

Setting Up SAML SSO on Azure AD

Prerequisites

To get started you need the following items:

- An Azure AD subscription
- UpCodes SAML SSO enabled subscription

Adding UpCodes

To configure the integration of UpCodes into Azure AD, you need to add UpCodes from the gallery to your list of managed SaaS apps.

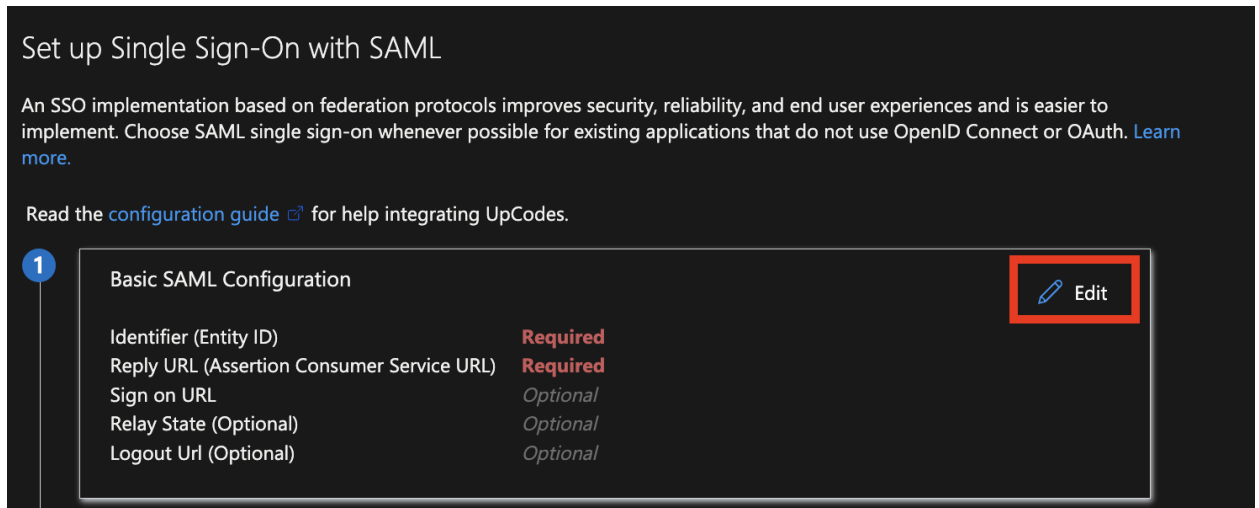
1. Sign in to the Azure portal using either a work or school account, or a personal Microsoft account.
2. On the left navigation pane, select the **Azure Active Directory** service.
3. Navigate to **Enterprise Applications** and then select **All Applications**.
4. To add a new application, select **New application**.
5. Select **Create your own application**.
6. Under “What’s the name of your app?” input **UpCodes**.
7. Under “What are you looking to do with your application?” select **Integrate any other application you don’t find in the gallery (Non-gallery)**. If a list of recommended gallery applications are shown, do not select any.
8. Select **Create** in the bottom of the pane. Wait a few seconds while the app is added to your tenant.

Configure Azure AD SSO

Follow these steps to enable Azure AD SSO in the Azure portal.

1. In the Azure portal, on the **UpCodes** application integration page, find the **Manage** section and select **single sign-on**.
2. On the **Select a single sign-on method** page, select **SAML**.

3. On the **Set up single sign-on with SAML** page, click the edit/pen icon for **Basic SAML Configuration** to edit the settings.




Set up Single Sign-On with SAML

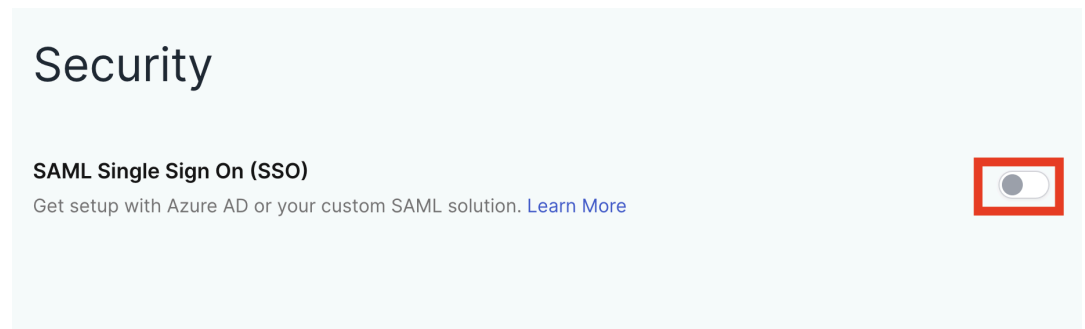
An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating UpCodes.

1

Basic SAML Configuration		 Edit
Identifier (Entity ID)	Required	
Reply URL (Assertion Consumer Service URL)	Required	
Sign on URL	Optional	
Relay State (Optional)	Optional	
Logout Url (Optional)	Optional	

4. On the **Basic SAML Configuration** section, enter the values for the following fields:
 1. In the **Identifier** text box, enter the URL that you can obtain from your UpCodes account by going to UpCodes in a different browser window:
 1. Sign in to your UpCodes account as an admin, then navigate to <https://up.codes/security>.
 2. Enable **SAML Single Sign On (SSO)** by selecting the toggle on the right.



Security

SAML Single Sign On (SSO)

Get setup with Azure AD or your custom SAML solution. [Learn More](#)

☒

3. Under the **Step 1** section, copy **Entity ID** then paste in into the **Identifier** text box. Keep the window open for the next step.

SAML Credential Details

Step 1

To start your configuration copy the following URLs and finish your setup on the Azure side.

Assertion Consumer Service (ACS) URL

Copy URL

Entity ID

Copy URL

Step 2

Once done, finish your setup by filling out the details below

SAML/SSO Policy:

☒ Optional (Recommended to test the configuration first)
 ☐ Required for all members

Upload SAML Metadata XML:

Click to upload or drag and drop

Save Details

2. In the **Reply URL** text box, enter the URL that you can obtain from your UpCodes account:
 1. Under the **Step 1** section, copy **Assertion Consumer Service (ACS) URL** then paste it into the **Reply URL** textbox.
5. The UpCodes application expects the SAML assertions to be in the default format. Ensure they match the following screenshot.

2

Attributes & Claims		Edit
givenname	user.givenname	
surname	user.surname	
emailaddress	user.mail	
name	user.userprincipalname	
Unique User Identifier	user.userprincipalname	


6. On the **Set up single sign-on with SAML** page, in the **SAML Certificate** section, find **Federation Metadata XML** and select **Download** to download the certificate and save it on your computer.

SAML Certificates

Token signing certificate

Status

Active

 Edit

Thumbprint

Expiration

Notification Email

App Federation Metadata Url

Certificate (Base64)

[Download](#)

Certificate (Raw)

[Download](#)


Federation Metadata XML

[Download](#)

Verification certificates (optional)

Required

No

 Edit

Active

0

Expired

0


7. On the **Set up single sign-on with SAML** page, in the **SAML Certificate** section, select **Edit** in the **Token signing certificate** section.

SAML Certificates

Token signing certificate

Status

Active

 Edit

Thumbprint

Expiration

Notification Email

App Federation Metadata Url

Certificate (Base64)

[Download](#)

Certificate (Raw)

[Download](#)


Federation Metadata XML

[Download](#)

Verification certificates (optional)

Required

No

 Edit

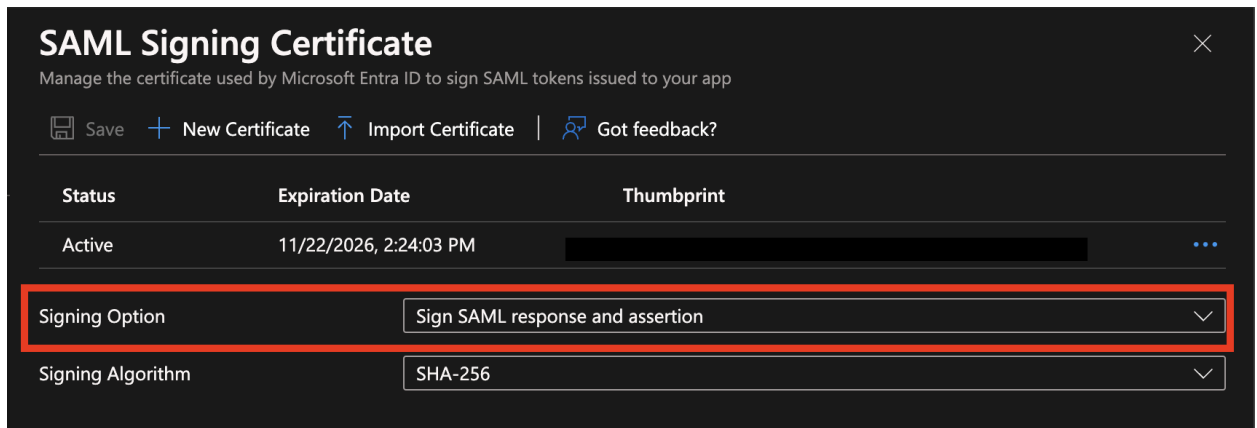
Active

0

Expired

0

- Find **Signing Option**, select **Sign SAML response and assertion**, then click **save**.



SAML Signing Certificate

Manage the certificate used by Microsoft Entra ID to sign SAML tokens issued to your app

Save + New Certificate ↑ Import Certificate | Got feedback?

Status	Expiration Date	Thumbprint
Active	11/22/2026, 2:24:03 PM	[Redacted]

Signing Option: Sign SAML response and assertion

Signing Algorithm: SHA-256

Create an Azure AD test user

In this section, you'll create a test user in the Azure portal called B.Simon.

- From the left pane in the Azure portal, select **Azure Active Directory**, select **Users**, and then select **All users**.
- Select **New user** at the top of the screen.
- In the **User** properties, follow these steps:
 - In the **Name** field, enter B.Simon.
 - In the **User name** field, enter the username@companydomain.extension. For example, B.Simon@contoso.com.
 - Select the **Show password** check box, and then write down the value that's displayed in the **Password** box.
 - Click **Create**.

Assign the Azure AD test user

In this section, you'll enable B.Simon to use Azure single sign-on by granting access to Slack.

- In the Azure portal, select **Enterprise Applications**, and then select **All applications**.
- In the applications list, select **UpCodes**.
- In the app's overview page, find the **Manage** section and select **Users and groups**.
- Select **Add user**, then select **Users and groups** in the **Add Assignment** dialog.
- In the **Users and groups** dialog, select **B.Simon** from the Users list, then click the **Select** button at the bottom of the screen.
- If you are expecting a role to be assigned to the users, you can select it from the **Select a role** dropdown. If no role has been set up for this app, you see "Default Access" role selected.
- In the **Add Assignment** dialog, click the **Assign** button.

Configure UpCodes SSO

1. Sign in to your UpCodes account as an admin, then navigate to <https://up.codes/security>.
2. Locate **Step 2**, in **Upload SAML Metadata XML** upload the **Federation Metadata XML** file, which you have downloaded from Azure portal.

SAML Credential Details

Step 1

To start your configuration copy the following URLs and finish your setup on the Azure side.

Assertion Consumer Service (ACS) URL

Copy URL

Entity ID

Copy URL

Step 2

Once done, finish your setup by filling out the details below

SAML/SSO Policy:

☒ Optional (Recommended to test the configuration first)

☐ Required for all members

Upload SAML Metadata XML:

Click to upload or drag and drop

Save Details

3. Select **Save Details**.

Create UpCodes test user

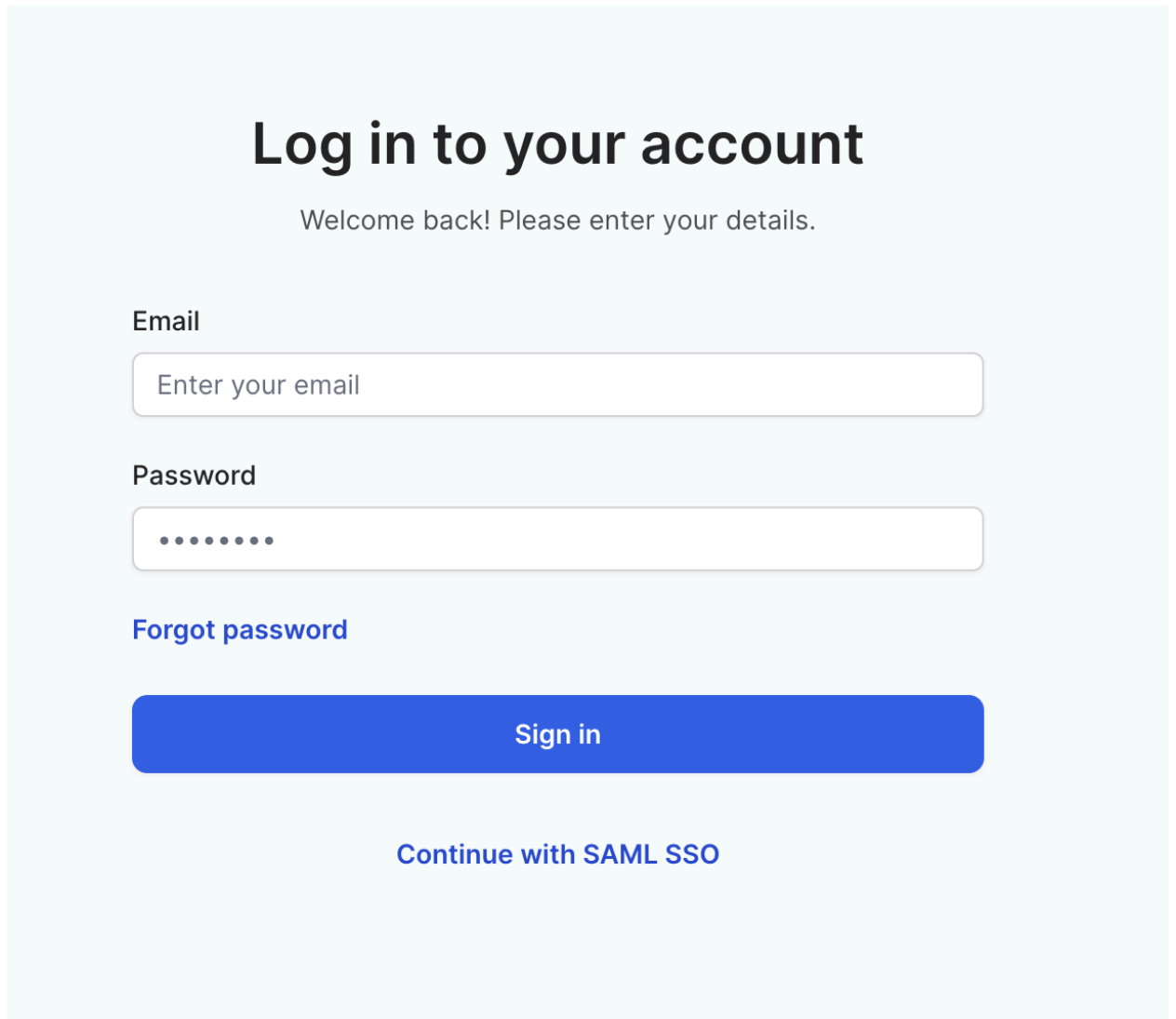
In this section, a user called B.Simon is created in UpCodes. UpCodes supports just-in-time user provisioning, which is enabled by default. There is no action item for you in this section. If a user doesn't already exist in UpCodes, a new one is created after authentication.

Test SSO

In this section, you test your Azure AD single sign-on configuration with the following options.

SP initiated:

1. Go to the UpCodes login page and select **Continue with SAML SSO**.

A mockup of the UpCodes login page. It features a light blue background. At the top, the text "Log in to your account" is displayed in a large, bold, black font. Below this, a smaller line of text says "Welcome back! Please enter your details." The form includes an "Email" label above a white input field with the placeholder text "Enter your email". Below the email field is a "Password" label above a white input field with a masked password ".....". To the left of the password field is a blue link that says "Forgot password". At the bottom of the form is a large blue button with the text "Sign in" in white. Below the button is a blue link that says "Continue with SAML SSO".

Log in to your account

Welcome back! Please enter your details.

Email

Enter your email

Password

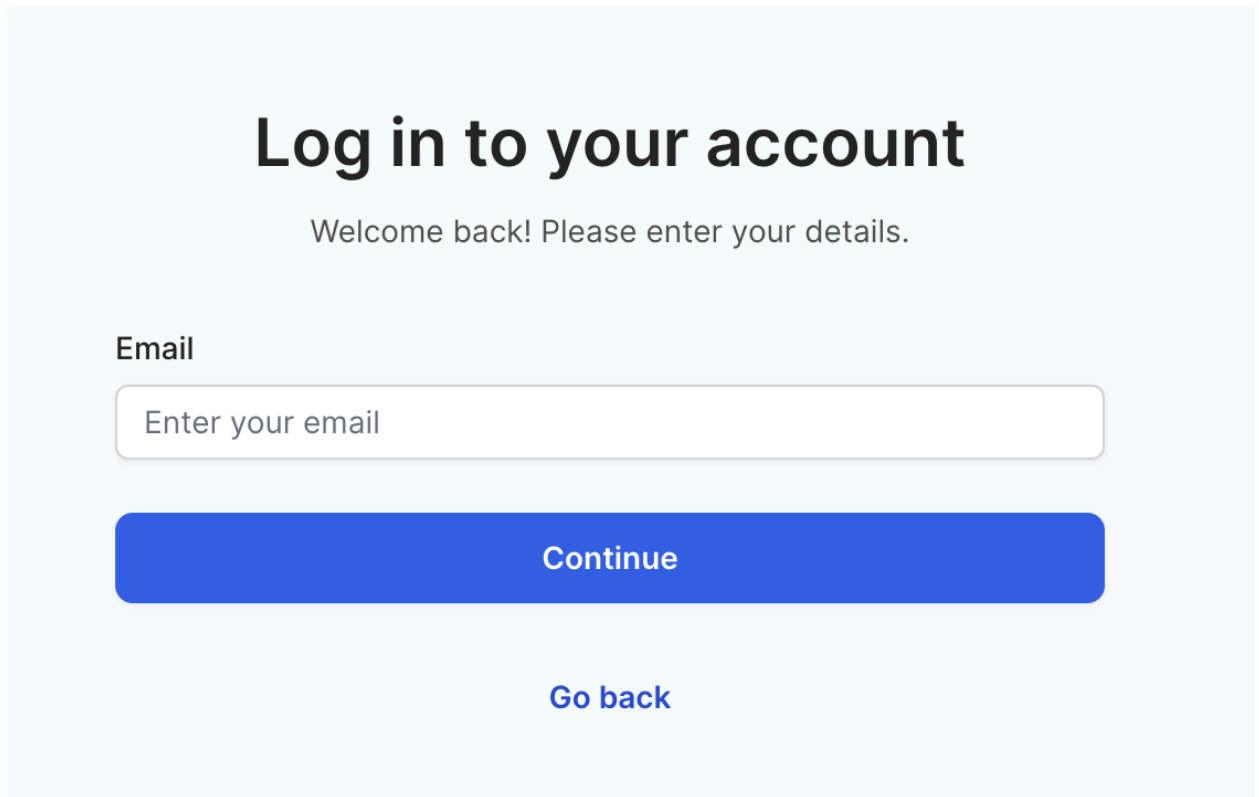
.....

[Forgot password](#)

Sign in

[Continue with SAML SSO](#)

2. Input your test user's email address, then select **Continue**.



Log in to your account

Welcome back! Please enter your details.

Email

Continue

[Go back](#)

IDP initiated:

Click on **Test this application** in Azure portal and you should be automatically signed in to UpCodes.