bitwarden | Hilfezentrum Artikel

ADMINISTRATOR KONSOLE > MELDEN SIE SICH MIT SSO AN >

Google SAML Implementierung

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

Google SAML Implementierung

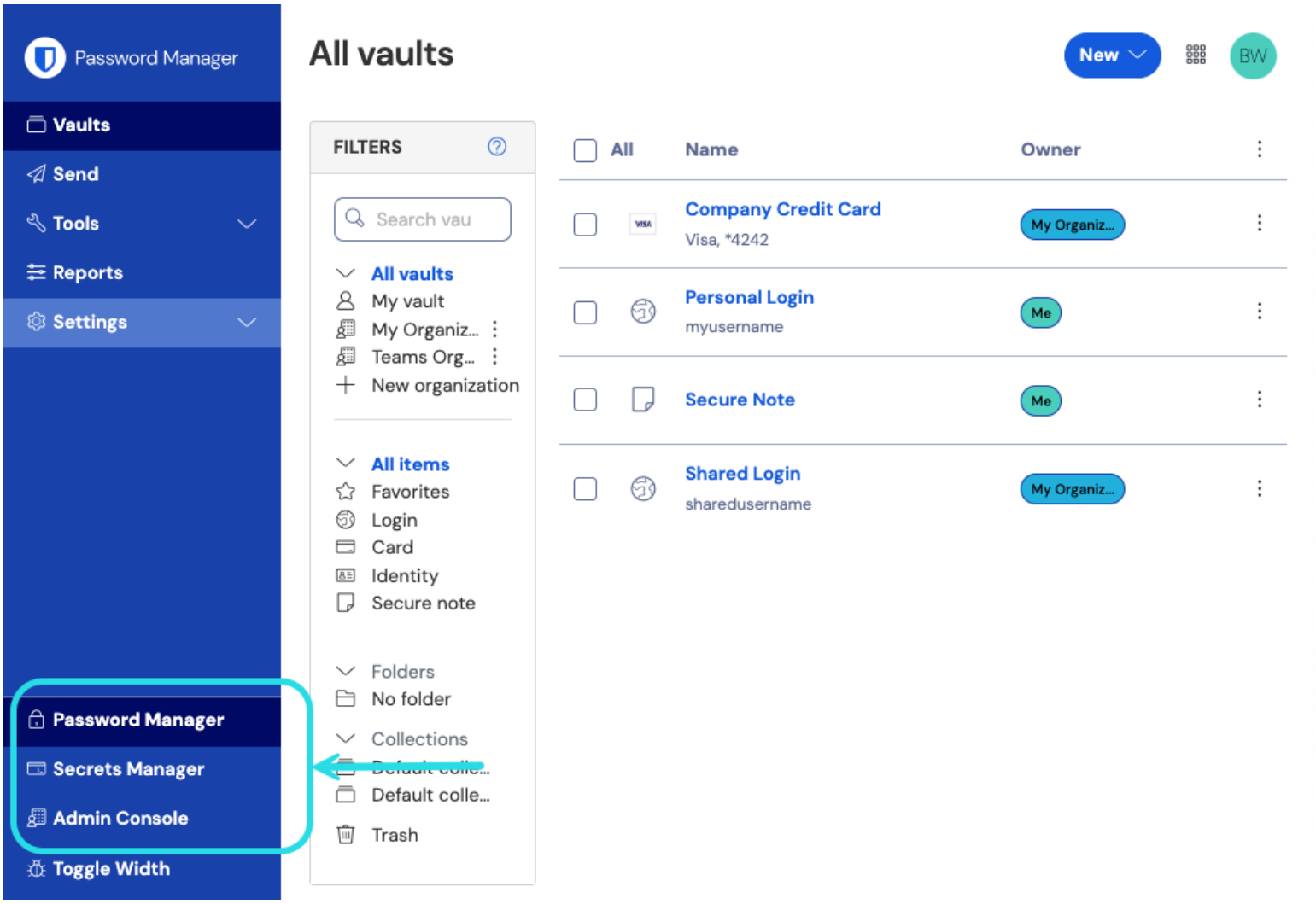
Dieser Artikel enthält **Google Workspace-spezifische** Hilfe zur Konfiguration der Zugangsdaten mit SSO über SAML 2.0. Für Hilfe bei der Konfiguration der Zugangsdaten mit SSO für einen anderen IdP, verweisen Sie auf SAML 2.0 Konfiguration.

Die Konfiguration beinhaltet die gleichzeitige Arbeit mit der Bitwarden-Web-App und der Google Workspace Administrator-Konsole. 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

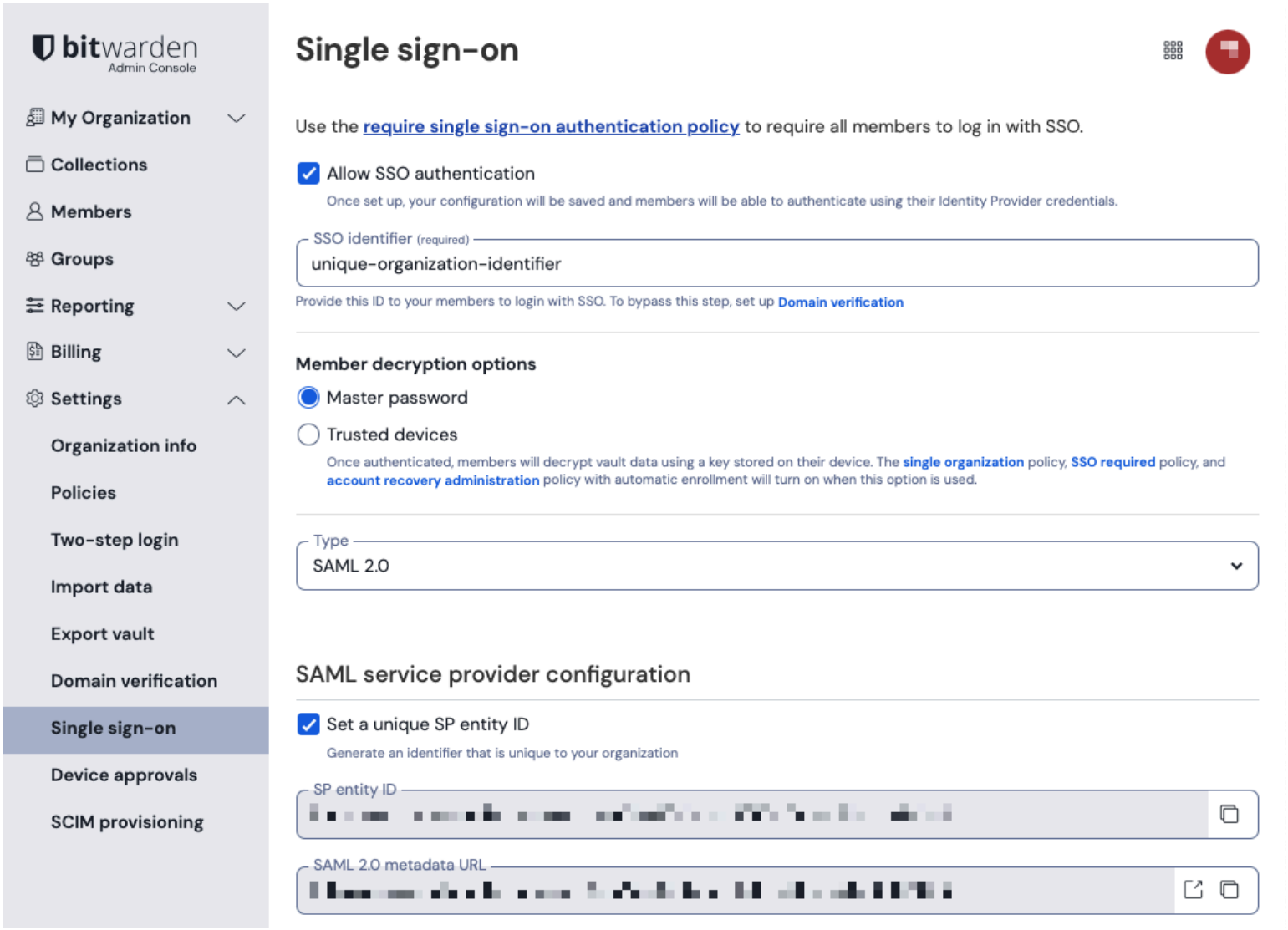
Öffnen Sie SSO in der Web-App

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



Produktwechsler

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



SAML 2.0 Konfiguration

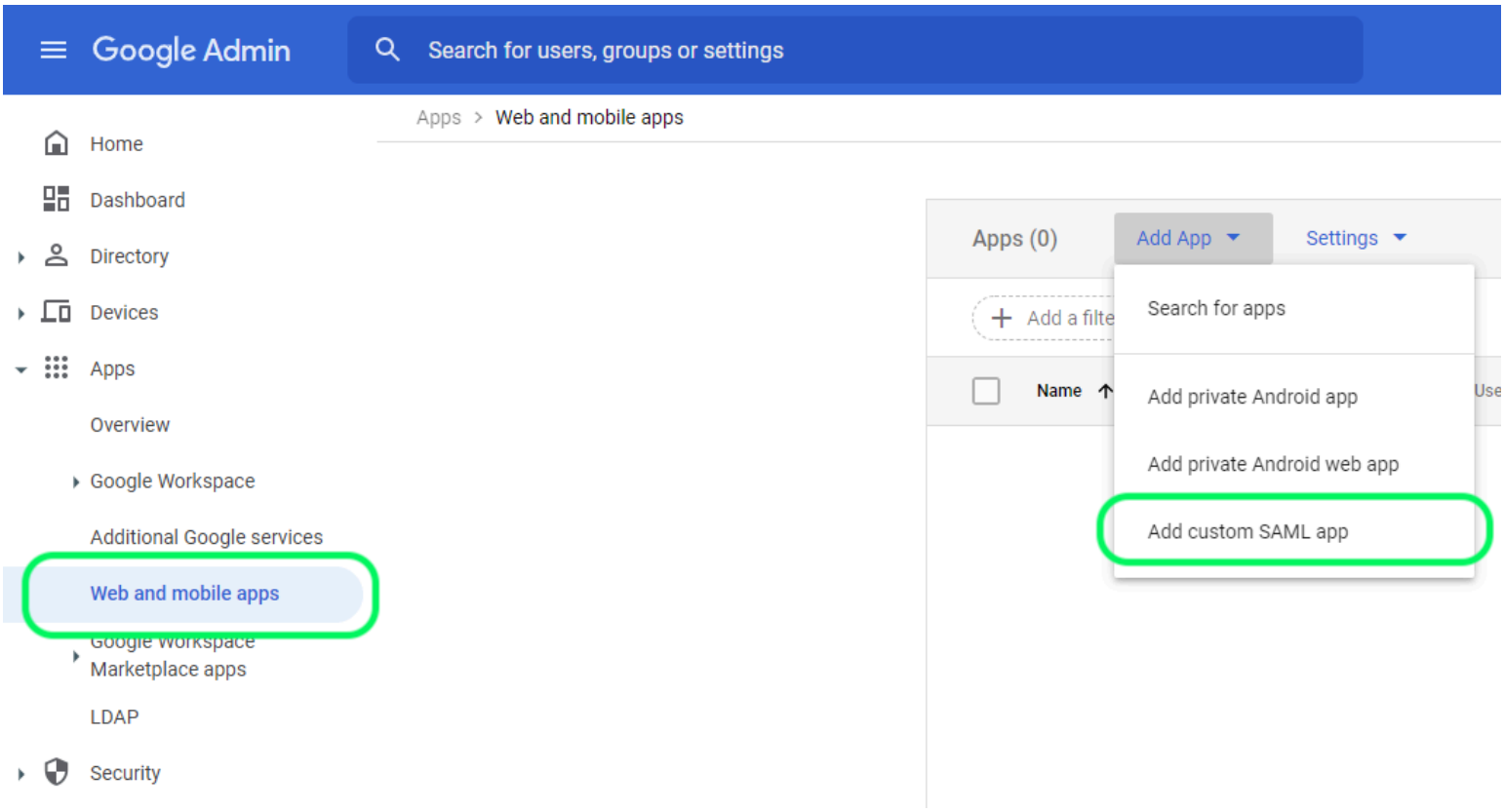
Wenn Sie es noch nicht getan haben, erstellen Sie einen einzigartigen **SSO-Identifikator** für Ihre Organisation und wählen Sie **SAML** aus dem **Typ**-Dropdown aus. Lassen Sie diesen Bildschirm geöffnet, um leicht darauf zugreifen zu können.

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 SAML-App

Im Google Workspace Administrator-Konsole, wählen Sie **Apps** → **Web- und mobile Apps** aus der Navigation. Auf dem Bildschirm für Web und mobile Apps, wählen Sie **App hinzufügen** → **Benutzerdefinierte SAML-App hinzufügen**:



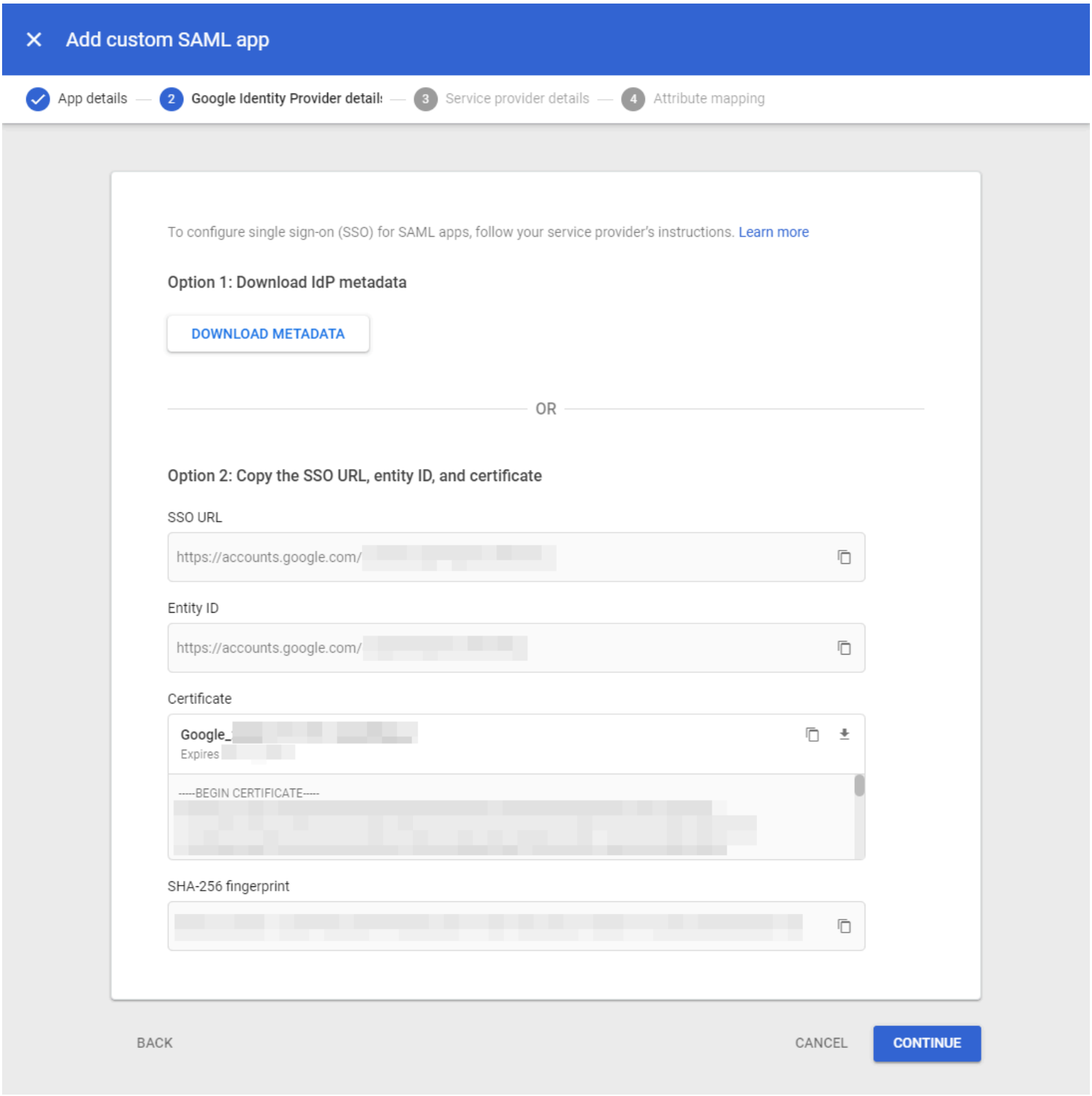
Create a SAML App

App-Details

Auf dem Bildschirm für App-Details geben Sie der Anwendung einen einzigartigen, speziell für Bitwarden bestimmten Namen und wählen Sie die Schaltfläche **Weiter**.

Details zum Google Identität Anbieter

Auf dem Google Identität Provider Details-Bildschirm, kopieren Sie Ihre **SSO URL**, **Entity ID** und **Zertifikat** für die Verwendung in einem späteren Schritt:



IdP Details

Wählen Sie **Weiter**, wenn Sie fertig sind.

Details zum Dienstleister

Auf dem Bildschirm für die Details des Dienstanbieters konfigurieren Sie die folgenden Felder:

Feld	Beschreibung
ACS-URL	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.
Entitäts-ID	Setzen Sie dieses Feld auf die vorab generierte **SP Entity ID**. Dieser automatisch generierte Wert kann von der **Einstellungen** → **Single Sign-On** Bildschirm der Organisation kopiert werden und variiert je nach Ihrer Konfiguration.
Start-URL	Optional können Sie dieses Feld auf die URL der Zugangsdaten setzen, von der aus Benutzer auf Bitwarden zugreifen werden. 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`.
Unterzeichnete Antwort	Markieren Sie dieses Kästchen, wenn Sie möchten, dass Workspace SAML-Antworten signiert. Wenn nicht überprüft, wird Workspace nur die SAML-Behauptung signieren.
Namen ID-Format	Stellen Sie dieses Feld auf **Persistent**.
Namens-ID	Wählen Sie das Benutzerattribut des Arbeitsbereichs aus, um NameID zu füllen.

Wählen Sie **Weiter**, wenn Sie fertig sind.

Attributzuordnung

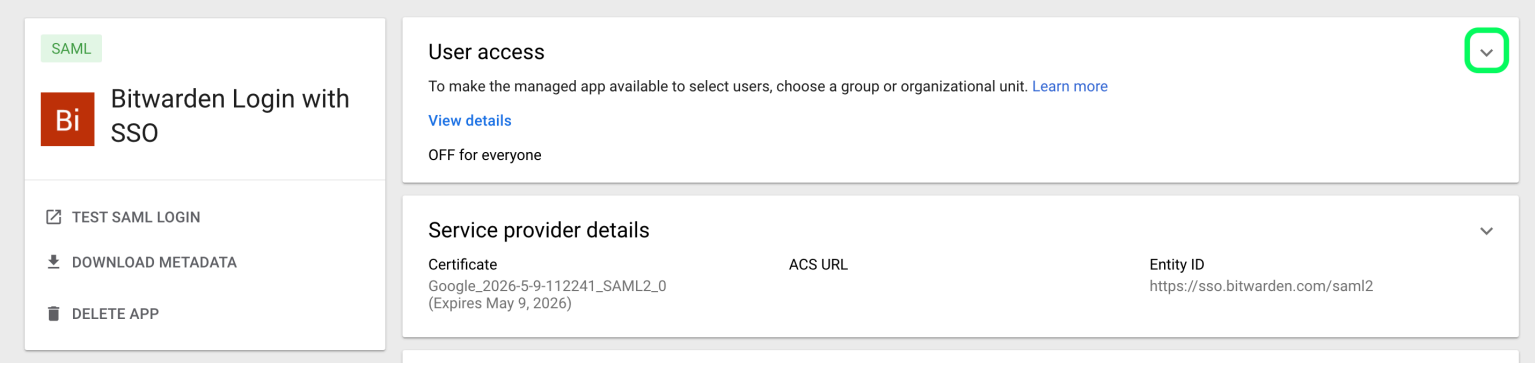
Auf dem Bildschirm für die Attributzuordnung wählen Sie die Schaltfläche **Zuordnung hinzufügen** und erstellen Sie die folgende Zuordnung:

Google Verzeichnisattribute	App-Attribute
Primäre E-Mail-Adresse	E-Mail-Adresse

Wählen Sie **Fertigstellen**.

Schalte die App ein

Standardmäßig werden Workspace SAML-Apps für alle **AUSGESCHALTET sein**. Öffnen Sie den Benutzerzugriffsbereich für die SAML-App und stellen Sie auf **EIN für alle** oder für spezifische Gruppen, je nach Ihren Bedürfnissen:



User Access

Speichern Sie Ihre Änderungen. Bitte beachten Sie, dass es bis zu 24 Stunden dauern kann, bis eine neue Workspace-App für die bestehenden Sitzungen der Benutzer verbreitet wird.

Zurück zur Web-App

Bis zu diesem Zeitpunkt haben Sie alles konfiguriert, was Sie im Kontext der Google Workspace Administrator-Konsole 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 gemäß den in der Workspace Administrator Konsole während der Einrichtung getroffenen Auswahlmöglichkeiten:

Feld	Beschreibung
Namens-ID-Format	Setzen Sie dieses Feld auf das Name ID-Format ausgewählt in Workspace.
Ausgehendes Signaturalgorithmus	Der Algorithmus, den Bitwarden zur Signierung von SAML-Anfragen verwenden wird.
Unterzeichnungsverhalten	Ob/wann SAML-Anfragen signiert werden.

Feld	Beschreibung
Mindesteingehendes Signaturalgorithmus	Standardmäßig wird Google Workspace mit RSA SHA-256 signieren. Wählen Sie `sha-256` aus dem Dropdown-Menü.
Signierte Assertions erwarten	Ob Bitwarden erwartet, dass SAML-Behauptungen signiert werden. Diese Einstellung sollte **nicht markiert** sein.
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 mit dem 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 die Workspace-Administrator-Konsole beziehen, um Anwendungswerte abzurufen:

Feld	Beschreibung
Entitäts-ID	Setzen Sie dieses Feld auf die **Entity ID** des Arbeitsbereichs, die Sie aus dem Abschnitt Details zum Google Identität Provider abgerufen oder mit der Schaltfläche **Metadaten herunterladen** verwendet haben. Dieses Feld ist Groß- und Kleinschreibungssensitiv.
Bindungsart	Einstellen auf **HTTP POST** oder **Weiterleitung**.
Einmaliges Anmelden Service URL	Setzen Sie dieses Feld auf die **SSO-URL** des Arbeitsbereichs, die Sie aus dem Abschnitt Google Identität Provider Details abgerufen haben oder verwenden Sie die Schaltfläche **Metadaten herunterladen**.
Einzelne Abmelden 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 Zertifikat ein und entfernen Sie es. `-----BEGIN ZERTIFIKAT-----`

Feld	Beschreibung
	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	Standardmäßig wird Google Workspace mit RSA SHA-256 signieren. Wählen Sie `sha-256` aus dem Dropdown-Menü.
Deaktivieren Sie ausgehende Abmeldeanfragen	Die Anmeldung mit SSO unterstützt derzeit **nicht** SLO. Diese Option ist für zukünftige Entwicklungen geplant.
Möchte Authentifizierungsanfragen signiert haben	Ob Google Workspace 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.

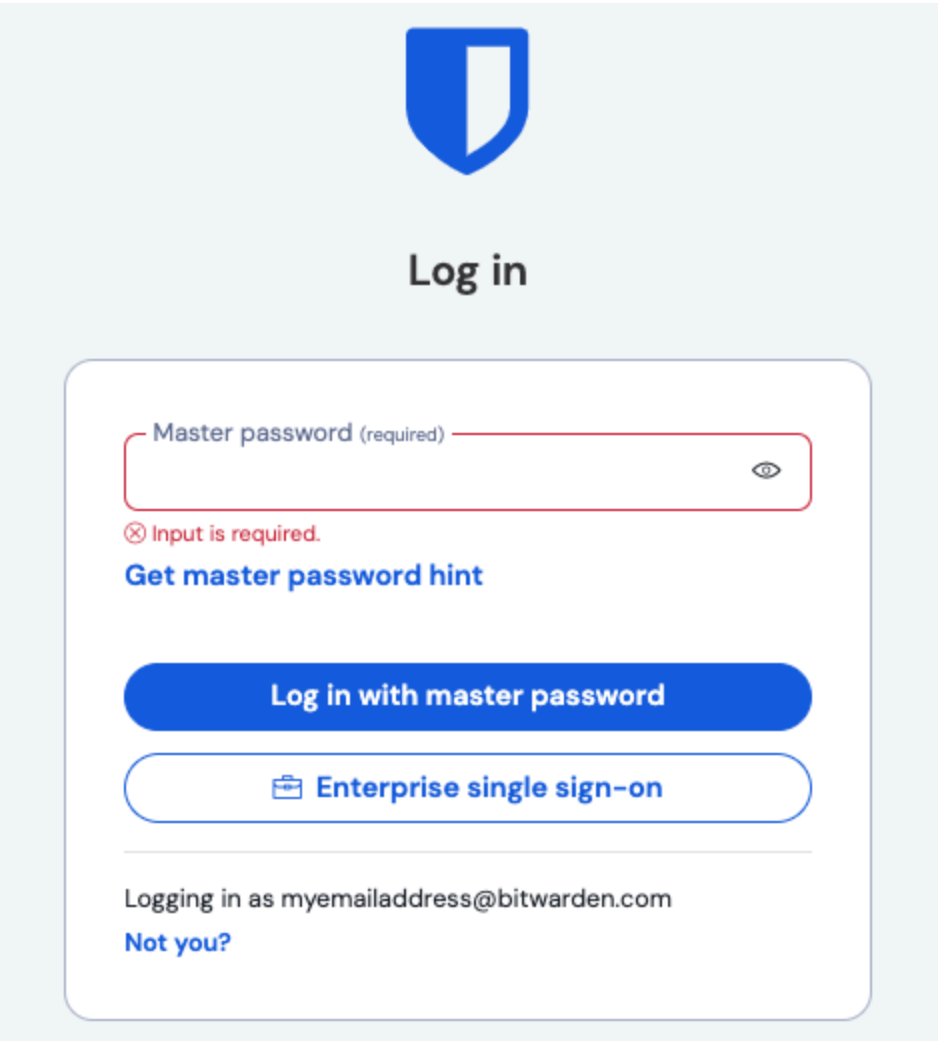
Wenn Sie mit der Konfiguration des Identitätsanbieters fertig sind, **speichern** Sie Ihre Arbeit.

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.

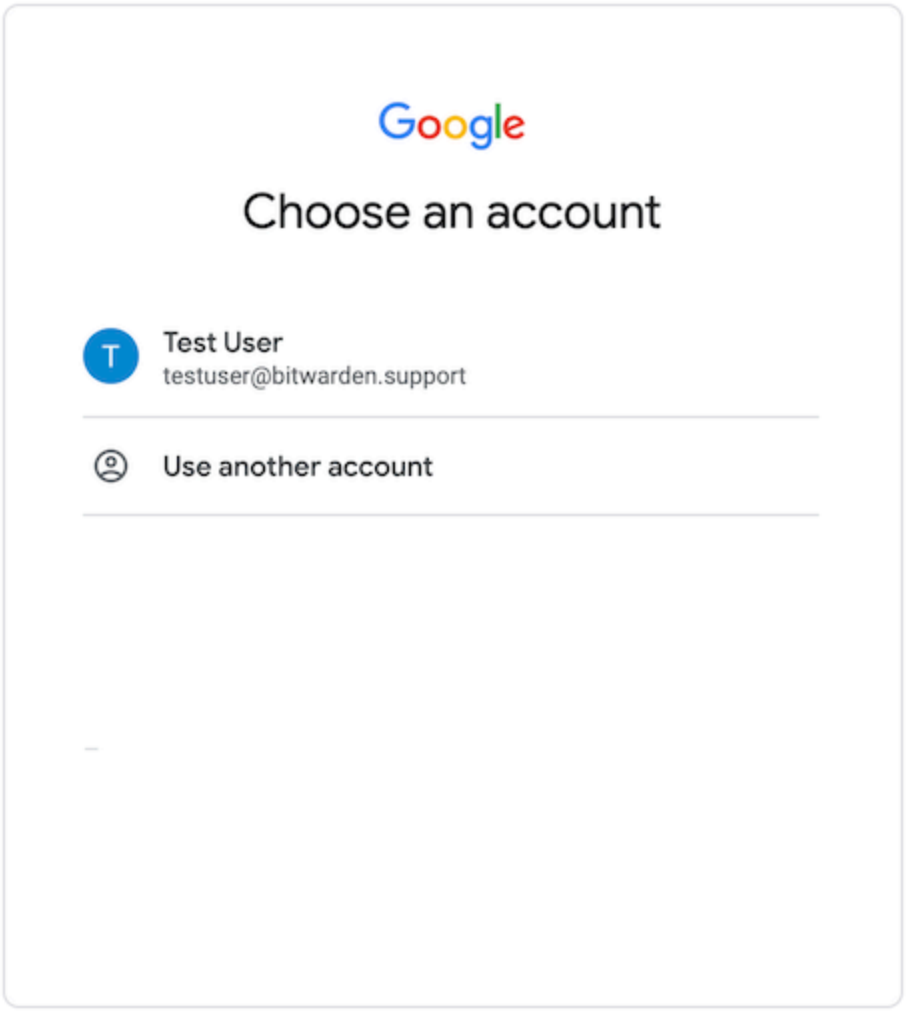
Testen Sie die Konfiguration

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 Google Workspace Zugangsdaten-Bildschirm weitergeleitet:



Login

Nachdem Sie sich mit Ihren Workspace-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.