

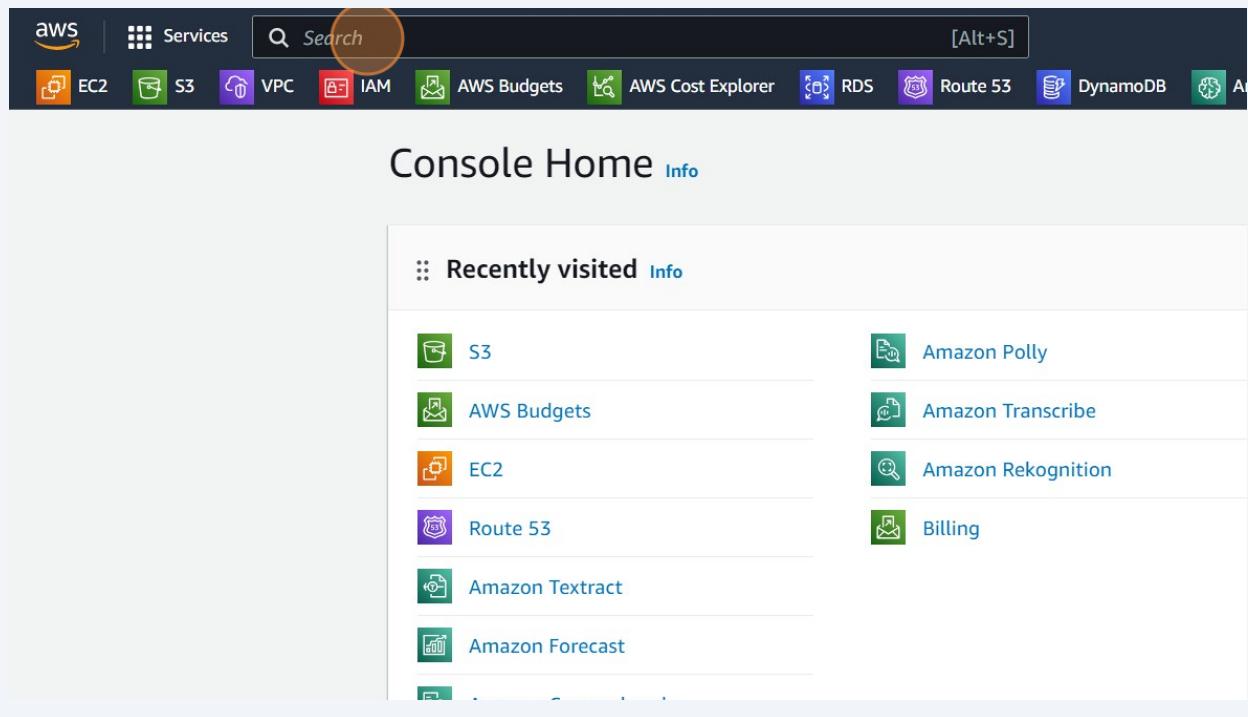
S3 Bucket Permissions

This guide provides step-by-step instructions on how to configure bucket permissions in AWS S3. By following these steps, users can ensure that their S3 bucket is secure and has the appropriate access settings. This guide covers enabling block public access, setting bucket policies, and verifying file access.

This guide was created by Nijat Hajiyev

- 1 Navigate to aws.amazon.com

- 2 Click the "Search" field.



- 3 Type "S3"

4 Click "S3"

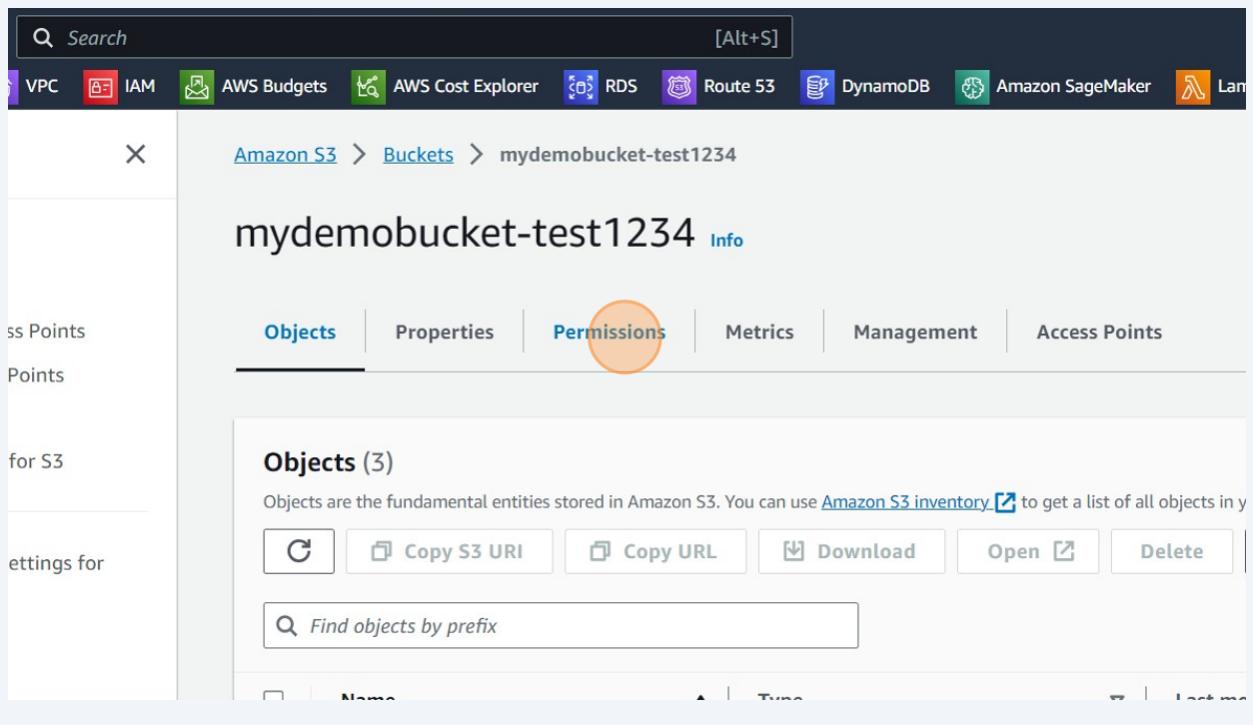
The screenshot shows the AWS search interface with the query 'S3' entered in the search bar. The results are categorized under 'Services (8)'. The top result is 'S3 Scalable Storage in the Cloud', which is highlighted with a yellow circle around its icon. Below it are other services: 'S3 Glacier Archive Storage in the Cloud' and 'AWS Snow Family Large Scale Data Transport'.

5 Click "mydemobucket-test1234"

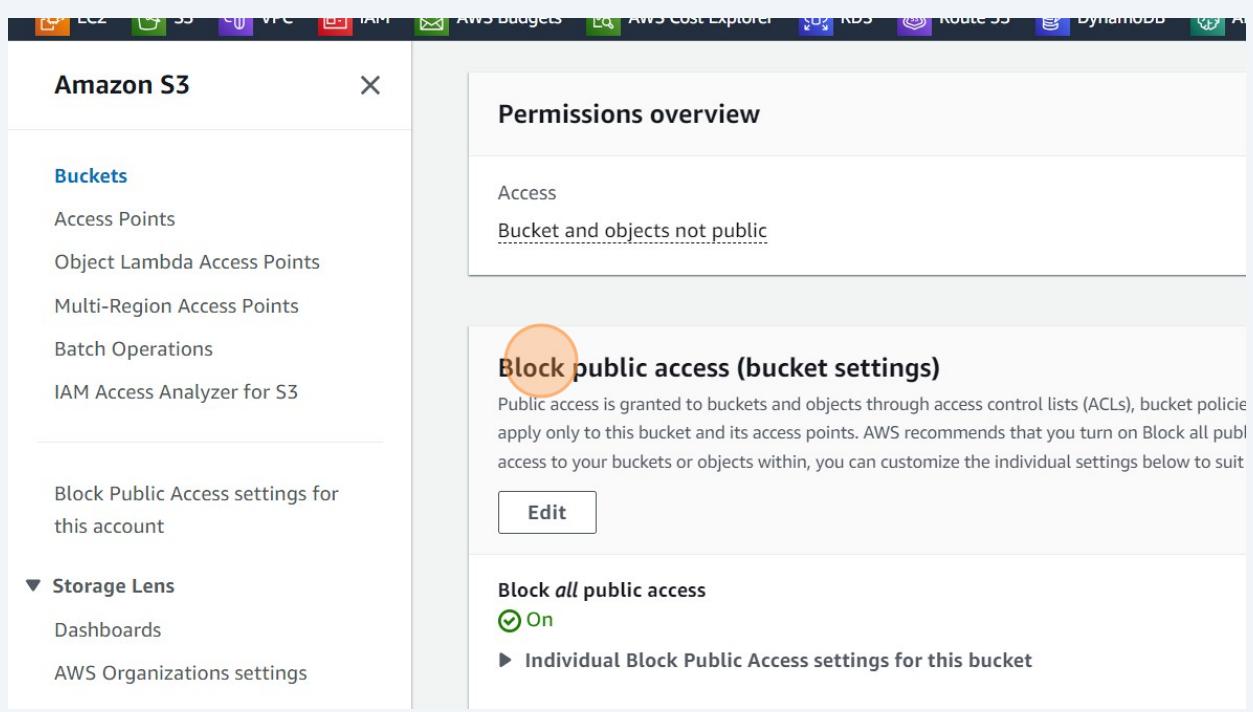
The screenshot shows the AWS S3 Buckets page. On the left, there's a sidebar with links like 'Batch Operations', 'Storage Lens', and 'Feature spotlight'. The main area is titled 'Buckets (5) Info' and contains a table of buckets. One bucket, 'mydemobucket-test1234', is highlighted with a yellow circle around its name in the 'Name' column.

Name	AWS Region
cf-templates-ifb7oz4v95cf-us-east-1	US East (N. Virginia)
elasticbeanstalk-us-east-1-337238043030	US East (N. Virginia)
mydemobucket-test1234	Europe (Frankfurt)
sagemaker-studio-291xtdyoxgd	US East (N. Virginia)
textract-console-eu-central-1-ab0c1123-5774-4d11-a50d-061abce7f	Europe (Frankfurt)

6 Click "Permissions"



7 Check "Block public access (bucket settings)"



8 Check "On"

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

▼ Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight 7

► AWS Marketplace for S3

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies apply only to this bucket and its access points. AWS recommends that you turn on Block all public access to your buckets or objects within, you can customize the individual settings below to suit

[Edit](#)

Block all public access

On

► Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies apply only to this bucket and its access points.



Public access is blocked because Block Public Access settings are turned on.

9 Click "Edit"

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

▼ Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight 7

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 apply only to this bucket and its access points. AWS recommends that you turn on Block all public access to your buckets or objects within, you can customize the individual settings below to suit

[Edit](#)

Block all public access

On

► Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies apply only to this bucket and its access points.

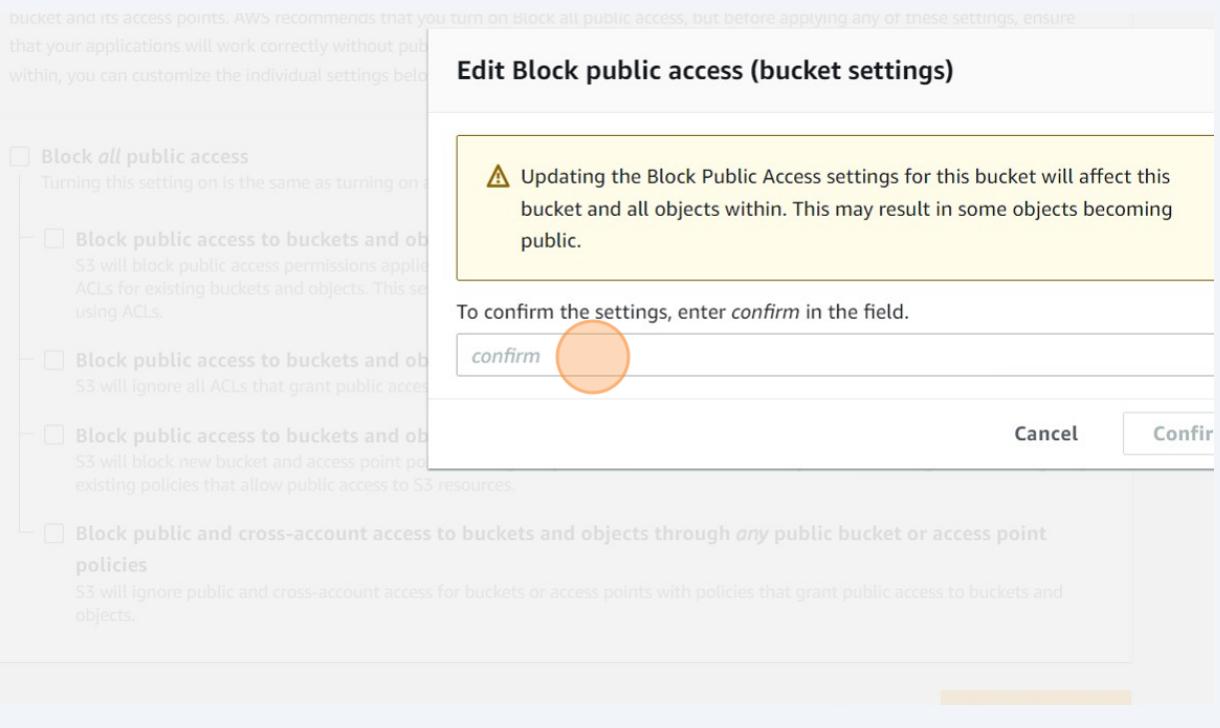
10 Click this checkbox.

The screenshot shows the 'Edit Block public access (Bucket settings)' page. On the left sidebar, under 'Buckets', there's a section for 'Block Public Access settings for this account'. Below it, 'Storage Lens' is expanded, showing 'Dashboards' and 'AWS Organizations settings'. A 'Feature spotlight' section is also present. The main content area is titled 'Block public access (bucket settings)'. It contains a heading 'Block all public access' with a checked checkbox, which is highlighted with a red circle. Below this, three other checkboxes are listed: 'Block public access to buckets and objects granted through new access control lists (ACLs)', 'Block public access to buckets and objects granted through any access control lists (ACLs)', and 'Block public access to buckets and objects granted through new public bucket or access point policies'. The 'Block all public access' checkbox is checked.

11 Click "Save changes"

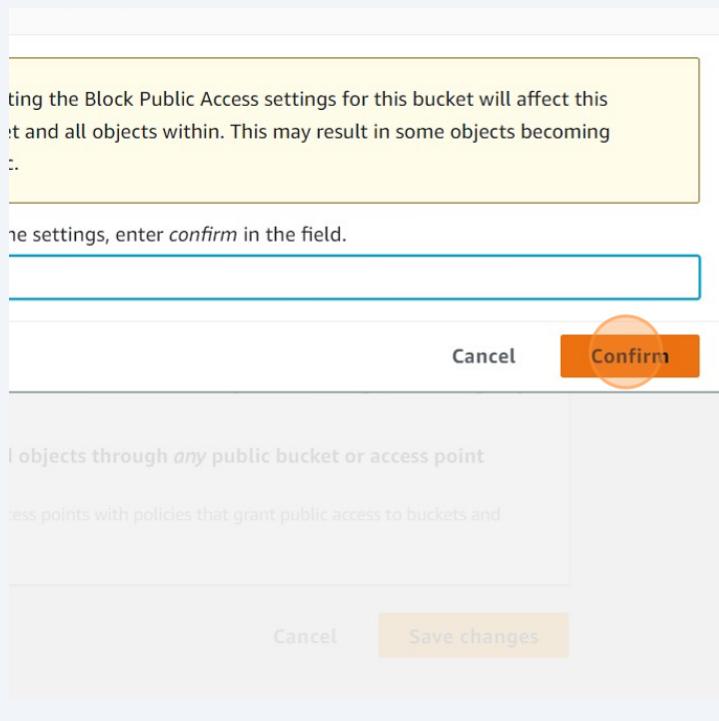
The screenshot shows the 'Edit Block public access (bucket settings)' dialog box. At the top, the title is 'Edit Block public access (bucket settings)'. The main content area is titled 'Block public access (bucket settings)'. It contains a heading 'Block all public access' with a checked checkbox, which is highlighted with a red circle. Below this, three other checkboxes are listed: 'Block public access to buckets and objects granted through new access control lists (ACLs)', 'Block public access to buckets and objects granted through any access control lists (ACLs)', and 'Block public access to buckets and objects granted through new public bucket or access point policies'. The 'Block all public access' checkbox is checked. At the bottom of the dialog box, there are 'Cancel' and 'Save changes' buttons, with 'Save changes' highlighted with a red circle.

12 Click the "confirm" field.



13 Type "confirm"

14 Click "Confirm"



15 Check "Off"

The screenshot shows the AWS S3 Bucket Properties page. On the left, there's a sidebar with links like "Batch Operations", "IAM Access Analyzer for S3", "Block Public Access settings for this account", "Storage Lens", "Dashboards", "AWS Organizations settings", "Feature spotlight (7)", and "AWS Marketplace for S3". The main content area is titled "Block public access (bucket settings)". It explains that public access is granted through ACLs and bucket policies and recommends turning on "Block all public access". A large "Edit" button is present. Below it, a section titled "Block all public access" shows a toggle switch set to "Off", which is also circled in red. A note below says "Individual Block Public Access settings for this bucket". Another section titled "Bucket policy" is partially visible at the bottom.

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, and other AWS services. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access to your buckets or objects within; you can customize the individual settings below to suit your needs.

Edit

Block all public access

Off

Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies can be used to grant or deny access to objects in the bucket based on specific conditions.

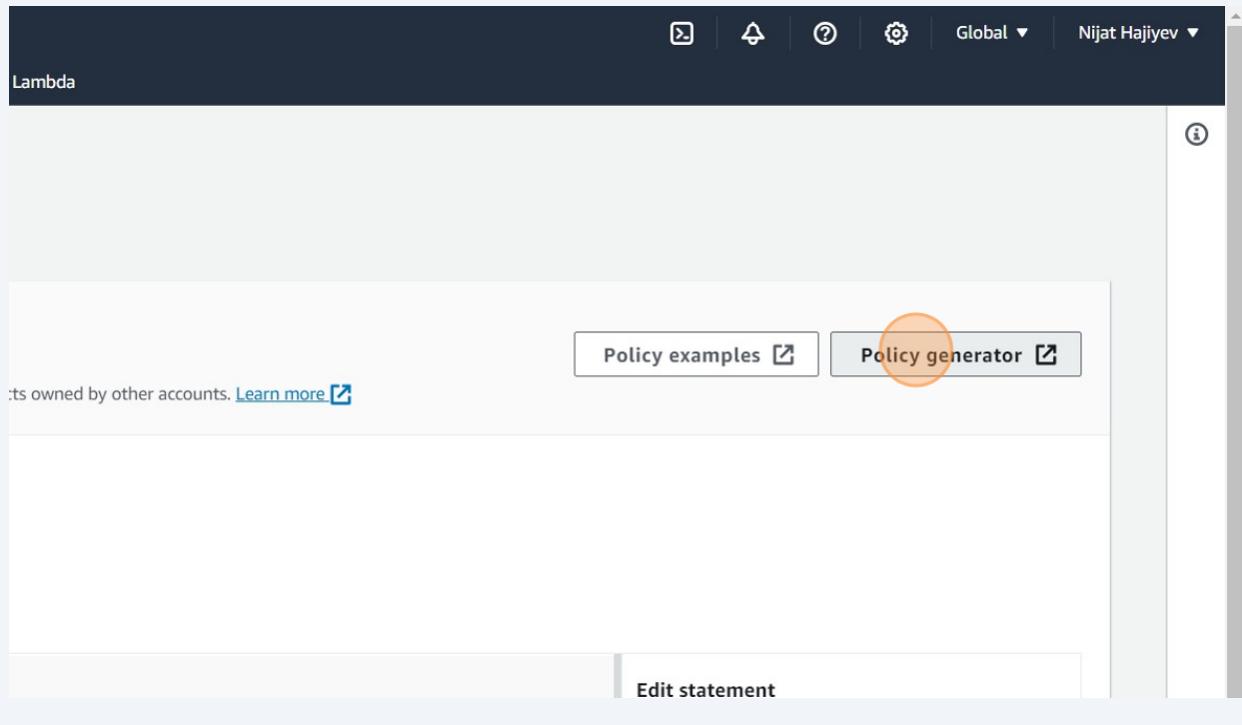
16 Click "Bucket policy"

The screenshot shows the AWS S3 console. In the top navigation bar, there are links for EC2, S3, VPC, IAM, AWS Budgets, AWS Cost Explorer, RDS, Route 53, DynamoDB, and CloudWatch Metrics. Below the navigation bar, the title "Amazon S3" is followed by a close button (X). A green success message banner at the top right says "Successfully edited Block Public Access settings for this bucket." On the left sidebar, under the "Buckets" section, there are links for Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and IAM Access Analyzer for S3. Under "Block Public Access settings for this account", there is a link for "Storage Lens". The main content area displays the "Bucket policy" settings. It shows that "Block all public access" is set to "Off". A link "Individual Block Public Access settings for this bucket" is also present. The "Bucket policy" section is titled "Bucket policy" and contains the note: "The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies can be used to grant or deny access to objects in the bucket." Below this, it says "No policy to display.".

17 Click "Edit"

The screenshot shows the AWS Lambda console. The top navigation bar has a dark header with the word "Lambda". Below the navigation bar, there is a green success message banner with an "X" icon and an information icon. The main content area shows a table with one row. The first column of the table contains the text "Owned by other accounts. [Learn more](#)". The second column contains two buttons: "Edit" (which is highlighted with an orange circle) and "Delete". In the bottom right corner of the table cell, there is a "Copy" button.

18 Click "Policy generator"



19 Click this dropdown and select "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

Principal

Use a comma to separate multiple values.

AWS Service All Services (*)

20 Click "Allow"

Key concepts in using AWS Identity and Access Management. Here are sample policies.

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, or a Lambda Execution Role Policy.

Select Type of 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

Principal

Use a comma to separate multiple values.

AWS Service

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

Actions All Actions ('*')

Amazon Resource Name (ARN)

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

21 Click the "Principal" field.

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, or a Lambda Execution Role Policy.

Select Type of 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.

22 Type "*"

23 Click "-- Select Actions --"

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 s

Effect Allow Deny

Principal

Use a comma to separate multiple values.

AWS Service All

Actions All Actions ('*')

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)

No Action selected. You must select at least one Act

Step 3: Generate Policy

24 Click "GetObject"

The screenshot shows the AWS Policy Generator interface. The 'Actions' dropdown menu is open, displaying various S3 actions. The 'GetObject' action is highlighted with a red circle. A red box highlights the 'GetObject' action in the list.

Use a comma to separate multiple values.

AWS Service: Amazon S3

Actions: -- Select Actions --

Amazon Resource Name (ARN)

Must select at least one Action

All Actions ('*')

- GetMetricsConfiguration
- GetMultiRegionAccessPoint
- GetMultiRegionAccessPointPolicy
- GetMultiRegionAccessPointPolicyStatus
- GetMultiRegionAccessPointRoutes
- GetObject **(highlighted)**
- GetObjectAcl

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technology. Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not

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.

25 Click the "Amazon Resource Name (ARN)" field.

The screenshot shows the AWS Policy Generator interface. The 'Amazon Resource Name (ARN)' input field is highlighted with a red circle. A red box highlights the 'Amazon Resource Name (ARN)' field.

A statement is the formal description of a single permission. See a [description of elements](#) that you can use in statements.

Effect: Allow Deny

Principal: *

Use a comma to separate multiple values.

AWS Service: Amazon S3

Actions: 1 Action(s) Selected

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)

Add Statement Resource field is not valid. You must enter a valid ARN.

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.

26 Click here.

The screenshot shows the AWS S3 console's 'Edit bucket policy' page. On the left, there's a sidebar with various links like 'Access Points', 'Object Lambda Access Points', etc. A section titled 'Storage Lens' is expanded, showing 'Dashboards' and 'AWS Organizations settings'. At the bottom of the sidebar, there's a 'Feature spotlight' section with a blue button containing the number '7'. The main area is titled 'Edit bucket policy' and contains a 'Bucket policy' section. Below it, the 'Bucket ARN' field is highlighted with an orange circle, showing the value 'arn:aws:s3:::mydemobucket-test1234'. The 'Policy' field is currently empty, with the number '1' displayed in a dark box.

27 Type "/" after "Bucket ARN"

bucket arn + /*

28 Click this button.

Use a comma to separate multiple values.

AWS Service Amazon S3 All S

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:::mydemobucket

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

Add Conditions (Optional)

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 technologies and Generator is provided **as is** without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the

29 Click "Generate Policy"

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

Principal(s)	Effect	Action	Resource
• *	Allow	• s3:GetObject	arn:aws:s3:::mydemobucket-test12

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 and Generator is provided **as is** without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the

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

An [amazon.com](#) company

30

Click "{
"Id": "Policy1699043131160",
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Stmt1699043124391",
"Action": [
"..."

The screenshot shows the AWS Policy Generator interface. At the top, it says 'Actions' and 'Amazon Resource Name (ARN)'. Below that, a message says 'You added the following statements.' followed by a table:

Principal(s)	Effect
*	Allow

Below the table, it says 'Step 3: Generate Policy'. A note states: 'A policy is a document (written in the JSON format) that defines what actions are allowed or denied for specific users or groups.' There is a 'Close' button and a 'Generate Policy' button.

The JSON code shown is:

```
{
  "Id": "Policy1699043131160",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1699043124391",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::mydemobucket-test1234/*",
      "Principal": "*"
    }
  ]
}
```

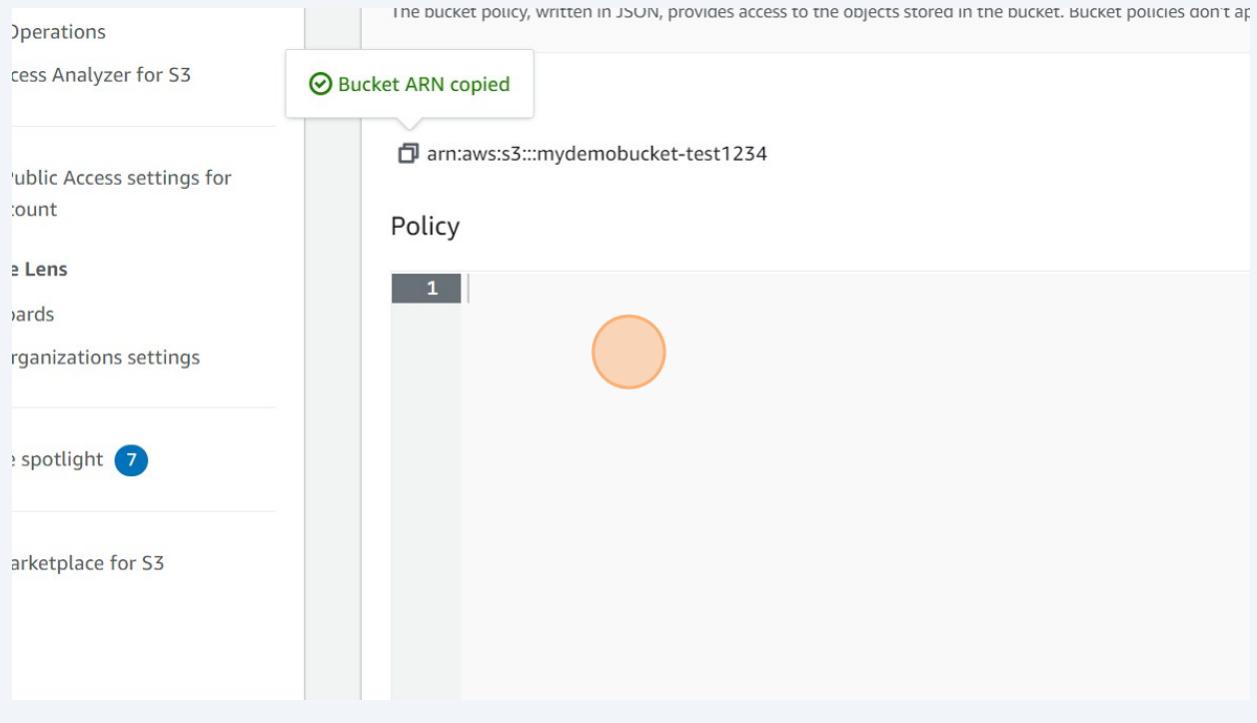
31

Copy. Press **ctrl + c**

32

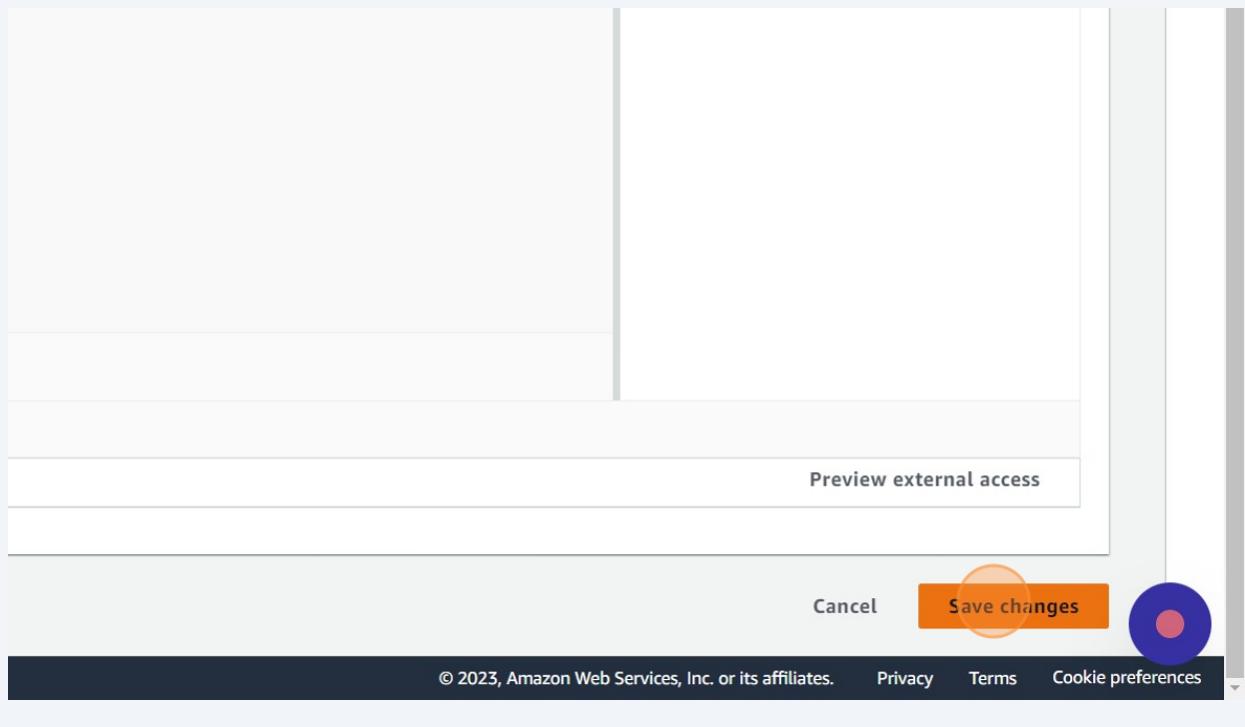
Press **ctrl + c**

33 Click here.



34 Paste. Press **ctrl + v**

35 Click "Save changes"



Access file from Object URL

36 Click "Objects"

A screenshot of the AWS S3 bucket permissions overview page. On the left, there is a sidebar with options like 'Buckets', 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', and 'IAM Access Analyzer for S3'. Below this is a section for 'Block Public Access settings for this account'. On the right, the main content area shows the bucket name 'mydemobucket-test1234' and its 'Permissions' tab is selected. Under the 'Permissions overview' section, it says 'Bucket and objects not public'. At the bottom, there is a link 'Block public access (bucket settings)'.

37 Click "beach.jpg"

The screenshot shows the AWS S3 console. On the left, there's a sidebar with links like 'Batch Operations', 'IAM Access Analyzer for S3', 'Block Public Access settings for this account', 'Storage Lens' (which is expanded), 'Dashboards', 'AWS Organizations settings', 'Feature spotlight' (with a '7' badge), and 'AWS Marketplace for S3'. The main area is titled 'Objects (3)' and contains a table with three rows:

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	beach.jpg	jpg
<input type="checkbox"/>	coffee.jpg	jpg
<input type="checkbox"/>	index.html	html

A search bar at the top says 'Find objects by prefix'.

38 Click "Object URL" link

The screenshot shows the AWS S3 Object Details page for the object 'beach.jpg'. The object has the following metadata:

- Amazon Resource Name (ARN): [arn:aws:s3:::mydemobucket-test1234/beach.jpg](#)
- Entity tag (Etag): [1c6defc638f71abd065d8dd2f450b207](#)
- Object URL: <https://mydemobucket-test1234.s3.eu-central-1.amazonaws.com/beach.jpg>

At the bottom of the page, there's a note: 'Configurations impact the behavior of this object.'

39 Check file opened.

