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.

Ω 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 Produktumschalter (翻):

D Password Manager	All vaults			New 🗸	BW BW
🗇 Vaults	FILTERS		Name	Owner	:
🖉 Send			Name	Owner	•
\ll Tools \sim	Q Search vau	ASIV	Company Credit Card Visa, *4242	My Organiz	÷
≅ Reports	✓ All vaults		Demonstration in		
🕸 Settings 🛛 🗸 🗸	A My vault	0 3	Personal Login myusername	Me	:
	gia 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				
Secrete Manager	✓ Collections				
	Default colle				
Admin Console	🖻 Trash				
🔆 Toggle Width					
		Droduktu	rechelor		

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

Secure and trusted open source password manager for business

D bit Warden	Single sign-on 🗰 🖪	
g My Organization $$	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.	
绺 Groups	SSO identifier (required) unique-organization-identifier	٦
$ agreen arrow = 1 \ \text{Reporting} \bigtriangledown$	Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification	
😫 Billing 🗸 🗸	Member decryption options	
Settings	Master password	
Organization info	Trusted devices Once authenticated members will decrypt you't data using a key stored on their device. The single organization policy SSO required policy 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 SP entity ID	
SCIM provisioning	i a com a comunicación e com a contractiva e diferencia e del máxima de la comunicación de la comuni	
	SAML 2.0 metadata URL	٦

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.

Keycloak Einrichtung

Melden Sie sich bei Keycloak an und wählen Sie Clients \rightarrow Client erstellen.

					0)	admin 🔻	
master 🗸	Clients Clients are applications ar	d services that can reques	authentication	of a user. Learn more 🗹				
Manage								
Clients	Clients list Initial acc	cess token Client regis	tration					
Client scopes	Q Search for client	→ Create client	Import clie	ent			1-6 💌 <	>
Realm roles								
Users	Client ID	Name	Туре	Description	Home URL			
Groups	account	\${client_account}	OpenID Connect	-				***
	account-console	\${client_account-console}	OpenID Connect	-				***
Sessions	admin-cli	\${client_admin-cli}	OpenID Connect	-	_			•
Events	broker	\${client_broker}	OpenID Connect	-	_			* *
Configure	master-realm	master Realm	OpenID Connect	-	-			***
Realm settings	security-admin-console	\${client_security-admin	OpenID Connect	-				0 0 0

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.

master 🔹	Clients > Client details							
	https://mat.bitwarden.support/sso/saml2 SAML O Enabled O Action -							
Manage	Clients are applications and services that can request authentication of a user.							
Clients	Settings Keys Roles Client scopes Sessions Advanced							
Client scopes								
Realm roles								
Users	Signing keys config							
Groups	If you enable the "Client signature required" below, you must configure the signing keys by generating or importing keys, and the							
Sessions	client will sign their saml requests and responses. The signature will be validated.							
Events	Client signature Off required ③							
Configure								
Realm settings								

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.

U bitwarden

Secure and trusted open source password manager for business

master -	<	General L	ogin Email.	Themes	Keys	Events	Localizati	on	Security defenses	Sessions	Tokens	Clie	>
Manage	Keys list	Providers											
Clients	T Active	keys 🔻	Q Search ke	ey.		\rightarrow					1-4	. <	>
Client scopes													
Realm roles	Algorithm	Туре	Kid					Use	Provider	Publi	c keys		
Users	AES	ост	a3282835-0	6db-42cc-b29	9a-ff9692	26eca9		ENC	aes-generated				
Groups									5				
Sessions	HS256	ОСТ	be68f437-88	3a6-4c3b-b92	2f-bf3b114	beeb6		SIG	hmac-generate	d			
Events													
Configure	RSA-OAEF	P RSA	zXKBnvtriZQ	U7MbyXJIIf6	DwGotgDl	oZwpG8_x7	wE1QQ	ENC	rsa-enc-genera	ited Pu	blic key	Certi	ficate
Realm settings													
Authentication	RS256	RSA	T3IREov-EM	gD0EnJ5AsH	sv0GX-Z(s89jCy1oy6	ofmlsE	SIG	rsa-generated	Pu	blic key	Certi	ficate
Identity providers													
User federation											1-4 💌	<	>

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	Wählen Sie den Algorithmus aus, den der Keycloak-Client verwendet, um SAML-Dokumente
Signieralgorithmus	oder Behauptungen zu signieren.
Möchte Behauptungen	Ob Bitwarden erwartet, dass SAML-Behauptungen signiert werden. Wenn aktiviert, stellen Sie
unterschrieben haben	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//p rotokoll/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.

(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.

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.
Unterschriftsbehauptungen	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).

U bitwarden

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:



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	
Log In Username or email	
Password	
Log In	

Keycloak Login Screen

Nachdem Sie sich mit Ihren Keycloak-Anmeldedaten 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.