

ADMINISTRATOR KONSOLE > MELDEN SIE SICH MIT SSO AN >

Keycloak SAML Implementierung

Ansicht im Hilfezentrum:

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

Keycloak SAML Implementierung

Dieser Artikel enthält **Keycloak-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 mit der Bitwarden-Webanwendung und dem Keycloak-Portal. 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

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

All vaults

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:

bitwarden
Admin Console

- 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)

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 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.



Es gibt alternative **Mitglied Entschlüsselungsoptionen**. Erfahren Sie, wie Sie mit [SSO auf vertrauenswürdigen Geräten](#) oder mit [Key Connector](#) beginnen können.

Keycloak Einrichtung

Melden Sie sich bei Keycloak an und wählen Sie **Clients** → **Client erstellen**.

Clients
Clients are applications and services that can request authentication of a user. [Learn more](#)

Clients list | Initial access token | Client registration

Search for client → **Create client** | Import client

Client ID	Name	Type	Description	Home URL
account	`\${client_account}`	OpenID Connect	–	
account-console	`\${client_account-console}`	OpenID Connect	–	
admin-cli	`\${client_admin-cli}`	OpenID Connect	–	–
broker	`\${client_broker}`	OpenID Connect	–	–
master-realm	master Realm	OpenID Connect	–	–
security-admin-console	`\${client_security-admin-...}`	OpenID Connect	–	

[Create a Client](#)

Auf dem Bildschirm "Client erstellen" füllen Sie die folgenden Felder aus:

Feld	Beschreibung
Client-Typ	Wählen Sie SAML.
Client-ID	Setzen Sie dieses Feld auf die vorab generierte SP Entity ID . Dieser automatisch generierte Wert kann von der Einstellungen → Single Sign-On Seite der Organisation kopiert werden und variiert je nach Ihrer Konfiguration.
Name	Geben Sie einen Namen Ihrer Wahl für den Keycloak-Client ein.

Sobald Sie die erforderlichen Felder auf der Seite **Allgemeine Einstellungen** ausgefüllt haben, klicken Sie auf **Weiter**.

Auf dem Bildschirm für die **Zugangsdaten Einstellungen**, füllen Sie das folgende Feld aus:

Feld	Beschreibung
Gültige Weiterleitungs-URIs	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.

Wählen Sie **Speichern**.

Wählen Sie die Tab "Keys" und schalten Sie die Option **Client-Signatur erforderlich** auf **Aus** um.

The screenshot shows the Keycloak administration interface. On the left is a dark sidebar with a navigation menu. The 'Clients' menu item is highlighted with a red circle. The main content area shows the 'Client details' page for a client with ID 'https://mat.bitwarden.support/sso/saml2'. The 'Keys' tab is selected and highlighted with a red circle. In the 'Signing keys config' section, the 'Client signature required' toggle is set to 'Off' and is also highlighted with a red circle. Other elements include a 'master' dropdown, a 'SAML' label, an 'Enabled' toggle, and an 'Action' dropdown menu.

Keycloak Keys Config

Zuletzt, in der Hauptnavigation von Keycloak, wählen Sie **Realm Einstellungen** und dann das **Keys** Tab. Finden Sie das **RS256** Zertifikat und wählen Sie **Zertifikat** aus.

Algorithm	Type	Kid	Use	Provider	Public keys
AES	OCT	a3282835-06db-42cc-b29a-ff969226eca9	ENC	aes-generated	
HS256	OCT	be68f437-88a6-4c3b-b92f-bf3b114beeb6	SIG	hmac-generated	
RSA-OAEP	RSA	zXKBNvtriZQU7MbyXJlIf60wGotgDbZwpG8_x7wE1QQ	ENC	rsa-enc-generated	Public key Certificate
RS256	RSA	T3IREov-EMgD0EnJ5AsHsv0GX-Z0s89jCyloy6fmlsE	SIG	rsa-generated	Public key Certificate

Keycloak RS256 Certificate

Der Wert für das Zertifikat wird für den folgenden [Abschnitt](#) benötigt.

Zurück zur Web-App

Bis zu diesem Zeitpunkt haben Sie alles, was Sie im Kontext des Keycloak-Portals benötigen, konfiguriert. Kehren Sie zur Bitwarden-Web-App zurück und wählen Sie **Einstellungen** → **Einmaliges Anmelden** aus der Navigation aus.

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.

Füllen Sie die folgenden Felder im Abschnitt **SAML Service Provider Konfiguration** aus:

Feld	Beschreibung
Namen ID-Format	Wählen Sie E-Mail-Adresse .
Ausgehendes Signaturalgorithmus	Der Algorithmus, den Bitwarden zur Signierung von SAML-Anfragen verwenden wird.
Unterzeichnungsverhalten	Ob/wann SAML-Anfragen signiert werden.

Feld	Beschreibung
Minimales Eingehendes Signieralgorithmus	Wählen Sie den Algorithmus aus, den der Keycloak-Client verwendet , um SAML-Dokumente oder Behauptungen zu signieren.
Möchte Behauptungen unterschrieben haben	Ob Bitwarden erwartet, dass SAML-Behauptungen signiert werden. Wenn aktiviert, stellen Sie sicher, dass Sie den Keycloak-Client so konfigurieren, dass er Behauptungen signiert .
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 mit den Bitwarden Zugangsdaten mit SSO Docker-Image konfiguriert.

Füllen Sie die folgenden Felder im Abschnitt **SAML Identitätsanbieter Konfiguration** aus:

Feld	Beschreibung
Entitäts-ID	Geben Sie die URL des Keycloak-Bereichs ein, in dem der Client erstellt wurde, zum Beispiel https://Reiche/ . Dieses Feld ist Groß- und Kleinschreibungssensitiv.
Bindungstyp	Wählen Sie Umleiten .
Single Sign-on-Dienst-URL	Geben Sie Ihre Master-SAML-Verarbeitungs-URL ein, zum Beispiel https://Reiche//protokoll/saml .
URL des Einzelabmeldedienstes	Die Anmeldung mit SSO unterstützt derzeit nicht SLO. Diese Option ist für zukünftige Entwicklungen geplant, jedoch können Sie sie vorab mit Ihrer Abmelde-URL konfigurieren, wenn Sie möchten.
Öffentliches X509-Zertifikat	Geben Sie das RS256 Zertifikat ein, das im vorherigen Schritt kopiert wurde. Der Zertifikatswert ist Groß- und Kleinschreibungssensitiv, zusätzliche Leerzeichen, Zeilenumbrüche und andere überflüssige Zeichen werden dazu führen, dass die Zertifikatsvalidierung fehlschlägt .

Feld	Beschreibung
Ausgehendes Signaturalgorithmus	Wählen Sie den Algorithmus aus, den der Keycloak-Client verwendet , um SAML-Dokumente oder Behauptungen zu signieren.
Deaktivieren Sie ausgehende Abmeldeanfragen	Die Anmeldung mit SSO unterstützt derzeit nicht SLO. Diese Option ist für zukünftige Entwicklungen geplant.
Möchte Authentifizierungsanfragen signiert haben	Ob Keycloak 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](#).

Zusätzliche Keycloak-Einstellungen

Auf der **Registerkarte „Keycloak-Client-Einstellungen“** stehen zusätzliche Konfigurationsoptionen zur Verfügung:

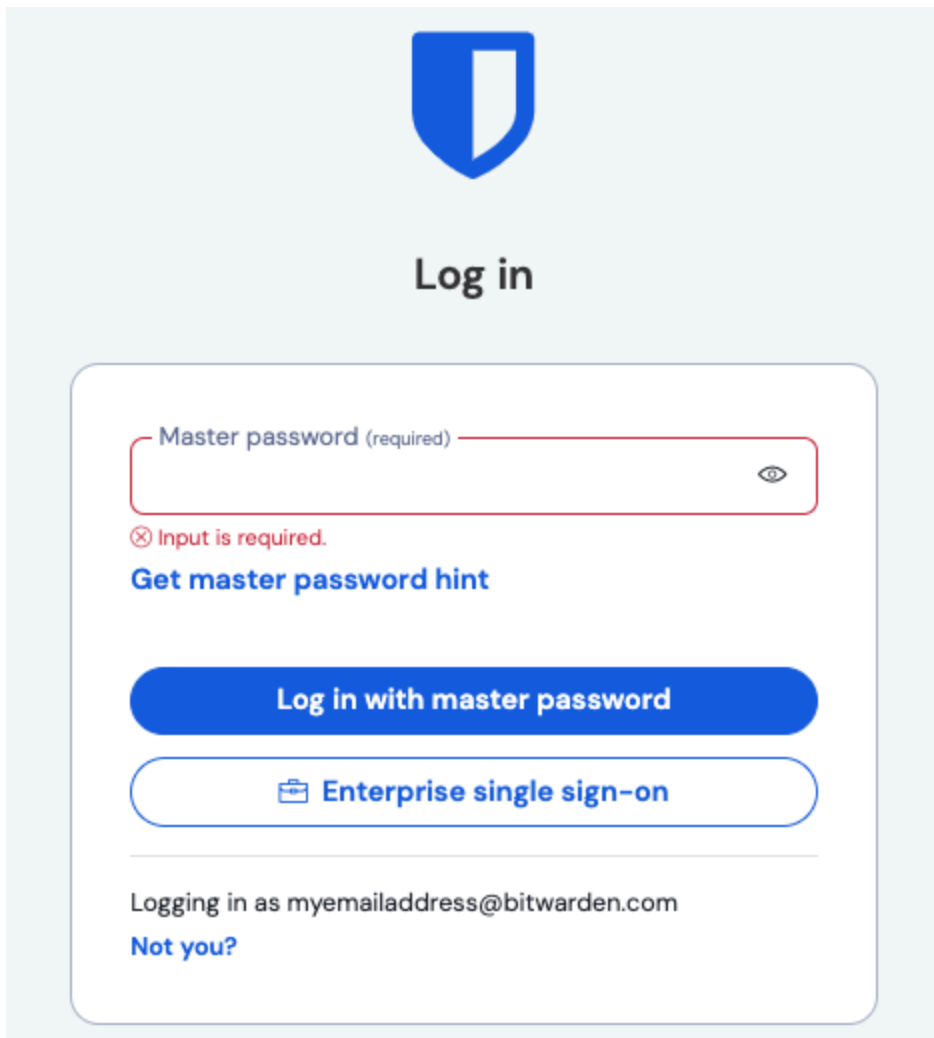
Feld	Beschreibung
Unterzeichnen Sie Dokumente	Geben Sie an, ob SAML-Dokumente von der Keycloak-Domäne signiert werden sollen.
Unterschriftenbehauptungen	Geben Sie an, ob SAML-Behauptungen von der Keycloak-Domäne signiert werden sollen.
Signaturalgorithmus	Wenn Sign Assertions aktiviert ist, wählen Sie aus, mit welchem Algorithmus signiert werden soll (sha-256 standardmäßig).

Feld	Beschreibung
Namens-ID-Format	Wählen Sie das Name-ID-Format, das Keycloak in SAML-Antworten verwenden soll.

Sobald Sie das Forum ausgefüllt haben, wählen Sie **Speichern**.

Testen Sie die Konfiguration

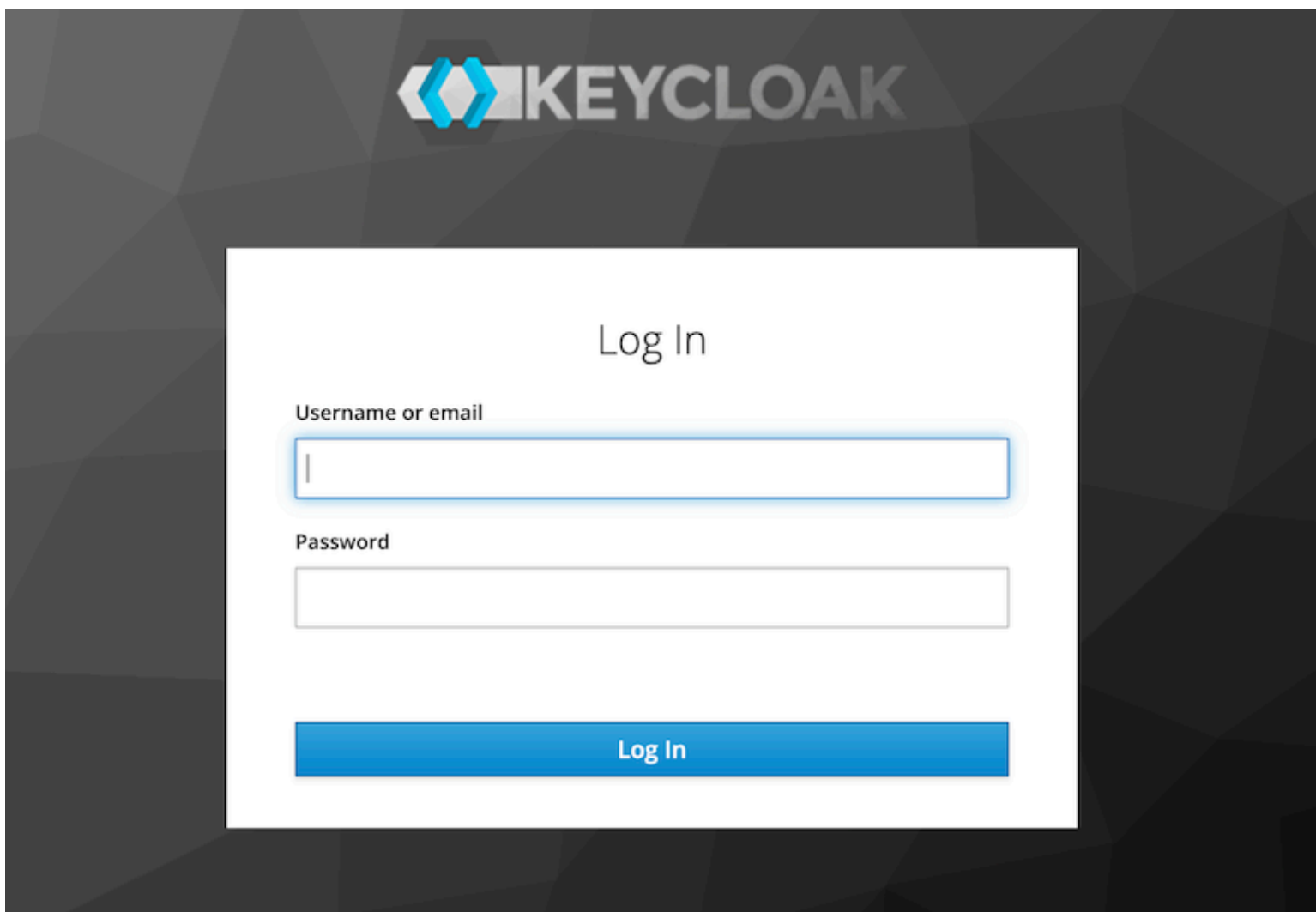
Sobald Ihre Konfiguration abgeschlossen ist, testen Sie diese, indem Sie zu <https://vault.bitwarden.com> navigieren, Ihre E-Mail-Adresse eingeben, **Weiter** auswählen und den **Enterprise Single-On** Button auswählen:



The screenshot shows the Bitwarden login interface. At the top is the Bitwarden logo and the text "Log in". Below this is a form with a "Master password (required)" input field. The field is empty and has a red border, with a red error message "Input is required." below it. To the right of the input field is an eye icon for toggling visibility. Below the error message is a link "Get master password hint". There are two buttons: a blue "Log in with master password" button and a white "Enterprise single sign-on" button with a briefcase icon. At the bottom of the form, it says "Logging in as myemailaddress@bitwarden.com" and a link "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 zum Keycloak Zugangsdaten-Bildschirm weitergeleitet:



Keycloak Login Screen

Nachdem Sie sich mit Ihren Keycloak-Anmeldedaten 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.