AWS IAM (Identity and Access Management) and MFA (Multi-Factor Authentication)

IAM (Identity and Access Management)

What is IAM?

IAM (Identity and Access Management) is a **global AWS service** that allows you to **securely manage access** to AWS services and resources for users, groups, and roles.

With IAM, you can:

- Create users and groups
- Assign permissions through **policies**
- Manage **roles** for service-to-service communication
- Enforce **least privilege access**

Types of Users in AWS

1. **Root User** – The account owner with **full access** to all AWS services.
2. **IAM User** – A user created by the root or admin, with **limited or managed permissions**.

Note: The root user should only be used for initial setup and critical tasks like billing or account closure. Use IAM users for daily operations.

IAM Concepts

Policy

A **policy** is a JSON document that defines **permissions** (allow/deny) for an entity to access AWS resources.

Types of Policies

Type	Description
AWS Managed Policy	Predefined by AWS, maintained by AWS.
Customer Managed	Created and managed by the user (more flexible).
Inline Policy	Embedded directly within a user, group, or role for **granular access**.

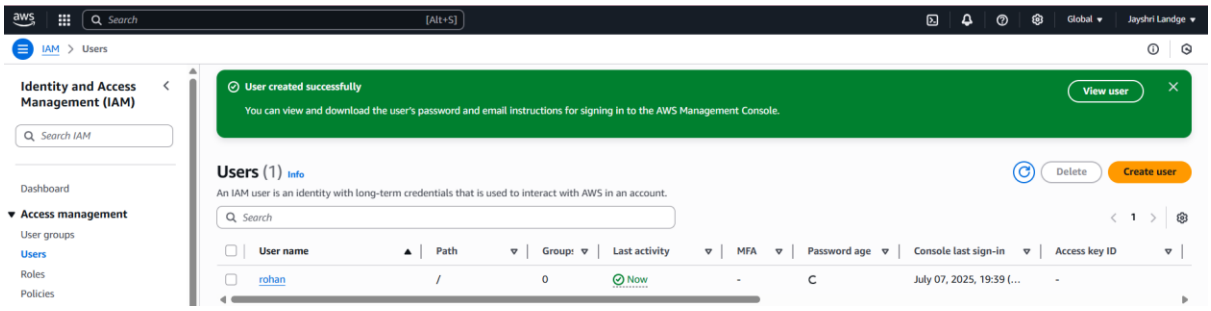
Root User vs IAM Admin User

Capability	Root User	IAM Admin User
Delete AWS Account	✅	❌
Access All Services	✅	✅ (with policy)
Enable/Disable MFA	✅	✅

Hands-On: IAM Configuration

Step 1: Create an IAM User

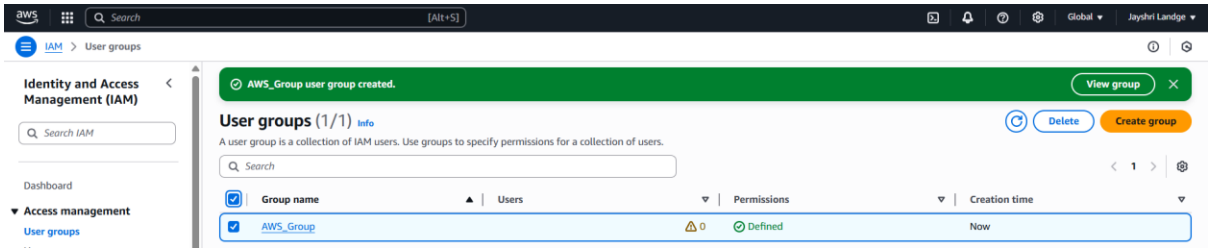
1. Open the **AWS Management Console**.
2. Go to **IAM → Users → Add users**.
3. Enter **User name**.
4. Select **Access type**:
    - AWS Management Console access
    - Programmatic access (for CLI/API access)



Screenshot 1: IAM User Creation – Select Access Type

Step 2: Create a Group

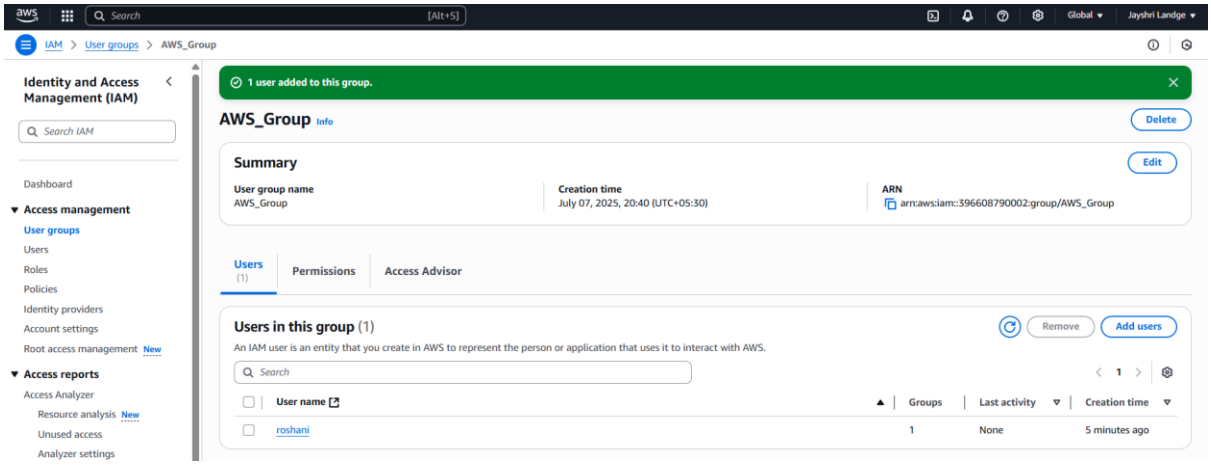
1. Navigate to **IAM → User groups → Create group**.
2. Enter a **group name** (e.g., AWS_Group).
3. Attach a **policy** (e.g., AmazonS3FullAccess).



Screenshot 2: Create IAM Group and Attach AdministratorAccess Policy

Step 3: Add User to Group

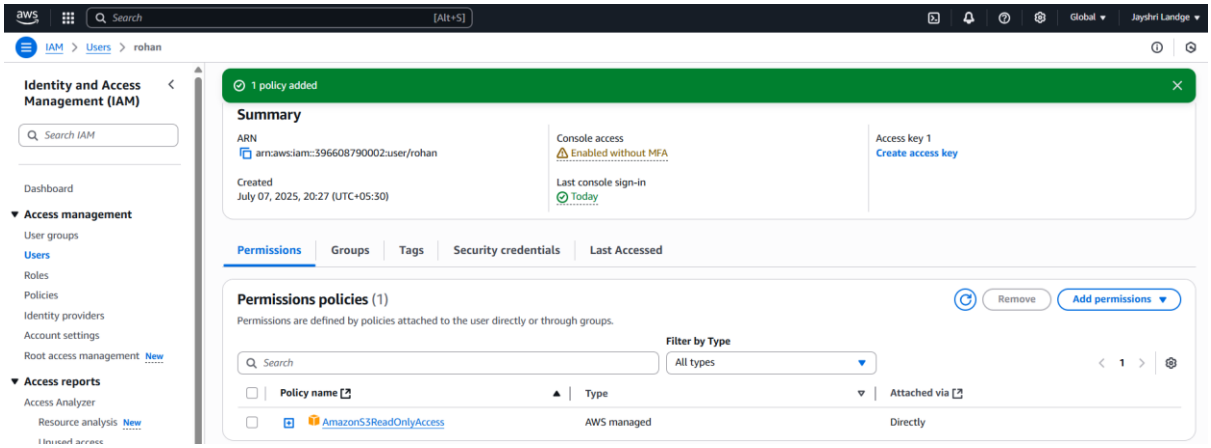
1. Go to the created **user's settings**.
2. Choose **Add user to group**.
3. Select the previously created group.



Screenshot 3: Add IAM User to Created Group

Step 4: Attach Policy Directly (Optional)

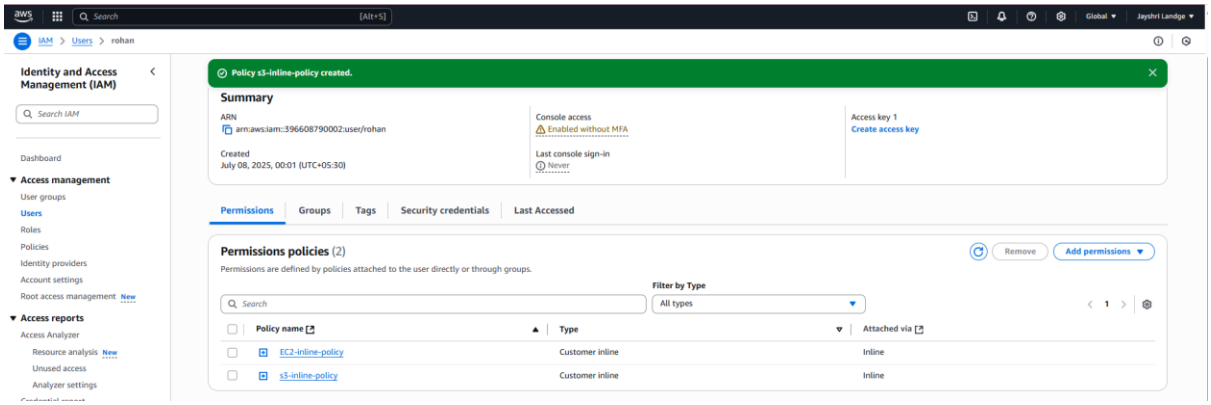
1. Go to IAM → Users → [Your User].
2. Click on the **Permissions** tab.
3. Click **Add permissions → Attach policies directly**.
4. Choose a policy like AmazonS3ReadOnlyAccess.



Screenshot 4: Attach AmazonS3ReadOnlyAccess Policy to User

Step 5: Add Inline Policy for Granular Control

1. Go to **IAM → Users → [User] → Add Inline Policy**.
2. Use the JSON editor to define custom permissions.
   Example:
   Allow EC2 to view and launch instances but deny deletion.

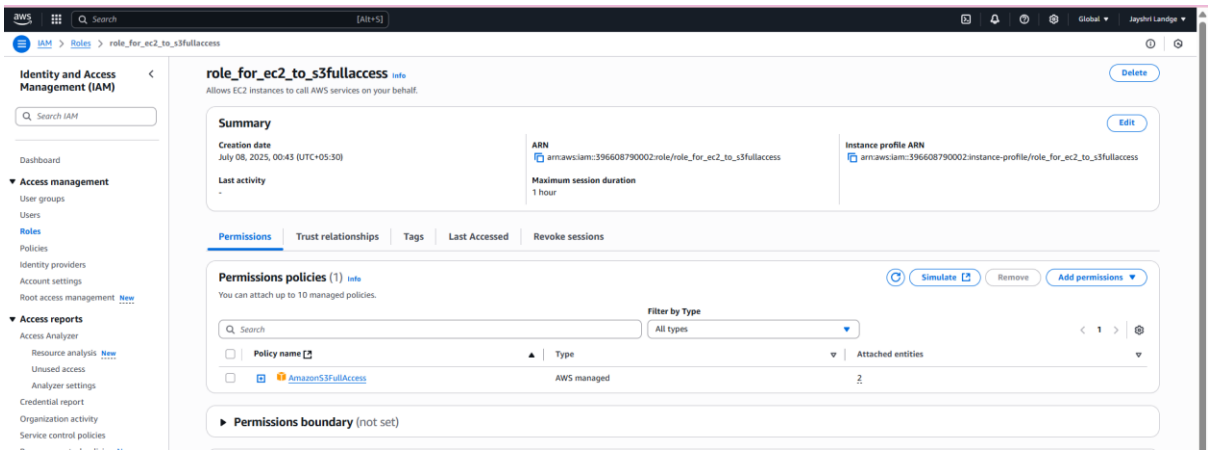


Screenshot 5: Add Inline Policy Using JSON Editor

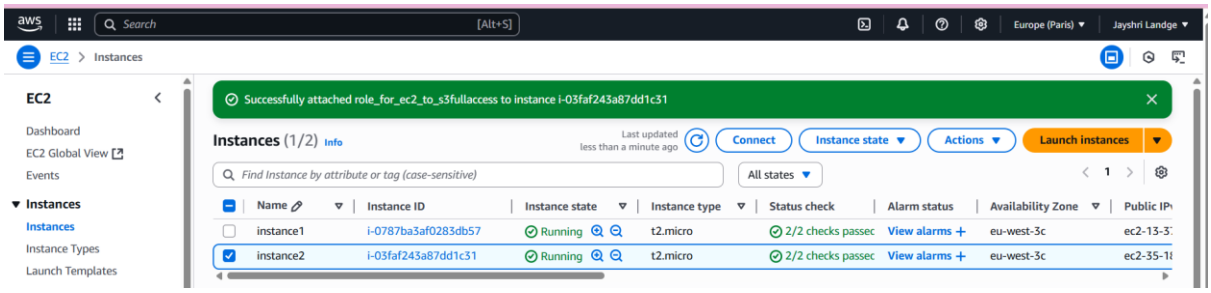
Example Use Case of IAM Role

You want an EC2 instance to access an S3 bucket:

1. Create a **Role** with AmazonS3ReadOnlyAccess.
2. Attach the role to the EC2 instance.
3. The EC2 instance now inherits the role's permissions.



Screenshot 6: Create IAM Role with AmazonS3ReadOnlyAccess



Screenshot 7: Attach IAM Role to EC2 Instance

Multi-Factor Authentication (MFA)

What is MFA?

MFA (Multi-Factor Authentication) is a **security enhancement** that requires two forms of verification:

1. Your account **password**
2. A **temporary one-time passcode (OTP)** generated by an authenticator app

It helps protect accounts from **unauthorized access** even if the password is compromised.

How MFA Works

When logging into the AWS Console:

1. Enter **username and password**
2. Enter **OTP from your device** (e.g., Google Authenticator)

Even if someone steals your password, they cannot log in without your second device (MFA code).

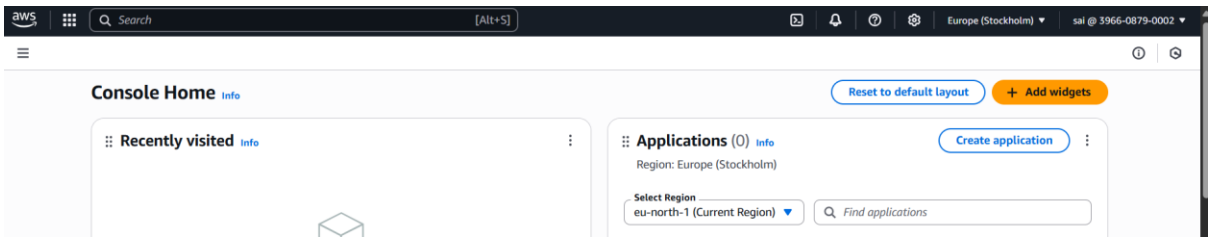
Supported MFA Apps

- Google Authenticator
- Authy
- Duo Mobile
- Microsoft Authenticator

Hands-On: Enable MFA for IAM User

Step 1: Log in as the IAM User

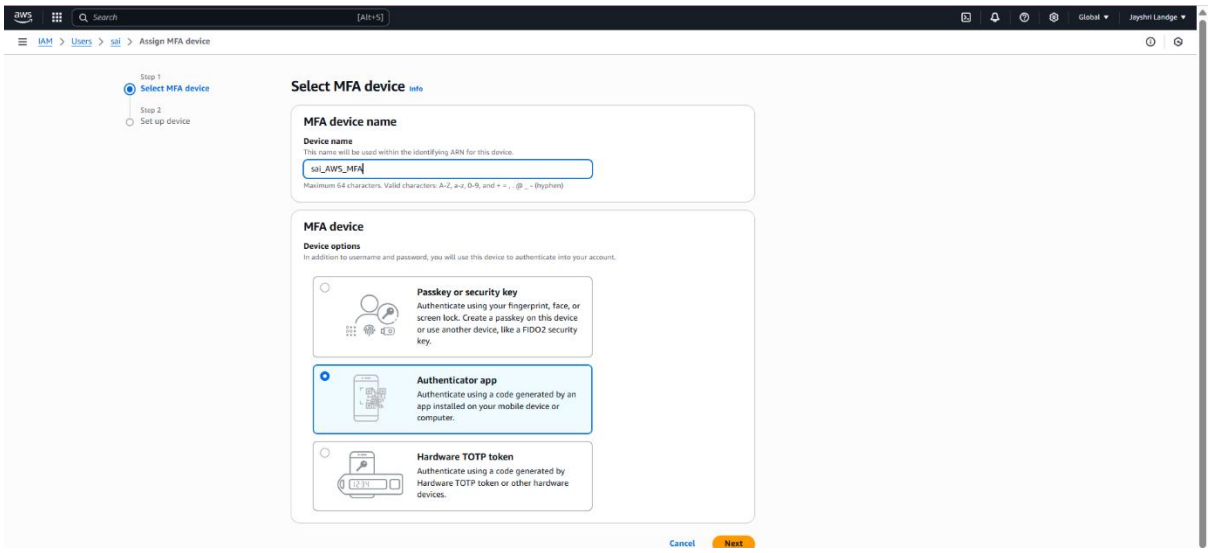
Use the credentials sent during IAM user creation.



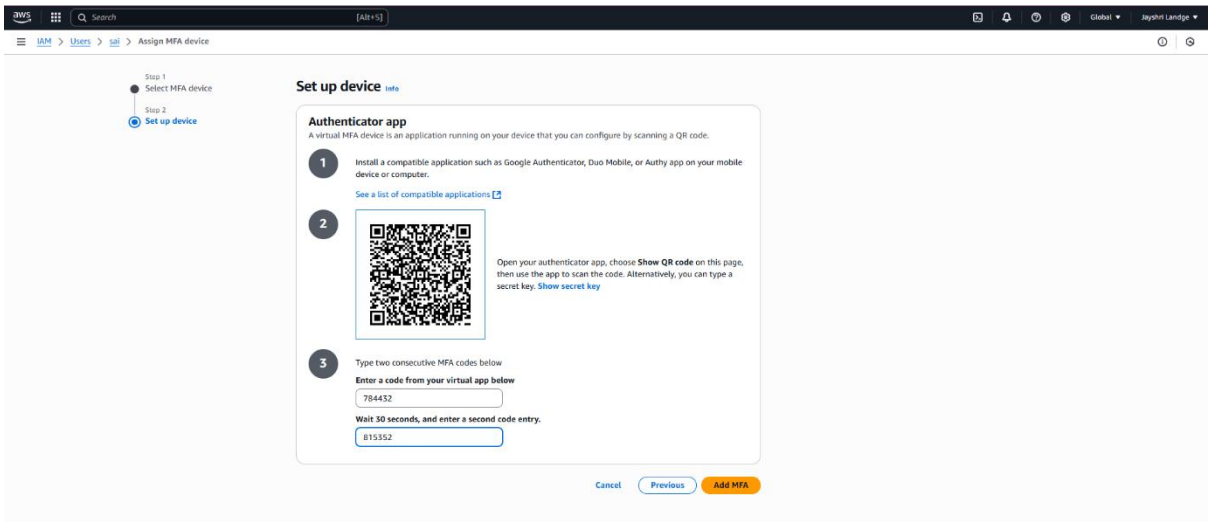
Screenshot 8: IAM User Console Login

Step 2: Set Up MFA

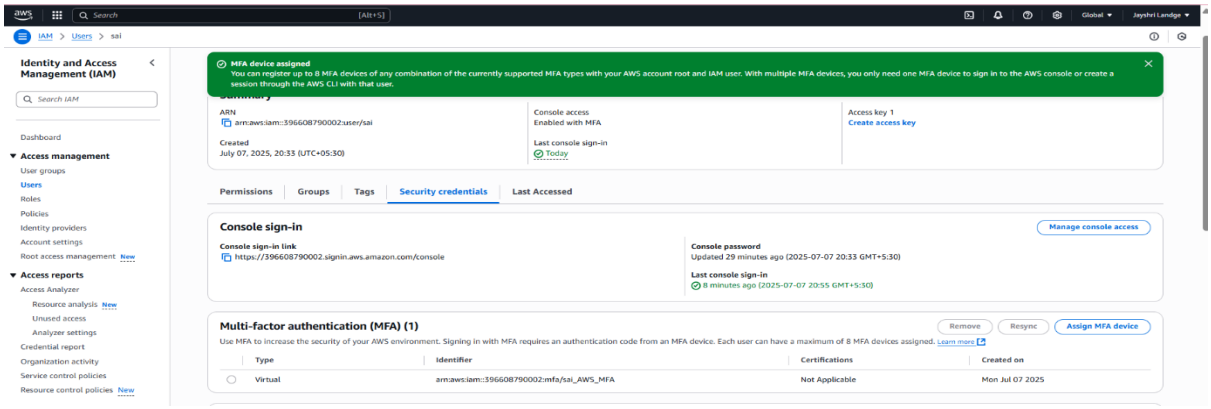
1. Go to **My Security Credentials** in the top right.
2. Choose **Multi-Factor Authentication (MFA)**.
3. Select **Assign MFA device**.
4. Choose **Authenticator App**.
5. Scan the QR code using Google Authenticator or any supported app.
6. Enter the 2 consecutive OTPs shown.



Screenshot 9: Navigate to My Security Credentials for MFA Setup



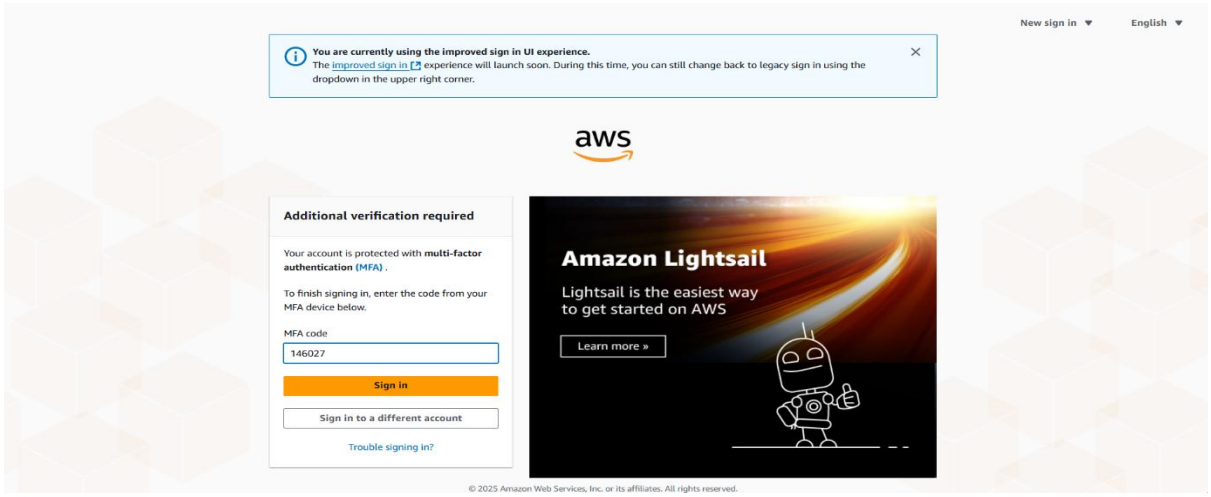
Screenshot 10: Assign MFA Device and Scan QR Code



Screenshot 11: Enter OTP Codes to Complete MFA Setup

Step 3: Verify and Activate

After entering valid codes, MFA is enabled successfully for that IAM user.



Screenshot 12: MFA Successfully Enabled for IAM User

Conclusion

- IAM is essential for controlling **who can access** AWS resources and **what actions** they can perform.
- IAM policies (Managed, Inline, and Customer Managed) offer **flexibility** in access control.
- IAM roles are used for **service-to-service access** (e.g., EC2 to S3).
- MFA significantly **enhances account security** by introducing an additional layer of authentication.

Always follow the **principle of least privilege** and **enable MFA** for both root and IAM users.