Centralizing Authentication with AWS IAM Identity Centre

Table of Contents

1. Objective
2. Project Scope
3. Architecture Diagram
4. Basic Explanation about POC
    - Why Use AWS IAM Identity Centre?
    - Why AWS IAM Identity Centre is Perfect for Enterprise SSO
5. Let's Set It Up
    - Enable AWS IAM Identity Centre
    - Configure AWS Organizations
    - Initial Identity Centre Configuration
6. Setting Up Okta with AWS IAM Identity Centre
    - Attribute Mapping Setup
    - Step-by-Step Setup
    - SCIM Setup (Automatic User Sync)
    - Test the Setup
7. Setting Up SSO Authentication Logging and Monitoring
    - Set Up Basic Logging
    - Set Up Basic Alerts
8. Security Hardening Guide for IAM Identity Centre
    - Basic Security Settings
    - IP Restrictions Setup
    - Guard Duty.
9. IAM Access Analyser.
10. Load Testing & Scalability for IAM Identity Centre
    - Testing Different User Loads
    - Multi-Account Testing
11. AWS IAM Identity Centre Cost & Scaling

- Base Service Costs
- AWS IAM Identity Centre Cost Estimate

1. 🎯 Objective

To implement a robust, scalable Single Sign-On (SSO) solution using AWS IAM Identity Center that will:

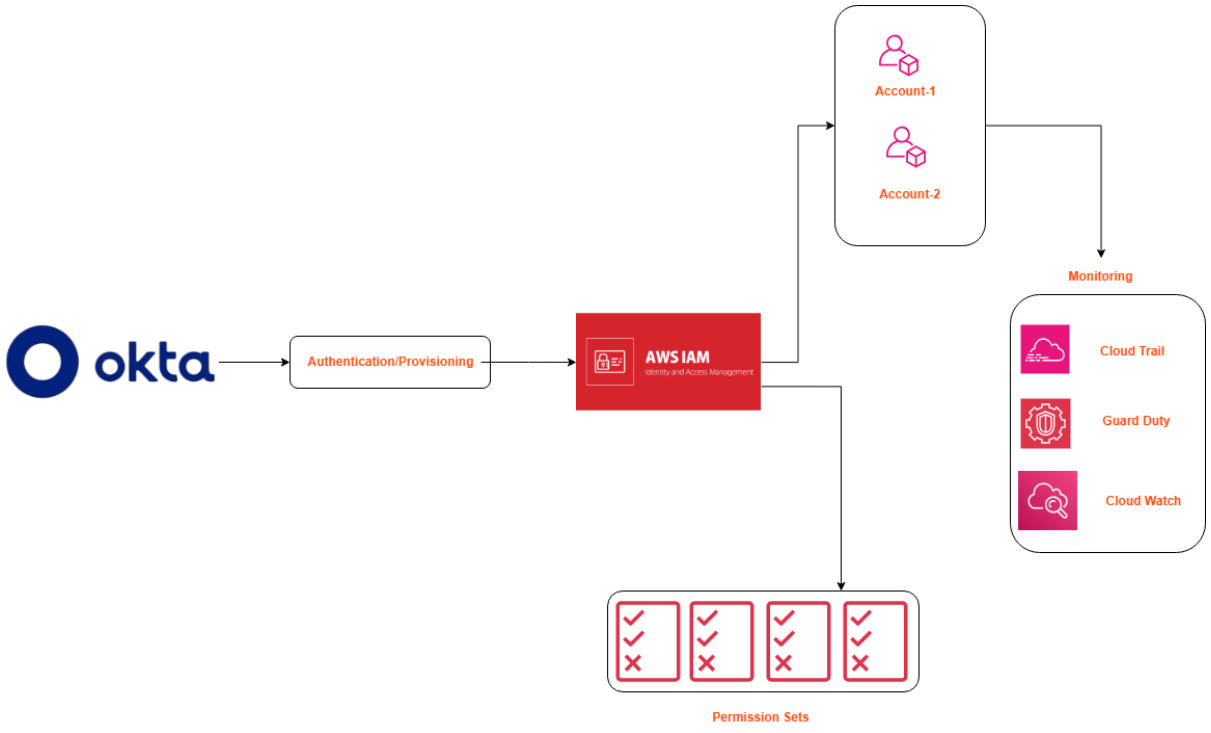
- **Simplify** access management across multiple AWS accounts
- **Secure** enterprise resources with centralized authentication
- **Streamline** user experience with one-click access
- **Standardize** identity management practices

2. 🔍 Project Scope

In Scope ✅

- Implementation of AWS IAM Identity Center as primary SSO solution
- Integration with Okta as Identity Provider
- Multi-account AWS access management
- User/Group permission mapping
- Security monitoring and logging setup
- Performance testing and optimization

3. Architecture Diagram



4.Basic Explanation about POC

4.1 Why Use AWS IAM Identity Centre?

1. IAM Federated Access

IAM Identity Center	IAM Federated Access
✅ Built-in user portal	❌ No unified portal
✅ Simplified permission sets	❌ Complex IAM role management
✅ Direct integration with major IdPs	⚠️ Requires custom federation setup
✅ Centralized multi-account access	⚠️ Per-account configuration needed

2. AWS Cognito

IAM Identity Center	Amazon Cognito
✅ Enterprise-focused	⚠️ Customer/application-focused
✅ Built for AWS resource access	❌ Primarily for app authentication
✅ Native AWS Console integration	❌ No direct console access
✅ Simplified compliance	⚠️ Requires additional setup for compliance

4.2Why Identity Center is Ideal for Enterprise SSO

1. Enterprise-Ready Features

- Pre-built integrations with major IdPs
- Automated user provisioning (SCIM)
- Granular permission management

2. Operational Efficiency

- Single dashboard for all AWS accounts
- Automated access provisioning
- Reduced administrative overhead

3. Security & Compliance

- Centralized access controls
- Built-in audit trails

- Automated access reviews

4. Cost-Effective

- No additional charges for the service

4.3 Business Benefits

🔒 **Enhanced Security**

- Reduced security risks through centralized access control
- 90% reduction in password-related security incidents
- Real-time access revocation capabilities
- Automated security compliance reporting

💰 **Cost Optimization**

- 30-40% reduction in IT administrative costs
- Zero additional licensing fees for AWS IAM Identity Center
- Reduced help desk costs for password resets
- Minimized overhead for access management

⚡ **Operational Efficiency**

- 75% faster user onboarding/offboarding
- Single dashboard for multi-account management
- 5x faster access provisioning
- Automated workflows for access requests

👥 **Improved User Experience**

- One-click access to all AWS resources
- Zero password fatigue with SSO
- Self-service access management
- Seamless integration with existing tools

📊 **Compliance & Governance**

- Automated audit trails
- Simplified compliance reporting
- Standardized access policies

- Enhanced visibility into user activities

🚀 **Scalability**

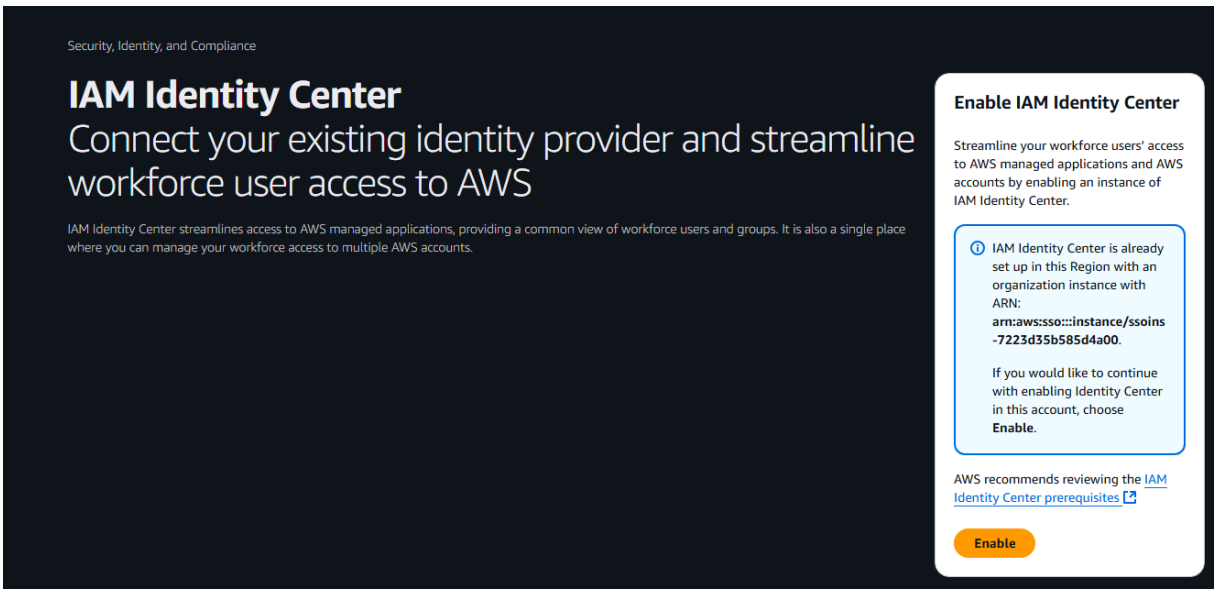
- Effortless scaling across AWS accounts
- Quick integration with new applications
- Flexible user management for growing teams
- Future-proof identity solution

5. Let's Set It Up

5.1 Enable AWS IAM Identity Center

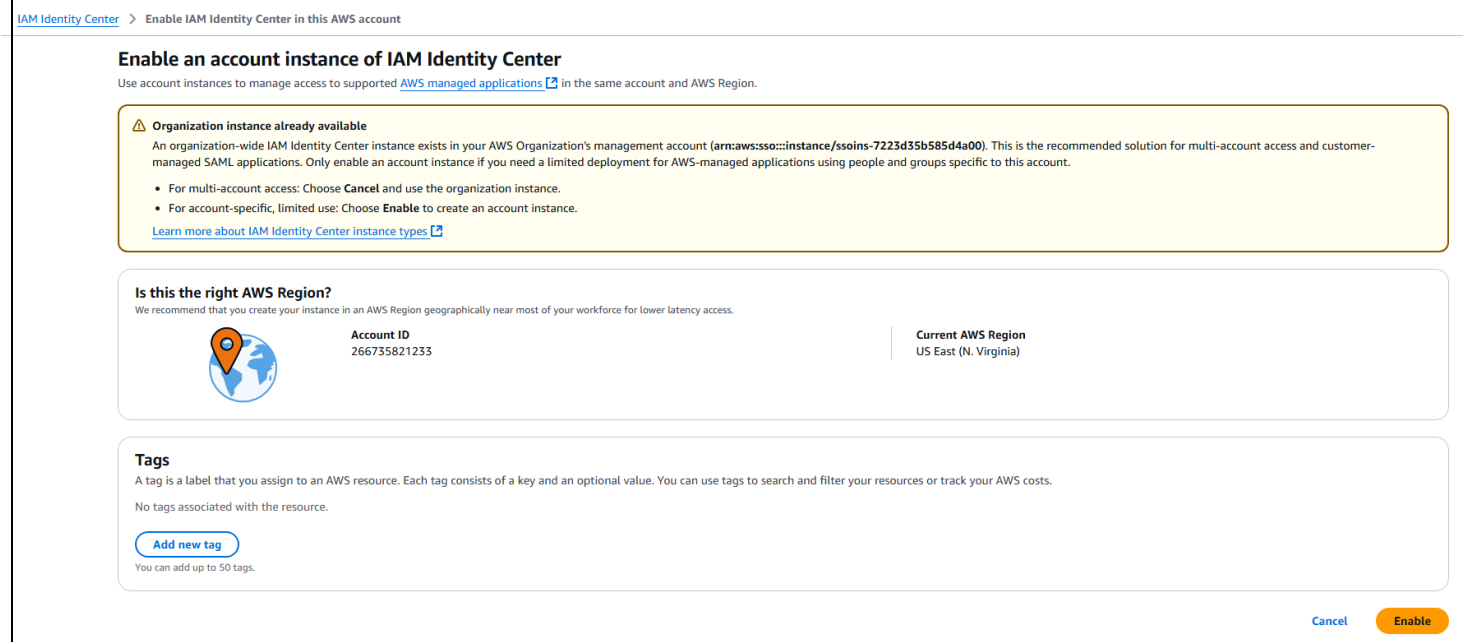
1. Log into AWS Console

- Go to AWS Console
- Sign in as Root user or IAM admin

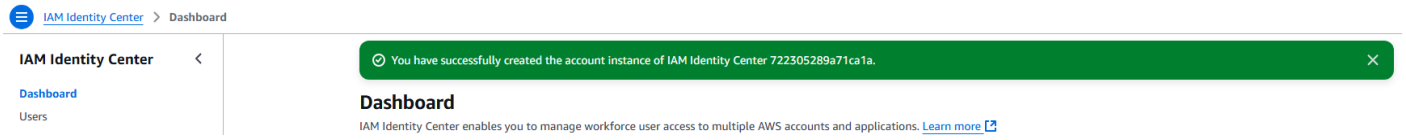


2. Navigate to IAM Identity Center

- Search for IAM Identity Center in the AWS Console



- Click Enable IAM Identity Center



Note:

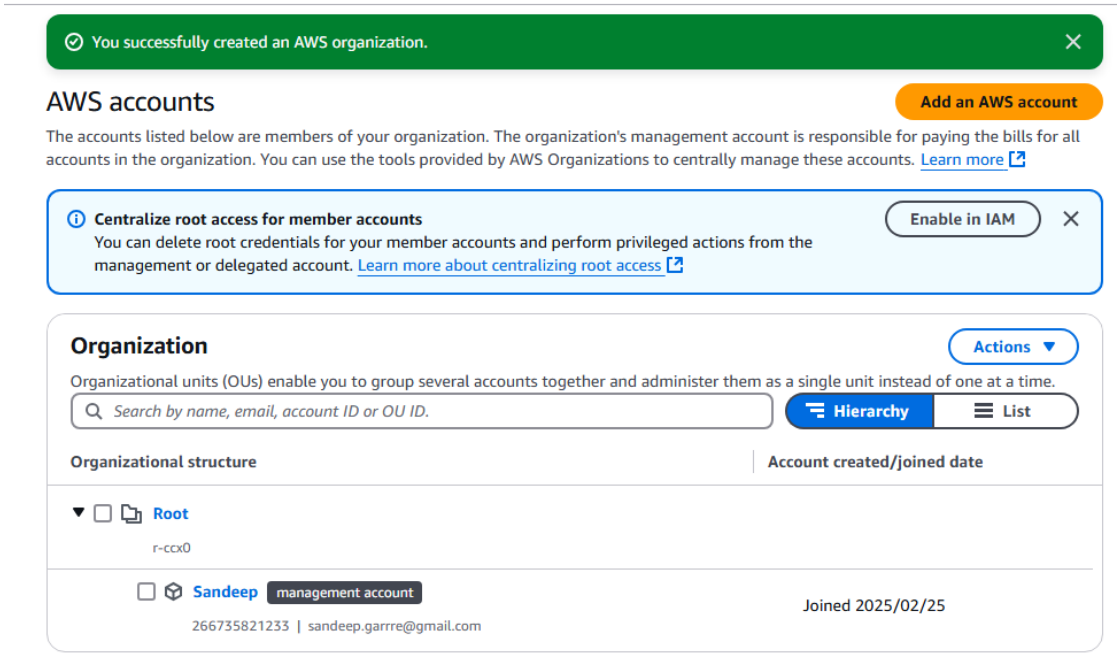
Once enabled, IAM Identity Center creates a service-linked role in all accounts within the organization in AWS Organizations. IAM Identity Center also creates the same service-linked role in every account that is subsequently added to your organization. This role allows IAM Identity Center to access each account's resources on your behalf.

5.2 Configure AWS Organizations

- In the **AWS Console** at the top left corner next to **Services** click into the search box and type **AWS Organizations** and click on that service.

- Click **Create Organization**. By default, the organization is created with all features enabled.

- The organization is created and the **AWS accounts** page appears. The only account present is your management account, and it's currently under the root organizational unit (OU)



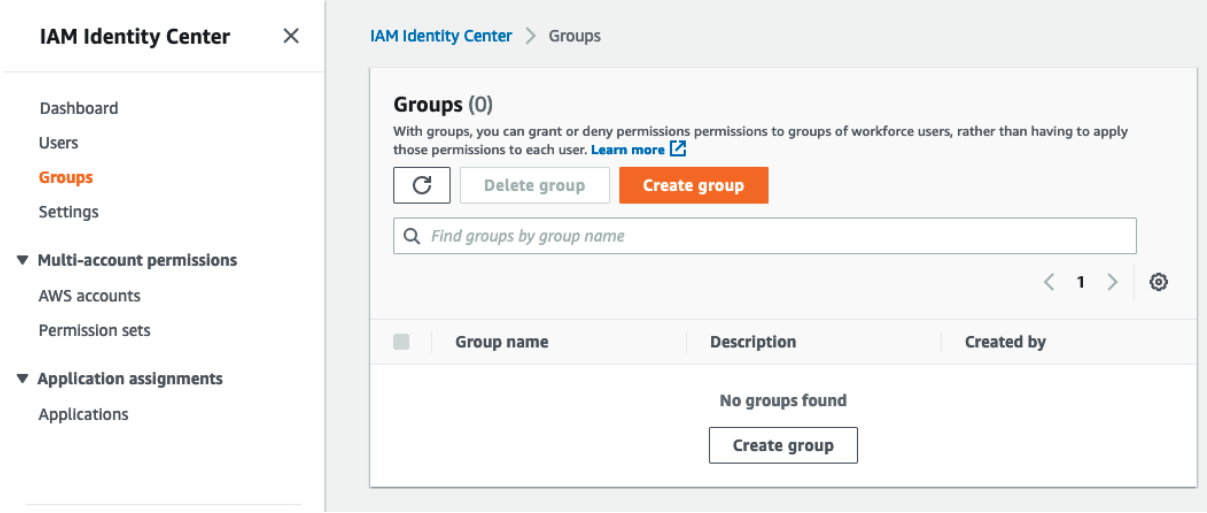
5.3 Initial Identity Centre Configuration

5.3.1 Create User and Groups

Create Groups

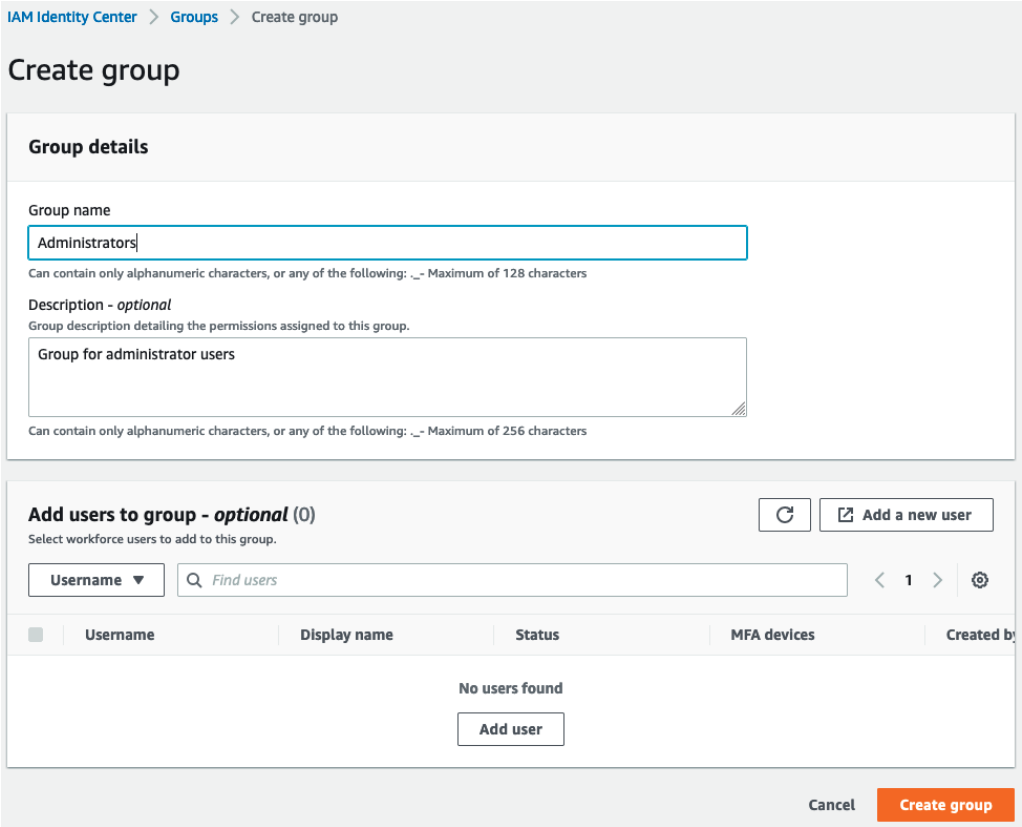
1.Navigate to the IAM Identity Centre.

2.Choose **Groups** and click **Create Group**.



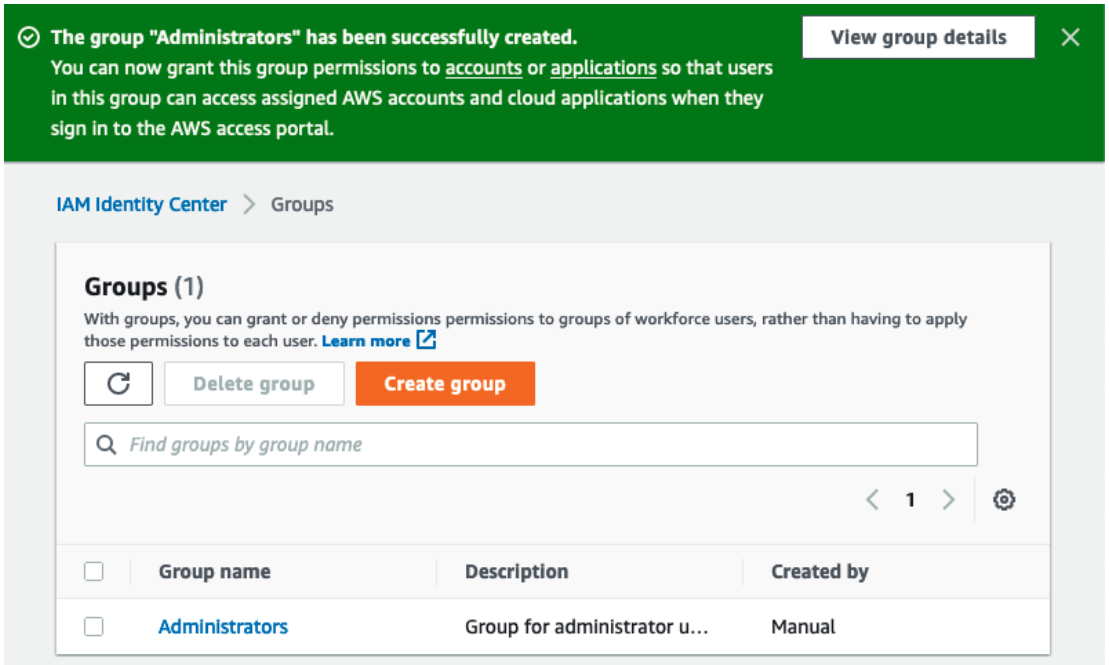
3.In the **Create group** page:

- Provide a **Group Name** , example Administrators



- Provide a **Description** , example Group for administrator users
- Click Create Group.

4.A green banner will appear indicating that the **Administrators** group was successfully created

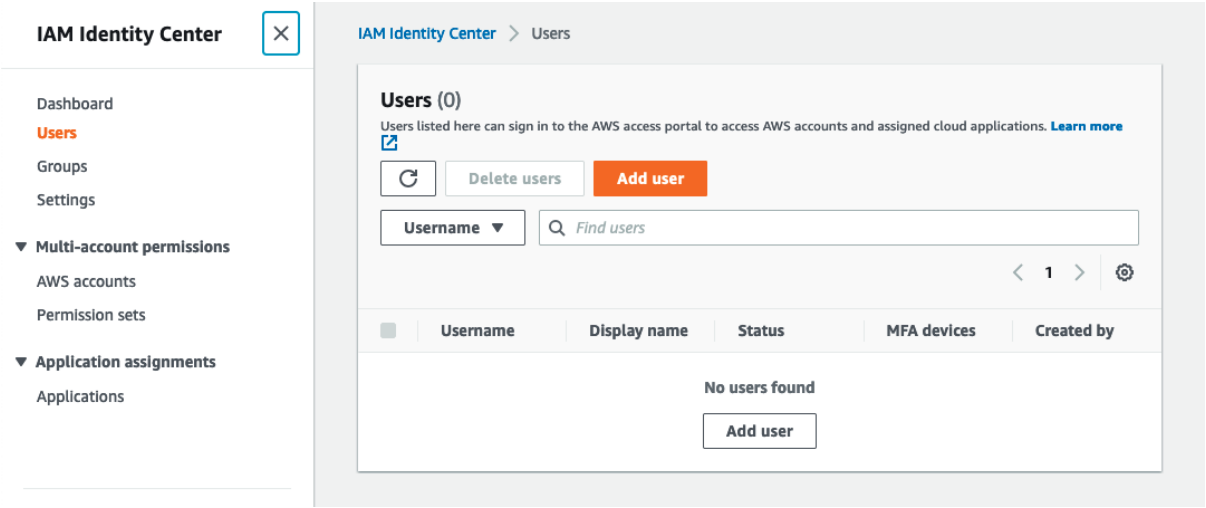


Create Users

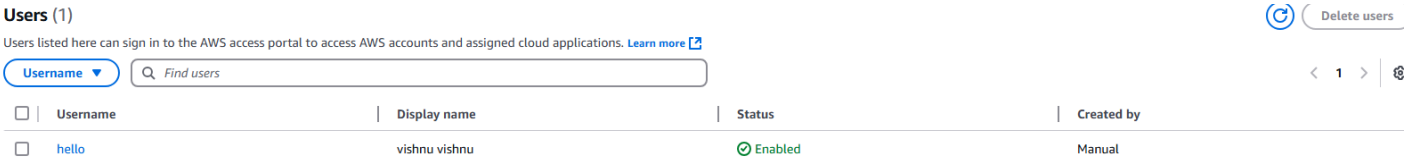
1.Choose Users under Workplace pool and click Add User.

2.In the Add User page:

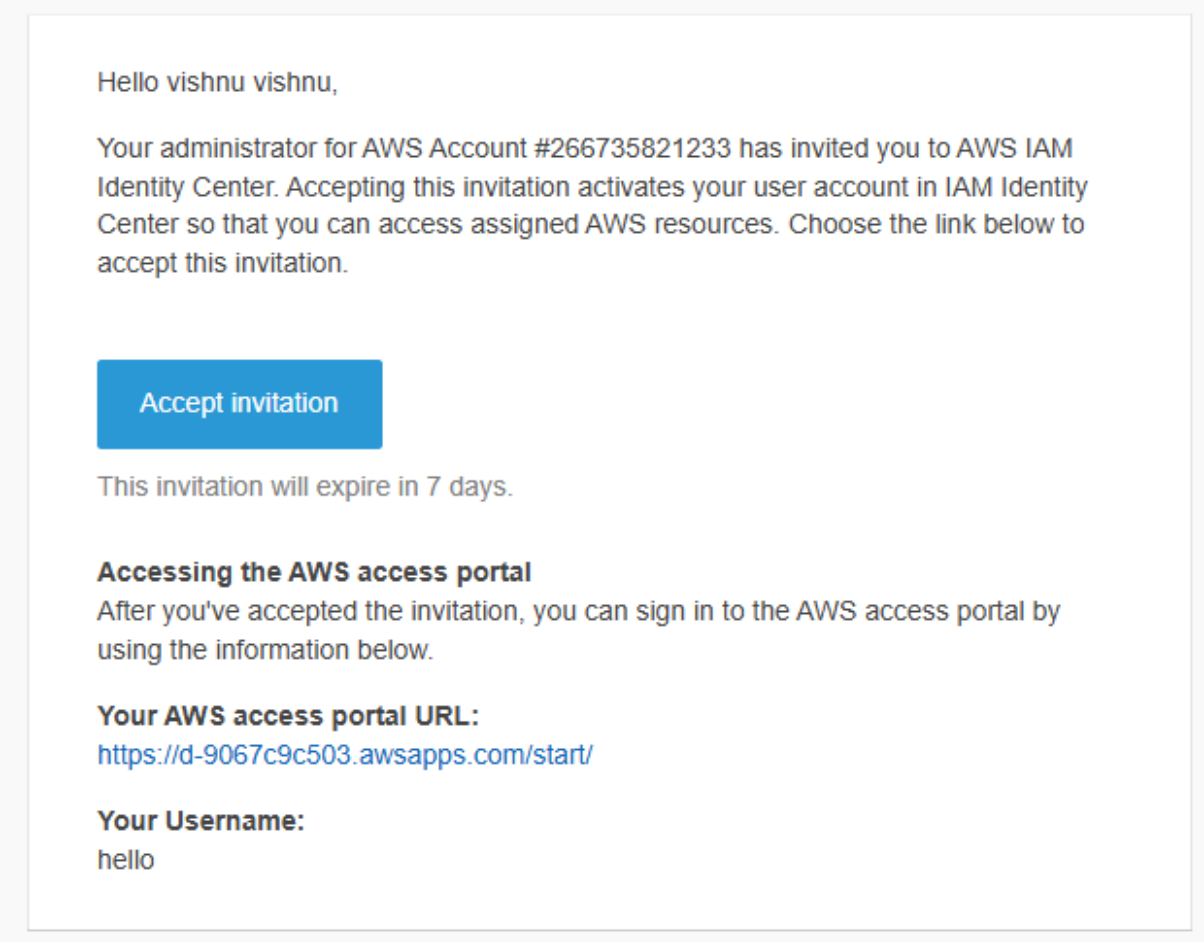
- Provide a Username, example **hello**
- For Password choose Generate a one-time password that you can share with the user radio button
- Provide an Email Address, use the format email+admin@domain.com



- Confirm the same email address provided in the previous field
- Provide a **First name**
- Provide a **Last name**
- Leave Display name as entered



- Once You created successfully an email is sent to your registered email address.



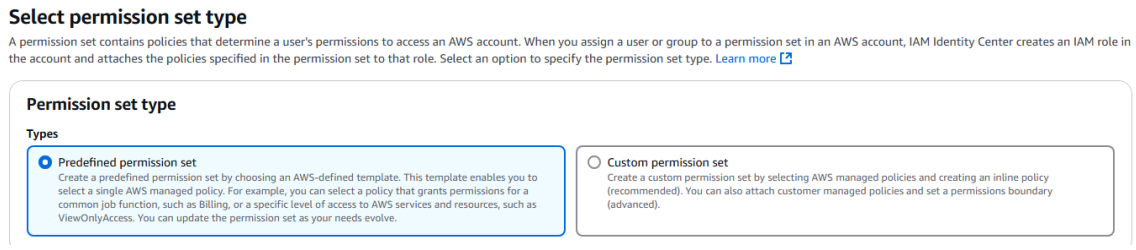
- Click on Accept Invitation and it will shows you to create new password and a green tag shows like user successfully created.

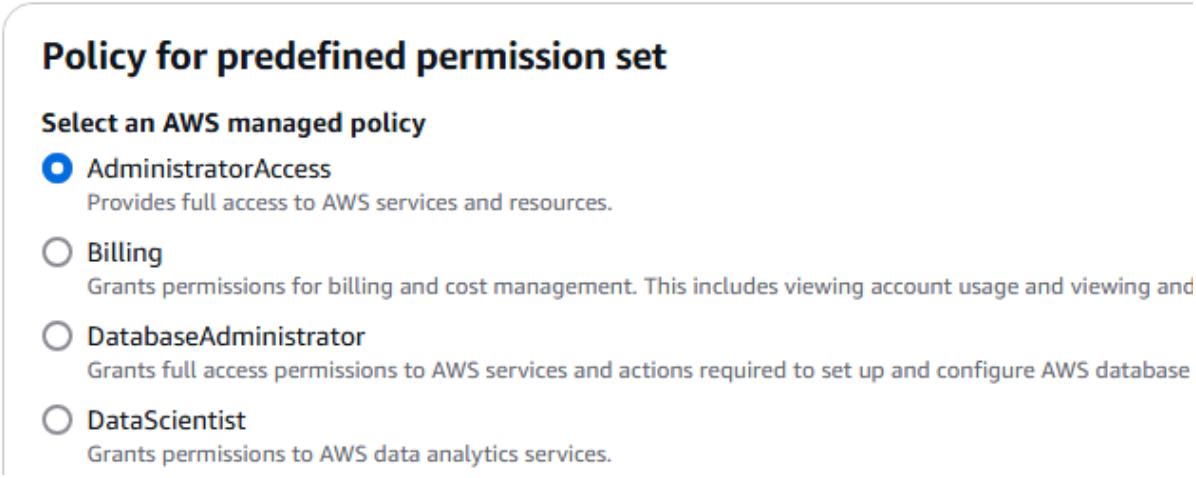
5.3.2 Create Permission Sets

1.Click on **Permission sets** on the left menu under Multi-account permissions and Click on **Create permission set** button.

2.On the **Select permission set type** page

- Under Permission set type, choose **Predefined permission set**.
- Under **Policy for predefined permission set**, select an AWS managed policy **AdministratorAccess** then click **Next**.

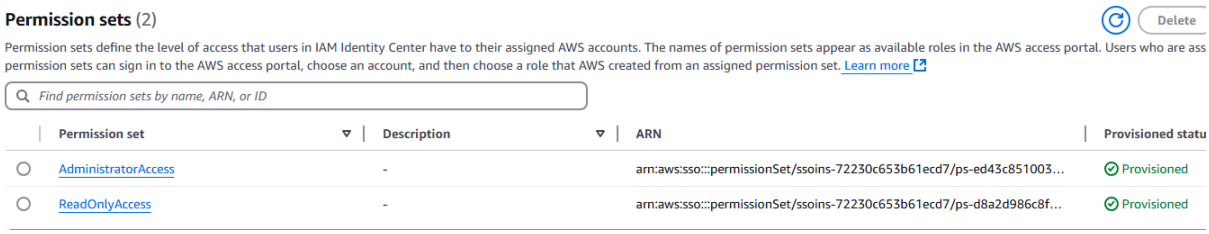




3.On the **Specify permission set details** page, keep all defaults.

4.Click **Next**.

5.On the **Review and create page**, review the selections that you made, and then click **Create**.



5.3.2 Provision Permission Sets

1.Choose **AWS accounts** and select an account where you want the user to have access. Click **Assign users or groups**.

2.In **Select users and groups** page, choose **Groups**, select **Administrators** and click **Next**

3. In Select permission sets page,

- Under Permission sets, select AdministratorsAccess
- Click next

4.In **Review and submit** page, review the information and click **Submit.**

5. IAM Identity Center will now associate the User group with the Permission set and assign it to the select AWS Account(s). You should see a page with **green** banner like below.

5.3.3 Testing the access based on user, group and permission set assignments

Create Permission Sets

1. Go to AWS IAM Identity Center console

2. Click on "Permission sets"

3. Create First Permission Set:

- Click "Create permission set"
- Select "Predefined permission set"
- Choose "AdministratorAccess"
- Name: " AdministratorAccess "
- Click "Create"

4. Create Second Permission Set:

- Click "Create permission set"
- Select "Predefined permission set"
- Choose "ReadOnlyAccess"
- Name: "ReadOnlyAccess"
- Click "Create"

Create User

1. Go to "Users" in IAM Identity Center

2. Click "Add user"

3. Create User:

- Username: teja

- Email: narravula070@gmail.com

- First name: Teja

- Last name: User

- Click "Next" and "Add user"

2. Assign Access 📋

Assign Permission Sets to Groups

1. Go to "AWS accounts"

2. Select your AWS account

3. Click "Assign users or groups"

4. For AdminGroup:

   - Select "Groups"

   - Choose "AdminGroup"

   - Select "AdminAccess" permission set

   - Click "Submit"

5. For ReadOnlyGroup:

   - Select "Groups"

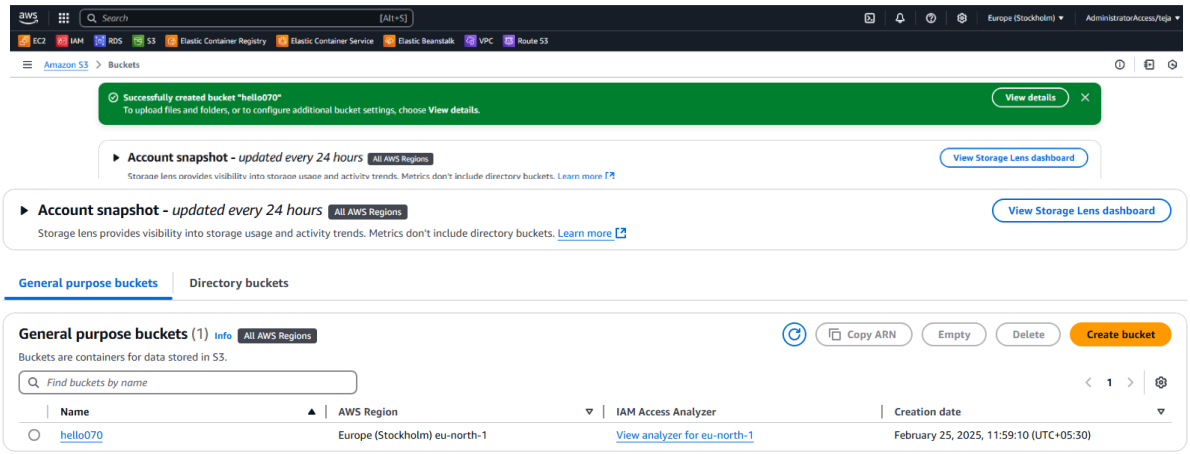
   - Choose "ReadOnlyGroup"

   - Select "ReadOnlyAccess" permission set

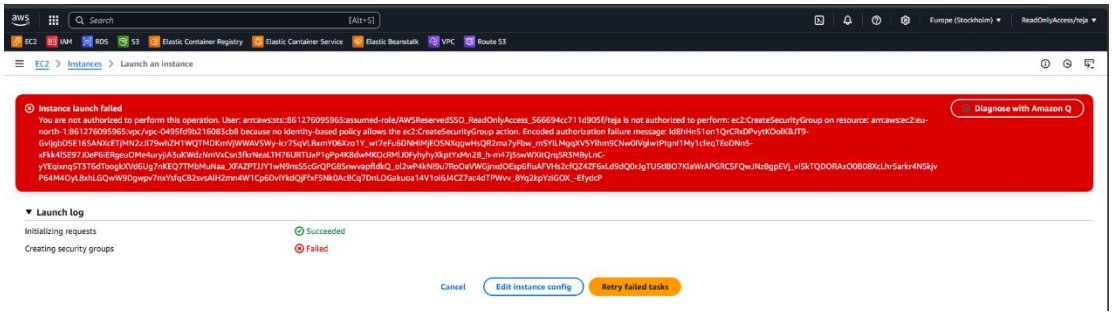
   - Click "Submit"

3. Testing Process 🔍

- Here first you login as “Teja” with Admin permission set you have permissions to create s3 bucket.

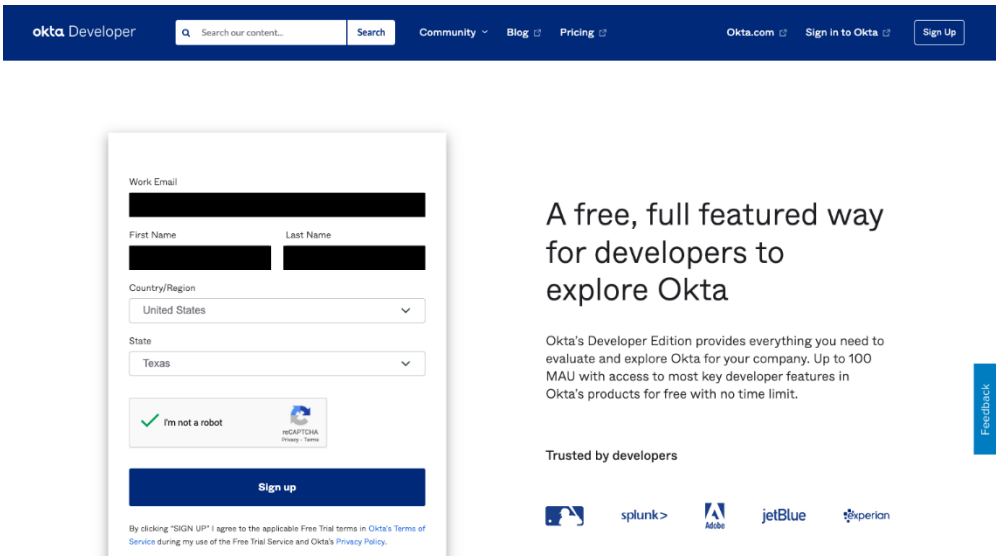


- Now it's time to login as "Teja" with ReadOnly permissions and you getting an error message as below shown in image.

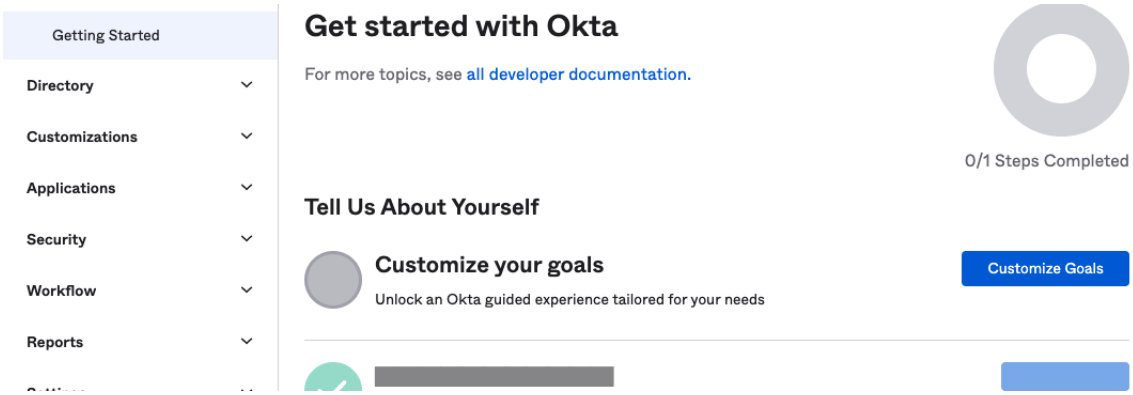


6. Setting Up Okta with AWS IAM Identity Centre

- Create Okta developer free version.
- Fill out the details to create a free account.



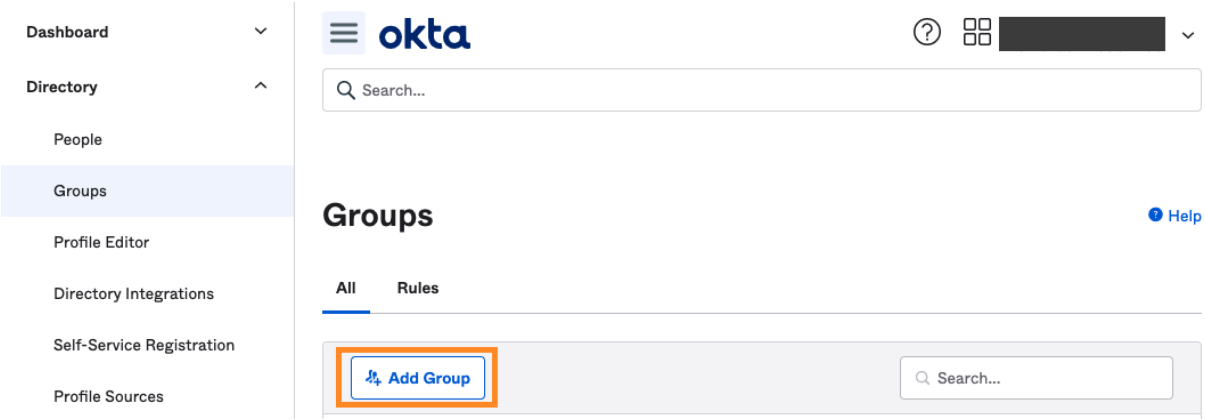
- You should be navigated to a sign-up confirmation page.
- Check your email to click the activation link to activate the Okta developer account
- Set your password to successfully finish creating your account.
- You should be redirected to your Admin dashboard.



Create Users/Groups

Create Groups:

- Navigate to the Directory section on the left-hand side of the page.
- Choose Groups
- Click on Add Group button

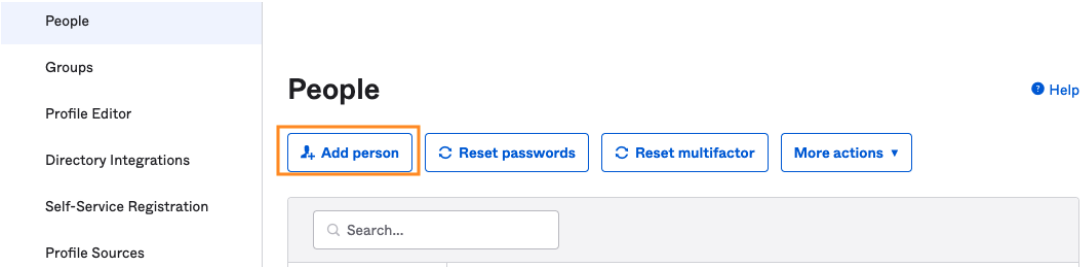


In the Add Group dialog:

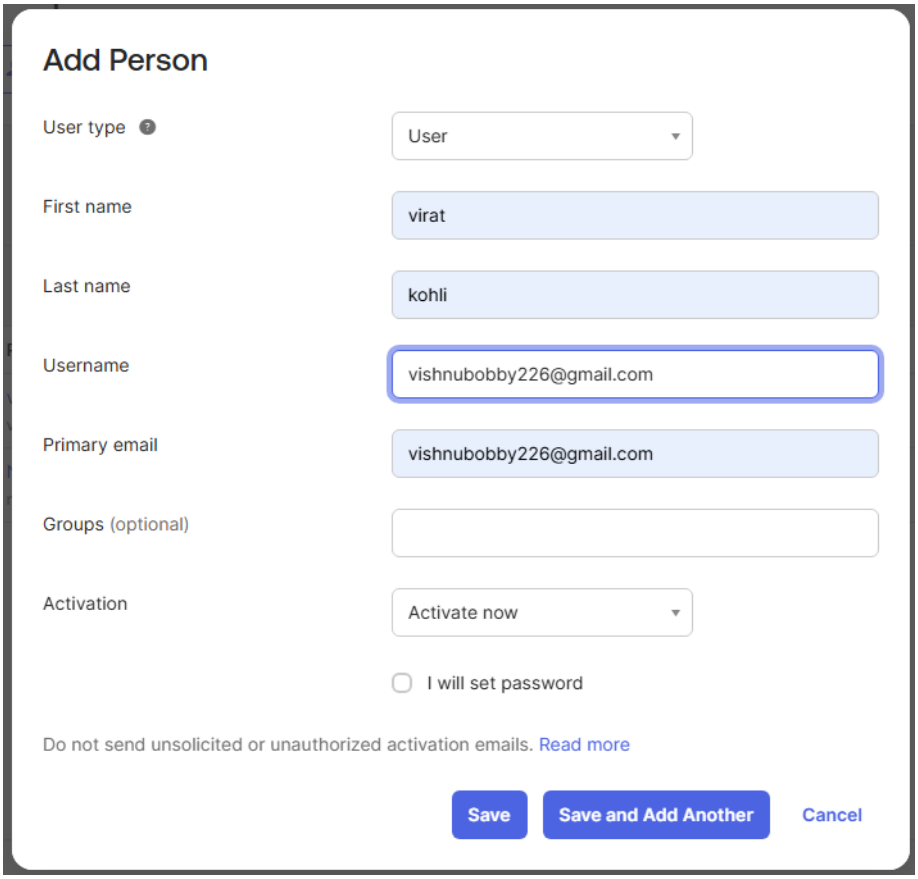
- Provide the name of the group <Group Name>
- Provide the description for the group.

Create User:

- Navigate to the Directory section on the left-hand side of the page.
- Choose People
- Click on **Add person** button

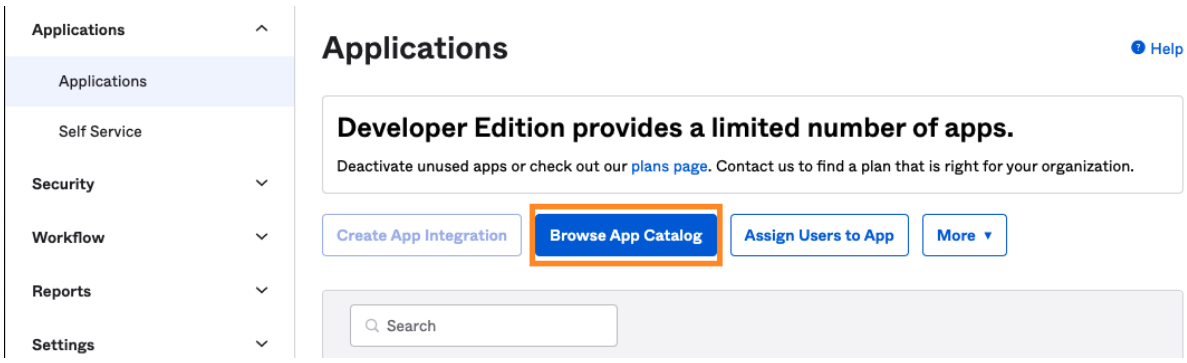


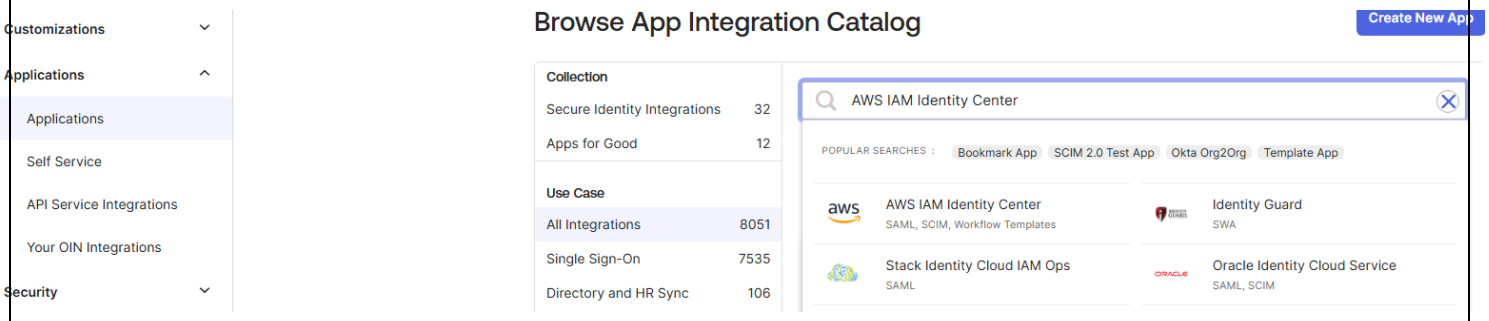
- Fill the User Details as shown in below image.

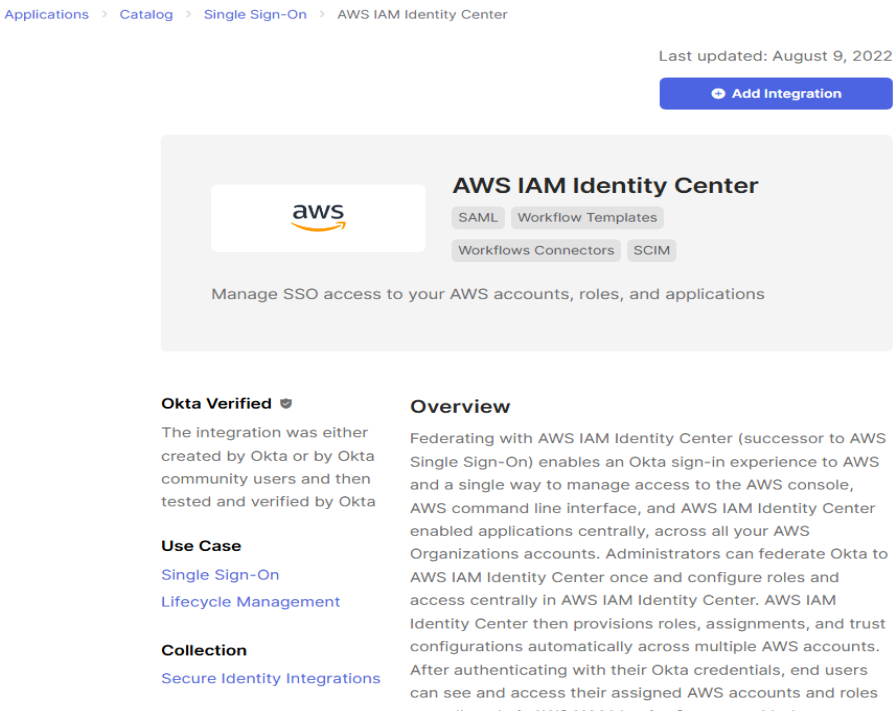


6.1 Create IAM Identity Centre Application in Okta

- Navigate to the Applications section on the left-hand side of the page.
- Choose Applications
- Click on Browse App Catalog button

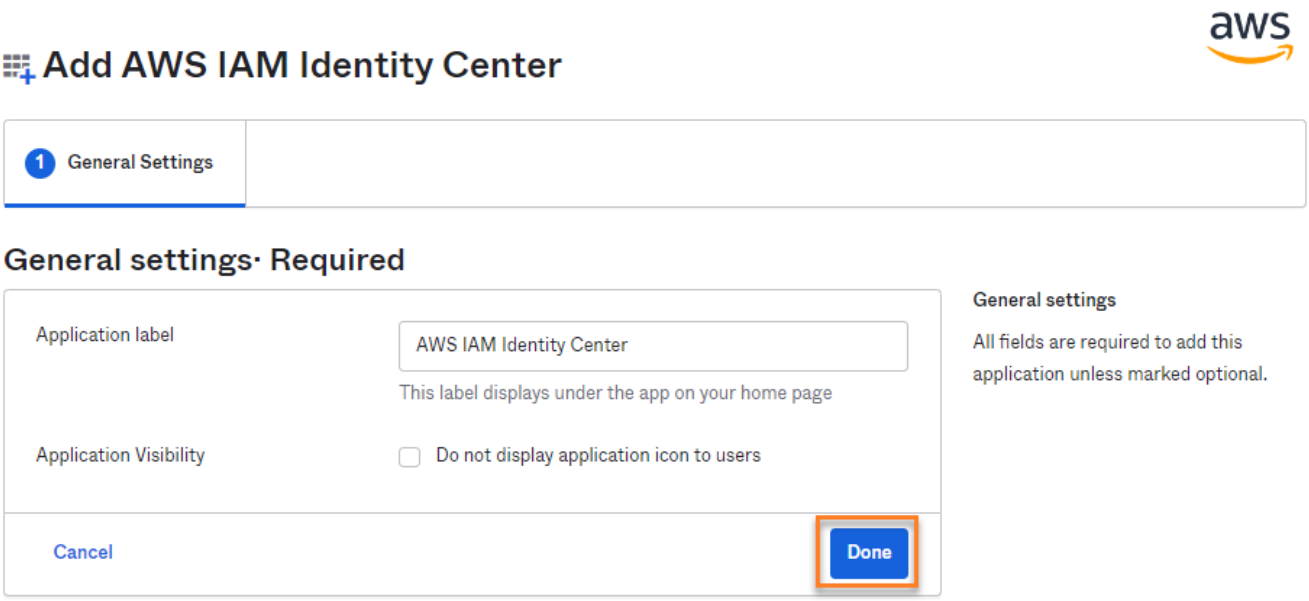






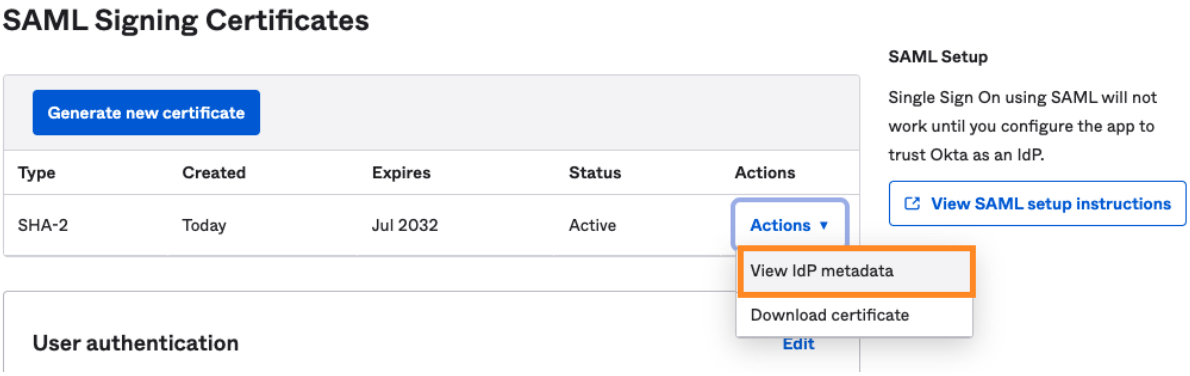
In the Browse Application Integration Catalog page:

- Search for AWS IAM Identity Center
- Select AWS IAM Identity Center App and Click on the Add Integration button
- In the application Wizard page for the Application
- Click on Done Button.



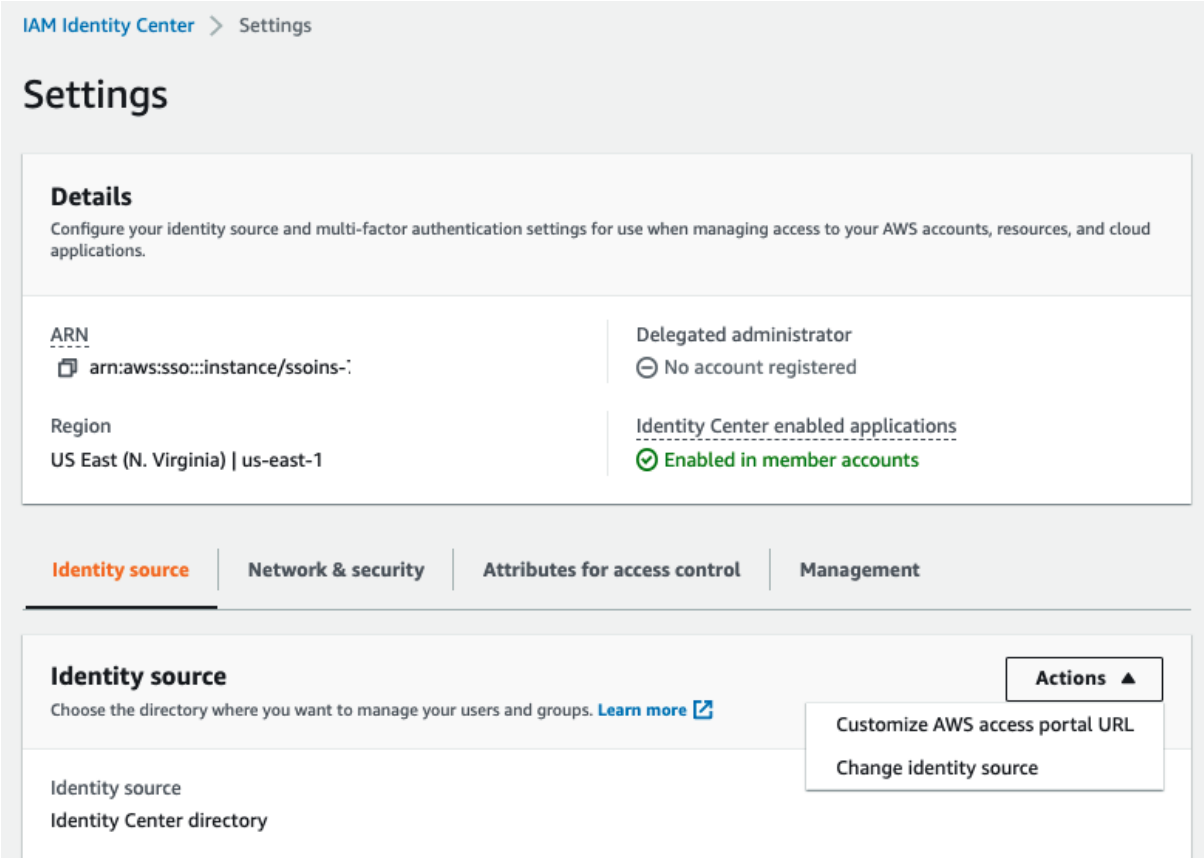
Navigate to the Sign On tab

- Under the SAML Signing Certificates section, from the **Actions** drop-down menu, right-click on **View IDP metadata** and save the link as okta_metadata.xml to a file locally.



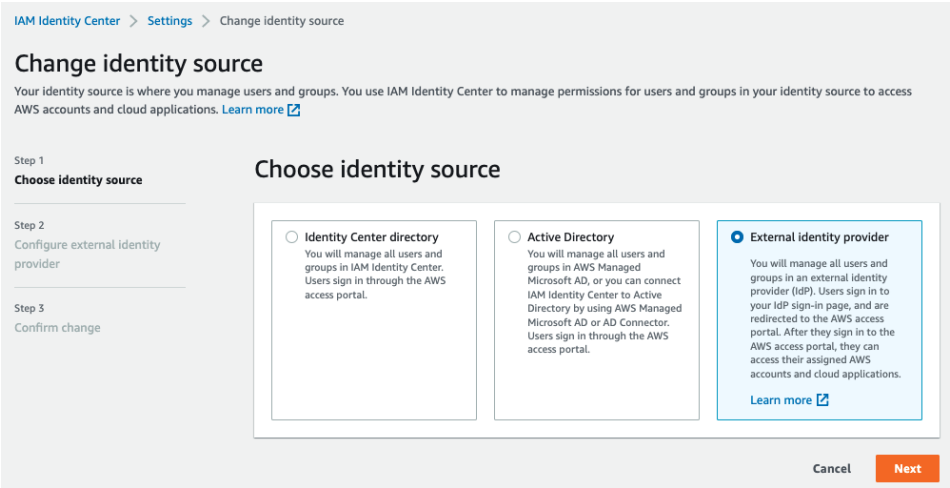
6.2 Change the Identity source in IAM Identity Centre

- Navigate to IAM Identity Centre in AWS Console.
- Select Settings from the left menu
- In the Setting page , Choose **Change Identity Source** from **Actions** drop-down menu



In the **Choose identity source** page:

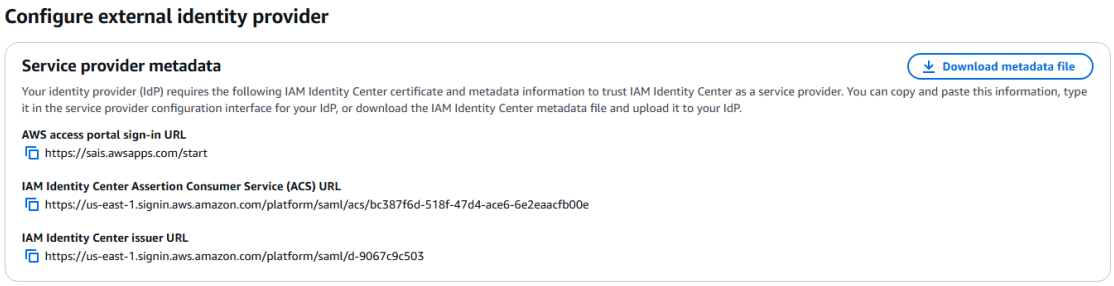
- Choose External identity provider



- Click on next

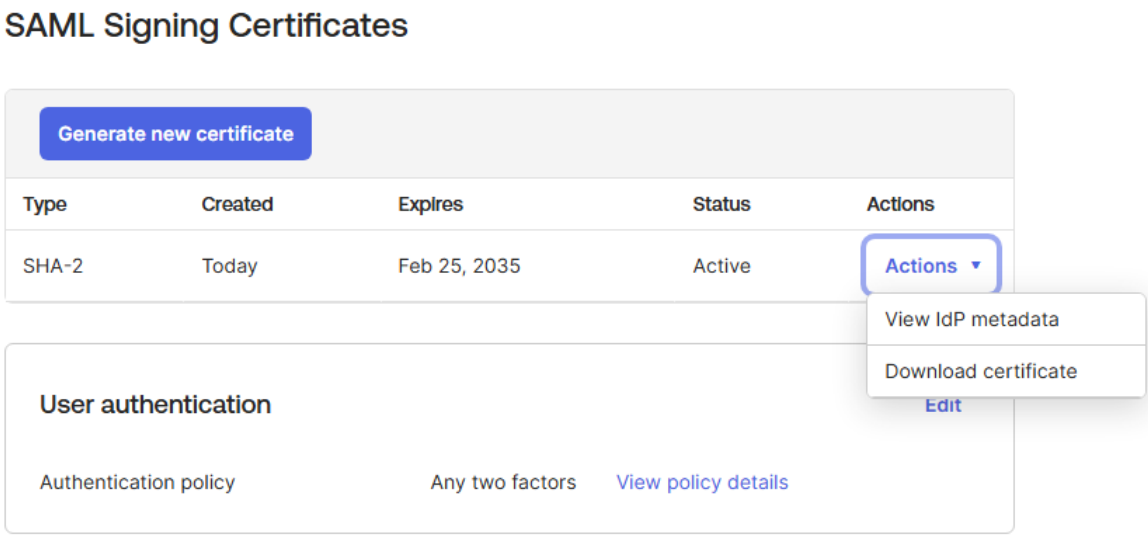
In the **Configure external identity provider** page:

- Make a Make a copy of the **IAM Identity Center ACS URL**, and **IAM Identity Center issuer URL** values in the Service provider metadata section. These values will be used later.



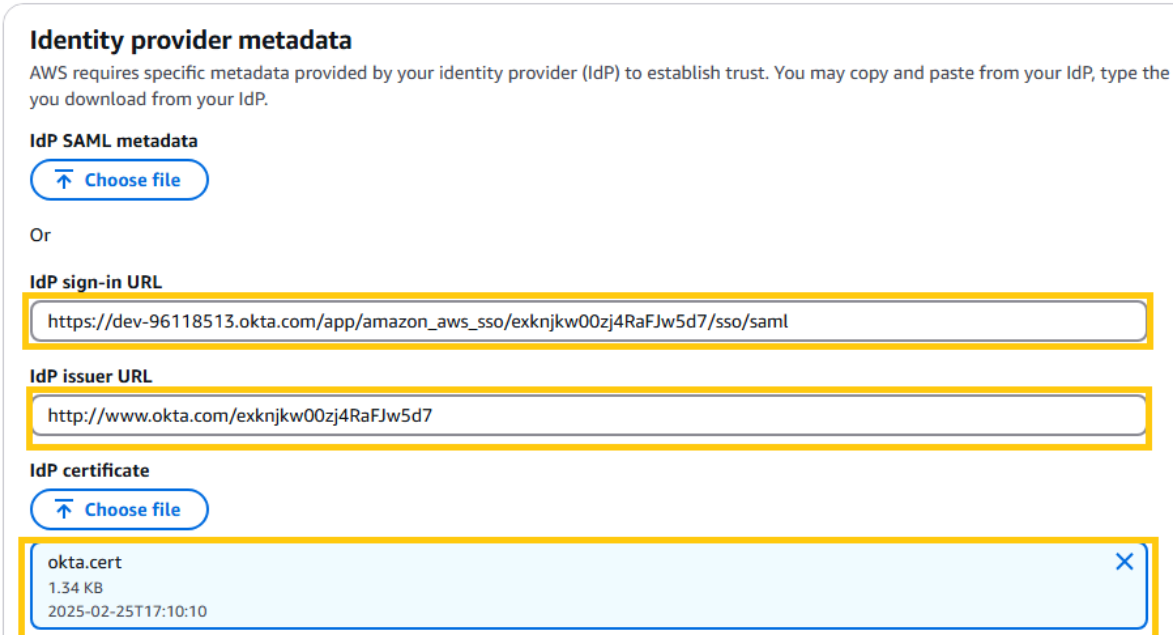
In the **Identity provider metadata** section.

- Fill the details **IdP sign-in URL** and **IdP issuer URL and IdP Certificate.**
- Get these details in Okta.

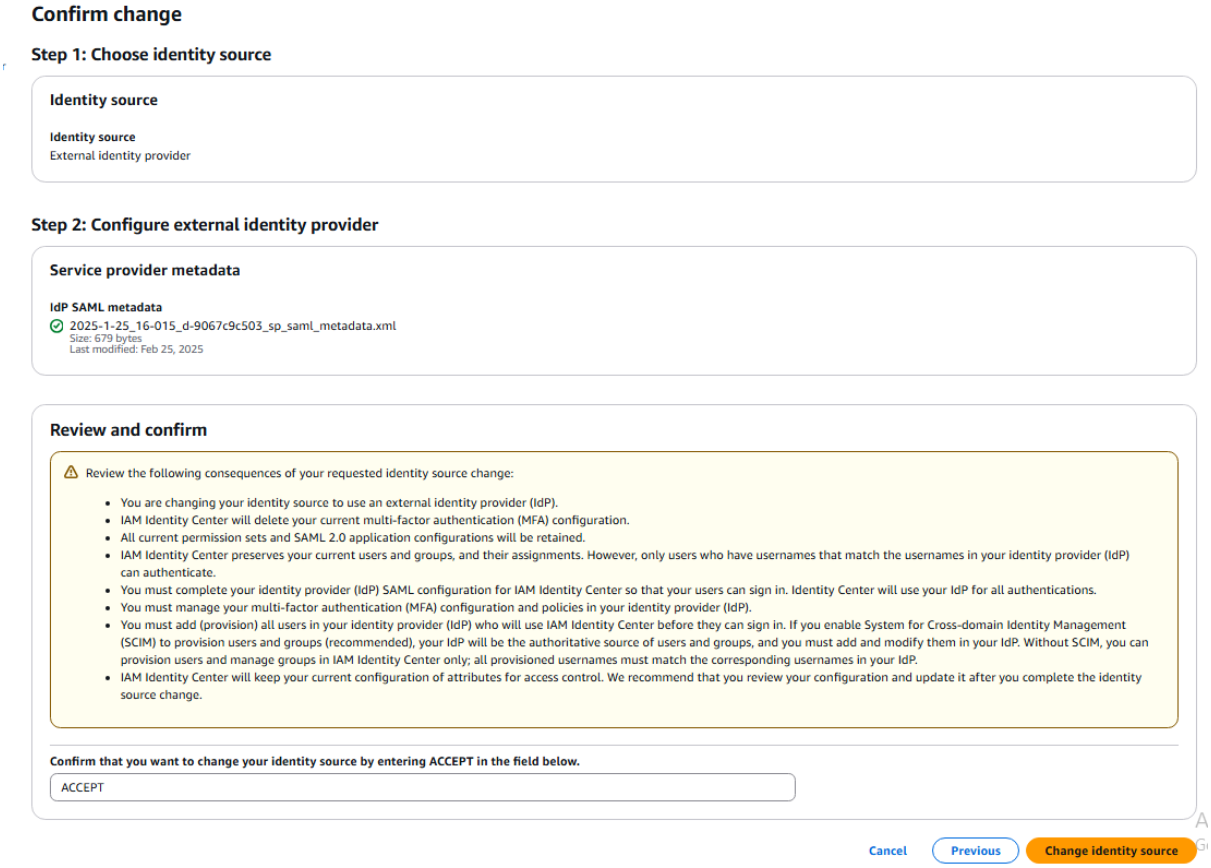


- Click on View IdP metadata it will appear like this

- Copy and paste the URL's in AWS Identity Centre.



In the **Confirm change** page:

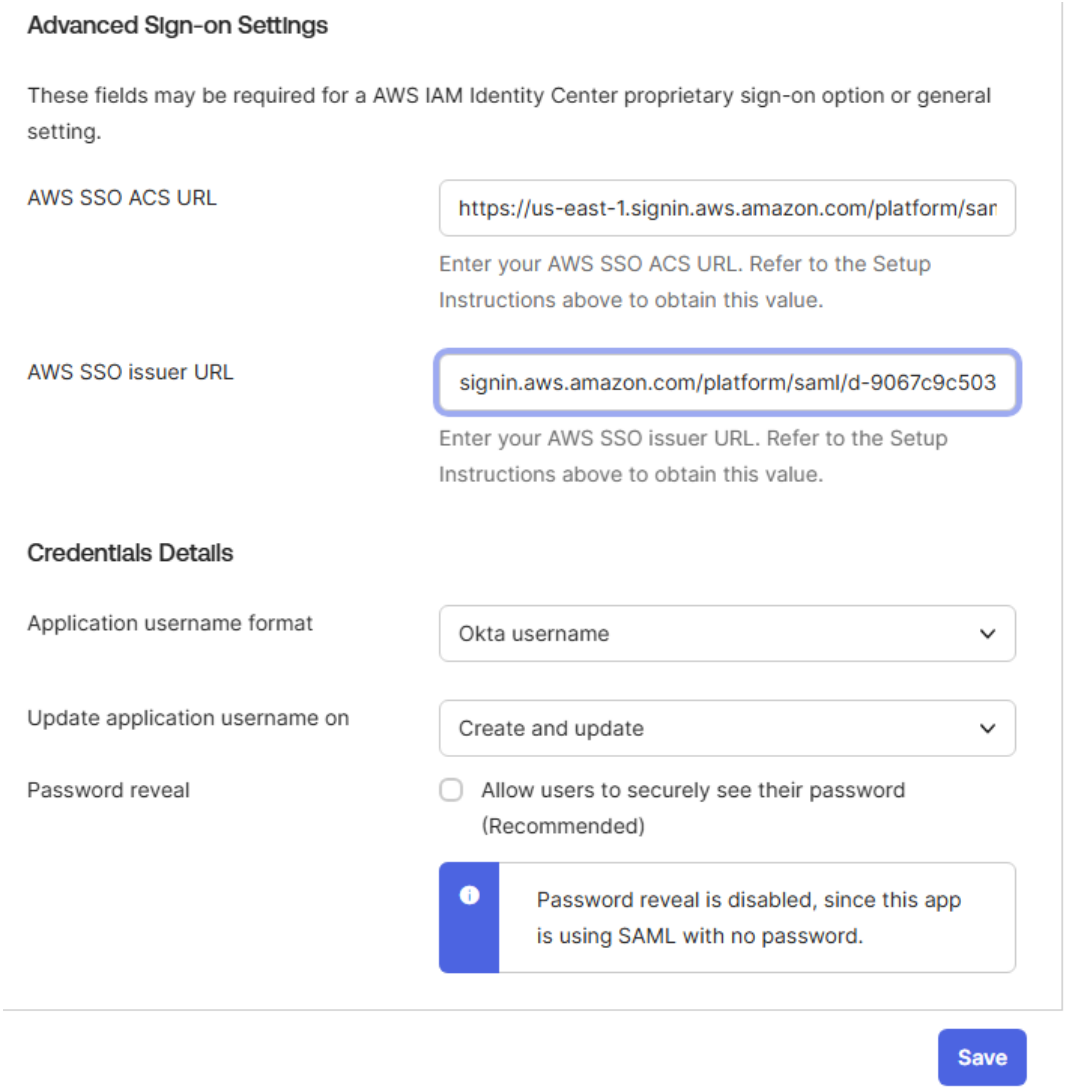


- Type **ACCEPT** and Change identity source

6.3 Configure IAM Identity Centre Sign-on Configuration.

In the AWS Single Sign-on App page

1. Navigate to the Sign On Tab, click on the **Edit button**
2. Under the Advanced Sign-on Settings section
   - Enter your **IAM Identity Center ACS URL** and **IAM Identity Center issuer URL** values you made a copy in Step 5 in previous section
   - Leave the Credentials Details Configuration as to default selections.

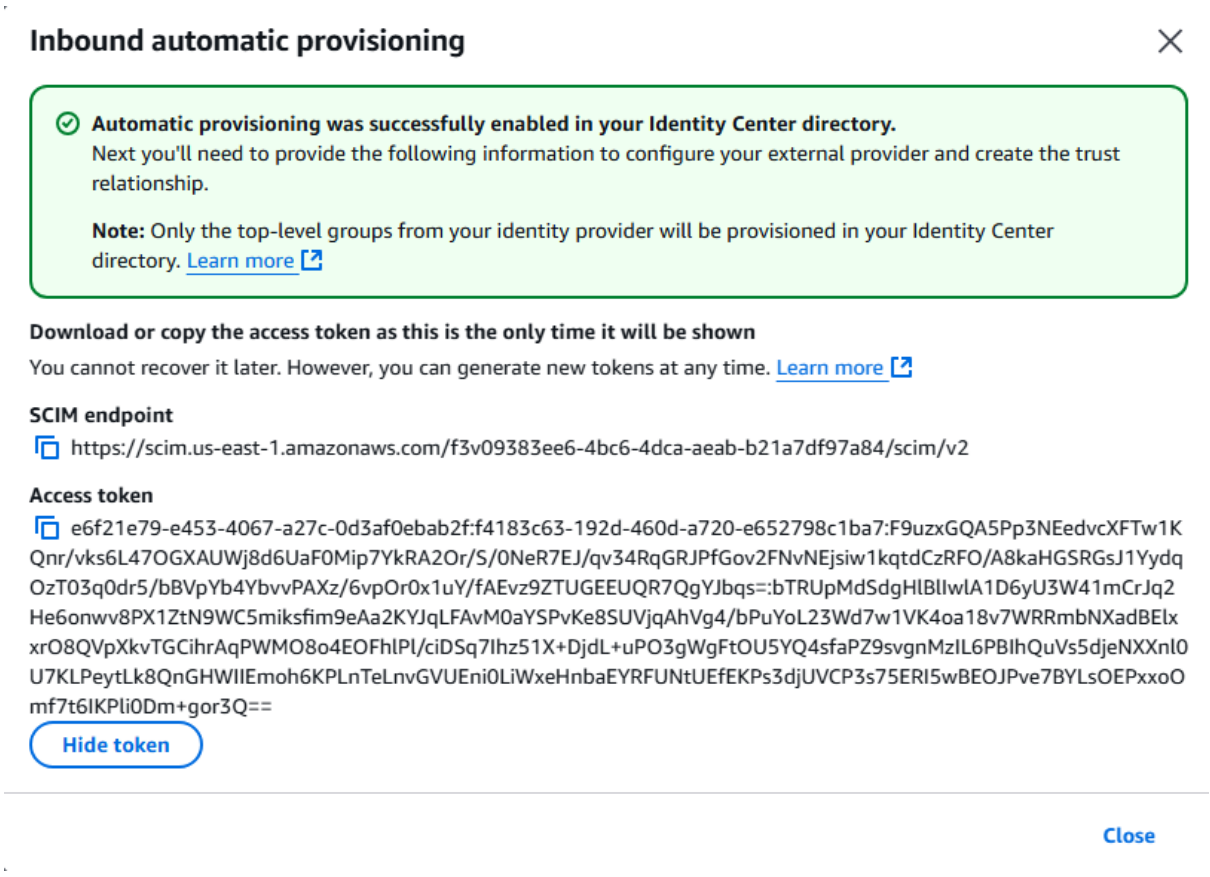


3. Click **Save**

6.4 Configure provision in Okta

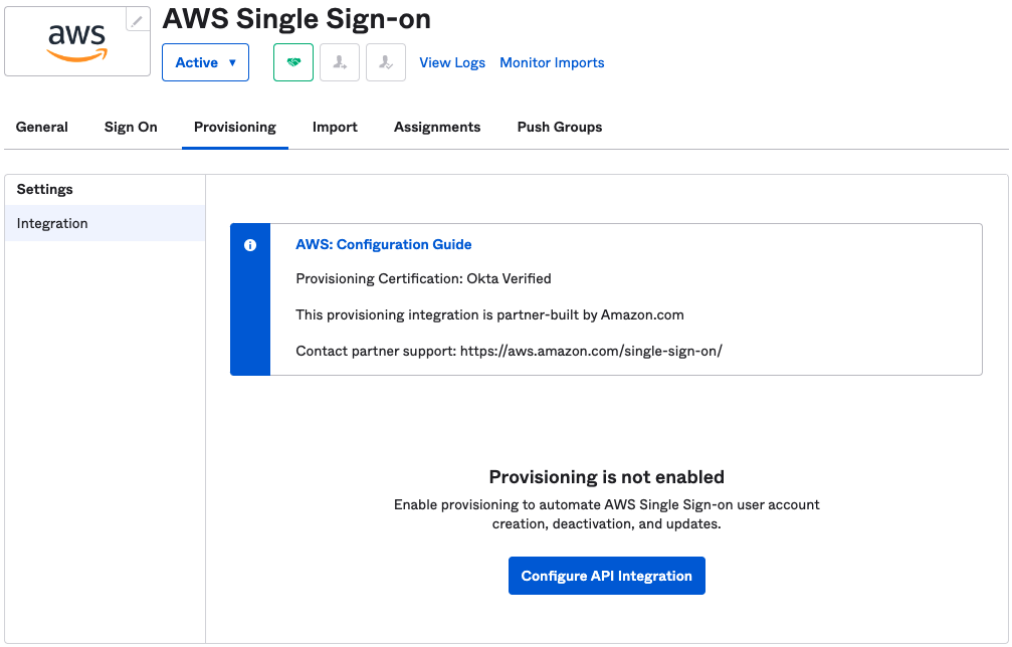
Here you will configure SCIM to enable the users and groups from Okta to be automatically sync ‘ed into the Identity Centre.

1. Navigate to IAM Identity Centre.
2. Select Settings from the left menu
3. In the Setting page , Click on **Enable** within the Automatic Provisioning info block
4. In the Inbound automatic provisioning dialog
    - Copy the **SCIM endpoint** and the **Access Token** , we will use it to configure it within the Okta admin dashboard

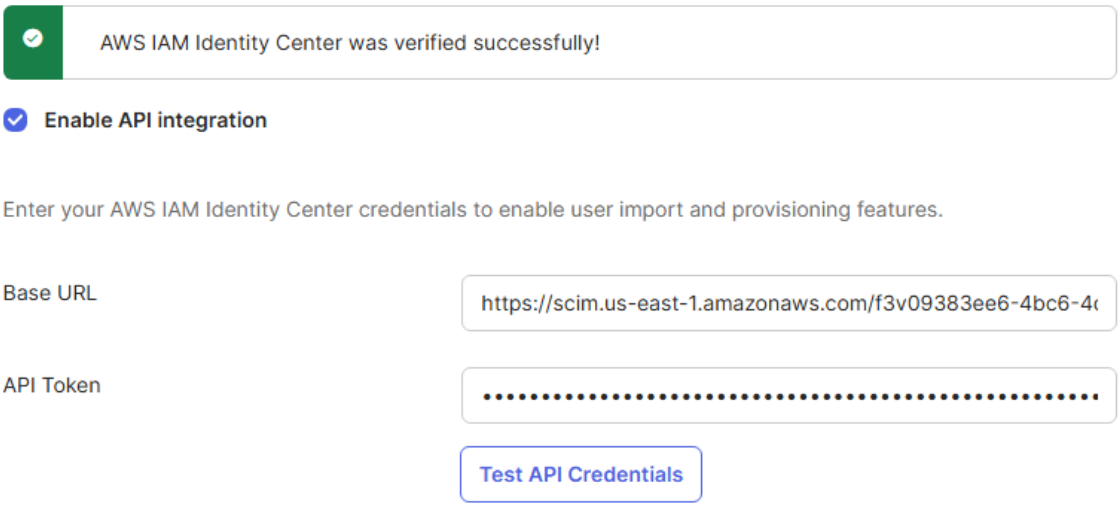


In Okta Admin Dashboard:

1. Navigate to the **Provisioning** tab within the IAM Identity Center Application
2. Click on **Configure API Integration**



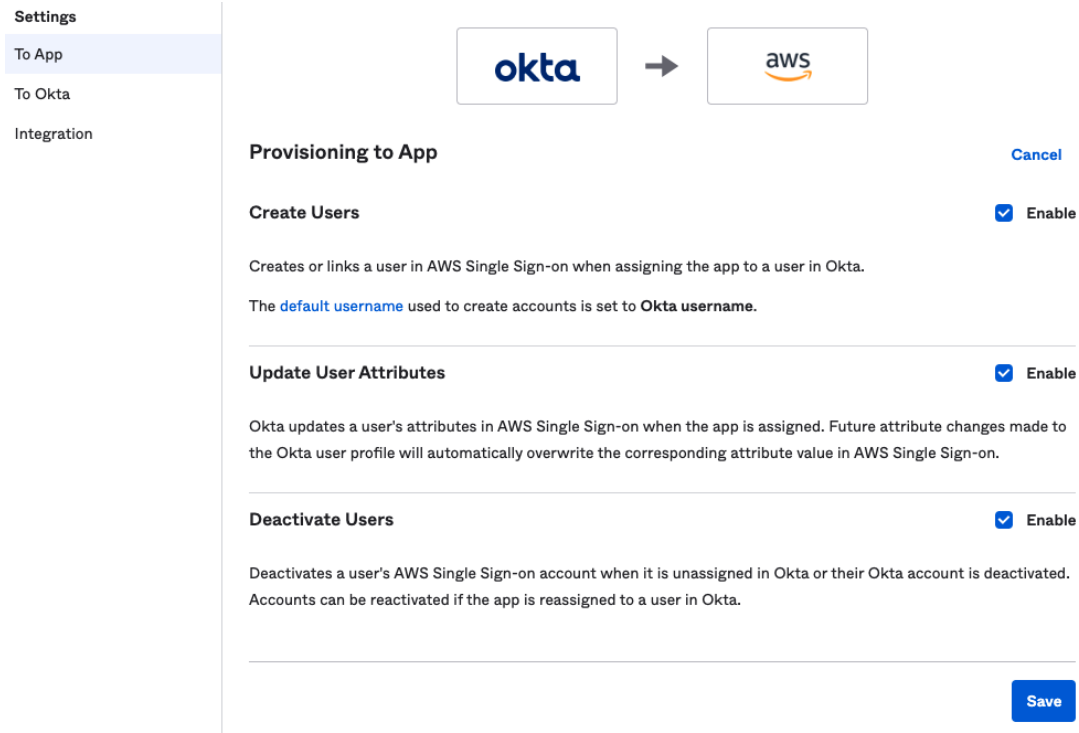
- Select the checkbox for **Enable API Integration**
- Provide the Base URL value with the **SCIM endpoint** copied from step 4 in the previous section
- Provide API Token value with the **Access Token** copied from step 4 in the previous section
- Click Test API Credentials to test the end-point



- Click save to save the configuration.

3.In the “Provisioning” tab make sure that “To App” is selected.

- Click on **Edit**
- Select **Enable** for Create, Update and Deactivate Users.



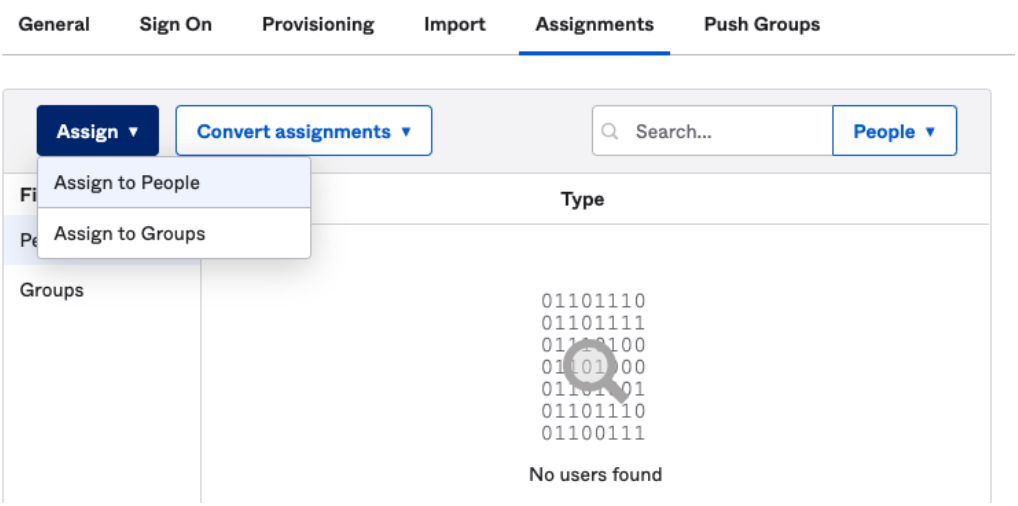
- Click on **Save.**

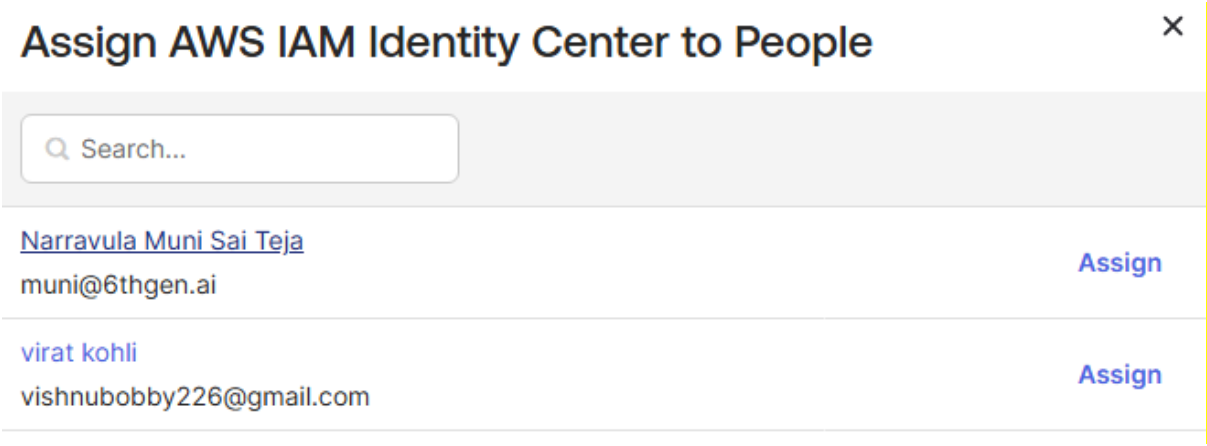
6.5 Assign User/Groups to IAM Identity Centre Application in Okta

To allow users access via SSO, we must assign them to the IAM Identity Center Application in Okta. As soon as you assign a user or group, Okta will call in the background the APIs to create the user in IAM Identity centre. If you change a mapped attribute e.g. FirstName, Okta will update the attribute also in IAM Identity Center. If you unassign a user, it will be deactivated in IAM Identity Center. Okta takes care of the full user life-cycle management.

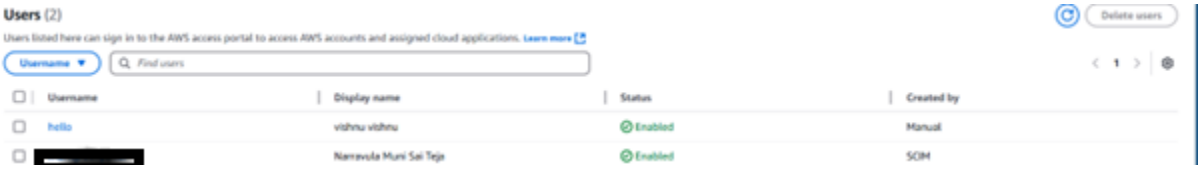
1.In Okta admin dashboard, Go to “Assignment” tab then

- Click on **Assign to Groups** within the **Assign** pull-down button



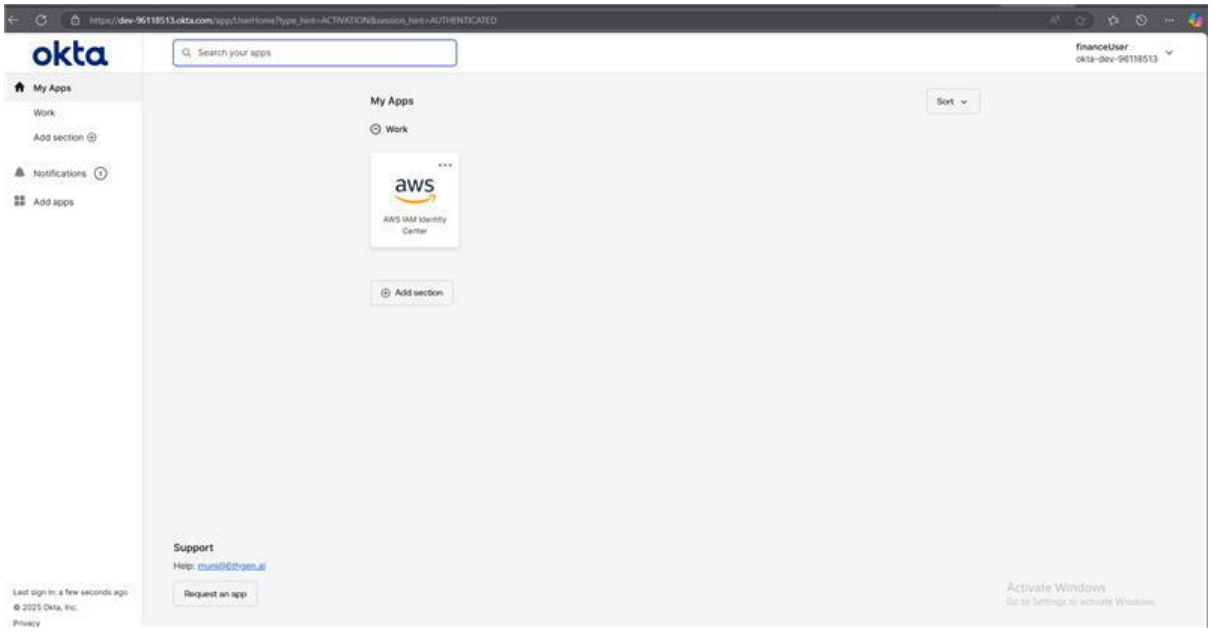


- Choose **Narravula Muni Sai Teja** and click **Assign.**



Let's validate the new user is now **synced** into Identity Center

- Now give the permission set to the user with the account. And check with the login URL there in Dashboard

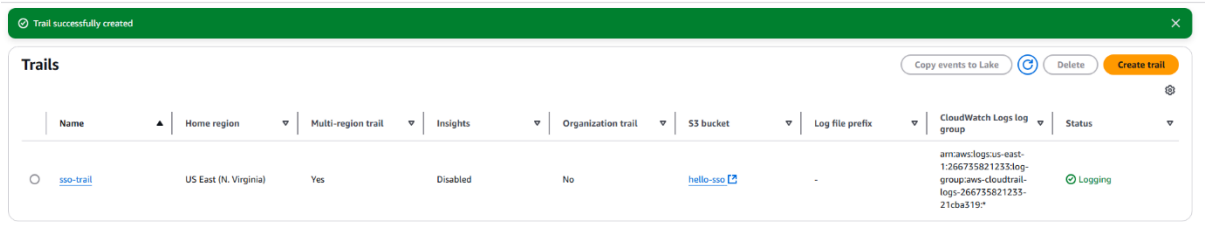


- Here Now it will be login with Okta.

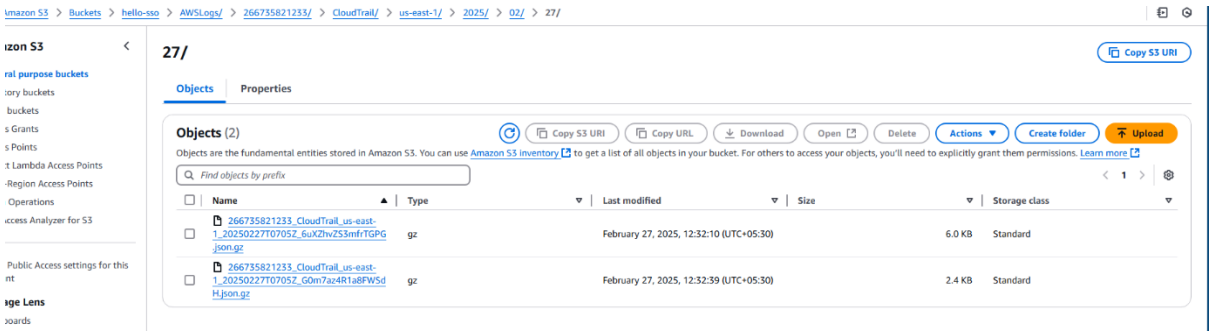
7. Setting Up SSO Authentication Logging and Monitoring

7.1 Enable CloudTrail

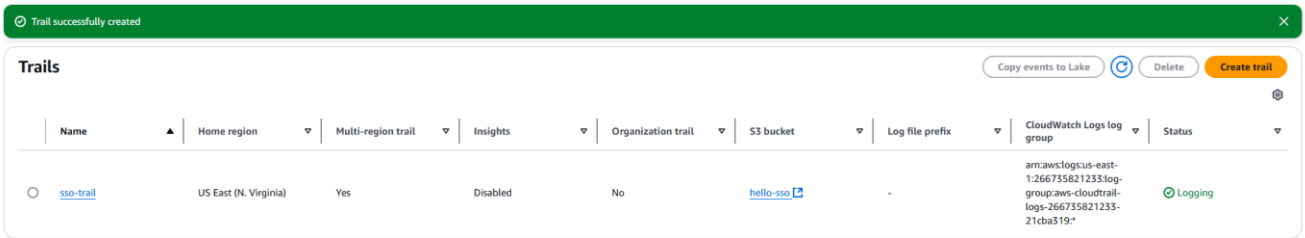
1. Sign in to AWS Console
2. Go to CloudTrail service
3. Click "Create trail"
4. Fill in the following:
    - Trail name: SSO- Trail



    - Storage location: Create new S3 bucket
    - Bucket name: hello-sso



5. Under "Log event selections":
    - Select "Management events"
    - Choose "Read/Write events"
6. Click "Next"
7. Click "Create trail"



Lets check here CloudTrail events.

☐	CreateBearerToken	February 27, 2025, 10:36:57 (UT...	Kranthi_user	sso-directory.amazonaws.com
☐	CreateProvisioningTenant	February 27, 2025, 10:36:57 (UT...	Kranthi_user	sso-directory.amazonaws.com
☐	EnableExternalIdPConfigurationForDirectory	February 27, 2025, 10:36:02 (UT...	Kranthi_user	sso-directory.amazonaws.com
☐	CreateExternalIdPConfigurationForDirectory	February 27, 2025, 10:36:01 (UT...	Kranthi_user	sso-directory.amazonaws.com
☐	DeleteExternalIdPConfigurationForDirectory	February 27, 2025, 10:36:00 (UT...	Kranthi_user	sso-directory.amazonaws.com
☐	DisableExternalIdPConfigurationForDirectory	February 27, 2025, 10:36:00 (UT...	Kranthi_user	sso-directory.amazonaws.com
☐	DeleteProvisioningTenant	February 27, 2025, 10:35:59 (UT...	Kranthi_user	sso-directory.amazonaws.com

Check the logs in Cloud Watch as well.

sso-trail Delete Stop logging

General details Edit

Trail logging: Logging
Trail name: sso-trail
Multi-region trail: Yes
Apply trail to my organization: Not enabled
Trail log location: hello-sso/AWSLogs/266735821233
Last log file delivered: February 27, 2025, 12:32:09 (UTC+05:30)
Log file SSE-KMS encryption: Enabled
AWS KMS key: arn:aws:kms:us-east-1:266735821233:key/4cb674bd-9c72-453b-9819-2bb12b3c5b3c
AWS KMS key alias: sso-monitoring-key
Log file validation: Enabled
Last file validation delivered: -
SNS notification delivery: Disabled
Last SNS notification: -

CloudWatch Logs Edit

Log group: aws-cloudtrail-logs-266735821233-21cba319
IAM Role: arn:aws:iam::266735821233:role/service-role/sso-cloudtrail-role

7.2 Set Up Basic Alerts

Its time to set up Cloud Watch Alarms

Setup the Cloud Watch alarm for **IncomingLogEvents .**

- IncomingLogEvents counts the number of individual SSO actions (like logins, authentication attempts) where each action = 1 event, useful for security monitoring and activity patterns.

Think of it Like:

- Events = Counting number of emails

IncomingLogEvents:

- Counts the NUMBER of log entries/events
- Each login attempt = 1 event
- Each authentication = 1 event
- Useful for: Monitoring frequency of actions
- Example: 50 events = 50 different SSO actions

Once you create Alarm you get this email for subscription.

AWS Notification - Subscription Confirmation Inbox ×

AWS Notifications <no-reply@sns.amazonaws.com>
to me

You have chosen to subscribe to the topic:
arn:aws:sns:us-east-1:266735821233:sso_CloudWatch_Alarms_Topic

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
Confirm subscription

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to sns-opt-out

- The actions is happened in the SSO for any thing the alarm triggers and sent to you a like as shown in below image.

Alarms (1)

Hide Auto Scaling alarms | Clear selection | Create composite alarm | Actions | Create alarm

Search | Alarm state: Any | Alarm type: Any | Actions status: Any | 1

Name	State	Last state update (UTC)	Conditions	Actions
sso-alaram	In alarm	2025-02-27 07:17:28	IncomingLogEvents > 3 for 1 datapoints within 5 minutes	Actions enabled Warning

ALARM: "sso-alaram" in US East (N. Virginia) Inbox ×

AWS Notifications <no-reply@sns.amazonaws.com>
to me
12:47 PM (2 minutes ago)

You are receiving this email because your Amazon CloudWatch Alarm "sso-alaram" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [20.375 (27/02/25 07:12:00)] was greater than the threshold (3.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Thursday 27 February, 2025 07:17:28 UTC".

View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarmsV2:alarm/sso-alaram

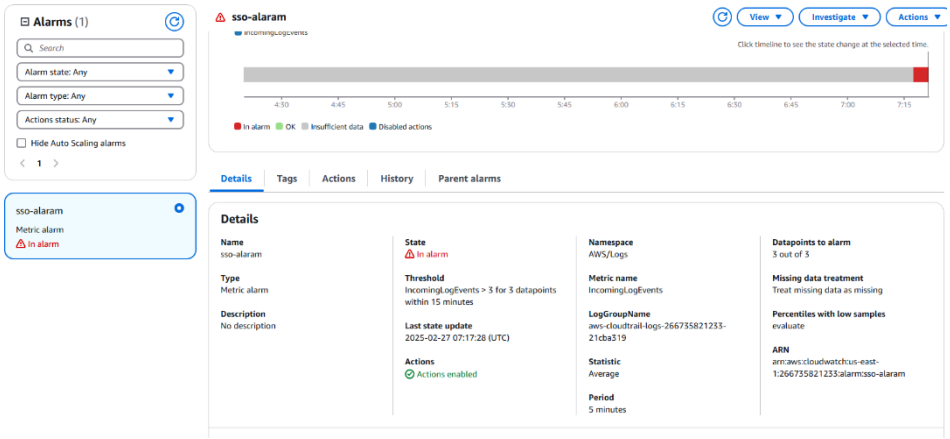
Alarm Details:
- Name: sso-alaram
- Description:
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [20.375 (27/02/25 07:12:00)] was greater than the threshold (3.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Thursday 27 February, 2025 07:17:28 UTC
- AWS Account: 266735821233
- Alarm Arn: arn:aws:cloudwatch:us-east-1:266735821233:alarm:sso-alaram

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanThreshold 3.0 for at least 1 of the last 1 period(s) of 300 seconds.

Monitored Metric:
- MetricNamespace: AWS/Logs
- MetricName: IncomingLogEvents
- Dimensions: [LogGroupName = aws-cloudtrail-logs-266735821233-21cba319]
- Period: 300 seconds
- Statistic: Average
- Unit: not specified
- TreatMissingData: missing

State Change Actions:
- OK:
- ALARM: [arn:aws:sns:us-east-1:266735821233:sso_CloudWatch_Alarms_Topic]
- INSUFFICIENT_DATA:

- Once Alarm triggers then alarm state change insufficient data to in-alarm state.

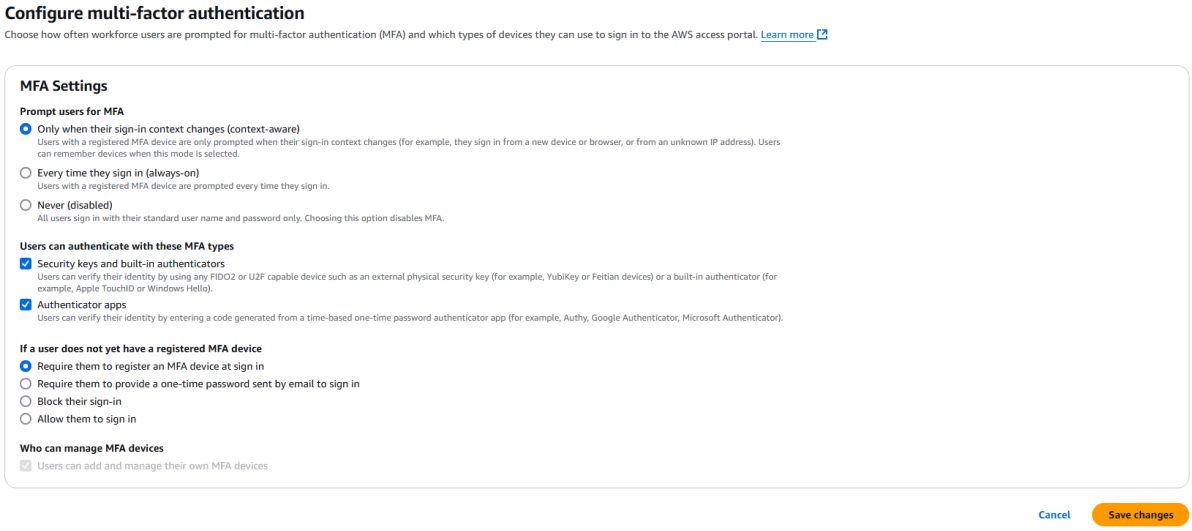


8. Security Hardening Guide for IAM Identity Centre

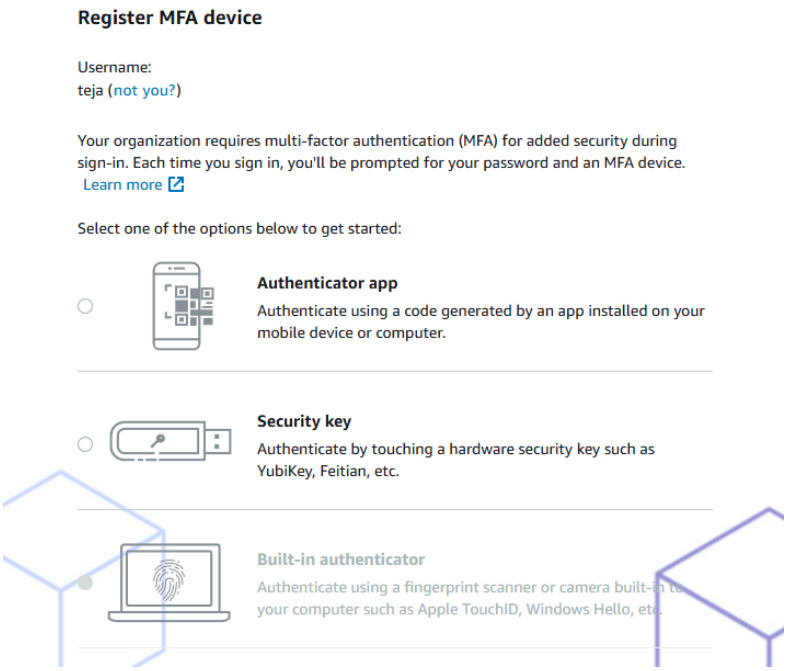
8.1 Basic Security Settings

1.Configure MFA Settings

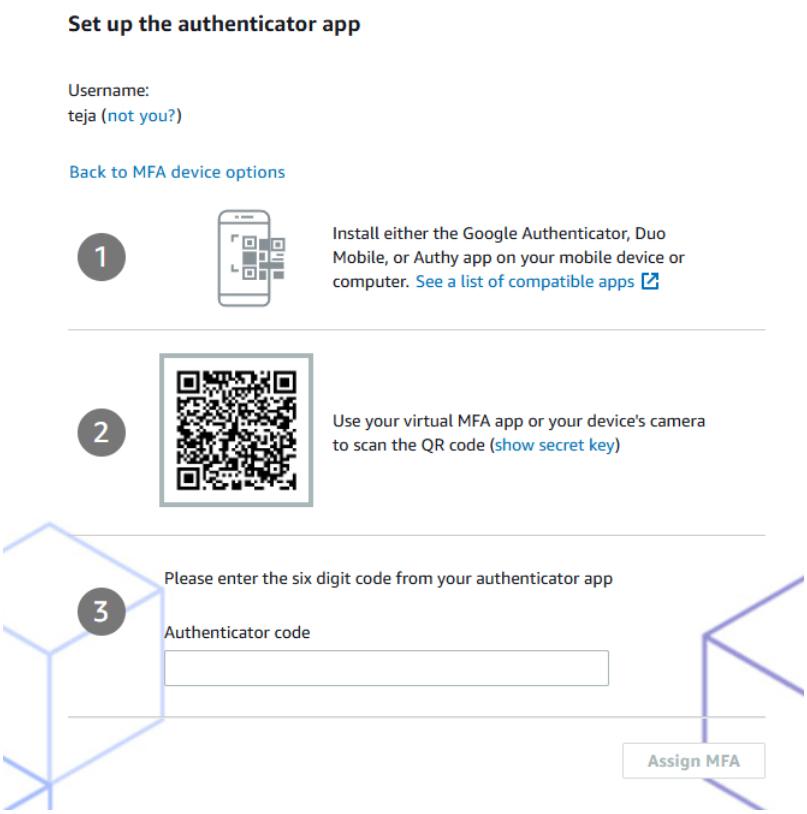
1. Go to IAM Identity Center console
2. Navigate to "Settings" → "Security settings"
3. Click "Configure"
4. Enable:
    - "Require MFA"
    - Select "Every time they sign in"



Once you enter username and password it will shows like this.

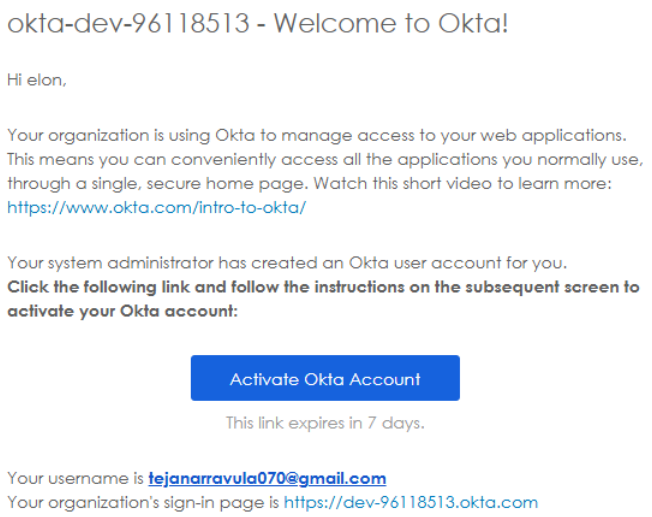


5. Under MFA methods, enable:
    - Security key
    - Built-in authenticator
    - Authenticator apps
6. Click "Save changes"

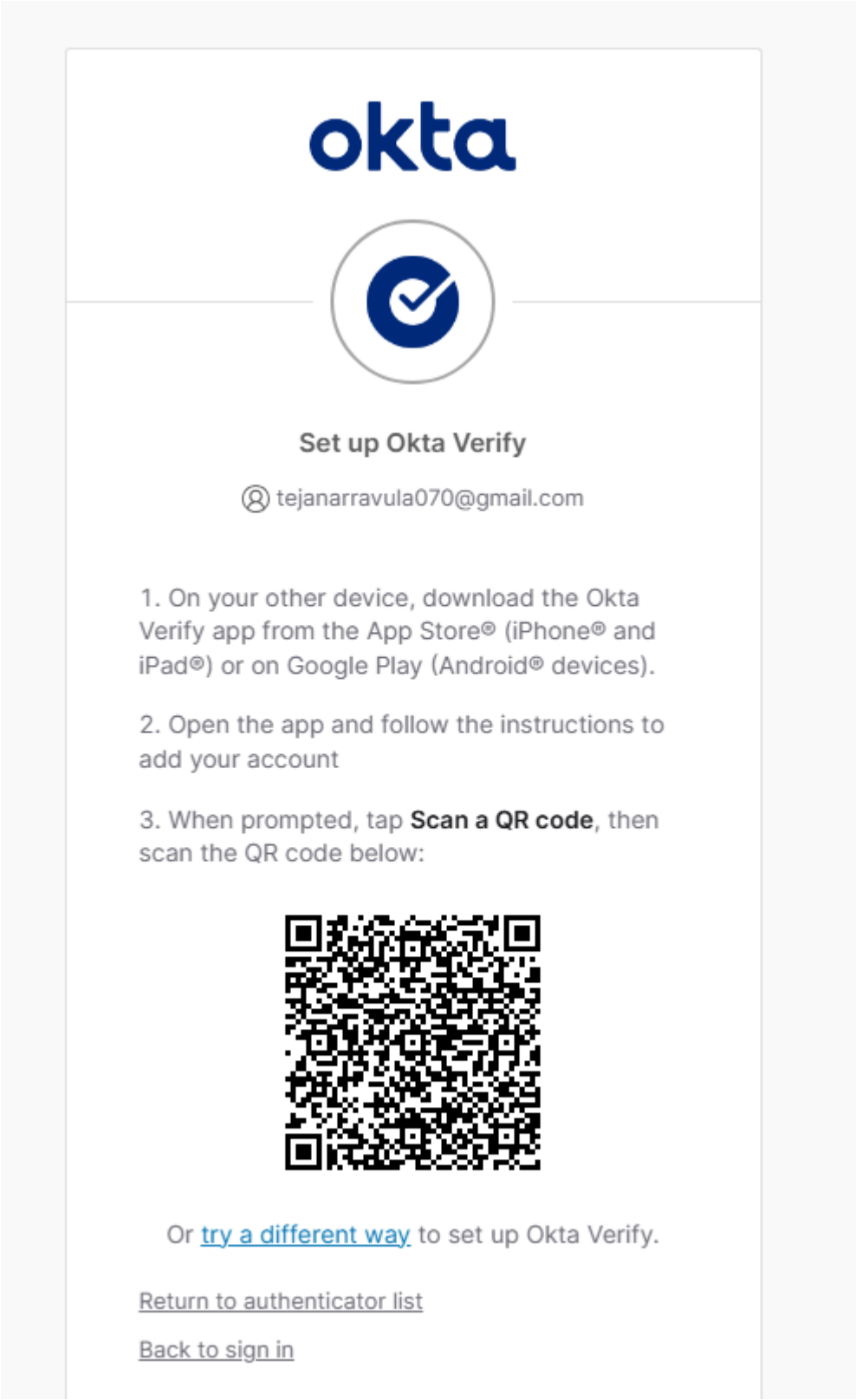


Same for Okta user login also you need to setup MFA to login into the account.

- After create an your in Okta you get an email for activate your user.



After clicking on Activate your Okta Account it will appear for add MFA as like below image.



8.2 IP Restrictions Setup with EC2 Instance Access Control

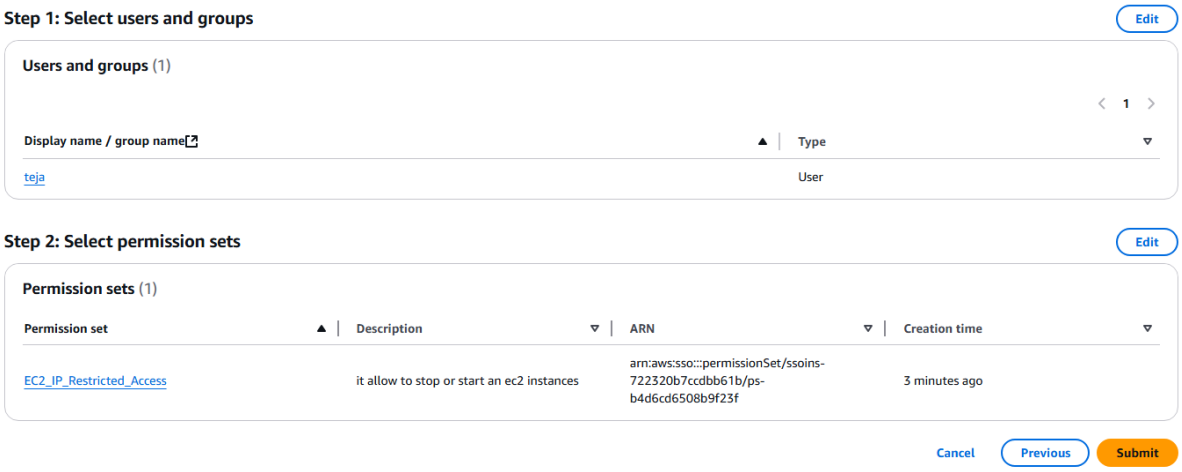
1. Create EC2 Instances

- Create 2 EC2 Instances for testing purposes.
- Enable Public IP for Both the servers.

2.Create the permissions set for IAM Identity Centre.

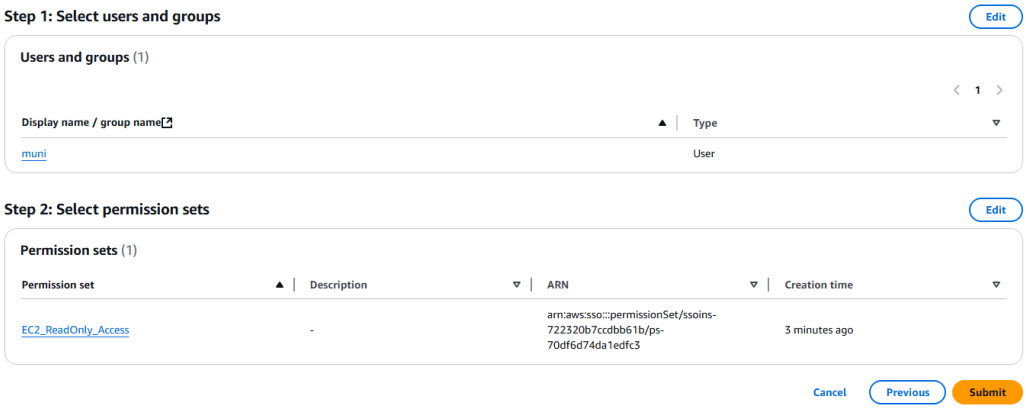
For Teja User:

- Go to IAM Identity Center
- Click "Permission sets" → "Create permission set"
- Choose "Custom permission set"
- Name: "EC2-Control-Access"
- Create inline policy:



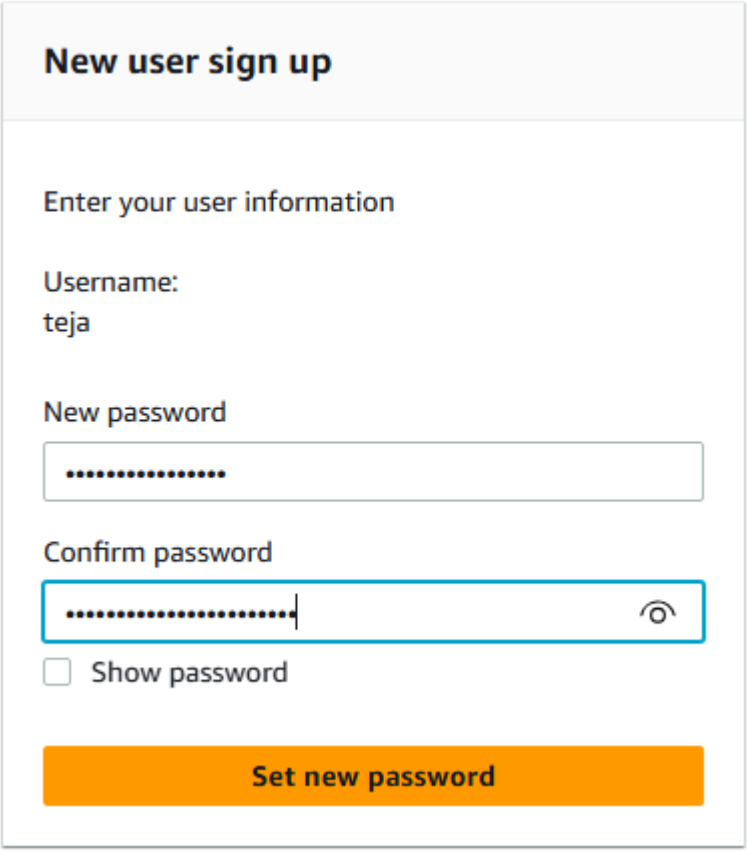
For Muni

- Create another permission set
- Name: "EC2-ReadOnly-Access"
- Create in-line policy:

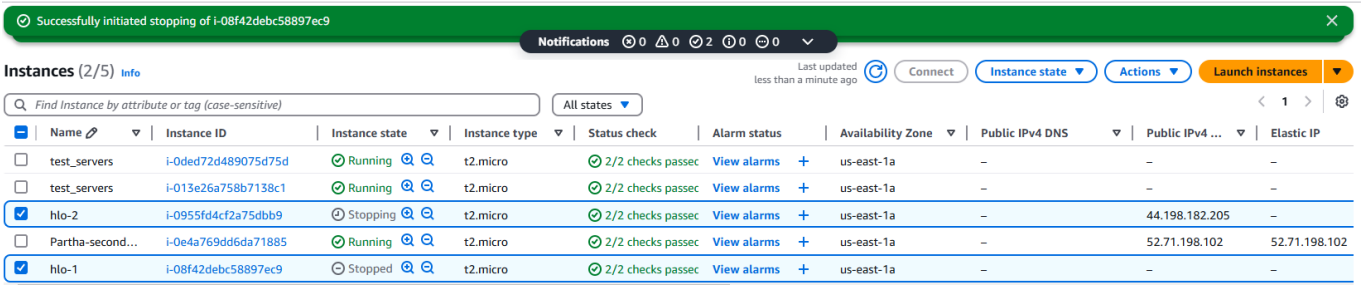


Testing process:

Login with user Teja:

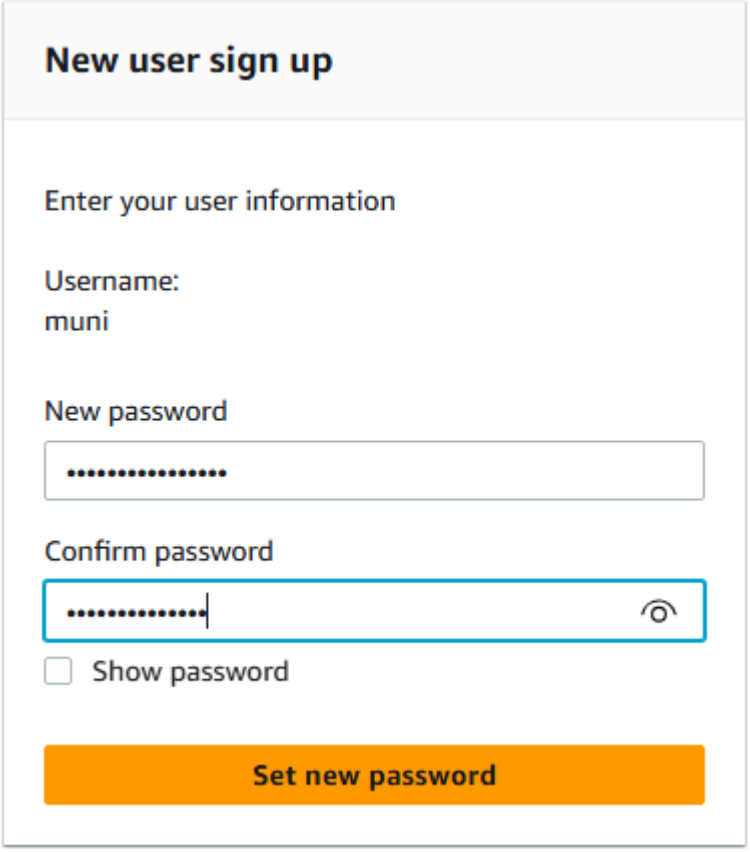


Teja has access to stop the servers.

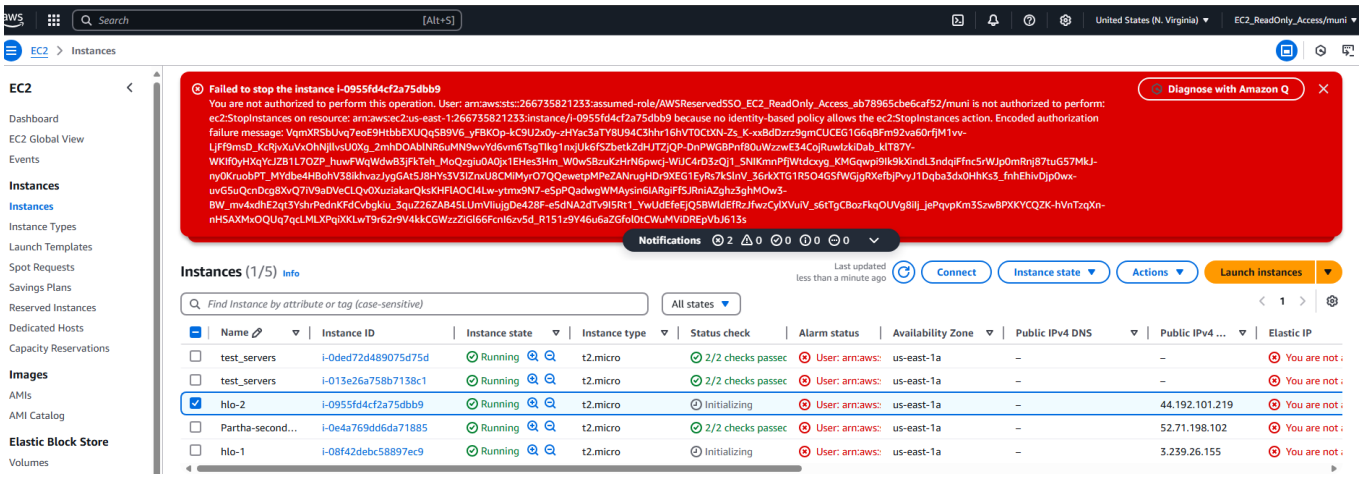


- As shown in above image with Teja user he is able to stop the servers.
- The servers are in stopping state.

Login with user Muni:

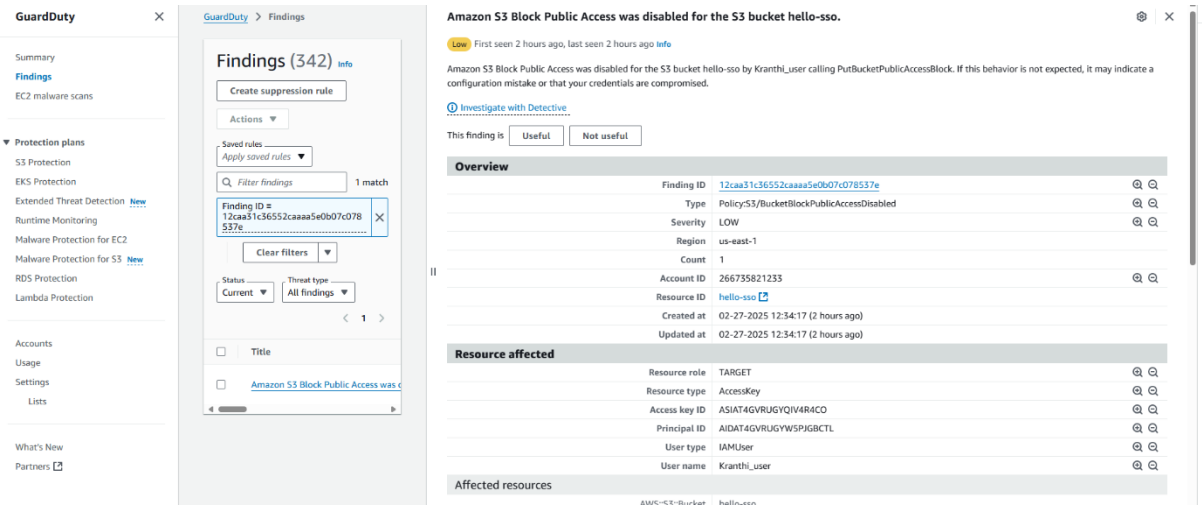


- Muni having Read-only permissions so he cant able to stop the servers and getting error like as shown in the below image.



8.3 Guard Duty Setup

- Sign in to AWS Console and navigate to Guard Duty.
- Click Enable Guard Duty if not already enabled.
- Once enabled, go to Findings in the left panel.
- Review findings like "Amazon S3 Block Public Access was disabled for the S3 bucket".
- Click on a Finding ID to see details.
- Check the affected resource, IAM user, and timestamp.
- If necessary, click Investigate with Detective for further analysis.
- Use Actions → Create suppression rule to ignore similar findings if required.
- Regularly monitor Findings and take corrective actions.



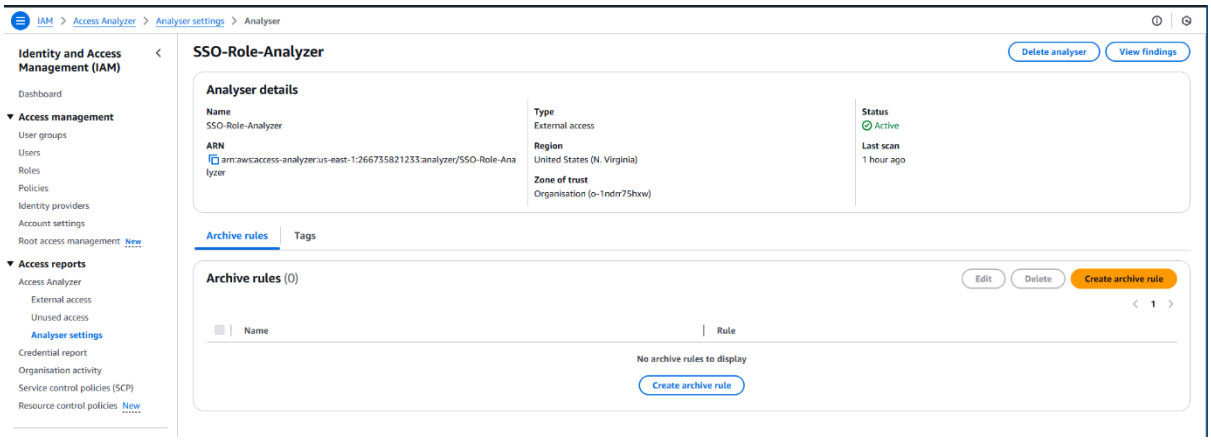
Title	Severity	Finding type	Resource	Count
Amazon S3 Block Public Access was disabled for the S3 bucket hello-sso.	Low	Policy:S3/BucketBlockPublic AccessDisabled	Access Key: ASIAT4GVRUGYQIV4R4CO	1

Finding Type: Policy:S3/BucketBlockPublicAccessDisabled

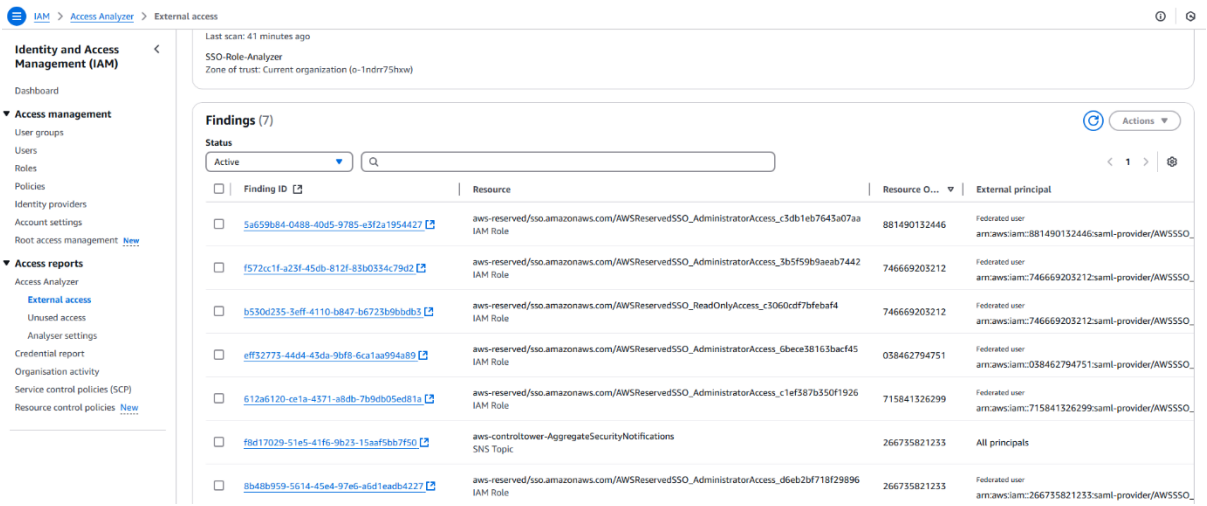
- **Issue:** S3 Block Public Access was disabled for bucket hello-sso by Kranthi_user.
- **Severity:** Low
- **Possible Causes:** Intentional change, misconfiguration, or compromised credentials.
- **Actions:**
  - ✅ Verify if the change was authorized.
  - ✅ Re-enable Block Public Access if needed.
  - ✅ Check CloudTrail logs for unauthorized activity.

9.AWS IAM Access Analyser

Access Analyzer helps identify external access to AWS resources, ensuring security by detecting unintended permissions and policy misconfigurations.



- **Open IAM Console** → Go to **Access Analyzer**.
- Click **Create Analyzer** and set the **Zone of Trust** (e.g., current organization).
- Access **External Access** under **Access Reports** to review findings.
- Check findings for IAM roles, S3 buckets, SNS topics, etc.
- Analyze **External Principal** details and update policies if needed.
- Regularly monitor and refine access settings for security.



Here **AWS IAM Access Analyzer** findings for **external access** in your organization. It highlights **IAM roles and an SNS topic** with potential external access. The findings indicate **federated users (SSO) and all principals** having permissions to certain AWS resources. You need to **review and adjust policies** to ensure security.

10. Load Testing & Scalability for IAM Identity Centre

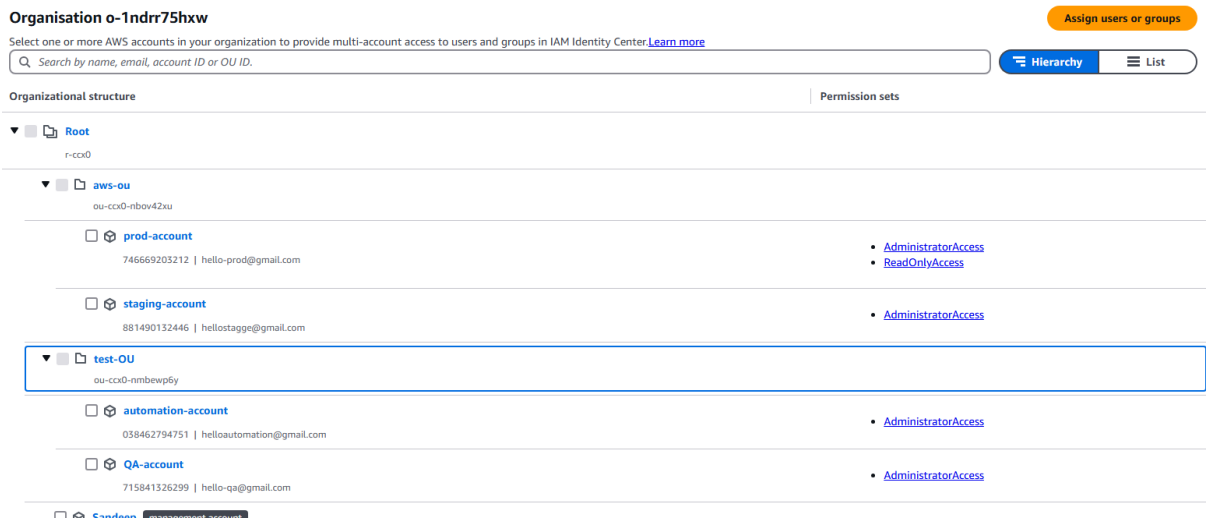
Setup Test Accounts

1.Create Test AWS Accounts:

- Development Account
- Testing Account
- Staging Account

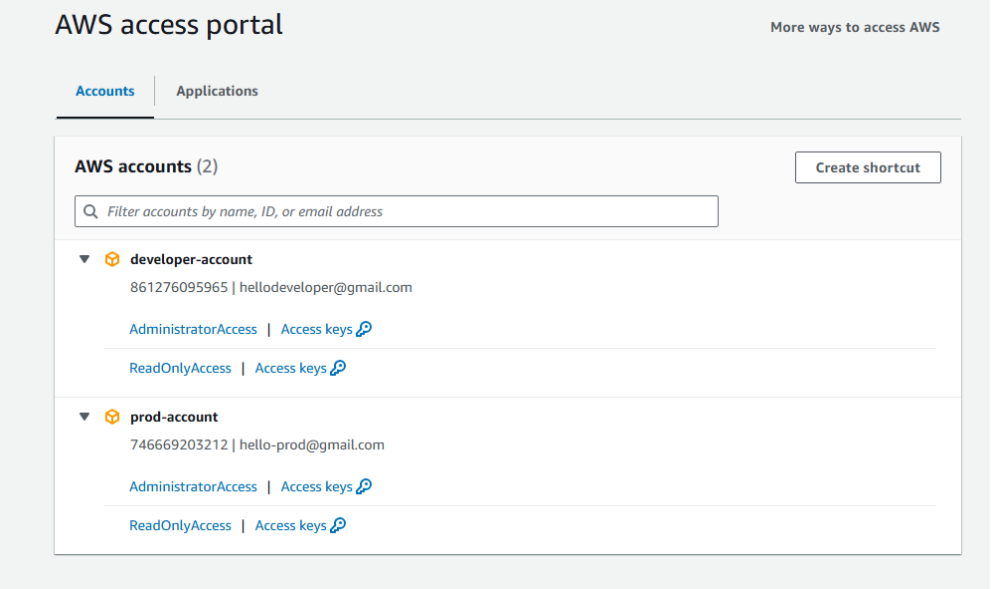
2.Configure AWS Organizations:

- Add test accounts to organization
- Enable trusted access for IAM Identity Center



Configure Multi-Account Access

- Create and assign users for any 3 accounts

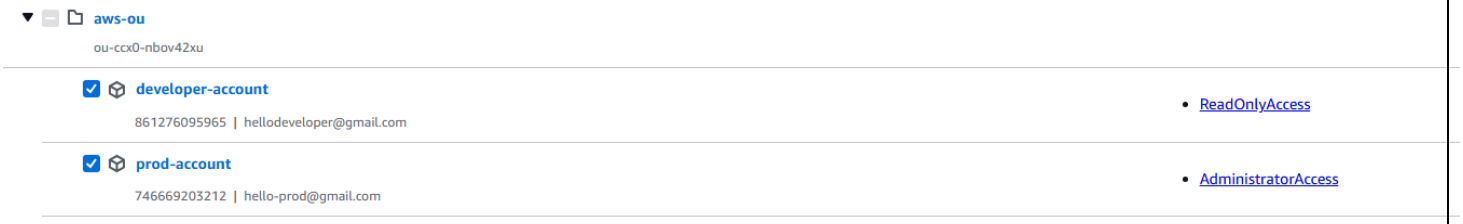


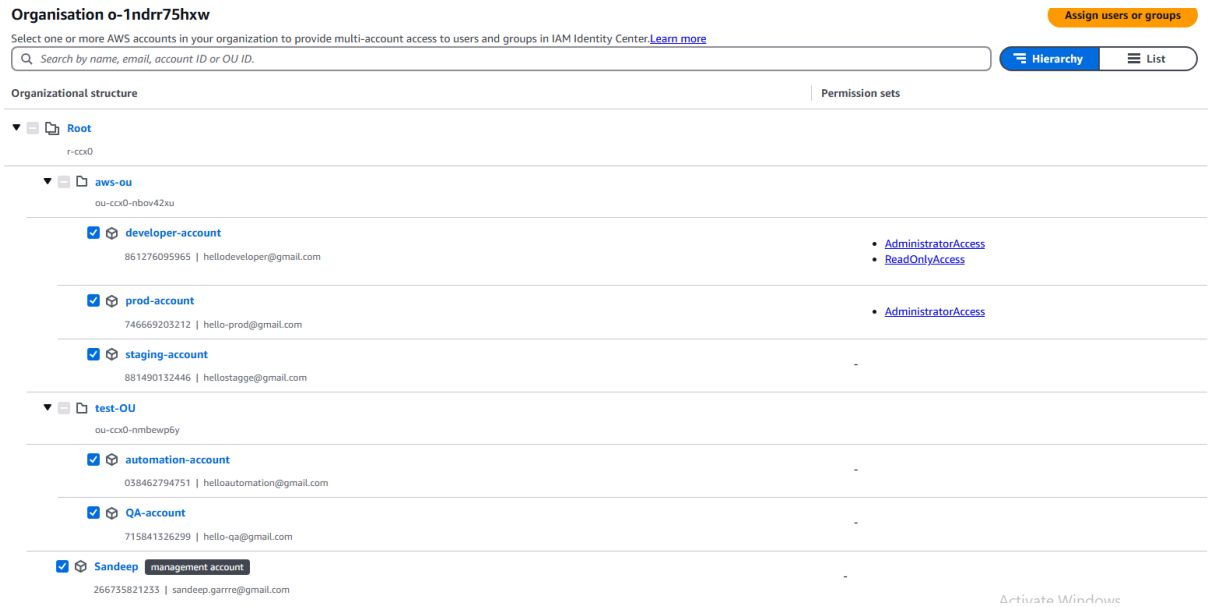
Sequential Account Access:

- Test users accessing multiple accounts

Look At this below image :

An user having access for 2 different accounts with different permissions sets to working in both accounts.





SCP Policy-Based Access for SSO

1. Navigate to AWS Organizations

- Sign in to the AWS Management Console as an Administrator.
- Open the AWS Organizations service.
- Click on Policies in the left panel.
- Select Service Control Policies (SCPs).

2. Create the SCP Policy

- Click Create Policy.
- Enter a Name (e.g., Restrict-EC2-Instance-Type).
- In the Policy JSON Editor, paste the SCP JSON provided.
- Click Create Policy.

```
{
 "Version": "2012-10-17",
"Statement": [
  {
   "Sid": "RequireMicroInstanceType",
  "Effect": "Deny",
  "Action": "ec2:RunInstances",
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
   ],
  "Condition": {
    "StringNotEquals": {
      "ec2:InstanceType": "t2.micro"
     }
   }
  }
 ]
}
```

How This SCP Policy Works

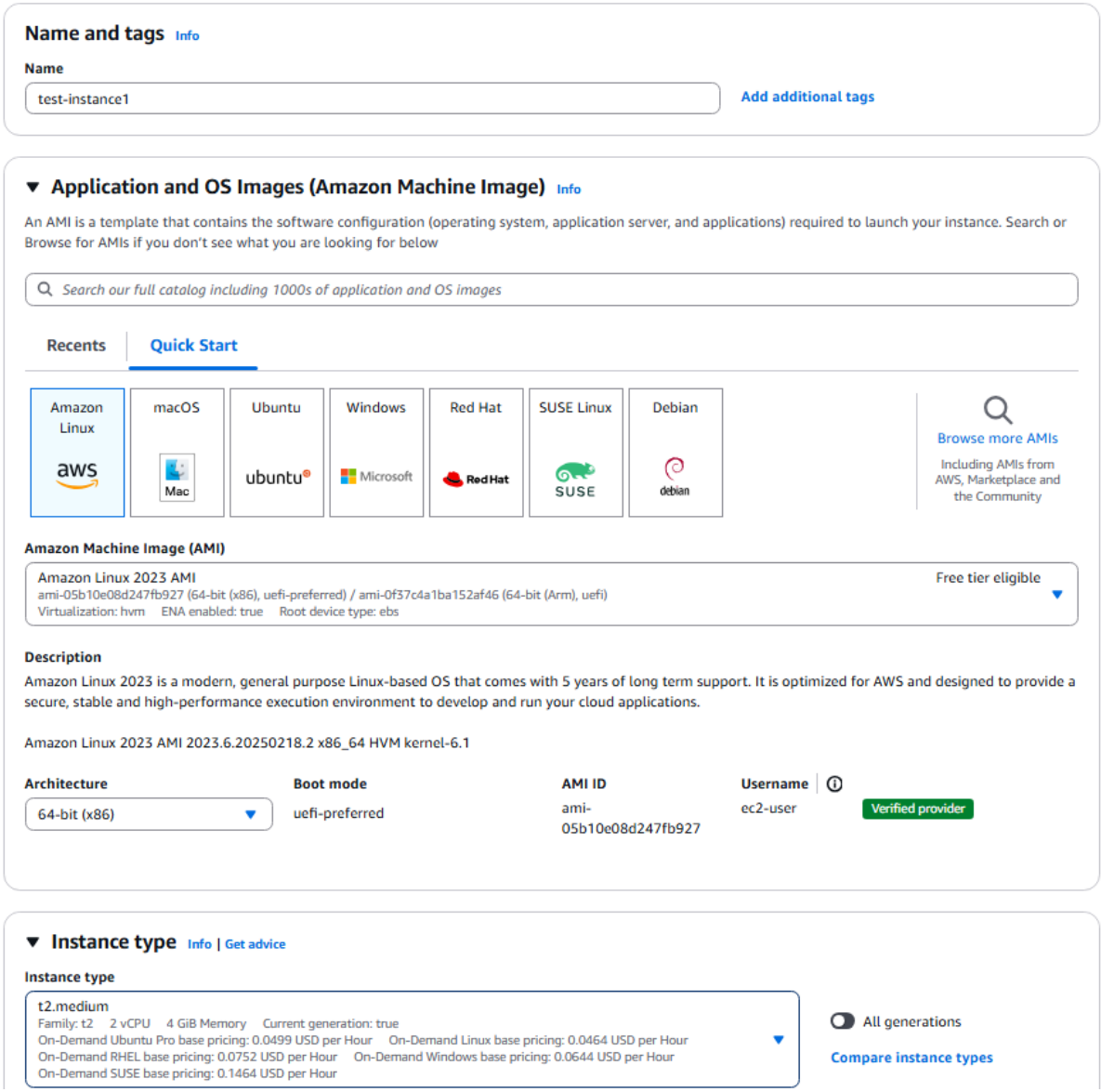
- **Effect:** "Deny" → Prevents users from launching EC2 instances unless they meet the condition.
- **Action:** "ec2:RunInstances" → Blocks instance launch operations.
- **Resource:** "arn:aws:ec2:*:*:instance/*" → Applies the restriction to all EC2 instances across all AWS accounts in the organization.
- **Condition:**
    1. "StringNotEquals": { "ec2:InstanceType": "t2.micro" }

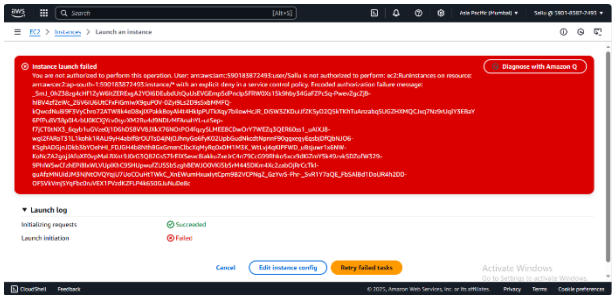
2. This means **any instance type other than t2.micro will be denied**.
3. Only t2.micro instances are allowed to be launched.

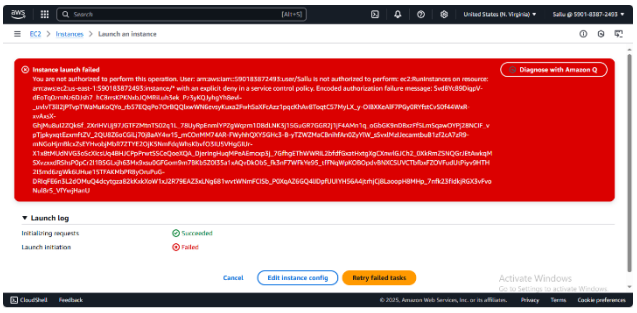
3. Attach the SCP to Organizational Units (OUs) or Accounts

- Select the created policy.
- Click Attach Policy.
- Choose the target OU or AWS account where you want this restriction applied.
- Click Attach.

Here I am trying to launch an t2.medium instance type it will get an error like below images in different regions also.







- Now I am trying to launch t2.micro instance it will created successfully.

Name and tags Info

Name

test-instance1

Add additional tags

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Recents | Quick Start

Amazon Linux | macOS | Ubuntu | Windows | Red Hat | SUSE Linux | Debian

Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI
ami-05b10e08d247fb927 (64-bit (x86), uefi-preferred) / ami-0f37c4a1ba152af46 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs
Free tier eligible

Description

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.6.20250218.2 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Username
64-bit (x86)	uefi-preferred	ami-05b10e08d247fb927	ec2-user Verified provider

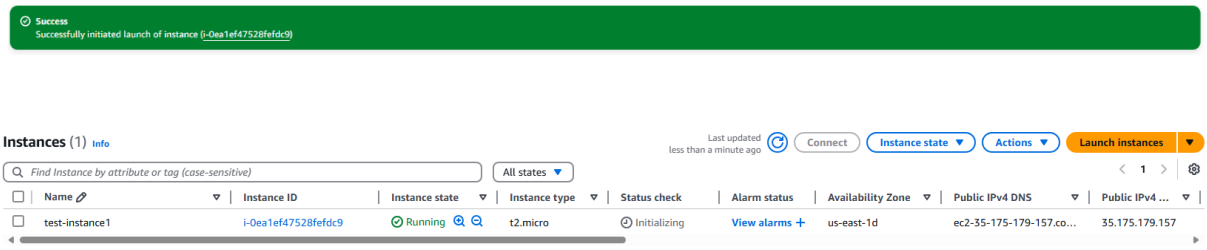
Instance type Info | Get advice

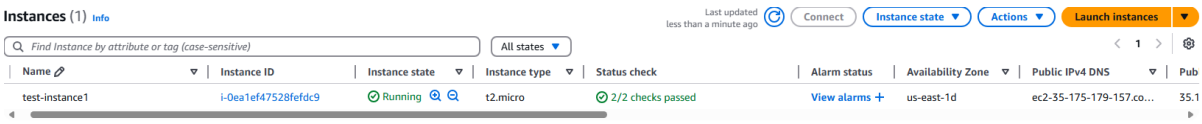
Instance type

t2.micro
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour
Free tier eligible

All generations

Compare instance types





Expected Outcome

- Users in the affected accounts **will only be able to launch t2.micro instances**.
- If they try to launch any other instance type, they will receive a **permission denied error.**

11.AWS IAM Identity Centre Cost & Scaling

Base Costs

1. AWS IAM Identity Center
   - Core Service: FREE
   - SCIM Integration with Okta: FREE
   - AWS Account Access: FREE

Small Organization (50 Users)

Monthly Estimate:

1. IAM Identity Center

- Base service: $0

- User management: $0

2. Logging & Monitoring

- CloudWatch Logs: ~$2-5

- CloudTrail: $0-2

- S3 Storage: ~$1

Total Estimated Cost: $3-8/month

Associated Service Costs

1.**CloudWatch Logs:**

Storage Costs:

- First 5GB/month: FREE
- $0.50 per GB-month (after first 5GB)

Log Ingestion:

- First 5GB: FREE
- $0.50 per GB thereafter

2.Cloud Trail:

Management Events:

- First trail: FREE
- Additional trails: $2/100,000 events

Data Events:

- $0.10 per 100,000 events

3.S3 storage (for logs):

Standard Storage:

- First 50 TB/month: $0.023 per GB
- Next 450 TB/month: $0.022 per GB

Okta costs (monthly)

- Free for up to Free trail access

Scaling Considerations

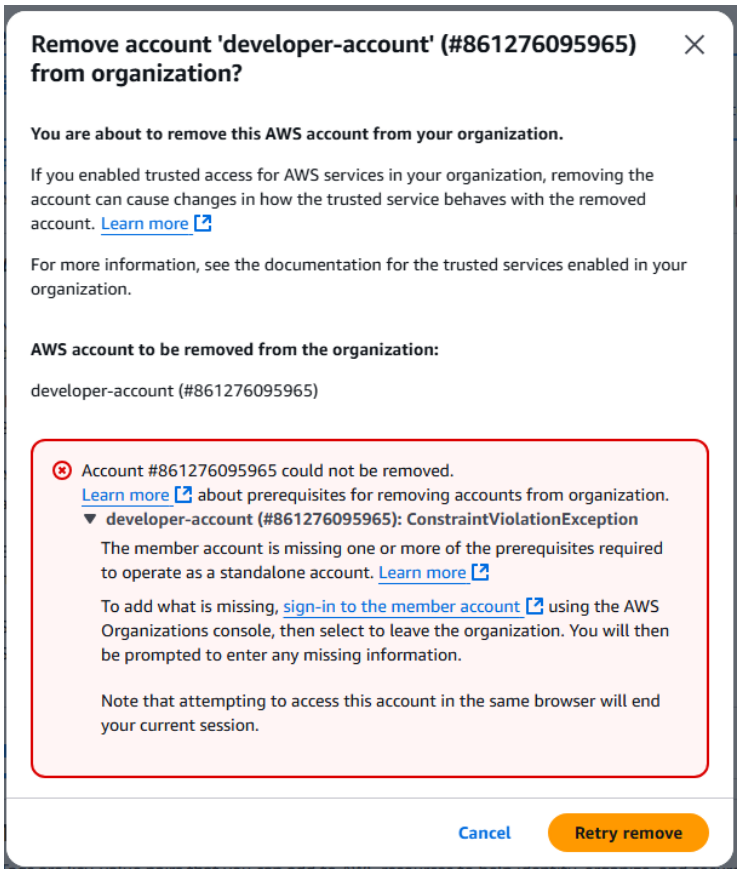
- Auto-scaling with Okta sync: No additional AWS costs
- User growth: Only affects Okta licensing
- Additional AWS accounts: No extra cost

Total Monthly AWS Cost Estimate: $8-17 (excluding Okta)

Common Issues and Troubleshooting

Issue 1:

The AWS account removal failed due to a ConstraintViolationException, likely caused by active dependencies like AWS services, policies, or trusted access.



Solution:

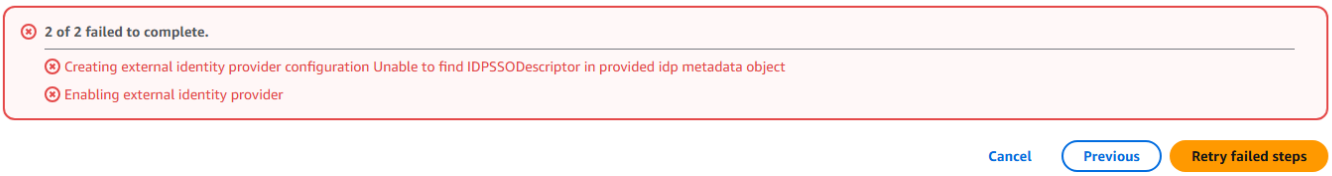
Steps to Remove an AWS Member Account from an Organization:

1. **Create an AWS Account** – Ensure you provide all necessary billing details and complete the profile setup properly.
2. **Log in to the Member Account** – Access the specific AWS account you want to remove.
3. **Navigate to AWS Organizations** – In the AWS Management Console, go to the **AWS Organizations** service.
4. **Leave the Organization** – Click on **"Leave Organization"**, and the account will be successfully removed.

Issue 2:

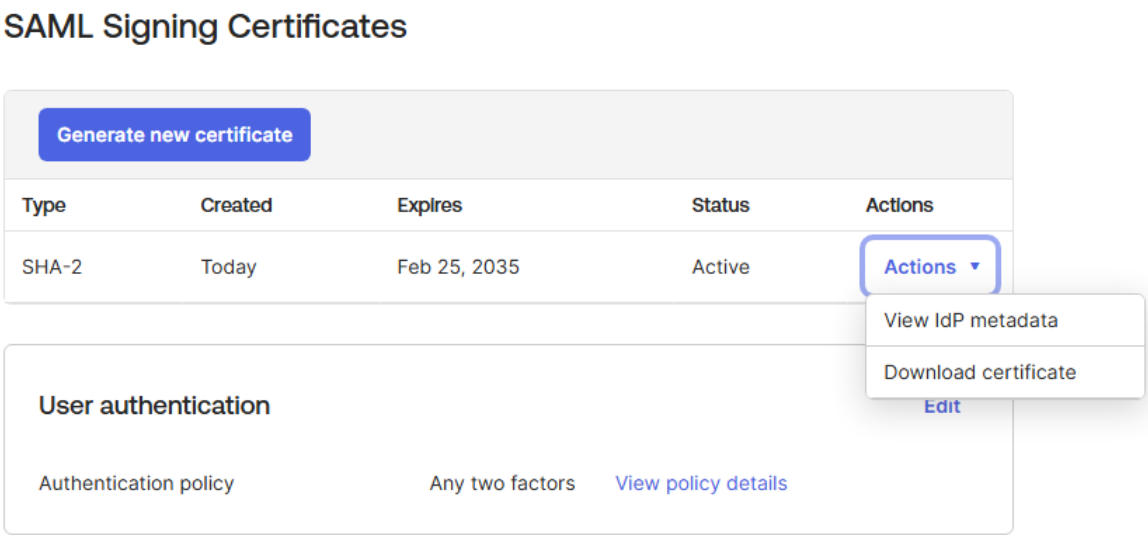
The external identity provider setup failed due to a missing IDPSSODescriptor in the provided IdP metadata.

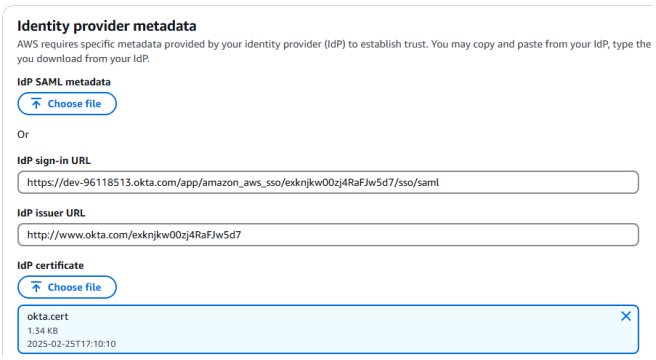
Confirm change



Solution:

- In Okta go to SAML signing certificates



- Click on View IdP metadata and that will open the link like this below image.

- Download Certificate from second option .
- Enter the details properly in AWS Identity centre.