



Try the new sign in UI

See our new improved Amazon Web Services sign in experience before we officially launch.



Enable new sign in



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

username@example.com

Next

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.

— New to AWS? —

Amazon Nova, new foundation models that deliver frontier intelligence and industry leading price performance

[Learn more ›](#)



Try the new sign in UI

See our new improved Amazon Web Services sign in experience before we officially launch.



Enable new sign in



Root user sign in 

Email:

Password

[Forgot password?](#)

.....

Sign in

[Sign in to a different account](#)

[Create a new AWS account](#)

**Amazon Nova, new
foundation models that
deliver frontier intelligence
and industry leading
price performance**

[Learn more ›](#)



Try the new sign in UI

See our new improved Amazon Web Services sign in experience before we officially launch.



Enable new sign in



Confirm you're you

We sent an email with a verification code to

[tushar@amazon.com](#)

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?](#)

**Amazon Nova, new
foundation models that
deliver frontier intelligence
and industry leading
price performance**










[Learn more ›](#)

Console Home [Info](#)

Reset to default layout

+ Add widgets

Recently visited [Info](#)

-  IAM
-  S3
-  EC2
-  Billing and Cost Management
-  IAM Identity Center
-  EC2 Global View
-  AWS Billing Conductor
-  CloudWatch
-  Trusted Advisor

[View all services](#)

Applications (0) [Info](#)

Create application

Region: US East (N. Virginia)

Select Region

us-east-1 (Current Region) ▼

< 1 >

Name ▼	Description ▼	Region ▼	Origin ★ ▲
--------	---------------	----------	------------

No applications
Get started by creating an application.

Create application

[Go to myApplications](#)

Welcome to AWS










AWS Health [Info](#)

Cost and usage [Info](#)



Console Home [Info](#)

Recently visited [Info](#)

-  IAM
-  S3
-  EC2
-  Billing and Cost Management
-  IAM Identity Center
-  EC2 Global View
-  AWS Billing Conductor
-  CloudWatch
-  Trusted Advisor

[View all services](#)

Applications (0) [Info](#)

Region: US East (N. Virginia)

Select Region

us-east-1 (Current Region) ▼


Name ▼	Description
--------	-------------

No applications
Get started by creating an application.

[Create application](#)

[Go to myApplications](#)

Account ID

 1 [redacted]

[Account](#)

[Organization](#)

[Service Quotas](#)

[Billing and Cost Management](#)

[Security credentials](#)

[Turn on multi-session support](#)

[Sign out](#)

Welcome to AWS

AWS Health [Info](#)

Cost and usage [Info](#)

My security credentials

Root user

Info

The root user has access to all AWS resources in this account, and we recommend following [best practices](#). To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference

You don't have MFA assigned

As a security best practice, we recommend you assign MFA.

Assign MFA

Account details

Account name

ModestusMadu

AWS account ID

Email address

Canonical user ID

Actions

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

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

- Step 1
- Select MFA device
- Step 2
- Set up device

Select MFA device [Info](#)

MFA device name

Device name

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


Account2MFA

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

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/security_credentials/mfa

aws

Search

[Alt+S]

IAM

IAM > Security credentials > Assign MFA device

Step 1

Select MFA device

Step 2

Set up device

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

MFA Code 1

Wait 30 seconds, and enter a second code entry.

MFA Code 2

Cancel

Previous

Add MFA

1

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 1

Select MFA device

Step 2

 Set up device

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



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

MFA Code 1

Wait 30 seconds, and enter a second code entry.

MFA Code 2

Cancel

[Previous](#)

Add MFA

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/security_credentials

aws

Search

[Alt+S]

🔍

🔔

?

⚙️

Global

ModestusMadu

IAM

Security credentials

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

Users groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Resource control policies

IAM Identity Center

AWS Organizations

✔️ MFA device assigned

You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

Account details

Account name

Account ID

Email address

Canonical user ID

Multi-factor authentication (MFA) (1)

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
Virtual	arn:aws:iam::111111111111:mfa/Account2MFA	Not Applicable	Wed May 07 2025

Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

Access key ID	Created on	Access key last used	Region last used	Service last used	Status
No access keys					

As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more](#)

CloudFront key pairs (0)

You use key pairs in Amazon CloudFront to create signed URLs. You can have a maximum of two CloudFront key pairs (active or inactive) at a time.

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)