

# Create Public AWS S3 Bucket Step-by-Step Guide

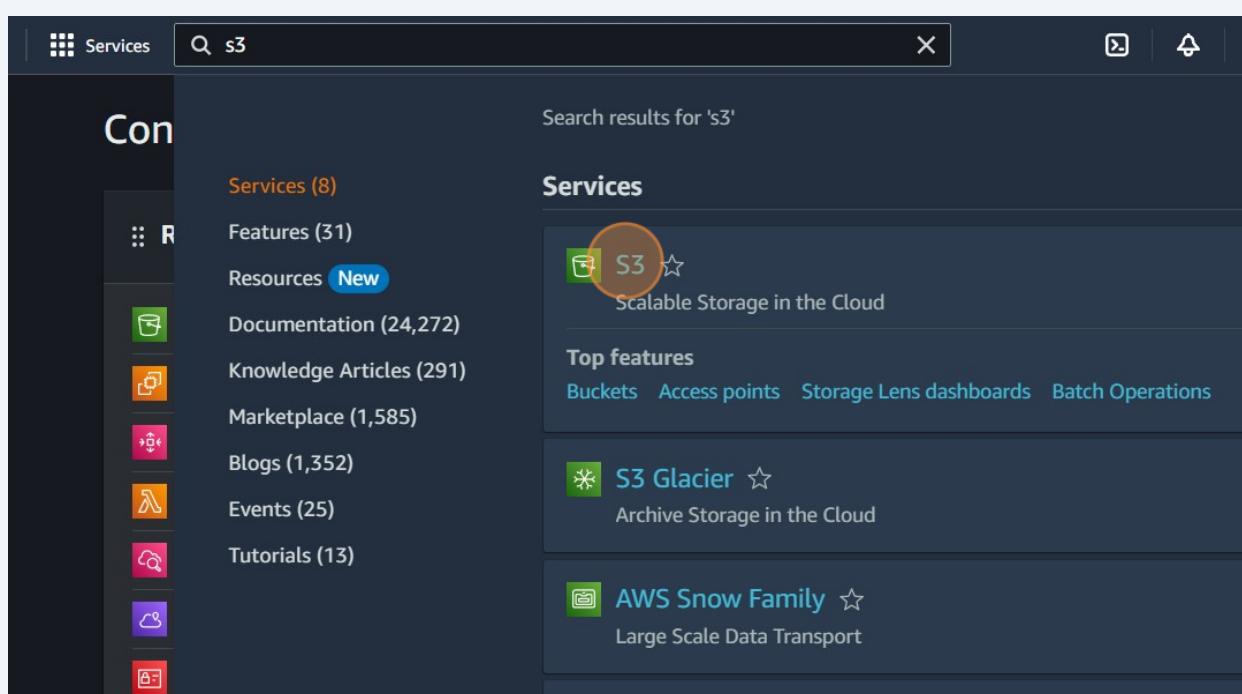
Scribe

1

Navigate to  
<https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1>

2

Click the Search field and navigate to S3



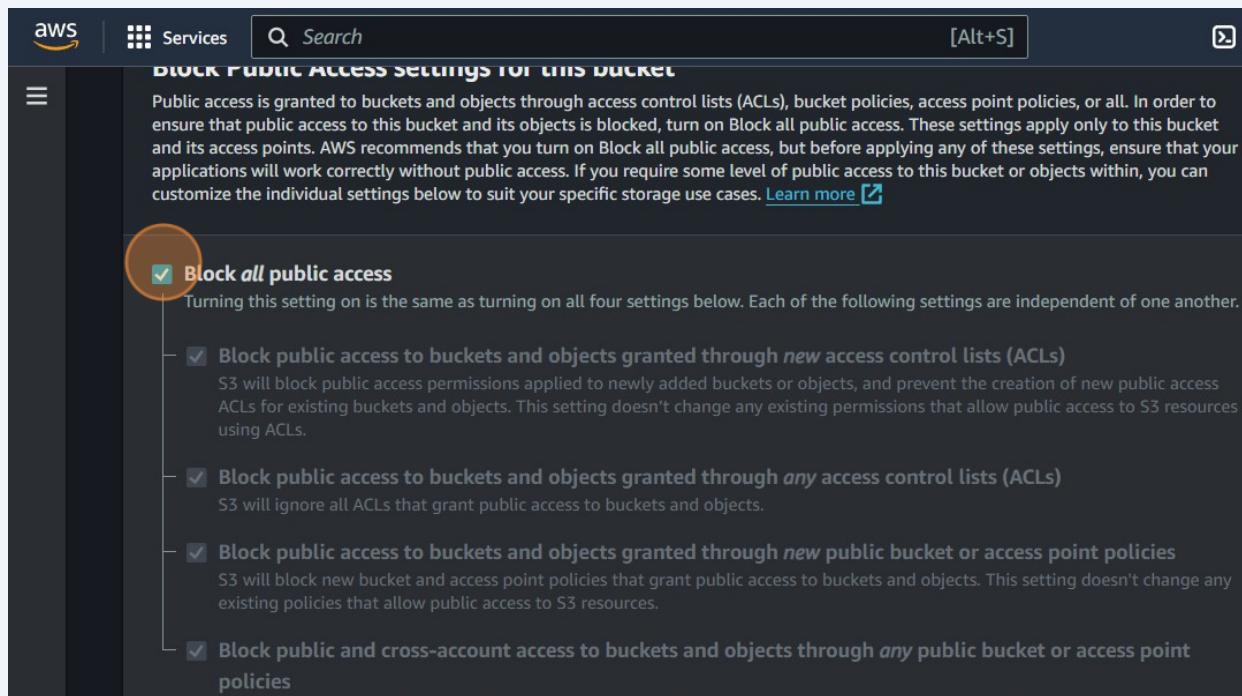
**3** Click "Create bucket" to create a new S3 bucket.

The screenshot shows the Amazon S3 console. At the top, there's an 'Account snapshot' section with metrics like Total storage (Pending), Object count (Pending), and Average object size (Pending). Below this, there are tabs for 'General purpose buckets' and 'Directory buckets', with 'General purpose buckets' selected. It shows a list of 8 buckets, including 'buc83' which was created on February 20, 2024. At the bottom right of the list, there are buttons for 'Create bucket' (which is circled in red), 'Copy ARN', 'Empty', and 'Delete'.

**4** Name the bucket

The screenshot shows the 'Create New Bucket' wizard. It has two options: 'General purpose' (selected) and 'Directory - New'. The 'General purpose' section describes it as recommended for most use cases and mentions redundancy across multiple Availability Zones. The 'Bucket name' field is filled with 'myawsbucket' and is circled in red. Below the field, a note says the name must be unique. There's also a 'Copy settings from existing bucket - optional' section with a 'Choose bucket' button. At the bottom, there's an 'Object Ownership' section with a note about controlling access via ACLs.

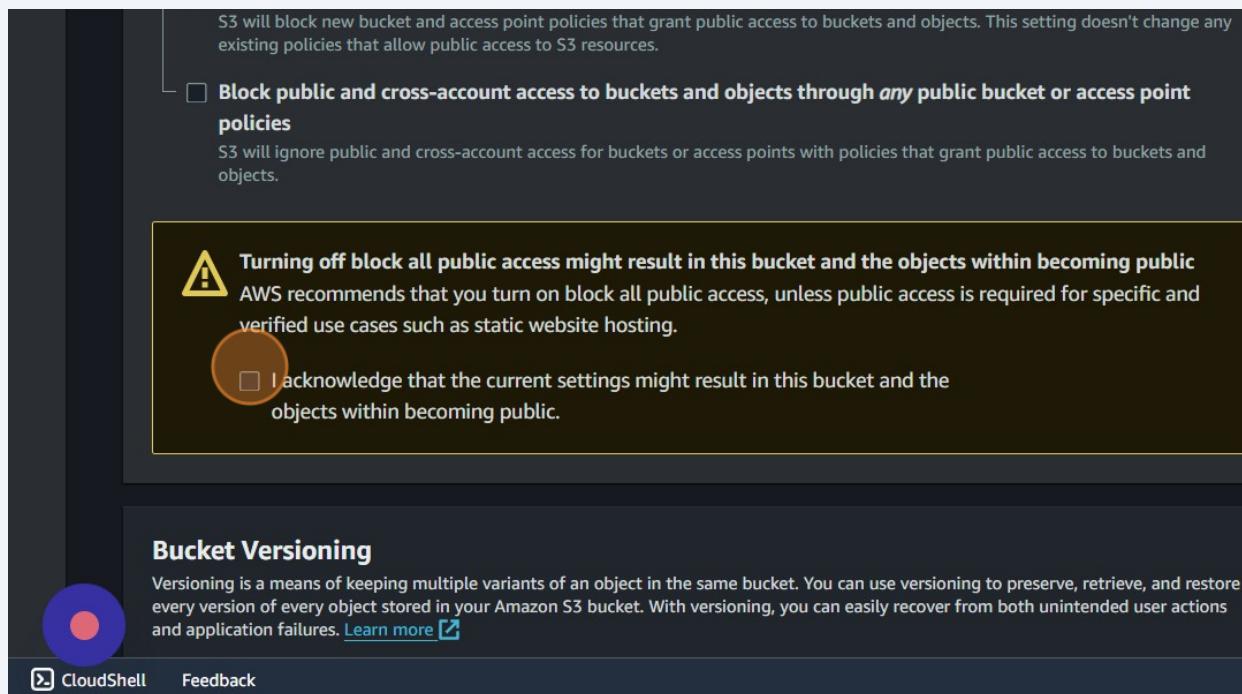
5 Uncheck the field.



The screenshot shows the 'BLOCK PUBLIC ACCESS SETTINGS FOR THIS BUCKET' section. At the top, there is a note about public access being granted through various methods like ACLs, bucket policies, and access point policies. Below this, the 'Block all public access' checkbox is checked and circled in red. A note below it states: 'Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.' Below this note are four additional checkboxes, each with a descriptive subtitle and a note:

- 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**

6 Click "I acknowledge that the current settings might result in this bucket and the objects within becoming public."

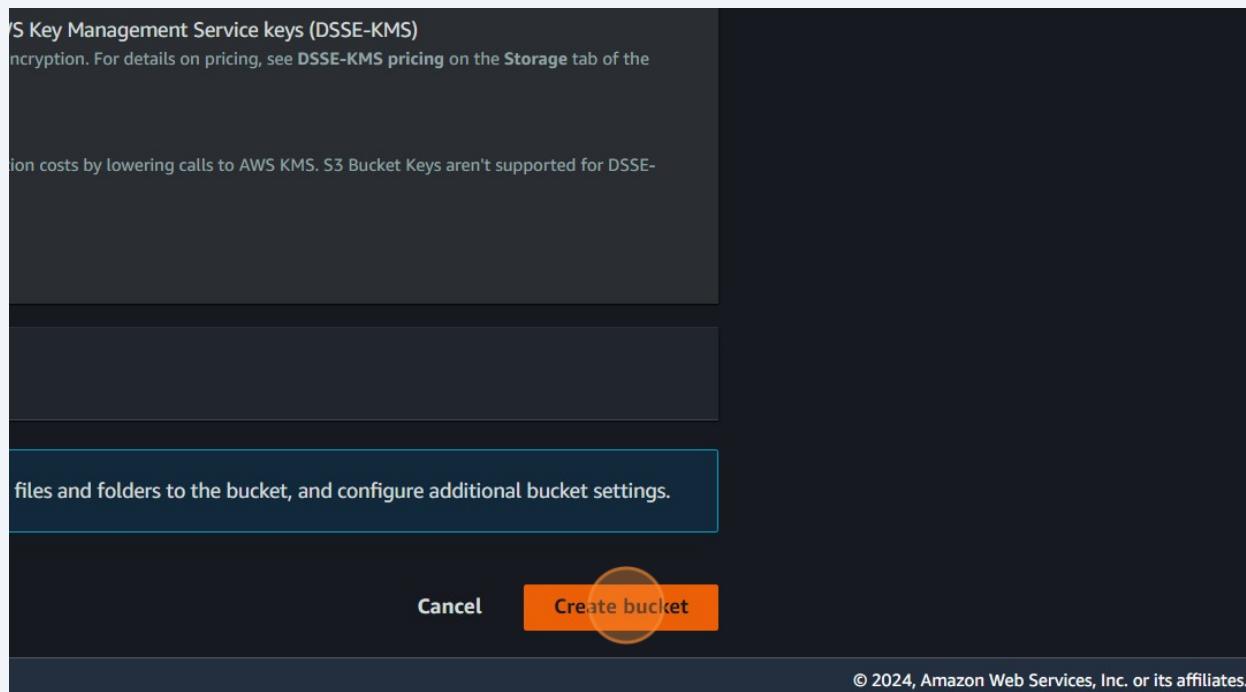


The screenshot shows a confirmation dialog box with a warning icon and text: 'Turning off block all public access might result in this bucket and the objects within becoming public. AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.' Below this is a checkbox labeled 'I acknowledge that the current settings might result in this bucket and the objects within becoming public.' which is currently unchecked and circled in red.

**Bucket Versioning**  
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

 CloudShell   [Feedback](#)

## 7 Create the bucket.



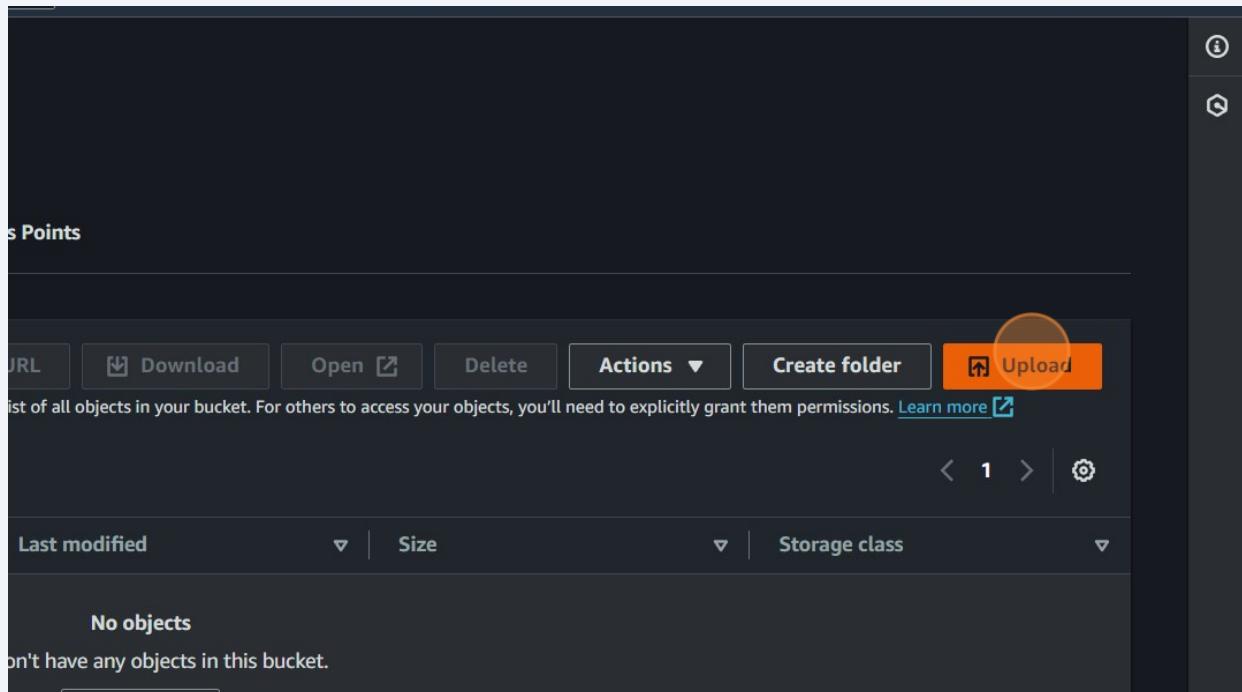
## 8 Check the created bucket and click it.

The screenshot shows the 'Buckets' page in the AWS S3 console. A search bar at the top says 'Find buckets by name'. Below is a table with columns: Name, AWS Region, and Access. The table lists several buckets:

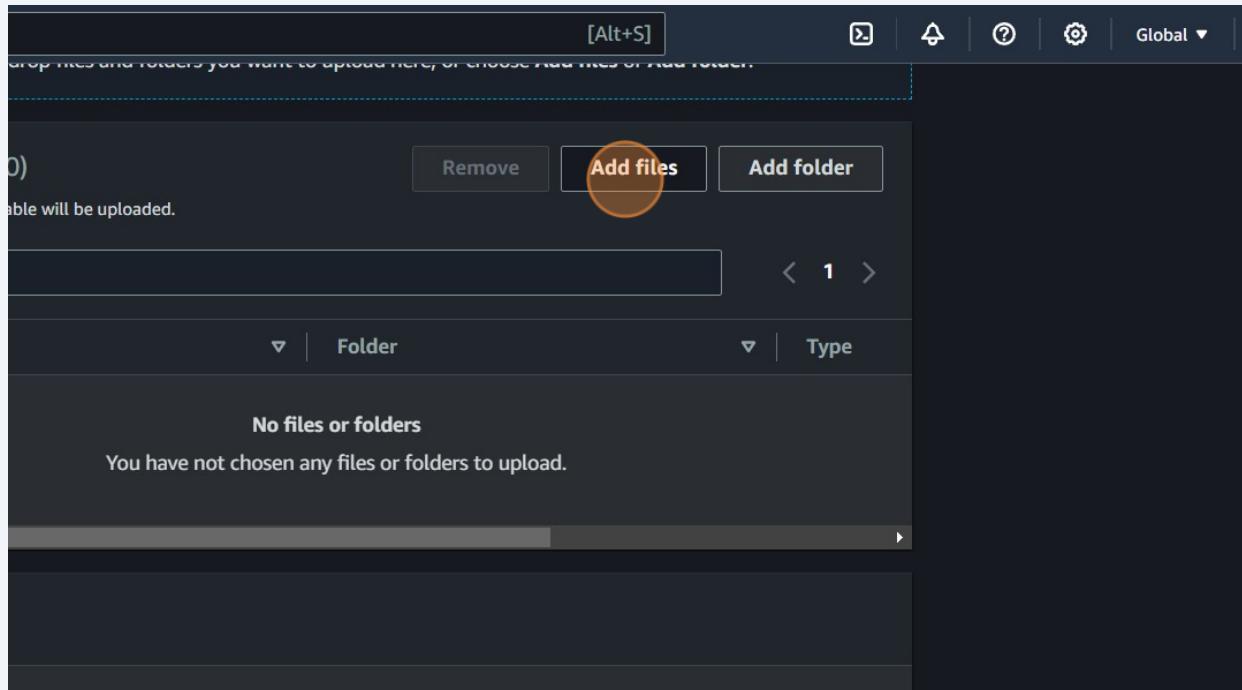
	Name	AWS Region	Access
○	buc83	US East (N. Virginia) us-east-1	Bucket
○	bucketii	US East (N. Virginia) us-east-1	Bucket
○	bucketnew121	US East (N. Virginia) us-east-1	Bucket
○	s3-buc8gate	US East (N. Virginia) us-east-1	Objects
○	s3buc-1-1	US East (N. Virginia) us-east-1	Bucket
○	s3buc-1-2	US East (N. Virginia) us-east-1	Bucket
○	s3buc-1-3	US East (N. Virginia) us-east-1	Bucket
○	s3buc3	US East (N. Virginia) us-east-1	Bucket
○	s3bucket3811	US East (N. Virginia) us-east-1	Objects

A small circular selection highlights the row for 's3bucket3811'. In the bottom left corner, there's a purple circular icon with a white dot, and the text 'CloudShell' and 'Feedback'.

9 Click "Upload" to add new files



10 Click "Add files"



## 11 Add the files

Services Search [Alt+S] Global

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

**Files and folders (2 Total, 450.0 B)**

All files and folders in this table will be uploaded.

Find by name < 1 >

<input type="checkbox"/>	Name	Folder	Type
<input type="checkbox"/>	error.html	-	text/html
<input type="checkbox"/>	index.html	-	text/html

**Destination** Info

Destination  
s3://s3bucket3811

▶ Destination details Bucket settings that impact new objects stored in the specified destination.

▶ Permissions Grant public access and access to other AWS accounts.

## 12 Upload the files

will be uploaded.

< 1 >

<input type="checkbox"/>	Folder	Type
<input type="checkbox"/>	-	text/html

new objects stored in the specified destination.

other AWS accounts.

settings, tags, and more.

Cancel **Upload**

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

**13** Click the "Permissions"

The screenshot shows the AWS S3 console. In the top navigation bar, there's a search bar and a services dropdown. Below the navigation, the breadcrumb path shows 'Amazon S3 > Buckets > s3bucket3811'. The main title is 's3bucket3811' with an 'Info' link. A horizontal menu bar below the title includes 'Objects', 'Properties', 'Permissions' (which has a yellow circle around it), 'Metrics', 'Management', and 'Access Points'. Under the 'Bucket overview' section, there are two main items: 'AWS Region' (US East (N. Virginia) us-east-1) and 'Amazon Resource Name (ARN)' (arn:aws:s3:::s3bucket3811). Below this, there's a 'Bucket Versioning' section with a note about versioning.

**14** Check the policy

The screenshot shows the 'Edit' page for a bucket policy. At the top, there's a search bar and a global dropdown. The main content area has a heading 'public access' with a note about Block Public Access settings. Below this is a 'policy' section with a JSON editor. The JSON code is as follows:

```
policy
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::s3bucket3811/*"
        }
    ]
}
```

At the bottom right of the JSON editor, there's a 'Copy' button. On the far right of the page, there are 'Edit', 'Delete', and other navigation links.

**15** Since no policy is defined, go to <https://awspolicygen.s3.amazonaws.com/policygen.html> to generate the policy.

## 16 Copy the ARN

The screenshot shows the AWS S3 Bucket Overview page. At the top, there's a search bar and a 'Copy' button with the text 'arn:aws:s3:::s3bucket3811'. A large orange circle highlights this button. Below the header, the bucket name 's3bucket3811' is displayed. Under the 'Bucket Versioning' section, it says 'Enabled' and provides a link to learn more about MFA delete.

## 17 Select S3 Bucket Policy as policy type. Deny the effect. In Principal write \*.In Actions, select PutObject and in Amazon Resource Name enter the value we found on the previous screen with the name Bucket ARN.

The screenshot shows the AWS IAM Policy Editor. It's a step-by-step guide for creating a policy. Step 3 is shown, where a new statement is being added. The 'Principal' field contains an asterisk (\*). The 'AWS Service' dropdown is set to 'Amazon S3'. The 'Actions' dropdown shows '1 Action(s) Selected'. The 'Amazon Resource Name (ARN)' field contains 'arn:aws:s3:::s3bucket3811/\*'. A large orange circle highlights the 'Add Statement' button at the bottom right of the form.

### 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.

**Add one or more statements above to generate a policy.**

## 18 Add the conditions.

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

Add Conditions (Optional)  
Conditions are any restrictions or details about the statement.(More Details).

Condition	Null
Key	s3:x-amz-server-side-encryption
Value	true

**Add Condition** **Add Statement**

**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.  
**Add one or more statements above to generate a policy.**

## 19 Click on add statement button.

Key	s3:x-amz-server-side-encryption
Value	

**Add Condition**

Condition	Keys
Null	• s3:x-amz-server-side-encryption: "true"

**Add Statement**

**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.  
**Add one or more statements above to generate a policy.**

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technology in compliance with all applicable terms and conditions. This AWS Policy Generator is provided **as is** without warranty of any kind, whether express or implied. The generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technology.

## 20 Click "Generate Policy"

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

Principal(s)	Effect	Action	Resource	Conditions
• *	Deny	• s3:PutObject	arn:aws:s3:::s3bucket3811/*	• Null ◦ s3:x-amz-server-side-encryption: "true"

### 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.

**Generate Policy**

[Start Over](#)

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies in compliance with all applicable terms and conditions. This AWS Policy Generator is provided **as is** without warranty of any kind, whether express, implied or otherwise. The AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.

An [amazon.com](#) company

## 21 Copy the policy details

You added the following statements:

Principal(s)	Effect	Action	Resource	Conditions
• *	Deny	• s3:PutObject	arn:aws:s3:::s3bucket3811/*	• Null ◦ s3:x-amz-server-side-encryption: "true"

**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.

**Actions** -- Select Actions --

**Amazon Resource Name (ARN)**

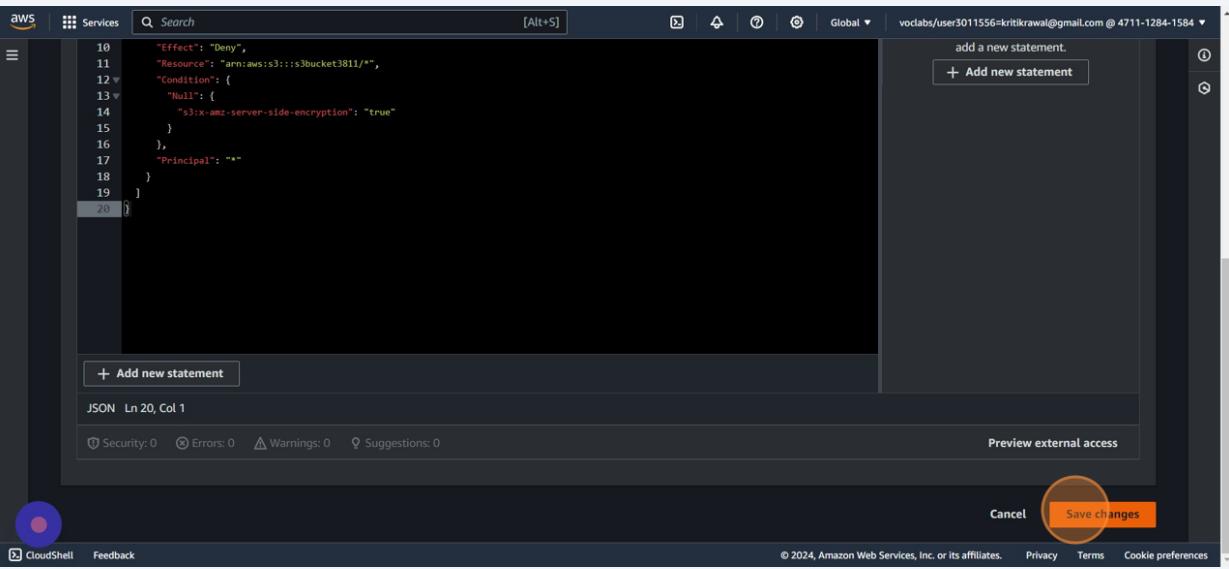
ARN should follow the following format: arn:aws:s3:::\${BucketName}

**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": "Policy1708451971752",
"Version": "2012-10-17",
"Statement": [
{
  "Sid": "Stmt1708451969218",
  "Action": [
    "s3:PutObject"
  ],
  "Effect": "Deny",
  "Resource": "arn:aws:s3:::s3bucket3811/*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption": "true"
    }
  },
  "Principal": "*"
}
```

**22** Paste the policy details and save it.



The screenshot shows the AWS IAM Policy Editor interface. A JSON policy document is displayed, containing a single deny statement that restricts access to objects in an S3 bucket if they are not encrypted with server-side encryption. The policy is being edited in a modal window. At the bottom right of the modal, there are 'Cancel' and 'Save changes' buttons, with 'Save changes' being highlighted by a red circle.

```
10 "Effect": "Deny",
11 "Resource": "arn:aws:s3:::s3bucket3811/*",
12 "Condition": {
13     "Null": {
14         "s3:x-amz-server-side-encryption": "true"
15     },
16 },
17 "Principal": "*"
18 }
19 ]
20 }
```

+ Add new statement

JSON Ln 20, Col 1

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Preview external access

Cancel Save changes

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

**23** The policy is defined.