## ADMIN CONSOLE $\rightarrow$ LOGGA IN MED SSO $\rightarrow$

# **AuthO SAML Implementation**

View in the help center: https://bitwarden.com/help/saml-authO/

## **AuthO SAML Implementation**

This article contains **AuthO-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 within the Bitwarden web app and the AuthO 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.

Jownload Sample ⊥

### Open SSO in the web app

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

Password Manager	All vaults			New 🗸	BW
🗇 Vaults	FILTERS ⑦		Name	Owner	:
🖉 Send					
$\sim$ Tools $\sim$	Q Search vau	VISA	Company Credit Card Visa, *4242	My Organiz	:
₩ Reports	✓ All vaults				
🕸 Settings 🛛 🗸 🗸	A My vault	0 6	Personal Login myusername	Me	÷
	g≝ Teams Org : + New organization		Secure Note	Ме	:
	<ul> <li>✓ All items</li> <li>☆ Favorites</li> <li>④ Login</li> <li>⊡ Card</li> <li>Identity</li> <li>☑ Secure note</li> </ul>		Shared Login sharedusername	My Organiz	:
A Password Manager	<ul><li>✓ Folders</li><li>☐ No folder</li></ul>				
Secrets Manager	Collections				
🗿 Admin Console	🔟 Trash				
🖞 Toggle Width					
		Product swi	tcher		

© 2025 Bitwarden Inc | Page 2 of 14

## **U bit**warden

### Säker och pålitlig lösenordshanterare med öppen källkod för företag

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

<b>D bit</b> warden Admin Console	Single sign-on 🗰 🕒
$\blacksquare$ My Organization $~~ \lor~$	Use the <b>require single sign-on authentication policy</b> 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.
뿅 Groups	SSO identifier (required) unique-organization-identifier
$ age = Reporting \qquad \lor$	Provide this ID to your members to login with SSO. To bypass this step, set up <b>Domain verification</b>
🗟 Billing $\checkmark$	Member decryption options
$\otimes$ Settings $\land$	Master password
Organization info	○ Trusted devices
Policies	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.
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
SCIM provisioning	
	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 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.

### **♀** Tip

There are alternative Member decryption options. Learn how to get started using SSO with trusted devices or Key Connector.

## **Create an AuthO application**

In the AuthO Portal, use the Applications menu to create a Regular Web Application:

### Säker och pålitlig lösenordshanterare med öppen källkod för företag

$\mathbf{\mathbf{Q}}$	dev-hn11g2a6 Development	Q Discuss your needs	II Docs 🗘 🙃
<b>₽</b>	Thank you for purchasing the Free Auth0 plan. You have 22 days features that are not in the Free plan. Like what you're seeing? P	left in your trial to experiment with lease enter your billing information here.	BILLING
\$			
6	Applications		- CREATE APPLICATION
i:	Setup a mobile, web or IoT application to use Auth0 for Authentication. Le	earn more 🕨	
റ			
)	Default App		
0	Generic Client ID: RM3UeXnRtL8CSjPF	Cg7HiitjInvQs0Be ℃	
ល			
		10	

AuthO Create Application

Click the **Settings** tab and configure the following information, some of which you will need to retrieve from the Bitwarden Single Sign-On screen:



AuthO Setting	Description
Application Login URI	Set this field to the pre-generated <b>SP Entity ID</b> . This automatically-generated value can be copied from the organization's <b>Settings → Single</b> <b>sign-on</b> screen and will vary based on your setup.
Allowed Callback URLS	Set this field to the pre-generated <b>Assertion Consumer Service (ACS) URL</b> . This automatically-generated value can be copied from the organization's <b>Settings → Single</b> <b>sign-on</b> screen and will vary based on your setup.

### **Grant Types**

In the Advanced Settings -> Grant Types section, ensure that the following Grant Types are selected (they may be pre-selected):

				bettee bettings	Application Metadata
					Grants
dentials	Client Creder	Refresh Token	de 🔽	Authorization Co	Implicit
]		]			
		ss OTP	Passwordle	MFA	Password
		ss OTP	Passwordle	MFA	Password

#### Application Grant Types

### Certificates

In the Advanced Settings  $\rightarrow$  Certificates section, copy or download up your signing certificate. You won't need to do anything with it just yet, but you will need to reference it later.

Advanced Settings					
Application Metadata	Device Settings	OAuth	Grant Types	WS-Federation	Certificates
igning Certificate					
					_
BEGIN CERT	IFICATE	(aMAGCCCa	COTHODOGROWIL	MCOvIT i A a DaNV	С) С
BEGIN CERT MIIDDTCCAfWgAwI BAMTGWRldilobie	IFICATE BAgIJdp2+Lsu8Iył xZzJhNi51cv5hdXF	CMA0GCSq CoMC5ib20	GSIb3DQEBCwU wHhcNMiEwNDE	AMCQxIjAgBgNV 1MTUxMiUxWhcN	С)
BEGIN CERT MIIDDTCCAfWgAwI BAMTGWRldi1objE MzQxMjIzMTUxMjU	IFICATE BAgIJdp2+Lsu8IyH xZzJhNi51cy5hdXF xWjAkMSIwIAYDVQ0	(cMA0GCSq RoMC5jb20 QDEx1kZXY	GSIb3DQEBCwU wHhcNMjEwNDE taG4xMWcyYTY	AMCQxIjAgBgNV 1MTUxMjUxWhcN udXMuYXV0aDAu	6) I
BEGIN CERT MIIDDTCCAfWgAwI BAMTGWRldi1objE MzQxMjIzMTUxMjU Y29tMIIBIjANBgk	IFICATE BAgIJdp2+Lsu8IyH xZzJhNi51cy5hdXF xWjAkMSIwIAYDVQ0 qhkiG9w0BAQEFAA0	(cMA0GCSq RoMC5jb20 QDEx1kZXY QCAQ8AMII	GSIb3DQEBCwU wHhcNMjEwNDE taG4xMWcyYTY BCgKCAQEA2yR	AMCQxIjAgBgNV 1MTUxMjUxWhcN udXMuYXV0aDAu fsSC5LCYkTvuF	G
BEGIN CERT MIIDDTCCAfWgAwI BAMTGWRldi1objE MzQxMjIzMTUxMjU Y29tMIIBIjANBgko nCW0wCEE7jkTtdx	IFICATE BAgIJdp2+Lsu8IyH xZzJhNi51cy5hdXF xWjAkMSIwIAYDVQ0 qhkiG9w0BAQEFAA0 RGytTBwJEarqzmgM	(cMA0GCSq RoMC5jb20 QDEx1kZXY OCAQ8AMII MzktBmkU0	GSIb3DQEBCwU wHhcNMjEwNDE taG4xMWcyYTY BCgKCAQEA2yR BfuzjrtcaQx0	AMCQxIjAgBgNV 1MTUxMjUxWhcN udXMuYXV0aDAu fsSC5LCYkTvuF utRM679AD0PX9	G
BEGIN CERT MIIDDTCCAfWgAwI BAMTGWRldi1objE MzQxMjIzMTUxMjU Y29tMIIBIjANBgk nCW0wCEE7jkTtdx WZLqwiCErdeKP01	IFICATE BAgIJdp2+Lsu8IyH xZzJhNi51cy5hdXF xWjAkMSIwIAYDVQ0 qhkiG9w0BAQEFAA0 RGytTBwJEarqzmgM S3/TvqkNkPyf2UE2	(cMA0GCSq RoMC5jb20 QDExlkZXY OCAQ8AMII MZktBmkU0 27Qo4giJy	GSIb3DQEBCwU wHhcNMjEwNDE taG4xMWcyYTY BCgKCAQEA2yR BfuzjrtcaQx0 6FEUAgsqwTs/	AMCQxIjAgBgNV 1MTUxMjUxWhcN udXMuYXV0aDAu fsSC5LCYkTvuF utRM679AD0PX9 gtX6sxIogeH0N	G

AuthO Certificate

#### Endpoints

You don't need to edit anything in the Advanced Settings  $\rightarrow$  Endpoints section, but you will need the SAML endpoints to reference later.

### **♀** Tip

In smaller windows, the **Endpoints** tab can disappear behind the edge of the browser. If you're having trouble finding it, click the **Certificates** tab and hit the Right Arrow key ( $\rightarrow$ ).

tadata	Device Settings	OAuth	Grant Types	WS-Federation	Certificates	Endpoints
DAuth						
DAuth Au	uthorization URL					

AuthO Endpoints

## **Configure AuthO actions**

Create actions to customize the logic that AuthO will use during the post-login flow and dictate the parameters of the exchange with Bitwarden. To create the necessary action:

1. Navigate to Actions  $\rightarrow$  Library and select Create Action  $\rightarrow$  Build from scratch.

- 2. Give you action a name like Bitwarden SSO, chose the Login / Post Login Trigger, choose the Node 18 (Recommended) Runtime option, and select Create.
- 3. In the integrated code editor, add the following rule:

#### Säker och pålitlig lösenordshanterare med öppen källkod för företag

## **D** bit warden

## JavaScript

```
exports.onExecutePostLogin = async (event, api) => {
    // Modify SAML configuration settings
    if (event.request.protocol === 'samlp') {
        api.saml.updateConfiguration({
            signatureAlgorithm: "rsa-sha256",
            digestAlgorithm: "sha256",
            signResponse: true,
            nameIdentifierFormat: "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
            binding: "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
        });
    };
};
```

#### 4. Select Deploy.

5. Navigate to Actions  $\rightarrow$  Triggers and select the post-login trigger.

6. Drag and drop your new action into the **Post Login** flow and select **Apply**.

When configuring the above action, you can customize any of the following attributes to fit your needs:

Кеу	Description
signatureAl gorithm	Algorithm AuthO will use to sign the SAML assertion or response. This value should be set to rsa-sha256. You must also set: -Set digestAlgorithm to sha256. -Set (in Bitwarden) the Minimum Incoming Signing Algorithm to rsa-sha256.
digestAlgor ithm	Algorithm used to calculate digest of SAML assertion or response. Set to sha-256.
signRespons e	By default, AuthO will sign only the SAML assertion. Set this to <b>true</b> to sign the SAML response instead of the assertion.

Кеу	Description
nameIdentif ierFormat	By default, urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified. You can set this value to any SAML NameID format. If you do, change the SP Name ID Format field to the corresponding option (see here).

### Migrate from rules to actions

On November 18, 2024 AuthO will deprecate rules. If you are currently using a rule as described in a previous version of this document, you can use a **Migrate to Action** button on the AuthO Rules screen to make this process easier. If you do this:

- Do not toggle the pre-existing rule off.
- Do add the new action to your **post-login** trigger as described above in steps 5 & 6.

### Back to the web app

At this point, you have configured everything you need within the context of the AuthO Portal. Return to the Bitwarden web app to complete configuration.

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.

#### Service provider configuration

Unless you have configured custom rules, your service provider configuration will already be complete. If you configured custom rules or want to make further changes to your implementation, edit the relevant fields:

Field	Description
Name ID Format	NameID Format to specify in the SAML request (NameIDPolicy). To omit, set to Not Configured.
Outbound Signing Algorithm	Algorithm used to sign SAML requests, by default rsa-sha256.
Signing Behavior	Whether/when Bitwarden SAML requests will be signed. By default, AuthO will not require requests to be signed.

Field	Description
Minimum Incoming Signing Algorithm	The minimum signing algorithm Bitwarden will accept in SAML responses. Select <b>rsa-sha256</b> from the dropdown unless you have configured a custom signing rule.
Want Assertions Signed	Whether Bitwarden wants SAML assertions signed. By default, AuthO will sign SAML assertions, so check this box unless you've configured a custom signing rule.
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 within the Bitwarden Login with SSO docker image.

When you are done with the service provider configuration, **Save** your work.

## Identity provider configuration

Identity provider configuration will often require you to refer back to the AuthO Portal to retrieve application values:

Field	Description
Entity ID	Enter the <b>Domain</b> value of your AuthO application (see here), prefixed by urn:, for example urn: bw-help.us.auth0.com. This field is case sensitive.
Binding Type	Select <b>HTTP POST</b> to match the Token Endpoint Authentication Method value specified in your AuthO application.
Single Sign On Service URL	Enter the <b>SAML Protocol URL</b> (see Endpoints) of your AuthO application. For example, <a href="https://bw-help.us.auth0.com/samlp/HcpxD63h7Qzl420u8qachPWoZEG0Hho2">https://bw-help.us.auth0.com/samlp/HcpxD63h7Qzl420u8qachPWoZEG0Hho2</a> .
Single Log Out Service URL	Login with SSO currently <b>does not</b> support SLO. This option is planned for future development, however you may pre-configure it if you wish.
X509 Public Certificate	Paste the retrieved signing certificate, removingBEGIN CERTIFICATE

Field	Description
	and
	END CERTIFICATE
	The certificate value is case sensitive, extra spaces, carriage returns, and other extraneous characters <b>will cause certification validation to fail</b> .
Outbound Signing Algorithm	Select rsa-sha256 unless you've configured a custom signing rule.
Disable Outbound Logout Requests	Login with SSO currently <b>does not</b> support SLO. This option is planned for future development.
Want Authentication Requests Signed	Whether AuthO expects SAML requests to be signed.
(i) 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 are 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.

### 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 to Bitwarden
Email ad	Idress (required)
	Continue
	or
	😞 Log in with passkey
$\square$	🖻 Use single sign-on
N	lew to Bitwarden? Create account

#### 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 AuthO login screen:



AuthO Login

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

#### (i) 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.