



Configuring Amazon S3 security settings and access controls



Getting started at an AWS hosted workshop

▼ S3 Security Best Practices

▼ Prepare Your Lab

- Attach IAM Role to EC2 Instance
- Connect to the EC2 Instance
- Bucket Name

▼ Lab 1 - S3 Security Exercises

- Require HTTPS
- Require SSE-KMS Encryption
- Restrict Access to an S3 VPC Endpoint
- Use AWS Config Rules to Detect a Public Bucket
- Use Amazon Access Analyzer for S3

▼ Lab 2 - S3 Access Grants

- S3 Access Grants Lab - Initial Setup
- Configure S3 Access Grants for IAM user

▼ Lab 3 - Enabling Malware Protection for S3 by using GuardDuty

- Enabling Malware Protection for S3 for your bucket
- Testing GuardDuty Malware with an object.

▼ Lab 4 - S3 Access Control Lists

- Block Public ACLs
- [Configure S3 Block Public Access](#)

Disable S3 ACLs

- Finding S3 access control lists with S3 Inventory
- Use Amazon Athena to query CloudTrail logs and identify S3 requests that depend on ACLs

Lab Summary

[Configuring Amazon S3 security settings and access controls](#) > [S3 Security Best Practices](#) > [Lab 4 - S3 Access Control](#)

Configure S3 Block Public Access

In this exercise, we will configure S3 Block Public Access, an easy way to prevent public access to your bucket.

From the AWS console in the top search bar, search and select S3.

- Click the bucket name starting with sid-security-xxxxxxx.
- Click on the Permissions tab.
- Under Bucket Policy click Delete.
- Type delete and click Delete to confirm.

Under Block public access (bucket settings) click Edit.

Select Block public access to buckets and objects granted through **new** access control lists (ACLs).

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](#)

Click [Save changes](#).

Type confirm to confirm the new settings then click Confirm.

From your SSH session run the following command.

```
aws s3api put-object --key text01 --body textfile --bucket ${bucket}
```



The request succeeds since the default for an object ACL is private.

```
[ec2-user@storage-workshop ~]$ aws s3api put-object --key text01 --body textfile --bucket ${bucket}
{"SSEKMSKeyId": "arn:aws:kms:us-west-2:121049687582:key/7f76ab8c-d042-4392-afd8-020e04f9439a",
 "ETag": "\"f39bb2ed7b4776e409bea6ac19e188db\"",
 "ServerSideEncryption": "aws:kms"
}
[ec2-user@storage-workshop ~]$
```

From you SSH session run the following command.

```
aws s3api put-object --key text01 --body textfile --acl public-read --bucket ${bucket}
```



Since we configured Block public access to buckets and objects granted through **new** access control lists (ACLs) for the bucket, this request fails because S3 prevents new objects from being granted access public access via ACLs.

```
[ec2-user@storage-workshop ~]$ aws s3api put-object --key text01 --body textfile --acl public-read --bucket ${bucket}
An error occurred (AccessDenied) when calling the PutObject operation: User: arn:aws:sts::092526071050:assumed-role/ssw-base-template-SidS3AccessRole-xggCgtNjPrb8/i-06ee8c015c1d6e501 is not authorized to perform: s3:PutObject on resource: "arn:aws:s3:::sid-security-ca51ea00-acec-11ef-ab19-02dc4668901f/text01" because public access control lists (ACLs) are blocked by the BlockPublicAcls block public access setting.
```

From the AWS console in the top search bar, search and select S3.

- Click the bucket name starting with sid-security-xxxxxxx.
- Click on the Permissions tab.
- Under Block public access (bucket settings) click Edit.
- Unselect Block public access to buckets and objects granted through new access control lists (ACLs).

Click Save changes.

Type confirm to confirm the new settings, then click Confirm.

[Previous](#)[Next](#)