AWS SAML Implementierung

AWS SAML Implementierung

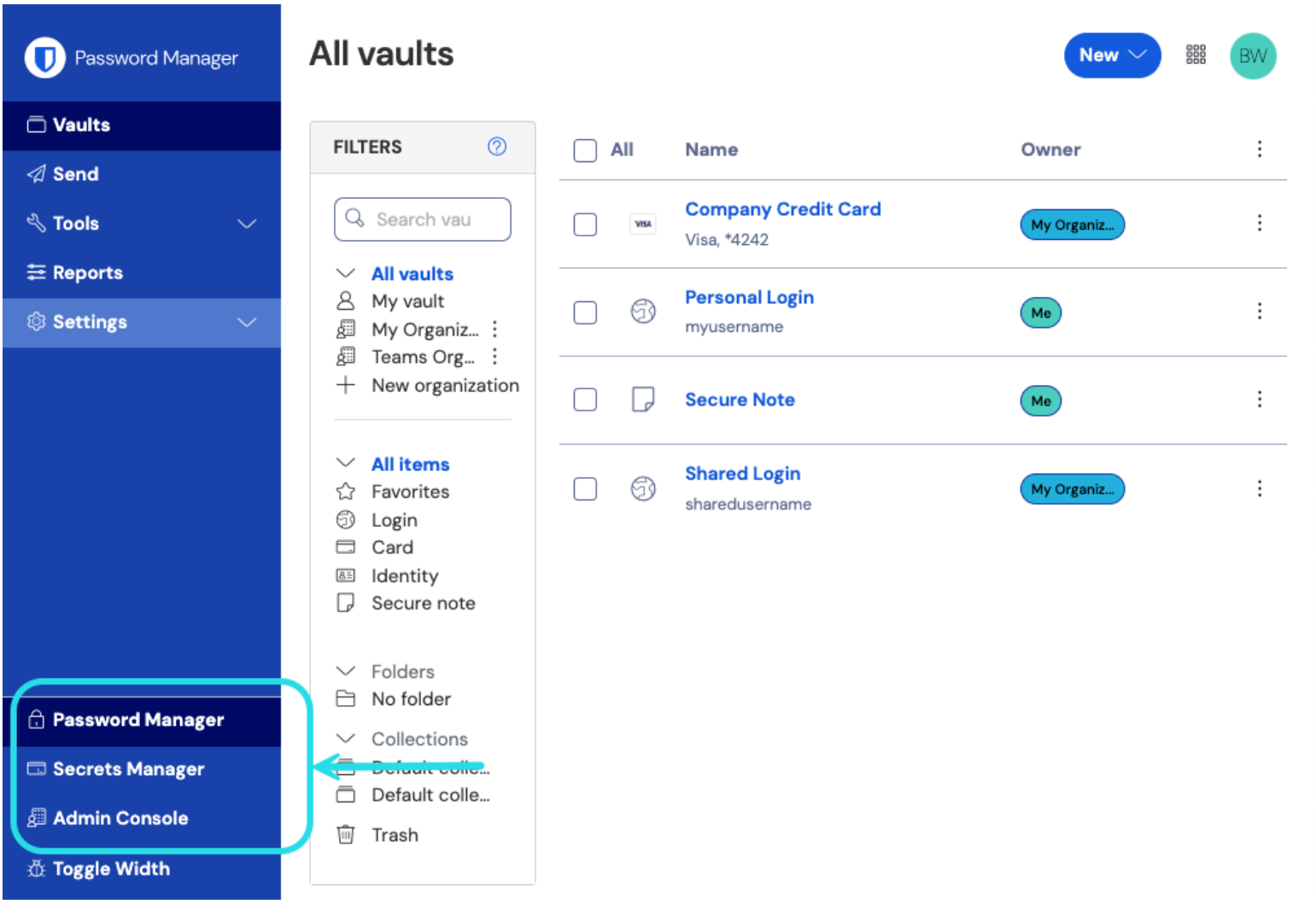
Dieser Artikel enthält **AWS-spezifische** Hilfe zur Konfiguration der Zugangsdaten mit SSO über SAML 2.0. Für Hilfe bei der Konfiguration der Zugangsdaten mit SSO für einen anderen IdP, verweisen Sie auf SAML 2.0 Konfiguration.

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: K4Z8nyORzKkHKIJIZ4hh1

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 (▦):



Produktwechsler

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

SAML 2.0 Konfiguration

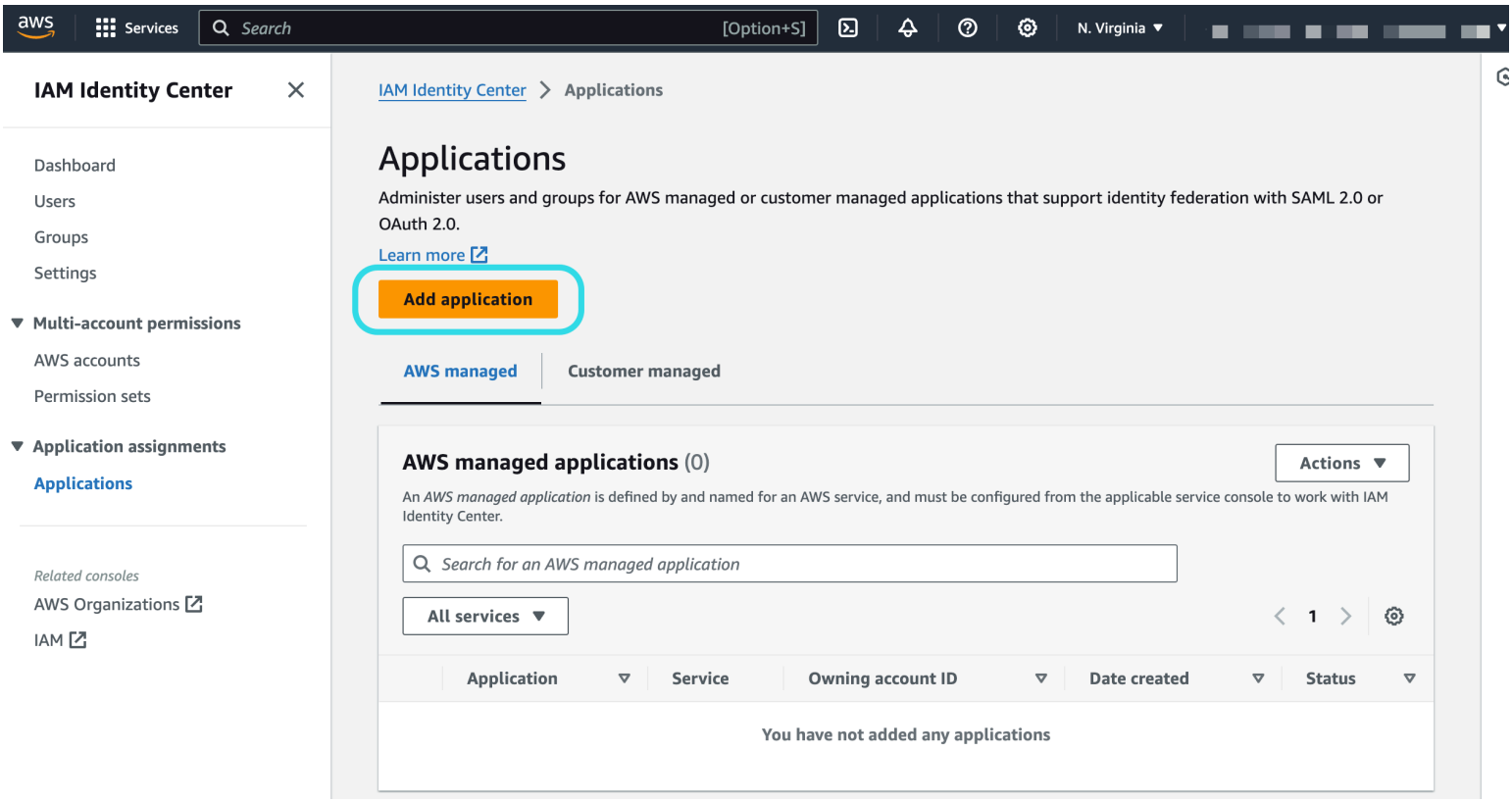
Wenn Sie es noch nicht getan haben, erstellen Sie einen einzigartigen **SSO-Identifikator** für Ihre Organisation und wählen Sie **SAML** aus dem **Typ**-Dropdown aus. Lassen Sie diesen Bildschirm geöffnet, um leicht darauf zugreifen zu können.

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.

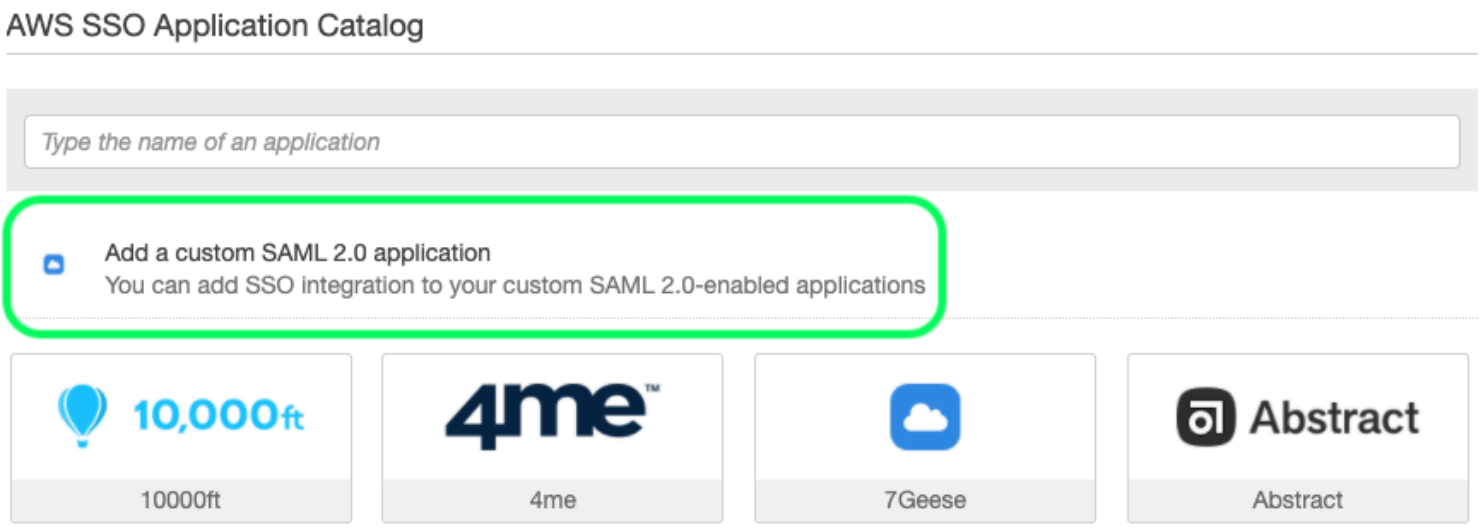
Erstellen Sie eine AWS SSO-Anwendung

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**:



Fügen Sie eine neue Anwendung hinzu

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



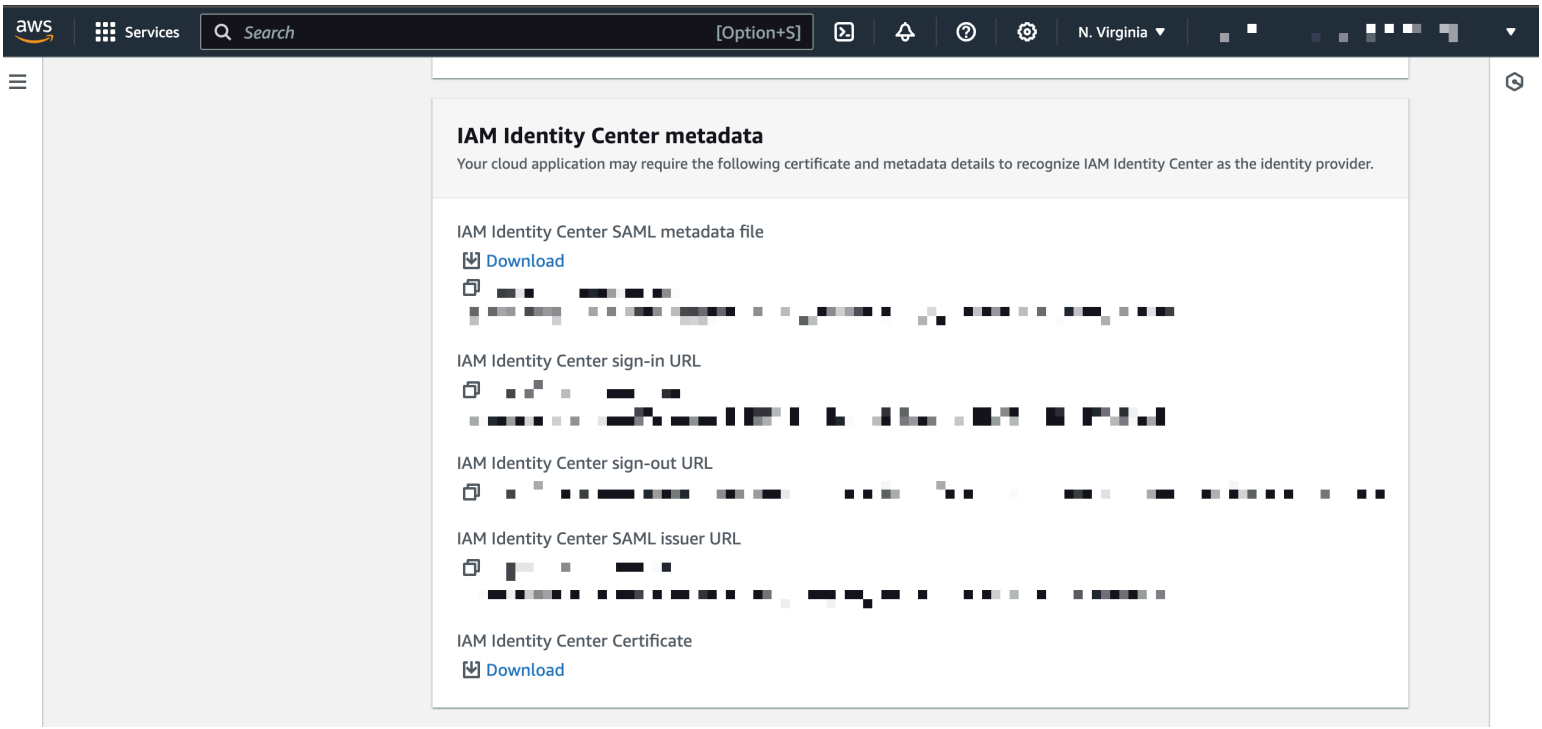
Fügen Sie eine benutzerdefinierte SAML-App hinzu

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:



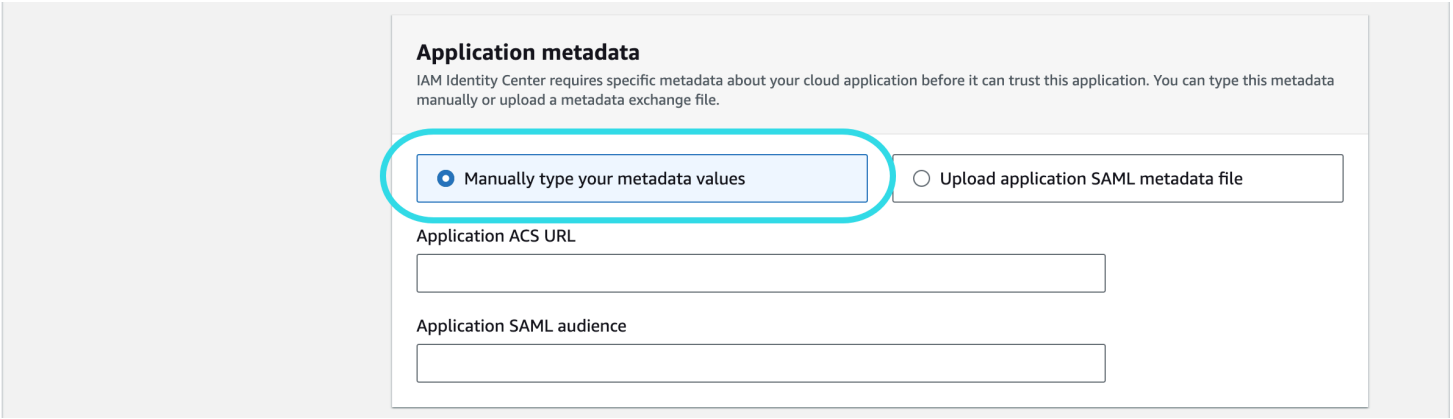
AWS SSO Metadaten

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:



Geben Sie Metadatenwerte ein

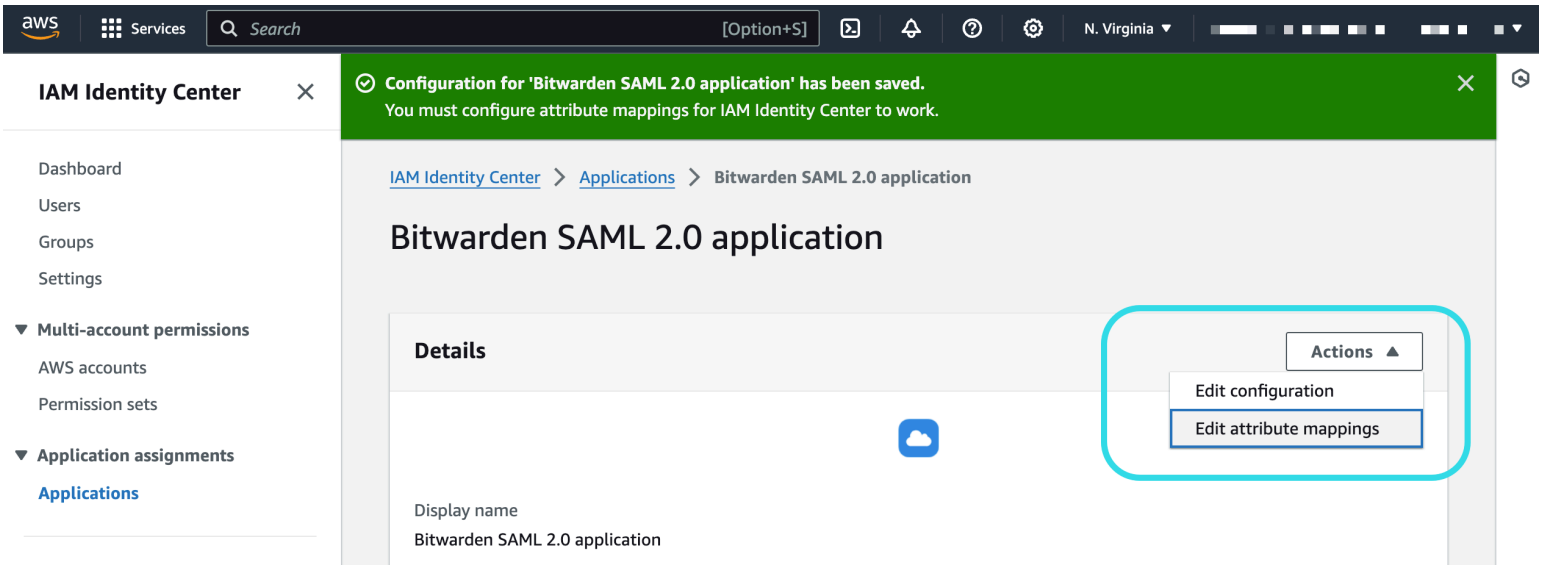
Konfigurieren Sie die folgenden Felder:

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:



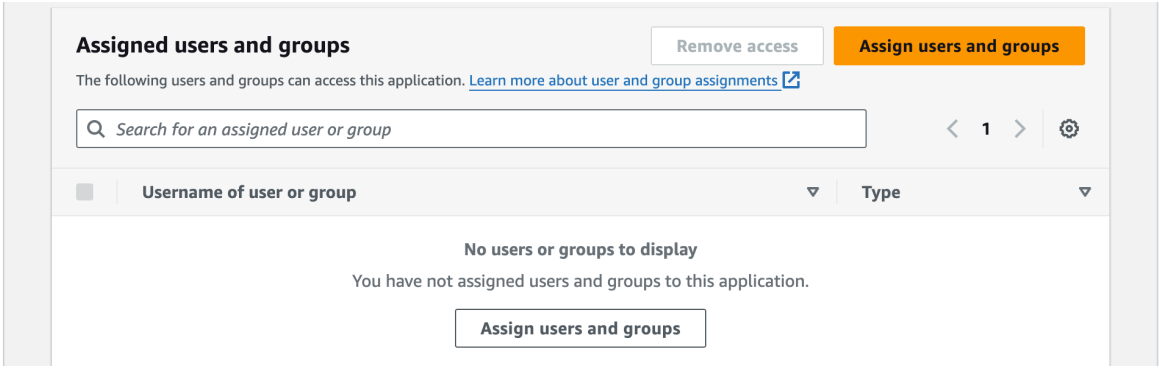
Attributzuordnungen

Benutzerattribut in der Anwendung	Kartiert auf diesen String-Wert oder Benutzerattribut in AWS SSO	Format
Betreff	`${user:email}`	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:



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**.

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 `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.

Feld	Beschreibung
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.
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.

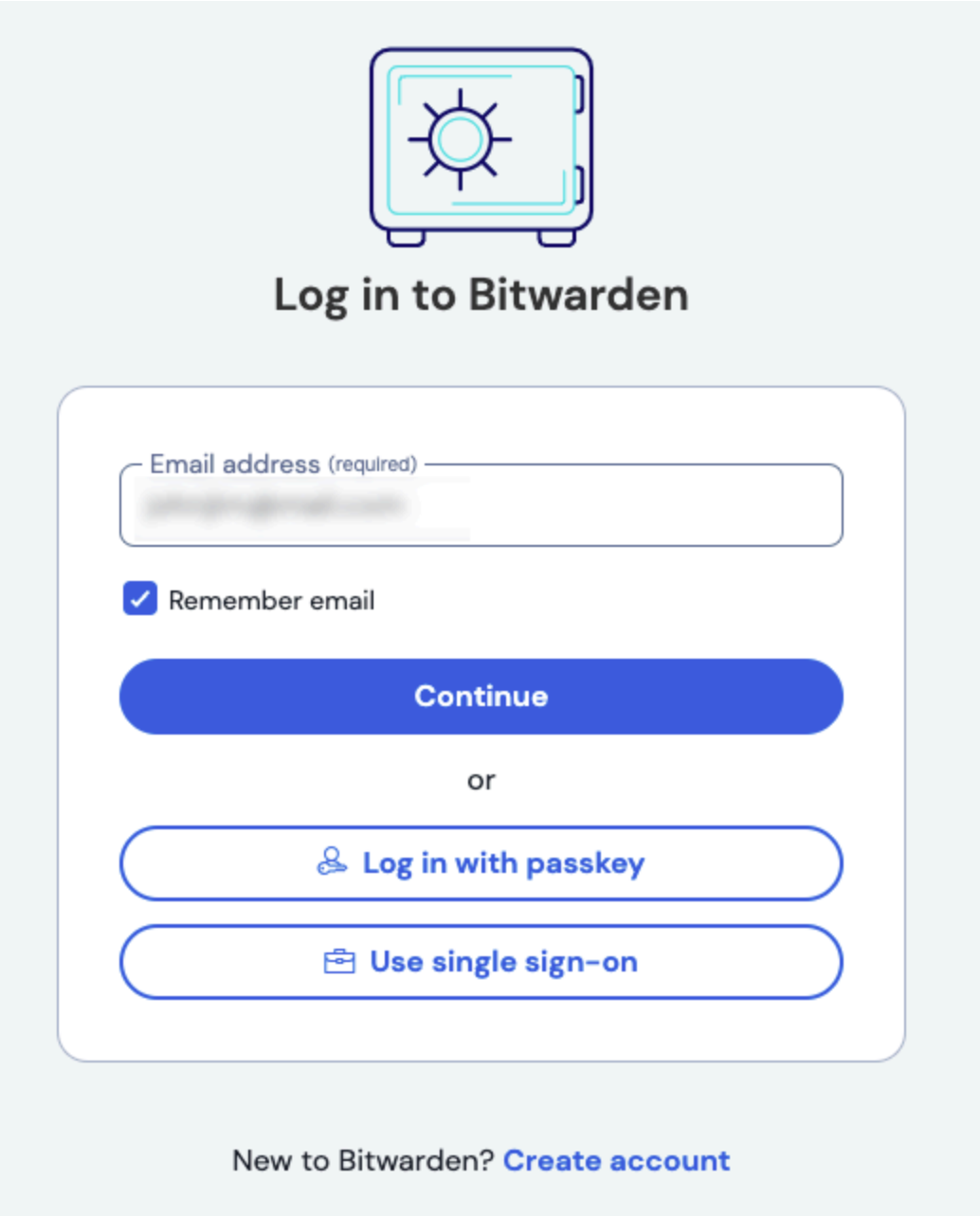
Wenn Sie mit der Konfiguration des Identitätsanbieters fertig sind, **speichern** Sie Ihre Arbeit.

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.

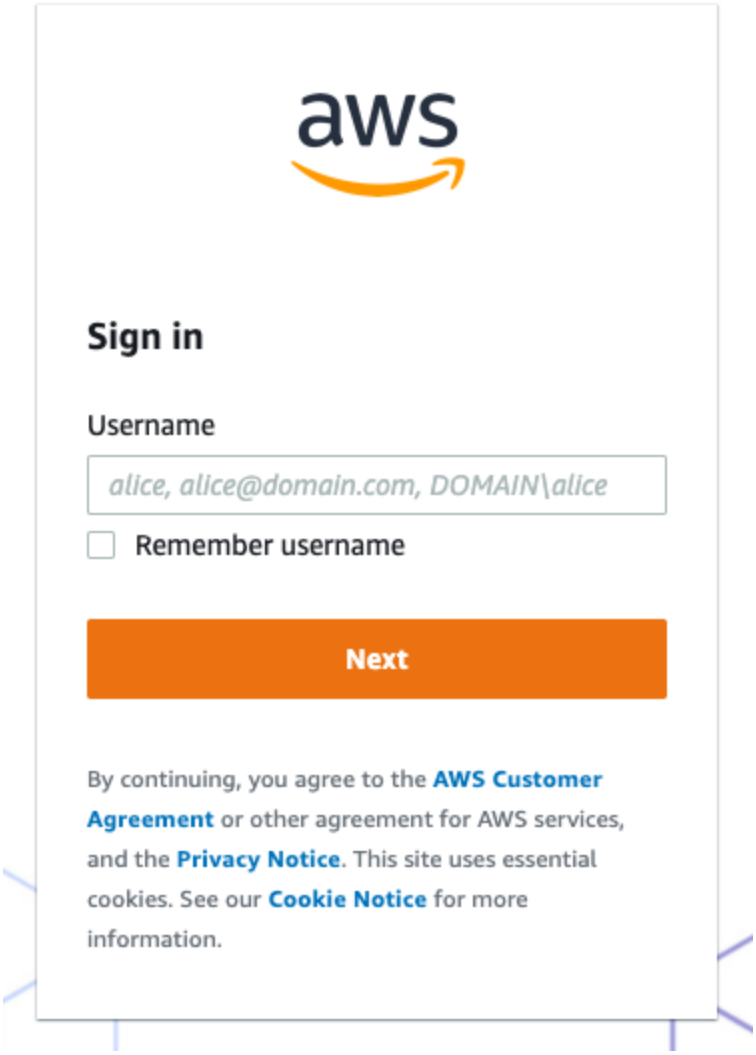
Testen Sie die Konfiguration

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:



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!

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.