Amazon S3

Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3

Block Public Access settings for this account

Storage Lens
Dashboards
AWS Organizations settings

Feature spotlight 3

AWS Marketplace for S3

arsany-frontend Info

Publicly accessible

Objects | Properties | Permissions | Metrics | Management | Access Points

Permissions overview

Access

Public

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

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 don't apply to objects owned by other accounts. Learn more

Edit | Delete

Copy

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

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.

Edit

Object Ownership

Bucket owner preferred

ACLs are enabled and can be used to grant access to this bucket and its objects. 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.

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. Learn more

Edit

The console displays combined access grants for duplicate grantees

To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.

AWS doesn't recommend granting access to the Everyone or Authenticated users group grantees
Anyone in the world can access the objects in this bucket.

Learn more

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: bd2ffa863969afe429c598234c897cb0240d2dce043d2e424169b22c043f9fb1	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	List	Read
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	List	Read
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	-	-

Cross-origin resource sharing (CORS)

The CORS configuration, written in JSON, defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. **Learn more**

Edit

No configurations to display

Copy