# OKTA INTEGRATION WITH AWS SSO

11.06.2024

SSO+SSM
AWS SSO: allows access to multiple AWS account and cloud apps with single credentials, issued by external identity providers
Integrated with SSM Parameter Store (a secret management soln) it provides a secure and effective way to store user creds

>Attributes in permission policies: who in our identity source can access our AWS resources: attributes to control access to SSM and attributes to SSO config
>creation of custom policy that stipulates user access based on attributes mentioned and added it to the aws sso permission set (list that acts as an IAM role in the target AWS acc)
>attributes to SSM params as tags to enable access to a db secret
>further secure params, add a restriction that users can only access those passwords whose path corresponds to their attributes
>multiple condition blocks: AWS evals the conditions w AND boolean

Users access the secret per a unique path that corresponds to their attributes
Allows centralized password management and enables sys admin to grant granular access for user credentials based on their attributes without hardcoding permission policies

How defined AWS IAM Identity Center source attributes can be used and custom attributes can be used to pass these attributes into AWS from an external identity provider using SAML 2.0

Attribute based access control (ABAC): usage of user attributes as tags creates fine grained permissions in AWS, enabling workforce access to only those AWS resources with matching tags

Prereq: use SAML(Security Assertion Markup Language) and SCIM(System for cross domain identity management) protocols
Attributes are created and updates in external directory for qg Okta which is an id management service built for cloud:

- For apps that support federated (temp access given by org) SSO through SAML or any auth protocol, Okta establishes a secure connection with a user's browser and auths the user
- With SSO a central domain performs auth and then shares the session w other domains

Gotta configure  ABAC in AWS using IAM identity center
https://docs.aws.amazon.com/singlesignon/latest/userguide/abac-checklist.html

AWS SSO can be integrated with Identity Providers such as Microsoft Active Directory, Okta, Azure AD(Microsoft Entra ID), CyberArk, Google Workspace, JumpCloud, OneLogin, Ping Identity or other supported IdP

IAM supports IdPs that are compatible with OpenID connect or SAML 2.0

Amazon cognito works with external IdP that support this

IdPs:

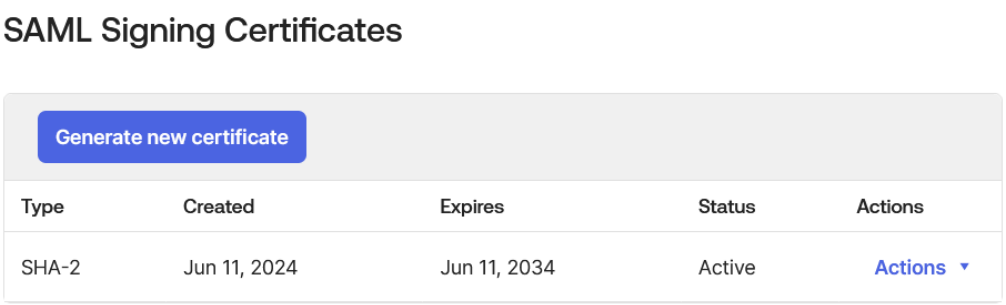
1. Azure AD(Microsoft Entra ID)- seamless integration with AWS SSO, supports SAML and SCIM, enables automated user provisioning, X docs
2. Okta- supports SAML and SCIM

Okta + AWS SSO

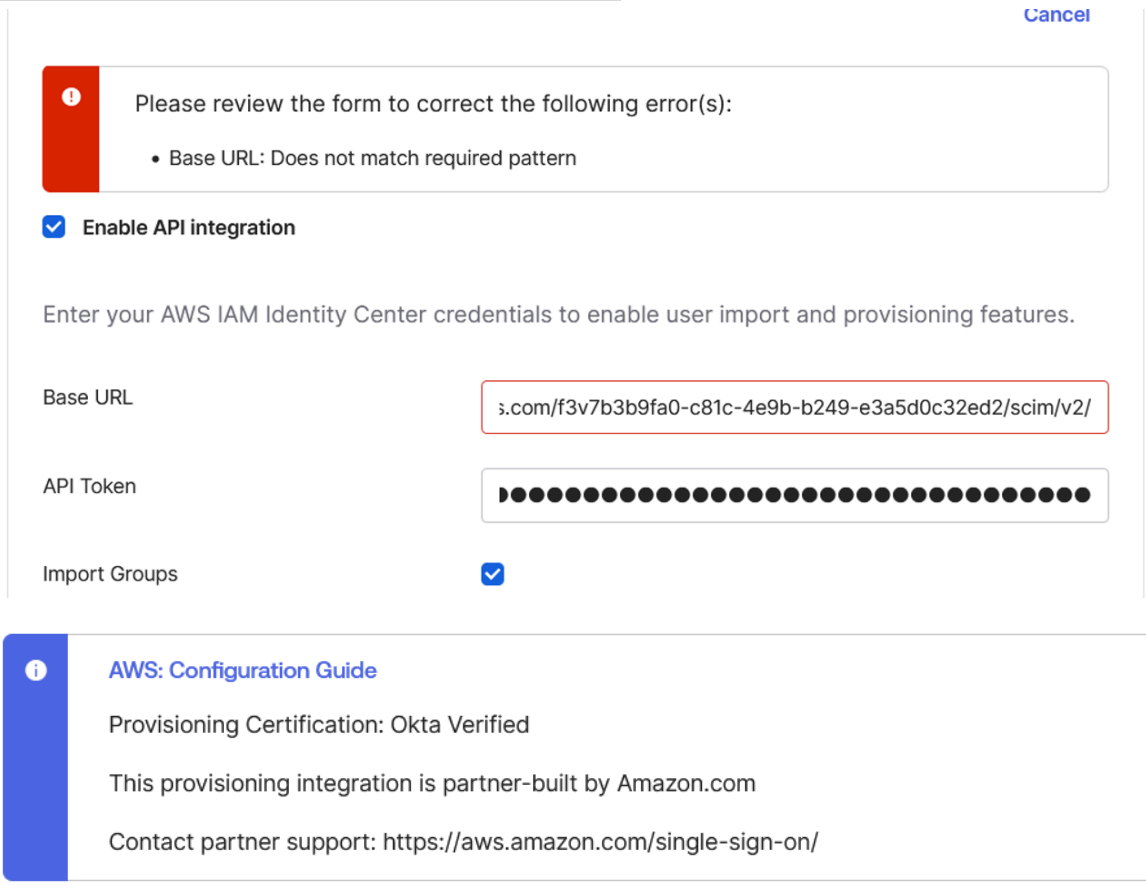

Okta Setup:
Dev side setup: workforce identity cloud

REFERENCED DOCUMENTATION:
https://saml-doc.okta.com/Provisioning_Docs/Okta-Org2Org_Provisioning.html

CREATED THE SAML CERTIFICATE BY ADDING THE IdP METADATA:

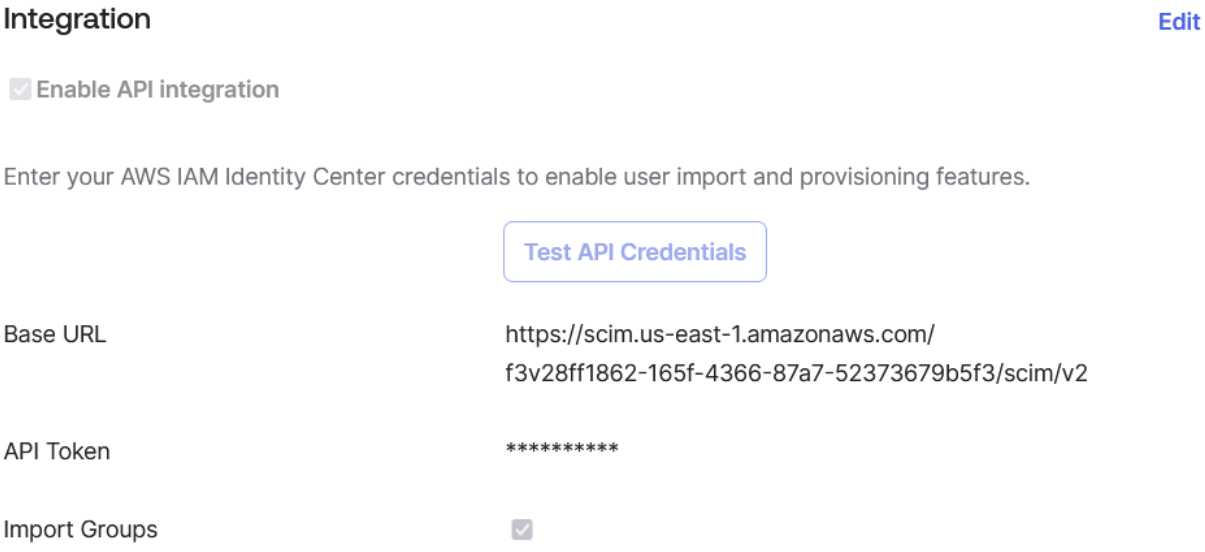


CONFIGURED THE AWS IAM API WITHIN OKTA

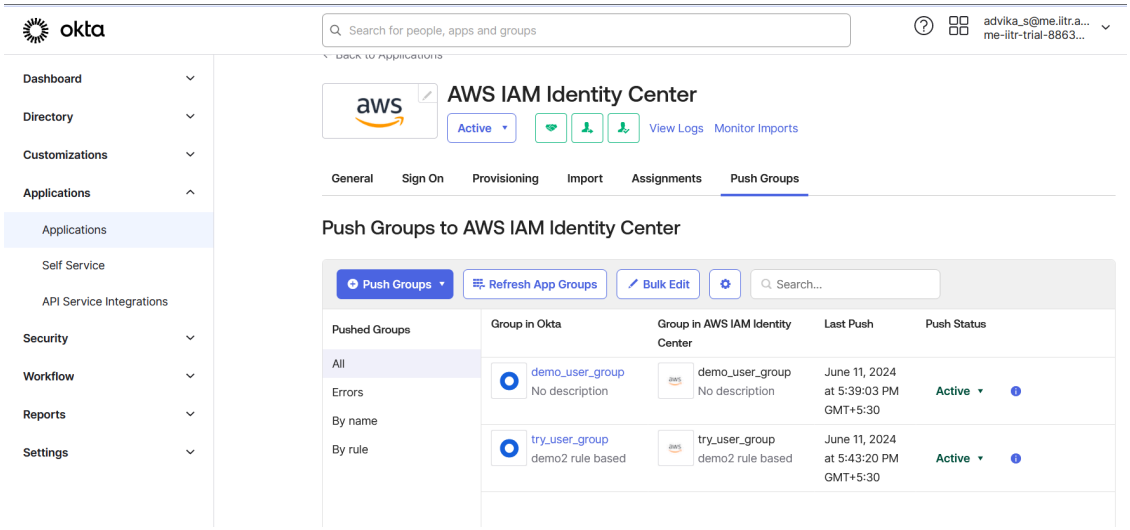


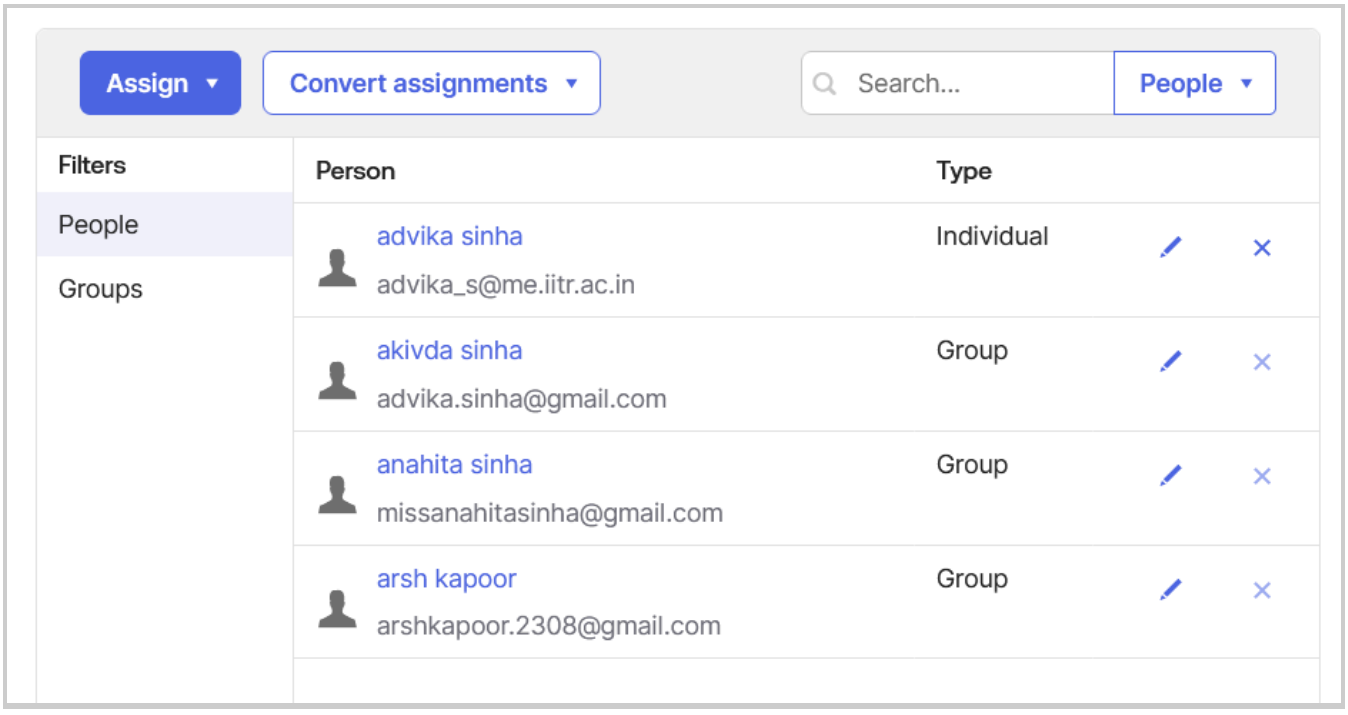




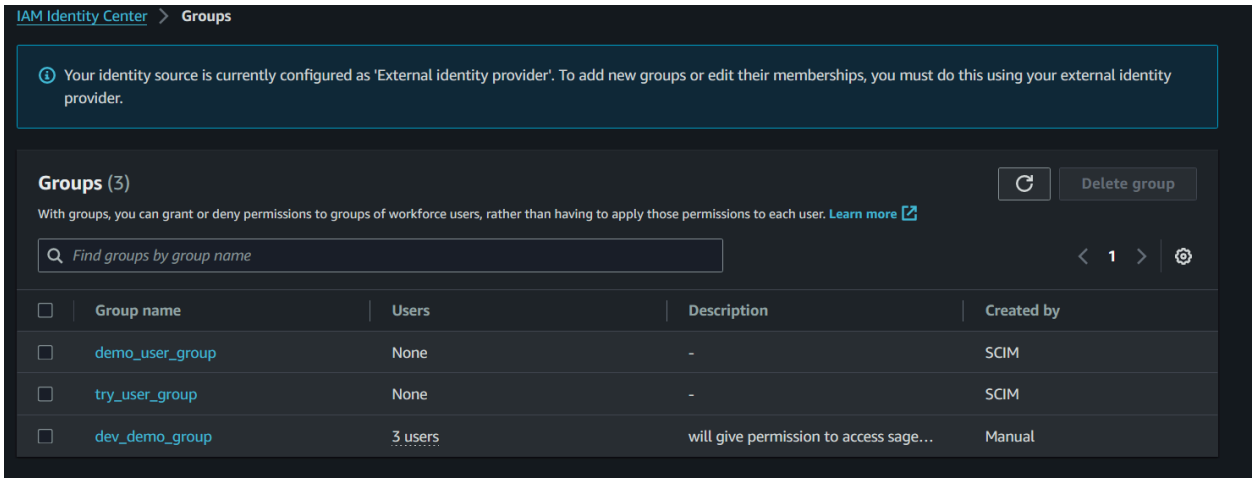


CREATED INDIVIDUAL USERS AND GROUPS TO PUSH TO IAM USING OKTA



PUSHED GROUPS FROM OKTA TO IAM CONSOLE




*The groups pushed are empty because there are no attribute mappings in the users*