

All AWS Regions

## General purpose buckets (1) [Info](#)

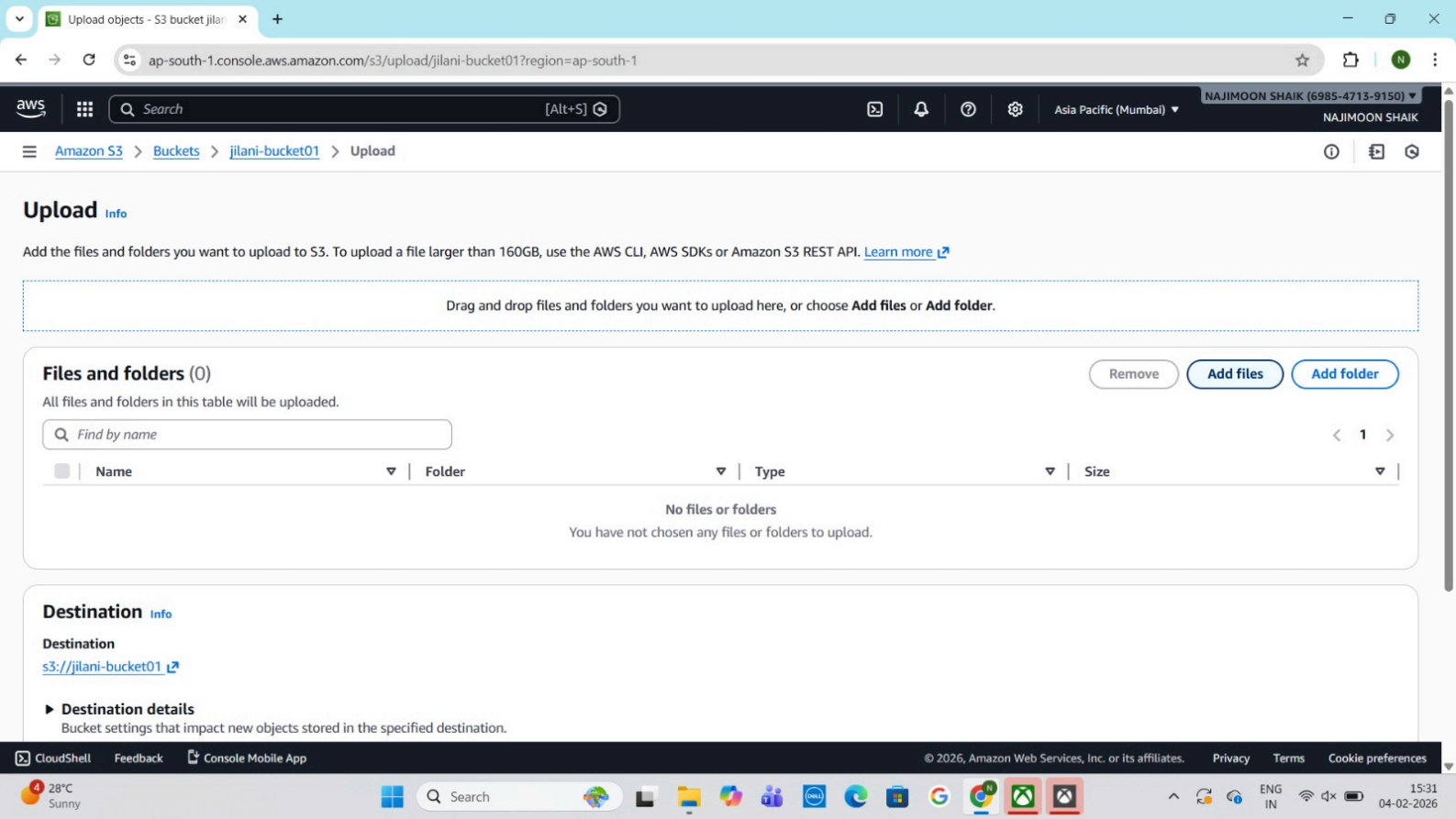
🔍 Find buckets by name

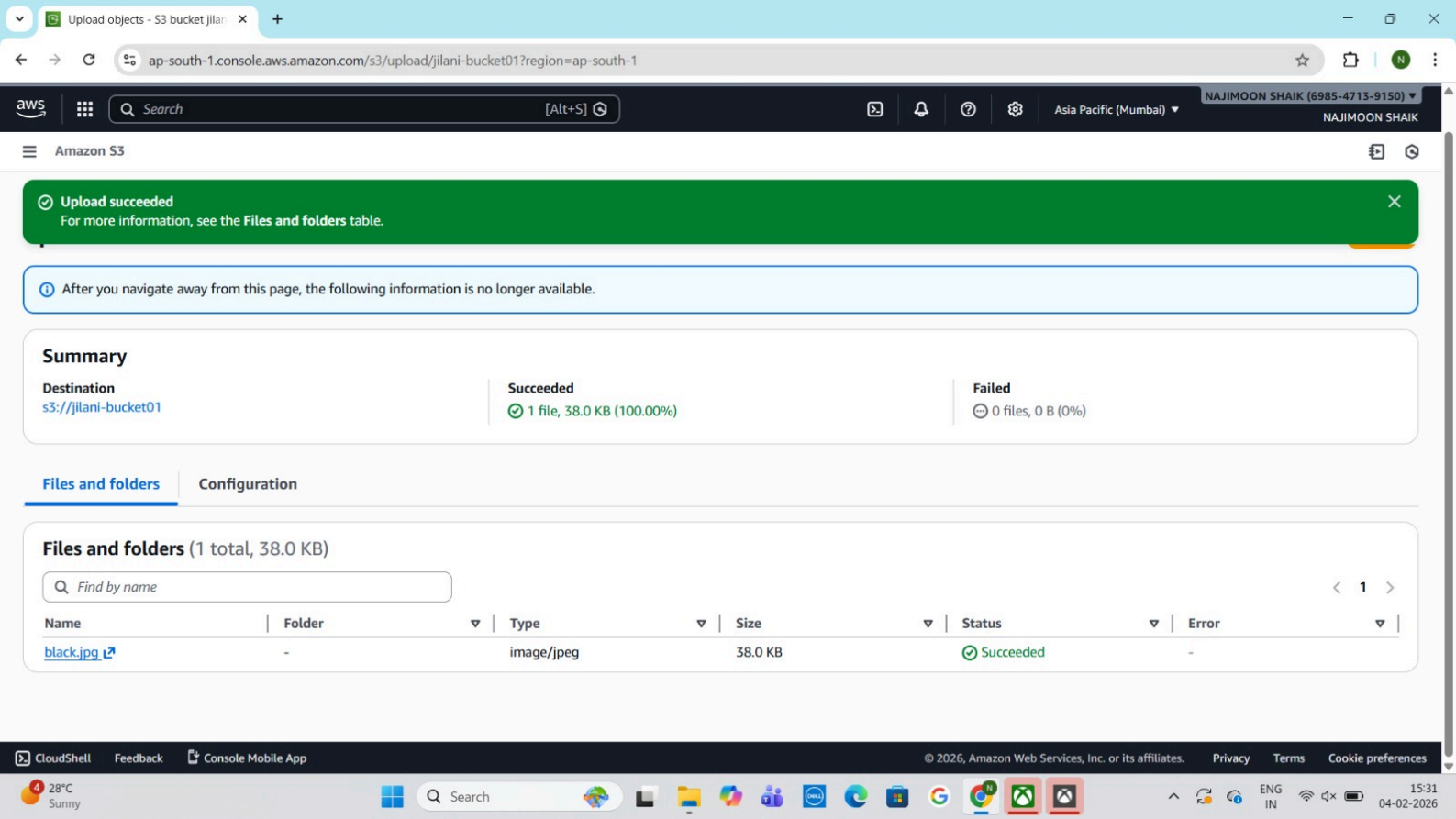
► **Account snapshot** [Info](#)

Storage Lens provides visibility into storage usage and activity trends.

## Updated daily

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.





Browser tabs: jilani-bucket01 - S3 bucket | S3, jilani-bucket01.s3.ap-south-1.amazonaws.com/black.jpg

Address bar: south-1.amazonaws.com/black.jpg

Page content: style information associated with it. The document tree is shown below.

Document tree snippet: <HostId>10vxxXU8fk3qFuRTmUe1hs0Tb5KvBI08sH72vHgPpceq/3hn+cgJcuuNsGsLuCe0iDAkp</HostId>

Taskbar: Memory usage: 675 MB

## jilani-bucket01 Info

Objects	Metadata	Properties	Permissions
---------	----------	------------	-------------

### Objects (1/1)

<input checked="" type="checkbox"/>	Name	Type
-------------------------------------	------	------

☒  black.jpg jpg

Share "black.jpg" with a presigned URL

Presigned URLs are used to grant access to an object for a limited time. [Learn more](#)

- ❗ Anyone can access the object with this presigned URL until it expires, even if the bucket, and object are private.

## Time interval until the presigned URL expires

Using the S3 console, you can share an object with a presigned URL for up to 12 hours or until your session expires. To create a presigned URL with a longer time interval, use the AWS CLI or AWS SDK. Time intervals for presigned URLs can be restricted by your IAM policy.

 Minutes

☐ Hours

## Number of minutes

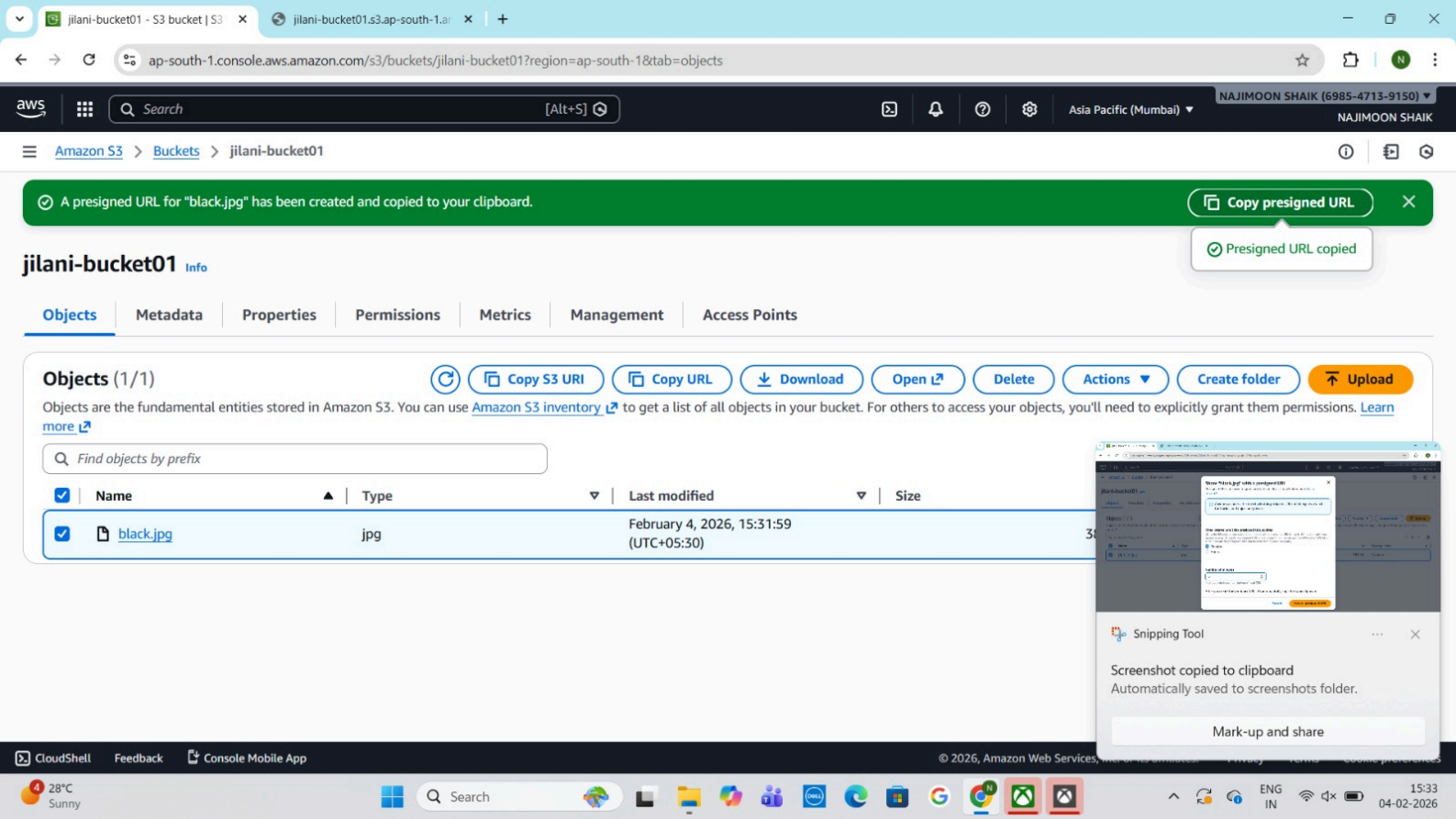
5

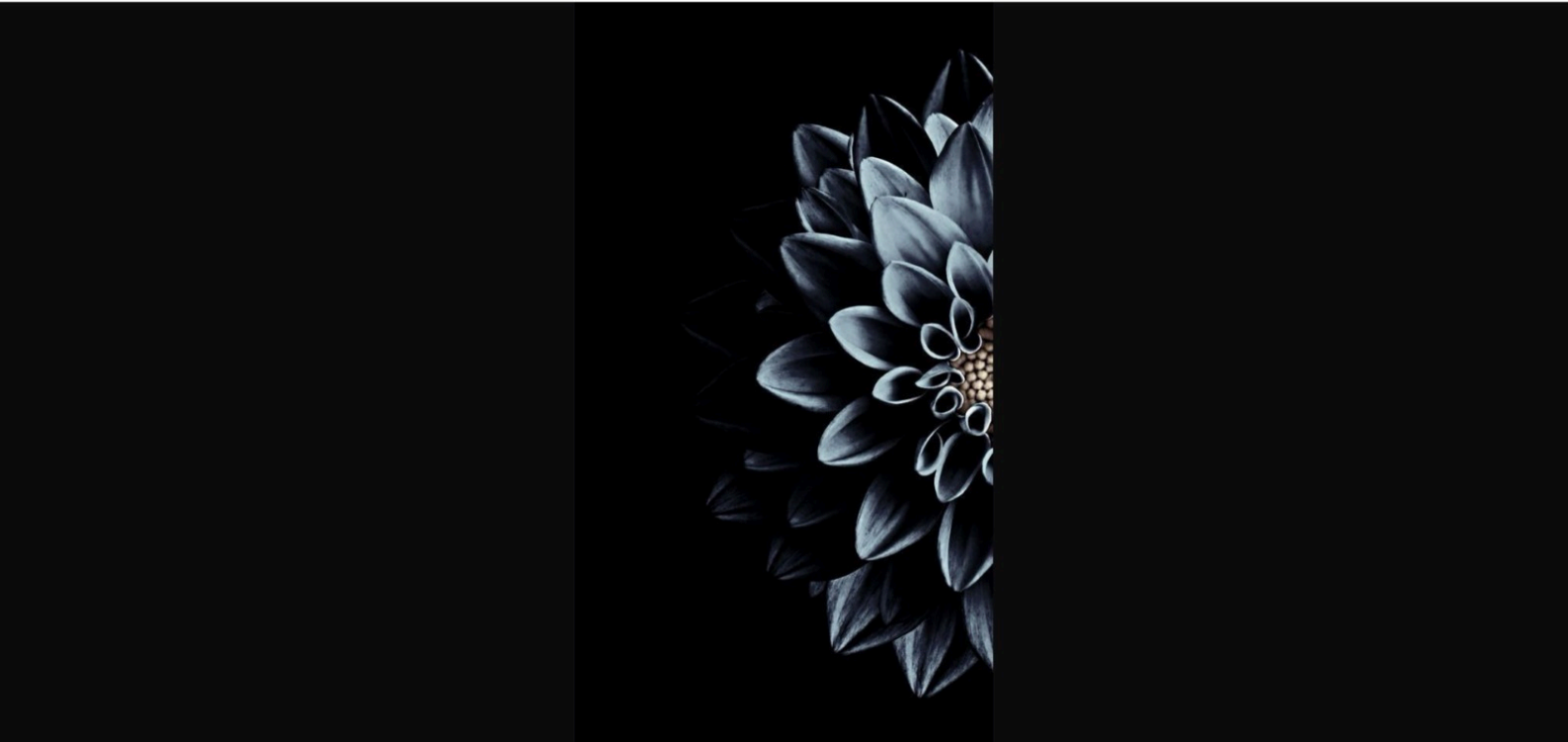
Must be a whole number between 1 and 720.

After you create the presigned URL, it's automatically copied to your clipboard.

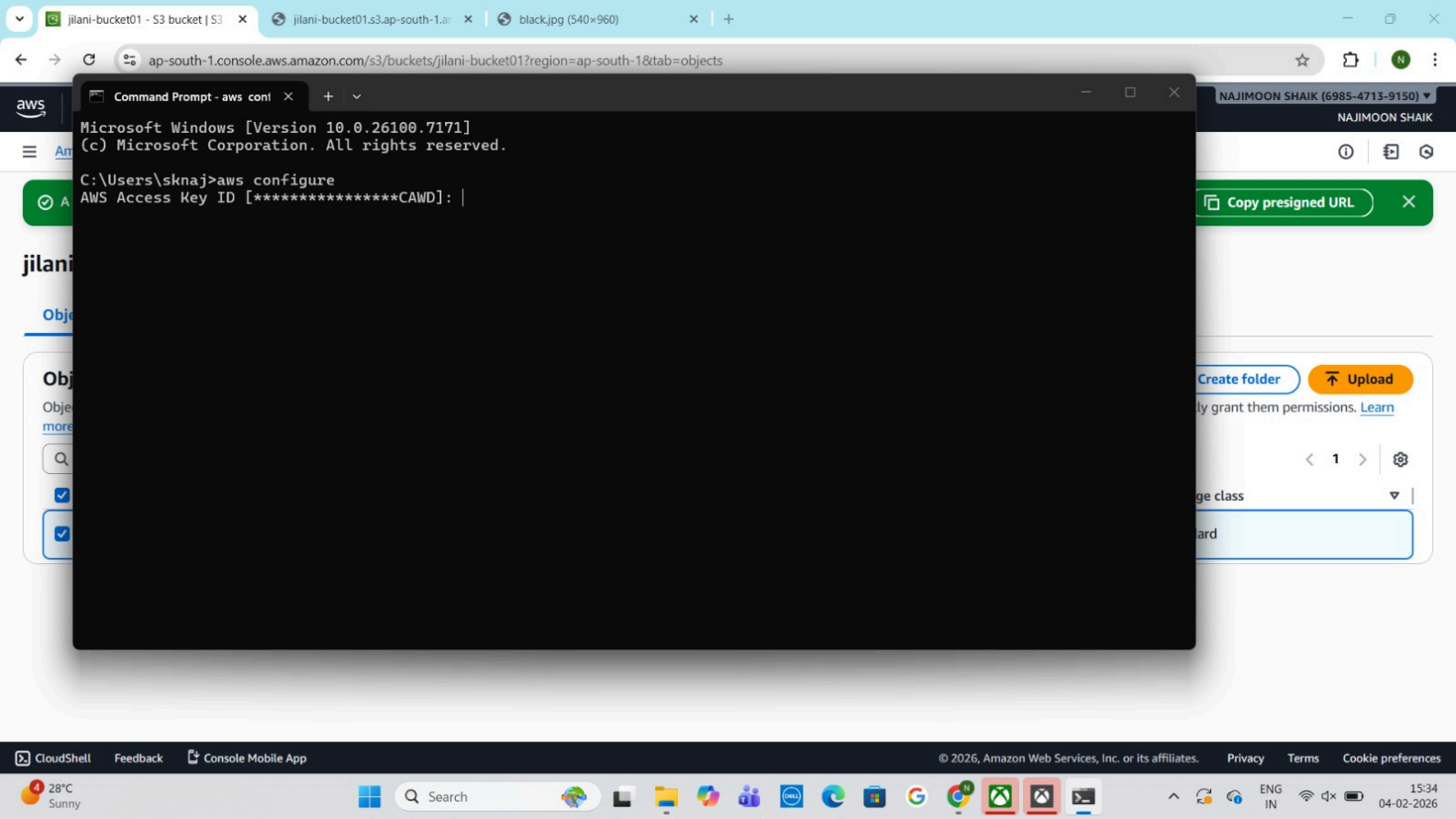
Cancel

Create presigned URL









## Identity and Access Management (IAM)

Q Search IAM

Dashboard

### ▼ Access Management

### User groups

Users

## Roles

## Policies

### Identity providers

Account settings

### Root access management

### Temporary delegation requests

New

## ▼ Access reports

Access Analyzer

Resource analysis **New**


Unused access

### Account details

Account name

NAJIMOON SHAIK


**AWS account ID**

 698547139150

Email address

sknajimoon143@gmail.com

Canonical user ID

 a70b7829e4e60d59011ec3f89879096a3d3f0add71e65fde860dbcd054281375

Actions ▼

### 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](#)

Remove

Resync

### Assign MFA device

Type	Identifier	Certifications	Created on
Virtual	arn:aws:iam:698547139150:mfa/najimoon	Not Applicable	Tue Jan 20 2026

### Access keys (0)

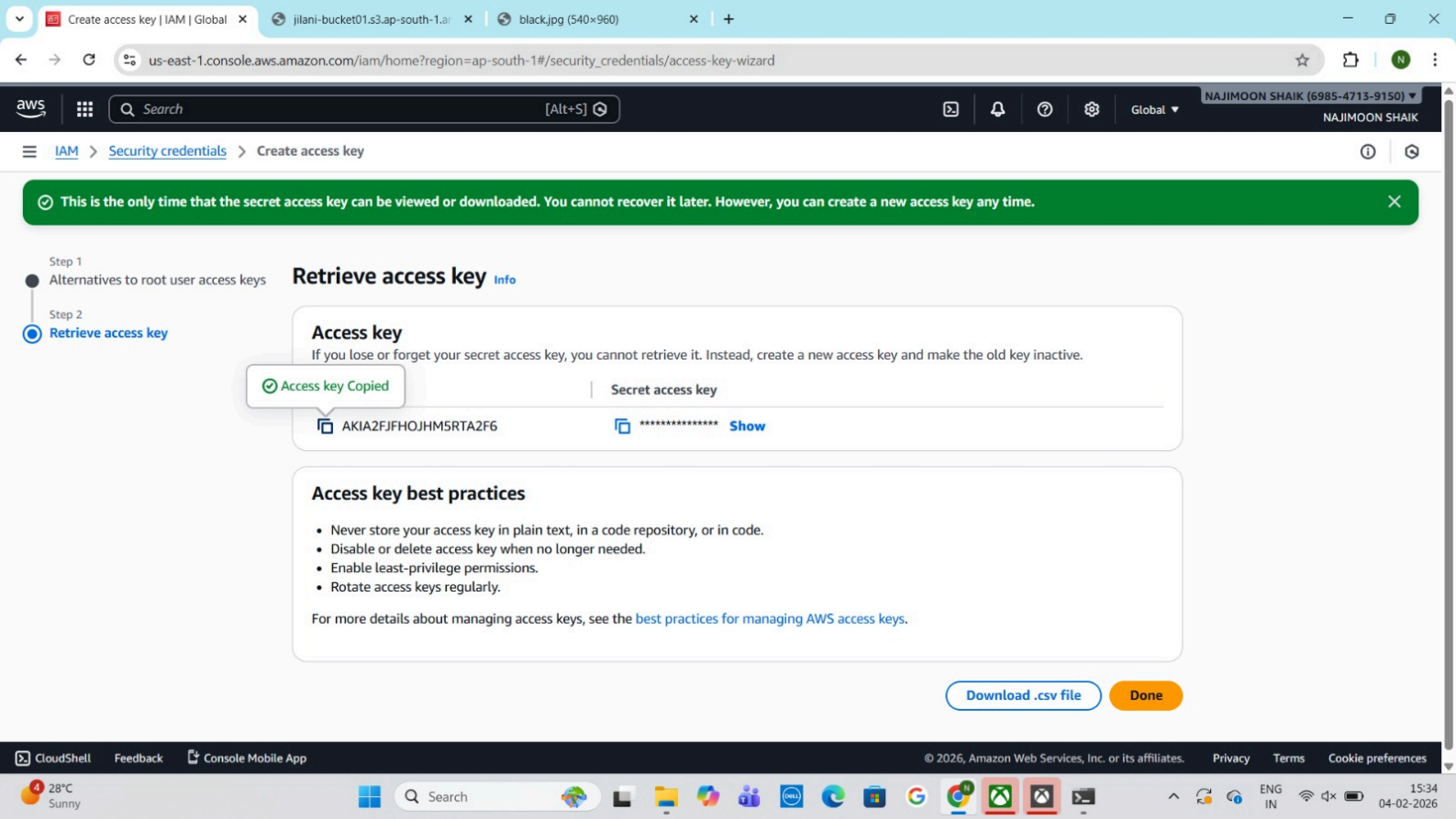
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

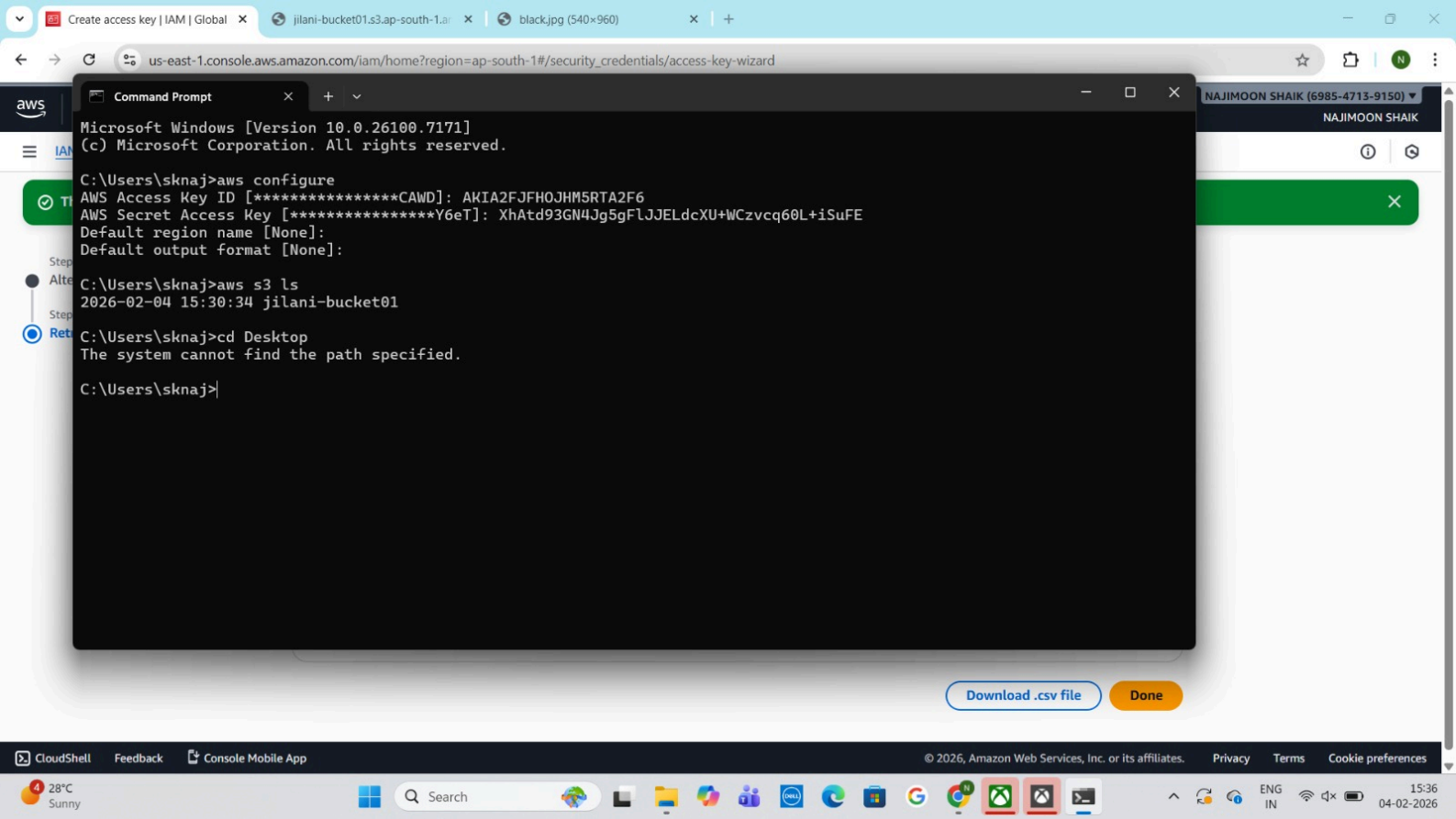
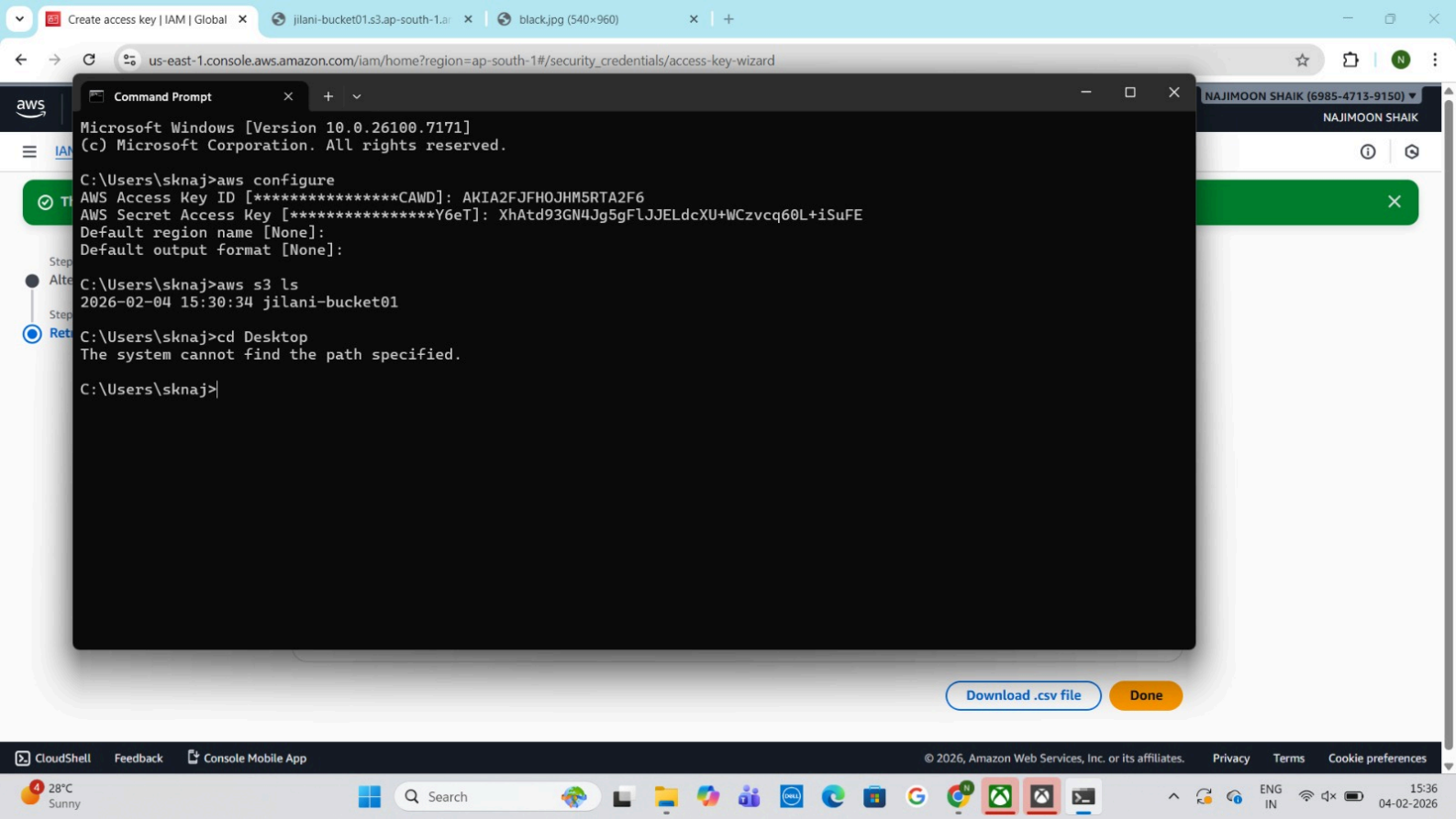
### Create access key

Access key ID	Created on	Access key last used	Region last used	Service last used	Status
---------------	------------	----------------------	------------------	-------------------	--------

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](#)





```
C:\Users\sknaj>cd onedrive\desktop

C:\Users\sknaj\OneDrive\Desktop>aws s3 ls
2026-02-04 15:30:34 jilani-bucket01

C:\Users\sknaj\OneDrive\Desktop>cd ansbile
The system cannot find the path specified.

C:\Users\sknaj\OneDrive\Desktop>mkdir ansbile

C:\Users\sknaj\OneDrive\Desktop>cd ansbile

C:\Users\sknaj\OneDrive\Desktop\ansbile>aws cps3://jilani-bucket01/black.jpg black.jpg

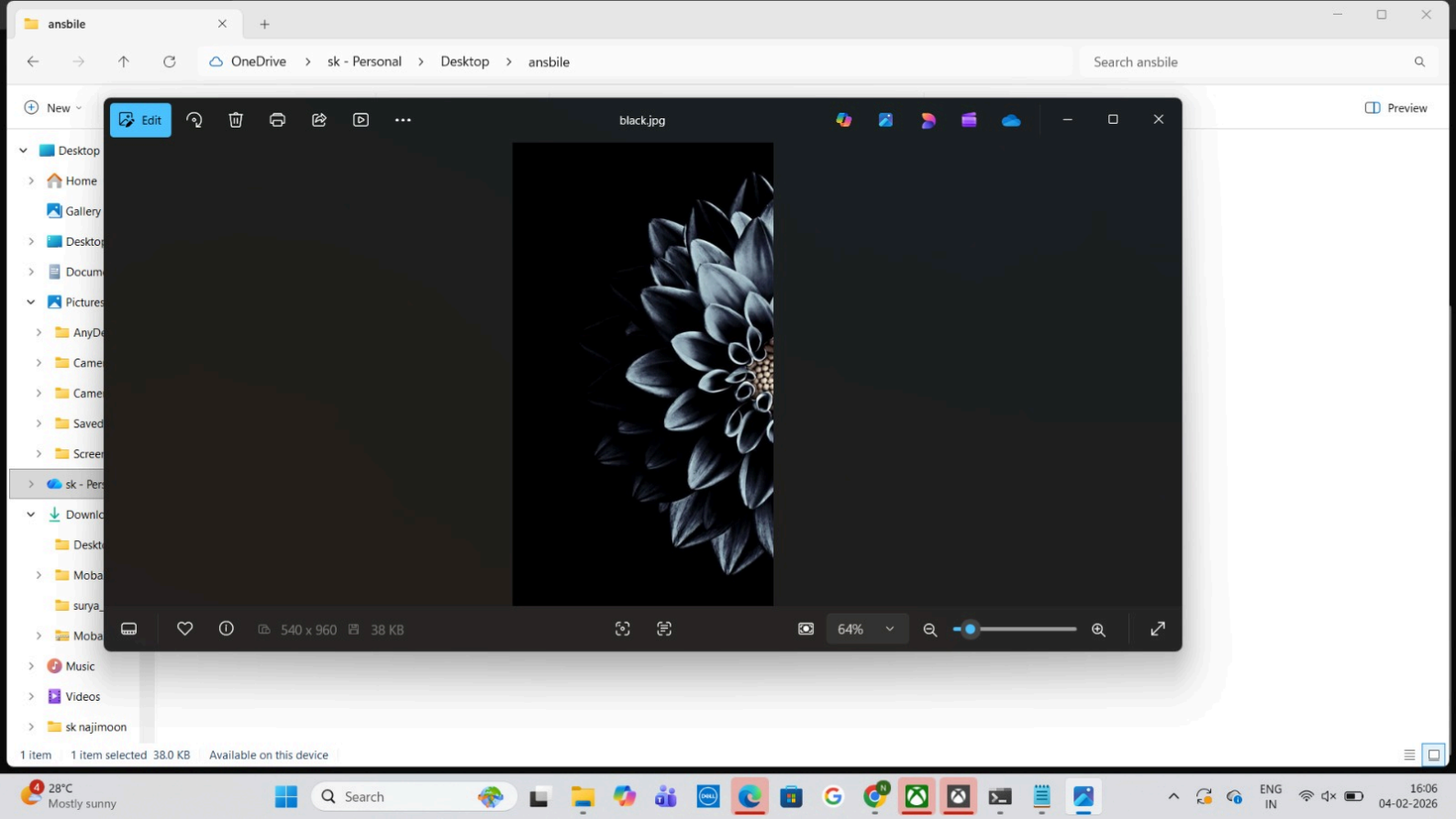
aws: [ERROR]: argument command: Found invalid choice 'cps3://jilani-bucket01/black.jpg'

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

aws help
aws <command> help
aws <command> <subcommand> help

C:\Users\sknaj\OneDrive\Desktop\ansbile>aws s3 cp s3://jilani-bucket01/black.jpg black.jpg
download: s3://jilani-bucket01/black.jpg to .\black.jpg

C:\Users\sknaj\OneDrive\Desktop\ansbile>
```



ap-south-1.console.aws.amazon.com/s3/buckets/jilani-bucket01?region=ap-south-1&tab=permissions

aws

Search

[Alt+S]

Asia Pacific (Mumbai)

NAJIMOON SHAIK (6985-4713-9150)

NAJIMOON SHAIK

Amazon S3

Buckets

jilani-bucket01

Amazon S3

Buckets

jilani-bucket01

General purpose buckets

Directory buckets

Table buckets

Vector buckets

Access management and security

Access Points

Access Points for FSx

Access Grants

IAM Access Analyzer

Storage management and insights

Storage Lens

Batch Operations

Account and organization settings

AWS Marketplace for S3

jilani-bucket01

Info

ObjectsMetadataPropertiesPermissionsMetricsManagementAccess Points

Permissions overview

Access finding

Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#)

[View analyzer for ap-south-1](#)

Block public access (bucket settings)

Edit

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

On

Individual Block Public Access settings for this bucket

Bucket policy

EditDelete

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

CloudShell

Feedback

Console Mobile App

© 2026, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

4

Search

Windows Taskbar Icons

16:07 04-02-2026



## Amazon S3

## ▼ Buckets

### General purpose buckets

## Directory buckets

### Table buckets

## Vector buckets

### ▼ Access management and security

## Access Points

### Access Points for FSx

## Access Grants

IAM Access Analyzer

### ▼ Storage management and insights

## Storage Lens

## Batch Operations

Account and organization settings

- ▶ AWS Marketplace for S3

### Edit Block public access (bucket settings) [Info](#)

### Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

- ☐ **Block *all* public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
  - ☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
  - ☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**

S3 will ignore all ACLs that grant public access to buckets and objects.
  - ☐ **Block public access to buckets and objects granted through *new* public bucket or access point policies**

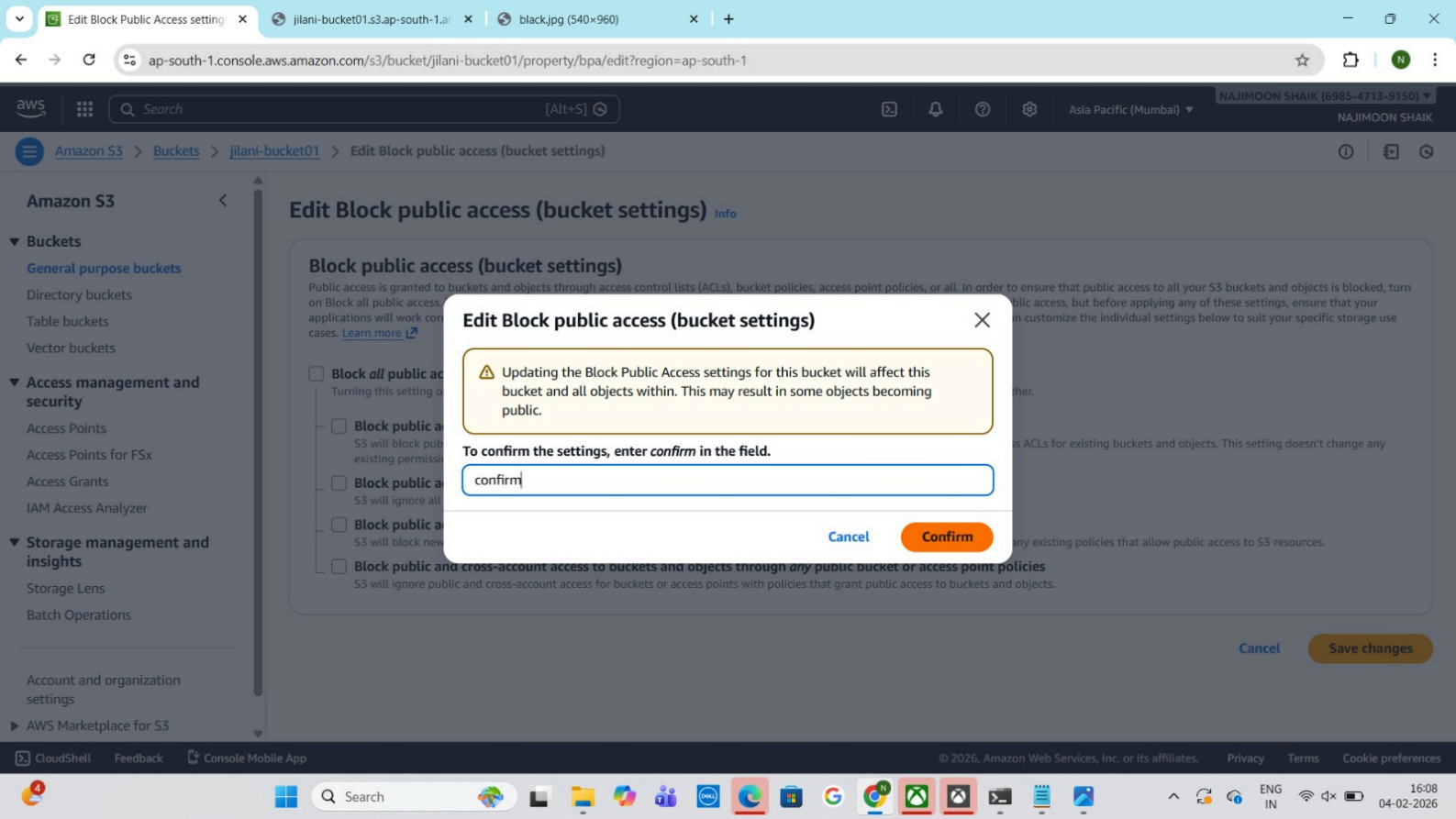
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
  - ☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**

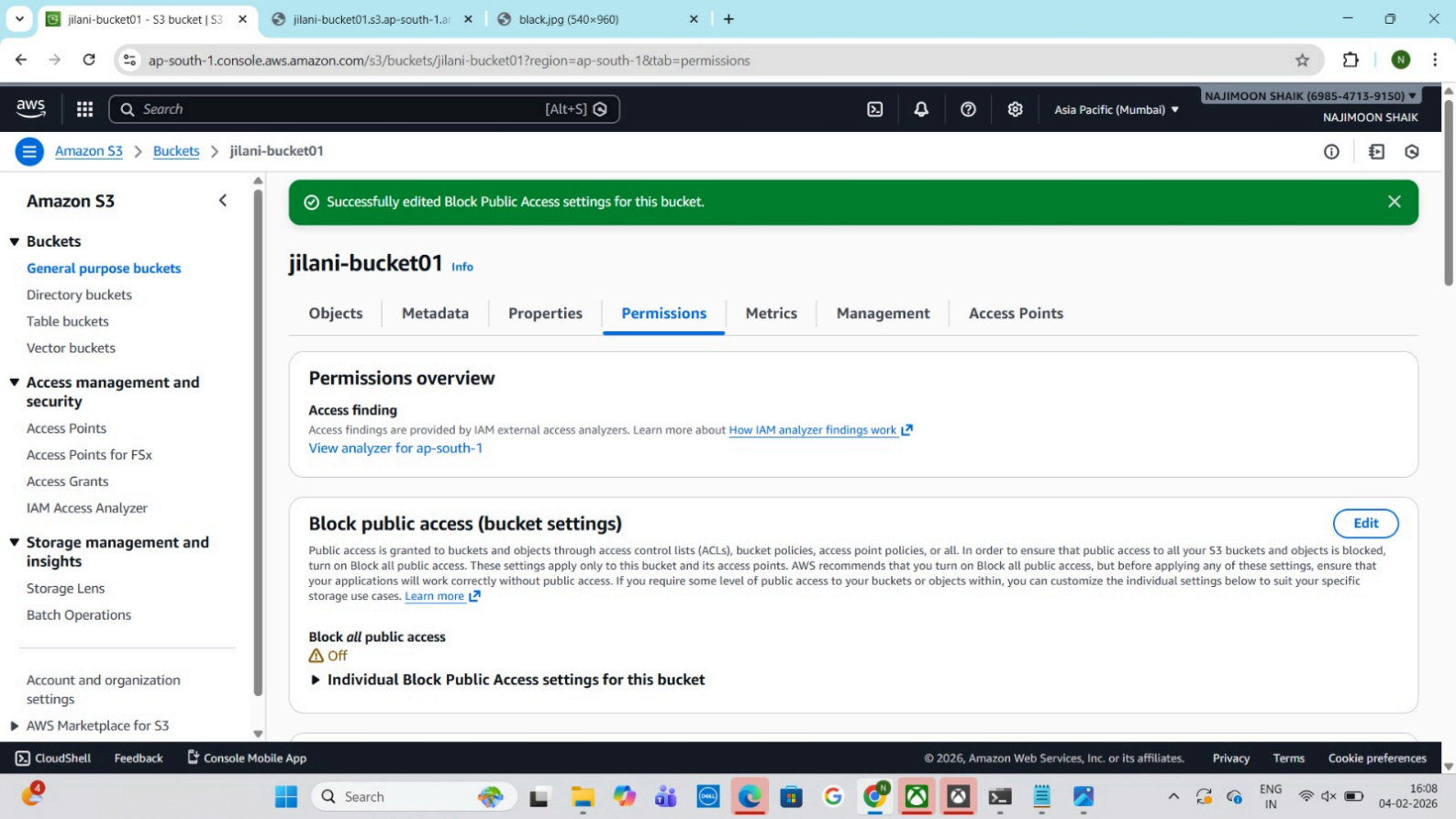
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Cancel

Save changes

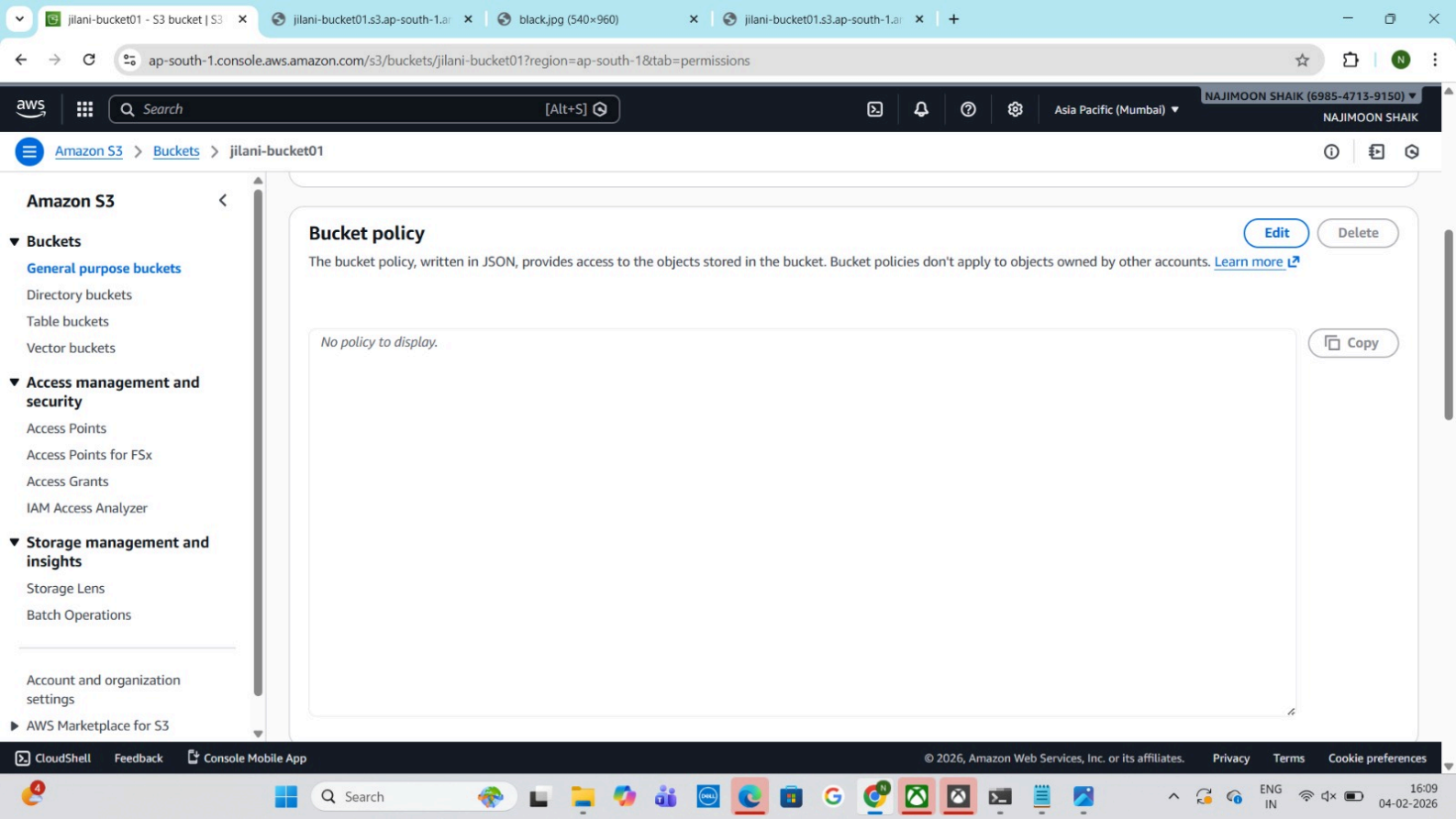






This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>Y1ZVZVRF84NN76WX</RequestId>
  <HostId>23qKsMvn7fXm7Jc6fMq4LaZhXAUfG15U44CJz6EBvfhyt6NUiaxSKy2WZTjKe8bRDSARZncxkw+N1sMf3PXm4+Pe5L3/oBm</HostId>
</Error>
```



ap-south-1.console.aws.amazon.com/s3/bucket/jilani-bucket01/property/policy/edit?region=ap-south-1

aws

Search

[Alt+S]

Asia Pacific (Mumbai)

NAJIMOON SHAIK (6985-4713-9150)

NAJIMOON SHAIK

Amazon S3

Buckets

jilani-bucket01

Edit bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Bucket ARN

arn:aws:s3::jilani-bucket01

Policy

```
1 {
2   "Id": "BucketPolicy",
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6       "Sid": "AllAccess",
7       "Action": "s3:*",
8       "Effect": "Allow",
9       "Resource": [
10        "arn:aws:s3::my-bucket",
11        "arn:aws:s3::my-bucket/*"
12      ],
13       "Principal": "*"
14     }
15   ]
16 }
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

Account and organization settings

AWS Marketplace for S3

CloudShell

Feedback

Console Mobile App

© 2026, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

4

Search

Windows Taskbar Icons

16:11 04-02-2026

