

Tuesday, 11 June 2024

Accessing AWS Using Azure Active Directory

Go to AWS account and search for IAM Identity Center. Go to IAM Identity Center.

The screenshot shows the AWS IAM Identity Center Dashboard. On the left, under 'Central management', there are two main sections: 'Use service control policies (SCPs)' and 'Monitor activities in your instances of IAM Identity Center'. In the 'Use service control policies' section, there is a note about account instances and a link to learn more. In the 'Monitor activities' section, there is a note about CloudTrail and a link to learn more. On the right, under 'Settings summary', there is a box for specifying a unique name for the instance, followed by fields for 'Instance name', 'Identity source', 'Region', 'Organization ID', 'AWS access portal URL', and 'Issuer URL'. At the bottom, there are links for CloudShell, Feedback, and a copyright notice.

Scroll Down and go to Settings, Identity Source.

The screenshot shows the AWS IAM Identity Center Settings page. The left sidebar has a 'Managing Instance' section with 'ssoins-7223f523c4674401' and a 'Settings' section selected. Below this are sections for 'Multi-account permissions' and 'Application assignments'. At the bottom, there are links for CloudTrail, AWS Organizations, and IAM. The main content area is titled 'Settings' and contains a 'Details' section with fields for 'Instance name', 'Organization ID', 'Region', 'Instance ARN', and 'Identity-aware sessions'. There are also sections for 'Enable Identity-aware sessions' and 'Attributes for access control' with 'Enable' buttons. At the bottom, there are links for CloudShell, Feedback, and a copyright notice.

Identity source Authentication Management Tags

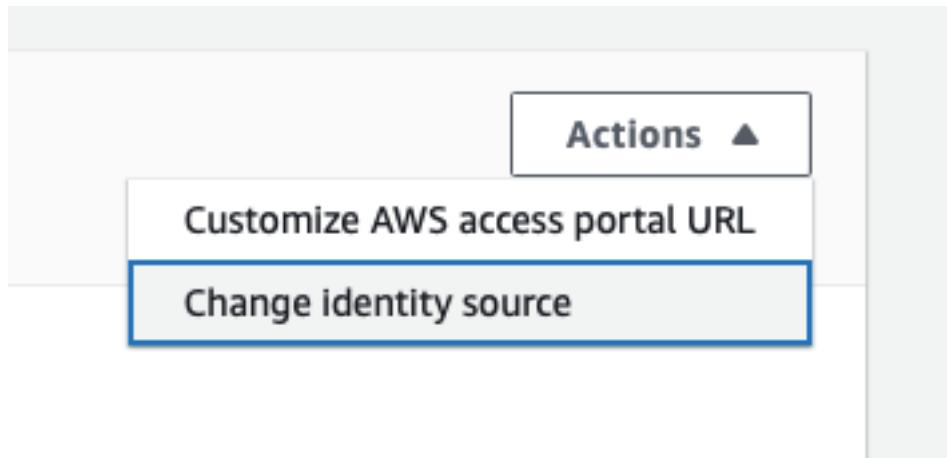
Identity source

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

Actions ▾

Identity source	Provisioning method
Identity Center directory	Direct
Authentication method	Identity store ID
Password	d-9067e6e88a
AWS access portal URL	
https://d-9067e6e88a.awsapps.com/start	
Issuer URL	
https://identitycenter.amazonaws.com/ssoins-7223f523c4674401	

Here we need to Change identity source, Go to Actions tab and select Change identity source.



Choose Identity Source External identity provider.

Choose identity source

Your identity source is where you manage users and groups. You use IAM Identity Center to manage permissions for users and groups in your identity source to access AWS accounts and cloud applications. [Learn more](#)

Identity Center directory

You will manage all users and groups in IAM Identity Center. Users sign in through the AWS access portal.

Active Directory

You will manage all users and groups in AWS Managed Microsoft AD, or you can connect IAM Identity Center to Active Directory by using AWS Managed Microsoft AD or AD Connector. Users sign in through the AWS access portal.

External identity provider

You will manage all users and groups in an external identity provider (IdP). Users sign in to your IdP sign-in page, and are redirected to the AWS access portal. After they sign in to the AWS access portal, they can access their assigned AWS accounts and cloud applications.

[Learn more](#)

Cancel

Next

In Configure external identity provider Download metadata file.

Configure external identity provider

Service provider metadata

 [Download metadata file](#)

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

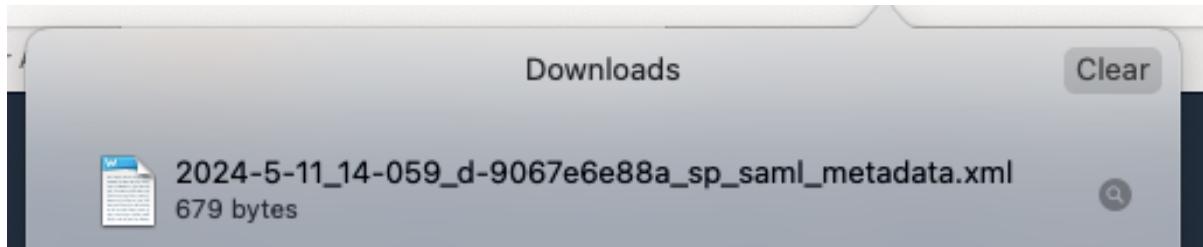
 <https://d-9067e6e88a.awsapps.com/start>

IAM Identity Center Assertion Consumer Service (ACS) URL

 <https://us-east-1signin.aws.amazon.com/platform/saml/acs/7063c836-6920-4a20-a594-fb6dc4ba40bf>

IAM Identity Center issuer URL

 <https://us-east-1signin.aws.amazon.com/platform/saml/d-9067e6e88a>



Then move Azure account and search for Enterprise applications.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes links for ChatGPT | OpenAI, Resume writer requested, Fake Mail Generator - Free te..., Azure AD Authentication for A..., Change identity source - Step..., Enterprise applications - Micr..., and a user profile for SuchetaSodage@Siddh... SIDDHANT TECHNOLOGIES (SBD...). The main title is "Enterprise applications | All applications". On the left, a sidebar menu is open under "Manage", specifically "All applications", which is highlighted with a blue border. Other options in the sidebar include Overview, User settings, App launchers, Custom authentication extensions, Security, Activity, and Troubleshooting + Support. The main content area displays a table with columns: Name, Object ID, Application ID, Homepage URL, Created on, Certificate Expir..., Active Certificat..., and Identifier URI (E...). A search bar at the top of the content area says "Search by application name or object ID" and has filters for "Application type == Enterprise Applications" and "Application ID starts with". Below the search bar, it says "0 applications found" and "No results".

Then go to New Application. Here we are adding AWS Identity Centre to Azure AD.

The screenshot shows the "New application" page. At the top, there are several buttons: "+ New application" (highlighted with a blue border), Refresh, Download (Export), Preview info, Columns, Preview features, and Got feedback?. Below these buttons, the text "New application" is displayed in a large, bold, black font.

Here we will get multiple options we will search for AWS and select AWS AM Identity Center (successor to AWS Single Sign-On).

The screenshot shows the Microsoft Azure portal interface with the URL portal.azure.com in the address bar. The top navigation bar includes links for ChatGPT | OpenAI, Resume writer requested, Fake Mail Generator - Free te..., Azure AD Authentication for A..., Change identity source - Step..., Browse Microsoft Entra Galler..., and a user profile for SuchetaSodage@Sidh... SIDHANT TECHNOLOGIES (SID...). The main content area is titled "Browse Microsoft Entra Gallery" and displays sections for "Cloud platforms" (Amazon Web Services (AWS), Google Cloud Platform, Oracle, SAP) and "On-premises applications" (Add an on-premises application, Learn about Application Proxy, On-premises application provisioning). At the bottom, there is a "Featured applications" section.

The screenshot shows the Microsoft Azure portal interface with the URL portal.azure.com in the address bar. The top navigation bar includes links for ChatGPT | OpenAI, Resume writer requested, Fake Mail Generator - Free te..., Azure AD Authentication for A..., Change identity source - Step..., Browse Microsoft Entra Galler..., and a user profile for SuchetaSodage@Sidh... SIDHANT TECHNOLOGIES (SID...). The main content area is titled "Browse Microsoft Entra Gallery" and displays search results for "aws". The search results show six applications: DICE AWS, AWS ClientVPN, AWS Console Sign-In, AWS Single-Account Access, AWS IAM Identity Center (successor to AWS Single Sign-On), and WATS. Below the search results, there is a callout for the "AWS IAM Identity Center (successor to AWS Single Sign-On)" application.

The screenshot shows the Microsoft Azure portal interface with the URL portal.azure.com in the address bar. The top navigation bar includes links for ChatGPT | OpenAI, Resume writer requested, Fake Mail Generator - Free te..., Azure AD Authentication for A..., Change identity source - Step..., AWS IAM Identity Center (succ..., and the user profile of SuchetaSodage@Sidh... from SIDHANT TECHNOLOGIES (SID...).

The main content area displays the "AWS IAM Identity Center (successor to AWS Single Sign-On) | Overview" page for an "Enterprise Application". The left sidebar lists navigation options: Overview, Deployment Plan, Diagnose and solve problems, Manage, Security, Activity, and Troubleshooting + Support. The "Properties" section shows the application details: Name (AWS IAM Identity Center (su...)), Application ID (3155138b-595d-4ced-bf2d-3...), and Object ID (734df40c-a19c-4044-b365-2...). The "Getting Started" section contains five numbered steps:

- 1. Assign users and groups**: Provide specific users and groups access to the applications. [Assign users and groups](#)
- 2. Set up single sign on**: Enable users to sign into their application using their Microsoft Entra credentials. [Get started](#)
- 3. Provision User Accounts**: Automatically create and delete user accounts in the application. [Get started](#)
- 4. Conditional Access**: Secure access to this application with a customizable access policy. [Create a policy](#)
- 5. Self service**: Enable users to request access to the application using their Microsoft Entra credentials. [Get started](#)

Below the steps, there is a "What's New" section.

2. Set up single sign on

Enable users to sign into their application using their Microsoft Entra credentials

[Get started](#)

In Set up single sign on we are using SAML Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

SAML, is a standardised way to tell external applications and services that a user is who they say they are.

Now we are going Set up Single Sign-On with SAML. For this we need to upload the downloaded metadata file from AWS identity source.

The screenshot shows the Microsoft Azure portal interface. The URL in the address bar is `portal.azure.com`. The top navigation bar includes links for ChatGPT | OpenAI, Resume writer requested, Fake Mail Generator - Free te..., Azure AD Authentication for A..., Change identity source - Step..., AWS IAM Identity Center (succ..., and the user profile of SuchetaSodage@Siddh... SIDHANT TECHNOLOGIES SID...>.

The main content area is titled "AWS IAM Identity Center (successor to AWS Single Sign-On) | Single sign-on". The left sidebar shows the navigation path: All services > AWS IAM Identity Center (successor to AWS Single Sign-On). The "Manage" section is expanded, showing options like Properties, Owners, Roles and administrators, Users and groups, and Single sign-on. The "Single sign-on" option is currently selected.

The main content area displays three methods for single sign-on:

- Disabled**: Single sign-on is not enabled. The user won't be able to launch the app from My Apps.
- SAML**: Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.
- Linked**: Link to an application in My Apps and/or Office 365 application launcher.

[Upload metadata file](#) [Change single sign-on mode](#) [Test this application](#) | [Got feedback?](#)

[Upload metadata file](#)

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating AWS IAM Identity Center (successor to AWS Single Sign-On).

Here we are uploading metadata file which we have downloaded from AWS AM Identity Center.

Upload metadata file.

Values for the fields below are provided by AWS IAM Identity Center (successor to AWS Single Sign-On). You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by AWS IAM Identity Center (successor to AWS Single Sign-On).

Select a file

[Add](#) [Cancel](#)

[Edit](#)

Check details and Save.

Basic SAML Configuration

X



Save



Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

https://us-east-1.signin.aws.amazon.com/platform/saml/d-9067e6e88a



Add identifier

Patterns: https://REGION.signin.aws.amazon.com/platform/saml/*

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index

Default

https://us-east-1.signin.aws.amazon.com/platform/saml/acs/7063c836-6920-4a20-... ✓



Add reply URL

Patterns: https://<REGION>.signin.aws.amazon.com/platform/saml/acs/<ID>

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Enter a sign on URL ✓

Relay State (Optional) ⓘ

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.



Save



Got feedback?

Patterns: https://REGION.signin.aws.amazon.com/platform/saml/*

We need SAML Certificates to upload to AWS Identity Source. Here we are downloading Federation Metadata XML file.

3

SAML Certificates

Token signing certificate  Edit

Status	Active
Thumbprint	F14820DEE01EFBB389806D A34F53B6A84A5294D3
Expiration	11/6/2027, 3:13:29 PM
Notification Email	SuchetaSodage@Siddhant Technologies.onmicrosoft.c om

**App Federation Meta
data Url** <https://login.micros...> 

Certificate (Base64) [Download](#)

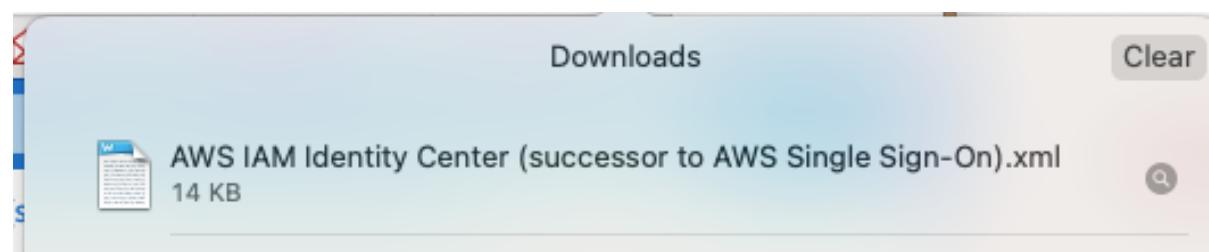
Certificate (Raw) [Download](#)

**Federation Metadata
XML** [Download](#)

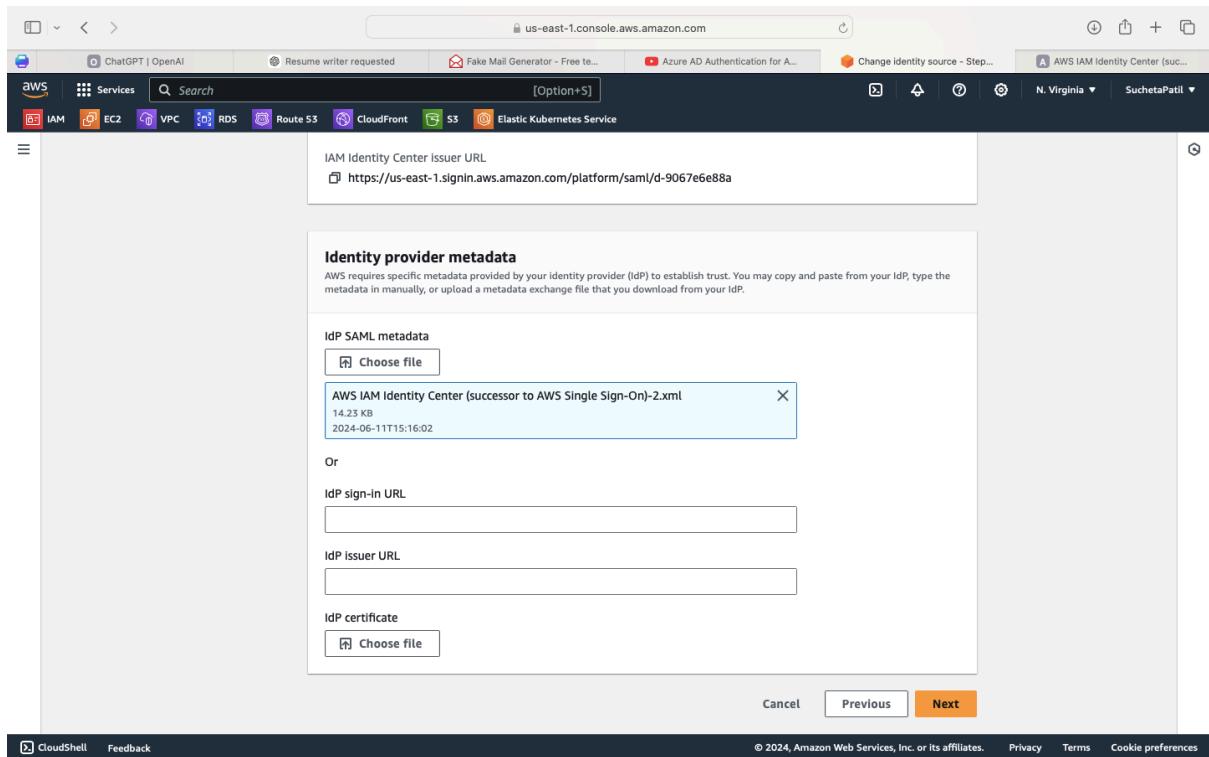
Verification certificates (optional)  Edit

Required	No
Active	0
Expired	0

[Open in a new tab](#)



Now go back to Identity provider metadata in AWS identity provider centre. And upload AWS AM Identity Center (successor to AWS Single Sign-On).xml file.



The screenshot shows the AWS IAM Identity Center console. The URL is us-east-1.console.aws.amazon.com. The top navigation bar includes links for ChatGPT | OpenAI, Resume writer requested, Fake Mail Generator - Free to..., Azure AD Authentication for A..., Change identity source - Step..., AWS IAM Identity Center (succ...), Services (selected), Search, [Option+S], N. Virginia, and SuchetaPatil.

The main content area is titled "Confirm change" and "Step 1: Choose identity source". It displays two options: "Identity source" and "External identity provider".

On the left sidebar, there are three steps: Step 1 (Choose identity source), Step 2 (Configure external identity provider), and Step 3 (Confirm change). Step 2 is currently selected.

At the bottom, there are links for CloudShell and Feedback, and standard footer links for Privacy, Terms, and Cookie preferences.

The screenshot shows the AWS IAM Identity Center console. The URL is us-east-1.console.aws.amazon.com. The top navigation bar includes links for ChatGPT | OpenAI, Resume writer requested, Fake Mail Generator - Free to..., Azure AD Authentication for A..., Change identity source - Step..., AWS IAM Identity Center (succ...), Services (selected), Search, [Option+S], N. Virginia, and SuchetaPatil.

The main content area is titled "Review and confirm" and displays a warning message: "⚠ Review the following consequences of your requested identity source change:" followed by a bulleted list of 11 items detailing the implications of changing the identity source.

Below the warning, there is a text input field labeled "Confirm that you want to change your identity source by entering ACCEPT in the field below." with the word "ACCEPT" typed into it. There are "Cancel", "Previous", and "Change identity source" buttons at the bottom.

At the bottom, there are links for CloudShell and Feedback, and standard footer links for Privacy, Terms, and Cookie preferences.

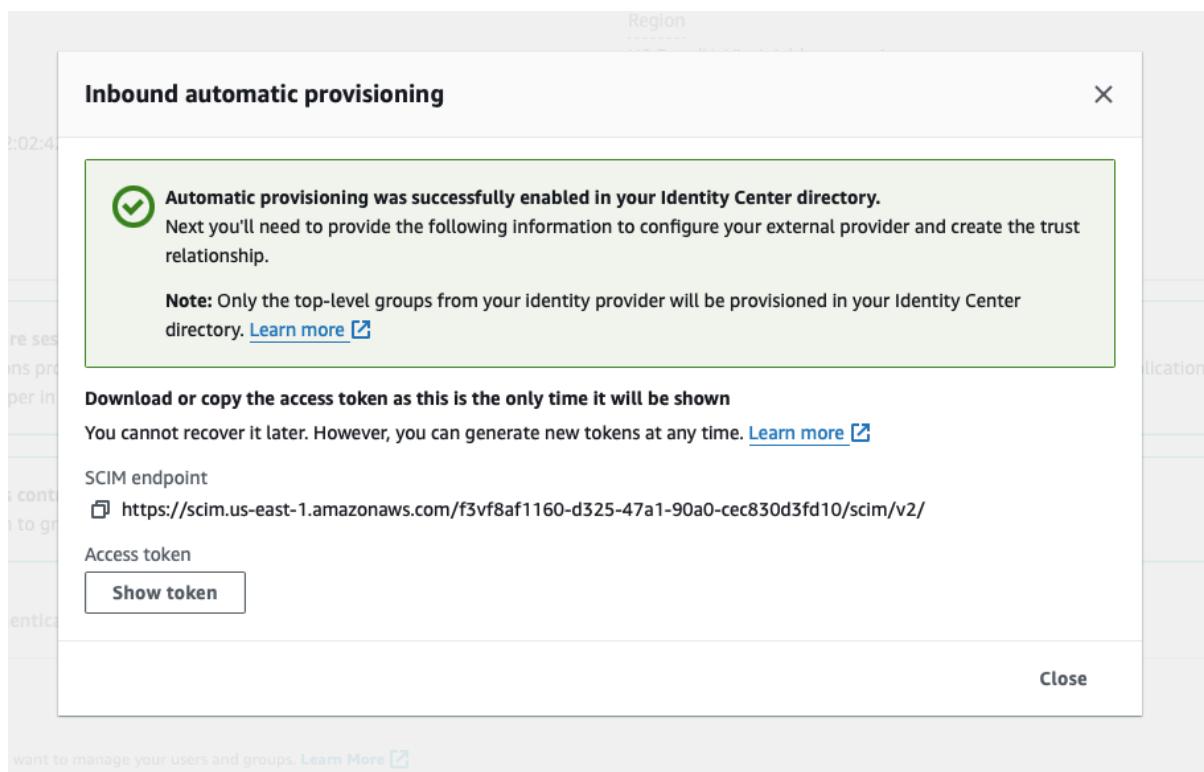
Type ACCEPT and click on Change identity source.

The screenshot shows the AWS IAM Identity Center Settings page. At the top, a confirmation message says: "Confirm that you want to change your identity source by entering ACCEPT in the field below." Below this is a text input field containing "ACCEPT". At the bottom of the page, there are three buttons: "Cancel", "Previous", and "Change identity source" (which is highlighted in orange). The main content area displays a success message: "You successfully changed the identity source from IAM Identity Center to an external identity provider (IdP)." The left sidebar shows the navigation menu for IAM Identity Center, including "Managing Instance", "Dashboard", "Users", "Groups", "Settings" (which is selected), "Multi-account permissions", "Application assignments", and "Related consoles".

In the Setting page we need to enable Automatic provisioning.

The screenshot shows the "Automatic provisioning" section of the AWS IAM Identity Center Settings page. It contains an informational message: "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." To the right of the message is an "Enable" button. The rest of the page is mostly blank, showing the standard AWS footer and navigation.

In this page click on Show Token. Which we need for further steps.



You successfully changed the identity source.

Organization ID: o-wm21y0p5r

Date created: Tuesday, June 11, 2024 at 2:02:44

Delegated administrator: No account registered

Enable identity-aware sessions: Identity-aware sessions provide secure access to your applications using Amazon Q Developer Identity.

Attributes for access control: Configure this option to grant specific permissions to users based on their attributes.

Identity source: Choose the directory where you want to provision users and groups.

Identity source: External identity provider

SCIM endpoint: <https://scim.us-east-1.amazonaws.com/f3vf8af1160-d325-47a1-90a0-cec830d3fd10/scim/v2/>

Access token
[Show token](#)

[Close](#)

Copy Token Tenant URL and Secret Token and save it in Notes.

11 JUNE 2024 01:31 PM

<https://scim.us-east-1.amazonaws.com/f3vf8af1160-d325-47a1-90a0-cec830d3fd10/scim/v2/>

c4560a3c-639f-4b2b-8b86-
d407c32d8d06:48090649-3c2f-4cc4-
ba00-981ab65b8ef6:Rv4yRZk9Etqe8P/
zdEr6jtSac9sQ4zmC5TsMwhSoSfrVGPH52B803EsY+pYO6hDzPSA
zH1cn7Era1VE13N/plCyR+h21FlsocA6pRefOEm8KmKULT/
pbvf7LSN5qxvc2P3YXtwWDBMRuzA84ydbZehrYStdFA+j3eg0=:Y1
J1I6VUu8T+OHcFKIA7dfJcdOGheSgNwpYAwtc7mdmraYafns41F7d
6qdGp2YXAMY5jxkpPZ9l892d41caNbNdWze5CLxlaQdGhQg/
gu1AJ642sOxjdcgTKeaW2OCqSdT138ahTdLKvviDj4NUM93Wa16F
T4jmbqbzuBxqos2jrEzGKGEfG4nTRPhqGt13UgyOwTwUDJF4TOO3
YtdJBumJY5O1qUAnxnKd5ob4ZbBI2dxeNPdS80ruyhBP42KzLTolA
1esznMLgrqt0QHG/
NY+TyCh6EccRb6ZoC5Az0O+khN6XIBH5PjahKUsBrCsvamFsG5a
AXKHp1OhsM5llHw==

Now go back to Azure AWS AM Identity Center (successor to AWS Single Sign-On) page.

The screenshot shows the AWS IAM Identity Center configuration page within the Microsoft Azure portal. The left sidebar menu is visible, showing options like Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Self-service, Custom security attributes), Security, Activity, and Troubleshooting + Support. The 'Single sign-on' option under 'Manage' is selected. The main content area displays three steps for SAML configuration:

- Basic SAML Configuration**:

Identifier (Entity ID)	https://us-east-1.sigin.aws.amazon.com/platform/saml/-9067e6e88a
Reply URL (Assertion Consumer Service URL)	https://us-east-1.sigin.aws.amazon.com/platform/saml/cs/7063c836-6920-4a20-a594-fb6dc4ba40bf
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- Attributes & Claims**:

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- SAML Certificates**:

Token signing certificate	Status: Active
---------------------------	----------------

In left side manu select Manage, in that Provisioning option.

The screenshot shows the Microsoft Azure navigation bar. The 'Overview' link is highlighted. Below it, the 'Provision on demand' and 'Manage' links are visible. The 'Manage' link is expanded, showing its sub-options: 'Provisioning', 'Monitor', and 'Troubleshoot'.

In Provisioning Mode select Automatic.

The screenshot shows the AWS IAM Identity Center Provisioning page in the Microsoft Azure portal. The 'Provisioning Mode' dropdown is set to 'Automatic'. The 'Admin Credentials' section contains fields for 'Tenant URL' and 'Secret Token', both of which have been populated with copied values. A 'Test Connection' button is visible below the credentials.

Paste copied Tenant URL and Secret Token.

The screenshot shows the 'Admin Credentials' section of the provisioning configuration. The 'Tenant URL' field contains the value 'https://scim.us-east-1.amazonaws.com/f3vf8af1160-d325-47a1-90a0-cec830d3fd10/scim/v2/'. The 'Secret Token' field contains a long string of characters, with a key icon and a copy/paste icon next to it. A 'Test Connection' button is located below these fields.

Test Connection.

Test Connection

- ✓ Testing connection to AWS IAM Identity Center (successor to AWS Single Sign-On) X

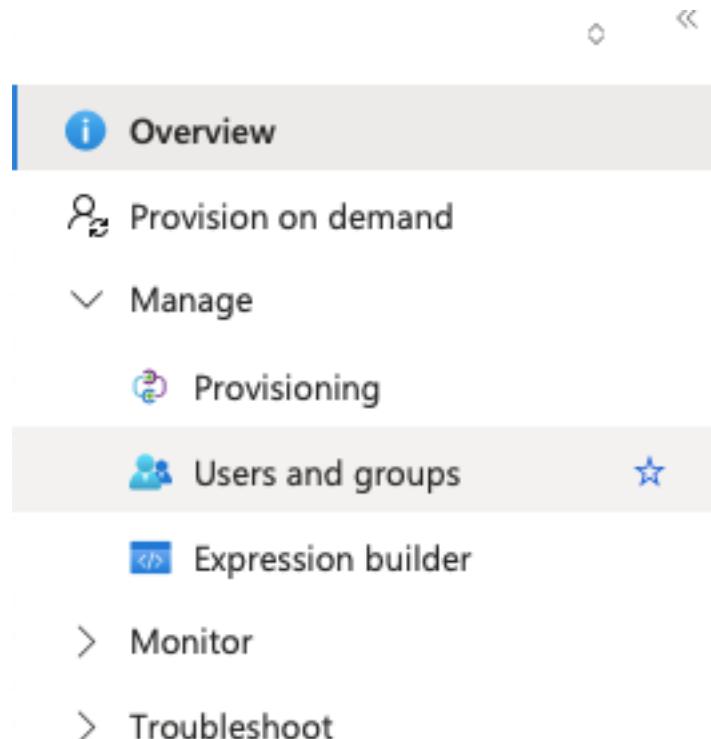
The supplied credentials are authorized to enable provisioning

a few seconds ago

Save the changes.

 Save  Discard

Now select Users and group option from left side options.



Add users and group.

The screenshot shows two windows side-by-side. The left window is titled 'AWS IAM Identity Center (successor to AWS Single Sign-On) | Users and groups'. It has a sidebar with 'Overview', 'Provision on demand', 'Manage', 'Provisioning', and 'Users and groups' (which is selected). The main area shows a table with columns 'Display Name', 'Object Type', and 'Role assigned'. A message at the top says 'No application assignments found'. The right window is titled 'Add Assignment - Microsoft A...'. It shows a list of users and groups under 'None Selected'. Below this, there's a section 'Select a role' with 'User' selected. At the bottom is a large 'Assign' button.

Click on Users and select User we want add to AWS account.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes links for ChatGPT, Resume writer requested, Fake Mail Generator, Azure AD Authentication, Identity Center, Users | IAM | Global, AWS IAM Identity Center, and the user profile 'SuchetaSodage@Siddh...'. The main title is 'AWS IAM Identity Center (successor to AWS Single Sign-On) | Users and groups'. The left sidebar has sections for Overview, Provision on demand, Manage, Provisioning, Users and groups (which is selected), Expression builder, Monitor, and Troubleshoot. The main content area displays a table with columns: Display Name, Object Type, and Role assigned. Two users are listed: 'aws' (User, User role) and 'Sucheta Sodage' (User, User role). A note at the top says: 'The application will appear for assigned users within My Apps. Set Visible to users? to no in properties to prevent this.' A search bar at the top says 'First 200 shown, to search all users & gro...'. A message bar at the bottom says 'Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration.'

The screenshot shows the 'Add Assignment' page within the Microsoft Azure portal. The top navigation bar is identical to the previous screenshot. The main title is 'Add Assignment'. The left sidebar shows 'Users and groups' with '1 user selected' (Sucheta Sodage). Below this, there is a 'Select a role' dropdown with 'User' selected. At the bottom of the page is a large blue 'Assign' button.

Again go back to Provisioning and change Provisioning Status to On.

The screenshot shows the AWS IAM Identity Center Provisioning page. On the left, there's a navigation sidebar with options like Overview, Provision on demand, Manage, Provisioning, Users and groups, Expression builder, Monitor, and Troubleshoot. The 'Provisioning' option is selected and highlighted in grey. In the main content area, under 'Provisioning Mode', it says 'Automatic'. Below that, there's a note: 'Use Microsoft Entra to manage the creation and synchronization of user accounts in AWS IAM Identity Center (successor to AWS Single Sign-On) based on user and group assignment.' There are sections for 'Admin Credentials' and 'Mappings'. At the bottom, there's a 'Settings' section with a 'Provisioning Status' toggle switch. The switch is currently set to 'On', indicated by a purple circle with the word 'On'.

The screenshot shows the AWS IAM Identity Center Users page. At the top, there's a navigation bar with links for Services, Search, and [Option+S]. The 'IAM' link is highlighted. Below the navigation is a message: 'Your identity source is currently configured as "External identity provider". To add new users or edit their attributes, you must do this using your external identity provider (IdP).'. The main area is titled 'Users (1)' and shows a table with one row. The table has columns for 'Username', 'Display name', 'Status', and 'Created by'. The single user listed is 'SuchetaSodag...' with 'Sucheta Sodage' as the display name, 'Enabled' status, and 'SCIM' as the created by source. There are buttons for 'Create user' and 'Delete users' at the top right of the table. At the bottom of the page, there are links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

Now we can able to see our Azure Active Directory user in our AWS IAM Identity Center.

Now go to AWS Account option from left side options.

The screenshot shows the IAM Identity Center console. At the top, it displays "IAM Identity Center" and a close button ("X"). Below this, there's a section titled "Managing instance" with the identifier "ssoins-7223f523c4674401". The main navigation menu on the left includes links for "Dashboard", "Users" (which is underlined in blue), "Groups", "Settings", and two collapsed sections: "Multi-account permissions" and "Application assignments". Under "Multi-account permissions", there are links for "AWS accounts" and "Permission sets". Under "Application assignments", there is a link for "Applications". At the bottom of the menu, there's a section titled "Related consoles" with links for "CloudTrail", "AWS Organizations", and "IAM", each accompanied by a small icon.

IAM Identity Center X

Managing instance
ssoins-7223f523c4674401

Dashboard

Users

Groups

Settings

▼ Multi-account permissions

AWS accounts

Permission sets

▼ Application assignments

Applications

Related consoles

CloudTrail Recommended

AWS Organizations

IAM

Select our user from there.

The screenshot shows the AWS IAM Identity Center console. On the left, a sidebar navigation includes 'Managing Instance' (with ID ssoins-7223f523c4674401), 'Dashboard', 'Users', 'Groups', 'Settings', 'Multi-account permissions' (selected, showing 'AWS accounts' and 'Permission sets'), and 'Application assignments' (showing 'Applications'). Under 'Related consoles', 'CloudTrail' is recommended. The main content area is titled 'AWS accounts' and shows the organizational structure. It lists a single account under 'Root': 'SuchetaPatil' (management account). A search bar at the top right says 'Assign users or groups'.

Now Assign users and groups you want to give multi-account access to.

The screenshot shows the 'Assign users and groups' step of a wizard. At the top, it says 'Assign users and groups to "SuchetaPatil"' and 'Select one or more users or groups in IAM Identity Center that you want to give multi-account access to.' Below this, there are tabs for 'Users' (selected) and 'Groups'. The 'Users' section shows a table with one row: 'SuchetaSodage@SiddhantTechnologies.onmicrosoft.com' (Display name: Sucheta Sodage, Status: Enabled). A 'Create users' button is available. At the bottom, a summary box shows 'Selected users and groups (1)' with a 'Remove' button. Navigation buttons 'Cancel' and 'Next' are at the very bottom.

We have to assign permission to the user for this select, Select permission set type

For assigning permission we have 2 options, Predefined permission set and Custom permission set.

Here we are Predefined permission set.

The screenshot shows the AWS IAM Identity Center 'Create permission set' wizard. The current step is 'Step 1: Select permission set type'. There are two options: 'Predefined permission set' (selected) and 'Custom permission set'. The 'Predefined permission set' section describes it as creating a permission set by choosing an AWS-defined template. The 'Custom permission set' section describes it as creating a custom permission set by selecting AWS managed policies and creating an inline policy (recommended). You can also attach customer managed policies and set a permissions boundary (advanced).

In this case we are providing Administrator Access.

The screenshot shows the 'Policy for predefined permission set' section. The 'AdministratorAccess' policy is selected, which provides full access to AWS services and resources.

The screenshot shows the AWS IAM Identity Center console with the URL `us-east-1.console.aws.amazon.com`. The top navigation bar includes links for ChatGPT | OpenAI, Resume writer req..., Fake Mail Generator..., Azure AD Authent..., Assign users and g..., Users | IAM | Global, Create permission..., AWS IAM Identity..., Global, and SuchetaPatil.

The main navigation bar has tabs for AWS, Services, Search, and [Option+S]. Below the main navigation are icons for IAM, EC2, VPC, RDS, Route 53, CloudFront, S3, and Elastic Kubernetes Service.

The left sidebar shows a three-step process: Step 1 (Select permission set type), Step 2 (Specify permission set details), and Step 3 (Review and create). The current step is Step 2.

The main content area is titled "Specify permission set details" and contains a sub-section titled "Permission set details". It includes fields for "Permission set name" (set to "AdministratorAccess"), "Description - optional" (with a placeholder "Enter a description"), "Session duration" (set to "1 hour"), and "Relay state - optional" (with a placeholder "Enter relay state").

At the bottom of the page are links for CloudShell, Feedback, © 2024, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

Review and create.

The screenshot shows the AWS IAM console with the URL us-east-1.console.aws.amazon.com. The top navigation bar includes links for ChatGPT | OpenAI, Resume writer req..., Fake Mail Generato..., Azure AD Authenti..., Assign users and g..., Users | IAM | Global, Create permission..., AWS IAM Identity..., Services, Search, and [Option+S]. The main menu bar has options for AWS, IAM, EC2, VPC, RDS, Route 53, CloudFront, S3, and Elastic Kubernetes Service. A dropdown menu shows 'Global' and 'SuchetaPatil'. The current page is 'IAM Identity Center / Permission sets / Create permission set'.

The main content area is titled 'Review and create' and contains three steps:

- Step 1: Select permission set type**: Shows 'Permission set type' with 'Type' set to 'Predefined permission set' and 'AWS managed policy' set to 'AdministratorAccess'.
- Step 2: Define permission set details**: Shows 'Permission set details' with 'Permission set name' set to 'AdministratorAccess-azureAD', 'Session duration' set to '2 hours', and 'Description' set to 'aws-azure-activedirectory'. It also shows a 'Tags (not set)' section.
- Step 3: Review and create**: Shows the same information as Step 1 and Step 2.

At the bottom, there are buttons for 'CloudShell', 'Feedback', and links to '© 2024, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

This screenshot is identical to the one above, showing the 'Review and create' step for creating a permission set named 'AdministratorAccess-azureAD'. The details, including session duration (2 hours), description (aws-azure-activedirectory), and the 'Tags (not set)' section, are the same. The 'Create' button is visible at the bottom right.

The screenshot shows the IAM Identity Center dashboard with the 'Permission sets' section selected. A success message at the top states: 'The permission set "AdministratorAccess-azureAD" was successfully created.' Below this, a callout box informs users that IAM Identity Center now supports customer managed policies and permissions boundaries. The main table lists one permission set:

Permission set	Description	ARN
AdministratorAccess-azureAD	aws-azure-active...	arn:aws:sso:::permissionSet/ssoins-7223f523c4674401/ps-66b32c58

Move to IAM Identity Center Dashboard.

The screenshot shows the IAM Identity Center dashboard with the 'Dashboard' section selected. It includes the following sections:

- Central management:** Includes a shield icon, a note about service control policies (SCPs), and a note about account instances.
- Monitor activities in your instances of IAM Identity Center:** Includes a cloud icon and a note about using CloudTrail for monitoring.
- IAM Identity Center setup:** Includes a cloud icon and a note about confirming the identity source.
- Settings summary:** A panel on the right where users can specify a unique name for their instance, choose a region (US East (N. Virginia)), and provide an AWS access portal URL.

In right side Settings summary, copy AWS access portal URL. Hit the URL.

