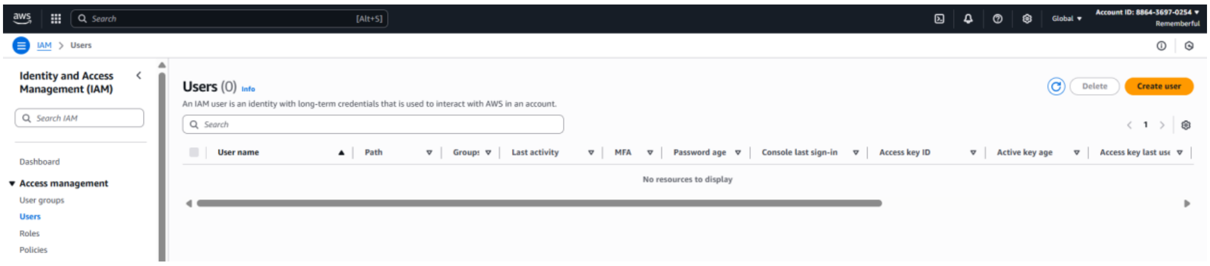
Day 23

“CLOUD SECURITY”

Implementing AWS Key Management Services:

Steps:

Open the “Users” section in the IAM:



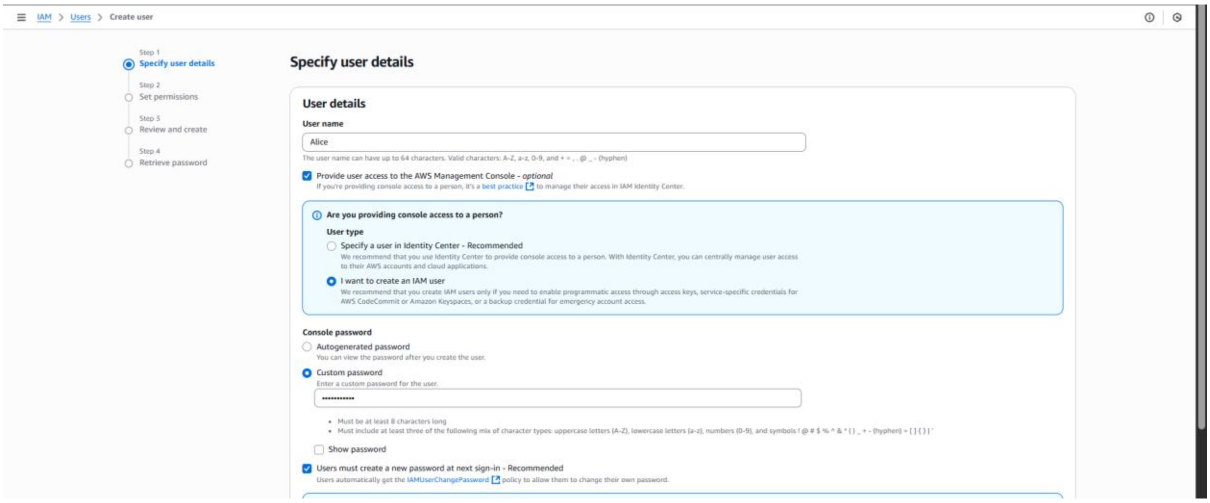
Users (0) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name ▲	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age	Access key last use

No resources to display

Click on “create user”: following screen will appear. Fill it accordingly, make sure to check mark the “Provide user access to the AWS Management Console – *optional*”



Specify user details

User details

User name: Alice

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.

Are you providing console access to a person?

User type

○ Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

● I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

○ Autogenerated password

You can view the password after you create the user.

● Custom password

Enter a custom password for the user.

••••••••••••

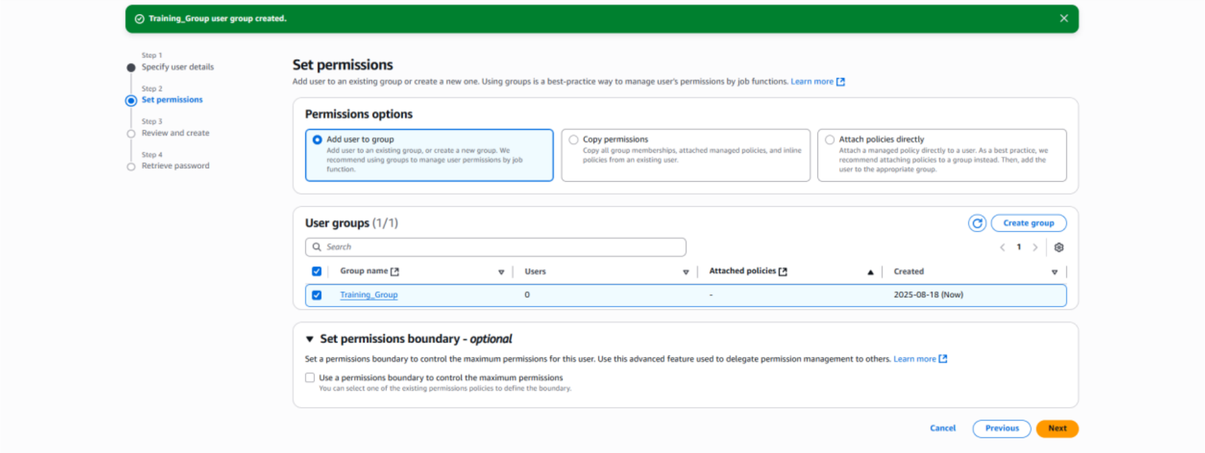
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ Show password

☑ Users must create a new password at next sign-in - Recommended

Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

Click on the “next” button: following screen will appear, select the respective group.



Training_Group user group created.

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 policies to a group instead. Then, add the user to the appropriate group.

User groups (1/1)

☑	Group name	Users	Attached policies ▲	Created
☑	Training_Group	0	-	2025-08-18 (Now)

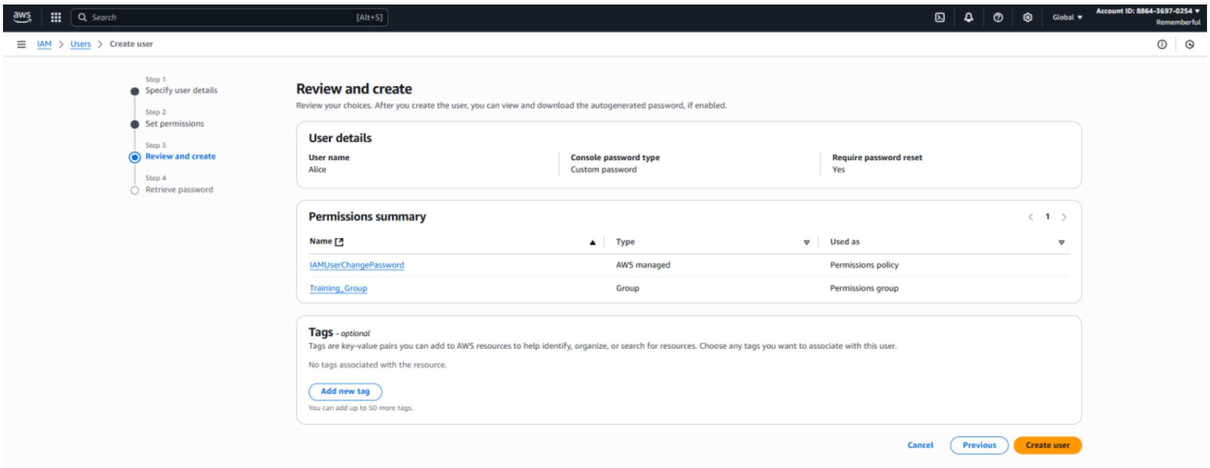
▾ Set permissions boundary - *optional*

Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more

□ Use a permissions boundary to control the maximum permissions

You can select one of the existing permissions policies to define the boundary.

Click on the “Next” button: following screen will appear. You may add the tag, and then click on the “Create User” button.



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	Console password type	Require password reset
Alice	Custom password	Yes

Permissions summary

Name	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy
Training_Group	Group	Permissions group

Tags - *optional*

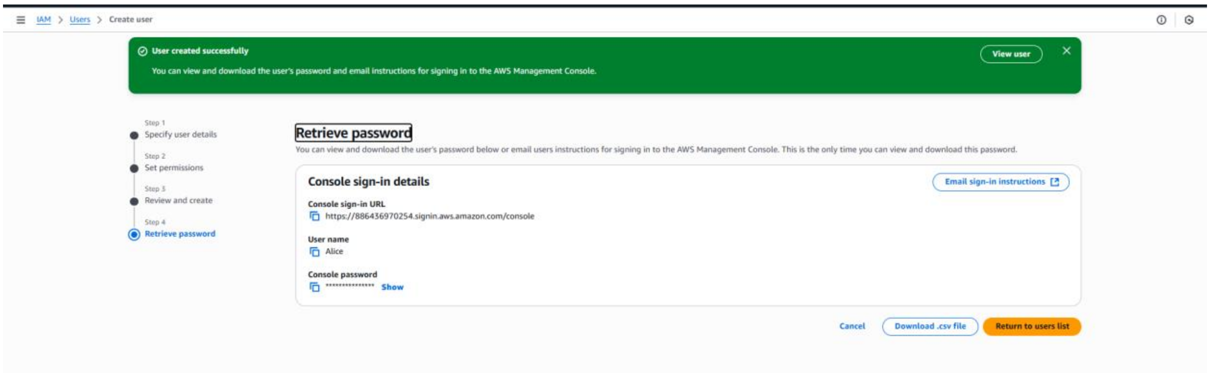
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Following confirmation occurs:



User created successfully

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

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.

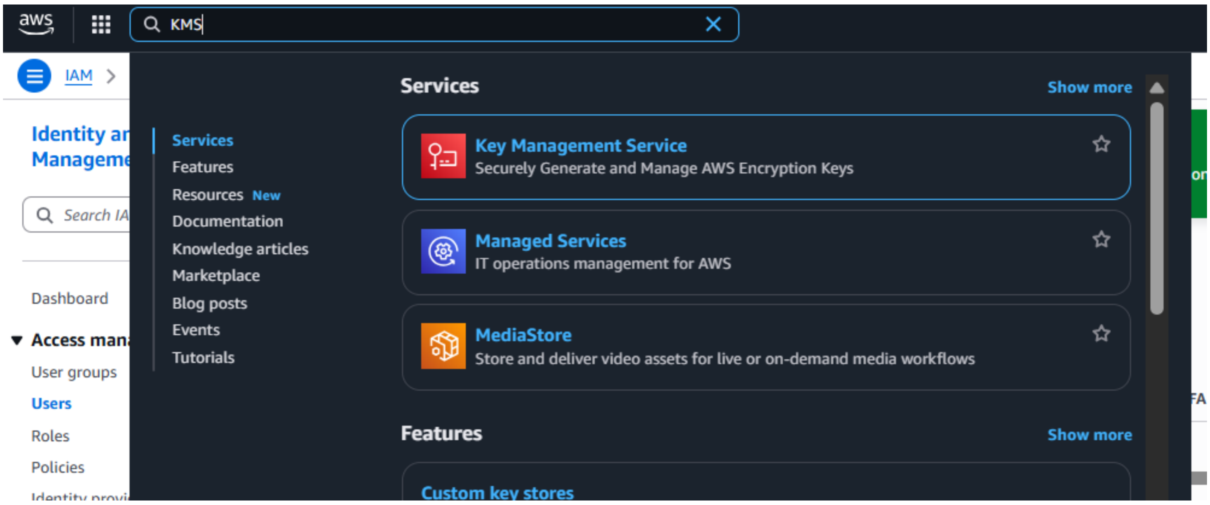
Console sign-in details

Console sign-in URL
https://886436970254.signin.aws.amazon.com/console

User name
Alice

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

Now, open the KMS:



Services

Key Management Service
Securely Generate and Manage AWS Encryption Keys

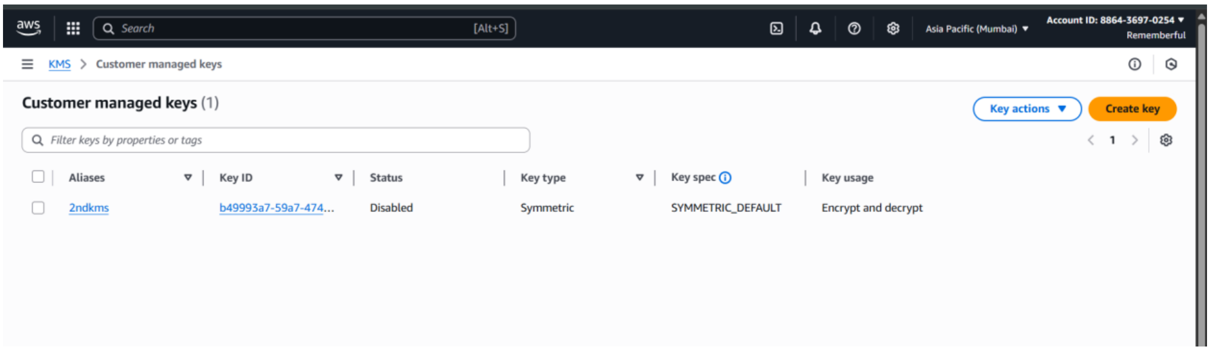
Managed Services
IT operations management for AWS

MediaStore
Store and deliver video assets for live or on-demand media workflows

Features

Custom key stores

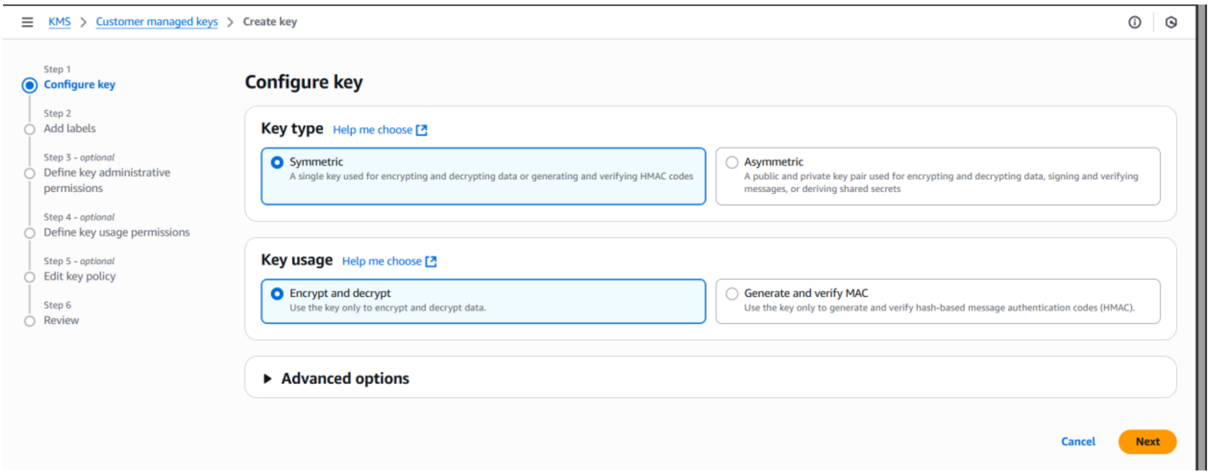
Following screen will appear:


aws
Search
[Alt+S]
Asia Pacific (Mumbai) ▾
Account ID: 8864-3697-0254 ▾
Rememberful
KMS > Customer managed keys
Key actions ▾
Create key
Filter keys by properties or tags
‹ 1 ›

Customer managed keys (1)

	Aliases	Key ID	Status	Key type	Key spec	Key usage
□	2ndkms	b49993a7-59a7-474...	Disabled	Symmetric	SYMMETRIC_DEFAULT	Encrypt and decrypt

Click on the “create key” button: following screen will appear.



Configure key

Key type

● Symmetric
A single key used for encrypting and decrypting data or generating and verifying HMAC codes

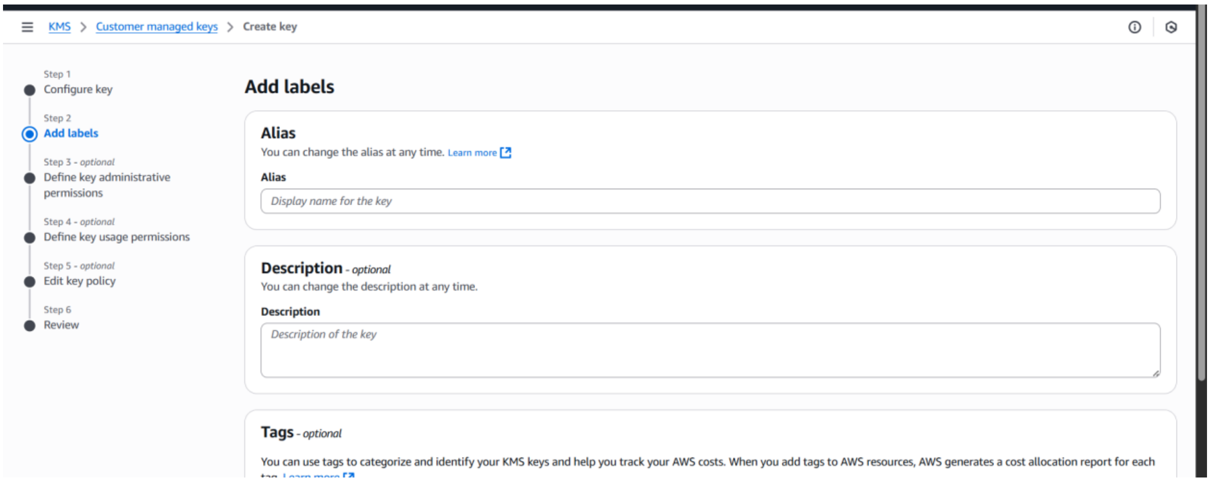
○ Asymmetric
A public and private key pair used for encrypting and decrypting data, signing and verifying messages, or deriving shared secrets

Key usage

● Encrypt and decrypt
Use the key only to encrypt and decrypt data.

○ Generate and verify MAC
Use the key only to generate and verify hash-based message authentication codes (HMAC).

Select accordingly and click on the “next” button: following screen will appear.



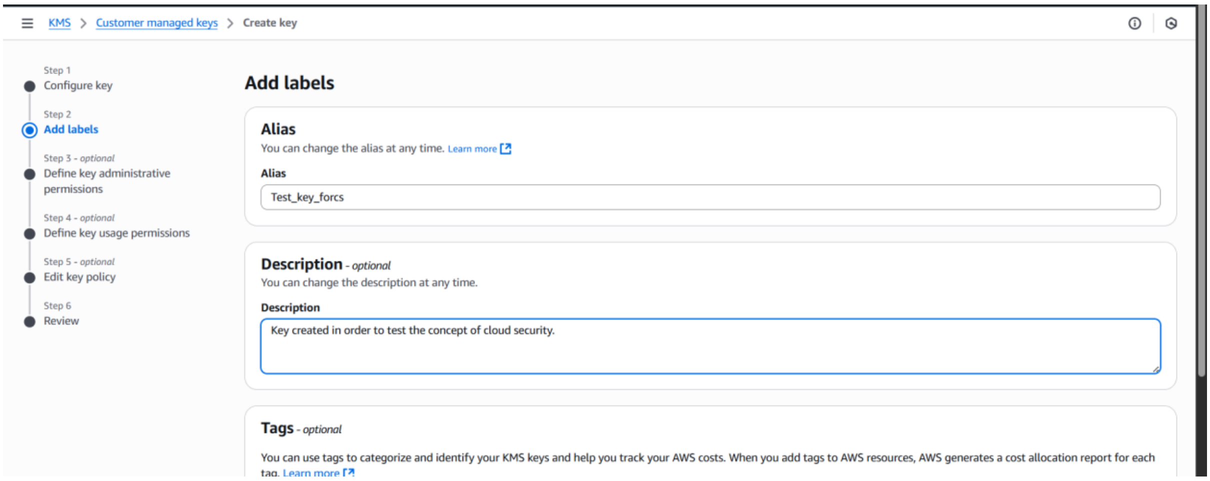
Add labels

Alias
You can change the alias at any time.
Alias: Display name for the key

Description - optional
You can change the description at any time.
Description: Description of the key

Tags - optional
You can use tags to categorize and identify your KMS keys and help you track your AWS costs. When you add tags to AWS resources, AWS generates a cost allocation report for each

Fill it accordingly:



Add labels

Alias

You can change the alias at any time. Learn more

Alias: Test_key_forcs

Description - optional

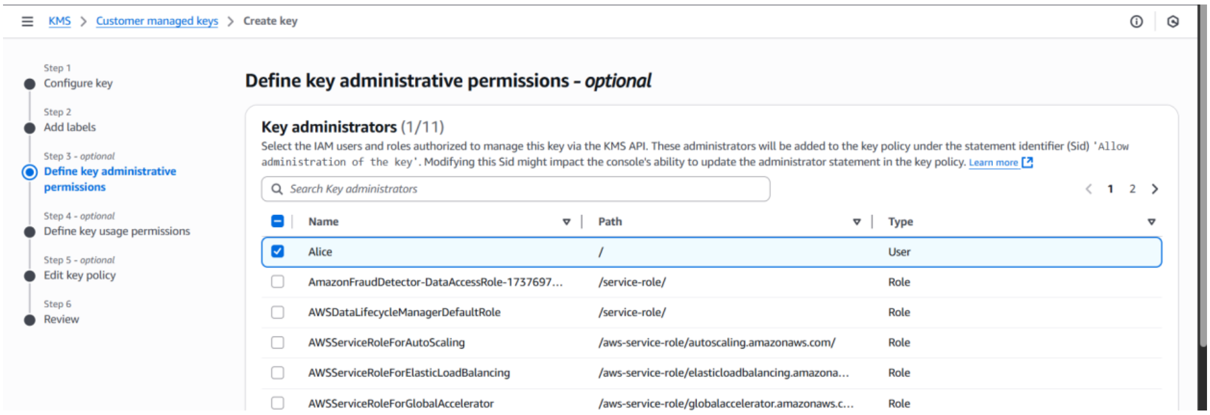
You can change the description at any time.

Description: Key created in order to test the concept of cloud security.

Tags - optional

You can use tags to categorize and identify your KMS keys and help you track your AWS costs. When you add tags to AWS resources, AWS generates a cost allocation report for each tag. Learn more

Click on the “Next” button: select the admin name (user created)


KMS > Customer managed keys > Create key
Step 1
Configure key
Step 2
Add labels
Step 3 - optional
Define key administrative permissions
Step 4 - optional
Define key usage permissions
Step 5 - optional
Edit key policy
Step 6
Review
Search Key administrators
< 1 2 >

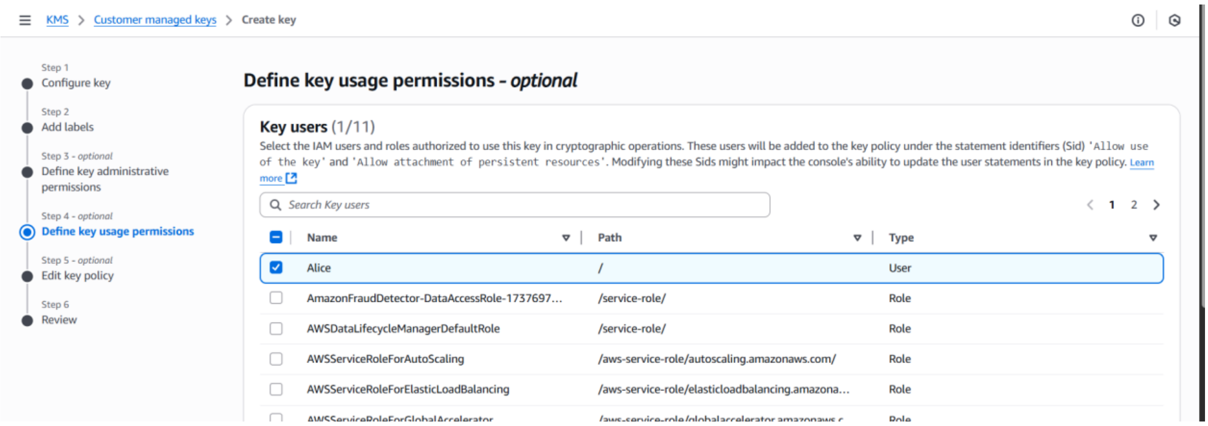
Define key administrative permissions - *optional*

Key administrators (1/11)

Select the IAM users and roles authorized to manage this key via the KMS API. These administrators will be added to the key policy under the statement identifier (Sid) `'Allow administration of the key'`. Modifying this Sid might impact the console's ability to update the administrator statement in the key policy. Learn more

	Name	Path	Type
☑	Alice	/	User
□	AmazonFraudDetector-DataAccessRole-1737697...	/service-role/	Role
□	AWSDataLifecycleManagerDefaultRole	/service-role/	Role
□	AWSServiceRoleForAutoScaling	/aws-service-role/autoscaling.amazonaws.com/	Role
□	AWSServiceRoleForElasticLoadBalancing	/aws-service-role/elasticloadbalancing.amazona...	Role
□	AWSServiceRoleForGlobalAccelerator	/aws-service-role/globalaccelerator.amazonaws.c...	Role

Click on the “Next” button: again select the name.



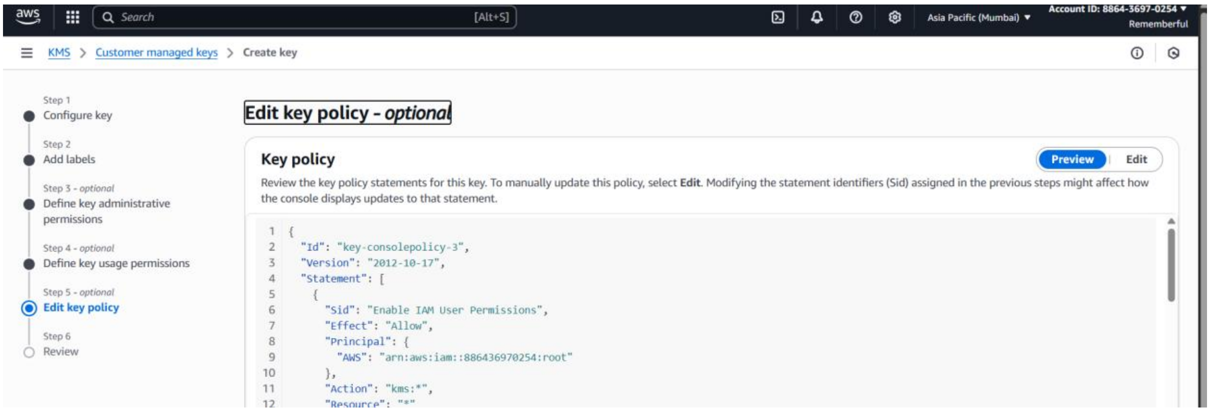
Define key usage permissions - *optional*

Key users (1/11)

Select the IAM users and roles authorized to use this key in cryptographic operations. These users will be added to the key policy under the statement identifiers (Sid) `'Allow use of the key'` and `'Allow attachment of persistent resources'`. Modifying these Sids might impact the console's ability to update the user statements in the key policy. Learn more

	Name	Path	Type
☑	Alice	/	User
□	AmazonFraudDetector-DataAccessRole-1737697...	/service-role/	Role
□	AWSDataLifecycleManagerDefaultRole	/service-role/	Role
□	AWSServiceRoleForAutoScaling	/aws-service-role/autoscaling.amazonaws.com/	Role
□	AWSServiceRoleForElasticLoadBalancing	/aws-service-role/elasticloadbalancing.amazona...	Role
□	AWSServiceRoleForGlobalAccelerator	/aws-service-role/globalaccelerator.amazonaws.c	Role

Click on the “Next” button: review the key policy, as shown below.



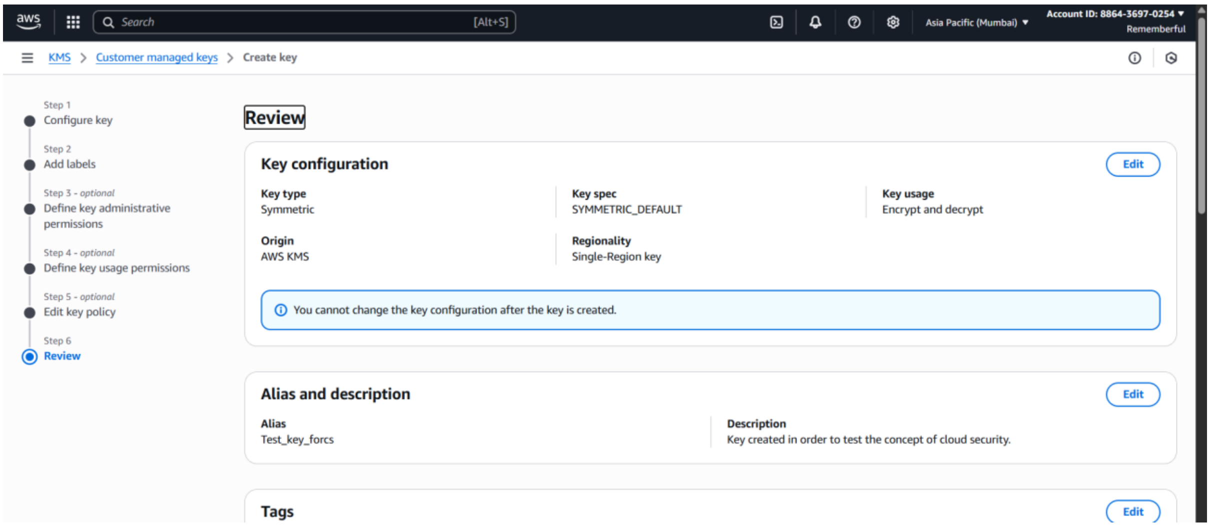
Edit key policy - *optional*

Key policy

Review the key policy statements for this key. To manually update this policy, select **Edit**. Modifying the statement identifiers (Sid) assigned in the previous steps might affect how the console displays updates to that statement.

```
{
  "Id": "key-consolepolicy-3",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::886436970254:root"
      },
      "Action": "kms:*",
      "Resource": "*"
```

Click on the “Next” button to open the review section as shown below:



Review

Key configuration

Key type: Symmetric
Key spec: SYMMETRIC_DEFAULT
Key usage: Encrypt and decrypt
Origin: AWS KMS
Regionality: Single-Region key

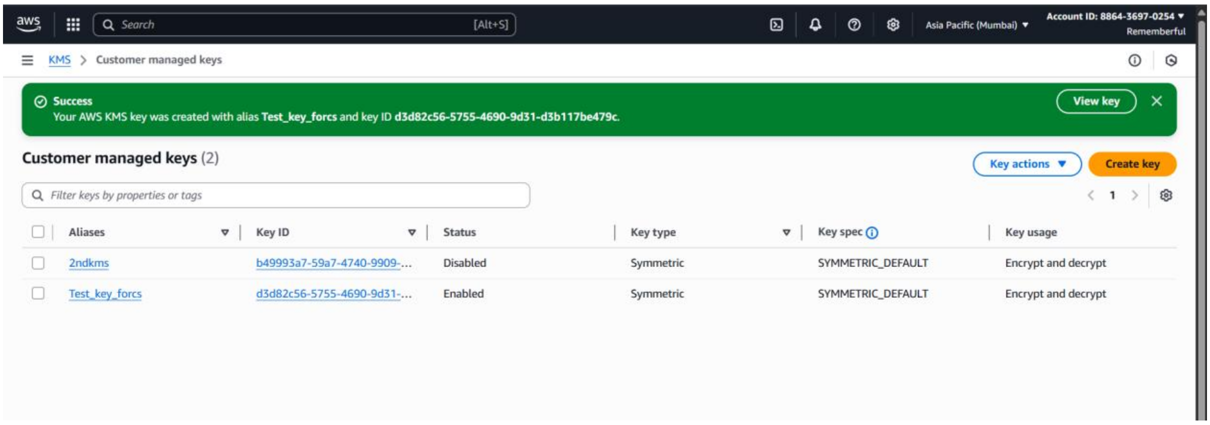
ⓘ You cannot change the key configuration after the key is created.

Alias and description

Alias: Test_key_forcs
Description: Key created in order to test the concept of cloud security.

Tags

Click on the “finish” button to create the key: following confirmation will occur.

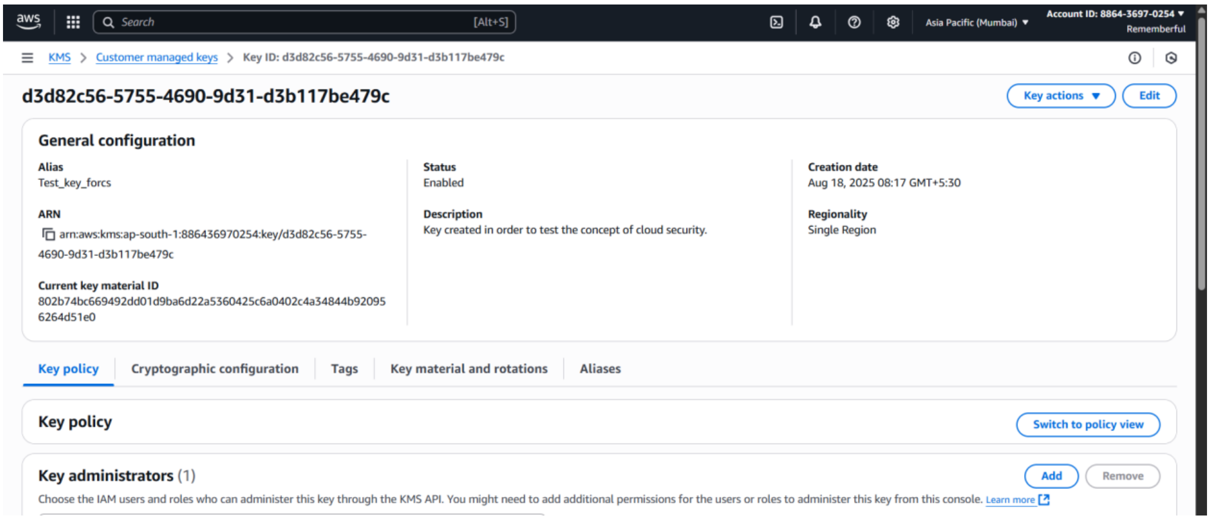

aws
Search
[Alt+S]
Asia Pacific (Mumbai) ▾
Account ID: 8864-3697-0254 ▾
Rememberful
KMS > Customer managed keys
View key
Key actions ▾
Create key
Filter keys by properties or tags
< 1 >

Success
Your AWS KMS key was created with alias **Test_key_forcs** and key ID **d3d82c56-5755-4690-9d31-d3b117be479c**.

Customer managed keys (2)

□	Aliases	Key ID	Status	Key type	Key spec	Key usage
□	2ndkms	b49993a7-59a7-4740-9909-...	Disabled	Symmetric	SYMMETRIC_DEFAULT	Encrypt and decrypt
□	Test_key_forcs	d3d82c56-5755-4690-9d31-...	Enabled	Symmetric	SYMMETRIC_DEFAULT	Encrypt and decrypt

You may check the properties of that key by clicking on it, following screen will appear:



KMS > Customer managed keys > Key ID: d3d82c56-5755-4690-9d31-d3b117be479c

d3d82c56-5755-4690-9d31-d3b117be479c

General configuration

Alias
Test_key_forcs

ARN
arn:aws:kms:ap-south-1:886436970254:key/d3d82c56-5755-4690-9d31-d3b117be479c

Current key material ID
802b74bc669492dd01d9ba6d22a5360425c6a0402c4a34844b92095 6264d51e0

Status
Enabled

Description
Key created in order to test the concept of cloud security.

Creation date
Aug 18, 2025 08:17 GMT+5:30

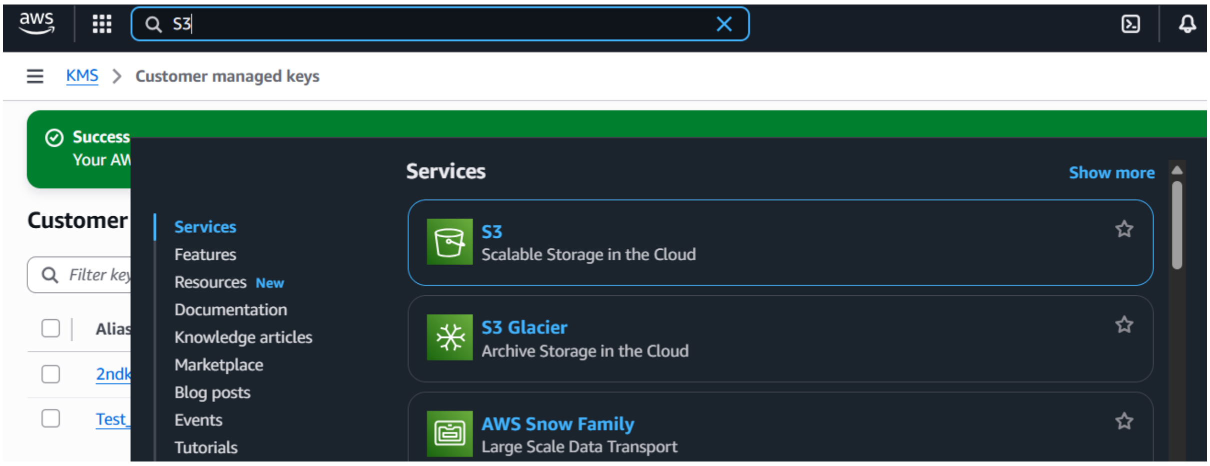
Regionality
Single Region

Key policy

Key administrators (1)

Choose the IAM users and roles who can administer this key through the KMS API. You might need to add additional permissions for the users or roles to administer this key from this console. Learn more

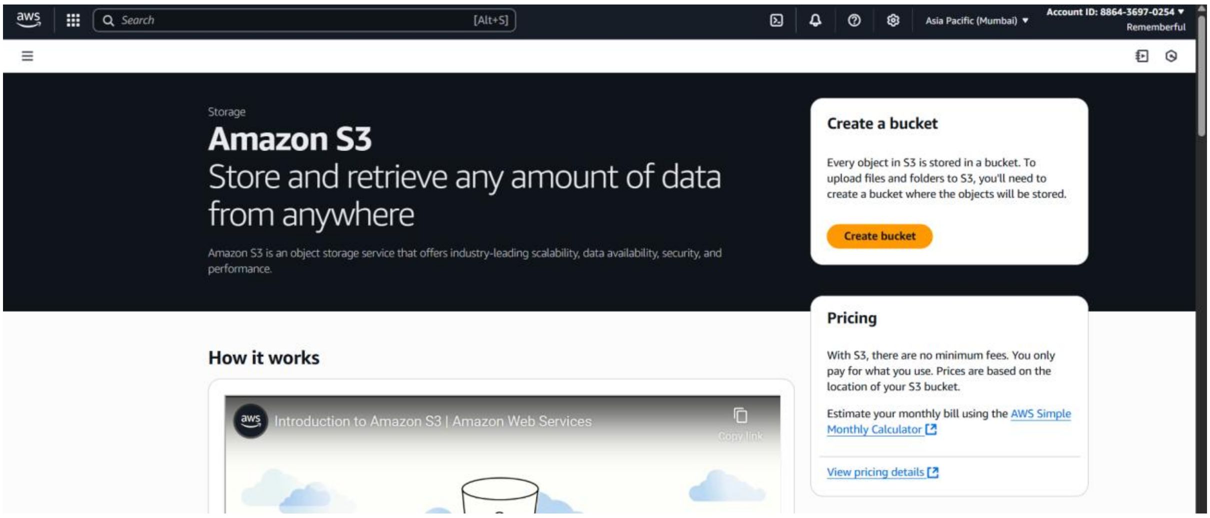
Now, click open the "S3"



S3

KMS > Customer managed keys

Following screen will appear:



Storage

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

How it works

Create a bucket

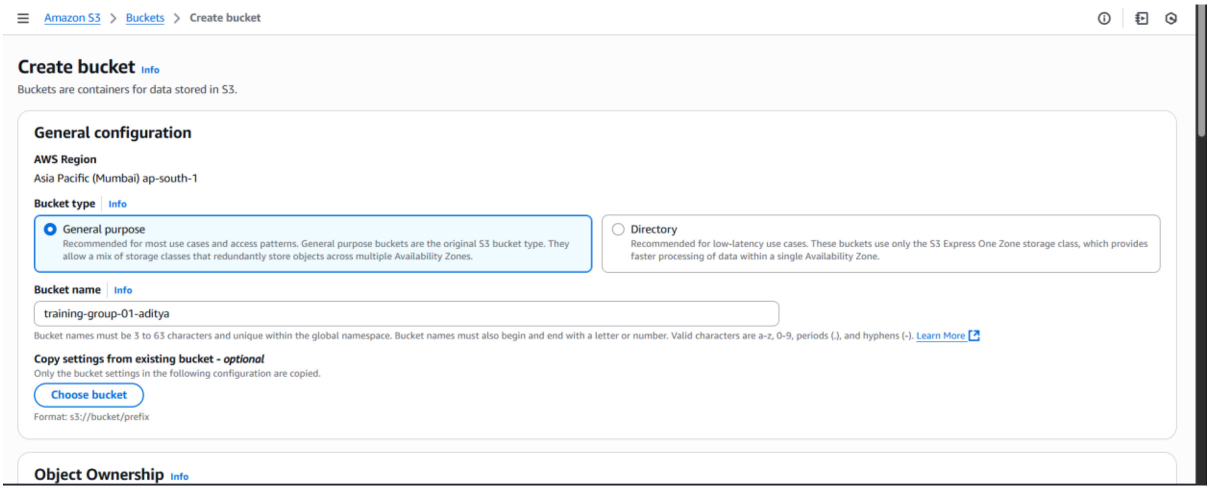
Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

Pricing

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the AWS Simple Monthly Calculator

Click on the "Create Bucket" option: following screen will appear.



Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-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

training-group-01-aditya

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). Learn More

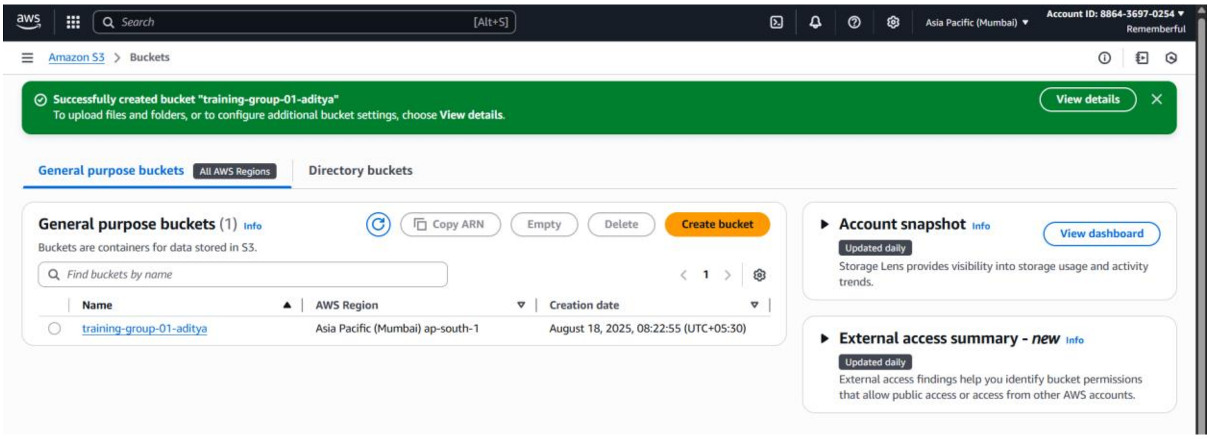
Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

Object Ownership Info

Keep everything as default and then click on the ‘Create bucket’ button at the bottom: following confirmation will occur.



Successfully created bucket "training-group-01-aditya"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

General purpose buckets (1) Info

Buckets are containers for data stored in S3.

	Name	AWS Region	Creation date
○	training-group-01-aditya	Asia Pacific (Mumbai) ap-south-1	August 18, 2025, 08:22:55 (UTC+05:30)

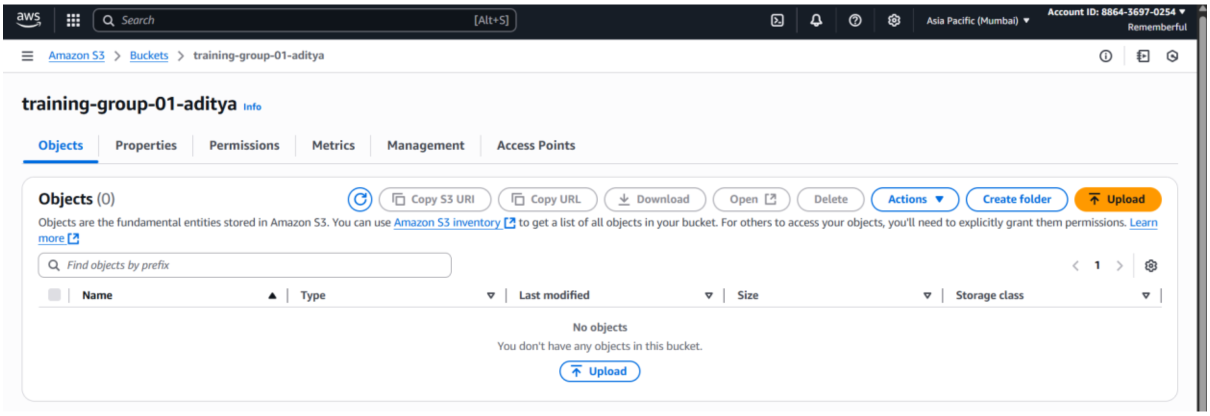
▶ Account snapshot Info

Storage Lens provides visibility into storage usage and activity trends.

▶ External access summary - *new* Info

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

Open that bucket:


aws
Search
[Alt+S]
Asia Pacific (Mumbai) ▼
Account ID: 8864-3697-0254 ▼
Rememberful
Amazon S3 > Buckets > training-group-01-aditya

training-group-01-aditya Info

Objects (0)

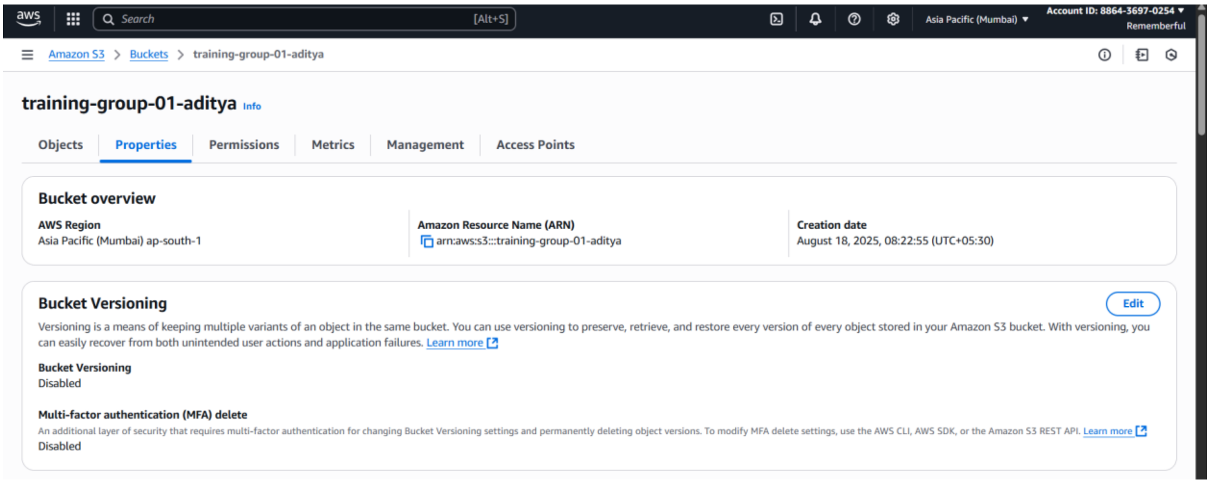
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.

Go to the “properties” section and click on the edit button at the “bucket versioning” section:



training-group-01-aditya

Bucket overview

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

Amazon Resource Name (ARN)
arn:aws:s3:::training-group-01-aditya

Creation date
August 18, 2025, 08:22:55 (UTC+05:30)

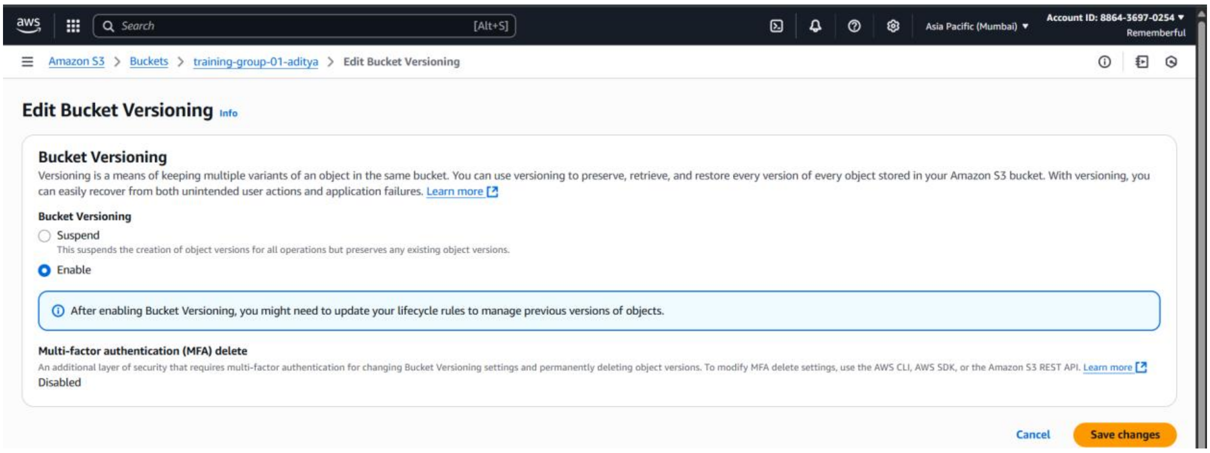
Bucket Versioning

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

Click on the “Enable” radio button: click on the save changes.


aws
Search
[Alt+S]
Asia Pacific (Mumbai) ▾
Account ID: 8864-3697-0254 ▾
Rememberful
Amazon S3 > Buckets > training-group-01-aditya > Edit Bucket Versioning
Info
Cancel
Save changes

Edit Bucket Versioning

Bucket Versioning

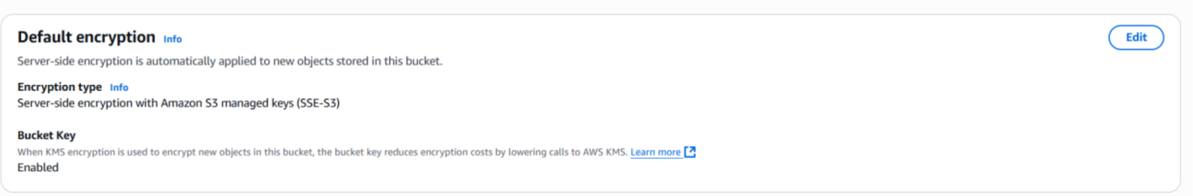
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning
○ Suspend
This suspends the creation of object versions for all operations but preserves any existing object versions.
● Enable

After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.

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

Under the “Properties” section, scroll down and reach the “Default Encryption” section:



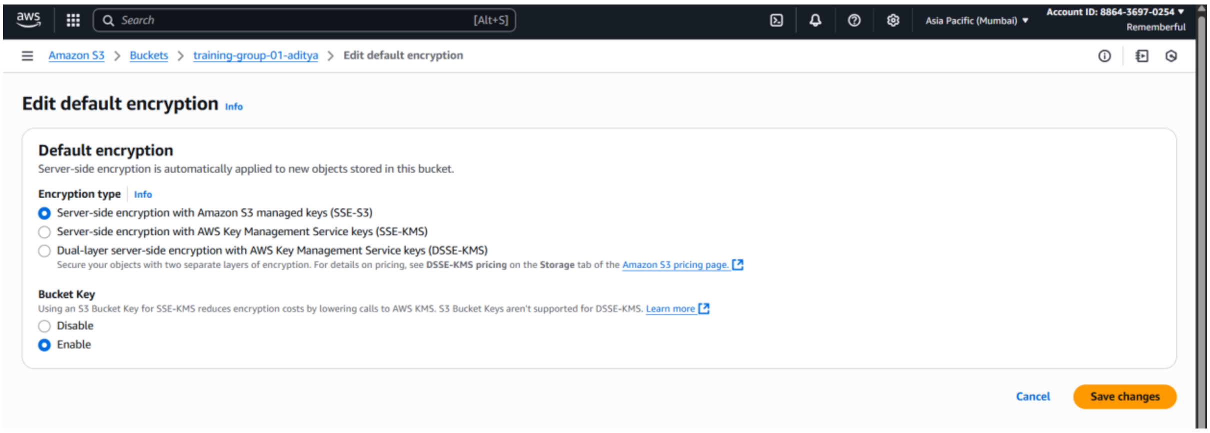
Default encryption

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

Encryption type
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

Click on the “edit” button: following options will appear.


aws
Search
[Alt+S]
Asia Pacific (Mumbai) ▾
Account ID: 8864-3697-0254 ▾
Rememberful
Amazon S3 > Buckets > training-group-01-aditya > Edit default encryption
Info
Cancel
Save changes

Edit default encryption

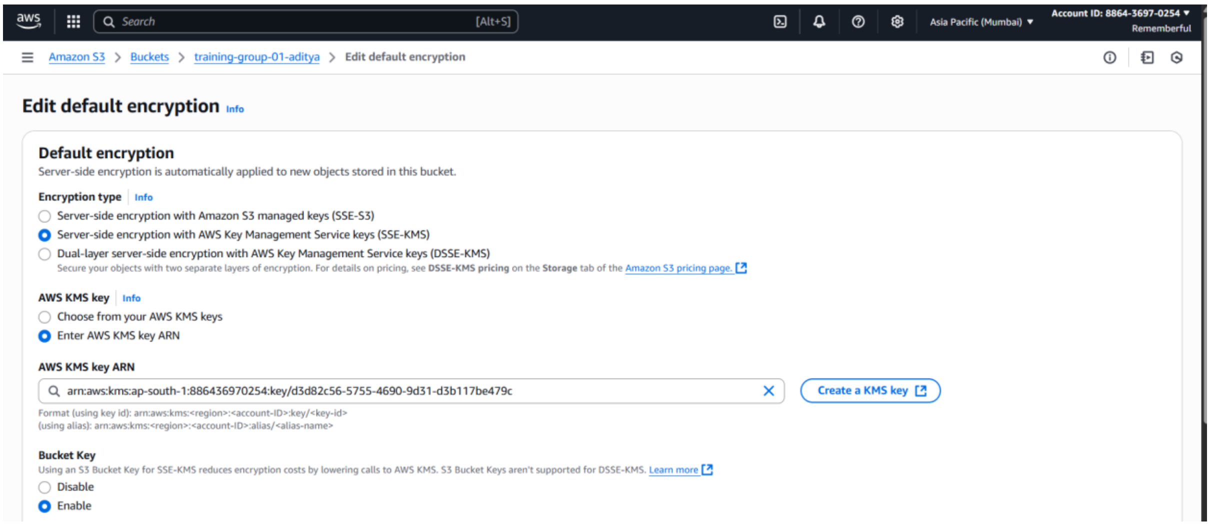
Default encryption

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

Encryption type
● Server-side encryption with Amazon S3 managed keys (SSE-S3)
○ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more
○ Disable
● Enable

Under the "encryption type" select the "Server-side encryption with AWS Key Management Service keys (SSE-KMS)": also specify the AWS KMS key ARN. Then click on the "Save changes" button.


aws
Search [Alt+S]
Asia Pacific (Mumbai) ▾
Account ID: 8864-3697-0254 ▾
Rememberful
Amazon S3 > Buckets > training-group-01-aditya > Edit default encryption

Edit default encryption Info

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

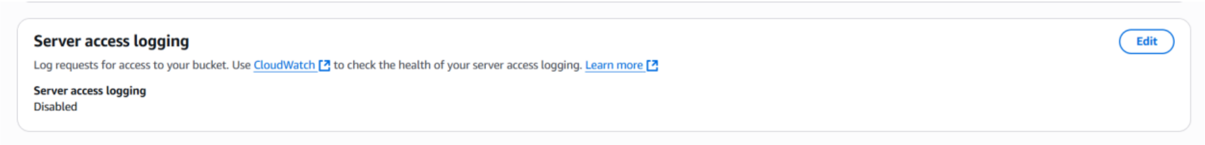
Encryption type | Info
○ Server-side encryption with Amazon S3 managed keys (SSE-S3)
● Server-side encryption with AWS Key Management Service keys (SSE-KMS)
○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

AWS KMS key | Info
○ Choose from your AWS KMS keys
● Enter AWS KMS key ARN

AWS KMS key ARN
arn:aws:kms:ap-south-1:886436970254:key/d3d82c56-5755-4690-9d31-d3b117be479c
Format (using key id): arn:aws:kms:<region>:<account-ID>:key/<key-id>
(using alias): arn:aws:kms:<region>:<account-ID>:alias/<alias-name>

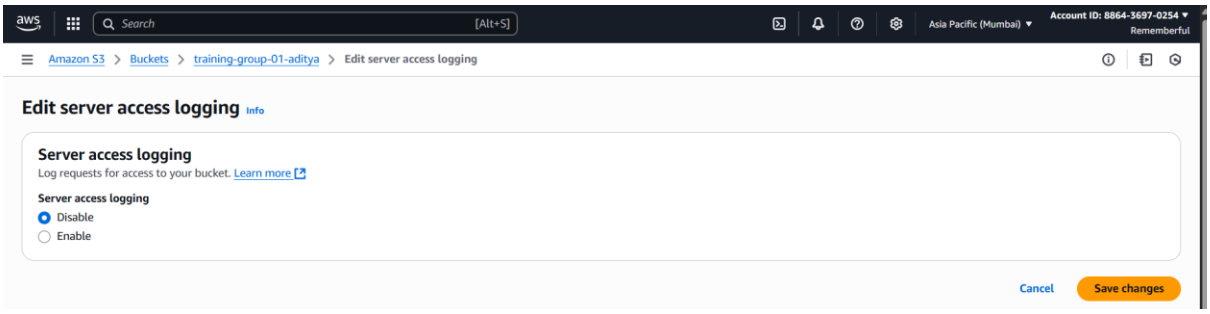
Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more
○ Disable
● Enable

Now, open the 'Server access logging' section:



Server access logging
Log requests for access to your bucket. Use CloudWatch to check the health of your server access logging. Learn more
Server access logging
Disabled

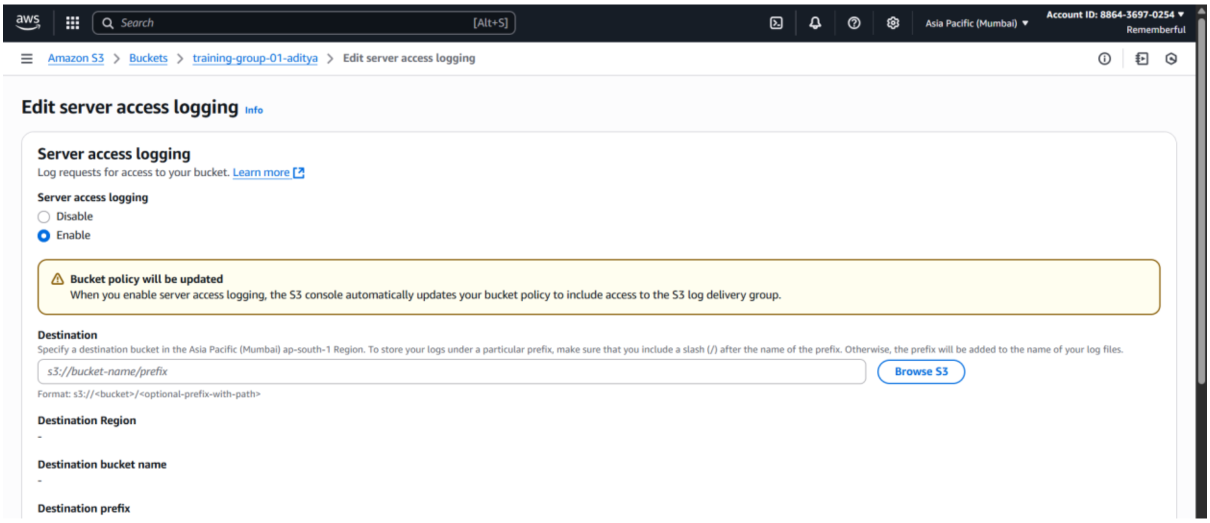
Click on the "edit" button: following screen will appear.


aws
Search [Alt+S]
Asia Pacific (Mumbai) ▾
Account ID: 8864-3697-0254 ▾
Rememberful
Amazon S3 > Buckets > training-group-01-aditya > Edit server access logging
Cancel
Save changes

Edit server access logging Info

Server access logging
Log requests for access to your bucket. Learn more
Server access logging
● Disable
○ Enable

Click on the "enable" button: screen changes to this.


aws
Search [Alt+S]
Asia Pacific (Mumbai) ▾
Account ID: 8864-3697-0254 ▾
Rememberful
Amazon S3 > Buckets > training-group-01-aditya > Edit server access logging
Browse S3

Edit server access logging Info

Server access logging
Log requests for access to your bucket. Learn more
Server access logging
○ Disable
● Enable

⚠ **Bucket policy will be updated**
When you enable server access logging, the S3 console automatically updates your bucket policy to include access to the S3 log delivery group.

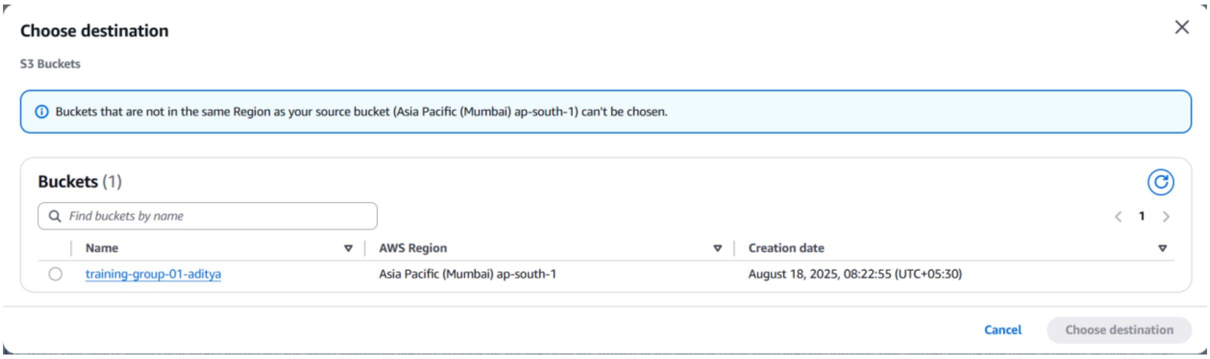
Destination
Specify a destination bucket in the Asia Pacific (Mumbai) ap-south-1 Region. To store your logs under a particular prefix, make sure that you include a slash (/) after the name of the prefix. Otherwise, the prefix will be added to the name of your log files.
s3://bucket-name/prefix
Format: s3://<bucket>/<optional-prefix-with-path>

Destination Region
-

Destination bucket name
-

Destination prefix

Click on the “Browse S3” button: select the Bucket.



Choose destination

S3 Buckets

ⓘ Buckets that are not in the same Region as your source bucket (Asia Pacific (Mumbai) ap-south-1) can't be chosen.

Buckets (1)

	Name	AWS Region	Creation date
○	training-group-01-aditya	Asia Pacific (Mumbai) ap-south-1	August 18, 2025, 08:22:55 (UTC+05:30)

And done!

--The End--