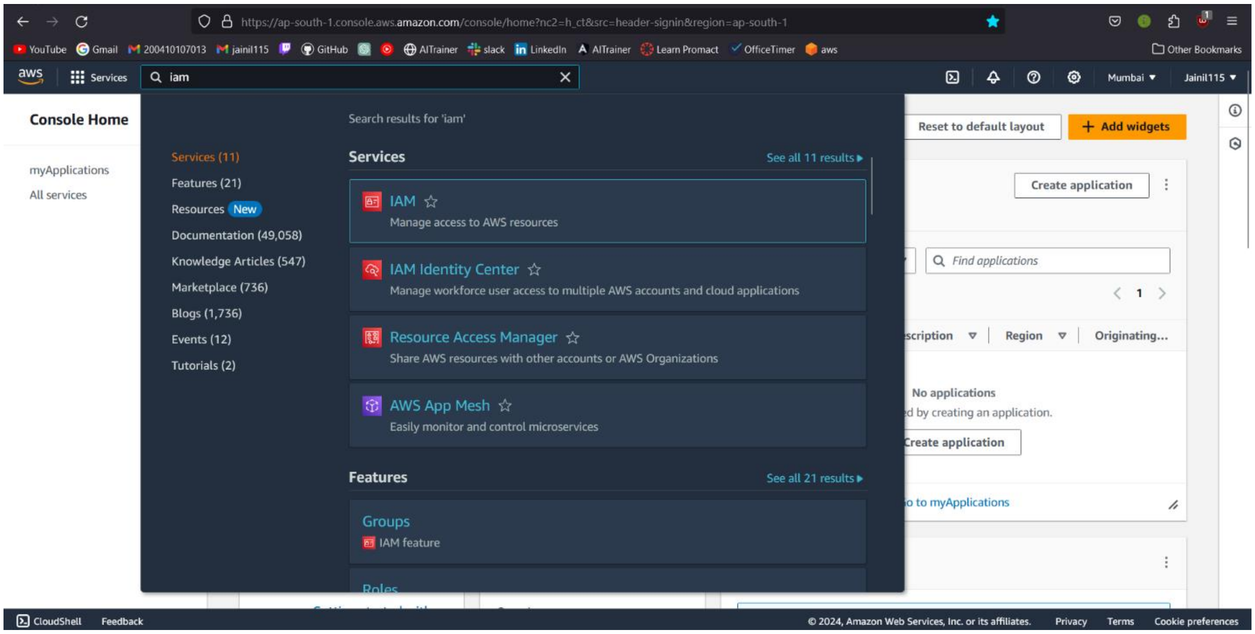
TASK 2: Create a New IAM User Named "S3-User":

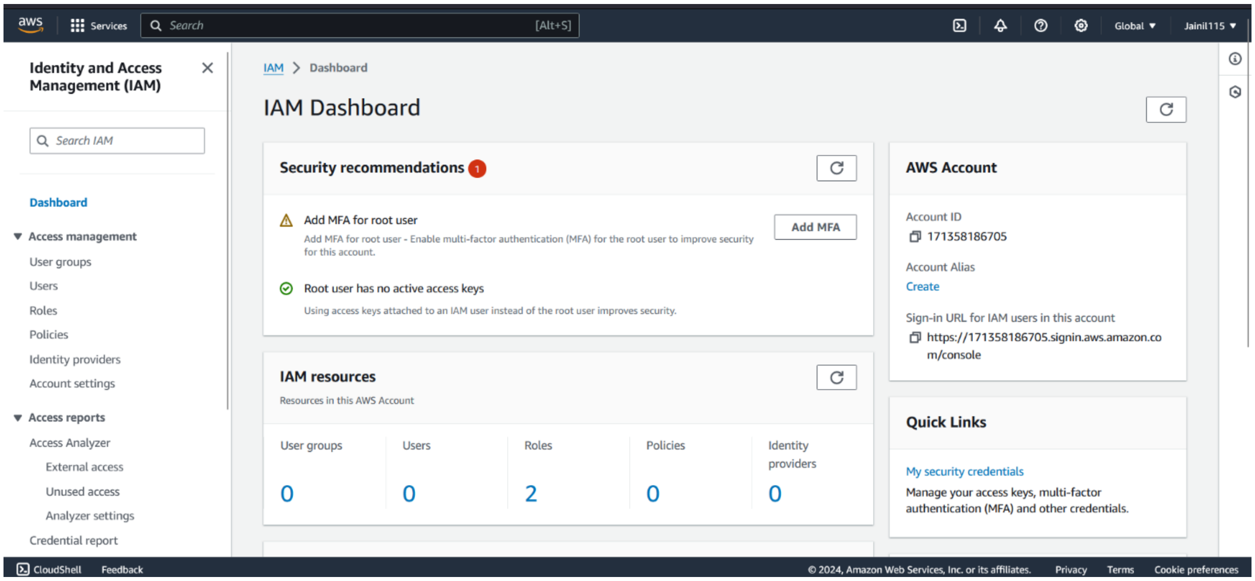
1. **Create a new IAM user with programmatic access.**
2. **Attach the AmazonS3FullAccess policy to the user.**
3. **Generate an access key and secret key for the IAM user**

Steps to create new IAM user with programmatic access:

1. To Create IAM account go to the aws console and search for “IAM” and select IAM.



2. Then select "Users" from the menu.



IAM Dashboard

Security recommendations 1

Add MFA for root user

Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	2	0	0

AWS Account

Account ID
171358186705

Account Alias
Create

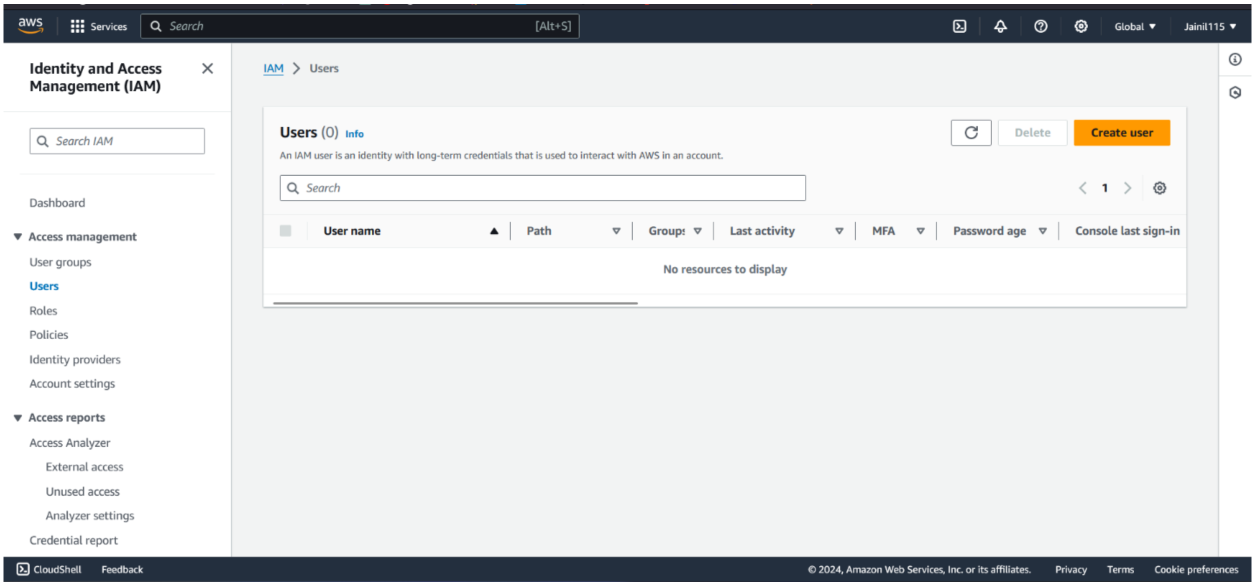
Sign-in URL for IAM users in this account
https://171358186705.signin.aws.amazon.com/console

Quick Links

My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

© 2024, Amazon Web Services, Inc. or its affiliates.

3. Then click on create user.



Users (0)

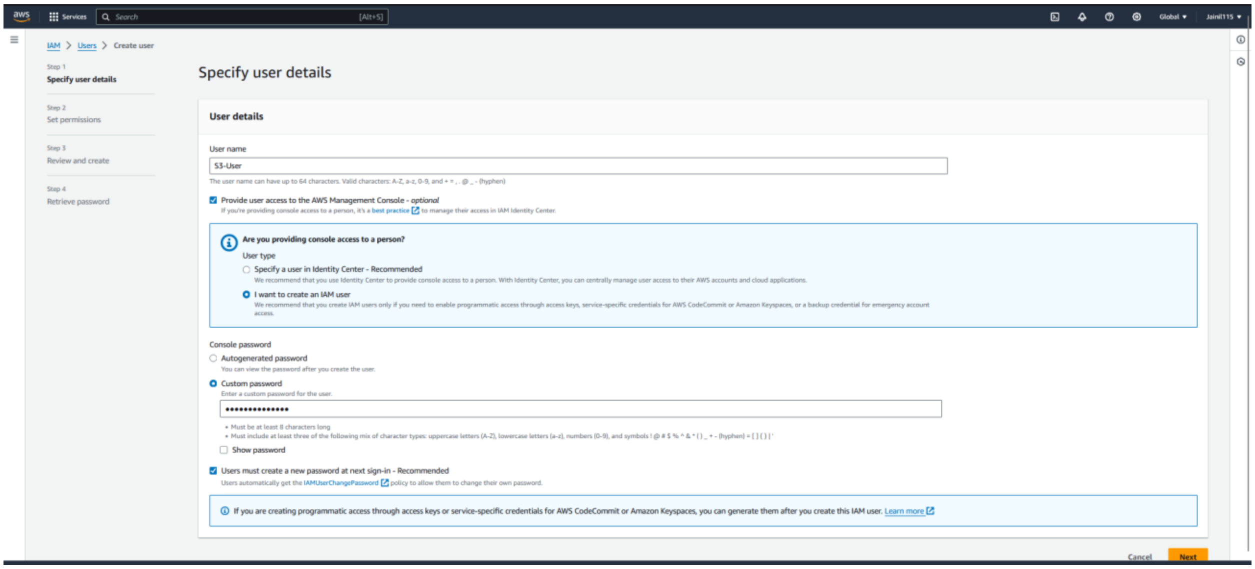
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name ▲	Path	Groups	Last activity	MFA	Password age	Console last sign-in

No resources to display

© 2024, Amazon Web Services, Inc. or its affiliates.

4. Then enter the user name and select "Provide user access to the AWS Management Console" and then select "I want to create an IAM user", This will provide programmatic access. Then select custom password and enter password that follows the password policy. Then uncheck "Users must create a new password at next sign-in". Then click on next.



Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Specify user details

User details

User name

S3-User

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

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

● Custom password
Enter a custom password for the user.

•••••••••••••••

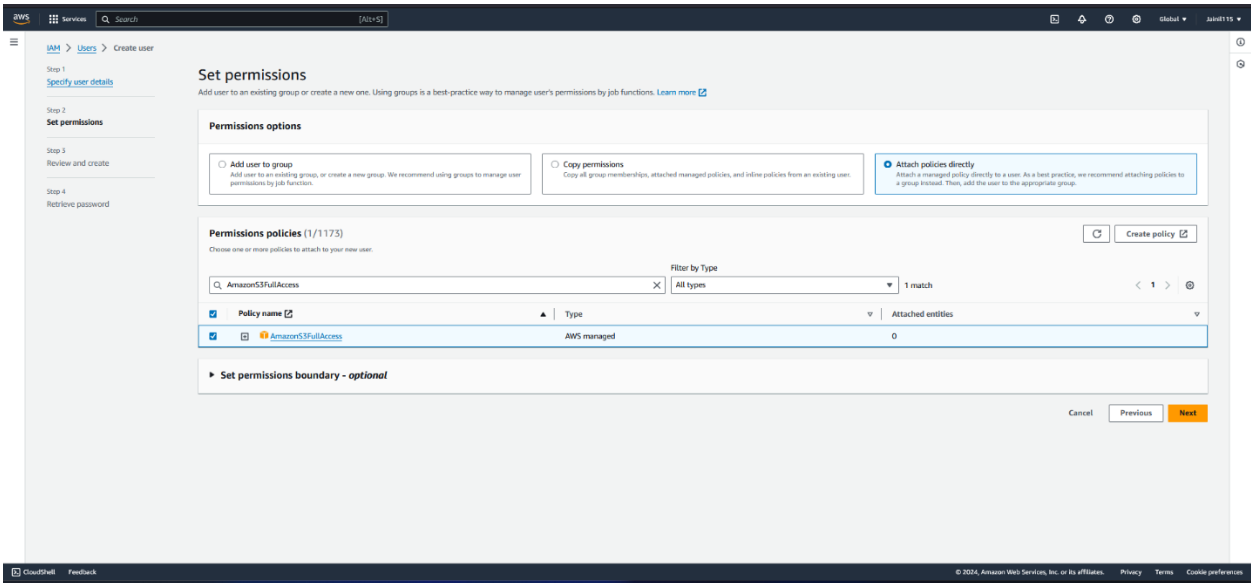
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ 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

5. Now Click select "Attach policies directly" in permission options. Now search for policy "AmazonS3FullAccess" then select it. Then click on next.



Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Permissions options

○ 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 (1/1173)

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

AmazonS3FullAccess

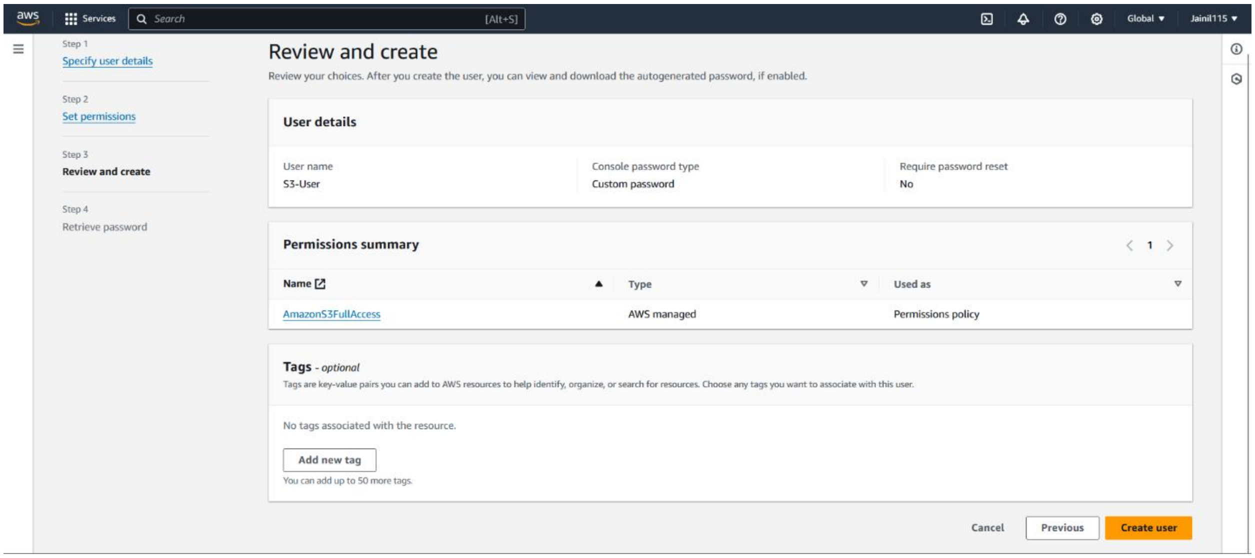
Filter by Type: All types

1 match

☑	Policy name	Type	Attached entities
☑	AmazonS3FullAccess	AWS managed	0

▸ **Set permissions boundary - *optional***

6. Then you will see Review and Create page. Now click on "Create User"



Review and create

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

User details

User name	Console password type	Require password reset
S3-User	Custom password	No

Permissions summary

Name	Type	Used as
AmazonS3FullAccess	AWS managed	Permissions policy

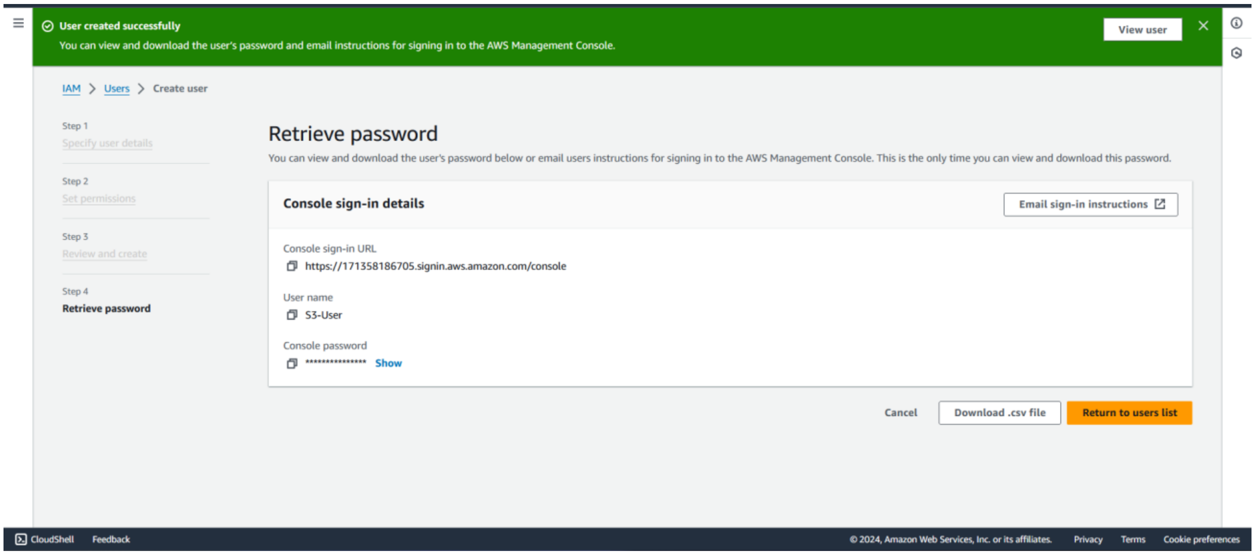
Tags - *optional*

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.

No tags associated with the resource.

You can add up to 50 more tags.

7. Now you can either download the user credential's .csv file. Then click on "Return to users list"



User created successfully

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

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

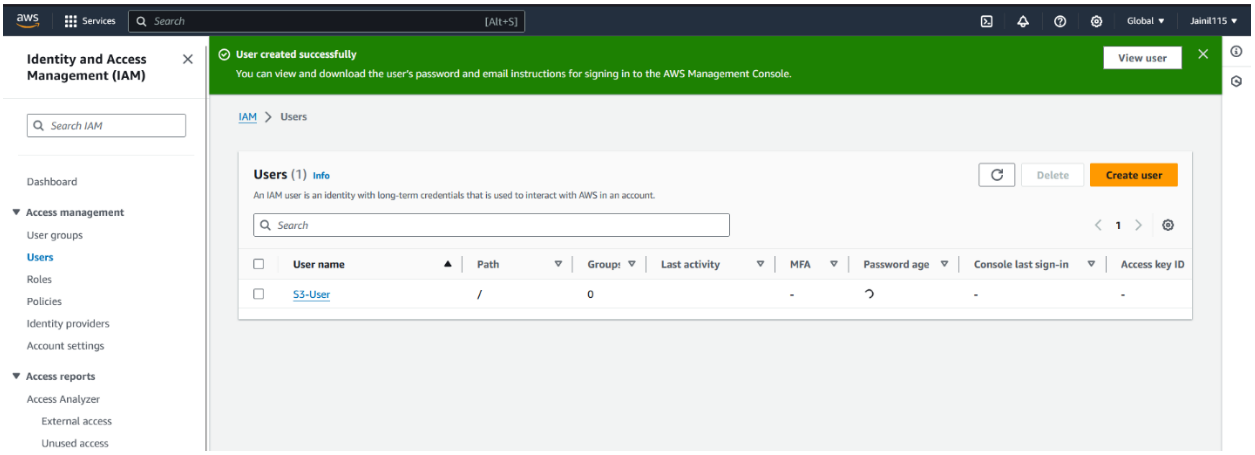
Console sign-in details

Console sign-in URL
https://171358186705.signin.aws.amazon.com/console

User name
S3-User

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

8. Now you will be able to see all the IAM users.



User created successfully

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

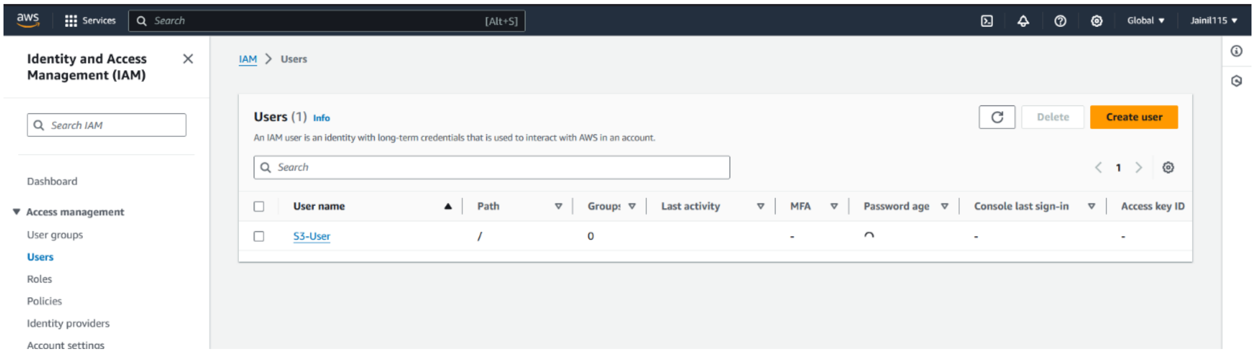
Users (1) Info

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
□	S3-User	/	0		-		-	-

Steps to create IAM user's access key:

1. Select "S3-User" from IAM users list of Users.

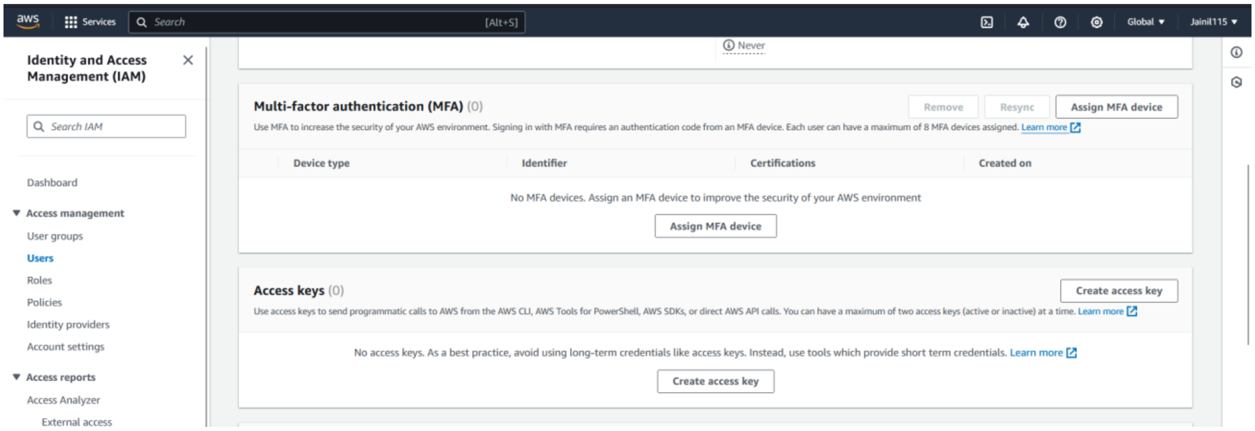


Users (1) Info

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
□	S3-User	/	0		-		-	-

2. Navigate to security credentials in "S3-User" info. And scroll down to Access keys and then click on "create access key"



Multi-factor authentication (MFA) (0)

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

No MFA devices. Assign an MFA device to improve the security of your AWS environment

Assign MFA device

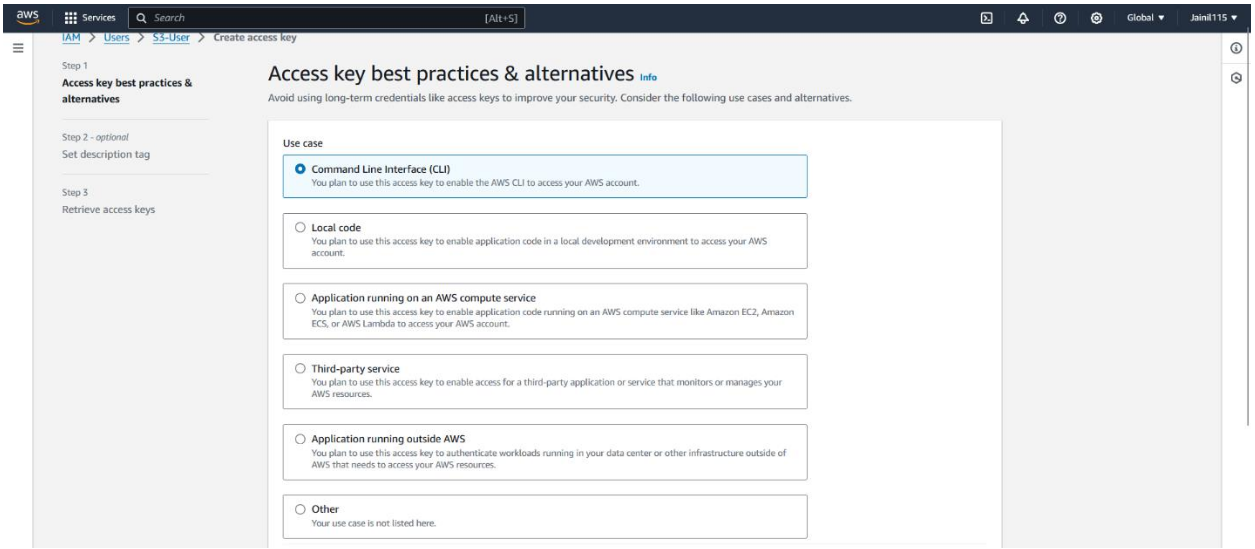
Access keys (0)

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

No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. Learn more

Create access key

3. Select "Command Line Interface (CLI)" from the use case. Then click on "next".



IAM > Users > S3-User > Create access key

Step 1
Access key best practices & alternatives

Step 2 - *optional*
Set description tag

Step 3
Retrieve access keys

Access key best practices & alternatives Info

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Use case

● Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.

○ Local code
You plan to use this access key to enable application code in a local development environment to access your AWS account.

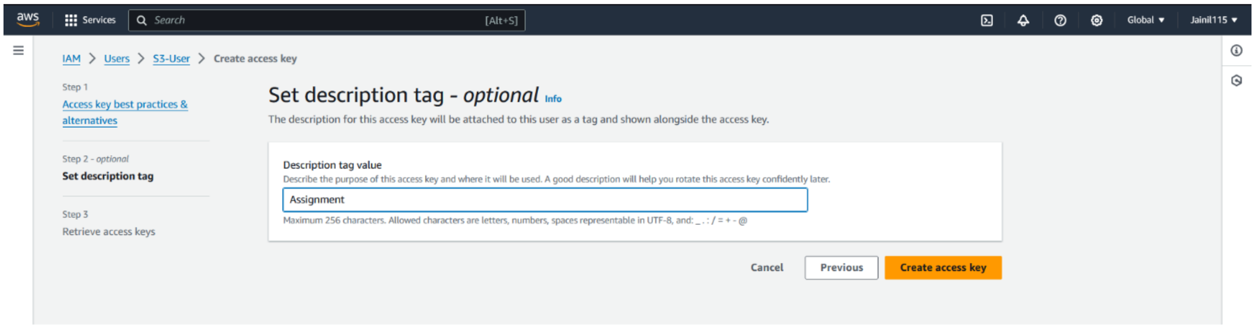
○ Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

○ Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

○ Application running outside AWS
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.

○ Other
Your use case is not listed here.

4. Then you can add an optional description tag. Then click on "Create access key".



IAM > Users > S3-User > Create access key

Step 1
Access key best practices & alternatives

Step 2 - *optional*
Set description tag

Step 3
Retrieve access keys

Set description tag - *optional* Info

The description for this access key will be attached to this user as a tag and shown alongside the access key.

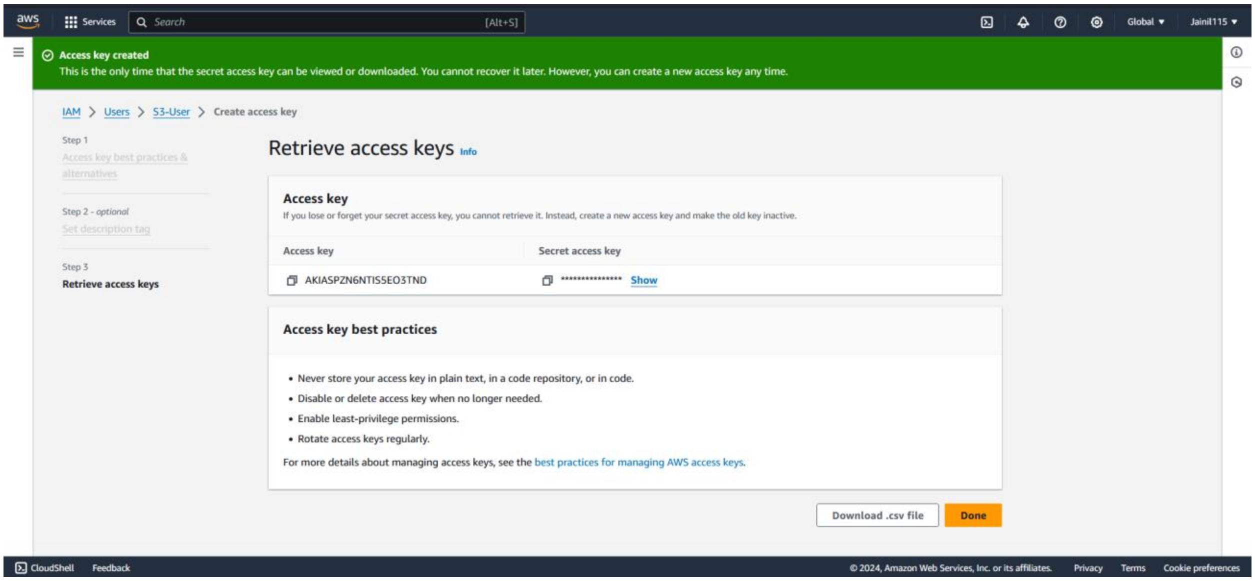
Description tag value
Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.

Assignment

Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . : / = + - @

Cancel | Previous | **Create access key**

5. Now you will be able to see the access key and secret access key.



Access key created
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

IAM > Users > S3-User > Create access key

Step 1
Access key best practices & alternatives

Step 2 - *optional*
Set description tag

Step 3
Retrieve access keys

Retrieve access keys Info

Access key
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIASPZN6NTIS5EO3TND	*************** Show

Access key best practices

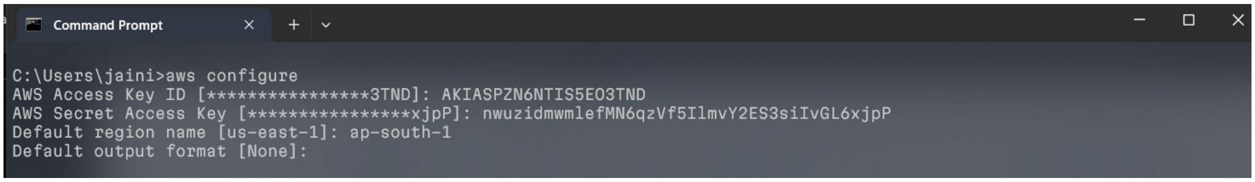
- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the best practices for managing AWS access keys.

Download .csv file | **Done**

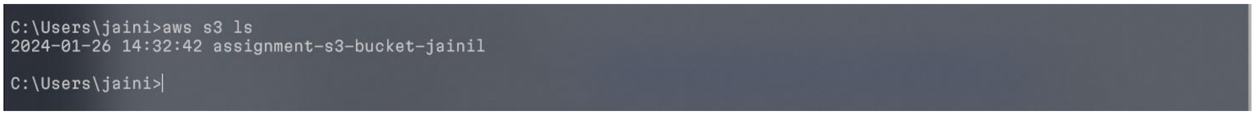
Steps to verify programmatic access with access key:

1. Download aws cli v2 using link: https://awscli.amazonaws.com/AWSCLIV2.msi, Then install aws cli v2.
2. After that open command prompt and enter command "aws configure". Then enter the access key, secret access key, Default region name and Default output format.



```
C:\Users\jaini>aws configure
AWS Access Key ID [****************3TND]: AKIASPZN6NTIS5EO3TND
AWS Secret Access Key [****************xjpP]: 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
Default region name [us-east-1]: ap-south-1
Default output format [None]:
```

3. This IAM user has AmazonS3FullAccess policy attached, So we can use command "aws s3 ls" to list s3 buckets.



```
C:\Users\jaini>aws s3 ls
2024-01-26 14:32:42 assignment-s3-bucket-jainil

C:\Users\jaini>
```