AWS IAM (Identify & Access Management)

1. AWS IAM (Access management of AWS Servies) implemented to overcome the issues like security aspects.

   For example : In a organisation have a AWS account but in that organisation different types of teams is available like Development team, Testing team. Both teams (testing & development) required AWS credentials to use the AWS services based on their requirement in that time we will create IAM user to set the restrictions & particular permissions on AWS services to ignore unnecessary usage of AWS source & security threats.

2. Based on the user requirement will create policies which services is required to access for that user & same policy will attach to the user.

   AWS IAM Concepts: Authentication and Authorization.

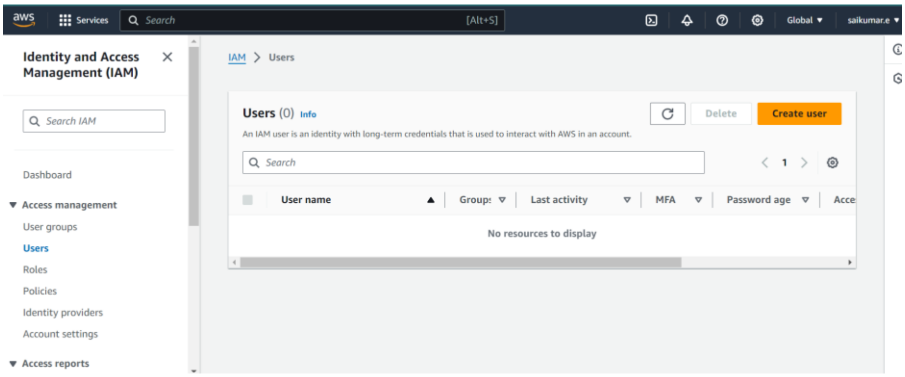
   - **Users (User authentication credentials is created to use AWS services based on requirement & now a days MFA is enabled in user creation)**
   -
   - **Policies (what are the services is required to a particular user is restricted in this policy & attach the same policy to a particular user)**

   - **Groups (If multiple users required same services & same permissions then will create group, add the users to these groups)**

   - **Roles (If any AWS service is required for only temporary (based on requirement) so roles will use in that cases.**

USERS:

1. IAM users is created to use AWS resources based on their requirement. Each user have unique authentication credentials. Once the user is created required to attach the policies. IAM user is useless without polices.



Identity and Access Management (IAM)

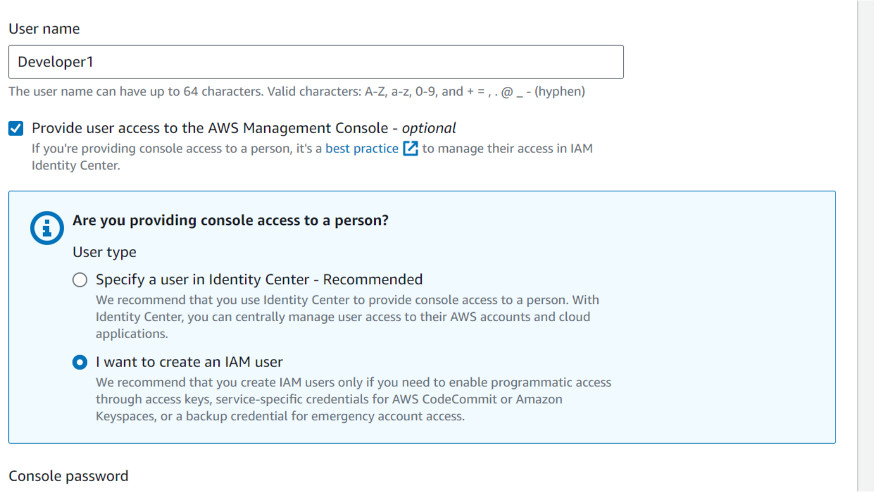
IAM > Users

Users (0) Info

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

User name	Groups	Last activity	MFA	Password age	Acce
No resources to display					

2.create a IAM user and select the auto generated password.



User name

Developer1

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☑ Provide user access to the AWS Management Console - *optional*
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

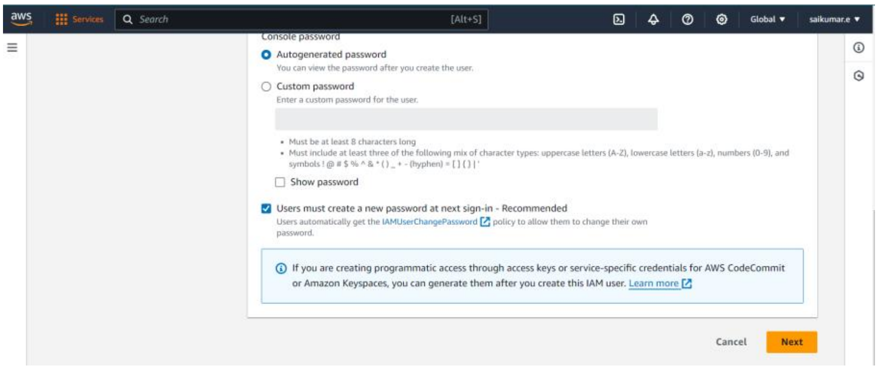
Are you providing console access to a person?

User type

○ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

● I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password



Console password

● Autogenerated password
You can view the password after you create the user.

○ Custom password
Enter a custom password for the user.

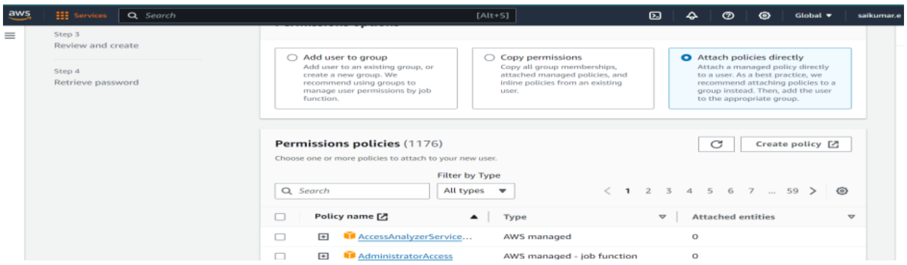
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ Show password

☑ Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more

3. Initially If you know the requirement of services then you can directly add a policies here or you can add the policies after user creation.



Step 3
Review and create

Step 4
Retrieve password

○ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

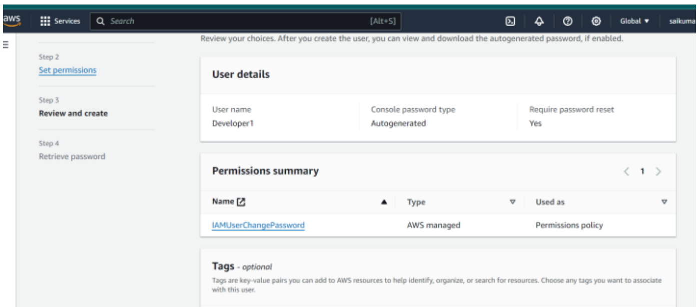
Permissions policies (1176)

Choose one or more policies to attach to your new user.

Filter by Type: All types

	Policy name	Type	Attached entities
□	AccessAnalyzerService...	AWS managed	0
□	AdministratorAccess	AWS managed - job function	0

4. Review the user details and create the user.



Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

User details

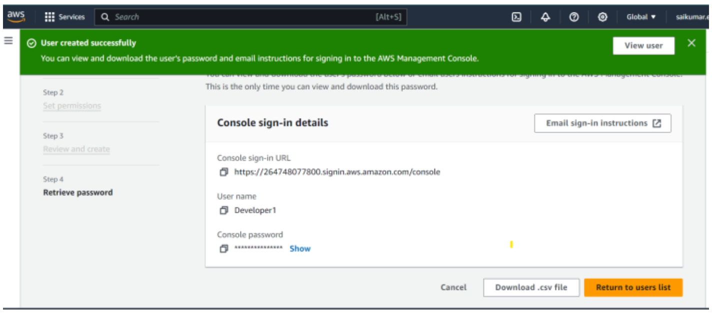
User name	Console password type	Require password reset
Developer1	Autogenerated	Yes

Permissions summary ‹ 1 ›

Name	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy

Tags - *optional*
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

5. Successfully user created & download the file for login user details. (The file contain the Account ID, User name & Password)



User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

This is the only time you can view and download this password.

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Console sign-in details

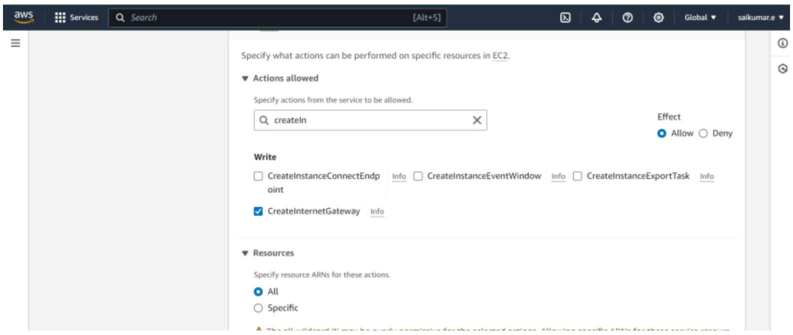
Console sign-in URL
https://264748077800.signin.aws.amazon.com/console

User name
Developer1

Console password
*************** Show

Policies :

1. First we need to know what are the requirements for the user & which services is used by the user.
2. Then will create a policies based on requirement. Select the services you require to use(like IAM, EC2 etc) & select the actions also which you perform within the service.



Specify what actions can be performed on specific resources in EC2.

▾ Actions allowed

Specify actions from the service to be allowed.

createIn

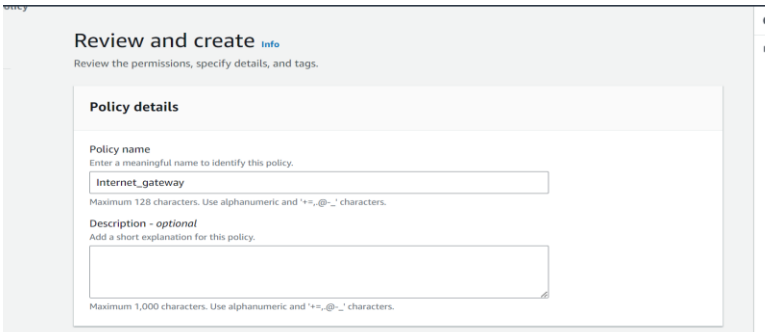
Effect
● Allow ○ Deny

Write
□ CreateInstanceConnectEndpoint Info □ CreateInstanceEventWindow Info □ CreateInstanceExportTask Info
☑ CreateInternetGateway Info

▾ Resources

Specify resource ARNs for these actions.
● All
○ Specific

3. Review & create the policy with a specified name.



Review and create Info
Review the permissions, specify details, and tags.

Policy details

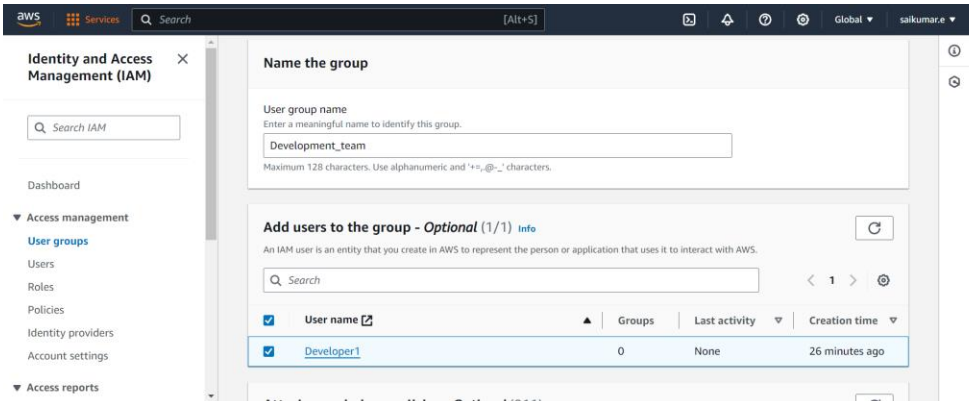
Policy name
Enter a meaningful name to identify this policy.
Internet_gateway
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

GROUPS:

1. Groups concept in IAM is used to manage the manual attention to create a each individual user policies.
2. In this groups based on the organisation requirement & teams (dev team, testing team)some groups already added with specified privileges.
3. So when ever new employee joins Devops engineer create a IAM user & add the same user to specified group.
4. Then the user have the specified privileges based on their team requirement.
5. Create a group, attach the policy & user.



Name the group

User group name

Enter a meaningful name to identify this group.

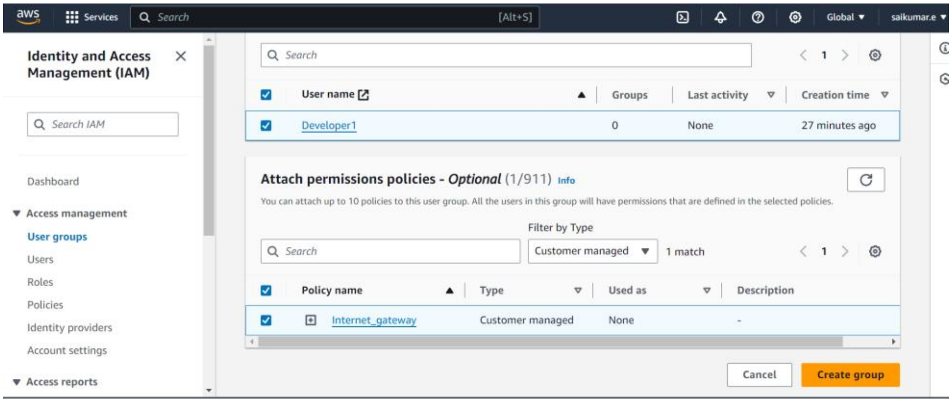
Development_team

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (1/1) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

☑	User name	Groups	Last activity	Creation time
☑	Developer1	0	None	26 minutes ago



☑	User name	Groups	Last activity	Creation time
☑	Developer1	0	None	27 minutes ago

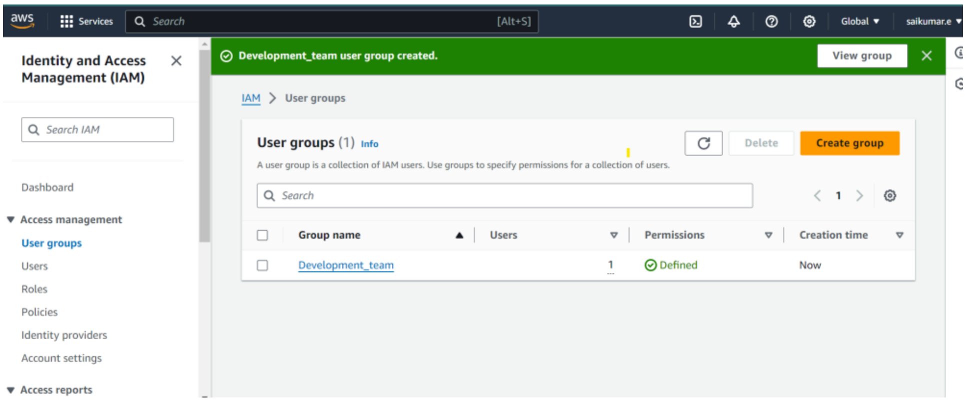
Attach permissions policies - *Optional* (1/911) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type: Customer managed — 1 match

☑	Policy name	Type	Used as	Description
☑	Internet_gateway	Customer managed	None	-

6. Successfully group created & attached the user to the created policy.

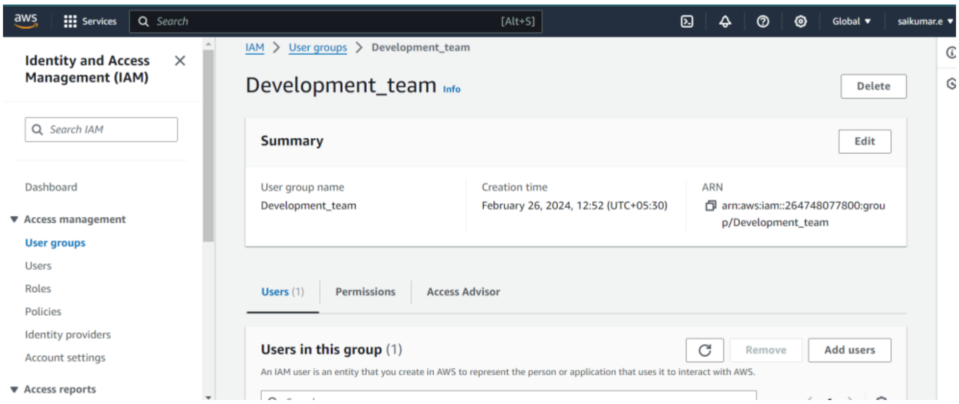


Development_team user group created.

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
□	Development_team	1	Defined	Now



Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

IAM > User groups > Development_team

Development_team Info

Delete

Summary

Edit

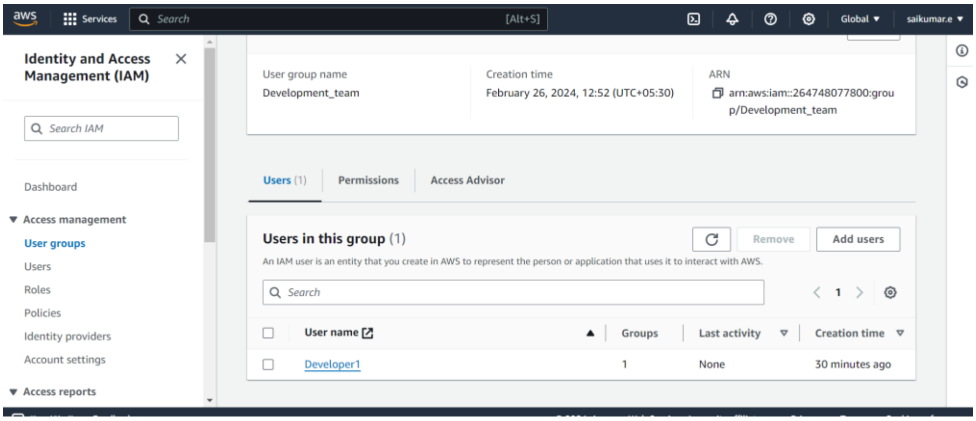
User group name	Creation time	ARN
Development_team	February 26, 2024, 12:52 (UTC+05:30)	arn:aws:iam::264748077800:group/Development_team

Users (1) | Permissions | Access Advisor

Users in this group (1)

Remove | Add users

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.



Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

User group name	Creation time	ARN
Development_team	February 26, 2024, 12:52 (UTC+05:30)	arn:aws:iam::264748077800:group/Development_team

Users (1) | Permissions | Access Advisor

Users in this group (1)

Remove | Add users

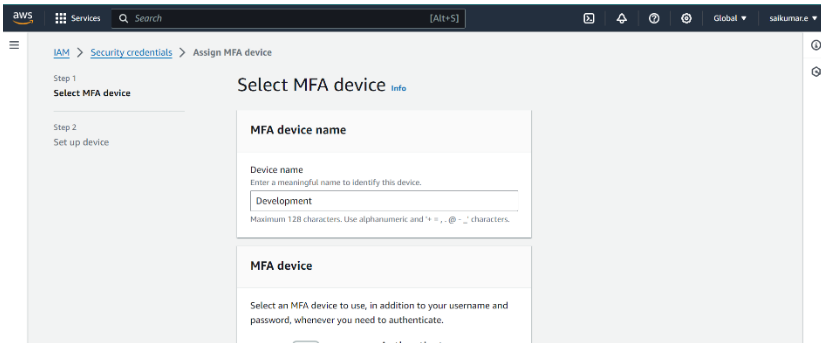
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search

□	User name	Groups	Last activity	Creation time
□	Developer1	1	None	30 minutes ago

NOTE: Based on the requirement we can enable the Multifactor Authentication for Root User or IAM User for more secure.

1.Enable the Multifactor Authentication.



IAM > Security credentials > 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.

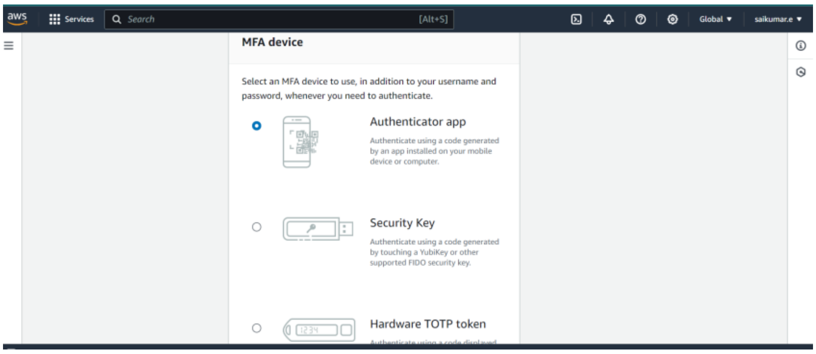
Development

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.

2. Select MFA based on your requirement (Authenticator app is preferred)



MFA device

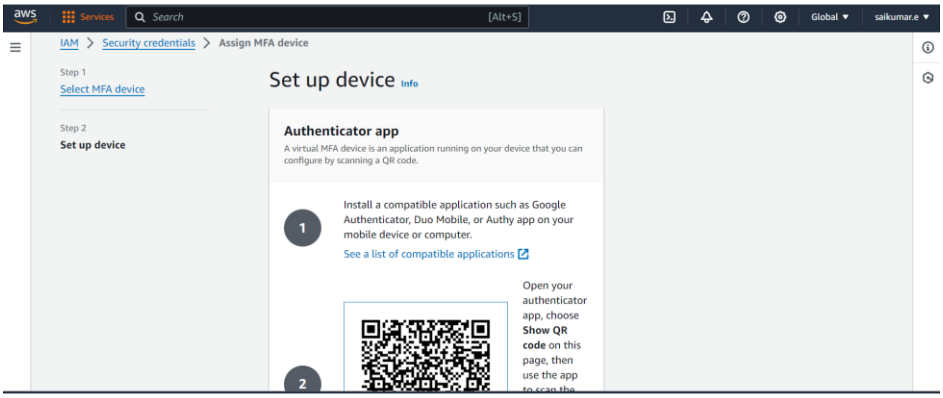
Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.

● 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.

○ Hardware TOTP token

3.Download authenticator app & scan the QR code then you will get the MFA code (OTP).



IAM > Security credentials > Assign MFA device

Step 1
Select MFA device

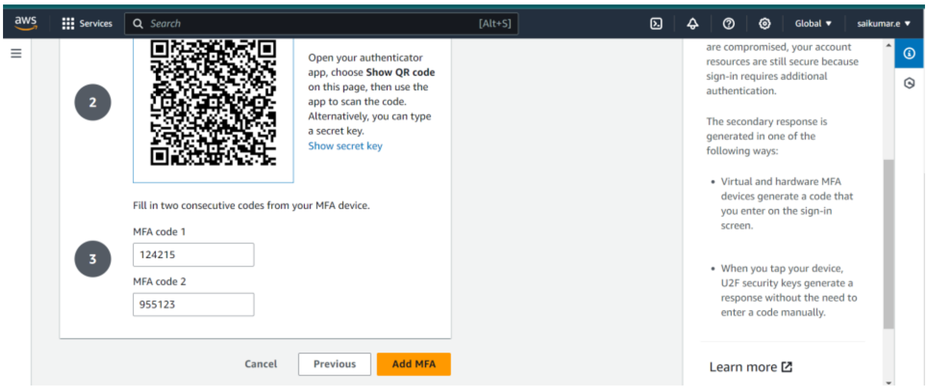
Step 2
Set up device

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



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: 124215
MFA code 2: 955123

Cancel | Previous | Add MFA

are compromised, your account resources are still secure because sign-in requires additional authentication.

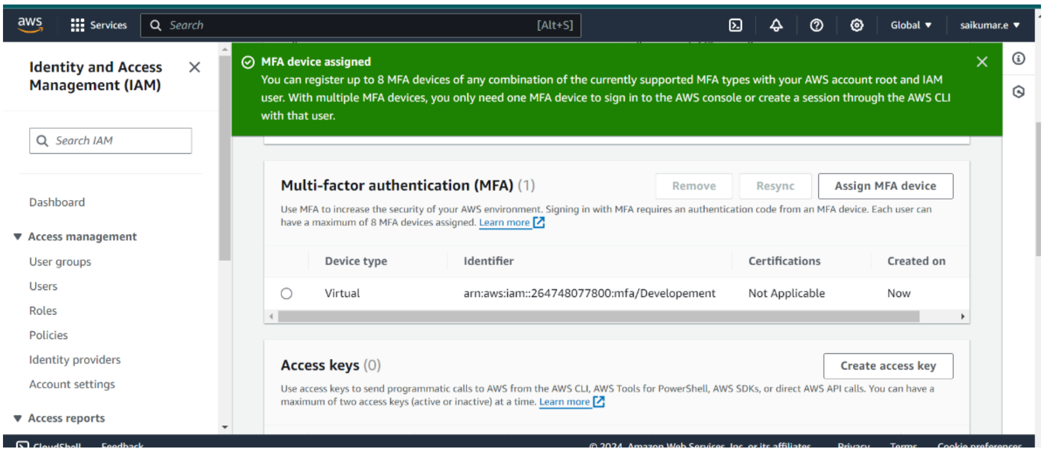
The secondary response is generated in one of the following ways:

- Virtual and hardware MFA devices generate a code that you enter on the sign-in screen.
- When you tap your device, U2F security keys generate a response without the need to enter a code manually.

Learn more

4.Once you enable the MFA every time MFA code is required when your login root or IAM user.

5. Successfully MFA enabled.



Identity and Access Management (IAM)

Search IAM

Dashboard
▼ Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
▼ Access reports

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.

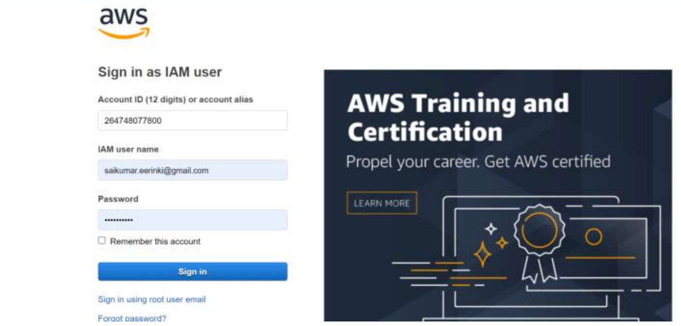
Multi-factor authentication (MFA) (1)
Remove | Resync | Assign MFA device
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

	Device type	Identifier	Certifications	Created on
○	Virtual	arn:aws:iam::264748077800:mfa/Developement	Not Applicable	Now

Access keys (0)
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 inactive) at a time. Learn more

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates Privacy Terms Cookie preferences

6.Then you can login into AWS account with IAM user (MFA also enabled)



Sign in as IAM user

Account ID (12 digits) or account alias: 264748077800

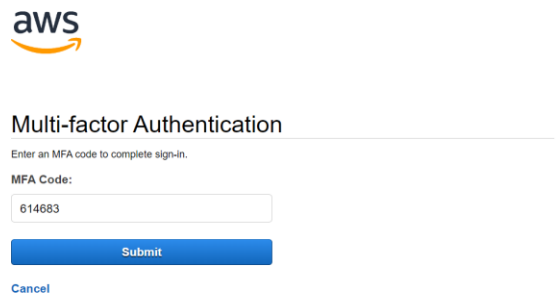
IAM user name: saikumar.eerinki@gmail.com

Password: •••••••••••

☐ Remember this account

aws
Sign in
Sign in using root user email
Forgot password?
AWS Training and Certification
Propel your career. Get AWS certified
LEARN MORE

7. Enter the MFA code (OTP) which is generated in QR code scanned mobile device.

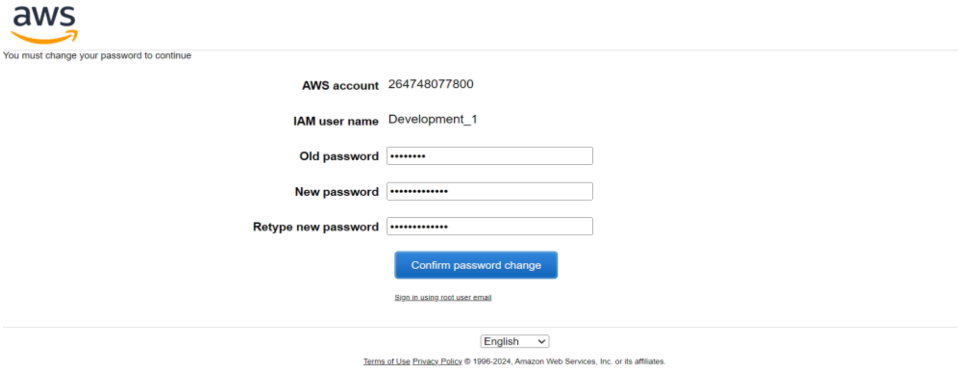


Multi-factor Authentication

Enter an MFA code to complete sign-in.

MFA Code: 614683

8. Initially modify the auto generated password into custom password



You must change your password to continue

AWS account: 264748077800

IAM user name: Development_1

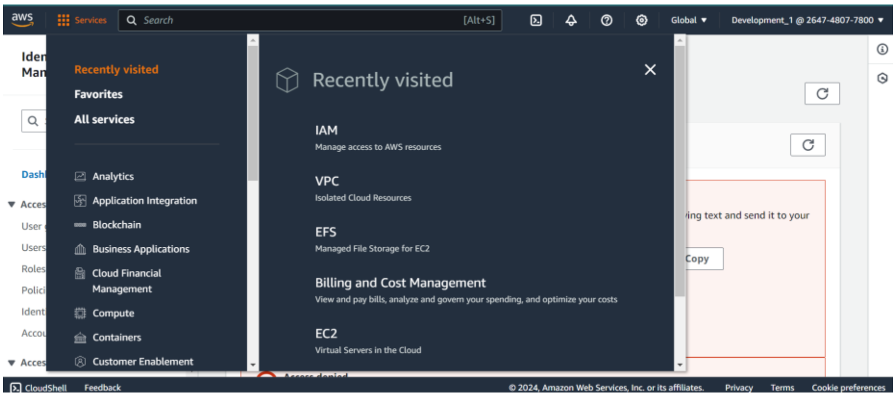
Old password: ••••••••

New password: •••••••••••••

Retype new password: •••••••••••••

aws
Confirm password change
Sign in using root user email
English
Terms of Use Privacy Policy © 1996-2024, Amazon Web Services, Inc. or its affiliates.

9. Successfully login into AWS account with IAM user.



aws
Services
Search
[Alt+S]
Global
Development_1 @ 2647-4807-7800
Recently visited
Favorites
All services
Analytics
Application Integration
Blockchain
Business Applications
Cloud Financial Management
Compute
Containers
Customer Enablement
Recently visited
IAM
Manage access to AWS resources
VPC
Isolated Cloud Resources
EFS
Managed File Storage for EC2
Billing and Cost Management
View and pay bills, analyze and govern your spending, and optimize your costs
EC2
Virtual Servers in the Cloud
Copy
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences