

IAM User creation for S3 Bucket Read Only Access

IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Specify user details

User details

User name

s3-bucket-user

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + , _ , @ , - (hyphen)

☐ Provide user access to the AWS Management Console - optional




If you're providing console access to a person, it's a best practice [to](#) manage their access in IAM Identity Center.

ⓘ

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)


Cancel

Next

<input type="checkbox"/>	 AmazonS3OutpostsFullAccess	AWS managed	0	
<input type="checkbox"/>	 AmazonS3OutpostsReadOnlyAccess	AWS managed	0	
<input type="checkbox"/>	 AmazonS3ReadOnlyAccess	AWS managed	0	

AmazonS3ReadOnlyAccess




Provides read only access to all buckets via the AWS Management Console.

 Copy JSON

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "s3:Get*",
8         "s3:List*",
9         "s3:Describe*",
10        "s3-object-lambda:Get*",
11        "s3-object-lambda:List*"
12      ],
13      "Resource": "*"
14    }
15  ]
16 }

```

<input type="checkbox"/>	 AWSBackupServiceRolePolicyForS3Backup	AWS managed	0	
<input type="checkbox"/>	 AWSBackupServiceRolePolicyForS3Restore	AWS managed	0	
<input type="checkbox"/>	 AWSSSONOutpostsServiceRolePolicy	AWS managed	0	

AWS

Services

Q Search

[Alt+S]

Global▼

arn

Identity and Access Management (IAM)

X

Q Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Related consoles

IAM Identity Center

IAM > Users > s3-bucket-user

s3-bucket-user Info

Delete

Summary

ARN
am:aws:iam::008971632097:user/s3-bucket-user

Console access
Disabled

Access key 1
[Create access key](#)

Created
July 29, 2024, 04:11 (UTC)

Last console sign-in
-

Permissions

Groups

Tags

Security credentials

Access Advisor

Permissions policies (1)

Refresh Remove Add permissions ▼

Permissions are defined by policies attached to the user directly or through groups.

Q Search

Filter by Type
All types

< 1 >

⊗

☐ Policy name ↗

Type

Attached via ↗

☐ AmazonS3ReadOnlyAccess

AWS managed

Directly

► Permissions boundary (not set)

Step 2 - optional
[Set description tag](#)

Step 3
Retrieve access keys

Use case

☐ Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.

☐ Local code
You plan to use this access key to enable application code running in a local development environment to access your AWS account.

☐ Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

☒ Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

☐ Application running outside AWS
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.

☐ Other
Your use case is not listed here.

Alternative recommended
As a best practice, use temporary security credentials (IAM roles) instead of creating long-term credentials like access keys, and don't create AWS account root user access keys. [Learn more](#)

Confirmation
☐ I understand the above recommendation and want to proceed to create an access key.

Cancel Next

Security Credentials-

AKIAQEFWAHXQ2CULKONP

A9RPMtHveBU8hYPCyIS61dj6dfTYyU8vLN3lh7k

Access key created
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

IAM > Users > s3-bucket-user > Create access key

Step 1
[Access key best practices & alternatives](#)

Step 2 - optional
[Set description tag](#)

Step 3
Retrieve access keys

Retrieve access keys [info](#)

Access key
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIAQEFWAHXQ2CULKONP	A9RPMtHveBU8hYPCyIS61dj6dfTYyU8vLN3lh7k Hide

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [best practices for managing AWS access keys](#).

[Download .csv file](#) [Done](#)

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

▼ Access reports

- Access Analyzer
- External access
- Unused access
- Analyzer settings
- Credential report
- Organization activity
- Service control policies

Related consoles

s3-bucket-user info Delete

Summary

ARN arn:aws:iam::008971632097:user/s3-bucket-user	Console access Disabled	Access key 1 AKIAQEFWAHQZCULKONP - Active ⓘ Never used. Created today.
Created July 29, 2024, 04:11 (UTC)	Last console sign-in -	Access key 2 Create access key

Permissions Groups Tags **Security credentials** Access Advisor

Console sign-in Enable console access

Console sign-in link
<https://008971632097.signin.aws.amazon.com/console>

Console password
Not enabled

Multi-factor authentication (MFA) (0) Remove Resync Assign MFA device

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
No MFA devices. Assign an MFA device to improve the security of your AWS environment			

[Assign MFA device](#)

S3 Bucket Creation

Amazon S3 > **Buckets** > **Create bucket**

Create bucket info

Buckets are containers for data stored in S3.

General configuration

AWS Region
Asia Pacific (Mumbai) ap-south-1

Bucket name Info

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.

Format: s3://bucket/prefix

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 enforced



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.

Bucket Versioning

aws

Services

Q Search

[Alt+S]

Amazon S3 > Buckets > audio-video-calls-data-dev > Create folder

Create folder [Info](#)

Use folders to group objects in buckets. When you create a folder, S3 creates an object using the name that you specify followed by a slash (/). This object then appears as folder on the console. [Learn more](#)

Your bucket policy might block folder creation

If your bucket policy prevents uploading objects without specific tags, metadata, or access control list (ACL) grantees, you will not be able to create a folder using this configuration. Instead, you can use the [upload configuration](#) to upload an empty folder and specify the appropriate settings.

Folder

Folder name

Audio Call Recordings/

Folder names can't contain "/" . [See rules for naming](#)

Server-side encryption [Info](#)

Server-side encryption protects data at rest.

The following encryption settings apply only to the folder object and not to sub-folder objects.

Server-side encryption

☒ Don't specify an encryption key

The bucket settings for default encryption are used to encrypt the folder object when storing it in Amazon S3.

☐ Specify an encryption key

The specified encryption key is used to encrypt the folder object before storing it in Amazon S3.

aws

Services

Q Search

[Alt+S]

Mumbai

array

Successfully created folder "Video Call Recordings".

Amazon S3 > Buckets > audio-video-calls-data-dev

audio-video-calls-data-dev [Info](#)

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (2) [Info](#)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

☐

Name

☐

Audio Call Recordings/

☐

Video Call Recordings/

Type

Folder

Folder

Last modified

-

-

Size

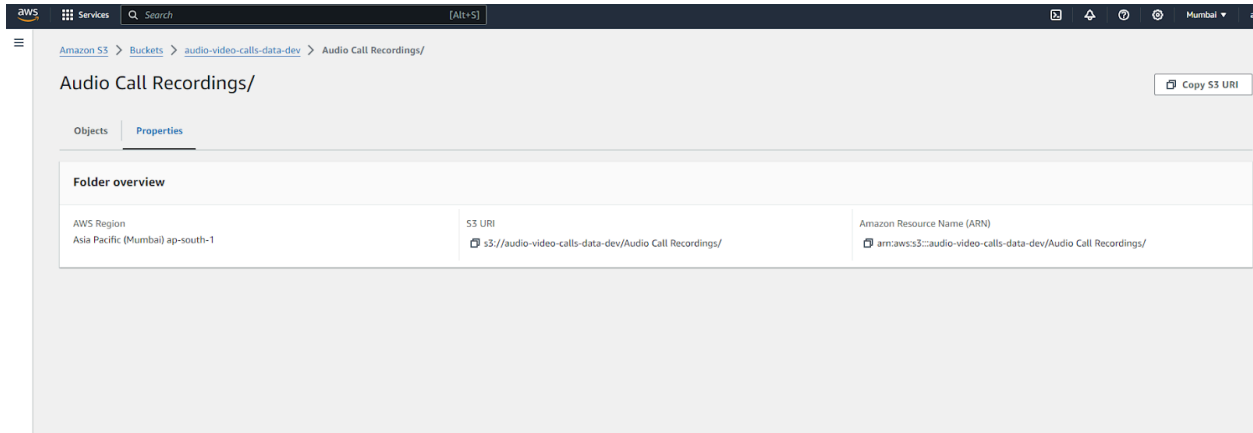
-

-

Storage class

-

-



Bucket Credentials-

AWS Region

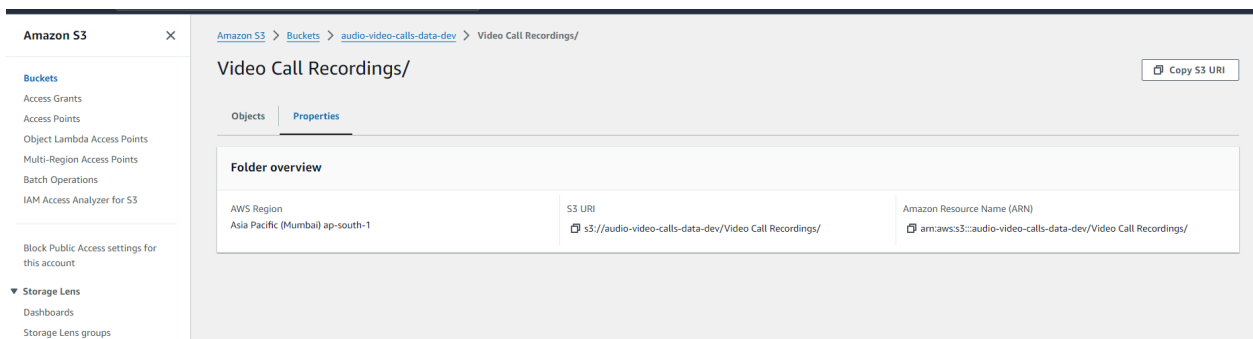
Asia Pacific (Mumbai) ap-south-1

S3 URI

s3://audio-video-calls-data-dev/Audio Call Recordings/

Amazon Resource Name (ARN)

arn:aws:s3:::audio-video-calls-data-dev/Audio Call Recordings/



AWS Region

Asia Pacific (Mumbai) ap-south-1

S3 URI

s3://audio-video-calls-data-dev/Video Call Recordings/

Amazon Resource Name (ARN)

arn:aws:s3:::audio-video-calls-data-dev/Video Call Recordings/