ADMINISTRATOR KONSOLE > MELDEN SIE SICH MIT SSO AN >

OneLogin SAML Implementierung

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

OneLogin SAML Implementierung

Dieser Artikel enthält **OneLogin-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 innerhalb der Bitwarden-Web-App und des OneLogin-Portals. 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.

Jownload 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 (闘):

D Password Manager	All vaults			New 🗸	BW
🗇 Vaults			Nome	Owner	
🖉 Send			Name	Owner	:
\ll Tools \sim	Q Search vau	VISA	Company Credit Card Visa, *4242	My Organiz	÷
æ Reports	✓ All vaults		Personal Legin		
🕸 Settings 🛛 🗸 🗸	 ∠ My vault ∠ My Organiz : 	0 9	myusername	Me	:
	gii Teams Org : + New organization		Secure Note	Ме	:
	 ✓ All items ☆ Favorites ④ Login □ Card □ Identity □ Secure note 		Shared Login sharedusername	My Organiz	:
Password Manager	 ✓ Folders ☐ No folder 				
Secrets Manager	Default colle				
Admin Console	前 Trash				
		Dresslauteture			

Produktwechsler

Öffnen Sie den **Einstellungen → Single sign-on** Bildschirm Ihrer Organisation:

Secure and trusted open source password manager for business

D bit Warden Admin Console	Single sign-on 📟	
${\ensuremath{\mathbb B}}$ My Organization $\ \lor$	Use the require single sign-on authentication policy to require all members to log in with SSO.	
Collections	Allow SSO authentication	
A Members	Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.	
왕 Groups	SSO identifier (required)	
$ agreen Equation = 1 \forall \forall \forall \forall \forall \forall \forall \forall \forall $	Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification	
\mathbb{B} Billing \checkmark	Member decryption options	
\otimes Settings \land	Master password	
Organization info	Trusted devices Once authenticated, members will decrypt vault data using a key stored on their device. The single organization policy, SSO required policy, are account recovery administration policy with automatic enrollment will turn on when this option is used.	nd
Two-step login	SAML 2.0	•
Export vault		
Domain verification	SAML service provider configuration	
Single sign-on	Set a unique SP entity ID	
Device approvals	Generate an identifier that is unique to your organization	
SCIM provisioning		
	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 für eine einfache Referenz.

Sie können die Option **Einen eindeutigen SP-Entity-ID festlegen** 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 OneLogin-App

Im OneLogin Portal navigieren Sie zum Anwendungen Bildschirm und wählen Sie die Schaltfläche App hinzufügen:

onelogin	Users	Applications	Devices	Authentication	Activity	Security	Settings	Developers	
Applicat	ions								Add App
Q search co	ompany a	pps							
No company	y apps hav	ve been added.							

Add an Application

Geben Sie in der Suchleiste saml test connector ein und wählen Sie die SAML Test Connector (Advanced) App aus:



SAML Test Connector App

Geben Sie Ihrer Anwendung einen Bitwarden-spezifischen Anzeigenamen und wählen Sie die Speichern Schaltfläche.

Konfiguration

Wählen Sie **Konfiguration** aus der linken Navigation aus und konfigurieren Sie die folgenden Informationen, einige davon müssen Sie vom Single Sign-On-Bildschirm abrufen:

U bitwarden

onelogin Users	Applications Dev	ces Authentication	Activity	Security	Settings	Developers	
Applications / SAML Test Conne	ctor (Advanc	ed)			Mo	ore Actions 🔻	Save
Info Configuration Parameters Rules SSO Access	Ap Rel Auc Rec	plication details ayState ience (EntityID) ipient					
		App Conf	iguration				
Anwendungseinstellungen	Beschreib	ung					
Publikum (EntityID)	Setzen Sie Dieser aut der Organ	dieses Feld auf die v omatisch generierte sation kopiert werde	vorab gene Wert kann n und varii	erierte SP E aus der Ei ert je nach	i ntity ID . nstellunge n Ihrer Konf	n → Single Sign-(iguration.)n Bildschirm
Empfänger	Setzen Sie (Entity ID)	dieses Feld auf die g Einstellung verwend	gleiche vor et wurde.	ab generie	erte SP Enti	ty ID , die für die	Audience
ACS (Verbraucher) URL- Validator	Obwohl es Informatio nächsten	von OneLogin als Er nen in dieses Feld ei Feld, ACS (Verbraucl	forderlich ngeben, ur ner) URL.	markiert is n sich mit	t, müssen S Bitwarden	Sie tatsächlich ke zu integrieren. Sp	eine oringen Sie zum
ACS (Verbraucher) URL	Setzen Sie Dieser aut der Organ	dieses Feld auf die v omatisch generierte sation kopiert werde	vorab gene Wert kann en und varii	erierte Ass o aus der Ei ert je nach	ertion Con nstellunge 1 Ihrer Konf	sumer Service (A n → Single Sign-C iguration.	ACS) URL. On Bildschirm

Anwendungseinstellungen	Beschreibung
SAML-Initiator	Wählen Sie Dienstleister aus. Die Anmeldung mit SSO unterstützt derzeit keine von IdP initiierten SAML-Behauptungen.
SAML NameID Format	Setzen Sie dieses Feld auf das SAML NamelD Format, das Sie für SAML-Behauptungen verwenden möchten.
SAML-Signaturelement	Standardmäßig wird OneLogin die SAML-Antwort signieren. Sie können dies auf Behauptung oder Beide einstellen.

Wählen Sie die Schaltfläche **Speichern**, um Ihre Konfigurationseinstellungen abzuschließen.

Parameter

Wählen Sie **Parameter** aus der linken Navigation aus und verwenden Sie das **+ Hinzufügen** Symbol, um die folgenden benutzerdefinierten Parameter zu erstellen:

Feldname	Wert
E-Mail-Adresse	E-Mail
Vorname	Vorname
Nachname	Nachname

Wählen Sie die Schaltfläche **Speichern**, um Ihre benutzerdefinierten Parameter abzuschließen.

SSO

Wählen Sie **SSO** aus der linken Navigation aus und vervollständigen Sie Folgendes:

1. Wählen Sie den Link **Details anzeigen** unter Ihrem X.509-Zertifikat:

	Enable SAML2.0	
	Sign on method	
	SAML2.0	
2	X.509 Certificate	
	Standard Strength Certificate (2048-bit)	
	Change View Details	
	SAML Signature Algorithm	
	SHA-256 🗸	
	Issuer URL	
	https://app.onelogin.com/saml/metadata/95eef6e7-560f-4531-9df3-02e7248415a8	ß
:	SAML 2.0 Endpoint (HTTP)	
	https://mmccabe.onelogin.com/trust/saml2/http-post/sso/95eef6e7-560f-4531-9df3-02e7248415a8	ß

View your Cert

Auf dem Zertifikatsbildschirm, laden Sie Ihr X.509 PEM-Zertifikat herunter oder kopieren Sie es, da Sie es später verwenden müssen. Einmal kopiert, kehren Sie zum Haupt-SSO-Bildschirm zurück.

2. Stellen Sie Ihren SAML-Signaturalgorithmus ein.

3. Notieren Sie sich Ihre Aussteller-URL und SAML 2.0-Endpunkt (HTTP). Sie werden diese Werte bald benötigen.

Zugriff

Wählen Sie **Zugang** aus der linken Navigation aus. Im Abschnitt **Rollen** weisen Sie allen Rollen, die Sie für die Nutzung von Bitwarden verwenden möchten, den Zugriff auf die Anwendung zu. Die meisten Implementierungen erstellen eine Bitwarden-spezifische Rolle und wählen stattdessen die Zuweisung basierend auf einer allgemeinen Lösung (zum Beispiel, **Standard**) oder basierend auf bereits bestehenden Rollen.

Privileges	Dalaa			
Setup	Roles			
	Bitwarden SSO Users	✓	Default	
	Role Assignme	nt		

Zurück zur Web-App

Bis zu diesem Zeitpunkt haben Sie alles, was Sie im Kontext des OneLogin 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 entsprechend den in dem OneLogin Portal während der App-Erstellung getroffenen Auswahlmöglichkeiten:

Feld	Beschreibung
Namens-ID-Format	Setzen Sie dieses Feld auf das, was Sie für das OneLogin SAML namelD Format Feld während der App-Konfiguration ausgewählt haben.
Ausgehendes Signatur- Algorithmus	Algorithmus, der zum Signieren von SAML-Anfragen verwendet wird, standardmäßig <mark>sha-256</mark> .
Unterzeichnungsverhalten	Ob/wann SAML-Anfragen signiert werden. Standardmäßig erfordert OneLogin keine Signatur für Anfragen.
Minimales Eingehendes Signatur-Algorithmus	Setzen Sie dieses Feld auf das, was Sie für den SAML-Signaturalgorithmus während der App- Konfiguration ausgewählt haben.
Möchte Behauptungen unterschrieben haben	Markieren Sie dieses Kästchen, wenn Sie das SAML-Signaturelement in OneLogin auf Behauptung oder Beides während der App-Konfiguration eingestellt 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 der 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 das OneLogin Portal beziehen, um Anwendungswerte abzurufen:

Feld	Beschreibung
Entitäts-ID	Geben Sie Ihre OneLogin Issuer URL ein, die Sie vom OneLogin App SSO Bildschirm abrufen können. Dieses Feld ist Groß- und Kleinschreibungssensitiv.
Bindungsart	Einstellen auf HTTP Post (wie im SAML 2.0 Endpoint (HTTP) angegeben).
Einmaliges Anmelden Service URL	Geben Sie Ihren OneLogin SAML 2.0 Endpunkt (HTTP) ein, den Sie vom OneLogin App SSO Bildschirm abrufen können.
URL des Einzelabmeldedienstes	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 X.509 Zertifikat ein, entfernen Sie BEGIN ZERTIFIKAT 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	Wählen Sie den SAML-Signaturalgorithmus aus, der im Abschnitt OneLogin SSO- Konfiguration ausgewählt wurde.
Deaktivieren Sie ausgehende Abmeldeanfragen	Die Anmeldung mit SSO unterstützt derzeit nicht SLO. Diese Option ist für zukünftige Entwicklungen geplant.
Möchte Authentifizierungsanfragen signiert haben	Ob OneLogin erwartet, dass SAML-Anfragen signiert werden.

(i) 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 zur OneLogin Zugangsdaten-Bildschirm weitergeleitet:

	Onelogin	
<•∍ Con	necting to Bitwarden SSO	
Usernam	ne	
Rem	ember my username	
	Continue	
	Forgot Password	

OneLogin Login

Nachdem Sie sich mit Ihren OneLogin-Anmeldeinformationen authentifiziert haben, geben Sie Ihr Bitwarden Master-Passwort ein, um Ihren Tresor zu entschlüsseln!

(i) 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.