

VOD on EdgeOne

Getting Started

Product Documentation



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Getting Started

Last updated : 2024-01-30 16:32:08

This guide will lead you through the process of activating VOD on EO, and creating a functional application within VOD on EO.

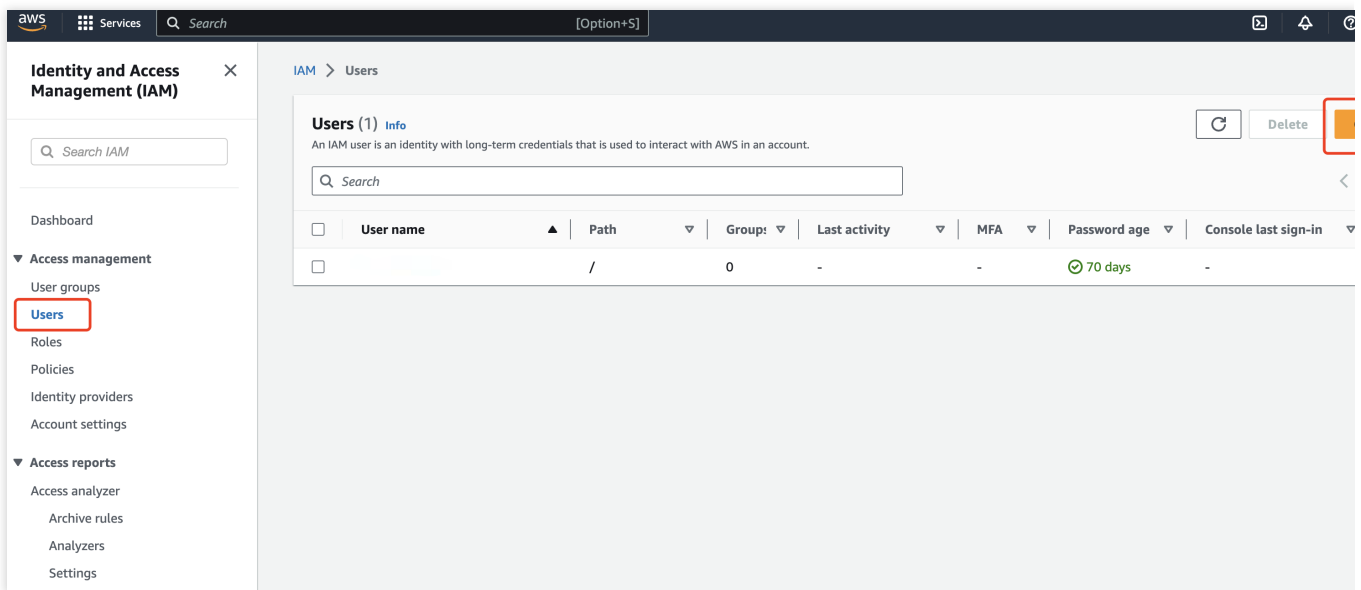
Preparations

A registered Tencent Cloud account has been established.

A third-party storage service has been registered and a bucket that already loaded with uploaded media file data is prepared. Take AWS's [S3](#) storage service as an example. A functional AWS S3 bucket, named BucketforVodeo, is located in the Asia Pacific (Sydney) ap-southeast-2 region.

Step One: Create an AWS sub-user and save the user's secret key

1. Navigate to the [Identity and Access Management \(IAM\)](#), click **Users**, then click **Create user** to add a new user.



2. Enter the **User name**, then click **Next** in the lower right corner.

Specify user details

User details

User name

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

3. Select **Attach policies directly**, enter S3 in the search box, locate **AmazonS3FullAccess** in the search results and check it, then click **Next** in the lower right corner.

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policy instead. Then, add the user to the appropriate group.

Permissions policies (1/1121)

Choose one or more policies to attach to your new user.

Q S3

Filter by Type

All types

11 matches

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	AWS managed	0
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	0
<input type="checkbox"/>	AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	0
<input type="checkbox"/>	AmazonS3OutpostsFullAccess	AWS managed	0
<input type="checkbox"/>	AmazonS3OutpostsReadOnlyAccess	AWS managed	0
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS managed	0
<input type="checkbox"/>	AWSBackupServiceRolePolicyForS3Backup	AWS managed	0
<input type="checkbox"/>	AWSBackupServiceRolePolicyForS3Restore	AWS managed	0
<input type="checkbox"/>	IVSRecordToS3	AWS managed	0
<input type="checkbox"/>	QuickSightAccessForS3StorageManagement...	AWS managed	0
<input type="checkbox"/>	S3StorageLensServiceRolePolicy	AWS managed	0

▶ **Set permissions boundary - optional**

Cancel **Pre**

4. Click **Create user** to complete the user creation process.

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name [redacted]	Console password type None	Require password reset No
-------------------------	-------------------------------	------------------------------

Permissions summary

Name	Type	Used as
AmazonS3FullAccess	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

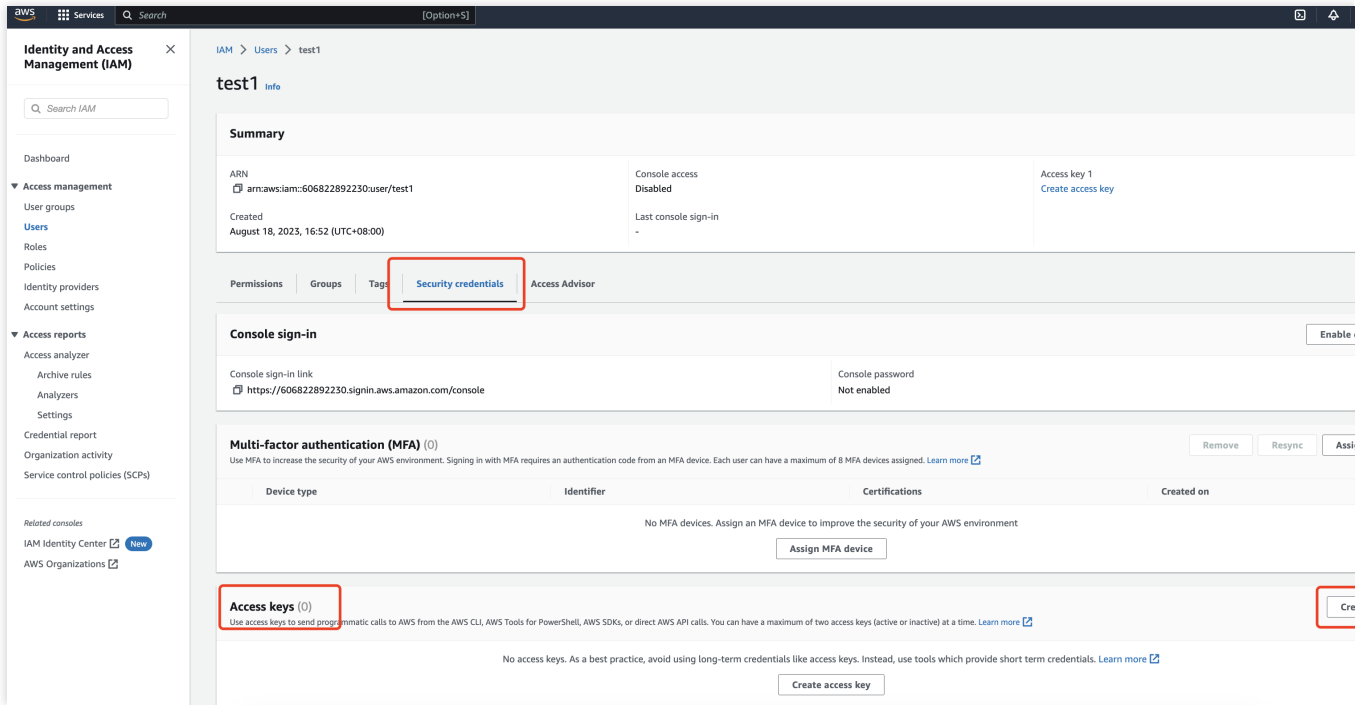
Cancel Previous Create

5. After creating the user, click the newly created **User name** in the Users list.

The screenshot shows the AWS IAM console interface. A green banner at the top indicates 'User created successfully'. The main content area shows the 'Users' list with the following columns: User name, Path, Group, Last activity, MFA, Password age, Console last sign-in, and Access key ID. The 'User name' column of the first user is highlighted with a red box.

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Access key ID
[redacted]	/	?	-	-	71 days	-	Active - AKIAV2SLWQL...
[redacted]	/	?	-	-	-	-	-

6. Click **Security credentials**, locate **Access Keys**, then click **Create access key**.



7. In the Use Case, select **Other**, click **Next** to create, and save the generated **Access key ID** and **Secret access key**.

Note:

The Secret Access Key for AWS S3 cannot be viewed subsequently, please ensure to copy and store it securely after creation.

Access key best practices & alternatives info

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

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 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 enable an application running on an on-premises host, or to use a local AWS client or third-party AWS plugin.
- Other**
Your use case is not listed here.

It's okay to use an access key for this use case, but follow the best practices:

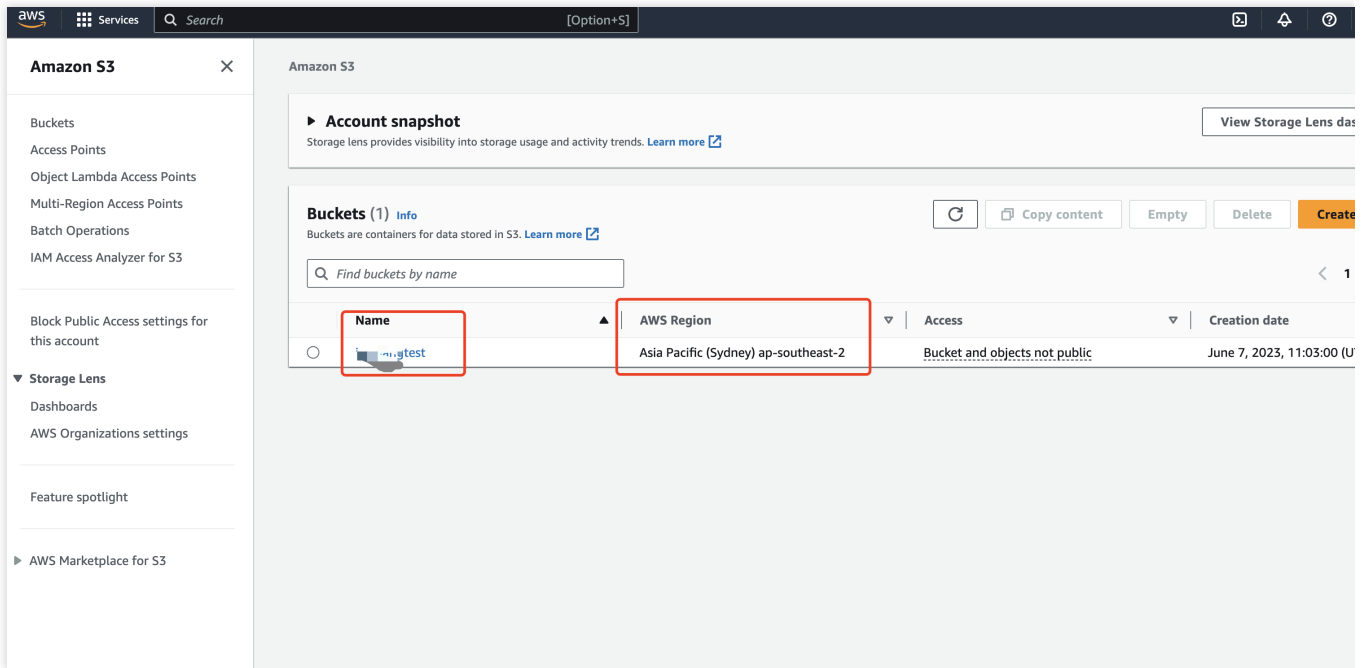
- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access keys when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

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

Cancel

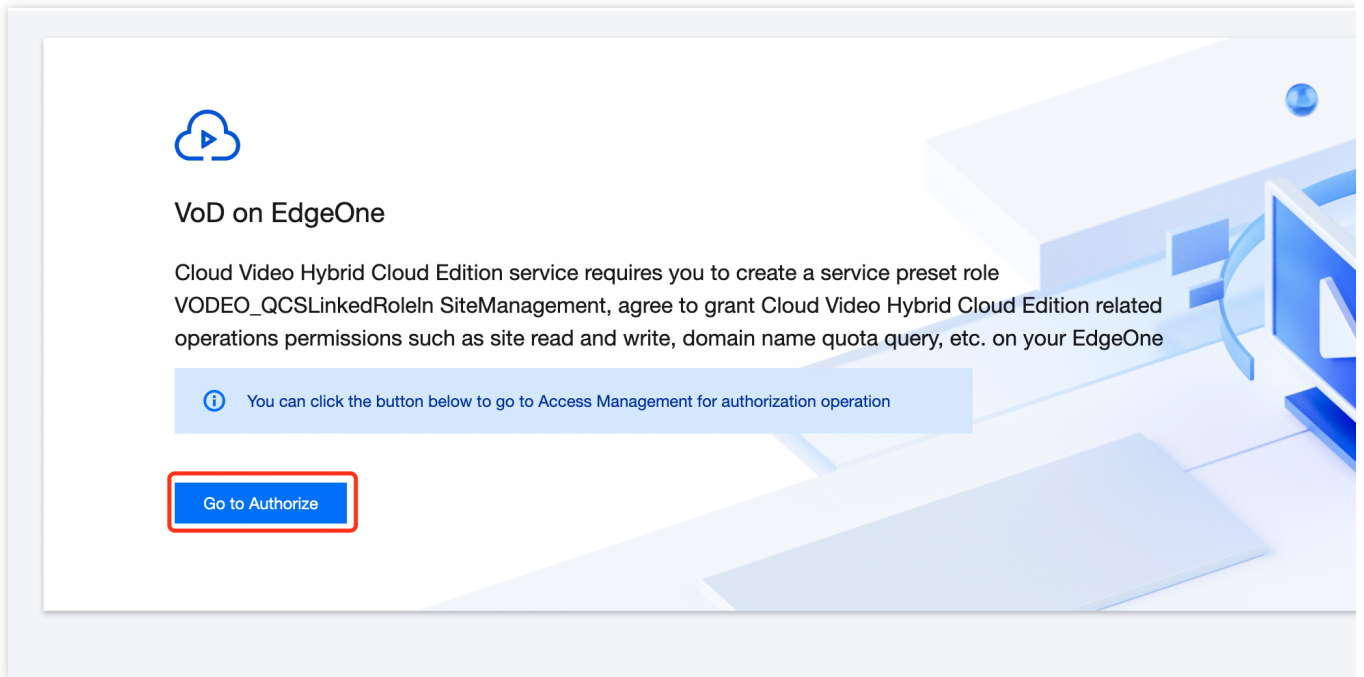
Step Two: Retrieve AWS S3 bucket information

- Navigate to the AWS [S3](#) bucket list and copy the name and region information of the bucket you wish to bind.



Step Three: Create a VOD on EO application

- Navigate to the VOD on EO [Console](#), then click **Go to Authorize**.



2. On the application creation page, fill in the application name (within 40 characters).
3. Enter the Access key ID and Secret access key created in Step One, along with the bucket information retrieved in Step Two. Select the corresponding region for the bucket, then click **Create** to complete the application creation.

Create Application

1 Application Basic Information

Application Name *
Application name cannot exceed 40 characters

2 Bind storage bucket

Storage service provider * Tencent Cloud COS Amazon Simple Storage Service

After creating the application, you can continue to add buckets

Account Information *

AccessKey *
SecretKey *

[Storage Managed Authorization Information](#)

Select storage bucket *

Region *

Bucket Name *

3 Default site check ⓘ

✔ Default site is in available status, can directly create application