

Hands-on tutorials

Setting Up Your AWS Environment



Setting Up Your AWS Environment: Hands-on tutorials

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Setting Up Your AWS Environment	i
Overview	1
What you will accomplish	1
Modules	1
Module 1: Create Your AWS Account	2
What you will accomplish	1
Implementation	2
Conclusion	13
Module 2: Secure Your AWS Account	14
Overview	1
Implementation	2
Conclusion	13
Module 3: (Optional) Set Up the AWS CLI	52
Introduction	52
Implementation	2
Conclusion	13

Setting Up Your AWS Environment

AWS experience	Beginner
Time to complete	35 minutes
Cost to complete	Free Tier eligible
Requires	Recommended internet browser: The latest version of Chrome or Firefox
Last updated	April 24, 2024

Overview

In this tutorial, you will set up your AWS account and development environment. This will allow you to interact with your AWS account and programmatically provision any resources you need.

What you will accomplish

In this tutorial, you will learn how to:

- Create a new AWS account
- Configure users
- (Optional) Set up the AWS CLI

Modules

This tutorial is divided into the following short modules. You must complete each module before moving to the next one.

1. [Module 1: Create Your AWS Account](#) (10 minutes)
2. [Module 2: Secure Your AWS Account](#) (15 minutes)
3. [Module 3: \(Optional\) Set Up the AWS CLI](#) (10 minutes)

Module 1: Create Your AWS Account

Time to complete	10 minutes
Module requirements	An internet browser
Get help	Troubleshooting AWS account sign-in issues

What you will accomplish

- Sign up for an AWS account
- Verify your contact details

Implementation

An AWS account is the starting point to allow provisioning infrastructure. In this module, we cover how to set up your account.

Step 1: Select email, account name, and password

To create a new AWS account, go to aws.amazon.com and choose [Create an AWS Account](#).

1. Enter your information

Enter an **email address** and an **account name**.

- Carefully consider which email address you want to use. If you are setting up for a personal account, we don't recommend using a work email address because you may change jobs at some point. Conversely, for business accounts, we recommend using an email alias that can be managed because the person setting up the account may, at some point, change roles or companies.

- Step 1
 Specify user details
- Step 2 - optional
 Add user to groups
- Step 3
 Review and add user

Specify user details

Primary information

Username
 This username will be required for this user to sign in to the AWS access portal. The username can't be changed later.

Maximum length of 128 characters. Can only contain alphanumeric characters or any of the following: +, -, @, _.

Password
 Choose how you want this user to receive their password. [Learn more](#)

Send an email to this user with password setup instructions.
 Generate a one-time password that you can share with this user.

Email address

Confirm email address

First name

Last name

Display name
 This is typically the full name of the workforce user (first and last name), is searchable, and appears in the users list.

▶ **Contact methods - optional**

▶ **Job-related information - optional**

▶ **Address - optional**

▶ **Preferences - optional**

▶ **Additional attributes - optional**

[Cancel](#) Next

2. Enter the email verification code

Select **Verify email address**.

- You will get a verification code in your email. Enter the verification code and choose **Verify**.

You will be redirected to a new screen where you will create your **root user password**.

3. Create a password

Create your **root user password**.

- The password you choose is extremely sensitive, and should be shared only with people who have access to the credit card that will be used on this account.
- Your password must include: uppercase letters, lowercase letters, numbers, and non-alphabetic characters.



Explore Free Tier products with a new AWS account.

To learn more, visit aws.amazon.com/free.



Sign up for AWS

Create your password

✔ It's you! Your email address has been successfully verified. ✕

Your password provides you with sign in access to AWS, so it's important we get it right.

Root user password

Confirm root user password

Continue (step 1 of 5)

OR

Sign in to an existing AWS account

4. Choose continue

Once you have entered and confirmed your password, choose **Continue (step 1 of 5)**.

Step 2: Add contact information

Now you need to add your contact information and select how you plan to use AWS.

1. Choose an account type

Choose between a **business** or **personal** account.

- There is no difference in account type or functionality, but there is a difference in the type of information required to open the account for billing purposes.
- For a business account, choose a **phone number** that is tied to the business and can be reached if the person setting up the account is not available.

2. Enter contact details

Once you have selected the account type, fill out the the **contact information** about the account.

- Save these details in a safe place. If you ever lose access to the email or your two-factor authentication device, AWS Support can use these details to confirm your identity.



Free Tier offers

All AWS accounts can explore 3 different types of free offers, depending on the product used.



Always free
Never expires



12 months free
Start from initial sign-up date



Trials
Start from service activation date

Sign up for AWS

Contact Information

How do you plan to use AWS?

- Business - for your work, school, or organization
- Personal - for your own projects

Who should we contact about this account?

Full Name

Country Code Phone Number

+1 ▼	222-333-4444
------	--------------

Country or Region

Address line 1

Address line 2

City

State, Province, or Region

Postal Code

- I have read and agree to the terms of the [AWS Customer Agreement](#).

Agree and Continue (step 2 of 5)

3. Accept the AWS Customer Agreement

At the end of this form, read through the terms of the [AWS Customer Agreement](#) and select the checkbox to accept them.

4. Choose Continue

Choose **Agree and Continue (step 2 of 5)** to proceed to the next screen.

Step 3: Add payment method

In the following screen, add your preferred credit or debit card to use for payment.

1. Enter billing information

Enter your **Billing Information** details.

- A small hold will be placed on the card, so the address must match what your financial institution has on file for you or your business.



Secure verification

i We will not charge you for usage below AWS Free Tier limits. We may temporarily hold up to \$1 USD (or an equivalent amount in local currency) as a pending transaction for 3-5 days to verify your identity.



Sign up for AWS

Billing Information

Billing country

Your billing country determines the payment methods available to you to pay for AWS services.

United States ▼

Credit or Debit card number



AWS accepts most major credit and debit cards. To learn more about payment options, review our [FAQ](#)

Expiration date

Month ▼

Year ▼

Security code **i**

CVV/CVC

Cardholder's name

Billing address

Use my contact address

Use a new address

Verify and continue (step 3 of 5)

You might be redirected to your bank's website to authorize the verification charge.

2. Choose Continue

Select **Verify and continue (step 3 of 5)** to proceed.

Step 4: Confirm your identity

Now you need to verify your account.

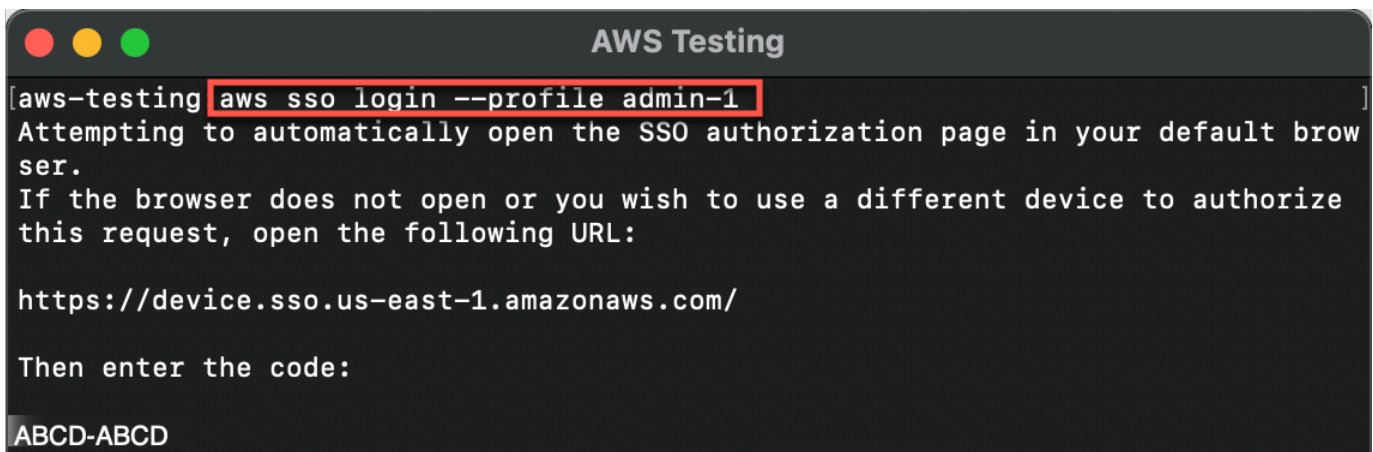
1. Choose a verification method

Choose how you want to **confirm your identity**.

- You can verify your account either through a text message (SMS) or a voice call on the number you are associating with this account.
- For the text message (SMS) option, you will be sent a numeric code to enter on the next screen after you choose **Send SMS (step 4 of 5)**.
- For the **Voice call** option, you will be shown a code on the screen to enter after being prompted by the automated voice verification system.

2. Send the SMS

Choose your verification choice, then choose **Send SMS (step 4 of 5)** to proceed to verification.


A terminal window titled "AWS Testing" with a dark background. The command `aws sso login --profile admin-1` is entered and highlighted with a red box. The output text reads: "Attempting to automatically open the SSO authorization page in your default browser. If the browser does not open or you wish to use a different device to authorize this request, open the following URL: https://device.sso.us-east-1.amazonaws.com/ Then enter the code: ABCD-ABCD".



```
aws-testing [aws sso login --profile admin-1]
Attempting to automatically open the SSO authorization page in your default browser.
If the browser does not open or you wish to use a different device to authorize
this request, open the following URL:
https://device.sso.us-east-1.amazonaws.com/
Then enter the code:
ABCD-ABCD
```

3. Solve the CAPTCHA

Enter the **CAPTCHA** as appropriate, then choose **Submit** to receive a call or SMS.

Security Verification ✕



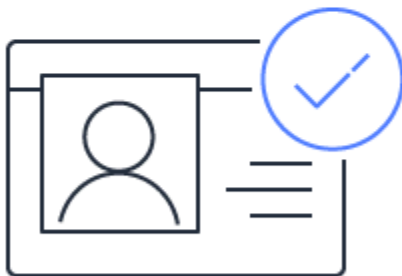


Type the characters as shown above

Reset Submit

4. Enter the verification code

Enter the **code** as appropriate for your verification choice, then choose **Continue (step 4 of 5)** to proceed to the final step.



Sign up for AWS

Confirm your identity

Verify code

[Continue \(step 4 of 5\)](#)

Having trouble? Sometimes it takes up to 10 minutes to retrieve a verification code. If it's been longer than that, [return to the previous page](#) and try again.

Step 5: Select a support plan

Choose a support plan for your AWS account.

1. Select a support plan

Choose a **support plan**. For this tutorial, we recommend the default selection.


- You have three options for support plans. The default option is called Basic Support and is free of charge. If you are not sure, select Basic Support. You can always change support tiers at a later date.

To see the full list of differences between the tiers, see [Compare AWS Support Plans](#).



Sign up for AWS

Select a support plan

Choose a support plan for your business or personal account. [Compare plans and pricing examples](#) . You can change your plan anytime in the AWS Management Console.

Basic support - Free

- Recommended for new users just getting started with AWS
- 24x7 self-service access to AWS resources
- For account and billing issues only
- Access to Personal Health Dashboard & Trusted Advisor



Developer support - From \$29/month

- Recommended for developers experimenting with AWS
- Email access to AWS Support during business hours
- 12 (business)-hour response times



Business support - From \$100/month

- Recommended for running production workloads on AWS
- 24x7 tech support via email, phone, and chat
- 1-hour response times
- Full set of Trusted Advisor best-practice recommendations



Need Enterprise level support?

From \$15,000 a month you will receive 15-minute response times and concierge-style experience with an assigned Technical Account Manager. [Learn more](#) 

Complete sign up

2. Choose Complete sign up

To finish creating your account, choose **Complete sign up**.

Conclusion

Congratulations! Your account is now set up and being activated. When activation is complete, you will receive an email from AWS. Use the credentials you created in this module to log in to your root account.

In the next module, you will learn how to secure your root account and set up additional users.

Module 2: Secure Your AWS Account

Time to complete	15 minutes
Module requirements	<ul style="list-style-type: none">• An internet browser• An AWS account
Get help	Troubleshooting IAM issues

Overview

When you create an AWS account, a root user is created automatically for your account. The root user is a special entity that has full access to the account, and can perform all actions, including changing the payment methods or closing the account. When you sign-in using the root user you have complete access to all AWS service and resources in the account. Due to this level of permissions, we recommend that you:

- Enable additional security for the root user with multi-factor authentication
- Set up additional users to perform daily tasks related to your account

AWS has two identity services:

- [AWS Identity and Access Management \(IAM\)](#). This service provides access control policies and manages long-term users like the root user. If you create users in IAM, those users have long-term access credentials. As a security best practice, it is recommended that you minimize the use of long-term credentials in AWS. In this tutorial you will not create an IAM user.
- [AWS IAM Identity Center](#). This service provides temporary credentials that are granted each time a user signs in for a session. It can integrate with any existing identity providers you might already have, like Microsoft Active Directory or Okta, so that your users can use the same sign on for AWS as they use for other services in your organization. If you don't have another identity provider, you can create users in IAM Identity Center. This is the recommended way to create additional users for your AWS account and is the method we will walk through in this tutorial.

Implementation

Step 1: Sign in as the root user

The AWS account root user is accessed by signing in with the email address and password that you used to create the account.

1. Open the console

Sign in to the [AWS Management Console](#).

2. Sign in as root user

Select **Root user** or **Sign in using root user email** (may be one of the two forms due to browser caching), and enter the email address you specified when you created your account and then choose **Next**.



Sign in

Root user

Account owner that performs tasks requiring unrestricted access. [Learn more](#)

IAM user

User within an account that performs daily tasks. [Learn more](#)

Root user email address

Next

3. Enter your password

On the sign-in page, enter your **password**, and choose **Sign in**.



Root user sign in ⓘ

Email: `someone@example.com`

Password

[Forgot password?](#)

Sign in

[Sign in to a different account](#)

[Create a new AWS account](#)

4. Complete verification

You may need to confirm your identity.

Enter the **code** sent to the root user email, and choose **Verify and continue**.



Confirm you're you

We sent an email with a verification code to

[Redacted email address]

To continue, confirm your identity using the code below.

Verification code

Verify and continue

Resend code (45)

Didn't get the code?

- Codes can take up to 5 minutes to arrive.
- Check your spam folder.
- Still having [problems signing in?](#)

Congratulations

You have just signed in to the AWS Management Console as your root user. But you don't want to use your root user for everyday tasks. The root user should only be used for specific account management tasks, two of which we are going to do in the next part of this tutorial.

- Enable MFA for the root user
- Create an administrative user in IAM Identity Center

For the complete list of tasks that require you to sign in as the root user, see [Tasks that require root user credentials](#).

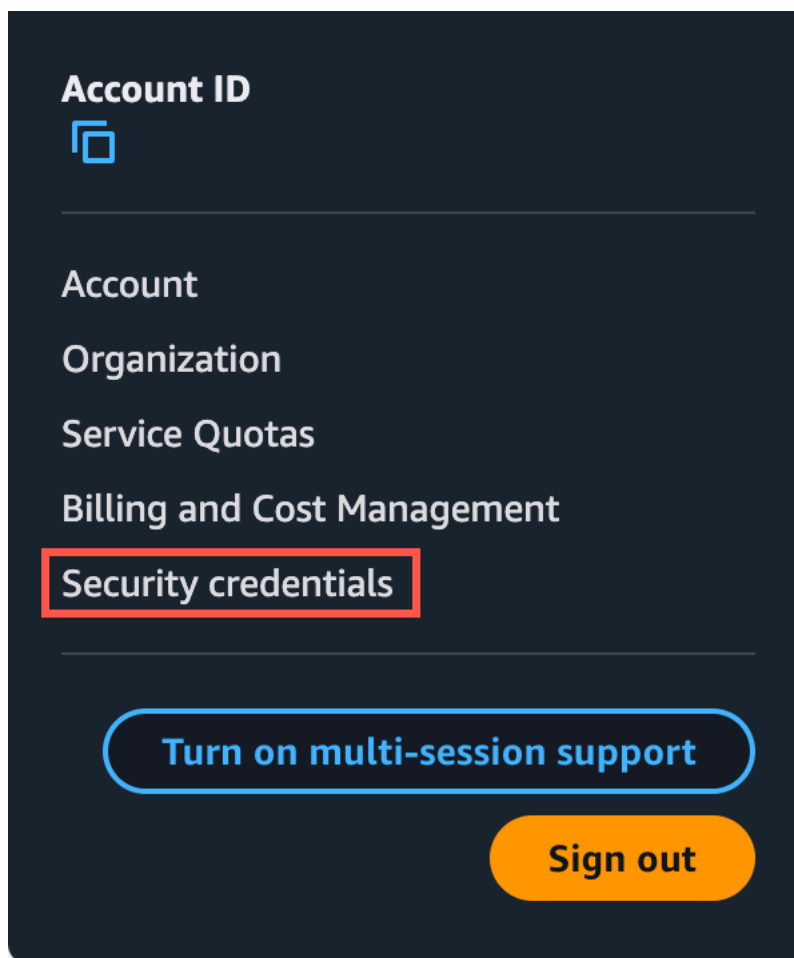
Step 2: Add more security to the root user sign in

To help keep your root user credentials secure, we strongly recommend that you enable multi-factor authentication (MFA) for your root user sign-in. When you enable MFA, in addition to providing the email address and password for the root user you will also provide credentials from another authenticator, making it much more difficult for someone to use your root user credentials without your permission.

To add more security to the root user sign-in, you will use the AWS Identity and Access Management (IAM) service. For more information, see [What is IAM?](#)

1. View security credentials

On the right side of the navigation bar, choose your account name, and choose **Security credentials**. If necessary, choose **Continue to Security credentials**.



2. Add an MFA device

In the **Multi-factor authentication** section, choose **Assign MFA device**.

Multi-factor authentication (MFA) (0) Remove Resync Assign MFA device

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Type	Identifier	Certifications	Created on
------	------------	----------------	------------

No MFA devices. Assign an MFA device to improve the security of your AWS environment

[Assign MFA device](#)

3. Select an authenticator app

On the Register MFA device page, name the **Device**, choose the **Authenticator app** option, and then choose **Next**.

Tip: You need a mobile device or hardware device to enable MFA. Find out how to get a [free MFA security key from AWS](#).

Select MFA device [Info](#)

MFA device name

Device name


This name will be used within the identifying ARN for this device.


Maximum 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)


MFA device

Device options

In addition to username and password, you will use this device to authenticate into your account.

 **Passkey or security key**
Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.

 **Authenticator app**
Authenticate using a code generated by an app installed on your mobile device or computer.

 **Hardware TOTP token**
Authenticate using a code generated by Hardware TOTP token or other hardware devices.

[Cancel](#)[Next](#)

4. Set up your MFA device

Set up the **Authenticator app** on your mobile device.

Several different authenticator apps are supported for both Android and iOS devices. See the **Virtual authenticator apps** section on the [Multi-Factor Authentication \(MFA\) for IAM](#) page for a list of supported apps and links to their download locations.

- a. **Open** the authenticator app on your mobile device.
- b. Select the **Show QR code** link to show a unique QR code for your account. If you can't scan the QR code, select the **Show secret key** link to display a text key that you can enter into the Authenticator app to identify your account.

Either **scan** the QR code with your authenticator app or **enter** the code in your authenticator app to **link** your authenticator device to your account.

- c. After your authenticator has established the link to your account, it will start generating secret codes that are good for a limited number of seconds. In **MFA code 1**, type the code you see in the app. Wait for that code to change to the next code, then type that code in **MFA code 2**, then select **Add MFA** before the second code has expired.

You are returned to the **Security credentials** page. A notification message is displayed at the top that states the MFA device is assigned.

Your root user credentials are now more secure.

Set up device [Info](#)

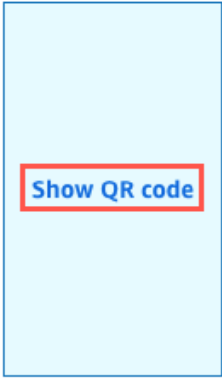
Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1

Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.

[See a list of compatible applications](#) 

2

Show QR code

Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. [Show secret key](#)

3

Type two consecutive MFA codes below

Enter a code from your virtual app below

Wait 30 seconds, and enter a second code entry.

[Cancel](#)

[Previous](#)

[Add MFA](#)

5. Verify MFA setup

You are returned to the **Security credentials** page. A notification message is displayed at the top that states the MFA device is assigned.

Your root user credentials are now more secure.

The screenshot shows the AWS IAM console interface. At the top, a green notification banner states "MFA device assigned" and "You now must authenticate with this MFA device when you sign in to the AWS console." Below this, the "Security credentials" tab is selected. The "Console sign-in" section shows the "Console sign-in link" as "https://[redacted]signin.aws.amazon.com/console" and the "Console password" as "Not enabled". The "Multi-factor authentication (MFA) (1)" section includes a "Remove" button and a "Resync" button. Below this is a table with the following data:

	Device type	Identifier	Certifications	Created on
<input type="radio"/>	Virtual	arn:aws:iam::[redacted]:mfa/[redacted]	Not Applicable	Now

Step 3: Set up users in IAM Identity Center

It is considered a security best practice to not use your root account for everyday tasks, but right now you only have a root user. In this tutorial, we will use IAM Identity Center to create an administrative user. We are using IAM Identity Center because it provides users with unique credentials for every session, also known as temporary credentials. Providing users these credentials results in enhanced security for your AWS account, because they are generated each time the user signs in. Once you have an administrative user, you can sign in with that user to create additional Identity Center users and assign them to groups with permissions to perform specific job functions. Another benefit to creating users in IAM Identity Center is that the users are automatically granted access to the the [AWS Billing and Cost Management console](#).

For more information about billing, see the [AWS Billing and Cost Management](#) user guide.

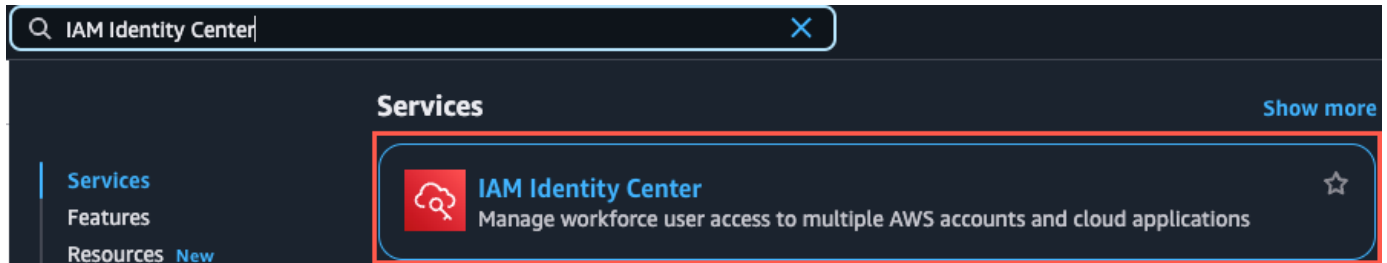
This section of the tutorial has the following steps:

- Enable IAM Identity Center
 - Add users
 - Add users to groups
- Configure your identity source

- Create an administrative permission set
- Sign in to the AWS access portal with your administrative credentials

1. Open the IAM Identity Center console

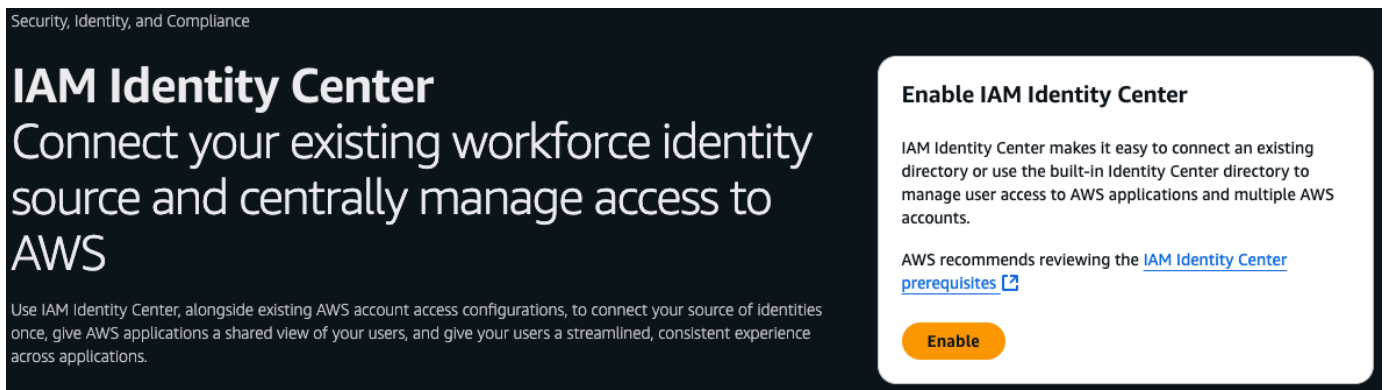
In the search bar, enter **IAM Identity Center**, and then select **IAM Identity Center**.



2. Enable IAM Identity Center

The **IAM Identity Center service** overview page opens. Review the information to learn about the features of the IAM Identity Center service.

In the **Enable IAM Identity Center**, select **Enable**.



3. Enable AWS Organizations

When you enable IAM Identity Center you also need to enable AWS Organizations. AWS Organizations lets you organize multiple AWS accounts so that you can have separate AWS accounts for different use cases. AWS Organizations is a feature of your AWS account offered at no additional charge.

Choose **Enable**.

- The root user is now the management account for the AWS Organization.

- At this point, AWS Organizations sends a verification email to the root user. Verifying your root user account allows you to invite other accounts to become members of your organization, so you don't need to verify your account before continuing with this tutorial. For more information about account management, see the [AWS Organizations](#) user guide.

Note

The verification link is only valid for 24 hours, so if you wait longer than that to verify the email address, you will need to resend the verification email. For more information about how to do this, see [Email address verification](#).

[IAM Identity Center](#) > Enable IAM Identity Center with AWS Organizations



Enable IAM Identity Center with AWS Organizations

When you enable IAM Identity Center with AWS Organizations, you're creating an [organization instance](#) of IAM Identity Center. Whether you want to connect your existing workforce users to AWS managed applications, or to AWS accounts, we recommend AWS Organizations and IAM Identity Center.

If you need to support isolated deployments of applications in a single AWS account, you can [enable an account instance of IAM Identity Center](#).

Let's confirm some details

Help make sure we configure the right setup for you.



Does this AWS account contain resources?

This account will be the [management account](#) of your organization. We recommend as a security best practice that you do not store resources in this account.

Account ID



Is this the right AWS Region?

We recommend that you create your instance in an AWS Region geographically near most of your workforce for lower latency access.

Current AWS Region

US East (Ohio)

Cancel

Enable

Step 4: Configure your identity source

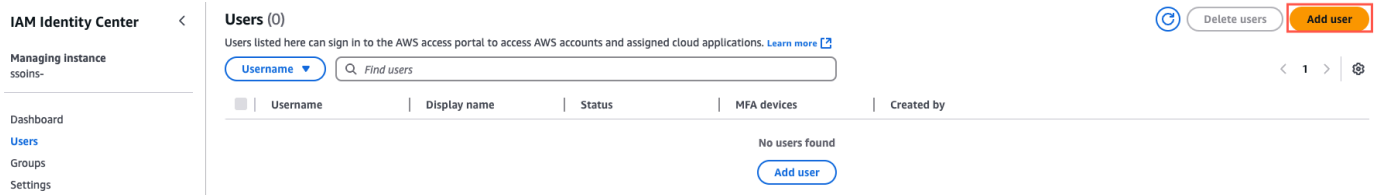
Your identity source is where your users and groups are managed. After you configure your identity source, you can look up users or groups to grant them single sign-on access to AWS accounts, cloud applications, or both.

When you enable IAM Identity Center for the first time, it is automatically configured with an IAM Identity Center directory as your default identity source. [Learn more about identity sources](#).

Complete the following steps to create a user in IAM Identity Center.

- Open the IAM Identity Center console

Navigate to the [IAM Identity Center](#) console, and choose **Users**. Then, select **Add user**.



2. Add user details

On the **Specify user details** page, complete the following information:

- **Username** – Choose a **name** that will be easy to remember. For this tutorial, we will be adding the user **John**.
- **Password** – Choose **Send an email to this user with password setup instructions (Recommended)**. This option sends the user an email addressed from Amazon Web Services, with the subject line Invitation to join IAM Identity Center (successor to AWS IAM Identity Center). The email will come from either **no-reply@signin.aws** or **no-reply@login.awsapps.com**. Add these email addresses to your approved senders list so that they are not treated as junk or spam.
- **Email address** – Enter an email address for the user where you can receive the email. Then, enter it again to confirm it. Each user must have a unique email address.

Tip

During testing, you might be able to use email subaddressing to create valid email addresses for multiple fictitious users. If your email provider supports it, you can create a new email address by appending the plus sign (+) and then numbers or characters to your current email address, such as `someone@example.com`, `someone+1@example.com`, and `someone+test@example.com`. All of those email addresses would result in an email being received at the same email address.

- **First name** – Enter the first name for the user.
- **Last name** – Enter the last name for the user.
- **Display name** – This is automatically filled in with the first and last name of the user. If you want to change the display name, you can enter something different. The display name is visible in the sign-in portal and users list.
- Complete the **optional information** if desired. It isn't used during this tutorial and can be added later.

Choose Next.

- Step 1
 Specify user details
- Step 2 - optional
 Add user to groups
- Step 3
 Review and add user

Specify user details

Primary information

Username
This username will be required for this user to sign in to the AWS access portal. The username can't be changed later.

Maximum length of 128 characters. Can only contain alphanumeric characters or any of the following: +, -, @, _.

Password
Choose how you want this user to receive their password. [Learn more](#)

Send an email to this user with password setup instructions.
 Generate a one-time password that you can share with this user.

Email address

Confirm email address

First name

Last name

Display name
This is typically the full name of the workforce user (first and last name), is searchable, and appears in the users list.

▶ **Contact methods - optional**

▶ **Job-related information - optional**

▶ **Address - optional**

▶ **Preferences - optional**

▶ **Additional attributes - optional**

[Cancel](#) [Next](#)

Step 5: (Optional) Add users to groups

User groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users.

1. Create a group

On the **Step 2 - optional Add user to groups** page, select **Create group**.

Step 1
Specify user details

Step 2 - optional
Add user to groups

Step 3
Review and add user

Add user to groups - optional

You can assign this user to one or more groups.

Groups (0)

Find groups by group name

Group name | Description

No groups found

Cancel Previous Next

2. Specify a group name

Under **Group details**, for **Group name**, enter **Admins**.

Select **Create group**.

Create group

Group details

Group name

Admins

Maximum of 128 characters

Description - optional

Group description detailing the permissions assigned to this group.

Enter description

Maximum of 256 characters

Add users to group - optional (0)

Select workforce users to add to this group.

Find users

Username | Display n... | Status | MFA devices | Created by

No users found

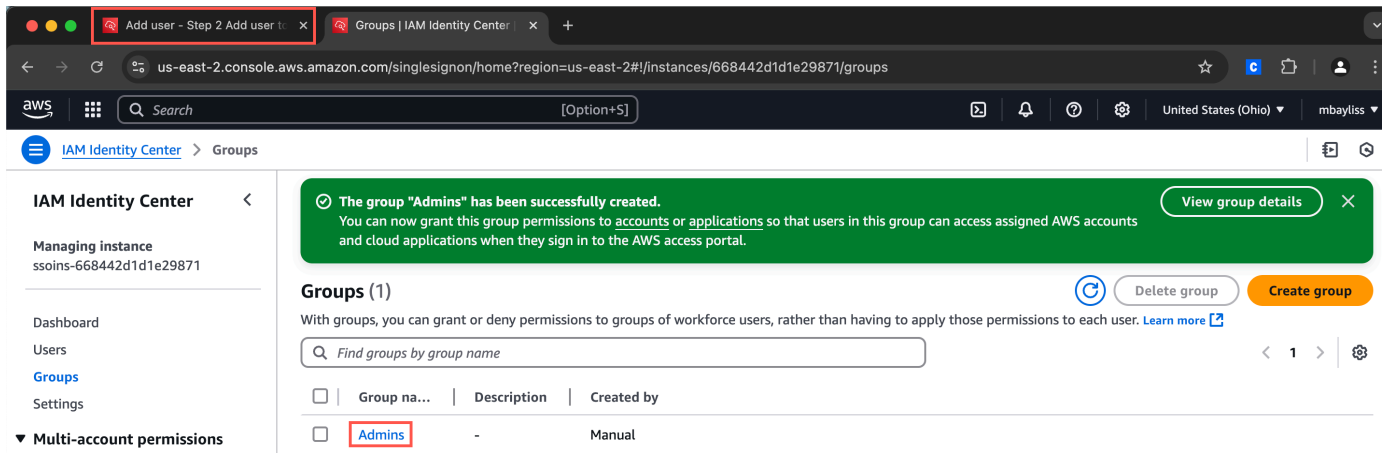
Add user

Cancel Create group

3. Return to Add user

The **Groups** page is displayed, showing your new **Admins** group.

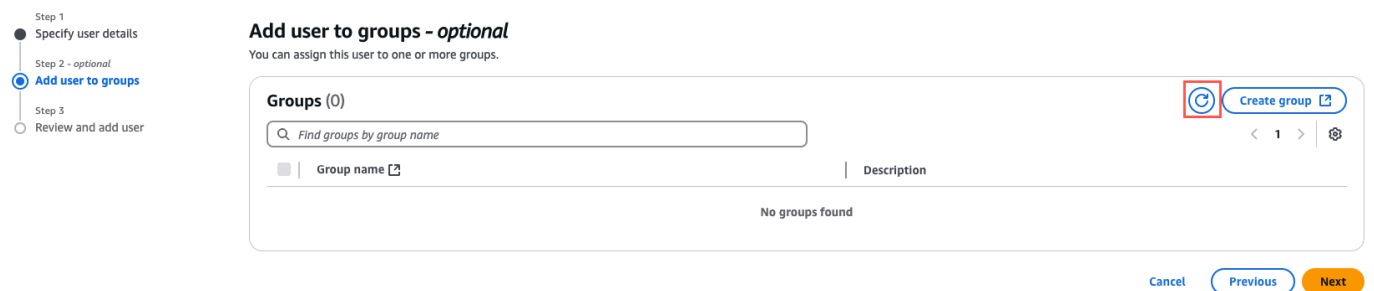
Exit out or navigate away from the **Groups** browser tab and return to the **Add user** browser tab.



4. Refresh groups

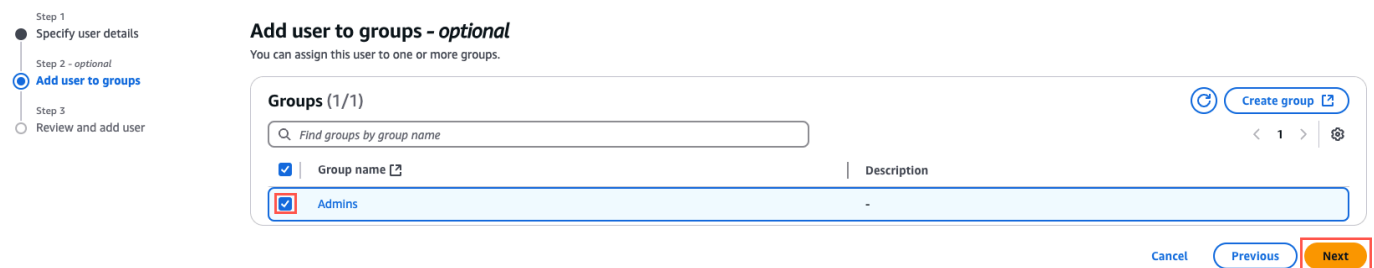
On the **Add users to groups- optional** page, select the **Refresh** button.

The new **Admins** group appears in the list.



5. Add group membership

Select the **check box** next to the **Admins** group, and then choose **Next**.



6. Review and confirm

On the **Review and add user** page confirm the following:

- Primary information appears as you intended
- Groups shows the user added to the group you created

If you need to make changes, choose **Edit** to make the updates.

Once everything is correct, select **Add user**.

Review and add user

Step 1: Specify user details Edit

Primary information

Attribute key	Value
Username	John
Email	someone@example.com
First name	John
Last name	Smith
Display name	John Smith

► Contact methods - optional

► Job-related information - optional

► Address - optional

► Preferences - optional

► Additional attributes - optional

Step 2: Add user to groups - optional Edit

Groups (1) < 1 >

Group name	Description
Admins	-

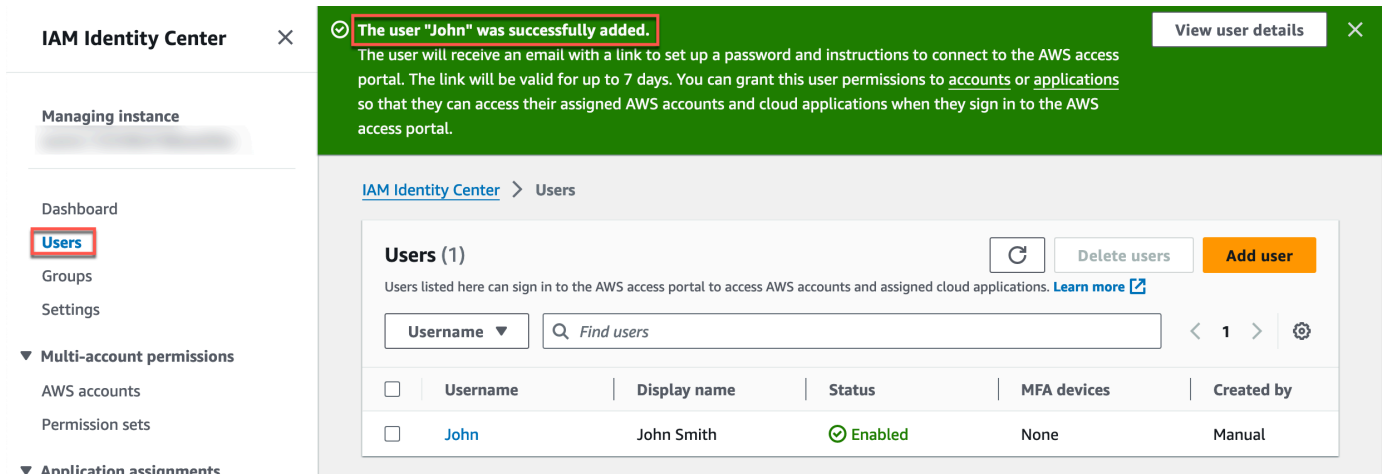
Cancel Previous Add user

7. (Optional) Create additional users and groups

You are returned to the main **IAM Identity Center > Users** page.

A notification message informs you that the user was successfully added.

Congratulations, you now have a user in your AWS Organization. You can repeat these steps to add additional users and groups.



The screenshot shows the IAM Identity Center console. A green notification banner at the top states: "The user 'John' was successfully added." Below the notification, the "Users" page is displayed, showing a table with one user: "John" (John Smith, Enabled, None, Manual).

Username	Display name	Status	MFA devices	Created by
John	John Smith	Enabled	None	Manual

Step 6: Manage access to your AWS account

Your new user exists but does not have access to any resources, services, or applications, so the user can't replace your root user for daily administrative tasks yet. Let's give your new user access to your AWS account. Since we put the user into a group, we will assign the group to an account and then we will add a permission set that defines what the members of the group can access.

Note

We will still be using the **root user** credentials for this step.

1. Set up multi-account permissions

In [IAM Identity Center](#) console left hand navigation, choose **Dashboard**.

In the **Recommended setup** steps, under **Manage permissions to multiple AWS accounts**, choose **Manage permissions**.

2. Select your AWS account

In the left hand navigation, choose **AWS accounts**.

Under **Organizational structure > Root**, choose the **account** you created in Module 1.

Note

For this tutorial, we are using a placeholder AWS account name.

3. Add users and groups

On the **Test-acct** page, choose the **User and groups** tab.

Select **Assign users or groups**.

The Assign users and groups workflow displays.

mb

Overview

Account name: mb Account ID: [redacted] Email: [redacted]

Users and groups Permission sets (0)

Assigned users and groups (0) Change permission sets Remove access **Assign users or groups** ↻

The following users and groups in IAM Identity Center can select this AWS account from within their AWS access portal. [Learn more](#)

Find users by username, find groups by group name < 1 > ⚙️

Username / group name	Permission sets	Type
<p>No users or groups assigned to this account</p> <p>You have not yet assigned any users or groups to this account.</p> <p>Assign users or groups</p>		

4. Select a group

For **Step 1: Select users and groups** select the **Admins** group you created previously in this tutorial. Then, choose **Next**.

Step 1: **Select users and groups** Step 2: Select permission sets Step 3: Review and submit

Select users and groups

Assign users and groups to "mb"

Select one or more users or groups in IAM Identity Center that you want to give multi-account access to.

Users **Groups**

Groups (1/1) ↻ [Create groups](#)

Find groups by group name < 1 > ⚙️

<input checked="" type="checkbox"/>	Group name	Description
<input checked="" type="checkbox"/>	Admins	-

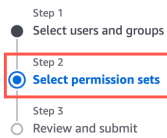
▶ **Selected users and groups (Groups: 1)** Remove

[Cancel](#) **Next**

5. Select a permission set

For **Step 2: Select permission sets**, select **Create permission set**.

A new browser tab will open and will walk you through the three sub-steps involved in creating the permission set.



Select permission sets

Assign permission sets to "mb [redacted]"

Permission sets define the level of access that users and groups in IAM Identity Center have to an AWS account. You can assign more than one permission set to a user. To ensure least privilege access to AWS accounts, users in IAM Identity Center with multiple permission sets on an AWS account must pick a specific permission set when selecting the account and then return to the AWS access portal to pick a different set when necessary. [Learn more](#)

Permission sets (0) Refresh Create permission set

Find permission sets by name, ARN, or ID (i.e., ps-abcdefg123456789)

Permission set	Description	ARN
No permission sets		
You have not yet created any permission sets.		

Create permission set

6. Choose a permission type

In the new browser tab, for **Step 1: Select permission set type**. Make the following selections:

- For **Permissions set type**, select **Predefined permission set**
- For **Policy for predefined permission set**, select **AdministratorAccess**
- For more information on managing permissions, see the [Predefined permissions for AWS managed policies](#) in the **AWS IAM Identity Center** guide.

Then, choose **Next**.

- Step 1
 Select permission set type
- Step 2
 Specify permission set details
- Step 3
 Review and create

Select permission set type

A permission set contains policies that determine a user's permissions to access an AWS account. When you assign a user or group to a permission set in an AWS account, IAM Identity Center creates an IAM role in the account and attaches the policies specified in the permission set to that role. Select an option to specify the permission set type. [Learn more](#)

Permission set type

Types

Predefined permission set

Create a predefined permission set by choosing an AWS-defined template. This template enables you to select a single AWS managed policy. For example, you can select a policy that grants permissions for a common job function, such as Billing, or a specific level of access to AWS services and resources, such as ViewOnlyAccess. You can update the permission set as your needs evolve.

Custom permission set

Create 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).

Policy for predefined permission set

Select an AWS managed policy

AdministratorAccess

Provides full access to AWS services and resources.

Billing

Grants permissions for billing and cost management. This includes viewing account usage and viewing and modifying budgets and payment methods.

DatabaseAdministrator

Grants full access permissions to AWS services and actions required to set up and configure AWS database services.

DataScientist

Grants permissions to AWS data analytics services.

NetworkAdministrator

Grants full access permissions to AWS services and actions required to set up and configure AWS network resources.

PowerUserAccess

Provides full access to AWS services and resources, but does not allow management of Users and groups.

ReadOnlyAccess

Provides read-only access to AWS services and resources.

SecurityAudit

The security audit template grants access to read security configuration metadata. It is useful for software that audits the configuration of an AWS account.

SupportUser

This policy grants permissions to troubleshoot and resolve issues in an AWS account. This policy also enables the user to contact AWS support to create and manage cases.

SystemAdministrator

Grants full access permissions necessary for resources required for application and development operations.

ViewOnlyAccess

This policy grants permissions to view resources and basic metadata across all AWS services.

Cancel

Next

7. Configure permission settings

For **Step 2: Specify permission set details**, keep the default settings, and choose **Next**.

Note

The default settings create a permission set named **AdministratorAccess** with session duration set to one hour.

- Step 1
● Select permission set type
- Step 2
● Specify permission set details
- Step 3
○ Review and create

Specify permission set details

Enter a name for the permission set and specify additional configuration details.

Permission set details

Permission set name
The name that you specify for this permission set appears in the AWS access portal as an available role. After users in IAM Identity Center sign in to the AWS access portal and select an AWS account, they can choose the role.

AdministratorAccess

Permission set names are limited to 32 characters or less. Names may only contain alphanumeric characters and the following special characters: + = , . @ - _

Description - optional
Add a short explanation for this permission set.

Enter a description

Permission set descriptions are limited to 700 characters or less. Descriptions should match the regular expression: [\u0009\u000A\u000D\u0020-\u007E\u00A1-\u00FF]*

Session duration
The length of time a user can be logged on before the console logs them out of their session. [Learn more](#)

1 hour

Relay state - optional
The value used in the federation process for redirecting users within the account. [Learn more](#)

Enter relay state

Relay states support up to 320 characters. Relay states may only contain alphanumeric characters, spaces and the following special characters: & \$ @ # \ / % ? = ~ - _ ' | ! : , ; * + [] () { }

▶ **Tags - optional** (not set)

[Cancel](#)
[Previous](#)
[Next](#)

8. Review and create

For **Step 3: Review and create**, verify that the **Permission set type** uses the AWS managed policy **AdministratorAccess**. Choose **Create**.

You are returned to the **Permission sets** page. A notification appears at the top of the page informing you that the permission set was successfully created.

- Step 1
● Select permission set type
- Step 2
● Specify permission set details
- Step 3
● Review and create

Review and create

Step 1: Select permission set type [Edit](#)

Permission set type	AWS managed policy
Type Predefined permission set	AdministratorAccess

Step 2: Define permission set details [Edit](#)

Permission set details	
Permission set name AdministratorAccess Description -	Session duration 1 hour Relay state -

Tags (not set)

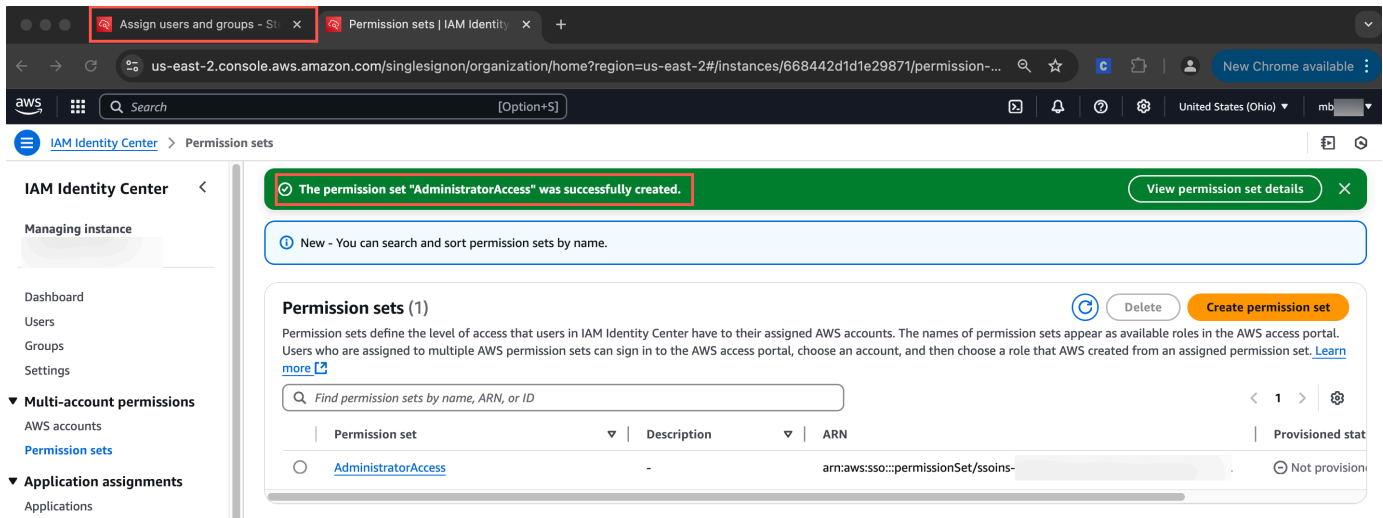
Key	Value
No resources <small>You have not added any tags</small>	

[Cancel](#)
[Previous](#)
[Create](#)

9. Return to assign users page

You are returned to the **Permission sets** page. A notification appears at the top of the page informing you that the permission set was successfully created.

Select **X** to close the current browser tab, and navigate back to the **IAM Identity Center Assign Users** page to continue the previous workflow.

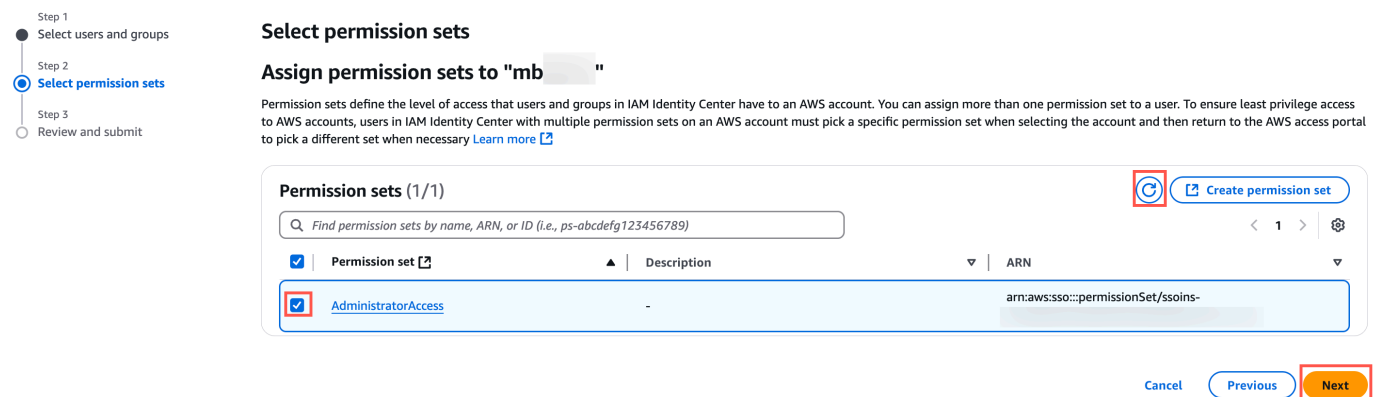


10. Select permission set

On the **Assign users and groups browser tab**, for **Step 2: Select permission sets**, in the **Permission sets** section, select **Refresh**.

- The **AdministratorAccess** permission set you created appears in the list.

Select the **checkbox** for the AdministratorAccess permission set, and choose **Next**.



11. Submit assignment

For **Step 3: Review and submit**, review the selected users and groups and permission set, then choose **Submit**.

Review and submit

Review and submit assignments to "mb [redacted]"

Step 1: Select users and groups Edit

Users and groups (1)

Display name / group name	Type
Admins	Group

Step 2: Select permission sets Edit

Permission sets (1)

Permission set	Description	ARN	Creation time
AdministratorAccess	-	arn:aws:sso::permissionSet/ssoin-	minutes ago

Cancel Previous Submit

12. Verify configuration completion

The page updates with a message that your AWS account is being configured. **Wait** until the process completes.

You are returned to the AWS accounts page in **IAM Identity Center**. A notification message informs you that your AWS account has been reprovisioned and the updated permission set applied.

Configuring your AWS account... do not leave this page Expand details

Configuring in progress

0% 0 of 1 assignments completed

Do not leave this page while we are configuring your AWS accounts. This process may take a few minutes based on the accounts and permission sets being configured. If you close this window before the process is complete, you may need to start it again.

13. Verify configuration

Choose the **AWS Organizations: AWS accounts** breadcrumb.

You can see in the Organization structure section that your AWS account is now the management account under the root of the AWS organization.

- **Reminder:** In this tutorial, we are using a placeholder AWS account name. You will see the name of **your AWS account** instead.

Congratulations, your user can now sign in to your AWS access portal and access resources in your AWS account.

The screenshot shows the IAM Identity Center console for an AWS account named 'mb'. A green notification banner at the top states: "We reprovisioned your AWS account successfully and applied the updated permission set to the account." The account details include the Account ID and email. Under the "Assigned users and groups (1)" section, a table lists the assigned group:

Username / group name	Permission sets	Type
Admins	AdministratorAccess	Group

Step 7: Sign in to the AWS access portal with your administrative credentials

Your new user exists but does not have access to any resources, services, or applications, so the user can't replace your root user for daily administrative tasks yet. Let's give your new user access to your AWS account. Since we put the user into a group, we will assign the group to an account and then we will add a permission set that defines what the members of the group can access.

Note

We will still be using the **root user** credentials for this step.

Now you are ready to sign in using your new administrative user.

If you tried to sign in previously you would have only been able to establish your password and enable up multi-factor authentication (MFA) for your user, because no other permissions had been granted to the user.

Now, the user will have full permissions to your AWS resources, but they will still need to configure a password and set up MFA.

1. Select the **Show QR code** link to show a unique QR code.
 - If you can't scan the QR code, choose the **Show secret key** link to display a text key that you can enter into the Authenticator app to identify your organization. Either scan the QR code with your authenticator app or enter the code in your authenticator app to link your authenticator device to your organization.
 - Once your authenticator has established the link to your organization, it will start generating secret codes that are good for a limited number of seconds.
2. In **Authenticator code box**, type the code you see in the app, and choose **Assign MFA**.

 **Note**

When registering an MFA device with IAM identity Center, only one authenticator code is required for registration.

3. Your authenticator app is successfully registered, select **Done**.

You can register another device, rename or delete your existing MFA device or from the MFA devices page.



Authenticator app registered

✔ Your authenticator app has been successfully registered. You can now use it when prompted for additional verification at sign in.

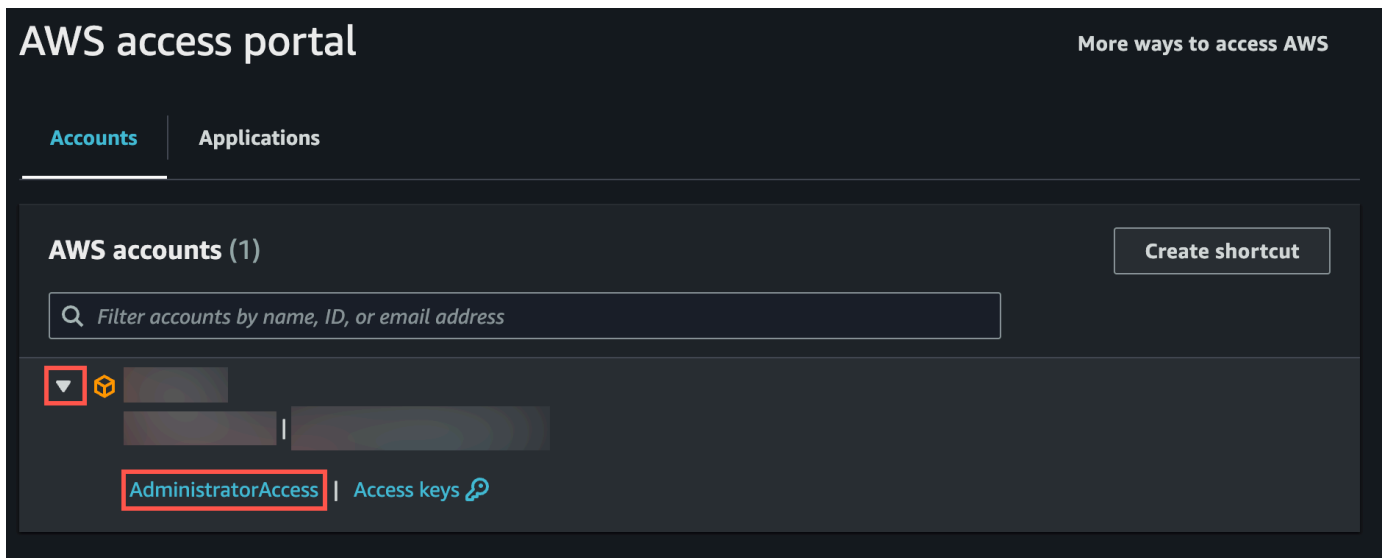
John's MFA 1 [Rename](#)

Type and description: Authenticator app



Done

4. From the access portal, select **AWS Account**, select your **<account name>**. Then, select **Management console**.
 - The AWS management console opens. As a user with administrative access, you can add services, add additional users, and configure policies and permissions. You no longer need to use your root user to accomplish these tasks.



5. Open IAM Identity Center

An email was sent to the email address you specified when you created the user. The email contains three important items:

- A link to accept the invitation to join
- The URL of your AWS access portal
- Your username that you will use to sign in

Open the email and **record the AWS access portal URL** and the **Your Username**. You will need this information later in this tutorial.

Select the **Accept invitation** button in the email.

Tip: If you don't see the Invitation to join IAM Identity Center email in your inbox folder, check your spam, junk, and deleted items (or trash) folders. All emails sent by the IAM Identity Center service will come from either the address `no-reply@signin.aws` or `no-reply@login.awsapps.com`. If you can't find the email, **sign in** as the root user and **reset** the Identity Center user's password. For instructions, see [Reset an IAM Identity Center user password](#). If you still don't receive the email, reset the password again and choose the option to **Generate a one-time password** that you can share with the user instead.



Hello John,

Your administrator has requested you to verify your email address. To complete email verification, choose the following link:

[Verify your email address](#)

This link will expire in 7 days.

6. Sign in to AWS

The link opens a browser window and displays a **Sign in** page.

In the **Sign in** page, enter the password used for creating the IAM user sign in earlier in this tutorial.



Sign in

Username

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

7. Enter your password

Enter your password, and choose **Sign in**.



Sign in

Username:
John ([not you?](#))

Password

Show password [Forgot password](#)

Sign in

Cancel

This is a trusted device. [Learn more](#)

8. Set up MFA

The AWS console opens.

You will be automatically prompted to **Register MFA device**.

Choose one of the options to get started. For this tutorial, we have selected **Authenticator app**.

Notes:

- Options not supported by your browser or platform are dimmed and can't be selected.
- This is similar to the process you followed when you **set up the MFA device for your root user in Module 2**. The difference is that this MFA device is being registered with IAM Identity Center instead of IAM.
- If you select a different MFA device, follow the instructions for the device you selected.

Register MFA device

Username:

John ([not you?](#))

Your organization requires multi-factor authentication (MFA) for added security during sign-in. Each time you sign in, you'll be prompted for your password and an MFA device.

[Learn more](#) 

Select one of the options below to get started:



Authenticator app

Authenticate using a code generated by an app installed on your mobile device or computer.



Security key

Authenticate by touching a hardware security key such as YubiKey, Feitian, etc.



Built-in authenticator

Authenticate using a fingerprint scanner or camera built-in to your computer such as Apple TouchID, Windows Hello, etc.


Next

9. Configure MFA device

Select the **Show QR code** link to show a unique QR code.

- If you can't scan the QR code, choose the **Show secret key** link to display a text key that you can enter into the Authenticator app to identify your organization. Either scan the QR code with your authenticator app or enter the code in your authenticator app to link your authenticator device to your organization.
- Once your authenticator has established the link to your organization, it will start generating secret codes that are good for a limited number of seconds.

In **Authenticator code box**, type the code you see in the app, and choose **Assign MFA**.

 **Note**

When registering an MFA device with IAM identity Center, only one authenticator code is required for registration.

Set up the authenticator app


Username:

John ([not you?](#))

[Back to MFA device options](#)

1



Install either the Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer. [See a list of compatible apps](#) 

2



Use your virtual MFA app or your device's camera to scan the QR code ([show secret key](#))

3

Please enter the six digit code from your authenticator app

Authenticator code

123456

Assign MFA

10. Complete MFA setup

Your authenticator app is successfully registered, select **Done**.

You can register another device, rename or delete your existing MFA device or from the MFA devices page.



Authenticator app registered

✔ Your authenticator app has been successfully registered. You can now use it when prompted for additional verification at sign in.

John's MFA 1 [Rename](#)

Type and description: Authenticator app

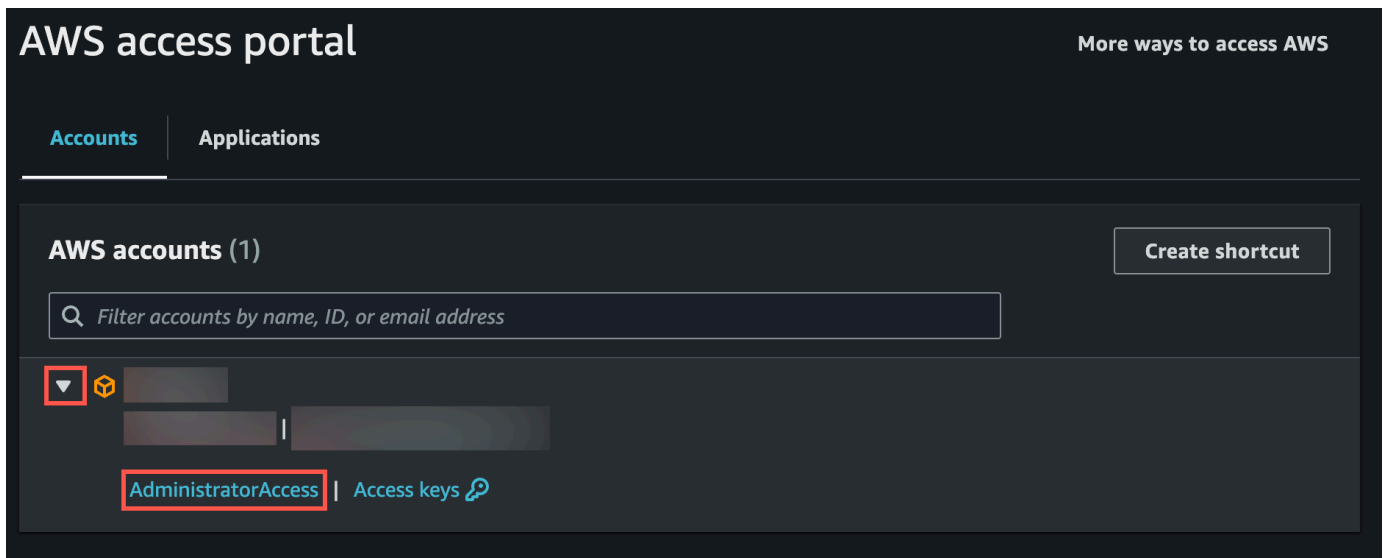


Done

11. Open the AWS Management Console

From the access portal, select **AWS Account**, select your **<account name>**. Then, select **Management console**.

- The AWS Management Console opens. As a user with administrative access, you can add services, add additional users, and configure policies and permissions. You no longer need to use your root user to accomplish these tasks.



Conclusion

Congratulations! You have now completed the sign-in process, created an administrative user in IAM Identity Center, added enhanced security for both your root user and your administrative user, and are ready to start working with AWS services and applications. Remember, when you sign in using your Identity Center administrative user, you will use the access portal URL you received in your invitation email.

⚠ Important

Each AWS Organization has a unique access portal URL. Make sure you keep a record of it with your user sign-in information.

Module 3: (Optional) Set Up the AWS CLI

Time to complete	10 minutes
Module requirements	An internet browser An AWS account
Get help	Common CLI errors

Introduction

The AWS CLI is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

To interact with AWS using the CLI, you need to configure credentials for it to use when making API calls. In this module, you will also learn how you can set up multiple profiles to access more than one AWS account, either with additional credentials, or through IAM role switching.

Implementation

Step 1: Install the AWS CLI

There are different ways to install the AWS CLI, depending on your operating system or preference to use containers.

Install the AWS CLI v2 for your operating system (OS), using the instructions [here](#).

```
aws --version
```

Example: the response when installing the AWS CLI on macOS Ventura 13.6 is as follows:

```
aws-cli/2.15.9 Python/3.11.6 Darwin/22.6.0 exe/x86_64 prompt/off
```

The AWS CLI is now installed and you are ready to configure your credentials.

Step 2: Configure the AWS CLI

To configure the credentials, you will need to include the credentials of the user you created in Module 2 of this tutorial.

You will be prompted to provide the following information for each of these items in the CLI:

- **SSO session name:** Provides a name for the session that is included in the AWS CloudTrail logs for entries associated with this session. If you don't enter a name, one is generated automatically. For this tutorial, use `<Test1>`.
- **SSO start URL:** The **AWS Access portal URL** you were provided when you configured IAM Identity Center.

Note

The URL can be found in the Settings summary in the IAM Identity Center console Dashboard.

- **SSO region:** In this tutorial the examples use `<us-east-1>`. You must **specify the region** in which you have enabled IAM Identity Center.

Note

You can find this information in the Settings summary in the IAM Identity Center console Dashboard.

- **SSO registration scopes:** Scopes authorize access to different endpoints. In this tutorial, we will use the minimum scope of `<sso:account:access>` to get a refresh token back from the IAM Identity Center service.

1. Run configuration command

In your CLI, **run** the following command:

```
aws configure sso
```

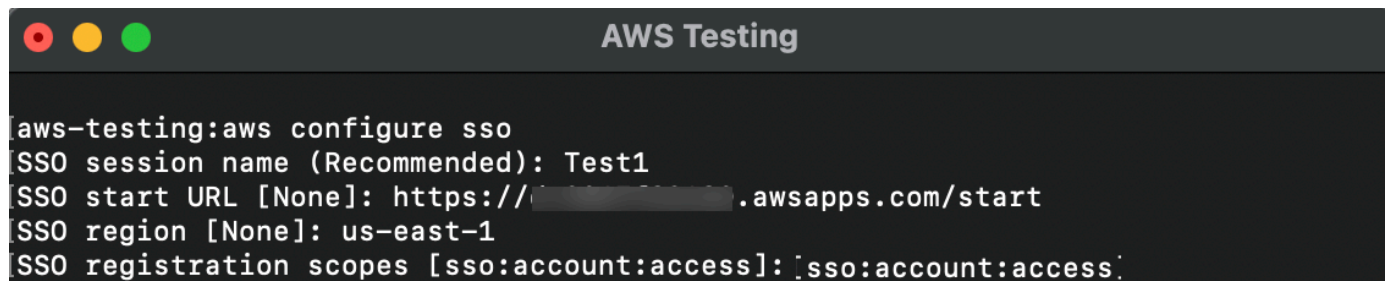
2. Enter SSO details

Provide the **required information** when prompted. Remember to use your **SSO start URL** and **SSO region**.

- SSO session name (Recommended): **Test1**
- SSO start URL [None]: **<https://my-sso-portal.awsapps.com/start>**
- SSO region [None]: **<us-east-1>**
- SSO registration scopes [None]: **sso:account:access**

The following image is an example of the CLI content at this stage.

The CLI attempts to automatically open the SSO authorization page in your default browser and begins the sign in process for your IAM Identity Center account.

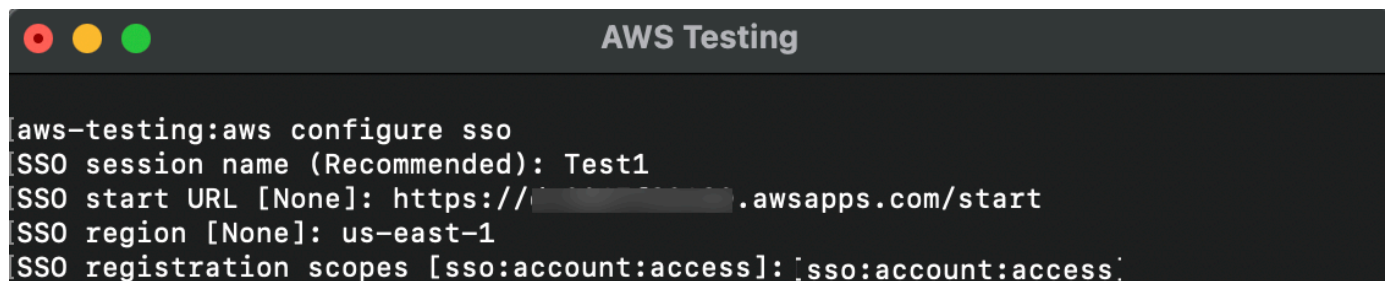
A terminal window titled "AWS Testing" with a dark background and light text. The prompt is "aws-testing:aws configure sso". The user has entered "Test1" for the session name, a URL ending in ".awsapps.com/start" for the start URL, "us-east-1" for the region, and "sso:account:access" for the registration scopes.

```
aws-testing:aws configure sso
SSO session name (Recommended): Test1
SSO start URL [None]: https://[REDACTED].awsapps.com/start
SSO region [None]: us-east-1
SSO registration scopes [sso:account:access]: [sso:account:access]
```

3. Authorize CLI access

You might be asked to provide your password (and MFA credential, if enabled). On the Authorization requested page, select Confirm and continue.

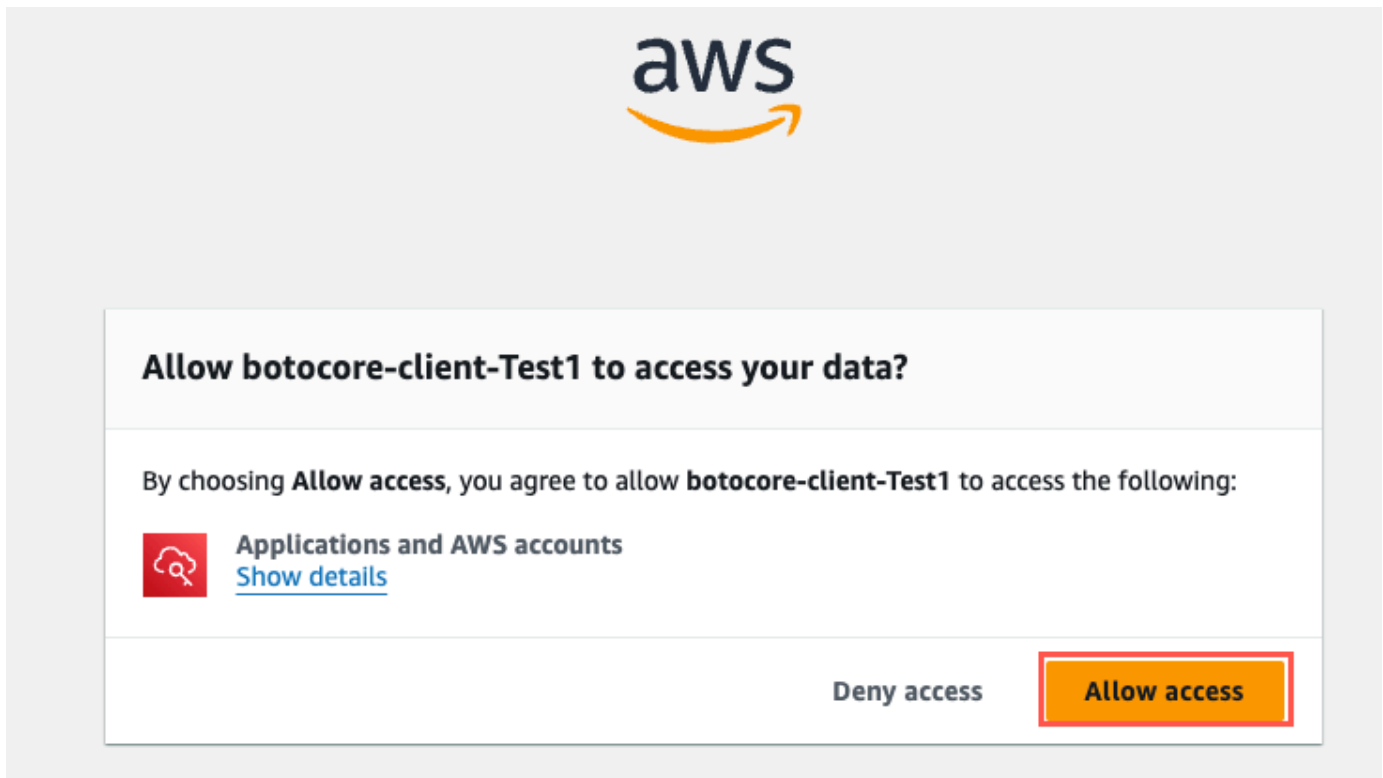
This gives permissions to the AWS CLI to retrieve and display the AWS accounts and roles that you are authorized to use with IAM Identity Center.

A terminal window titled "AWS Testing" with a dark background and light text. The prompt is "aws-testing:aws configure sso". The user has entered "Test1" for the session name, a URL ending in ".awsapps.com/start" for the start URL, "us-east-1" for the region, and "sso:account:access" for the registration scopes.

```
aws-testing:aws configure sso
SSO session name (Recommended): Test1
SSO start URL [None]: https://[REDACTED].awsapps.com/start
SSO region [None]: us-east-1
SSO registration scopes [sso:account:access]: [sso:account:access]
```

4. Grant permissions

Since the AWS CLI is built on top of the SDK for Python, permission messages may contain variations of the botocore name, such as **botocore-client-Test1**. Select **Allow access**. After authentication, you will be told that you can close the window.



5. Review available accounts

Navigate back to your **CLI window**. The CLI will update and show you the **AWS accounts** and **roles** that are available to you.

- Because you have only set up one AWS account with the **AdministratorAccess** role at this point that is the account and role you are signed in with.

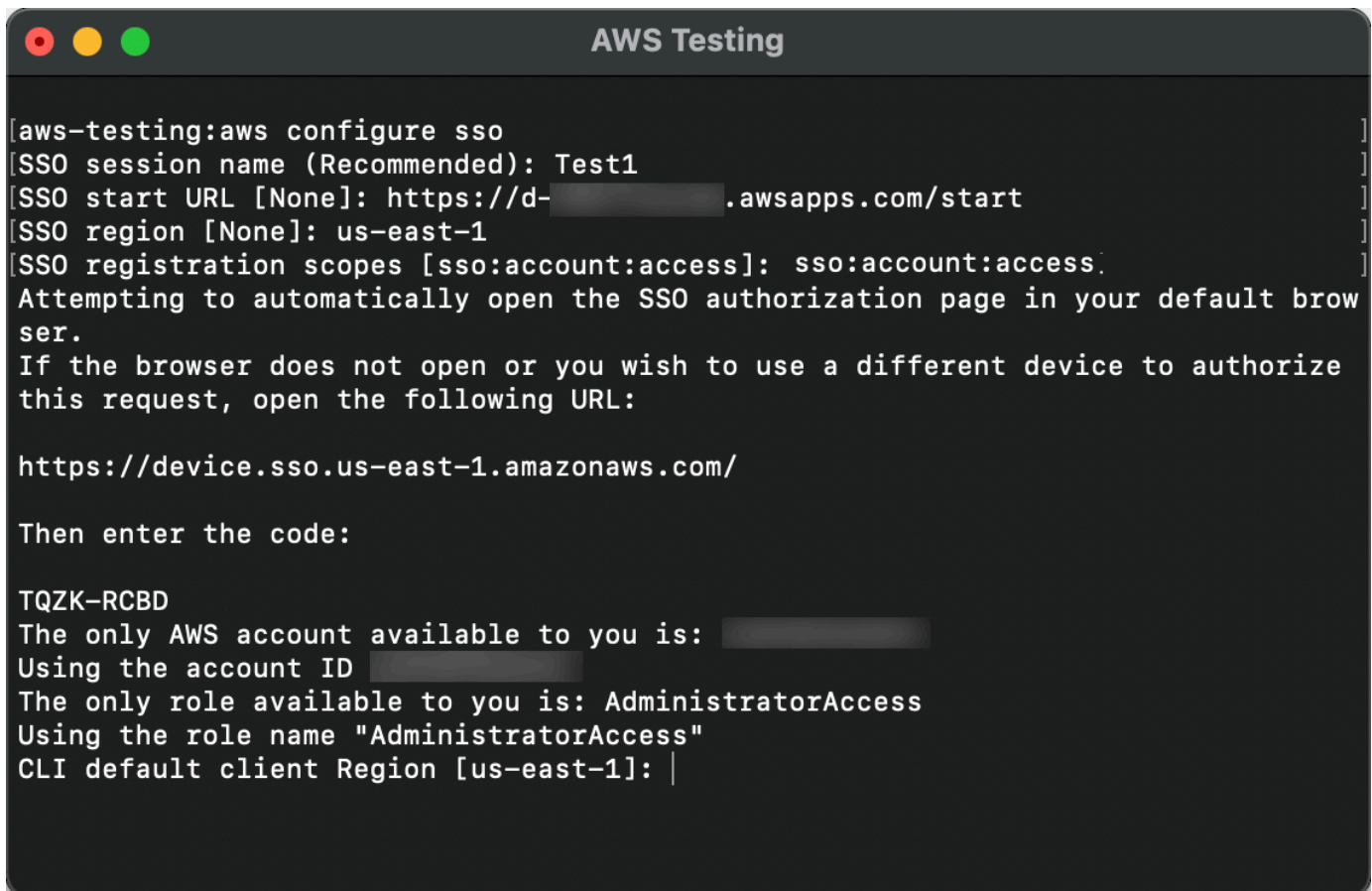
Your CLI window should now look like the example image to the right and have the following lines displayed.

The only AWS account available to you is: 111122223333

Using the account ID 111122223333

The only role available to you is: AdministratorAccess

Using the role name "AdministratorAccess"



```
aws-testing:aws configure sso
[SSO session name (Recommended): Test1
[SSO start URL [None]: https://d-.....awsapps.com/start
[SSO region [None]: us-east-1
[SSO registration scopes [sso:account:access]: sso:account:access
Attempting to automatically open the SSO authorization page in your default browser.
If the browser does not open or you wish to use a different device to authorize this request, open the following URL:

https://device.sso.us-east-1.amazonaws.com/

Then enter the code:

TQZK-RCBD
The only AWS account available to you is: .....
Using the account ID .....
The only role available to you is: AdministratorAccess
Using the role name "AdministratorAccess"
CLI default client Region [us-east-1]: |
```

6. Set CLI preferences

In the terminal window, when prompted, enter the following information:

- For **CLI default client Region [<your-region>]**: enter the Region where you enabled IAM Identity Center. For this tutorial we used **us-east-1**
- For **CLI default output format [None]**: enter **json**
- For **CLI profile name [AdministratorAccess-xxxxxxxxxxxx]**: enter **admin-1**
 - The **suggested profile name** is the account ID number followed by an underscore followed by the role name, however for this tutorial, we are going to use a shorter profile name, **admin-1**.

Your CLI window should now look similar to the example image on the right and have these lines displayed:

To use this profile, specify the profile name using `--profile`, as shown: `aws s3 ls --profile admin-1`

```

AWS Testing
[CLI default client Region [us-east-1]: us-east-1 ]
[CLI default output format [None]: json ]
[CLI profile name [AdministratorAccess-...]: admin-1 ]

To use this profile, specify the profile name using --profile, as shown:

aws s3 ls --profile admin-1
aws-testing:

```

7. (Optional) View the configuration file

This session created a config file located at `~/.aws/config` on computers running Linux or macOS, or at `C:\Users\USERNAME\.aws\config` on computers running Windows. Your config file will look similar to the example image.

```

config
[default]
region = us-east-1
output = json
[ss-session 'Test 1']
sso_start_url = https://d-...awsapps.com/start
sso_region = us-east-1
sso_registration_scopes = sso
[ss-session Test]
sso_start_url = https://d-...awsapps.com/start
sso_region = us-east-1
sso_registration_scopes = sso:account:access

```

8. Start SSO session

You can now use this **sso-session and profile** to request credentials by **running** the following command:

```
aws sso login --profile admin-1
```

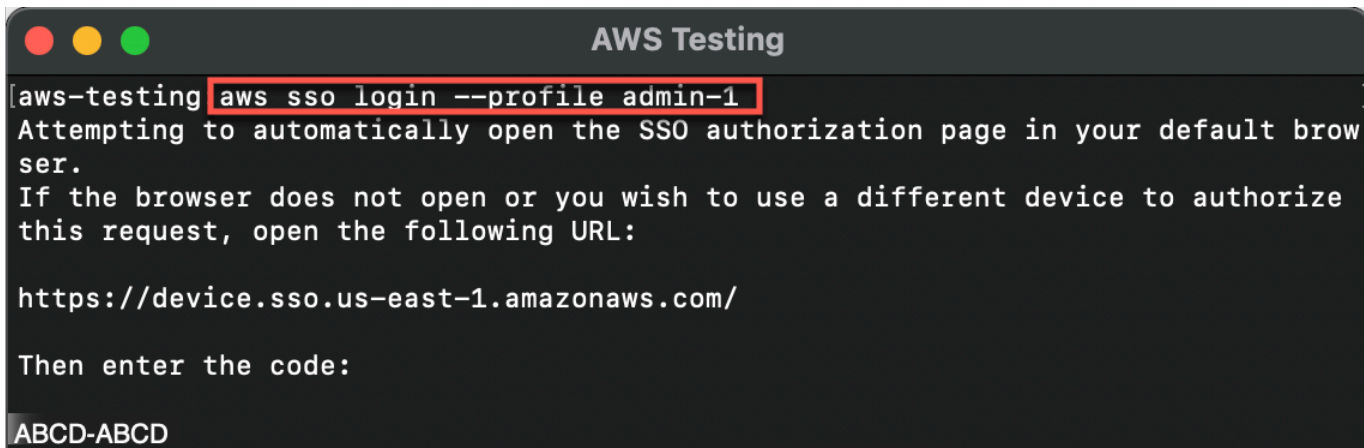
Your CLI window should now look similar to the example image on the right and have these lines displayed:

aws sso login --profile admin-1 Attempting to automatically open the SSO authorization page in your default browser.

If the browser does not open or you wish to use a different device to authorize this request, open the following URL: <https://device.sso.us-east1.amazonaws.com/>

Then enter the code:

ABCD-ABCD



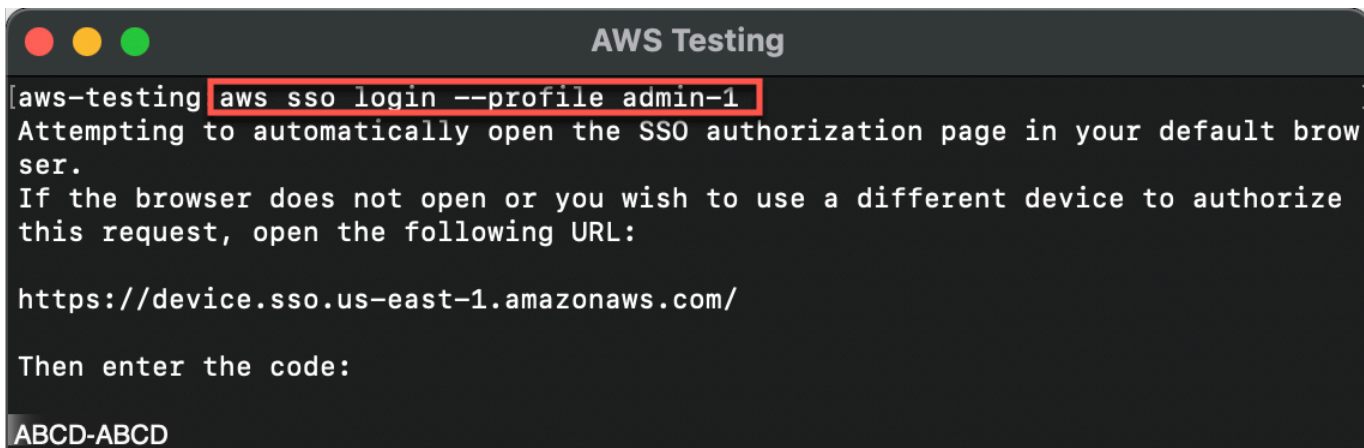
```
aws-testing [aws sso login --profile admin-1]
Attempting to automatically open the SSO authorization page in your default browser.
If the browser does not open or you wish to use a different device to authorize this request, open the following URL:
https://device.sso.us-east-1.amazonaws.com/
Then enter the code:
ABCD-ABCD
```

9. Complete authentication

Navigate to the browser window and **allow access** to your data. When you return to the CLI window the following message should be displayed:

Successfully logged into Start URL: <https://my-sso-portal.awsapps.com/start>

For more information about CLI file credential, see the [Configuration and credential file settings in the AWS CLI](#) in the **AWS Command Line Interface** user guide.



```
aws-testing [aws sso login --profile admin-1]
Attempting to automatically open the SSO authorization page in your default browser.
If the browser does not open or you wish to use a different device to authorize this request, open the following URL:
https://device.sso.us-east-1.amazonaws.com/
Then enter the code:
ABCD-ABCD
```

Step 3: (Optional) Configure multiple profiles

As you add roles to your AWS account and add additional AWS accounts to your organization, repeat the procedure above to create a profile for those roles and accounts.

As you add complexity having a profile naming strategy that associates AWS account IDs and role names is recommended so that you can distinguish between the profiles.

For more information about configuring and formatting multiple roles, see the [Format of the configuration and credential files](#) in the **AWS Command Line Interface** user guide.

Conclusion

Congratulations! You have now completed the sign-in process, created an administrative user in IAM Identity Center, added enhanced security for both your root user and your administrative user, and set up the AWS CLI and configured a named profile.