bitwarden | Help Center Article

ADMIN CONSOLE > LOGGA IN MED SSO >

# AuthO SAML Implementation

View in the help center:
https://bitwarden.com/help/saml-auth0/

# Auth0 SAML Implementation

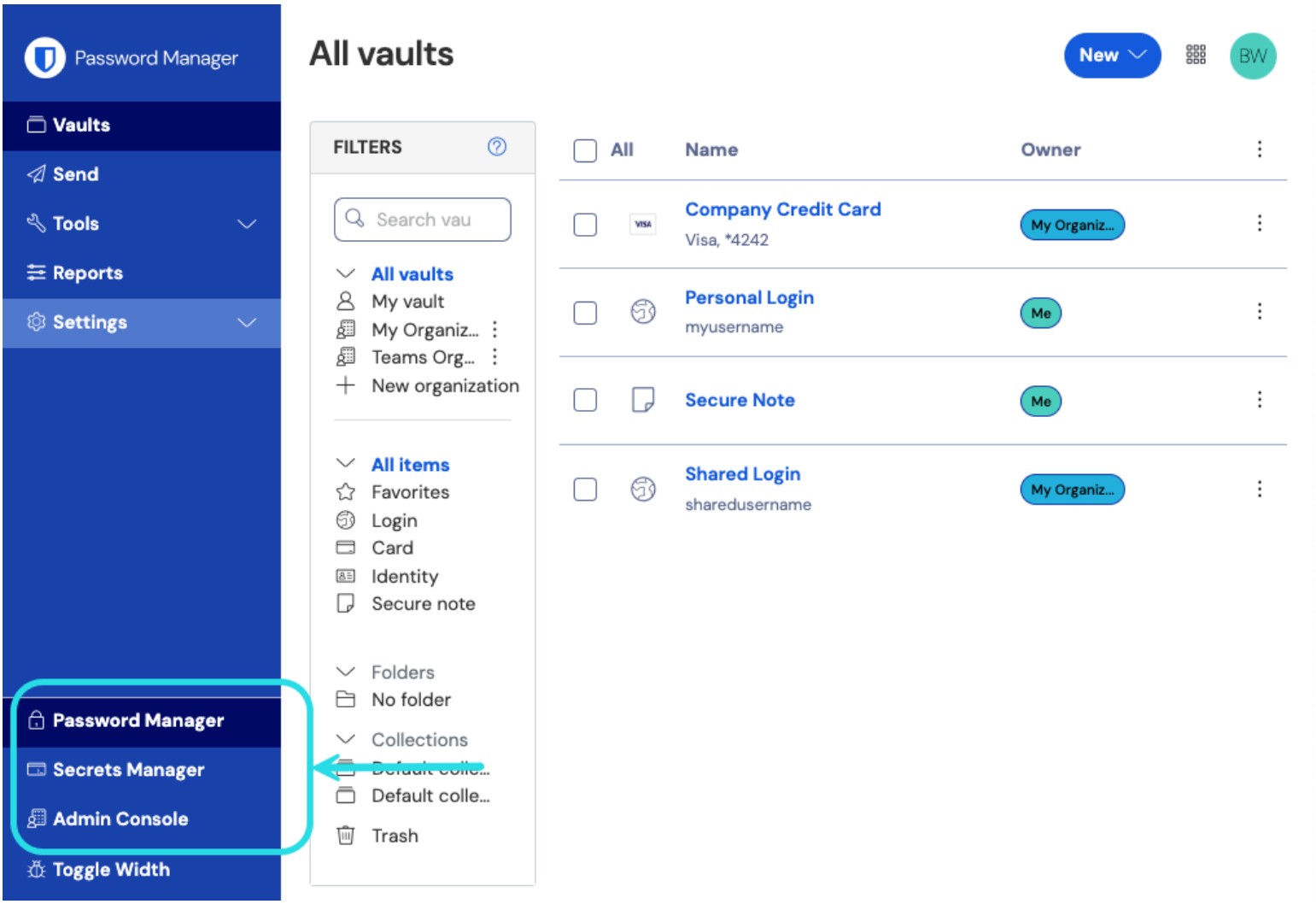
This article contains **Auth0-specific** help for configuring Login with SSO via SAML 2.0. For help configuring login with SSO for another IdP, refer to SAML 2.0 Configuration.

Configuration involves working simultaneously within the Bitwarden web app and the Auth0 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:




Product switcher

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


SAML 2.0 configuration

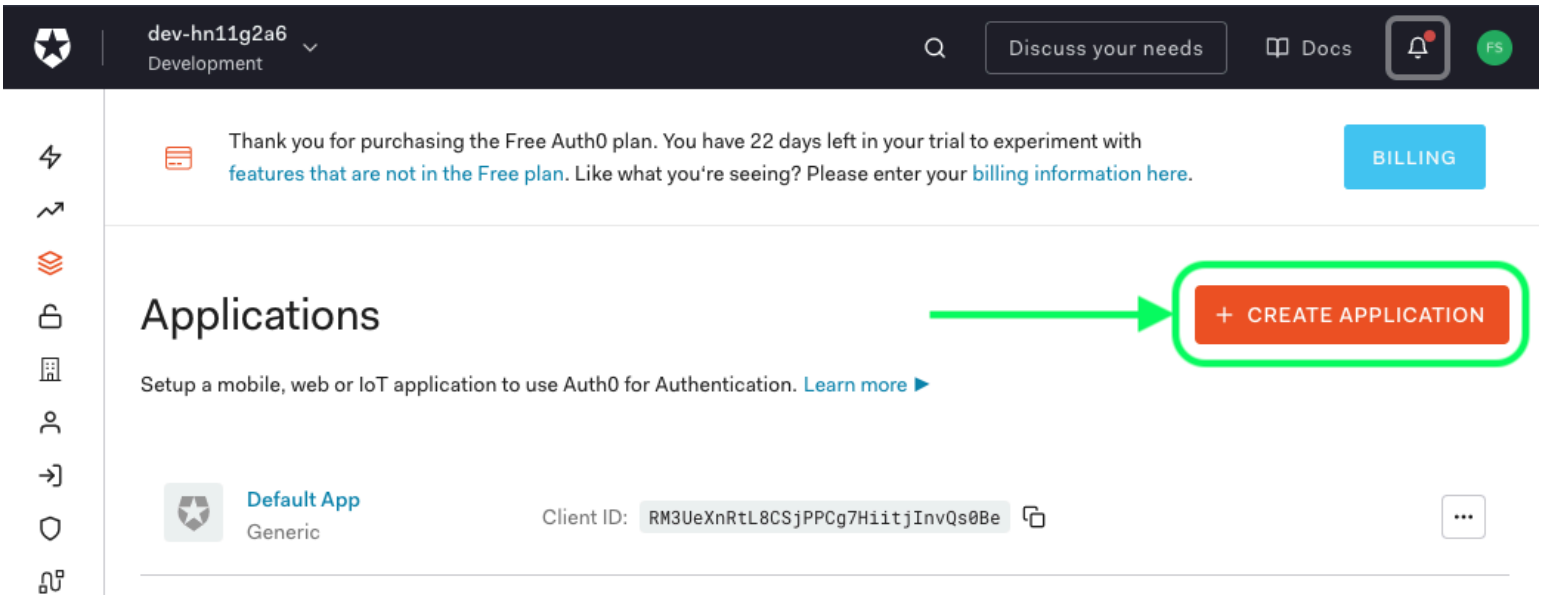
If you haven't already, create a unique **SSO identifier** for your organization and select **SAML** from the the **Type** dropdown. Keep this screen open for easy reference.

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.

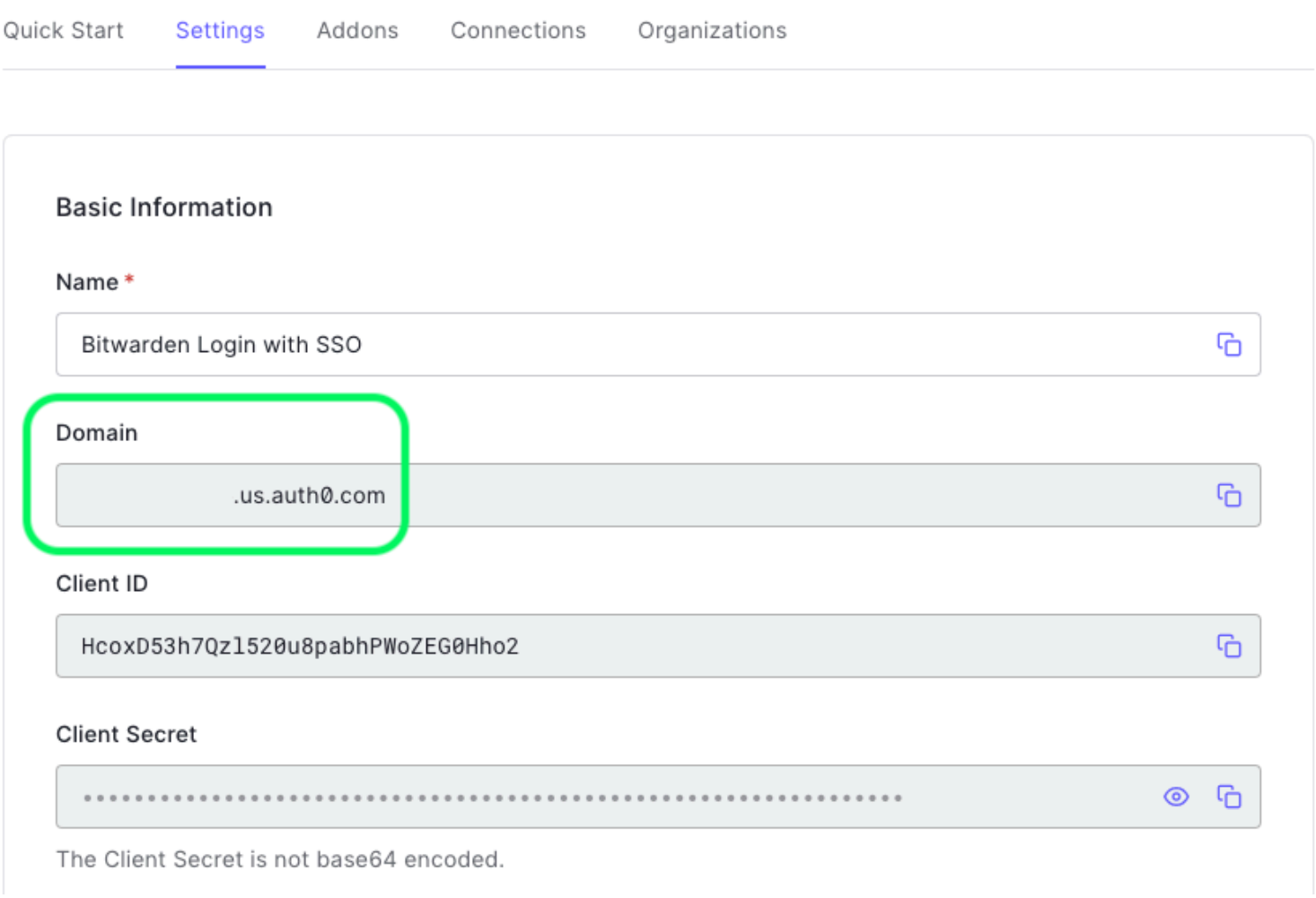
## Create an Auth0 application

In the Auth0 Portal, use the Applications menu to create a **Regular Web Application**:




Auth0 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:



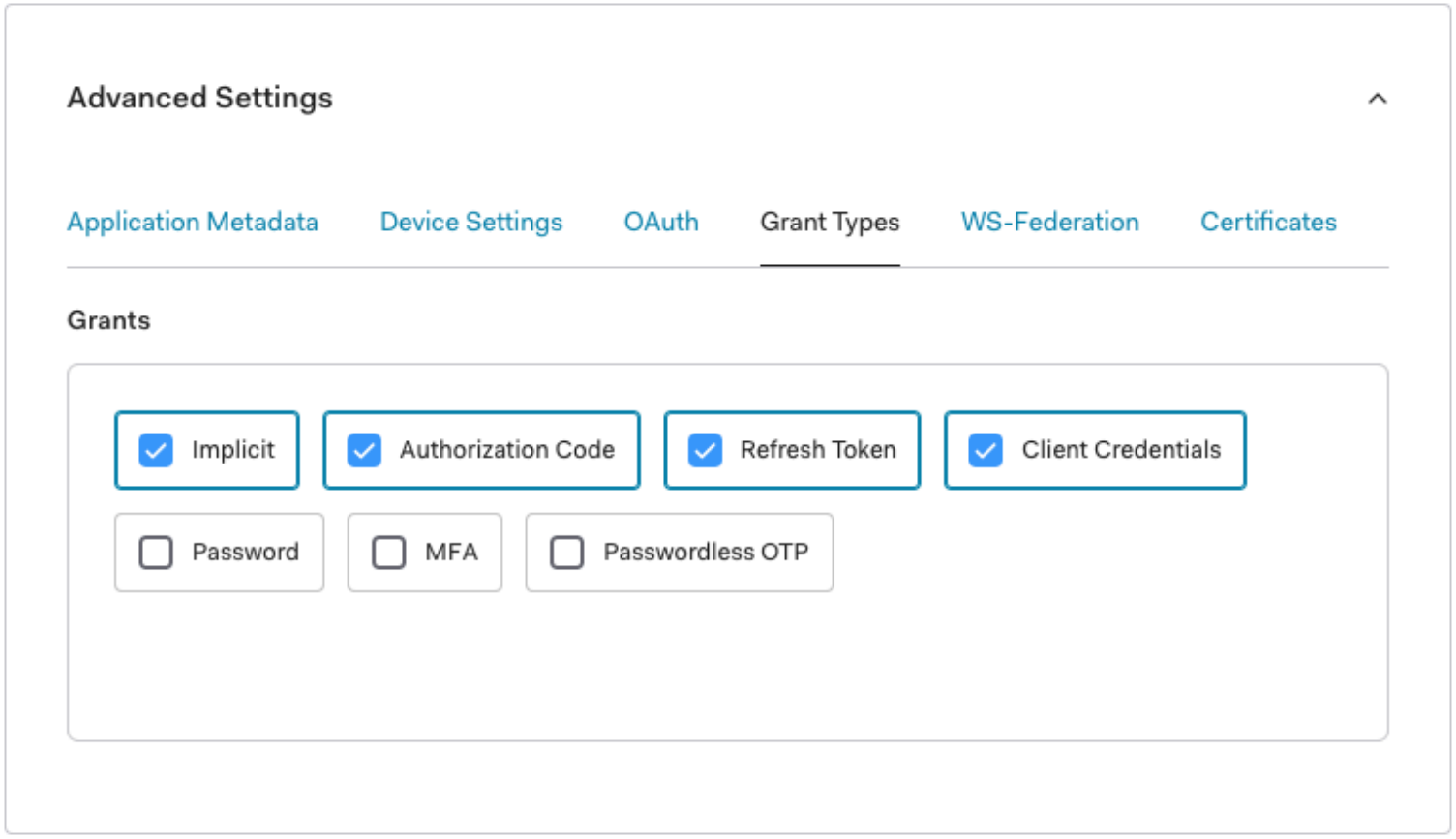

AuthO Settings

| AuthO Setting | Description |
|---|---|
| Name | Give the application a Bitwarden-specific name. |
| Domain | Take note of this value. You will need it during a later step. |
| Application Type | Select **Regular Web Application**. |
| Token Endpoint Authentication Method | Select **Client Secret (Post)**, which will map to a **Binding Type** attribute you will configure later. |

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

### Grant Types

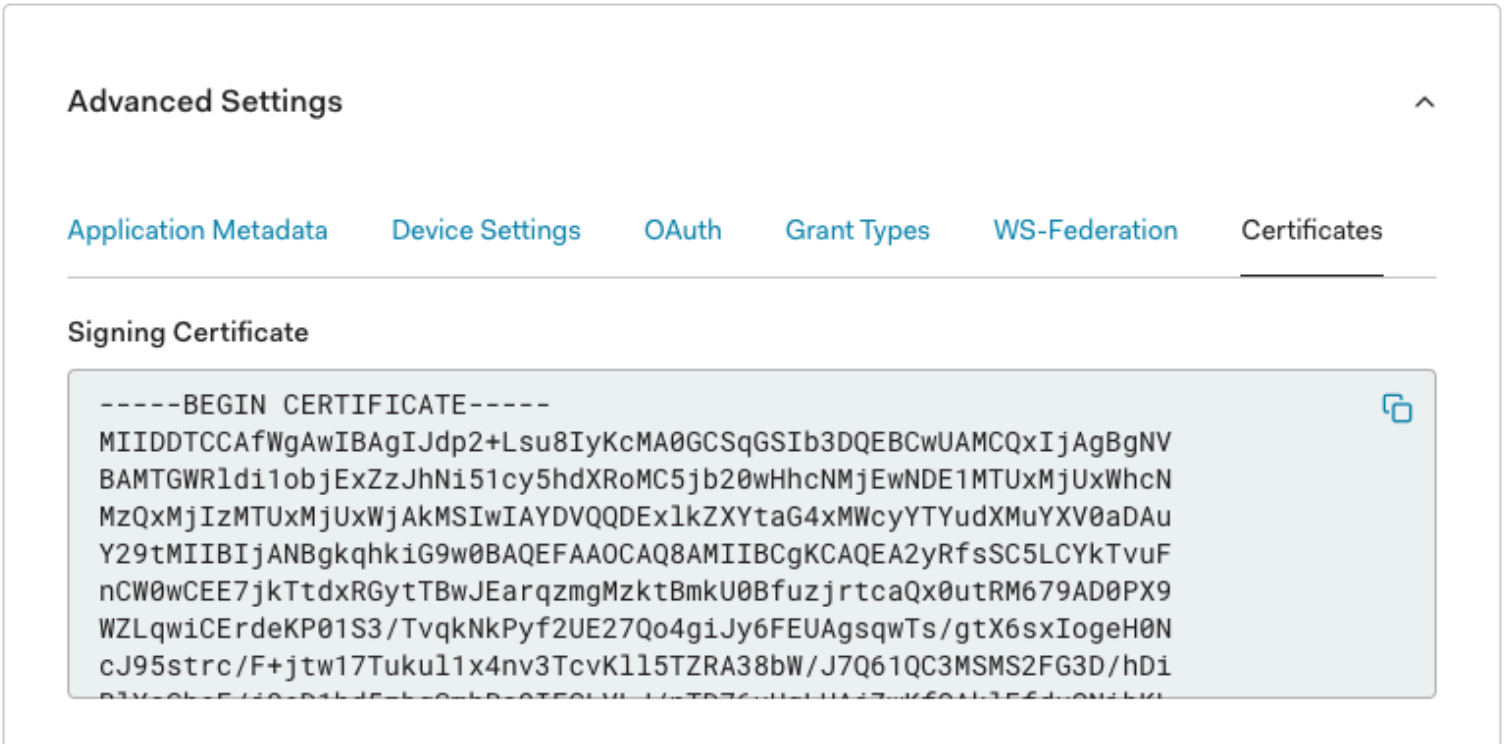
In the **Advanced Settings → Grant Types** section, ensure that the following Grant Types are selected (they may be pre-selected):




Application Grant Types

### Certificates

In the **Advanced Settings → 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.

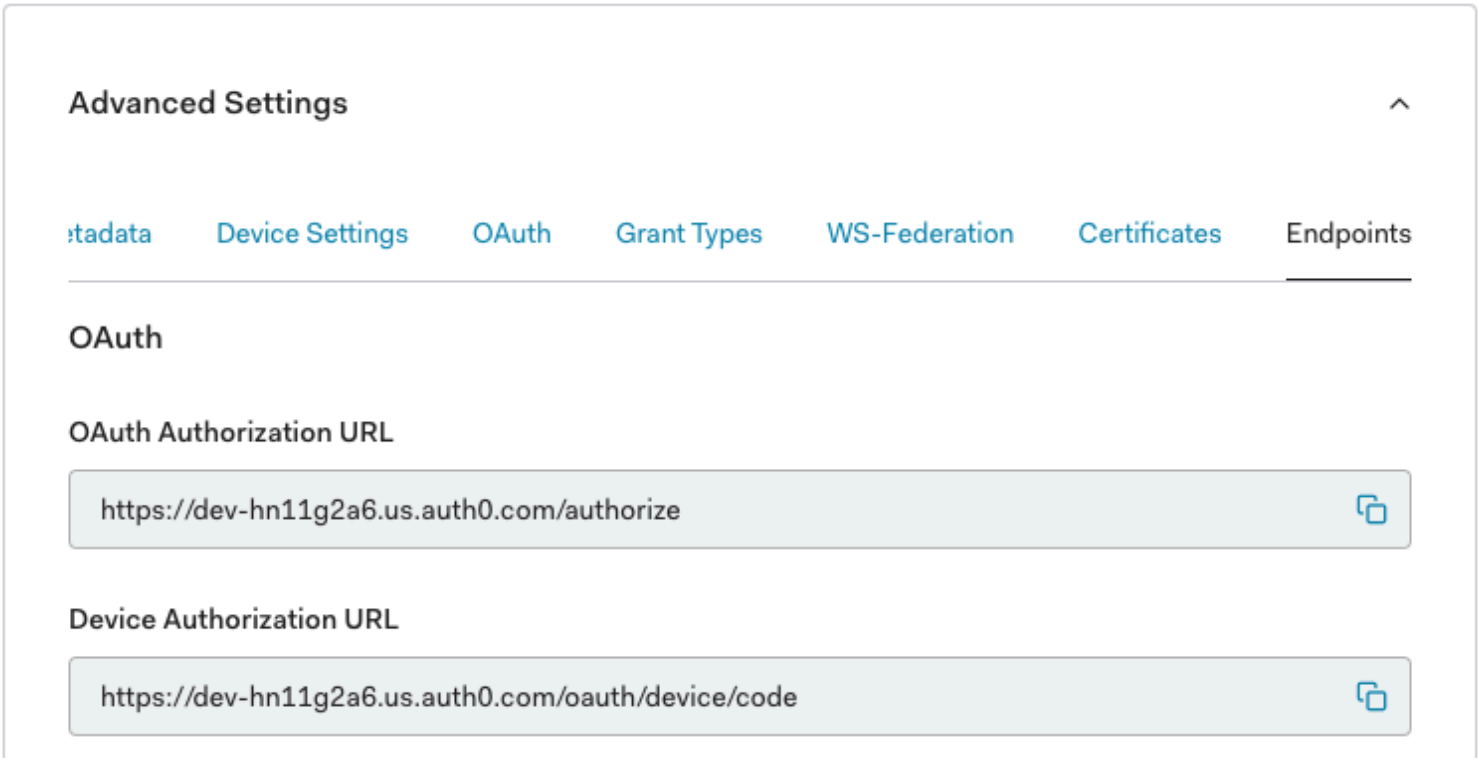



Auth0 Certificate

### Endpoints

You don't need to edit anything in the **Advanced Settings → 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 (→).




Auth0 Endpoints

## Configure Auth0 actions

Create actions to customize the logic that Auth0 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 → Library** and select **Create Action → 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:

```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 → 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:

| Key | Description |
|---|---|
| `signatureAlgorithm` | Algorithm Auth0 will use to sign the SAML assertion or response. This value should be set to `rsa-sha256`. You must also set:<br><br>-Set `digestAlgorithm` to `sha256`.<br>-Set (in Bitwarden) the **Minimum Incoming Signing Algorithm** to `rsa-sha256`. |
| `digestAlgorithm` | Algorithm used to calculate digest of SAML assertion or response. Set to `sha-256`. |
| `signResponse` | By default, Auth0 will sign only the SAML assertion. Set this to `true` to sign the SAML response instead of the assertion. |

| Key | Description |
| --- | --- |
| `nameIdentifierFormat` | 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 Auth0 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 Auth0 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 Auth0 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, Auth0 will not require requests to be signed. |

| Field | Description |
|---|---|
| Minimum Incoming Signing Algorithm | The minimum signing algorithm Bitwarden will accept in SAML responses. Select `rsa-sha256` from the dropdown unless you have configured a custom signing rule. |
| Want Assertions Signed | Whether Bitwarden wants SAML assertions signed. By default, Auth0 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 Auth0 Portal to retrieve application values:

| Field | Description |
|---|---|
| Entity ID | Enter the **Domain** value of your Auth0 application (see here), prefixed by `urn:`, for example `urn:bw-help.us.auth0.com`. This field is case sensitive. |
| Binding Type | Select **HTTP POST** to match the Token Endpoint Authentication Method value specified in your Auth0 application. |
| Single Sign On Service URL | Enter the **SAML Protocol URL** (see Endpoints) of your Auth0 application. For example, `https://bw-help.us.auth0.com/samlp/HcpxD63h7Qzl420u8qachPWoZEG0Hho2`. |
| Single Log Out Service URL | Login with SSO currently **does not** 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, removing<br>`-----BEGIN CERTIFICATE-----` |

| Field | Description |
| --- | --- |
| | and<br>`-----END CERTIFICATE-----`<br>The certificate value is case sensitive, extra spaces, carriage returns, and other extraneous characters **will cause certification validation to fail**. |
| Outbound Signing Algorithm | Select `rsa-sha256` unless you've configured a custom signing rule. |
| Disable Outbound Logout Requests | Login with SSO currently **does not** support SLO. This option is planned for future development. |
| Want Authentication Requests Signed | Whether Auth0 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.

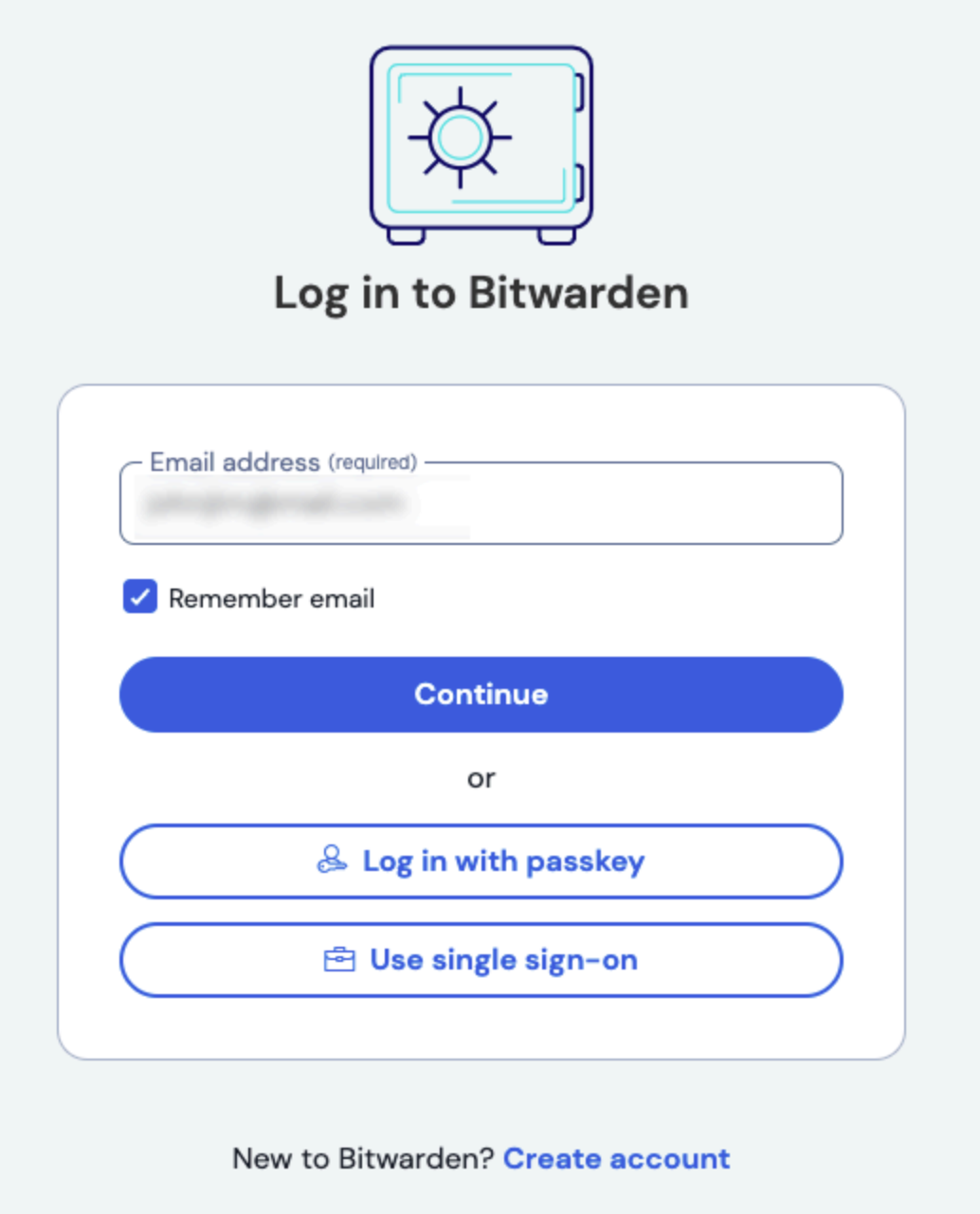
When you are done with the identity provider configuration, **Save** your work.

**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.

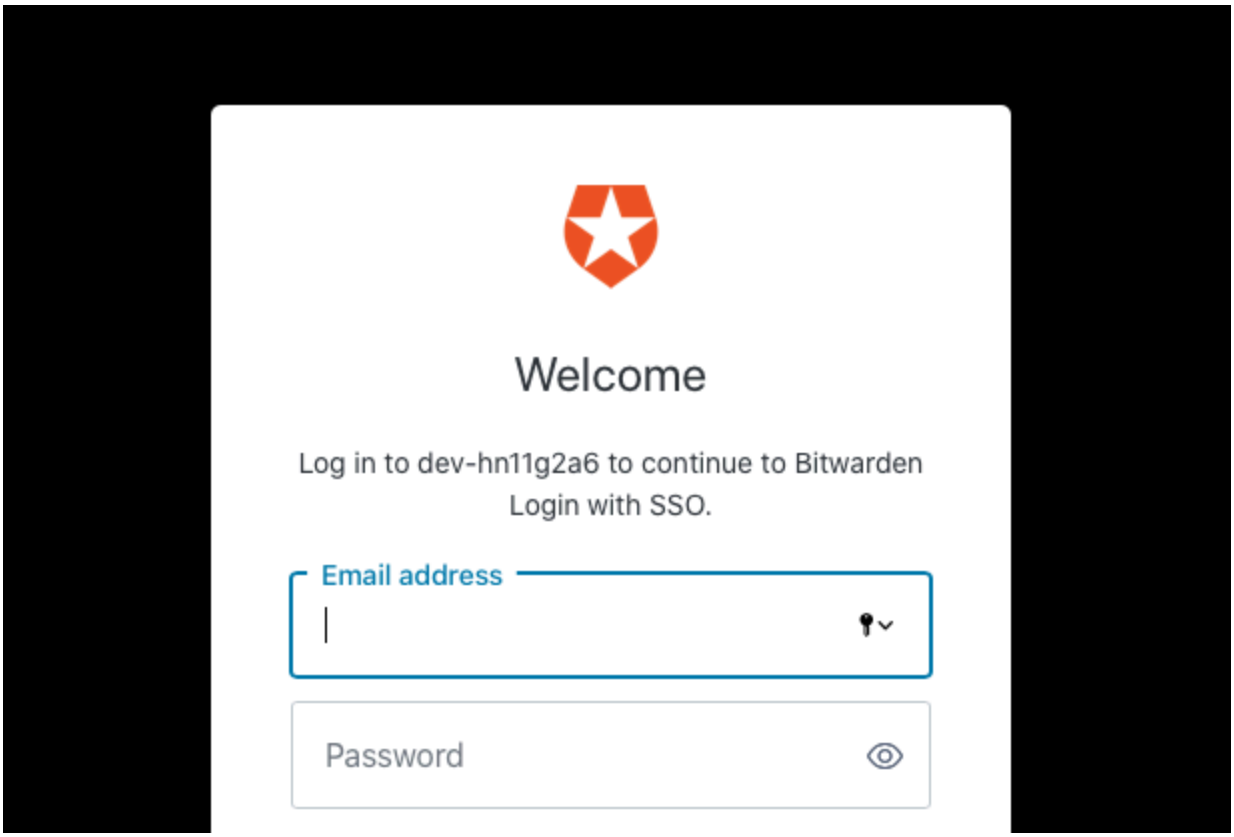
## Test the configuration

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 options screen

Enter the configured organization identifier and select **Log In**. If your implementation is successfully configured, you will be redirected to the Auth0 login screen:




Auth0 Login

After you authenticate with your Auth0 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.