AWS S3 Glacier Practical

To understand how Amazon S3 Glacier works for storing and managing data, and to practice creating a vault using three methods:

1. AWS Management Console
2. Third-party app (FastGlacier)
3. AWS Command Line Interface (CLI)

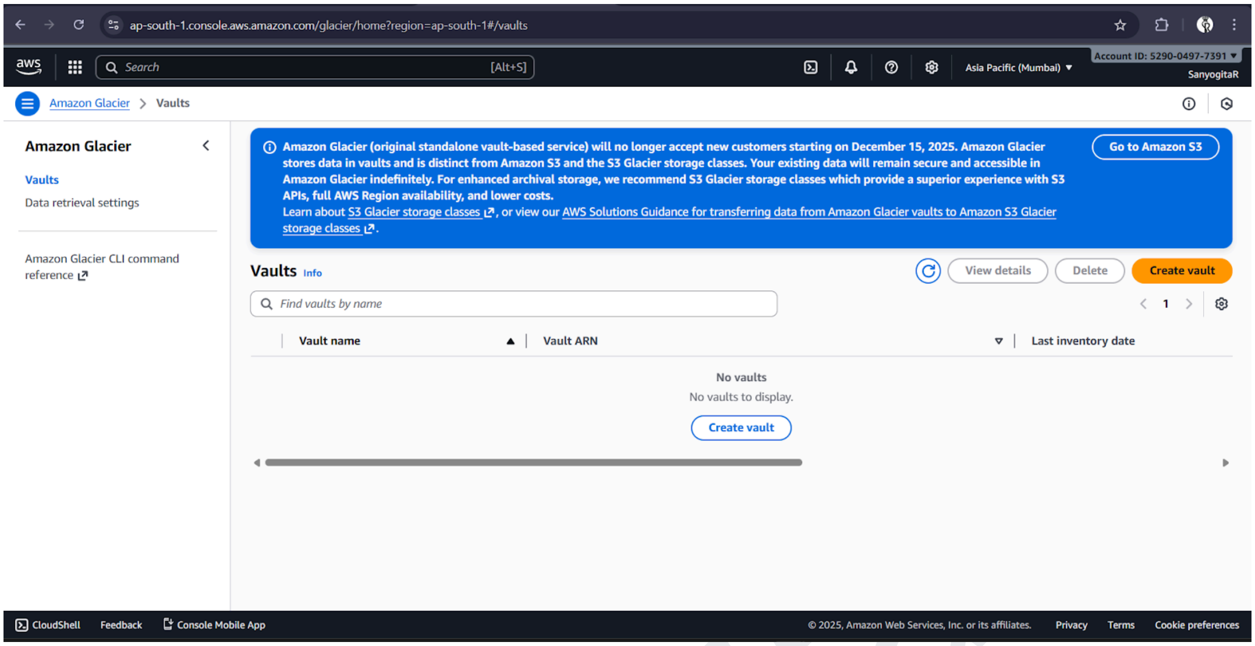
What is AWS S3 Glacier?

Amazon S3 Glacier is a **secure, low-cost storage service** from AWS used mainly for **data archiving and long-term backup**.
It’s not like normal cloud storage — it’s meant for **rarely accessed data** that you still want to keep safe.

Part 1 — Creating a Vault in AWS Console

Step-by-Step Explanation:

1. **Login to AWS Management Console** using your AWS account.



Amazon Glacier (original standalone vault-based service) will no longer accept new customers starting on December 15, 2025. Amazon Glacier stores data in vaults and is distinct from Amazon S3 and the S3 Glacier storage classes. Your existing data will remain secure and accessible in Amazon Glacier indefinitely. For enhanced archival storage, we recommend S3 Glacier storage classes which provide a superior experience with S3 APIs, full AWS Region availability, and lower costs.
Learn about S3 Glacier storage classes, or view our AWS Solutions Guidance for transferring data from Amazon Glacier vaults to Amazon S3 Glacier storage classes.

No vaults
No vaults to display.

2. From the services menu, search and open **Amazon S3 Glacier** (sometimes listed under “Storage”).

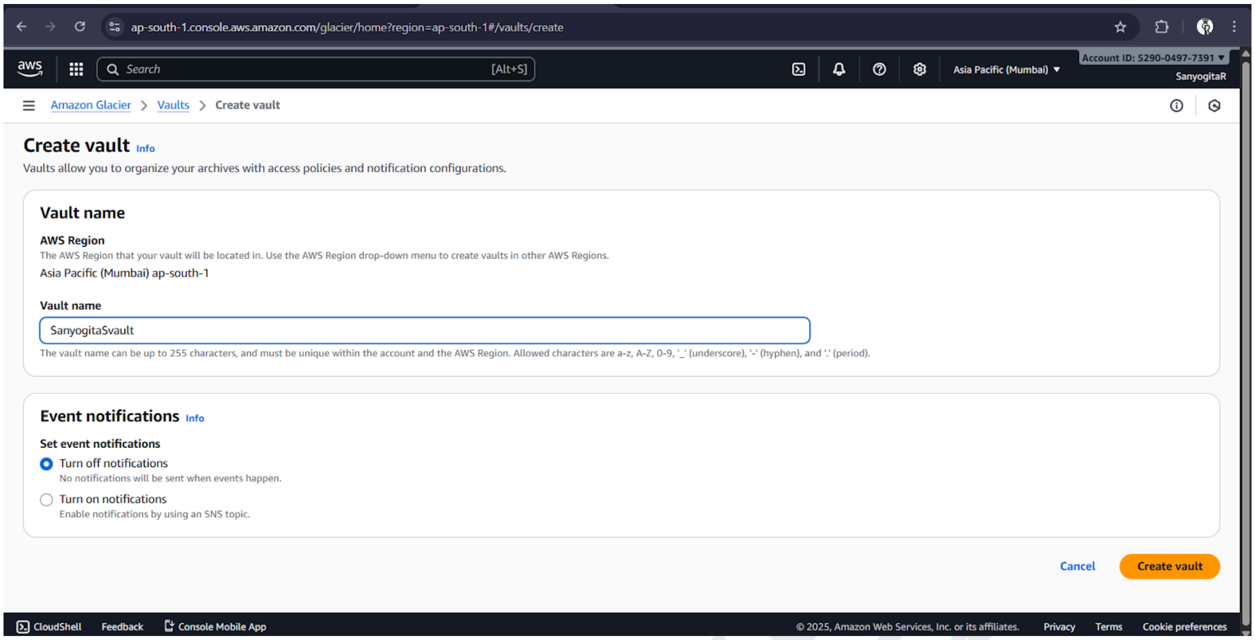
3. Click **Create Vault**.

4. Choose:

    - A **region** (for example, `ap-south-1` for Mumbai)

    - A **vault name** (e.g., `my-first-vault`)

5. Click **Create Vault** to confirm.


ap-south-1.console.aws.amazon.com/glacier/home?region=ap-south-1#/vaults/create
Search [Alt+S]
Asia Pacific (Mumbai)
Account ID: 5290-0497-7391
SanyogitaR
Amazon Glacier > Vaults > Create vault
Cancel
Create vault
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Create vault Info

Vaults allow you to organize your archives with access policies and notification configurations.

Vault name

AWS Region

The AWS Region that your vault will be located in. Use the AWS Region drop-down menu to create vaults in other AWS Regions.

Asia Pacific (Mumbai) ap-south-1

Vault name

SanyogitaSvault

The vault name can be up to 255 characters, and must be unique within the account and the AWS Region. Allowed characters are a-z, A-Z, 0-9, '_' (underscore), '-' (hyphen), and '.' (period).

Event notifications Info

Set event notifications

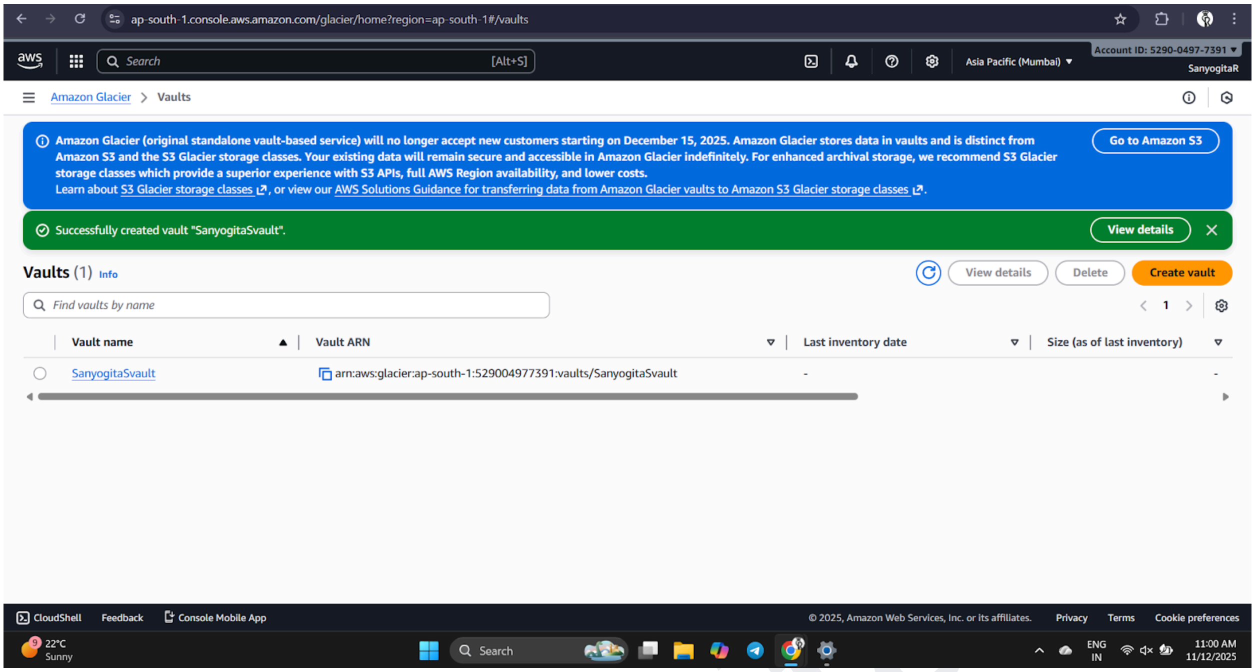
● Turn off notifications
No notifications will be sent when events happen.

○ Turn on notifications
Enable notifications by using an SNS topic.

Now AWS will create your vault and show details like:

- Vault Name
- Vault ARN (Amazon Resource Name)
- Creation Date and Region

📝 **Note:** You can only delete a vault when it’s completely empty (no files inside).



Amazon Glacier (original standalone vault-based service) will no longer accept new customers starting on December 15, 2025. Amazon Glacier stores data in vaults and is distinct from Amazon S3 and the S3 Glacier storage classes. Your existing data will remain secure and accessible in Amazon Glacier indefinitely. For enhanced archival storage, we recommend S3 Glacier storage classes which provide a superior experience with S3 APIs, full AWS Region availability, and lower costs.
Learn about S3 Glacier storage classes, or view our AWS Solutions Guidance for transferring data from Amazon Glacier vaults to Amazon S3 Glacier storage classes.

Successfully created vault "SanyogitaSvault".

Vaults (1) Info

	Vault name	Vault ARN	Last inventory date	Size (as of last inventory)
○	SanyogitaSvault	arn:aws:glacier:ap-south-1:529004977391:vaults/SanyogitaSvault	-	-

Part 2 — Connecting via FastGlacier (Third-Party App)

What is FastGlacier?

FastGlacier is a Windows application that helps you manage Amazon Glacier vaults easily — like a file manager for Glacier.

Steps I Followed:

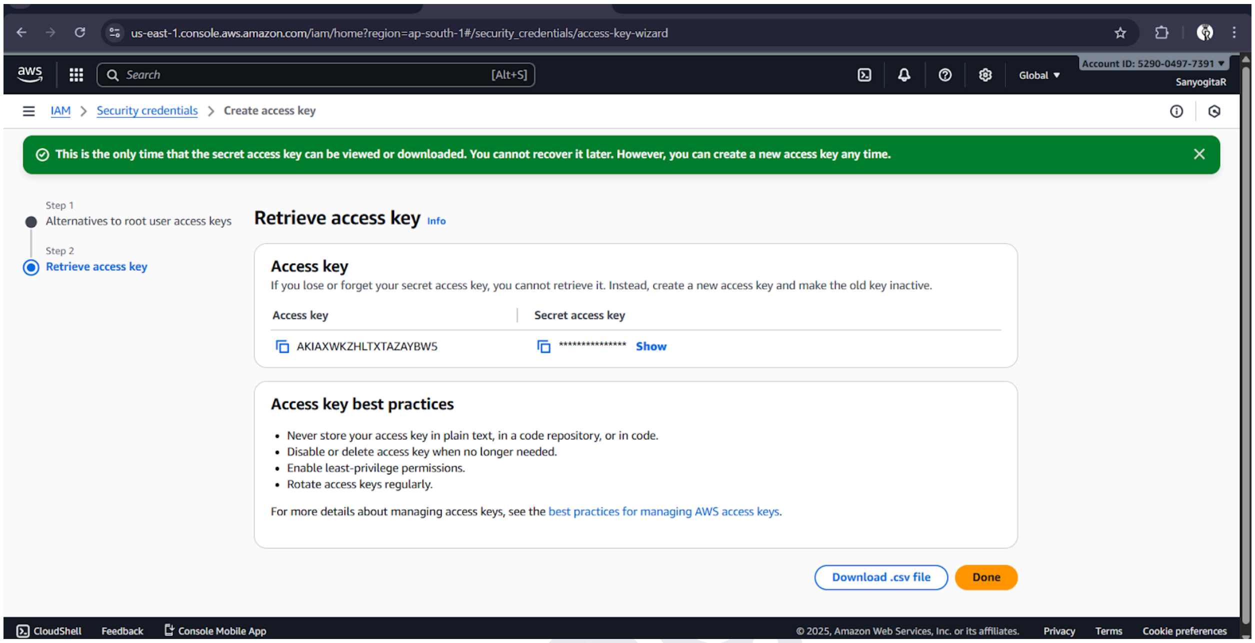
1. Opened the **AWS Management Console** → went to **IAM (Identity and Access Management)**.

2. Clicked **Add User** and created a new IAM user named `fastglacier-user`.

3. Gave **Programmatic Access** so I could get an **Access Key ID** and **Secret Access Key**.

4. Attached a policy like `AmazonGlacierFullAccess` (for testing).

5. Copied the Access Key ID and Secret Key (⚠️ never share or upload these keys).



us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/security_credentials/access-key-wizard
aws
Search [Alt+S]
Global ▾
Account ID: 5290-0497-7391 ▾
SanyogitaR
IAM > Security credentials > Create access key
Step 1
Alternatives to root user access keys
Step 2
Retrieve access key
Info
Download .csv file
Done
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

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.

Retrieve access key

Access key

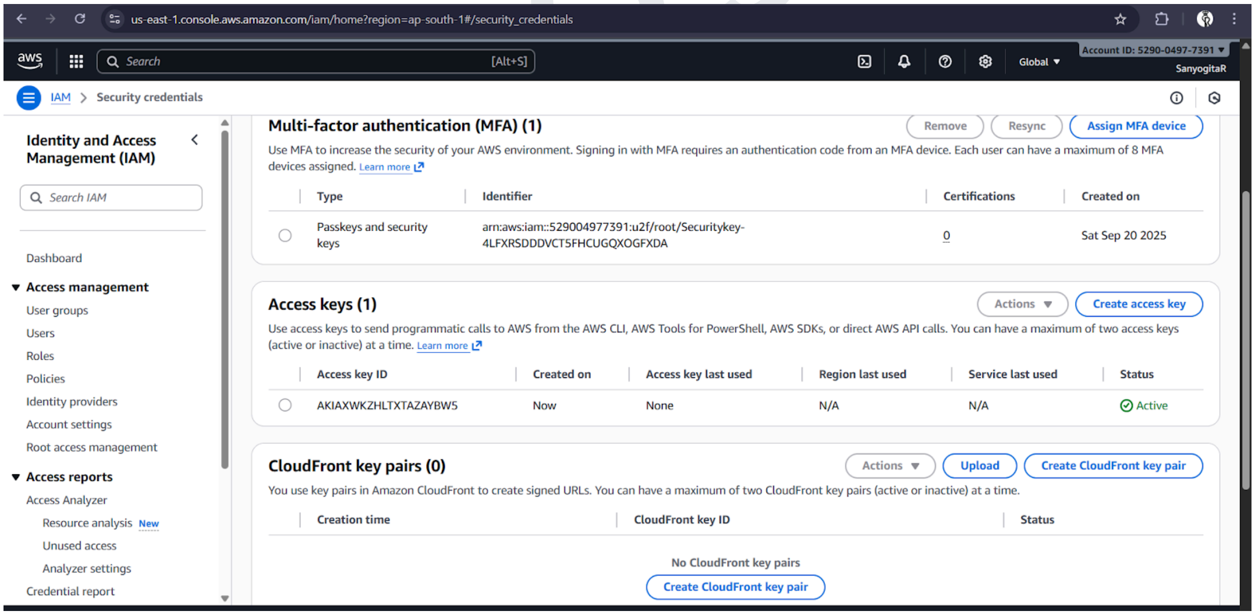
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIAXWKZHLTXTAZAYBW5	*************** 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.



Multi-factor authentication (MFA) (1)

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

	Type	Identifier	Certifications	Created on
○	Passkeys and security keys	arn:aws:iam::529004977391:u2f/root/Securitykey-4LFXRSDDDVCT5FHCUGQXOGFXDA	0	Sat Sep 20 2025

Access keys (1)

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

	Access key ID	Created on	Access key last used	Region last used	Service last used	Status
○	AKIAXWKZHLTXTAZAYBW5	Now	None	N/A	N/A	✓ Active

CloudFront key pairs (0)

You use key pairs in Amazon CloudFront to create signed URLs. You can have a maximum of two CloudFront key pairs (active or inactive) at a time.

Creation time	CloudFront key ID	Status

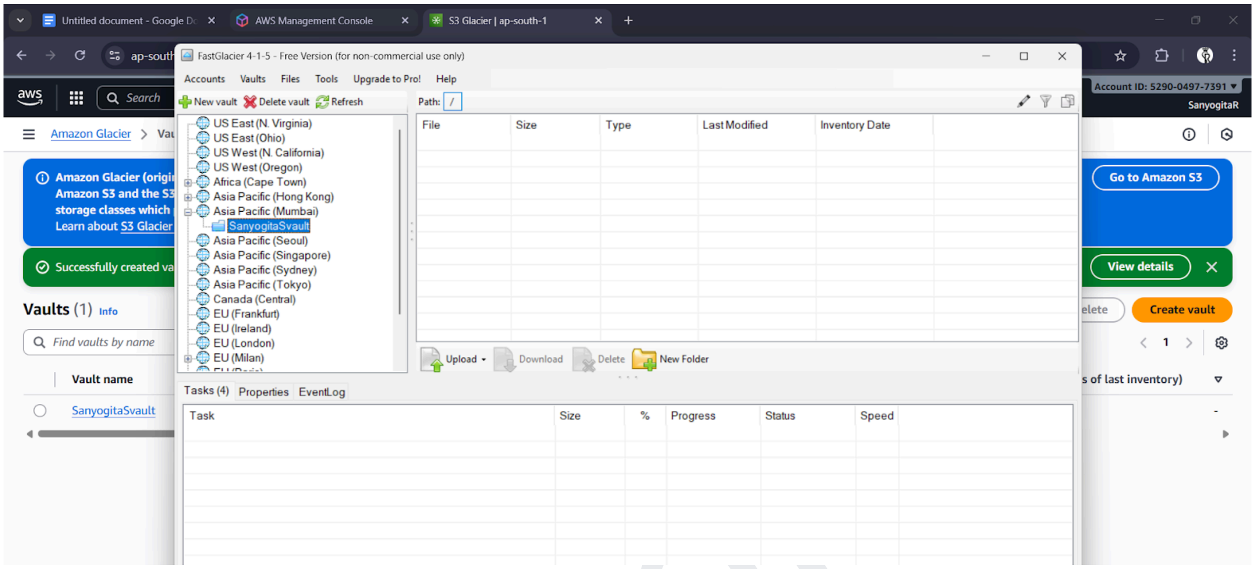
No CloudFront key pairs

Then, in **FastGlacier:**

1. Opened the app and clicked **Add New Account**.

2. Entered the Access Key ID, Secret Key, and selected the correct AWS region.

3. Connected successfully — it showed the vaults from my AWS account.



4. Uploaded a small test file to the vault to check the connection.

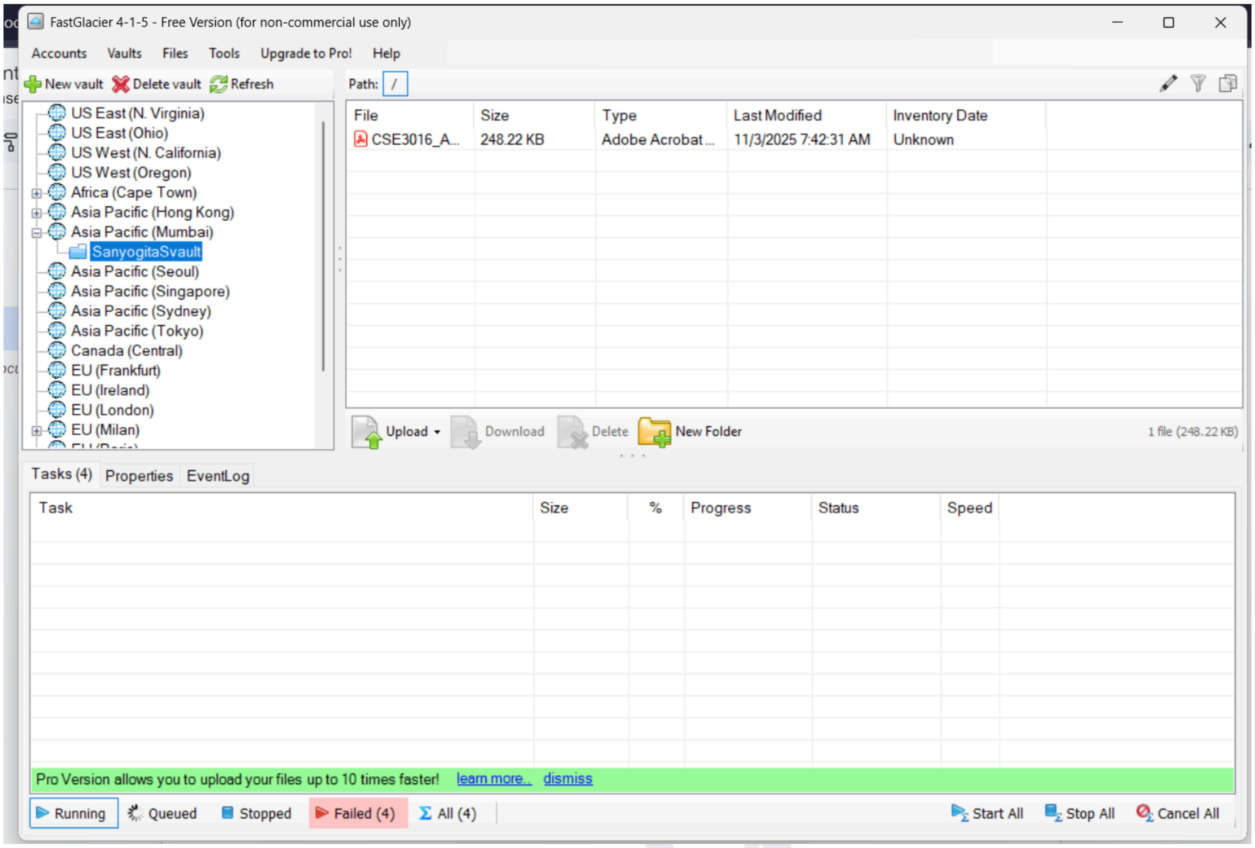
5. Deleted the file later to avoid storage costs.

⚠️ Security Tip:

- Logging out of FastGlacier does **not** remove AWS access.

- You must **delete or deactivate the IAM access key** from the AWS Console to fully disconnect it.

- After the experiment, go to **IAM** → **Users** → **Security Credentials** → **Access Keys** → **Delete**.



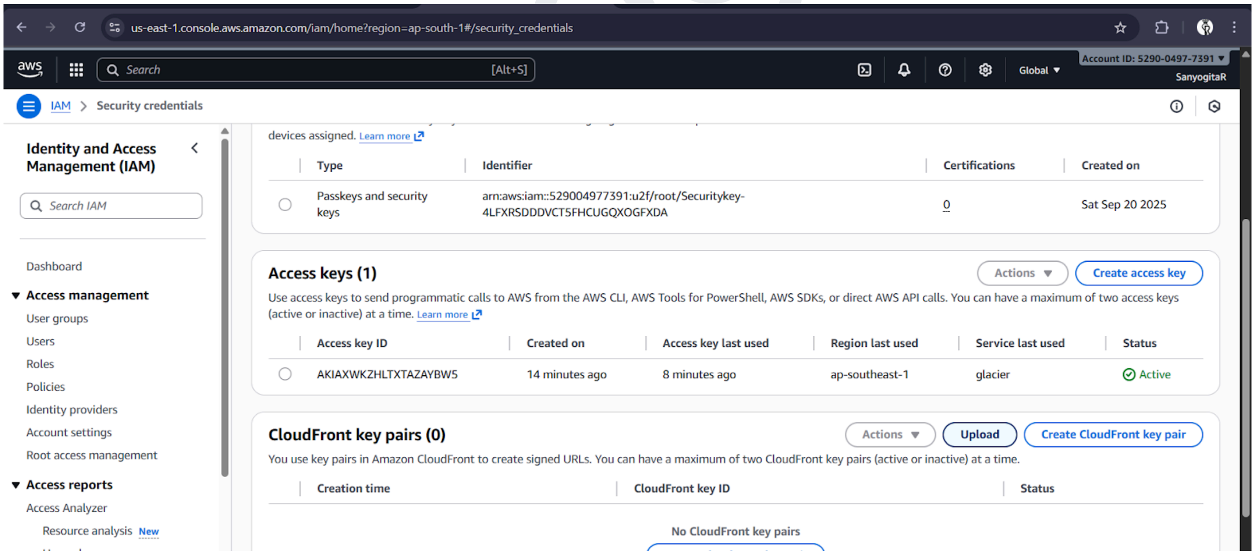
FastGlacier 4-1-5 - Free Version (for non-commercial use only)

File	Size	Type	Last Modified	Inventory Date
CSE3016_A...	248.22 KB	Adobe Acrobat ...	11/3/2025 7:42:31 AM	Unknown

1 file (248.22 KB)

Task	Size	%	Progress	Status	Speed

Pro Version allows you to upload your files up to 10 times faster! learn more... dismiss



us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/security_credentials

devices assigned. Learn more

Type	Identifier	Certifications	Created on
Passkeys and security keys	arn:aws:iam::529004977391:u2f/root/Securitykey-4LFXRSDDDVCT5FHCUGQXOGFXDA	0	Sat Sep 20 2025

Access keys (1)

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

Access key ID	Created on	Access key last used	Region last used	Service last used	Status
AKIAXWKZHLTXTAZAYBW5	14 minutes ago	8 minutes ago	ap-southeast-1	glacier	Active

CloudFront key pairs (0)

You use key pairs in Amazon CloudFront to create signed URLs. You can have a maximum of two CloudFront key pairs (active or inactive) at a time.

Creation time	CloudFront key ID	Status

No CloudFront key pairs

Part 3 — Using AWS CLI (Command Line Interface)

The AWS CLI allows you to manage Glacier directly through commands.

Steps I Performed:

1. **Opened Command Prompt** on my system.

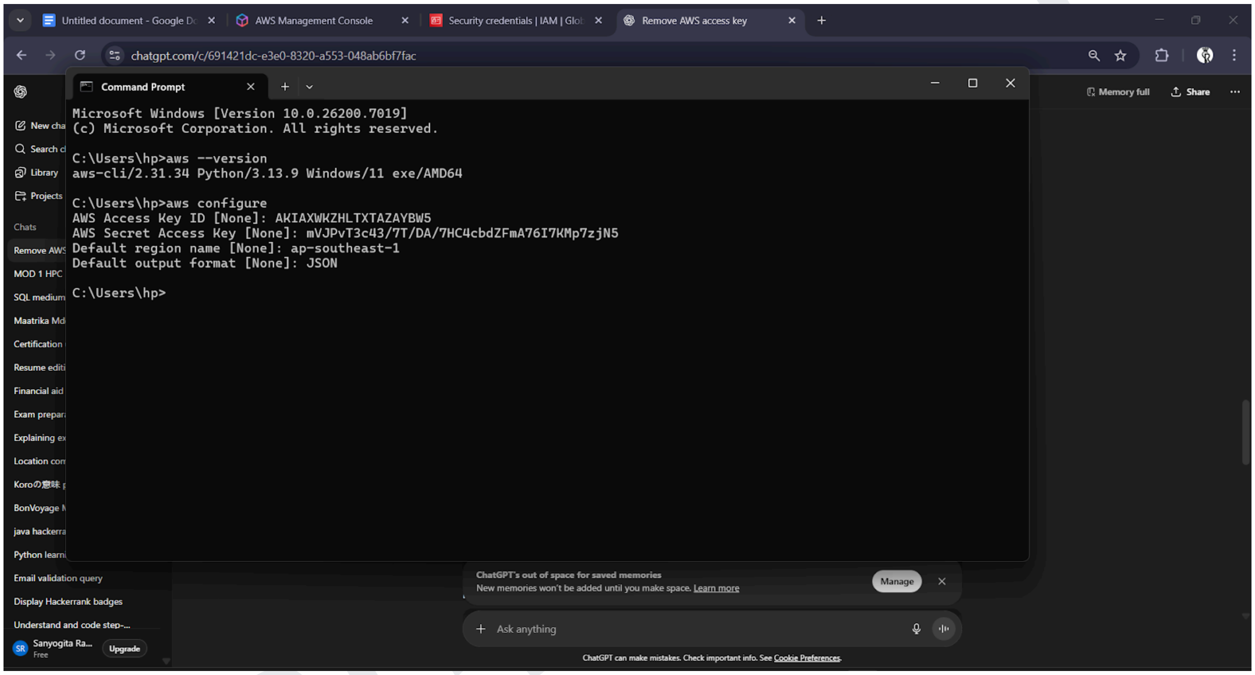
Checked that AWS CLI was installed:

```
aws --version
```

2.

Configured my AWS credentials:

```
aws configure
```



```
Microsoft Windows [Version 10.0.26200.7019]
(c) Microsoft Corporation. All rights reserved.

C:\Users\hp>aws --version
aws-cli/2.31.34 Python/3.13.9 Windows/11 exe/AMD64

C:\Users\hp>aws configure
AWS Access Key ID [None]: AKIAXWKZHLTXTAZAYBW5
AWS Secret Access Key [None]: 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
Default region name [None]: ap-southeast-1
Default output format [None]: JSON

C:\Users\hp>
```

ChatGPT's out of space for saved memories
New memories won't be added until you make space. Learn more

ChatGPT can make mistakes. Check important info. See Cookie Preferences.

3. Then entered:
   - Access Key ID
   - Secret Access Key
   - Default region (e.g., `ap-south-1`)
   - Output format (kept as JSON)

Created a new vault using:

```
aws glacier create-vault --account-id - --vault-name my-cli-vault
--region ap-south-1
```

4. ✔️ This command created a vault directly from the terminal.

Listed all vaults to verify:

```
aws glacier list-vaults --account-id - --region ap-south-1
```

5.

Described the specific vault to check details:

```
aws glacier describe-vault --account-id - --vault-name my-cli-vault
--region ap-south-1
```

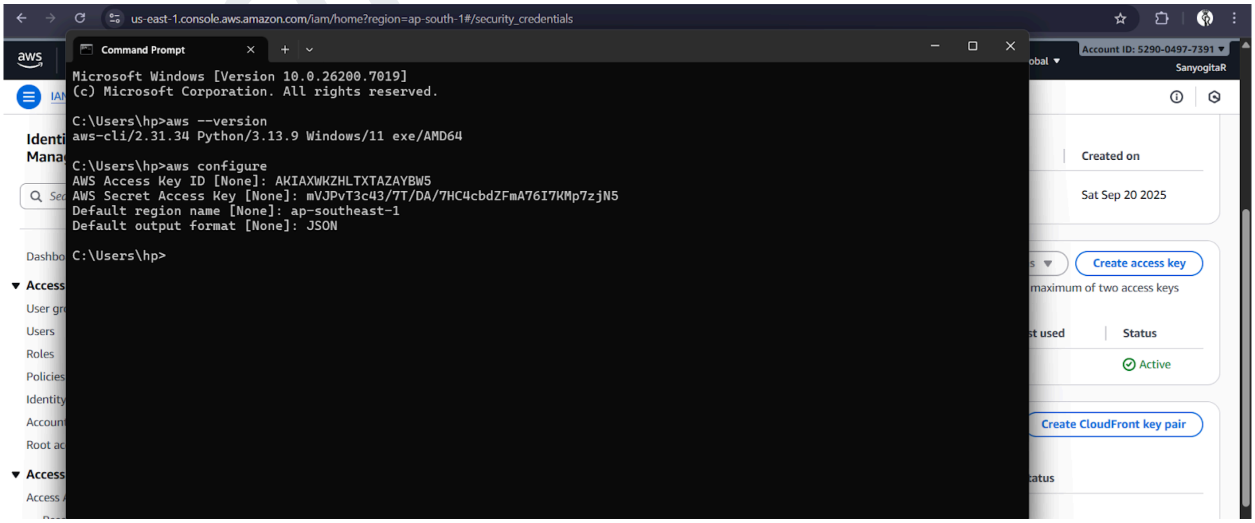
6.

(Optional) Uploaded a small test file:

```
aws glacier upload-archive --account-id - --vault-name my-cli-vault
--body test.txt --region ap-south-1
```

7.
8. Later, deleted the uploaded file to avoid charges and tested vault deletion using:

   ```
   aws glacier delete-vault --account-id - --vault-name my-cli-vault
   --region ap-south-1
   ```


us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/security_credentials
Command Prompt
aws
Account ID: 5290-0497-7391 ▾
SanyogitaR
Created on
Sat Sep 20 2025
Create access key
maximum of two access keys
Status
Active
Create CloudFront key pair

```
Microsoft Windows [Version 10.0.26200.7019]
(c) Microsoft Corporation. All rights reserved.

C:\Users\hp>aws --version
aws-cli/2.31.34 Python/3.13.9 Windows/11 exe/AMD64

C:\Users\hp>aws configure
AWS Access Key ID [None]: AKIAXWKZHLTXTAZAYBW5
AWS Secret Access Key [None]: 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
Default region name [None]: ap-southeast-1
Default output format [None]: JSON

C:\Users\hp>
```