

Public Bucket

1 Step: Making a public bucket

Permissions - Block public access(Edit) - Off

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

Buckets (2)

Info

Refresh

Copy ARN

Empty

Delete

Create bucket

Buckets are containers for data stored in S3. [Learn more](#)

Find buckets by name

< 1 > ⚙

	Name	AWS Region	Access	Creation date
<input type="radio"/>	git-prosimplee-bucket	US East (N. Virginia) us-east-1	Bucket and objects not public	April 3, 2022, 00:31:30 (UTC+03:00)
<input type="radio"/>	testing-bucket-git-prosimplee	EU (London) eu-west-2	<div>Public</div>	April 3, 2022, 11:50:27 (UTC+03:00)

2 Step: Upload your files

Objects

PropertiesPermissionsMetricsManagementAccess Points

Objects (1)

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](#)

Refresh

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

Show versions

< 1 > ⚙

	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	<div>file_with_text.txt</div>	txt	April 3, 2022, 11:58:34 (UTC+03:00)	18.0 B	Standard

3 Step: Add files

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, 357.0 B)

RemoveAdd filesAdd folder

All files and folders in this table will be uploaded.

Find by name

< 1 >

	Name	Folder	Type	Size
<input type="checkbox"/>	test_read_s3.txt	-	text/plain	357.0 B

4 Step: Choose Permissions

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

Info

AWS recommends using S3 bucket policies or IAM policies for access control. [Learn more](#)

Access control list (ACL)

☐ Choose from predefined ACLs

☒ Specify individual ACL permissions

Grantee

Objects

Object ACL

Object owner (your AWS account)

☒ Read

☒ Read

☒ Write

Canonical ID:

3e2f5e44da6d2be77dba43c1be5653ab4097664524b305321958d7dfe7c0467b

Everyone (public access)

☒

Read

☐ Read

Group:

http://acs.amazonaws.com/groups/global/AllUsers

☐ Write

5 Step: Choose Storage class

Storage class

Amazon S3 offers a range of storage classes designed for different use cases. [Learn more](#) or see [Amazon S3 pricing](#)

Storage class	Designed for	Availability Zones	Min storage duration
<input checked="" type="radio"/> Standard	Frequently accessed data (more than once a month) with milliseconds access	≥ 3	-
<input type="radio"/> Intelligent-Tiering	Data with changing or unknown access patterns	≥ 3	-
<input type="radio"/> Standard-IA	Infrequently accessed data (once a month) with milliseconds access	≥ 3	30 days
<input type="radio"/> One Zone-IA	Recreateable, infrequently accessed data (once a month) stored in a single Availability Zone with milliseconds access	1	30 days

6 Step: Upload your file