

ADMINISTRATOR KONSOLE > MELDEN SIE SICH MIT SSO AN >

Duo SAML Implementierung

Ansicht im Hilfezentrum:

<https://bitwarden.com/help/saml-duo/>

Duo SAML Implementierung

Dieser Artikel enthält **Duo-spezifische** Hilfe zur Konfiguration von Zugangsdaten mit SSO über SAML 2.0. Für Hilfe bei der Konfiguration von Zugangsdaten mit SSO für einen anderen IdP, siehe [SAML 2.0 Konfiguration](#).

Die Konfiguration beinhaltet die gleichzeitige Arbeit zwischen der Bitwarden-Webanwendung und dem Duo-Administratorportal. 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



Warning

This article assumes that you have already set up Duo with an Identity Provider. If you haven't, see [Duo's documentation](#) for details.

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

Filters:

- Search vaults
- All vaults
 - My vault
 - My Organiz...
 - Teams Org...
 - New organization
- All items
 - Favorites
 - Login
 - Card
 - Identity
 - Secure note
- Folders
 - No folder
- Collections
 - Default colle...
 - Default colle...
- Trash

| <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 den **Einstellungen** → **Single Sign-On** Bildschirm Ihrer Organisation:

- 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)

unique-organization-identifier

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

SAML 2.0

SAML service provider configuration

Set a unique SP entity ID

Generate an identifier that is unique to your organization

SP entity ID

[Masked SP entity ID]

SAML 2.0 metadata URL

[Masked SAML 2.0 metadata URL]

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.

Eine Anwendung schützen

Bevor Sie fortfahren, beziehen Sie sich bitte auf die [Dokumentation von Duo](#), um zu überprüfen, ob Duo Single Sign-On mit Ihrem SAML-Identitätsanbieter für die Authentifizierung konfiguriert wurde.

Im Duo Administrator Portal navigieren Sie zum **Anwendungen** Bildschirm und wählen Sie **Eine Anwendung schützen** aus. Geben Sie **Bitwarden** in die Suchleiste ein und wählen Sie **Konfigurieren** für die **Bitwarden 2FA mit SSO, gehostet von Duo** Anwendung:

Dashboard > Applications > Protect an Application

Protect an Application

Add an application that you'd like to protect with Duo two-factor authentication. You can start with a small "proof-of-concept" installation — it takes just a few minutes, and you're the only one that will see it, until you decide to add others.

Documentation: [Getting Started](#)

Choose an application below to get started.

| Application | Protection Type | Documentation | Action |
|-------------|---|-------------------------------|-----------|
| Bitwarden | 2FA | Documentation | Protect |
| Bitwarden | 2FA with SSO hosted by Duo (Single Sign-On) | Documentation | Configure |

Duo Bitwarden Application

Wählen Sie **Aktivieren und Einrichtung starten** für die neu erstellte Anwendung:

Dashboard > Single Sign-On

Single Sign-On

Simplify access to the applications your users rely on. With Duo's cloud-hosted SSO, protecting your applications while reducing user friction has never been easier. [Learn how it works](#)

Duo-hosted SSO requires Duo to collect and validate users' primary Active Directory credentials and/or directly receive SAML assertions. During authentication, usernames and passwords are encrypted when passed to your [Authentication Proxy server\(s\)](#). Duo caches the AD password and SAML assertions only long enough to complete the authentication. [Learn more](#)

I have read and understand these Duo-hosted SSO updates, the [Privacy Statement](#) and [Duo's Privacy Data Sheet](#)

[Activate and Start Setup](#)

Duo Activation and Setup

Führen Sie die folgenden Schritte und Konfigurationen auf dem Bildschirm für die Anwendungskonfiguration durch, einige davon müssen Sie vom Bitwarden Single Sign-On-Bildschirm abrufen:

- Dashboard
- Device Insight
- Policies
- Applications
- Single Sign-On**
- Duo Central
- Passwordless
- Users
- Groups
- Endpoints
- 2FA Devices
- Administrators
- Trusted Endpoints

[← Back to Single Sign-On](#)

SAML Identity Provider Configuration ✓ Enabled

Status: Enabled [Disable Source](#)

Configure a SAML Identity Provider to provide primary authentication for Duo Single Sign-On by following the sections below.
[Learn more about configuring the SAML Identity Provider with Duo Single Sign-On](#)

1. Configure the SAML Identity Provider

Provide this information about your Duo Single Sign-On account to your SAML identity provider.

| | | |
|---------------------------------------|---|----------------------|
| Entity ID | <code>https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/metadata</code> | Copy |
| Assertion Consumer Service URL | <code>https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/acs</code> | Copy |
| Audience Restriction | <code>https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/metadata</code> | Copy |
| Metadata URL | <code>https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/metadata</code> | Copy |
| XML File | Download Metadata XML | |

DUO SAML Identity Provider Configuration

Metadaten

Sie müssen nichts im Abschnitt **Metadaten** bearbeiten, aber Sie werden [diese Werte später verwenden](#) müssen:

Metadata

| | | |
|---------------------------|--|----------------------|
| Entity ID | <code>https://sso-ff27df13.sso.duosecurity.com/saml2/sp/DI4GBHNTLEJZVCCZ6EQM/metadata</code> | Copy |
| Single Sign-On URL | <code>https://sso-ff27df13.sso.duosecurity.com/saml2/sp/DI4GBHNTLEJZVCCZ6EQM/sso</code> | Copy |

URLs for Configuration

Downloads

Wählen Sie die Schaltfläche **Zertifikat herunterladen**, um Ihr X.509-Zertifikat herunterzuladen, da Sie es [später in der Konfiguration](#) verwenden müssen.

Dienstleister

| Feld | Beschreibung |
|-------------|--|
| 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> |

| Feld | Beschreibung |
|--|---|
| Assertion Consumer Service (ACS) URL | <p>Setzen Sie dieses Feld auf die vorab generierte Assertion Consumer Service (ACS) URL.</p> <p>Dieser automatisch generierte Wert kann aus den Einstellungen → Single Sign-On Bildschirm der Organisation kopiert werden und variiert je nach Ihrer Konfiguration.</p> |
| URL für die Zugangsdaten des Dienstbieters | <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://your.domain.com/#/sso.</p> |

SAML-Antwort

| Feld | Beschreibung |
|-------------------------|--|
| NameID-Format | Setzen Sie dieses Feld auf das SAML NameID Format , damit Duo in SAML-Antworten senden kann. |
| Attribut "NameID" | Setzen Sie dieses Feld auf das Duo-Attribut, das den NameID in den Antworten füllen wird. |
| Signaturalgorithmus | Stellen Sie dieses Feld auf den Verschlüsselungsalgorithmus ein, der für SAML-Behauptungen und Antworten verwendet werden soll. |
| Unterzeichnungsoptionen | Wählen Sie aus, ob Sie die Antwort unterschreiben , die Behauptung unterschreiben , oder beides. |
| Kartenattribute | Verwenden Sie diese Felder, um IdP-Attribute auf SAML-Antwortattribute abzubilden. Unabhängig davon, welches NameID-Attribut Sie konfiguriert haben, ordnen Sie das IdP E-Mail-Adresse Attribut zu E-Mail , wie im folgenden Screenshot: |

Map attributes

IdP Attribute

SAML Response Attribute

| | |
|--|--|
| <input type="text" value="x <Email Address>"/> | <input type="text" value="Email"/> + |
|--|--|

Map the values of an IdP attribute to another attribute name to be included in the SAML response (e.g. Username to User.Username). Enter in an IdP attribute or select one of Duo's preconfigured attributes that automatically chooses the SAML response attribute based on the IdP. There are five preconfigured attributes: <Email Address>, <Username>, <First Name>, <Last Name> and <Display Name>. Consult your service provider for more information on their attribute names.

Required Attribute Mapping

Sobald Sie diese Felder konfiguriert haben, **Speichern** Sie Ihre Änderungen.

Zurück zur Web-App

Bis zu diesem Zeitpunkt haben Sie alles, was Sie im Kontext des Duo-Portals benötigen, konfiguriert. Kehren Sie zur Bitwarden-Web-App 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 im Duo Administrator Portal [während der Anwendungseinrichtung](#) getroffenen Auswahlmöglichkeiten:

| Feld | Beschreibung |
|----------------------------------|---|
| Namens-ID-Format | NameID Format, der in der SAML-Anfrage verwendet werden soll (NameIDPolicy). Setzen Sie dieses Feld auf das ausgewählte NameID-Format . |
| Ausgehendes Signatur-Algorithmus | Algorithmus, der zum Signieren von SAML-Anfragen verwendet wird, standardmäßig rsa-sha256 . |
| Unterzeichnungsverhalten | Ob/wann SAML-Anfragen signiert werden. Standardmäßig wird Duo keine Unterschrift für Anfragen verlangen. |

| Feld | Beschreibung |
|--|--|
| Mindesteingehendes Signaturalgorithmus | Der Mindestsignaturalgorithmus, den Bitwarden in SAML-Antworten akzeptiert. Standardmäßig wird Duo mit rsa-sha256 signieren, wählen Sie also diese Option aus dem Dropdown-Menü, es sei denn, Sie haben eine andere Option ausgewählt . |
| Möchte Behauptungen unterschrieben haben | Ob Bitwarden SAML-Behauptungen signiert haben möchte. Markieren Sie dieses Kästchen, wenn Sie die Option Signaturbestätigung ausgewählt 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 des Bitwarden Zugangsdaten mit SSO Docker-Images 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 Duo Administrator Portal beziehen, um Anwendungswerte abzurufen:

| Feld | Beschreibung |
|-------------------------------|--|
| Entitäts-ID | Geben Sie den Entity ID -Wert Ihrer Duo-Anwendung ein, den Sie aus dem Duo-App Metadatenbereich abrufen können. Dieses Feld ist Groß- und Kleinschreibungssensitiv. |
| Bindungsart | Setzen Sie dieses Feld auf HTTP Post . |
| Einmalanmeldung Service URL | Geben Sie den Single Sign-On URL -Wert Ihrer Duo-Anwendung ein, den Sie aus dem Duo-App Metadatenbereich abrufen können. |
| URL des Einzelabmeldedienstes | Die Anmeldung mit SSO unterstützt derzeit nicht SLO. Diese Option ist für zukünftige Entwicklung geplant, jedoch können Sie vorab mit dem Single Log-Out URL Wert Ihrer Duo-Anwendung konfigurieren. |
| X509 Öffentliches Zertifikat | Fügen Sie das heruntergeladene Zertifikat ein und entfernen Sie es. -----BEGIN ZERTIFIKAT----- |

| Feld | Beschreibung |
|--|--|
| | <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 | Setzen Sie dieses Feld auf den ausgewählten SAML Response Signaturalgorithmus . |
| Deaktivieren Sie ausgehende Abmeldeanfragen | Die Anmeldung mit SSO unterstützt derzeit nicht SLO. Diese Option ist für zukünftige Entwicklungen geplant. |
| Möchte Authentifizierungsanfragen signiert haben | Ob Duo 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

Master password (required)

⊗ Input is required.

[Get master password hint](#)

[Log in with master password](#)

[Enterprise single sign-on](#)

Logging in as myemailaddress@bitwarden.com

[Not you?](#)

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 zu dem Anmeldebildschirm Ihres Quell-IdP mit Ihren Zugangsdaten weitergeleitet.

Nachdem Sie sich mit Ihren IdP-Zugangsdaten und Duo-Zwei-Faktor-Authentifizierung 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.