

ADMINISTRATOR KONSOLE > MELDEN SIE SICH MIT SSO AN >

Microsoft Entra ID OIDC Implementierung

Ansicht im Hilfezentrum:

<https://bitwarden.com/help/oidc-microsoft-entra-id/>

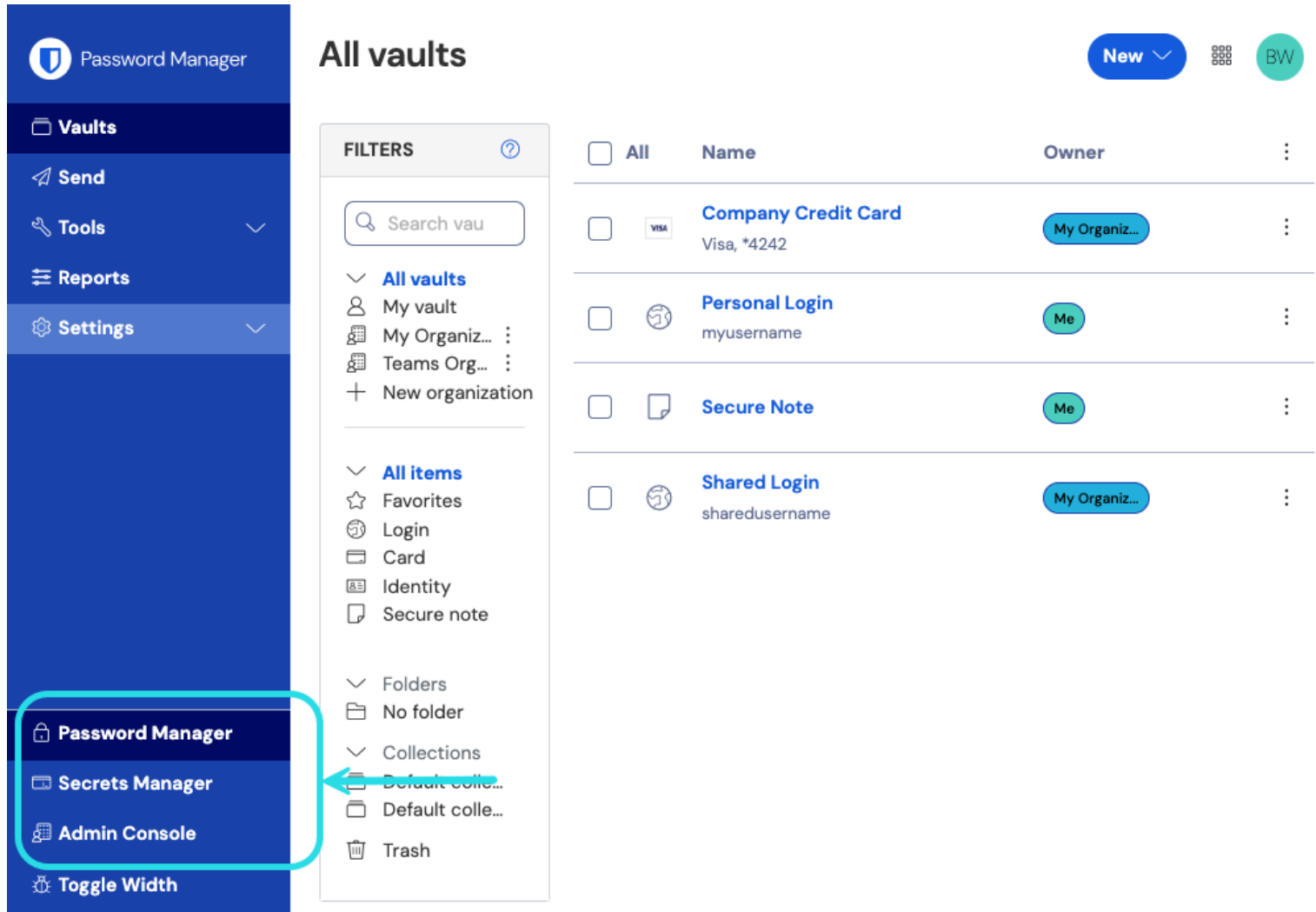
Microsoft Entra ID OIDC Implementierung

Dieser Artikel enthält **Azure-spezifische** Hilfe zur Konfiguration der Zugangsdaten mit SSO über OpenID Connect (OIDC). Für Hilfe bei der Konfiguration von Zugangsdaten mit SSO für einen anderen OIDC IdP oder bei der Konfiguration von Microsoft Entra ID über SAML 2.0, siehe [OIDC Konfiguration](#) oder [Microsoft Entra ID SAML Implementierung](#).

Die Konfiguration beinhaltet die gleichzeitige Arbeit innerhalb der Bitwarden-Web-App und des Azure-Portals. Während Sie fortfahren, empfehlen wir, beides griffbereit zu haben und die Schritte in der Reihenfolge durchzuführen, in der sie dokumentiert sind.

Öffnen Sie SSO im Web-Tresor

Melden Sie sich bei der Bitwarden [Web-App](#) an und öffnen Sie die Administrator-Konsole mit dem Produktschalter (☰):



Produktwechsler

Wählen Sie **Einstellungen** → **Einmaliges Anmelden** aus der Navigation:

bitwarden Admin Console

- My Organization
- Collections
- Members
- Groups
- Reporting
- Billing
- Settings
- Organization info
- Policies
- Two-step login
- Import data
- Export vault
- Domain verification
- Single sign-on**
- Device approvals
- SCIM provisioning

Single sign-on



Use the [require single sign-on authentication policy](#) to require all members to log in with SSO.

Allow SSO authentication

Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.

SSO identifier (required)

Provide this ID to your members to login with SSO. To bypass this step, set up [Domain verification](#)

Member decryption options

Master password

Trusted devices

Once authenticated, members will decrypt vault data using a key stored on their device. The [single organization](#) policy, [SSO required](#) policy, and [account recovery administration](#) policy with automatic enrollment will turn on when this option is used.

Type

OpenID connect configuration

Callback path

Signed out callback path

OIDC-Konfiguration

Wenn Sie es noch nicht getan haben, erstellen Sie einen einzigartigen **SSO-Identifizier** für Ihre Organisation. Andernfalls müssen Sie auf diesem Bildschirm noch nichts bearbeiten, lassen Sie ihn aber offen für eine einfache Referenz.



Es gibt alternative **Mitglied Entschlüsselungsoptionen**. Erfahren Sie, wie Sie mit SSO auf [vertrauenswürdigen](#) Geräten oder mit [Key Connector](#) beginnen können.

Erstellen Sie eine App-Registrierung

Im Azure Portal navigieren Sie zu **Microsoft Entra ID** und wählen Sie **App-Registrierungen**. Um eine neue App-Registrierung zu erstellen, wählen Sie die Schaltfläche **Neue Registrierung**:

Home >

App registrations ✦ ... ✕

[+ New registration](#) [Endpoints](#) [Troubleshooting](#) [Refresh](#) [Download](#) [Preview features](#) | [Got feedback?](#)

All applications **Owned applications** Deleted applications (Preview) Applications from personal account

Application (client) ID starts with [Add filters](#)

2 applications found

[Create App Registration](#)

You didn't provide any fields to complete. Please provide the information you want translated.

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Default Directory only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

| | |
|---|--|
| Select a platform  | e.g. https://example.com/auth |
|---|--|

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#) 

Register

Register redirect URI

1. Auf dem Bildschirm **Eine Anwendung registrieren**, geben Sie Ihrer App einen Bitwarden-spezifischen Namen und legen Sie fest, welche Konten die Anwendung nutzen können sollten. Diese Auswahl bestimmt, welche Benutzer Bitwarden Zugangsdaten mit SSO verwenden können.
2. Wählen Sie **Authentifizierung** aus der Navigation und klicken Sie auf den **Eine Plattform hinzufügen** Button.

3. Wählen Sie die Option **Web** auf dem Bildschirm Plattformen konfigurieren aus und geben Sie Ihren **Callback-Pfad** in das Eingabefeld für die Umleitungs-URLs ein.

Note

Callback Path can be retrieved from the Bitwarden SSO Configuration screen. For cloud-hosted customers, this is <https://sso.bitwarden.com/oidc-signin> or <https://sso.bitwarden.eu/oidc-signin>. For self-hosted instances, this is determined by your configured server URL, for example <https://your.domain.com/sso/oidc-signin>.

Erstellen Sie ein Client-Geheimnis

Wählen Sie **Zertifikate & Geheimnisse** aus der Navigation aus und klicken Sie auf die Schaltfläche **Neues Client-Geheimnis**:

The screenshot shows the Azure portal interface for configuring Bitwarden SSO. The left-hand navigation pane includes sections for Overview, Quickstart, Integration assistant, Manage (with sub-items like Branding, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators | Preview, Manifest), and Support + Troubleshooting. The main content area is titled 'Bitwarden Login with SSO (OIDC) | Certificates & secrets'. It contains a search bar, a 'Got feedback?' link, and a description of credentials. Below this, there are sections for 'Certificates' (with an 'Upload certificate' button) and 'Client secrets' (with a '+ New client secret' button highlighted by a green circle and arrow). A table header for client secrets is visible with columns: Description, Expires, Value, and Secret ID. At the bottom, there is a 'Create Client Secret' link.

Geben Sie dem Zertifikat einen Bitwarden-spezifischen Namen und wählen Sie einen Ablaufzeitraum.

Erstellen Sie eine Administrator-Zustimmung

Wählen Sie **API-Berechtigungen** und klicken Sie auf ✓ **Administrator-Zustimmung für Standardverzeichnis erteilen**. Die einzige benötigte Berechtigung wird standardmäßig hinzugefügt, Microsoft Graph > User.Read.

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 folgenden Felder zu konfigurieren:

| Feld | Beschreibung |
|--|--|
| Zertifizierungsstelle | Geben Sie https://login.microsoft.com/v2.0 ein, wo TENANT_ID der Verzeichnis (Mandant) ID Wert ist, der vom Überblicksbildschirm der App-Registrierung abgerufen wurde. |
| Client-ID | Geben Sie die Anwendungs- (Client) ID der App-Registrierung ein, die vom Übersichtsbildschirm abgerufen werden kann. |
| Client-Geheimnis | Geben Sie den geheimen Wert des erstellten Client-Geheimnisses ein. |
| Metadatenadresse | Für dokumentierte Azure-Implementierungen können Sie dieses Feld leer lassen. |
| OIDC-Umleitungsverhalten | Wählen Sie entweder Formular POST oder Umleiten GET . |
| Fordern Sie Ansprüche vom Benutzerinformationsendpunkt an | Aktivieren Sie diese Option, wenn Sie Fehlermeldungen erhalten, dass die URL zu lang ist (HTTP 414), abgeschnittene URLs und/oder Fehler während des SSO auftreten. |
| Zusätzliche/Individuelle Bereiche | Definieren Sie benutzerdefinierte Bereiche, die der Anfrage hinzugefügt werden sollen (durch Kommas getrennt). |
| Zusätzliche/Benutzerdefinierte Benutzer-ID-Anspruchs-Typen | Definieren Sie benutzerdefinierte Schlüssel für den Anspruchstyp zur Benutzeridentifikation (durch Kommas getrennt). Wenn definiert, werden benutzerdefinierte Anspruchstypen gesucht, bevor auf Standardtypen zurückgegriffen wird. |

| Feld | Beschreibung |
|---|--|
| Zusätzliche/angepasste E-Mail-Adresse Anspruchstypen | Definieren Sie benutzerdefinierte Anspruchstyp-Schlüssel für die E-Mail-Adressen der Benutzer (durch Kommas getrennt). Wenn definiert, werden benutzerdefinierte Anspruchstypen gesucht, bevor auf Standardtypen zurückgegriffen wird. |
| Zusätzliche/angepasste Namensanspruchs-Typen | Definieren Sie benutzerdefinierte Anspruchstyp-Schlüssel für die vollständigen Namen oder Anzeigenamen der Benutzer (durch Kommas getrennt). Wenn definiert, werden benutzerdefinierte Anspruchstypen gesucht, bevor auf Standardtypen zurückgegriffen wird. |
| Angeforderte Authentifizierungskontextklassenreferenzwerte | Definieren Sie Authentifizierungskontextklassenreferenz-Identifikatoren (acr_values) (durch Leerzeichen getrennt). Liste acr_values in Präferenzreihenfolge. |
| Erwarteter "acr" Anspruchswert in der Antwort | Definieren Sie den acr Claim-Wert, den Bitwarden in der Antwort erwarten und validieren soll. |

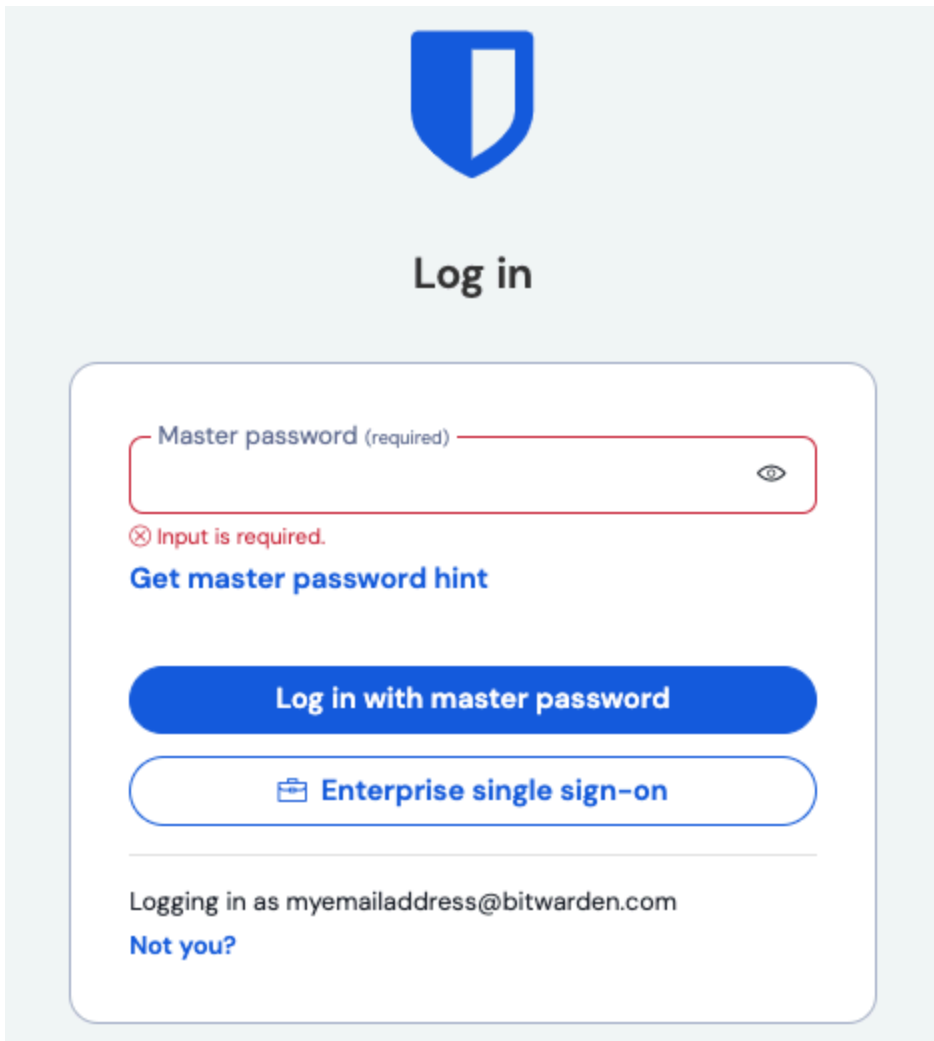
Wenn Sie mit der Konfiguration dieser Felder fertig sind, **Speichern** Sie Ihre Arbeit.

 **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.](#)

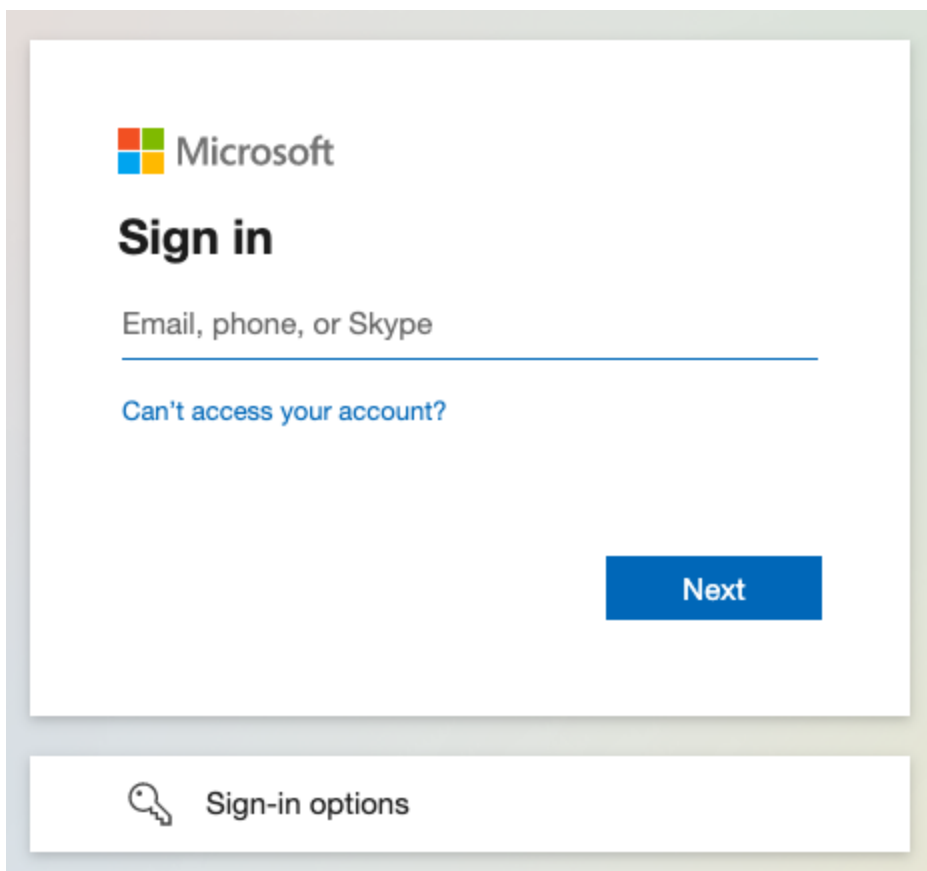
Testen Sie die Konfiguration

Sobald Ihre Konfiguration abgeschlossen ist, testen Sie diese, indem Sie zu <https://vault.bitwarden.com> navigieren, Ihre E-Mail-Adresse eingeben, **Weiter** auswählen und die Schaltfläche **Enterprise Single-On** 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 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.

Nächste Schritte

1. Bilden Sie die Mitglieder Ihrer Organisation darüber aus, wie man die [Zugangsdaten mit SSO verwendet](#).