Identity and Access Management (IAM)

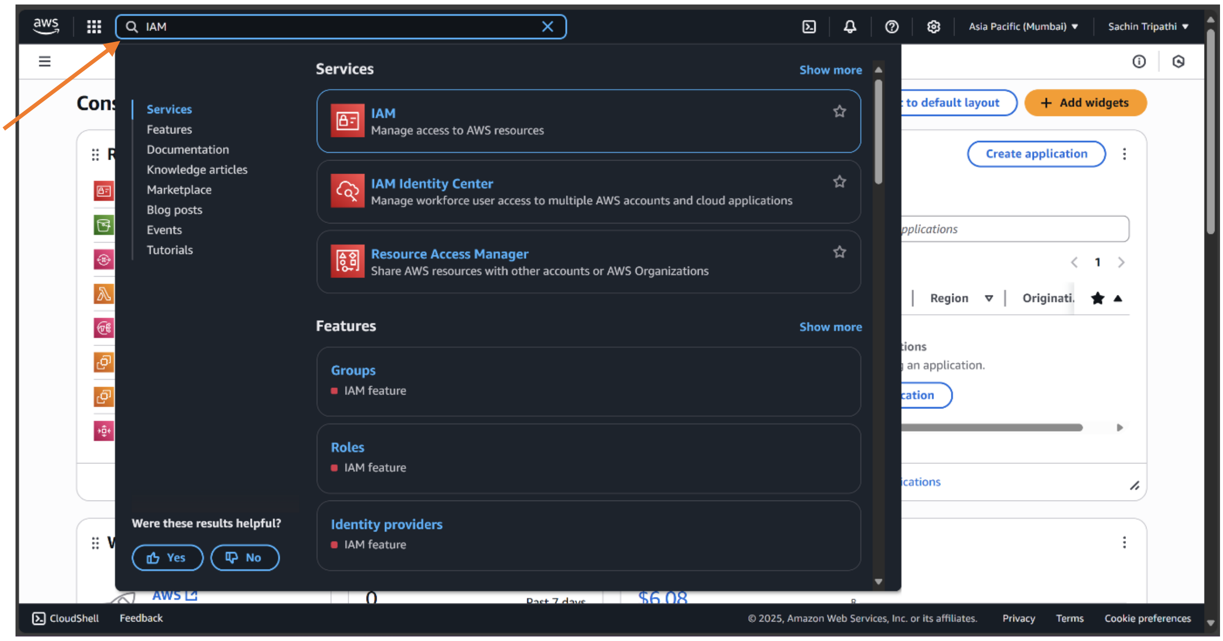
Identity and Access Management (IAM) is an AWS service used to manage who can access your AWS resources and what actions they can perform. It lets you create users, groups, and roles, and assign them specific permissions. IAM helps keep your account secure by allowing only authorized users to do certain tasks. For example, one user can only view files, while another can upload or delete them. It also supports multi-factor authentication (MFA) for extra security. IAM is free and essential for managing access in any AWS project.

Here are the key features of IAM (Identity and Access Management) in point-wise format:

1. User Management – Create and manage individual users in your AWS account.
2. Group Management – Organize users into groups and apply permissions to the whole group.
3. Permissions Control – Define what users and groups can access and do using policies (read, write, delete, etc.).
4. Roles – Create roles with specific permissions that can be assumed by users, services, or applications.
5. Policy Management – Use JSON-based policies to allow or deny access to AWS resources.
6. Temporary Access – Grant time-limited access using IAM roles and AWS STS (Security Token Service).
7. Multi-Factor Authentication (MFA) – Add an extra layer of security to user sign-ins.
8. Audit and Logging – Monitor user activity using AWS CloudTrail for auditing and security analysis.
9. Cross-Account Access – Share resources securely between different AWS accounts using IAM roles.
10. Free to Use – IAM is a global service and is free of cost.

Step1:-

- Go to “AWS Management Console” and search “IAM” and click on “IAM”.



Services

IAM
Manage access to AWS resources

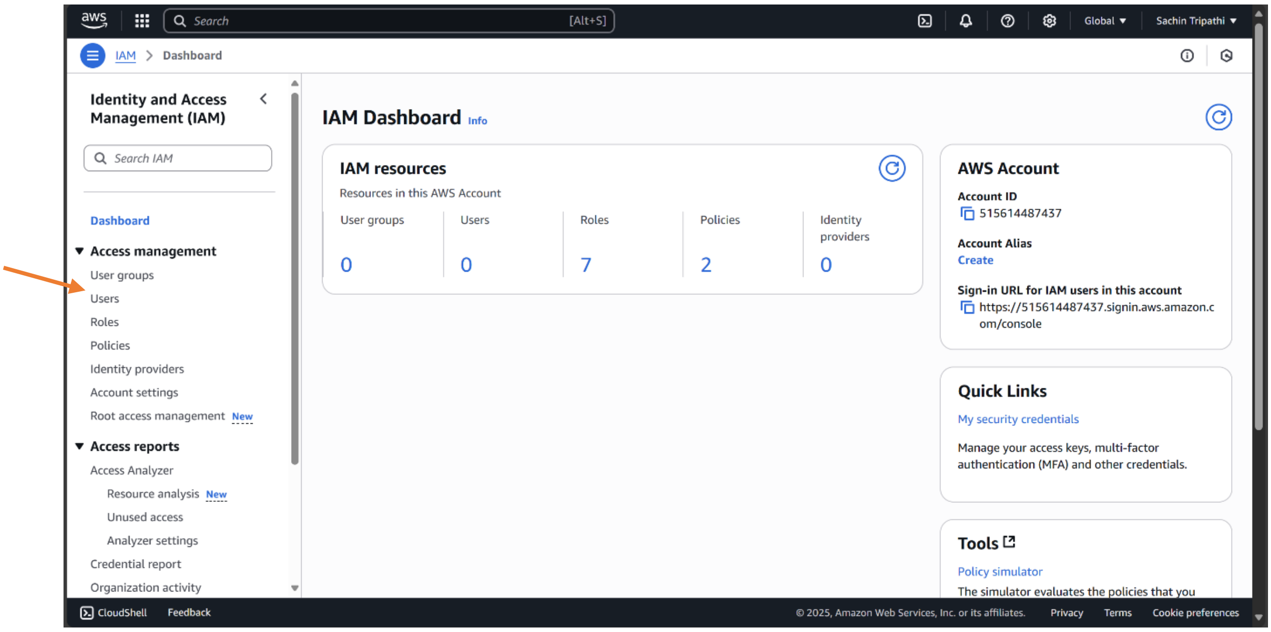
IAM Identity Center
Manage workforce user access to multiple AWS accounts and cloud applications

Resource Access Manager
Share AWS resources with other accounts or AWS Organizations

Features

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

- Click on “Users”(left-side).



IAM Dashboard

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	7	2	0

AWS Account

Account ID
515614487437

Account Alias
Create

Sign-in URL for IAM users in this account
https://515614487437.signin.aws.amazon.com/console

Quick Links

My security credentials

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

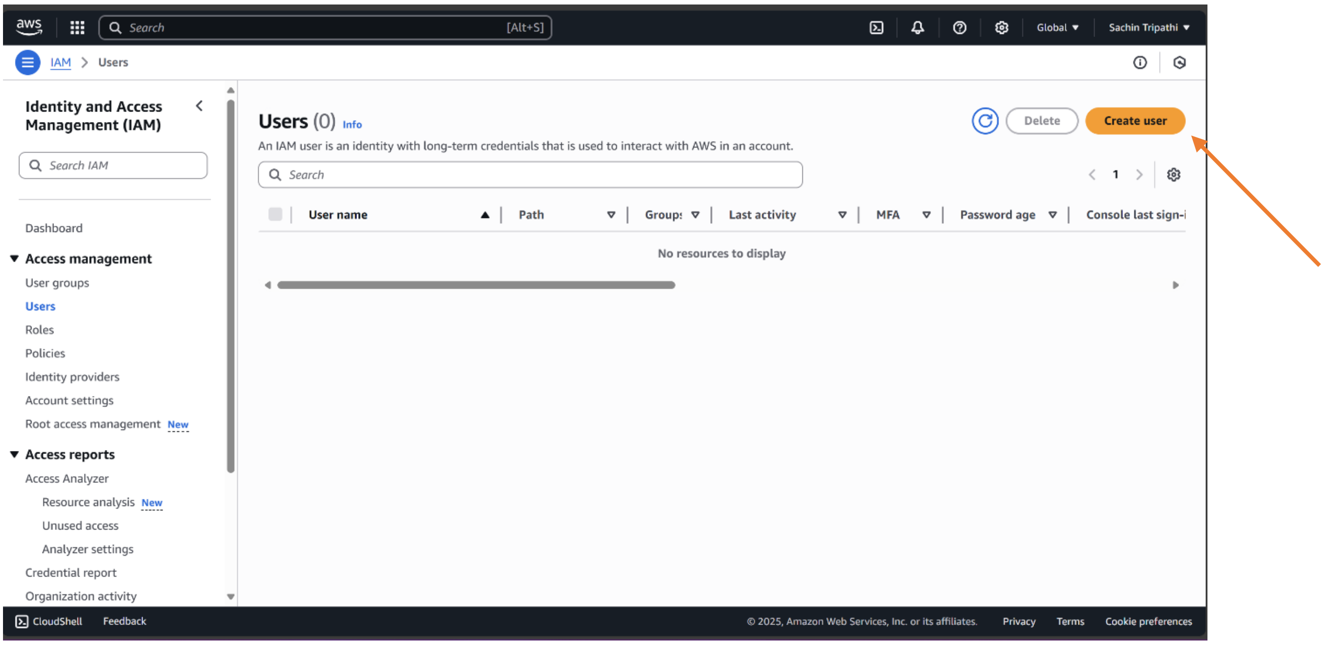
Tools

Policy simulator

The simulator evaluates the policies that you

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

- Click on “Create User”.



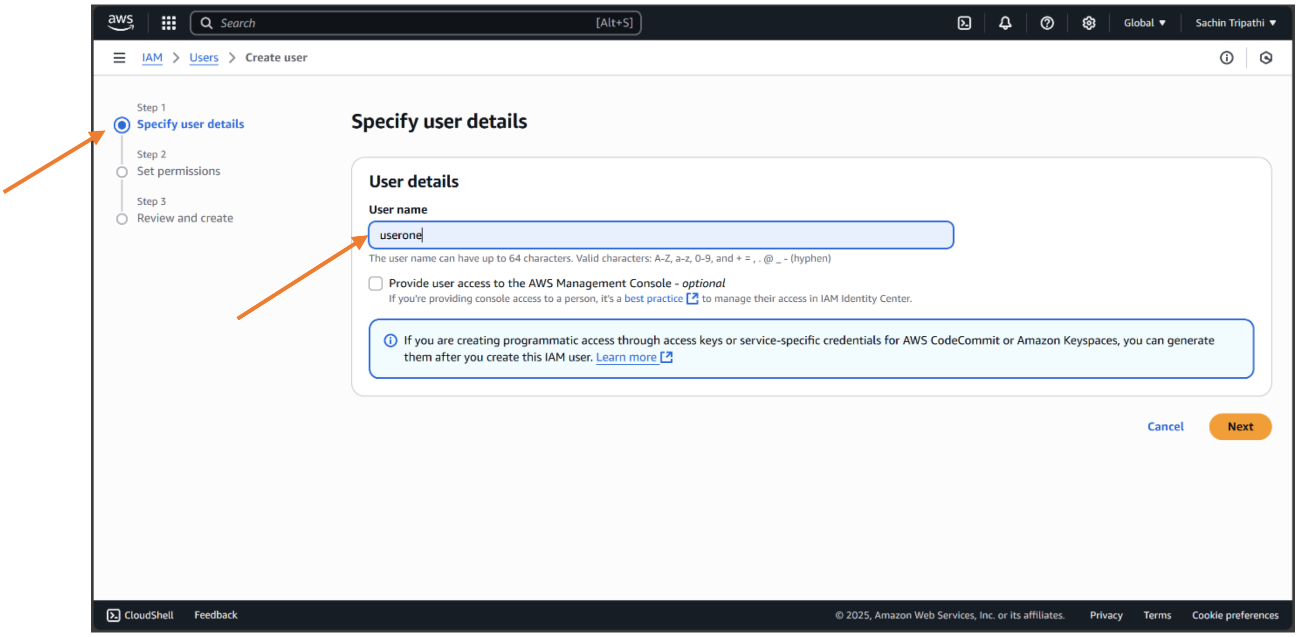
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

No resources to display

Creating user using IAM:-

Step 2:-

- In “Specify user details”, write the “User name”.



User name: userone

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

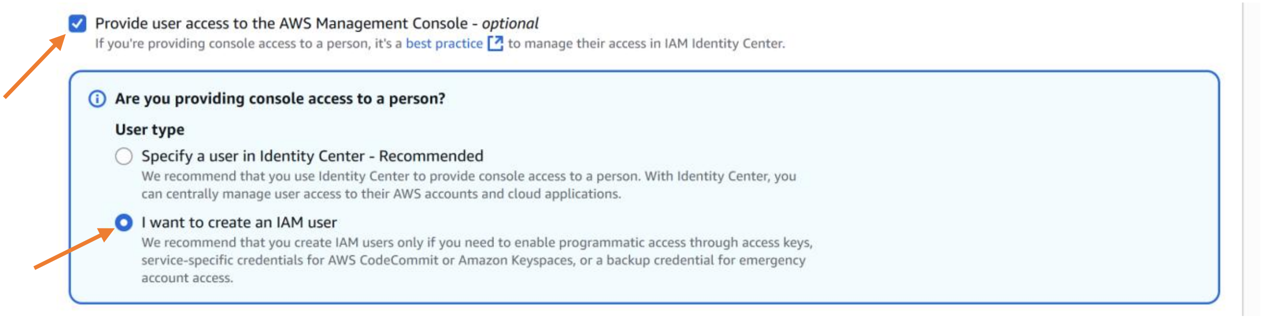
□ Provide user access to the AWS Management Console - *optional*

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

Step 3:-

- Check the “Provide user access to the AWS Management Console”.
- Select “I want to Create an IAM user”.



☑ 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?**

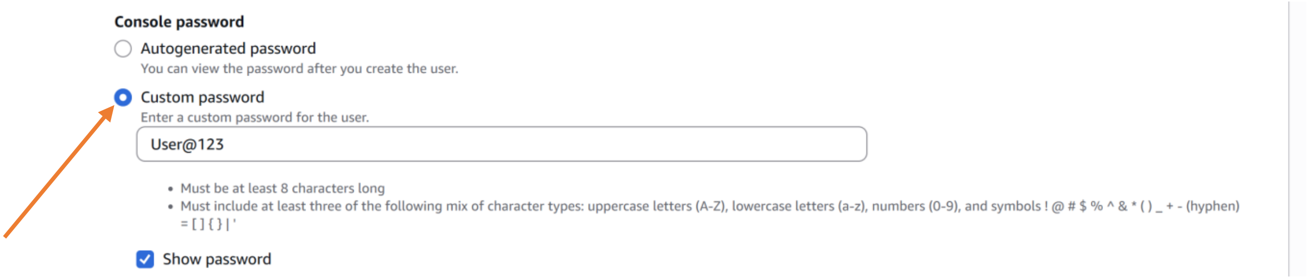
User type

○ 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.

Step 4:-

- In “Console password” click on “Custom password”. Ex:-User@123



Console password

○ Autogenerated password
You can view the password after you create the user.

● Custom password
Enter a custom password for the user.

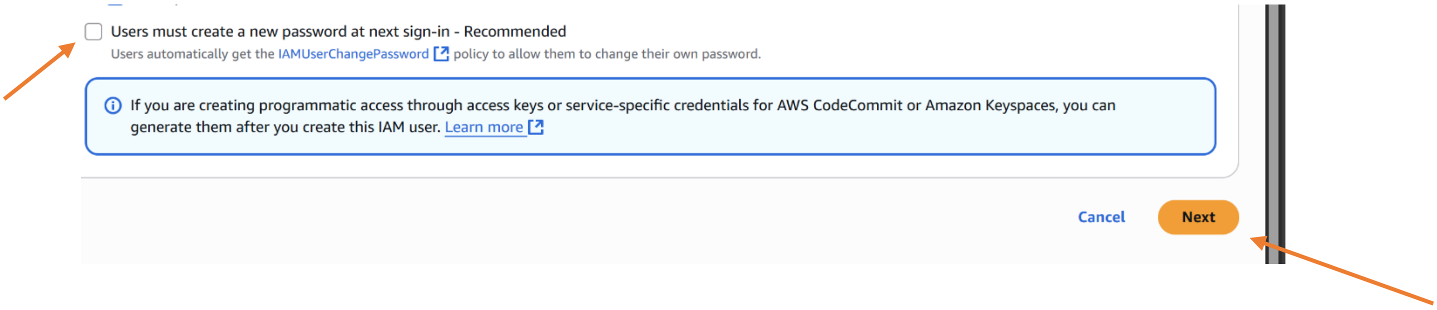
User@123

- 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

Step 5:-

- Uncheck the “User must create a new password at next sig-in”.
- Click on “Next”.

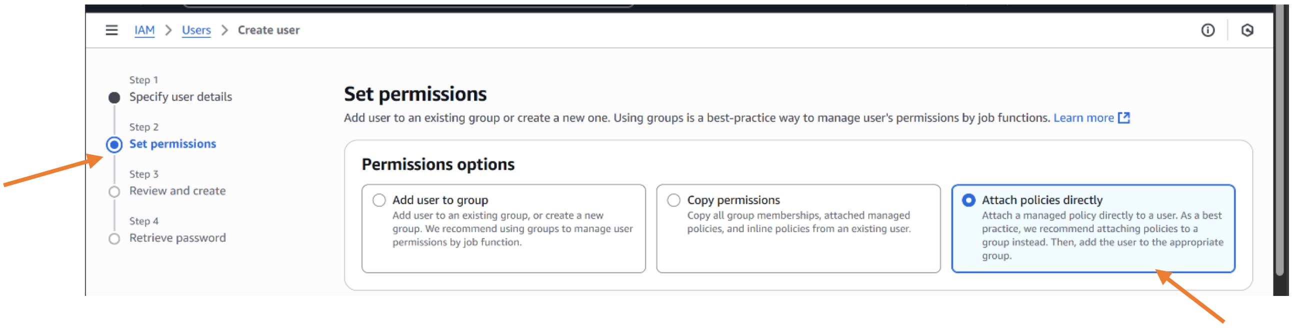


□ Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

ⓘ 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 6:-

- In “Set permissions”, select “Attach policies directly” as “Permissions options”.



IAM > Users > Create user

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

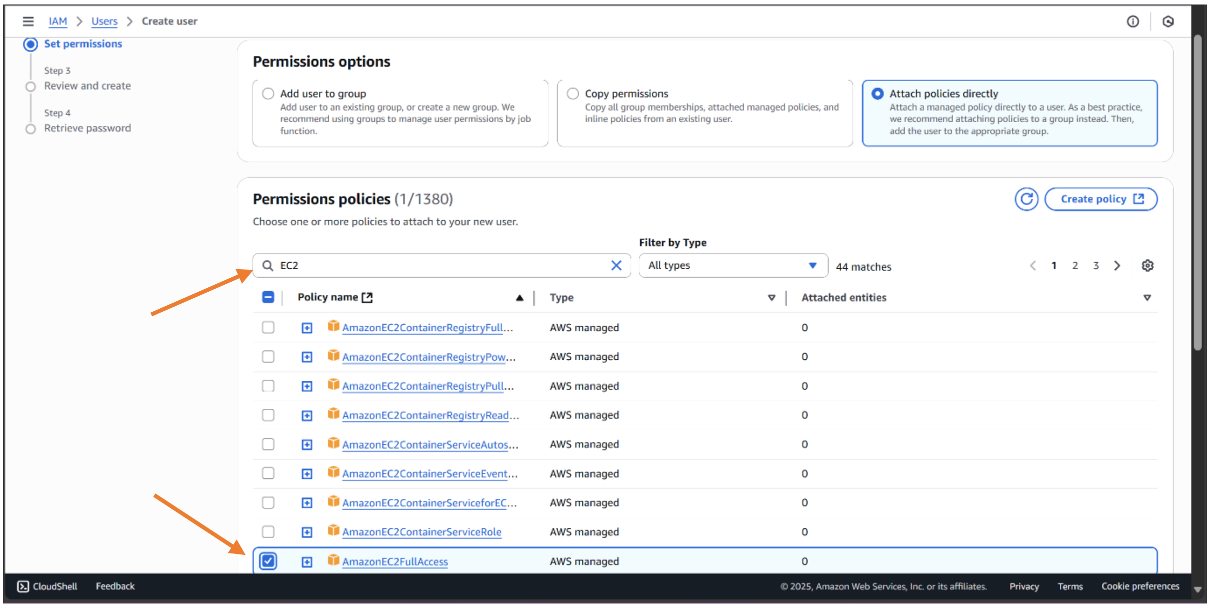
Permissions options

○ 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.

- Now select the “Permissions policies” that you want to add.
- Also you can add permission according to your need.



IAM > Users > Create user

Set permissions

Step 3
Review and create

Step 4
Retrieve password

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 (1/1380)

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

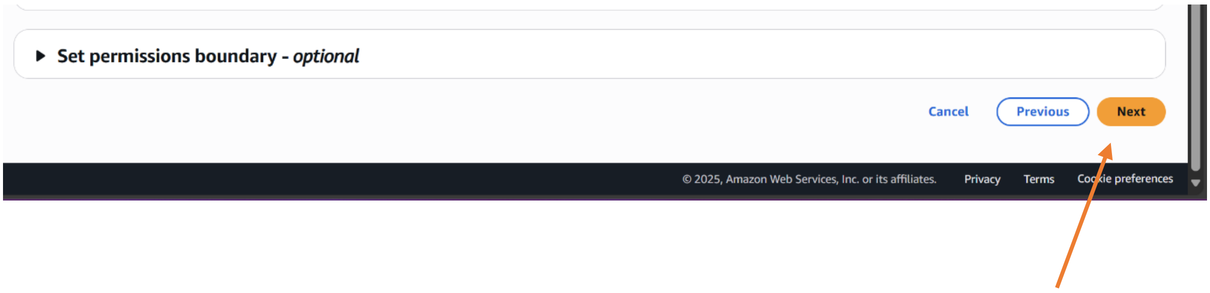
Create policy

Filter by Type: All types

EC2 — 44 matches — 1 2 3

	Policy name	Type	Attached entities
□	AmazonEC2ContainerRegistryFull...	AWS managed	0
□	AmazonEC2ContainerRegistryPow...	AWS managed	0
□	AmazonEC2ContainerRegistryPull...	AWS managed	0
□	AmazonEC2ContainerRegistryRead...	AWS managed	0
□	AmazonEC2ContainerServiceAutos...	AWS managed	0
□	AmazonEC2ContainerServiceEvent...	AWS managed	0
□	AmazonEC2ContainerServiceforEC...	AWS managed	0
□	AmazonEC2ContainerServiceRole	AWS managed	0
☑	AmazonEC2FullAccess	AWS managed	0

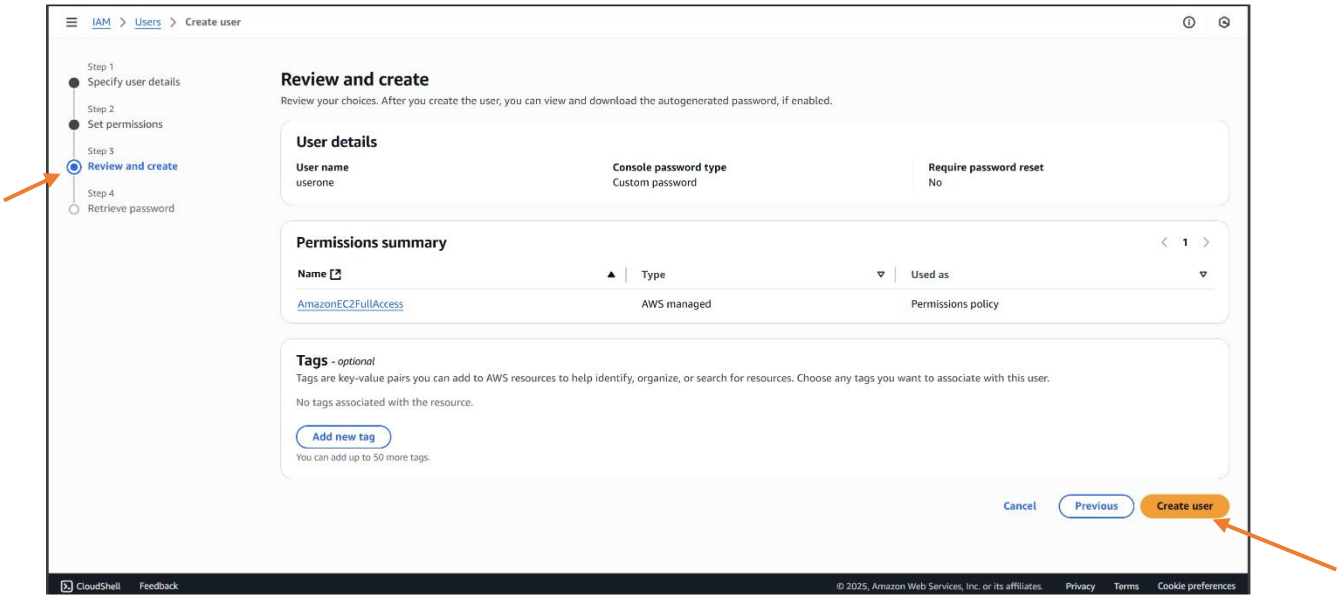
- Click on “Next”.



▶ Set permissions boundary - *optional*

Step 7:-

- In “Review and create” click on “Create User”.



IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

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
userone	Custom password	No

Permissions summary

Name	Type	Used as
AmazonEC2FullAccess	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.

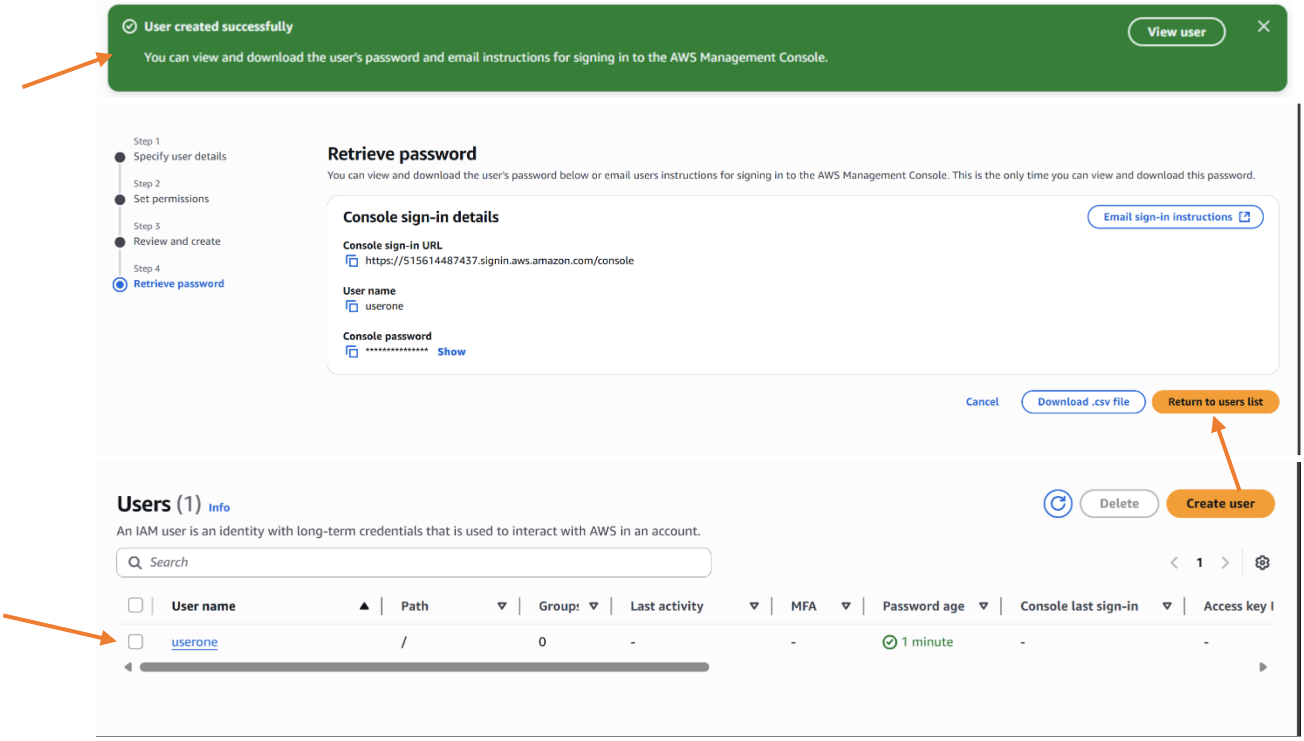
No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Previous Create user

- User is Created Successfully.
- Click on “Return to the Users list”



User created successfully

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

View user

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

Email sign-in instructions

Console sign-in URL
https://515614487437.signin.aws.amazon.com/console

User name
userone

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

Cancel Download .csv file Return to users list

Users (1) Info

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

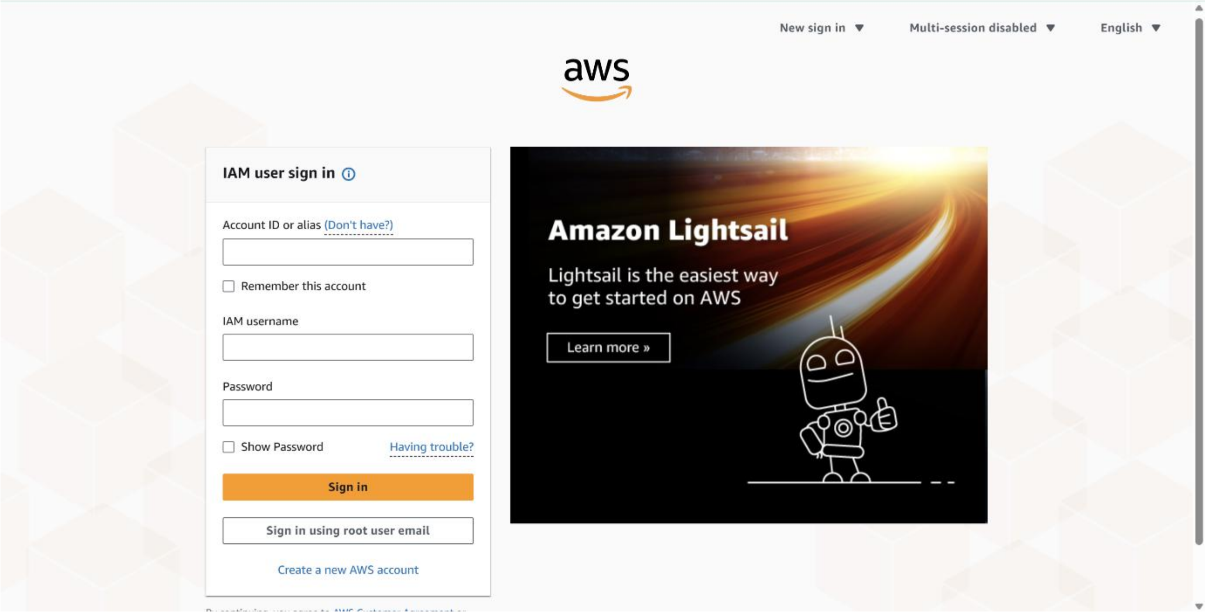
Delete Create user

Search

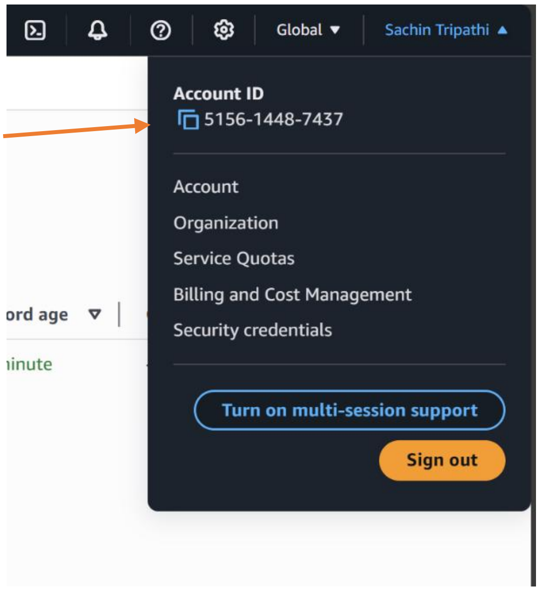
User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key I
userone	/	0	-	-	✓ 1 minute	-	-

Step 8:-

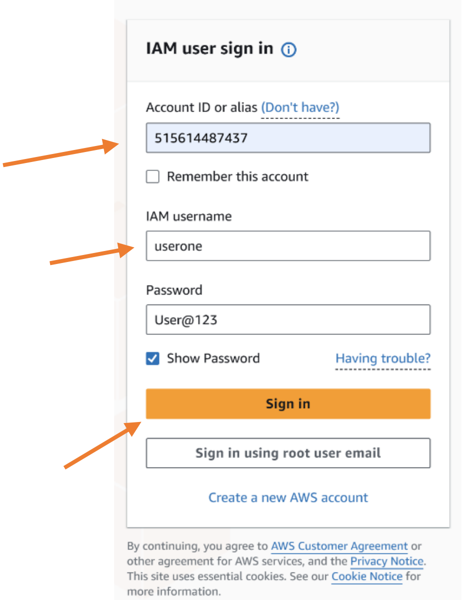
- Now go on another browser or incognito tab , open “AWS Management Console”.
- Click on sign in.
- Select “IAM user sign in”.



- Copy your root account ID in “Account ID or alias” box.



- Paste the copied “Account ID or alias”.
- Enter the “IAM username”. that you have created. Ex:-“userone”.
- Enter the password and click on “Sign in”.



IAM user sign in

Account ID or alias (Don't have?): 515614487437

□ Remember this account

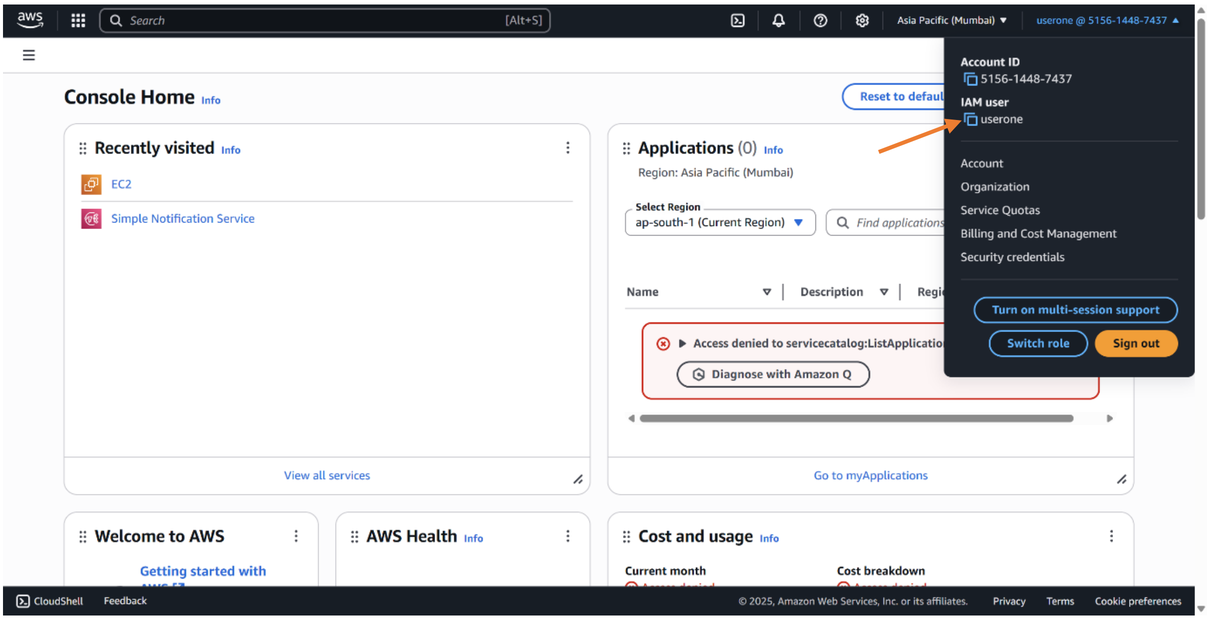
IAM username: userone

Password: User@123

☑ Show Password

By continuing, you agree to AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

- Now “userone” is signed in to the root user account.



Account ID: 5156-1448-7437

IAM user: userone

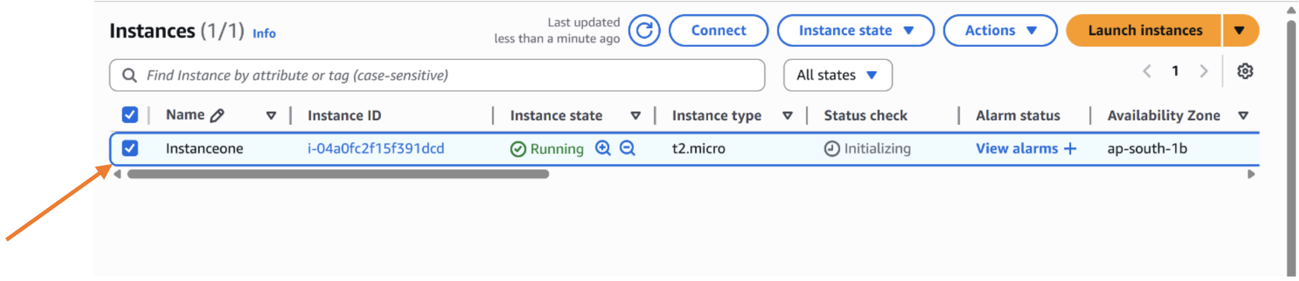
Region: Asia Pacific (Mumbai)

Select Region: ap-south-1 (Current Region)

Access denied to servicecatalog:ListApplicatio

Step 9:-

- “userone” can easily access all the properties of EC2.But it cannot access other option access.
- For example, “user1” can easily launch an instance.

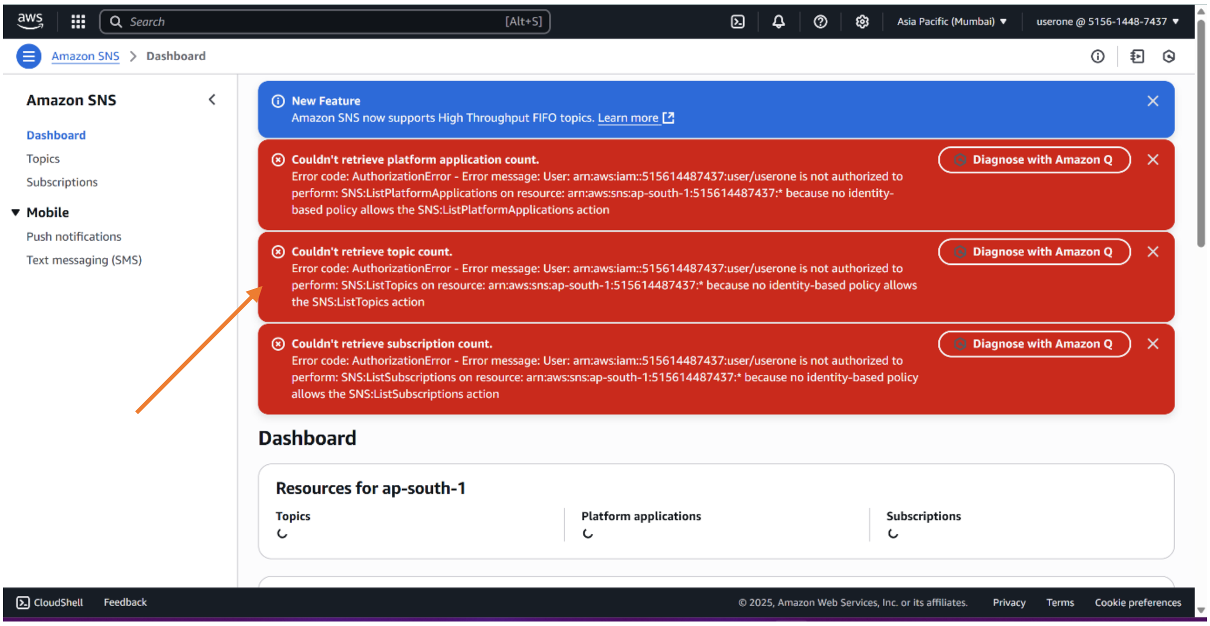


Instances (1/1) Info

Last updated less than a minute ago

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
☑	Instanceone	i-04a0fc2f15f391dcd	Running	t2.micro	Initializing	View alarms +	ap-south-1b

- But if “userone” tries to create a topic in SNS, it will be able to do anything or access.



New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more

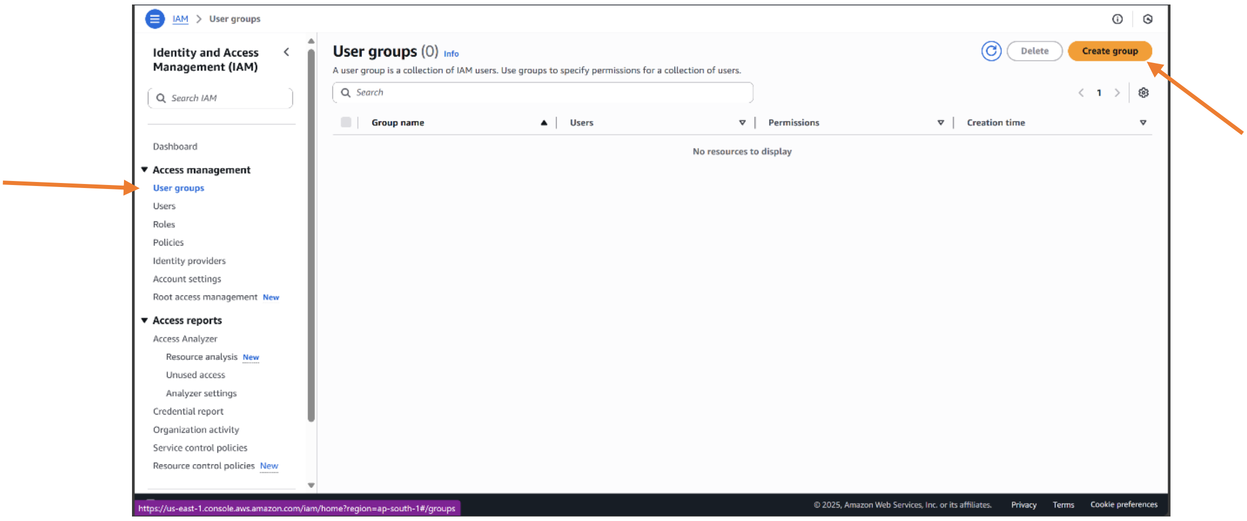
Couldn't retrieve platform application count.
Error code: AuthorizationError - Error message: User: arn:aws:iam::515614487437:user/userone is not authorized to perform: SNS:ListPlatformApplications on resource: arn:aws:sns:ap-south-1:515614487437:* because no identity-based policy allows the SNS:ListPlatformApplications action

Couldn't retrieve topic count.
Error code: AuthorizationError - Error message: User: arn:aws:iam::515614487437:user/userone is not authorized to perform: SNS:ListTopics on resource: arn:aws:sns:ap-south-1:515614487437:* because no identity-based policy allows the SNS:ListTopics action

Couldn't retrieve subscription count.
Error code: AuthorizationError - Error message: User: arn:aws:iam::515614487437:user/userone is not authorized to perform: SNS:ListSubscriptions on resource: arn:aws:sns:ap-south-1:515614487437:* because no identity-based policy allows the SNS:ListSubscriptions action

Step 10:-

- In “Access management”, go to “User groups” and click on “Create group”.



IAM > User groups

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

Resource analysis New

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Resource control policies New

User groups (0) Info

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

Delete | Create group

Search

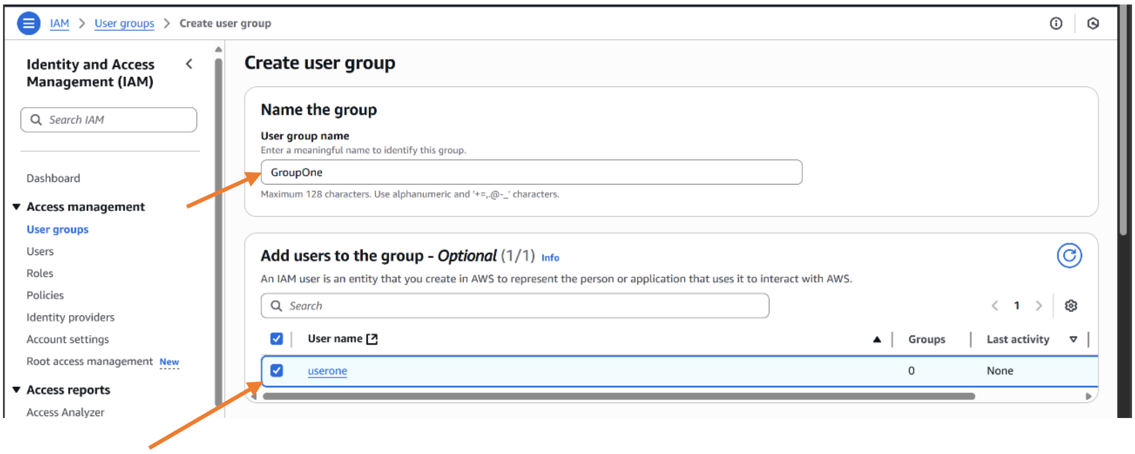
Group name	Users	Permissions	Creation time

No resources to display

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

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

- Enter the “user group name”.
- Select the users whom you want to add to the group. Ex:-Add userone.



IAM > User groups > Create user group

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

Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

GroupOne

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

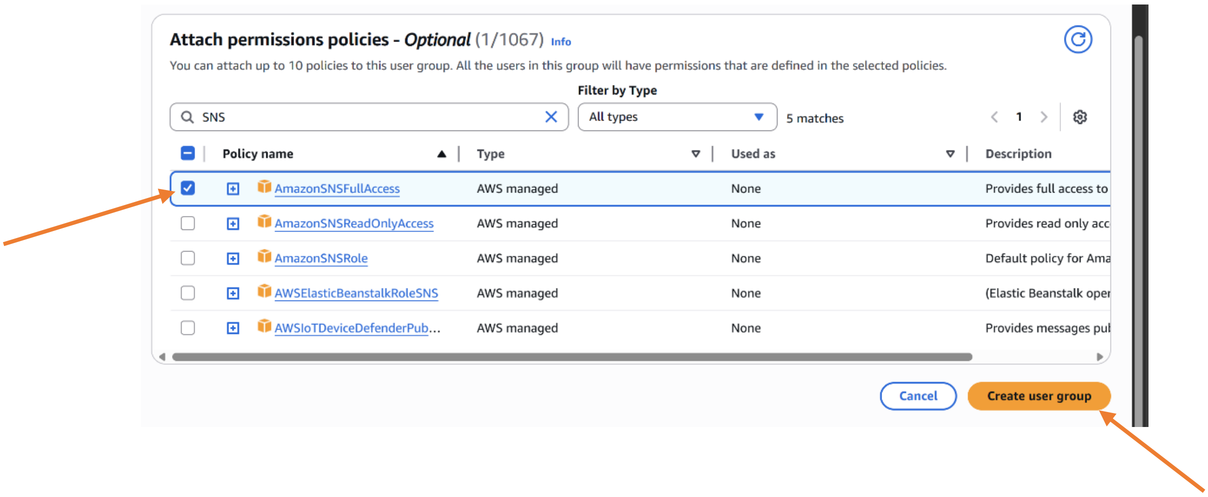
Add users to the group - *Optional* (1/1) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search

☑	User name	Groups	Last activity
☑	userone	0	None

- “Attach permissions policies” to the group according to your need.
- Ex:- AmazonSNSFullAccess.
- Click on “Create user group”.



Attach permissions policies - *Optional* (1/1067) 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.

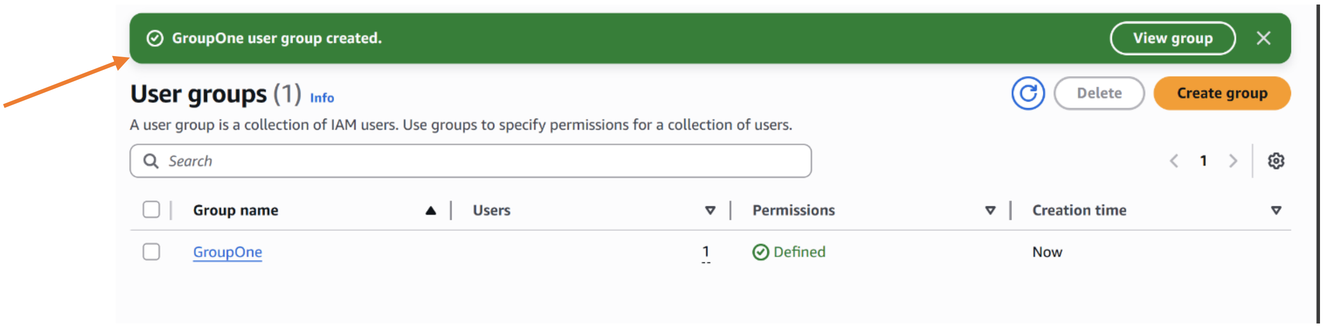
Filter by Type

SNS | All types | 5 matches

	Policy name	Type	Used as	Description
☑	AmazonSNSFullAccess	AWS managed	None	Provides full access to
□	AmazonSNSReadOnlyAccess	AWS managed	None	Provides read only acc
□	AmazonSNSRole	AWS managed	None	Default policy for Ama
□	AWSElasticBeanstalkRoleSNS	AWS managed	None	(Elastic Beanstalk oper
□	AWSIoTDeviceDefenderPub...	AWS managed	None	Provides messages pul

Cancel | Create user group

- User group is created.



GroupOne user group created.

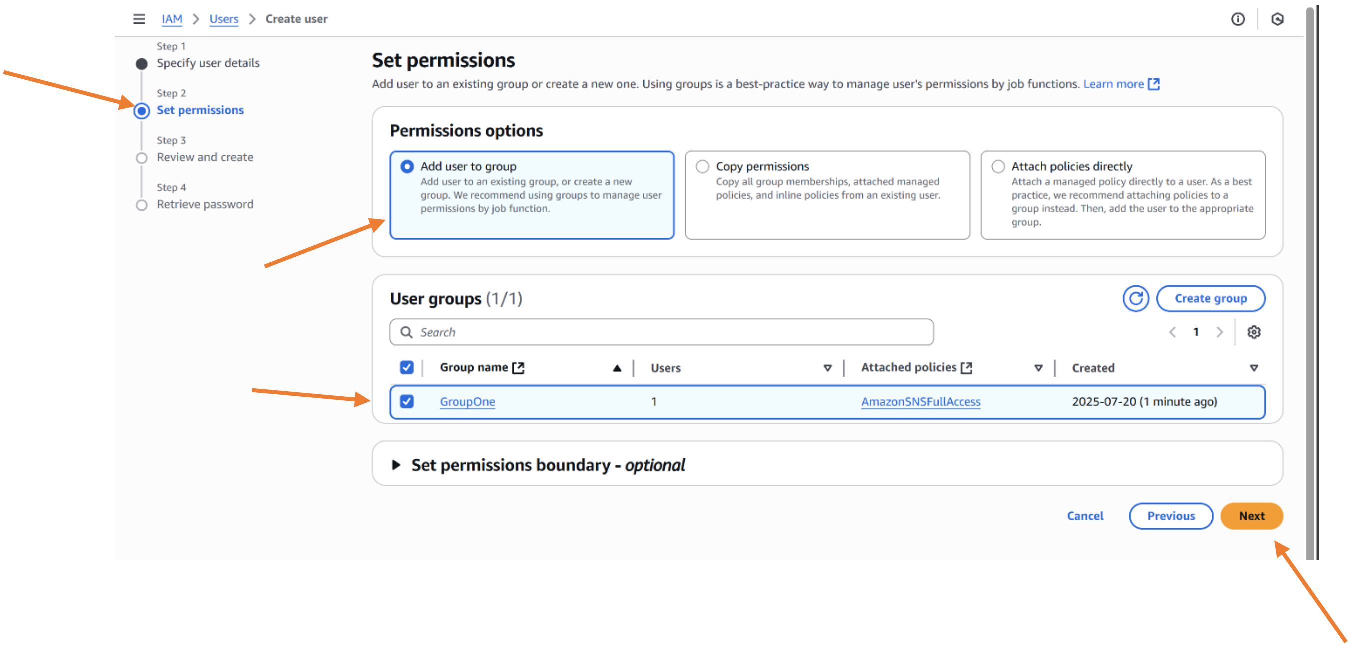
User groups (1) Info

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

□	Group name	Users	Permissions	Creation time
□	GroupOne	1	✓ Defined	Now

Step 11:-

- Now, create another user (usertwo).
- In "Set permissions" select "Add user to group".
- In this user is directly add to the group.
- Select on "GroupOne".
- Click on "Next".



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.

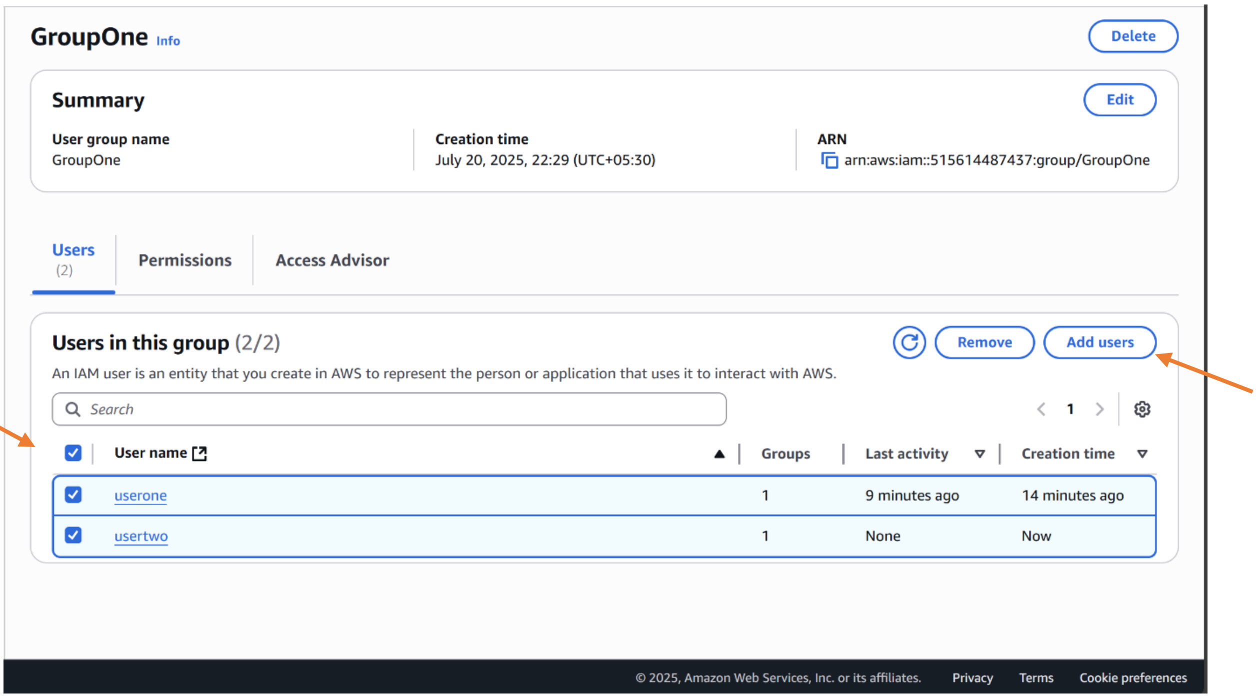
○ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1/1)

☑	Group name	Users	Attached policies	Created
☑	GroupOne	1	AmazonSNSFullAccess	2025-07-20 (1 minute ago)

▶ Set permissions boundary - *optional*

- Now there are two users (userone, usertwo) in "GroupOne".
- Directly add user in the group by click on "Add userd".



User group name
GroupOne

Creation time
July 20, 2025, 22:29 (UTC+05:30)

ARN
arn:aws:iam::515614487437:group/GroupOne

Users in this group (2/2)

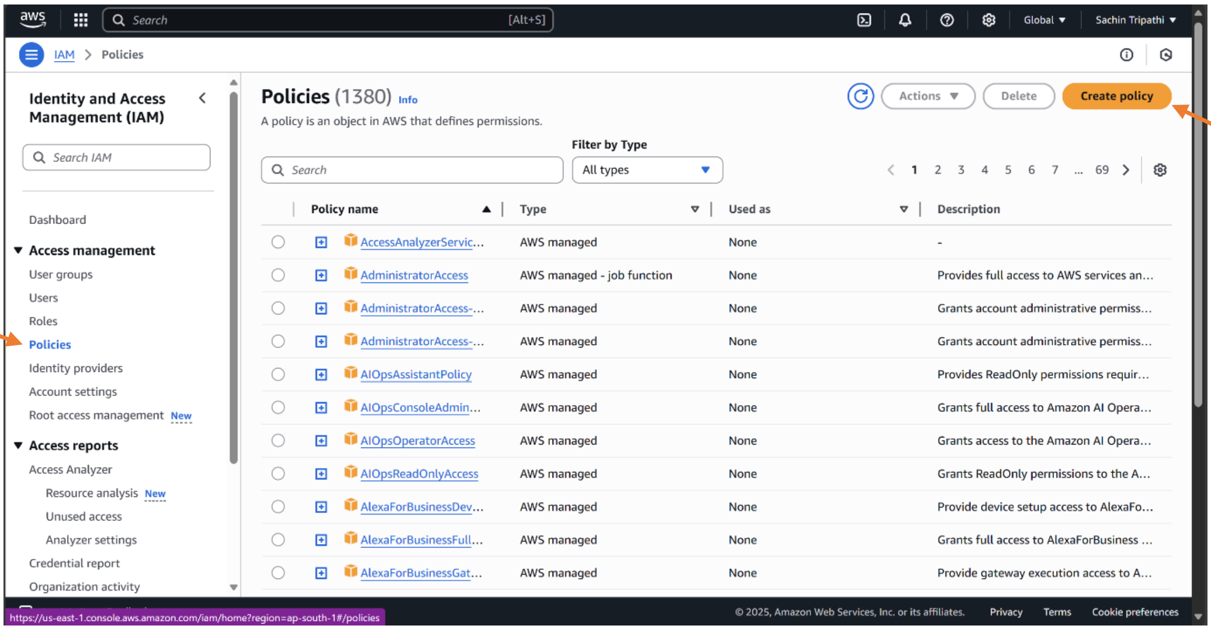
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

☑	User name	Groups	Last activity	Creation time
☑	userone	1	9 minutes ago	14 minutes ago
☑	usertwo	1	None	Now

Creating Policies:-

Step 12:-

- In “Access management” goto “Policies”.
- there are already 1380 policies.
- For creating new policies click on “Create policy”.



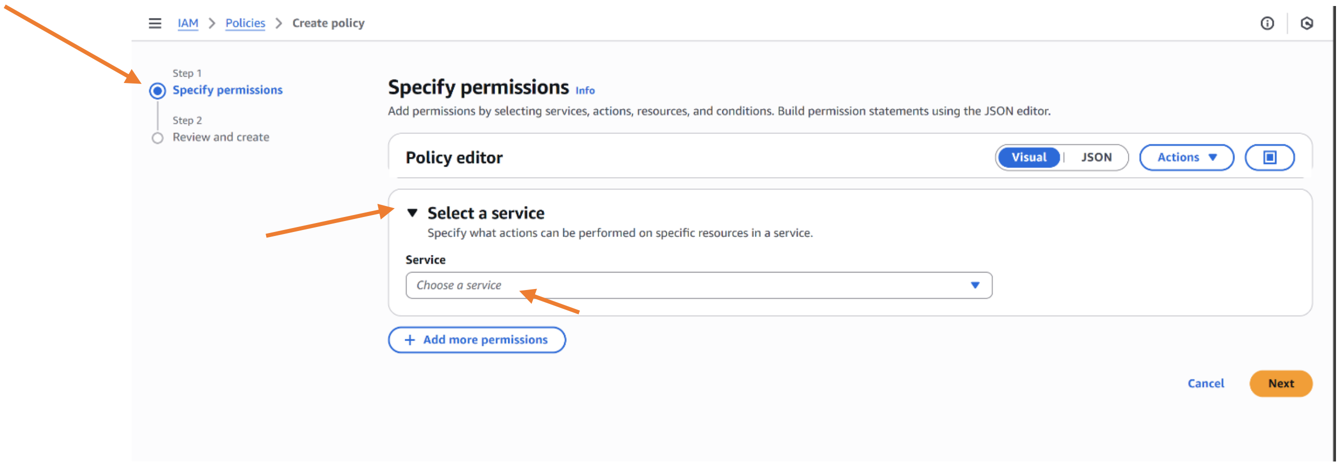
Policies (1380) Info

A policy is an object in AWS that defines permissions.

	Policy name	Type	Used as	Description
○	AccessAnalyzerServic...	AWS managed	None	-
○	AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
○	AdministratorAccess-...	AWS managed	None	Grants account administrative permiss...
○	AdministratorAccess-...	AWS managed	None	Grants account administrative permiss...
○	AIOpsAssistantPolicy	AWS managed	None	Provides ReadOnly permissions requir...
○	AIOpsConsoleAdmin...	AWS managed	None	Grants full access to Amazon AI Opera...
○	AIOpsOperatorAccess	AWS managed	None	Grants access to the Amazon AI Opera...
○	AIOpsReadOnlyAccess	AWS managed	None	Grants ReadOnly permissions to the A...
○	AlexaForBusinessDev...	AWS managed	None	Provide device setup access to AlexaFo...
○	AlexaForBusinessFull...	AWS managed	None	Grants full access to AlexaForBusiness ...
○	AlexaForBusinessGat...	AWS managed	None	Provide gateway execution access to A...

https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

- In “Specify permissions” click on “Select a service”.
- Click on “services”.



Specify permissions Info

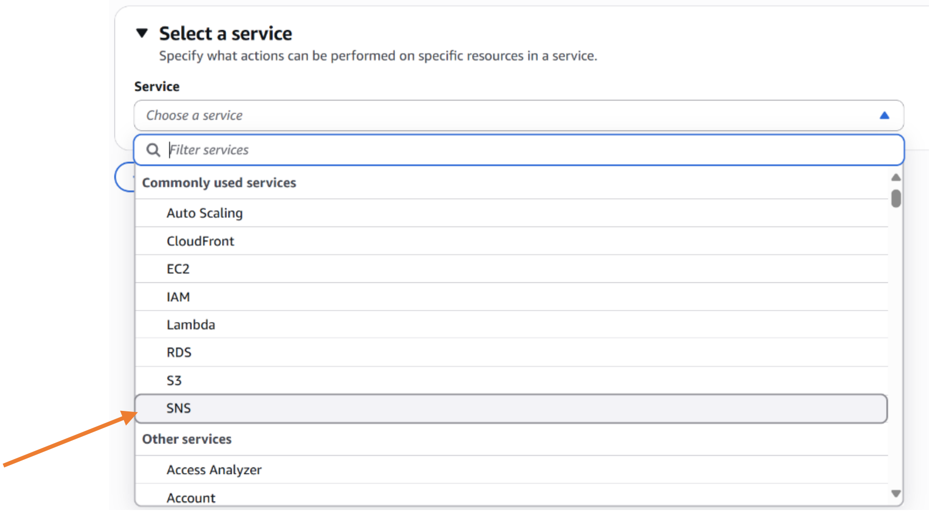
Add permissions by selecting services, actions, resources, and conditions. Build permission statement using the JSON editor.

▼ Select a service

Specify what actions can be performed on specific resources in a service.

Service: Choose a service ▼

- Select “SNS”.



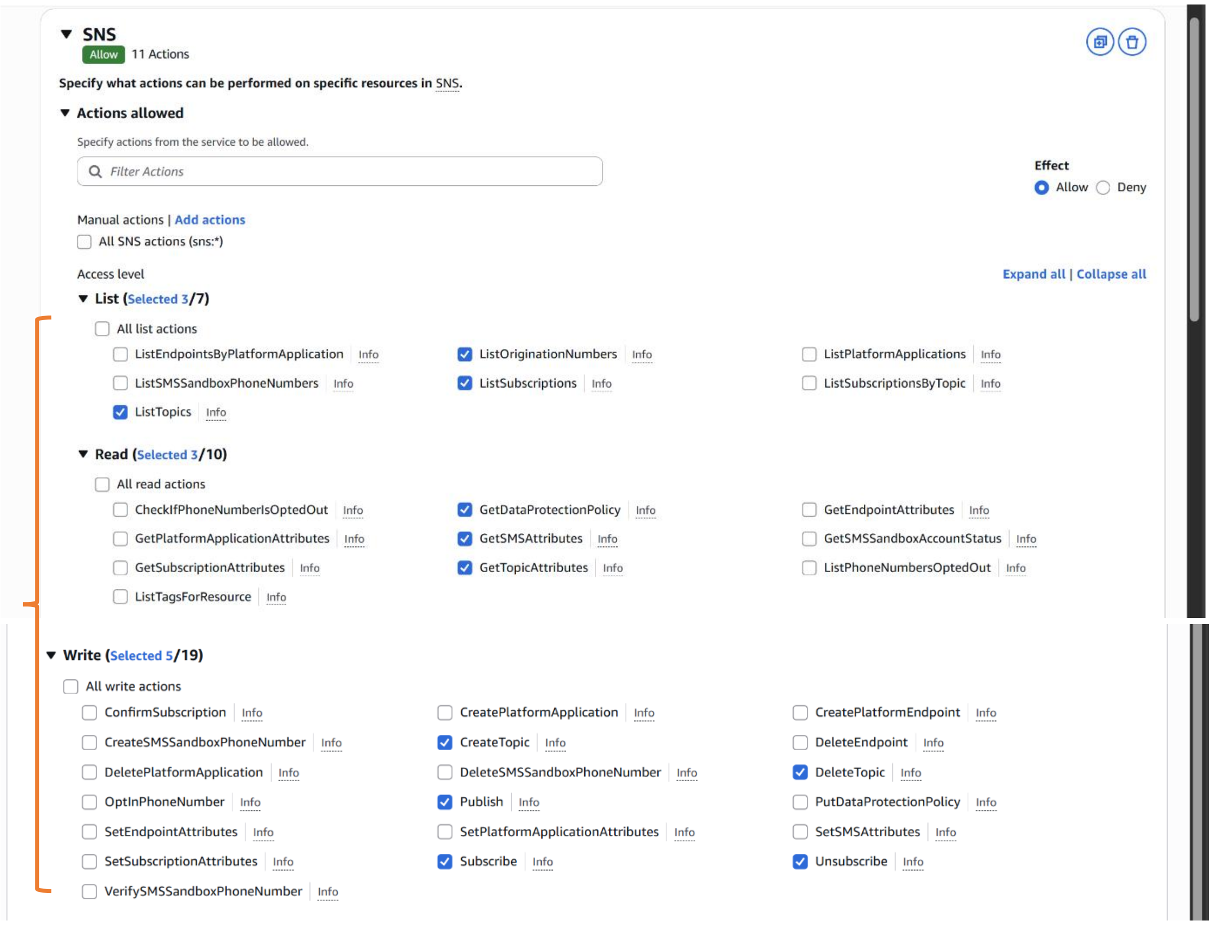
▼ Select a service

Specify what actions can be performed on specific resources in a service.

Service: Choose a service ▲

Step 13:-

- In “Action allowed”, select permission according to the need.
- Select from “List(7)”, “Read(10)”, “Write(19)”, “Permissions management (3)”, “Tagging (2)”.



▼ SNS
Allow 11 Actions

Specify what actions can be performed on specific resources in SNS.

▼ Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Effect
● Allow ○ Deny

Manual actions | Add actions
□ All SNS actions (sns:*)

Access level

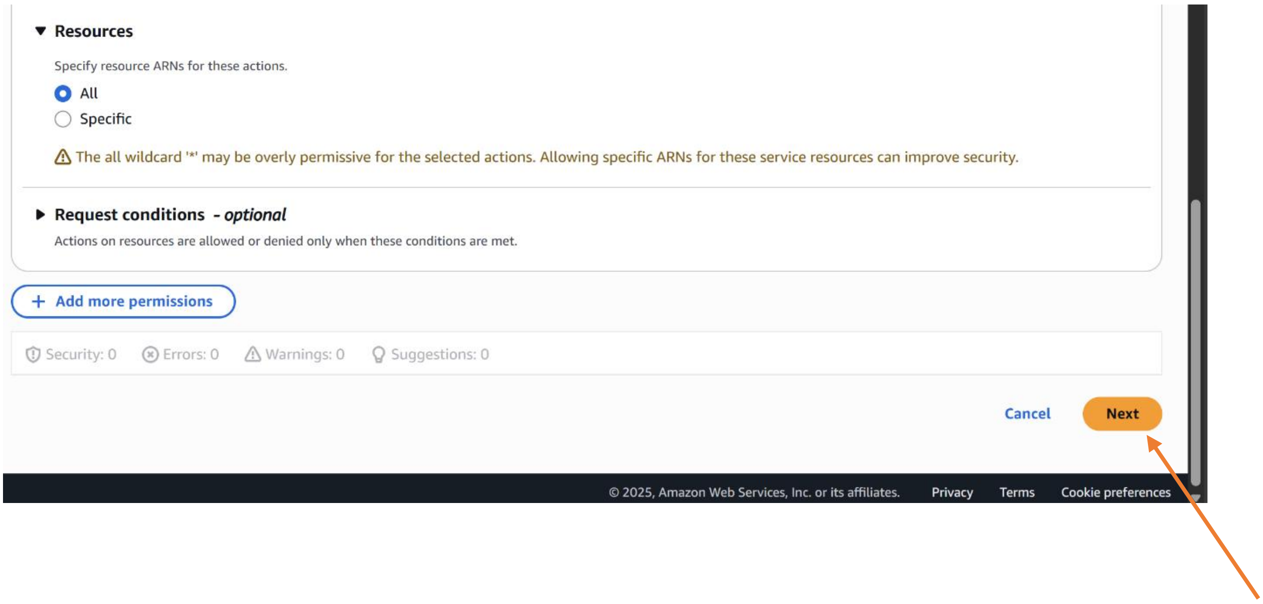
Expand all | Collapse all

▼ List (Selected 3/7)
□ All list actions
□ ListEndpointsByPlatformApplication Info
☑ ListOriginationNumbers Info
□ ListPlatformApplications Info
□ ListSMSSandboxPhoneNumbers Info
☑ ListSubscriptions Info
□ ListSubscriptionsByTopic Info
☑ ListTopics Info

▼ Read (Selected 3/10)
□ All read actions
□ CheckIfPhoneNumberIsOptedOut Info
☑ GetDataProtectionPolicy Info
□ GetEndpointAttributes Info
□ GetPlatformApplicationAttributes Info
☑ GetSMSAttributes Info
□ GetSMSSandboxAccountStatus Info
□ GetSubscriptionAttributes Info
☑ GetTopicAttributes Info
□ ListPhoneNumbersOptedOut Info
□ ListTagsForResource Info

▼ Write (Selected 5/19)
□ All write actions
□ ConfirmSubscription Info
□ CreatePlatformApplication Info
□ CreatePlatformEndpoint Info
□ CreateSMSSandboxPhoneNumber Info
☑ CreateTopic Info
□ DeleteEndpoint Info
□ DeletePlatformApplication Info
□ DeleteSMSSandboxPhoneNumber Info
☑ DeleteTopic Info
□ OptInPhoneNumber Info
☑ Publish Info
□ PutDataProtectionPolicy Info
□ SetEndpointAttributes Info
□ SetPlatformApplicationAttributes Info
□ SetSMSAttributes Info
□ SetSubscriptionAttributes Info
☑ Subscribe Info
☑ Unsubscribe Info
□ VerifySMSSandboxPhoneNumber Info

- Click on "Next".



▼ Resources

Specify resource ARNs for these actions.
● All
○ Specific

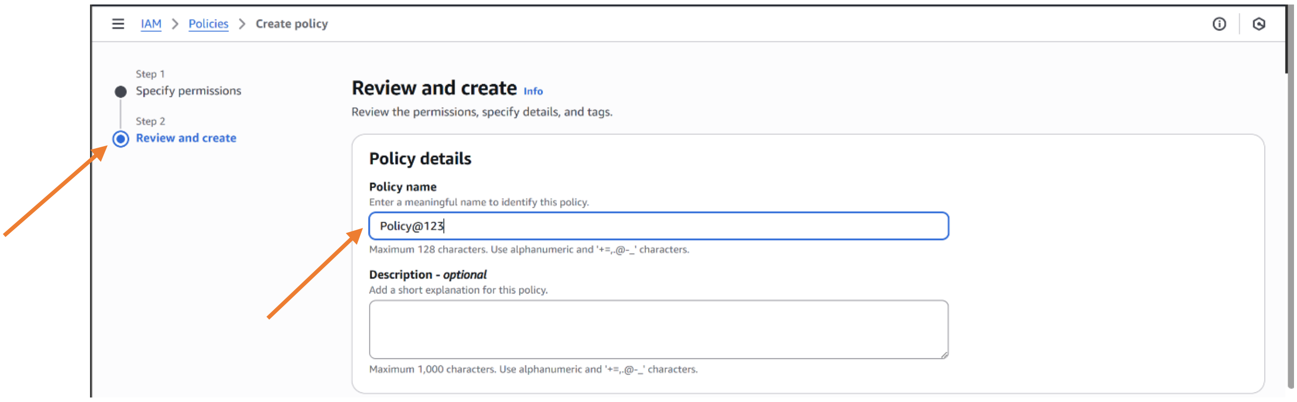
⚠ The all wildcard '*' may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

▶ Request conditions - *optional*

Actions on resources are allowed or denied only when these conditions are met.

Step 14:-

- In “Review and create”, Enter “Policy name”. Ex:-policy@123.



IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Review and create Info

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

Policy@123

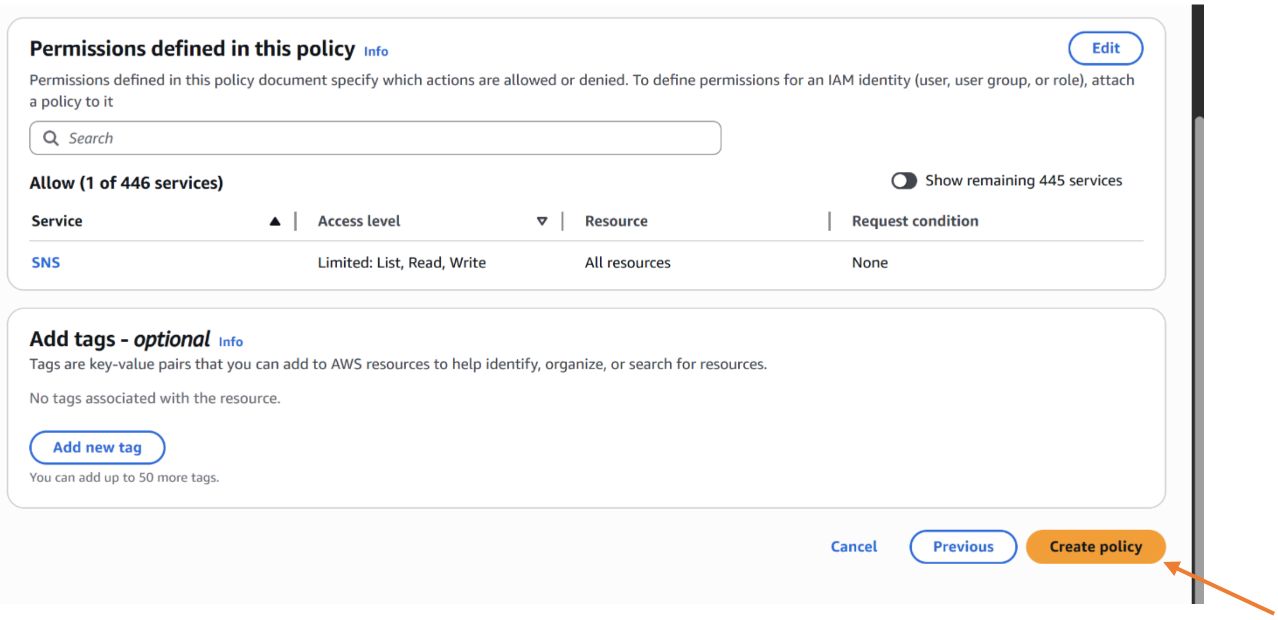
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*

Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

- Click on “Create policy”.



Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (1 of 446 services)

Show remaining 445 services

Service	Access level	Resource	Request condition
SNS	Limited: List, Read, Write	All resources	None

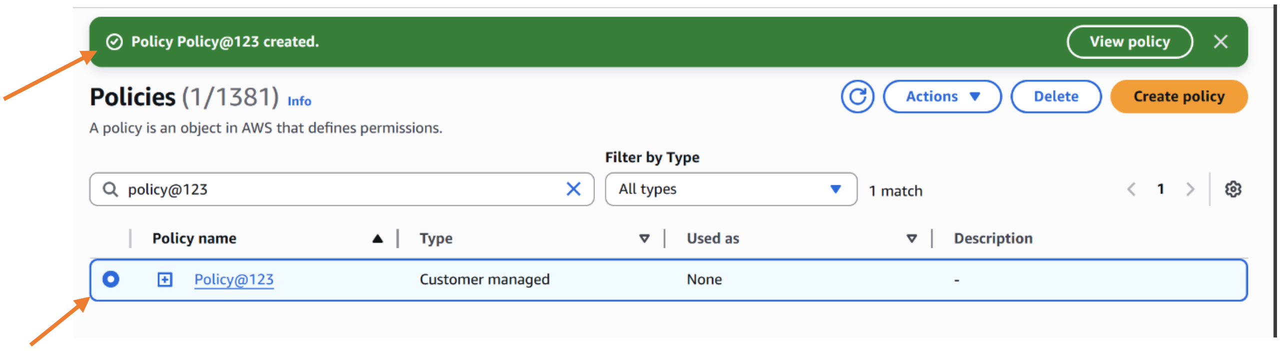
Add tags - *optional* Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

You can add up to 50 more tags.

- Policy is created.



Policy Policy@123 created.

Policies (1/1381) Info

A policy is an object in AWS that defines permissions.

Filter by Type

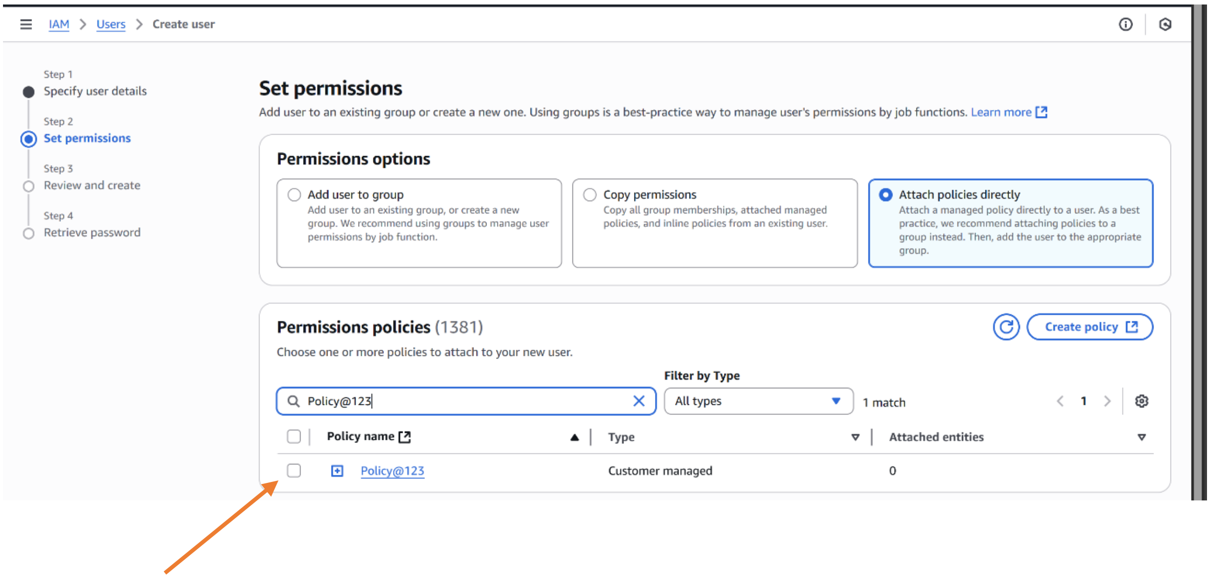
policy@123

All types

1 match

	Policy name	Type	Used as	Description
●	Policy@123	Customer managed	None	-

- Now, This Policy is used when we create user next time.



IAM > Users > Create user

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 (1381)

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

Filter by Type

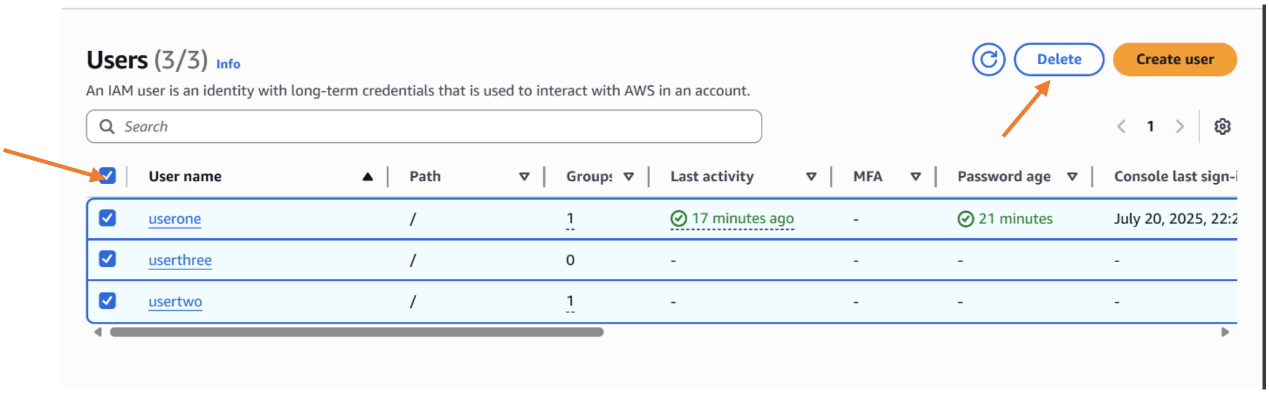
Policy@123 | All types | 1 match

□	Policy name	Type	Attached entities
□	Policy@123	Customer managed	0

Delete user:

Step 15:-

- Select the user which you want to delete. Ex:- userone, usertwo, userthree.
- Click on "Delete".

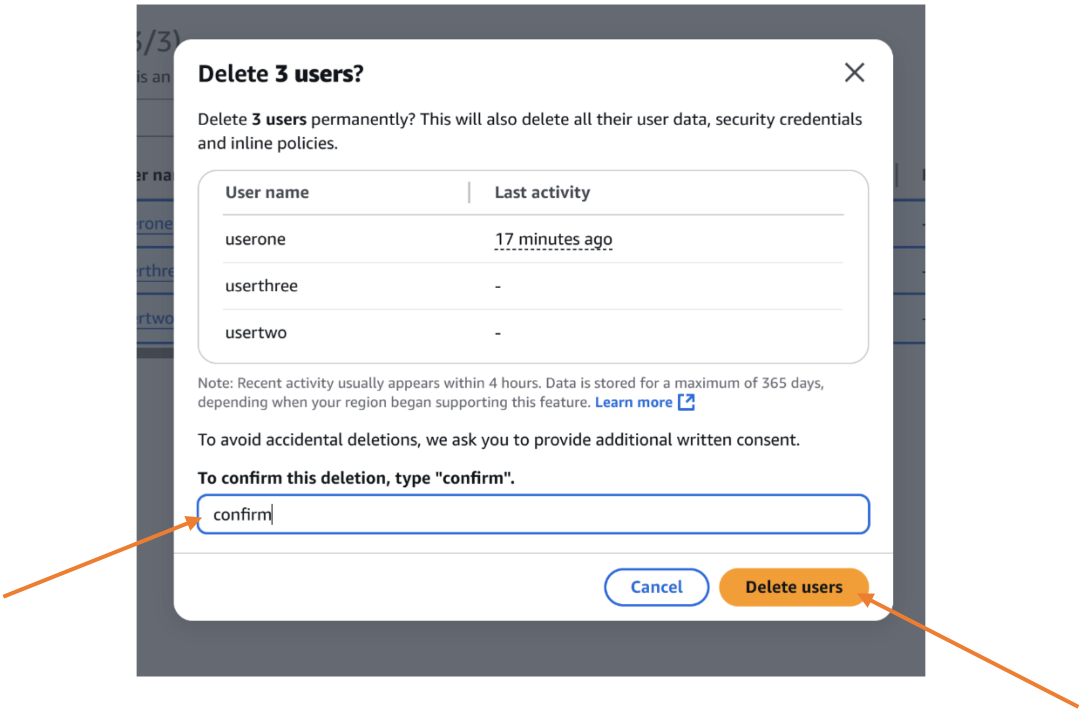


Users (3/3) Info

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-i
☑	userone	/	1	17 minutes ago	-	21 minutes	July 20, 2025, 22:2
☑	userthree	/	0	-	-	-	-
☑	usertwo	/	1	-	-	-	-

- Enter "confirm".
- Click on "Delete user".



Delete 3 users?

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

User name	Last activity
userone	17 minutes ago
userthree	-
usertwo	-

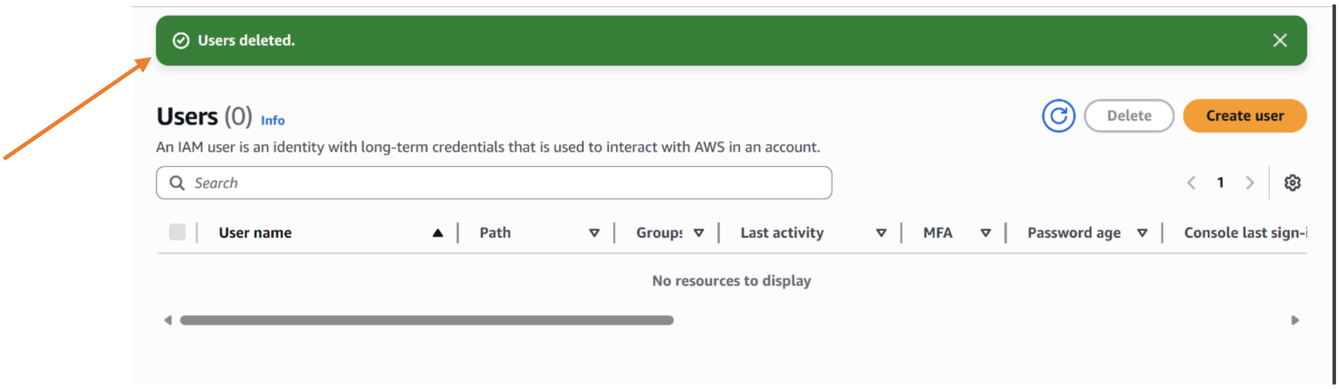
Note: Recent activity usually appears within 4 hours. Data is stored for a maximum of 365 days, depending when your region began supporting this feature. Learn more

To avoid accidental deletions, we ask you to provide additional written consent.

To confirm this deletion, type "confirm".

confirm

- User is deleted.



Users deleted.

Users (0) Info

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

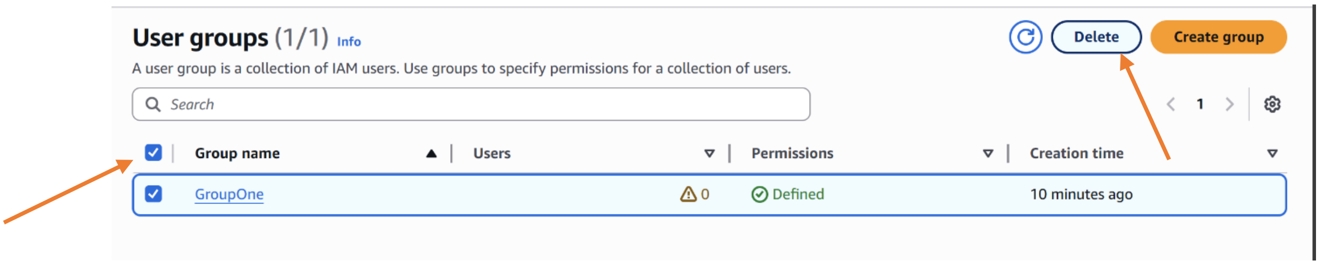
□	User name	Path	Groups	Last activity	MFA	Password age	Console last sign-i

No resources to display

Delete user groups:

Step 16 :-

- Goto to the group.
- Select the group which you want to delete.
- Click on “Delete”.

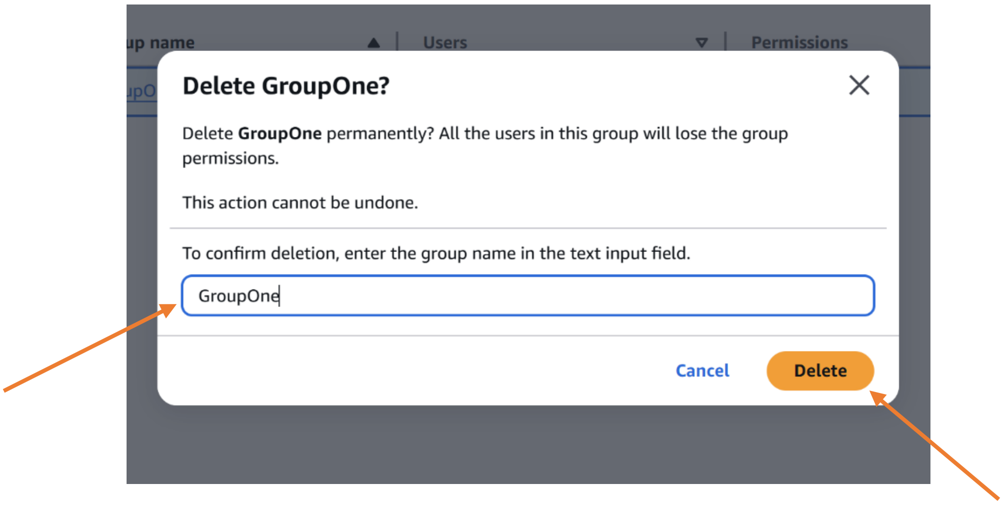


User groups (1/1) Info

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

☑	Group name	Users	Permissions	Creation time
☑	GroupOne	⚠ 0	✓ Defined	10 minutes ago

- Enter “Group name”. Ex:- GroupOne.
- Click on “Delete”.



Delete GroupOne?

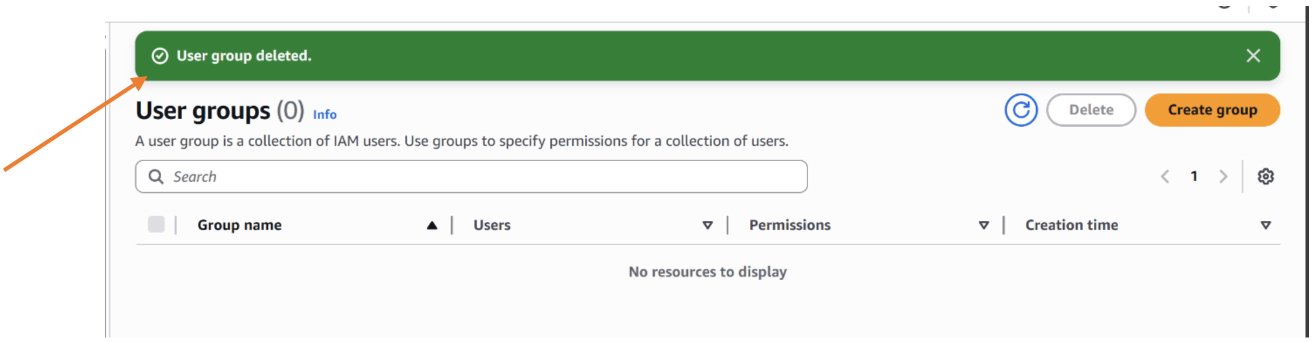
Delete **GroupOne** permanently? All the users in this group will lose the group permissions.

This action cannot be undone.

To confirm deletion, enter the group name in the text input field.

GroupOne

- User group is deleted.



✓ User group deleted.

User groups (0) Info

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

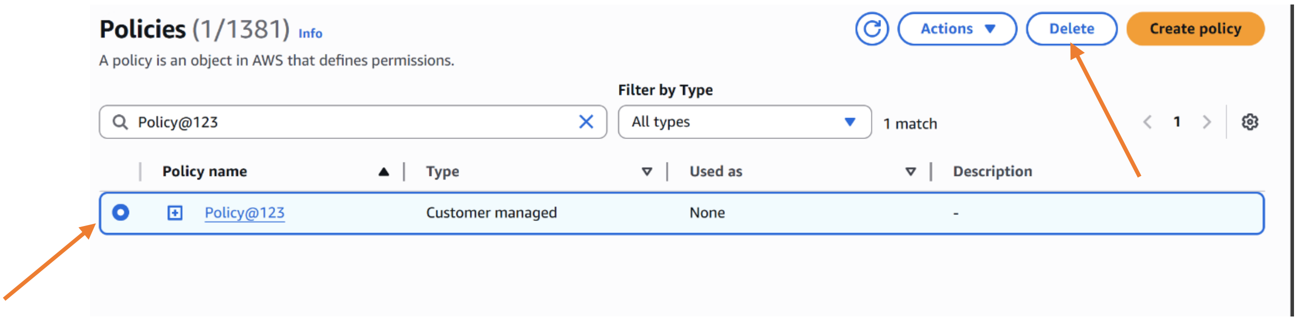
□	Group name	Users	Permissions	Creation time

No resources to display

Delete policy:

Step 16 :-

- Goto policy.
- Search policy.
- Select policy.
- Click on "Delete".



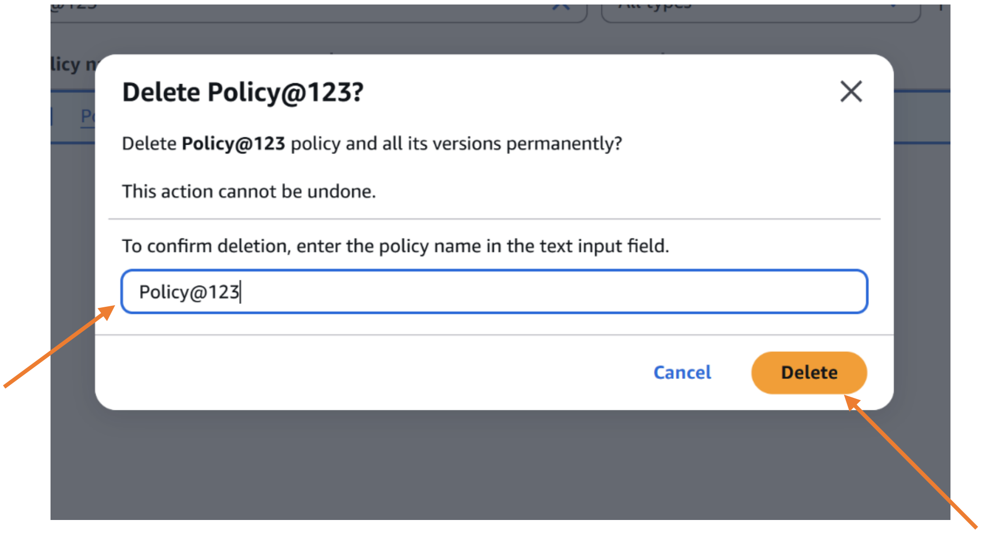
Policies (1/1381) Info

A policy is an object in AWS that defines permissions.

Policy@123 ✕ | All types ▼ | 1 match

○	Policy name ▲	Type	Used as	Description
●	⊞ Policy@123	Customer managed	None	-

- Enter the "Policy name". Ex:-Policy@123.
- Click on "Delete".



Delete Policy@123?

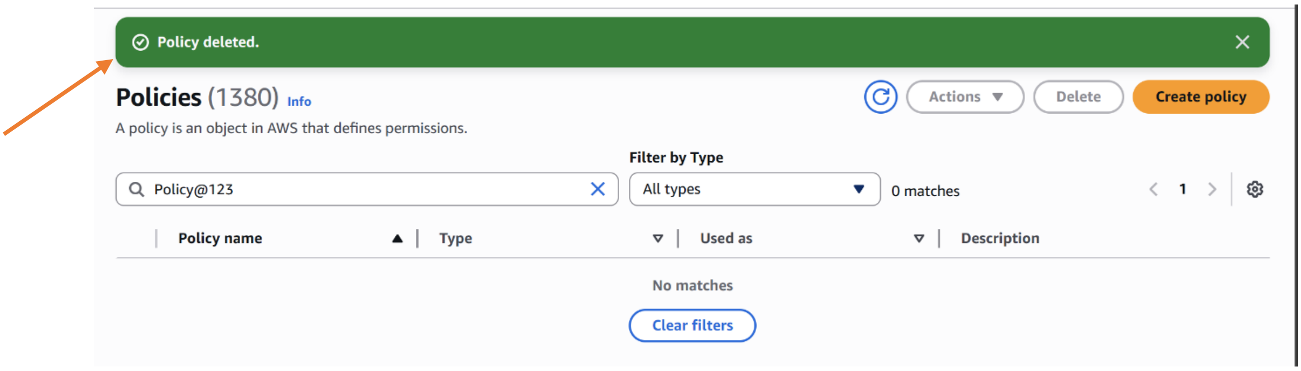
Delete **Policy@123** policy and all its versions permanently?

This action cannot be undone.

To confirm deletion, enter the policy name in the text input field.

Policy@123

- Policy is deleted



Policy deleted.

Policies (1380) Info

A policy is an object in AWS that defines permissions.

Policy@123 ✕ | All types ▼ | 0 matches

Policy name ▲	Type	Used as	Description

No matches