

Identity and Access Management (IAM) on AWS

Lab Report

Network Security · Lab Task

Prepared by:
Rabya Hassan

1. Objective

To learn how to create IAM users and groups in AWS and assign permissions using policies. To implement secure access control using the principle of least privilege and Multi-Factor Authentication (MFA).

1. Create and manage IAM users and groups in AWS.
2. Assign permissions to groups using IAM policies.
3. Enable MFA to strengthen user account security.
4. Configure and test a custom password policy.

2. Introduction

AWS Identity and Access Management (IAM) is a foundational security service that enables fine-grained control over who can access AWS resources and what actions they can perform. IAM uses users, groups, roles, and policies to implement the principle of least privilege — ensuring that each entity has only the minimum permissions required to do its job.

3. Tools Used

- AWS Management Console — web-based interface for managing AWS services
- AWS IAM Service — Identity and Access Management
- Google Authenticator / Authy — MFA authentication app

4. Procedure

5. Log in to the AWS Management Console.
6. Navigate to IAM and create user groups (Students-Group, Teachers-Group).
7. Attach appropriate permission policies to each group.
8. Create IAM users and assign them to the relevant groups.
9. Enable MFA for each user account.
10. Configure a custom password policy for the account.
11. Test and verify that permissions are correctly applied.

5. Lab Tasks & Results

Task 01 Login to AWS & Open IAM

Logged in to the AWS Management Console and navigated to the IAM service via the search bar.

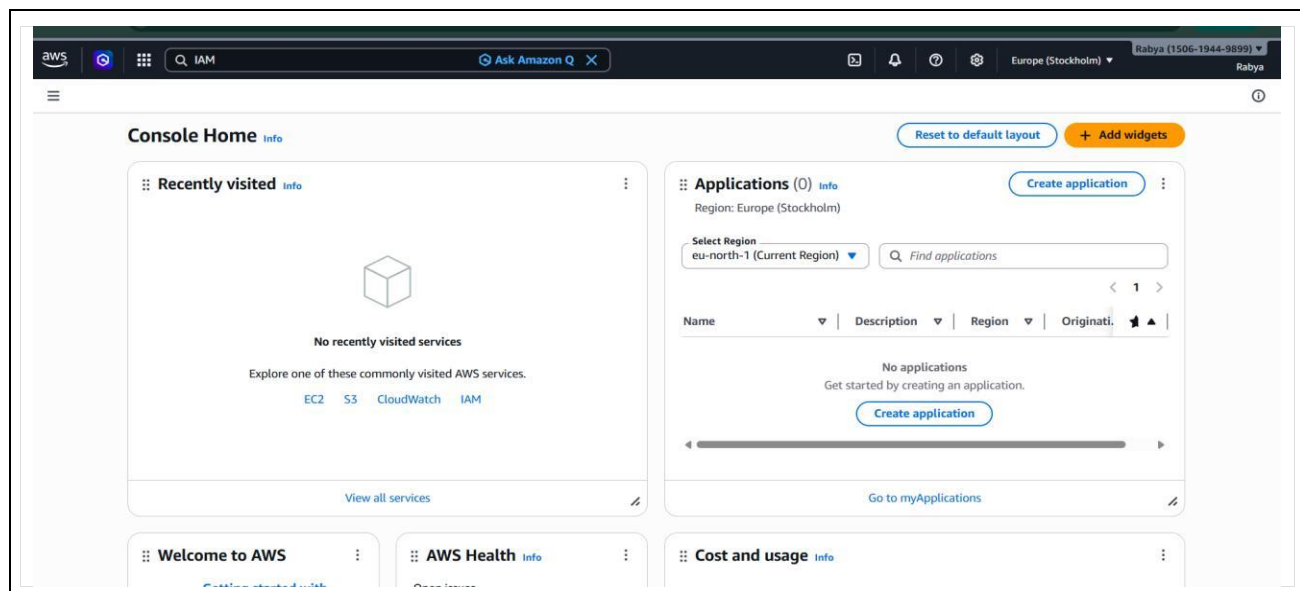


Figure 1 — AWS Console Home after login

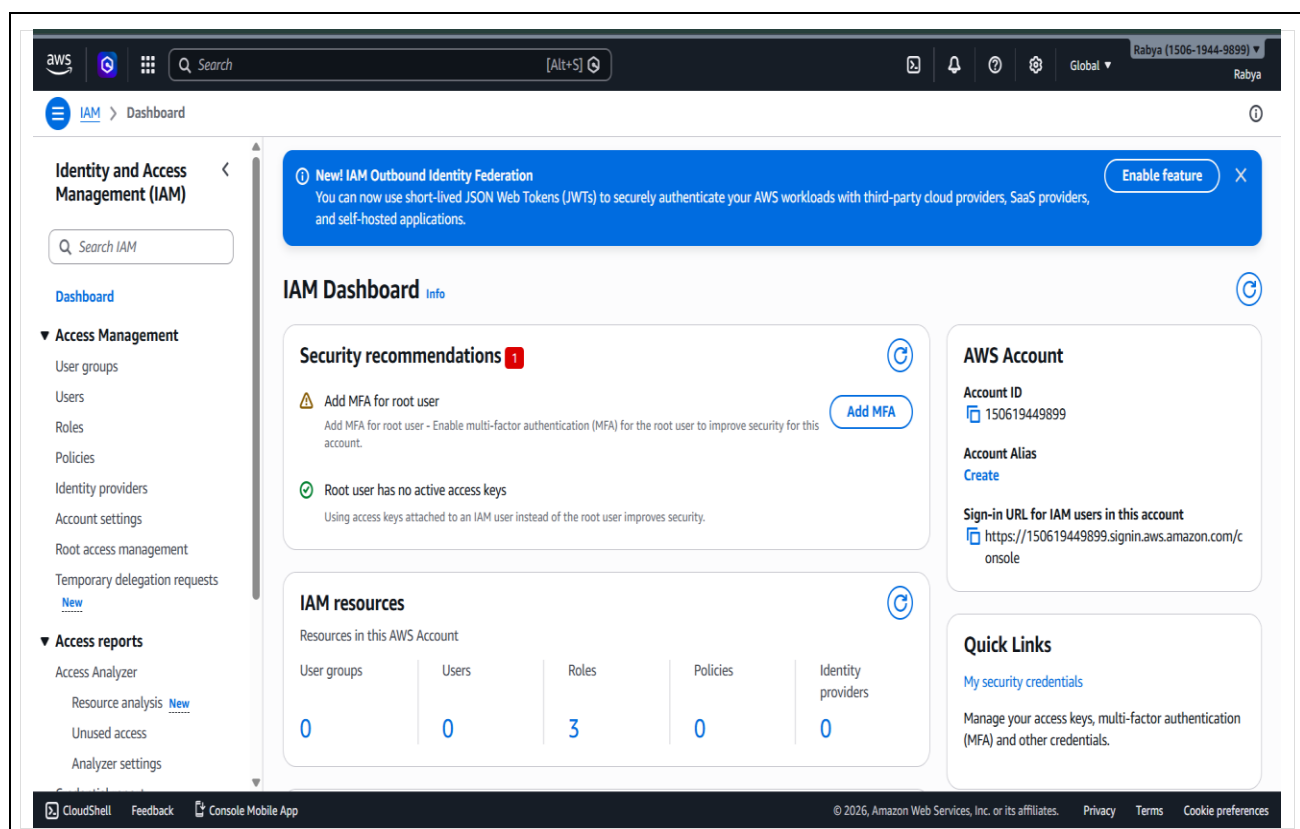


Figure 2 — IAM Dashboard showing 0 users and 0 groups initially

Task 02 Create User Groups

Two IAM user groups were created: Students-Group (with read-only permissions) and Teachers-Group (with full-access permissions). Groups allow permissions to be managed centrally for multiple users.

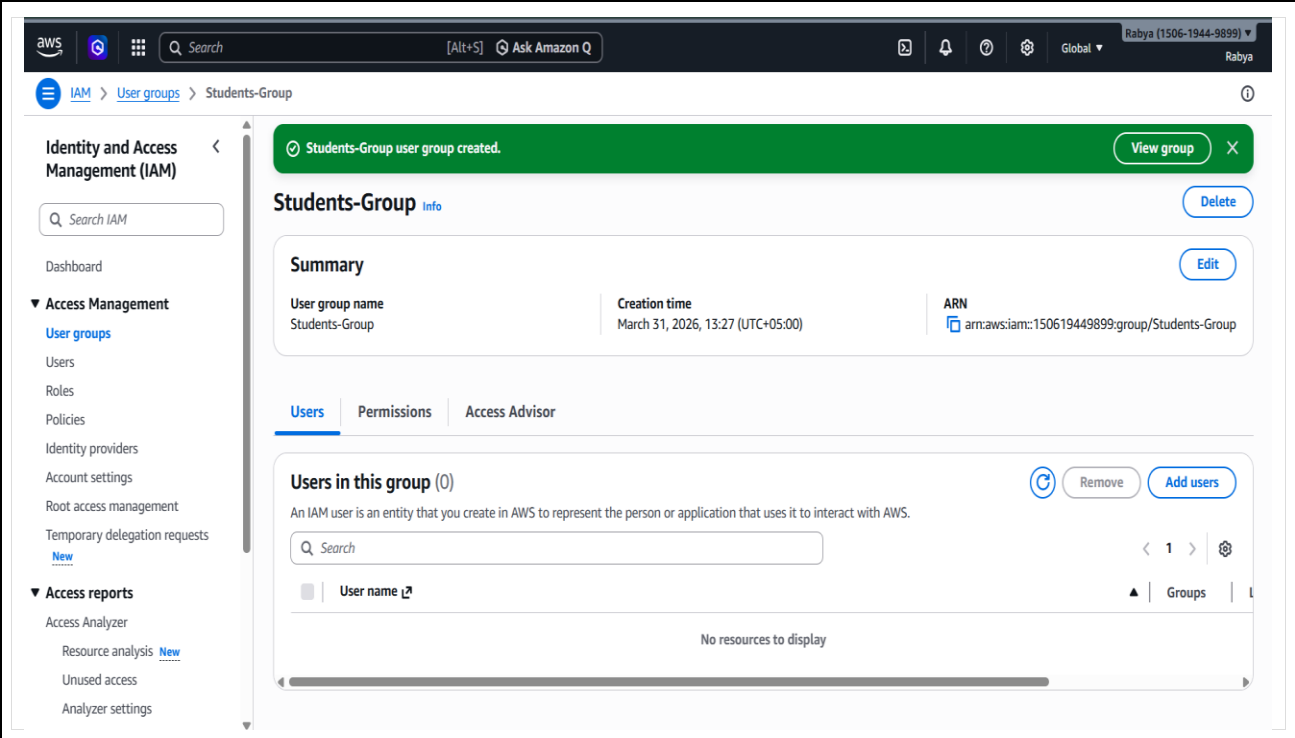


Figure 3 — Students-Group created successfully

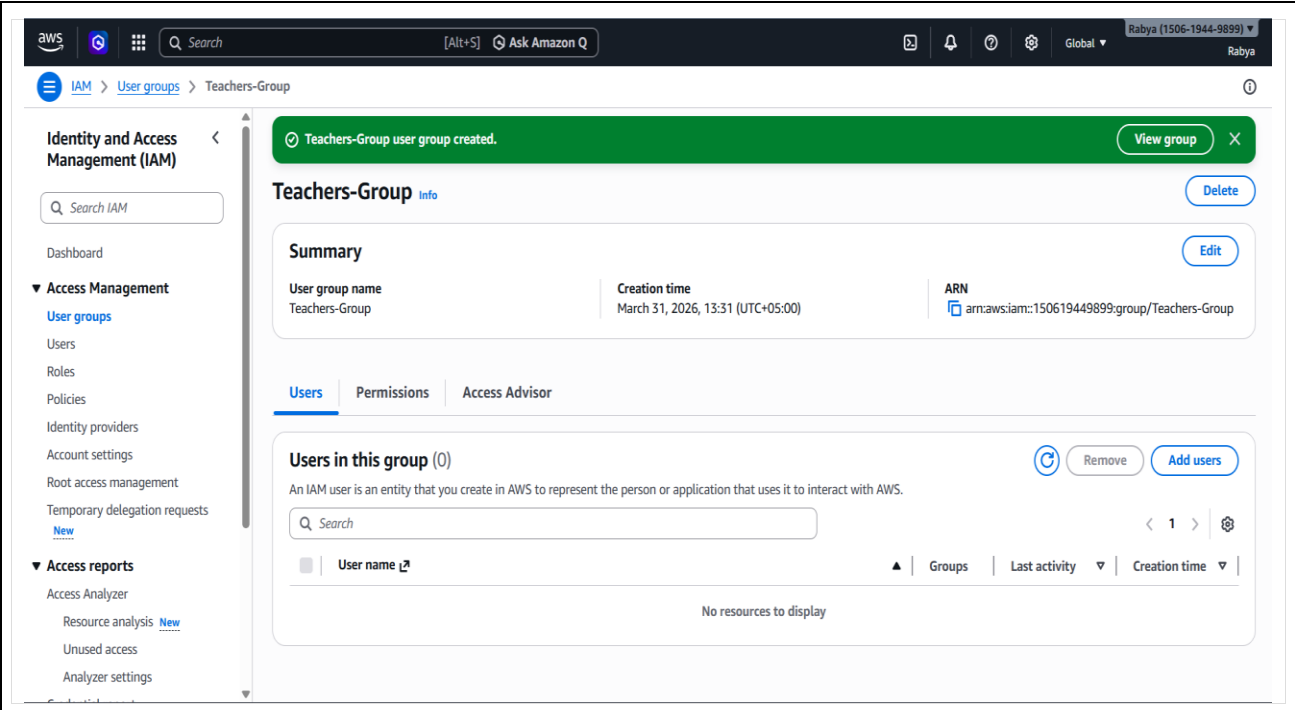


Figure 4 — Teachers-Group created successfully

Task 03 Attach Permissions Policies

Read-only policies were attached to the Students-Group, limiting access to viewing resources only. Full-access policies were attached to the Teachers-Group, granting broader administrative permissions.

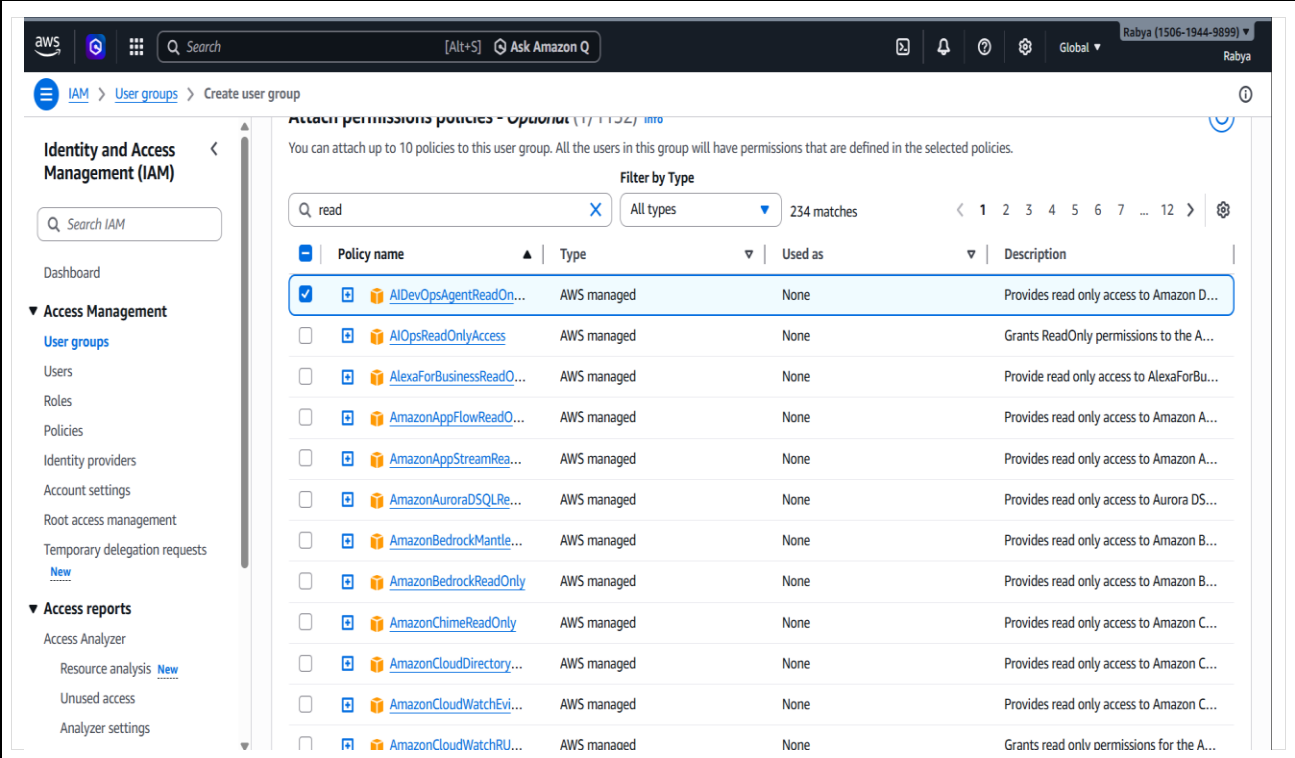


Figure 5 — Attaching read-only policies to Students-Group

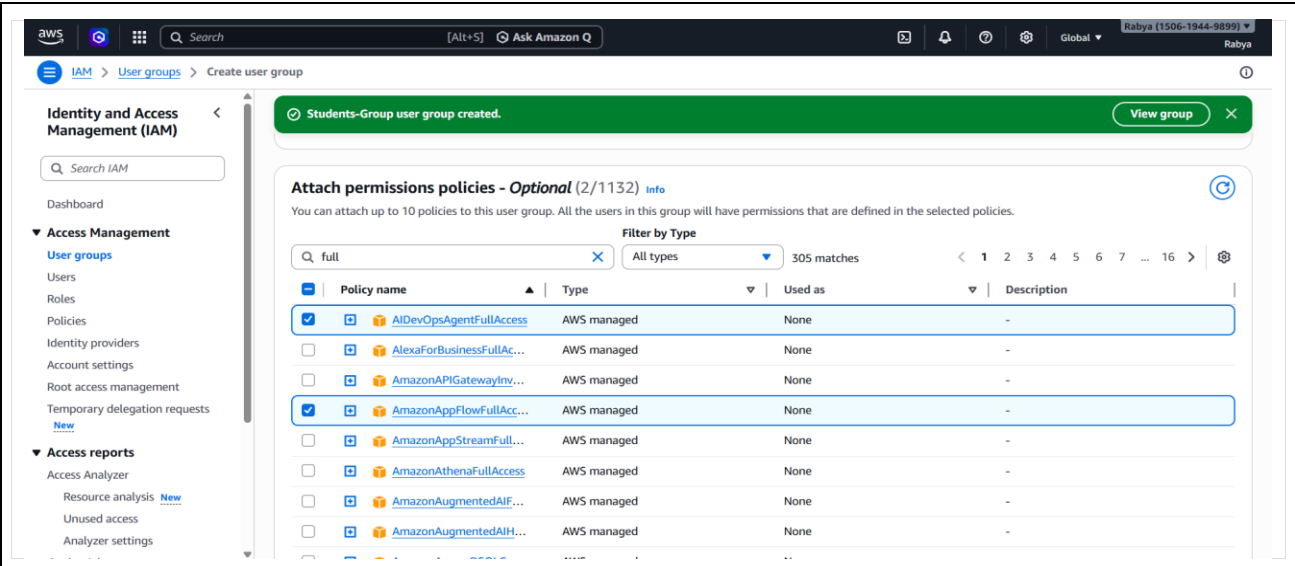


Figure 6 — Attaching full-access policies to Students-Group (FullAccess policies selected)

Task 04 Create IAM Users

IAM user Student1 was created and added to the Students-Group. A second user assistant1 was created and added to the Teachers-Group. Both users were given console access with auto-generated passwords.

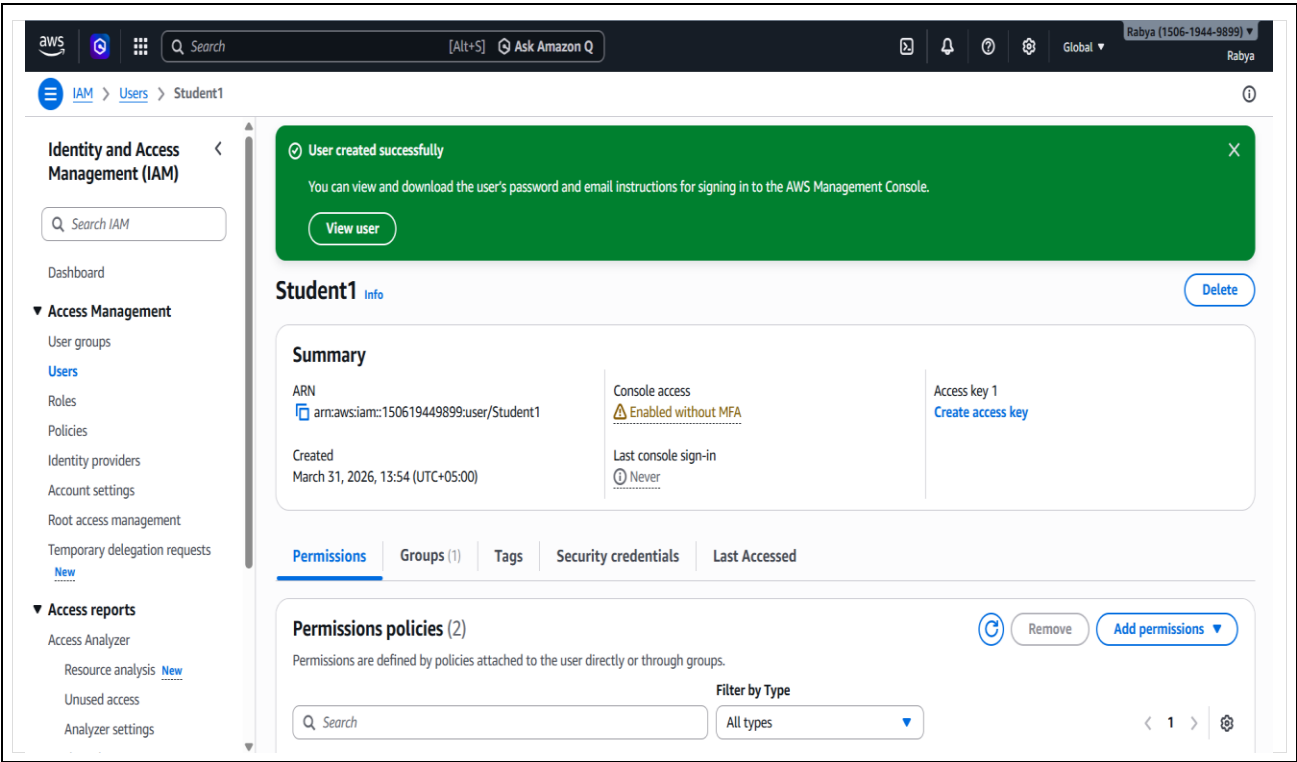


Figure 7 — Student1 user created successfully and assigned to Students-Group

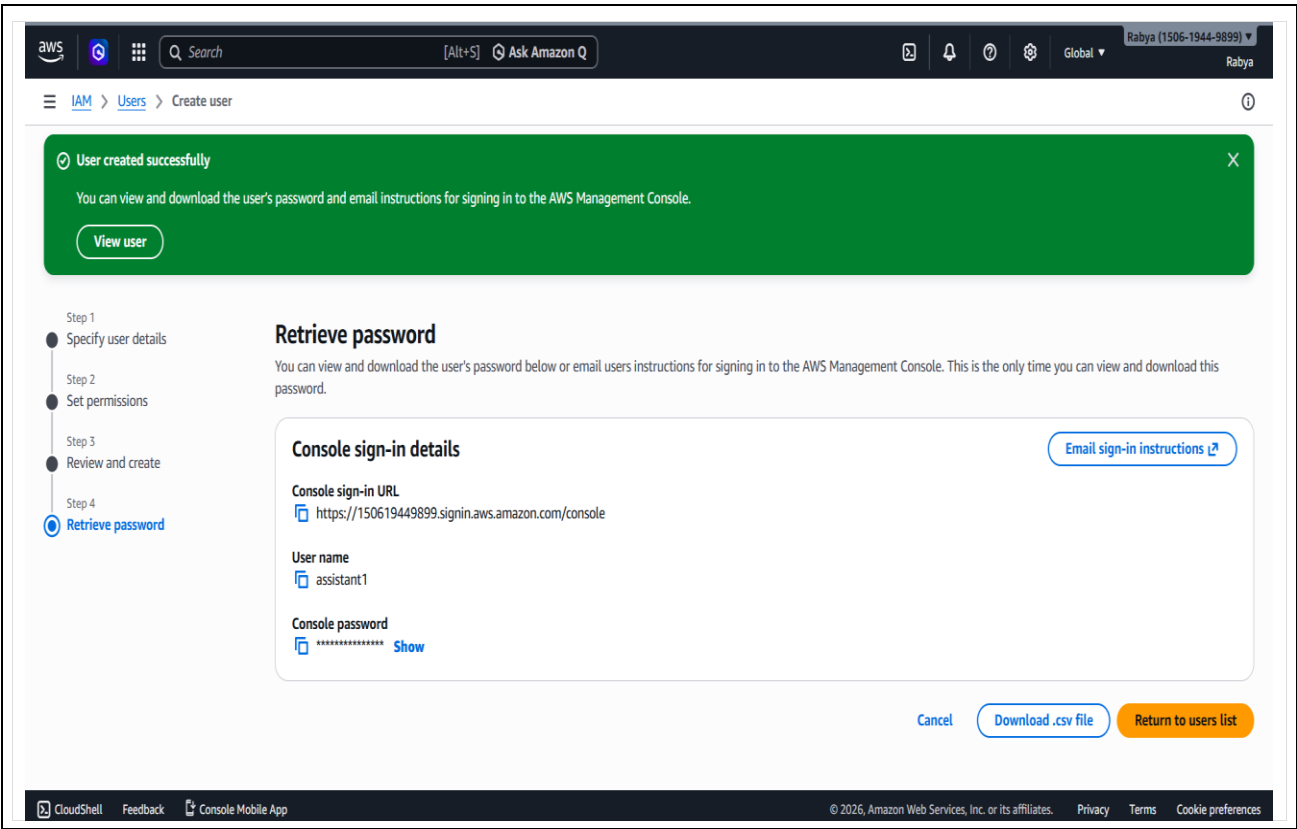


Figure 8 — Console sign-in credentials retrieved for user assistant1

Task 06 Enable Multi-Factor Authentication (MFA)

MFA was enabled for both Student1 and assistant1 using an authenticator app. Once enabled, users must provide a time-based one-time password (TOTP) in addition to their password at sign-in.

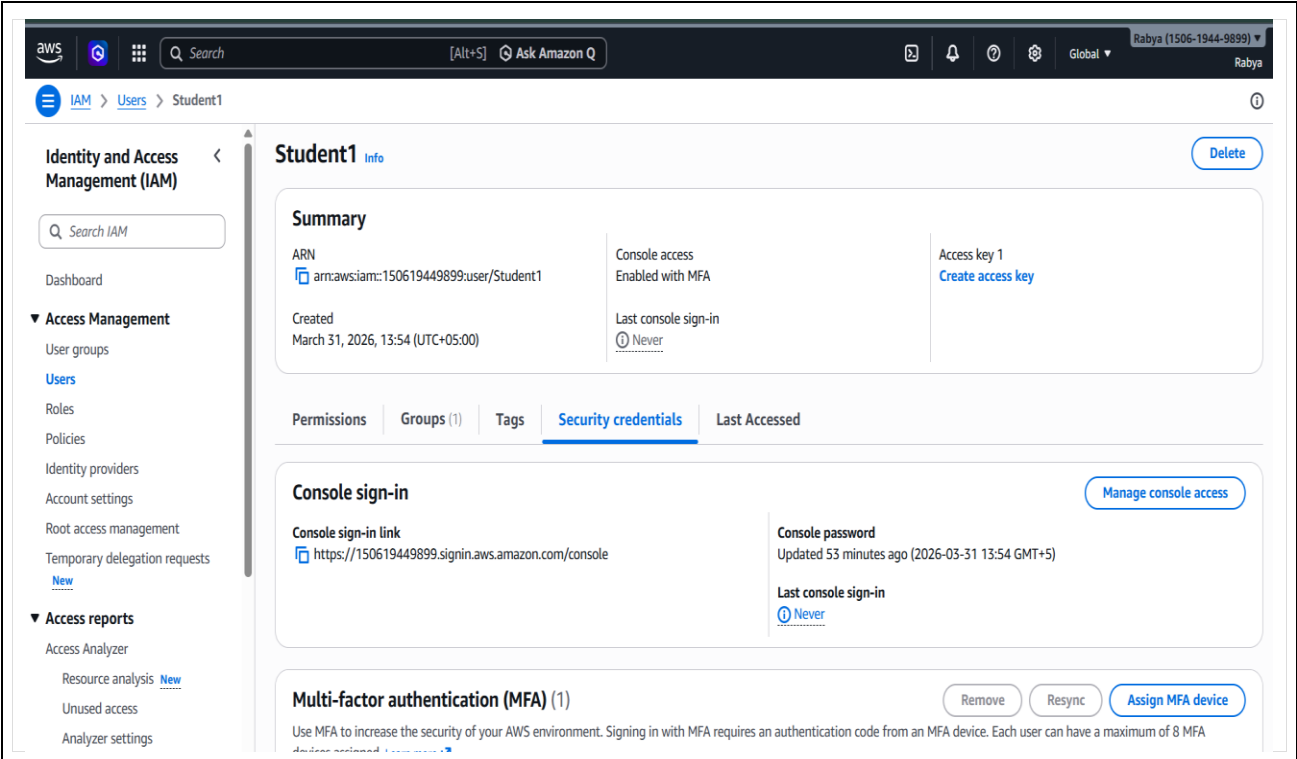


Figure 9 — Student1 showing Console access: Enabled with MFA

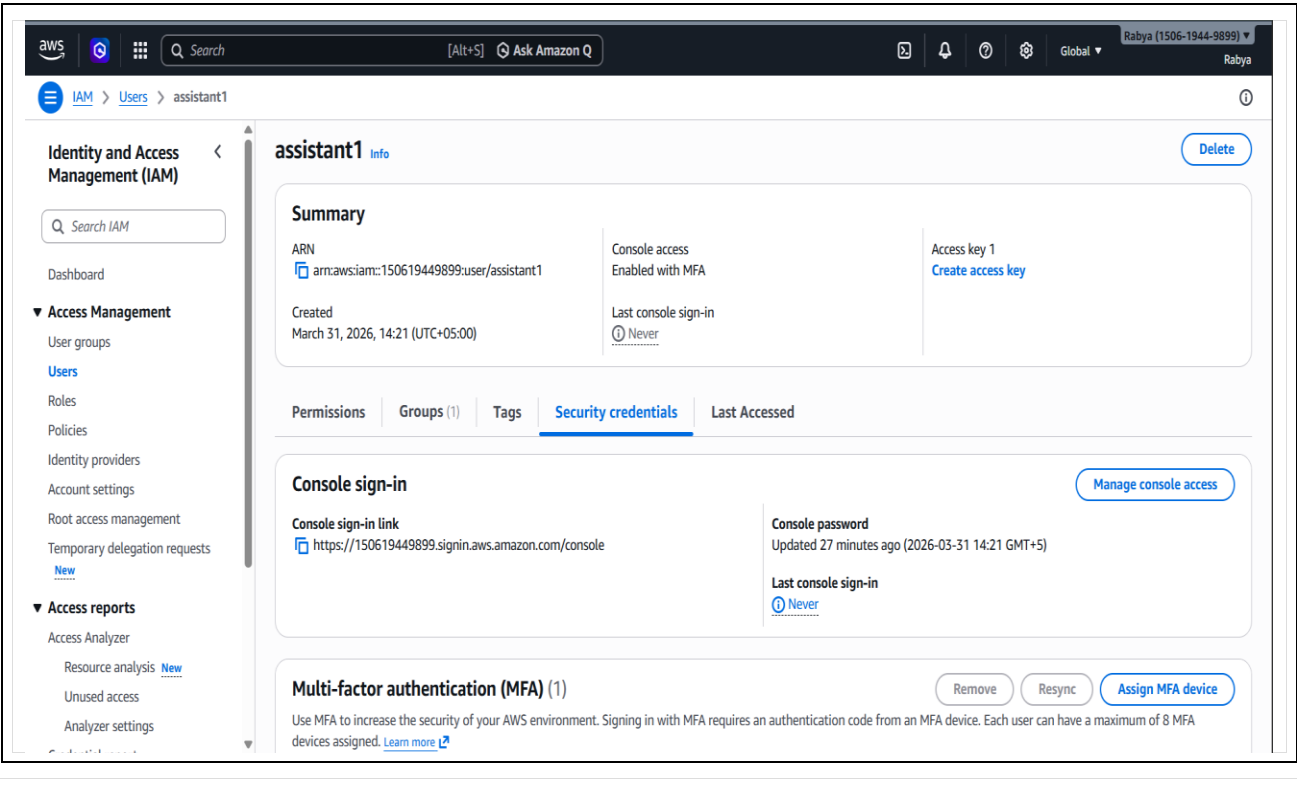


Figure 10 — assistant1 showing Console access: Enabled with MFA

Task 07 Configure Password Policy

A custom password policy was configured for the AWS account. The policy enforces a minimum length of 8 characters, requires at least one uppercase letter, and enables password expiration to ensure regular credential rotation.

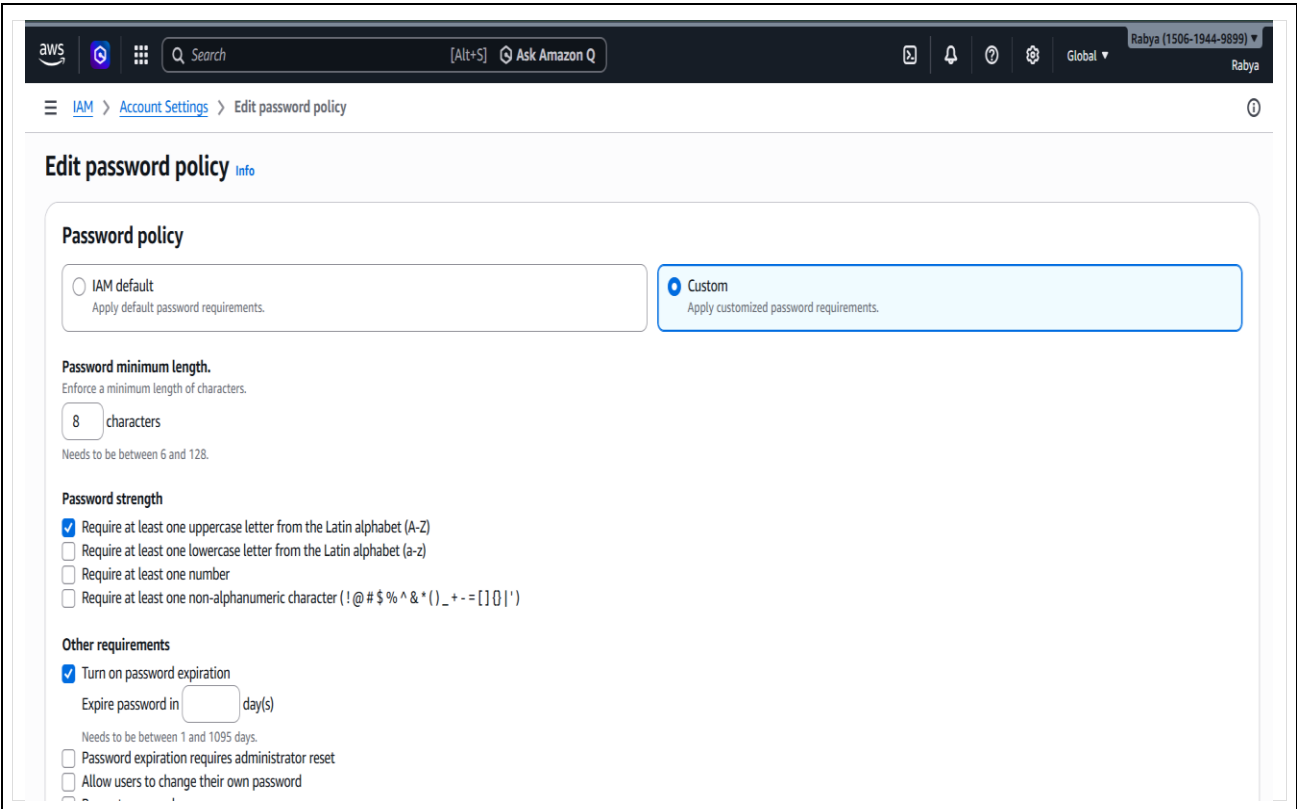


Figure 11 — Custom password policy configured with 8-character minimum and expiration enabled

6. What is IAM Used For?

AWS IAM (Identity and Access Management) is the primary mechanism for controlling access to AWS resources. Key use cases include:

- Creating and managing users and groups with distinct roles.
- Controlling access to specific AWS services and resources.
- Assigning permissions securely through managed and inline policies.
- Implementing least privilege access — granting only the permissions actually required.
- Enforcing strong authentication through MFA and password policies.

7. Other AWS Security Features

Beyond IAM, AWS provides a comprehensive suite of security tools to protect cloud workloads:

Feature	Description
MFA	Adds an extra layer of login security beyond passwords.

IAM Policies & Roles	Provides fine-grained, resource-level permission control.
AWS Shield	Protects against DDoS (Distributed Denial of Service) attacks.
AWS WAF	Web Application Firewall — protects web apps from common attacks.
Amazon GuardDuty	AI-powered threat detection that monitors for malicious activity.
AWS CloudTrail	Logs and tracks all user activity and API calls for auditing.
AWS Config	Continuously monitors and records AWS resource configuration changes.

8. Lessons Learned

This lab provided practical experience with AWS IAM as a cloud access control system. Key takeaways include:

- How to create IAM users and groups and assign appropriate permission policies to enforce role-based access control.
 - The importance of the principle of least privilege — granting only the minimum permissions necessary reduces the risk of accidental or malicious damage.
 - How MFA adds a critical second layer of authentication, significantly reducing the risk of account compromise even if passwords are exposed.
 - How custom password policies enforce minimum security standards, including complexity requirements and expiration schedules.
 - How testing user permissions after assignment verifies that access control is correctly configured before deployment.
-