IAM Identity Center Integration

The TEAM application needs to be onboarded as a SAML 2.0 application on AWS IAM Identity Center before it can be fully accessed.

SAML Configuration Parameters

The following parameters will be required for configuring the TEAM application as a SAML app in AWS Identity Center:

- **applicationStartURL** - AWS IAM Identity Center application properties configuration settings
- **applicationACSURL** - AWS IAM Identity Center application metadata configuration settings
- **applicationSAMLAudience** - URN for the AWS Cognito user pool ID for the TEAM application

The **integration.sh** bash script in the **deployment** folder can be used to obtain the SAML configuration parameters:

Execute the following command in the root directory to deploy the **integration.sh** script:

```
cd deployment
./integration.sh
```

The result should be similar to the below:

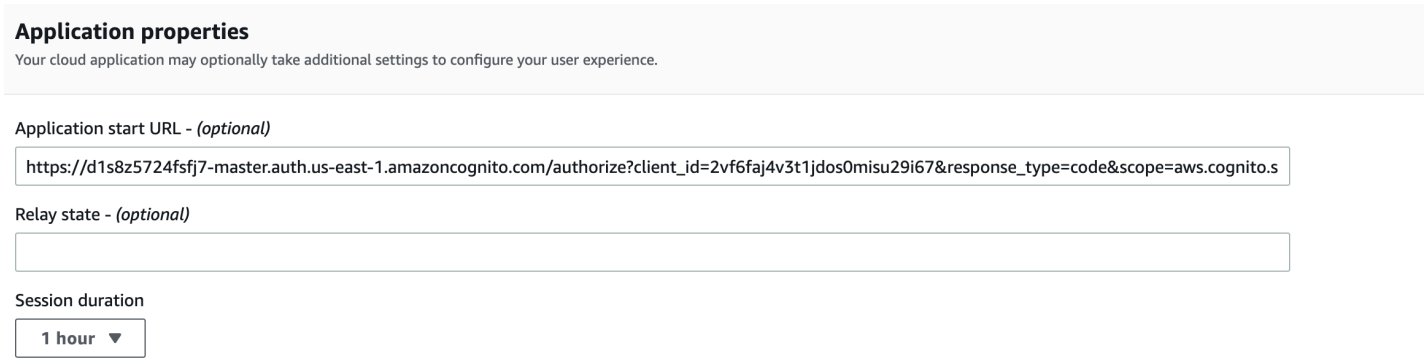
```
applicationStartURL: https://d1s8z5724fsfj7-main.auth.amazoncognito.com/authorize?client_id=2vf61
applicationACSURL: https://d1s8z5724fsfj7-main.auth.amazoncognito.com/saml2/idpresponse
applicationSAMLAudience: urn:amazon:cognito:sp:us-east-1_GXaUCfcno
```

Configure IAM Identity Center SAML Integration

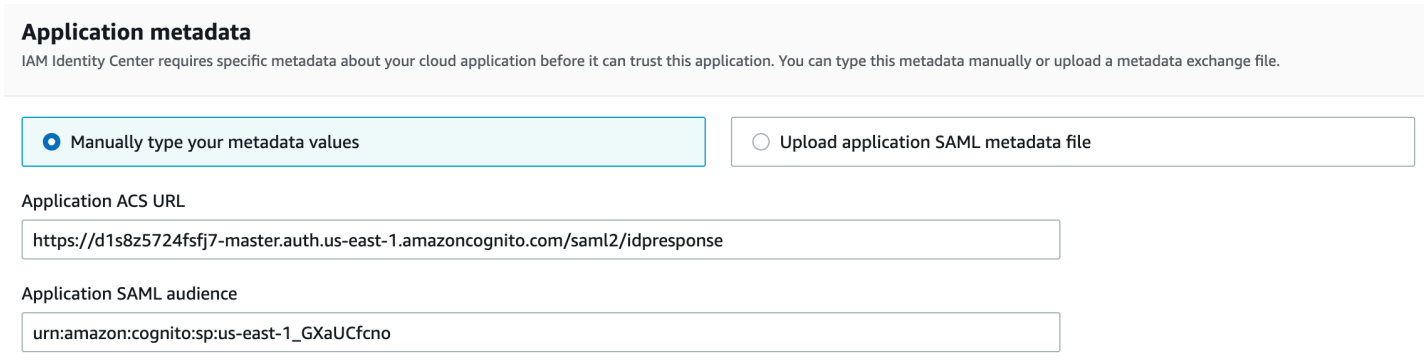
Follow the steps below to integrate the TEAM application with AWS IAM Identity Center as a SAML application:

In AWS IAM Identity Center console > **Application assignment** > **Applications** > **Add application**

- Select ***Add custom SAML 2.0 Application*** and click on ***Next***
- Type **TEAM IDC APP** as display name and add a description for the TEAM application under **Configure application** section.
- Copy and save the URL of **AWS IAM Identity Center SAML metadata file URL**. It would be used later for configuring Cognito User pool.
- Enter the value of ***applicationStartURL*** parameter in ***Application start URL*** under the ***Application properties*** section:



- In the **Application Metadata** section select ***Manually type your metadata values***.
- Enter the value of ***applicationACSURL*** parameter in **Application ACS URL**.
- Enter the value of ***applicationSAMLAudience*** parameter in **Application SAML audience**.

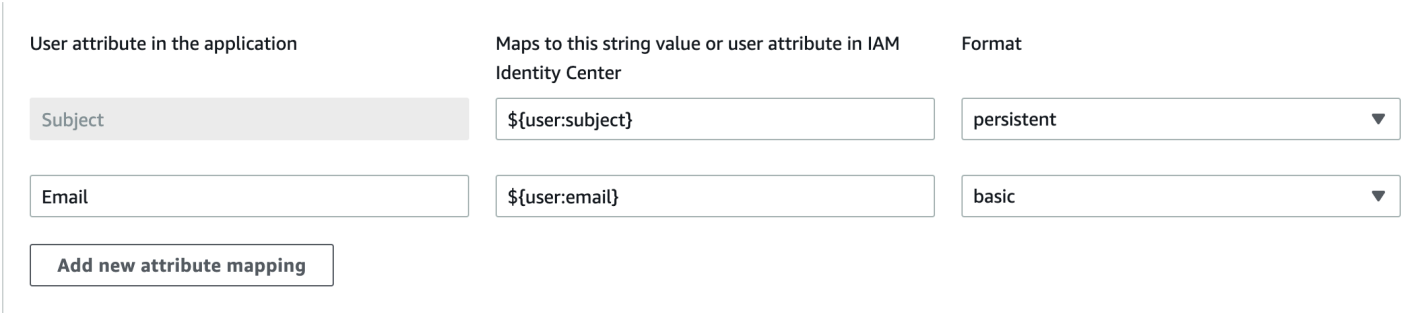


Click **Submit** to save configuration.

Configure Attribute Mapping

- Click the ***Actions*** dropdown and select ***Edit attribute mappings*** and add the following values

```
Subject – ${user:subject} – persistent
Email – ${user:email} – basic
```

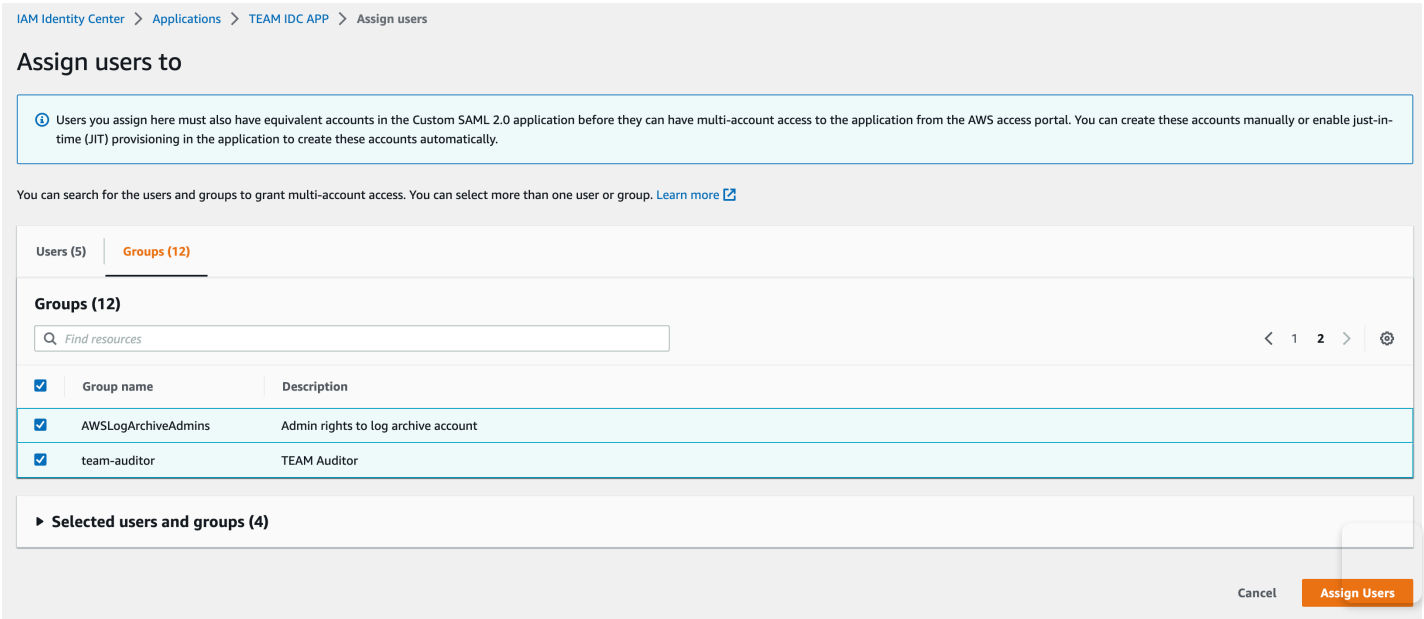


Click **Save changes**

Assign users or groups to TEAM application

Under **Assigned Users** Click the ***Assign users*** and add users. This will grant assigned users and groups access to login to the TEAM application.

> **IMPORTANT**
> Remember to add the **team-admin** and **team-auditor** group to the team application in addition to other application users and groups



🚀 Next Step: Update Cognito user pool configuration