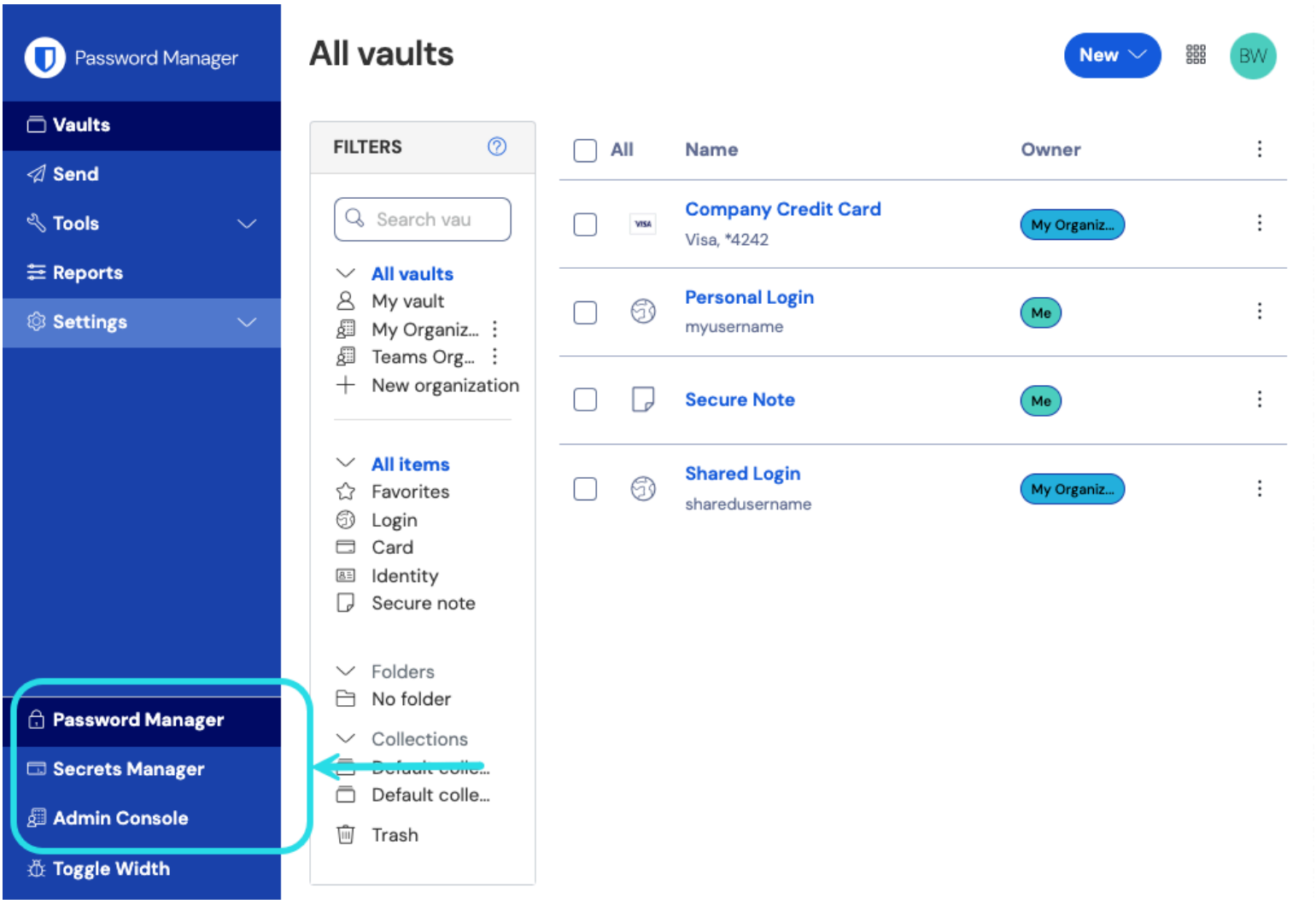
Dieser Artikel enthält **OneLogin-spezifische** Hilfe zur Konfiguration der Zugangsdaten mit SSO über SAML 2.0. Für Hilfe bei der Konfiguration der Zugangsdaten mit SSO für einen anderen IdP, verweisen Sie auf SAML 2.0 Konfiguration.

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

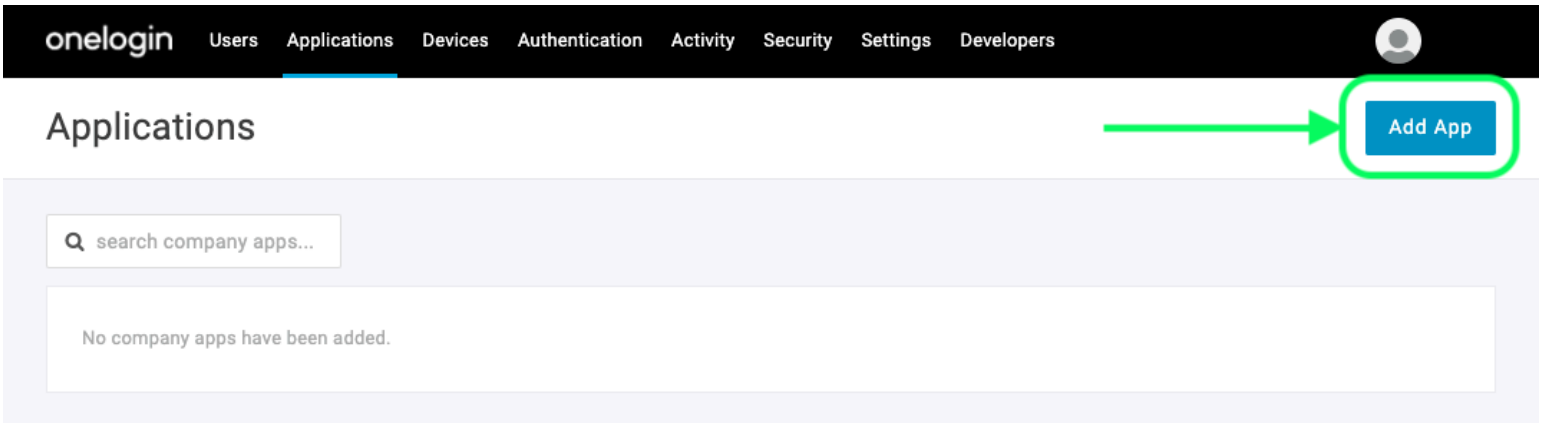
Wenn Sie es noch nicht getan haben, erstellen Sie einen einzigartigen **SSO-Identifikator** für Ihre Organisation und wählen Sie **SAML** aus dem **Typ**-Dropdown aus. Lassen Sie diesen Bildschirm geöffnet für eine einfache Referenz.

Sie können die Option **Einen eindeutigen SP-Entity-ID festlegen** 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.

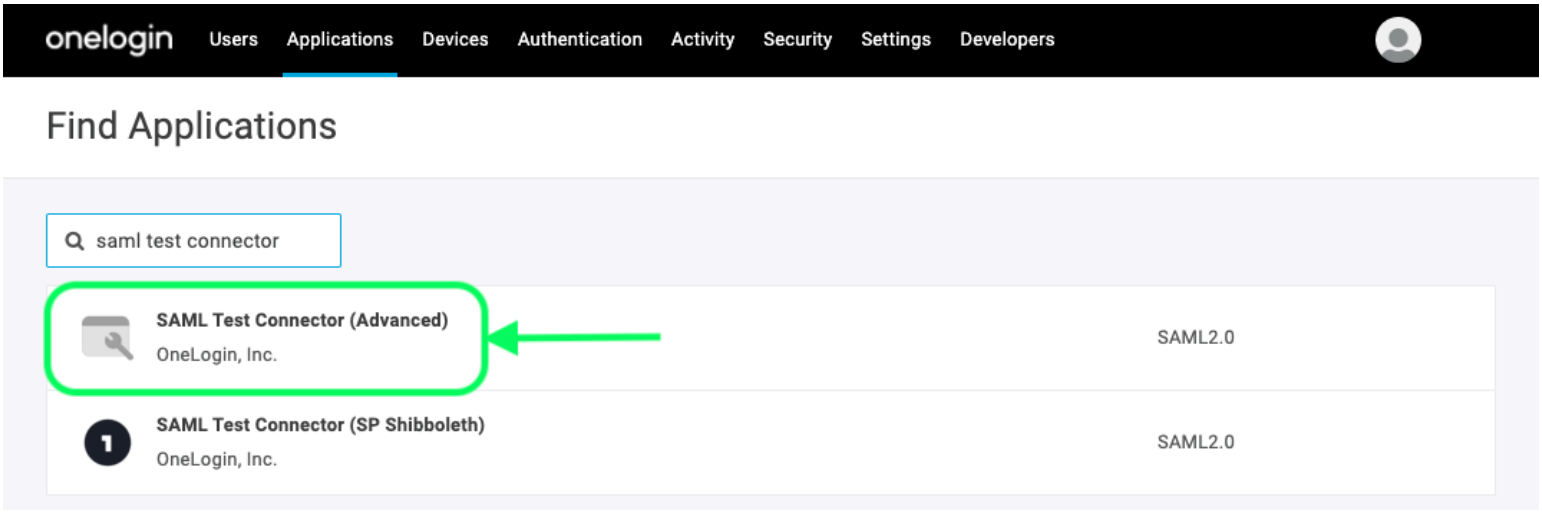
Erstellen Sie eine OneLogin-App

Im OneLogin Portal navigieren Sie zum **Anwendungen** Bildschirm und wählen Sie die Schaltfläche **App hinzufügen**:



Add an Application

Geben Sie in der Suchleiste `saml test connector` ein und wählen Sie die **SAML Test Connector (Advanced)** App aus:

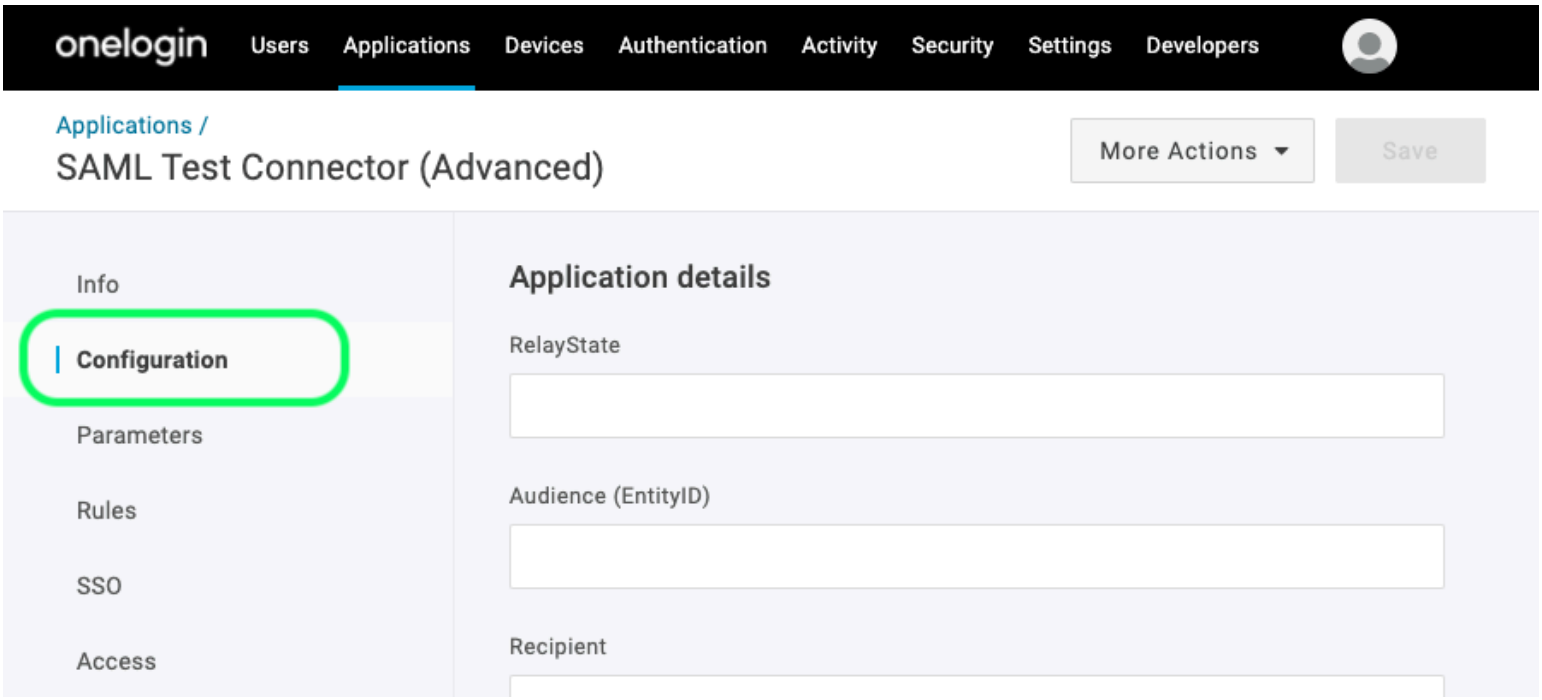


SAML Test Connector App

Geben Sie Ihrer Anwendung einen Bitwarden-spezifischen **Anzeigenamen** und wählen Sie die **Speichern** Schaltfläche.

Konfiguration

Wählen Sie **Konfiguration** aus der linken Navigation aus und konfigurieren Sie die folgenden Informationen, einige davon müssen Sie vom Single Sign-On-Bildschirm abrufen:



App Configuration

Anwendungseinstellungen	Beschreibung
Publikum (EntityID)	Setzen Sie dieses Feld auf die vorab generierte **SP Entity ID**. Dieser automatisch generierte Wert kann aus der **Einstellungen → Single Sign-On** Bildschirm der Organisation kopiert werden und variiert je nach Ihrer Konfiguration.
Empfänger	Setzen Sie dieses Feld auf die gleiche vorab generierte **SP Entity ID** , die für die **Audience (Entity ID)** Einstellung verwendet wurde.
ACS (Verbraucher) URL-Validator	Obwohl es von OneLogin als **Erforderlich** markiert ist, müssen Sie tatsächlich keine Informationen in dieses Feld eingeben, um sich mit Bitwarden zu integrieren. Springen Sie zum nächsten Feld, **ACS (Verbraucher) URL**.
ACS (Verbraucher) URL	Setzen Sie dieses Feld auf die vorab generierte **Assertion Consumer Service (ACS) URL**. Dieser automatisch generierte Wert kann aus der **Einstellungen → Single Sign-On** Bildschirm der Organisation kopiert werden und variiert je nach Ihrer Konfiguration.

Anwendungseinstellungen	Beschreibung
SAML-Initiator	Wählen Sie **Dienstleister** aus. Die Anmeldung mit SSO unterstützt derzeit keine von IdP initiierten SAML-Behauptungen.
SAML NameID Format	Setzen Sie dieses Feld auf das SAML NameID Format, das Sie für SAML-Behauptungen verwenden möchten.
SAML-Signaturelement	Standardmäßig wird OneLogin die SAML-Antwort signieren. Sie können dies auf **Behauptung** oder **Beide** einstellen.

Wählen Sie die Schaltfläche **Speichern**, um Ihre Konfigurationseinstellungen abzuschließen.

Parameter

Wählen Sie **Parameter** aus der linken Navigation aus und verwenden Sie das + **Hinzufügen** Symbol, um die folgenden benutzerdefinierten Parameter zu erstellen:

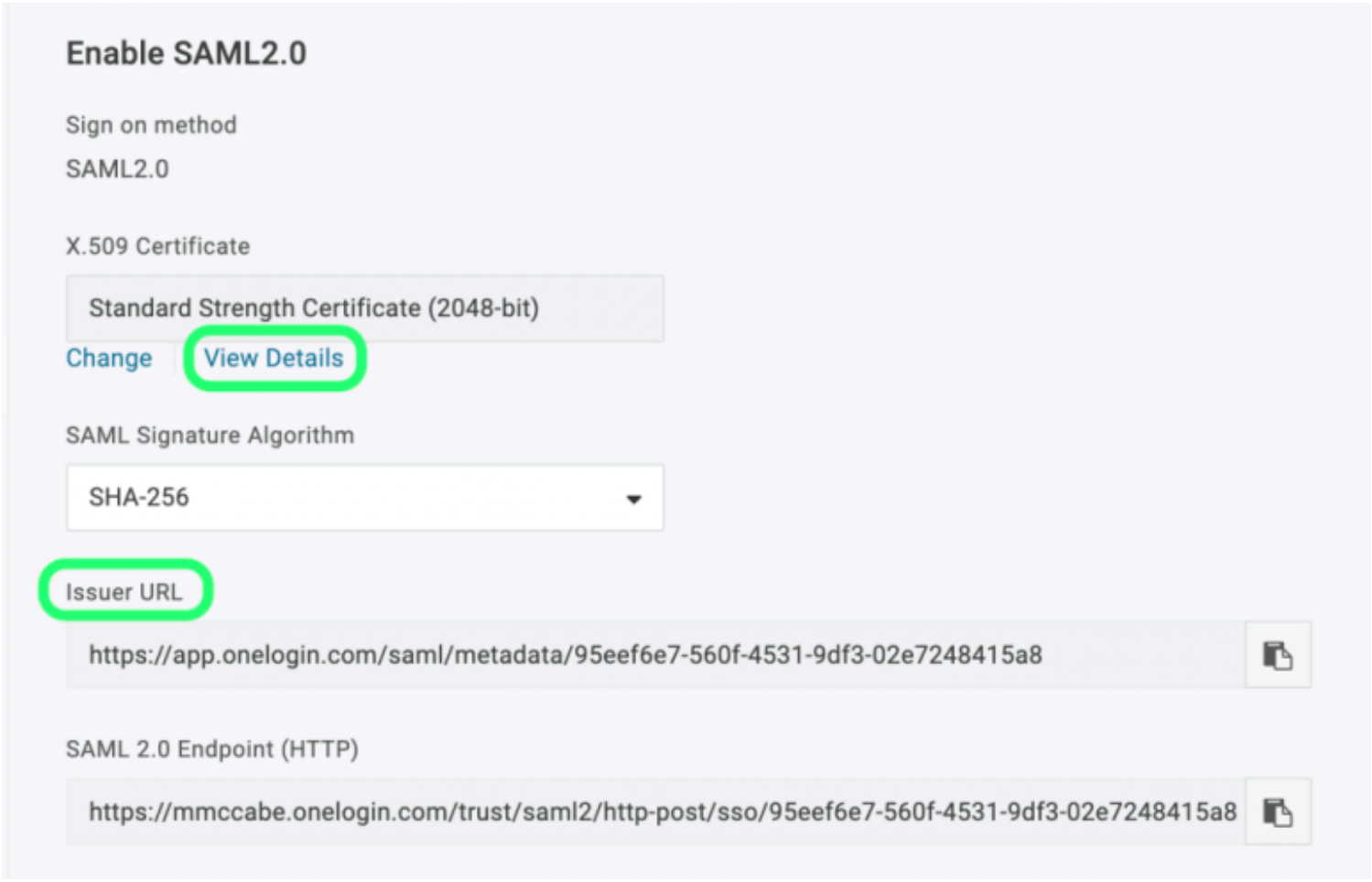
Feldname	Wert
E-Mail-Adresse	E-Mail
Vorname	Vorname
Nachname	Nachname

Wählen Sie die Schaltfläche **Speichern**, um Ihre benutzerdefinierten Parameter abzuschließen.

SSO

Wählen Sie **SSO** aus der linken Navigation aus und vervollständigen Sie Folgendes:

1. Wählen Sie den Link **Details anzeigen** unter Ihrem X.509-Zertifikat:



View your Cert

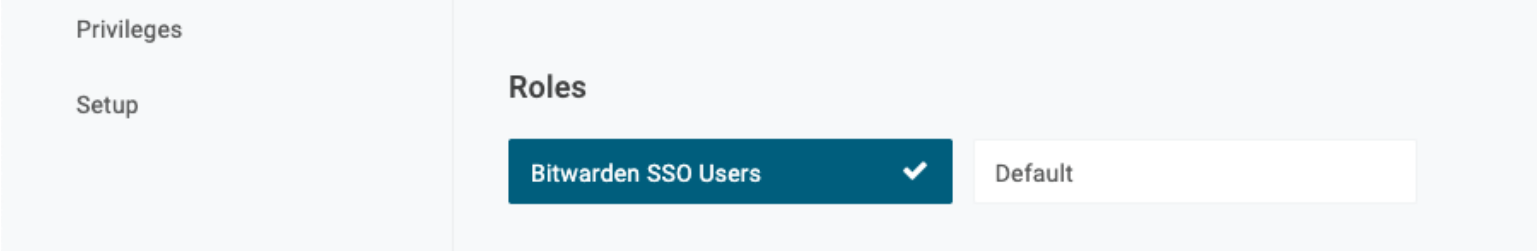
Auf dem Zertifikatsbildschirm, laden Sie Ihr X.509 PEM-Zertifikat herunter oder kopieren Sie es, da Sie es später verwenden müssen. Einmal kopiert, kehren Sie zum Haupt-SSO-Bildschirm zurück.

2. Stellen Sie Ihren **SAML-Signaturalgorithmus** ein.

3. Notieren Sie sich Ihre **Aussteller-URL** und **SAML 2.0-Endpunkt (HTTP)**. Sie werden diese Werte bald benötigen.

Zugriff

Wählen Sie **Zugang** aus der linken Navigation aus. Im Abschnitt **Rollen** weisen Sie allen Rollen, die Sie für die Nutzung von Bitwarden verwenden möchten, den Zugriff auf die Anwendung zu. Die meisten Implementierungen erstellen eine Bitwarden-spezifische Rolle und wählen stattdessen die Zuweisung basierend auf einer allgemeinen Lösung (zum Beispiel, **Standard**) oder basierend auf bereits bestehenden Rollen.



Role Assignment

Zurück zur Web-App

Bis zu diesem Zeitpunkt haben Sie alles, was Sie im Kontext des OneLogin 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

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

Feld	Beschreibung
Namens-ID-Format	Setzen Sie dieses Feld auf das, was Sie für das OneLogin **SAML nameID Format** Feld während der App-Konfiguration ausgewählt haben.
Ausgehendes Signatur-Algorithmus	Algorithmus, der zum Signieren von SAML-Anfragen verwendet wird, standardmäßig `sha-256`.
Unterzeichnungsverhalten	Ob/wann SAML-Anfragen signiert werden. Standardmäßig erfordert OneLogin keine Signatur für Anfragen.
Minimales Eingehendes Signatur-Algorithmus	Setzen Sie dieses Feld auf das, was Sie für den **SAML-Signaturalgorithmus** während der App-Konfiguration ausgewählt haben.
Möchte Behauptungen unterschrieben haben	Markieren Sie dieses Kästchen, wenn Sie das **SAML-Signaturelement** in OneLogin auf **Behauptung** oder **Beides** während der App-Konfiguration eingestellt 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, die richtigen 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 OneLogin Portal beziehen, um Anwendungswerte abzurufen:

Feld	Beschreibung
Entitäts-ID	Geben Sie Ihre OneLogin **Issuer URL** ein, die Sie vom OneLogin App SSO Bildschirm abrufen können. Dieses Feld ist Groß- und Kleinschreibungssensitiv.
Bindungsart	Einstellen auf **HTTP Post** (wie im SAML 2.0 Endpoint (HTTP) angegeben).
Einmaliges Anmelden Service URL	Geben Sie Ihren OneLogin **SAML 2.0 Endpunkt (HTTP)** ein, den Sie vom OneLogin App SSO Bildschirm abrufen können.
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 abgerufene X.509 Zertifikat ein, entfernen Sie
	`-----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 Signaturalgorithmus	Wählen Sie den SAML-Signaturalgorithmus aus, der im Abschnitt OneLogin SSO-Konfiguration ausgewählt wurde.
Deaktivieren Sie ausgehende Abmeldeanfragen	Die Anmeldung mit SSO unterstützt derzeit **nicht** SLO. Diese Option ist für zukünftige Entwicklungen geplant.
Möchte Authentifizierungsanfragen signiert haben	Ob OneLogin erwartet, dass SAML-Anfragen signiert werden.

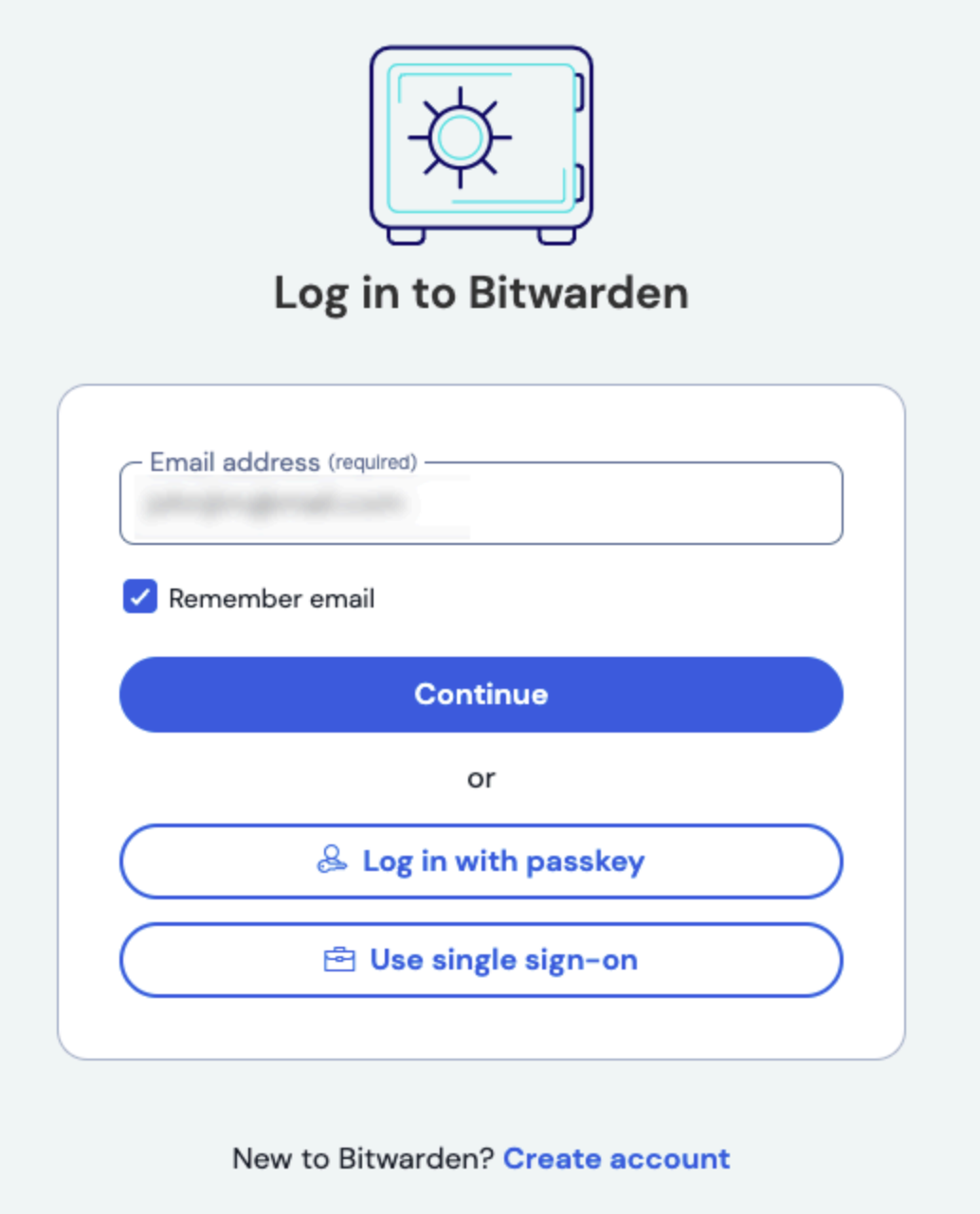
> **Note**
>
> Bei der Ausstellung des X509-Zertifikats, machen Sie eine Notiz vom Ablaufdatum. Zertifikate müssen erneuert werden, um jegliche Unterbrechungen im Dienst für SSO-Endbenutzer zu verhindern. Wenn ein Zertifikat abgelaufen ist, können sich Administrator- und Eigentümer-Konten immer mit E-Mail-Adresse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

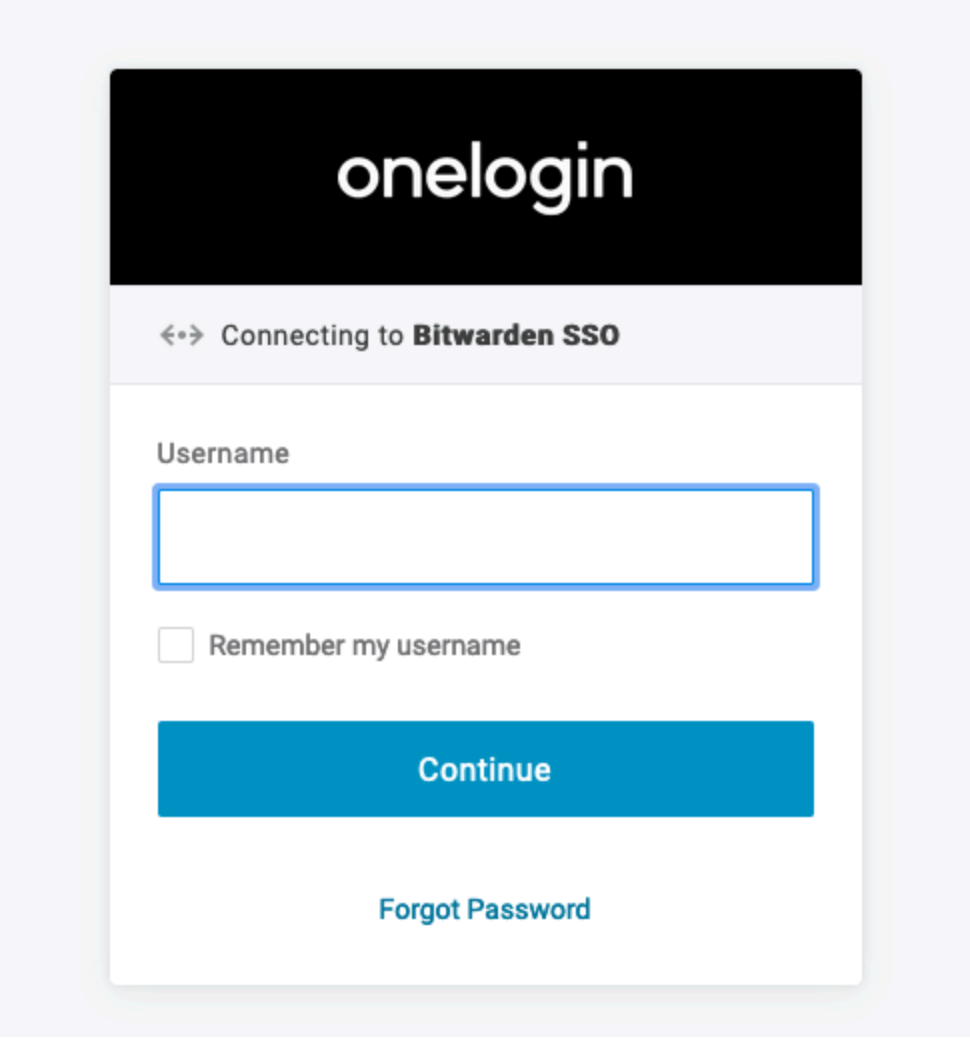
Testen Sie die Konfiguration

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 OneLogin Zugangsdaten-Bildschirm weitergeleitet:



OneLogin Login

Nachdem Sie sich mit Ihren OneLogin-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.