

Create an IAM Identity Center application

1. Login to the AWS console and open [IAM Identity Center](#).
2. Navigate to **Applications** → **Add application**.
3. Select **I have an application I want to setup** and chose **SAML 2.0**.
4. Enter the following details
 - **Display name:** `Sandbox Studio` (or your preferred name)
 - **Description:** e.g. `Sandbox Studio allows users to access AWS sandbox accounts`
 - Leave **Application start URL** and **Relay state** blank.
 - **Application Metadata**
 - Select **Manually type your metadata values**
 - **Application ACS URL** will be `https://<your-app-url>/api/auth/login/callback`
(for now, use the **CloudFrontDistributionUrl**; if you later add a custom domain, come back and update this)
 - **Audience (Entity ID):** `SandboxStudio`
 - **Submit.**
5. From the list of applications, choose the SAML application you just set up.
6. Click **Actions** → **Edit attribute mappings**.
7. Enter the following attributes:

User attribute in the application	Maps to this value...	Format
Subject	<code>\${user:email}</code>	emailAddress
ID	<code>\${user:AD_GUID}</code>	unspecified

8. **Save changes.**
9. On the application, page click **Assign users or groups**.
10. Assign the **three groups** created by the `SandboxStudio-IDC` stack (Admin / Manager / User) to this application.
11. **Done.**

You have now successfully set up a custom IAM Identity Center Application.

Extract application details

Before proceeding to the next step, you will need to extract the following information which will be used in subsequent steps.

1. Click **Actions** → **Edit configuration**.

2. Take note of:

- **IAM Identity Center sign-in URL**
- **IAM Identity Center sign-out URL**
- Download the **IAM Identity Center Certificate**

3. Also take note of the:

1. **Web App URL** - this will be the same URL as the **Application ACS URL** in the previous step **without** the `/api/auth/login/callback` part.
2. **Audience (Entity ID)** from the previous step.
3. **AWS Access Portal URL** - this is always
`https://<IdentityStoreId>.awsapps.com/start`

Keep these details handy as you will need them in one of the upcoming steps.

Revision #7

Created 2025-07-14 21:16:57 UTC

Updated 2025-08-27 08:11:33 UTC by Andy