

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”

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

Monitor activities in your instances of IAM Identity Center

With AWS CloudTrail, you can monitor and audit activity in your organization instance and account instances of IAM Identity Center. [Learn about monitoring IAM Identity Center](#)

IAM Identity Center setup (red arrow)

Confirm your identity source

The identity source is where you administer users and groups, and it is the service that authenticates your users. By default, IAM Identity Center creates an Identity Center directory. [Learn more about identity sources](#)

Confirm identity source (red box)

Manage permissions for multiple AWS accounts

Give users and groups access to specific AWS accounts in your organization. [Learn more about multi-account permissions](#)

Manage permissions

US East (N. Virginia) | us-east-1

Organization ID o-rg69g9u1si

AWS access portal URL - Edit <https://d-9067d1a147.awsapps.com/start>

Issuer URL <https://identitycenter.amazonaws.com/ssoins-72235769295ffdf5>

What's new

Introducing the improved AWS access portal

We've implemented layout updates for improved usability and discoverability of applications, accounts, and roles. We've added a Create shortcut button so you can generate secure shortcut links to AWS Management Console pages that you can bookmark or share with users that

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

Attributes for access control

Configure this option to grant access to users based on specific characteristics. [Learn more](#)

Identity source (red arrow)

Identity source (red arrow)

Choose the directory where you want to manage your users and groups. [Learn More](#)

Actions ▲

Customize AWS access portal URL

Change identity source (red box)

Identity source

Identity source
Identity Center directory

Authentication method
Password

Provisioning method
Direct

AWS access portal URL
<https://d-9067d1a147.awsapps.com/start>

Identity store ID
d-9067d1a147

Issuer URL
<https://identitycenter.amazonaws.com/ssoins-72235769295ffdf5>

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

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

IAM Identity Center > Settings > Change identity source

Step 1
[Choose identity source](#)

Step 2
Configure external identity provider

Step 3
Confirm change

Configure external identity provider

Service provider metadata

Your identity provider (IdP) requires the following IAM Identity Center certificate and metadata information to trust IAM Identity Center as a service provider. You can copy and paste this information, type it in the service provider configuration interface for your IdP, or download the IAM Identity Center metadata file and upload it to your IdP.

AWS access portal sign-in URL
 [Copy](#) https://[REDACTED].amazon.com/start

IAM Identity Center Assertion Consumer Service (ACS) URL
 [Copy](#) https://us-east-1.signin.aws.amazon.com/platform/saml<REDACTED>:768

IAM Identity Center issuer URL
 [Copy](#) https://us-east-1.signin.aws.amazon.com/platform/<REDACTED>:7

[Download metadata file](#)

Identity provider metadata

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.

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'

The screenshot shows the Okta Applications page. On the left, there's a sidebar with a navigation menu. The 'Applications' item under 'Applications' is highlighted with a red box. The main content area is titled 'Applications' and contains a message about the Developer Edition app limit. Below the message are four buttons: 'Create App Integration' (blue), 'Browse App Catalog' (red box), 'Assign Users to App' (light blue), and 'More' (light blue). To the right of these buttons is a search bar labeled 'Search'. Below the search bar is a table with two rows: 'ACTIVE' (0) and 'INACTIVE' (0). Each row has a small icon and a link: 'Okta Admin Console', 'Okta Browser Plugin', 'Okta Dashboard', and 'Okta OIN Submission Tester'.

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

The screenshot shows the 'Browse App Integration Catalog' page. The sidebar on the left shows the 'Applications' menu is expanded, with 'Applications' highlighted. The main content area shows a search bar with 'AWS IAM' typed into it. A red circle highlights the search input field. Below the search bar is a table of 'Use Case' categories. To the right of the table is a search results panel. The 'AWS IAM Identity Center' result is highlighted with a red box. It includes a thumbnail with the AWS logo, the text 'AWS IAM Identity Center', and a description 'Workflow Templates, SCIM, Workflows Conn...'. Other results include 'Bookmark App', 'SCIM 2.0 Test App', 'Okta Org2Org', and 'Template App'. Further down, there are entries for 'IAM Connector SCIM', 'Authress Authorization IAM OIDC', and 'Stack Identity Cloud IAM Ops SAML'. At the bottom right of the search results panel is a link 'See All Results →'.

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

The screenshot shows the Okta Applications page. The left sidebar has sections for Dashboard, Directory, Customizations, Applications (selected), Security, Workflow, Reports, and Settings. The main content area shows the path Applications > Catalog > Single Sign-On > AWS IAM Identity Center. It includes a search bar, a breadcrumb trail, a last updated date (August 9, 2022), and a red "Add Integration" button. The central panel displays the "AWS IAM Identity Center" integration card, which features the AWS logo, tabs for Workflow Templates, Workflows Connectors, SAML, and SCIM, and a description: "Manage SSO access to your AWS accounts, roles, and applications". Below the card, there's an "Okta Verified" badge and an "Overview" section.

The screenshot shows the "Add AWS IAM Identity Center" configuration screen. The "General Settings" tab is selected. The form contains fields for "Application label" (set to "JJTech-App-IAM-ID-Center") and "Application Visibility" (with a checked checkbox for "Do not display application icon to users"). To the right, a "General settings" sidebar provides instructions: "All fields are required to add this application unless marked optional." At the bottom are "Cancel" and "Done" buttons.

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

The screenshot shows the AWS IAM Identity Center interface. The top navigation bar includes the AWS logo, a search bar, and tabs for Active, View Logs, and Monitor Imports. Below the navigation is a sub-navigation bar with tabs: General, Sign On (which is selected and highlighted with a red box), Provisioning, Import, Assignments, and Push Groups. The main content area is titled "Settings" and contains a section for "Sign on methods". It explains that the sign-on method determines how users sign into and manage their credentials. It notes that some methods require additional configuration in a 3rd party application. It also states that the application username is determined by user profile mapping. A link to "Configure profile mapping" is provided. Under "Sign on methods", there is a radio button selected for "SAML 2.0". This section includes fields for "Default Relay State" (checkbox checked), "Disable Force Authentication" (checkbox checked), "Maximum App Session Lifetime" (checkbox unchecked), and "Send value in response" (checkbox unchecked). Below this is a "Metadata details" section with a "Metadata URL" field containing the value "https://dev-51904097.okta.com/app/exkjavuys5E4fBPdP5d7/sso/saml/metadata" and a "Copy" button. To the right of the main content is a sidebar titled "About" which provides information about SAML 2.0. At the bottom right of the main content area is a blue button with the text "View SAML setup instructions", which is also highlighted with a red box and has a red arrow pointing towards it from the bottom right.

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**

The screenshot shows the Okta application settings interface for an AWS IAM Identity Center application. The left sidebar shows navigation options like Dashboard, Directory, Customizations, Applications (selected), Self Service, API Service Integrations, Your OIN Integrations, Security, Workflow, Reports, and Settings. The main content area has two sections: 'Advanced Sign-on Settings' and 'Credentials Details'. In 'Advanced Sign-on Settings', there is a 'Metadata URL' field containing `https://dev-51904097.okta.com/app/exkjavuys5E4fBPdP5d7/sso/saml/metadata`, with a 'Copy' button. Below it is a 'More details' link. In 'Credentials Details', there are fields for 'Application username format' (set to 'Okta username'), 'Update application username on' (set to 'Create and update'), and 'Password reveal' (with a note: 'Allow users to securely see their password (Recommended)'). A blue info icon next to the note says 'Password reveal is disabled, since this app is using SAML with no password.' At the bottom right is a 'Save' button.

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.

SAML Signing Certificates

The screenshot shows the Okta SAML Signing Certificates interface. At the top right, there's a "SAML Setup" button. Below it is a table with one row, showing a certificate entry:

Type	Created	Expires	Status	Actions
SHA-2	Today	Sep 2032	Active	Actions

A context menu is open over the "Actions" button, containing options: "View IdP metadata" and "Download certificate". At the bottom right of the table area, there's a "Sign On Policy" button.

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.

```

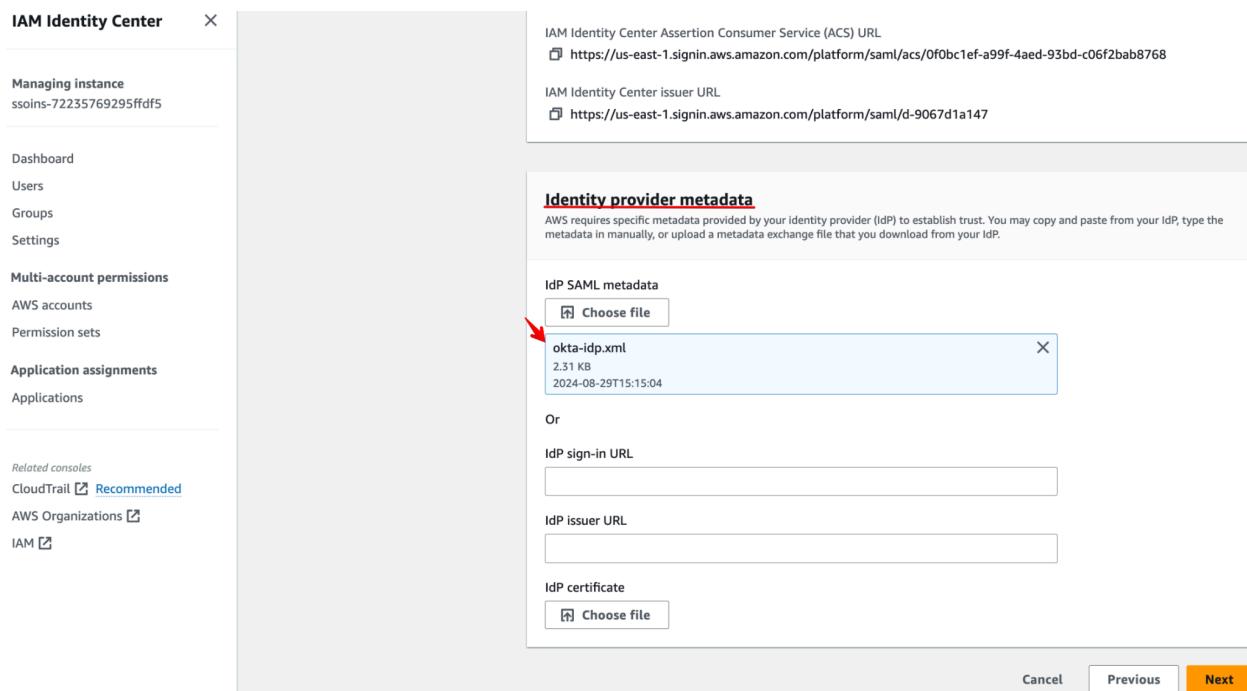
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://www.okta.com/exk6eckp9qS0qnITw5d7">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIDQgDCCApCgAwIBAgIgAYMPeBGqMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2fsawZvcm5pYTEwMBQGA1UEBwwNU2fUIEZyW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUhJvdmlkZXIxFTATBgNVBAMMDGr1di04NzA3NjIyMjEcMB0GCSqGSIb3DQEJ
ARYNaW5mb0Bva3RhLmNvbAeFw0yMjA5MDUxOTA5NTRaFw0zhjA5MDUxOTExNTRaMIGUMQswCQYD
VQ0GEwJVUzETMBEAGA1UECawKQ2fsawZvcm5pYTEwMBQGA1UEBwwNU2fUIEZyW5jaXNjbzENMAsG
A1UECgwET2t0YTEUMBIGA1UECwwLU1NPUhJvdmlkZXIxFTATBgNVBAMMDGr1di04NzA3NjIyMjEc
MB0GCSqGSIb3DQEJARYNaW5mb0Bva3RhLmNvbTCCASiDQYJKoZIhvNAQEQQADggEPADCCAQoC
ggEBAMGiMnew2q0EXXpLHw+bIenTJ3g1w9qb0IMnaewFg/C2yemCxLNaiUUCCCCpyO0UJ2y9VUmsht+
CEWxWfh0iRPysZt6ZEov0LrjKJ/Hyz0h12yBkccFpA6NVJhBh6mRi2zVQKLdnC80cVEB5kbGnj
8e/S6Zdy5fnjaIm7v0g4nxm6LOGsjCm8kiFRNQu1P+jYPPVwldu68++kp0zj3TQXAUf0HFc
jjsuo68lb8jMuSEXGjgST/SogYZ0GmpSE4+jh81vGKv5Vxd3/pnXA84e4jjJTXKFnxQt2negOpU
YoNQQG/tHQ5CTyff2DUmLOZELxPqR4+ajfmRZYEsCaEAATANBgkqhkiG9w0BAQsFAAOCAQEA
AGHmgdc1j2S3jn24CGOC1k//70FDXvd+f2pzNRV6u5YdqalozAxqcGwA06Ko2V/P77vhvWrtnZw
ozcvZkFOTYEFbwucCoc5DE2/NNwIyoRVOLqgj7/AsCtf000c8VFn6c5lpLgvrQTGkUr4CURqTF1
7SY7bYcfWfn3fGhcaK23AeDPySR1TmID/oLxTG7EFHtGSA3jJ40PvYmrwOA/dJcWxJ6gIxdyTe12
Qe700aPkPem8sYRqKXifusWQTza8IczpqpkKYktuaIXUV5VhrPTbhFxlamXBaz+MMAnQ01V0CB 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/exk6eckp9qS0qnITw5d7/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/exk6eckp9qS0qnITw5d7/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 X

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



Choose identity source

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://.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 metadata

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

The screenshot shows the AWS IAM Identity Center settings page. On the left, there's a sidebar with options like Dashboard, Users, Groups, and Settings (which is selected). Below that are Multi-account permissions, AWS accounts, and Permission sets. Under Application assignments, it lists Applications and IAM. At the bottom of the sidebar, it says 'Related consoles' with CloudTrail (Recommended) and AWS Organizations. The main content area has tabs for Instance name, Region, Delegated administrator, and Identity-aware sessions. Below these are three sections: 'Enable identity-aware sessions' (with an 'Enable' button), 'Attributes for access control' (with an 'Enable' button), and 'Automatic provisioning' (with an 'Enable' button that is highlighted with a red box). At the bottom of the main content area are tabs for Identity source, Authentication, Management, and Tags.

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

The screenshot shows the AWS IAM Identity Center configuration page within the Okta interface. The 'Provisioning' tab is active. On the right, there's a section titled 'AWS: Configuration Guide' with information about provisioning certification and contact support. Below this, a message states 'Provisioning is not enabled' and provides instructions to enable provisioning. A prominent red box surrounds the 'Configure API Integration' button.

- o **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**

This screenshot shows the 'Configure API Integration' dialog box. It includes a checkbox labeled 'Enable API integration' which is checked and highlighted with a red box. Below the checkbox, there's a note: 'Enter your AWS IAM Identity Center credentials to enable user import and provisioning features.' There are two input fields: 'Base URL' containing '< your SCIM endpoint here >' and 'API Token' containing '< YOUR TOKEN HERE>'. At the bottom, there are 'Test API Credentials' and 'Save' buttons.

- o Click Test API Credentials if you get an error:

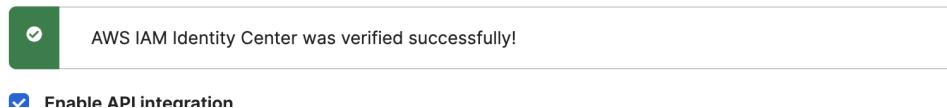


Please review the form to correct the following error(s):

- Base URL: Does not match required pattern

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

A successful test pic shown below:



* Click **Save**

General Sign On Mobile Provisioning Import Assignments Push Groups

SETTINGS

To App To Okta Integration

Provisioning to App

Create Users

Creates or links a user in AWS Single Sign-on when assigning the app to a user in Okta.
The [default username](#) used to create accounts is set to Okta username.

Enable

Update User Attributes

Okta updates a user's attributes in AWS Single Sign-on when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in AWS Single Sign-on.

Enable

Deactivate Users

Deactivates a user's AWS Single Sign-on account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

Enable

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

The screenshot shows the AWS IAM Identity Center interface with the 'Provisioning' tab selected. On the left, a sidebar lists 'Settings' with 'To App' selected, 'To Okta', and 'Integration'. The main area shows a flow from 'okta' to 'aws'. Under 'Provisioning to App', there are three sections: 'Create Users' (checkbox checked), 'Update User Attributes' (checkbox checked), and 'Deactivate Users' (checkbox checked). A large red box highlights the 'Enable' checkboxes for all three sections. At the bottom right is a red-bordered 'Save' button.

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: **realmAWS**

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

[← Back to Applications](#)

AWS IAM Identity Center

Active ▾ View Logs Monitor Imports

General Sign On Provisioning Import Assignments Push Groups

Push Groups to AWS IAM Identity Center

Pushed Groups

All Errors By name By rule

Push groups by rule

Create a search rule that pushes any matching groups to AWS IAM Identity Center automatically.

Rule name: AWS Groups

Group name: starts with realmAWS

Group description: starts with Enter string to match...

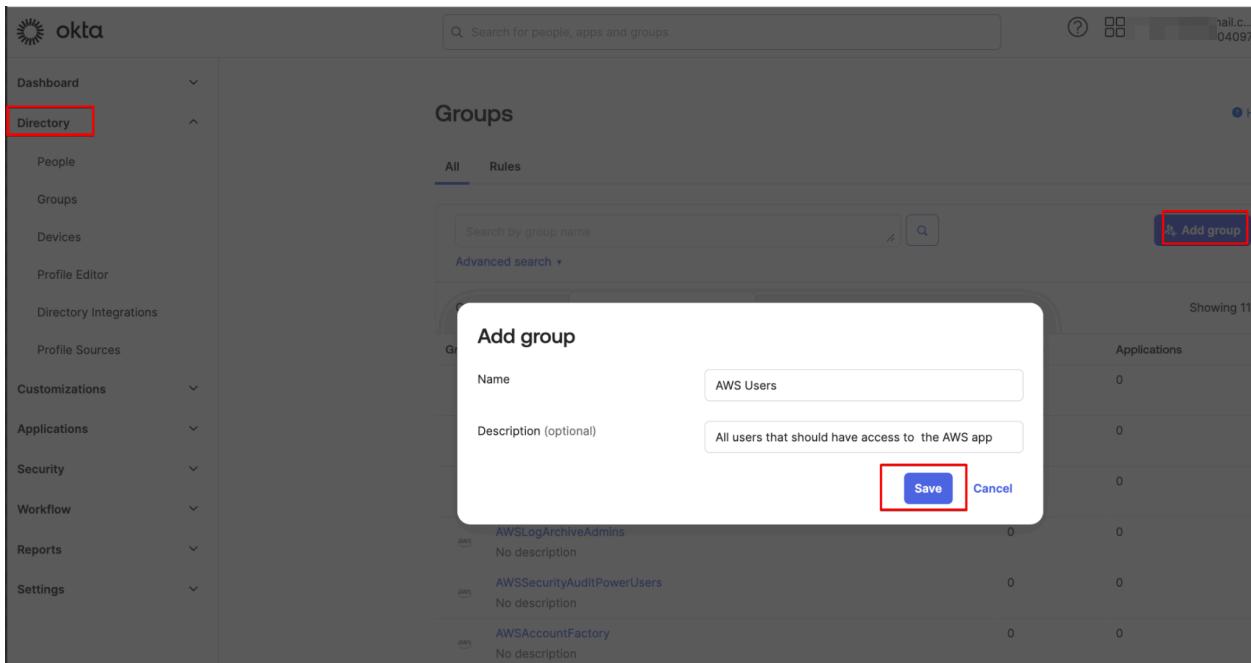
Immediately push groups found by this rule

Create Rule Cancel

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

The screenshot shows the Okta interface. On the left, a sidebar menu includes 'Dashboard', 'Directory' (expanded to show 'People' and 'Groups'), 'Devices', 'Profile Editor', 'Directory Integrations', 'Profile Sources', 'Customizations' (expanded to show 'Applications'), 'Security', 'Workflow', and 'Reports'. The 'Groups' item is highlighted with a red arrow. The main content area is titled 'AWS Users' with a subtitle 'All users that should have access to the AWS app'. It shows creation and modification dates (Created: 8/29/2024, Last modified: 8/29/2024) and a 'View logs' link. Below this, a navigation bar has tabs for 'People', 'Applications' (which is selected and highlighted with a red box), 'Profile', 'Directories', and 'Admin roles'. A sub-section titled 'Applications' shows a list of user IDs: 01101110, 01101111, 01101100, 01101000, 0110101, 01101110, and 01100111. A button labeled 'Assign applications' is also highlighted with a red box.

c. Click **Assign**

- This is the app users will launch into the AWS Console
- Leave all fields blank

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

The screenshot shows the Okta interface with a dark theme. On the left, a sidebar menu includes 'Dashboard', 'Directory' (expanded to show 'People' and 'Groups'), 'Devices', 'Profile Editor' (selected and highlighted with a blue box), 'Directory Integrations', 'Profile Sources', 'Customizations' (expanded to show 'Applications'), 'Security', 'Workflow', 'Reports', and 'Settings'. The main content area shows a list of user profile fields with their corresponding Okta attribute names. Fields include: Preferred language (user.preferredLanguage), Locale Name (user.locale), Time zone (user.timezone), User type (user.userType), Cost center (user.costCenter), Organization (user.organization), Division (user.division), and Department (user.department). Each field has a note indicating it is the default value with an 'Override' link. At the bottom, there are 'Save and Go Back' and 'Cancel and Go Back' buttons.

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`. 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: `realmAWSFinOpsUsers`
 - 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 `realmAWSFinOpsUsers` listed and marked as Active

The screenshot shows the AWS IAM Identity Center interface. At the top, there's a navigation bar with the AWS logo, a search bar, and tabs for Active, General, Sign On, Provisioning, Import, Assignments, and Push Groups. The Push Groups tab is currently selected. Below the tabs, there's a heading "Push Groups to AWS IAM Identity Center". A sidebar on the left lists filtering options: Pushed Groups (All, Errors, By name, By rule, AWS Groups), Group in Okta (realmAWSFinOpsUsers, Cross Account Financ...), Group in AWS IAM Identity Center (realmAWSFinOpsUsers, Cross Account Financ...), Last Push (August 29, 2024 at 4:34:43 PM GMT+2), and Push Status (Active). The main table area displays the pushed group details.

Pushed Groups	Group in Okta	Group in AWS IAM Identity Center	Last Push	Push Status
All	realmAWSFinOpsUsers Cross Account Financ...	realmAWSFinOpsUsers Cross Account Financ...	August 29, 2024 at 4:34:43 PM GMT+2	Active
Errors				
By name				
By rule				
AWS Groups				

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

	Group name	Users	Description	Created by
<input type="checkbox"/>	AWSLogArchiveAdmins	None	Admin rights to log archive ac...	Manual
<input type="checkbox"/>	AWSServiceCatalogAdmins	None	Admin rights to account facto...	Manual
<input type="checkbox"/>	DevOpsAdmin	2 users	-	Manual
<input type="checkbox"/>	AWSControlTowerAdmins	1 user	Admin rights to AWS Control ...	Manual
<input type="checkbox"/>	AWSAccountFactory	1 user	Read-only access to account f...	Manual
<input checked="" type="checkbox"/>	realmAWSFinOpsUsers	None	-	SCIM
<input type="checkbox"/>	AWSecurityAuditPowerUsers	None	Power user access to all accou...	Manual
<input type="checkbox"/>	AWSecurityAuditors	None	Read-only access to all accoun...	Manual

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
 - o Select **Predefined Permission set**
 - o scroll down select **Billing**, then click **Next**
 - o leave everything as default and click **Next**
 - o Click **Create**

Assign Permission Set

Click on “Billing” in the list of permission sets
 Billing - Permissions tab
 0 Click Edit
 0 Delete
<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) `realmAWSFinOpsUsers` 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**

The screenshot shows the AWS IAM Identity Center interface for managing AWS accounts. At the top, there's a search bar and buttons for 'Hierarchy' and 'List'. Below that, the 'Organizational structure' section shows a tree view with 'Root' expanded, revealing 'r-2uwt' and two child nodes, one of which is 'management account'. This node has a red box around its checkbox. To the right, under 'Permission sets', a list of available sets is provided: AWSAdministratorAccess, AWSPowerUserAccess, AWSReadOnlyAccess, and '3 more'. The 'Assign users or groups' button at the top right is also highlighted with a red box.

- To Assign Users:
 - Click the **Groups** tab
 - Check `realmAWSFinOpsUsers`
 - 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 realmAWSFinOpsUsers
 - 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**

Add Person

User type ?

First name

Last name

Username

Primary email

Groups (optional)

Activation

I will set password

User must change password on first login

Do not send unsolicited or unauthorized activation emails. [Read more](#)

Go back to people, select the user you 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 you 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 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:
 - aliasAWSFinOpsUsers
 - AWS Users
- Close the Okta account [optional]

Copyright 2020, Amazon Web Services, All Rights Reserved.