

ADMIN CONSOLE > LOGIN WITH SSO >

Keycloak SAML Implementation

View in the help center:

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

Keycloak SAML Implementation

This article contains **Keycloak-specific** help for configuring login with SSO via SAML 2.0. For help configuring login with SSO for another IdP, refer to [SAML 2.0 Configuration](#).

Configuration involves working simultaneously with the Bitwarden web app and the Keycloak Portal. As you proceed, we recommend having both readily available and completing steps in the order they are documented.

Tip

Already an SSO expert? Skip the instructions in this article and download screenshots of sample configurations to compare against your own.

[Download Sample](#)

Open SSO in the web app

Log in to the Bitwarden web app and open the Admin Console using the product switcher:

The screenshot shows the Bitwarden web app interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, and Settings. At the bottom of the sidebar is the product switcher, which includes Password Manager, Secrets Manager, Admin Console, and Toggle Width. A red circle highlights the product switcher, and a red arrow points to the Admin Console option. The main content area is titled 'All vaults' and features a 'New' button, a grid icon, and a 'BW' profile icon. Below this is a table of vaults with columns for 'All', 'Name', and 'Owner'. The table lists several vaults: Company Credit Card (Owner: My Organiz...), Personal Login (Owner: Me), Secure Note (Owner: Me), and Shared Login (Owner: My Organiz...). A 'FILTERS' sidebar is open on the left, showing a search bar and a list of categories: All vaults, All items, Favorites, Login, Card, Identity, Secure note, Folders, Collections, and Trash.

Product switcher

Open your organization's **Settings** → **Single sign-on** screen:

- 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 configuration

If you haven't already, create a unique **SSO identifier** for your organization and select **SAML** from the **Type** dropdown. Keep this screen open for easy reference.

You can turn off the **Set a unique SP entity ID** option at this stage if you wish. Doing so will remove your organization ID from your SP entity ID value, however in almost all cases it is recommended to leave this option on.



There are alternative **Member decryption options**. Learn how to get started using [SSO with trusted devices](#) or [Key Connector](#).

Keycloak setup

Login to Keycloak and select **Clients** → **Create Client**.

The screenshot shows the Keycloak Admin Console interface. On the left is a navigation sidebar with 'Clients' highlighted. The main content area is titled 'Clients' and includes a search bar, a 'Create client' button (circled in red), and a table of existing clients.

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

On the Create client screen fill in the following fields:

Field	Description
Client type	Select SAML.
Client ID	Set this field to the pre-generated SP Entity ID . This automatically-generated value can be copied from the organization's Settings → Single sign-on screen and will vary based on your setup.
Name	Enter a name of your choice for the Keycloak client.

Once you have filled in the required fields on the **General Settings** page, click **Next**.

On the **Login settings** screen, fill in the following field:

Field	Description
Valid redirect URIs	Set this field to the pre-generated Assertion Consumer Service (ACS) URL . This automatically-generated value can be copied from the organization's Settings → Single sign-on screen and will vary based on your setup.

Select **Save**.

Select the Keys tab and toggle the **Client signature required** option to **Off**.

The screenshot shows the Bitwarden interface for configuring a client. On the left is a dark sidebar with a navigation menu including 'Clients', 'Client scopes', 'Realm roles', 'Users', 'Groups', 'Sessions', 'Events', 'Configure', and 'Realm settings'. The 'Clients' menu item is highlighted with a red circle. The main content area shows 'Client details' for a client with the URL 'https://mat.bitwarden.support/sso/saml2' and a 'SAML' protocol. A red circle highlights the 'Keys' tab in the top navigation bar. Below the tabs, the 'Signing keys config' section is visible, containing a red circle around the 'Client signature required' toggle, which is currently set to 'Off'.

Keycloak Keys Config

Lastly, on the Keycloak main navigation, select **Realm settings** and then the **Keys** tab. Locate the **RS256** Certificate and select **Certificate**.

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-Z0s89jCyl0y6fmlsE	SIG	rsa-generated	Public key Certificate

Keycloak RS256 Certificate

The value for the certificate will be required for the following [section](#).

Back to the web app

At this point, you have configured everything you need within the context of the Keycloak Portal. Return to the Bitwarden web app and select **Settings** → **Single sign-on** from the navigation.

The Single sign-on screen separates configuration into two sections:

- **SAML service provider configuration** will determine the format of SAML requests.
- **SAML identity provider configuration** will determine the format to expect for SAML responses.

Complete the following fields in the **SAML service provider configuration** section:

Field	Description
Name ID format	Select Email .
Outbound Signing Algorithm	The algorithm Bitwarden will use to sign SAML requests.
Signing Behavior	Whether/when SAML requests will be signed.

Field	Description
Minimum Incoming Signing Algorithm	Select the algorithm the Keycloak client is configured to use to sign SAML documents or assertions.
Want Assertions Signed	Whether Bitwarden expects SAML assertions to be signed. If toggled on, make sure you configure the Keycloak client to sign assertions .
Validate Certificates	Check this box when using trusted and valid certificates from your IdP through a trusted CA. Self-signed certificates may fail unless proper trust chains are configured with the Bitwarden login with SSO docker image.

Complete the following fields in the **SAML identity provider configuration** section:

Field	Description
Entity ID	Enter the URL of the Keycloak realm on which the client was created, for example <a href="https://<keycloak_domain>/realms/<realm_name>">https://<keycloak_domain>/realms/<realm_name> . This field is case sensitive.
Binding type	Select Redirect .
Single sign-on service URL	Enter your master SAML processing URL, for example <a href="https://<keycloak_domain>/realms/<realm_name>/protocol/saml">https://<keycloak_domain>/realms/<realm_name>/protocol/saml .
Single Log Out Service URL	Login with SSO currently does not support SLO. This option is planned for future development, however you may preconfigure it with your Logout URL if you wish.
X509 public certificate	Enter the RS256 certificate that was copied in the previous step. The certificate value is case sensitive, extra spaces, carriage returns, and other extraneous characters will cause certificate validation to fail .
Outbound Signing Algorithm	Select the algorithm the Keycloak client is configured to use to sign SAML documents or assertions.

Field	Description
Disable Outbound Logout Requests	Login with SSO currently does not support SLO. This option is planned for future development.
Want Authentication Requests Signed	Whether Keycloak expects SAML requests to be signed.

Note
 When completing the X509 certificate, take note of the expiration date. Certificates will have to be renewed in order to prevent any disruptions in service to SSO end users. If a certificate has expired, Admin and Owner accounts will always be able to log in with email address and master password.

When you're done with the identity provider configuration, **Save** your work.

Tip
 You can require users to log in with SSO by activating the single sign-on authentication policy. Please note, this will require activating the single organization policy as well. [Learn more](#).

Additional Keycloak settings

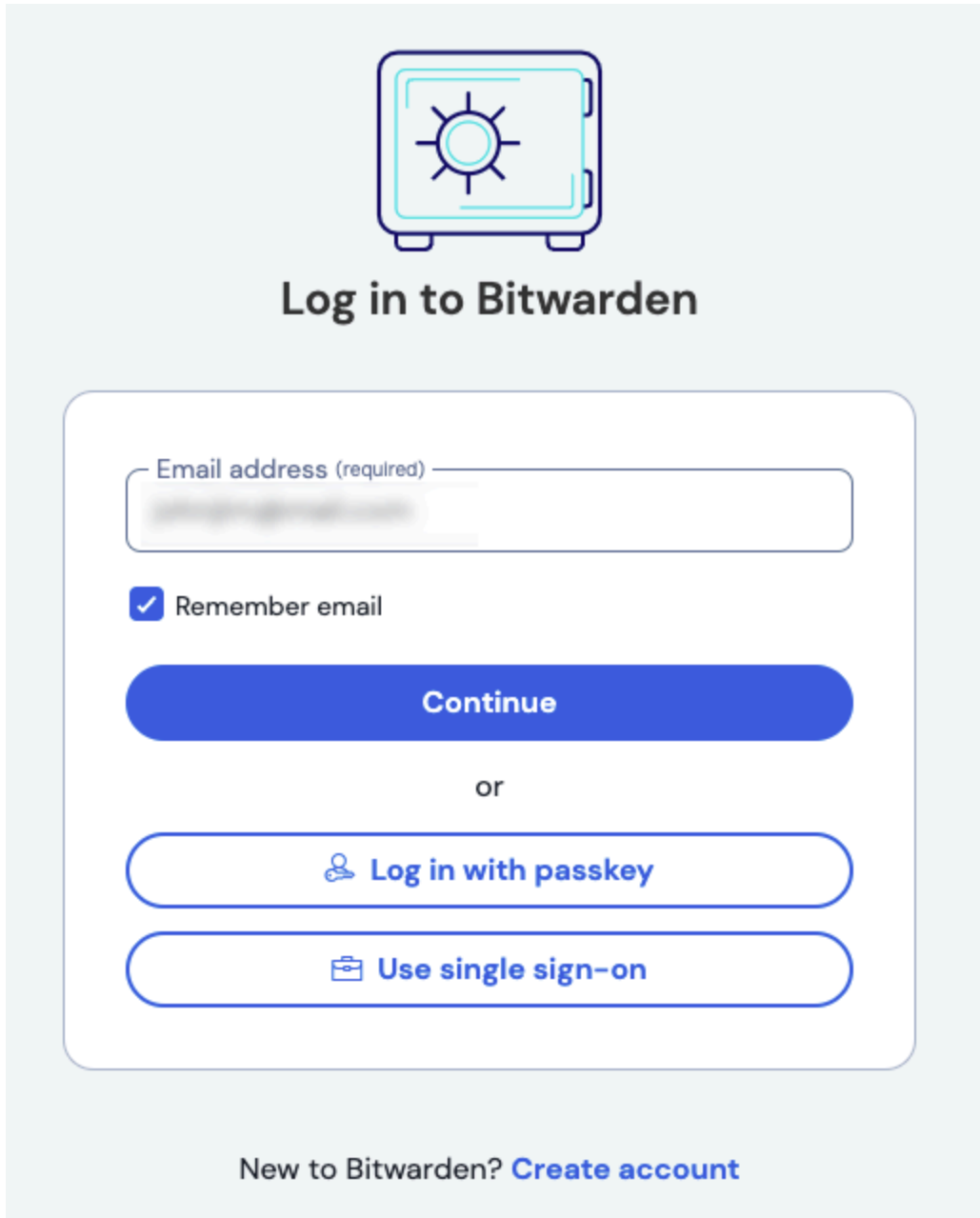
On the Keycloak Client **Settings** tab, additional configuration options are available:

Field	Description
Sign Documents	Specify whether SAML documents should be signed by the Keycloak realm.
Sign Assertions	Specify whether SAML assertions should be signed by the Keycloak realm.
Signature Algorithm	If Sign Assertions is enabled, select what algorithm to sign with (sha-256 by default).
Name ID Format	Select the Name ID Format for Keycloak to use in SAML responses.

Once you have completed the forum, select **Save**.

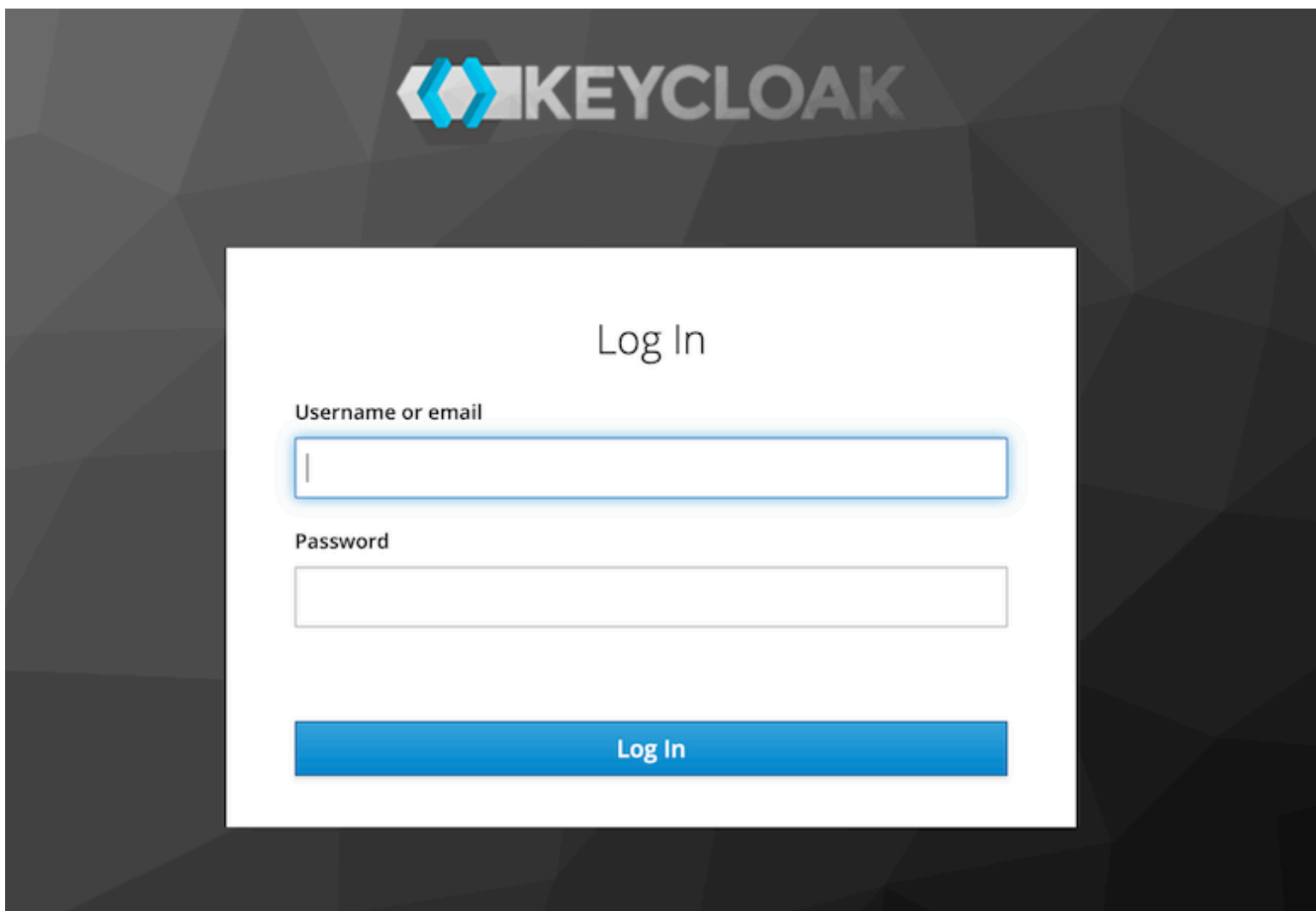
Test the configuration

Once your configuration is complete, test it by navigating to <https://vault.bitwarden.com>, entering your email address and selecting the **Use single sign-on** button:



Log in options screen

Enter the [configured organization identifier](#) and select **Log In**. If your implementation is successfully configured, you will be redirected to the Keycloak login screen:



Keycloak Login Screen

After you authenticate with your Keycloak credentials, enter your Bitwarden master password to decrypt your vault!

Note

Bitwarden does not support unsolicited responses, so initiating login from your IdP will result in an error. The SSO login flow must be initiated from Bitwarden.