

ADMINISTRATOR
KONSOLE

> MELDEN SIE SICH MIT
SSO AN

> IMPLEMENTIERUNGSLEITFÄDEN

AWS SAML Implementierung

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.

⬇ Typ: Asset-Hyperlink ID: K4Z8ny0RzKkHKIJIZ4hh1

Öffnen Sie SSO in der Web-App

Melden Sie sich bei der Bitwarden-Web-App an und öffnen Sie die Administrator-Konsole mit dem Produktschalter :



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

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.

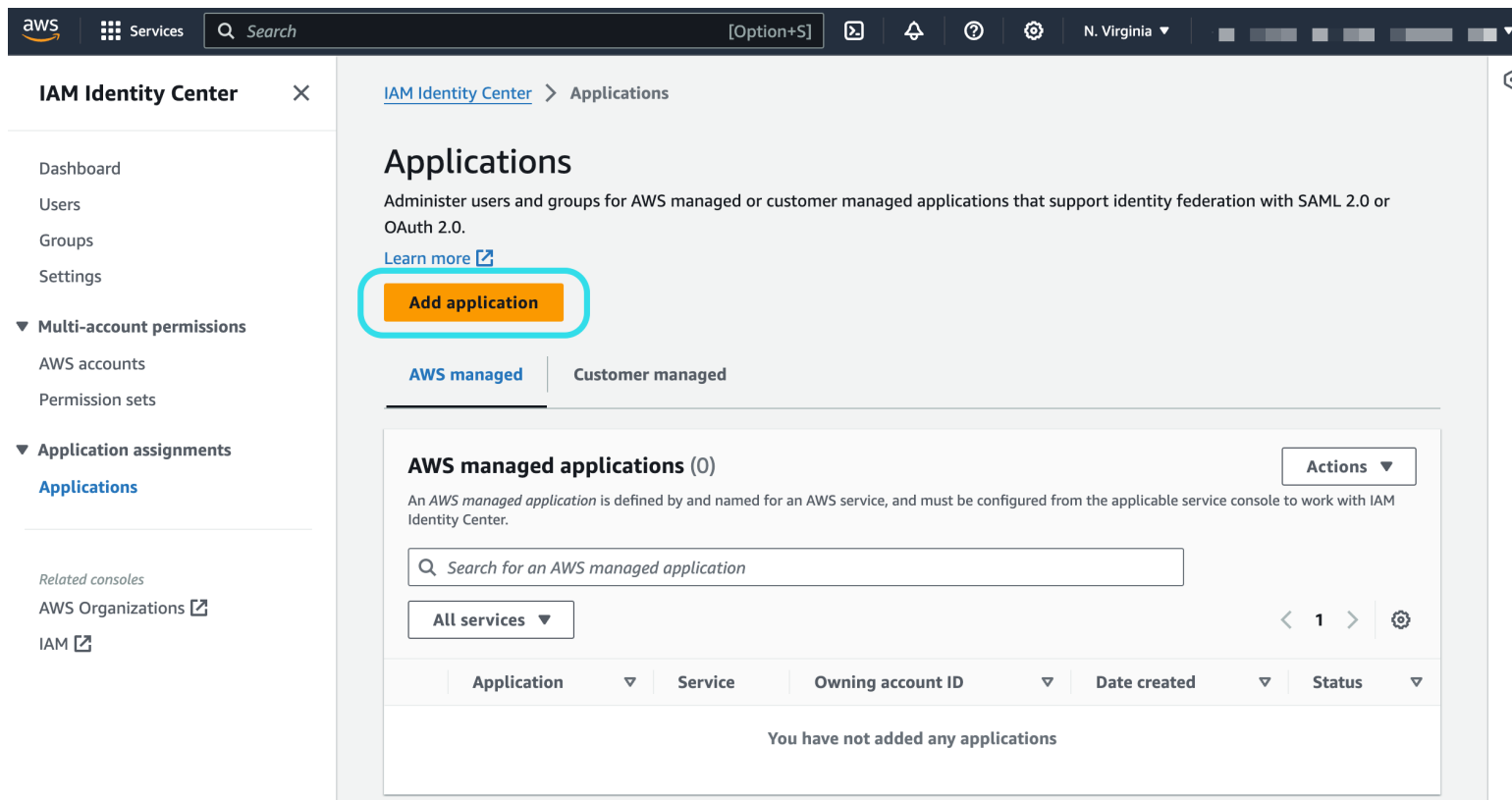


Tip

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**:



IAM Identity Center ×

Dashboard
Users
Groups
Settings

▼ Multi-account permissions
AWS accounts
Permission sets

▼ Application assignments
Applications

Related consoles
AWS Organizations [↗](#)
IAM [↗](#)

[IAM Identity Center](#) > Applications

Applications

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](#) [↗](#)

Add application

AWS managed | Customer managed

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.

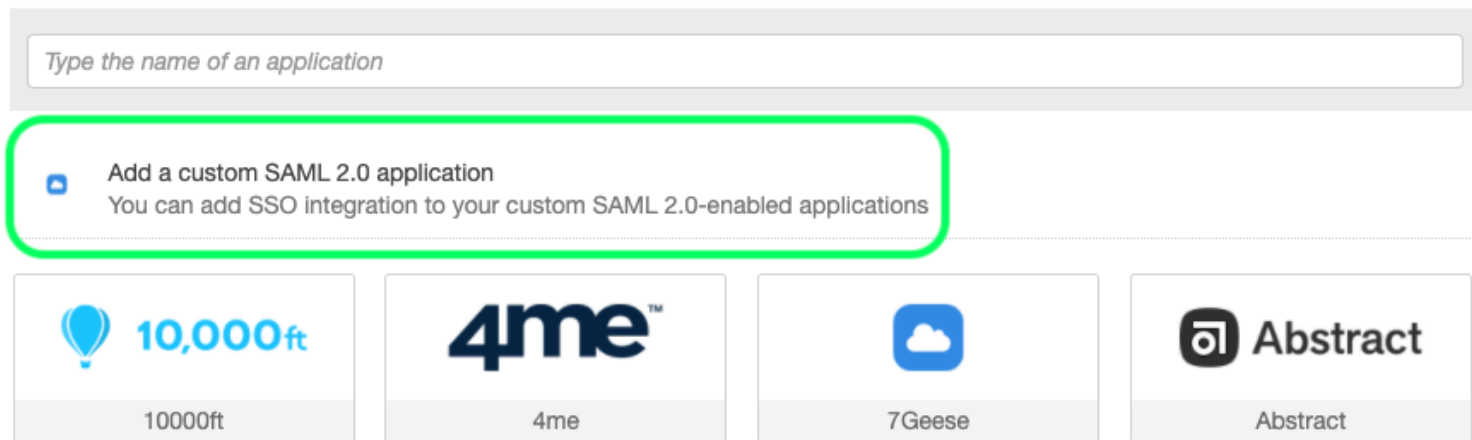
All services ▼ < 1 > ⚙

Application	Service	Owning account ID	Date created	Status
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

Add a custom SAML 2.0 application
You can add SSO integration to your custom SAML 2.0-enabled applications



10,000ft

10000ft



4me

4me



7Geese

7Geese



Abstract

Abstract

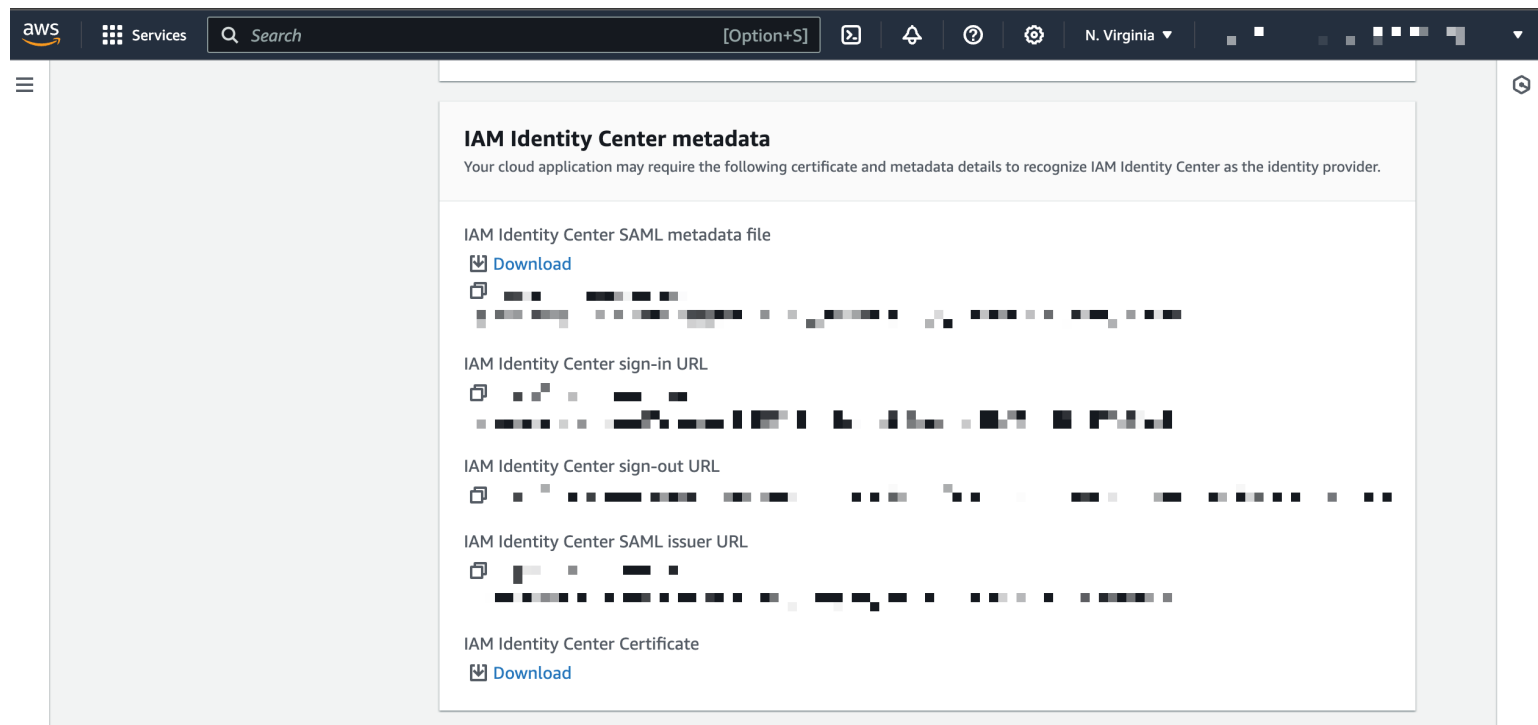
Fügen Sie eine benutzerdefinierte SAML-App hinzu

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 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 `https://vault.bitwarden.com/#/sso`. Für selbst gehostete Instanzen wird dies durch Ihre **konfigurierte Server-URL** bestimmt, zum Beispiel `https://your.domain/#/sso`.

Anwendungsmetadaten

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

Application metadata

IAM Identity Center requires specific metadata about your cloud application before it can trust this application. You can type this metadata manually or upload a metadata exchange file.

☒ Manually type your metadata values
 ☐ 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 Assertion Consumer Service (ACS) URL. Dieser automatisch generierte Wert kann von der Einstellungen → Single Sign-On Bildschirm der Organisation kopiert werden und variiert je nach Ihrer Konfiguration.
Anwendung SAML-Zielgruppe	Setzen Sie dieses Feld auf die vorab generierte SP Entity ID. Dieser automatisch generierte Wert kann aus den Einstellungen → Single Sign-On 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

Search

[Option+S]

N. Virginia

IAM Identity Center

Dashboard

Users

Groups

Settings

Multi-account permissions

AWS accounts

Permission sets

Application assignments

Applications

Configuration for 'Bitwarden SAML 2.0 application' has been saved.

You must configure attribute mappings for IAM Identity Center to work.

IAM Identity Center

Applications

Bitwarden SAML 2.0 application

Bitwarden SAML 2.0 application

Details

Actions

Edit configuration

Edit attribute mappings

Display name

Bitwarden SAML 2.0 application

Attributzuordnungen

Benutzerattribut in der Anwendung	Kartiert auf diesen String-Wert oder Benutzerattribut in AWS SSO	Format
Betreff	<code>\${user:email}</code>	E-Mail-Adresse
E-Mail-Adresse	<code>\${user:email}</code>	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 about user and group assignments](#)

Search for an assigned user or group

Username of user or group

Type

No users or groups to display

You have not assigned users and groups to this application.

Assign users 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 E-Mail-Adresse .
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 sha256 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 AWS SSO Aussteller URL ein, die Sie aus dem Abschnitt AWS SSO Metadaten in der AWS Konsole abgerufen haben. Dieses Feld ist Groß- und Kleinschreibungssensitiv.
Bindungsart	Einstellen auf HTTP POST oder Weiterleitung .
URL des Single Sign On Dienstes	Geben Sie die AWS SSO-Anmelde-URL ein, die Sie aus dem Abschnitt AWS SSO-Metadaten in der AWS-Konsole abgerufen haben.
Einzel Abmelden Service URL	Die Anmeldung mit SSO unterstützt derzeit nicht SLO. Diese Option ist für zukünftige Entwicklungen geplant, jedoch können Sie sie vorab mit der AWS SSO Abmelde-URL 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 sha256 signieren. Sofern Sie dies nicht geändert haben, wählen Sie sha256 aus dem Dropdown-Menü aus.
Deaktivieren Sie ausgehende Abmeldeanfragen	Die Anmeldung mit SSO unterstützt derzeit nicht SLO. Diese Option ist für zukünftige Entwicklungen geplant.

Feld	Beschreibung
Möchte Authentifizierungsanfragen signiert haben	Ob AWS SSO 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 AWS SSO Zugangsdaten-Bildschirm weitergeleitet:



Sign in

Username

alice, alice@domain.com, DOMAIN\alice

☐ Remember username

Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

AWS Zugangsdaten Bildschirm

Nachdem Sie sich mit Ihren AWS-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.