Assignment:1

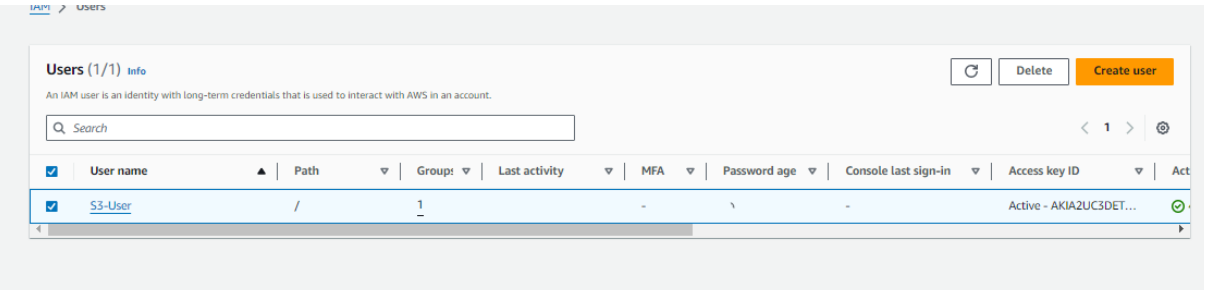
Task:4

Enable Multi-Factor Authentication (MFA) for "S3-User":

Step:1 Access AWS management console.

Step2: Navigate to IAM.

Step3: Select the user.

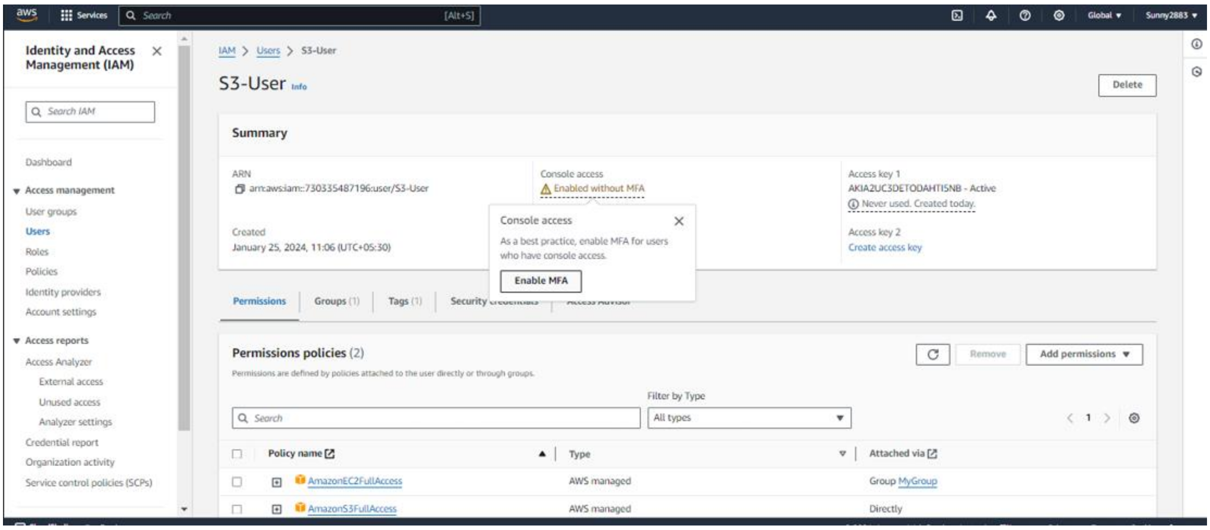


Users (1/1) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

☑	User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID	Act
☑	S3-User	/	1		-	`	-	Active - AKIA2UC3DET...	✓

Step4: In console access select enable MFA.



S3-User Info

Summary

ARN: arn:aws:iam::730335487196:user/S3-User

Created: January 25, 2024, 11:06 (UTC+05:30)

Console access: ⚠ Enabled without MFA

Access key 1: AKIA2UC3DETODAHTI5NB - Active

Never used. Created today.

Access key 2: Create access key

Console access

As a best practice, enable MFA for users who have console access.

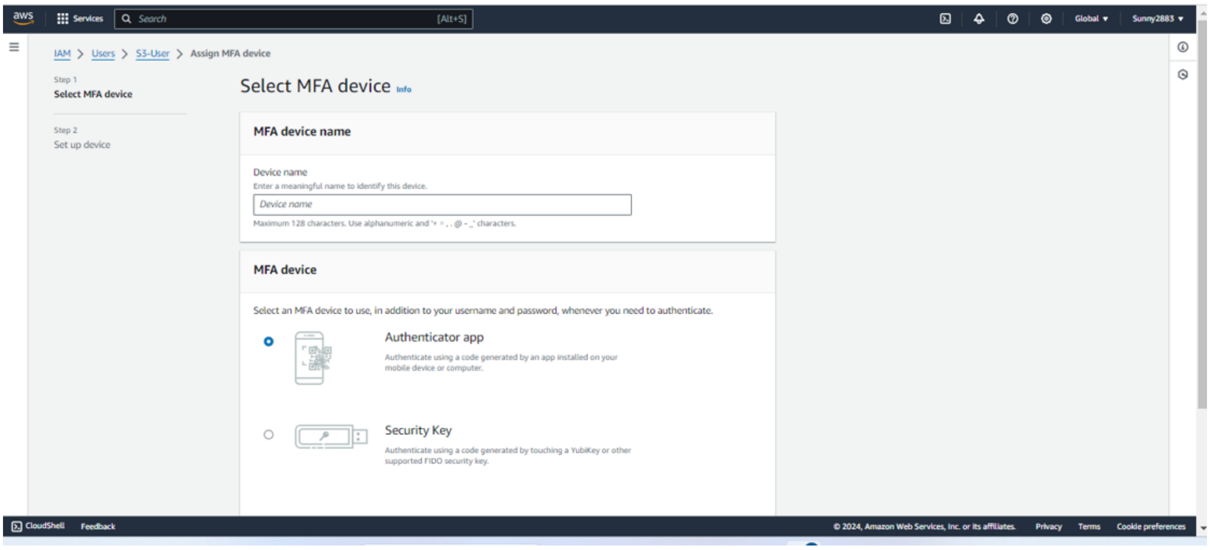
Permissions policies (2)

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

☐	Policy name	Type	Attached via
☐	AmazonEC2FullAccess	AWS managed	Group MyGroup
☐	AmazonS3FullAccess	AWS managed	Directly

Step5: Add MFA device.

Enter Device name and select the type of MFA device.



IAM > Users > S3-User > Assign MFA device

Step 1
Select MFA device

Step 2
Set up device

Select MFA device Info

MFA device name

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

MFA device

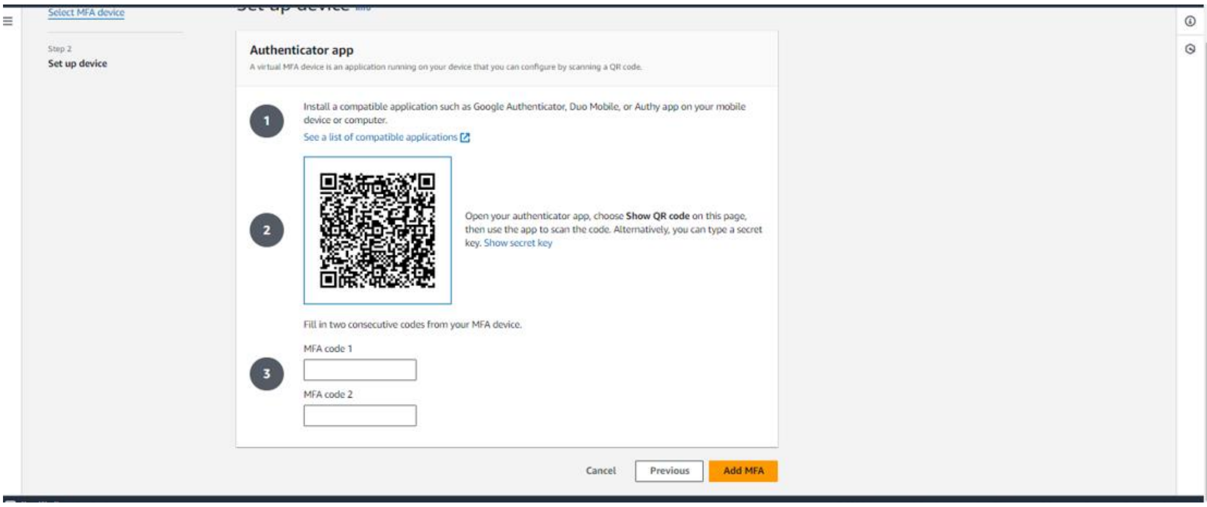
Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.

● 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.

Step6: Follow the setup Wizard.

We need to scan a QR code or enter a secret key into an authenticator app.



Select MFA device

Step 2
Set up device

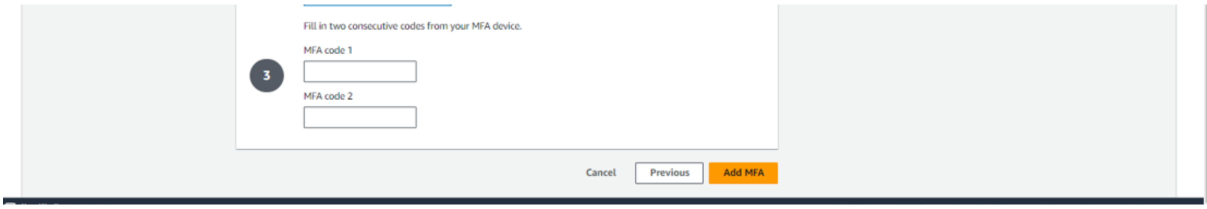
Authenticator app
A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

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

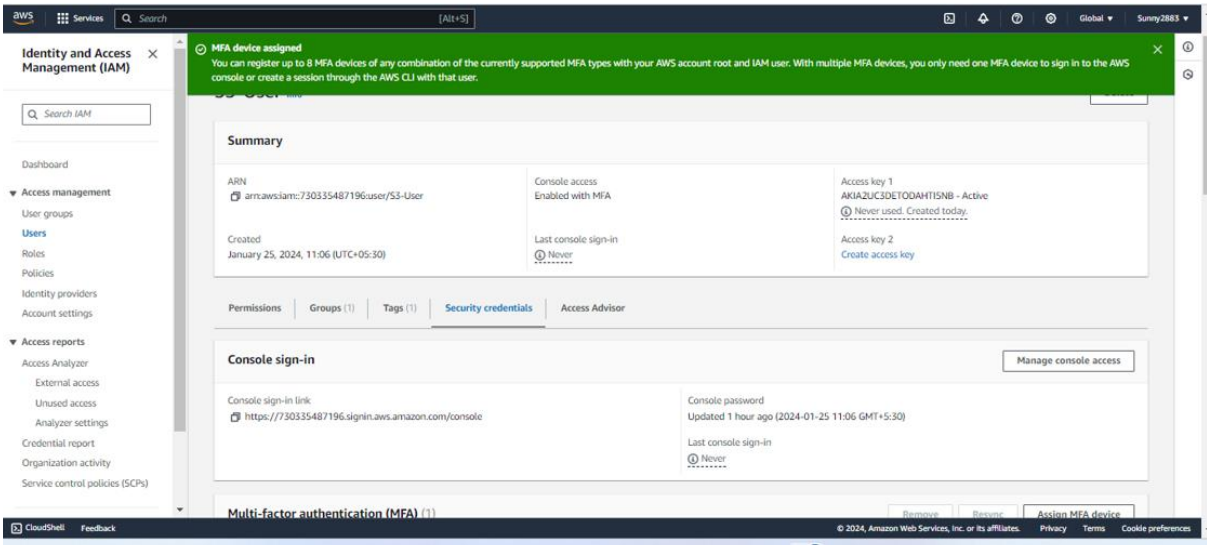
3 Fill in two consecutive codes from your MFA device.
MFA code 1
MFA code 2

Step7: After setting up the MFA device we need to enter the code generated by the device and click on add MFA.



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

Step8: MFA device assigned successfully.



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.

Summary

ARN
arn:aws:iam::730335487196:user/S3-User

Console access
Enabled with MFA

Access key 1
AKIA2UC3DETODAHTI5NB - Active
Never used. Created today.

Created
January 25, 2024, 11:06 (UTC+05:30)

Last console sign-in
Never

Access key 2
Create access key

Console sign-in

Console sign-in link
https://730335487196.signin.aws.amazon.com/console

Console password
Updated 1 hour ago (2024-01-25 11:06 GMT+5:30)

Last console sign-in
Never

Multi-factor authentication (MFA) (1)