

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 preferred

If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

Object writer

The object writer remains the object owner.

(i) If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more

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 or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

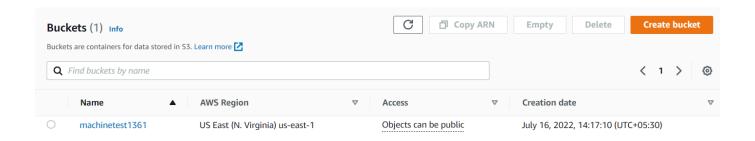
	Block all public access
	Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
ŀ	☐ Block public access to buckets and objects granted through <i>new</i> access control lists (ACLs)
	S3 will block public access permissions 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.
L	☐ Block public access to buckets and objects granted through <i>any</i> 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 <i>new</i> 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.
L	☐ Block public and cross-account access to buckets and objects through <i>any</i> 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

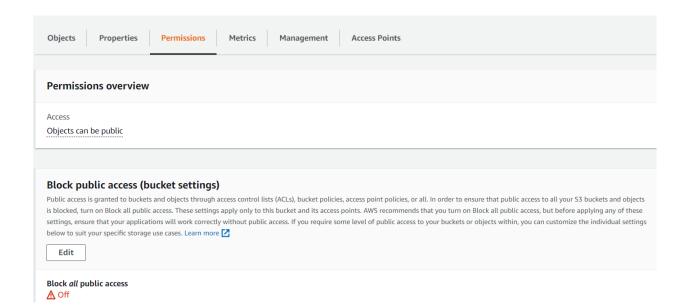
	oning
every version of ev	ns of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore ery object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions ures. Learn more
Bucket Versionir	g
Disable	
○ Enable	
Tags (0) - <i>op</i>	tional
_	or other criteria by tagging your bucket. Learn more 🗹
No tags associat	ed with this bucket.
Add tag	
rida tag	
Aud tug	
	vption
Default enci	yption ypt new objects stored in this bucket. Learn more
Default enci	ypt new objects stored in this bucket. Learn more 🔀
Default enc Automatically encr	ypt new objects stored in this bucket. Learn more 🔀
Default ence Automatically ence Server-side ence	ypt new objects stored in this bucket. Learn more 🔀
Default ence Automatically ence Server-side ence Disable	ypt new objects stored in this bucket. Learn more 🔀
Default ence Automatically ence Server-side ence Disable	ypt new objects stored in this bucket. Learn more 🔀
Default ence Automatically ence Server-side ence Disable	ypt new objects stored in this bucket. Learn more 🔀
Default ence Automatically ence Server-side ence Disable	ypt new objects stored in this bucket. Learn more 🔀
Default ence Automatically ence Server-side ence Disable	ypt new objects stored in this bucket. Learn more vpt in the stored in this bucket. Learn more vpt in the stored in this bucket. Learn more vpt in the stored in this bucket. Learn more vpt in the stored in this bucket. Learn more vpt in the stored in this bucket. Learn more vpt in the stored in this bucket. Learn more vpt in the stored in this bucket. Learn more vpt in the stored in this bucket. Learn more vpt in the stored in this bucket. Learn more vpt in the stored in this bucket. Learn more vpt in the stored in this bucket. Learn more vpt in the stored in this bucket. Learn more vpt in the stored in this bucket. Learn more vpt in the stored in the

(1) After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

Create bucket

Cancel





Edit Block public access (bucket settings) Info

objects.

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 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 S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and

Cancel

Save changes

