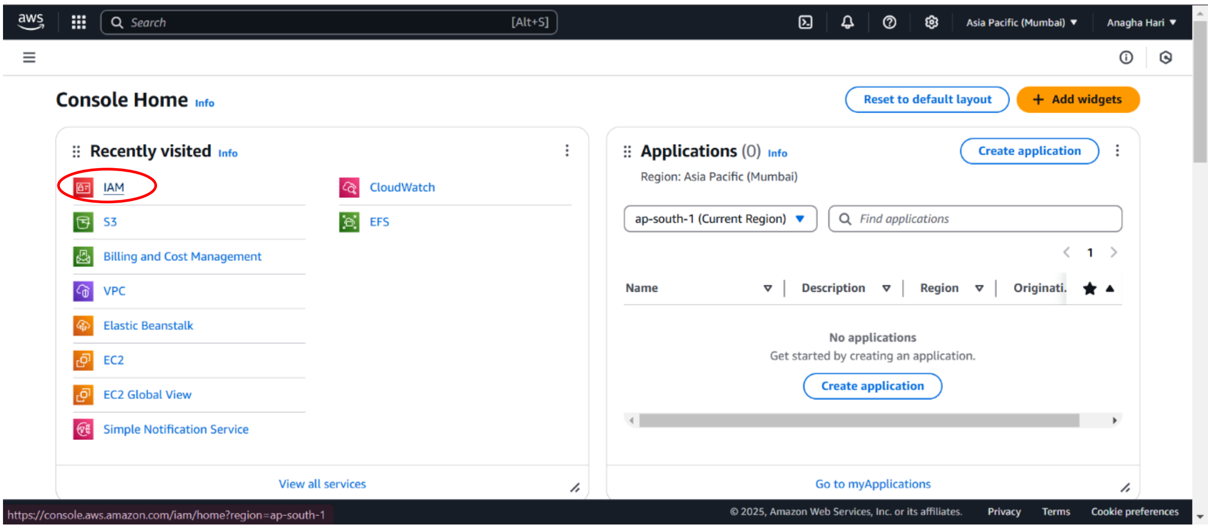
IAM- Identity Access and Management

Assignment 1

Creation of IAM account to have full access to S3 service

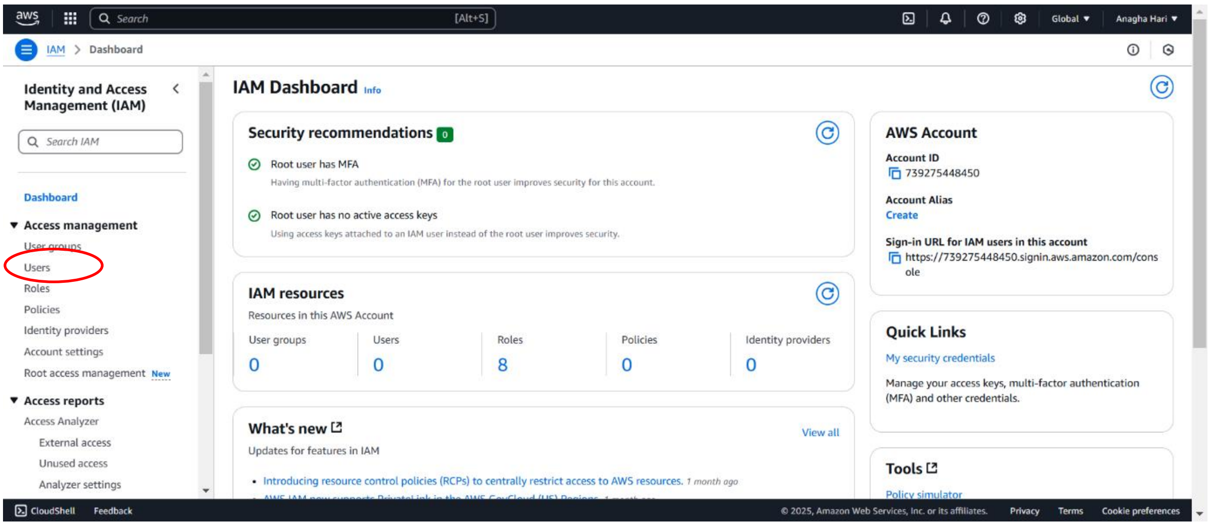
1. Login to AWS Console.
2. Go to IAM.
3. Select users.
4. Create a user providing permission to access S3 services fully.



No applications
Get started by creating an application.

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

© 2025, Amazon Web Services, Inc. or its affiliates.



Security recommendations 0

Root user has MFA
Having multi-factor authentication (MFA) for the root user improves 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
Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	8	0	0

What's new
Updates for features in IAM

- Introducing resource control policies (RCPs) to centrally restrict access to AWS resources. 1 month ago

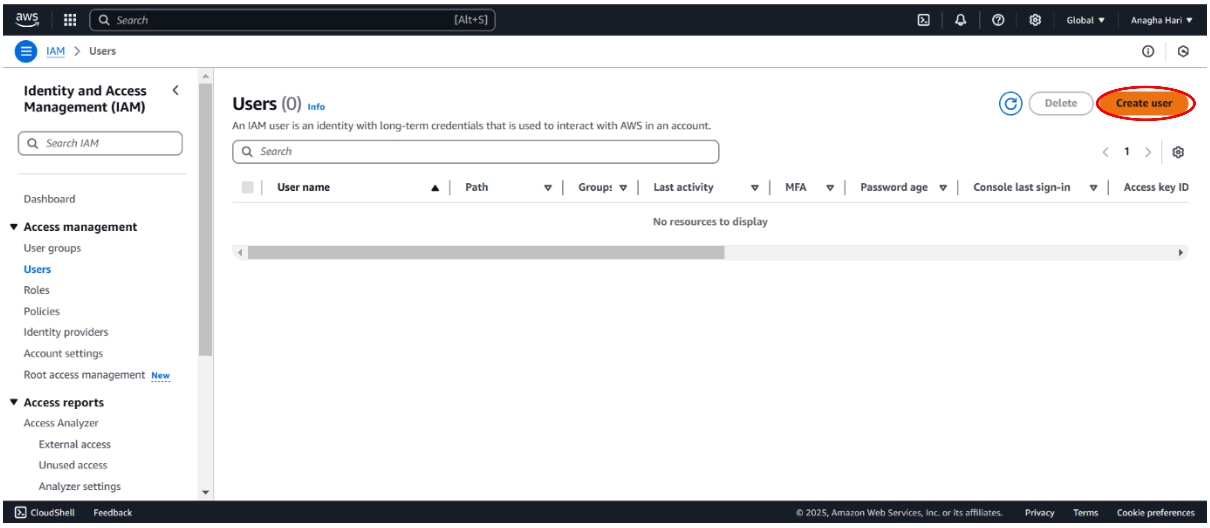
Account ID
739275448450

Account Alias
Create

Sign-in URL for IAM users in this account
https://739275448450.signin.aws.amazon.com/console

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

© 2025, Amazon Web Services, Inc. or its affiliates.



Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management New

▼ Access reports

Access Analyzer

External access

Unused access

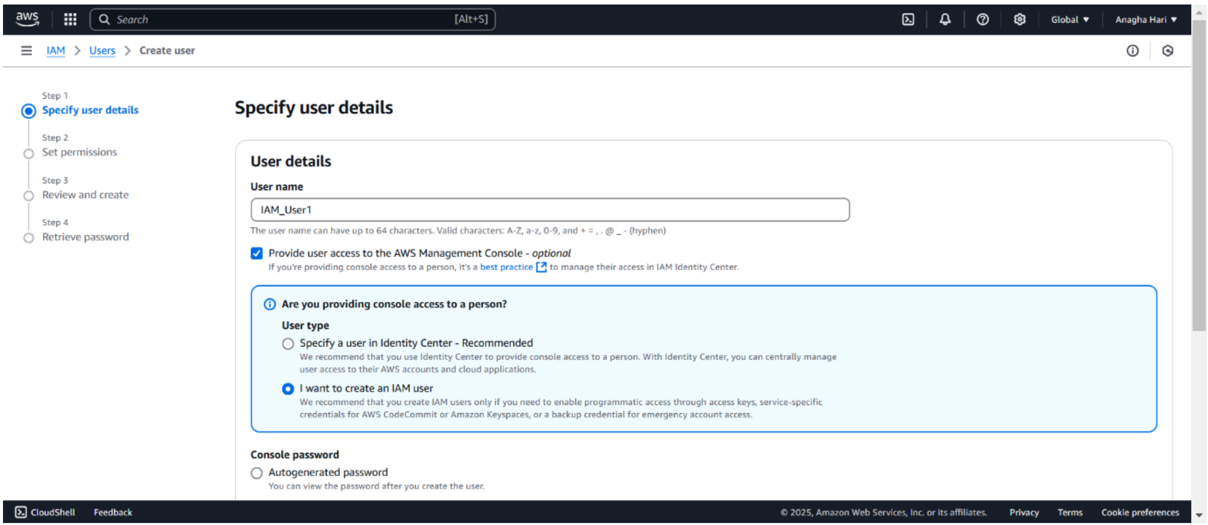
Analyzer settings

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

No resources to display



Step 1
● Specify user details

Step 2
○ Set permissions

Step 3
○ Review and create

Step 4
○ Retrieve password

Specify user details

User details

User name

IAM_User1

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.

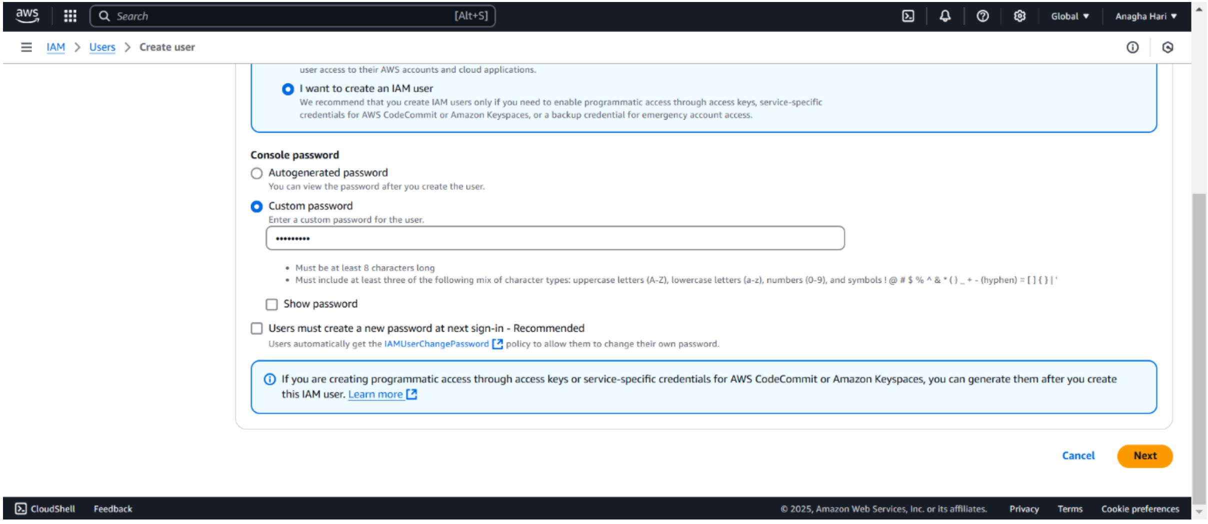
● I want to create an IAM user

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.



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.

•••••••••

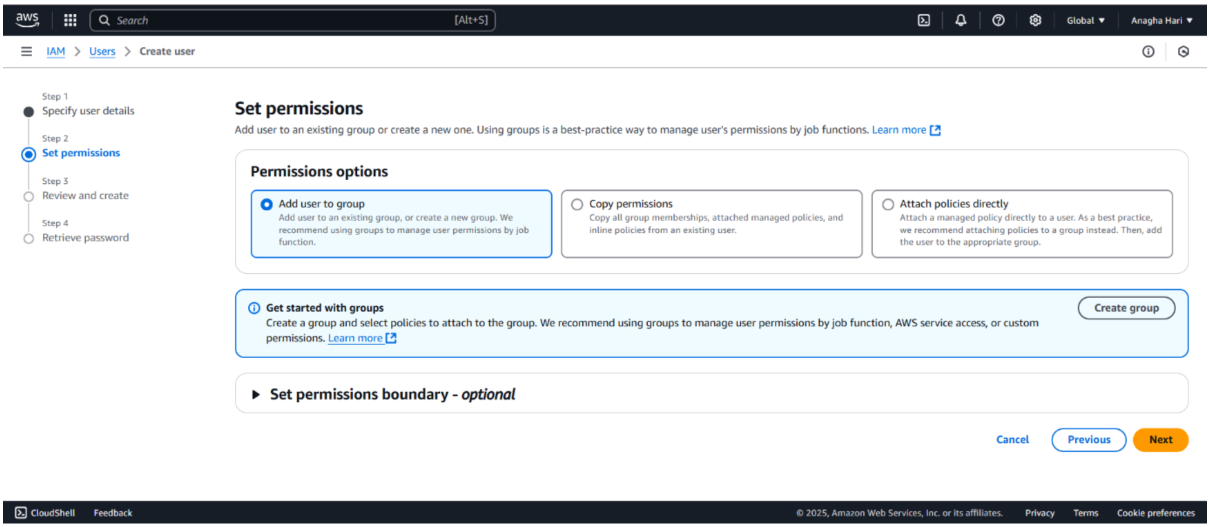
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ 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



Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

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

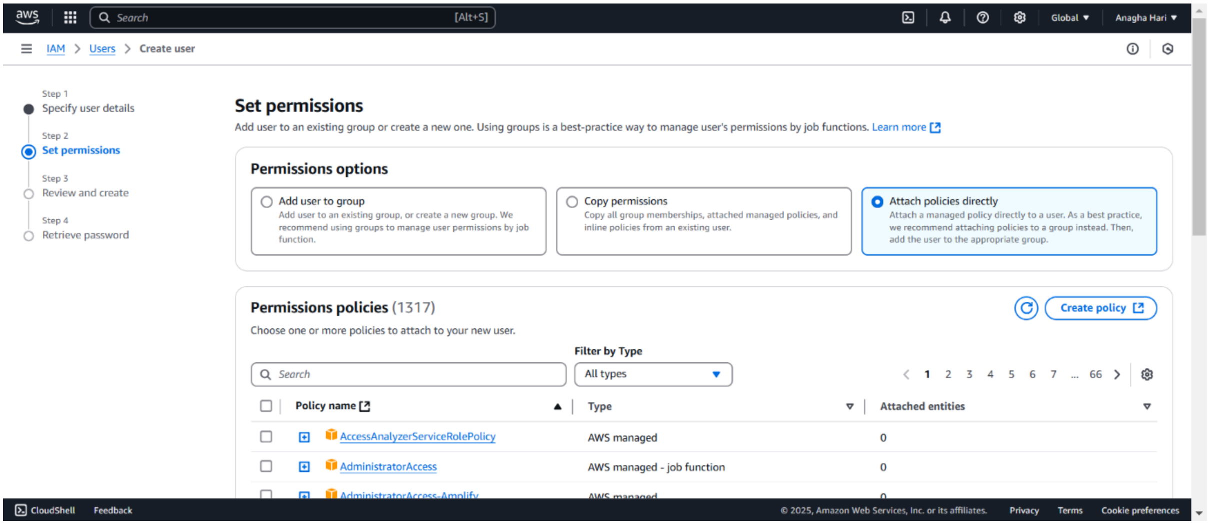
● Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ 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.

Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more

▶ Set permissions boundary - *optional*



Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

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.

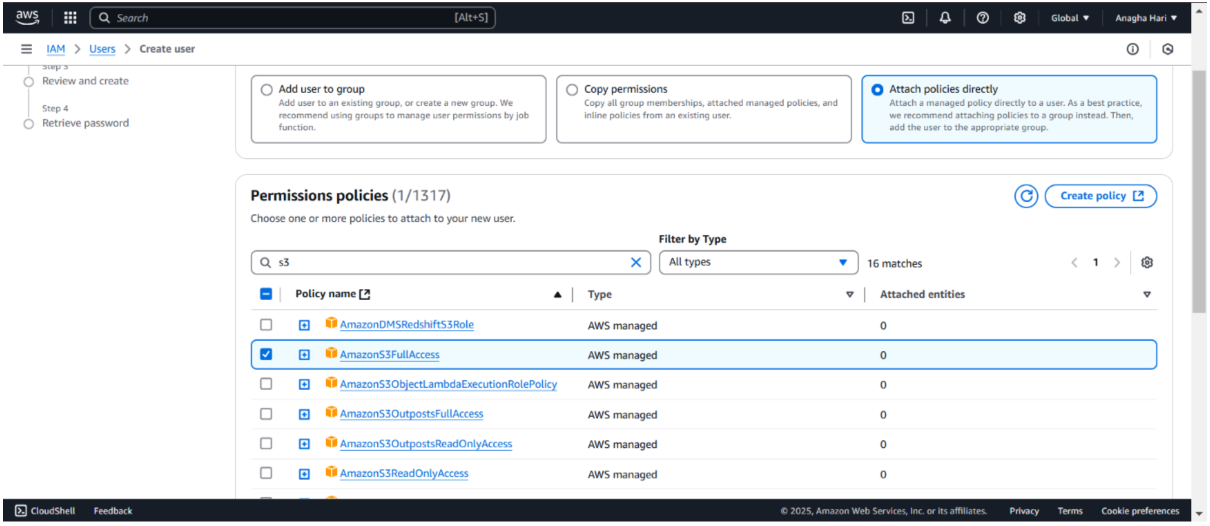
○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

● 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.

Permissions policies (1317)

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

□	Policy name	Type	Attached entities
□	AccessAnalyzerServiceRolePolicy	AWS managed	0
□	AdministratorAccess	AWS managed - job function	0
□	AdministratorAccess-Amplify	AWS managed	0



Step 3
Review and create

Step 4
Retrieve password

○ 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.

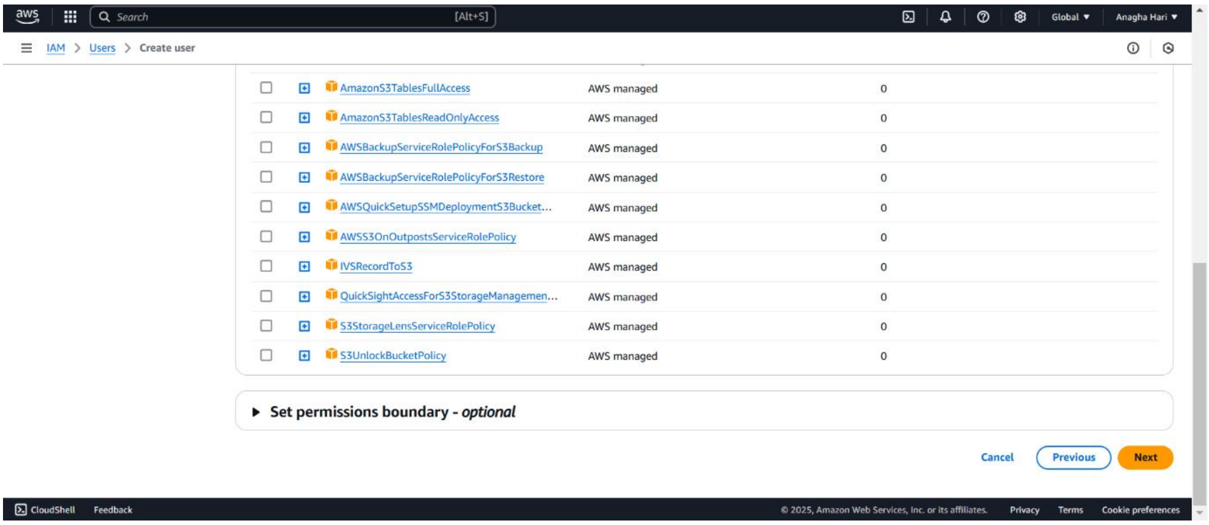
● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1317)

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

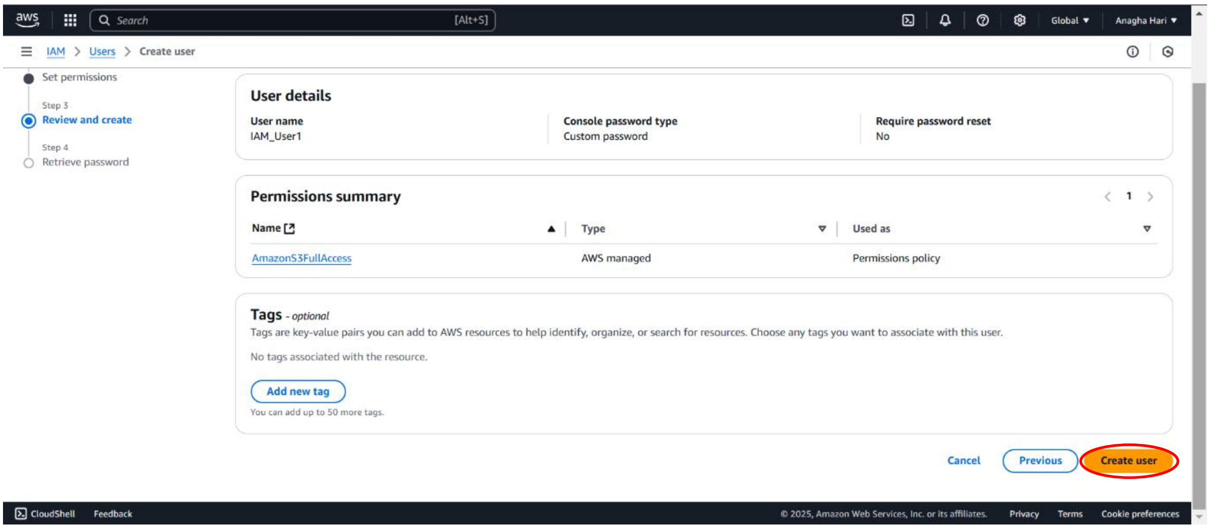
Search: s3
All types
16 matches

☐	Policy name	Type	Attached entities
□	AmazonDMSRedshiftS3Role	AWS managed	0
☑	AmazonS3FullAccess	AWS managed	0
□	AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	0
□	AmazonS3OutpostsFullAccess	AWS managed	0
□	AmazonS3OutpostsReadOnlyAccess	AWS managed	0
□	AmazonS3ReadOnlyAccess	AWS managed	0


aws
Search [Alt+S]
Global ▼
Anagha Hari ▼
IAM > Users > Create user
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

□	AmazonS3TablesFullAccess	AWS managed	0
□	AmazonS3TablesReadOnlyAccess	AWS managed	0
□	AWSBackupServiceRolePolicyForS3Backup	AWS managed	0
□	AWSBackupServiceRolePolicyForS3Restore	AWS managed	0
□	AWSQuickSetupSSMDeploymentS3Bucket...	AWS managed	0
□	AWSS3OnOutpostsServiceRolePolicy	AWS managed	0
□	IVSRecordToS3	AWS managed	0
□	QuickSightAccessForS3StorageManagemen...	AWS managed	0
□	S3StorageLensServiceRolePolicy	AWS managed	0
□	S3UnlockBucketPolicy	AWS managed	0

▶ Set permissions boundary - *optional*


aws
Search [Alt+S]
Global ▼
Anagha Hari ▼
IAM > Users > Create user
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

● Set permissions

Step 3
◉ Review and create

Step 4
○ Retrieve password

User details

User name	Console password type	Require password reset
IAM_User1	Custom password	No

Permissions summary

Name	Type	Used as
AmazonS3FullAccess	AWS managed	Permissions policy

Tags - *optional*

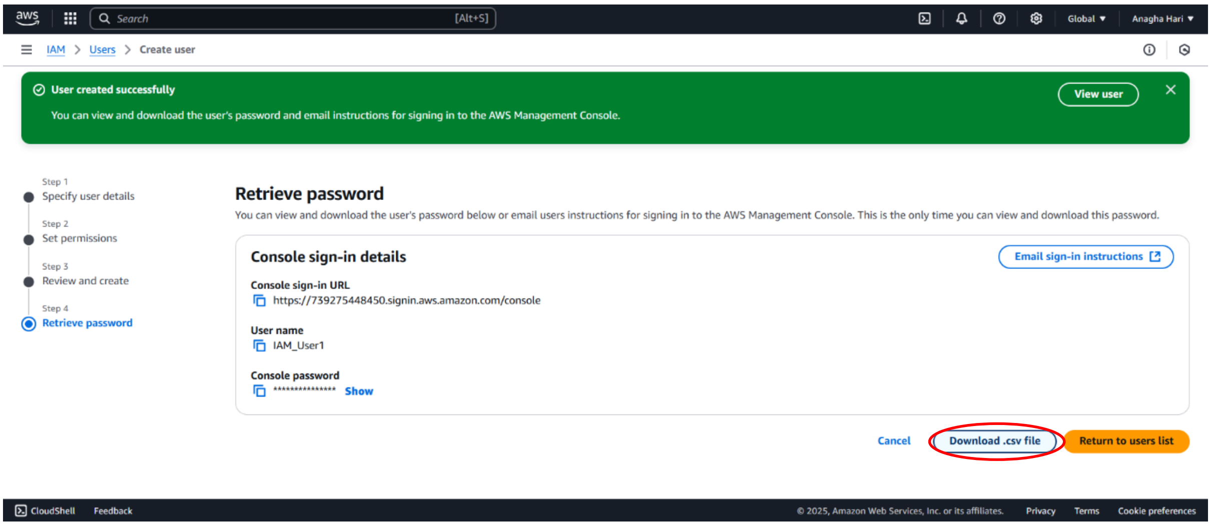
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel
Previous
Create user


aws
Search [Alt+S]
Global ▼
Anagha Hari ▼
IAM > Users > Create user
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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

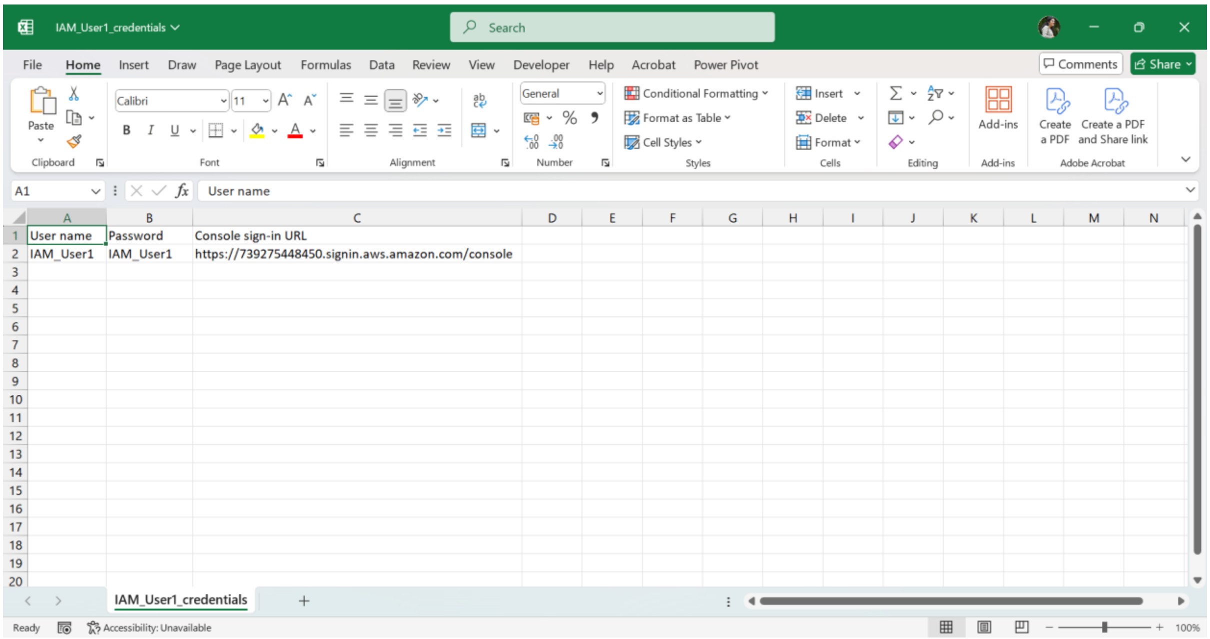
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Console sign-in URL
https://739275448450.signin.aws.amazon.com/console

User name
IAM_User1

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

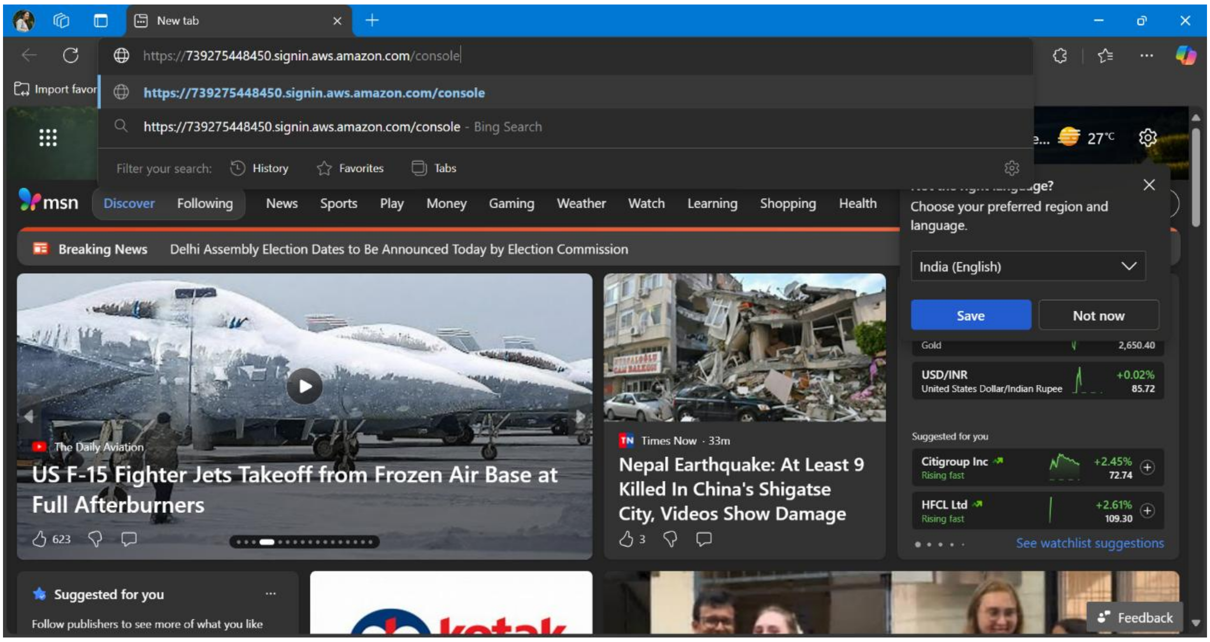


	A	B	C
1	User name	Password	Console sign-in URL
2	IAM_User1	IAM_User1	https://739275448450.signin.aws.amazon.com/console

The username, password and the console sign in details can be downloaded as a csv file.

To check the S3 accessibility.

1. Login to the console as IAM user in another web browser.
2. Search for the accessibility in S3 services.

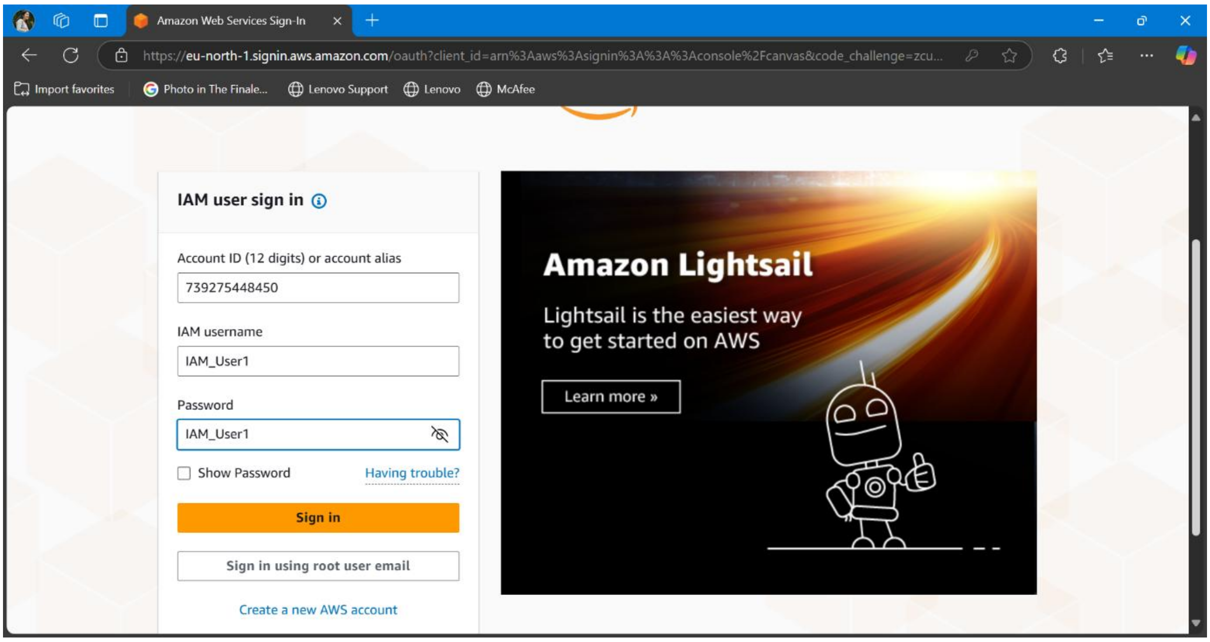


https://739275448450.signin.aws.amazon.com/console

https://739275448450.signin.aws.amazon.com/console

https://739275448450.signin.aws.amazon.com/console - Bing Search

New tab
Import favor
Filter your search:
History
Favorites
Tabs
msn
Discover
Following
News
Sports
Play
Money
Gaming
Weather
Watch
Learning
Shopping
Health
27°C
Breaking News
Delhi Assembly Election Dates to Be Announced Today by Election Commission
The Daily Aviation
US F-15 Fighter Jets Takeoff from Frozen Air Base at Full Afterburners
623
Times Now · 33m
Nepal Earthquake: At Least 9 Killed In China's Shigatse City, Videos Show Damage
3
Choose your preferred region and language.
India (English)
Save
Not now
Gold 2,650.40
USD/INR United States Dollar/Indian Rupee +0.02% 85.72
Suggested for you
Citigroup Inc Rising fast +2.45% 72.74
HFCL Ltd Rising fast +2.61% 109.30
See watchlist suggestions
Suggested for you
Follow publishers to see more of what you like
kotak
Feedback



Amazon Web Services Sign-In
https://eu-north-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=zcu...
Import favorites
Photo in The Finale...
Lenovo Support
Lenovo
McAfee

IAM user sign in

Account ID (12 digits) or account alias

739275448450

IAM username

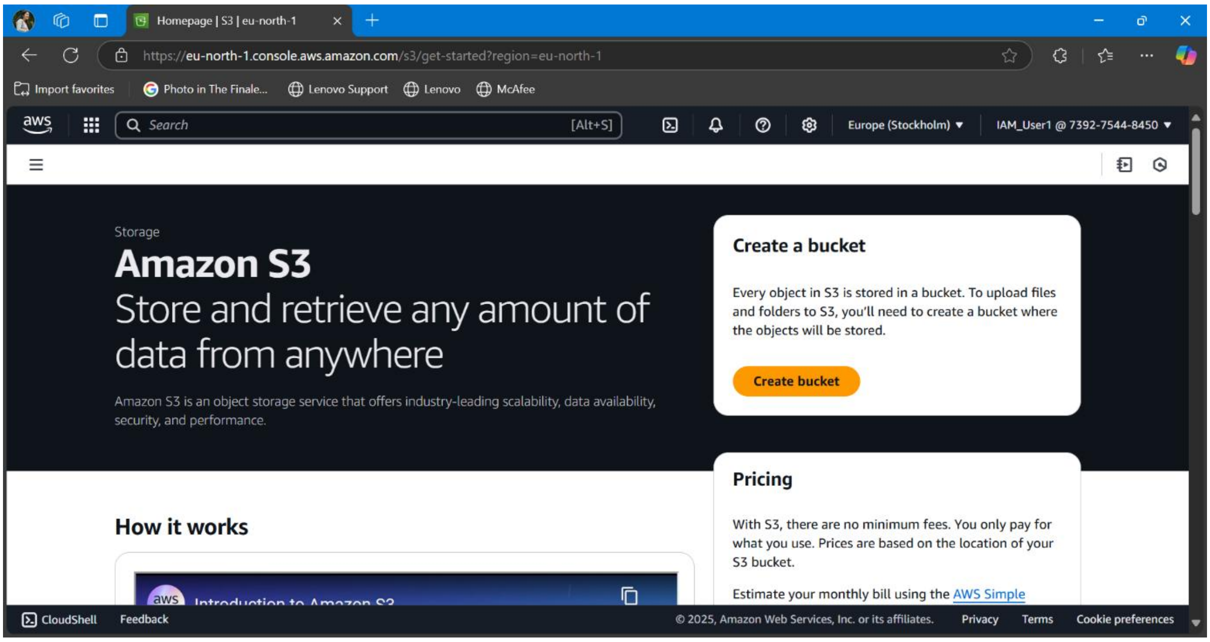
IAM_User1

Password

IAM_User1

□ Show Password

Having trouble?
Sign in
Sign in using root user email
Create a new AWS account
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »



Homepage | S3 | eu-north-1
https://eu-north-1.console.aws.amazon.com/s3/get-started?region=eu-north-1
Import favorites
Photo in The Finale...
Lenovo Support
Lenovo
McAfee
aws
Search
[Alt+S]
Europe (Stockholm) ▼
IAM_User1 @ 7392-7544-8450 ▼

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.

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.

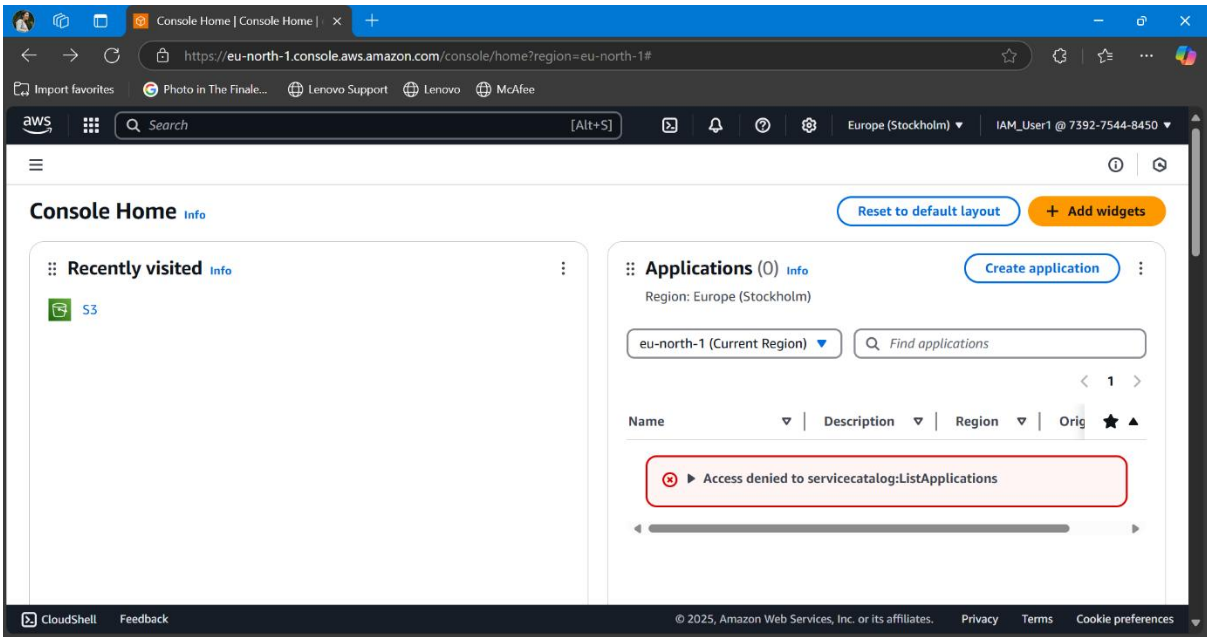
Pricing

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

How it works

Introduction to Amazon S3
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Console Home Info

Recently visited Info

S3

Applications (0) Info

Region: Europe (Stockholm)

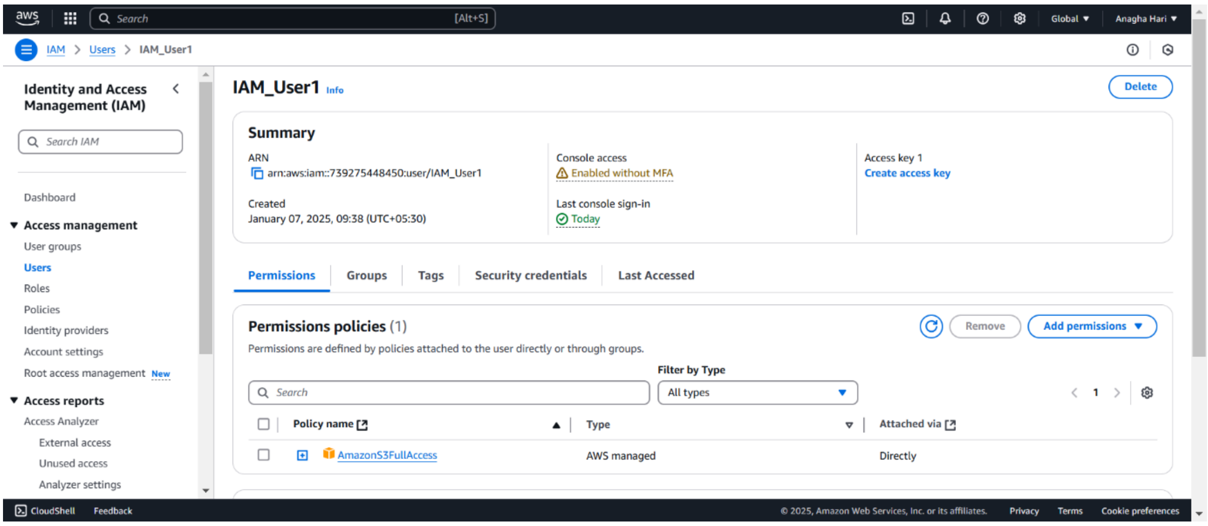
eu-north-1 (Current Region) ▾

Find applications

Name	Description	Region	Orig

Access denied to servicecatalog:ListApplications

S3 services are accessible while other services like EC2 are not accessible.



IAM_User1 Info

Summary

ARN
arn:aws:iam::739275448450:user/IAM_User1

Created
January 07, 2025, 09:38 (UTC+05:30)

Console access
Enabled without MFA

Last console sign-in
Today

Access key 1
Create access key

Permissions policies (1)

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

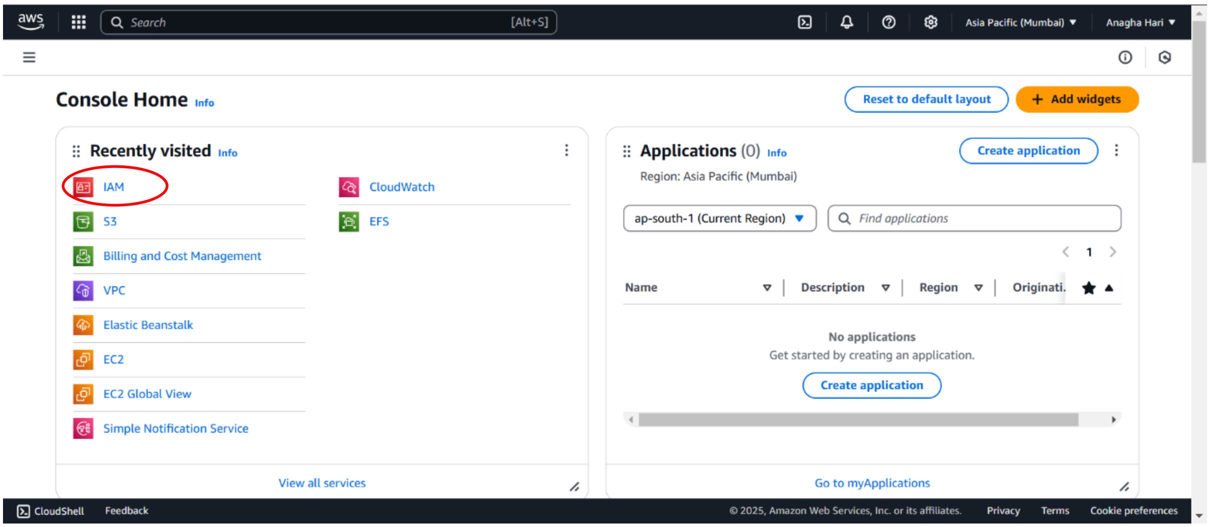
Filter by Type: All types

□	Policy name	Type	Attached via
□	AmazonS3FullAccess	AWS managed	Directly

An IAM user with full access to S3 services is created.

Setting up custom sign in URL || MFA

1. Login to AWS console.
2. Goto IAM and click on the dashboard.
3. Goto Security credentials.
4. Assign MFA to the device.

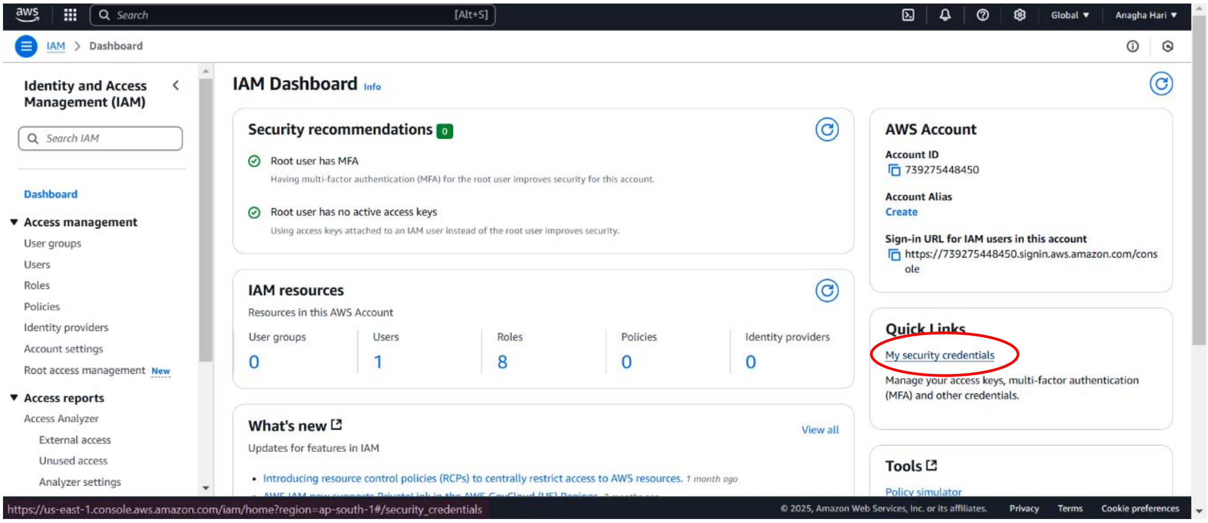


No applications

Get started by creating an application.

Create application

© 2025, Amazon Web Services, Inc. or its affiliates.



Security recommendations 0

✓ Root user has MFA

Having multi-factor authentication (MFA) for the root user improves 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

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	1	8	0	0

What's new

Updates for features in IAM

View all

- Introducing resource control policies (RCPs) to centrally restrict access to AWS resources. 1 month ago

AWS Account

Account ID
739275448450

Account Alias
Create

Sign-in URL for IAM users in this account
https://739275448450.signin.aws.amazon.com/console

Quick Links

My security credentials

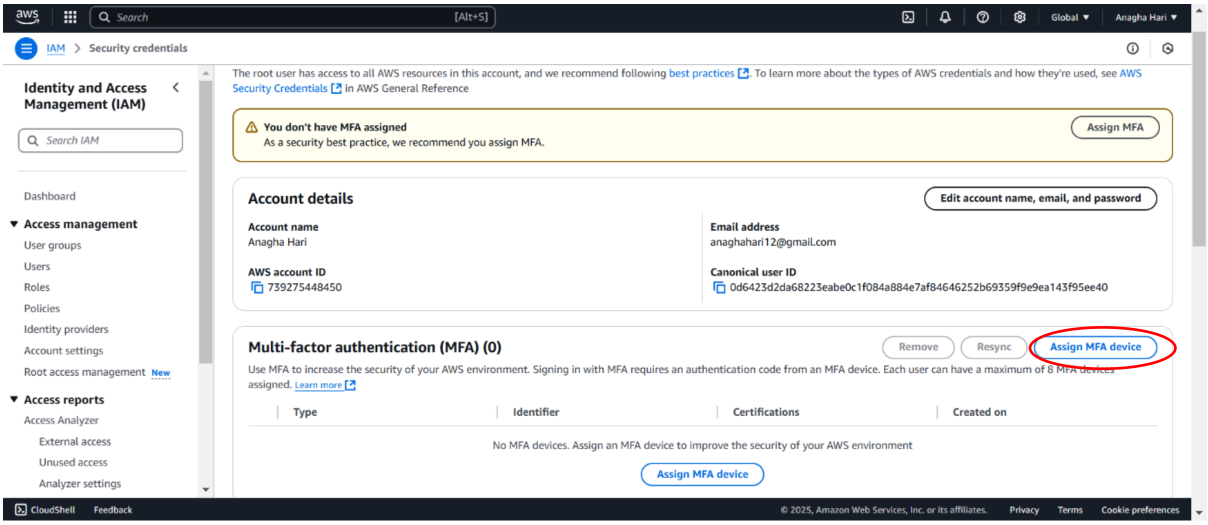
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

Policy simulator

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

© 2025, Amazon Web Services, Inc. or its affiliates.



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.

Assign MFA

Account details

Edit account name, email, and password

Account name
Anagha Hari

Email address
anaghahari12@gmail.com

AWS account ID
739275448450

Canonical user ID
0d6423d2da68223eabe0c1f084a884e7af84646252b69359f9e9ea143f95ee40

Multi-factor authentication (MFA) (0)

Remove | Resync | Assign MFA device

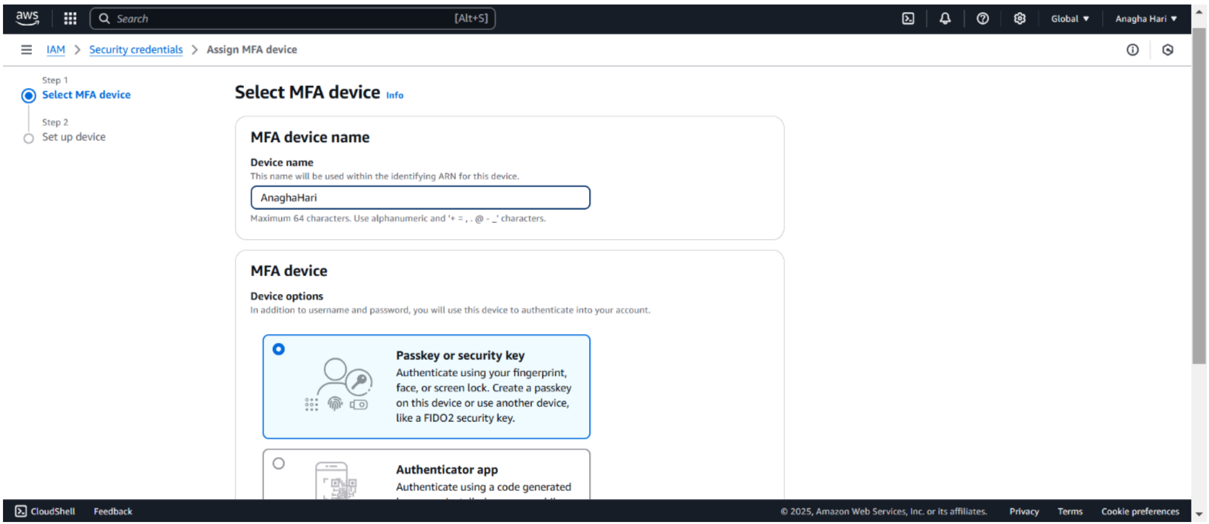
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

Type	Identifier	Certifications	Created on

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

Assign MFA device

© 2025, Amazon Web Services, Inc. or its affiliates.



Select MFA device Info

MFA device name

Device name
This name will be used within the identifying ARN for this device.

AnaghaHari

Maximum 64 characters. Use alphanumeric and '+ = , . @ - _' characters.

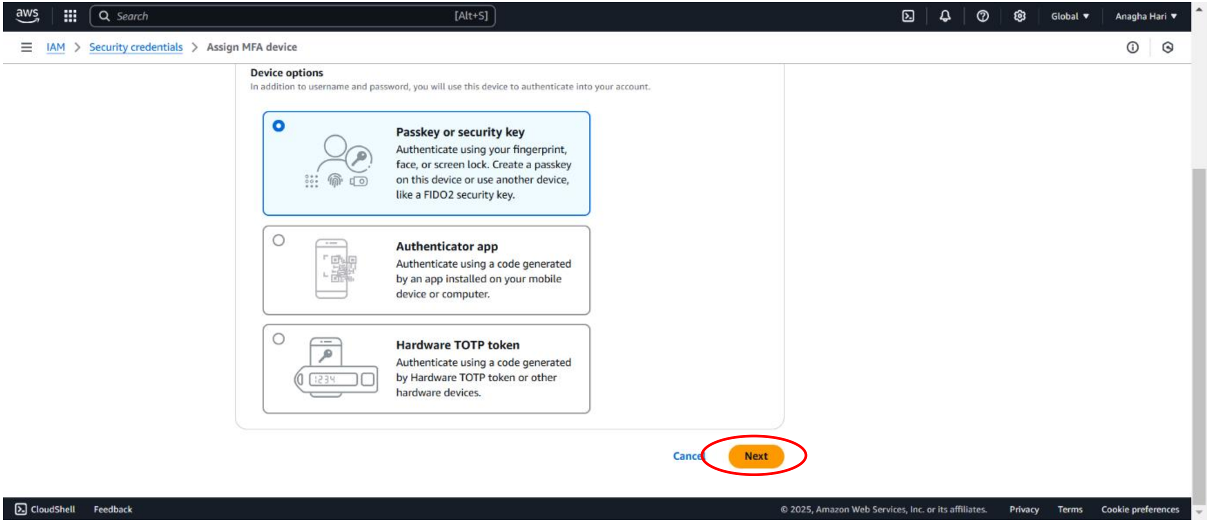
MFA device

Device options
In addition to username and password, you will use this device to authenticate into your account.

● **Passkey or security key**
Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.

○ **Authenticator app**
Authenticate using a code generated

CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

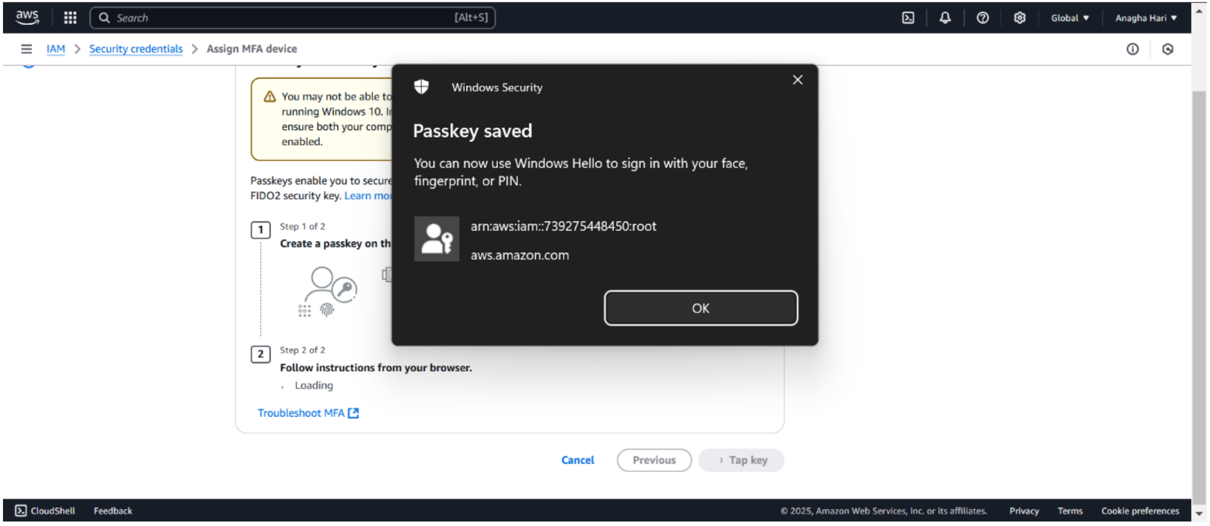

aws
Search [Alt+S]
Global ▾
Anagha Hari ▾
IAM > Security credentials > Assign MFA device

Device options
In addition to username and password, you will use this device to authenticate into your account.

● **Passkey or security key**
Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.

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

○ **Hardware TOTP token**
Authenticate using a code generated by Hardware TOTP token or other hardware devices.



⚠ You may not be able to running Windows 10. I ensure both your comp enabled.

Passkeys enable you to secure FIDO2 security key. Learn mo

1 Step 1 of 2
Create a passkey on th

2 Step 2 of 2
Follow instructions from your browser.
Loading

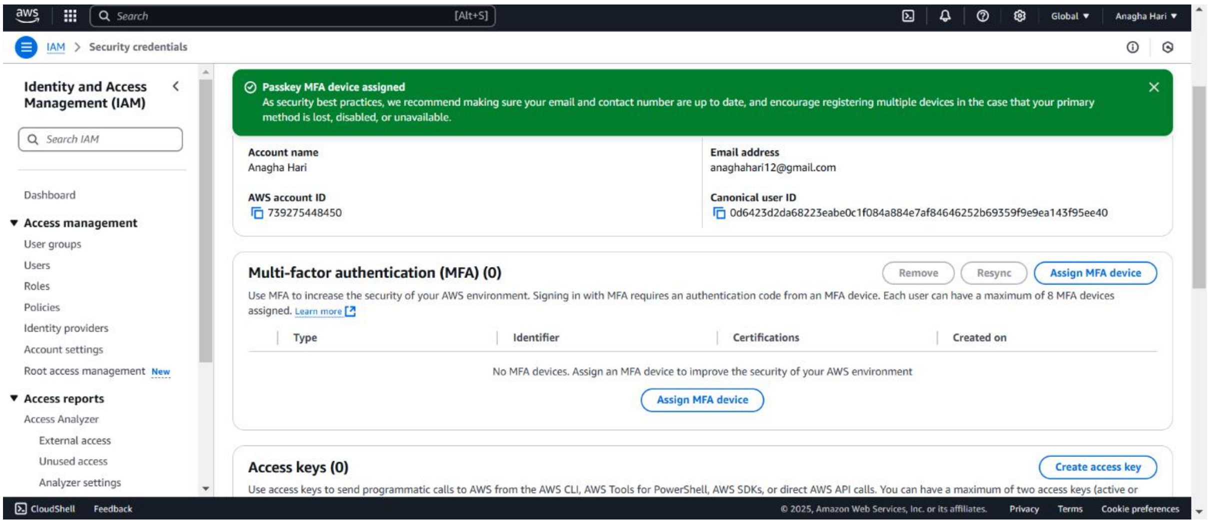
Troubleshoot MFA

Windows Security

Passkey saved

You can now use Windows Hello to sign in with your face, fingerprint, or PIN.

arn:aws:iam::739275448450:root
aws.amazon.com



Passkey MFA device assigned

As security best practices, we recommend making sure your email and contact number are up to date, and encourage registering multiple devices in the case that your primary method is lost, disabled, or unavailable.

Account name Anagha Hari	**Email address** anaghahari12@gmail.com
AWS account ID 739275448450	**Canonical user ID** 0d6423d2da68223eabe0c1f084a884e7af84646252b69359f9e9ea143f95ee40

Multi-factor authentication (MFA) (0)

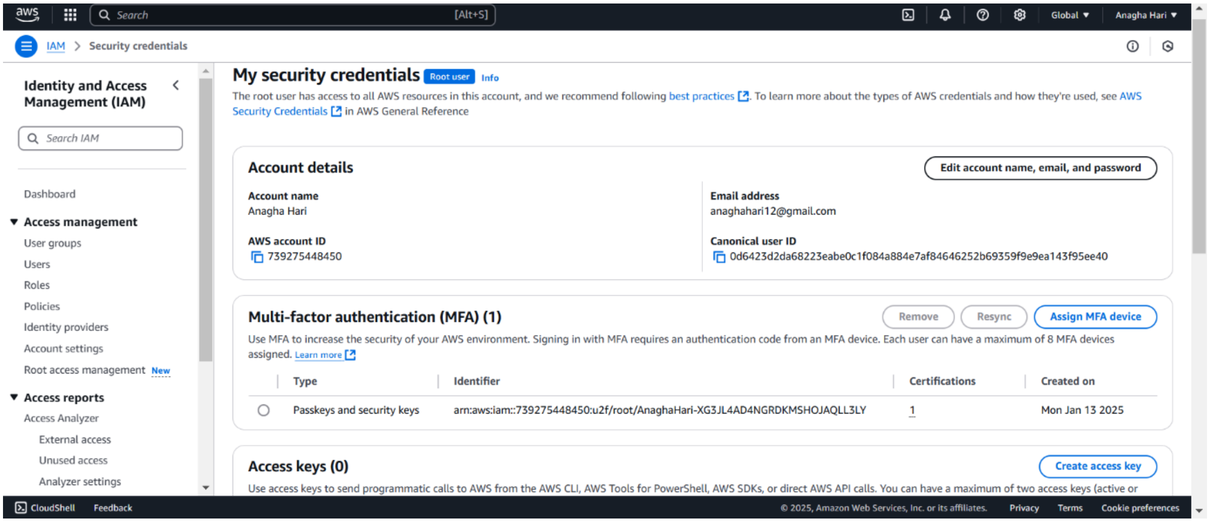
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

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



My security credentials

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

Account details

Account name Anagha Hari	**Email address** anaghahari12@gmail.com
AWS account ID 739275448450	**Canonical user ID** 0d6423d2da68223eabe0c1f084a884e7af84646252b69359f9e9ea143f95ee40

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
○	Passkeys and security keys	arn:aws:iam::739275448450:u2f/root/AnaghaHari-XG3JL4AD4NGRDKMSHOJAQLL3LY	1	Mon Jan 13 2025

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

MFA has been thus successfully created to the root user.