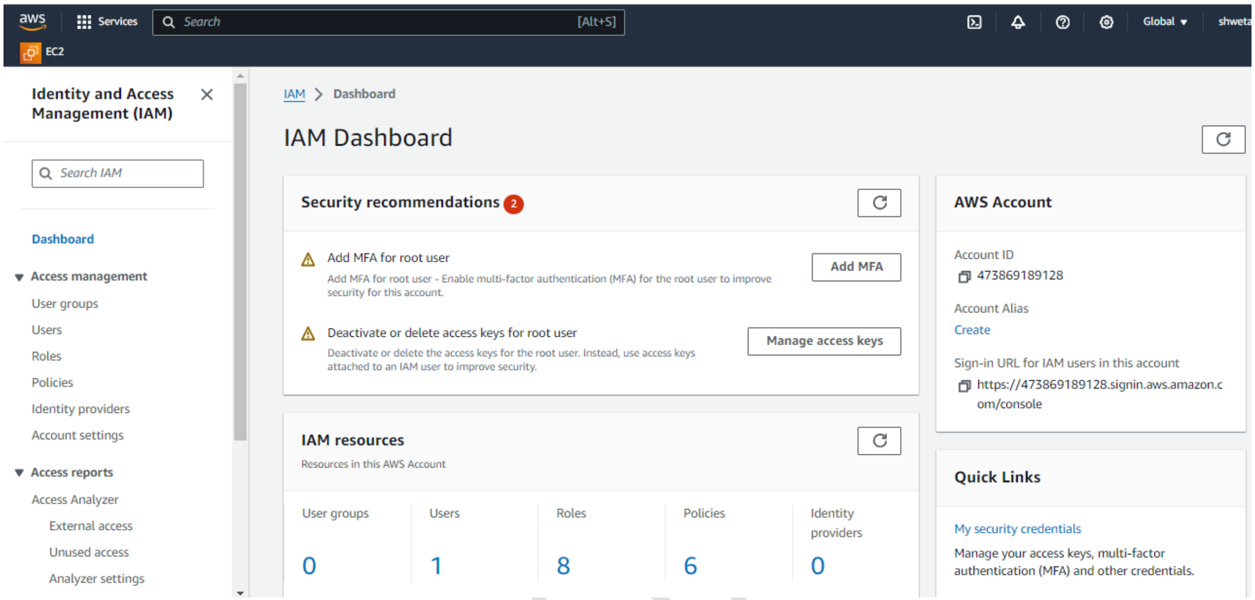
ADD MULTI-FACTOR AUTHENTICATION (MFA) FOR IAM USER

Navigate to the IAM Dashboard:



Identity and Access Management (IAM)

Search IAM

Dashboard

- Access management
  - User groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
- Access reports
  - Access Analyzer
    - External access
    - Unused access
    - Analyzer settings

IAM > Dashboard

IAM Dashboard

Security recommendations 2

Add MFA for root user — Add MFA

Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Deactivate or delete access keys for root user — Manage access keys

Deactivate or delete the access keys for the root user. Instead, use access keys attached to an IAM user to improve security.

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	1	8	6	0

AWS Account

Account ID
473869189128

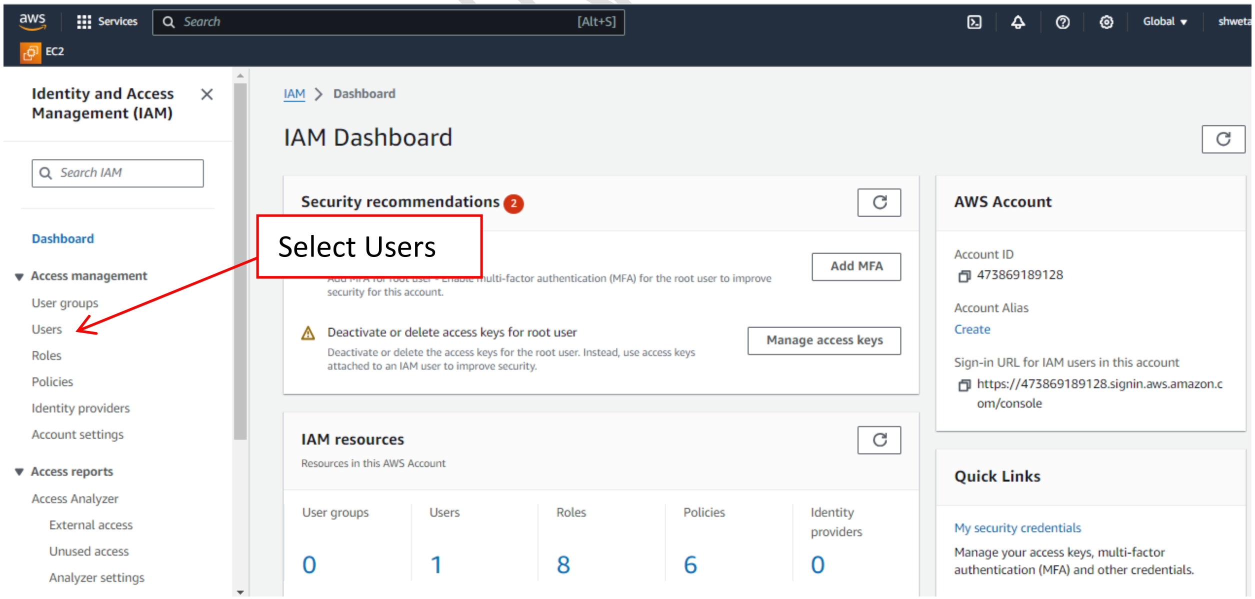
Account Alias
Create

Sign-in URL for IAM users in this account
https://473869189128.signin.aws.amazon.com/console

Quick Links

My security credentials

Manage your access keys, multi-factor authentication (MFA) and other credentials.



Select Users

Identity and Access Management (IAM)

Search IAM

Dashboard

- Access management
  - User groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
- Access reports
  - Access Analyzer
    - External access
    - Unused access
    - Analyzer settings

IAM > Dashboard

IAM Dashboard

Security recommendations 2

Add MFA

Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Deactivate or delete access keys for root user — Manage access keys

Deactivate or delete the access keys for the root user. Instead, use access keys attached to an IAM user to improve security.

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	1	8	6	0

AWS Account

Account ID
473869189128

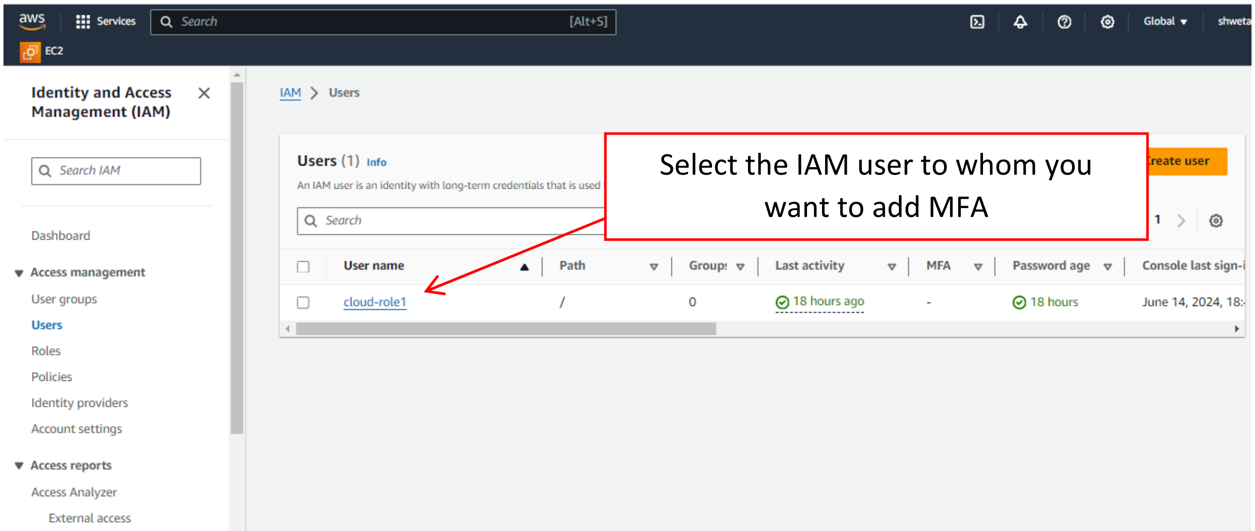
Account Alias
Create

Sign-in URL for IAM users in this account
https://473869189128.signin.aws.amazon.com/console

Quick Links

My security credentials

Manage your access keys, multi-factor authentication (MFA) and other credentials.

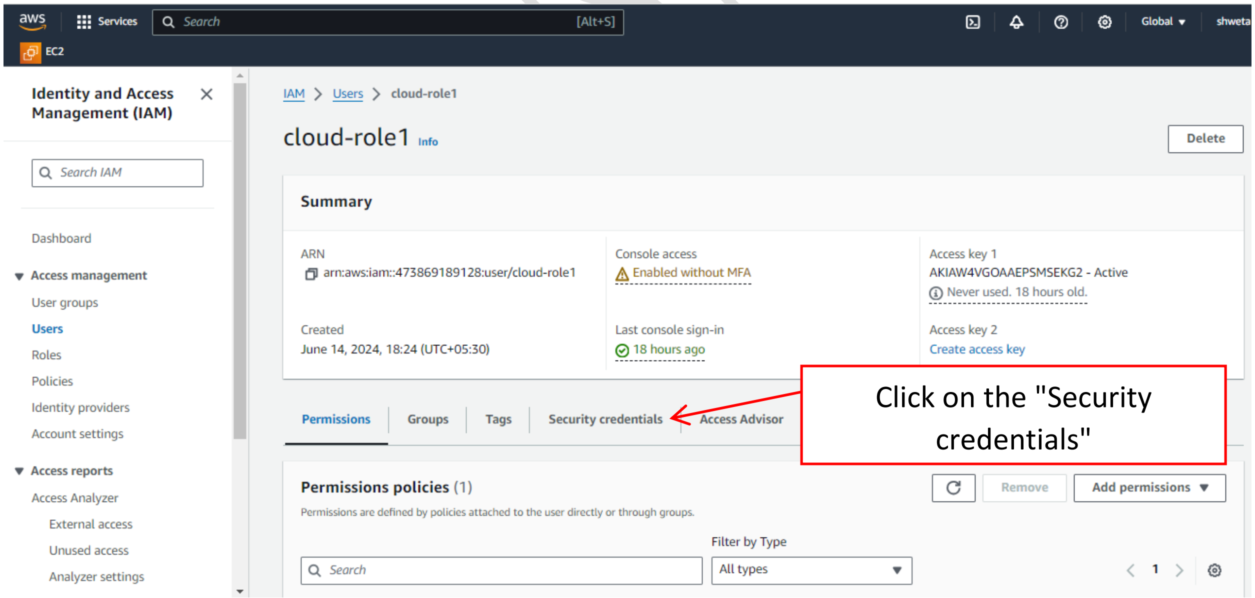


Select the IAM user to whom you want to add MFA

Users (1) Info

An IAM user is an identity with long-term credentials that is used

User name	Path	Group:	Last activity	MFA	Password age	Console last sign-i
cloud-role1	/	0	18 hours ago	-	18 hours	June 14, 2024, 18:



cloud-role1 Info

Summary

ARN
arn:aws:iam::473869189128:user/cloud-role1

Console access
Enabled without MFA

Access key 1
AKIAW4VGOAAEPSMSEKG2 - Active
Never used. 18 hours old.

Created
June 14, 2024, 18:24 (UTC+05:30)

Last console sign-in
18 hours ago

Access key 2
Create access key

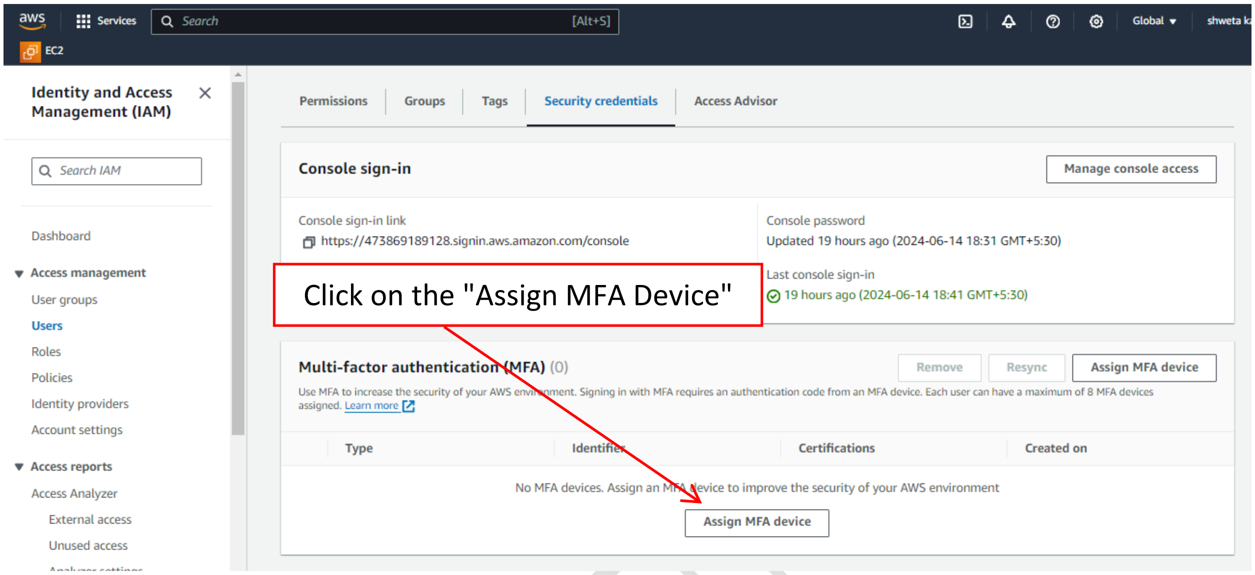
Click on the "Security credentials"

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type
All types

Scroll down to the "Multi-Factor Authentication (MFA)" section and click on the "Assign MFA Device".



Identity and Access Management (IAM)

Search IAM

Dashboard

▾ Access management
- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

▾ Access reports
- Access Analyzer
  - External access
  - Unused access
  - Analyzer settings

Permissions | Groups | Tags | Security credentials | Access Advisor

Console sign-in — Manage console access

Console sign-in link
https://473869189128.signin.aws.amazon.com/console

Console password
Updated 19 hours ago (2024-06-14 18:31 GMT+5:30)

Last console sign-in
✓ 19 hours ago (2024-06-14 18:41 GMT+5:30)

Click on the "Assign MFA Device"

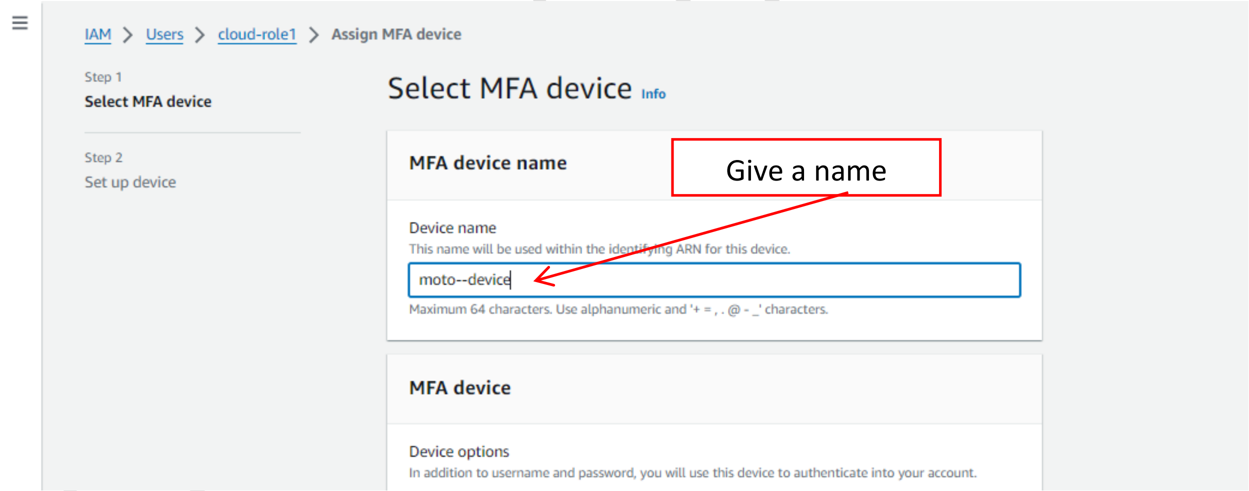
Multi-factor authentication (MFA) (0) — Remove | Resync | Assign MFA device

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


IAM > Users > cloud-role1 > Assign MFA device

Step 1
Select MFA device

Step 2
Set up device

Select MFA device Info

MFA device name

Give a name

Device name
This name will be used within the identifying ARN for this device.
moto--device
Maximum 64 characters. Use alphanumeric and '+ = , . @ - _' characters.

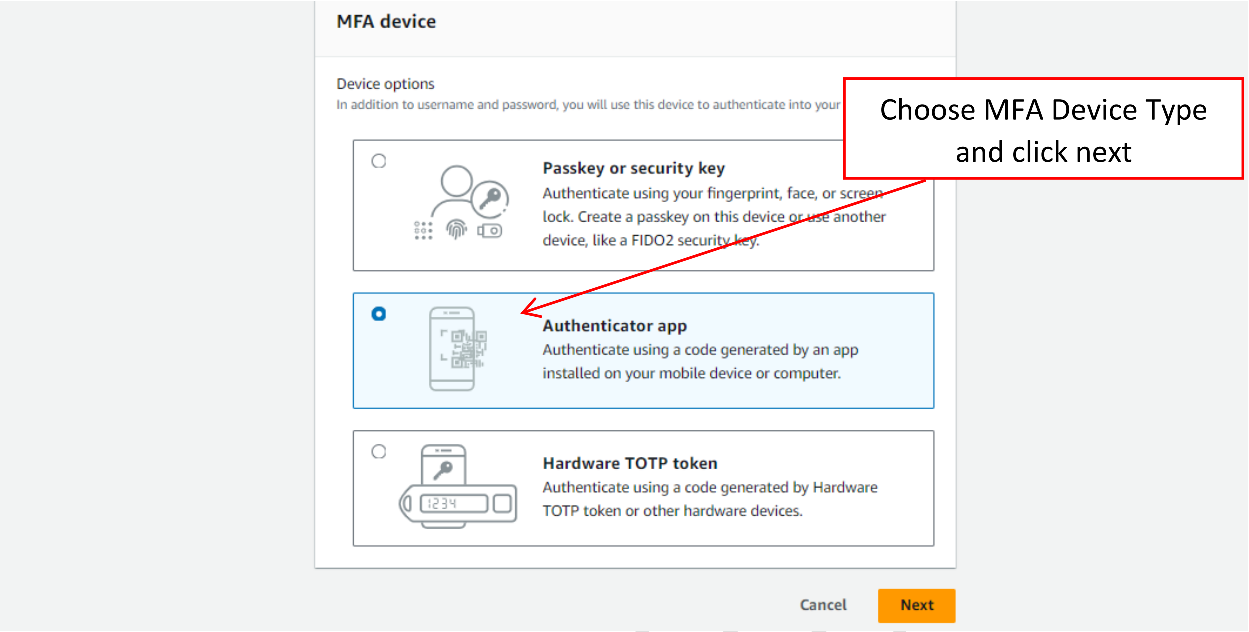
MFA device

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

Choose MFA Device Type:

You have several options for MFA devices, including Virtual MFA device (software-based like Google Authenticator), U2F security key, and Hardware MFA device.

For this example, we will use a Google Authenticator.



MFA device

Device options

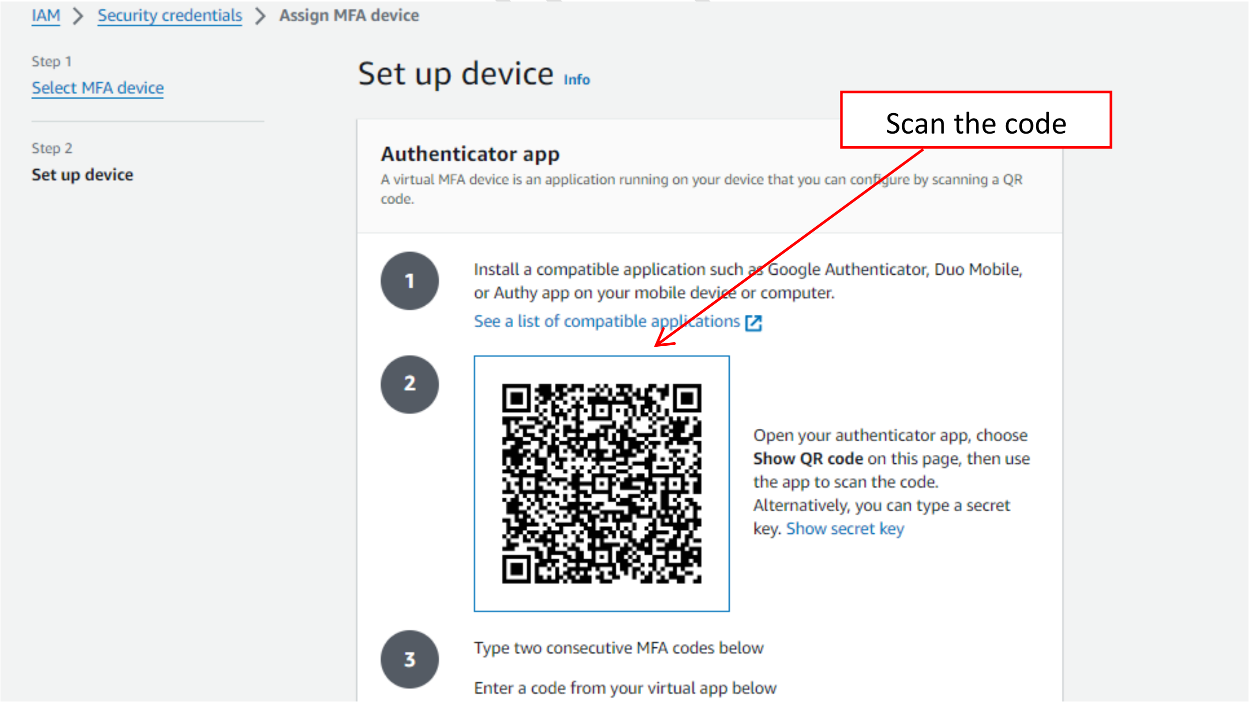
In addition to username and password, you will use this device to authenticate into your

○ **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.

Choose MFA Device Type and click next



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

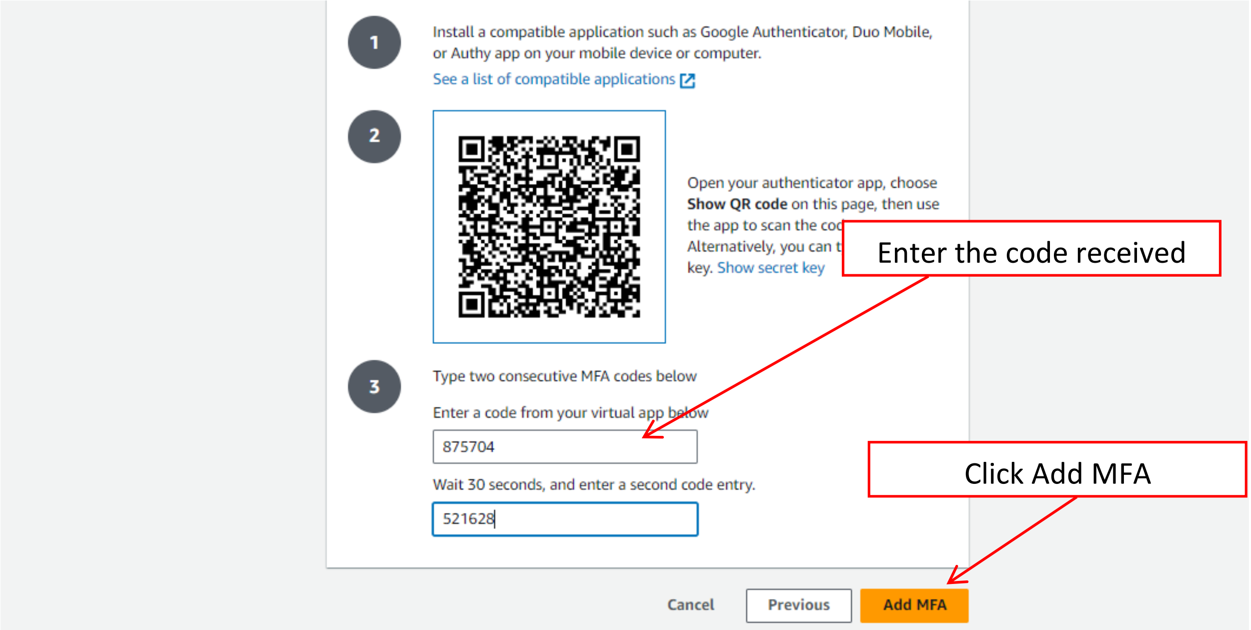
3 Type two consecutive MFA codes below

Enter a code from your virtual app below

Scan the code

If you're using a Virtual MFA device, you will need to scan the QR code with your MFA application (such as Google Authenticator) or manually enter the secret key provided by AWS into your MFA application.

The application will generate a six-digit authentication 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 cod… Alternatively, you can t… key. Show secret key

3 Type two consecutive MFA codes below

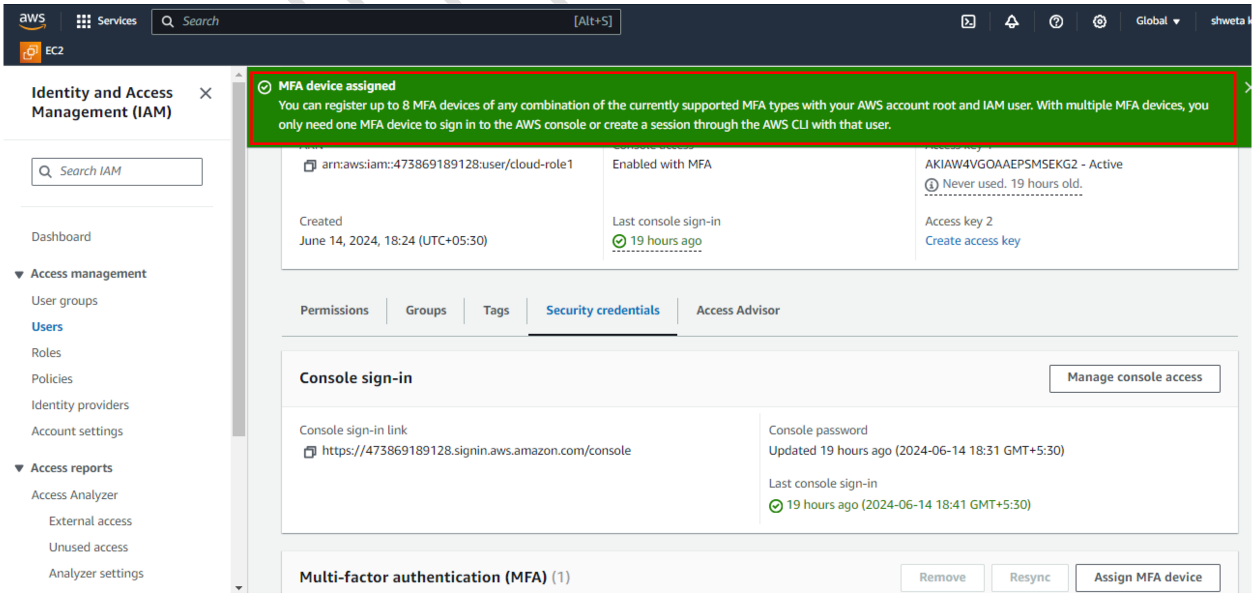
Enter a code from your virtual app below: 875704

Wait 30 seconds, and enter a second code entry: 521628

Enter the code received

Click Add MFA

If the codes are correct, the MFA device will be successfully assigned to the IAM user.



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.

arn:aws:iam::473869189128:user/cloud-role1

Enabled with MFA

AKIAW4VGOAAEPSMSEKG2 - Active
Never used. 19 hours old.

Created
June 14, 2024, 18:24 (UTC+05:30)

Last console sign-in
19 hours ago

Access key 2
Create access key

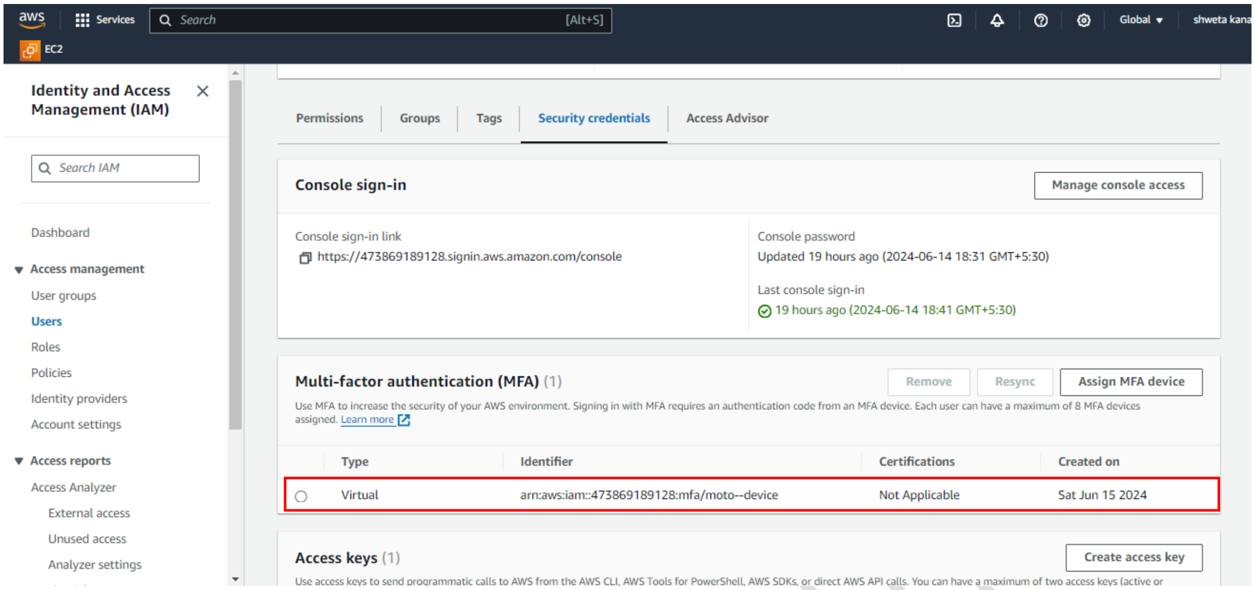
Console sign-in

Console sign-in link
https://473869189128.signin.aws.amazon.com/console

Console password
Updated 19 hours ago (2024-06-14 18:31 GMT+5:30)

Last console sign-in
19 hours ago (2024-06-14 18:41 GMT+5:30)

Multi-factor authentication (MFA) (1)



Identity and Access Management (IAM)

Search IAM

Dashboard

Access management
- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports
- Access Analyzer
  - External access
  - Unused access
  - Analyzer settings

Permissions | Groups | Tags | Security credentials | Access Advisor

Console sign-in — Manage console access

Console sign-in link
https://473869189128.signin.aws.amazon.com/console

Console password
Updated 19 hours ago (2024-06-14 18:31 GMT+5:30)

Last console sign-in
19 hours ago (2024-06-14 18:41 GMT+5:30)

Multi-factor authentication (MFA) (1) — Remove | Resync | Assign MFA device

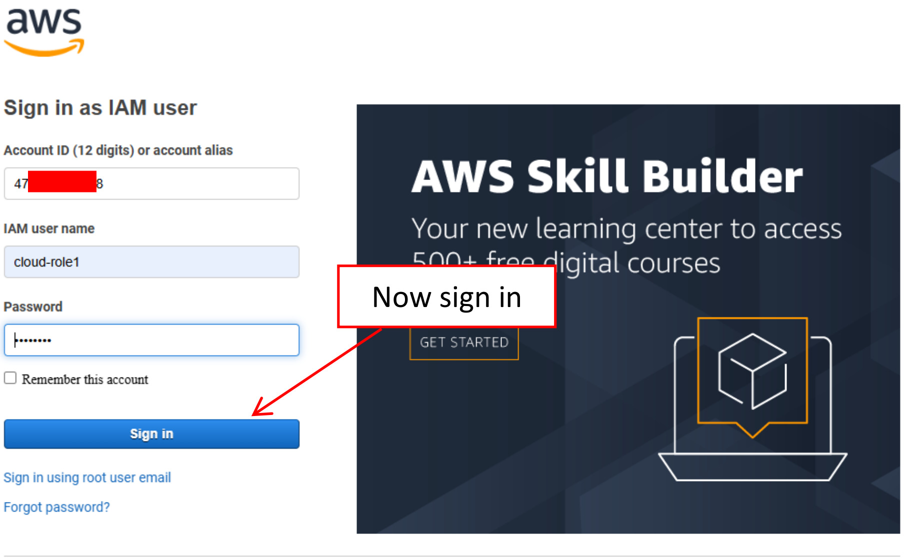
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

	Type	Identifier	Certifications	Created on
○	Virtual	arn:aws:iam::473869189128:mfa/moto--device	Not Applicable	Sat Jun 15 2024

Access keys (1) — 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

Now login to the IAM user



aws

Sign in as IAM user

Account ID (12 digits) or account alias
47[redacted]8

IAM user name
cloud-role1

Password
••••••••

□ Remember this account

Sign in

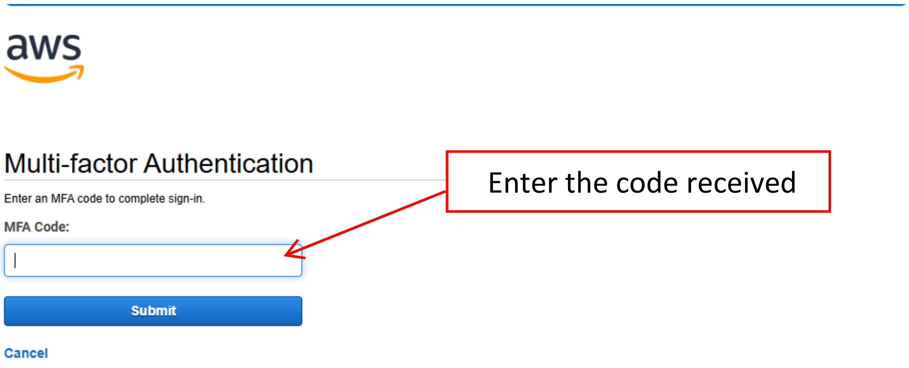
Sign in using root user email

Forgot password?

Now sign in

AWS Skill Builder
Your new learning center to access 500+ free digital courses
GET STARTED

Now, the IAM user will be required to use MFA when signing in to the AWS Management Console or when making certain API calls.



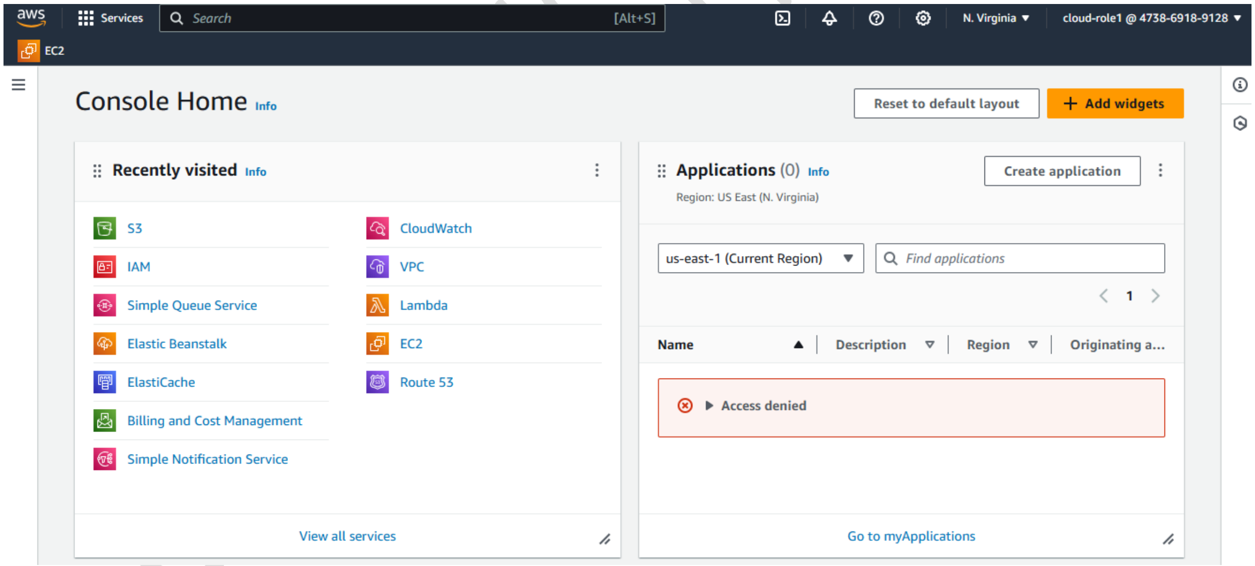
Multi-factor Authentication

Enter an MFA code to complete sign-in.

MFA Code:

Enter the code received

Successfully logged into the IAM user



aws
Services
Search
[Alt+S]
N. Virginia
cloud-role1 @ 4738-6918-9128
EC2
Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
S3
IAM
Simple Queue Service
Elastic Beanstalk
ElastiCache
Billing and Cost Management
Simple Notification Service
CloudWatch
VPC
Lambda
EC2
Route 53
View all services
Applications (0) Info
Region: US East (N. Virginia)
Create application
us-east-1 (Current Region)
Find applications
1
Name
Description
Region
Originating a...
Access denied
Go to myApplications