ADMINISTRATOR KONSOLE  $\rightarrow$  MELDEN SIE SICH MIT SSO AN  $\rightarrow$ 

# **AWS SAML Implementierung**

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

### AWS SAML Implementierung

Dieser Artikel enthält **AWS-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-Webanwendung und der AWS-Konsole. 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.

### 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 (
B):

D Password Manager	All vaults			New 🗸	BW
🗇 Vaults	FILTERS	□ A!!	Nome	Owner	
🖉 Send			Name	Owner	:
$\ll$ Tools $\sim$	Q Search vau	VISA	Company Credit Card Visa, *4242	My Organiz	÷
<b>≅</b> Reports	✓ All vaults		Demonal Login		
🕸 Settings 🛛 🗸 🗸	<ul> <li>∠ My vault</li> <li>∠ My Organiz :</li> </ul>	0 3	myusername	Me	:
	gii Teams Org : + New organization		Secure Note	Me	:
	<ul> <li>✓ All items</li> <li>☆ Favorites</li> <li>③ Login</li> <li>□ Card</li> <li>□ Identity</li> <li>□ Secure note</li> </ul>	0 Ø	Shared Login sharedusername	My Organiz	:
Password Manager	<ul><li>✓ Folders</li><li>☐ No folder</li></ul>				
🗔 Secrets Manager	Collections				
Admin Console	<ul><li>Default colle&lt;</li><li>通 Trash</li></ul>				
🍈 Toggle Width					
		Due du lature			

Produktwechsler

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

#### Secure and trusted open source password manager for business

<b>D bit</b> warden	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.
	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.
幋 Groups	SSO identifier (required) unique-organization-identifier
$ agreen Equation = 1  \text{Reporting}  \nabla$	Provide this ID to your members to login with SSO. To bypass this step, set up <b>Domain verification</b>
😫 Billing 🗸 🗸	Member decryption options
Settings	Master password
Organization info	Trusted devices     Construction provide a standard their device. The single construction policy. SSO required earlier, and
Policies	account recovery administration policy with automatic enrollment will turn on when this option is used.
Two-step login	C Type
Import data	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, 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 AWS SSO-Anwendung

Im AWS-Konsole navigieren Sie zu AWS SSO, wählen Sie Anwendungen aus der Navigation aus und klicken Sie auf die Schaltfläche Eine neue Anwendung hinzufügen:

aws Services Q Search	[Option+S] D 🗘 🕐 😨 N. Virginia 🔻 🗖 🗖 🗖 🗖
IAM Identity Center ×	IAM Identity Center > Applications
Dashboard Users Groups Settings V Multi-account permissions AWS accounts Permission sets	Administer users and groups for AWS managed or customer managed applications that support identity federation with SAML 2.0 or OAuth 2.0. Learn more 2 Add application AWS managed Customer managed
Application assignments     Applications  Related consoles	AWS managed applications (0)       Actions ▼         An AWS managed application is defined by and named for an AWS service, and must be configured from the applicable service console to work with IAM Identity Center.         Q. Search for an AWS managed application
AWS Organizations 🗹 IAM 🕻	All services         1           Application        Service       Owning account ID        Date created            You have not added any applications

Fügen Sie eine neue Anwendung hinzu

Unterhalb der Suchleiste wählen Sie die Option Eine benutzerdefinierte SAML 2.0-Anwendung hinzufügen:

### AWS SSO Application Catalog

Type the name of an application	7		
<ul> <li>Add a custom SAML 2.0 You can add SSO integra</li> </ul>	application tion to your custom SAML 2.0-enabl	ed applications	
<b>10,000</b> ft	<b>4me</b> <sup>**</sup>		Abstract
10000ft	4me	7Geese	Abstract

Fügen Sie eine benutzerdefinierte SAML-App hinzu

#### Einzelheiten

Geben Sie der Anwendung einen einzigartigen, Bitwarden-spezifischen Anzeigenamen.

### AWS SSO-Metadaten

Sie benötigen die Informationen in diesem Abschnitt für einen späteren Konfigurationsschritt. Kopieren Sie die AWS SSO Anmelde-URL und die AWS SSO Aussteller-URL und laden Sie das AWS SSO Zertifikat herunter:

aws	Services	Q Search	[Option+S] 🗵 🔷 ĝ Ĝ N. Virginia ▼ 🛛 ■ ■ ■	•
≡			IAM Identity Center metadata Your cloud application may require the following certificate and metadata details to recognize IAM Identity Center as the identity provider.	0
			IAM Identity Center SAML metadata file	

AWS SSO Metadaten

#### Anwendungseigenschaften

Im Feld **Start-URL der Anwendung** geben Sie die Zugangsdaten-URL an, von der aus Benutzer auf Bitwarden zugreifen werden. Für Kunden, die in der Cloud gehostet werden, ist dies immer <a href="https://walt.bitwarden.com/#/sso">https://walt.bitwarden.com/#/sso</a>. Für selbst gehostete Instanzen wird dies durch Ihre konfigurierte Server-URL bestimmt, zum Beispiel <a href="https://your.domain/#/sso">https://walt.bitwarden.com/#/sso</a>. Für selbst gehostete Instanzen

#### Anwendungsmetadaten

Im Abschnitt Anwendungsmetadaten wählen Sie die Option, Metadatenwerte manuell einzugeben:

Application metadata IAM Identity Center requires specific metadata about yo manually or upload a metadata exchange file.	ur cloud application before it can trust this application. You can type this metada
• Manually type your metadata values	O Upload application SAML metadata file
Application ACS URL	
Application SAML audience	

Geben Sie Metadatenwerte ein

Konfigurieren Sie die folgenden Felder:

Feld	Beschreibung
Anwendungs-ACS-URL	Setzen Sie dieses Feld auf die vorab generierte <b>Assertion Consumer Service (ACS) URL</b> . Dieser automatisch generierte Wert kann von der <b>Einstellungen → Single Sign-On</b> Bildschirm der Organisation kopiert werden und variiert je nach Ihrer Konfiguration.
Anwendung SAML- Zielgruppe	Setzen Sie dieses Feld auf die vorab generierte <b>SP Entity ID</b> . Dieser automatisch generierte Wert kann aus den <b>Einstellungen → Single Sign-On</b> der Organisation kopiert werden und variiert je nach Ihrer Konfiguration.

#### Wenn Sie fertig sind, wählen Sie Änderungen speichern.

### Attributzuordnungen

Navigieren Sie zum Attributzuordnungen Tab und konfigurieren Sie die folgenden Zuordnungen:

aws Services Q Search	[Option+S] D. 🗘 Ø Ø N. Virginia ▼ 💶 ■	
IAM Identity Center $\qquad  imes$	Configuration for 'Bitwarden SAML 2.0 application' has been saved. You must configure attribute mappings for IAM Identity Center to work.	× G
Dashboard Users Groups Settings	IAM Identity Center > Applications > Bitwarden SAML 2.0 application Bitwarden SAML 2.0 application	
<ul> <li>Multi-account permissions</li> <li>AWS accounts</li> </ul>	Details A Edit configuration	actions
<ul> <li>Permission sets</li> <li>Application assignments</li> <li>Applications</li> </ul>	Display name Bitwarden SAML 2.0 application	appings
	Attributzuordnungen	
Benutzerattribut in der Anwendung	Kartiert auf diesen String-Wert oder Benutzerattribut in AWS SSO	Format
Betreff	<pre>\${user:email}</pre>	E-Mail-Adresse

Benutzerattribut in der Anwendung	Kartiert auf diesen String-Wert oder Benutzerattribut in AWS SSO	Format
E-Mail-Adresse	\${user:email}	Unbestimmt

#### Zugewiesene Benutzer

Navigieren Sie zum Zugewiesene Benutzer Tab und wählen Sie die Benutzer zuweisen Schaltfläche:

Assigned users and groups	Remove access	Assign (	users and groups
The following users and groups can access this application. Learn more abo	ut user and group assignments 🔀		
Q Search for an assigned user or group			< 1 > ©
Username of user or group	$\nabla$	Туре	~
No users or gr	oups to display		
You have not assigned users	and groups to this application.		
Accian usor	s and groups		

Benutzer zuweisen

Sie können Benutzer auf individueller Ebene oder nach Gruppe der Anwendung zuweisen.

#### Zurück zur Web-App

Bis zu diesem Zeitpunkt haben Sie alles konfiguriert, was Sie im Kontext der AWS-Konsole benötigen. 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**

Die Konfiguration des Dienstanbieters sollte bereits abgeschlossen sein, jedoch können Sie sich dafür entscheiden, eines der folgenden Felder zu bearbeiten:

Feld	Beschreibung
Namens-ID-Format	Einstellen auf <b>E-Mail-Adresse</b> .

Feld	Beschreibung
Ausgehendes Signatur- Algorithmus	Der Algorithmus, den Bitwarden zur Signierung von SAML-Anfragen verwenden wird.
Unterzeichnungsverhalten	Ob/wann SAML-Anfragen signiert werden.
Minimales Eingehendes Signatur-Algorithmus	Standardmäßig wird AWS SSO mit SHA-256 signieren. Sofern Sie dies nicht geändert haben, wählen Sie <mark>sha256</mark> aus dem Dropdown-Menü aus.
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 singen. Selbstsignierte Zertifikate können fehlschlagen, es sei denn, die richtigen Vertrauensketten sind innerhalb des 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 die AWS-Konsole zurückgreifen, um Anwendungswerte abzurufen:

Feld	Beschreibung
Entitäts-ID	Geben Sie die <b>AWS SSO Aussteller URL</b> ein, die Sie aus dem Abschnitt AWS SSO Metadaten in der AWS Konsole abgerufen haben. Dieses Feld ist Groß- und Kleinschreibungssensitiv.
Bindungsart	Einstellen auf <b>HTTP POST</b> oder <b>Weiterleitung</b> .
URL des Single Sign On Dienstes	Geben Sie die <b>AWS SSO-Anmelde-URL</b> ein, die Sie aus dem Abschnitt AWS SSO- Metadaten in der AWS-Konsole abgerufen haben.

Feld	Beschreibung
Einzel Abmelden Service URL	Die Anmeldung mit SSO unterstützt derzeit <b>nicht</b> SLO. Diese Option ist für zukünftige Entwicklungen geplant, jedoch können Sie sie vorab mit der <b>AWS SSO Abmelde-URL</b> konfigurieren, die Sie im Abschnitt AWS SSO Metadaten in der AWS-Konsole abrufen können.
X509 Öffentliches Zertifikat	Fügen Sie das heruntergeladene Zertifikat ein und entfernen Sie es.        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 Signaturverfahren	Standardmäßig wird AWS SSO mit <mark>sha256</mark> signieren. Sofern Sie dies nicht geändert haben, wählen Sie <mark>sha256</mark> aus dem Dropdown-Menü aus.
Deaktivieren Sie ausgehende Abmeldeanfragen	Die Anmeldung mit SSO unterstützt derzeit <b>nicht</b> SLO. Diese Option ist für zukünftige Entwicklungen geplant.
Möchte Authentifizierungsanfragen signiert haben	Ob AWS SSO 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:



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 AWS SSO Zugangsdaten-Bildschirm weitergeleitet:



AWS Zugangsdaten Bildschirm

Nachdem Sie sich mit Ihren AWS-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.