# Module 3: IAM Users Assignment

**SUBMITTED BY :-HITESH CHAUHAN**

**COURSES OFFERED:ADVANCED CLOUD COMPUTING AND DEVELOPS**

## Problem Statement:

You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

## Tasks To Be Performed:

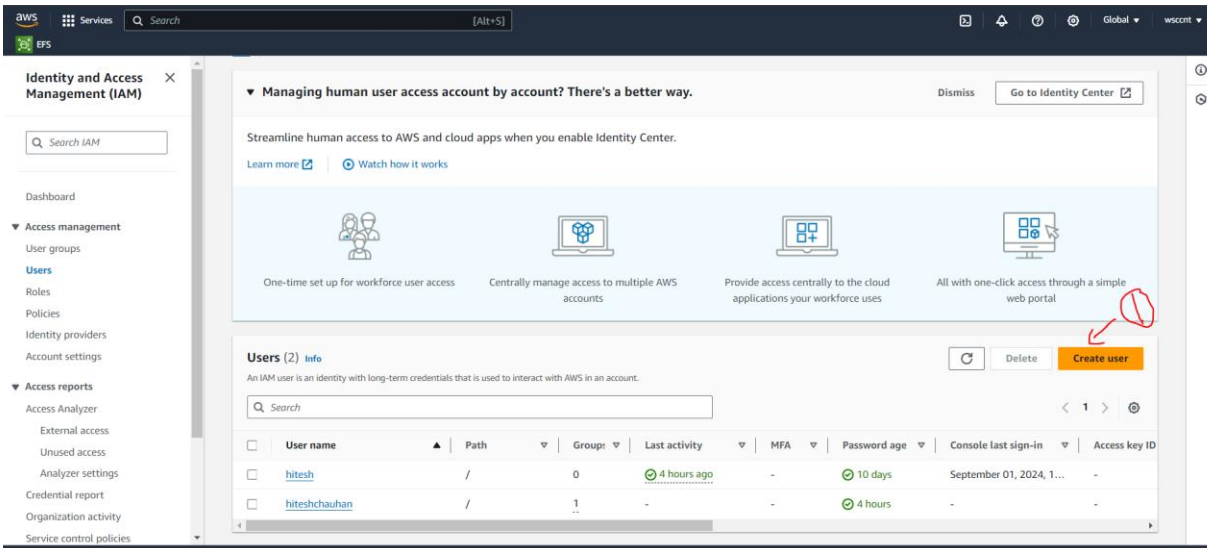
1. Create 4 IAM users named “Dev1”, “Dev2”, “Test1”, and “Test2”.

2. Create 2 groups named “Dev Team” and “Ops Team”.

3. Add Dev1 and Dev2 to the Dev Team.

4. Add Dev1, Test1 and Test2 to the Ops Team.

1. Create 4 IAM users named “Dev1”, “Dev2”, “Test1”, and “Test2”.



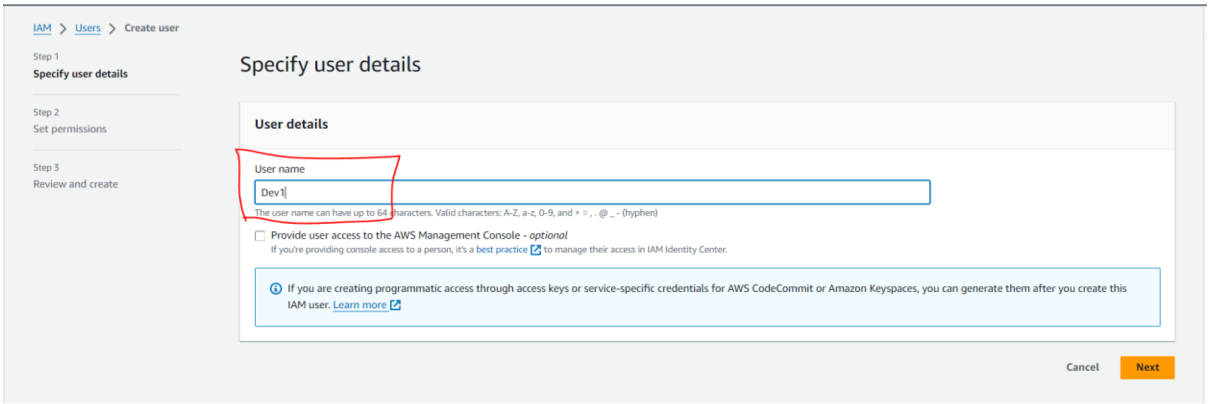
Managing human user access account by account? There's a better way.

Streamline human access to AWS and cloud apps when you enable Identity Center.

Users (2) 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 |
|---|---|---|---|---|---|---|---|
| hitesh | / | 0 | 4 hours ago | - | 10 days | September 01, 2024, 1... | - |
| hiteshchauhan | / | 1 | - | - | 4 hours | - | - |



IAM > Users > Create user

Step 1
**Specify user details**

Step 2
Set permissions

Step 3
Review and create

## Specify user details

**User details**

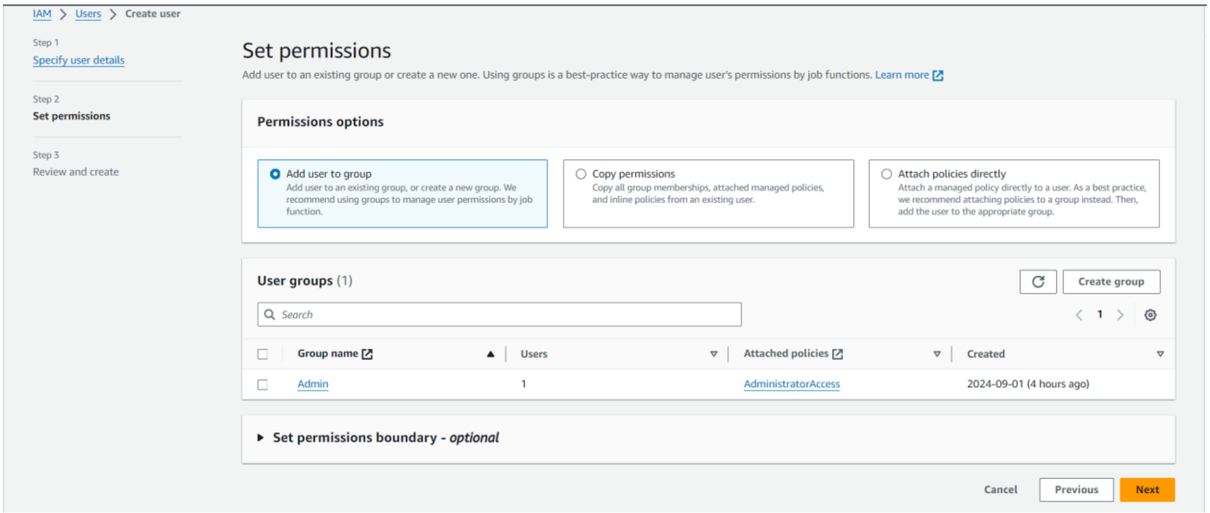
User name

Dev1

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



IAM > Users > Create user

Step 1
Specify user details

Step 2
**Set permissions**

Step 3
Review and create

## 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.

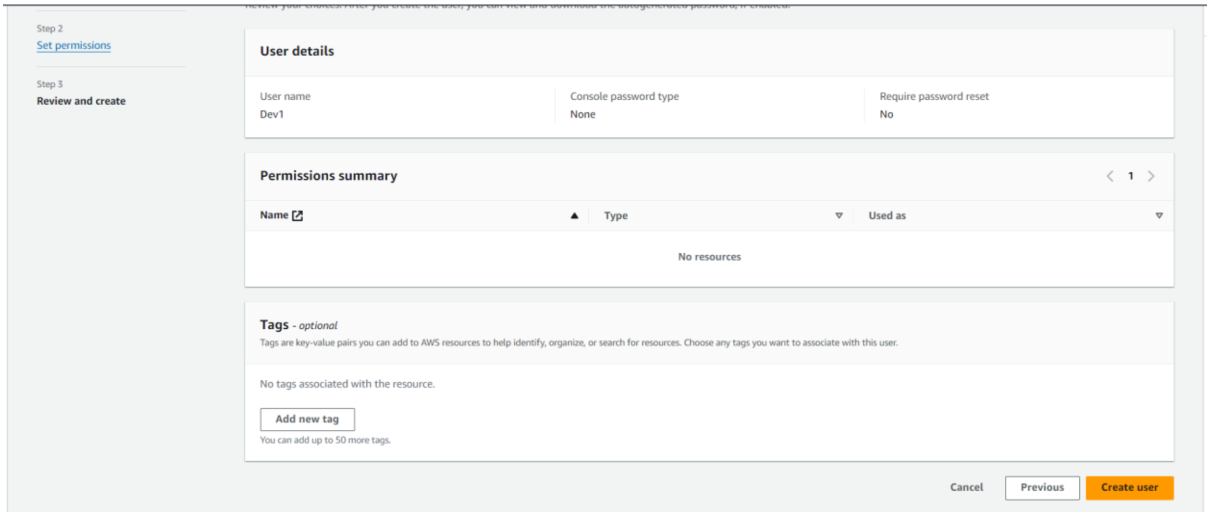
○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

○ 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)

| □ | Group name | Users | Attached policies | Created |
|---|---|---|---|---|
| □ | Admin | 1 | AdministratorAccess | 2024-09-01 (4 hours ago) |

▸ **Set permissions boundary - *optional***



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

Step 2
Set permissions

Step 3
**Review and create**

**User details**

| User name | Console password type | Require password reset |
|---|---|---|
| Dev1 | None | No |

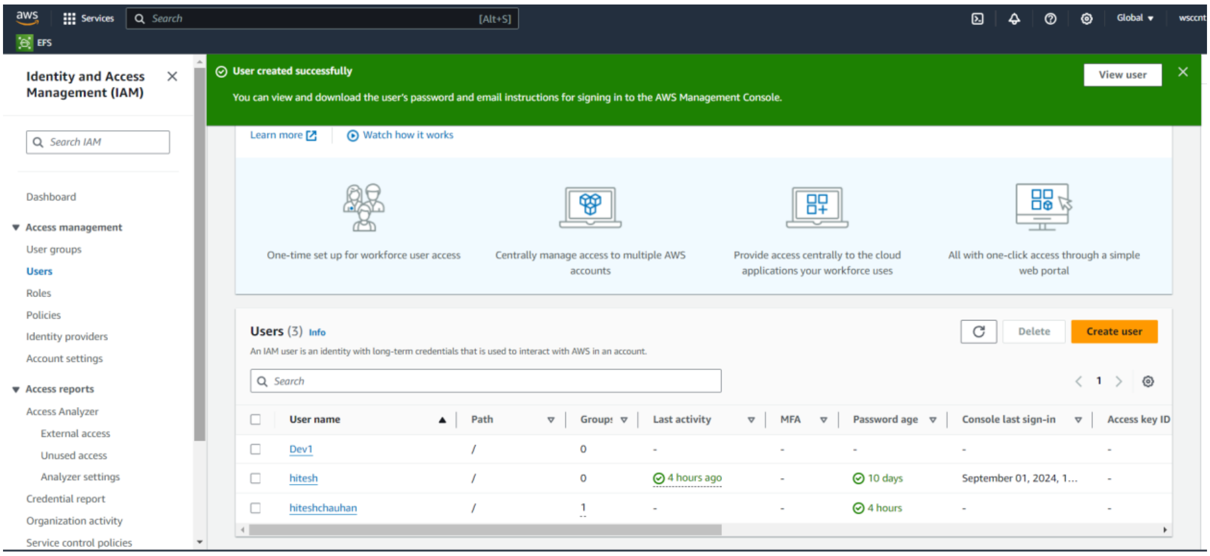
**Permissions summary**

| Name | Type | Used as |
|---|---|---|
| No resources | | |

**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.

You can add up to 50 more tags.



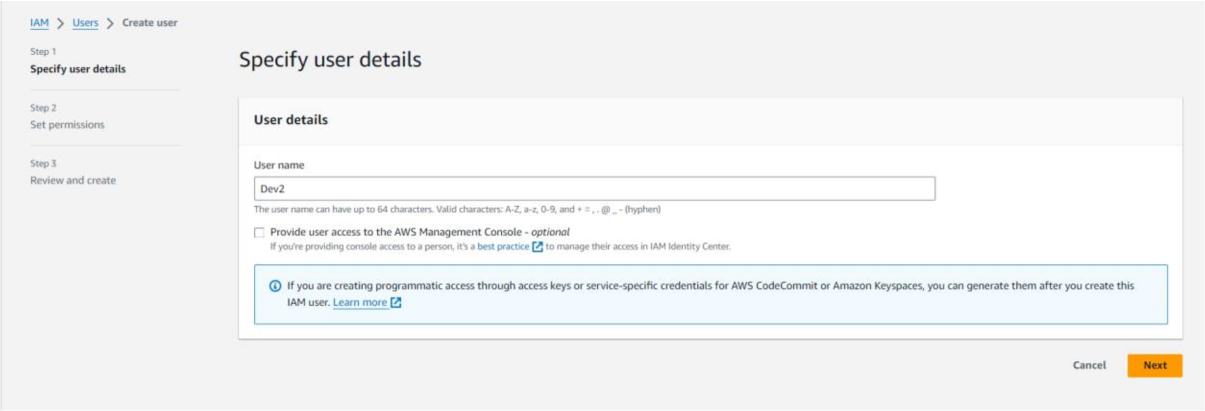
User created successfully

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

Users (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 | Group: | Last activity | MFA | Password age | Console last sign-in | Access key ID |
|---|---|---|---|---|---|---|---|---|
| □ | Dev1 | / | 0 | - | - | - | - | - |
| □ | hitesh | / | 0 | ✓ 4 hours ago | - | ✓ 10 days | September 01, 2024, 1... | - |
| □ | hiteshchauhan | / | 1 | - | - | ✓ 4 hours | - | - |



Specify user details

User details

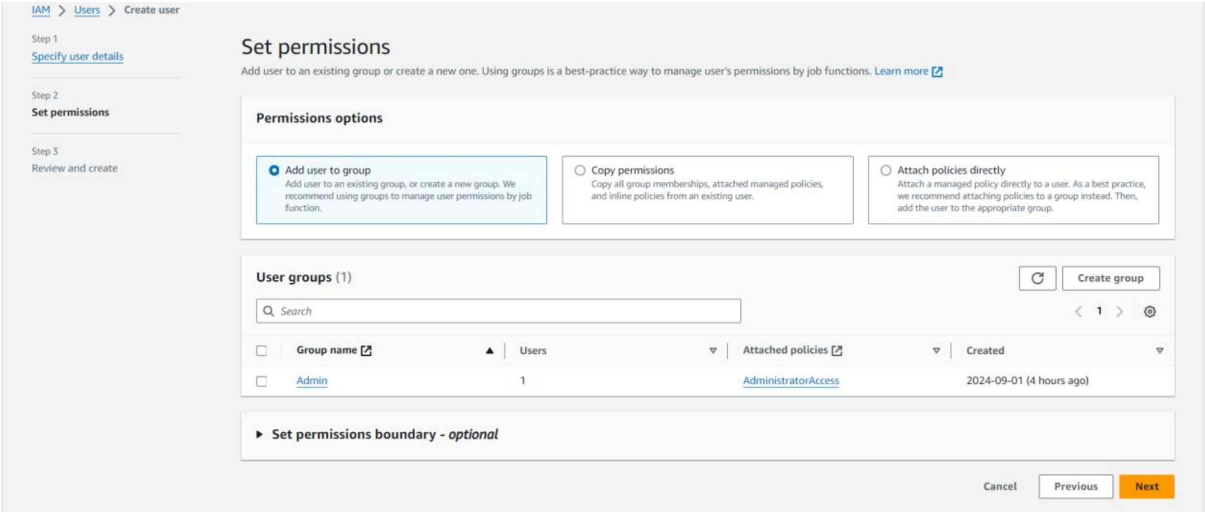
User name: Dev2

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



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.

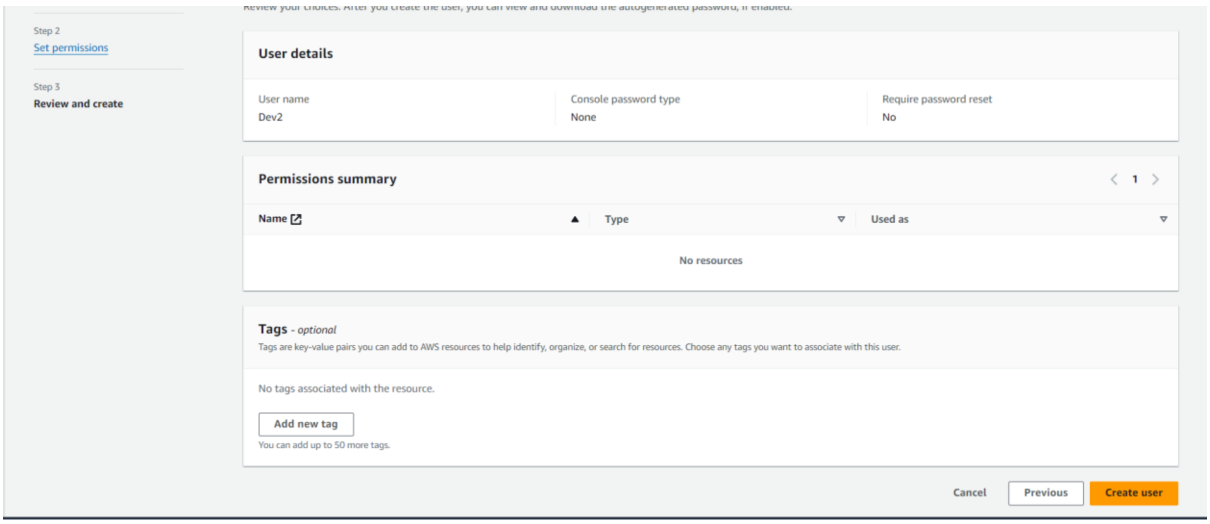
○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

○ 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)

| □ | Group name ▲ | Users | Attached policies | Created |
|---|---|---|---|---|
| □ | Admin | 1 | AdministratorAccess | 2024-09-01 (4 hours ago) |

▸ Set permissions boundary - *optional*



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

Step 2
Set permissions

Step 3
Review and create

**User details**

| User name | Console password type | Require password reset |
|---|---|---|
| Dev2 | None | No |

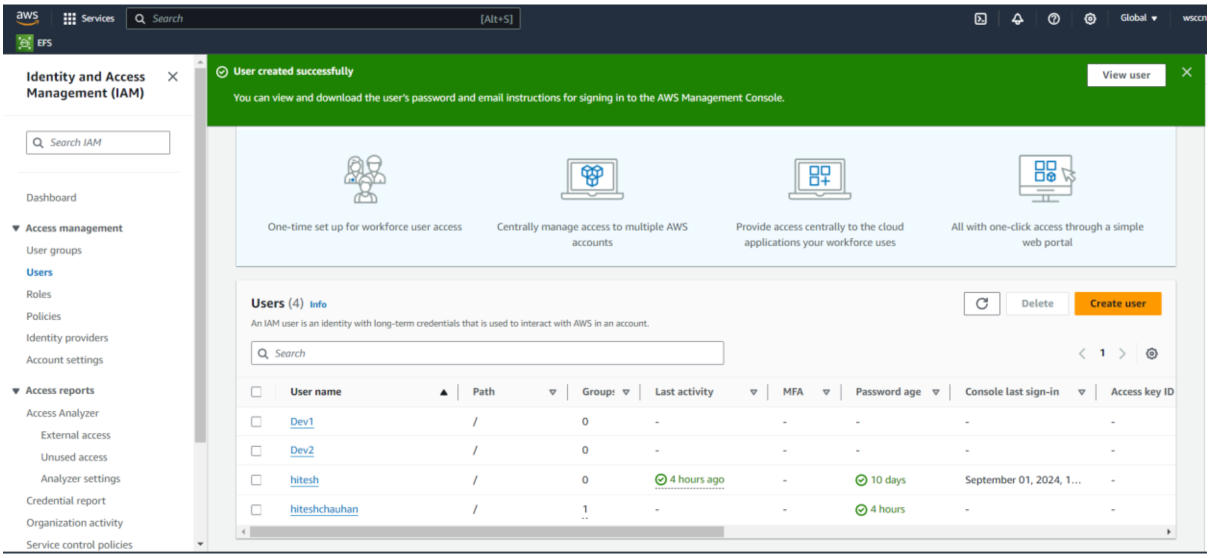
**Permissions summary**

| Name | Type | Used as |
|---|---|---|
| No resources | | |

**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.

You can add up to 50 more tags.

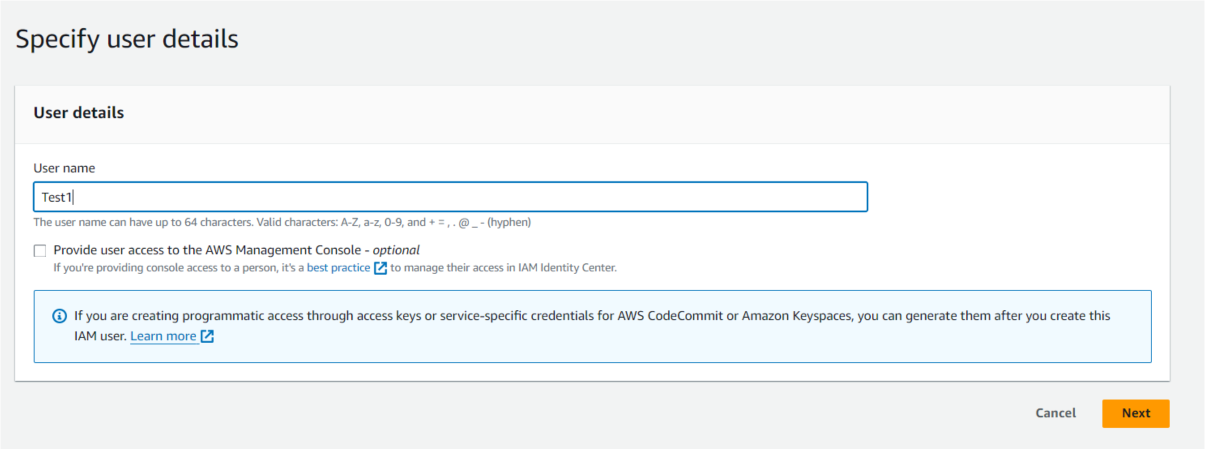


User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

View user
One-time set up for workforce user access
Centrally manage access to multiple AWS accounts
Provide access centrally to the cloud applications your workforce uses
All with one-click access through a simple web portal

**Users** (4) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

| □ | User name | Path | Group: | Last activity | MFA | Password age | Console last sign-in | Access key ID |
|---|---|---|---|---|---|---|---|---|
| □ | Dev1 | / | 0 | - | - | - | - | - |
| □ | Dev2 | / | 0 | - | - | - | - | - |
| □ | hitesh | / | 0 | ✓ 4 hours ago | - | ✓ 10 days | September 01, 2024, 1... | - |
| □ | hiteshchauhan | / | 1 | - | - | ✓ 4 hours | - | - |



## Specify user details

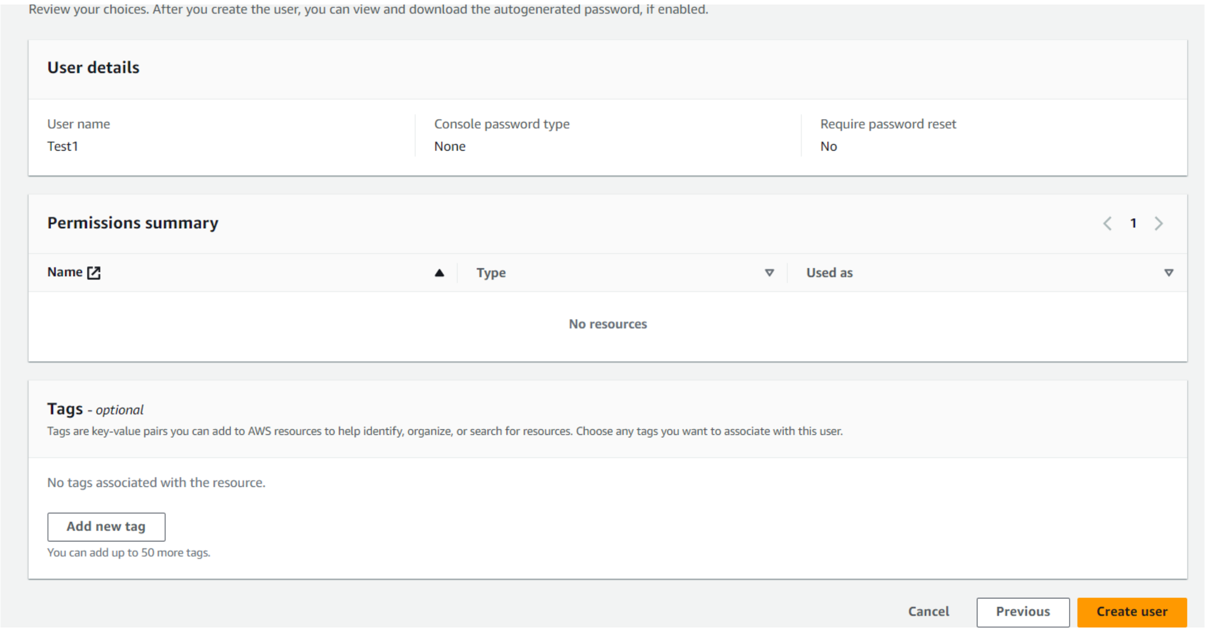
**User details**

User name
Test1

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



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 |
|---|---|---|
| Test1 | None | No |

**Permissions summary**

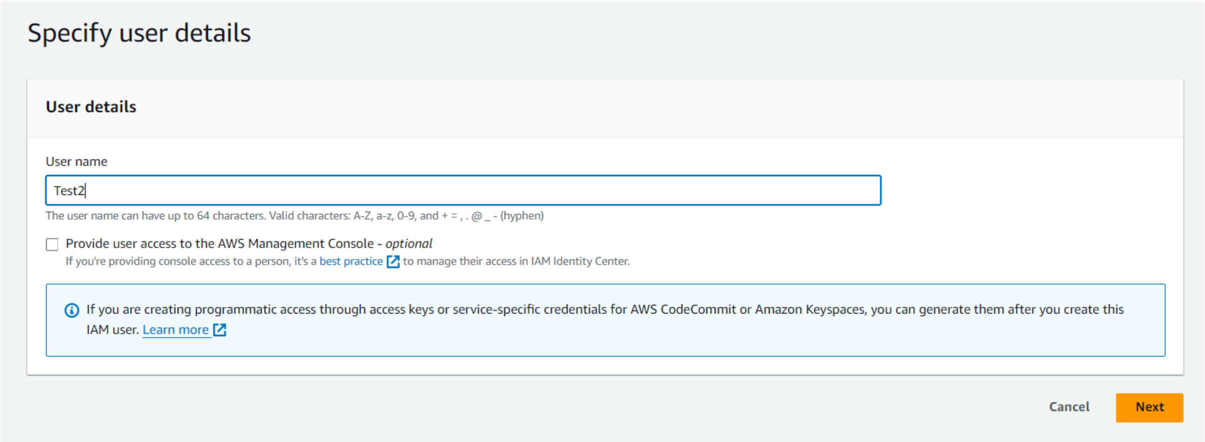
| Name | Type | Used as |
|---|---|---|
| No resources | | |

**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.

You can add up to 50 more tags.



## Specify user details

**User details**

User name

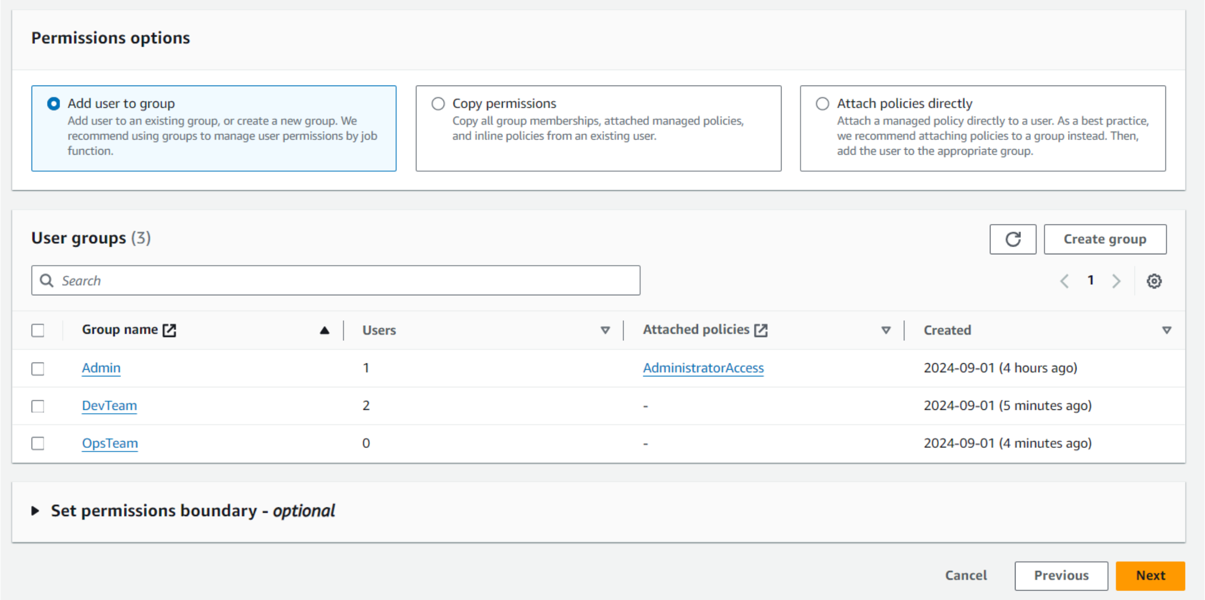
Test2

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



**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.

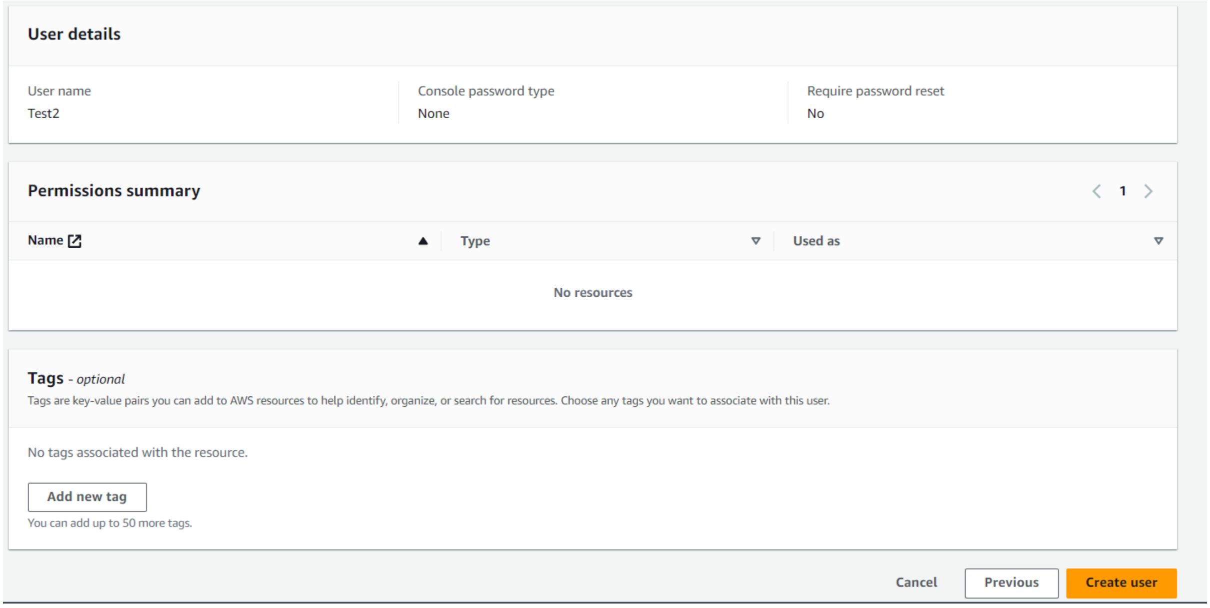
○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

○ 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** (3)

| □ | Group name | Users | Attached policies | Created |
|---|---|---|---|---|
| □ | Admin | 1 | AdministratorAccess | 2024-09-01 (4 hours ago) |
| □ | DevTeam | 2 | - | 2024-09-01 (5 minutes ago) |
| □ | OpsTeam | 0 | - | 2024-09-01 (4 minutes ago) |

▸ **Set permissions boundary - *optional***



**User details**

| User name | Console password type | Require password reset |
|---|---|---|
| Test2 | None | No |

**Permissions summary**

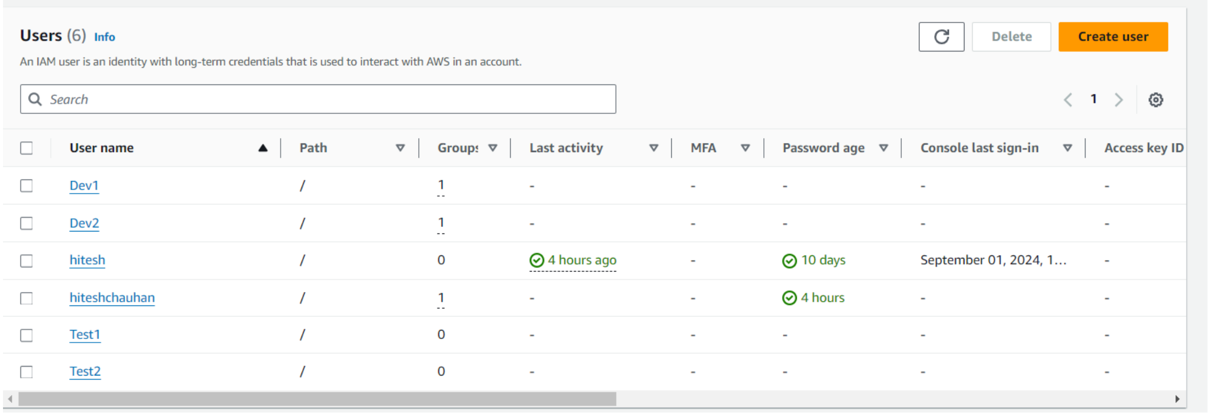
| Name | Type | Used as |
|---|---|---|
| No resources | | |

**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.

You can add up to 50 more tags.

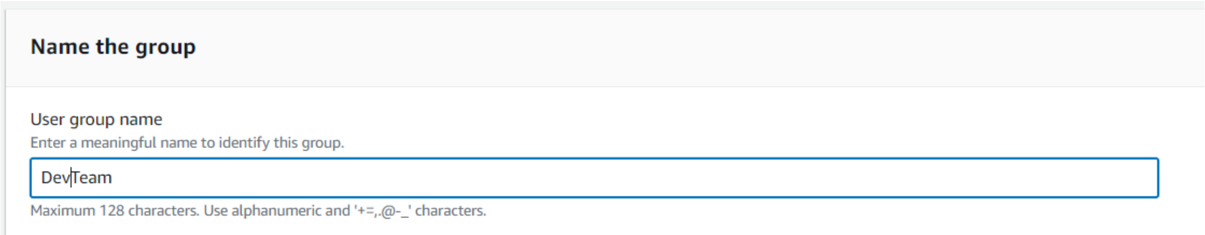


**Users** (6) Info

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 |
|---|---|---|---|---|---|---|---|---|
| □ | Dev1 | / | 1 | - | - | - | - | - |
| □ | Dev2 | / | 1 | - | - | - | - | - |
| □ | hitesh | / | 0 | ✓ 4 hours ago | - | ✓ 10 days | September 01, 2024, 1... | - |
| □ | hiteshchauhan | / | 1 | - | - | ✓ 4 hours | - | - |
| □ | Test1 | / | 0 | - | - | - | - | - |
| □ | Test2 | / | 0 | - | - | - | - | - |

2. Create 2 groups named “Dev Team” and “Ops Team”.



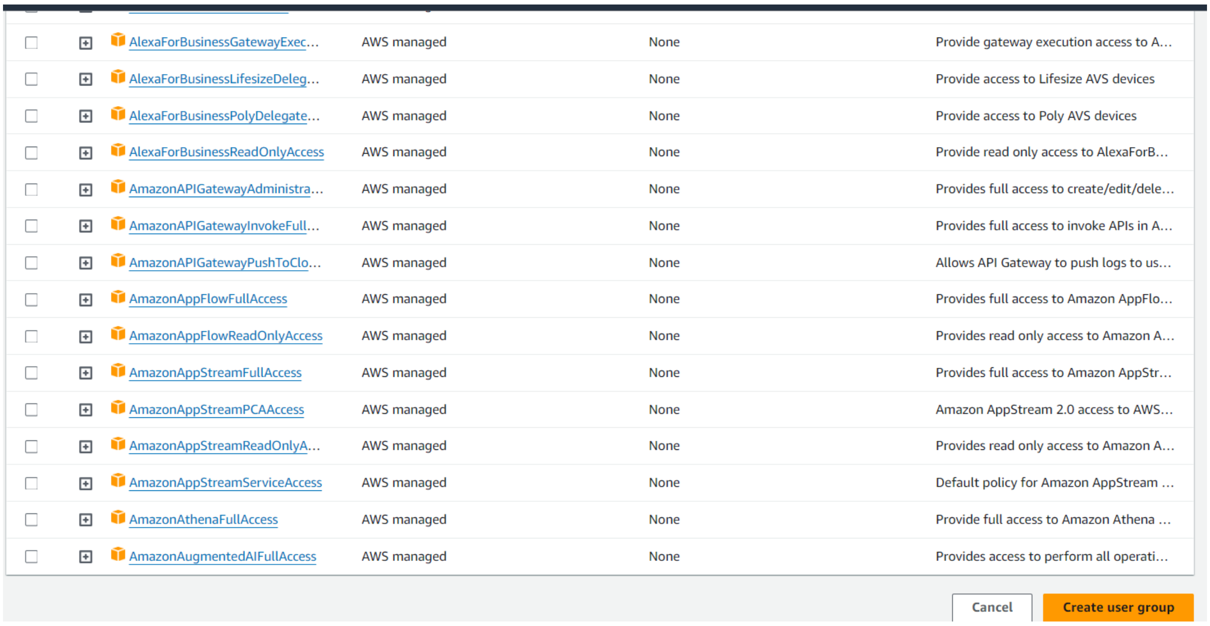
**Name the group**

User group name

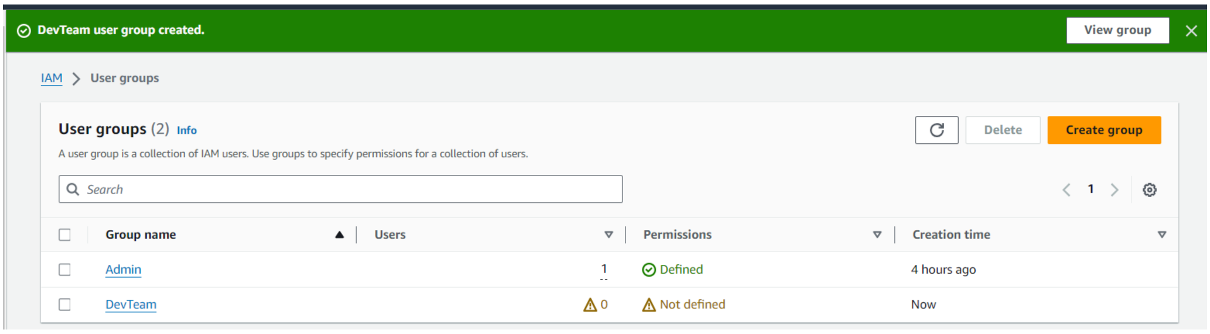
Enter a meaningful name to identify this group.

DevTeam

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



| | | | | | |
|---|---|---|---|---|---|
| □ | ⊞ | AlexaForBusinessGatewayExec… | AWS managed | None | Provide gateway execution access to A… |
| □ | ⊞ | AlexaForBusinessLifesizeDeleg… | AWS managed | None | Provide access to Lifesize AVS devices |
| □ | ⊞ | AlexaForBusinessPolyDelegate… | AWS managed | None | Provide access to Poly AVS devices |
| □ | ⊞ | AlexaForBusinessReadOnlyAccess | AWS managed | None | Provide read only access to AlexaForB… |
| □ | ⊞ | AmazonAPIGatewayAdministra… | AWS managed | None | Provides full access to create/edit/dele… |
| □ | ⊞ | AmazonAPIGatewayInvokeFull… | AWS managed | None | Provides full access to invoke APIs in A… |
| □ | ⊞ | AmazonAPIGatewayPushToClo… | AWS managed | None | Allows API Gateway to push logs to us… |
| □ | ⊞ | AmazonAppFlowFullAccess | AWS managed | None | Provides full access to Amazon AppFlo… |
| □ | ⊞ | AmazonAppFlowReadOnlyAccess | AWS managed | None | Provides read only access to Amazon A… |
| □ | ⊞ | AmazonAppStreamFullAccess | AWS managed | None | Provides full access to Amazon AppStr… |
| □ | ⊞ | AmazonAppStreamPCAAccess | AWS managed | None | Amazon AppStream 2.0 access to AWS… |
| □ | ⊞ | AmazonAppStreamReadOnlyA… | AWS managed | None | Provides read only access to Amazon A… |
| □ | ⊞ | AmazonAppStreamServiceAccess | AWS managed | None | Default policy for Amazon AppStream … |
| □ | ⊞ | AmazonAthenaFullAccess | AWS managed | None | Provide full access to Amazon Athena … |
| □ | ⊞ | AmazonAugmentedAIFullAccess | AWS managed | None | Provides access to perform all operati… |

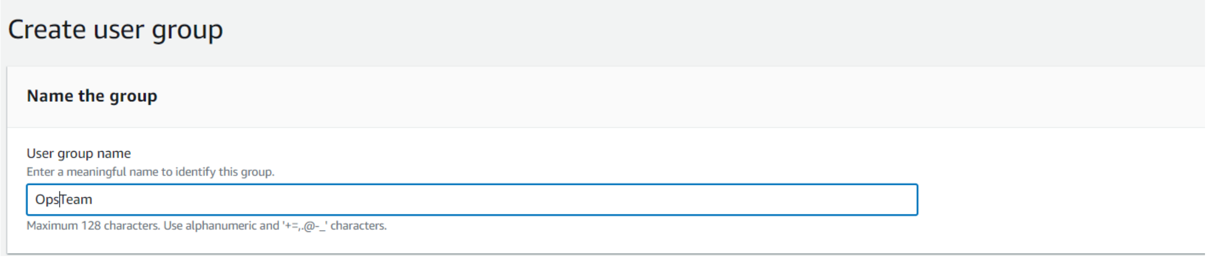


DevTeam user group created.

**User groups** (2) 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 |
|---|---|---|---|---|
| □ | Admin | 1 | ✓ Defined | 4 hours ago |
| □ | DevTeam | ⚠ 0 | ⚠ Not defined | Now |



# Create user group

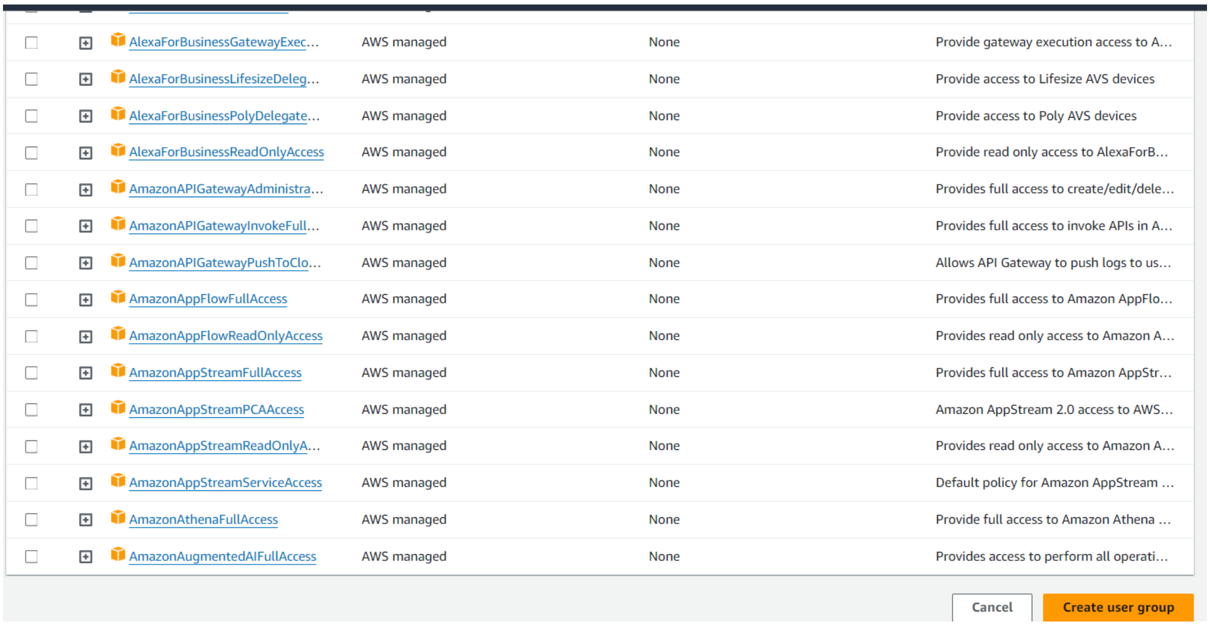
## Name the group

User group name

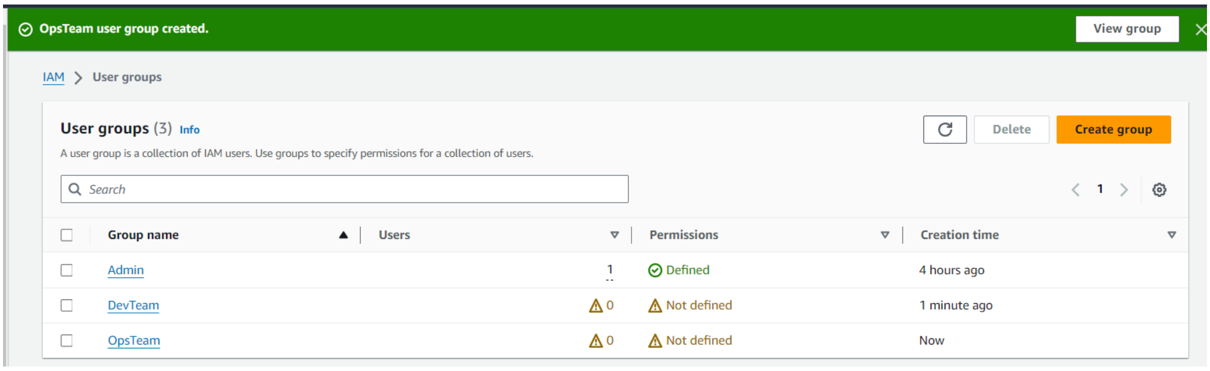
Enter a meaningful name to identify this group.

OpsTeam

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



| | | | | |
|---|---|---|---|---|
| □ | AlexaForBusinessGatewayExec… | AWS managed | None | Provide gateway execution access to A… |
| □ | AlexaForBusinessLifesizeDeleg… | AWS managed | None | Provide access to Lifesize AVS devices |
| □ | AlexaForBusinessPolyDelegate… | AWS managed | None | Provide access to Poly AVS devices |
| □ | AlexaForBusinessReadOnlyAccess | AWS managed | None | Provide read only access to AlexaForB… |
| □ | AmazonAPIGatewayAdministra… | AWS managed | None | Provides full access to create/edit/dele… |
| □ | AmazonAPIGatewayInvokeFull… | AWS managed | None | Provides full access to invoke APIs in A… |
| □ | AmazonAPIGatewayPushToClo… | AWS managed | None | Allows API Gateway to push logs to us… |
| □ | AmazonAppFlowFullAccess | AWS managed | None | Provides full access to Amazon AppFlo… |
| □ | AmazonAppFlowReadOnlyAccess | AWS managed | None | Provides read only access to Amazon A… |
| □ | AmazonAppStreamFullAccess | AWS managed | None | Provides full access to Amazon AppStr… |
| □ | AmazonAppStreamPCAAccess | AWS managed | None | Amazon AppStream 2.0 access to AWS… |
| □ | AmazonAppStreamReadOnlyA… | AWS managed | None | Provides read only access to Amazon A… |
| □ | AmazonAppStreamServiceAccess | AWS managed | None | Default policy for Amazon AppStream … |
| □ | AmazonAthenaFullAccess | AWS managed | None | Provide full access to Amazon Athena … |
| □ | AmazonAugmentedAIFullAccess | AWS managed | None | Provides access to perform all operati… |



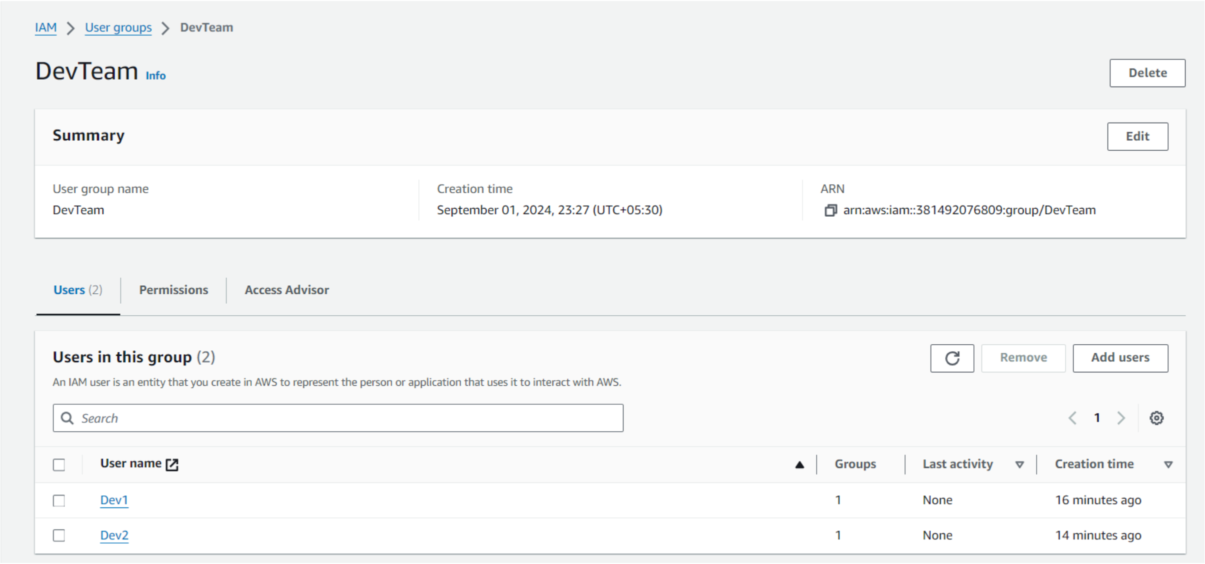
OpsTeam user group created.

**User groups** (3) 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 |
|---|---|---|---|---|
| □ | Admin | 1 | ✓ Defined | 4 hours ago |
| □ | DevTeam | ⚠ 0 | ⚠ Not defined | 1 minute ago |
| □ | OpsTeam | ⚠ 0 | ⚠ Not defined | Now |

3. Add Dev1 and Dev2 to the Dev Team.



DevTeam Info

**Summary**

User group name: DevTeam

Creation time: September 01, 2024, 23:27 (UTC+05:30)

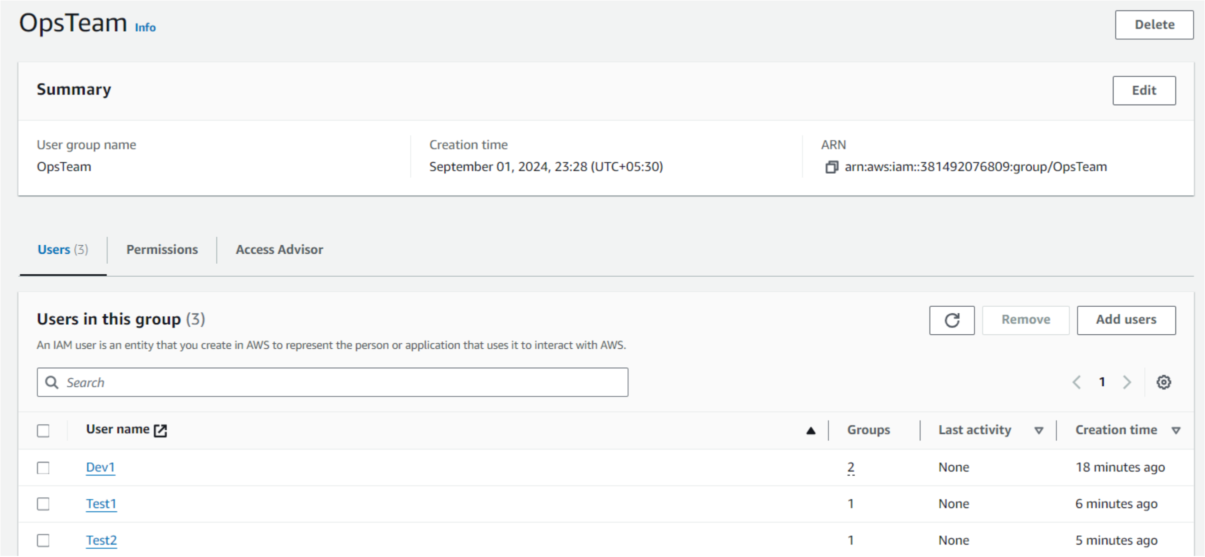
ARN: arn:aws:iam::381492076809:group/DevTeam

**Users in this group** (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 |
|---|---|---|---|---|
| □ | Dev1 | 1 | None | 16 minutes ago |
| □ | Dev2 | 1 | None | 14 minutes ago |

4. Add Dev1, Test1 and Test2 to the Ops Team.



User group name
OpsTeam

Creation time
September 01, 2024, 23:28 (UTC+05:30)

ARN
arn:aws:iam::381492076809:group/OpsTeam

Users in this group (3)

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 |
|---|---|---|---|---|
| □ | Dev1 | 2 | None | 18 minutes ago |
| □ | Test1 | 1 | None | 6 minutes ago |
| □ | Test2 | 1 | None | 5 minutes ago |