

ADMIN CONSOLE > LOGGA IN MED SSO >

AWS SAML Implementation

View in the help center:
<https://bitwarden.com/help/saml-aws/>

AWS SAML Implementation

This article contains **AWS IAM Identity Center-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 AWS Console. As you proceed, we recommend having both readily available and completing steps in the order they are documented.



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

[Download Sample](#)

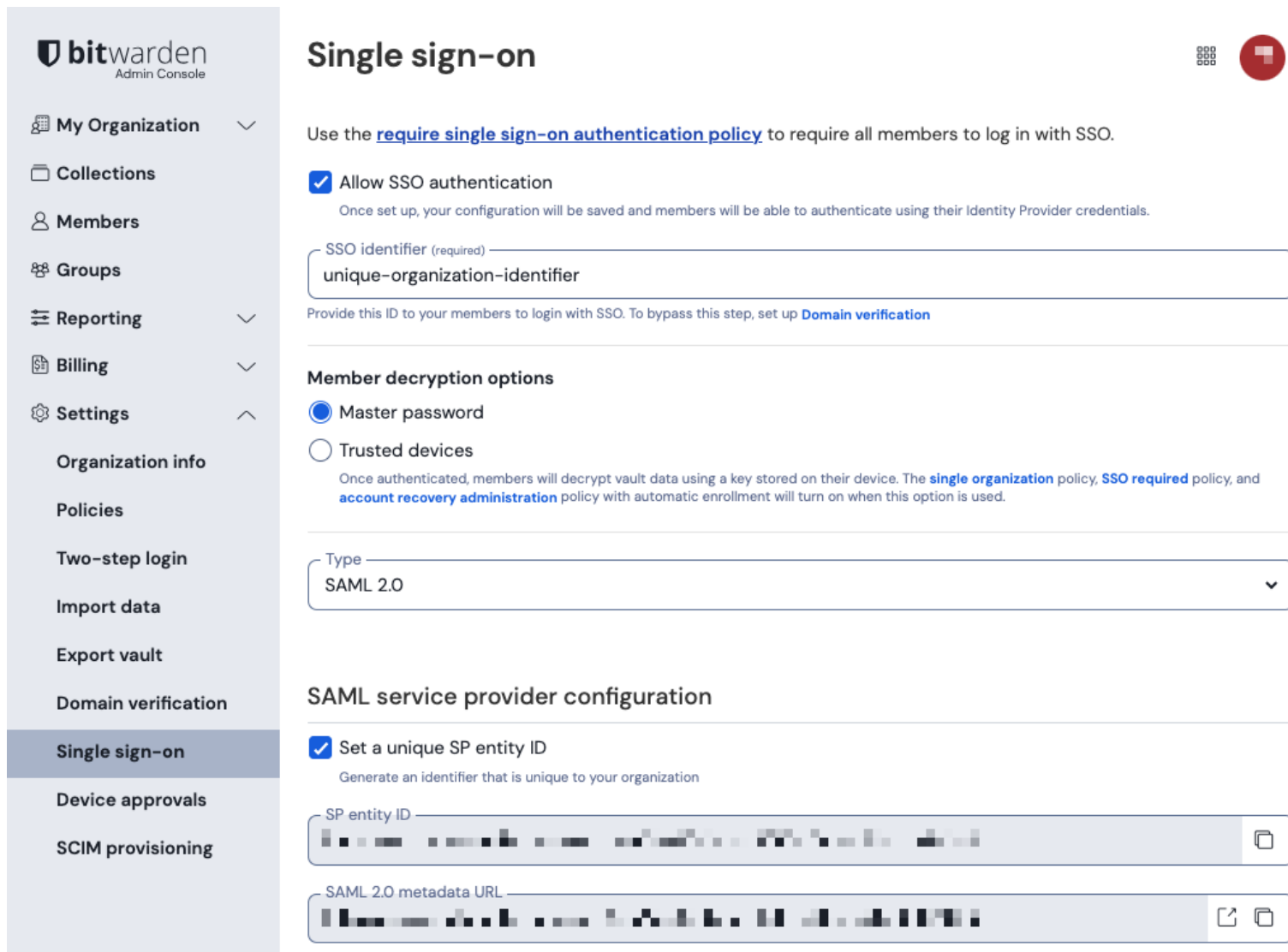
Open SSO in the web app

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

The screenshot displays the Bitwarden web app interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, and Settings. A red box highlights the bottom section of the sidebar, which includes Password Manager, Secrets Manager, Admin Console, and Toggle Width. A red arrow points to the Admin Console option. The main content area is titled 'All vaults' and features a 'FILTERS' sidebar on the left with a search bar and categories like 'All vaults', 'All items', 'Folders', 'Collections', and 'Trash'. The main list shows vaults such as 'Company Credit Card', 'Personal Login', 'Secure Note', and 'Shared Login'. In the top right corner, there is a 'New' button, a grid icon, and a circular 'Product switcher' button labeled 'BW'.

Product switcher

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



The screenshot shows the Bitwarden Admin Console interface. On the left is a sidebar with navigation links: My Organization, Collections, Members, Groups, Reporting, Billing, Settings (expanded), Organization info, Policies, Two-step login, Import data, Export vault, Domain verification, Single sign-on (selected), Device approvals, and SCIM provisioning. The main content area is titled 'Single sign-on' and includes a QR code icon and a red arrow icon. The instructions state: 'Use the [require single sign-on authentication policy](#) to require all members to log in with SSO.' There is a checked checkbox for 'Allow SSO authentication' with a note: 'Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.' Below this is a text field for 'SSO identifier (required)' containing 'unique-organization-identifier'. A note says: 'Provide this ID to your members to login with SSO. To bypass this step, set up [Domain verification](#)'.

The 'Member decryption options' section has two radio buttons: 'Master password' (selected) and 'Trusted devices'. A note for 'Trusted devices' states: '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.'

A dropdown menu for 'Type' is set to 'SAML 2.0'. Below this is the 'SAML service provider configuration' section, which has a checked checkbox for 'Set a unique SP entity ID' with a note: 'Generate an identifier that is unique to your organization'. There are two text fields: 'SP entity ID' containing a long alphanumeric string and 'SAML 2.0 metadata URL' containing a long alphanumeric string. Both fields have copy icons on the right.

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.

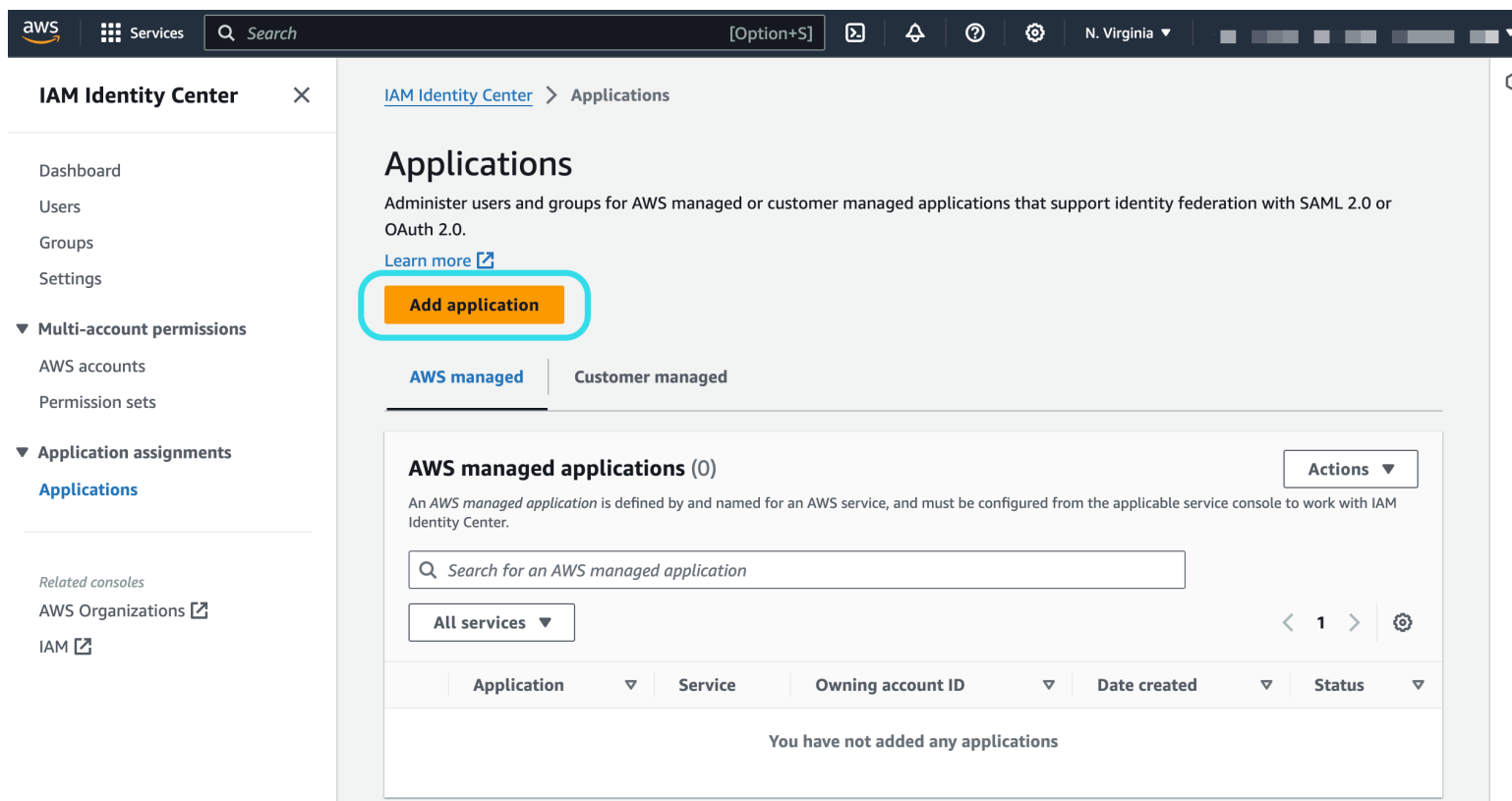
You can turn off the **Set a unique SP entity ID** option at this stage if you wish. Doing so will remove your organization ID from your SP entity ID value, however in almost all cases it is recommended to leave this option on.



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

Create an application

In the AWS Console, navigate to **IAM Identity Center**, select **Application assignments** → **Applications** from the navigation, and select the **Add application** button:



IAM Identity Center Applications

Administer users and groups for AWS managed or customer managed applications that support identity federation with SAML 2.0 or OAuth 2.0.

[Learn more](#)

Add application

AWS managed | Customer managed

AWS managed applications (0) Actions

An *AWS managed application* is defined by and named for an AWS service, and must be configured from the applicable service console to work with IAM Identity Center.

Search for an AWS managed application

All services

Application	Service	Owning account ID	Date created	Status
You have not added any applications				

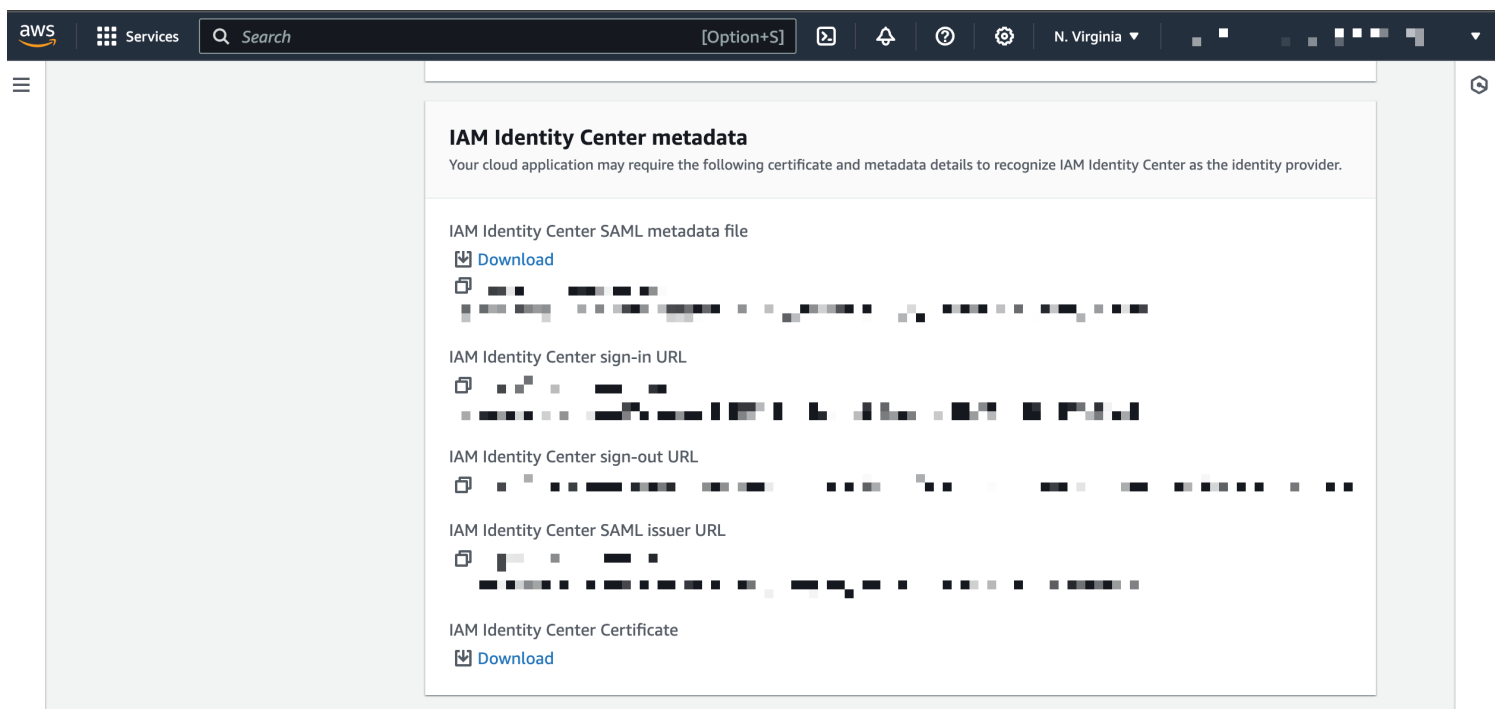
Add a new application

On the Select application type screen, select **I have an application I want to set up** and **SAML 2.0**.

Configure application

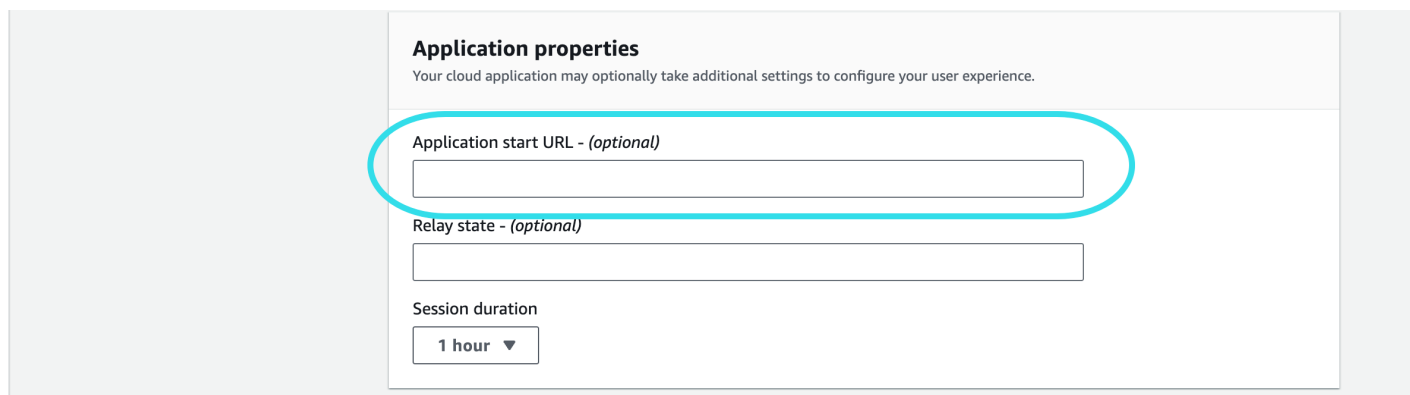
On the Configure application screen:

1. Give the application a unique, Bitwarden-specific **Display name**.
2. Copy the **IAM Identity Center sign-in URL** and **IAM Identity Center issuer URL**, and download the **IAM Identity Center Certificate**:



IAM Identity Center metadata

- In the **Application start URL** field, specify the login URL from which users will access Bitwarden. For cloud-hosted customers, this is always <https://vault.bitwarden.com/#/sso> or <https://vault.bitwarden.eu/#/sso>. For self-hosted instances, this is determined by your configured server URL, for example <https://your.domain/#/sso>:



IAM Identity Center application properties

- In the Application metadata section, select the option to **Manually type your metadata values**:

Application metadata

IAM Identity Center requires specific metadata about your cloud application before it can trust this application. You can type this metadata manually or upload a metadata exchange file.

Manually type your metadata values

Upload application SAML metadata file

Application ACS URL

Application SAML audience

Enter metadata values

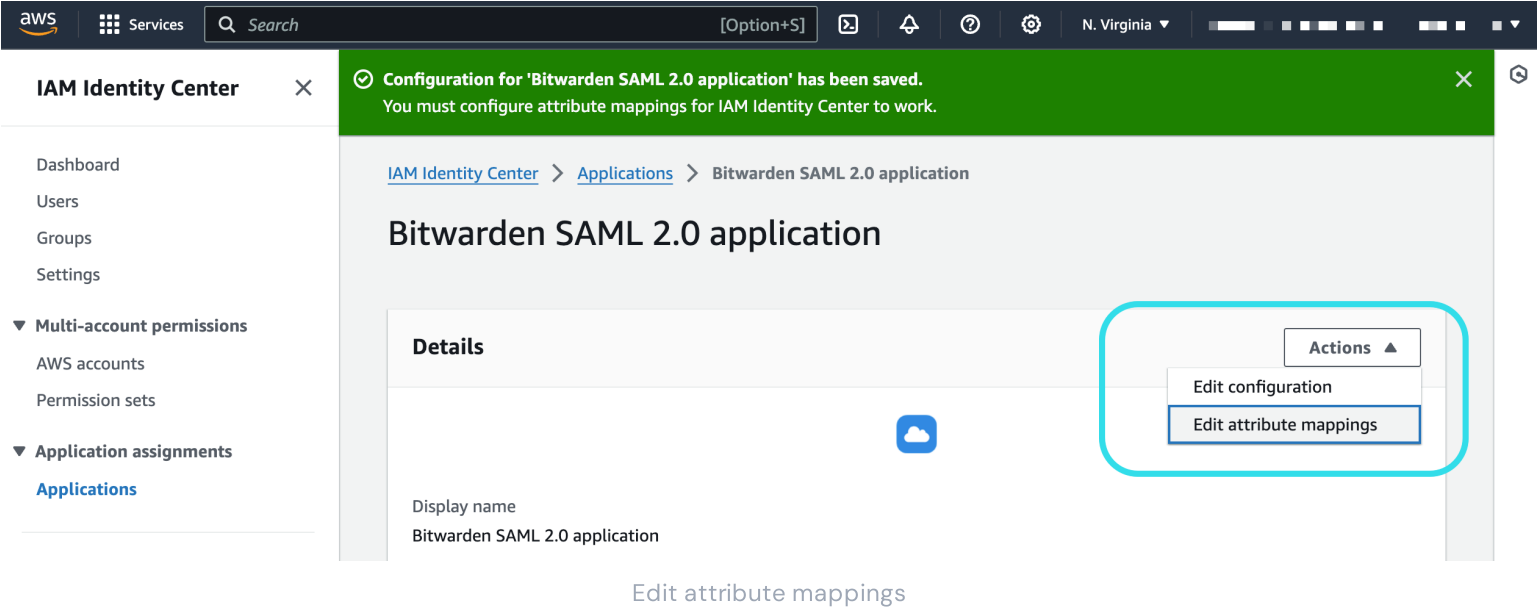
In that section, configure the following fields:

Field	Description
Application ACS URL	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.
Application SAML audience	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.

When you are finished, select **Submit**.

Attribute mappings

Once the application is created, open it again from the **Application assignments → Applications** screen. Use the **Actions** dropdown to **Edit attribute mappings**:

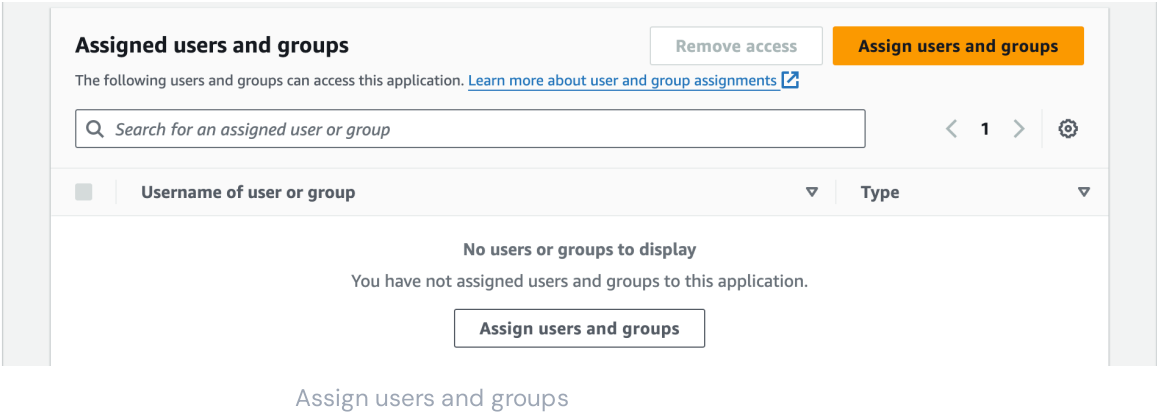


Configure the following mappings and **Save changes**:

User attribute in the application	Maps to this string value or user attribute in IAM Identity Center	Format
Subject	<code>\${user:email}</code>	emailAddress
email	<code>\${user:email}</code>	Unspecified

Assigned users

From your application, scroll down to the Assigned users and groups section and select the **Assign users and groups** button:



Assign users and groups to the application.

Back to the web app

At this point, you have configured everything you need within the context of the AWS Console. 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

Service provider configuration should already be complete, however you may choose to edit any of the following fields:

Field	Description
Name ID Format	Set to Email Address .
Outbound Signing Algorithm	The algorithm Bitwarden will use to sign SAML requests.
Signing Behavior	Whether/when SAML requests will be signed.
Minimum Incoming Signing Algorithm	By default, IAM Identity Center will sign with SHA-256. Unless you have changed this, select sha256 from the dropdown.
Want Assertions Signed	Whether Bitwarden expects SAML assertions to be signed.
Validate Certificates	Check this box when sing 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 AWS Console to retrieve application values:

Field	Description
Entity ID	Enter the IAM Identity Center issuer URL , retrieved from the IAM Identity Center metadata section for your application in the AWS Console. This field is case sensitive.
Binding Type	Set to HTTP POST or Redirect .
Single Sign On Service URL	Enter the IAM Identity Center sign-in URL , retrieved from the IAM Identity Center metadata section for your application in the AWS Console.
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 with the IAM Identity Center sign-out URL retrieved from the IAM Identity Center metadata section for your application in the AWS Console.
X509 Public Certificate	Paste the downloaded certificate, removing: -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- The certificate value is case sensitive, extra spaces, carriage returns, and other extraneous characters will cause certificate validation to fail.
Outbound Signing Algorithm	By default, IAM Identity Center will sign with sha256 . Unless you have changed this, select sha256 from the dropdown.
Disable Outbound Logout Requests	Login with SSO currently does not support SLO. This option is planned for future development.
Want Authentication Requests Signed	Whether IAM Identity Center 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 to Bitwarden

Email address (required)

☒ Remember email

Continue

or

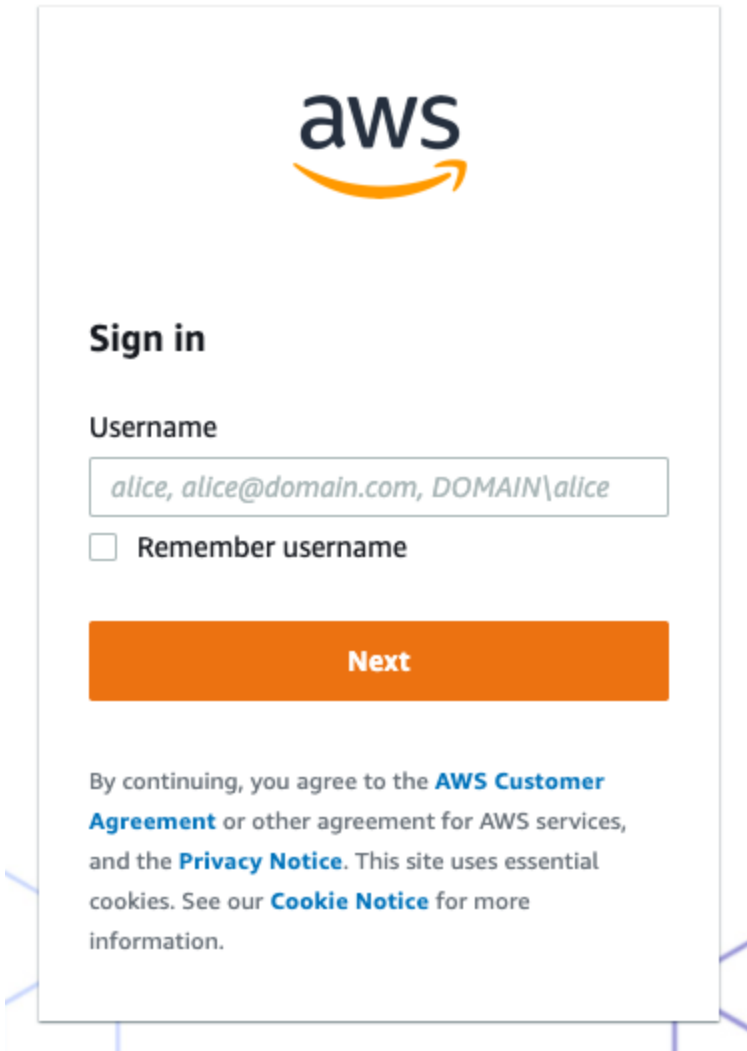
 Log in with passkey

 Use single sign-on

New 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 IAM Identity Center login screen:



AWS login screen

After you authenticate with your IAM Identity Center 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.