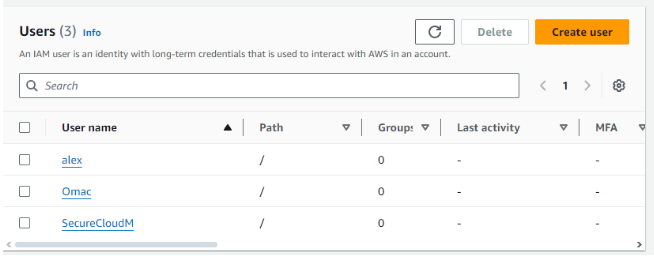
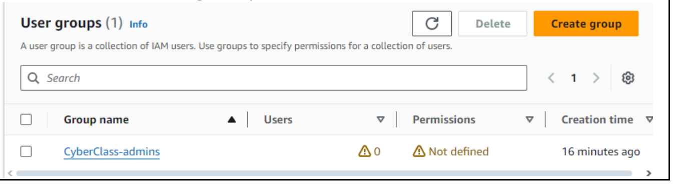
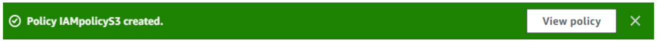
Lab Logbook Week 4

Student ID GAR22521797 Date------------------------------------

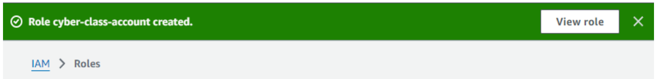
Briefly introduce the aim of this lab	The aim of this lab was to explore AWS IAM by configuring users, roles, policies, and multi-factor authentication to secure cloud resources.
Identify the tools used for each task and why it was required.	S3 Bucket - provides storage with encryption and access controls it is required to secure data in the cloud IAM Services – allows secure management of user and role permissions Google authenticator – to set up the multi factor authentication
What are your observations from each task?	For activity 1, I had to create several users named Omac and SecureCloudM as IAM accounts with their own respective passwords. I also had to create a new user group named CyberClass-admins. After this I had to go to the policies section in IAM console and create a new policy through JSON and review it and create it. For activity 2, I created a new role with the right configuration and the addition of a new policy "AmazonS3ReadOnlyAccess". For activity 3, I selected the user "alex" and went to the security credentials tab when clicking on the user to assign MFA device. I then selected the authenticator app and used google authentication to provide 2 codes to set up the MFA. I then tested to see whether it was working by logging in with the user IAM ID etc and it asked me for an MFA code. For exercise 1, I created a new role with policies "amazons3readonlyaccess" and named the role "CrossAccountReadAccess". I then created a new policy and defined the permissions in JSON format.
Report your lab experimental result for each task	I created the users Omac. SecureCloud  Users (3) Info An IAM user is an identity with long-term credentials that is used to interact with AWS in an account. □ User name · Path · Group: · Last activity · MFA □ alex · / · 0 · - · - □ Omac · / · 0 · - · - □ SecureCloudM · / · 0 · - · - I created a user group.  User groups (1) Info A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. □ Group name · Users · Permissions · Creation time □ CyberClass-admins · ⚠ 0 · ⚠ Not defined · 16 minutes ago

I created a policy and gave it a name.



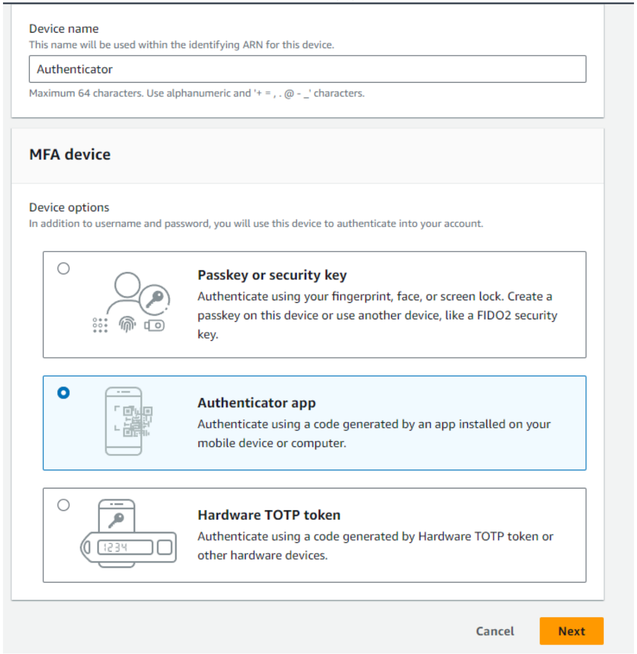
Policy IAMpolicyS3 created.

New role creation “cyber-class-account"



Role cyber-class-account created.

Selection of authenticator app



Device name

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

Authenticator

Maximum 64 characters. Use alphanumeric and '+ = , . @ - _' characters.

MFA device

Device options

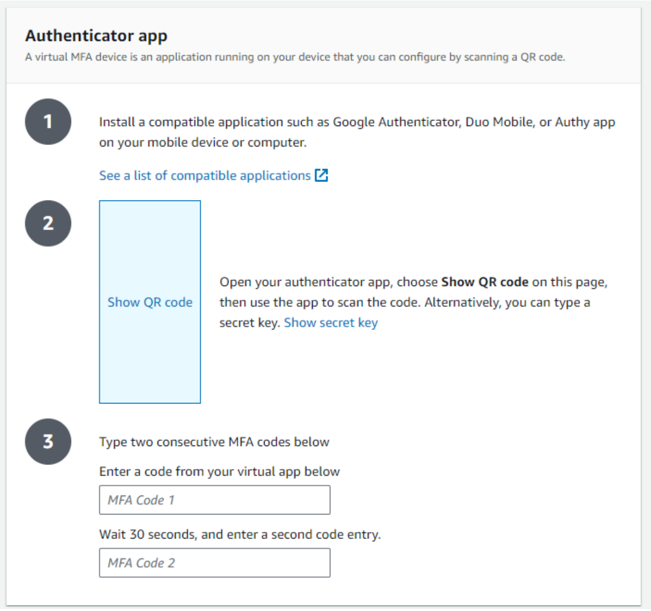
In addition to username and password, you will use this device to authenticate into your account.

○ **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.

Followed the steps



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

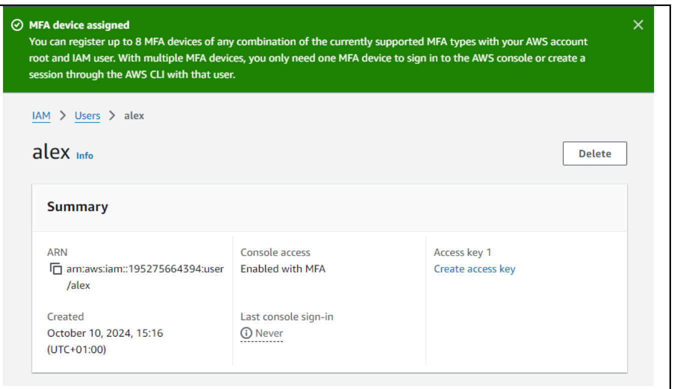
Enter a code from your virtual app below

MFA Code 1

Wait 30 seconds, and enter a second code entry.

MFA Code 2

Successful MFA set up using google authenticator



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::195275664394:user/alex

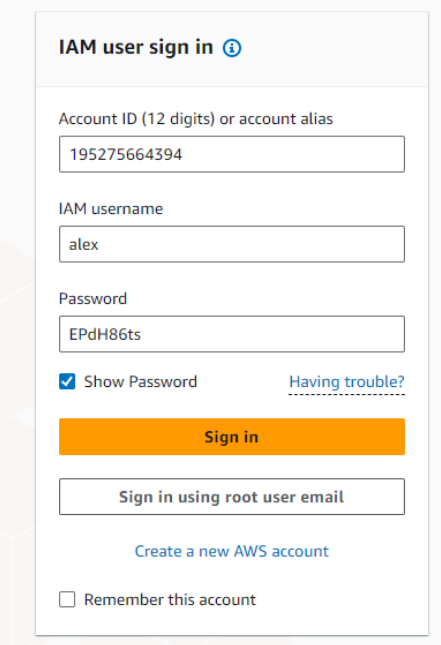
Console access: Enabled with MFA

Access key 1: Create access key

Created: October 10, 2024, 15:16 (UTC+01:00)

Last console sign-in: Never

Logging credentials for IAM user ”alex”



IAM user sign in

Account ID (12 digits) or account alias: 195275664394

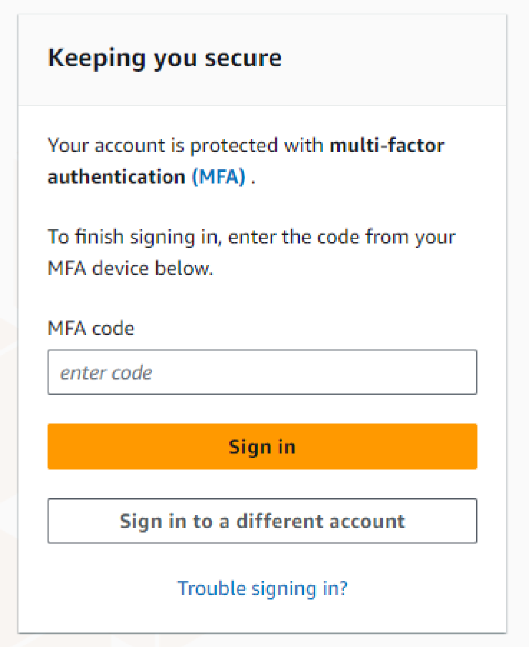
IAM username: alex

Password: EPdH86ts

☑ Show Password

☐ Remember this account

Successful MFA Integration

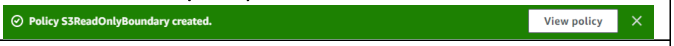


Keeping you secure

Your account is protected with **multi-factor authentication (MFA)** .

To finish signing in, enter the code from your MFA device below.

MFA code: *enter code*

	Exercise 1 new policy creation  Policy S3ReadOnlyBoundary created.
What was your takeaway from the tasks	I learnt how to manage user permissions effectively by setting the right policies and adding multi factor authentication as an extra layer of security for IAM users.