# PRJ-SEC-010: Identity Federation & SSO with Okta

## AWS Console Step-by-Step Deployment Guide

**Author:** Mo Suleiman | **Project:** PRJ-SEC-010 | **Certification:** AWS Security Specialty — Identity & Access Management

## Overview

This guide provides a comprehensive walkthrough for setting up identity federation and Single Sign-On (SSO) between **Okta** and **AWS IAM Identity Center**. This architecture eliminates the need for long-lived IAM users and allows your team to access AWS using their existing corporate Okta credentials, enforcing centralized identity management and the principle of least privilege.

## GRC Mapping

| Framework | Control | Description |
|---|---|---|
| **NIST CSF** | PR.AC-1 | Identity and access management policies and procedures are established. |
| **ISO 27001** | A.9.1.1 | An access control policy shall be established, documented, and reviewed. |
| **PCI-DSS** | Req. 8.1 | Assign all users a unique ID before allowing them to access system components or cardholder data. |
| **SOC 2** | CC6.1 | The entity implements logical access security software, infrastructure, and architectures. |
| **Business Value** | — | Centralizes user lifecycle management, reduces credential sprawl, improves user experience, and provides a single, auditable point of entry into the AWS environment. |

## Authentication Flow with Okta

1. **Login Request:** A user navigates to the AWS access portal URL.
2. **Redirection to Okta:** IAM Identity Center redirects the user to your Okta organization for authentication.
3. **Okta Authentication:** The user authenticates with their Okta credentials and MFA.
4. **SAML Assertion:** Okta sends a SAML 2.0 assertion back to IAM Identity Center, containing the user's identity and group memberships.
5. **Role Assumption:** IAM Identity Center validates the assertion, maps the user's Okta groups to AWS Permission Sets, and uses STS to generate temporary credentials.
6. **Console Access:** The user is redirected to the AWS Management Console, fully authenticated with the appropriate role.

---

# Prerequisites

- **AWS Account:** You must be signed into the **AWS Organizations management (root) account** with `AdministratorAccess` or the `AWSSSOMasterAccountAdministrator` managed policy. IAM Identity Center cannot be enabled from a member account.
- **AWS Organizations:** Must be enabled with at least one member account visible.
- **AWS Region:** Choose a single home region (e.g., `us-east-1`) for IAM Identity Center. All configuration must be done in this region, and it cannot be changed later without a full teardown.
- **Okta Developer Account:** A free Okta Developer account (Integrator Free Plan). You can sign up at developer.okta.com. *Note: You must use a business or school email address to sign up; personal emails like Gmail may be rejected.*

---

# Part 1: Configure Okta

## 1.1 — Create Groups in Okta

First, we simulate corporate user groups in Okta.

1. Log in to your Okta Admin Console.
2. Navigate to **Directory → Groups**.
3. Click **Add Group**.
   - **Name:** `aws-administrators`
   - **Description:** `Users with full administrator access to the AWS production account.`
4. Click **Save**.
5. Repeat the process to create a second group named `aws-developers`.

## 1.2 — Create Users and Assign to Groups

1. Navigate to **Directory → People → Add person**.

2. Create two users:
    - `jane.doe@yourdomain.com` (as an Administrator)
    - `john.doe@yourdomain.com` (as a Developer)
3. Assign `jane.doe` to the `aws-administrators` group and `john.doe` to the `aws-developers` group. Sam Blue Mary Pink

### 1.3 — Create the AWS IAM Identity Center Application in Okta

4. Navigate to **Applications → Applications → Browse App Catalog**.
5. Search for **AWS IAM Identity Center** and select it.
6. Click **Add Integration**.
7. On the **Sign On** tab, click **Edit**.
8. Scroll down to **SAML Signing Certificates**.
9. Click the **Actions** dropdown next to the active certificate and select **View IdP Metadata**. This will open an XML file in a new tab.
10. Save the page to your computer as `metadata.xml` (File → Save As). You will need this for the AWS configuration.

---

## Part 2: Configure AWS IAM Identity Center

### 2.1 — Enable IAM Identity Center

1. In the AWS Management Console, navigate to **IAM Identity Center**. Ensure you are in your chosen home region (e.g., `us-east-1`).
2. If it is not already enabled, click **Enable**. This will set up the necessary resources in your AWS Organization.
3. Once enabled, copy the **AWS access portal URL** to your text editor.

## 2.2 — Change the Identity Source to Okta

1. In the IAM Identity Center console, go to **Settings**.
2. Under **Identity source**, click **Actions → Change identity source**.
3. Select **External identity provider** and click **Next**.
4. Under **Service provider metadata**, copy the **IAM Identity Center ACS URL** and the **IAM Identity Center issuer URL** to your text editor.
5. Under **Identity provider metadata**, click **Choose file** and upload the `metadata.xml` file you downloaded from Okta.
6. Click **Next**, type `ACCEPT`, and confirm the change.

## 2.3 — Configure AWS Values and SAML Attributes Back in Okta

*This is a critical step to ensure the two-way SAML handshake works.*

1. Return to your Okta Admin Console → **Applications → AWS IAM Identity Center**.
2. Go to the **Sign On** tab and click **Edit**.
3. Under **Advanced Sign-on Settings**, paste the **ACS URL** into the `ACS URL` field and the **Issuer URL** into the `Audience URI (SP Entity ID)` field.
4. Set **Application username format** to `Email`.
5. Under **Attribute Statements**, ensure the following is configured:
   - **Name:** `https://aws.amazon.com/SAML/Attributes/email`
   - **Value:** `user.email`
6. Ensure the **Subject (NameID)** format is set to `EmailAddress`.
7. Click **Save**.

## 2.4 — Assign Groups to the Okta Application

*Before you can push groups to AWS, they must be assigned to the app.*

1. In the Okta app, go to the **Assignments** tab.
2. Click **Assign → Assign to Groups**.
3. Select both `aws-administrators` and `aws-developers` and click **Assign**.

4. Click **Done**.

### 2.5 — Configure Automatic Provisioning (SCIM)

This step automatically syncs users and groups from Okta to AWS.

1. In the AWS IAM Identity Center **Settings**, under **Automatic provisioning**, click **Enable**.
2. Copy the **SCIM endpoint** and the **Access token** to your text editor. *(Note: The Access token is shown only once. Save it securely.)*
3. Go back to your Okta application → **Provisioning** tab → **Configure API Integration**.
4. Check **Enable API integration**.
5. Paste the **SCIM endpoint** into the **Base URL** field and the **Access token** into the **API Token** field.
6. Click **Test API Credentials**. You should see a success message.
7. Click **Save**.
8. Under **To App**, click **Edit** and enable **Create Users**, **Update User Attributes**, and **Deactivate Users**. Click **Save**.
9. Go to the **Push Groups** tab. Click **Push Groups → Find groups by name**.
10. Find and push both `aws-administrators` and `aws-developers`.

> *Your Okta users and groups will now automatically sync to IAM Identity Center.*

---

## Part 3: Create and Assign Permission Sets

### 3.1 — Create Permission Sets

1. In IAM Identity Center, go to **Permission sets → Create permission set**.
2. Choose **Use an existing AWS managed policy**.
3. Select `AdministratorAccess`.
4. Name the permission set `Okta-Administrator-Access` and set the session duration to **1 hour**.

5. Repeat to create a second permission set named `Okta-Developer-ReadOnly-Access` using the `ReadOnlyAccess` policy.

### 3.2 — Assign Groups to Permission Sets

1. Go to **AWS accounts**.
2. Select your **production** AWS account from the list.
3. Click **Assign users or groups**.
4. On the **Groups** tab, select `aws-administrators`.
5. Click **Next**.
6. Select the `Okta-Administrator-Access` permission set.
7. Click **Next** and **Submit**.
8. Repeat the process to assign the `aws-developers` group to the `Okta-Developer-ReadOnly-Access` permission set in your **development** account.

---

## Part 4: Test the SSO Experience

1. Open a new incognito browser window.
2. Navigate to the **AWS access portal URL**.
3. You will be immediately redirected to the Okta login page.
4. Log in as `jane.doe`.
5. You will be redirected back to the AWS portal, where you will see the production account with the `Okta-Administrator-Access` role.
6. Click **Management console** to access the AWS Console with full admin rights.
7. Log out and log back in as `john.doe`. You will see the development account with read-only access.

---

## Part 5: Cleanup

1. **Remove account assignments** in IAM Identity Center.

2. **Delete the Permission Sets**.
3. **Disable automatic provisioning** in IAM Identity Center.
4. **Change the identity source** back to the Identity Center directory.
5. In Okta, **deactivate and delete** the AWS IAM Identity Center application.
6. **Delete the users and groups** in Okta.