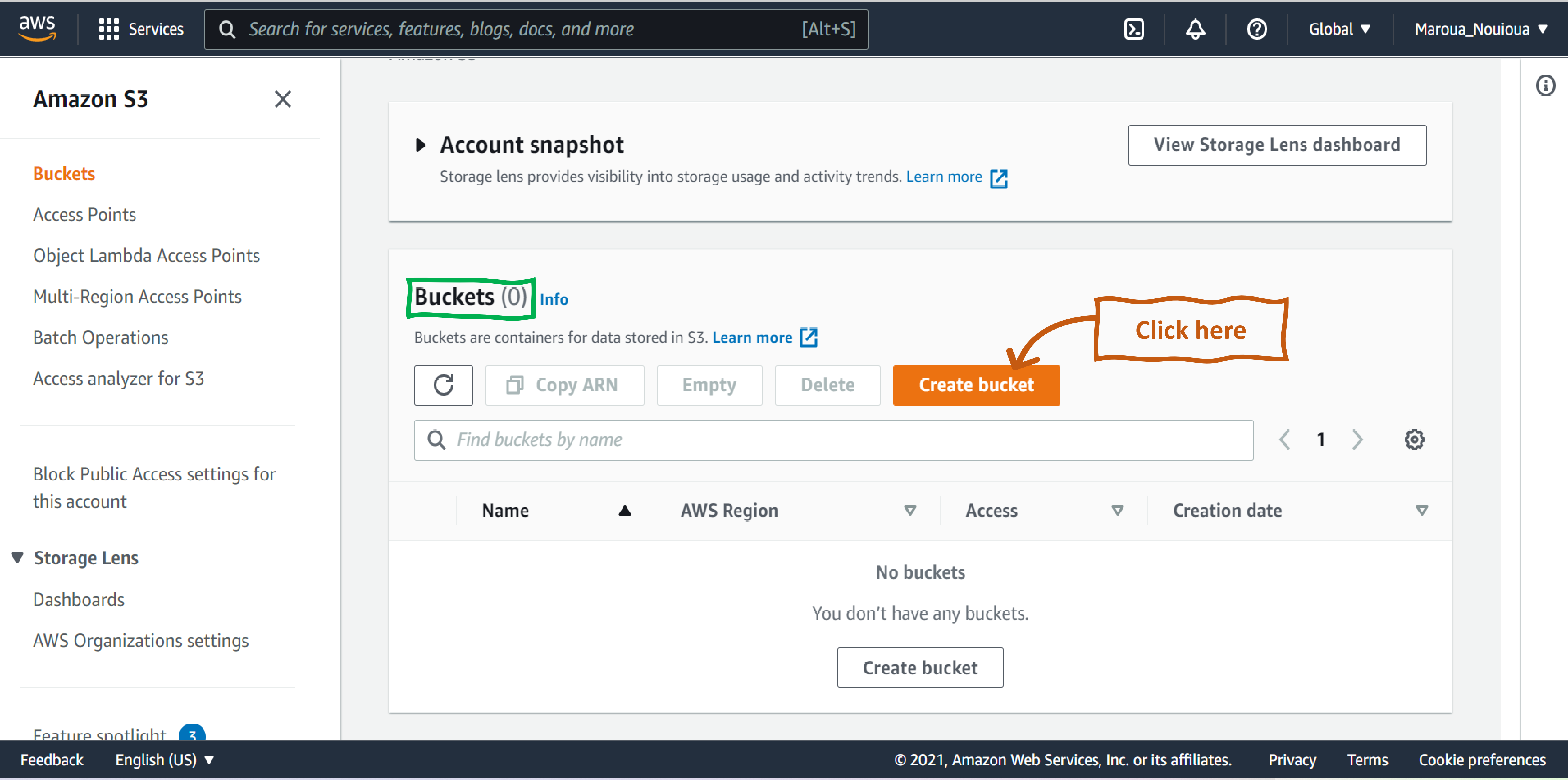
SUP'COM
Higher School of Communication of Tunis

Your first website on S3

Maroua Nouioua



aws Services Search for services, features, blogs, docs, and more [Alt+S] Global ▼ Maroua_Nouioua ▼

Amazon S3

- Buckets
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- Access analyzer for S3

Block Public Access settings for this account

▼ Storage Lens

- Dashboards
- AWS Organizations settings

Feature spotlight 3

▸ **Account snapshot**

Storage lens provides visibility into storage usage and activity trends. Learn more

View Storage Lens dashboard

Buckets (0) Info

Buckets are containers for data stored in S3. Learn more

Copy ARN | Empty | Delete | Create bucket

Click here

Find buckets by name

< 1 >

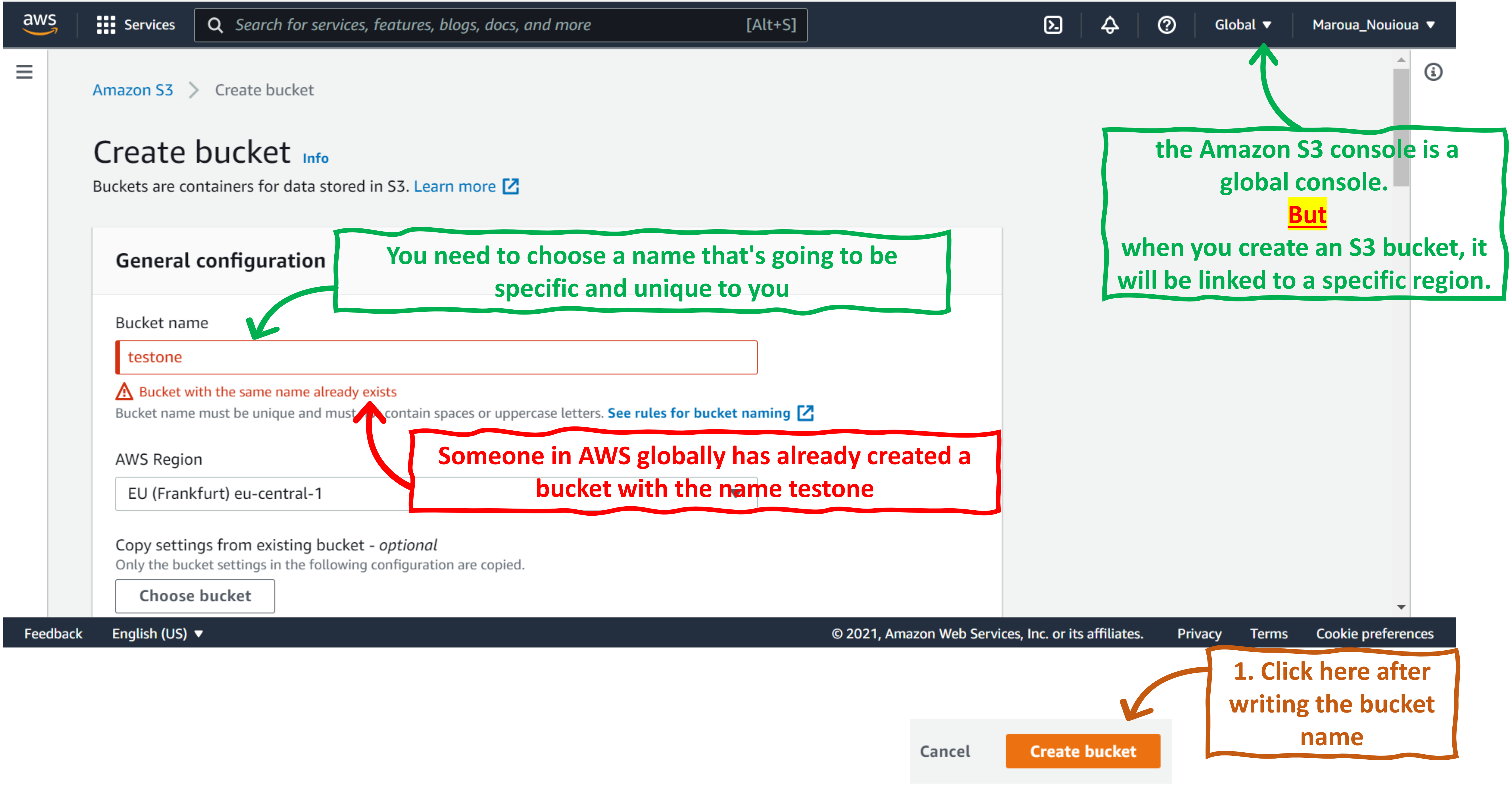
Name ▲	AWS Region ▽	Access ▽	Creation date ▽

No buckets

You don't have any buckets.

Create bucket

Feedback English (US) ▼ © 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



Amazon S3 > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

testone

⚠ Bucket with the same name already exists

Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming

AWS Region

EU (Frankfurt) eu-central-1

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

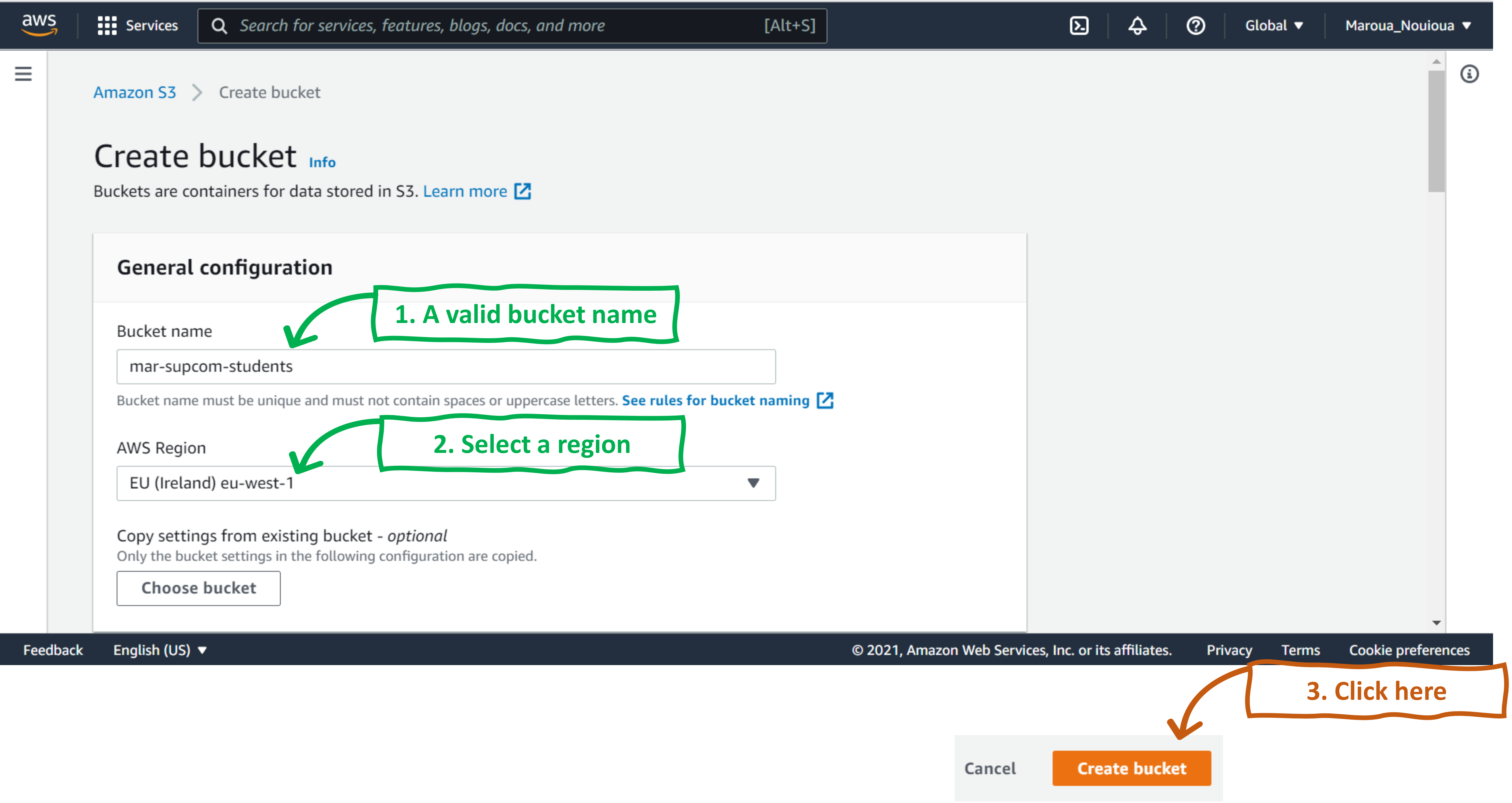
Choose bucket

the Amazon S3 console is a global console.
But
when you create an S3 bucket, it will be linked to a specific region.

You need to choose a name that's going to be specific and unique to you

Someone in AWS globally has already created a bucket with the name testone

1. Click here after writing the bucket name



Amazon S3 > Create bucket

Create bucket

Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

mar-supcom-students

Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming

AWS Region

EU (Ireland) eu-west-1

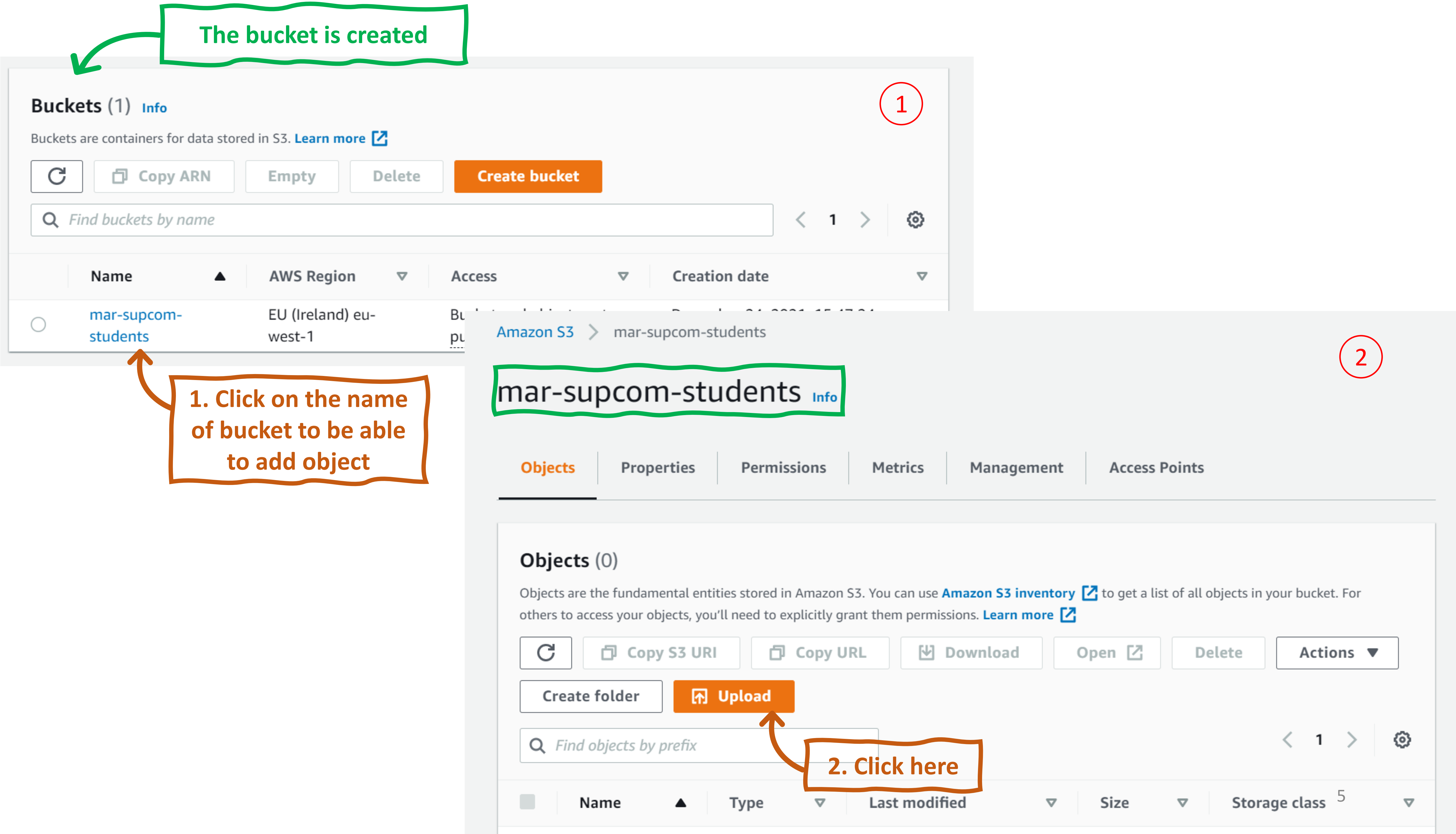
Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

1. A valid bucket name

2. Select a region

3. Click here



The bucket is created

1

Buckets (1) Info

Buckets are containers for data stored in S3. Learn more

Name	AWS Region	Access	Creation date
○ mar-supcom-students	EU (Ireland) eu-west-1	Bu pu	

1. Click on the name of bucket to be able to add object

2

Amazon S3 > mar-supcom-students

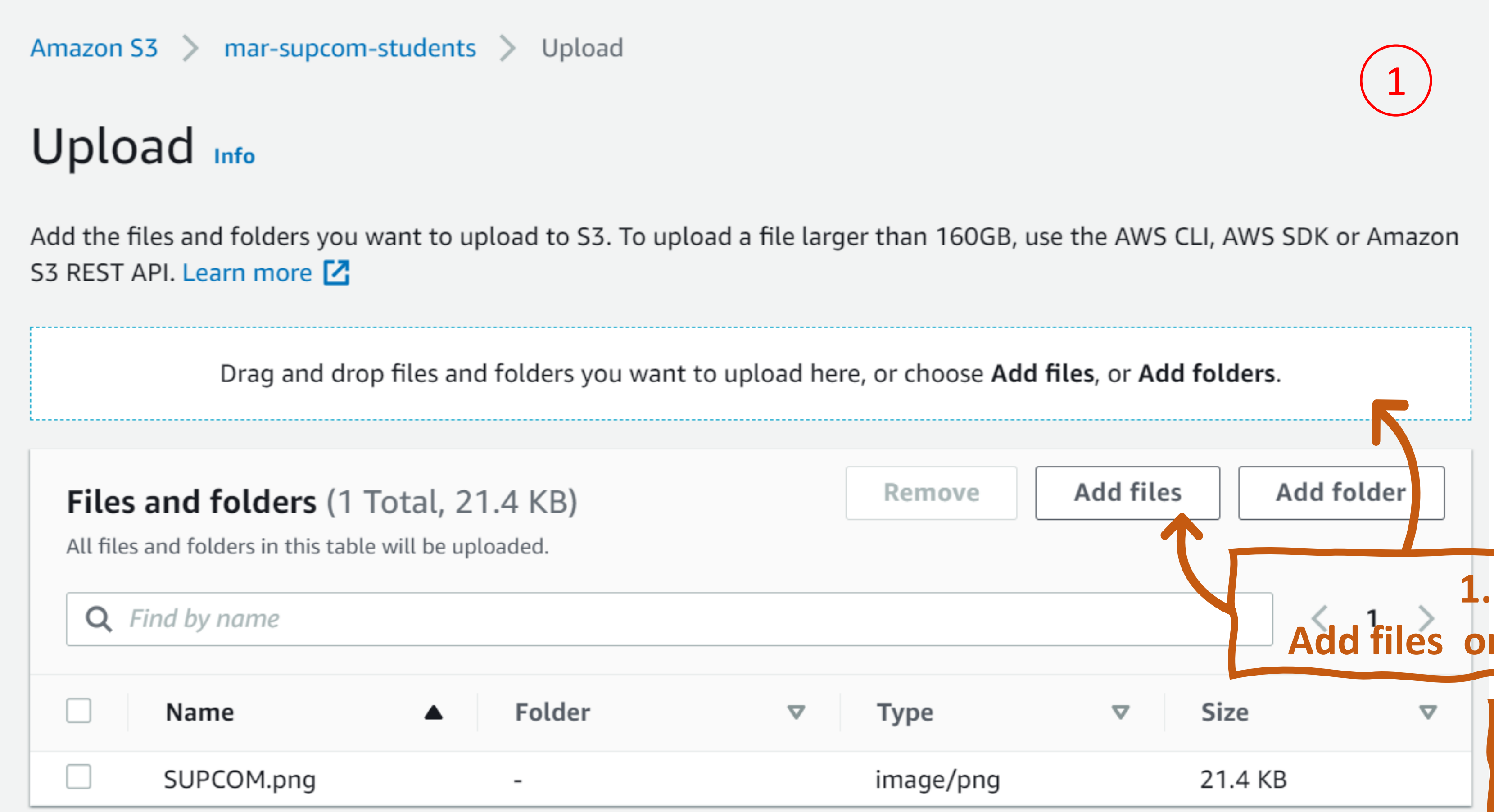
mar-supcom-students Info

Objects (0)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

2. Click here

☐	Name	Type	Last modified	Size	Storage class



Amazon S3 > mar-supcom-students > Upload

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files**, or **Add folders**.

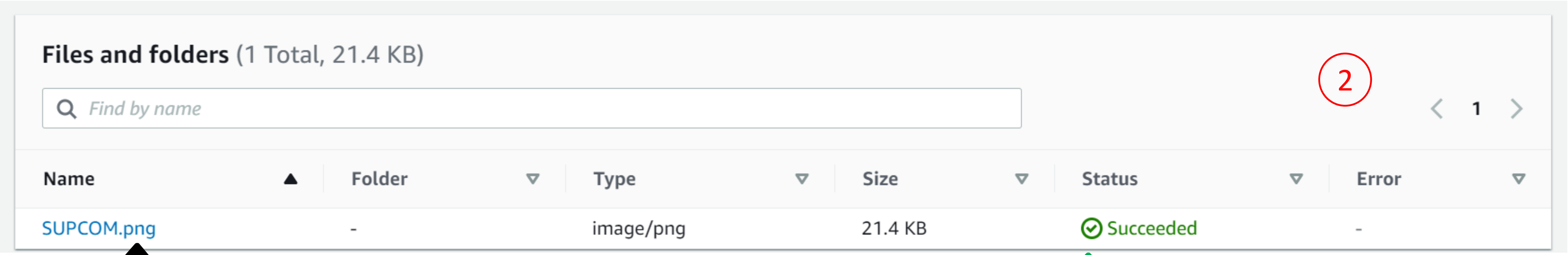
Files and folders (1 Total, 21.4 KB)

All files and folders in this table will be uploaded.

□	Name ▲	Folder ▽	Type ▽	Size ▽
□	SUPCOM.png	-	image/png	21.4 KB

1. Click:
Add files or Drag and drop

2. Click on Upload again after adding your file

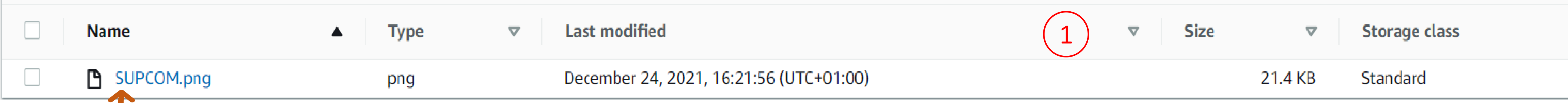


Files and folders (1 Total, 21.4 KB)

Name ▲	Folder ▽	Type ▽	Size ▽	Status ▽	Error ▽
SUPCOM.png	-	image/png	21.4 KB	✓ Succeeded	-

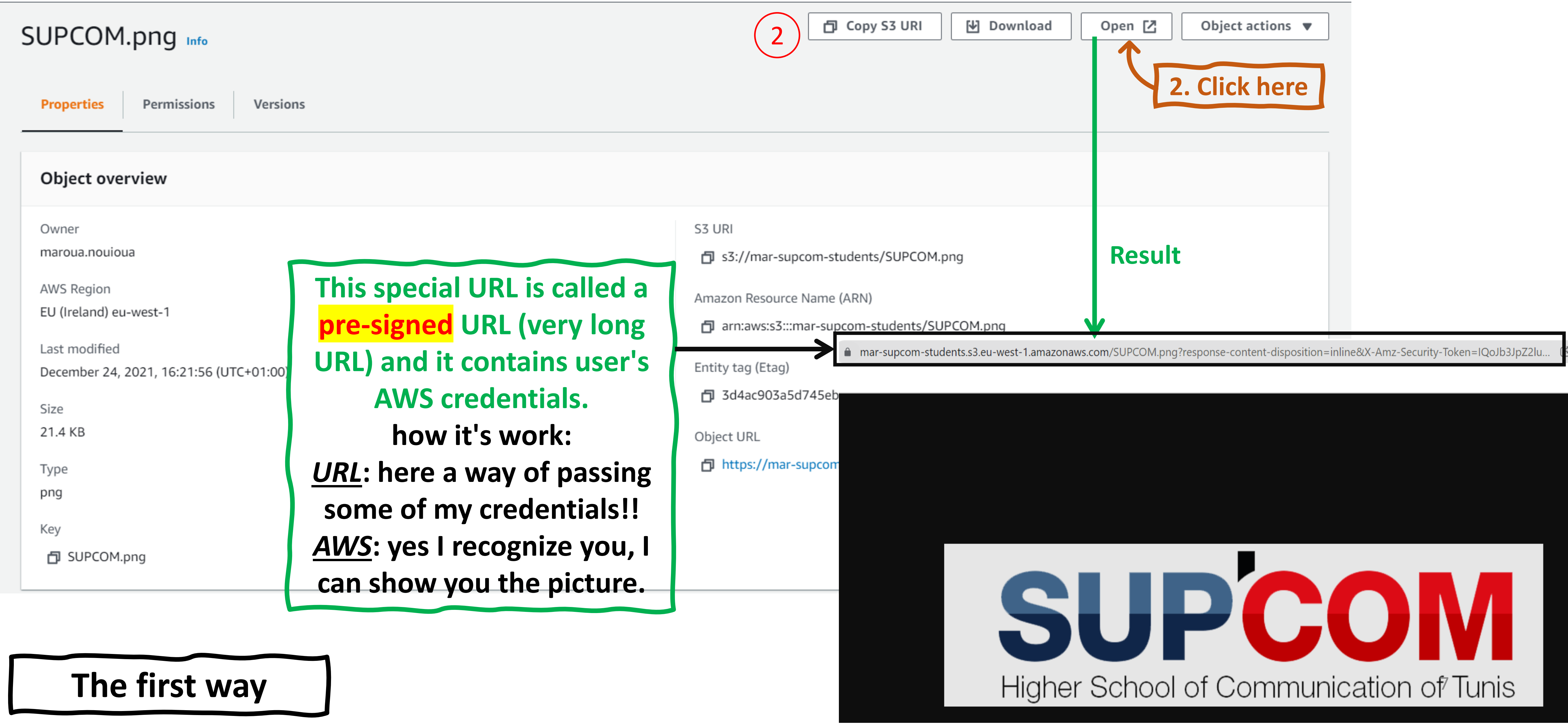
How to open this file?
How can i see the contents of this file?

The file is uploaded successfully



□	Name ▲	Type ▽	Last modified ▽	Size ▽	Storage class
□	SUPCOM.png	png	December 24, 2021, 16:21:56 (UTC+01:00)	21.4 KB	Standard

1. Click here



SUPCOM.png Info

2. Click here

Object overview

Owner
maroua.nouioua

AWS Region
EU (Ireland) eu-west-1

Last modified
December 24, 2021, 16:21:56 (UTC+01:00)

Size
21.4 KB

Type
png

Key
SUPCOM.png

S3 URI
s3://mar-supcom-students/SUPCOM.png

Amazon Resource Name (ARN)
arn:aws:s3:::mar-supcom-students/SUPCOM.png

Entity tag (Etag)
3d4ac903a5d745eb

Object URL
https://mar-supcom

Result

mar-supcom-students.s3.eu-west-1.amazonaws.com/SUPCOM.png?response-content-disposition=inline&X-Amz-Security-Token=IQoJb3JpZ2lu...

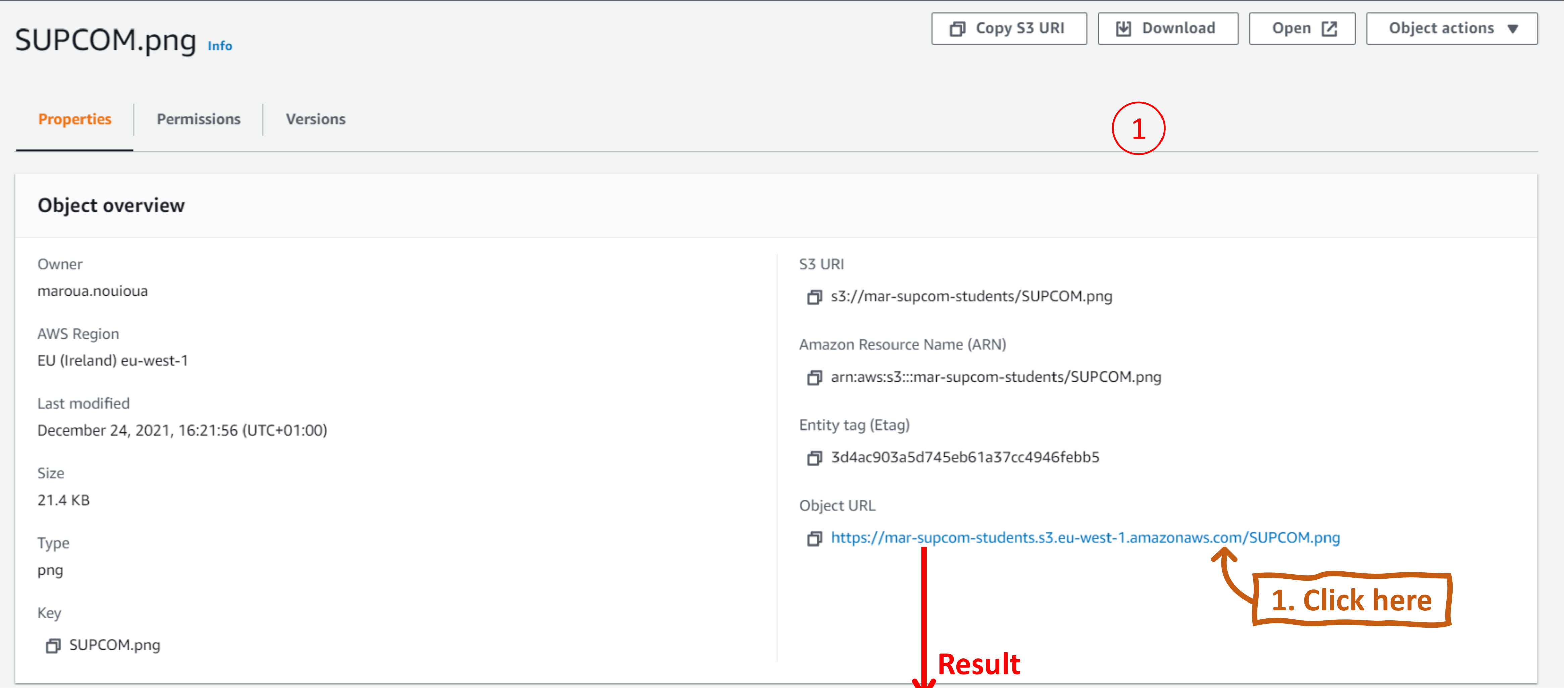
This special URL is called a **pre-signed** URL (very long URL) and it contains user's AWS credentials.

how it's work:

URL: here a way of passing some of my credentials!!

AWS: yes I recognize you, I can show you the picture.

The first way



1

Object overview

Owner
maroua.nouioua

AWS Region
EU (Ireland) eu-west-1

Last modified
December 24, 2021, 16:21:56 (UTC+01:00)

Size
21.4 KB

Type
png

Key
SUPCOM.png

S3 URI
s3://mar-supcom-students/SUPCOM.png

Amazon Resource Name (ARN)
arn:aws:s3:::mar-supcom-students/SUPCOM.png

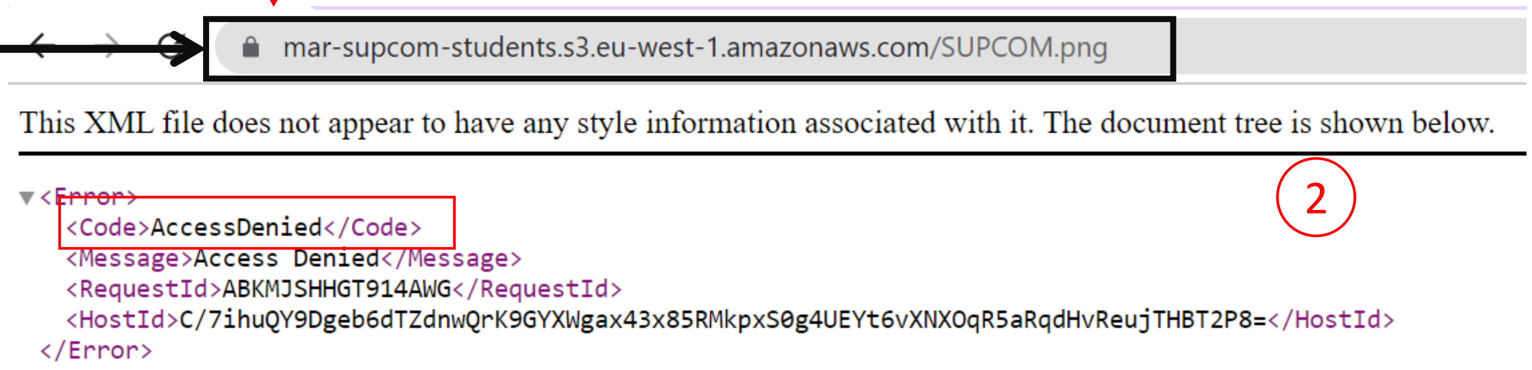
Entity tag (Etag)
3d4ac903a5d745eb61a37cc4946febb5

Object URL
https://mar-supcom-students.s3.eu-west-1.amazonaws.com/SUPCOM.png

1. Click here

Result

If we try to open the file using its public URL, it's not going to work because our bucket is not public.



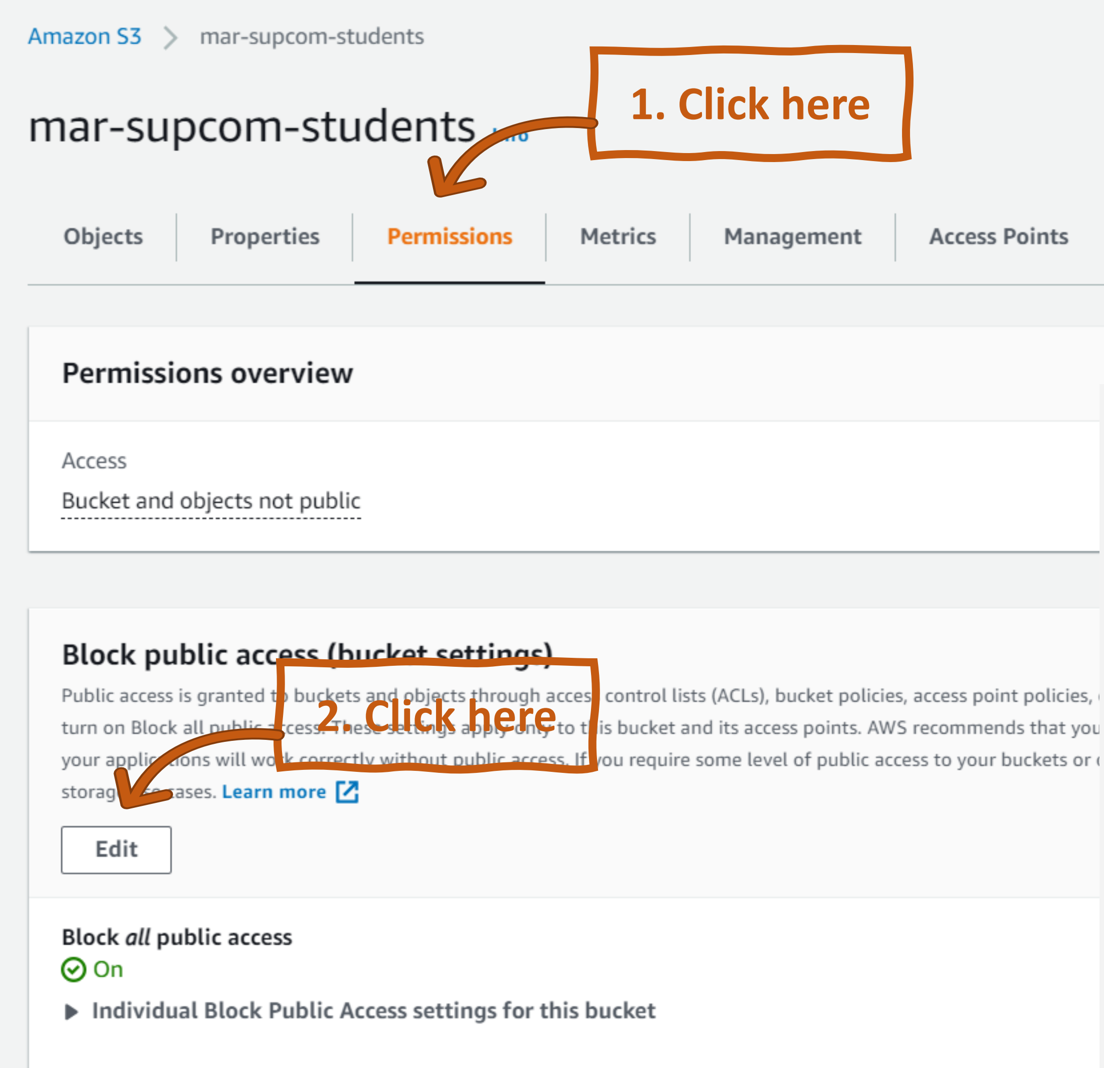
mar-supcom-students.s3.eu-west-1.amazonaws.com/SUPCOM.png

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

2

```
▼<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>ABKMJSHHGT914AWG</RequestId>
  <HostId>C/7ihuQY9Dgeb6dTZdnwQrK9GYXWgax43x85RMkpxS0g4UEYt6vXNXOqR5aRqdHvReujTHBT2P8=</HostId>
</Error>
```

The second way



1

Amazon S3 > mar-supcom-students

Objects | Properties | Permissions | Metrics | Management | Access Points

Edit

1. Click here

mar-supcom-students

Permissions overview

Access

Bucket and objects not public

Block public access (bucket settings)

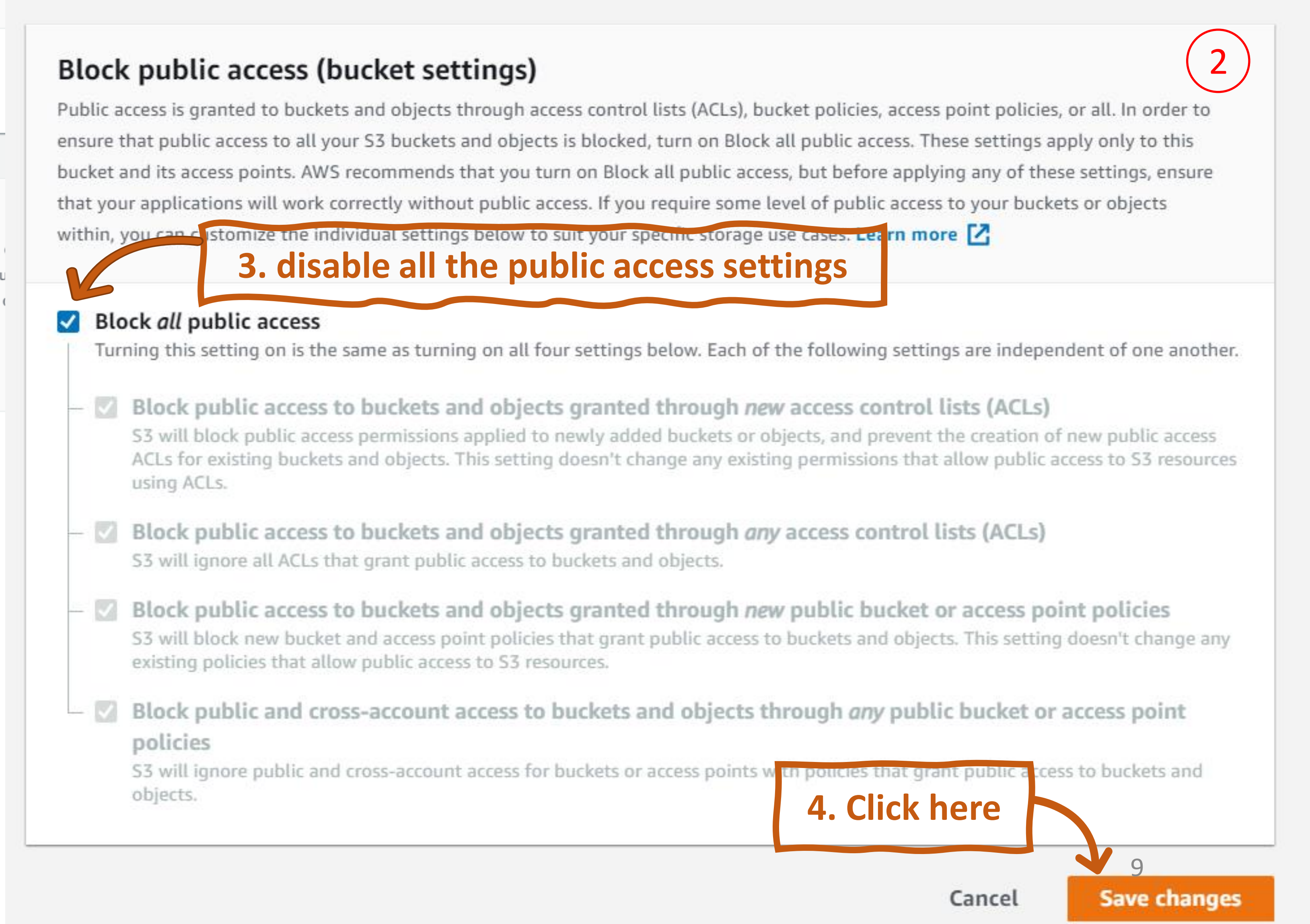
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you your applications will work correctly without public access. If you require some level of public access to your buckets or storage use cases. Learn more

2. Click here

Block *all* public access

On

▶ Individual Block Public Access settings for this bucket



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

3. disable all the public access settings

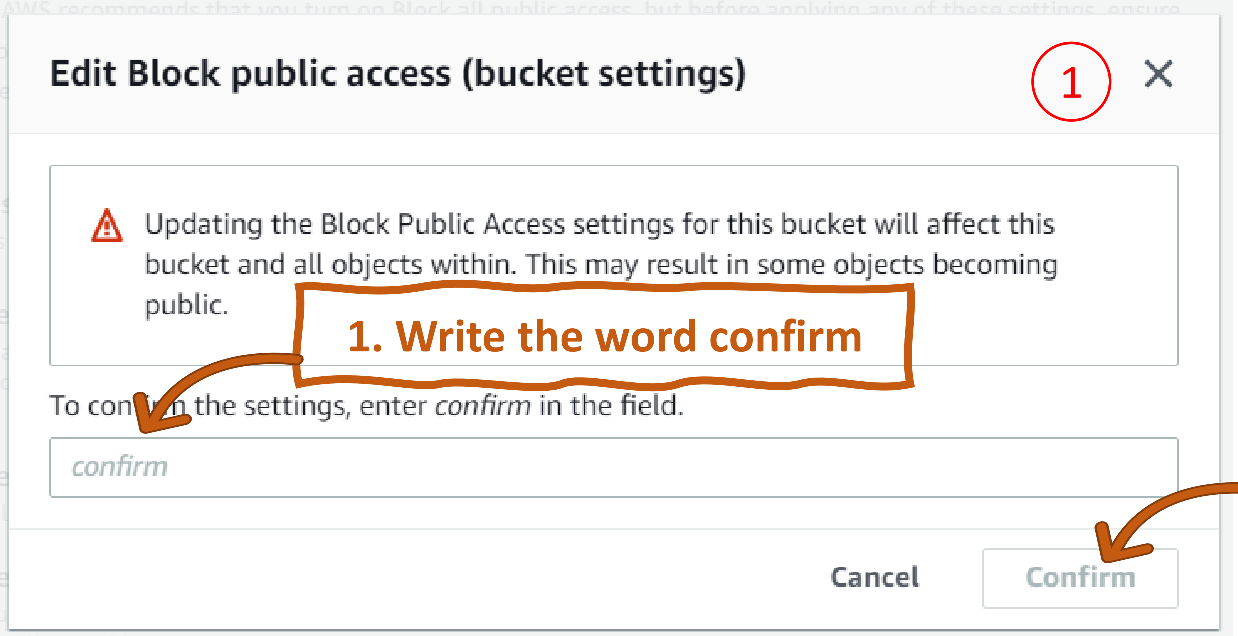
☑ Block *all* public access

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.

4. Click here

We need to create a public bucket policy. This is why we do 2 and 3 steps.



1

Edit Block public access (bucket settings)

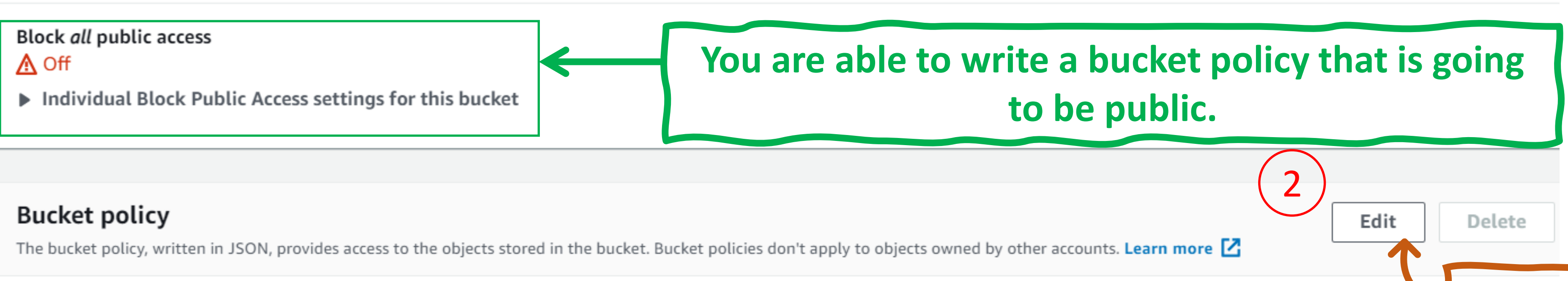
⚠ Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.

To confirm the settings, enter *confirm* in the field.

confirm

1. Write the word confirm

2. Click here



Block *all* public access
⚠ Off
▶ Individual Block Public Access settings for this bucket

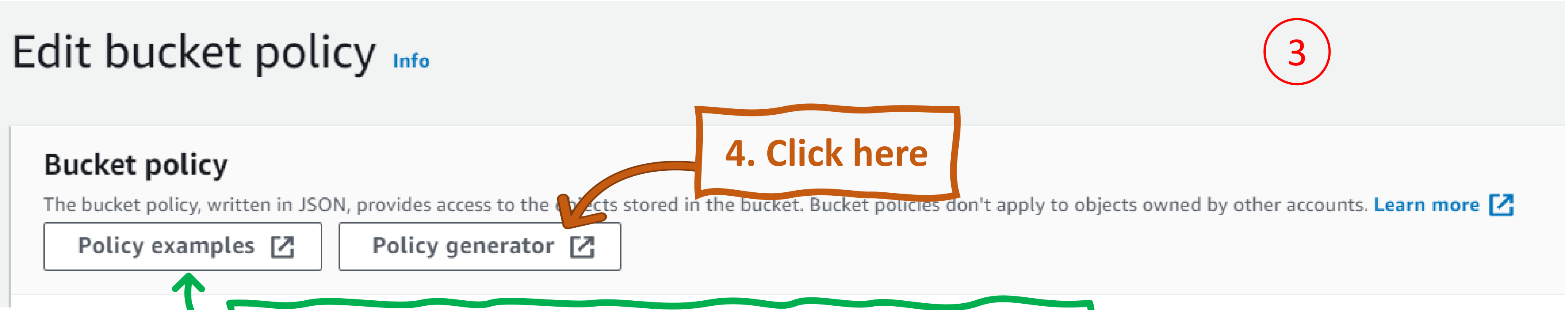
You are able to write a bucket policy that is going to be public.

2

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

3. Click here



3

Edit bucket policy Info

Bucket policy

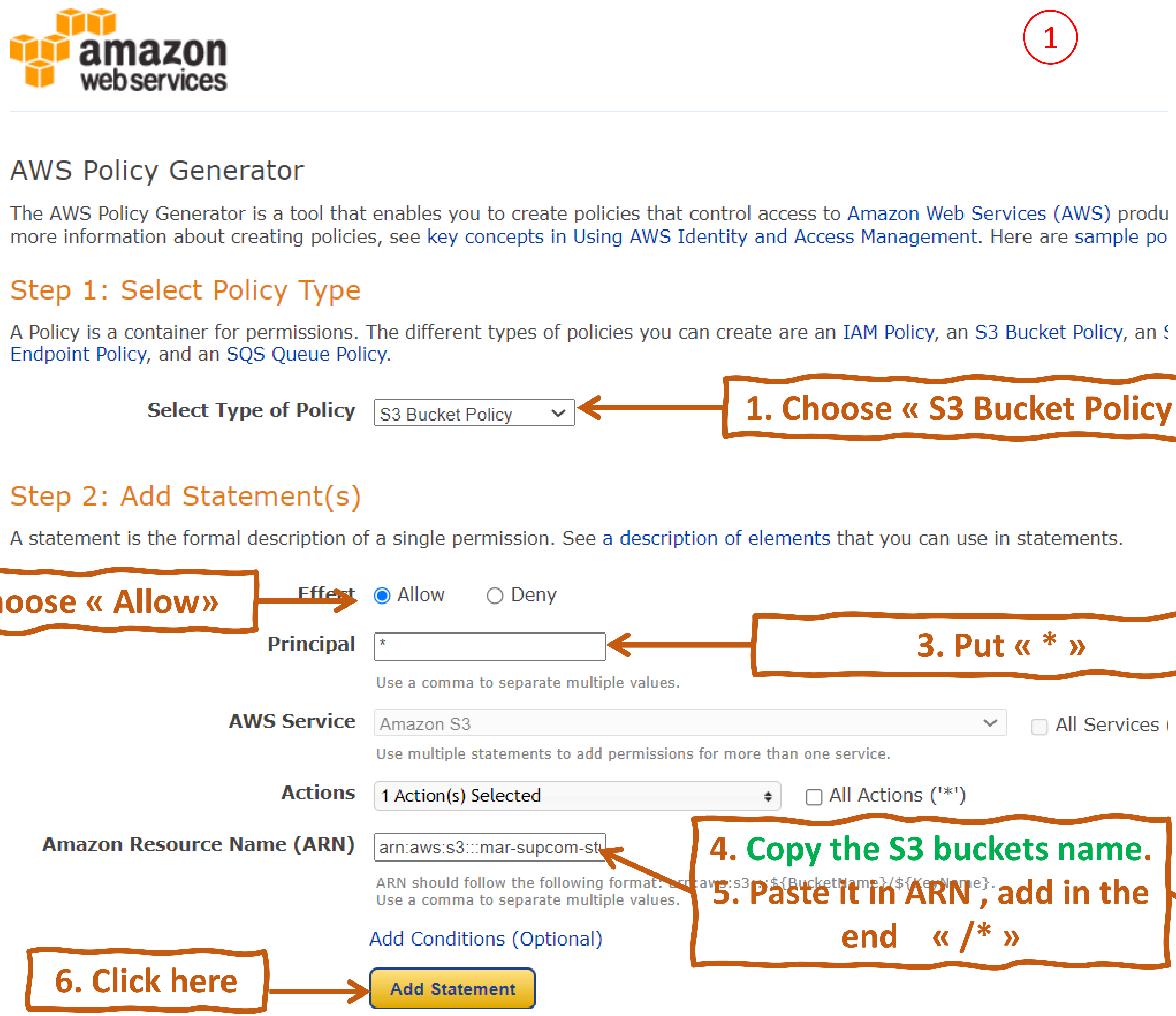
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

4. Click here

Here some policy examples, please take a look

We want to « Allow » everyone « * » to do « GetObject » to be able to read the objects in our bucket

1



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) produ more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample po

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an S Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy: S3 Bucket Policy

1. Choose « S3 Bucket Policy »

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect: ● Allow ○ Deny

2. Choose « Allow»

Principal: *

Use a comma to separate multiple values.

3. Put « * »

AWS Service: Amazon S3 □ All Services

Use multiple statements to add permissions for more than one service.

Actions: 1 Action(s) Selected □ All Actions ('*')

Amazon Resource Name (ARN): arn:aws:s3:::mar-supcom-st

ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.

Add Conditions (Optional)

Add Statement

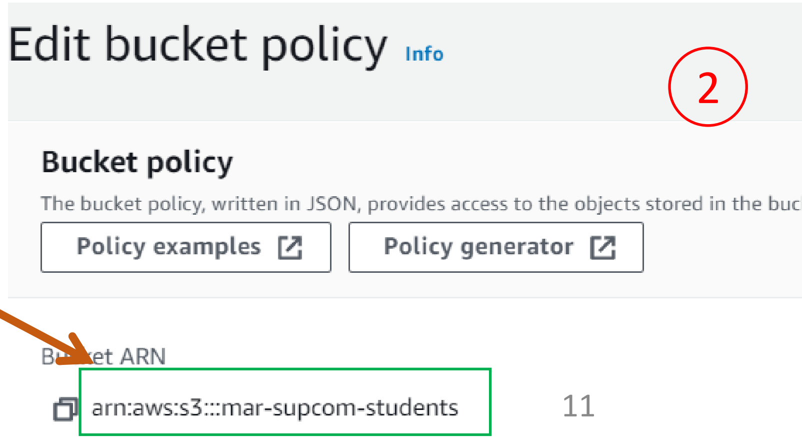
4. Copy the S3 buckets name.

5. Paste it in ARN , add in the end « /* »

6. Click here

Why we added « /* » after our ARN in the 5th step?
Because the action we have chosen called « GetObjects » applies to the objects in our buckets.
Which are whatever coming after the bucket names.

2



Edit bucket policy Info

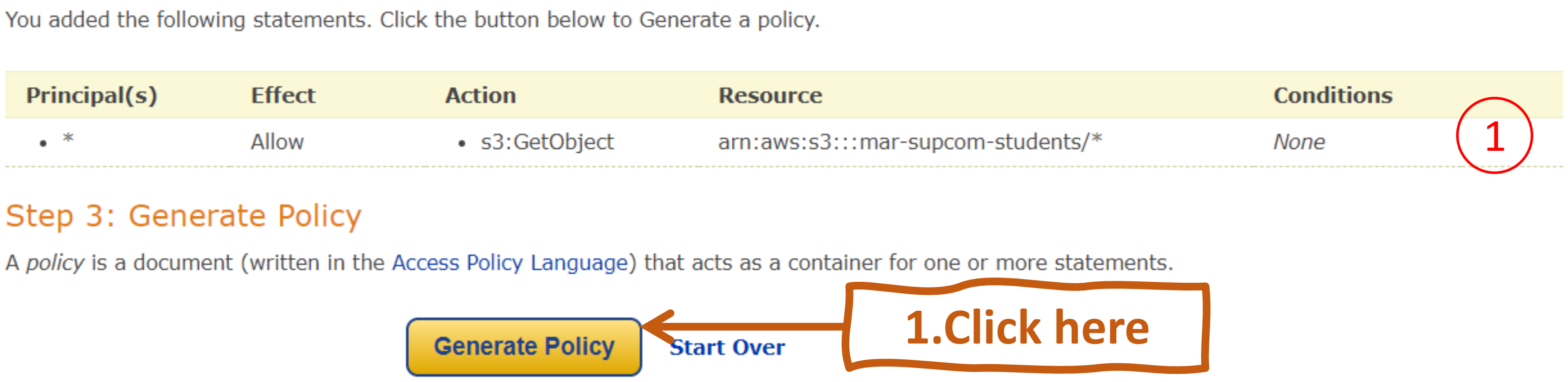
Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the buc

Policy examples | Policy generator

Bucket ARN

arn:aws:s3:::mar-supcom-students

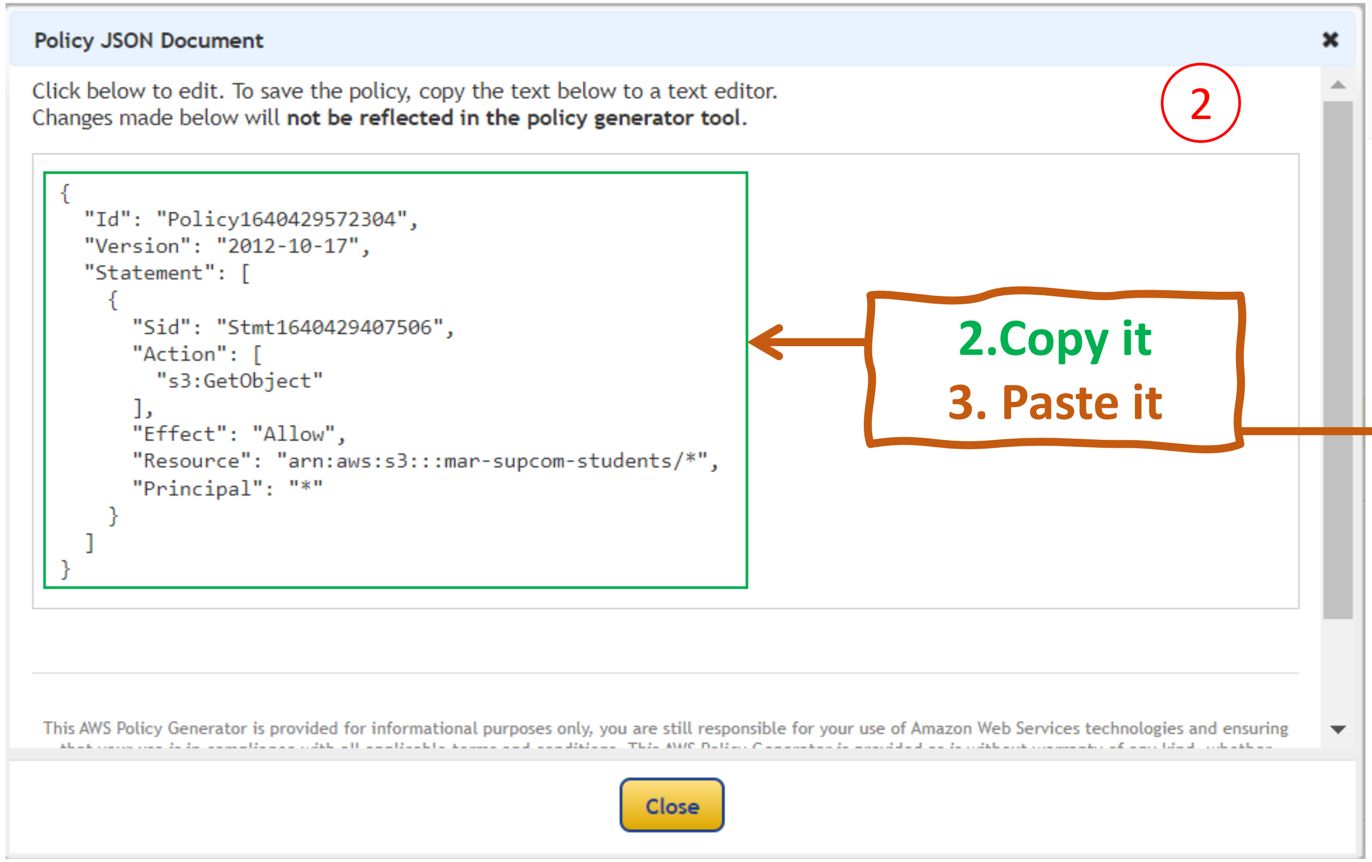


You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• *	Allow	• s3:GetObject	arn:aws:s3:::mar-supcom-students/*	*None*

Step 3: Generate Policy

A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more statements.

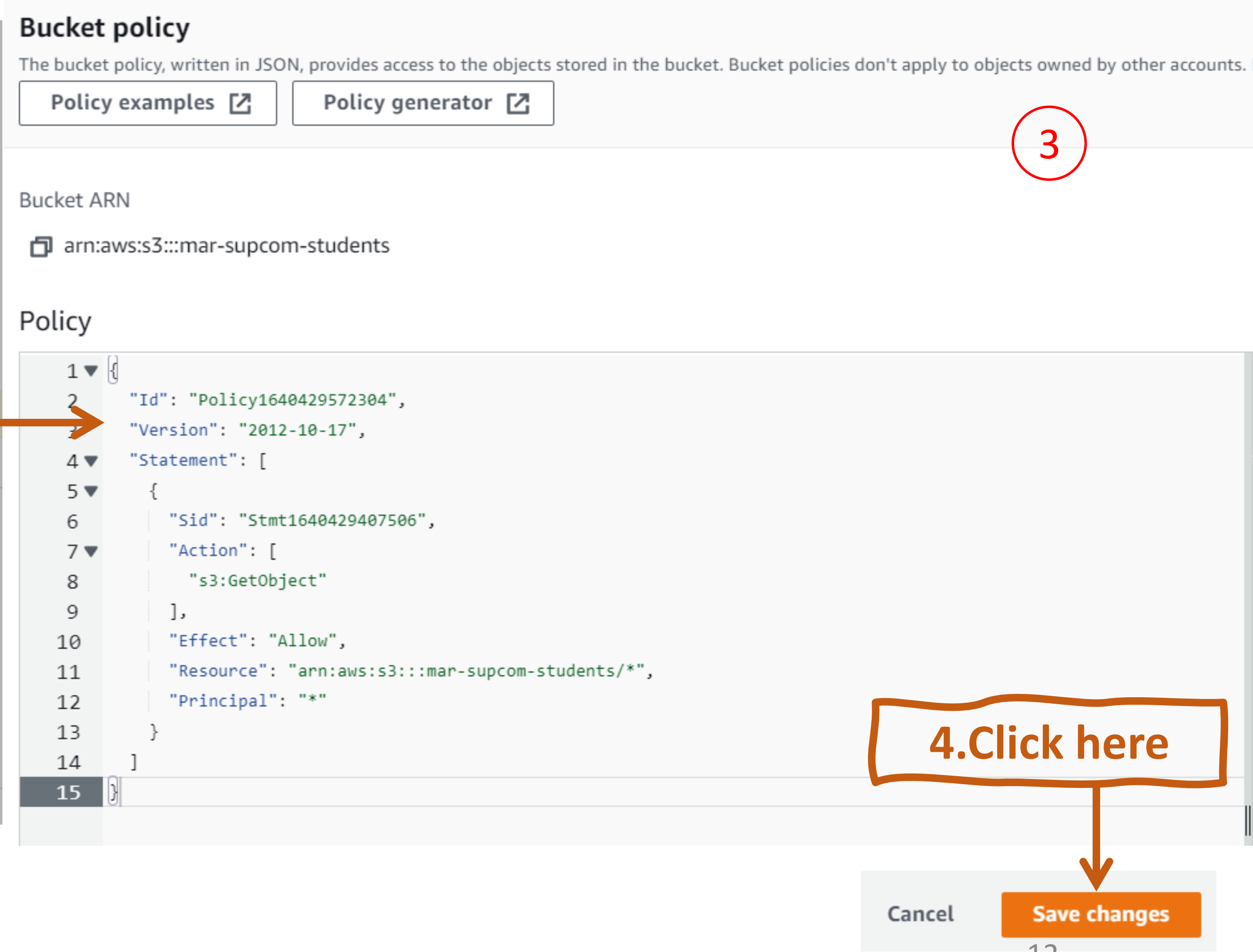


Policy JSON Document ×

Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will **not be reflected in the policy generator tool.**

```
{
  "Id": "Policy1640429572304",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1640429407506",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::mar-supcom-students/*",
      "Principal": "*"
    }
  ]
}
```

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring



Bucket policy

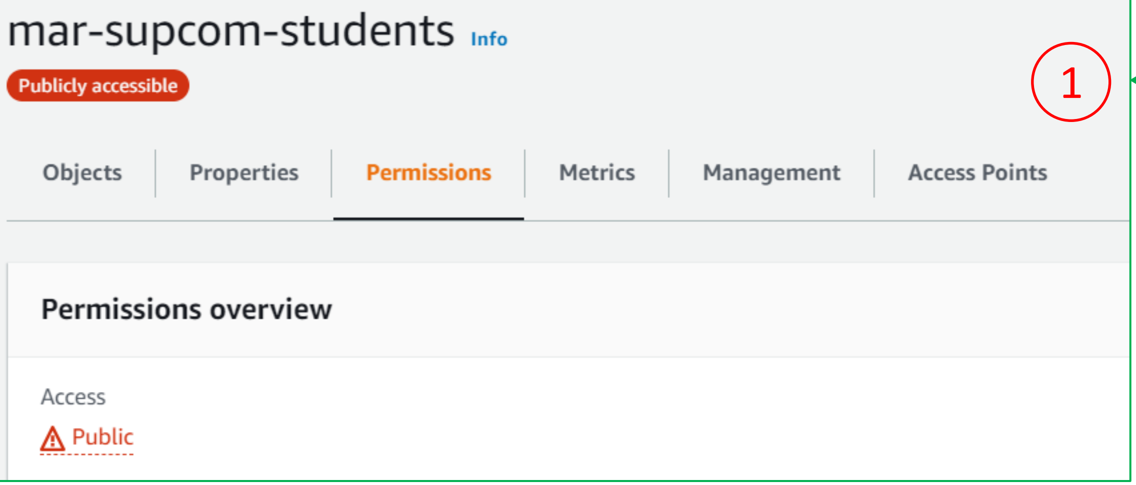
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts.

Bucket ARN

arn:aws:s3:::mar-supcom-students

Policy

```
{
  "Id": "Policy1640429572304",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1640429407506",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::mar-supcom-students/*",
      "Principal": "*"
    }
  ]
}
```



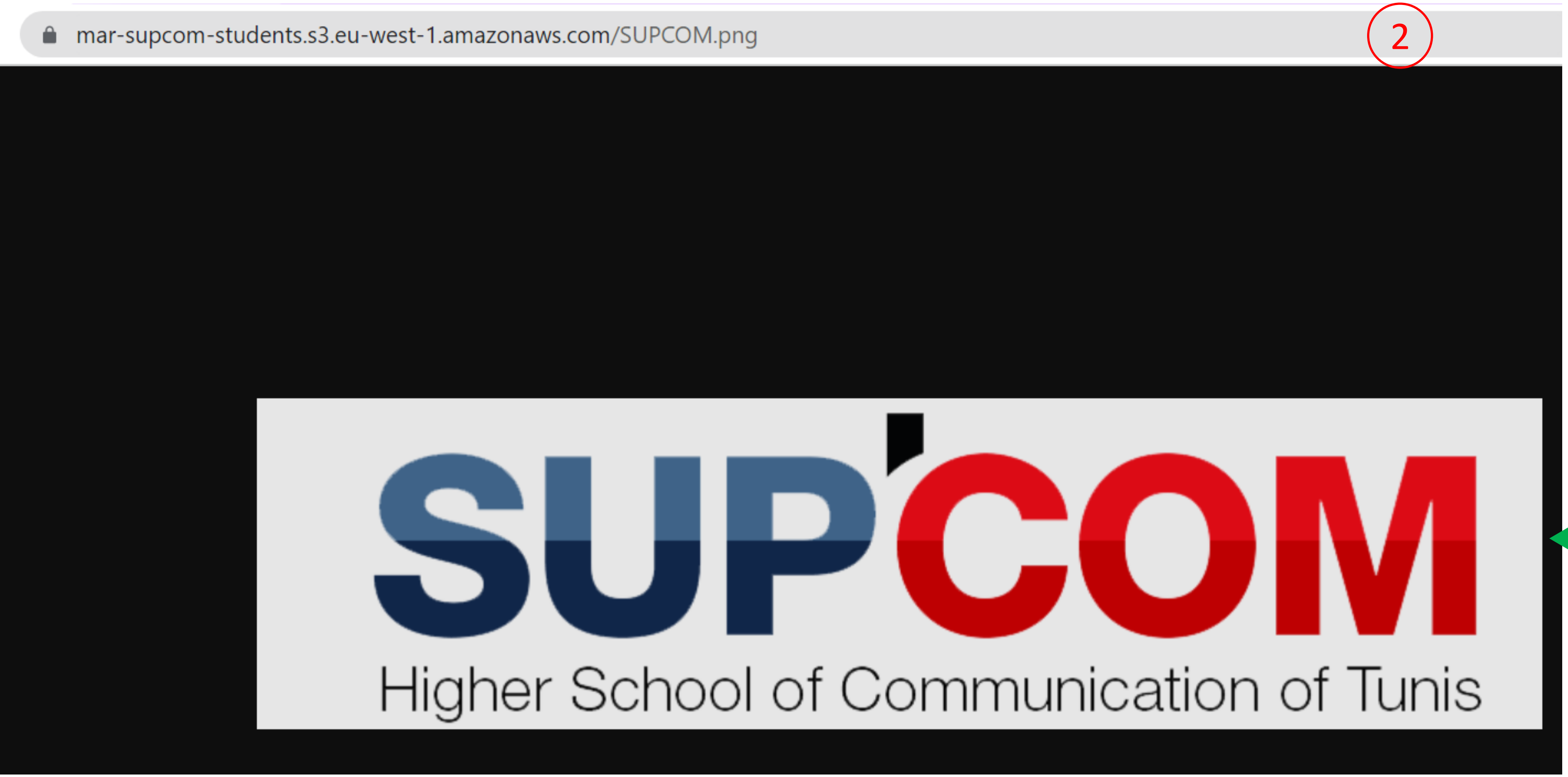
mar-supcom-students Info

Publicly accessible

Permissions overview

Access
⚠ Public

The access has been changed to public



mar-supcom-students.s3.eu-west-1.amazonaws.com/SUPCOM.png

1. Click on « Objects »
2. Click on « SUPCOM.png »
3. Click on « Object URL » (in mycase : https://mar-supcom-students.s3.eu-west-1.amazonaws.com/SUPCOM.png)

After doing the 3 steps above, the picture will appear normally

Acknowledgement