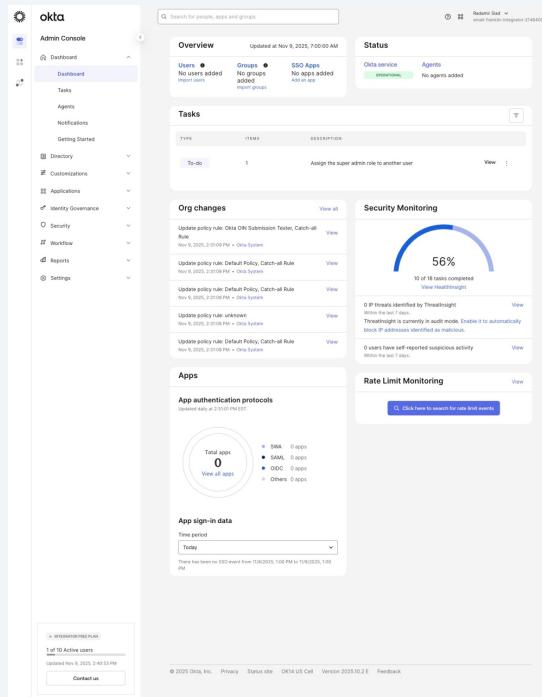


# Configure AWS IAM Identity Center with Okta

Scribe 

1

Navigate and authenticate to the site <https://integrator-2146409-admin.okta.com/admin/dashboard>



The screenshot shows the Okta Admin Console dashboard. On the left, there's a sidebar with navigation links: Admin Console, Dashboard, Tasks, Agents, Notifications, Getting Started, Directory, Customizations, Applications, Identity Governance, Security, Workflow, Reports, and Settings. The main area has several sections:

- Overview:** Shows 0 users added, 0 groups added, 0 SSO Apps added, and 0 agents added. It also shows the status of Okta services (green) and Agents (yellow).
- Tasks:** A table with one task: "Assign the super admin role to another user".
- Org changes:** A list of recent policy rule updates:
  - Update policy rule: Okta CN Submission Tester, Catch-all Rule (Nov 9, 2023, 2:30:09 PM) - Okta System
  - Update policy rule: Default Policy, Catch-all Rule (Nov 9, 2023, 2:30:08 PM) - Okta System
  - Update policy rule: Default Policy, Catch-all Rule (Nov 9, 2023, 2:30:08 PM) - Okta System
  - Update policy rule: Default Policy, Catch-all Rule (Nov 9, 2023, 2:30:08 PM) - Okta System
  - Update policy rule: Default Policy, Catch-all Rule (Nov 9, 2023, 2:30:08 PM) - Okta System
- Security Monitoring:** A progress bar at 56% completion of 18 tasks. It also shows 0 IP threats identified by ThreatInsight and 0 users have self-reported suspicious activity.
- Rate Limit Monitoring:** A button to search for rate limit events.
- Apps:** A section showing 0 total apps, categorized as 0 SSO, 0 APIs, 0 OAuth, 0 SAML, 0 OpenID Connect, and 0 Others.
- App sign-in data:** A chart showing sign-in data for today, indicating no SSO events from 11/9/2023, 10:00 PM to 11/10/2023, 1:00 AM.

At the bottom, there's a footer with links to Information Plan, 1 of 10 Active users, Contact us, and copyright information: © 2023 Okta, Inc. Privacy Status site OKTA US Cell Version 2023.10.2 E Feedback.

2

Successful login would look like this

The screenshot shows the Okta Admin Console dashboard. On the left, there's a sidebar with navigation links: Dashboard, Tasks, Agents, Notifications, Getting Started, Directory, Customizations, Applications, Identity Governance, Security, Workflow, Reports, and Settings. The main area has several sections:

- Overview**: Updated at Nov 9, 2025, 7:00:00 AM. It shows 0 users, 0 groups, and 0 SSO Apps. Buttons for Import users, Import groups, Add user, and Add group are available.
- Status**: Shows Okta service (OPERATIONAL) and Agents (No agents added).
- Tasks**: A table with one item: "To-do" (1 item), "Assign the super admin role to another user". A "View" button is next to it.
- Org changes**: A list of policy rule updates:
  - Update policy rule: Okta OIN Submission Tester, Catch-all Rule (Nov 9, 2025, 2:31:09 PM • Okta System)
  - Update policy rule: Default Policy, Catch-all Rule (Nov 9, 2025, 2:31:08 PM • Okta System)
  - Update policy rule: Default Policy, Catch-all Rule (Nov 9, 2025, 2:31:08 PM • Okta System)
  - Update policy rule: unknown (Nov 9, 2025, 2:31:08 PM • Okta System)
  - Update policy rule: Default Policy, Catch-all Rule (Nov 9, 2025, 2:31:08 PM • Okta System)A "View all" link is at the top right.
- Security Monitoring**: A progress bar showing 56% completion (10 of 18 tasks completed). It also lists 0 IP threats identified by ThreatInsight (Within the last 7 days) and 0 users have self-reported suspicious activity (Within the last 7 days). A "View HealthInsight" link is present.
- Rate Limit Monitoring**: A section with a search bar: "Click here to search for rate limit events".
- Apps**: A section showing 0 total apps. It includes a chart and a legend: SWA (0 apps), SAML (0 apps), and OAuth (0 apps).

3

Under "Directory" select "People" -> Users can be created here. Users created are Alice Johnson and Bob Miller

The screenshot shows the Okta Admin Console interface. On the left, there is a sidebar with various navigation options under 'Admin Console'. The 'People' option is highlighted. The main area is titled 'People' and contains a search bar at the top. Below the search bar are buttons for 'Add person', 'Reset passwords', and 'More actions'. A table displays user information, showing one user named Radamir Siad with the primary email siad02@email.franklin.edu and status Active. There are also buttons for 'Advanced search' and 'Status' (set to All). The bottom right corner of the main content area has a vertical scroll bar.

Person & username	Primary email	Status
Radamir Siad siad02@email.franklin.edu	siad02@email.franklin.edu	Active

4

Under "Directory" select "Groups". Groups can be created here. Groups created are Managers and Marketing.

The screenshot shows the Okta Admin Console interface. On the left, there is a sidebar with various navigation options under 'Admin Console'. The 'Groups' option is selected and highlighted in blue. The main content area is titled 'Groups' and shows a list of existing groups. There is a search bar at the top of the list. A button labeled 'Add group' is visible. The table lists two groups: 'Everyone' and 'Okta Administrators'. The 'Okta Administrators' row has a circled orange highlight around it. The table includes columns for 'Group name', 'People', and 'Applications'.

Group name	People	Applications
Everyone All users in your organization	1	0
Okta Administrators Okta manages this group, which contains all administrators in your organization.		

5

Under "Security" select authentication. Adjust security to enable username, password and MFA when logging on

The screenshot shows the Okta Admin Console interface. On the left, there is a navigation sidebar with various menu items like Dashboard, Directory, Customizations, Applications, Identity Governance, Security (which is expanded to show General and HealthInsight), and Authenticators (which is selected and highlighted with a blue background). Below these are sections for Authentication Policies, Global Session Policy, User Profile Policies, Identity Providers, Delegated Authentication, Networks, Behavior Detection, Advanced Posture Checks, Device Assurance Policies, Device Integrations, and Administrators.

The main content area is titled "Authenticators" and has two tabs: "Setup" (which is active) and "Enrollment". Below the tabs is a button labeled "Add authenticator". A table lists the available authenticators:

Name	Factor type	Characteristics	Status	Action
Email	Possession		Active	Actions
Okta Verify	Possession Possession + Knowledge <sup>1</sup> Possession + Biometric <sup>1</sup>	Device bound Hardware protected Phishing resistant (Okta FastPass) <sup>2</sup>	Active	Actions
Password	Knowledge		Active	Actions

At the bottom of the page, there are two small notes: <sup>1</sup> Multiple factor requirements may be satisfied based on the device used to enroll and <sup>2</sup> Phishing resistance may vary based on combinations of apps, browser, operating system, and more. [Learn more](#).

6

As seen below the users Alice Johnson and Bob Miller have been created.

The screenshot shows the Okta Admin Console interface. On the left, there's a sidebar with various navigation options like Dashboard, Directory, People (which is selected and highlighted in blue), Groups, Devices, Profile Editor, etc. The main area is titled 'People' and contains a search bar at the top. Below the search bar are buttons for 'Add person', 'Reset passwords', and 'More actions'. A table lists three users: Bob Miller, Alice Johnson, and Radamir Siad. An orange circle highlights the row for Alice Johnson. The table columns are 'Person & username', 'Primary email', and 'Status'. Alice Johnson's status is 'Pending user action'.

Person & username	Primary email	Status
Bob Miller bobmiller@demo.local	bobmiller@demo.local	Pending user action
Alice Johnson alicejohnson@demo.local	alicejohnson@demo.local	Pending user action
Radamir Siad siad02@email.franklin.edu	siad02@email.franklin.edu	Active

## 7 Groups Marketing and Managers can be seen below.

The screenshot shows the Okta Admin Console interface. On the left, there is a sidebar with various navigation options under 'Admin Console'. The 'Groups' option is selected and highlighted in blue. The main content area is titled 'Groups' and shows a list of four groups:

Group name	People	Applications
Managers No description	0	0
Marketing No description	0	0
Everyone All users in your organization	3	0
Okta Administrators Okta manages this group, which contains all administrators in your organization.		

A blue button labeled 'Add group' is located in the top right corner of the main content area. The entire screenshot is framed by a large white circle.

## 8 Process to add Alice Johnson into the "Marketing" group.

The screenshot shows the Okta Admin Console interface. On the left, there's a sidebar with various navigation options like Admin Console, Dashboard, Directory, People, Groups (which is selected), Devices, Profile Editor, etc. The main area is titled 'Marketing' and shows details about its creation and last modification. Below this, there are tabs for People, Applications, Profile, Directories, and Admin roles, with 'People' being active. A search bar at the top right allows searching for people, apps, and groups. The 'People' section displays a single user entry: 'Alice Johnson' with email 'alicejohnson@demo.local' and status 'Pending user action'. There's also an 'Assign people' button and an orange circular highlight on the status column.

## 9 Process to add Bob Miller in the "Managers" group.

The screenshot shows the Okta Admin Console interface. On the left, there's a sidebar with various navigation options like Dashboard, Directory, People, Groups, Devices, Profile Editor, etc. The 'Groups' option is selected. The main area shows a 'Managers' group page with a search bar at the top. Below it, there's a header with 'Created: 11/9/2025', 'Last modified: 11/9/2025', and a 'View logs' link. A 'Actions' button is also present. The main content area is titled 'People' and contains a table with one row. The table has columns for 'Person & username' and 'Status'. The row shows 'Bob Miller' and 'bobmiller@demo.local' under 'Person & username', and 'Pending user action' under 'Status'. An orange circle highlights the status cell. At the bottom right of the table, there's a blue 'Assign people' button.

Person & username	Status
Bob Miller bobmiller@demo.local	Pending user action

## 10 Adjustments to authentication

The screenshot shows the Okta Admin Console interface. On the left, there's a sidebar with various navigation options under 'Admin Console'. The 'Authenticators' option is highlighted. The main area is titled 'Authenticators' and has tabs for 'Setup' and 'Enrollment'. A large orange circle is overlaid on the page. Below the tabs is a button labeled 'Add authenticator'. A table lists existing authenticators:

Name	Factor type	Characteristics	Status	Action
Email	Possession		Active	Actions
Okta Verify	Possession Possession + Knowledge <sup>1</sup> Possession + Biometric <sup>1</sup>	Device bound Hardware protected Phishing resistant (Okta FastPass) <sup>2</sup>	Active	Actions
Password	Knowledge		Active	Actions

<sup>1</sup> Multiple factor requirements may be satisfied based on the device used to enroll.  
<sup>2</sup> Phishing resistance may vary based on combinations of apps, browser, operating system, and more. [Learn more](#).

## 11 Adjusting policy when authenticating.

The screenshot shows the Okta Admin Console interface. On the left is a sidebar with various navigation options like Dashboard, Directory, Customizations, Applications, Identity Governance, Security, General, HealthInsight, and several policy categories. The 'Authenticators' category is selected. The main area is titled 'Authenticators' with tabs for 'Setup' and 'Enrollment'. A prominent message box states: 'OIE Upgrade Change' and 'Authenticator enrollment policy is evaluated alongside password policy'. It explains that users may be required to enroll in email or security question, and may be given an option to enroll in Phone or Okta Verify, even if they were selected as optional or disabled in the enrollment policy, because of password policy configurations. Below this is a section titled 'Manage authenticator availability and enrollment' which describes how a policy enrolls an authenticator based on configuration: Required (prompted), Optional (enroll anytime), or Disabled (not allowed). The central part of the screen is a modal window titled 'Edit Policy'. It shows the 'Default Policy' is active. The 'Policy description' field contains the placeholder 'The default policy applies in all situations if no other policy applies.' Under 'Assign to groups', 'Everyone' is selected. In the 'Authenticators' section, three options are listed: 'Email' (disabled), 'Okta Verify' (required), and 'Password' (required). At the bottom of the modal are 'Update policy' and 'Cancel' buttons.

## 12 Alice Johnson profile enabled.

The screenshot shows the Okta Admin Console interface. On the left, there's a sidebar with various navigation options like Dashboard, Directory, People, Groups, Devices, etc. The 'People' option is currently selected. In the main content area, the user profile for 'Alice Johnson' is displayed. Her email is listed as 'alicejohnson@demo.local'. Below her name is a large orange circular placeholder for a profile picture. There are two buttons at the top right of the profile card: 'Reset or Remove password' and 'More Actions'. Underneath the profile card, there are tabs for 'User', 'Active', and 'View Logs'. The 'Applications' tab is currently selected. A sub-section titled 'Assigned Applications' shows a table with columns 'Application' and 'Assignment & App Username'. The table is empty, displaying the message 'No apps assigned to this user.' At the bottom of the application section, there's a blue button labeled 'Assign Applications' and a search bar.

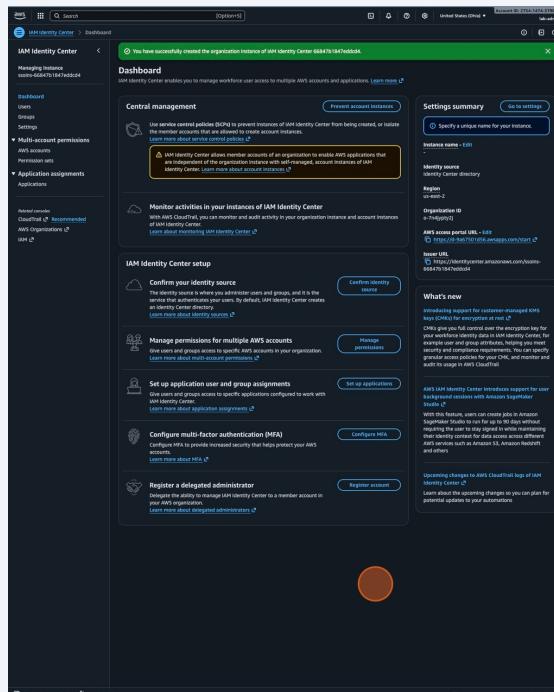
## 13 Bob Miller profile enabled.

The screenshot shows the Okta Admin Console interface. On the left, there's a sidebar with various navigation options like Dashboard, Directory, People, Applications, Customizations, and Settings. The 'People' section is currently selected. In the main content area, a user profile for 'Bob Miller' is displayed. The profile card includes the email 'bobmiller@demo.local'. Below the card are buttons for 'Reset or Remove password' and 'More Actions'. A navigation bar below the card shows tabs for User, Active, and View Logs, with 'Applications' being the active tab. Under the 'Applications' tab, there's a section titled 'Assigned Applications' with a button to 'Assign Applications'. A search bar is also present. The main body of the page displays a table with columns for Application and Assignment & App Username, which is currently empty, showing the message 'No apps assigned to this user.'

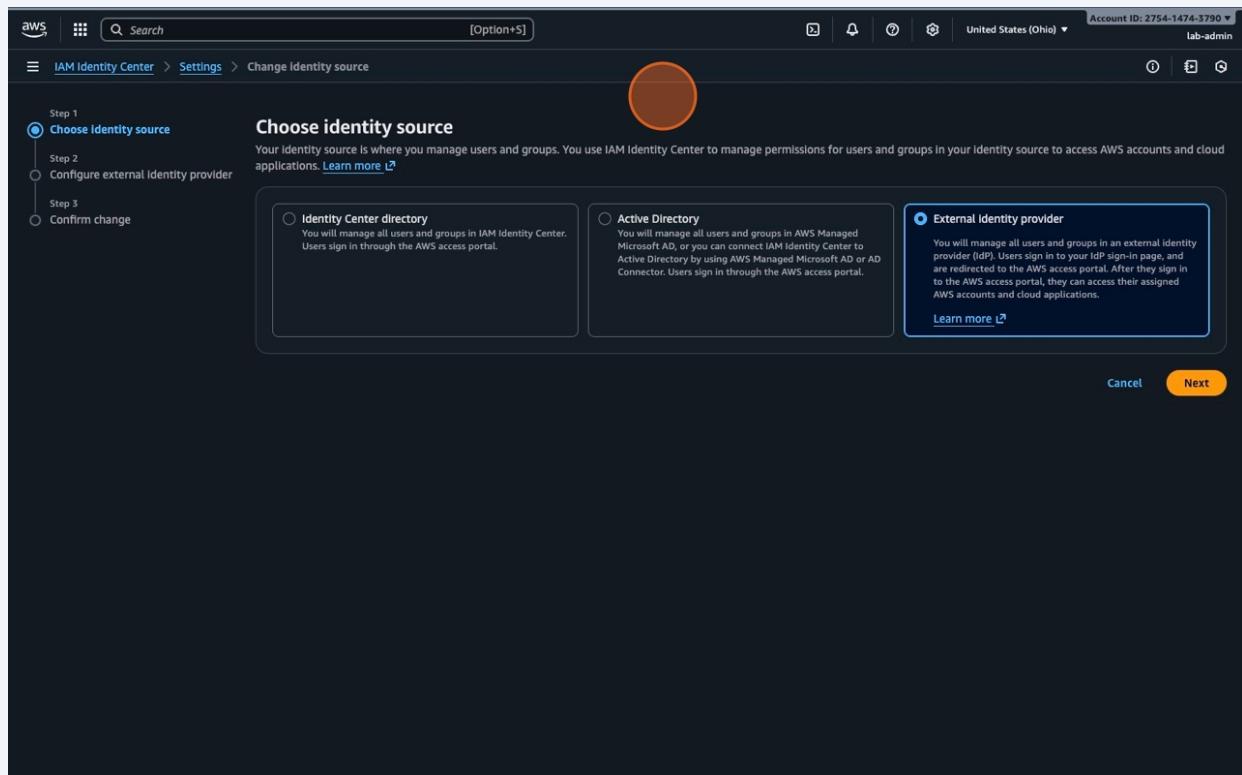
## 14 Process to enable OIDC. This would connect to AWS.

The screenshot shows the Okta Admin Console interface, specifically the 'Applications' section. A new application named 'OIDC-SPA-Demo' has been created and is shown in the list. The application card indicates it is 'Active' and has a 'View Logs' button. Below the application list, the 'General' tab is selected for the 'OIDC-SPA-Demo' application. The 'Client Credentials' section contains fields for 'Client ID' (set to '0oaxa82cvzk5PmeFt697') and 'Client authentication' (set to 'None'). There's also a checkbox for 'Proof Key for Code Exchange (PKCE)' which is checked, and another for 'Require PKCE as additional verification' which is also checked. The 'General Settings' section shows the 'Edit' button and the following details: 'App integration name' is 'OIDC-SPA-Demo', 'Application type' is 'Single Page App (SPA)', and there are two sections for 'Application notes' (one for end users and one for admins) which are currently empty.

## 15 Within the AWS IAM Identity Center process to linked external authentication



## 16 Select "External identity provider."



## 17 Download the metadata file.

The screenshot shows the 'Configure external identity provider' page in the AWS IAM Identity Center. The left sidebar indicates 'Step 2 Configure external identity provider' is selected. The main area is titled 'Service provider metadata' and contains three sections: 'AWS access portal sign-in URL' (with a link to https://d-9a67501d56.awsapps.com/start), 'IAM Identity Center Assertion Consumer Service (ACS) URL' (with a link to https://us-east-2.sigin.aws.amazon.com/platform/saml/acss/434d482d40f060e4-0bc3-4bac-8ae4-50a59b75fc12), and 'IAM Identity Center Issuer URL' (with a link to https://us-east-2.sigin.aws.amazon.com/platform/saml/d-9a67501d56). Below this, the 'Identity provider metadata' section includes fields for 'IdP SAML metadata' (with a 'Choose file' button), 'IdP sign-in URL' (input field), 'IdP issuer URL' (input field), and 'IdP certificate' (with a 'Choose file' button). At the bottom right are 'Cancel', 'Previous', and 'Next' buttons. A large orange circle highlights the 'Download metadata file' button in the top right corner of the service provider metadata section.

## 18 Under applications locate "AWS IAM Identity Center" and "Add integration".

The screenshot shows the Okta Admin Console with the navigation bar at the top. The main content area is titled "AWS IAM Identity Center" and includes a sub-section "Secure Identity Integrations - Advanced". Below this, there are tabs for "Workflow Templates" and "Workflows Connectors", and links for "Identity Security Posture Management" and "SAML". A large orange circle highlights the "Add Integration" button. The central part of the screen displays the "AWS IAM Identity Center" integration details, including its use cases (Single Sign-On, Lifecycle Management, Collection, Secure Identity Integrations, Functionality), and an overview of federating with AWS IAM Identity Center.

## 19 Within the "AWS IAM Identity Center" select "Sign on methods". Make sure correct "AWS SSO ACS URL" and "AWS SSO issue URL" have been entered. Once confirmed select "Save".

This screenshot shows the configuration of the "AWS IAM Identity Center" application within the Okta Admin Console. The "Sign on methods" section is open, displaying the "SAML 2.0" sign-on option. The "Metadata URL" field contains the URL: <https://integrator-2146409.okta.com/app/awsiamidentitycenter/sso/metadata>. The "AWS SSO ACS URL" field contains the URL: <https://aws-iam-2.singlesignon.amazon.com/platform/saml>. The "AWS SSO issue URL" field contains the URL: <https://aws-iam-2.singlesignon.amazon.com/platform/saml>. The "Credentials Details" section shows the "Application username format" set to "Okta username". The "Password reveal" checkbox is checked. At the bottom right, the "Save" button is highlighted with an orange circle.

20

Back in 'AWS IAM Identity Center' make sure the "IdP certificate from OKTA was attached", the correct "IdP Sign-in URL" and "IdP Issuer URL" have been entered correctly.

The screenshot shows the 'Change Identity source' wizard in AWS IAM Identity Center. The current step is 'Step 3: Confirm change'. The process has three steps:

- Step 1: Choose identity source (Completed)
- Step 2: Configure external identity provider (Completed)
- Step 3: Confirm change (In Progress)

**Confirm change**

**Step 1: Choose identity source**

**Identity source**

Identity source: External identity provider

**Step 2: Configure external identity provider**

**Service provider metadata**

<b>IdP certificate</b> okta.cert Size: 1360 bytes Last modified: Nov 9, 2025	<b>IdP sign-in URL</b> https://integrator-2146409.okta.com/app/amazon_aws_sso/exxa8yv22lqlPWP1697	<b>IdP Issuer URL</b> http://www.okta.com/exxa8yv22lqlPWP1697
---	--	--

**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

21 If options selected were correct this would be the confirmation screen.

The screenshot shows the AWS IAM Identity Center Settings page. A green success message at the top states: "You successfully changed the identity source from IAM Identity Center to an external identity provider (IdP). Learn more". The main section is titled "Details" and displays the following information:

Instance name - <a href="#">Edit</a>	Instance ID ssolns-66847b1847edddc4	Organization ID o-7n4jyptv2
Region us-east-2	Date created Sunday, November 9, 2025 at 4:35:27 PM EST	Instance ARN arn:aws:sso::instance/ssolns-66847b1847edddc4
Delegated administrator No account registered	Identity-enhanced sessions - <a href="#">Enable</a> <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	

Below this are three configuration sections:

- Enable Identity-enhanced sessions**: Provides personalized experiences for users of AWS managed applications. Identity-enhanced sessions are required for some of these applications, such as Amazon Q Developer in the console. [Learn about Identity-enhanced sessions](#). [Enable](#)
- Attributes for access control**: Configure this option to grant access to users based on specific characteristics. [Learn more](#). [Enable](#)
- Automatic provisioning**: When your identity source is set to an external identity provider (IdP), you can configure how best to provision all your users and groups into IAM Identity Center so that you can make assignments to the AWS accounts or cloud applications you have configured. [Enable](#)

The "Identity source" tab is selected. The "Identity source" section shows:

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

Identity source External identity provider	Provisioning method Manual
Authentication method SAML 2.0	Identity Store ID d-9a67501d56
AWS access portal URL <a href="https://d-9a67501d56.awsapps.com/start">https://d-9a67501d56.awsapps.com/start</a>	
Issuer URL <a href="https://identitycenter.amazonaws.com/ssolns-66847b1847edddc4">https://identitycenter.amazonaws.com/ssolns-66847b1847edddc4</a>	

**22** Click "Assign Applications" to assign the "AWS IAM Identity Center" in OKTA

The screenshot shows the Okta Admin Console interface for managing user Alice Johnson. The main navigation bar includes 'Dashboard', 'Directory', 'People' (selected), 'Groups', 'Devices', 'Profile Editor', 'Directory Integrations', 'Profile Sources', 'Customizations', 'Applications' (selected), 'Identity Governance', 'Security', 'Workflow', 'Reports', and 'Settings'. The 'Applications' tab is active, and the 'Assigned Applications' section is visible. A modal window titled 'Assign Applications' is open, listing several applications with their icons and names, each followed by an 'Assign' button. The 'AWS IAM Identity Center' application is highlighted with a blue border and has a large orange circle drawn around it. The 'Done' button is at the bottom right of the modal.

Application	Assignment & App Username
Okta Admin Console	01101110
Okta Access Certification Reviews	01101111
Okta Workflows	01101100
Okta Workflows OAuth	01101101
OIDC-SPA-Demo	01101100
AWS IAM Identity Center	01101100

## 23 Confirmed "Alice Johnson" now has the AWS OKTA tile

The screenshot shows the Okta Admin Console interface. On the left, there is a sidebar with various navigation options under 'Admin Console'. The 'People' option is selected and highlighted in blue. In the main content area, a user profile for 'Alice Johnson' is displayed. Her name is at the top, followed by her email address 'alicejohnson@demo.local'. Below the name, there are two buttons: 'Reset or Remove password' and 'More Actions'. Underneath these buttons, there are filter options: 'User', 'Active', and 'View Logs'. A horizontal navigation bar below the filters includes 'Applications', 'Groups', 'Profile', 'Devices', 'Admin roles', and 'Pre-enrolled authenticators'. The 'Applications' tab is currently active. A sub-section titled 'Assigned Applications' is shown, featuring a button labeled 'Assign Applications'. A table lists the assigned application, its provider (aws), and the assignment details ('Individual' and 'alicejohnson@demo.local'). There is also a search bar at the top of this section.