

ADMINISTRATOR KONSOLE > MELDEN SIE SICH MIT SSO AN >

Microsoft Entra ID SAML Implementierung

Microsoft Entra ID SAML Implementierung

Dieser Artikel enthält **Azure-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 dem Azure-Portal. Während Sie fortfahren, empfehlen wir, beides griffbereit zu haben und die Schritte in der Reihenfolge durchzuführen, in der sie dokumentiert sind.

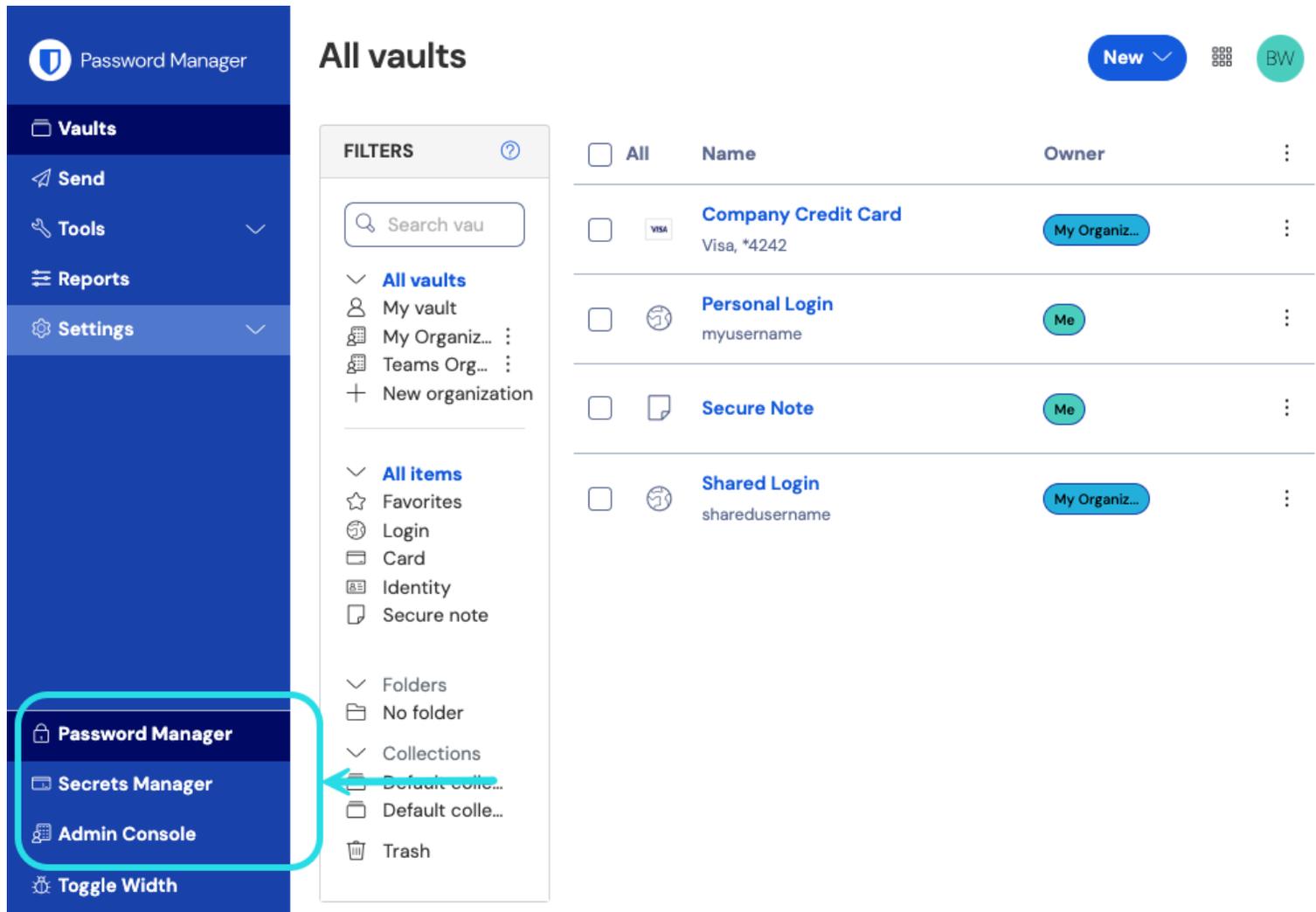
💡 Tip

Bereits ein SSO-Experte? Überspringen Sie die Anweisungen in diesem Artikel und laden Sie Screenshots von Beispielkonfigurationen herunter, um sie mit Ihren eigenen zu vergleichen.

↓ Typ: Asset-Hyperlink ID: 7CKe4TX98FPF86eAimKgak

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 :



<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login sharedusername	My Organiz...	⋮

Produktwechsler

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

Home >

Default Directory | Overview

Microsoft Entra ID

+ Add Manage tenants What's new Preview features Got feedback?

Overview Monitoring Properties Recommendations Tutorials

Search your tenant

Basic information

Name		Users
Tenant ID		Groups
Primary domain		Applications
License		Devices

Alerts



Microsoft Entra Connect v1 Retirement

All version 1.x builds of Microsoft Entra Connect (formerly AAD Connect) will soon stop working between October 2023 – March 2024. You must move to Cloud Sync or Microsoft Entra Connect v2.x.

[Learn more](#)



Azure AD is now Microsoft Entra ID

Microsoft Entra ID is the new name for Azure Active Directory. No action is required from you.

[Learn more](#)

Enterprise applications

Wählen Sie die **+ Neue Anwendung** Schaltfläche:

Create new application

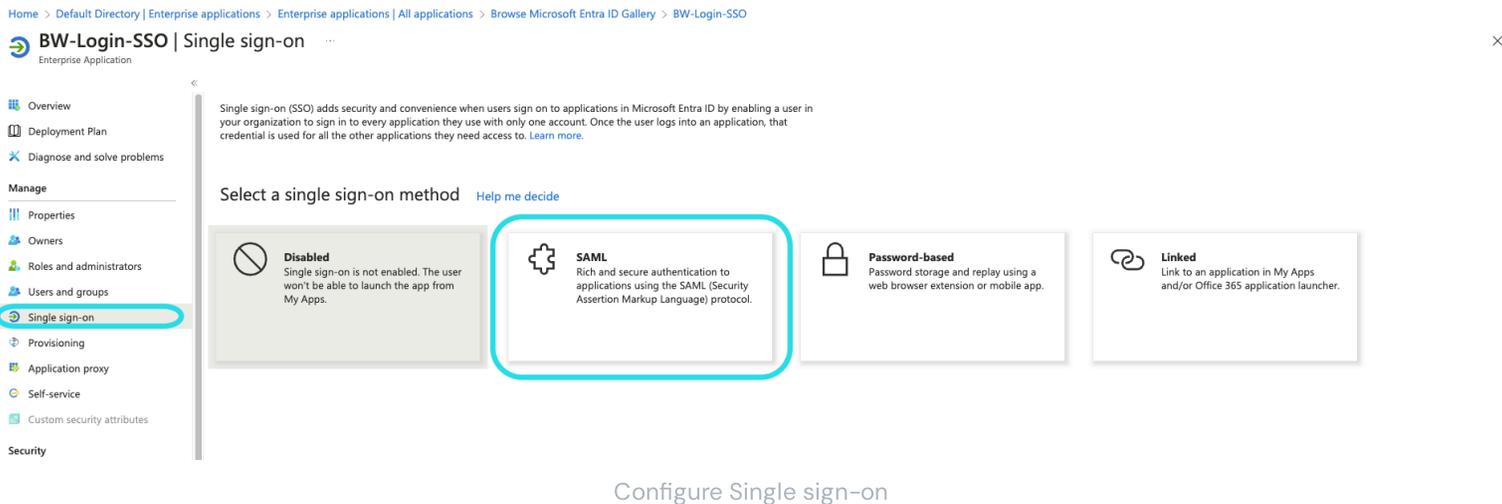
Auf dem Bildschirm Microsoft Entra ID Galerie durchsuchen, wählen Sie die Schaltfläche **+ Erstellen Sie Ihre eigene Anwendung**:

Create your own application

Auf dem Bildschirm "Erstellen Sie Ihre eigene Anwendung" geben Sie der Anwendung einen einzigartigen, Bitwarden-spezifischen Namen und wählen Sie die Option (Nicht-Galerie) aus. Wenn Sie fertig sind, klicken Sie auf die **Erstellen** Schaltfläche.

Einzelanmeldung aktivieren

Vom Anwendungsübersichtsbildschirm aus wählen Sie **Einmaliges Anmelden** aus der Navigation:



Auf dem Single Sign-On Bildschirm, wählen Sie **SAML**.

SAML-Einrichtung

Grundlegende SAML-Konfiguration

Wählen Sie die Schaltfläche **Bearbeiten** und konfigurieren Sie die folgenden Felder:

Feld	Beschreibung
Kennzeichner (Entitäts-ID)	<p>Setzen Sie dieses Feld auf die vorab generierte SP Entity ID.</p> <p>Dieser automatisch generierte Wert kann von der Einstellungen → Single Sign-On Bildschirm der Organisation kopiert werden und variiert je nach Ihrer Konfiguration.</p>
Antwort-URL (Assertion Consumer Service URL)	<p>Setzen Sie dieses Feld auf die vorab generierte Assertion Consumer Service (ACS) URL.</p> <p>Dieser automatisch generierte Wert kann von der Einstellungen → Single Sign-On Bildschirm der Organisation kopiert werden und variiert je nach Ihrer Konfiguration.</p>
Anmelden bei URL	<p>Legen Sie dieses Feld auf die Zugangsdaten-URL fest, von der aus Benutzer auf Bitwarden zugreifen werden.</p> <p>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://ihre-domain.com/#/sso.</p>

Benutzerattribute & Ansprüche

Die standardmäßig von Azure erstellten Ansprüche funktionieren mit den Zugangsdaten mit SSO, jedoch können Sie optional diesen Abschnitt verwenden, um das von Azure in SAML-Antworten verwendete NameID-Format zu konfigurieren.

Wählen Sie die **Bearbeiten** Schaltfläche und wählen Sie den **Eindeutigen Benutzeridentifikator (Name ID)** Eintrag, um den NameID Anspruch zu bearbeiten:

Attributes & Claims ...

[+ Add new claim](#)
[+ Add a group claim](#)
[☰ Columns](#)
[🗨️ Got feedback?](#)

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname

Advanced settings

Bearbeiten Sie die NameID-Anspruch

Optionen beinhalten Standard, E-Mail-Adresse, Beständig, Unspezifiziert und Windows qualifizierter Domain-Name. Für weitere Informationen, siehe [Microsoft Azure Dokumentation](#).

SAML-Signaturzertifikat

Laden Sie das Base64-Zertifikat für die Verwendung [in einem späteren Schritt](#) herunter.

Richten Sie Ihre Anwendung ein

Kopieren Sie oder machen Sie eine Notiz von der **URL der Zugangsdaten** und dem **Microsoft Entra ID Identifier** in diesem Abschnitt zur Verwendung [in einem späteren Schritt](#):

4

Set up BW-Login-SSO

You'll need to configure the application to link with Microsoft Entra ID.

Login URL

Microsoft Entra ID Identifier

Logout URL

Azure URLs

Note

If you receive any key errors when logging in via SSO, try copying the X509 certificate information from the Federation Metadata XML file instead.

Benutzer und Gruppen

Wählen Sie **Benutzer und Gruppen** aus der Navigation aus:

Assign users or groups

Wählen Sie die Schaltfläche **Benutzer/Gruppe hinzufügen**, um den Zugangsdaten mit der SSO-Anwendung auf Benutzer- oder Gruppenebene Zugriff zu gewähren.

Zurück zur Web-App

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

Feld	Beschreibung
Namens-ID-Format	Standardmäßig wird Azure die E-Mail-Adresse verwenden. Wenn Sie diese Einstellung geändert haben, wählen Sie den entsprechenden Wert aus. Andernfalls setzen Sie dieses Feld auf Nicht spezifiziert oder E-Mail-Adresse .
Ausgehendes Signaturalgorithmus	Der Algorithmus, den Bitwarden zur Signierung von SAML-Anfragen verwenden wird.
Unterzeichnungsverhalten	Ob/wann SAML-Anfragen signiert werden.
Mindesteingehendes Signaturalgorithmus	Standardmäßig wird Azure mit RSA SHA-256 signieren. Wählen Sie rsa-sha256 aus dem Dropdown-Menü.
Möchte Behauptungen unterschrieben haben	Ob Bitwarden erwartet, dass SAML-Behauptungen 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, die richtigen Vertrauensketten sind mit den 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 Azure Portal zurückverweisen, um Anwendungswerte abzurufen:

Feld	Beschreibung
Entitäts-ID	Geben Sie Ihre Microsoft Entra ID-Kennung ein, die Sie aus dem Abschnitt Richten Sie Ihre Anwendung ein des Azure-Portals abgerufen haben. Dieses Feld ist Groß- und Kleinschreibungssensitiv.
Bindungsart	Einstellen auf HTTP POST oder Umleitung .
Einmaliges Anmelden Service URL	Geben Sie Ihre Login URL ein, die Sie aus dem Abschnitt Richten Sie Ihre Anwendung ein des Azure Portals 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 mit Ihrer Abmelde-URL konfigurieren, wenn Sie möchten.
X509 Öffentliches Zertifikat	<p>Fügen Sie das heruntergeladene Zertifikat ein und entfernen Sie es.</p> <p>-----BEGIN ZERTIFIKAT-----</p> <p>und</p> <p>-----ENDE ZERTIFIKAT-----</p> <p>Der Zertifikatswert ist Groß- und Kleinschreibungssensitiv, zusätzliche Leerzeichen, Zeilenumbrüche und andere überflüssige Zeichen werden dazu führen, dass die Zertifikatsvalidierung fehlschlägt.</p>
Ausgehendes Signaturalgorithmus	Standardmäßig wird Azure mit RSA SHA-256 signieren. Wählen Sie rsa-sha256 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 Azure 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.

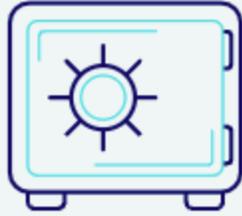
Wenn Sie mit der Konfiguration des Identitätsanbieters fertig sind, **speichern** Sie Ihre Arbeit.

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:



Log in to Bitwarden

Email address (required)

Remember email

Continue

or

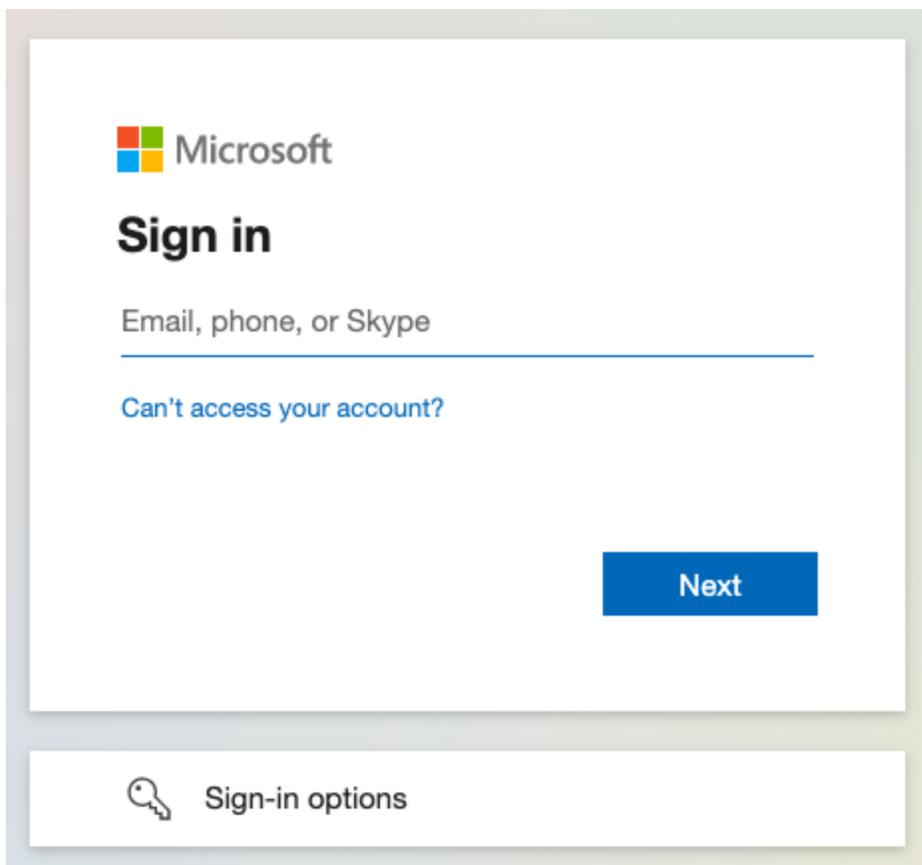
 Log in with passkey

 Use single sign-on

New to Bitwarden? [Create account](#)

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 Microsoft Zugangsdaten-Bildschirm weitergeleitet:



Azure login screen

Nachdem Sie sich mit Ihren Azure-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. Azure SAML Administratoren können eine [App-Registrierung](#) einrichten, damit Benutzer zur Bitwarden Web-Tresor Zugangsdaten Seite weitergeleitet werden.

1. Deaktivieren Sie die vorhandene Bitwarden-Schaltfläche auf der **Alle Anwendungen**-Seite, indem Sie zur aktuellen Bitwarden Enterprise-Anwendung navigieren und Eigenschaften auswählen und die Option **Sichtbar für Benutzer** auf **Nein** setzen.
2. Erstellen Sie die App-Registrierung, indem Sie zu **App-Registrierungen** navigieren und **Neue Registrierung** auswählen.
3. Geben Sie einen Namen für die Anwendung an, wie zum Beispiel **Bitwarden SSO**. Geben Sie keine Weiterleitungs-URL an. Wählen Sie **Registrieren** um das Forum abzuschließen.
4. Sobald die App erstellt wurde, navigieren Sie zu **Branding & Eigenschaften**, das sich im Navigationsmenü befindet.
5. Fügen Sie die folgenden Einstellungen zur Anwendung hinzu:
 1. Laden Sie ein Logo hoch für die Erkennung durch den Endbenutzer. Sie können das Bitwarden-Logo [hier](#) abrufen.
 2. Setzen Sie die **Startseiten-URL** auf Ihre Bitwarden Client Zugangsdaten Seite wie zum Beispiel <https://vault.bitwarden.com/#/login> oder [your-self-hostedURL.com](#).

Sobald dieser Prozess abgeschlossen ist, haben zugewiesene Benutzer eine Bitwarden-Anwendung, die sie direkt zur Bitwarden-Web-Tresor-Zugangsdaten-Seite verlinkt.