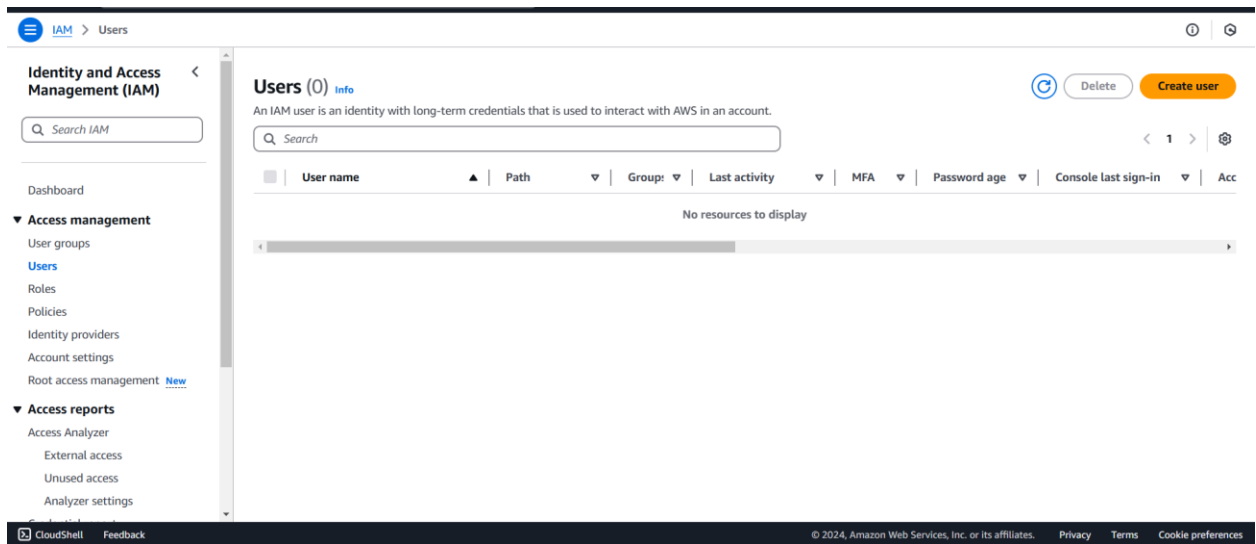


IAM(Identity and Access Management)

Q. > How to create GUI user in Amazon IAM?

- Open your web browser and navigate to the [AWS Management Console](#).
- Log in using your **root account** or **IAM credentials**.
- In the **AWS Console**, locate the **Search bar** at the top.
- Type **IAM** and press **Enter**.
- Select **IAM** from the search results.
- Once inside the IAM service, you will be on the **IAM Dashboard**.



Step 1:-

- Click on the **Users**.
- After then click on **create user**.
- Enter the user details. User name "**aws_user**"

IAM > Users > Create user

Step 1: Specify user details (selected)
 Step 2: Set permissions
 Step 3: Review and create
 Step 4: Retrieve password

Specify user details

User details

User name

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.

- Then choose the option **I want to create an IAM user**.
- After Then choose the **Autogenerated password** or **custom password**.
- When choose **custom password** “Temp12345” like that.

IAM > Users > Create user

Step 1: Specify user details
 Step 2: Set permissions (selected)
 Step 3: Review and create
 Step 4: Retrieve password

User details

User name

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.

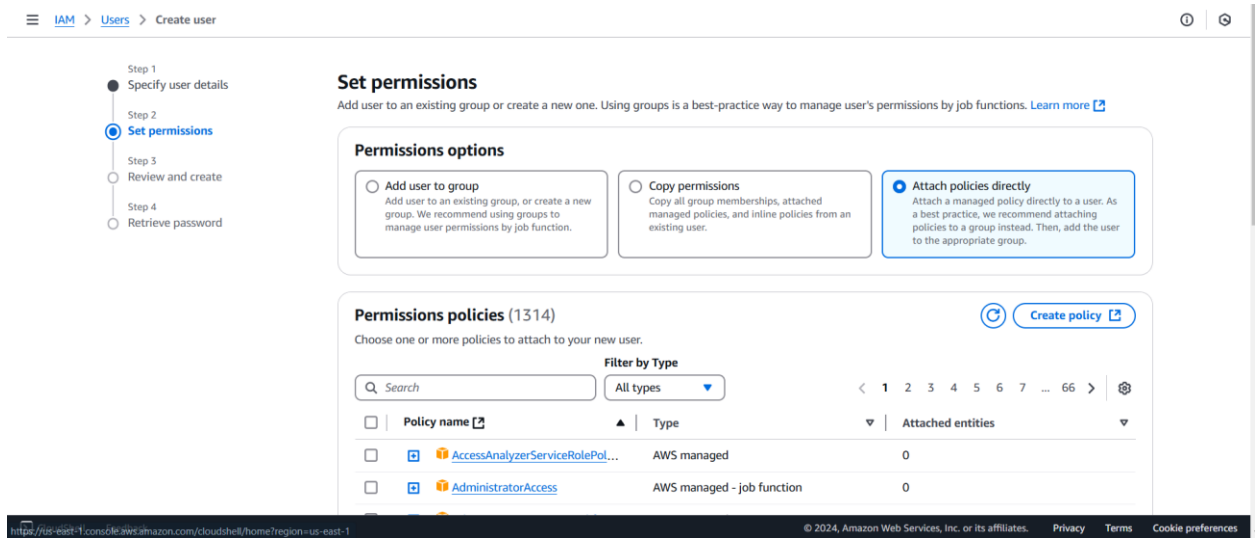
CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

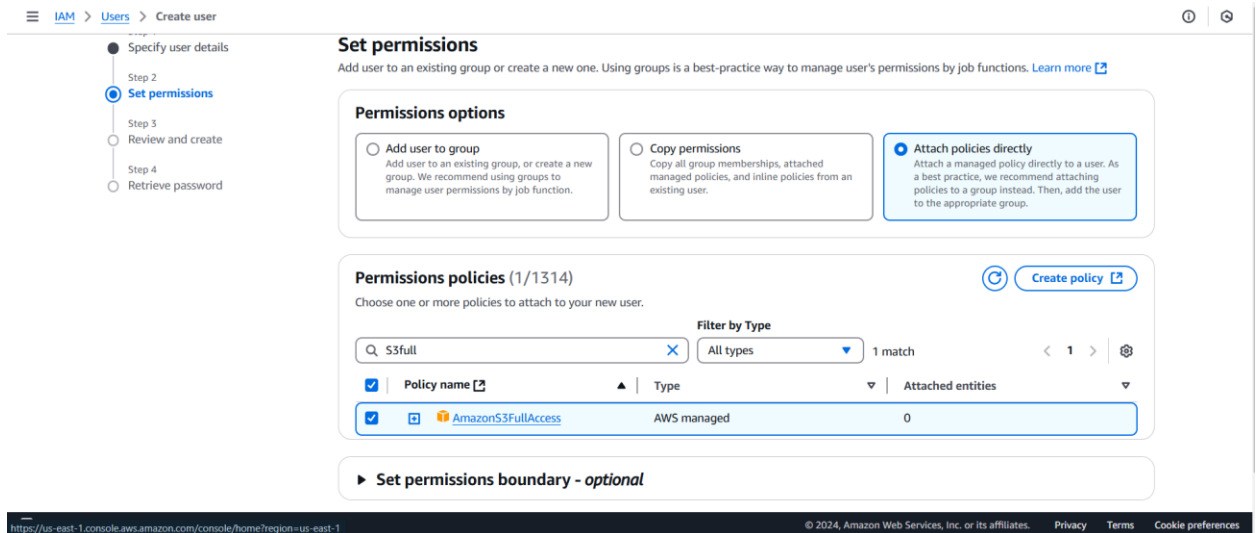
- Then click on **Next**.

Step 2:-

- Set permissions.
- Click on **Attach policies directly**.



- Go to the **Permissions policies search box** and search your permissions policies.
- Search like that “**S3fullaccess**”, “**Ec2fullaccess**” like that.



- Select the policies and click on **next**.

Step 3:-

- Review and create.
- In this step to check our policies and user details.
- Then click on the **create user**.

aws

Search

[Alt+S]

Global

Neeraj2001

IAM

Users

Create user

Step 1

Specify user details

Step 2

Set permissions

Step 3

Review and create

Step 4

Retrieve password

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

aws_user

Console password type

Custom password

Require password reset

Yes

Permissions summary

Name	Type	Used as
AmazonEC2FullAccess	AWS managed	Permissions policy
AmazonS3FullAccess	AWS managed	Permissions policy
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.

No tags associated with the resource.

CloudShell

Feedback

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

Privacy

Terms

Cookie preferences

IAM

Users

Create user

Step 4

Retrieve password

aws_user

Custom password

Yes

Permissions summary

Name	Type	Used as
AmazonEC2FullAccess	AWS managed	Permissions policy
AmazonS3FullAccess	AWS managed	Permissions policy
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.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Previous

Create user

CloudShell

Feedback

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

Privacy

Terms

Cookie preferences

Step 4:-

- Retrieve password.
- Console sign-in details
- **Console sign-in URL** Copy link and paste another browser.
- **User name and Console password** used to login the user.
-

IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

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://147997146235.signin.aws.amazon.com/console>

User name
aws_user

Console password
***** [Show](#)

[Email sign-in instructions](#)

[Cancel](#) [Download .csv file](#) [Return to users list](#)

IAM user sign in

Account ID (12 digits) or account alias
147997146235

IAM username
aws_user

Password
Temp12345

☒ Show Password [Having trouble?](#)

[Sign in](#)

[Sign in using root user email](#)

[Create a new AWS account](#)


☐ Remember this account

By continuing, you agree to [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

Amazon Lightsail

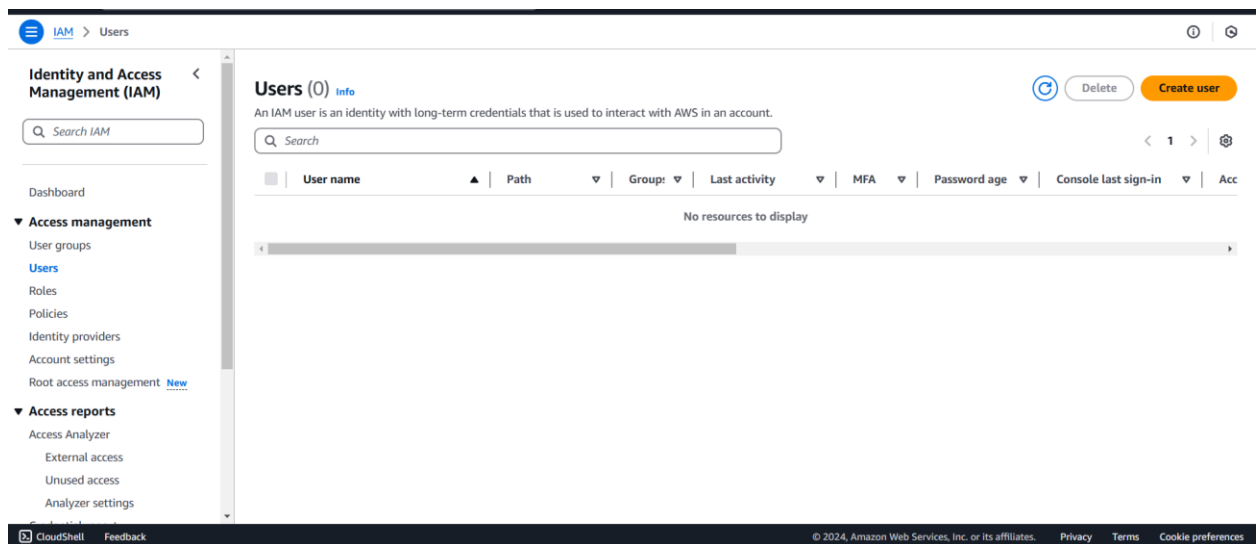
Lightsail is the easiest way to get started on AWS

[Learn more »](#)



Q.> How to create Programmatic User in Amazon IAM?

- Open your web browser and navigate to the [AWS Management Console](#).
- Log in using your **root account** or **IAM credentials**.
- In the **AWS Console**, locate the **Search bar** at the top.
- Type **IAM** and press **Enter**.
- Select **IAM** from the search results.
- Once inside the IAM service, you will be on the **IAM Dashboard**.



Step 1:-

- Click on the **Users**.
- After then click on **create user**.
- Enter the user details. User name **aws_user**

Step 1 **Specify user details**
 Step 2 Set permissions
 Step 3 Review and create

Specify user details

User details

User name

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.

① 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](#)

Cancel Next

➤ Then click on the **next**.

Step 2:-

- **Set permissions.**
- **Permissions options.**

- Add user to group
- Copy permissions
- **Attach policies directly.**

Step 3 Review and create

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 (1/1314)

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

Filter by Type: All types 1 match

<input checked="" type="checkbox"/>	Policy name	Type	Attached entities
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	0

▶ **Set permissions boundary - optional**

Cancel Previous Next

- Click on the **next**.

Step 3:-

- Review and create.

The screenshot shows the 'Create user' wizard in the AWS IAM console, specifically Step 3: Review and create. The left sidebar shows the progress: Step 1 (Create user), Step 2 (Set permissions), and Step 3 (Review and create). The main content area has a heading 'Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.' Below this are three sections: 'User details' with fields for 'User name' (aws_user), 'Console password type' (None), and 'Require password reset' (No); 'Permissions summary' showing a table with one entry 'AmazonSSFullAccess' of type 'AWS managed' used as a 'Permissions policy'; and 'Tags - optional' with a note that no tags are associated and an 'Add new tag' button. At the bottom right are 'Cancel', 'Previous', and 'Create user' buttons.

Name	Type	Used as
AmazonSSFullAccess	AWS managed	Permissions policy

User name	Console password type	Require password reset
aws_user	None	No

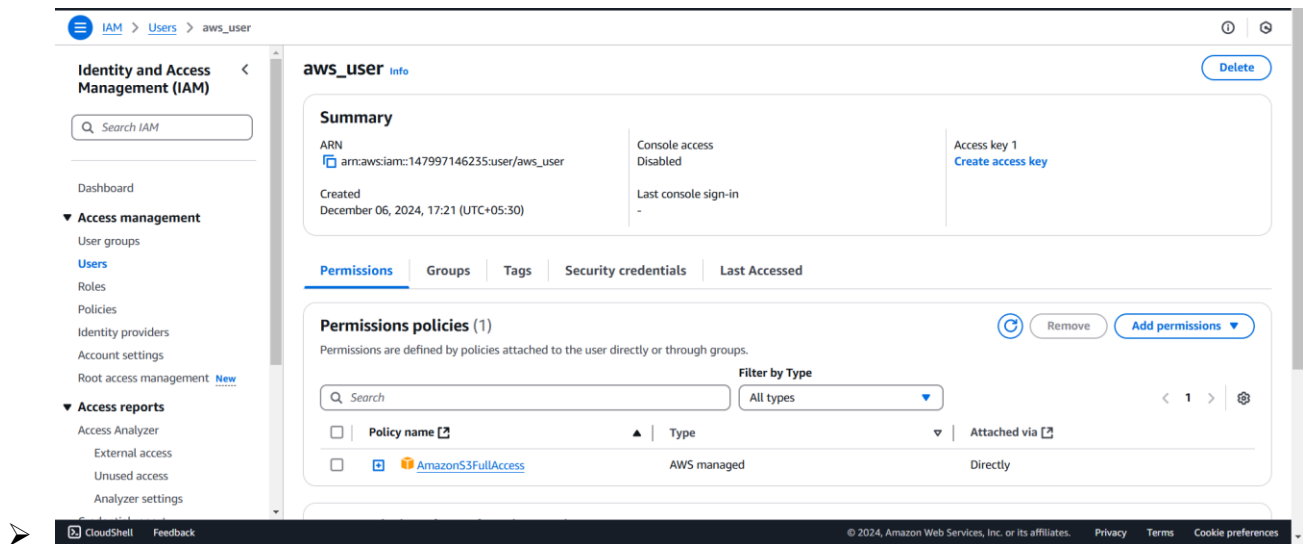
Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.
No tags associated with the resource.
[Add new tag](#)
You can add up to 50 more tags.

- After that **create user**.

The screenshot shows the 'Users' page in the AWS IAM console. A green banner at the top states 'User created successfully' with a 'View user' button. Below this, the 'Users (1)' section shows a table with one user, 'aws_user'. The left sidebar shows the 'Identity and Access Management (IAM)' navigation menu. At the bottom right are 'Delete' and 'Create user' buttons.

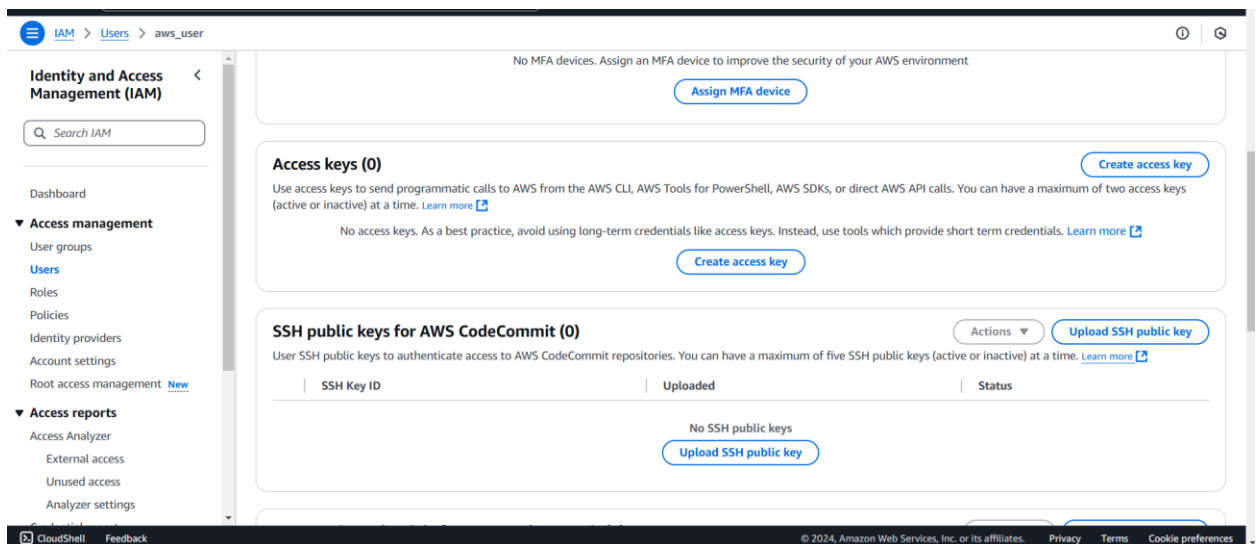
User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Acc
aws_user	/	0	-	-	-	-	-

- Click on the “aws_user”.

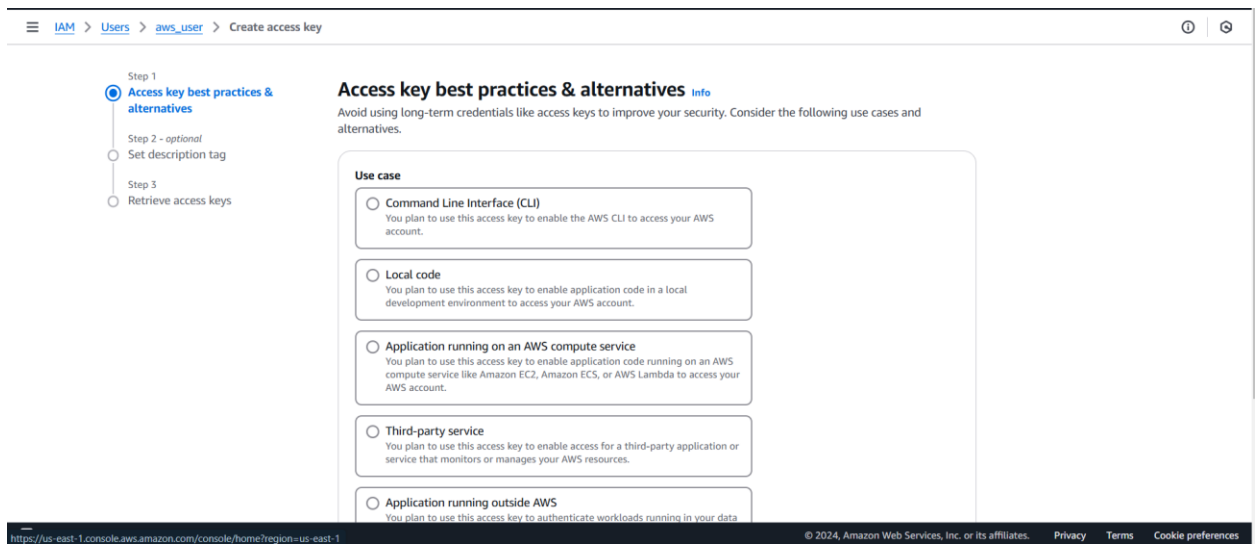


- After then click on the Security credentials.

- And scroll go to the Access Keys.



- And click on create access key .
- Go to create access key the dashboard.

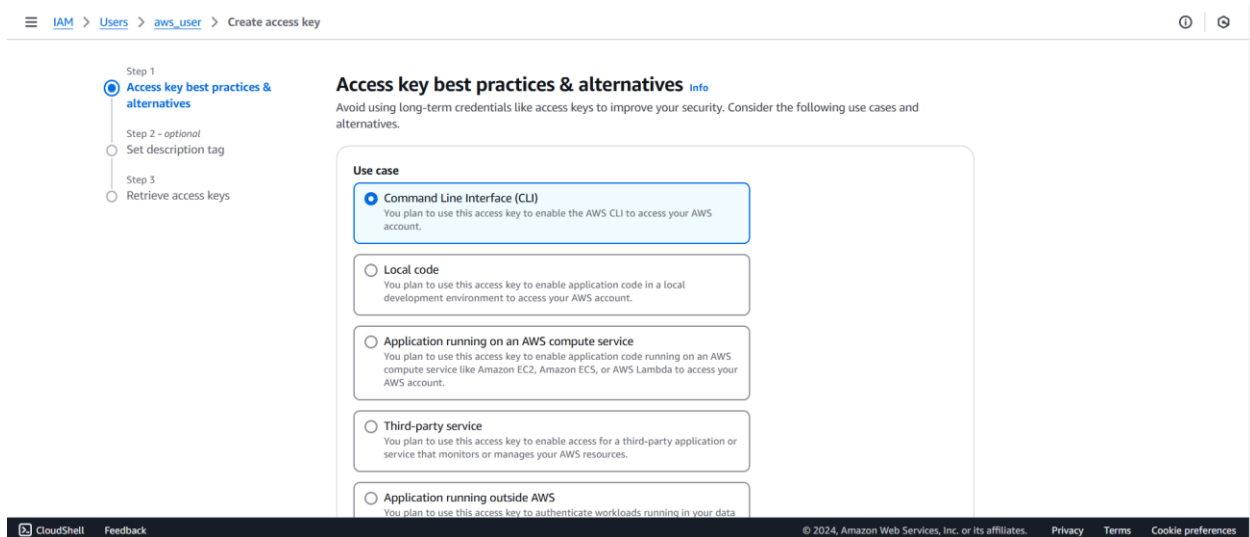


Step 1:-

➤ **Access key best practices & alternatives.**

➤ **Use case.**

✓ **Command Line Interface (CLI).**



➤ Scroll and check in the **confirmation.**

Step 2:-

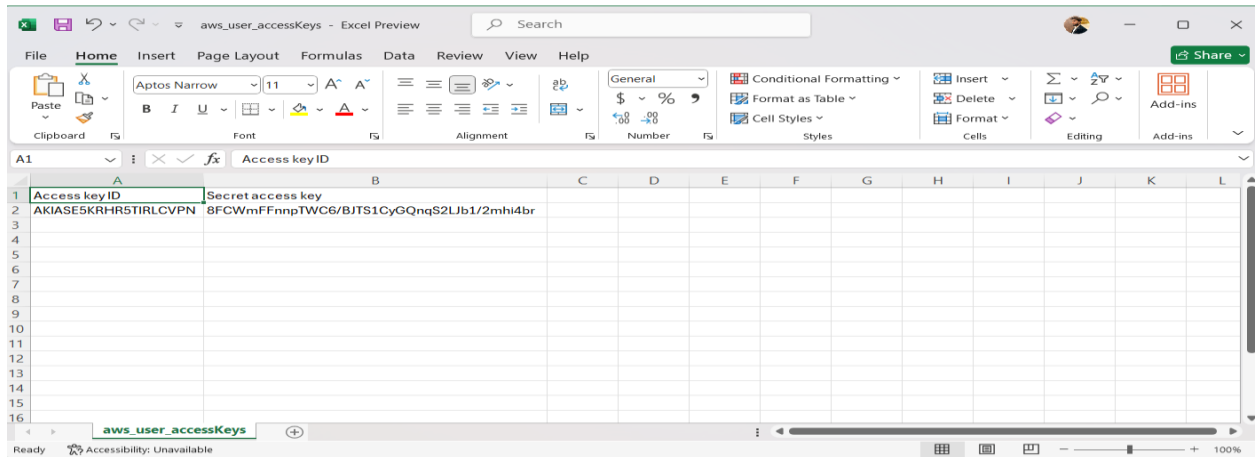
- Set description tag – *optional*

Step 3:-

- Retrieve access keys.
- Download .csv file

The screenshot shows the AWS IAM console interface for creating an access key. At the top, a green success banner reads: "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." Below this, a left-hand navigation pane shows a progress bar with three steps: "Step 1 - optional" (alternatives), "Step 2 - optional" (Set description tag), and "Step 3" (Retrieve access keys, which is the active step). The main content area is titled "Access key" and includes a warning: "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." It displays the "Access key" as AKIA5ESKRHRSTIRLCVPN and the "Secret access key" as a masked string with a "Show" link. Below this, an "Access key best practices" section lists four guidelines: never store keys in plain text or code, disable/delete keys when no longer needed, enable least-privilege permissions, and rotate keys regularly. A link to "best practices for managing AWS access keys" is provided. At the bottom right, there are two buttons: "Download .csv file" and "Done". The footer of the console shows "CloudShell", "Feedback", and copyright information for Amazon Web Services, Inc. or its affiliates, along with links for "Privacy", "Terms", and "Cookie preferences".

- Open it excel file.



-
- **Connect to the command prompt .**
- **Download AWS CLI V2 and install.**
- **Then connect cmd “aws configure.”**
- **Then used access key ID**

```

Microsoft Windows [Version 10.0.26100.2454]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Lenovo>aws configure
AWS Access Key ID [*****IR74]:
AWS Secret Access Key [*****tA6P]: 8FCWmFFnpTWC6/BJTS1CyGQnqS2LJb1/2mhi4br
Default region name [ap-south-1]:
Default output format [json]:

C:\Users\Lenovo>aws configure
AWS Access Key ID [*****IR74]: AKIA5E5KRHR5TIRLCVPM
AWS Secret Access Key [*****i4br]: 8FCWmFFnpTWC6/BJTS1CyGQnqS2LJb1/2mhi4br
Default region name [ap-south-1]:
Default output format [json]:

C:\Users\Lenovo>

```

-
- **Now connected aws user.**