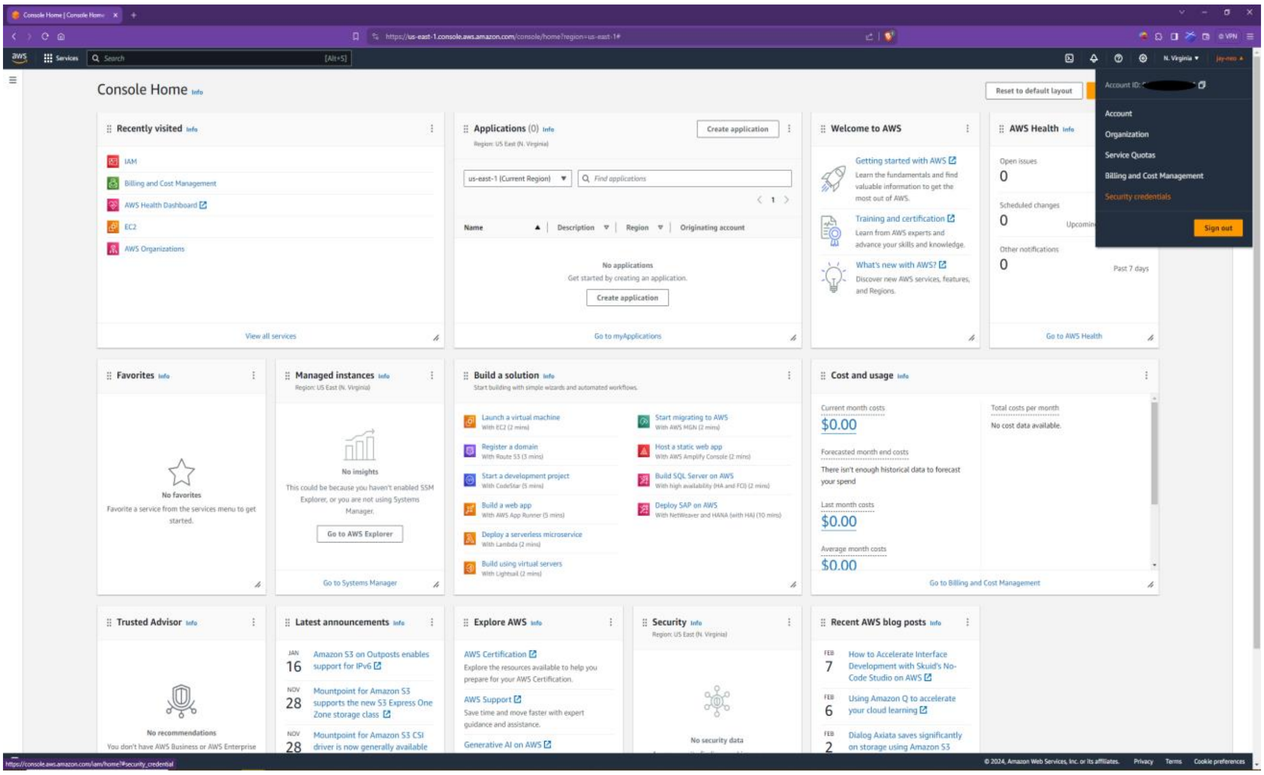
Assignment 2

Statement: Create MFA for authentication.

Steps: Multi-Factor Authentication (MFA) is an AWS identity and Access Management(IAM) best practice that requires a second authentication factor in addition to username and password sign-in credential.

a) At first download Google authentication app in mobile.
b) Now go to Account and click on 'Security credentials'.



Account ID: [redacted]

No applications
Get started by creating an application.

Learn the fundamentals and find valuable information to get the most out of AWS.

Learn from AWS experts and advance your skills and knowledge.

Discover new AWS services, features, and Regions.

No favorites
Favorite a service from the services menu to get started.

No insights
This could be because you haven't enabled SSM Explorer, or you are not using Systems Manager.

Start building with simple wizards and automated workflows.

No cost data available.

There isn't enough historical data to forecast your spend

No recommendations
You don't have AWS Business or AWS Enterprise

Amazon S3 on Outposts enables support for IPv6

Mountpoint for Amazon S3 supports the new S3 Express One Zone storage class

Mountpoint for Amazon S3 CSI driver is now generally available

Explore the resources available to help you prepare for your AWS Certification.

Save time and move faster with expert guidance and assistance.

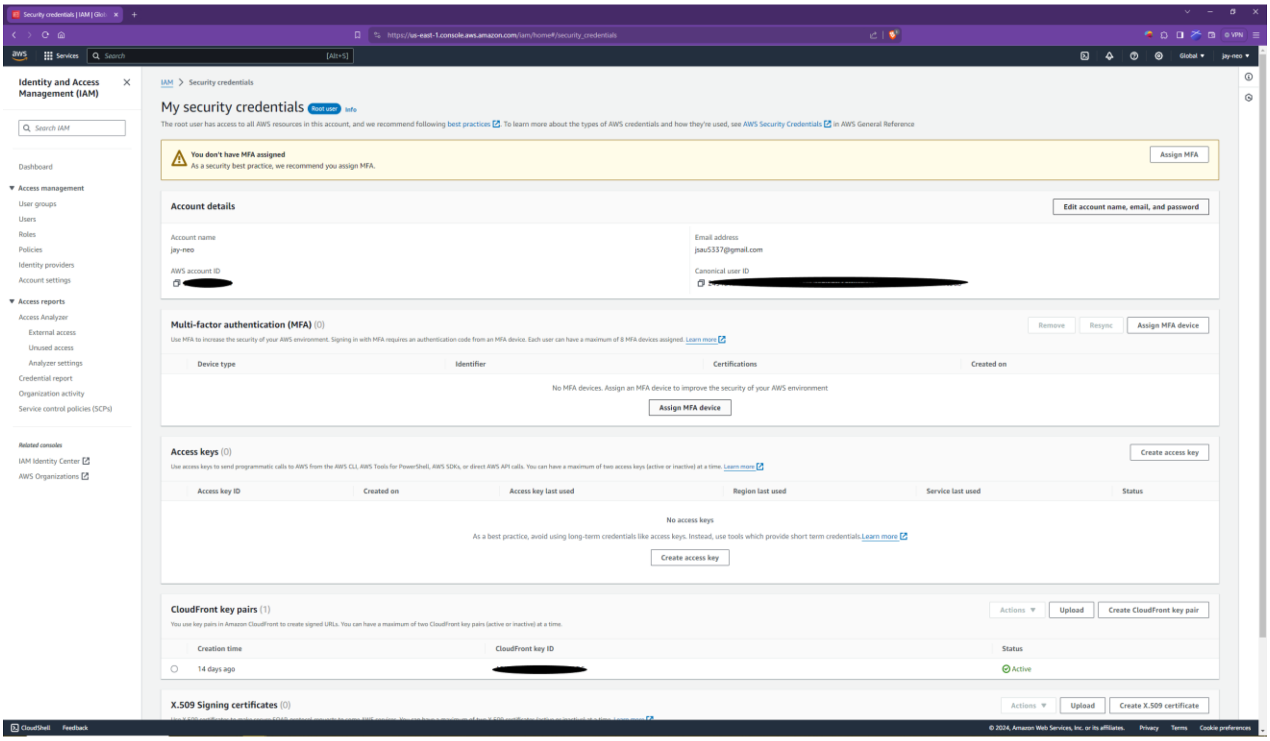
No security data

How to Accelerate Interface Development with Skuid's No-Code Studio on AWS

Using Amazon Q to accelerate your cloud learning

Dialog Axiata saves significantly on storage using Amazon S3

c) Click on 'Assign MFA device'



My security credentials

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.

Account details

Account name
jay-neo

Email address
jsau5337@gmail.com

AWS account ID
[redacted]

Canonical user ID
[redacted]

Multi-factor authentication (MFA) (0)

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

Device type	Identifier	Certifications	Created on

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

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

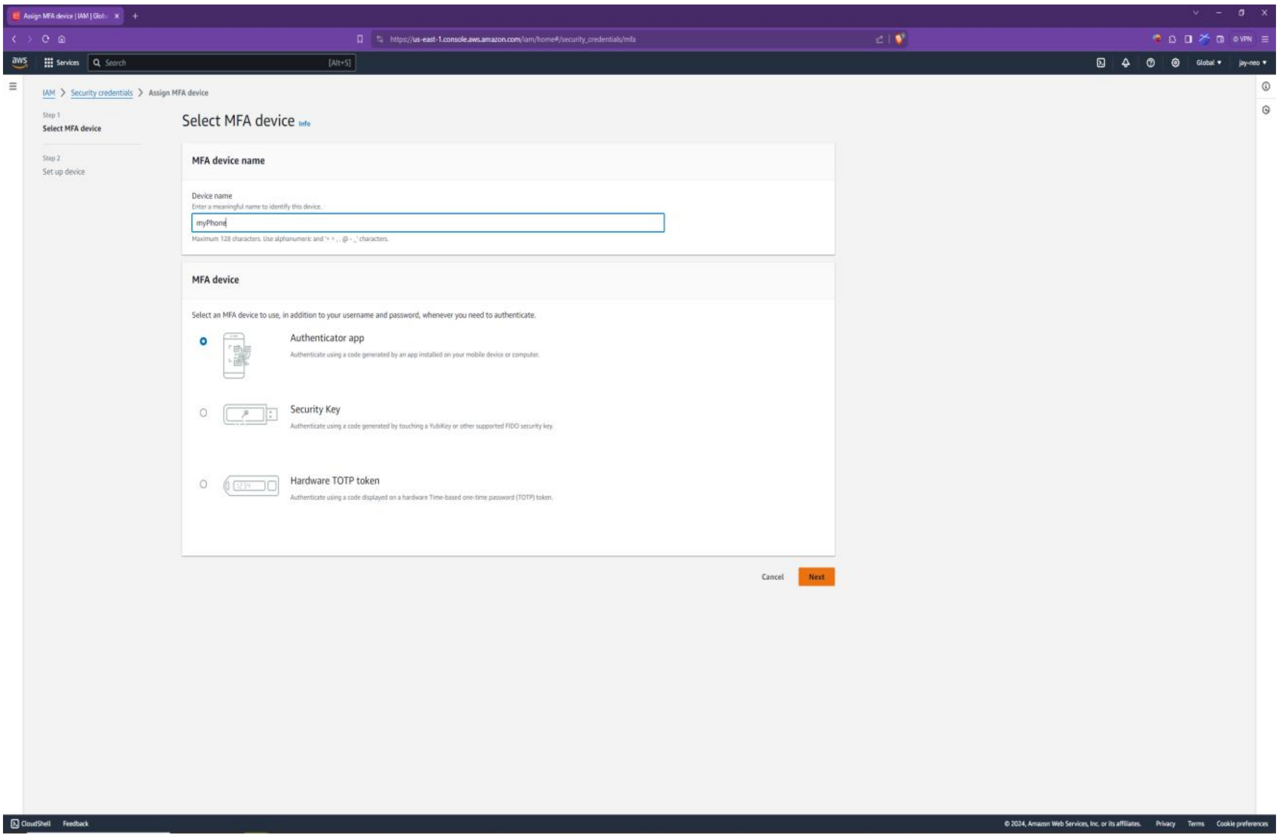
CloudFront key pairs (1)

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.

	Creation time	CloudFront key ID	Status
○	14 days ago	[redacted]	Active

X.509 Signing certificates (0)

d) Give one device name (Here myPhone is the device name given). After that from the list of MFA device choose the option ‘Authenticator app’ (default).


Assign MFA device | IAM | Glob
https://us-east-1.console.aws.amazon.com/iam/home#/security_credentials/mfa
aws
Services
Search
[Alt+S]
Global
jay-neo
IAM > Security credentials > Assign MFA device
Step 1
Select MFA device
Step 2
Set up device
Info
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Select MFA device

MFA device name

Device name
Enter a meaningful name to identify this device.
myPhone
Maximum 128 characters. Use alphanumeric and '+ = , . @ - _' characters.

MFA device

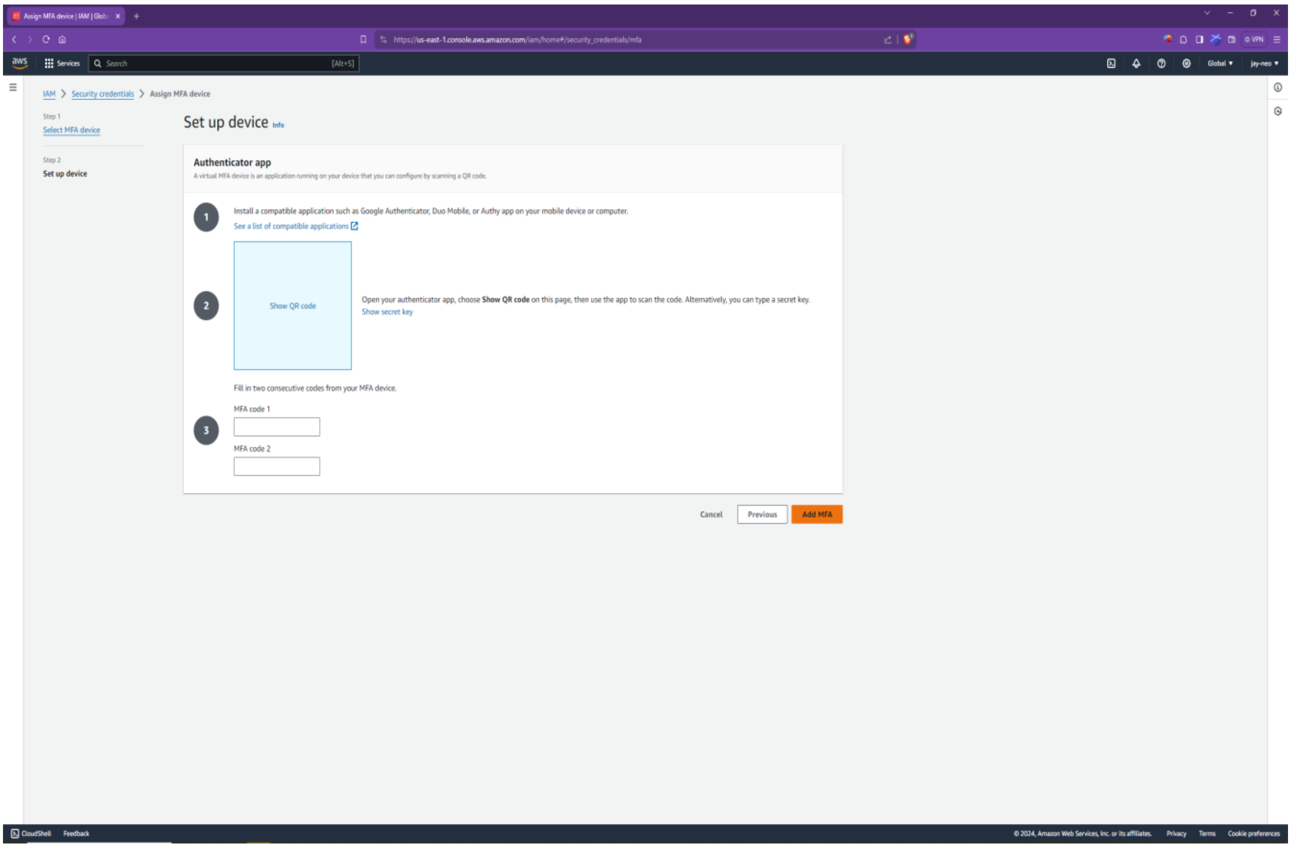
Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.

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

○ Security Key
Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.

○ Hardware TOTP token
Authenticate using a code displayed on a hardware Time-based one-time password (TOTP) token.

e) Then select the option ‘Next’ in the bottom


Assign MFA device | IAM | Glob
https://us-east-1.console.aws.amazon.com/iam/home#/security_credentials/mfa
aws
Services
Search
[Alt+S]
Global
jay-neo
IAM > Security credentials > Assign MFA device
Step 1
Select MFA device
Step 2
Set up device
Info
Show QR code
Cancel
Previous
Add MFA
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Set up device

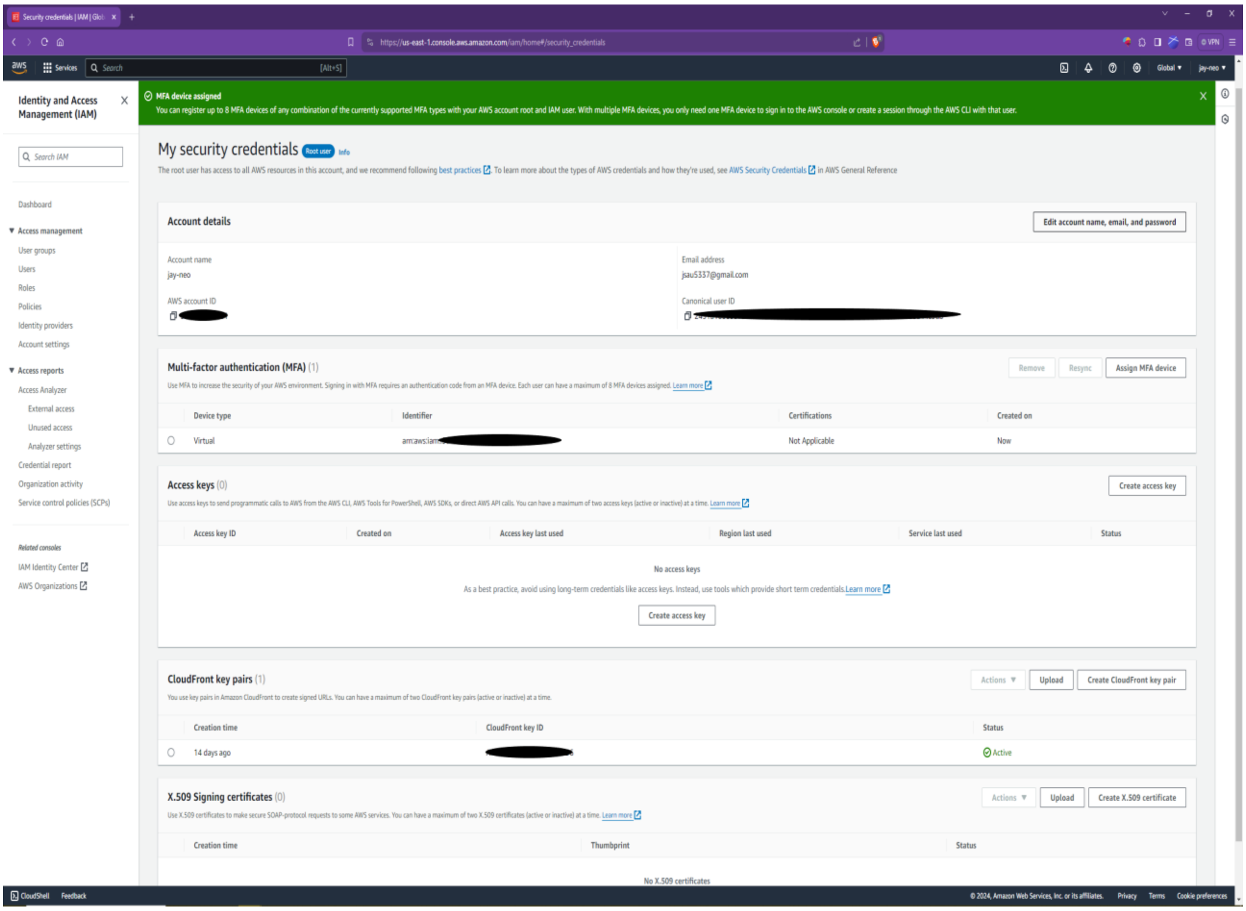
Authenticator app
A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

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 Fill in two consecutive codes from your MFA device.
MFA code 1
MFA code 2

g) Now give two MFA codes .In app at first MFA code 1 will be generated then code 2 will be generated. we have to copy those. h) After copying those two code and click on 'Add MFA', MFA will create for this account.



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.

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

Account details Edit account name, email, and password

Account name
jay-neo

Email address
jsau5337@gmail.com

AWS account ID
[redacted]

Canonical user ID
[redacted]

Multi-factor authentication (MFA) (1) 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

	Device type	Identifier	Certifications	Created on
○	Virtual	arn:aws:iam[redacted]	Not Applicable	Now

Access keys (0) Create access key

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

Create access key

CloudFront key pairs (1) Actions ▾ Upload Create CloudFront key pair

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.

	Creation time	CloudFront key ID	Status
○	14 days ago	[redacted]	Active

X.509 Signing certificates (0) Actions ▾ Upload Create X.509 certificate

Use X.509 certificates to make secure SOAP-protocol requests to some AWS services. You can have a maximum of two X.509 certificates (active or inactive) at a time. Learn more

Creation time	Thumbprint	Status

No X.509 certificates