bitwarden | Hilfezentrum Artikel

ADMINISTRATOR KONSOLE > MELDEN SIE SICH MIT SSO AN

SAML 2.0 Konfiguration

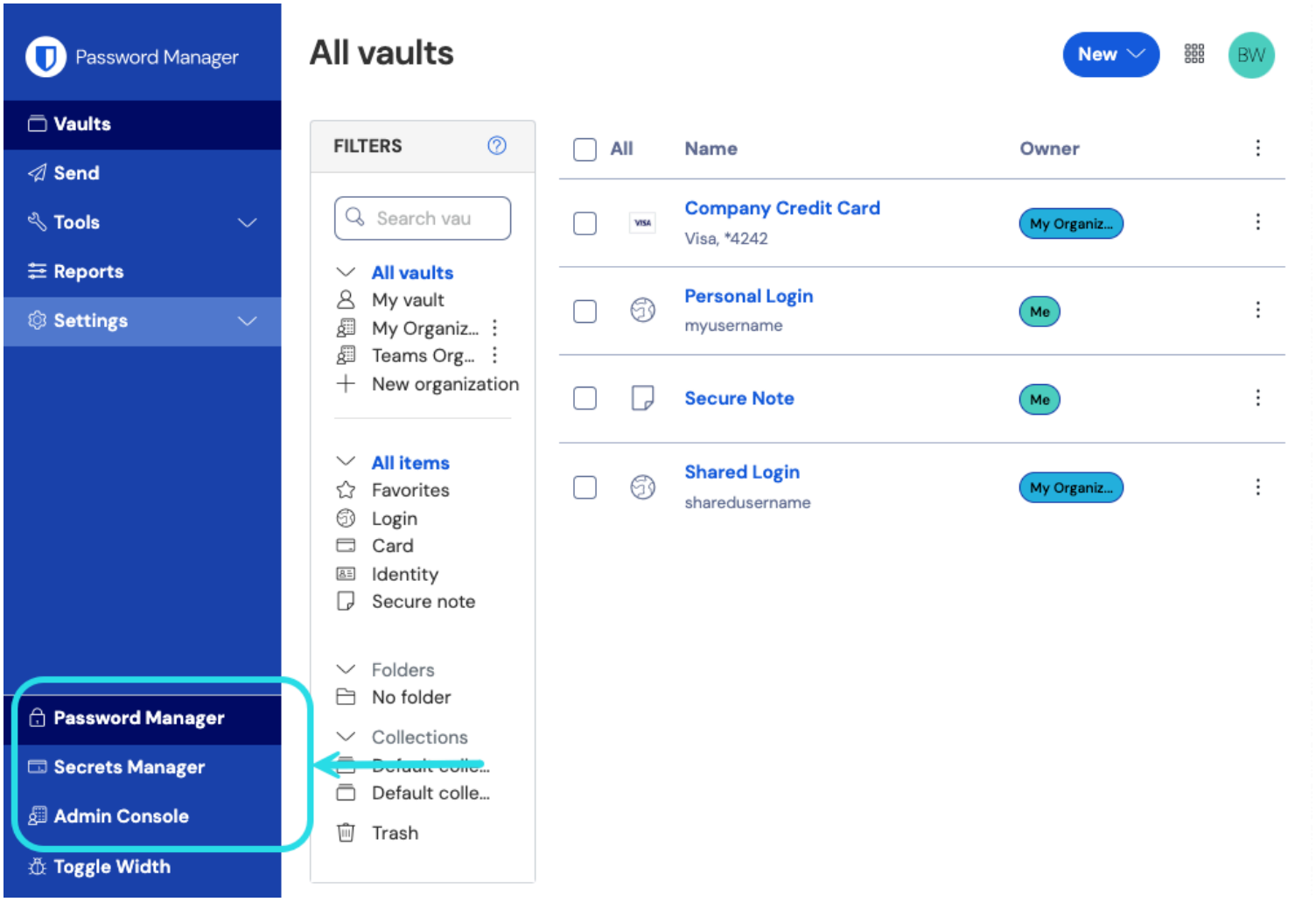
Ansicht im Hilfezentrum:
https://bitwarden.com/help/configure-sso-saml/

SAML 2.0 Konfiguration

Schritt 1: Legen Sie einen SSO-Identifikator fest

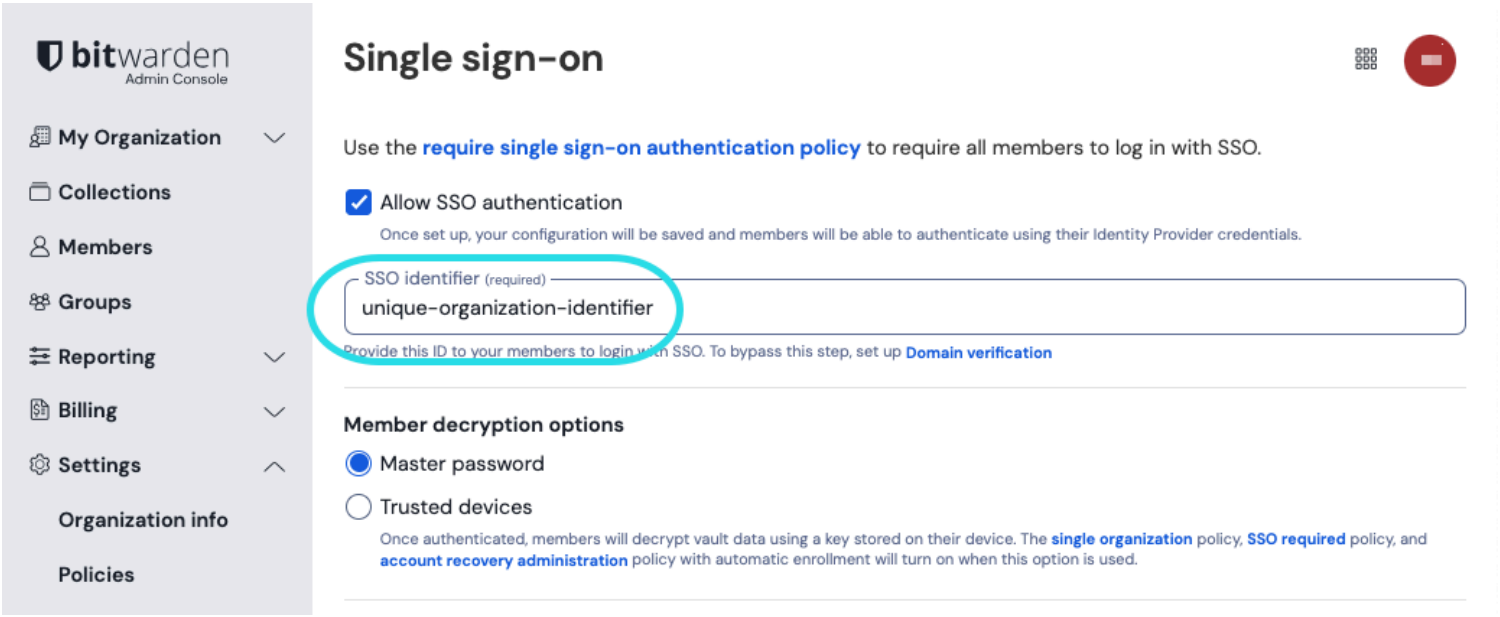
Benutzer, die ihre Identität mit SSO authentifizieren, müssen einen **SSO-Identifikator** eingeben, der die Organisation (und daher die SSO-Integration) zur Authentifizierung angibt. Um einen einzigartigen SSO-Identifier festzulegen:

1. Melden Sie sich bei der Bitwarden Web-App an und öffnen Sie die Administrator-Konsole mit dem Produktumschalter (▦):



Produktwechsler

2. Navigieren Sie zu **Einstellungen** → **Einmaliges Anmelden** und geben Sie einen eindeutigen **SSO-Identifier** für Ihre Organisation ein:



Geben Sie einen Bezeichner ein

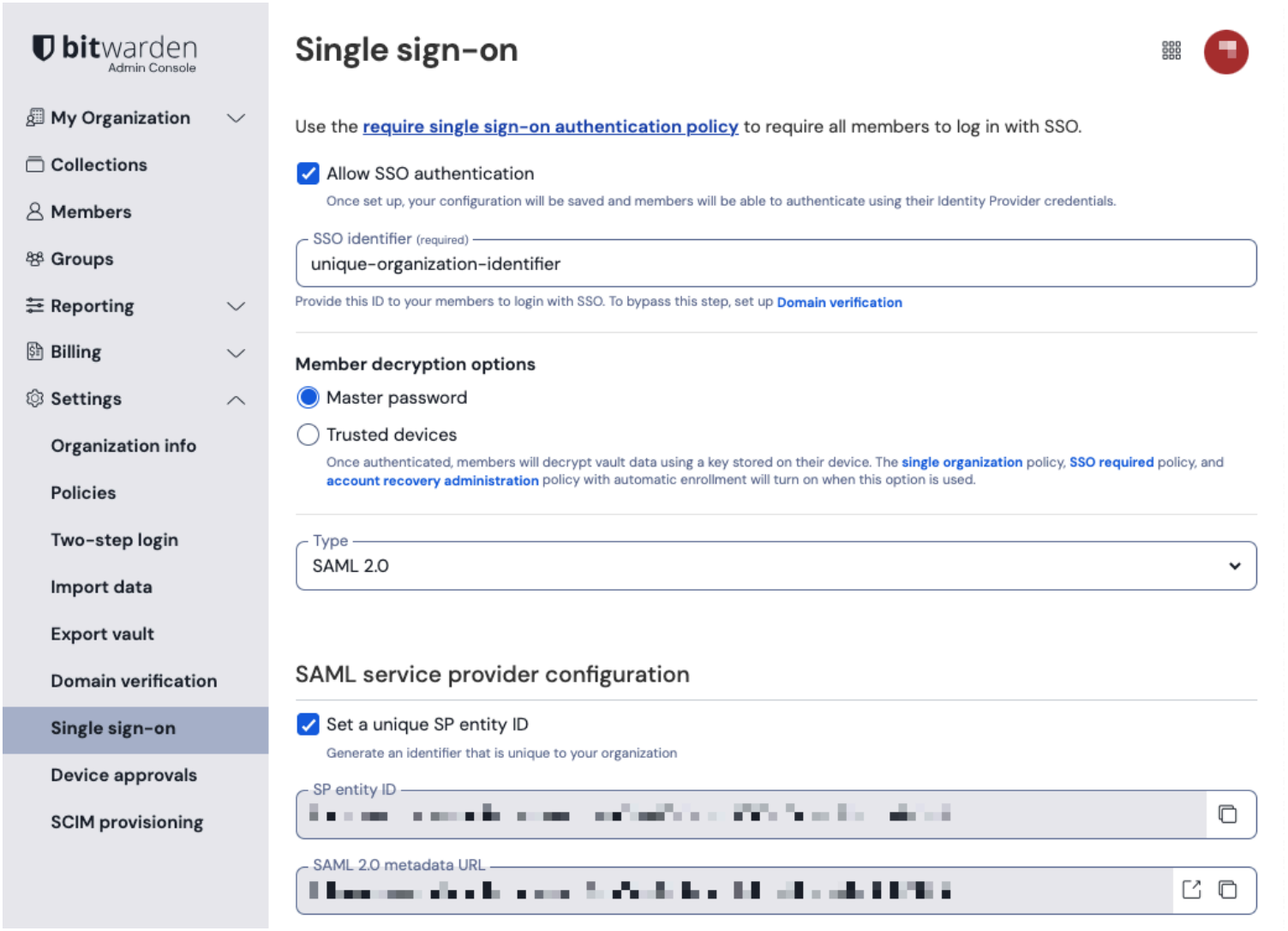
3. Fahren Sie fort zu **Schritt 2: Aktivieren Sie die Zugangsdaten mit SSO**.

> **Tip**
> You will need to share this value with users once the configuration is ready to be used.

Schritt 2: Aktivieren Sie die Zugangsdaten mit SSO

Sobald Sie Ihren SSO-Identifier haben, können Sie mit der Aktivierung und Konfiguration Ihrer Integration fortfahren. Um die Anmeldung mit SSO zu ermöglichen:

1. Auf der **Einstellungen** → **Single Sign-On** Ansicht, markieren Sie das **SSO-Authentifizierung erlauben** Kontrollkästchen:



SAML 2.0 Konfiguration

2. Wählen Sie aus dem Dropdown-Menü **Typ** die Option **SAML 2.0** aus. Wenn Sie stattdessen OIDC verwenden möchten, wechseln Sie zum OIDC Konfigurationshandbuch.

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.

Schritt 3: Konfiguration

Ab diesem Zeitpunkt wird die Umsetzung von Anbieter zu Anbieter variieren. Springen Sie zu einem unserer spezifischen **Implementierungsleitfäden** für Hilfe bei der Abschluss des Konfigurationsprozesses:

Anbieter	Leitfaden
AD FS	AD FS Implementierungsleitfaden
Auth0	Auth0 Implementierungsleitfaden
AWS	AWS Implementierungsleitfaden
Azur	Azure Implementierungsleitfaden
Duo	Duo Implementierungsleitfaden
Google	Google Implementierungsleitfaden
JumpCloud	JumpCloud Implementierungsleitfaden
Keycloak	Keycloak Implementierungsleitfaden
Okta	Okta Implementierungsleitfaden
OneLogin	OneLogin Implementierungsleitfaden
PingFederate	PingFederate Implementierungsleitfaden

Konfigurationsreferenzmaterialien

Die folgenden Abschnitte definieren die verfügbaren Felder während der Konfiguration der Einmalanmeldung, unabhängig davon, mit welchem IdP Sie sich integrieren. Felder, die konfiguriert werden müssen, werden markiert (**erforderlich**).

> **Tip**
>
> **Unless you are comfortable with SAML 2.0**, we recommend using one of the above implementation guides instead of the following generic material.

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

- Die Konfiguration des **SAML Service Providers** bestimmt das Format der SAML-Anfragen.
- Die Konfiguration des **SAML Identität Anbieters** bestimmt das erwartete Format für SAML-Antworten.

Konfiguration des Dienstanbieters

Feld	Beschreibung
SP-Entitäts-ID	(**Automatisch generiert**) Der Bitwarden-Endpunkt für Authentifizierungsanfragen. Dieser automatisch generierte Wert kann aus der **Einstellungen** → **Single Sign-On** Bildschirm der Organisation kopiert werden und variiert je nach Ihrer Konfiguration.
SAML 2.0 Metadaten-URL	(**Automatisch generiert**) Metadaten-URL für den Bitwarden-Endpunkt. Dieser automatisch generierte Wert kann von der **Einstellungen** → **Single Sign-On** Seite der Organisation kopiert werden und variiert je nach Ihrer Konfiguration.
Assertion Consumer Service (ACS) URL	(**Automatisch generiert**) Ort, von dem aus die SAML-Behauptung vom IdP gesendet wird. Dieser automatisch generierte Wert kann von der **Einstellungen** → **Single Sign-On** Seite der Organisation kopiert werden und variiert je nach Ihrer Konfiguration.
Namens-ID-Format	Format, den Bitwarden von der SAML-Behauptung anfordert. Muss als Zeichenkette ausgegeben werden. Optionen beinhalten: -Unspezifiziert (Standard) -E-Mail-Adresse -X.509 Subjektname -Qualifizierter Name der Windows-Domain -Kerberos-Principal-Name -Entitätskennzeichnung -Beharrlich -Flüchtig

Feld	Beschreibung
Ausgehendes Signatur-Algorithmus	Der Algorithmus, den Bitwarden zur Signierung von SAML-Anfragen verwenden wird. Optionen beinhalten: - `http://www.w3.org/2001/04/xmldsig-more#rsa-sha256` (Standard) - `http://www.w3.org/2000/09/xmldsig#rsa-sha1` - `http://www.w3.org/2000/09/xmldsig#rsa-sha384` - `http://www.w3.org/2000/09/xmldsig#rsa-sha512`
Unterzeichnungsverhalten	Ob/wann SAML-Anfragen signiert werden. Optionen beinhalten: -Wenn IdP signierte Authn-Anfragen wünscht (Standard) -Immer -Niemals
Mindesteingehendes Signaturalgorithmus	Minimale Stärke des Algorithmus, den Bitwarden in SAML-Antworten akzeptieren wird.
Erwarte signierte Behauptungen	Aktivieren Sie dieses Kontrollkästchen, wenn Bitwarden erwarten soll, dass die Antworten vom IdP signiert werden.
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.

Identität Anbieter Konfiguration

Feld	Beschreibung
Entitäts-ID	(**Erforderlich**) Adresse oder URL Ihres Identitätsservers oder die Identität des IdP Entity ID. Dieses Feld ist Groß- und Kleinschreibungssensitiv und muss genau dem IdP-Wert entsprechen.
Bindungsart	Methode, die vom IdP verwendet wird, um auf Bitwarden SAML-Anfragen zu antworten. Optionen beinhalten: -Umleitung (empfohlen) -HTTP POST

Feld	Beschreibung
Einmaliges Anmelden Service URL	(**Erforderlich, wenn die Entitäts-ID keine URL ist**) SSO-URL, die von Ihrem IdP ausgegeben wurde.
URL des Einzelabmeldedienstes	Die Anmeldung mit SSO unterstützt derzeit **nicht** SLO. Diese Option ist für die zukünftige Nutzung geplant, jedoch empfehlen wir dringend, dieses Feld vorzukonfigurieren.

X509 Öffentliches Zertifikat	(**Erforderlich**) Der X.509 Base-64 codierte Zertifikatskörper. Nicht einbeziehen
	
	`-----BEGIN ZERTIFIKAT-----`
	
	und
	
	`-----ENDE ZERTIFIKAT-----`
	
	Linien oder Teile des CER/PEM formatierten Zertifikats.
	
	Der Zertifikatswert ist Groß- und Kleinschreibungssensitiv, zusätzliche Leerzeichen, Zeilenumbrüche und andere überflüssige Zeichen in diesem Feld führen zu einer fehlgeschlagenen Zertifikatsvalidierung. Kopieren Sie **nur** die Zertifikatsdaten in dieses Feld.

Ausgehendes Signaturalgorithmus	Der Algorithmus, den Ihr IdP zur Signierung von SAML-Antworten/Behauptungen verwenden wird. Optionen beinhalten: - `http://www.w3.org/2001/04/xmldsig-more#rsa-sha256` (Standard) - `http://www.w3.org/2000/09/xmldsig#rsa-sha1` - `http://www.w3.org/2000/09/xmldsig#rsa-sha384` - `http://www.w3.org/2000/09/xmldsig#rsa-sha512`
Ausgehende Abmeldeanfragen erlauben	Die Anmeldung mit SSO unterstützt derzeit **nicht** SLO. Diese Option ist für die zukünftige Verwendung geplant, jedoch empfehlen wir dringend, dieses Feld vorzukonfigurieren.
Authentifizierungsanfragen signieren	Aktivieren Sie dieses Kontrollkästchen, wenn Ihr IdP erwarten sollte, dass SAML-Anfragen von Bitwarden 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.

SAML-Attribute & Ansprüche

Eine **E-Mail-Adresse ist für die Bereitstellung des Kontos erforderlich**, die als eines der Attribute oder Ansprüche in der folgenden Tabelle übergeben werden kann.

Eine eindeutige Benutzerkennung wird ebenfalls dringend empfohlen. Wenn abwesend, wird die E-Mail-Adresse stattdessen verwendet, um den Benutzer zu verlinken.

Attribute/Ansprüche sind in der Reihenfolge der Präferenz für die Übereinstimmung aufgelistet, einschließlich Ausweichmöglichkeiten, wo zutreffend:

Wert	Anspruch/Eigenschaft	Fallback-Anspruch/-Attribut
Eindeutige ID	NameID (wenn nicht vorübergehend) urn:oid:0.9.2342.19200300.100.1.1 Unter UID UPN EPPN	
E-Mail	E-Mail http://schemas.xmlsoap.org/ws/2005/05/identität/claims/emailadresse urn:oid:0.9.2342.19200300.100.1.3 Post E-Mail-Adresse	Bevorzugter_Benutzername Urn:oid:0.9.2342.19200300.100.1.1 UID
Name	Name http://schemas.xmlsoap.org/ws/2005/05/identität/claims/name urn:oid:2.16.840.1.113730.3.1.241 urn:oid:2.5.4.3 Anzeigename CN	Vorname + " " + Nachname (siehe unten)
Vorname	urn:oid:2.5.4.42 Vorname Vorname FN Vorname Spitzname	

Wert	Anspruch/Eigenschaft	Fallback-Anspruch/-Attribut
Nachname	urn:oid:2.5.4.4 SN Nachname Nachname	