

Automated S3 Remediation to Enforce Block Public Access

Scenario

This implementation ensures that AWS automatically enforces S3 Block Public Access settings across all S3 buckets. If Block Public Access is disabled on any bucket due to unintentional modifications or unauthorized actions, the system will detect the non-compliant configuration and restore the secure settings automatically.

As a security best practice, S3 buckets should always start as private. Public access should only be allowed in specific cases, such as hosting a public website. Ideally, private and public buckets should be kept in separate AWS accounts to enforce settings like Block Public Access at the account level.

For this demonstration, we will implement Block Public Access at the bucket level.

Steps to Implement

1. Log in to AWS Console

2. Create a Non-Compliant S3 Bucket

► **Account snapshot** - updated every 24 hours All AWS Regions View Storage Lens dashboard

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

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

Name	AWS Region	IAM Access Analyzer	Creation date
config-lab-875496488523	US East (N. Virginia) us-east-1	View analyzer for us-east-1	February 18, 2025, 15:24:06 (UTC+00:00)

- Create an S3 bucket with a unique name, e.g., test-noncompliant-s3bucket-1234.

Amazon S3 > Buckets > Create bucket

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
test-noncompliant-s3bucket1234
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

- Disable "Block Public Access" by unchecking the checkbox.

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.

☐ **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.

- Confirm the settings and create the bucket.

► Advanced settings

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

Cancel

Create bucket

3. Create an AWS Config Rule

1. Navigate to **AWS Config** → **Rules** → **Add Rule**.
2. Select **Add AWS Managed Rule** and search for **s3-bucket-level-public-access-prohibited**.

[AWS Config](#) > [Rules](#) > Add rule

Step 1
Specify rule type

Step 2
Configure rule

Step 3
Review and create

Specify rule type

Add rules to help you manage the ideal configuration settings of your AWS resources. You can add any of the following predefined, customizable AWS Config Managed rules, or you can create your own AWS Config Custom rule using AWS Lambda functions or Guard Custom policy.

Select rule type

☒ **Add AWS managed rule**
Deploy the following managed rules in their default state or customize to suit your needs.

☐ **Create custom Lambda rule**
Use a Lambda function with your custom code to evaluate whether your AWS resources comply with the rule.

☐ **Create custom rule using Guard**
Use Guard Custom policy that you write to evaluate whether your AWS resources comply with the rule.

AWS Managed Rules (580)

Q s3-bucket-level-public-access-prohibited X 1 match < 1 > ⚙

	Name	Labels	Supported evaluation mode	Description
<input type="radio"/>	s3-bucket-level-public-access-prohibited	S3, Bucket, PublicAccess	DETECTIVE	Checks if S3 buckets are publicly accessible. The rule is NON_COMPLIANT if an S3 bucket is not listed in the excludedPublicBuckets parameter and bucket level settings are public.

Cancel **Next**

3. Under **Evaluation mode**, select Resources to track AWS resource changes.

4. For **Resource category**, choose AWS resources.

Scope of changes
Choose when evaluations will occur.

☐ **All changes**
When any resource recorded by AWS Config is created, changed, or deleted

☒ **Resources**
When any resource that matches the specified type, or the type plus identifier, is created, changed, or deleted

☐ **Tags**
When any resource with the specified tag is created, changed, or deleted

Resources
This rule can be triggered only when the recorded resources are created, edited, or deleted. Specify the resources to record by editing the Settings page.

Resource category **Resource type**

All resource categories ▼

Multiple selected ▼

AWS S3 Bucket X

Resource identifier - optional

Q Enter resource identifier

Parameters
Rule parameters define attributes that your resources must adhere to for compliance with the rule. Example attributes include a required tag or a specified S3 bucket. **Optional** parameters that are not valid, such as missing a key or a value, will not be saved.

Key	Value	
excludedPublicBuckets	(optional)	Remove
Add another row		

5. Select **AWS S3 Bucket** as the **Resource type**.

6. (Optional) Use **excludedPublicBuckets** to exclude specific public buckets if needed.

7. Click **Next** and then **Save**.

[AWS Config](#) > [Rules](#) > Add rule

Step 1
[Specify rule type](#)

Step 2
[Configure rule](#)

Step 3
Review and create

Review and create

Review this rule before adding it to your account

Details

Rule name
s3-bucket-level-public-access-prohibited

Description
Checks if S3 buckets are publicly accessible. The rule is NON_COMPLIANT if an S3 bucket is not listed in the excludedPublicBuckets parameter and bucket level settings are public.

Managed rule name
S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED

Evaluation mode

Proactive evaluation
Disabled

Trigger type
• When configuration changes

Scope of changes
Resources

Detective evaluation
Enabled

Resource types
S3 Bucket

Resource identifier
-

Parameters

Key	Type	Value	Description
excludedPublicBuckets	CSV		Comma-separated list of known allowed public Amazon S3 bucket names.

Cancel Previous **Save**

4. Enable Automated Remediation

1. Select the created rule and go to **Actions** → **Manage remediation**.

✓ The rule: s3-bucket-level-public-access-prohibited has been added to your account.

[AWS Config](#) > [Rules](#)

Rules

A rule is a compliance check that helps you manage your ideal configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and displays the compliance results.

Rules

Filter by compliance status
All ▼

View details Edit rule Actions ▲ **Add rule**

- Manage remediation
- Re-evaluate
- Delete results
- Delete rule

Name	Remediation action	Type	Enabled evaluation mode	
• s3-bucket-level-public-access-prohibited	Not set	AWS managed	DETECTIVE	-

2. Choose **Automatic remediation**.

▼ Select remediation method

☒ **Automatic remediation**
The remediation action gets triggered automatically when the resources in scope become noncompliant.

☐ **Manual remediation**
The selected remediation action must be triggered manually by you in order to remediate the noncompliant resources in scope.

3. Under **Choose remediation action**, search and select **AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock**.

▼ Remediation action details

Remediation actions are run using AWS Systems Manager Automation.

Choose remediation action

Remediation action ▲

Q ConfigureS3BucketP X

AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock

4. For **Resource ID parameter**, select BucketName.

▼ Resource ID parameter

Using the dropdown list, you can pass the resource ID of noncompliant resources to a parameter of the remediation available in the dropdown list depend on the selected remediation action.

n/a ▲

Q |

n/a

BucketName

5. Configure parameters:

- Set all values to true.
- Provide an **AutomationAssumeRole ARN**.

▼ Parameters

Parameters allow you to pass specific information to your remediation action, such as resource IDs or configuration settings. Each remediation action has its own set of parameters. Valid values include StringList and String. Custom SSM documents for remediation with other data types are not supported.

For StringLists, enter values as an array of strings (value 1, value 2, value 3). For Strings, enter the value as a single string (value).

BucketName

>

RESOURCE_ID

RestrictPublicBuckets

>

true

BlockPublicAcls

>

true

IgnorePublicAcls

>

true

BlockPublicPolicy

>

true

AutomationAssumeRole

>

(required)

5. IAM Role for Remediation

This role must have the following permissions:

Search for “AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock” with your search engine and you’ll [find this page](#).

Towards the bottom, you’ll see “Required IAM permissions” which tells us we need:

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:GetAccountPublicAccessBlock
- s3:PutAccountPublicAccessBlock
- s3:GetBucketPublicAccessBlock
- s3:PutBucketPublicAccessBlock

In terms of the JSON IAM policy, this is what that would translate to:

```
C: > Users > shaik > {} imrole.json > [ ] Statement
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Action": [
7                  "ssm:StartAutomationExecution",
8                  "ssm:GetAutomationExecution"
9              ],
10             "Resource": "*"
11         },
12         {
13             "Effect": "Allow",
14             "Action": [
15                 "s3:GetAccountPublicAccessBlock",
16                 "s3:PutAccountPublicAccessBlock"
17             ],
18             "Resource": "*"
19         },
20         {
21             "Effect": "Allow",
22             "Action": [
23                 "s3:GetBucketPublicAccessBlock",
24                 "s3:PutBucketPublicAccessBlock"
25             ],
26             "Resource": "arn:aws:s3:::*"
27         }
28     ]
29 }
30
```

Use the following ARN format (replace <Account ID> with your AWS account ID):

arn:aws:iam::<Account ID>:role/AutomatedS3Remediation

ARN for the role created by my account id

"arn:aws:iam::875496488523:role/AutomatedS3Remediation"

Parameters

Key	Value	Description
AutomationAssumeRole	arn:aws:iam::875496488523:role/AutomatedS3Remediation	(Required) The ARN of the role that allows Automation to perform the actions on your behalf.
BucketName	RESOURCE_ID	(Required) The bucket name (not the ARN).
RestrictPublicBuckets	true	(Optional) Specifies whether Amazon S3 should restrict public bucket policies for this bucket. Setting this element to TRUE restricts access to the bucket.
BlockPublicPolicy	true	(Optional) Specifies whether Amazon S3 should block public bucket policies for this bucket. Setting this element to TRUE causes Amazon S3 to block public bucket policies.
BlockPublicAcls	true	(Optional) Specifies whether Amazon S3 should block public access control lists (ACLs) for this bucket and objects in this bucket.
IgnorePublicAcls	true	(Optional) Specifies whether Amazon S3 should ignore public ACLs for this bucket and objects in this bucket. Setting this element to TRUE causes Amazon S3 to ignore public ACLs.

Success! s3-bucket-level-public-access-prohibited has been updated.

AWS Config > Rules > s3-bucket-level-public-access-prohibited

s3-bucket-level-public-access-prohibited

Actions

Rule details

Description

Checks if S3 buckets are publicly accessible. The rule is NON_COMPLIANT if an S3 bucket is not listed in the excludedPublicBuckets parameter and bucket level settings are public.

Config rule ARN

arn:aws:config:us-east-1:875496488523:config-rule/config-rule-hokk2a

Enabled evaluation mode

- DETECTIVE

Last successful detective evaluation

February 18, 2025 3:46 PM

Detective evaluation trigger type

- Oversized configuration changes
- Configuration changes

Scope of changes

Resources

Resource types

S3 Bucket

Parameters

Key	Type	Value	Description
excludedPublicBuckets	CSV	-	Comma-separated list of known allowed public Amazon S3 bucket names.

Remediation action

Remediation action

AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock

Description

Document Name - AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock

What does this document do?

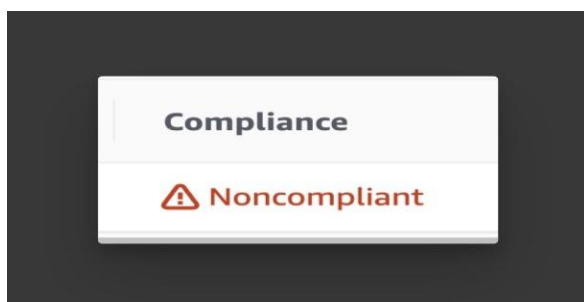
This document is used to create or modify the PublicAccessBlock configuration for an Amazon S3 bucket.

Input Parameters

- BucketName: (Required) Name of the S3 bucket (not the ARN).

6. Testing Automated Remediation

- Go to the **AWS Config Rule** page and check **Resources in scope**.



- If the bucket is not listed as non-compliant, wait a few minutes or click **Re-evaluate**.
- AWS Config will automatically remediate the issue within 10-30 minutes.
- Once remediation is successful, the bucket should be marked as compliant.

Compliant	test-compliant-s3bucket1234	S3 Bucket	-	-	Compliant
Noncompliant	test-noncompliant-s3bucket1234	S3 Bucket	-	-	Compliant

- Check the **Resource Timeline** in AWS Config to verify compliance changes.

6. Confirm in **S3 settings** that Block Public Access is enabled.

test-noncompliant-s3bucket1234 [Info](#)

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

Permissions overview

Access finding
Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#) [View analyzer for us-east-1](#)

Block public access (bucket settings) [Edit](#)

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
On

► Individual Block Public Access settings for this bucket

Conclusion & Next Steps

This setup ensures that any unauthorized attempt to disable Block Public Access on an S3 bucket will automatically be reverted, providing a strong security mechanism.

Next Steps:

1. Implement this setup using **Infrastructure as Code (IaC)** with Terraform or AWS CloudFormation.
2. Extend the remediation to enforce **account-level Block Public Access** instead of just at the bucket level for enhanced security.

References:

Amazon Web Services (AWS), n.d. *AWS Config Developer Guide*. Available at: <https://docs.aws.amazon.com/config/> [Accessed 18 Feb. 2025].

Amazon Web Services (AWS), n.d. *Automated S3 Remediation to Enforce Block Public Access*. Available at: <https://docs.aws.amazon.com/systems-manager-automation-runbooks/latest/userguide/automation-aws-block-public-s3.html> [Accessed 18 Feb. 2025].

Amazon Web Services (AWS), n.d. *Amazon S3 User Guide*. Available at: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html> [Accessed 18 Feb. 2025].

Cybr, n.d. *Introduction to AWS Security - Automated S3 Remediation to Enforce Block Public Access*. Available at: <https://cybr.com/courses/introduction-to-aws-security/lessons/lab-automated-s3-remediation-to-enforce-block-public-access/> [Accessed 18 Feb. 2025].