AWS IAM IDENTITY CENTER - OKTA INTEGRATION

Overview

In this simulation, we will be leveraging the external identity capabilities of AWS IAM Identity Center to integrate it with OKTA. Automated account provisioning will be enabled whilst roles and rights will be managed by the permissions sets feature.

Prerequisites

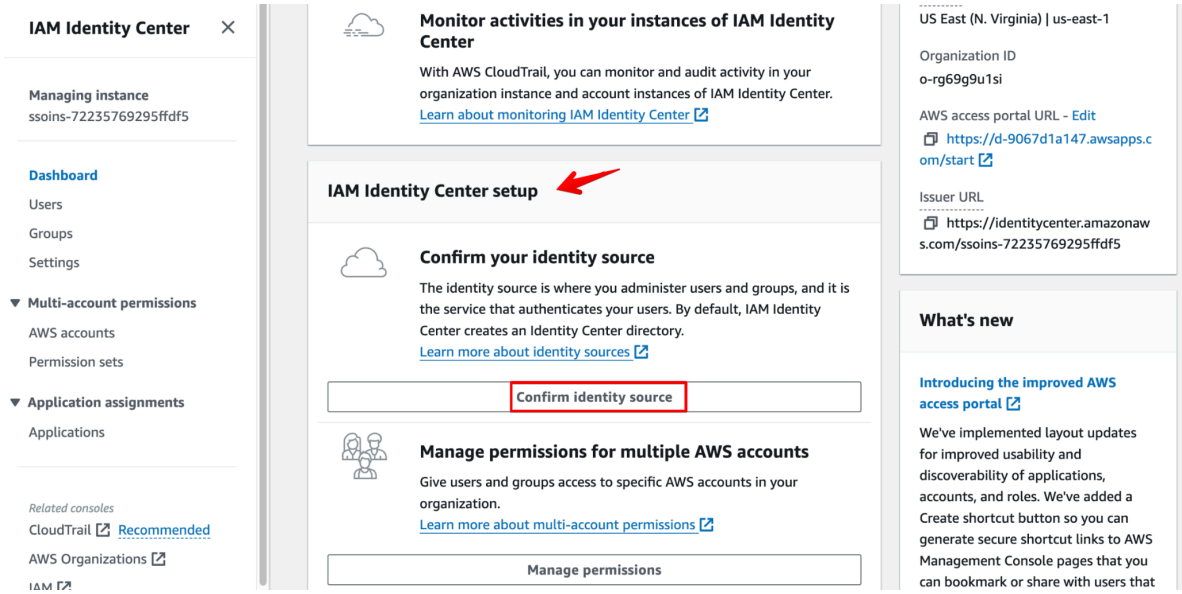
- AWS control tower set up
- Okta developer free account https://developer.okta.com/signup/
- You will need a gmail or github account. when you try to create your OKTA account it will asked for a business email, don't worry scroll down and select continue with Gmail or Github

AWS IAM Identity Center - Service Provider Metadata.

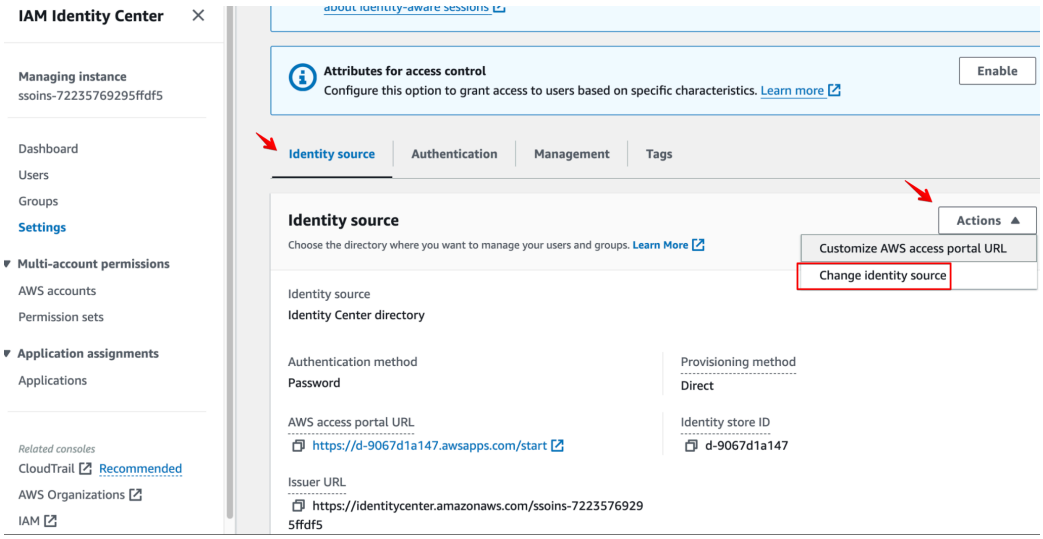
In this section we are going to configure AWS IAM Identity Center to use Okta as an External Identity Provider.

1. Log into the control tower master account as the administrator

2. Navigate to IAM Identity Center Setup and click on "Confirm identity source"

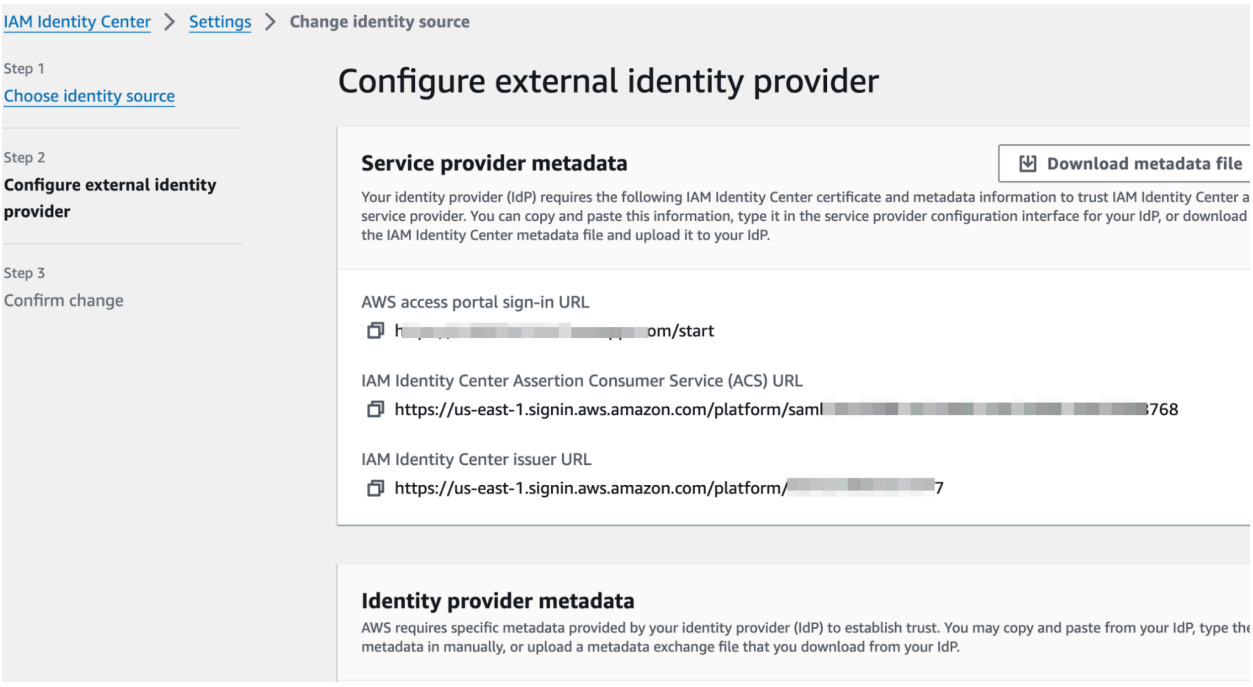


3. Scroll down to tab “identity source”, click on **Action** and select **Change identity source**



4. Select **External Identity Provider**. Click on **Next**

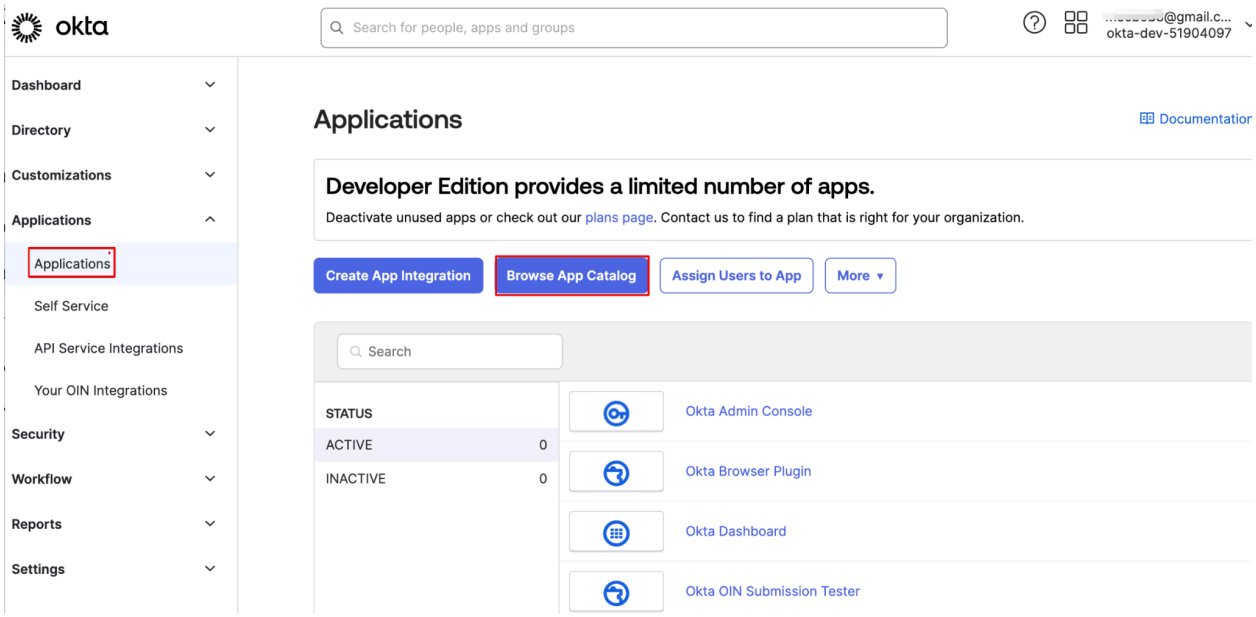
5. (optional)In the Service provider metadata section, click on Do**wnload metadata file**



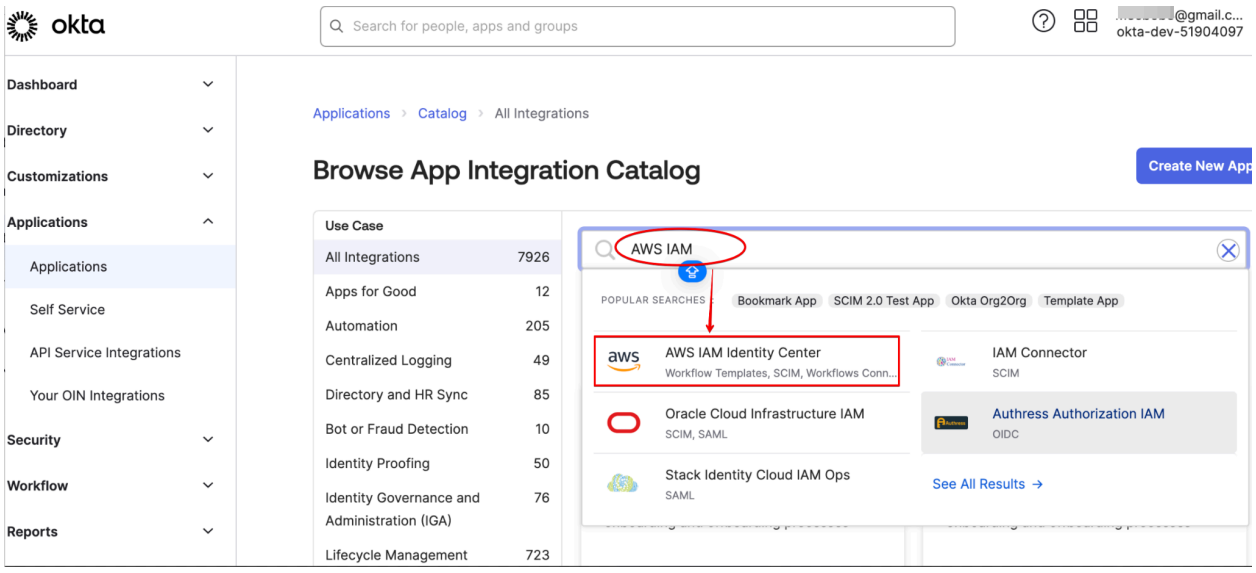
6. Leave this browser tab open, and open a new tab to access your Okta Console

Okta - Create an Amazon Web Services (AWS) App

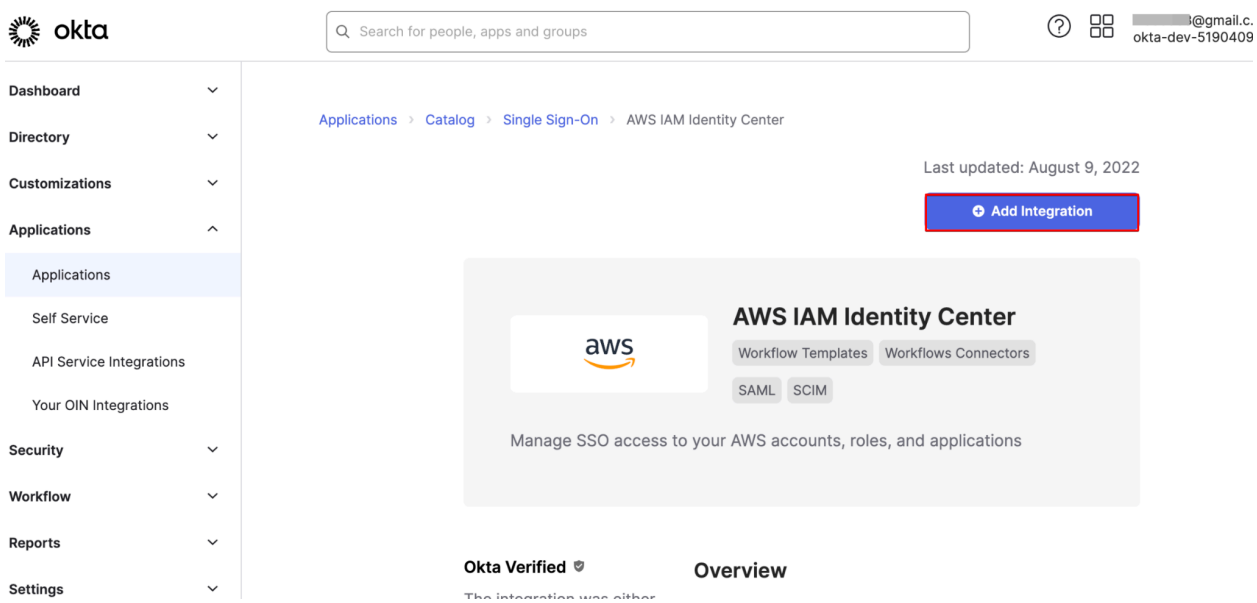
1. Sign in to the Okta console. On the very top of the screen if it shows Developer Console, change this to Classic UI
2. Click ’Applications’ on the left side toolbar and then Applications
3. Click ‘Browse App catalog’

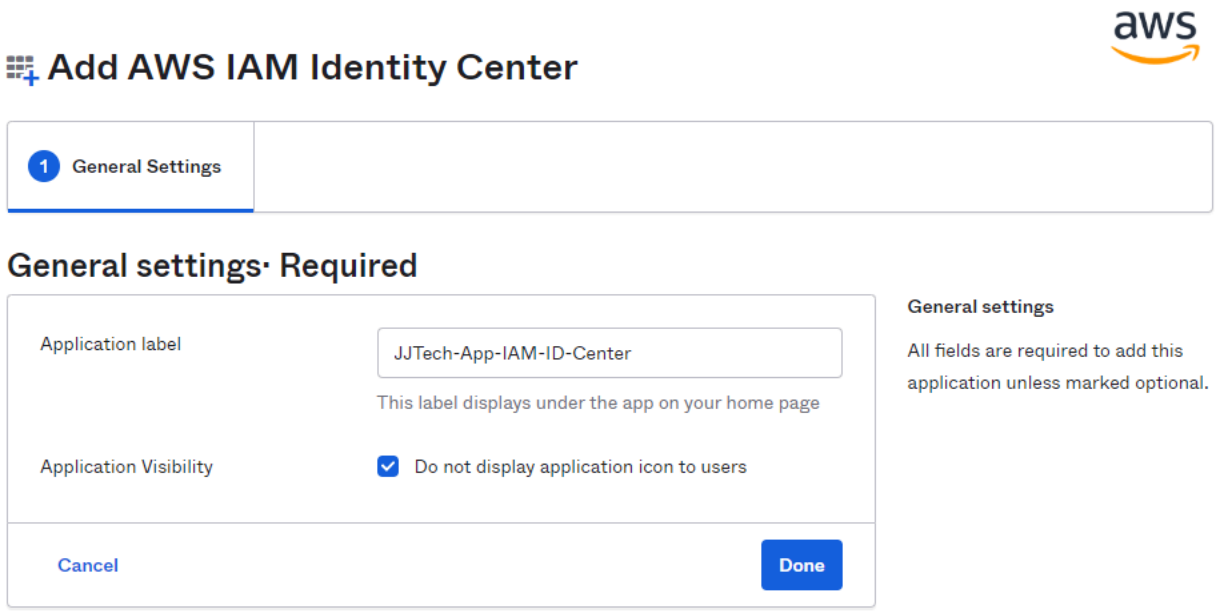


then click into the Search text field and type **AWS IAM Identity Center**



4. Click on the app AWS IAM Identity Center, and click **Add Integration**





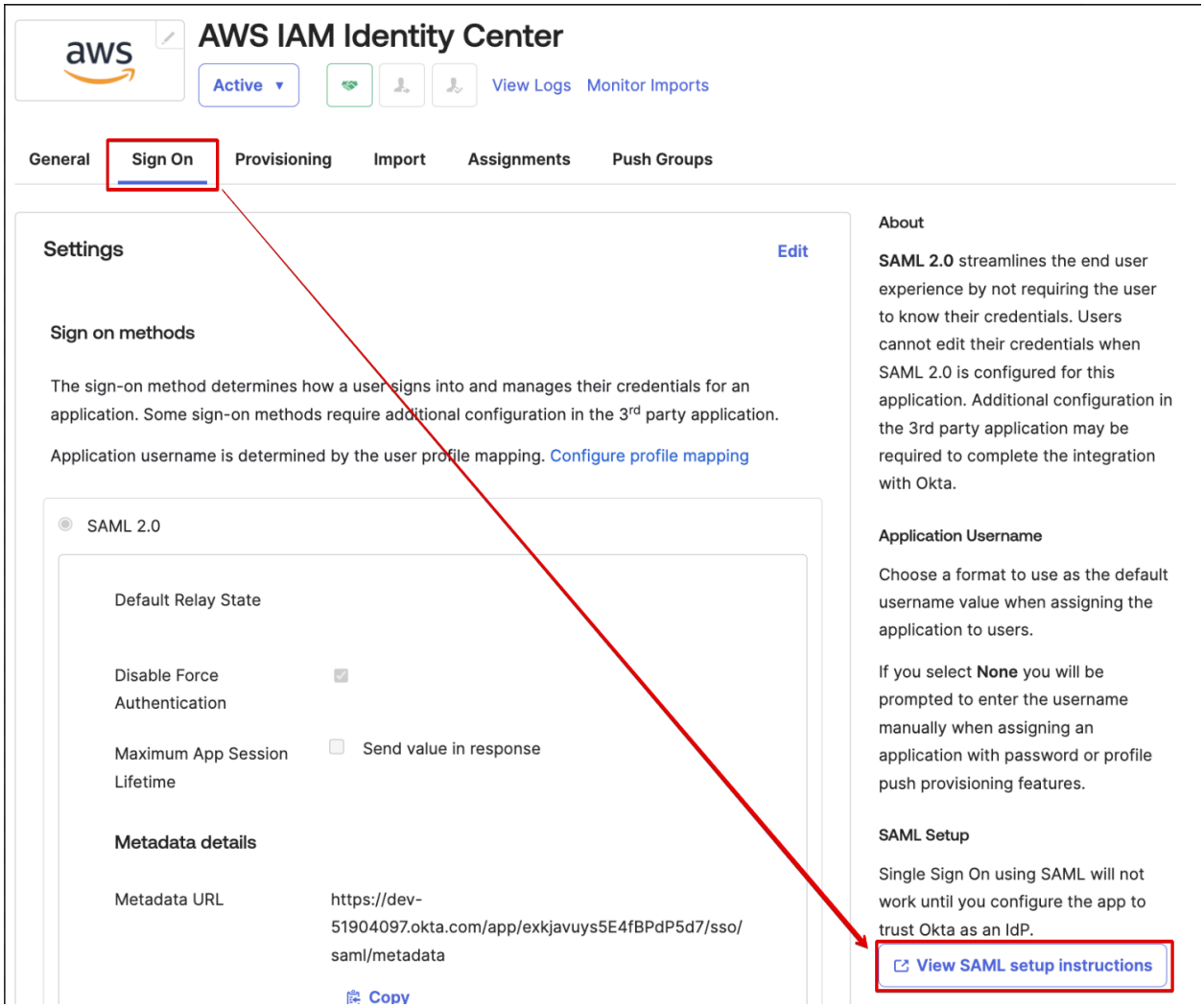
5. General Settings
    a. Application label: AWS: `Your Organization (ex AWS:JJTECH-demo)`
    b. (optional) Check **Do not display application icon in the Okta Mobile app**
    c. Click **Done**

6. Click **'Sign on'**

   You'll need to copy and paste the following fields from the tab you left open on the AWS IAM Identity Center - Identity Provider Metadata console,

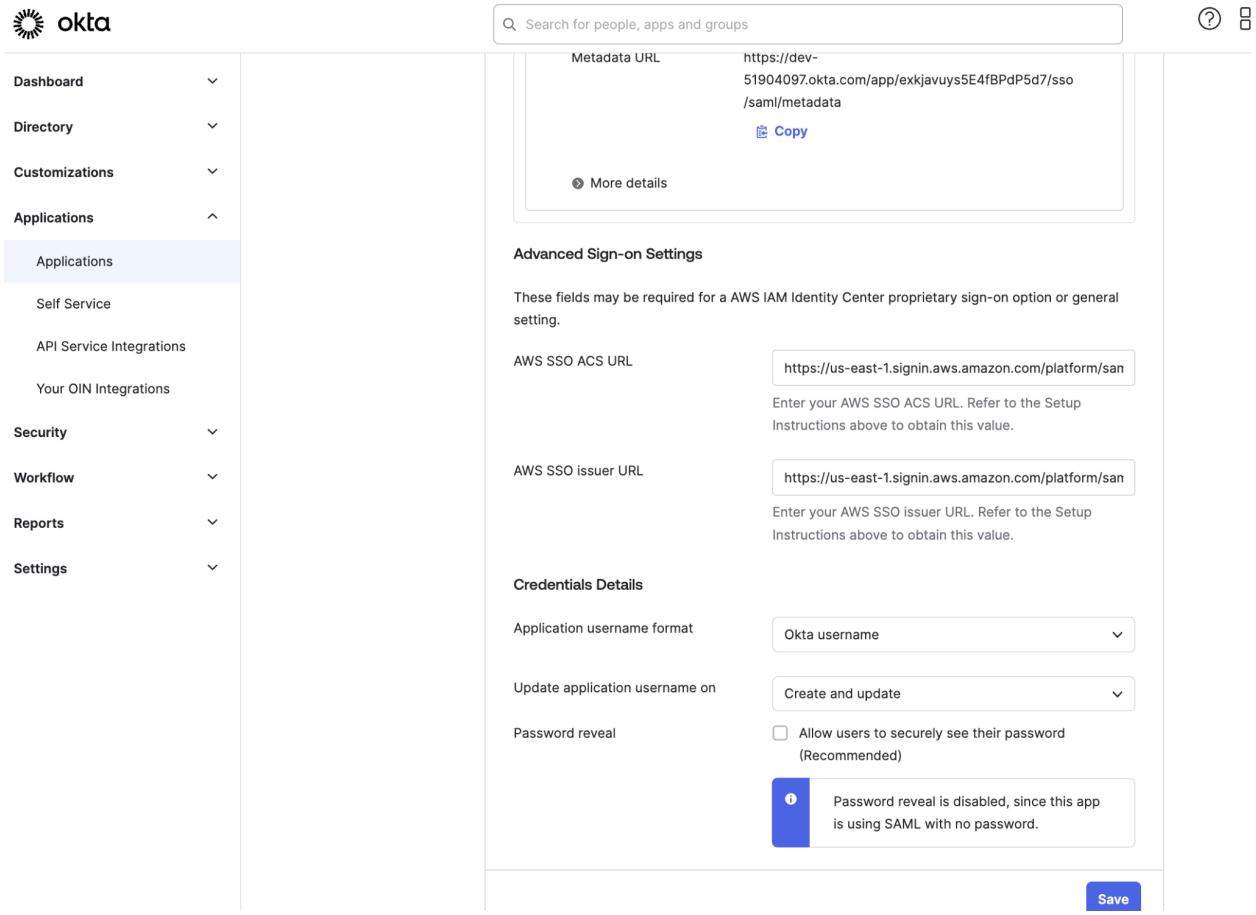
   when you click on "**view SAML setup instructions**" this dynamically creates the setup instructions in a new tab.

   NB: the following steps are from the file



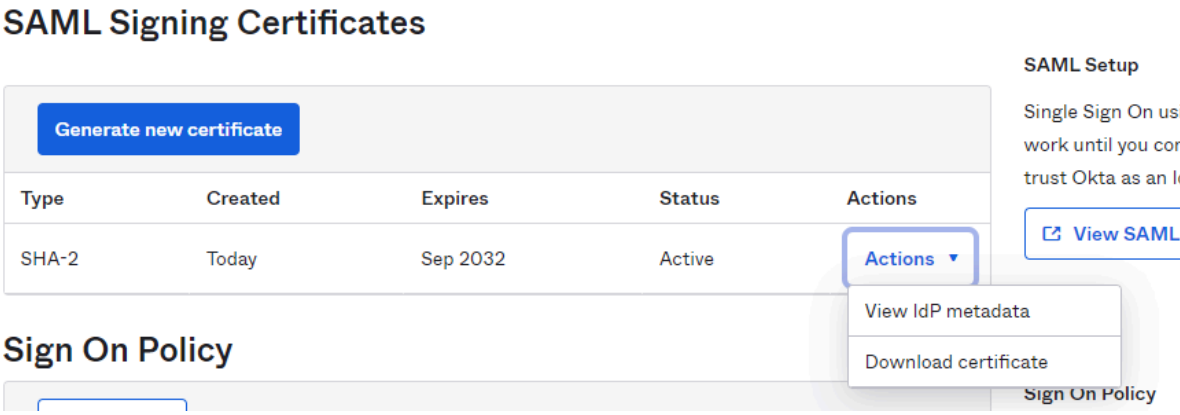
7. click Edit to get started

   in the Advanced Sign-on Settings section,
   a. **AWS IAM Identity Center ACS URL**: `AWS IAM Identity Center ACS URL (The second on the list)`
   b. **AWS IAM Identity Center issuer URL**: `AWS IAM Identity Center issuer URL (The third on the list)`
   c. Click **save**



8. Still on the Sign On page of the App,
   a. Under SAML Signing Certificates, click **Action** and then "**View IdP metadata**"

   b. save the xml it displays as **okta-idp.xml** on your computer, close the browser tab displaying the metadata.



The xml file is as below.

This XML file does not appear to have any style information associated with it. The document tree is shown below.

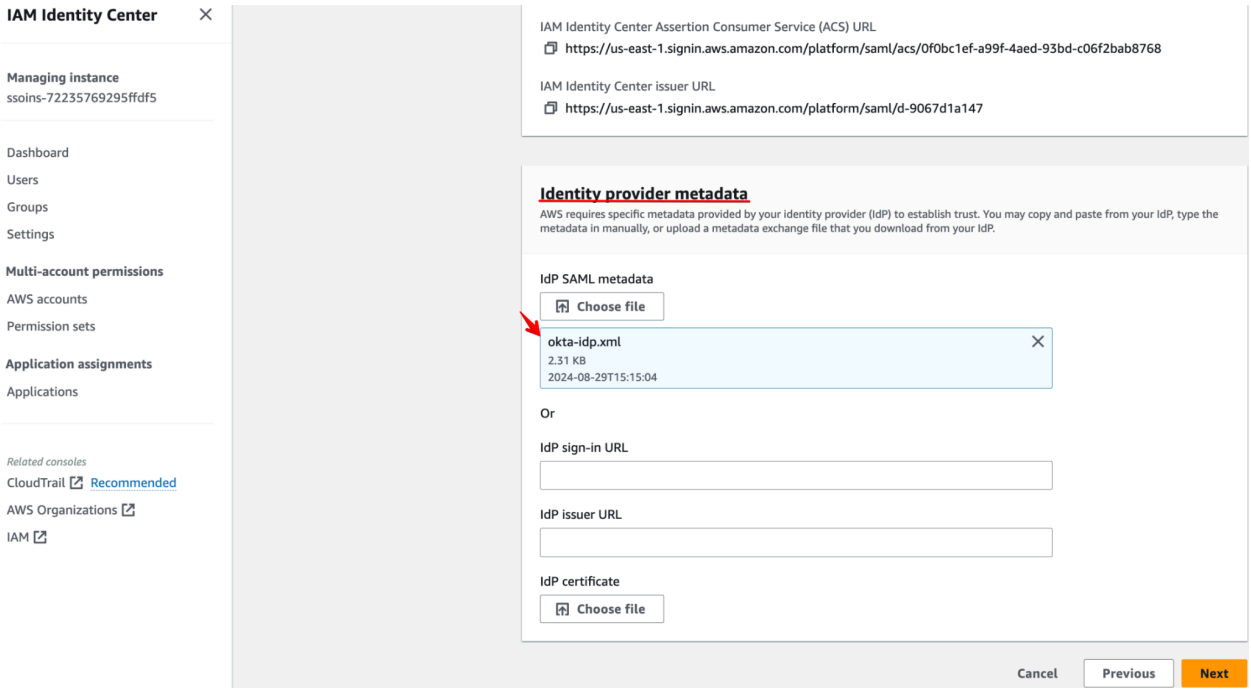

```
▼<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://www.okta.com/exk6eckp9qSQqnITw5d7">
  ▼<md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    ▼<md:KeyDescriptor use="signing">
      ▼<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        ▼<ds:X509Data>
            <ds:X509Certificate>MIIDqDCCApCgAwIBAgIGAYMPEBGqMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYDVQQGEwJVUzETMBEG
            A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
            MBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGRldi04NzA3NjIyMjEcMBoGCSqGSIb3DQEJ
            ARYNaW5mb0Bva3RhLmNvbTAeFw0yMjA5MDUxOTA5NTRaFw0zMjA5MDUxOTEwNTRaMIGUMQswCQYD
            VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsG
            A1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGRldi04NzA3NjIyMjEc
            MBoGCSqGSIb3DQEJARYNaW5mb0Bva3RhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
            ggEBAMGWmvew2qQEXXpLHw+bMenTJ3g1w9qb0IMaewFq/C2yemCxLNaiUUCYYpyO0UM2y9VUMsh+
            CEWXvWfh0iRPy5Zt6ZEOv0LrjKJ/HYzOh12yBkccFpA6NVJhBh6mRi2zVQKLdnC8OcVEB5kWBGWj
            8e/S6ZdY5fnjaTm7v0g4nxm6LOGSjCm8kiFhRNQuY1P+jIYPPVwMdu68++kpQozj3TQXAuSF0HfC
            jJsuo68LbBjMuXSEXGJgST/SogYZ0GmpSE4+jhB1vGKv5Vxd3/pnXA84e4jJjTXKFnxQf2negDpu
            YoNQQG/tNHQ5CTyxff2DUMmLOZELxPqR4+ajfmRZYEsCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEA
            AGHmgdcIj2S3jN24CGQC1k//7OFDXvd+f2pzNRV6u5YdqalozAXqcGWA06Ko2V/P77vbHvWrtWZw
            ozgcvZkFOTYEfbuwcCoc5DE2/NNwIyoRVOLqgJ7/AScTf000C8VFn6c5LpLgvrQTGkUr4CURqTF1
            7SY7bYcfWfn3fGhcaK23AeDPySR1TmID/oLxTG7EFHtGSA3jJ4OPvYmwrOA/dJcWXj6gMxdYTe12
            Qe70aPkPem8sYRqKXMfusWQTZa8IczpqpDKYktuaIXUV5VHrPTbHfXlamsXBaz+MWMAnQ01V0CB 4qheDk5ujI9QztapsJJ9aH4l9UKBTnQRJdiWRQ==
            </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://dev-
    87076222.okta.com/app/amazon_aws_sso/exk6eckp9qSQqnITw5d7/sso/saml"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://dev-
    87076222.okta.com/app/amazon_aws_sso/exk6eckp9qSQqnITw5d7/sso/saml"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

configure Okta in Identity Center

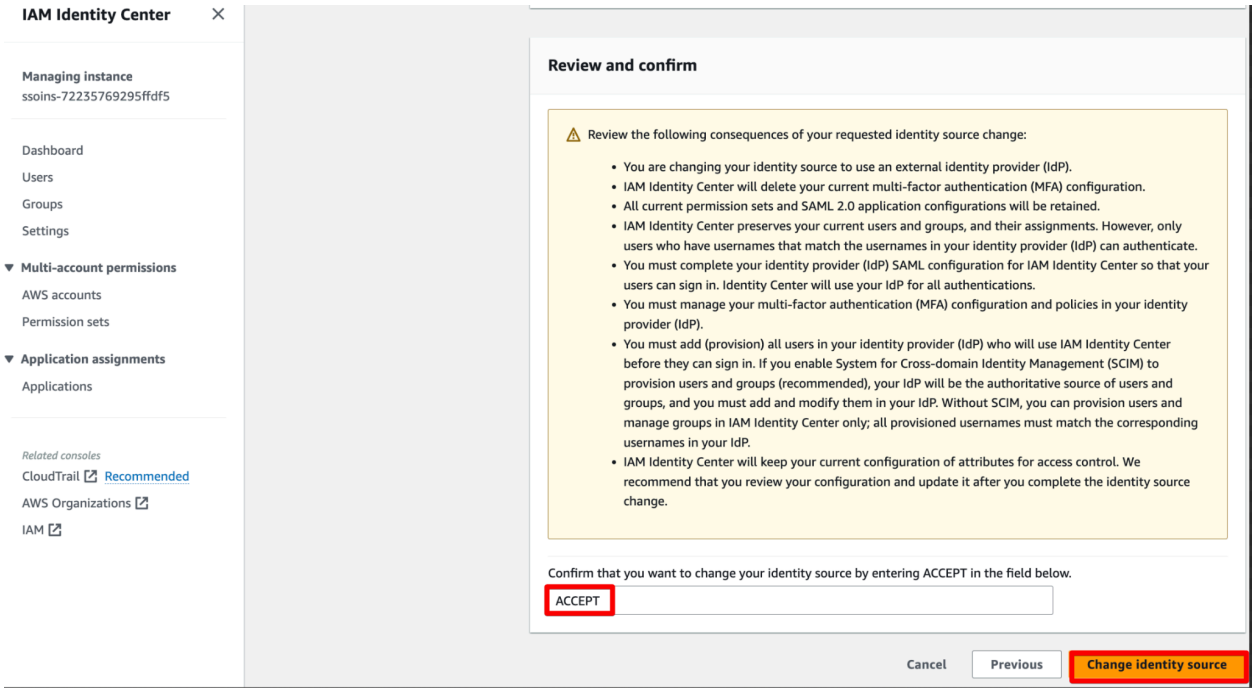
In this section we are going to upload the details of our Okta Identity Provider.

1. Switch back to the AWS IAM Identity Center -

2. Under the “**Identity provider metadata**” section, upload the xml document
    - Click Browse and select the **okta-idp.xml** document you saved above.



3. Click **Next**:
4. Review and confirm
    a. Review the information provided
    b. Type **ACCEPT** in the field at the bottom
    c. click **Change Identity source**


IAM Identity Center
Managing instance
ssoins-72235769295ffdf5
Dashboard
Users
Groups
Settings
Multi-account permissions
AWS accounts
Permission sets
Application assignments
Applications
Related consoles
CloudTrail
Recommended
AWS Organizations
IAM
Review and confirm
Review the following consequences of your requested identity source change:
You are changing your identity source to use an external identity provider (IdP).
IAM Identity Center will delete your current multi-factor authentication (MFA) configuration.
All current permission sets and SAML 2.0 application configurations will be retained.
IAM Identity Center preserves your current users and groups, and their assignments. However, only users who have usernames that match the usernames in your identity provider (IdP) can authenticate.
You must complete your identity provider (IdP) SAML configuration for IAM Identity Center so that your users can sign in. Identity Center will use your IdP for all authentications.
You must manage your multi-factor authentication (MFA) configuration and policies in your identity provider (IdP).
You must add (provision) all users in your identity provider (IdP) who will use IAM Identity Center before they can sign in. If you enable System for Cross-domain Identity Management (SCIM) to provision users and groups (recommended), your IdP will be the authoritative source of users and groups, and you must add and modify them in your IdP. Without SCIM, you can provision users and manage groups in IAM Identity Center only; all provisioned usernames must match the corresponding usernames in your IdP.
IAM Identity Center will keep your current configuration of attributes for access control. We recommend that you review your configuration and update it after you complete the identity source change.
Confirm that you want to change your identity source by entering ACCEPT in the field below.
ACCEPT
Cancel
Previous
Change identity source

Change identity source

1 Choose identity source — 2 Review

Choose where your identities are sourced

Your identity source is the place where you administer and authenticate identities. You use AWS SSO to manage permissions for identities from your identity source to access AWS accounts, roles, and applications. Learn more

- ○ **AWS SSO**
  You will administer all users, groups, credentials, and multi-factor authentication assignments in AWS SSO. Users sign in through the AWS SSO user portal.
- ○ **Active Directory**
  You will administer all users, groups, and credentials in AWS Managed Microsoft AD, or you can connect AWS SSO to your existing Active Directory using AWS Managed Microsoft AD or AD Connector. Users sign in through the AWS user portal.
- ◉ **External identity provider**
  You will administer all users, groups, credentials, and multi-factor authentication in an external identity provider (IdP). Users sign in through your IdP sign-in page to access the AWS SSO user portal, assigned accounts, roles, and applications.

Configure external identity provider

AWS SSO works as a SAML 2.0 compliant service provider to your external identity provider (IdP). To configure your IdP as your AWS SSO identity source, you must establish a SAML trust relationship by exchanging meta data between your IdP and AWS SSO. While AWS SSO will use your IdP to authenticate users, the users must first be provisioned into AWS SSO before you can assign permissions to AWS accounts and resources. You can either provision users manually from the Users page, or by using the automatic provisioning option in the Settings page after you complete this wizard. Learn more

Service provider metadata

Your identity provider (IdP) requires the following AWS SSO certificate and metadata details to trust AWS SSO as a service provider. You may copy and paste, or type this information into your IdP's service provider configuration interface, or you may download the AWS SSO metadata file and upload it into your IdP.

AWS SSO SAML metadata — Download metadata file

AWS SSO Sign-in URL — https://[redacted].awsapps.com/start

AWS SSO ACS URL — https://eu-west-1.signin.aws.amazon.com/platform/saml/acs

AWS SSO issuer URL — https://eu-west-1.signin.aws.amazon.com/platform/saml/d-

Hide individual metadata values

Identity provider metatdata

AWS requires specific metadata provided by your identity provider (IdP) to establish trust. You may copy and paste from your IdP, type the metadata in manually, or upload a metadata exchange file that you download from your IdP.

IdP SAML metadata* — Browse...

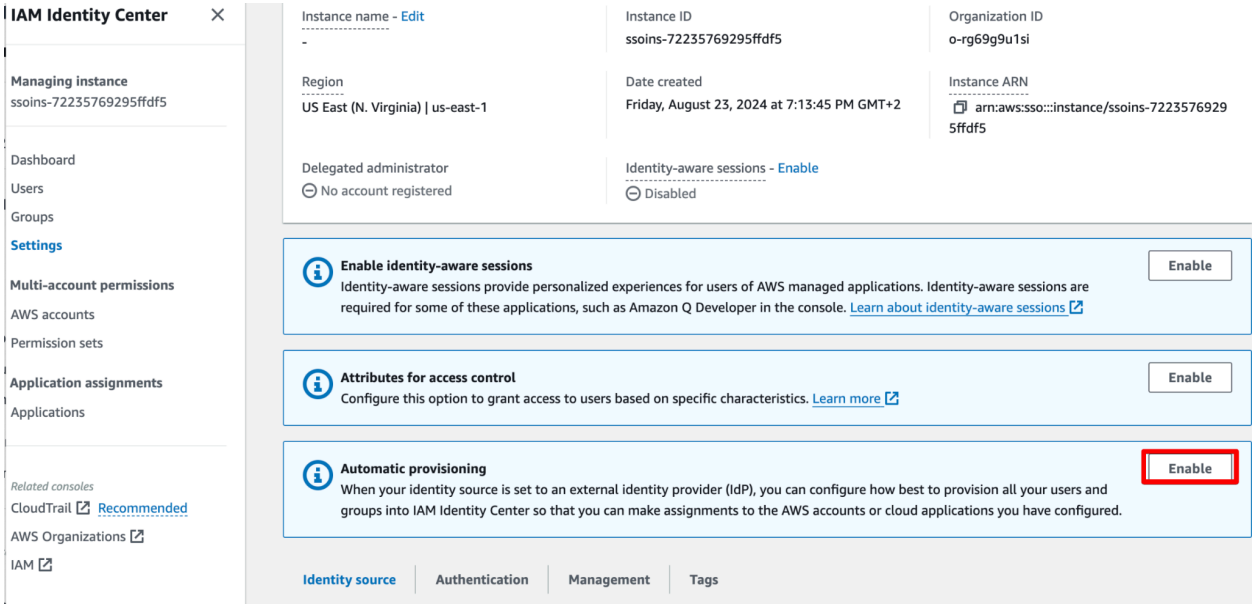
If you don't have a metadata file, you can manually type your metadata values

Cancel | Next: Review

IAM Identity Center - Enable Automated Provisioning

This is an optional setup although highly recommended for managing users at scale.

1. In the AWS IAM Identity Center console, Go to **Settings**, then click on **Enable automatic provisioning.** It should give you an SCIM endpoint and an Access token



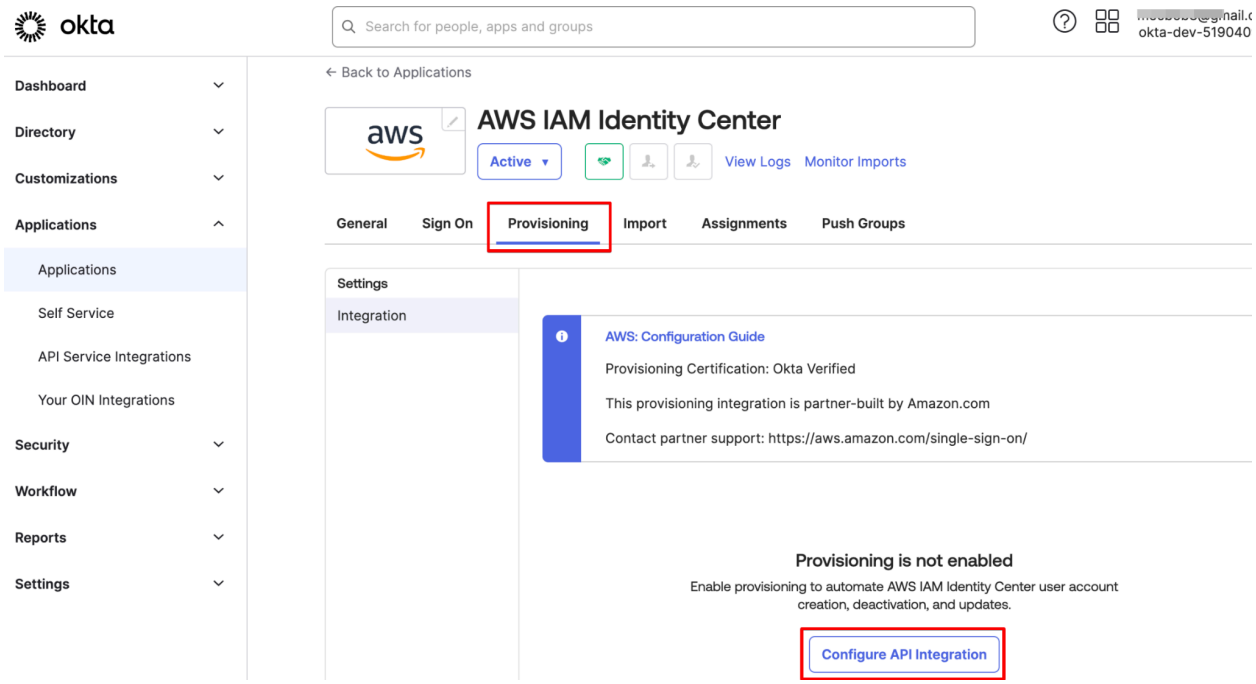
2. You'll need to copy and paste the following fields into the **Provisioning** form on the tab you left open on the Okta AWS IAM Identity Center - SCIM 2.0 (OAuth Bearer Token) console,

if you receive an error please delete the trailing '/' from the SCIM 2.0 Base URL.

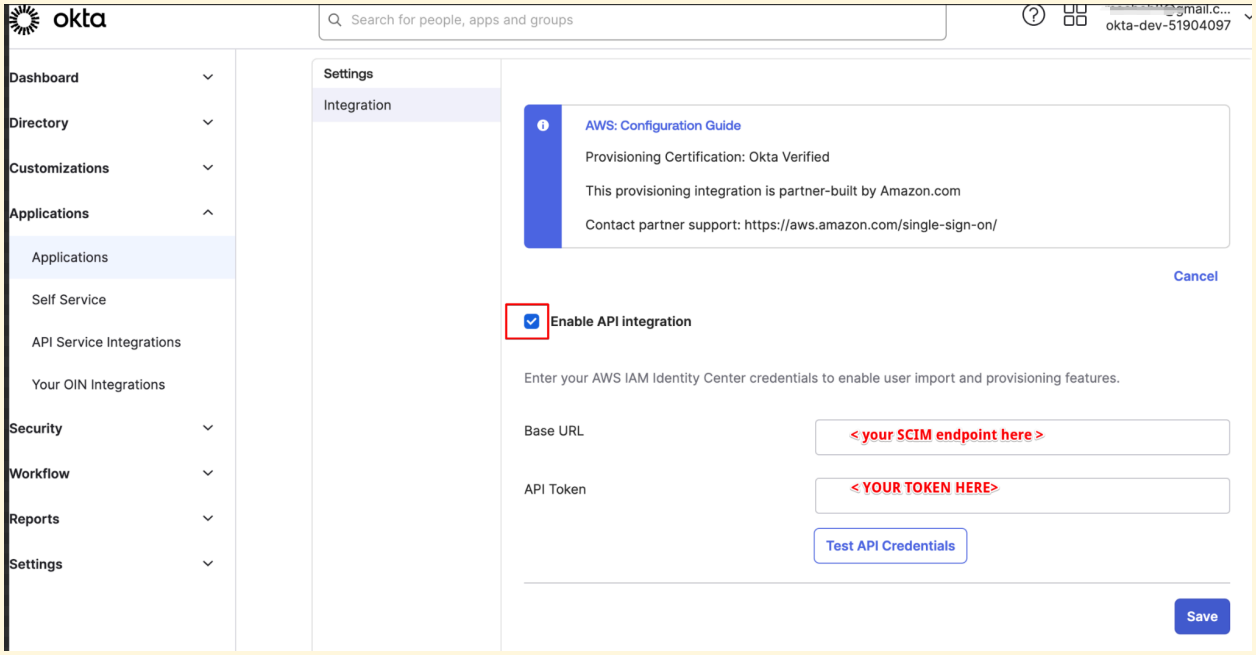
Okta - Enable Automated Provisioning

Go your Okta console and select the "Provisioning" tab

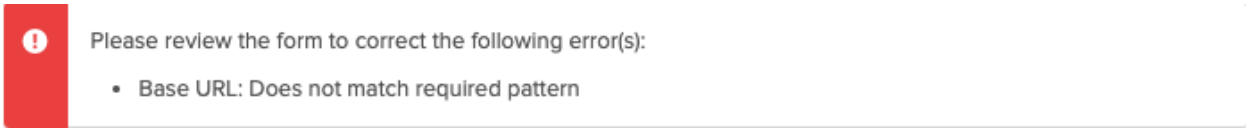
- On the Provisioning page
    - Click Configure API Integration



- **check** ”enable API integration” and enter the parameters from the AWS IAM Identity Center page
  - SCIM 2.0 Base Url: `SCIM endpoint`
  - OAuth Bearer Token: `Access token`

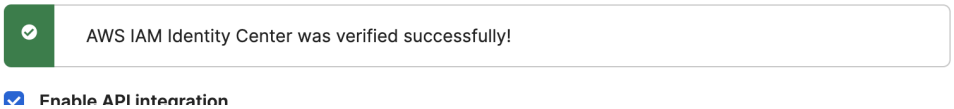


- Click Test API Credentials if you get an error:

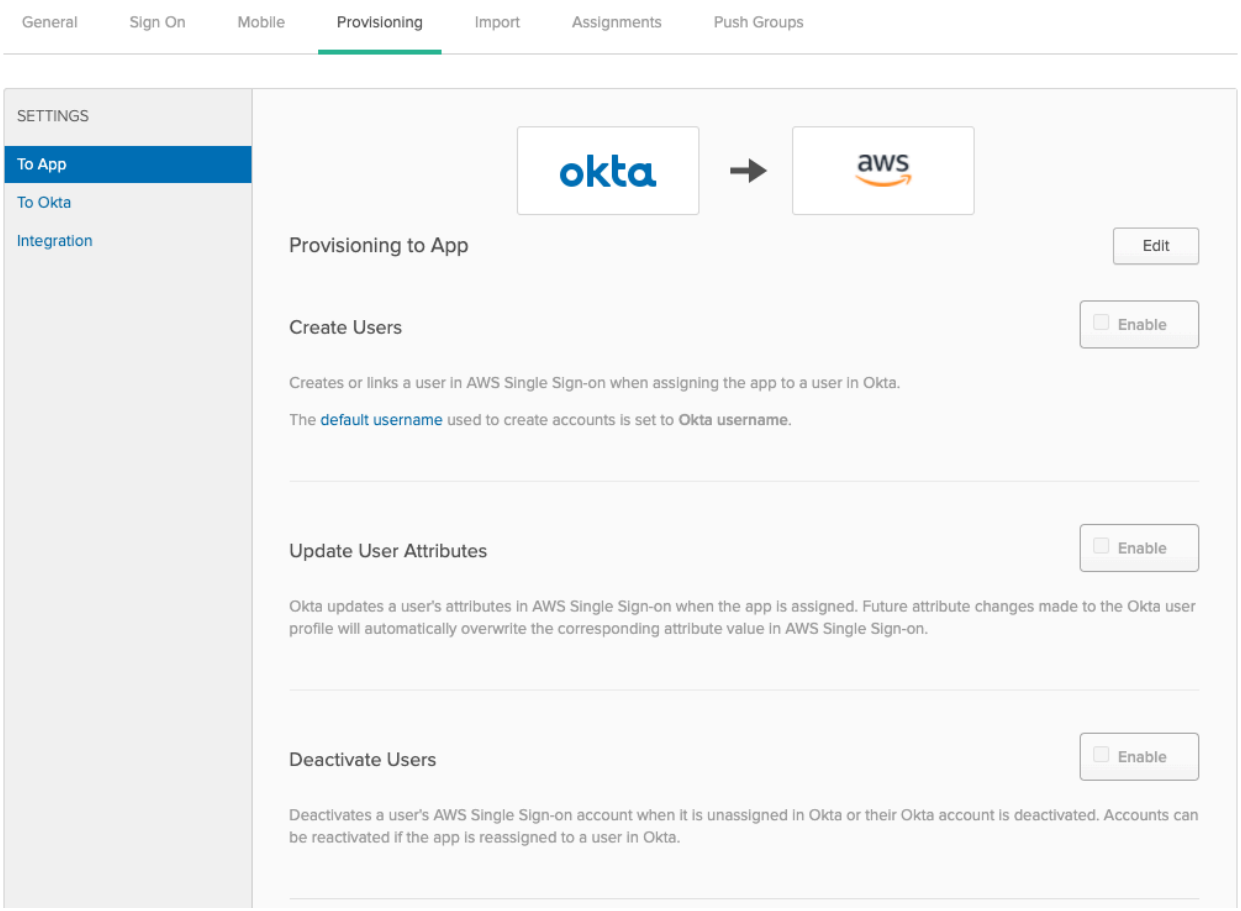


Then remove the trailing ‘/’ from the Base URL, and try again.

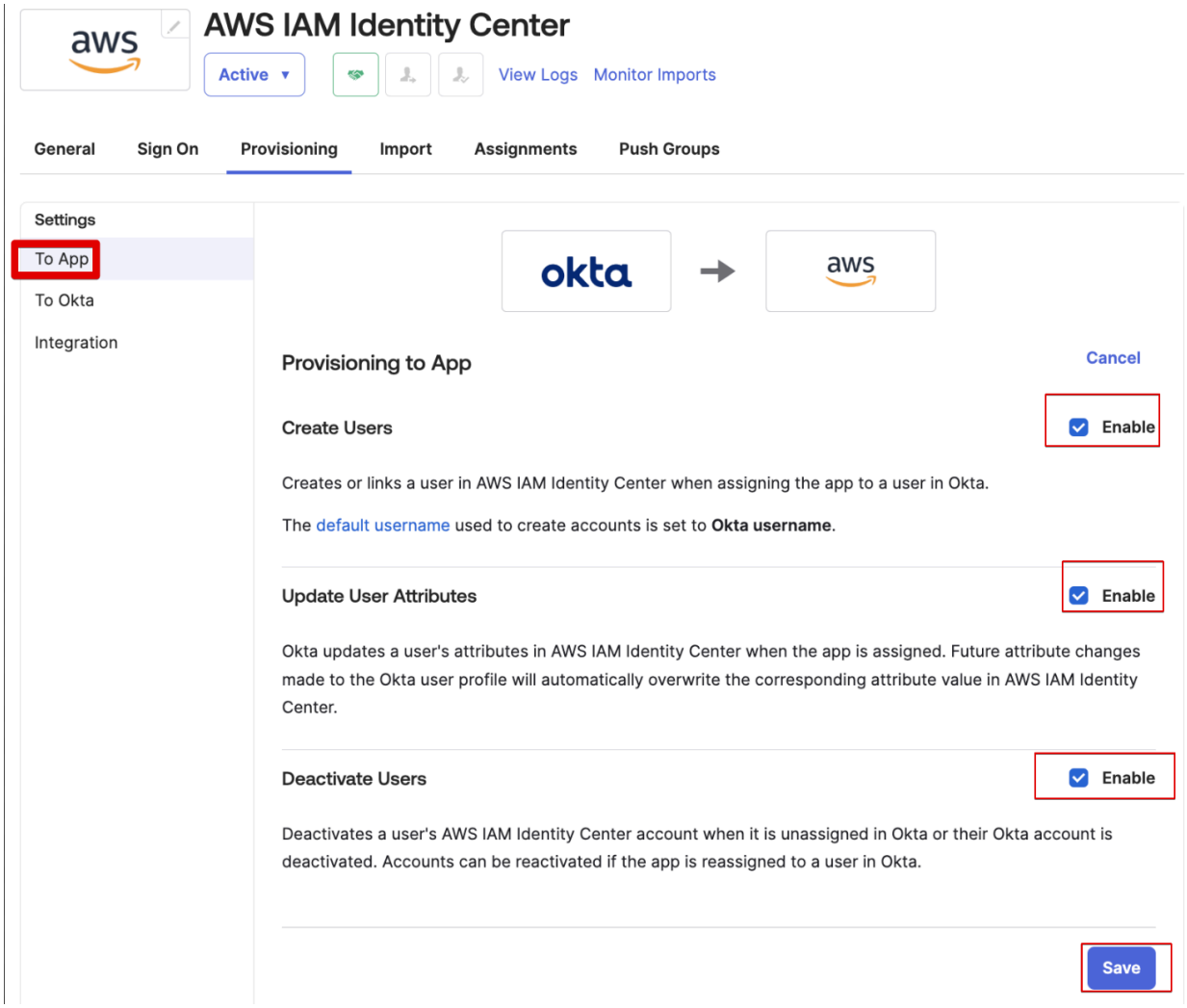
A successful test pic shown below:



* Click **Save**



- Click **To APP** in the left-hand menu
    - click **Edit**, and **check** ”Create Users”, “Update User Attributes”, “Deactivate Users”,
    - click **Save**

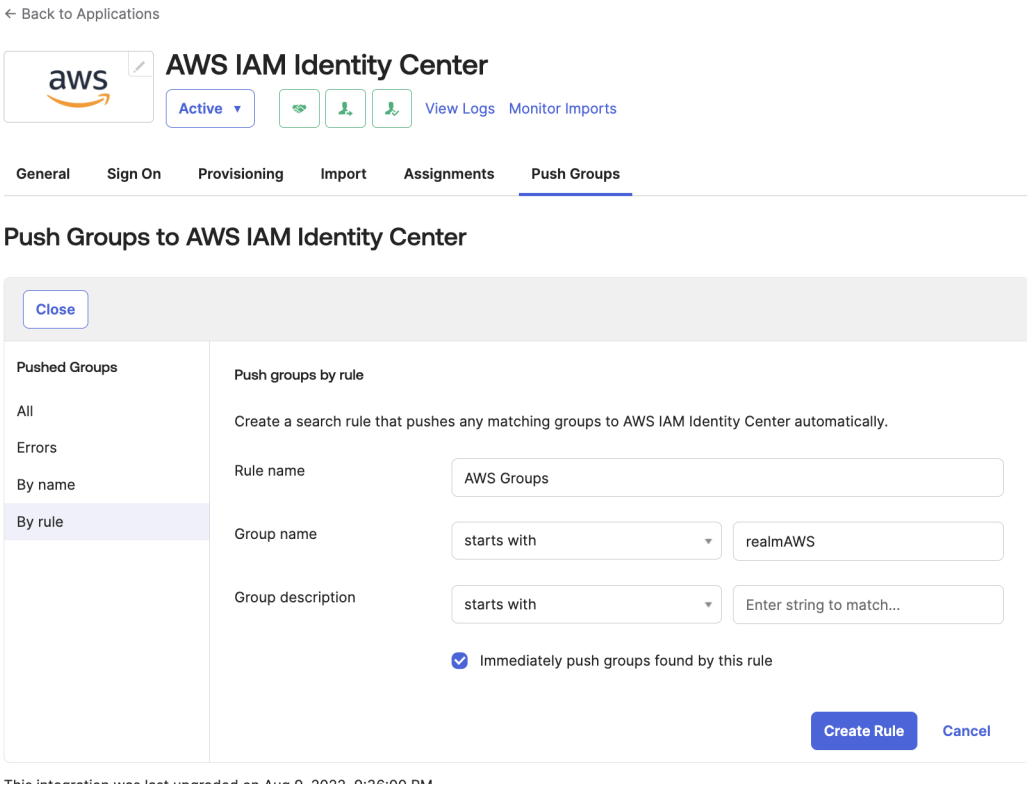


Assign Users

PUSH GROUPS

- Click on **Push Groups**
- Click on **+ Push Groups** then Click on “**Find Groups by Rule**”
    - Rule name: **AWS Groups**
    - Group name: starts with: `realm`AWS

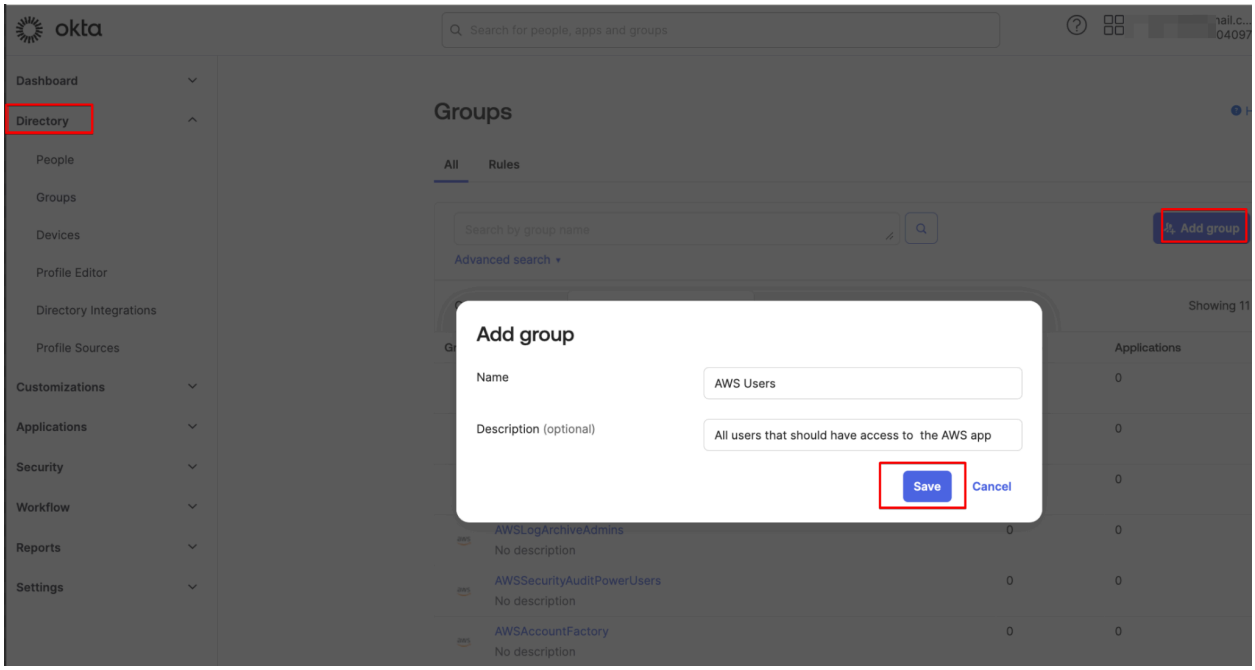
- Leave “Group description” empty
- check Immediately push groups found by this rule
- Click **Create Rule**



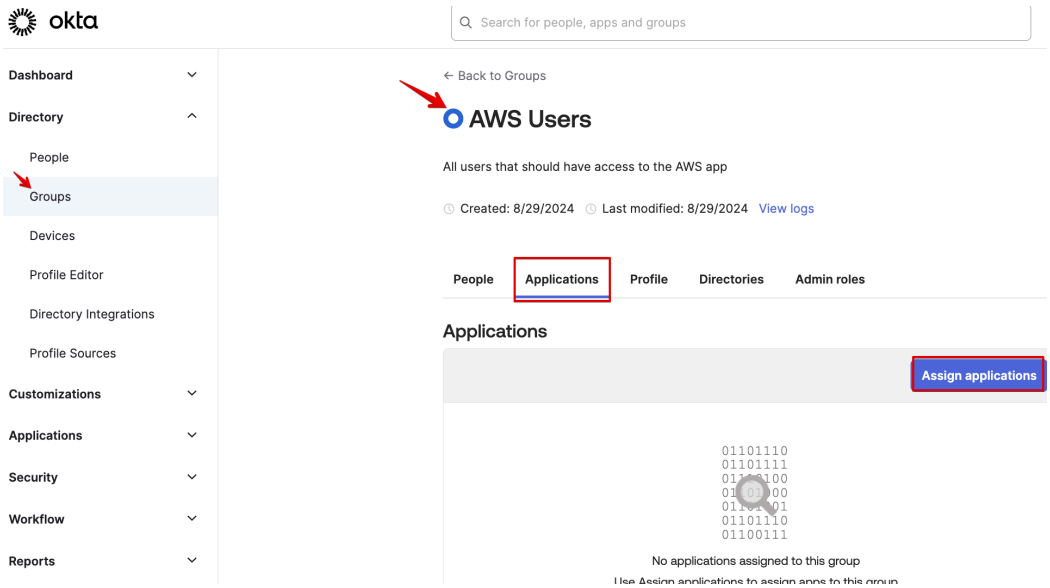
Okta - Assign the Apps to the Group of Users

First, we need to create a group, to represent users that should have access to the AWS app in Okta

1. On the Okta console (on the top ribbon), click **Directory** > **Groups**
2. Click **Add Group**

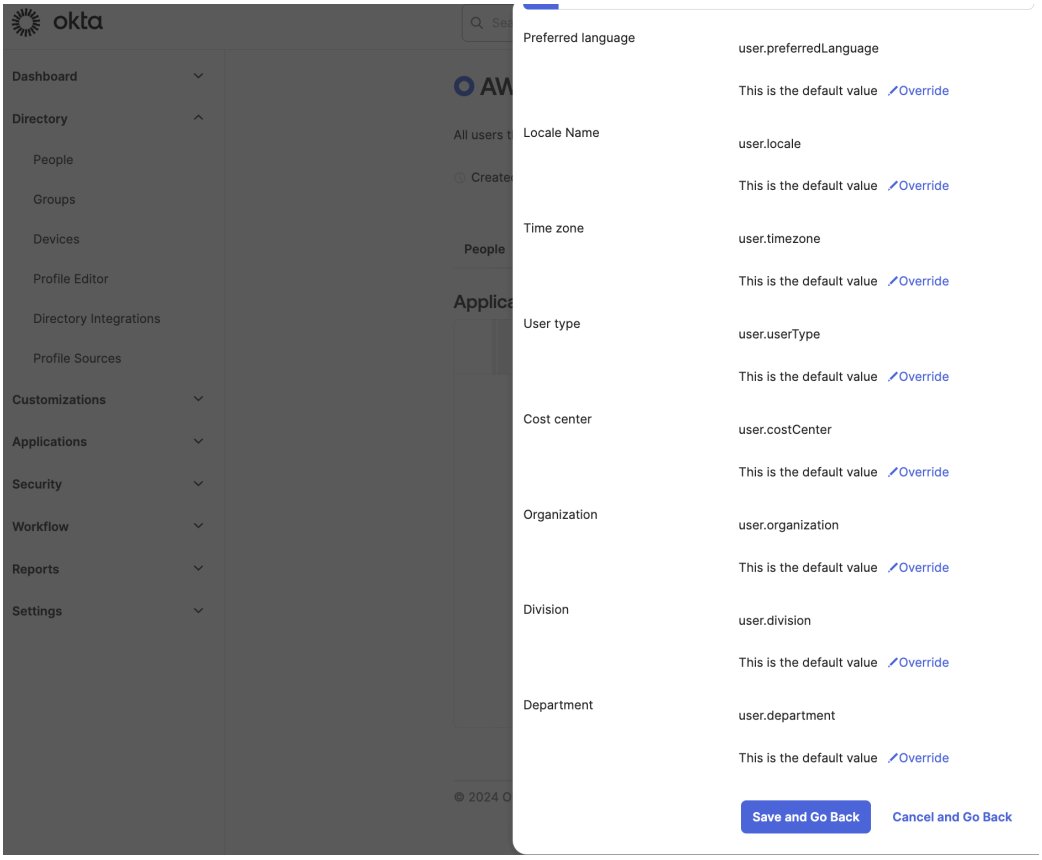


3. Add Group
    a. Name: AWS Users
    b. Group Description: All Users that should have access to the AWS app.
    c. Click save
4. Click on the Group "**AWS Users"** (created earlier) in the drop down list of Groups
    a. Click Applications
    b. Click **Assign applications** and select the App AWS: `Your Organization`



c. Click **Assign**
   i. This is the app users will launch into the AWS Console
   ii. Leave all fields blank

d. Scroll down Click **Save and go back**

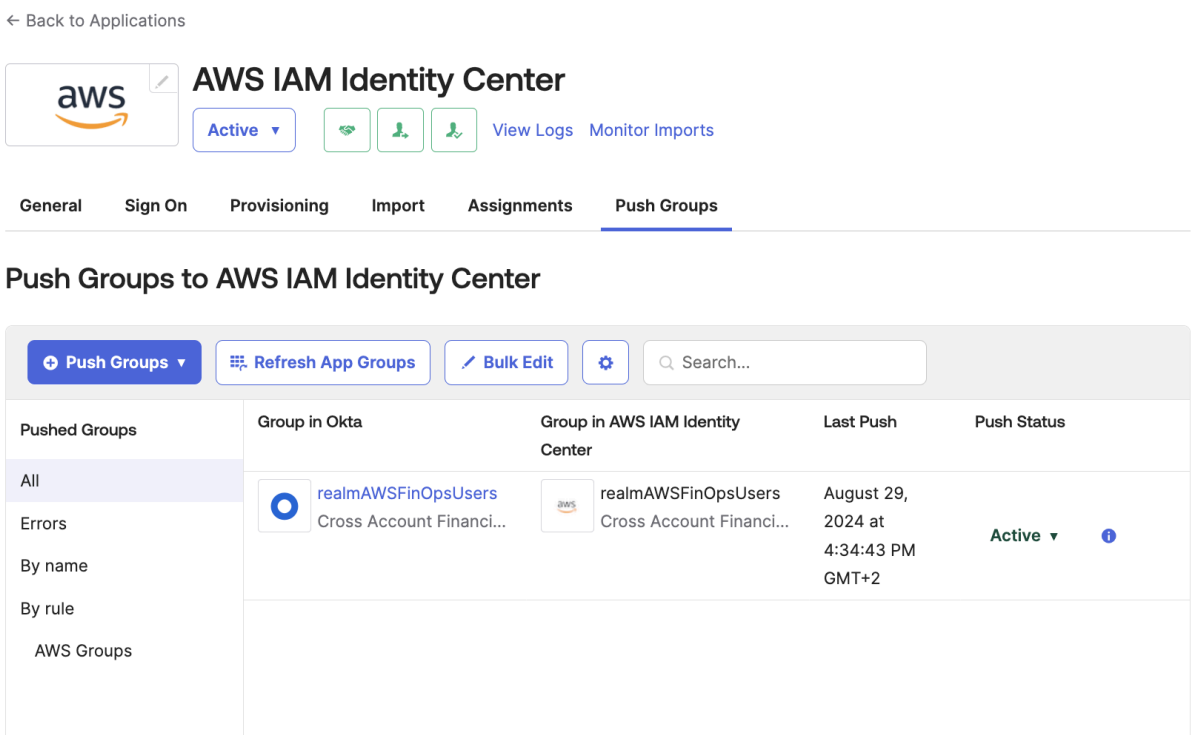


e. Click **Done**

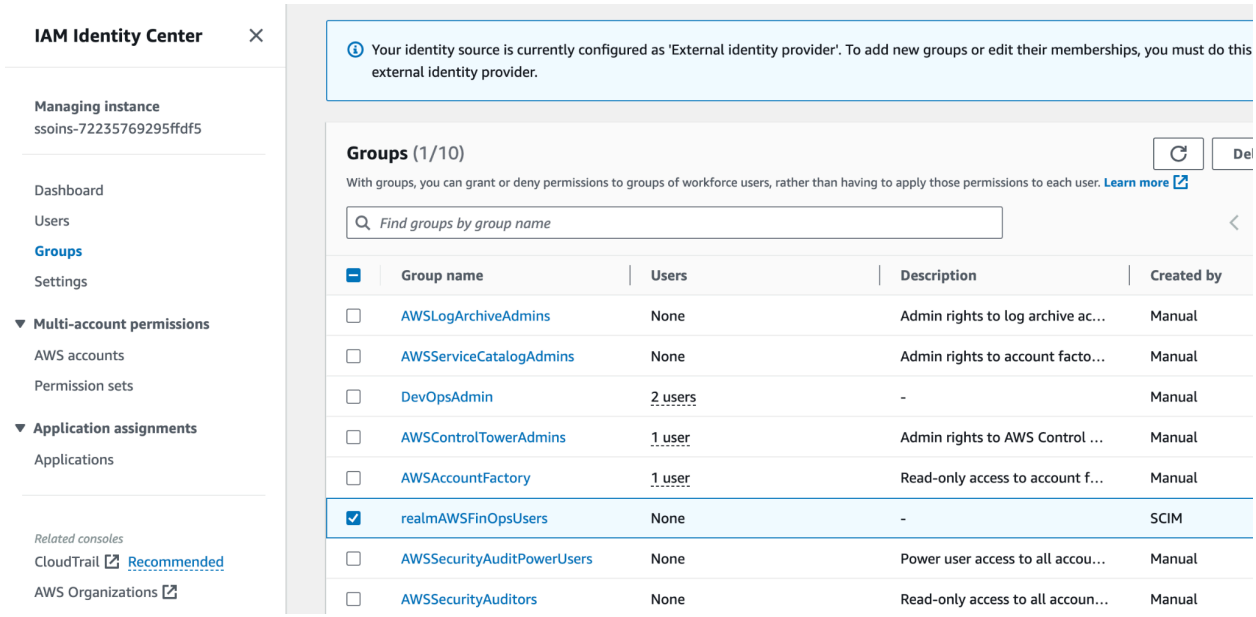
Okta - Create a Group

Earlier we created a rule to push Groups from OKTA to AWS IAM Identity Center that had the prefix `realm` AWS now let's create such a group and check if this happens. We are going to create a group to represent our Financial Operations team members, who should have permissions to access billing information on our Organizations Management payer account.

1. In the Okta console (on the top ribbon), click Directory then Groups
2. Click Add Group
3. Add Group
    a. Name: `realm`**AWSFinOpsUsers**
    b. Group Description: Cross Account Financial Operations Users.
4. Click **save**
5. Go to Application and select the AWS: `Your Organization` app and click on the **Push Groups** tab
6. We should see `realm`AWSFinOpsUsers listed and marked as Active



7. Switch to the browser tab On the AWS IAM Identity Center
8. In the left panel, click 'Groups' and you should see realmAWSFinOpsUsers listed with No users



AWS IAM Identity Center - Create/Assign Permission Sets

We'll now create a permission with appropriate rights for the Financial Operations Team.

- Switch to AWS IAM Identity Center

Create Permission Set

- In the left panel, under Multi-account permissions, select "Permission sets"
- Click **Create permission set**
- to create new permission set
    - Select **Predefined Permission set**
    - scroll down select **Billing,** then click **Next**
    - leave everything as default and click **Next**
    - Click Create

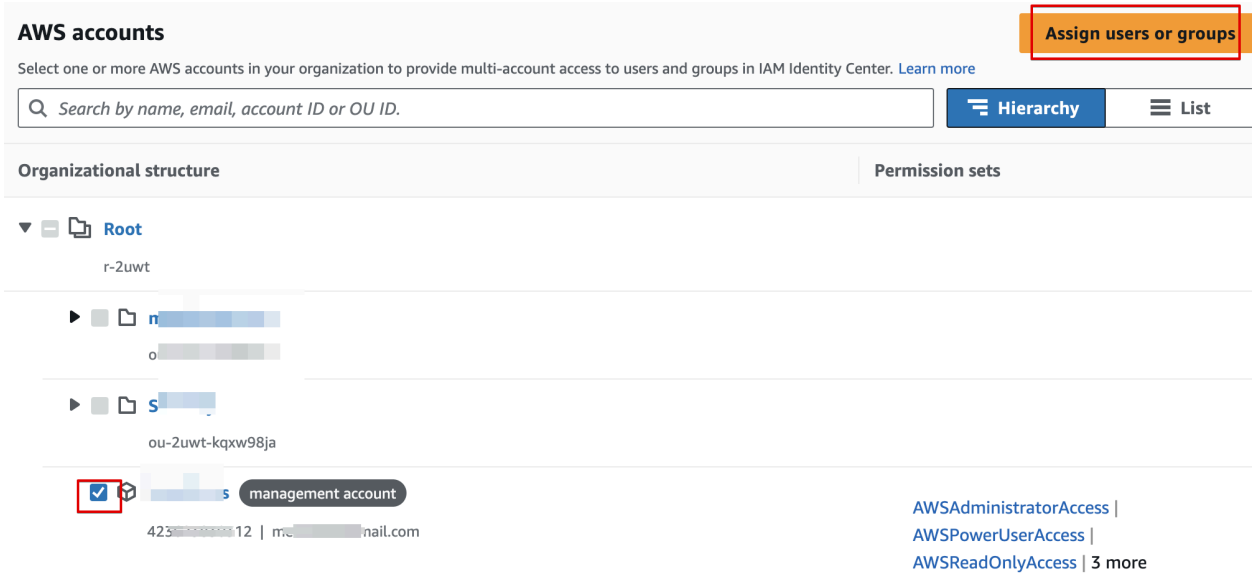
Assign Permission Set

- Click on "Billing" in the list of permission sets
- Billing - Permissions tab
    - Click Edit
    - Relay state: https://console.aws.amazon.com/billing/home?#/
    - Click save changes

AWS IAM Identity Center - Assign Users

We now need to add the group of users represented by the group (from Okta) `realm`AWSFinOpsUsers with the permission set Billing to the management/payer account.

- In AWS IAM Identity Center
- In the left panel, click AWS accounts,
- Under the root organization
    - Check `your Management account` and click **Assign users or groups**



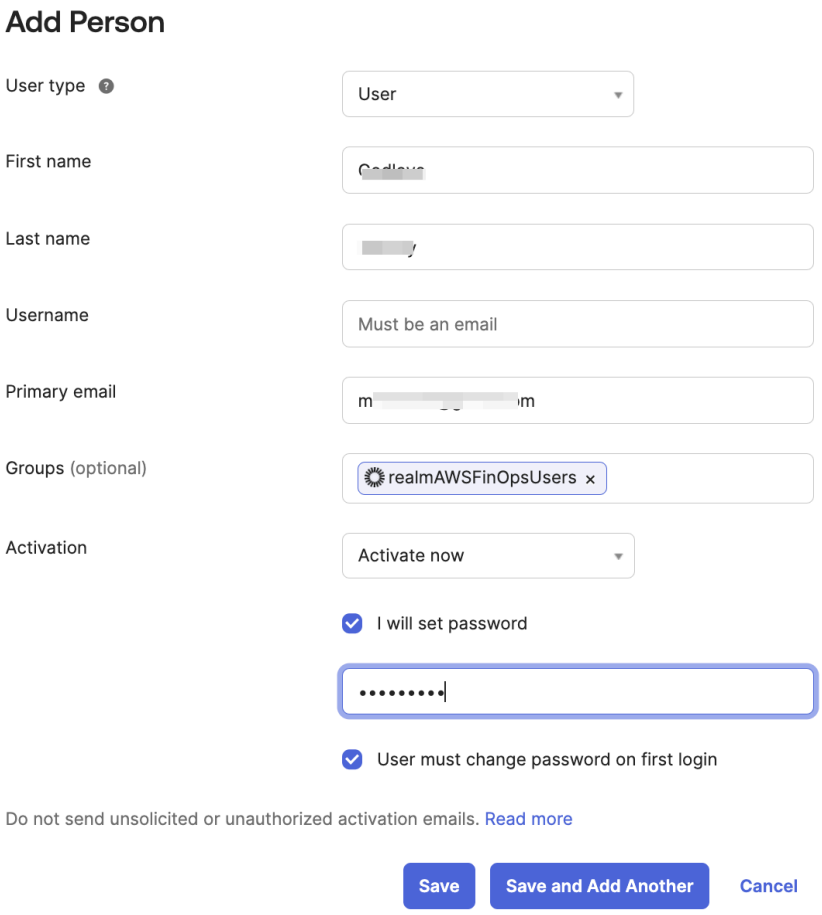
- To Assign Users:
    - Click the **Groups** tab
    - Check `realm`AWSFinOpsUsers
    - Click **Next:**
- Assign permission sets
    - check 'Billing' Permission set and click **'Next'**
    - Click **'Submit'**

Okta - Create a user

In this section, you'll create a test user in the Okta portal.

- Switch to the browser tab on the Okta console

- In the Okta console (on the top ribbon), click Directory > People
- Click **Add Person**
- Add Person
    - User type: User
    - First name: `your first name`
    - Last name: `your last name`
    - Primary email: `alias`@`realm`.local
    - Groups:
        - *start typing* `realm` AWS and click Add next to `realm`AWS FinOpsUsers
        - *start typing* AWS *and click Add next to AWSUsers
    - Activation: Activate now
        - Password: check I will set password
        - enter a password
    - check User must change password on first login (user should be able to change password at first login)
    - Click **Save**



Go back to people, select the user your created,
Select **Assign Application**
Select your Application **-e.g AWS:JJTECH-demo,**
Click on **Assign**
Click **Save and go Back**
and **Done**

- Switch to the browser tab On the AWS IAM Identity Center

- In the left panel, click Users,
    - In the list of users, you should now see the account we created (in Okta) above
    - you should see that the user was
        - Created By: SCIM

Explore as our FinOps User

Now we can see what the experience we've configured for our test user.

- Switch to the browser tab On the AWS IAM Identity Center
- In the left panel, click Dashboard,
- Copy the User portal URL:
- Open a browser window in Private or incognito mode and paste the user portal URL in to the address bar.
- Browser should redirect you to your Okta log in page,
    - username: `alias`@`realm`.local
    - password: `the one your created above`
    - you may be asked to provide additional security questions based on your okta configuration
- Once successfully logged in you should be return to the AWS AWS IAM Identity Center start page
- Click on AWS Account (1)
    - Click on the name of your Management account
    - On the line Billing click the link Management Console
    - A new tab should open and display the Billing & Cost Management Dashboard for your organization.

Deleting AWS resources deployed in this lab

In the Management account:

- In the AWS IAM Identity Center Dashboard
    - In the Identity Source section, in the row Identity Source, click the Change link.
    - Change identity source
        - Select AWS IAM Identity Center,
        - click Next: Review
    - Review and confirm
        - Review the information provided
        - Type CONFIRM in the field at the bottom
        - click Change Identity source
    - Once the reconfiguration has completed click Return to settings
- In the Okta console,
    - delete the app: AWSS: `Your Organization`
    - delete the user:
        - `alias`@`realm`.local
    - delete the groups:
        - `alias`*AWSFinOpsUsers*
        - *AWS Users*
- Close the Okta account [optional]