Working with Identity Access management (IAM)

Identity Access Management

It helps you manage access to AWS resources. It enables you to control who can access your AWS resources (authentication) and what actions they can perform (authorization) on those resources.

IAM allows you to create and manage users, groups, and roles within your AWS account.

Users: IAM users are entities with long-term credentials (username and password) or access keys that are used to interact with AWS services. You can create and manage IAM users, assign them permissions, and control their access to AWS resources.

Groups: IAM groups are collections of users. You can assign permissions to groups, making it easier to manage access for multiple users who need similar permissions. Users can be added to multiple groups, and their permissions are determined by the combination of group and individual user permissions.

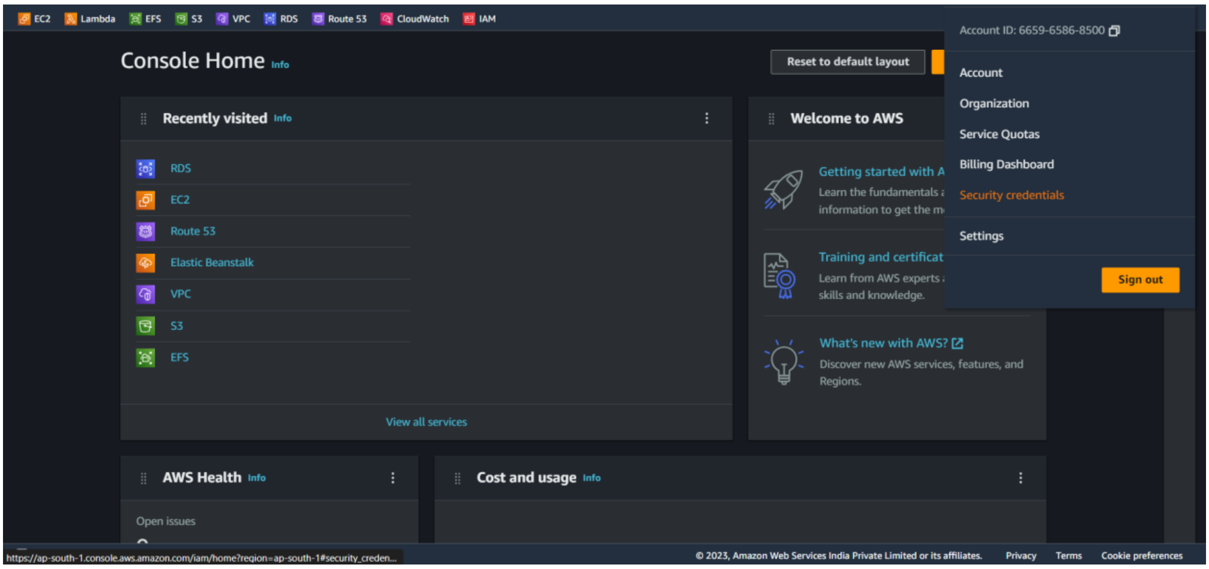
Roles: IAM roles are similar to users, but they are not associated with a specific individual. Roles are typically used to grant temporary permissions to entities such as EC2 instances, AWS services, or applications running on your behalf. Roles provide a secure way to delegate access to AWS resources without sharing long-term credentials.

Policies: IAM policies are JSON documents that define permissions and access control rules. Policies can be attached to users, groups, or roles to grant or deny access to AWS resources. Policies can be managed at a granular level, allowing fine-grained control over resource permissions.

Access Keys: IAM access keys consist of an access key ID and a secret access key. They are used to authenticate programmatic access to AWS services using AWS SDKs, command-line tools, or custom applications.

Multifactor Authentication: It is an additional layer of security that helps protect user accounts from unauthorized access, even if the username and password are compromised. MFA requires users to provide two or more different types of credentials to verify their identity.

1. Firstly Sign in to the AWS Management Console click on account name then click on security credentials or else search for IAM in services.



EC2 Lambda EFS S3 VPC RDS Route 53 CloudWatch IAM

Console Home Info

Reset to default layout

Recently visited Info

RDS
EC2
Route 53
Elastic Beanstalk
VPC
S3
EFS

View all services

Welcome to AWS

Getting started with A
Learn the fundamentals a
information to get the m

Training and certificat
Learn from AWS experts a
skills and knowledge.

What's new with AWS?
Discover new AWS services, features, and Regions.

Account ID: 6659-6586-8500

Account
Organization
Service Quotas
Billing Dashboard
Security credentials
Settings

Sign out

AWS Health Info

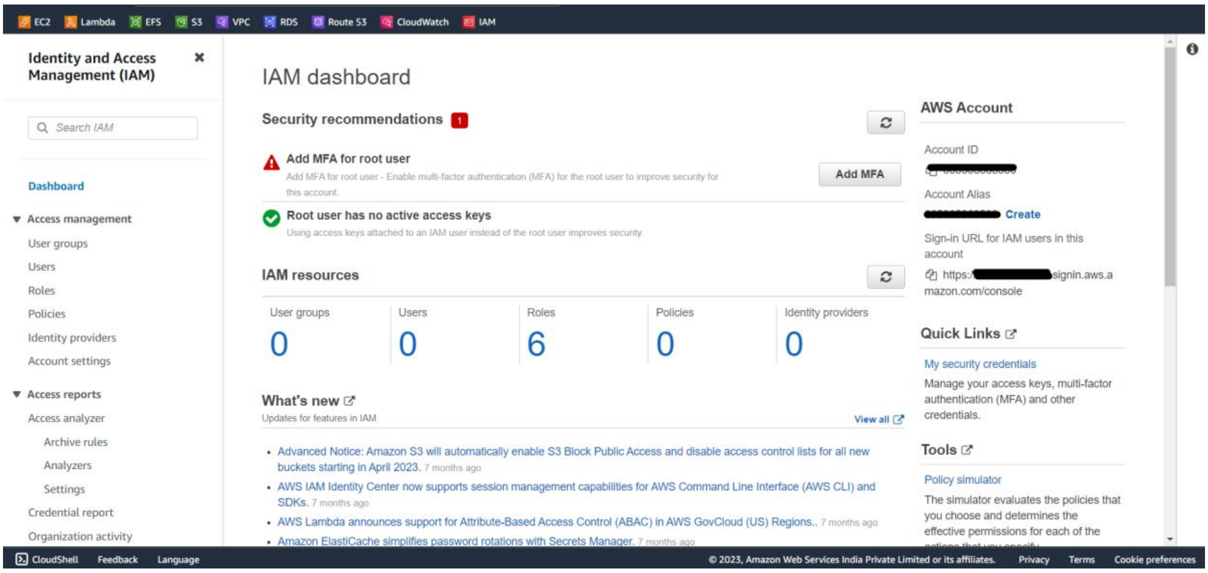
Open issues

Cost and usage Info

https://ap-south-1.console.aws.amazon.com/iam/home?region=ap-south-1#security_creden...

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

2. You will be navigated to IAM Dashboard where you can find all confidential information about your account



EC2 Lambda EFS S3 VPC RDS Route 53 CloudWatch IAM

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management
User groups
Users
Roles
Policies
Identity providers
Account settings

▼ Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity

IAM dashboard

Security recommendations 1

Add MFA for root user
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Add MFA

Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
0	0	6	0	0

What's new
Updates for features in IAM

View all

- Advanced Notice: Amazon S3 will automatically enable S3 Block Public Access and disable access control lists for all new buckets starting in April 2023. 7 months ago
- AWS IAM Identity Center now supports session management capabilities for AWS Command Line Interface (AWS CLI) and SDKs. 7 months ago
- AWS Lambda announces support for Attribute-Based Access Control (ABAC) in AWS GovCloud (US) Regions.. 7 months ago
- Amazon ElastiCache simplifies password rotations with Secrets Manager. 7 months ago

AWS Account

Account ID
[redacted]

Account Alias
[redacted] Create

Sign-in URL for IAM users in this account
https:/[redacted]signin.aws.amazon.com/console

Quick Links

My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

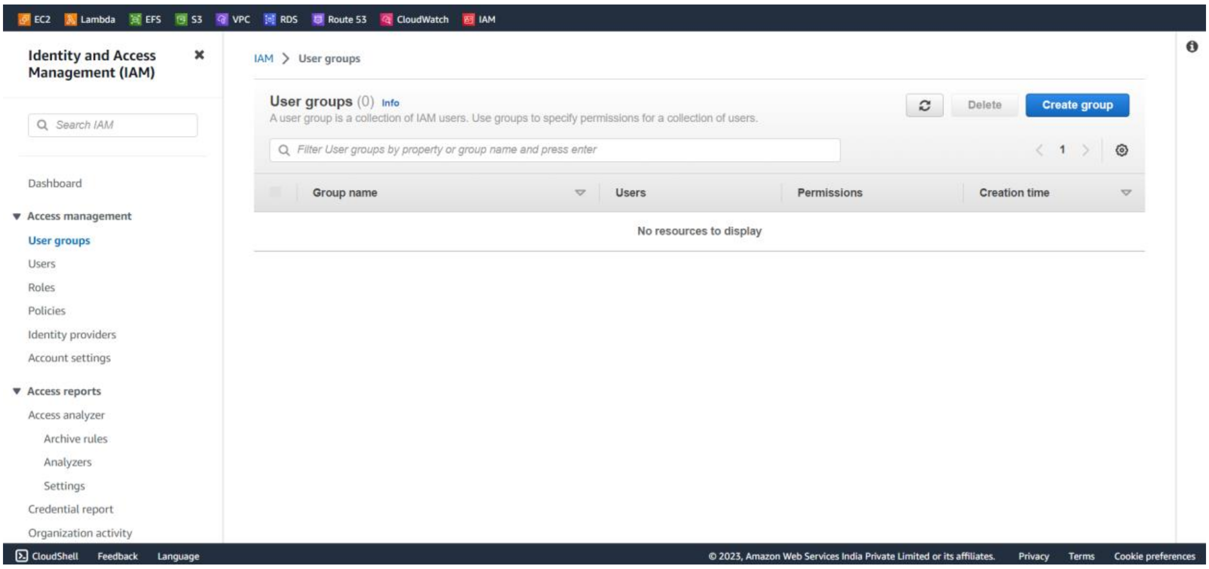
Tools

Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

3. In the IAM console, navigate to the "Users" section and click on the "Add user" button.



User groups (0) Info

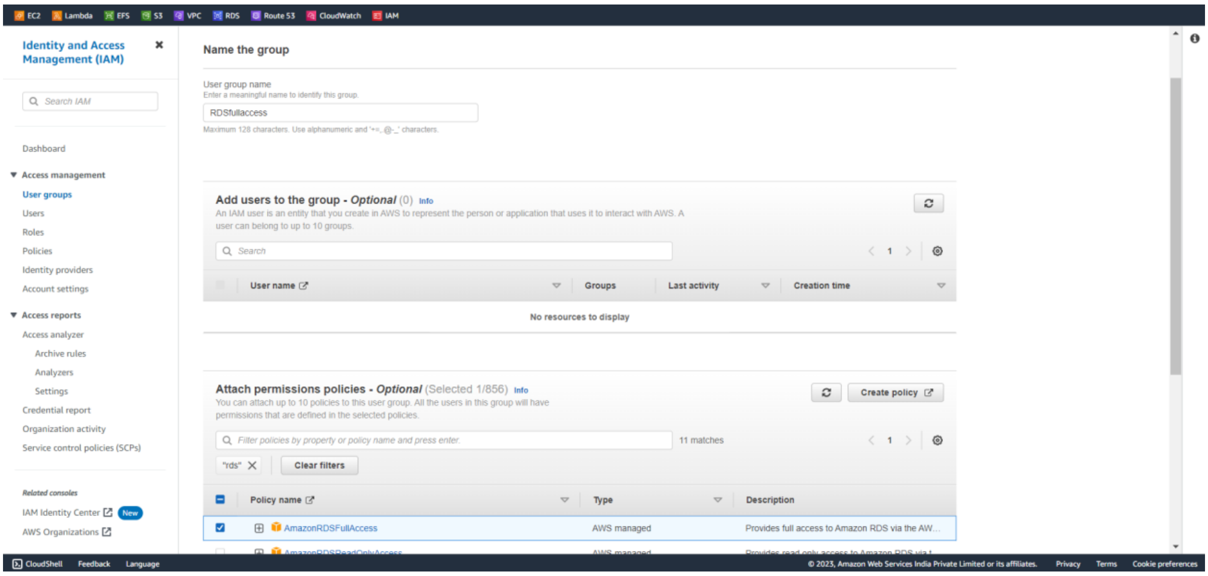
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

Group name	Users	Permissions	Creation time

No resources to display

4. Enter a name for the first user and select the access type. For this example, choose AWS Management Console access. Then click on the "Next: Permissions" button.



Name the group

User group name
Enter a meaningful name to identify this group.
RDSfullaccess
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (0) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

Search

User name	Groups	Last activity	Creation time

No resources to display

Attach permissions policies - *Optional* (Selected 1/856) Info

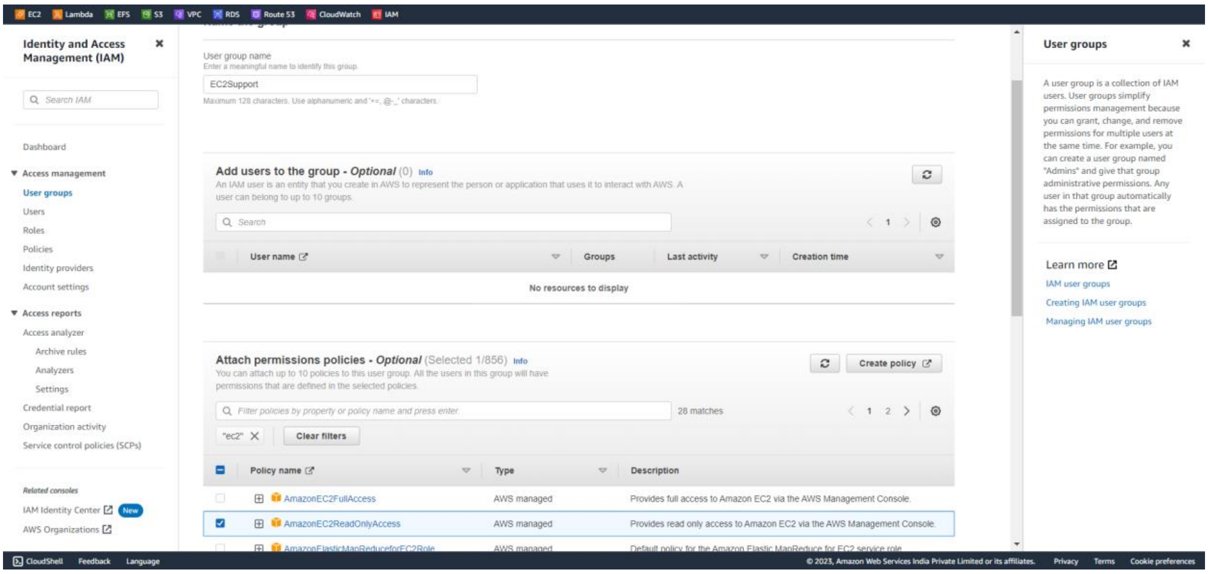
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter policies by property or policy name and press enter. 11 matches

"rds"

	Policy name	Type	Description
☑	AmazonRDSFullAccess	AWS managed	Provides full access to Amazon RDS via the AW...
□	AmazonRDSReadOnlyAccess	AWS managed	Provides read only access to Amazon RDS via t...

5. Now navigate to User groups section and click on create group button



User group name
Enter a meaningful name to identify this group.
EC2Support
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (0) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

□	User name	Groups	Last activity	Creation time

No resources to display

Attach permissions policies - *Optional* (Selected 1/856) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter policies by property or policy name and press enter. 28 matches

"ec2"

	Policy name	Type	Description
□	AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 via the AWS Management Console.
☑	AmazonEC2ReadOnlyAccess	AWS managed	Provides read only access to Amazon EC2 via the AWS Management Console.
□	AmazonElasticMapReduceforEC2Role	AWS managed	Default policy for the Amazon Elastic MapReduce for EC2 service role.

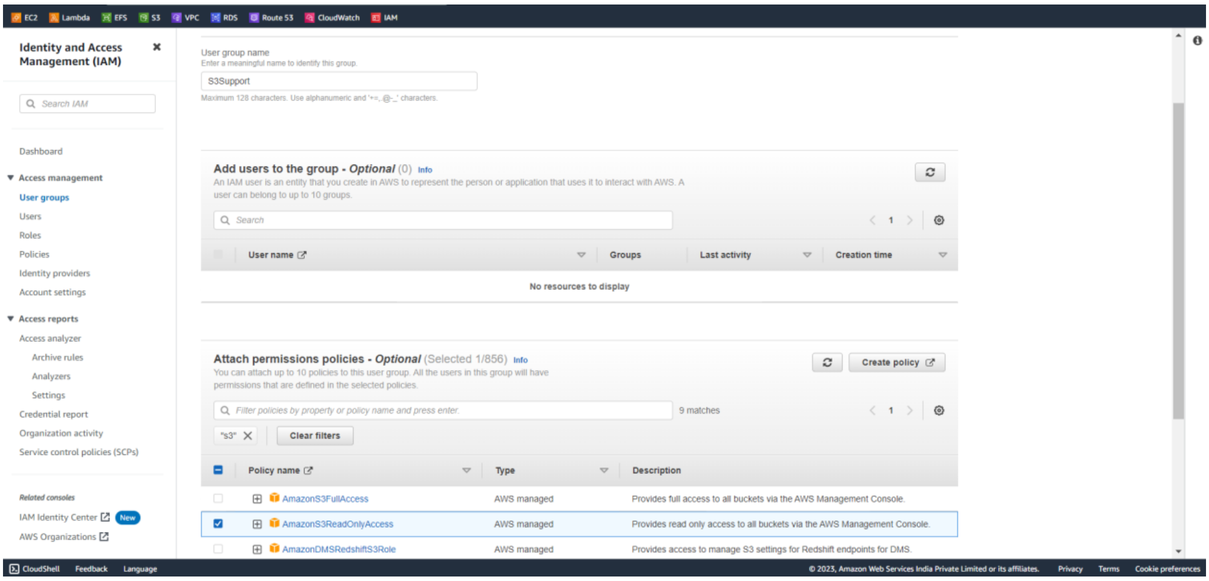
User groups

A user group is a collection of IAM users. User groups simplify permissions management because you can grant, change, and remove permissions for multiple users at the same time. For example, you can create a user group named "Admins" and give that group administrative permissions. Any user in that group automatically has the permissions that are assigned to the group.

Learn more
IAM user groups
Creating IAM user groups
Managing IAM user groups

© 2023, Amazon Web Services India Private Limited or its affiliates.

6. In the "Create group" dialog, enter a name for the first group and click on the "Create group" button and then "Set permissions" (policies) for the group.



User group name
Enter a meaningful name to identify this group.
S3Support
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (0) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

□	User name	Groups	Last activity	Creation time

No resources to display

Attach permissions policies - *Optional* (Selected 1/856) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

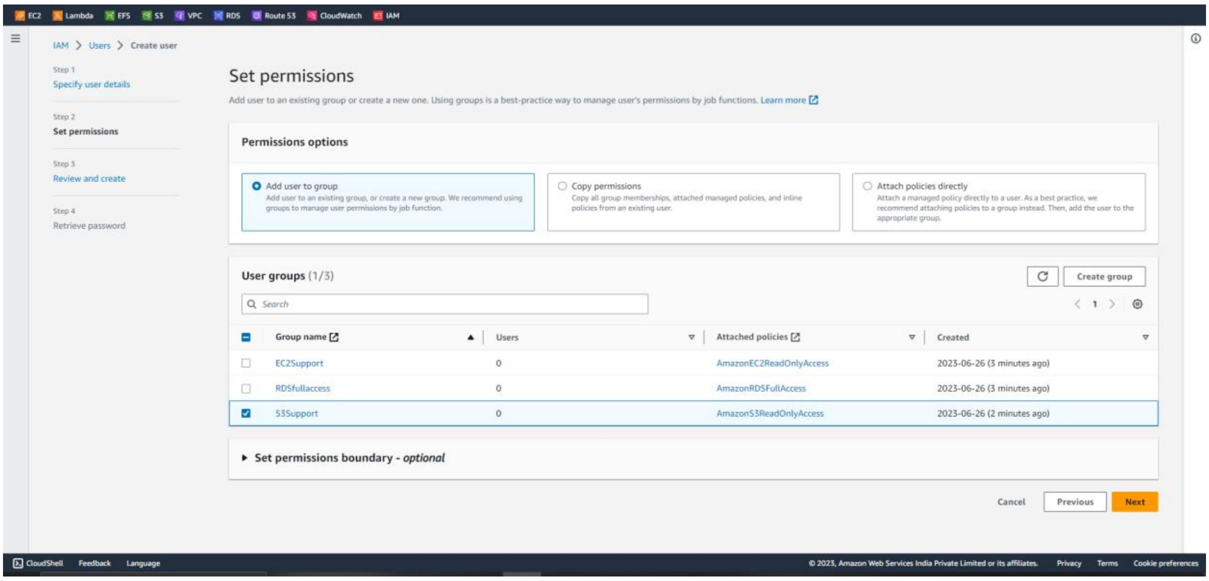
Filter policies by property or policy name and press enter. 9 matches

"s3"

	Policy name	Type	Description
□	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the AWS Management Console.
☑	AmazonS3ReadOnlyAccess	AWS managed	Provides read only access to all buckets via the AWS Management Console.
□	AmazonDMSRedshiftS3Role	AWS managed	Provides access to manage S3 settings for Redshift endpoints for DMS.

© 2023, Amazon Web Services India Private Limited or its affiliates.

7. Back on the "Set permissions" page, select the group you just created and click on the "Next: Tags" button. Add any desired tags for the user (optional) and click on the "Next: Review" button.



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 (1/3) Create group

Search

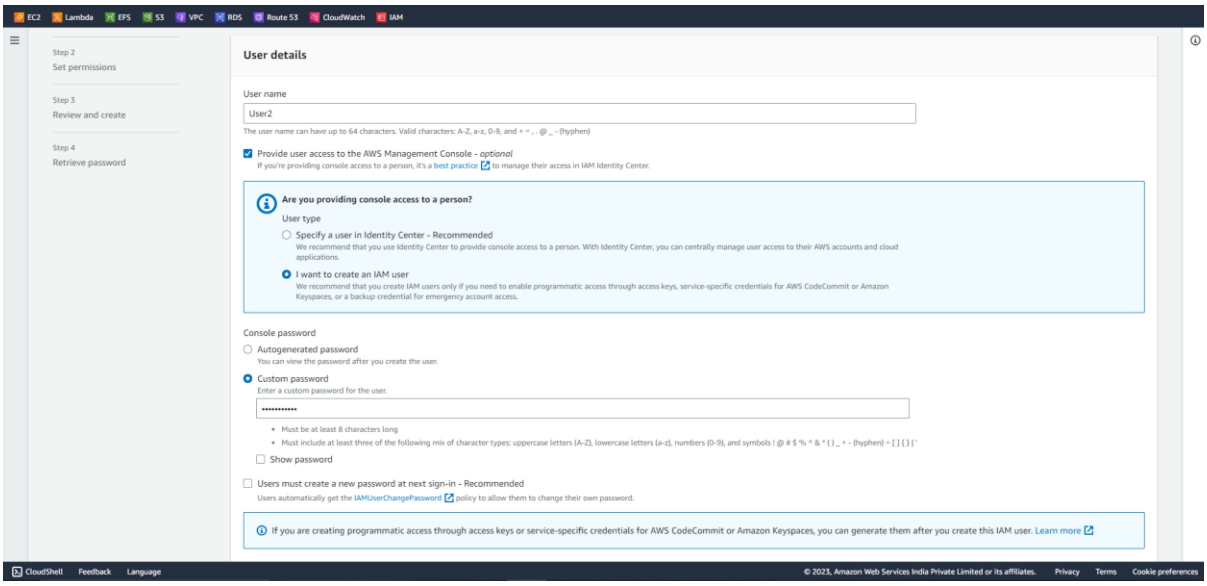
	Group name	Users	Attached policies	Created
□	EC2Support	0	AmazonEC2ReadOnlyAccess	2023-06-26 (3 minutes ago)
□	RDSfullaccess	0	AmazonRDSFullAccess	2023-06-26 (3 minutes ago)
☑	S3Support	0	AmazonS3ReadOnlyAccess	2023-06-26 (2 minutes ago)

▸ Set permissions boundary - *optional*

Cancel Previous Next

8. Review the user details and click on the "Create user" button. Review the user details and click on the "Create user" button.

Repeat the steps to create the remaining two users and groups.



User details

User name
User2
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) = [ ] { } | '

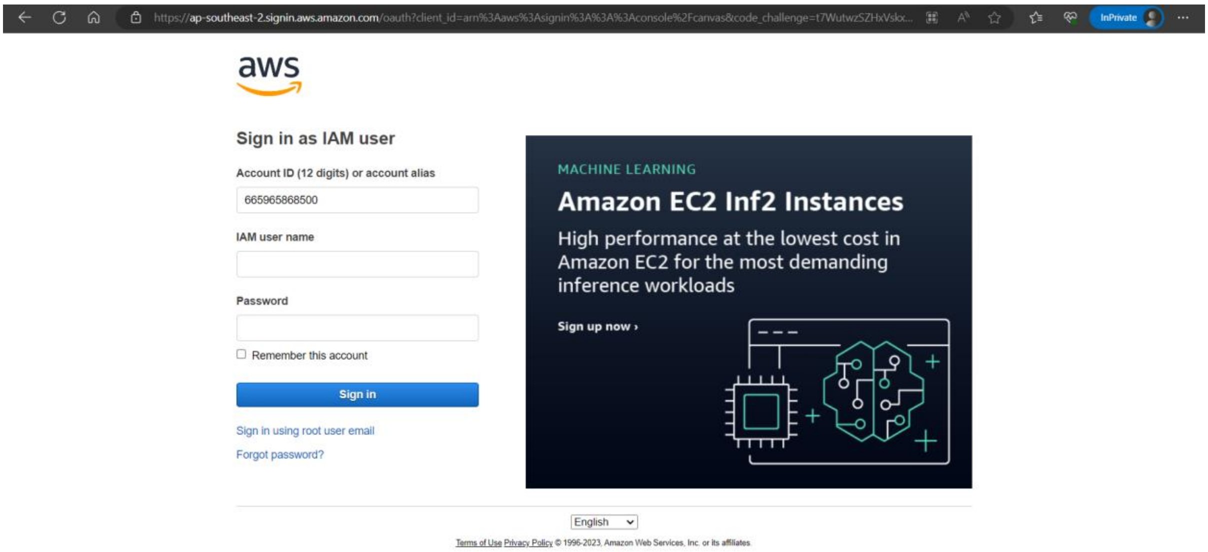
□ Show password

□ 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.

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

After the users and groups are set up, you can generate and download the credentials (access keys) for each user, which will be needed for programmatic access.

9. To login as one of the users in the AWS Management Console, click on the "Users" section in the IAM console, select the desired user, and click on the "Sign-in link" to access the AWS Management Console with that user's credentials.



https://ap-southeast-2.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=t7WutwzSZHxVskx...

Sign in as IAM user

Account ID (12 digits) or account alias: 665965868500

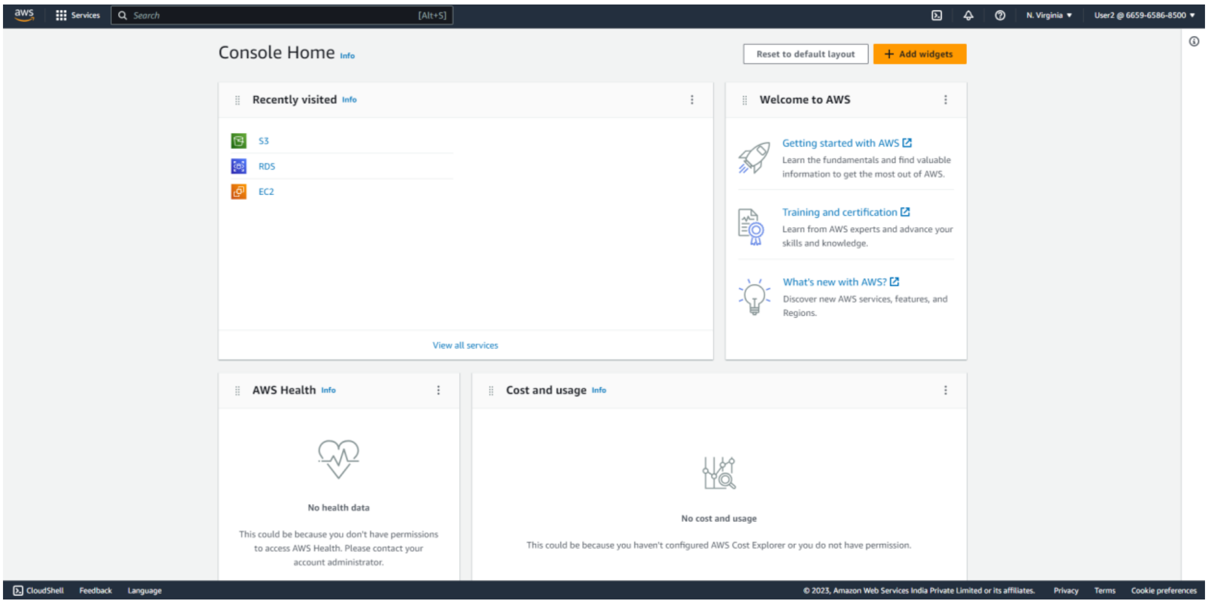
IAM user name:

Password:

□ Remember this account

InPrivate
aws
Sign in
Sign in using root user email
Forgot password?
MACHINE LEARNING
Amazon EC2 Inf2 Instances
High performance at the lowest cost in Amazon EC2 for the most demanding inference workloads
Sign up now ›
English
Terms of Use Privacy Policy © 1996-2023, Amazon Web Services, Inc. or its affiliates.

10. Now check the access for every user i.e.,
For User1- RDS full access
For User2- S3 Read only
For User3 – EC2 Read only



User2 @ 6659-6586-8500

Console Home

Recently visited: S3, RDS, EC2

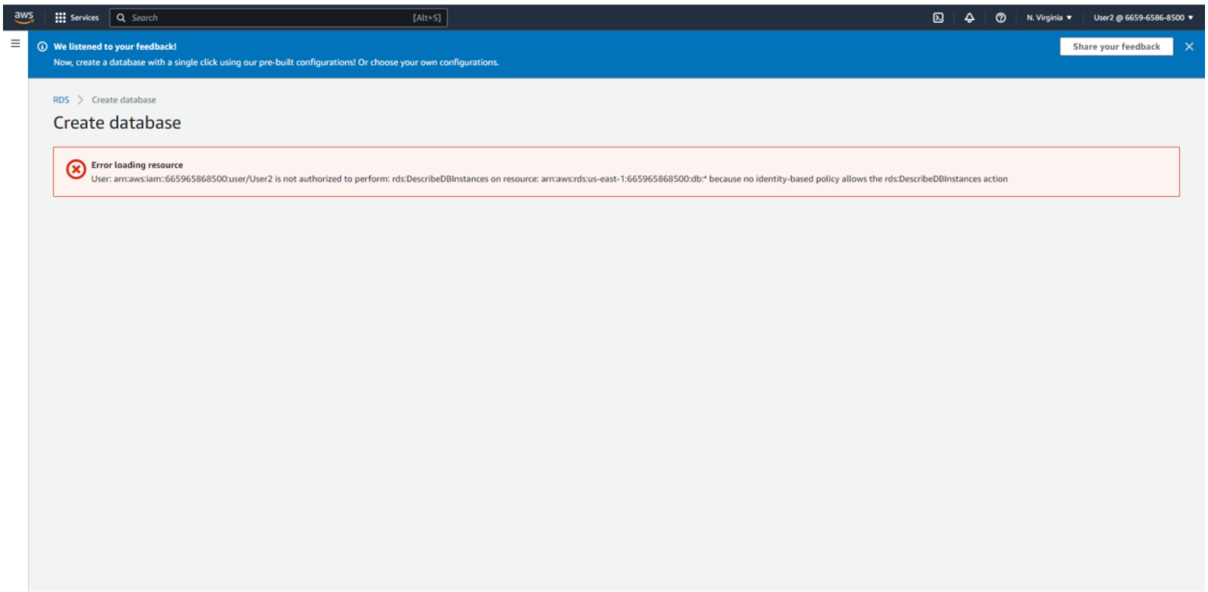
No health data

This could be because you don't have permissions to access AWS Health. Please contact your account administrator.

No cost and usage

This could be because you haven't configured AWS Cost Explorer or you do not have permission.

aws
Services
Search
[Alt+S]
N. Virginia ▾
Info
Reset to default layout
+ Add widgets
Recently visited
S3
RDS
EC2
View all services
Welcome to AWS
Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.
Training and certification
Learn from AWS experts and advance your skills and knowledge.
What's new with AWS?
Discover new AWS services, features, and Regions.
AWS Health
Cost and usage
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

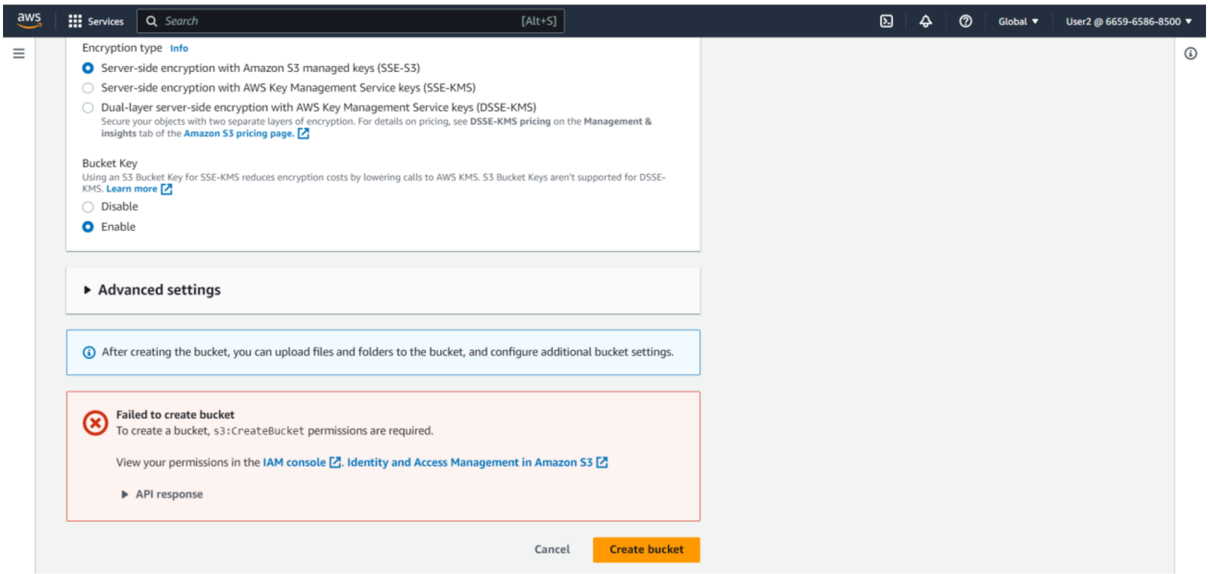


We listened to your feedback!
Now, create a database with a single click using our pre-built configurations! Or choose your own configurations.

RDS > Create database

Create database

Error loading resource
User: arn:aws:iam::665965868500:user/User2 is not authorized to perform: rds:DescribeDBInstances on resource: arn:aws:rds:us-east-1:665965868500:db:* because no identity-based policy allows the rds:DescribeDBInstances action



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 **Management & insights** 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

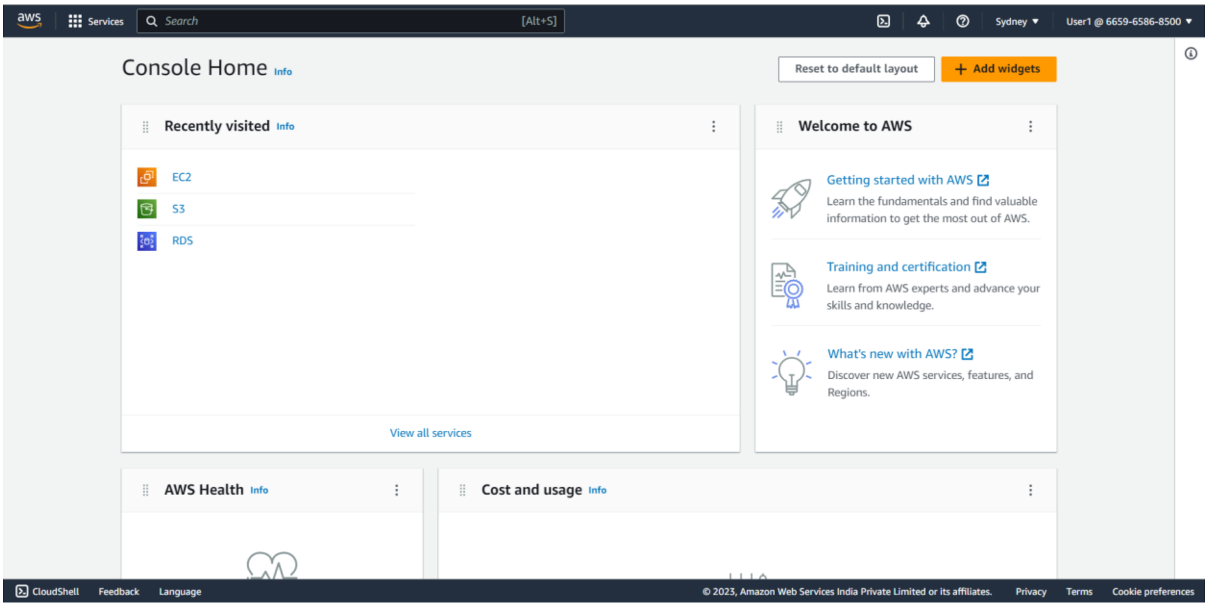
▸ Advanced settings

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

Failed to create bucket
To create a bucket, `s3:CreateBucket` permissions are required.

View your permissions in the IAM console. Identity and Access Management in Amazon S3

▸ API response



Console Home Info

Recently visited Info

- EC2
- S3
- RDS

View all services

Welcome to AWS

Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.

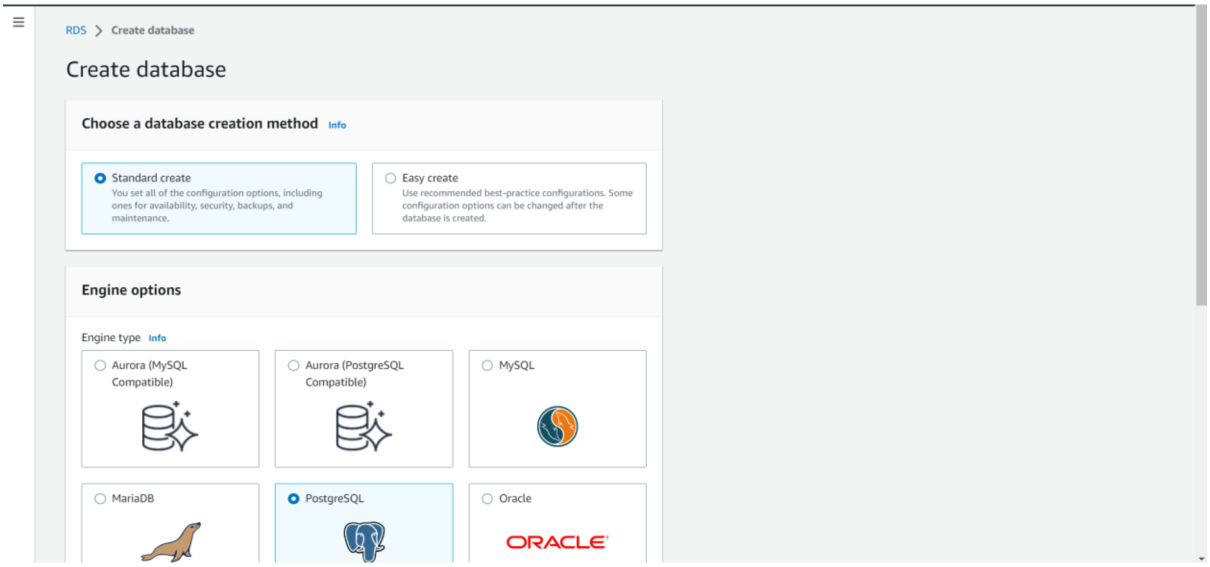
Training and certification
Learn from AWS experts and advance your skills and knowledge.

What's new with AWS?
Discover new AWS services, features, and Regions.

AWS Health Info

Cost and usage Info

CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences



RDS > Create database

Create database

Choose a database creation method Info

● Standard create
You set all of the configuration options, including ones for availability, security, backups, and maintenance.

○ Easy create
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine options

Engine type Info

○ Aurora (MySQL Compatible)

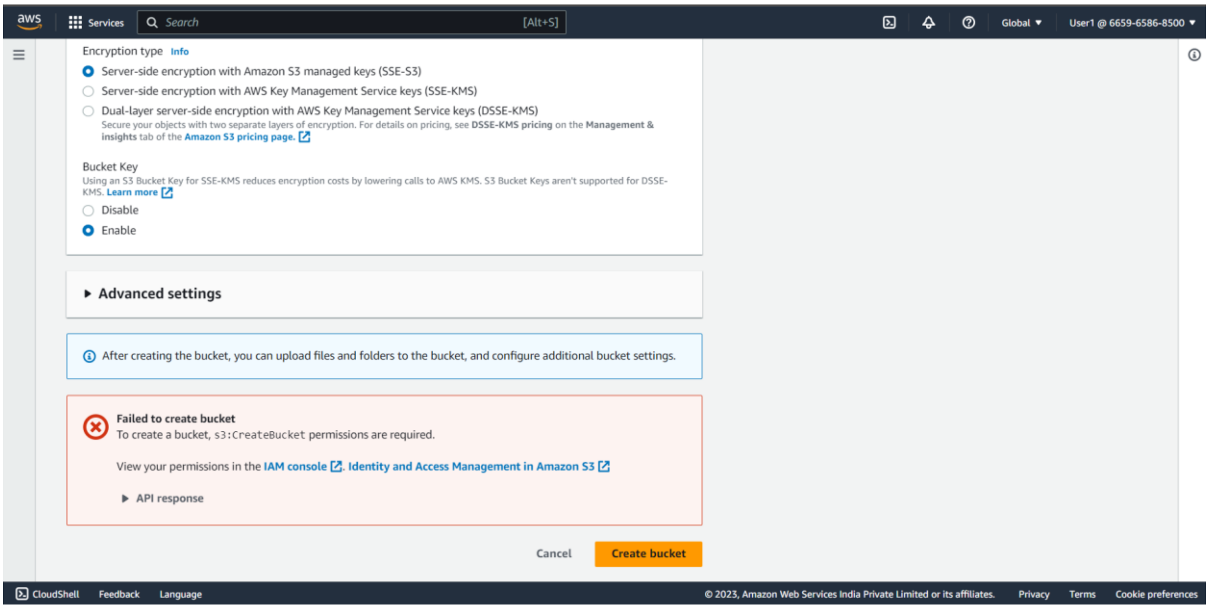
○ Aurora (PostgreSQL Compatible)

○ MySQL

○ MariaDB

● PostgreSQL

○ Oracle



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 **Management & insights** 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

▶ **Advanced settings**

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

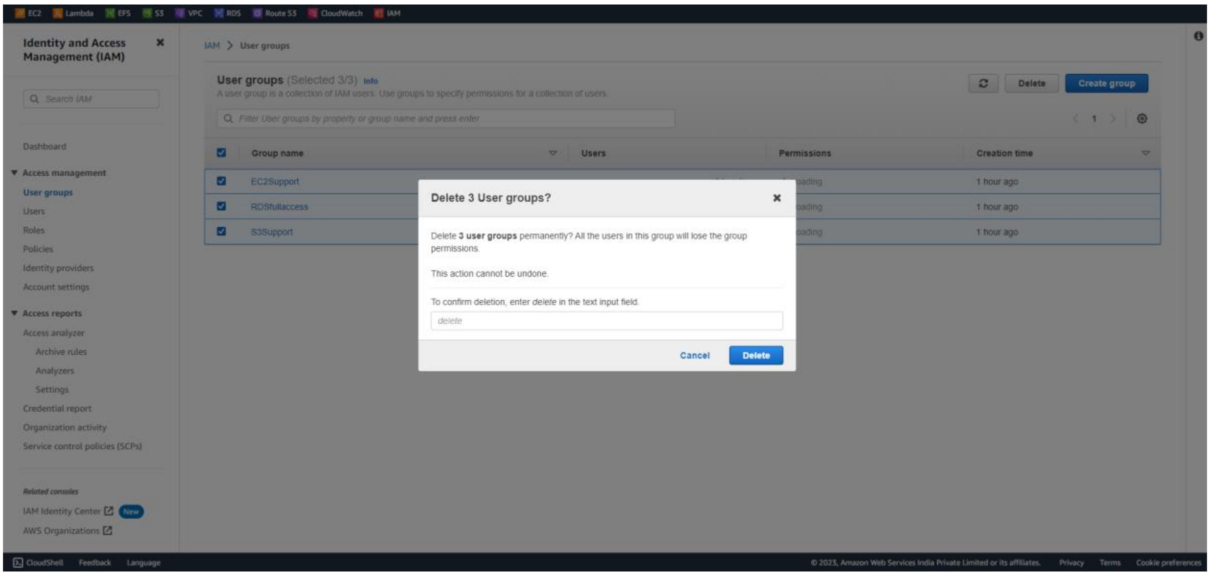
Failed to create bucket
To create a bucket, `s3:CreateBucket` permissions are required.

View your permissions in the **IAM console**. **Identity and Access Management in Amazon S3**

▶ API response

Cleaning Up

1. In the IAM console, navigate to the "Users" section. Select the user(s) you want to delete by checking the box next to their names. Click on the "Actions" button and select "Delete users".
   In the confirmation dialog, review the users you have selected to delete and click on the "Delete" button.



User groups (Selected 3/3) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

☑	Group name	Users	Permissions	Creation time
☑	EC2Support			1 hour ago
☑	RDSfullaccess			1 hour ago
☑	S3Support			1 hour ago

Delete 3 User groups?

Delete **3 user groups** permanently? All the users in this group will lose the group permissions.

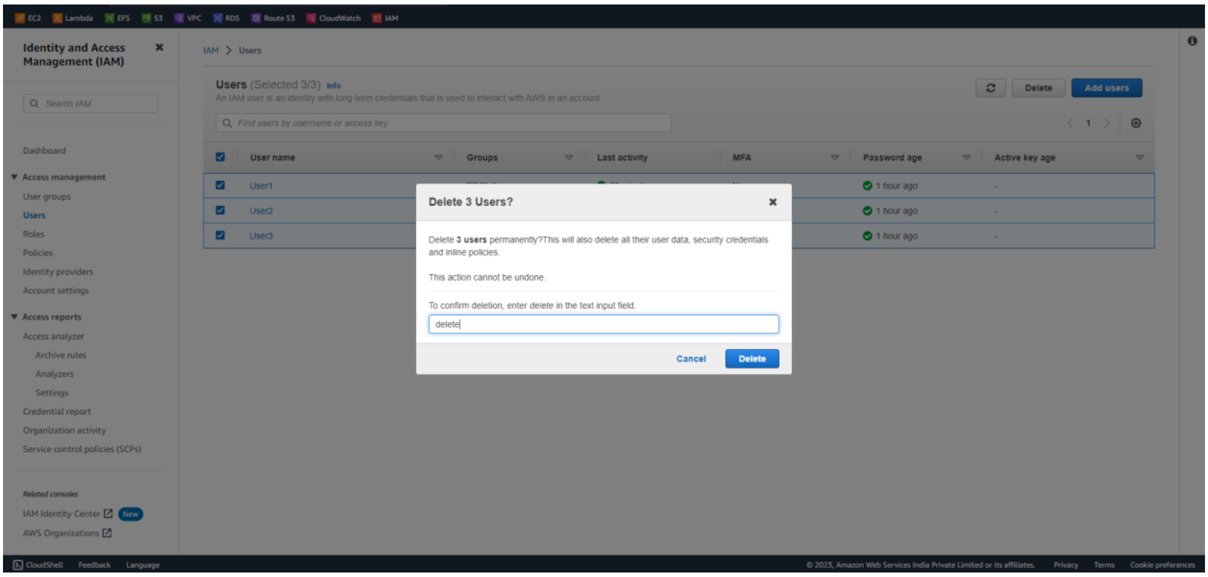
This action cannot be undone.

To confirm deletion, enter *delete* in the text input field.

delete

Cancel Delete

2. In the IAM console, navigate to the "Groups" section. Select the user group(s) you want to delete by checking the box next to their names. Click on the "Actions" button and select "Delete groups". In the confirmation dialog, review the groups you have selected to delete and click on the "Delete" button.



Users (Selected 3/3) Info

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

Find users by username or access key

☑	User name	Groups	Last activity	MFA	Password age	Active key age
☑	User1				✓ 1 hour ago	-
☑	User2				✓ 1 hour ago	-
☑	User3				✓ 1 hour ago	-

Delete 3 Users?

Delete **3 users** permanently?This will also delete all their user data, security credentials and inline policies.

This action cannot be undone.

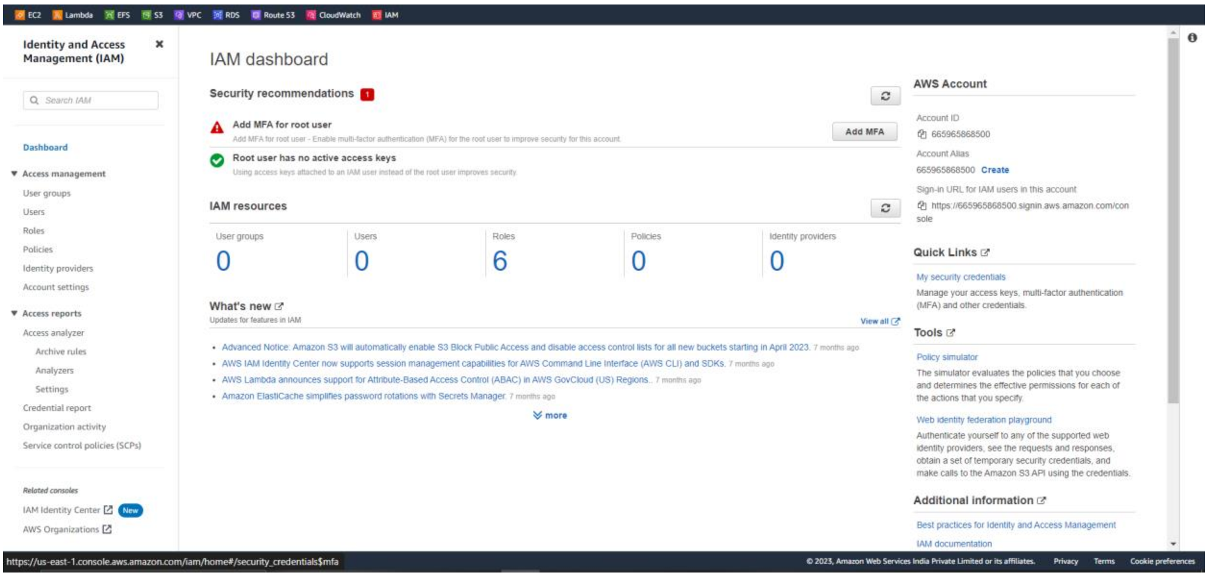
To confirm deletion, enter *delete* in the text input field.

delete

Cancel Delete

Setting MFA and access keys

1. Sign in to the AWS Management Console using your AWS account credentials. Open the IAM console by navigating to the IAM service.



IAM dashboard

Security recommendations 1

Add MFA for root user
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
0	0	6	0	0

What's new
Updates for features in IAM

- Advanced Notice: Amazon S3 will automatically enable S3 Block Public Access and disable access control lists for all new buckets starting in April 2023. 7 months ago
- AWS IAM Identity Center now supports session management capabilities for AWS Command Line Interface (AWS CLI) and SDKs. 7 months ago
- AWS Lambda announces support for Attribute-Based Access Control (ABAC) in AWS GovCloud (US) Regions.. 7 months ago
- Amazon ElastiCache simplifies password rotations with Secrets Manager. 7 months ago

AWS Account

Account ID
665965868500

Account Alias
665965868500

Sign-in URL for IAM users in this account
https://665965868500.signin.aws.amazon.com/console

Quick Links

My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

Web identity federation playground
Authenticate yourself to any of the supported web identity providers, see the requests and responses, obtain a set of temporary security credentials, and make calls to the Amazon S3 API using the credentials.

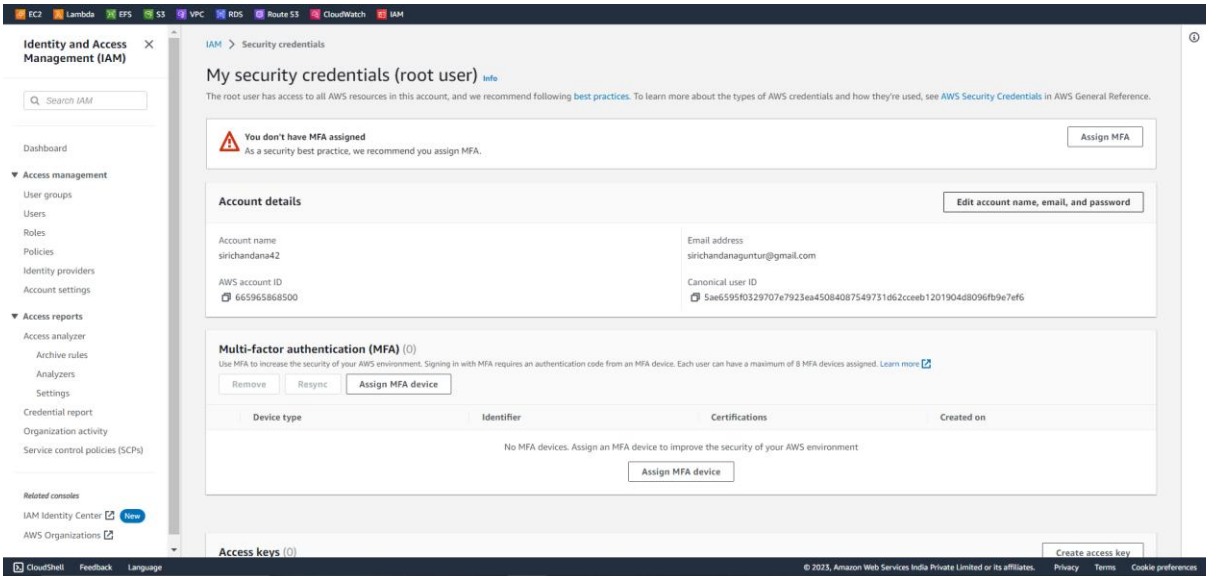
Additional information

Best practices for Identity and Access Management
IAM documentation

https://us-east-1.console.aws.amazon.com/iam/home#/security_credentials$mfa

© 2023, Amazon Web Services India Private Limited or its affiliates.

2. In the "Security credentials" tab, locate the "Multi-factor authentication (MFA)" section and click on the "Manage MFA" button.



My security credentials (root user)

The root user has access to all AWS resources in this account, and we recommend following best practices. To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

You don't have MFA assigned
As a security best practice, we recommend you assign MFA.

Account details

Account name
sirichandana42

Email address
sirichandanaguntur@gmail.com

AWS account ID
665965868500

Canonical user ID
5ae6595f0329707e7923ea45084087549731d62cceeb1201904d8096fb9e7ef6

Multi-factor authentication (MFA) (0)
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

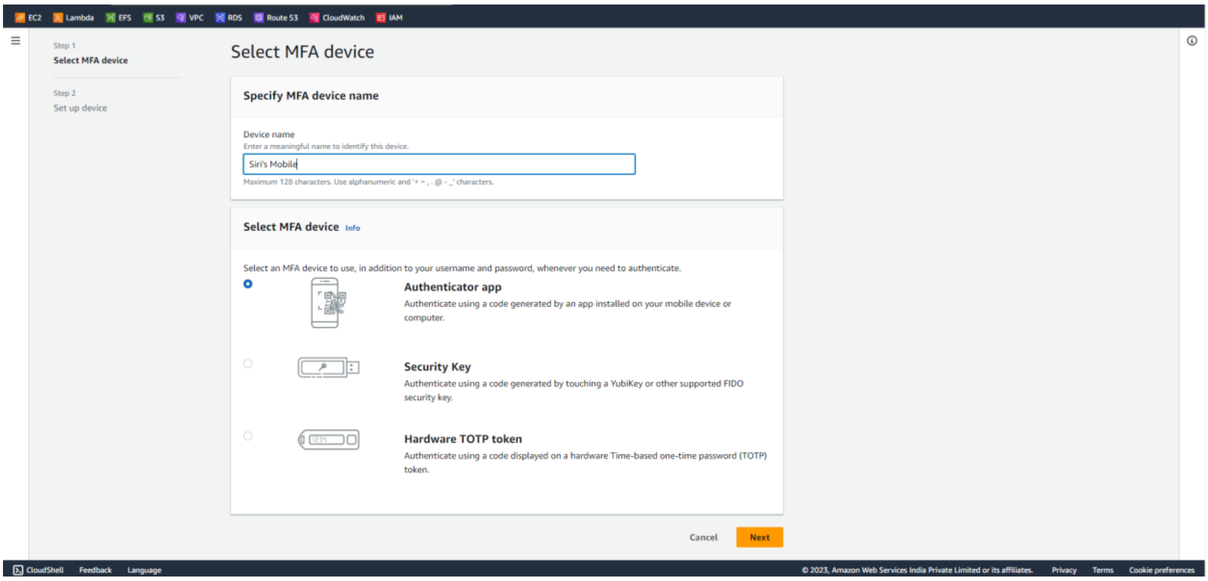
Device type	Identifier	Certifications	Created on

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

Access keys (0)

© 2023, Amazon Web Services India Private Limited or its affiliates.

3. Follow the on-screen instructions to associate an MFA device with the user. This typically involves selecting the type of MFA device (virtual or hardware)



Select MFA device

Specify MFA device name

Device name
Enter a meaningful name to identify this device.
Siri's Mobile
Maximum 128 characters. Use alphanumeric and '+ = , . @ - _' characters.

Select MFA device Info

Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.

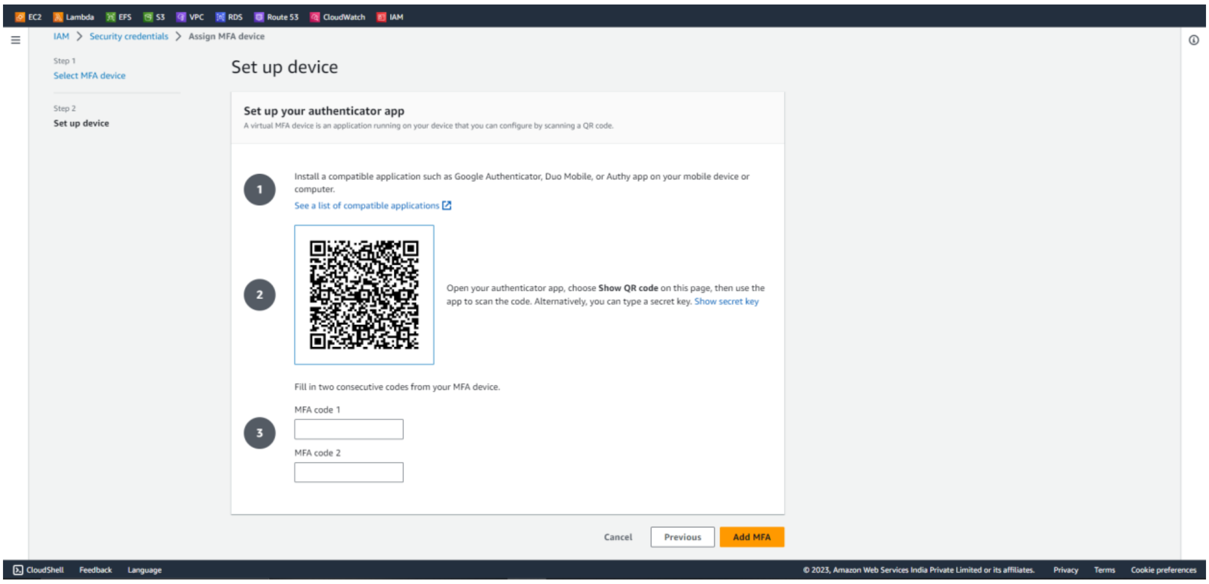
● **Authenticator app**
Authenticate using a code generated by an app installed on your mobile device or computer.

○ **Security Key**
Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.

○ **Hardware TOTP token**
Authenticate using a code displayed on a hardware Time-based one-time password (TOTP) token.

Cancel
Next
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

4. Then Scanning a QR code or entering a serial number, and setting up the MFA device.



Set up device

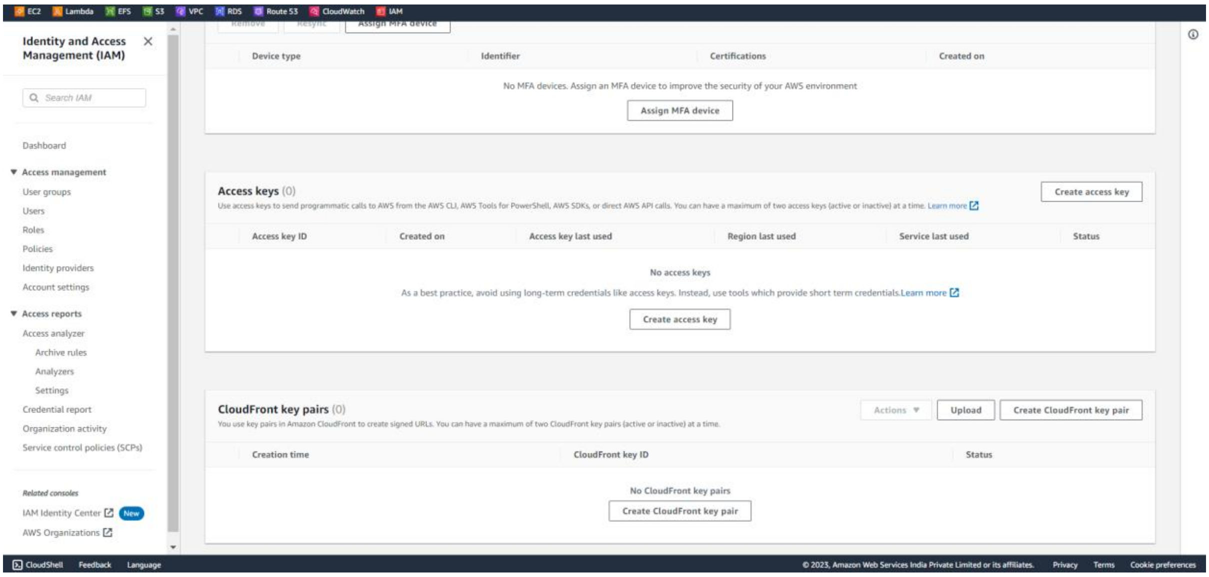
Set up your authenticator app
A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1. Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
See a list of compatible applications

2. Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. Show secret key

3. Fill in two consecutive codes from your MFA device.
MFA code 1
MFA code 2

5. In the "Security credentials" tab, locate the "Access keys" section and click on the "Create access key" button.



Device type	Identifier	Certifications	Created on

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

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

No access keys

As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials.Learn more

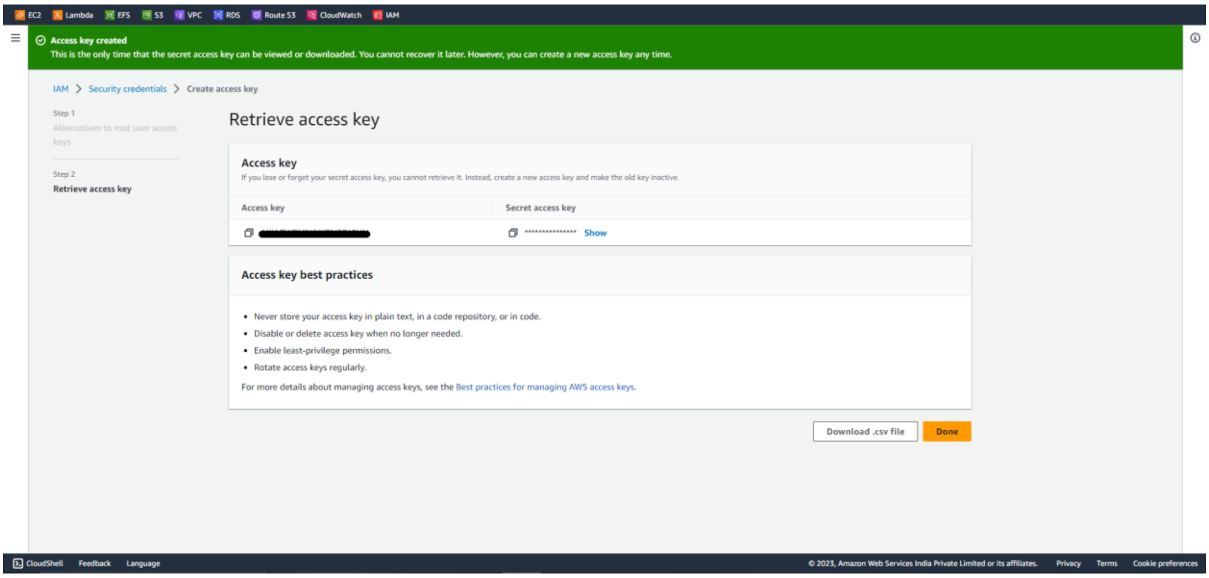
CloudFront key pairs (0)

You use key pairs in Amazon CloudFront to create signed URLs. You can have a maximum of two CloudFront key pairs (active or inactive) at a time.

Creation time	CloudFront key ID	Status

No CloudFront key pairs

6. The access key and secret access key will be generated. Make sure to download the CSV file containing the access key details, as the secret access key will not be displayed again. Use the access key and secret access key in your applications or scripts to authenticate and access AWS resources programmatically.



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.

Retrieve access key

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.

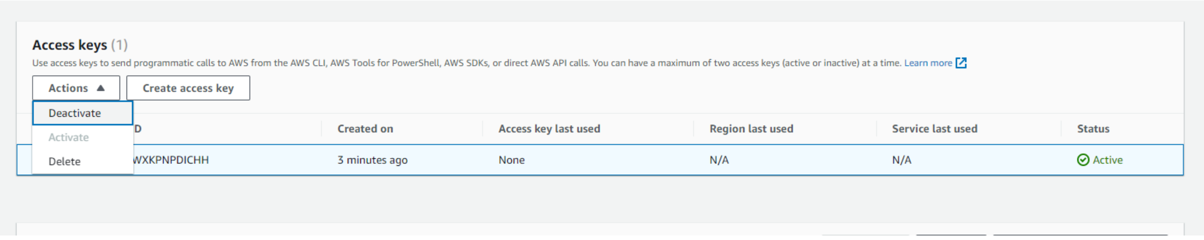
Access key	Secret access key
[redacted]	***************

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.

7. Find the access key(s) you want to delete. First deactivate the access key

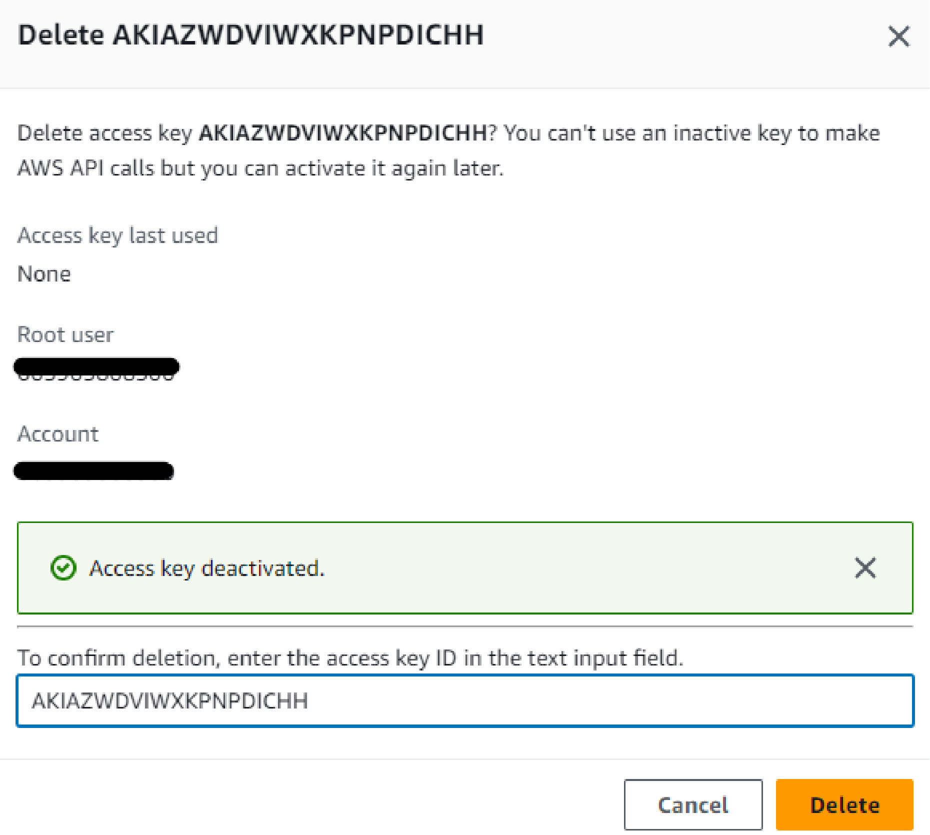


Access keys (1)

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

D	Created on	Access key last used	Region last used	Service last used	Status
WXKPNPDICHH	3 minutes ago	None	N/A	N/A	✓ Active

8. Click on the "Delete" button next to the access key you want to remove. A confirmation dialog will appear asking you to confirm the deletion.
Click on the "Yes, delete" button to proceed. The access key will be deleted and can no longer be used for accessing AWS resources.



Delete AKIAZWDVIWXKPNPDICHH

Delete access key **AKIAZWDVIWXKPNPDICHH**? You can't use an inactive key to make AWS API calls but you can activate it again later.

Access key last used

None

Root user

[redacted]

Account

[redacted]

✓ Access key deactivated.

To confirm deletion, enter the access key ID in the text input field.

AKIAZWDVIWXKPNPDICHH