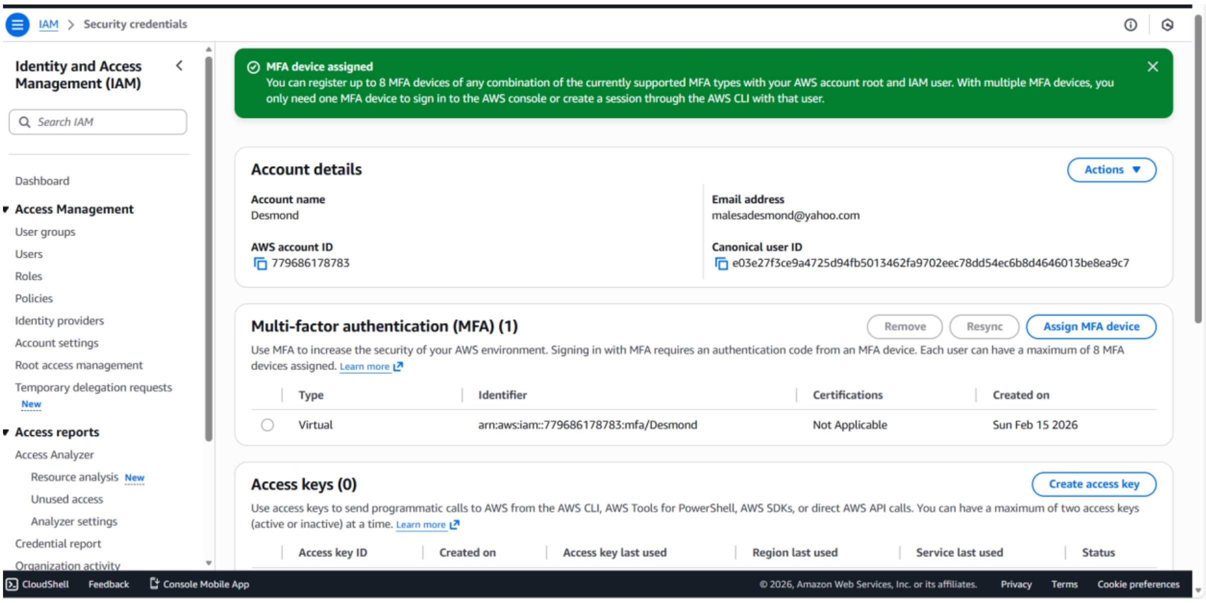
1. Implementing MFA enforcement for privileged access

Identity Access Management:

Registered MFA for my user/administrator account and linking it to my own device.



MFA device assigned
You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

Account details

Account name: Desmond

Email address: malesadesmond@yahoo.com

AWS account ID: 779686178783

Canonical user ID: e03e27f3ce9a4725d94fb5013462fa9702eec78dd54ec6b8d4646013be8ea9c7

Multi-factor authentication (MFA) (1)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

	Type	Identifier	Certifications	Created on
○	Virtual	arn:aws:iam::779686178783:mfa/Desmond	Not Applicable	Sun Feb 15 2026

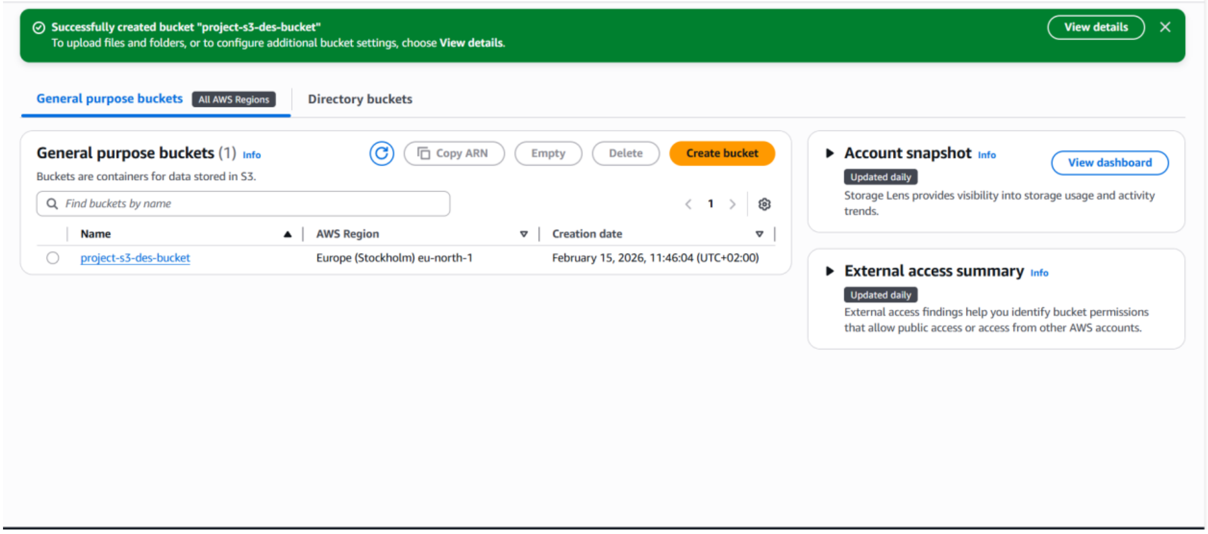
Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more

Access key ID	Created on	Access key last used	Region last used	Service last used	Status

© 2026, Amazon Web Services, Inc. or its affiliates.

Created an S3 bucket:



Successfully created bucket "project-s3-des-bucket"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

General purpose buckets (1)

Buckets are containers for data stored in S3.

	Name	AWS Region	Creation date
○	project-s3-des-bucket	Europe (Stockholm) eu-north-1	February 15, 2026, 11:46:04 (UTC+02:00)

Account snapshot

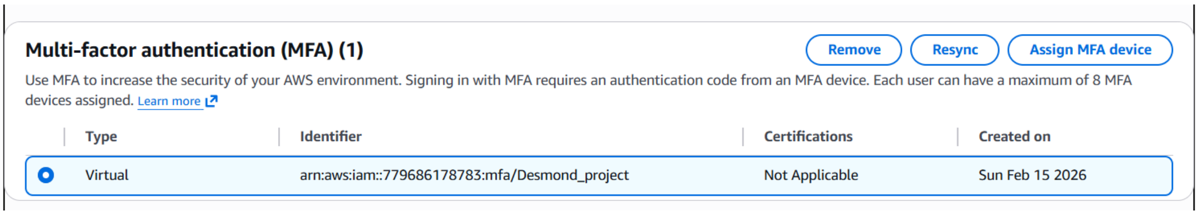
Storage Lens provides visibility into storage usage and activity trends.

External access summary

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

MFA-Implementation evidence:

Microsoft authenticator app used.



Multi-factor authentication (MFA) (1)

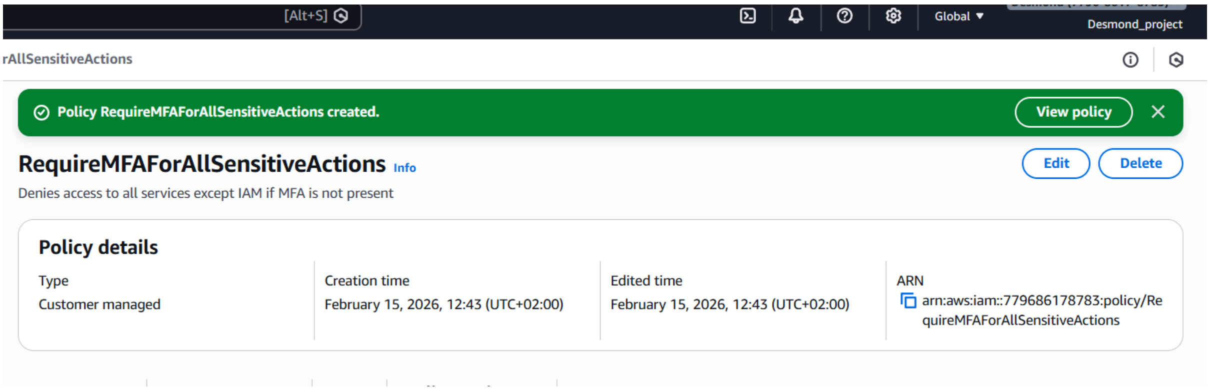
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

	Type	Identifier	Certifications	Created on
●	Virtual	arn:aws:iam::779686178783:mfa/Desmond_project	Not Applicable	Sun Feb 15 2026

MFA-Enforced policy:

Created a policy using JSON to deny all actions without Multi Factor Authentication being present.

As per screenshots below, I ran test to show that when I log into my user account MFA is required and I cannot log in without it.



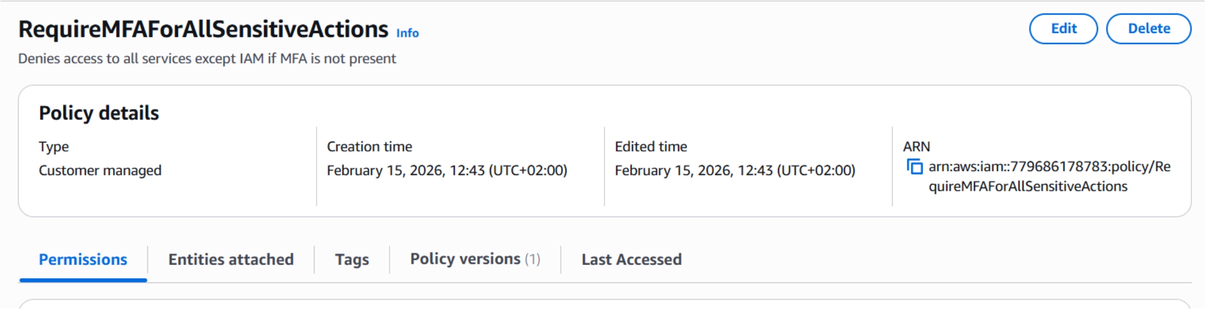
Policy RequireMFAForAllSensitiveActions created.

RequireMFAForAllSensitiveActions Info

Denies access to all services except IAM if MFA is not present

Policy details

Type	Creation time	Edited time	ARN
Customer managed	February 15, 2026, 12:43 (UTC+02:00)	February 15, 2026, 12:43 (UTC+02:00)	arn:aws:iam::779686178783:policy/RequireMFAForAllSensitiveActions

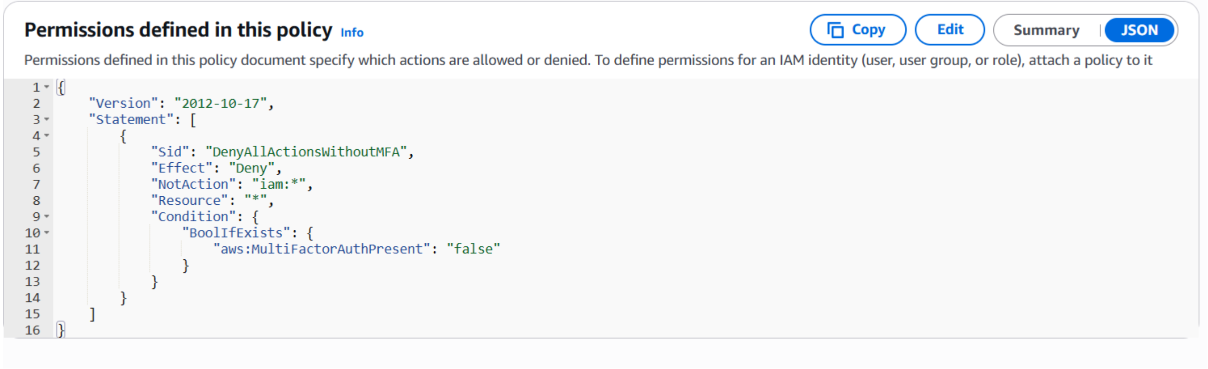


RequireMFAForAllSensitiveActions Info

Denies access to all services except IAM if MFA is not present

Policy details

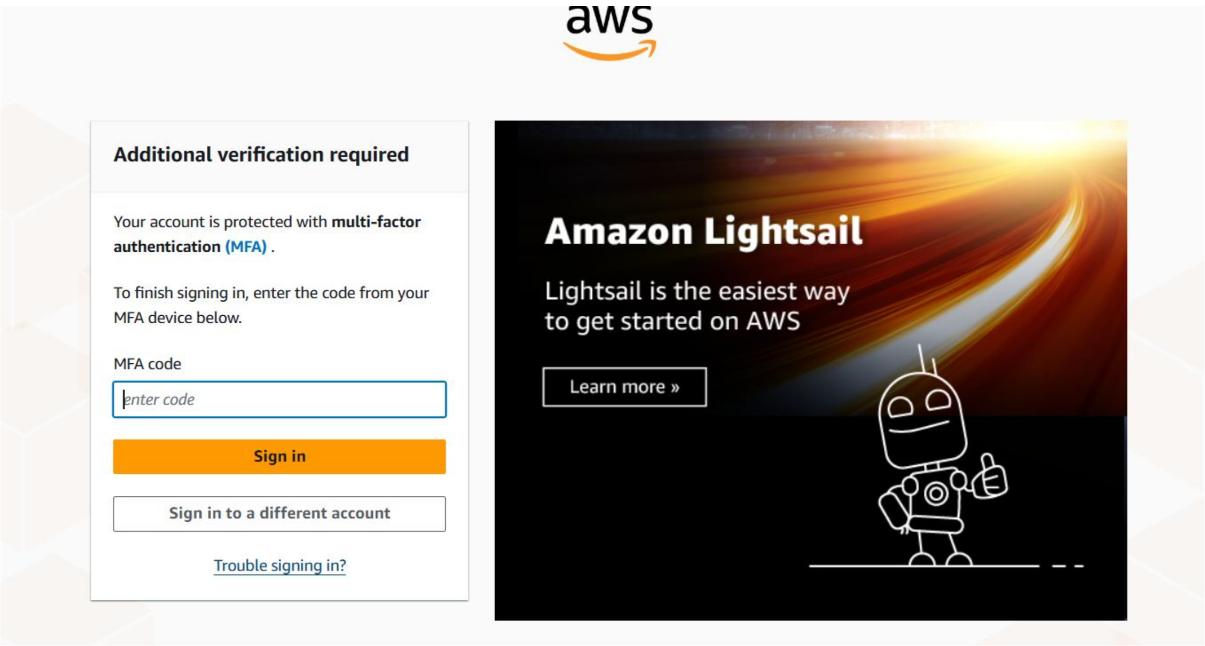
Type	Creation time	Edited time	ARN
Customer managed	February 15, 2026, 12:43 (UTC+02:00)	February 15, 2026, 12:43 (UTC+02:00)	arn:aws:iam::779686178783:policy/RequireMFAForAllSensitiveActions



Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllActionsWithoutMFA",
            "Effect": "Deny",
            "NotAction": "iam:*",
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "false"
                }
            }
        }
    ]
}
```



Additional verification required

Your account is protected with **multi-factor authentication** (MFA) .

To finish signing in, enter the code from your MFA device below.

MFA code

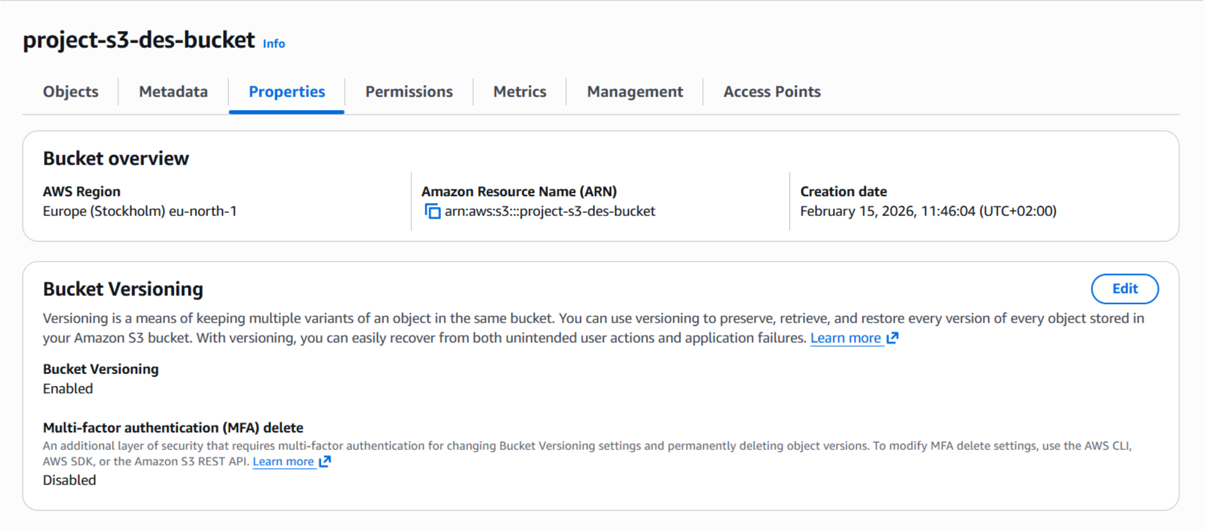
enter code

aws
Sign in
Sign in to a different account
Trouble signing in?
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »

This control prevents account takeover even if passwords are compromised, directly addressing the requirement for MFA.

2. Implementing S3 Bucket encryption controls:

Default encryption – uploaded sick note file without specifying encryption. The result was the file being automatically encrypted. Default encryption works as expected. See below screenshots for evidence.



project-s3-des-bucket

Bucket overview

AWS Region
Europe (Stockholm) eu-north-1

Amazon Resource Name (ARN)
arn:aws:s3:::project-s3-des-bucket

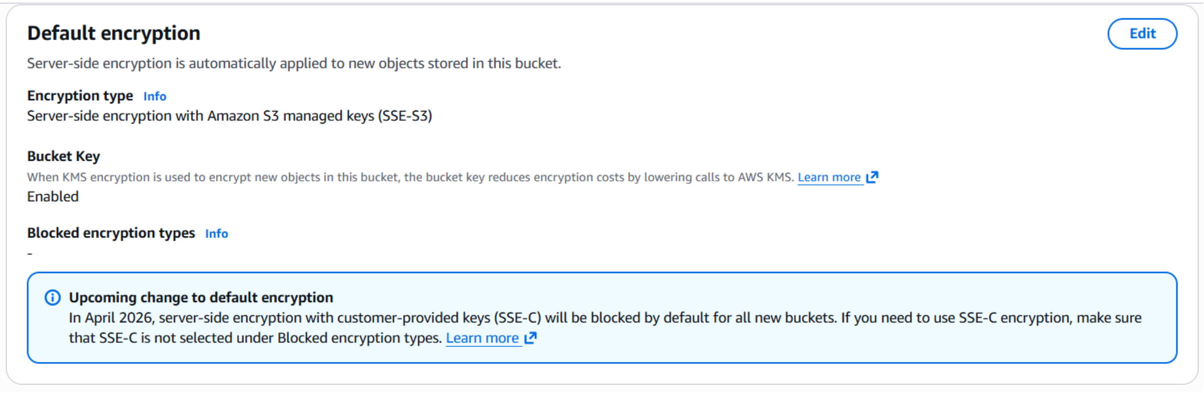
Creation date
February 15, 2026, 11:46:04 (UTC+02:00)

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
Enabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled



Default encryption

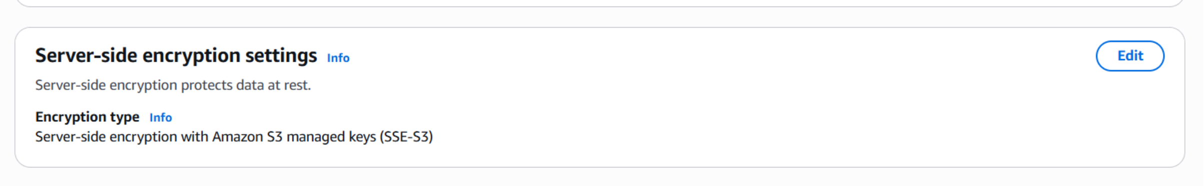
Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info
Server-side encryption with Amazon S3 managed keys (SSE-S3)

Bucket Key
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. Learn more
Enabled

Blocked encryption types Info
-

Upcoming change to default encryption
In April 2026, server-side encryption with customer-provided keys (SSE-C) will be blocked by default for all new buckets. If you need to use SSE-C encryption, make sure that SSE-C is not selected under Blocked encryption types. Learn more

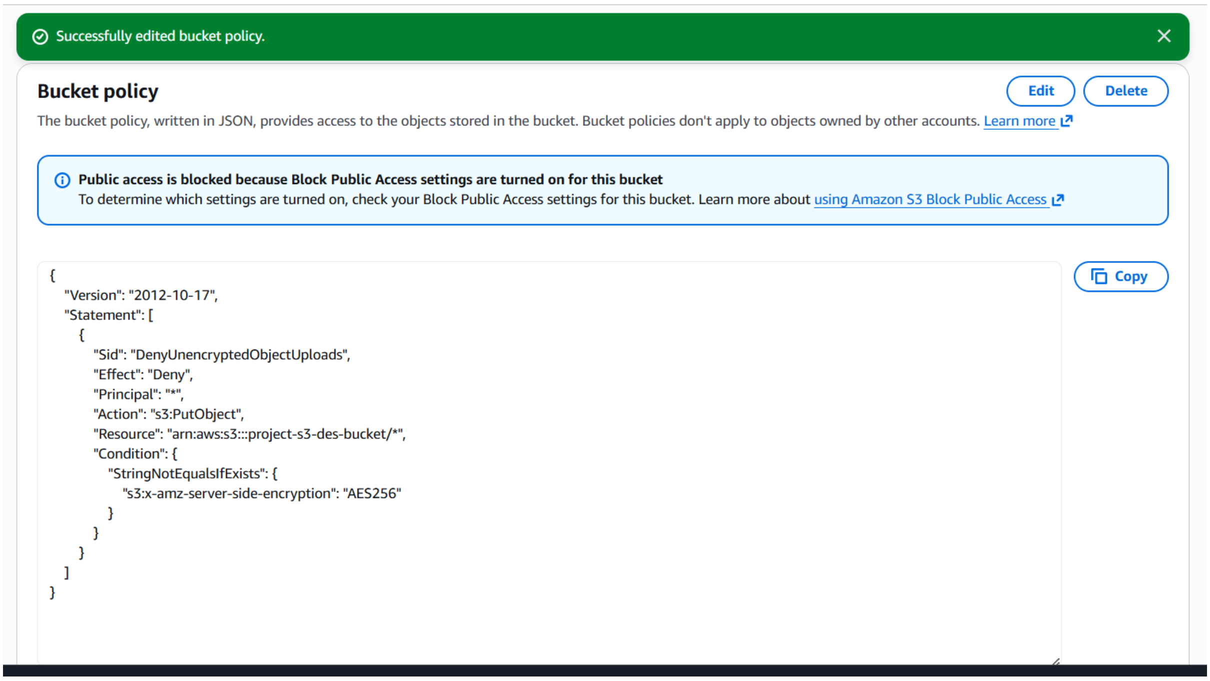


Server-side encryption settings Info

Server-side encryption protects data at rest.

Encryption type Info
Server-side encryption with Amazon S3 managed keys (SSE-S3)

Enforce encryption with Bucket policy – The below screenshots show the creation of the enforcement policy with JSON, then the error message of trying to upload an unencrypted file. Lastly the upload is successful when we change our permissions(with AES256 header).



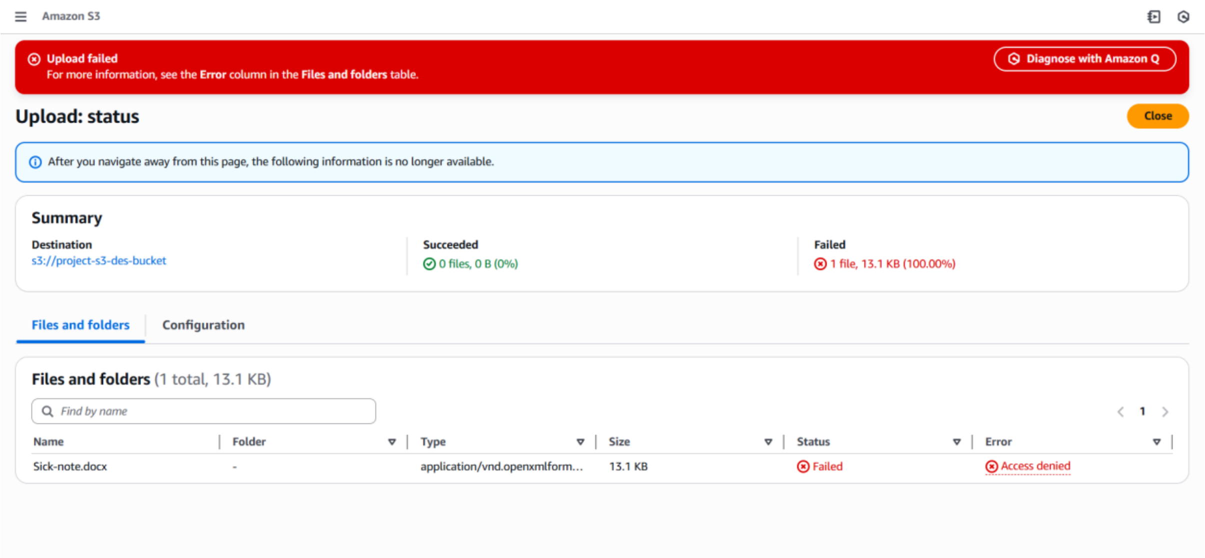
Successfully edited bucket policy.

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

Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyUnencryptedObjectUploads",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::project-s3-des-bucket/*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "s3:x-amz-server-side-encryption": "AES256"
        }
      }
    }
  ]
}
```



Upload failed
For more information, see the **Error** column in the **Files and folders** table.

Upload: status

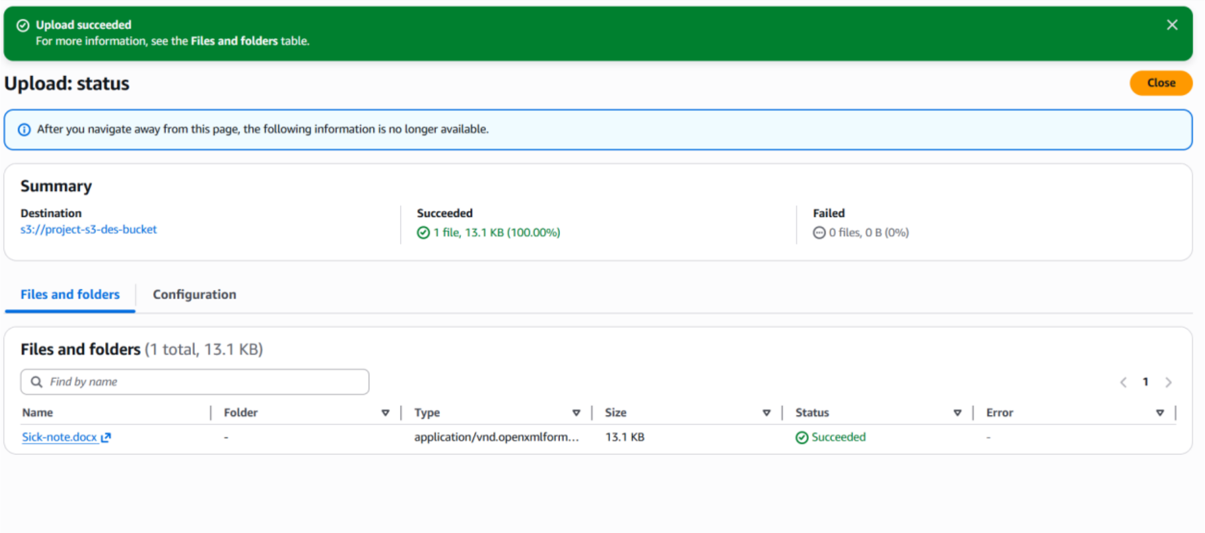
After you navigate away from this page, the following information is no longer available.

Summary

Destination	Succeeded	Failed
s3://project-s3-des-bucket	0 files, 0 B (0%)	1 file, 13.1 KB (100.00%)

Files and folders (1 total, 13.1 KB)

Name	Folder	Type	Size	Status	Error
Sick-note.docx	-	application/vnd.openxmlform...	13.1 KB	Failed	Access denied



Upload succeeded
For more information, see the **Files and folders** table.

Upload: status

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

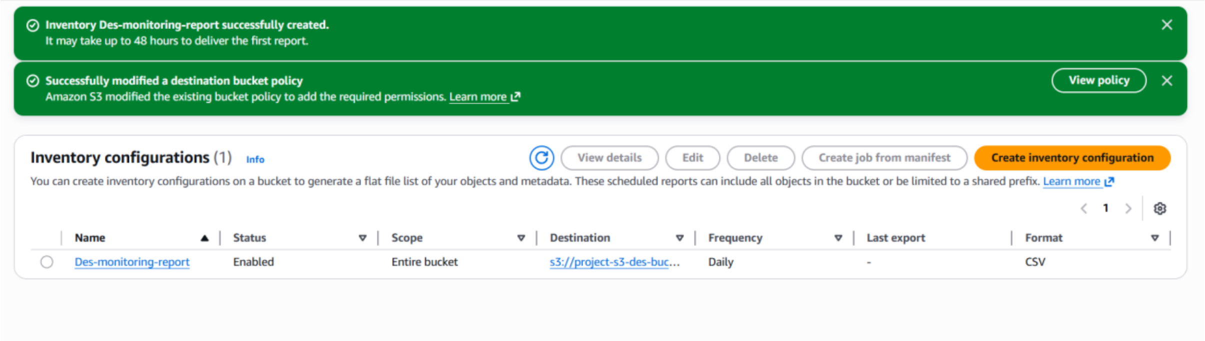
Summary

Destination	Succeeded	Failed
s3://project-s3-des-bucket	1 file, 13.1 KB (100.00%)	0 files, 0 B (0%)

Files and folders (1 total, 13.1 KB)

Name	Folder	Type	Size	Status	Error
Sick-note.docx	-	application/vnd.openxmlform...	13.1 KB	Succeeded	-

Encryption Monitoring – As per screenshot, created an inventory report to continuously track encryption status.



Inventory Des-monitoring-report successfully created.
It may take up to 48 hours to deliver the first report.

Successfully modified a destination bucket policy
Amazon S3 modified the existing bucket policy to add the required permissions. Learn more

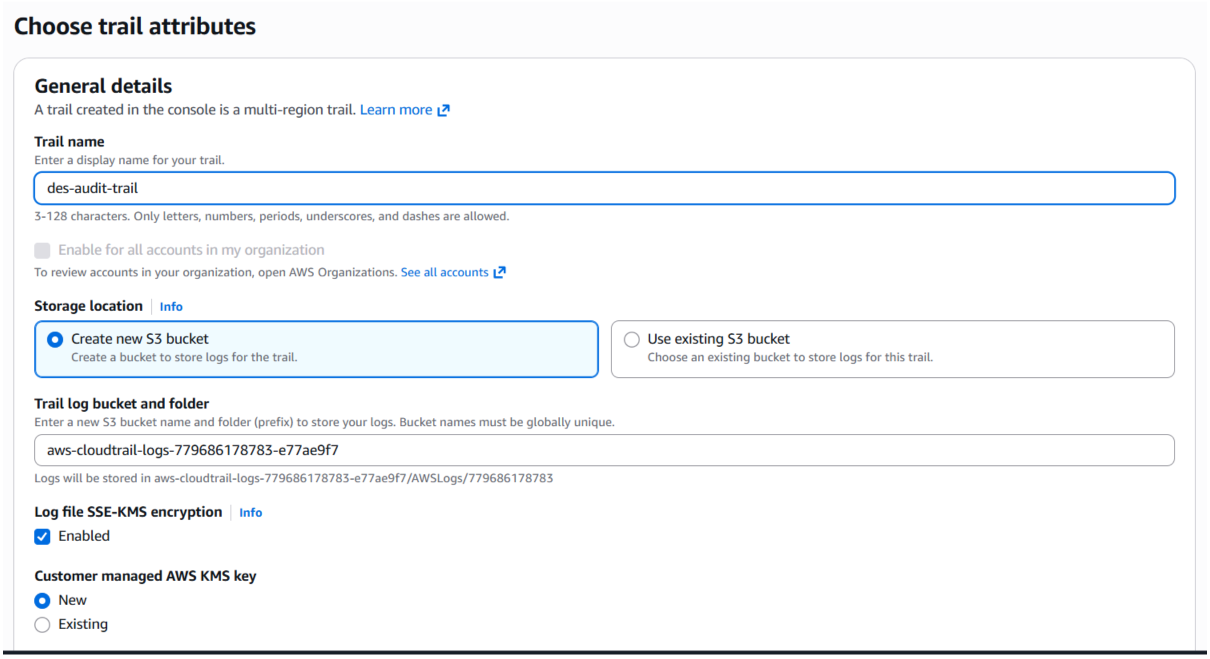
Inventory configurations (1) Info

You can create inventory configurations on a bucket to generate a flat file list of your objects and metadata. These scheduled reports can include all objects in the bucket or be limited to a shared prefix. Learn more

	Name	Status	Scope	Destination	Frequency	Last export	Format
○	Des-monitoring-report	Enabled	Entire bucket	s3://project-s3-des-buc...	Daily	-	CSV

3. CloudTrail logging:

Creating CloudTrail – As per below screenshots, I created a multi-region CloudTrail capturing all API activity. Enabled log file validation to ensure integrity. Configured CloudWatch metric filters and alarms for real-time alerting on failed login attempts.



Choose trail attributes

General details

A trail created in the console is a multi-region trail. Learn more

Trail name

Enter a display name for your trail.

des-audit-trail

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

□ Enable for all accounts in my organization

To review accounts in your organization, open AWS Organizations. See all accounts

Storage location | Info

● Create new S3 bucket
Create a bucket to store logs for the trail.

○ Use existing S3 bucket
Choose an existing bucket to store logs for this trail.

Trail log bucket and folder

Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

aws-cloudtrail-logs-779686178783-e77ae9f7

Logs will be stored in aws-cloudtrail-logs-779686178783-e77ae9f7/AWSLogs/779686178783

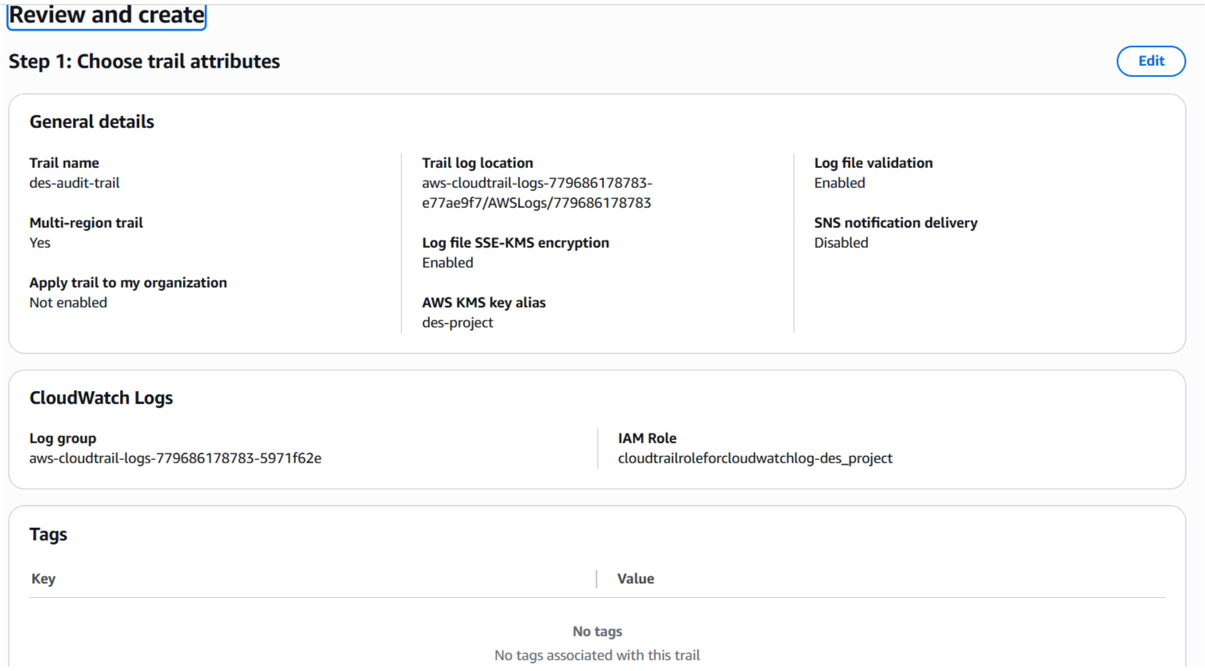
Log file SSE-KMS encryption | Info

☑ Enabled

Customer managed AWS KMS key

● New

○ Existing



Review and create

Step 1: Choose trail attributes

General details

Trail name
des-audit-trail

Multi-region trail
Yes

Apply trail to my organization
Not enabled

Trail log location
aws-cloudtrail-logs-779686178783-e77ae9f7/AWSLogs/779686178783

Log file SSE-KMS encryption
Enabled

AWS KMS key alias
des-project

Log file validation
Enabled

SNS notification delivery
Disabled

CloudWatch Logs

Log group
aws-cloudtrail-logs-779686178783-5971f62e

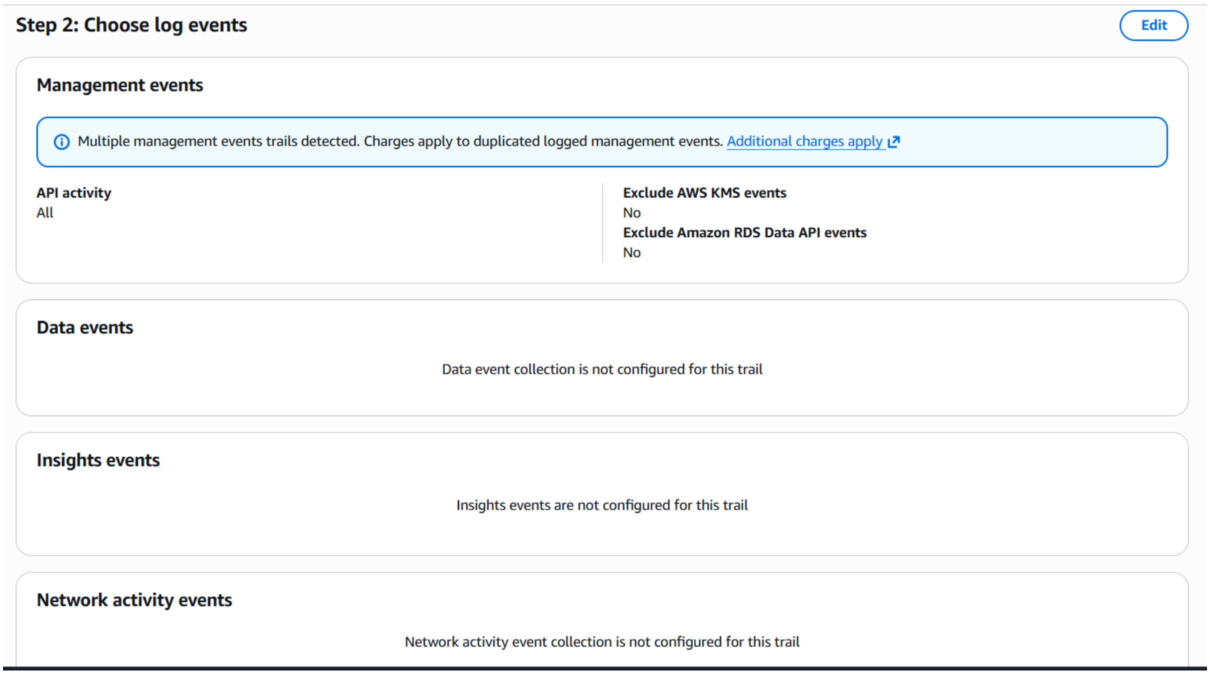
IAM Role
cloudtrailroleforcloudwatchlog-des_project

Tags

Key	Value

No tags

No tags associated with this trail



Step 2: Choose log events

Management events

ⓘ Multiple management events trails detected. Charges apply to duplicated logged management events. Additional charges apply

API activity
All

Exclude AWS KMS events
No

Exclude Amazon RDS Data API events
No

Data events

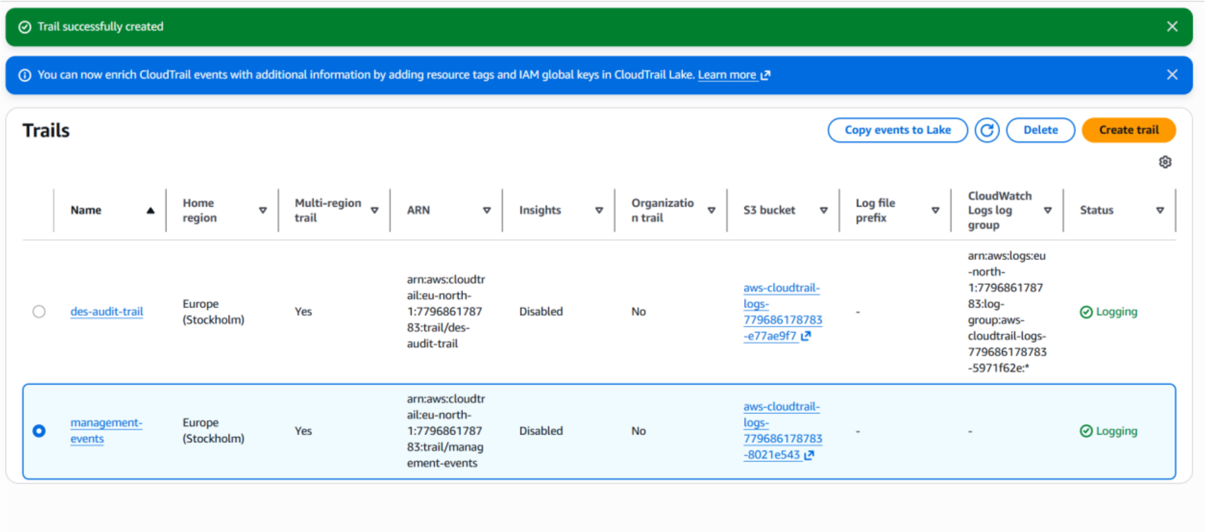
Data event collection is not configured for this trail

Insights events

Insights events are not configured for this trail

Network activity events

Network activity event collection is not configured for this trail

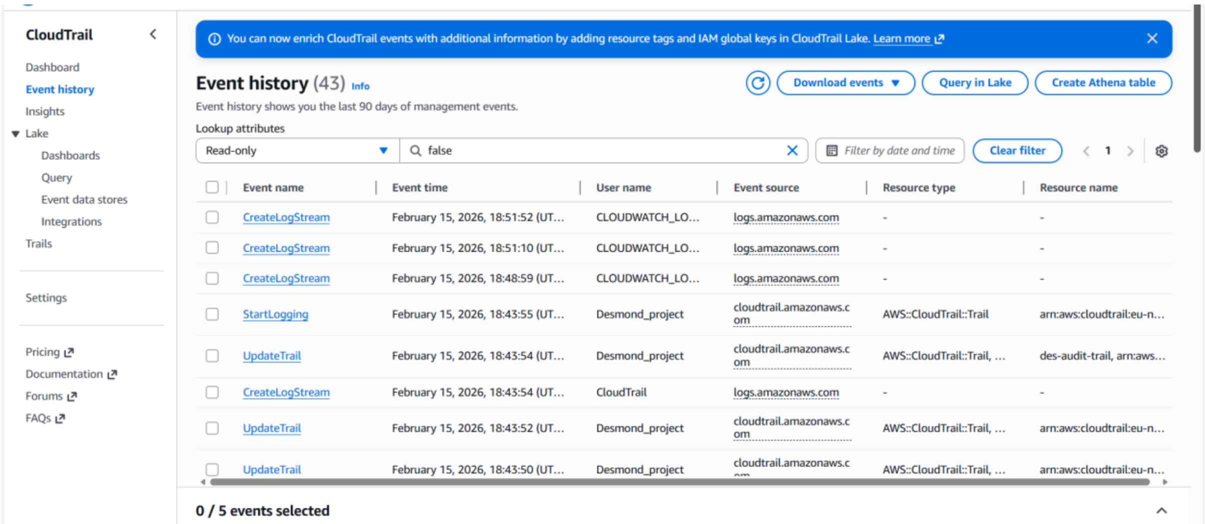


✓ Trail successfully created

ⓘ You can now enrich CloudTrail events with additional information by adding resource tags and IAM global keys in CloudTrail Lake. Learn more

Trails

	Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
○	des-audit-trail	Europe (Stockholm)	Yes	arn:aws:cloudtrail:eu-north-1:779686178783:trail/des-audit-trail	Disabled	No	aws-cloudtrail-logs-779686178783-e77ae9f7	-	arn:aws:logs:eu-north-1:779686178783:log-group:aws-cloudtrail-logs-779686178783-5971f62e:*	✓ Logging
●	management-events	Europe (Stockholm)	Yes	arn:aws:cloudtrail:eu-north-1:779686178783:trail/management-events	Disabled	No	aws-cloudtrail-logs-779686178783-8021e543	-	-	✓ Logging



ⓘ You can now enrich CloudTrail events with additional information by adding resource tags and IAM global keys in CloudTrail Lake. Learn more

Event history (43) Info

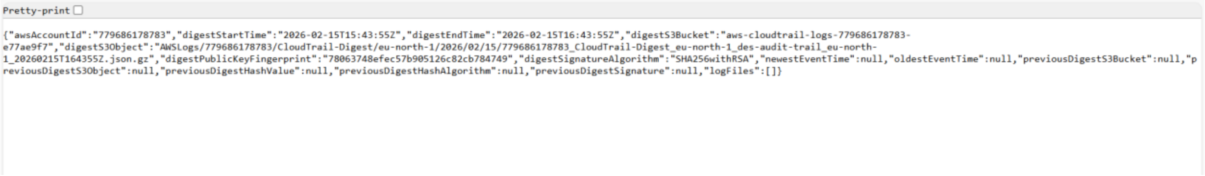
Event history shows you the last 90 days of management events.

Lookup attributes

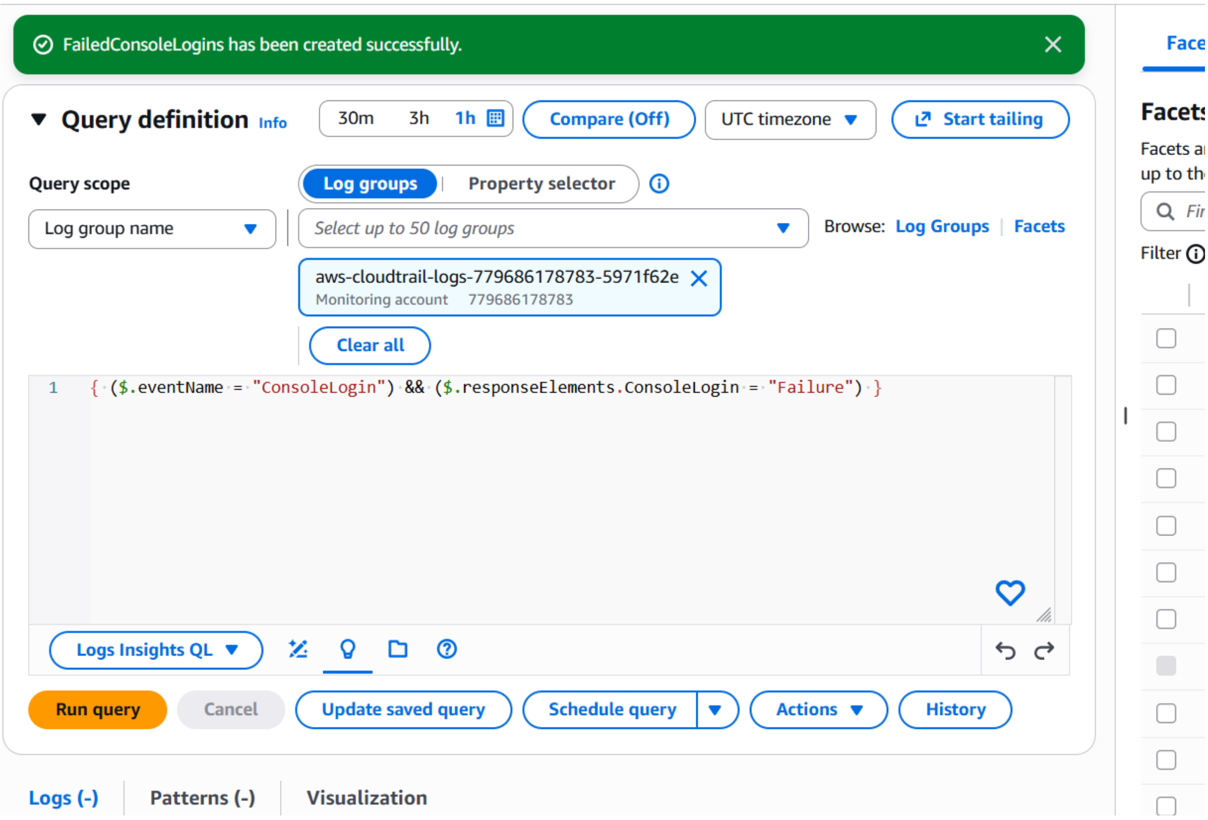
Read-only | false

□	Event name	Event time	User name	Event source	Resource type	Resource name
□	CreateLogStream	February 15, 2026, 18:51:52 (UT...	CLOUDWATCH_LO...	logs.amazonaws.com	-	-
□	CreateLogStream	February 15, 2026, 18:51:10 (UT...	CLOUDWATCH_LO...	logs.amazonaws.com	-	-
□	CreateLogStream	February 15, 2026, 18:48:59 (UT...	CLOUDWATCH_LO...	logs.amazonaws.com	-	-
□	StartLogging	February 15, 2026, 18:43:55 (UT...	Desmond_project	cloudtrail.amazonaws.com	AWS::CloudTrail::Trail	arn:aws:cloudtrail:eu-n...
□	UpdateTrail	February 15, 2026, 18:43:54 (UT...	Desmond_project	cloudtrail.amazonaws.com	AWS::CloudTrail::Trail, ...	des-audit-trail, arn:aws...
□	CreateLogStream	February 15, 2026, 18:43:54 (UT...	CloudTrail	logs.amazonaws.com	-	-
□	UpdateTrail	February 15, 2026, 18:43:52 (UT...	Desmond_project	cloudtrail.amazonaws.com	AWS::CloudTrail::Trail, ...	arn:aws:cloudtrail:eu-n...
□	UpdateTrail	February 15, 2026, 18:43:50 (UT...	Desmond_project	cloudtrail.amazonaws.c	AWS::CloudTrail::Trail, ...	arn:aws:cloudtrail:eu-n...

0 / 5 events selected



```
{"awsAccountId":"779686178783","digestStartTime":"2026-02-15T15:43:55Z","digestEndTime":"2026-02-15T16:43:55Z","digestS3Bucket":"aws-cloudtrail-logs-779686178783-
e77ae9f7","digestS3Object":"AWSLogs/779686178783/CloudTrail-Digest/eu-north-1/2026/02/15/779686178783_CloudTrail-Digest_eu-north-1_des-audit-trail_eu-north-
1_20260215T164355Z.json.gz","digestPublicKeyFingerprint":"78063748efec57b905126c82cb784749","digestSignatureAlgorithm":"SHA256withRSA","newestEventTime":null,"oldestEventTime":null,"previousDigestS3Bucket":null,"p
reviousDigestS3Object":null,"previousDigestHashValue":null,"previousDigestHashAlgorithm":null,"previousDigestSignature":null,"logFiles":[]}
```



FailedConsoleLogins has been created successfully.

Query scope: Log groups | Property selector

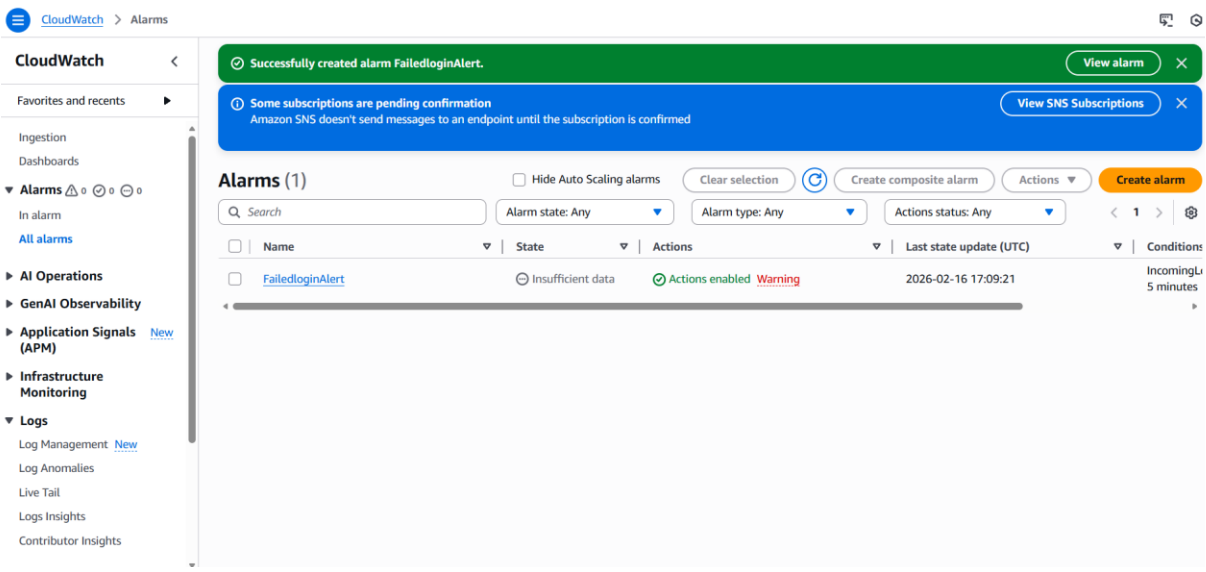
Log group name

Select up to 50 log groups

Browse: Log Groups | Facets

aws-cloudtrail-logs-779686178783-5971f62e
Monitoring account 779686178783

```
{ ($.eventName = "ConsoleLogin") && ($.responseElements.ConsoleLogin = "Failure") }
```



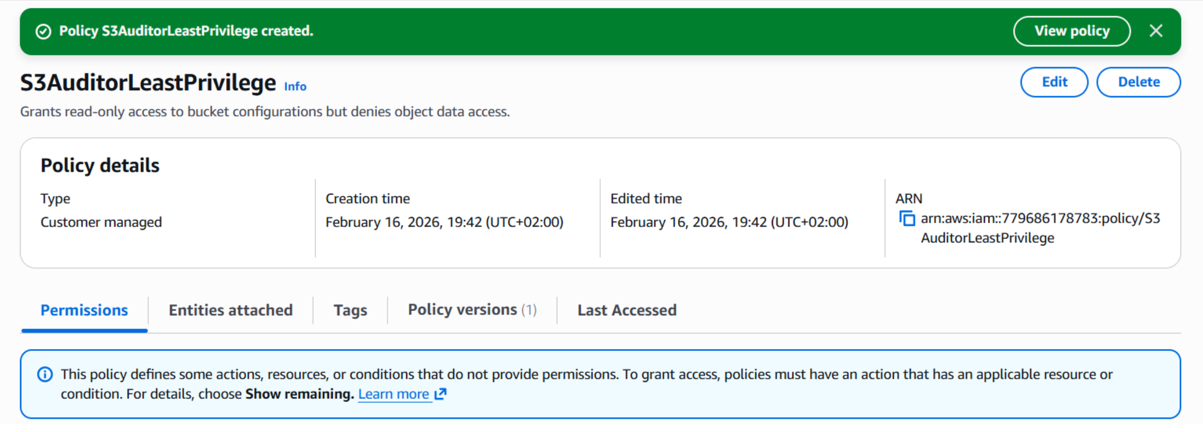
Successfully created alarm FailedloginAlert.

Some subscriptions are pending confirmation
Amazon SNS doesn't send messages to an endpoint until the subscription is confirmed

☐	Name	State	Actions	Last state update (UTC)	Condition
☐	FailedloginAlert	Insufficient data	Actions enabled Warning	2026-02-16 17:09:21	IncomingL 5 minutes

4. Implementing Least-Privilege IAM Policies

As per below screenshots, I created the Least-Privilege policy to define minimal permissions required: list buckets, view bucket configurations but Deny access to object data. IAM policy with granular Allow and Deny statements, attached the policy to test allowed and denied actions worked as intended.



Policy S3AuditorLeastPrivilege created.

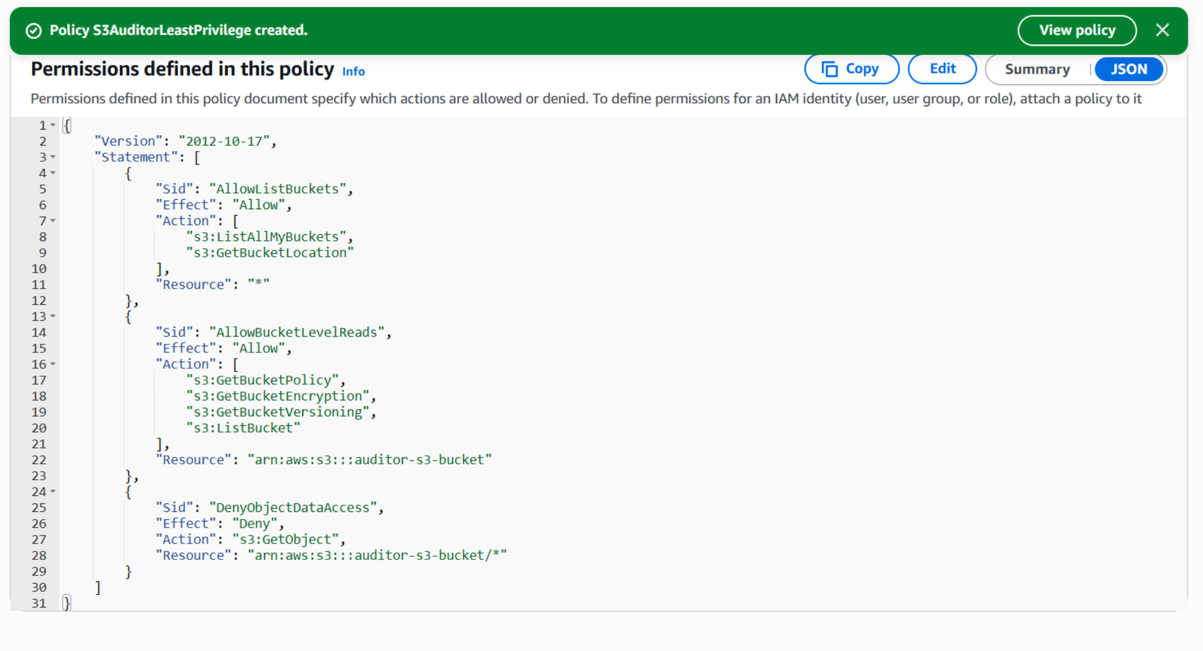
S3AuditorLeastPrivilege Info

Grants read-only access to bucket configurations but denies object data access.

Policy details

Type	Creation time	Edited time	ARN
Customer managed	February 16, 2026, 19:42 (UTC+02:00)	February 16, 2026, 19:42 (UTC+02:00)	arn:aws:iam::779686178783:policy/S3AuditorLeastPrivilege

This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that has an applicable resource or condition. For details, choose **Show remaining.** Learn more

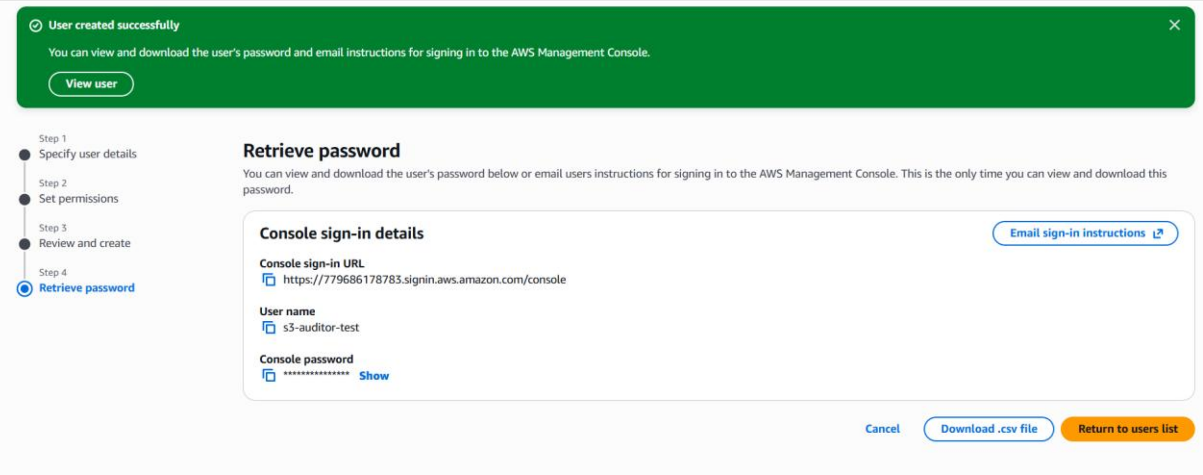


Policy S3AuditorLeastPrivilege created.

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowListBuckets",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowBucketLevelReads",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketPolicy",
                "s3:GetBucketEncryption",
                "s3:GetBucketVersioning",
                "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::auditor-s3-bucket"
        },
        {
            "Sid": "DenyObjectDataAccess",
            "Effect": "Deny",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::auditor-s3-bucket/*"
        }
    ]
}
```



User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Retrieve password

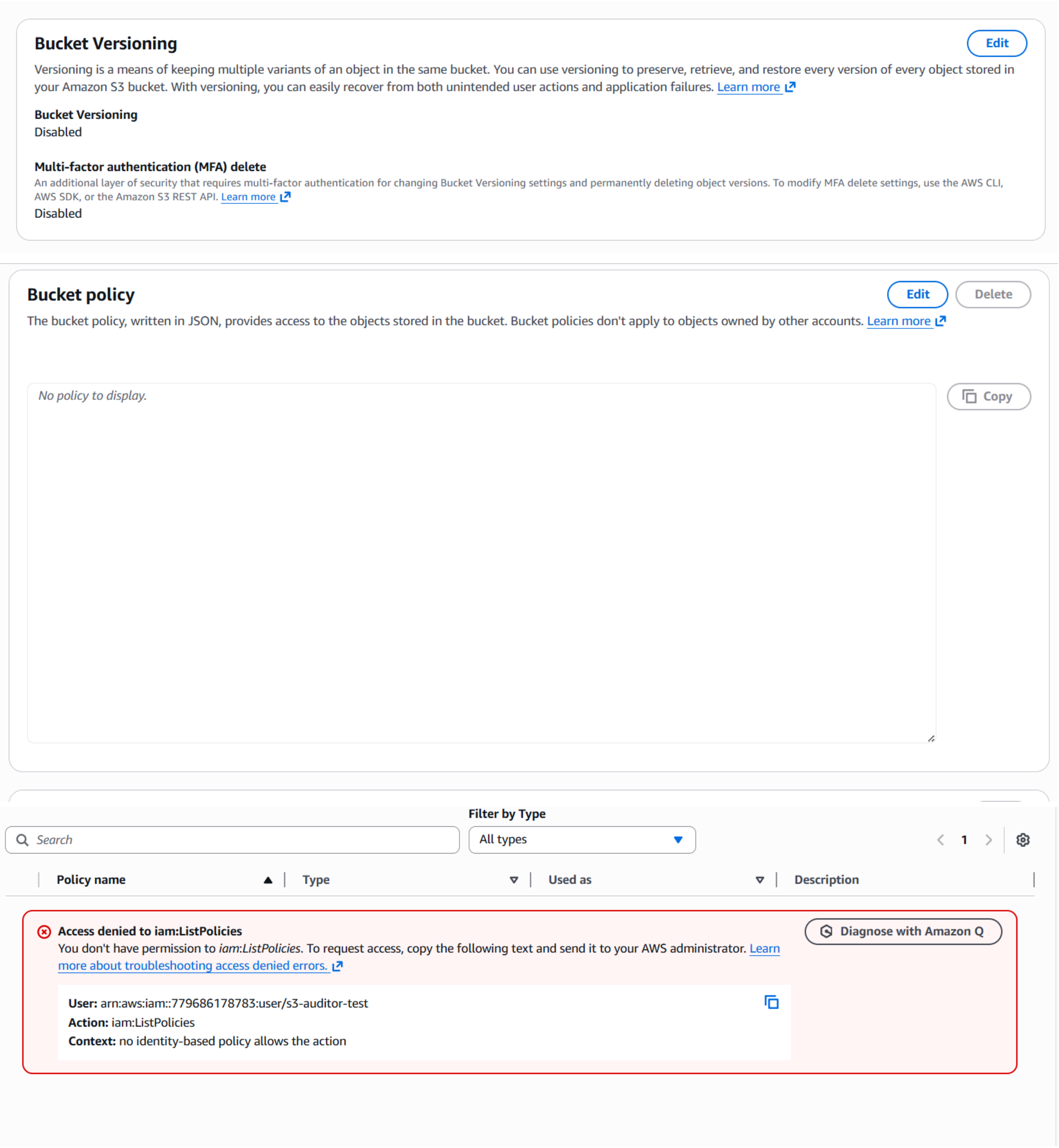
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Console sign-in URL
https://779686178783.signin.aws.amazon.com/console

User name
s3-auditor-test

Console password
*************** Show



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
Disabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled

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

No policy to display.

Filter by Type

Policy name ▲	Type	Used as	Description

Access denied to iam:ListPolicies
You don't have permission to *iam:ListPolicies*. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.

User: arn:aws:iam::779686178783:user/s3-auditor-test
Action: iam:ListPolicies
Context: no identity-based policy allows the action