

# AWS: CREATE S3 BUCKET

## STEP 1: Creating S3 bucket named **my-assessment-bucket-1**.

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)  
Buckets are containers for data stored in S3.

**General configuration**

**AWS Region**  
US East (N. Virginia) us-east-1

**Bucket type** [Info](#)  
☒ **General purpose**  
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.  
☐ **Directory**  
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

**Bucket name** [Info](#)  
  
Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#) [?](#)

**Copy settings from existing bucket - optional**  
Only the bucket settings in the following configuration are copied.  
[Choose bucket](#)  
Format: s3://bucket/prefix

**Object Ownership** [Info](#)  
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.  
☒ **ACLs disabled (recommended)**  
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.  
☐ **ACLs enabled**  
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

**Object Ownership**  
Bucket owner enforced


**Block Public Access settings for this bucket**  
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 this bucket and its 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 this bucket and its access points, [Learn more](#) [?](#)

☒ **ACLs disabled (recommended)**  
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.  
☐ **ACLs enabled**  
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

**Object Ownership**  
Bucket owner enforced

**Block Public Access settings for this bucket**  
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 this bucket and its 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 this bucket and its access points, 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.

 **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.  
☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

**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](#) [?](#)

**Bucket Versioning**  
☒ **Disable**  
☐ **Enable**

- Bucket has been created successfully.

Amazon S3 > Buckets

Successfully created bucket "my-assessment-bucket-1"

View details

Account snapshot - updated every 24 hours

View Storage Lens dashboard

General purpose buckets

Directory buckets

General purpose buckets (1)

Info

All AWS Regions

Buckets are containers for data stored in S3.

Find buckets by name

< 1 >

Copy ARN

Empty

Delete

Create bucket

Name	AWS Region	IAM Access Analyzer	Creation date
my-assessment-bucket-1	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	February 14, 2025, 12:10:40 (UTC+05:30)

STEP 2: Uploaded the file in the bucket which has been created.

Upload succeeded

For more information, see the Files and folders table.

Close

Upload: status

After you navigate away from this page, the following information is no longer available.

Summary

Destination

s3://my-assessment-bucket-1

Succeeded

1 file, 190.2 KB (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 total, 190.2 KB)

Find by name

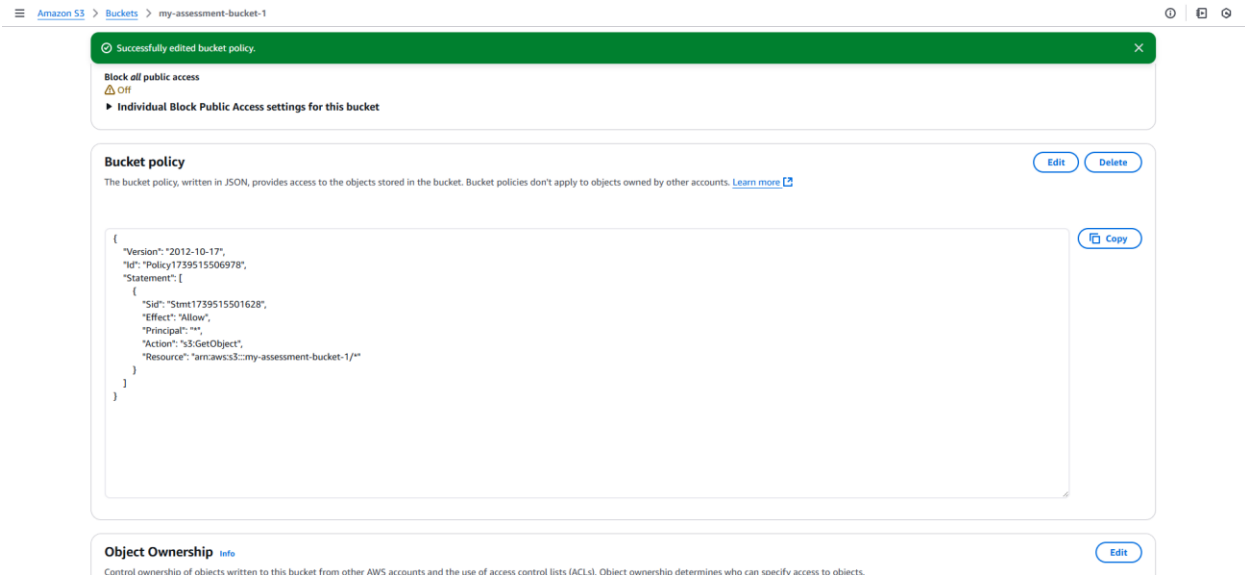
< 1 >

Name	Folder	Type	Size	Status	Error
<a href="#">GENERATING_CSR.pdf</a>	-	application/pdf	190.2 KB	Succeeded	-

STEP 3: Create policy for the S3 Bucket.

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

Principal(s)	Effect	Action	Resource	Conditions
<ul style="list-style-type: none"><li>*</li></ul>	Allow	<ul style="list-style-type: none"><li>s3:GetObject</li></ul>	arn:aws:s3:::my-assessment-bucket-1	None



- Successfully added the bucket policy.

#### STEP 4: Check the public access: [Public Access URL](#)

