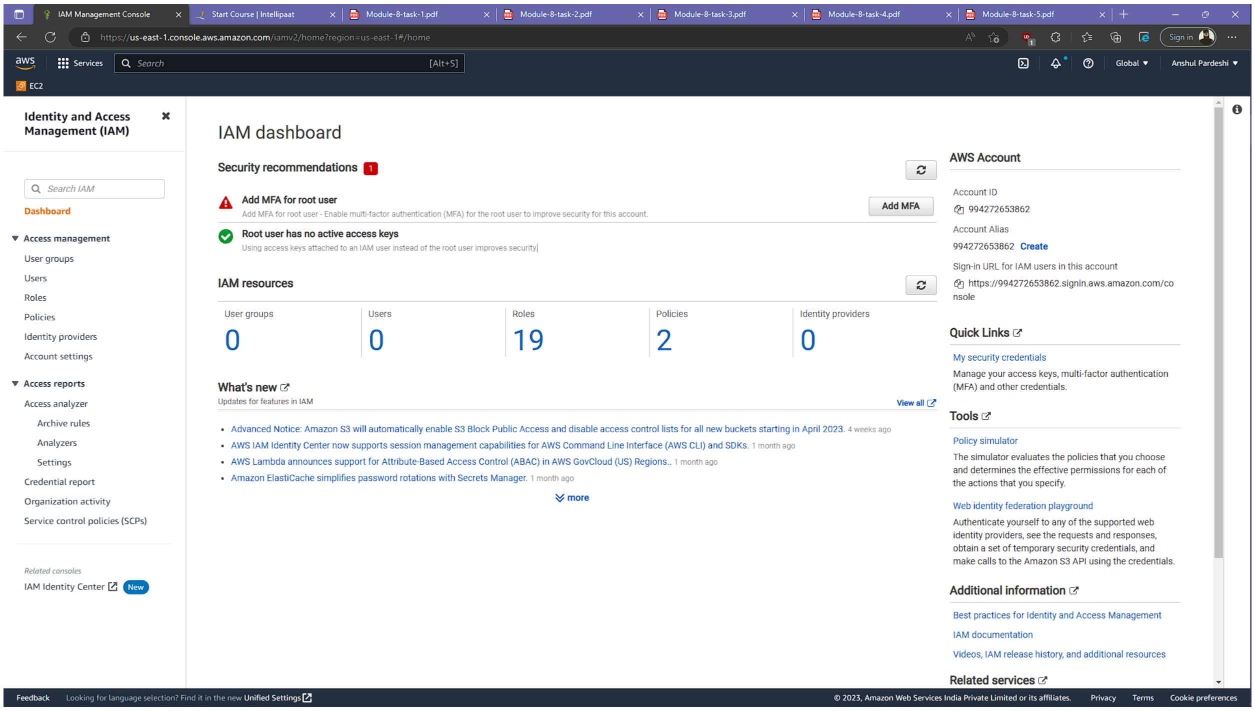
Module-8: IAM Assignment - 1

You have been asked to:

1. Create 4 IAM users named “user1”, “user2”, “user3”, and “user4” .
2. Create 2 Groups named “Dev Team” and “Ops Team” .
3. Add user1 and user2 to the Dev Team.
4. Add user1, user3 and user4 to the Ops team.

Go to the IAM dashboard.



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	19	2	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. 4 weeks ago
- AWS IAM Identity Center now supports session management capabilities for AWS Command Line Interface (AWS CLI) and SDKs. 1 month ago
- AWS Lambda announces support for Attribute-Based Access Control (ABAC) in AWS GovCloud (US) Regions.. 1 month ago
- Amazon ElastiCache simplifies password rotations with Secrets Manager. 1 month ago

more

AWS Account

Account ID
994272653862

Account Alias
994272653862 Create

Sign-in URL for IAM users in this account
https://994272653862.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.

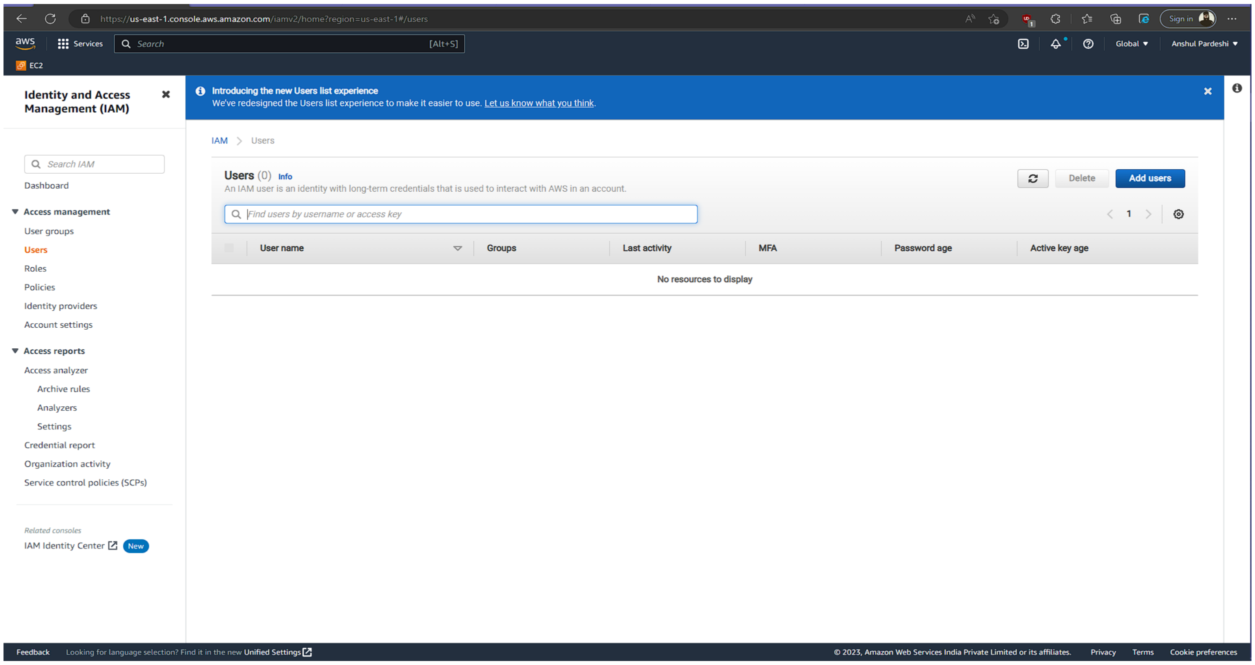
Web identity federation playground
Authenticate yourself to any of the supported web identity providers, see the requests and responses, obtain a set of temporary security credentials, and make calls to the Amazon S3 API using the credentials.

Additional information

Best practices for Identity and Access Management
IAM documentation
Videos, IAM release history, and additional resources

Related services

Click on users then add users.



Introducing the new Users list experience
We've redesigned the Users list experience to make it easier to use. Let us know what you think.

IAM > Users

Users (0) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

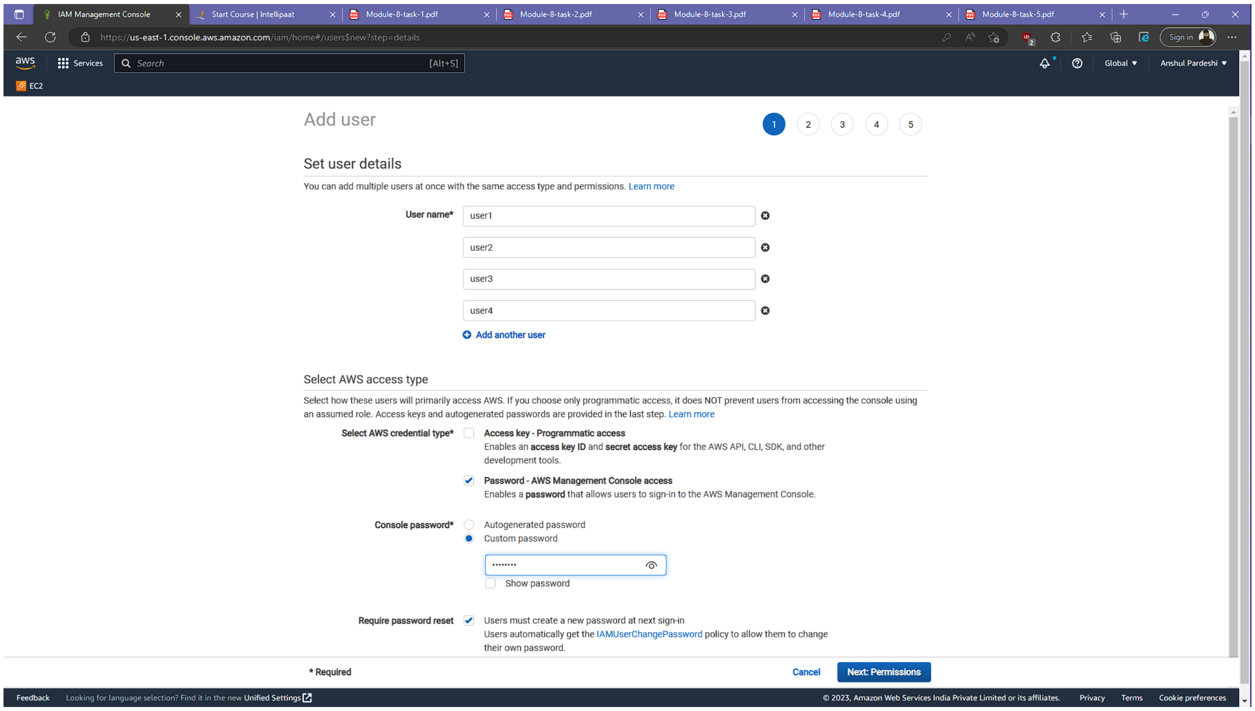
Delete
Add users

Find users by username or access key

User name	Groups	Last activity	MFA	Password age	Active key age

No resources to display

Name them as mentioned above in the statement. Assign password for their first login then user will reset according to them.



Add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* user1

user2

user3

user4

Add another user

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

Select AWS credential type* □ **Access key - Programmatic access** Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☑ **Password - AWS Management Console access** Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ○ Autogenerated password
● Custom password

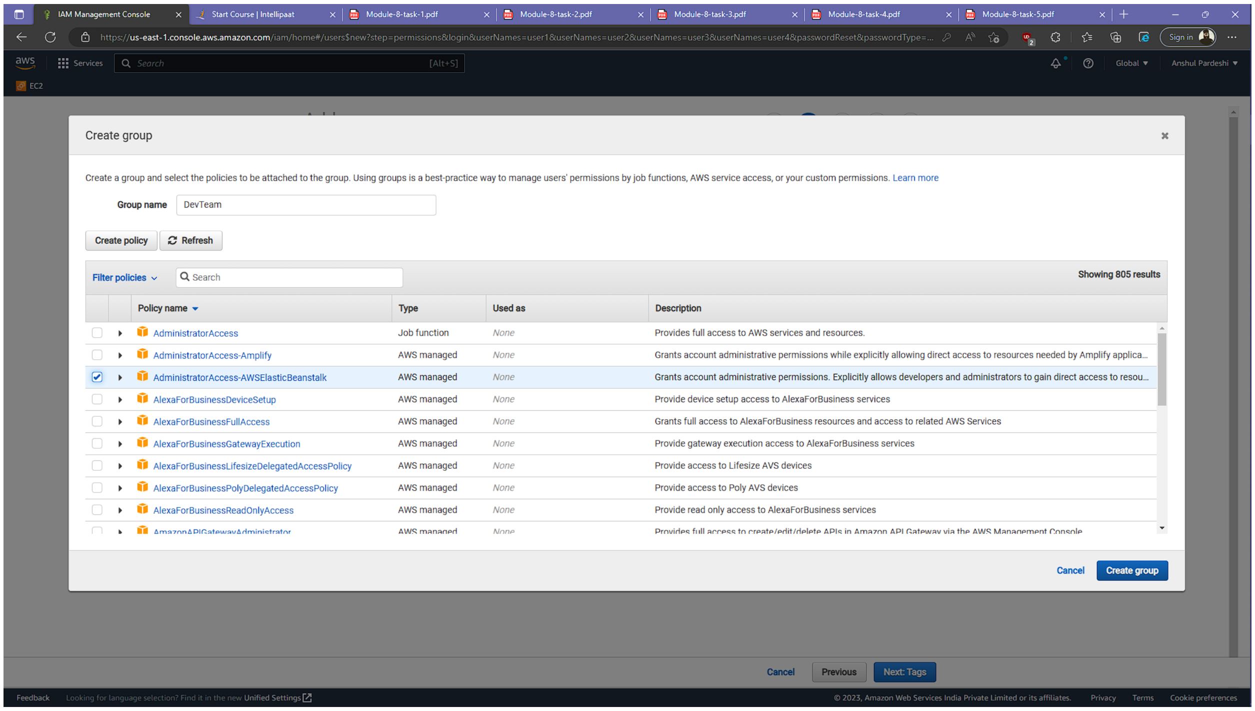
••••••••

□ Show password

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

* Required

Create Group. Name the first one as DevTeam.



Create group

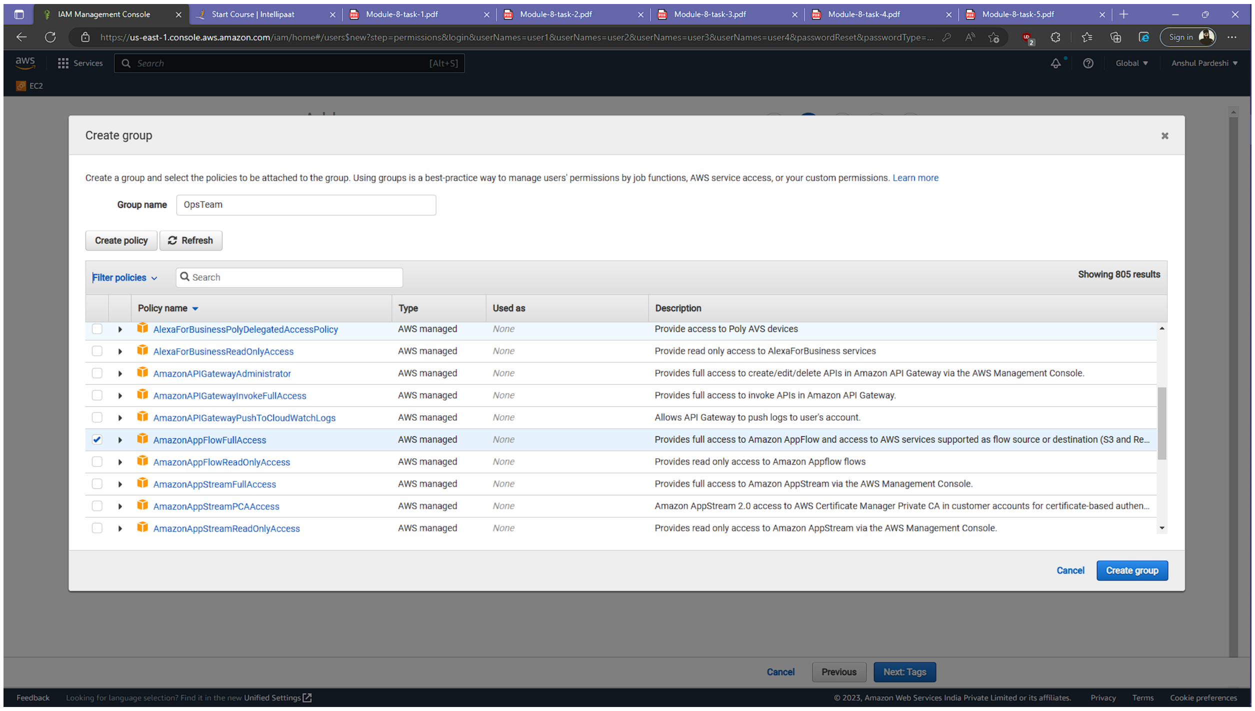
Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Learn more

Group name DevTeam

Showing 805 results

	Policy name	Type	Used as	Description
□	AdministratorAccess	Job function	None	Provides full access to AWS services and resources.
□	AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissions while explicitly allowing direct access to resources needed by Amplify applica...
☑	AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permissions. Explicitly allows developers and administrators to gain direct access to resou...
□	AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaForBusiness services
□	AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness resources and access to related AWS Services
□	AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to AlexaForBusiness services
□	AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS managed	None	Provide access to Lifesize AVS devices
□	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None	Provide access to Poly AVS devices
□	AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForBusiness services
□	AmazonAPIGatewayAdministrator	AWS managed	None	Provides full access to create/edit/delete APIs in Amazon API Gateway via the AWS Management Console

Second group with OpsTeam.



Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Learn more

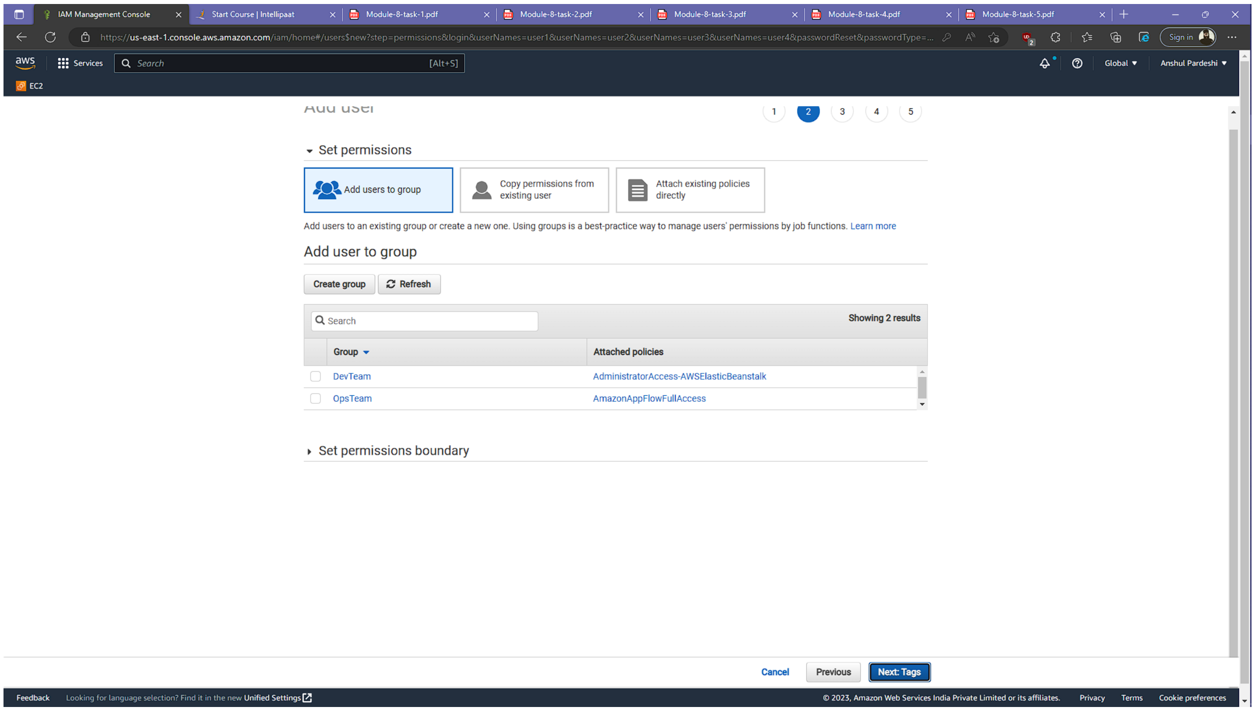
Group name: OpsTeam

Showing 805 results

	Policy name	Type	Used as	Description
□	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None	Provide access to Poly AVS devices
□	AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForBusiness services
□	AmazonAPIGatewayAdministrator	AWS managed	None	Provides full access to create/edit/delete APIs in Amazon API Gateway via the AWS Management Console.
□	AmazonAPIGatewayInvokeFullAccess	AWS managed	None	Provides full access to invoke APIs in Amazon API Gateway.
□	AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	None	Allows API Gateway to push logs to user's account.
☑	AmazonAppFlowFullAccess	AWS managed	None	Provides full access to Amazon AppFlow and access to AWS services supported as flow source or destination (S3 and Re...
□	AmazonAppFlowReadOnlyAccess	AWS managed	None	Provides read only access to Amazon Appflow flows
□	AmazonAppStreamFullAccess	AWS managed	None	Provides full access to Amazon AppStream via the AWS Management Console.
□	AmazonAppStreamPCAAccess	AWS managed	None	Amazon AppStream 2.0 access to AWS Certificate Manager Private CA in customer accounts for certificate-based authen...
□	AmazonAppStreamReadOnlyAccess	AWS managed	None	Provides read only access to Amazon AppStream via the AWS Management Console.

IAM Management Console
https://us-east-1.console.aws.amazon.com/iam/home#/users$new?step=permissions&login&userNames=user1&userNames=user2&userNames=user3&userNames=user4&passwordReset&passwordType=...
Services
Search
Global
Anshul Pardeshi
EC2
Create policy
Refresh
Filter policies
Search
Cancel
Create group
Cancel
Previous
Next: Tags
Feedback
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

Groups has been created.



Add user

Set permissions

Add users to group | Copy permissions from existing user | Attach existing policies directly

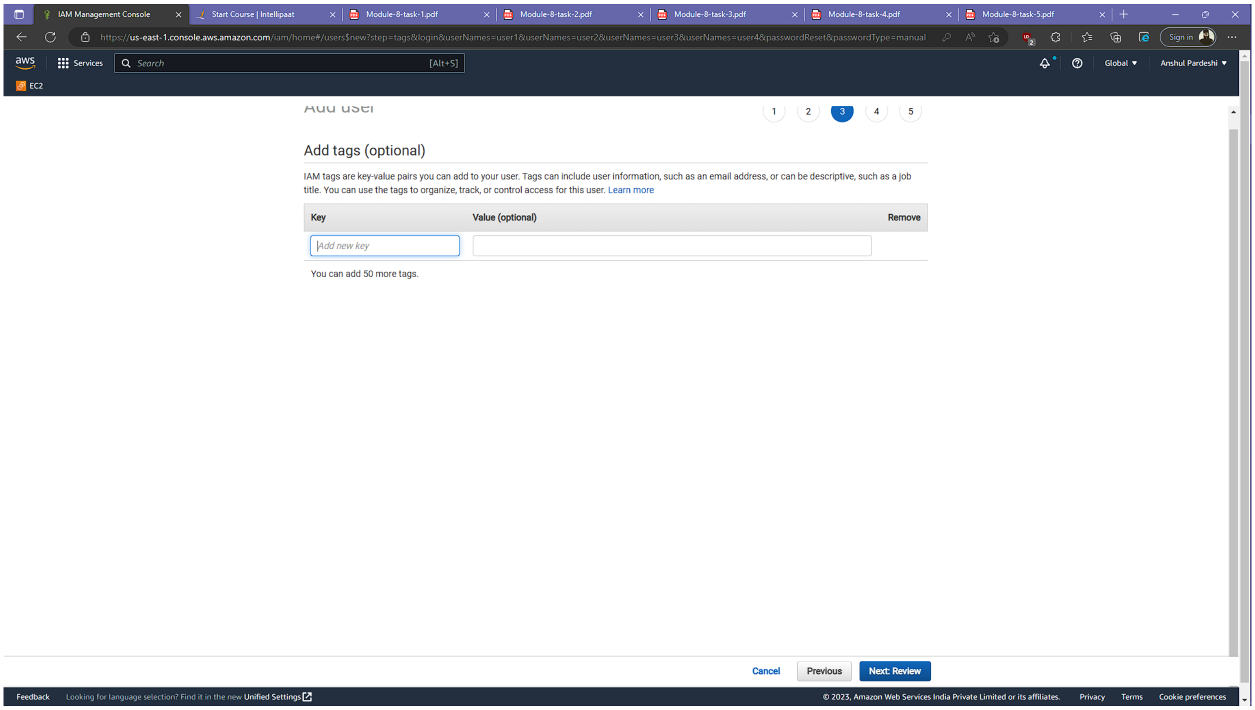
Add users to an existing group or create a new one. Using groups is a best-practice way to manage users' permissions by job functions. Learn more

Add user to group

Showing 2 results

	Group	Attached policies
□	DevTeam	AdministratorAccess-AWSElasticBeanstalk
□	OpsTeam	AmazonAppFlowFullAccess

Set permissions boundary


IAM Management Console
Start Course | Intellipaat
Module-8-task-1.pdf
Module-8-task-2.pdf
Module-8-task-3.pdf
Module-8-task-4.pdf
Module-8-task-5.pdf
https://us-east-1.console.aws.amazon.com/iam/home#/users$new?step=tags&login&userNames=user1&userNames=user2&userNames=user3&userNames=user4&passwordReset&passwordType=manual
Sign in
aws
Services
Search
[Alt+S]
Global
Anshul Pardeshi
EC2
Add user
1
2
3
4
5

Add tags (optional)

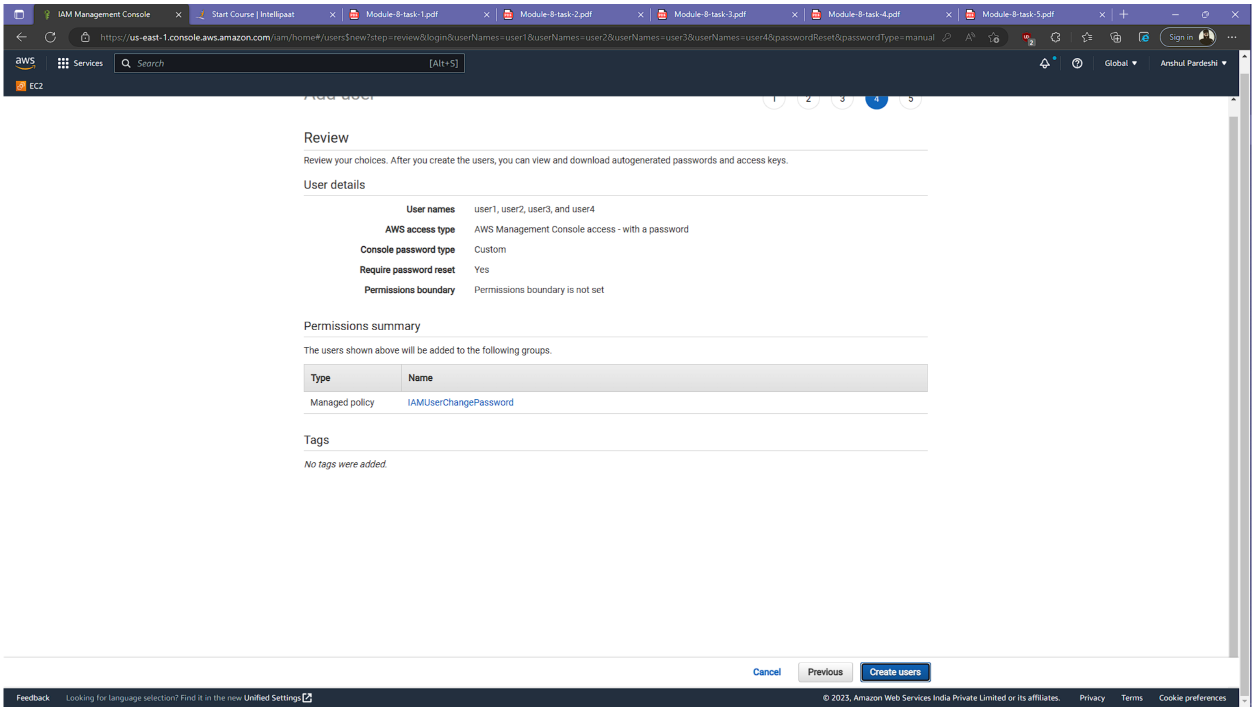
IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. Learn more

Key	Value (optional)	Remove
Add new key		

You can add 50 more tags.

Cancel
Previous
Next: Review
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

Users has been created.


IAM Management Console
Start Course | Intellipaat
Module-8-task-1.pdf
Module-8-task-2.pdf
Module-8-task-3.pdf
Module-8-task-4.pdf
Module-8-task-5.pdf
https://us-east-1.console.aws.amazon.com/iam/home#/users$new?step=review&login&userNames=user1&userNames=user2&userNames=user3&userNames=user4&passwordReset&passwordType=manual
Sign in
aws
Services
Search
[Alt+S]
Global
Anshul Pardeshi
EC2
Add user
1
2
3
4
5

Review

Review your choices. After you create the users, you can view and download autogenerated passwords and access keys.

User details

User names	user1, user2, user3, and user4
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The users shown above will be added to the following groups.

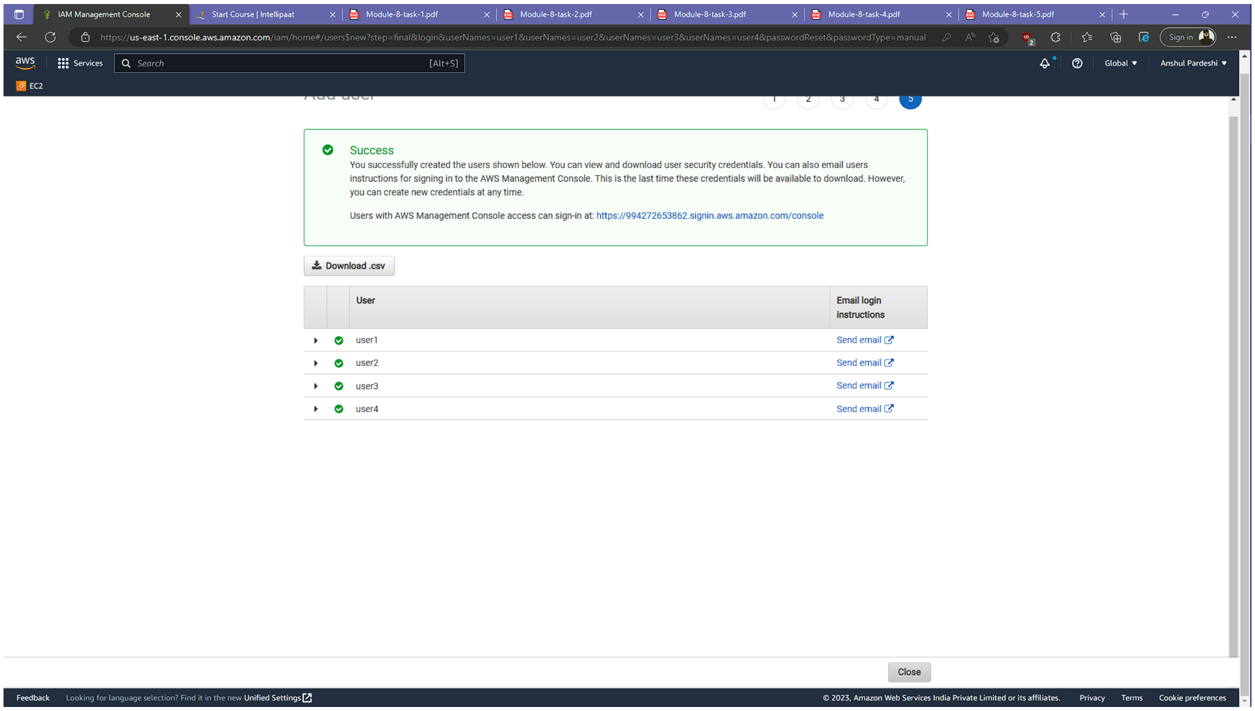
Type	Name
Managed policy	IAMUserChangePassword

Tags

No tags were added.

Cancel
Previous
Create users
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

These are the users.



Success

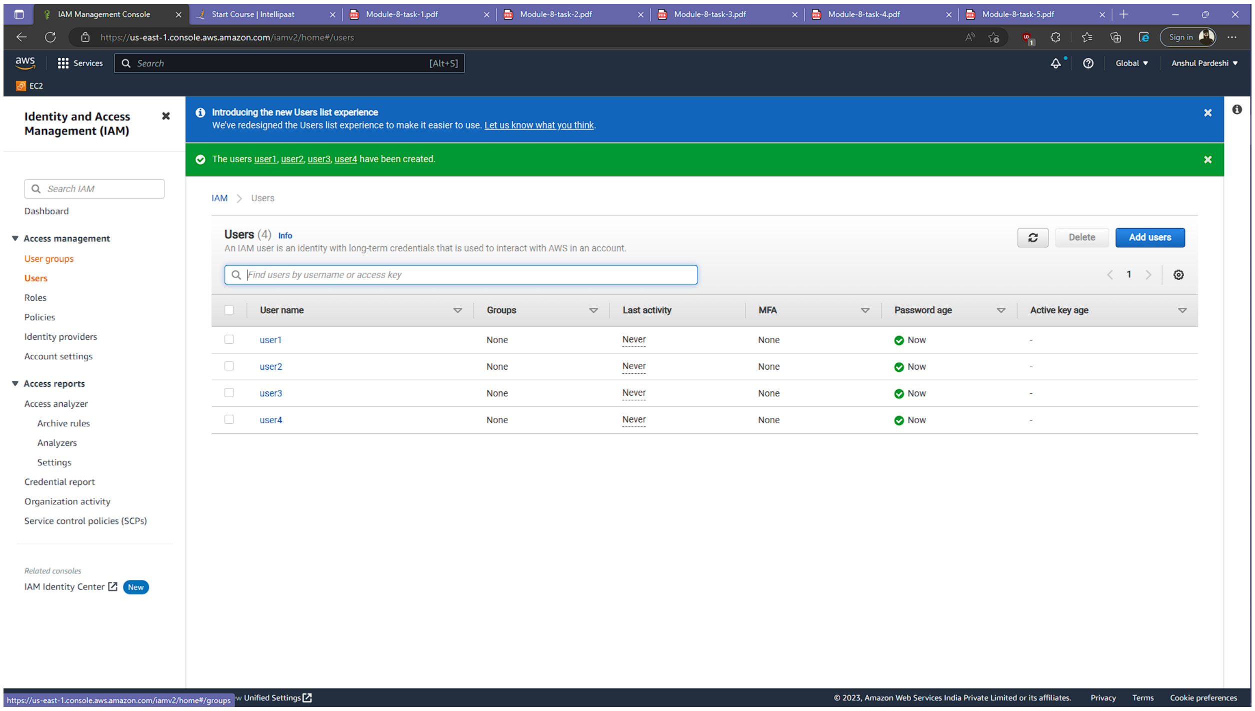
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://994272653862.signin.aws.amazon.com/console

User	Email login instructions
user1	Send email
user2	Send email
user3	Send email
user4	Send email

IAM Management Console
Start Course | Intellipaat
Module-8-task-1.pdf
Module-8-task-2.pdf
Module-8-task-3.pdf
Module-8-task-4.pdf
Module-8-task-5.pdf
https://us-east-1.console.aws.amazon.com/iam/home#/users$new?step=final&login&userNames=user1&userNames=user2&userNames=user3&userNames=user4&passwordReset&passwordType=manual
Sign in
Services
Search
[Alt+S]
Global
Anshul Pardeshi
EC2
Download .csv
Close
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

Go to user groups.



Introducing the new Users list experience

We've redesigned the Users list experience to make it easier to use. Let us know what you think.

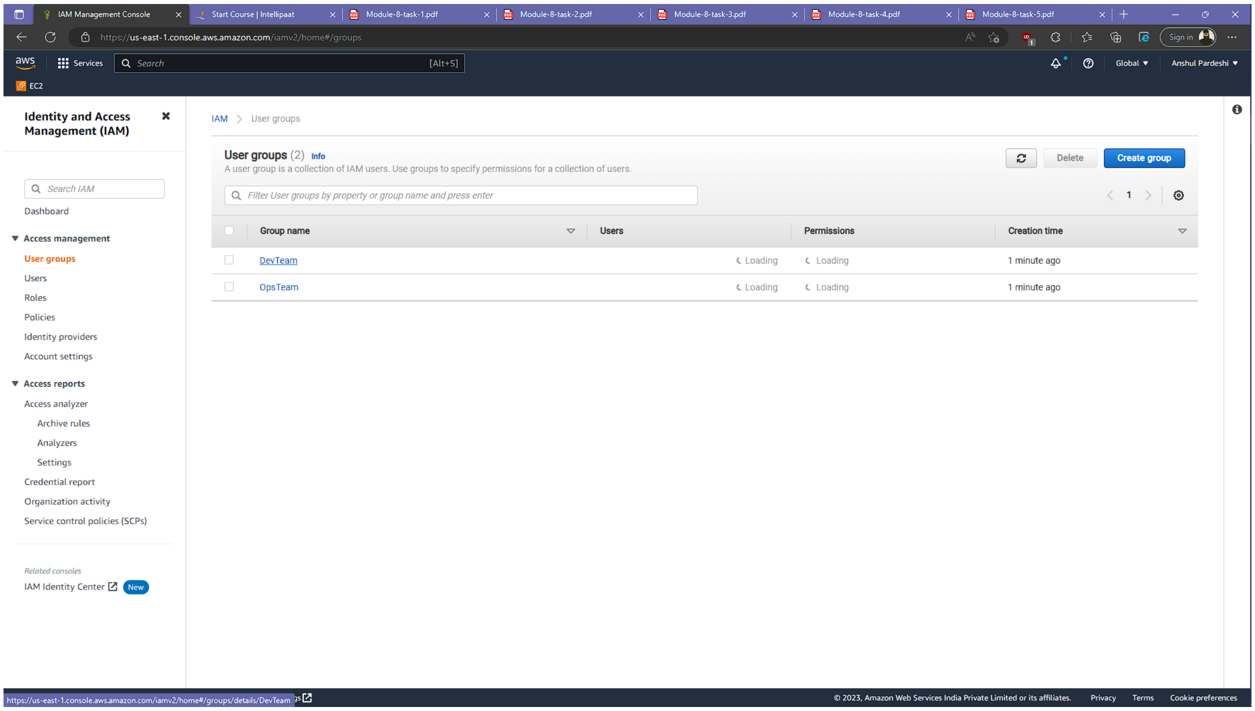
The users user1, user2, user3, user4 have been created.

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	Groups	Last activity	MFA	Password age	Active key age
user1	None	Never	None	✓ Now	-
user2	None	Never	None	✓ Now	-
user3	None	Never	None	✓ Now	-
user4	None	Never	None	✓ Now	-

Select the group.

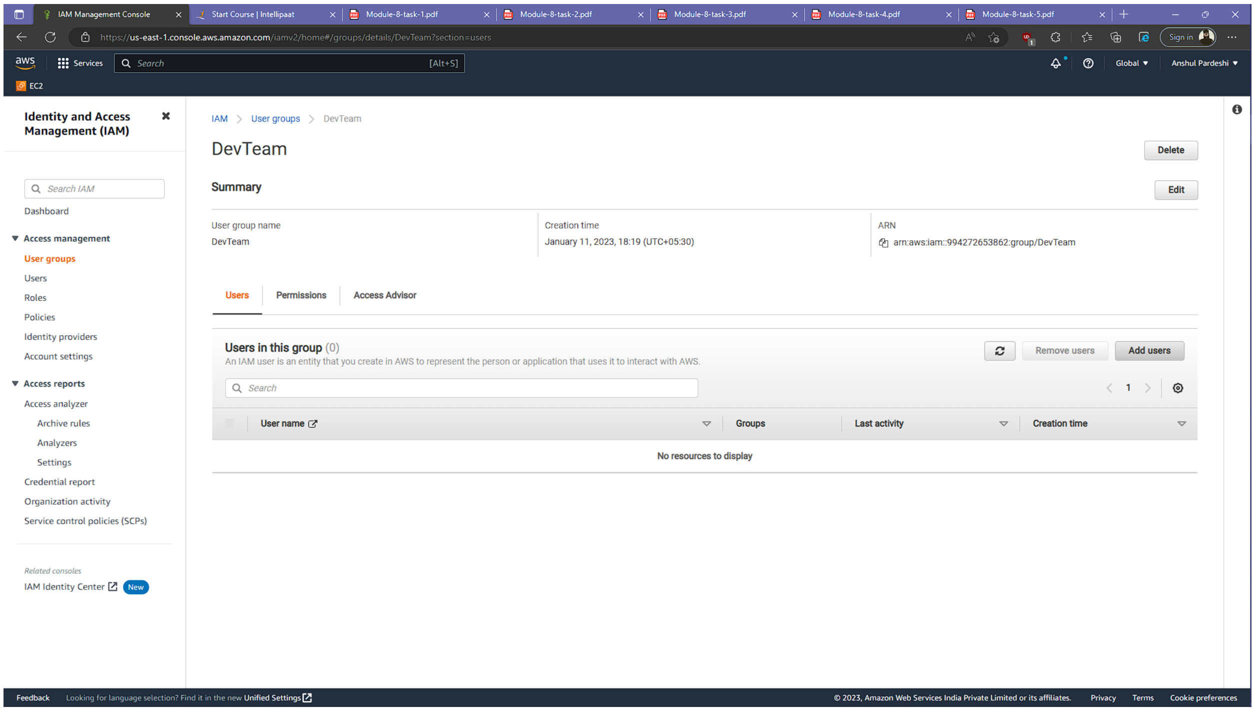


User groups (2) Info

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
□	DevTeam	Loading	Loading	1 minute ago
□	OpsTeam	Loading	Loading	1 minute ago

Ass users.



DevTeam

Summary

User group name	Creation time	ARN
DevTeam	January 11, 2023, 18:19 (UTC+05:30)	arn:aws:iam::994272653862:group/DevTeam

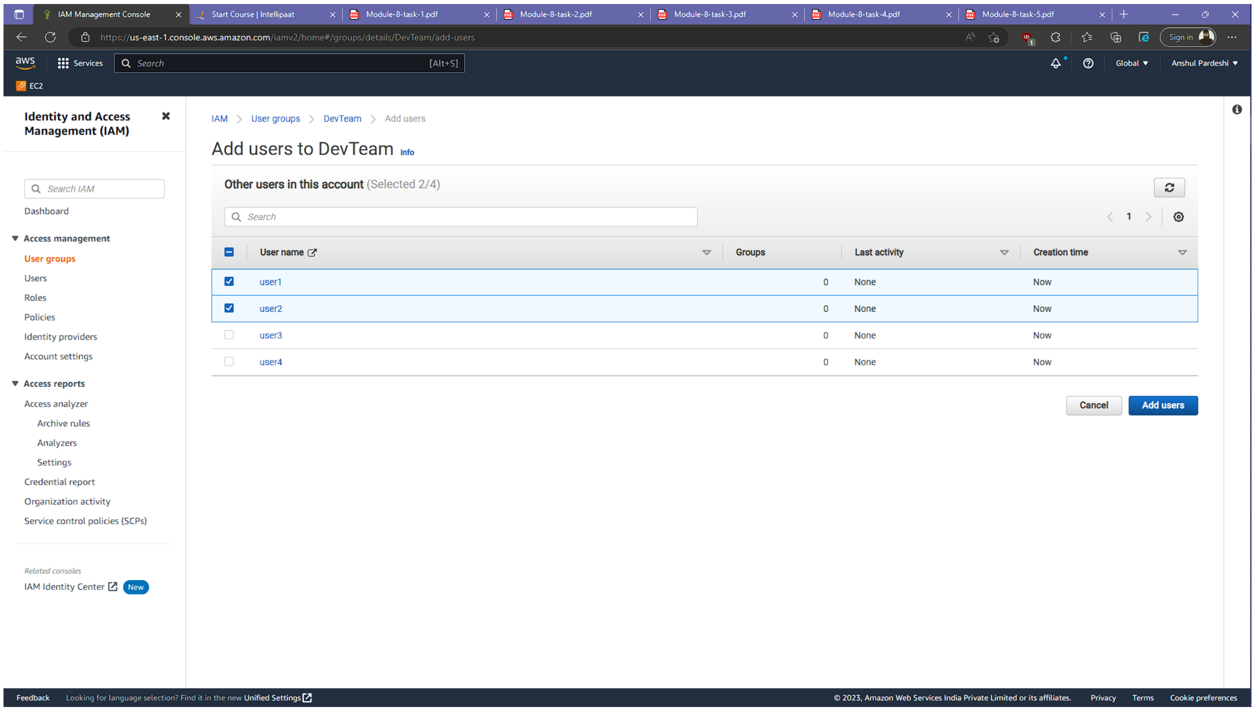
Users in this group (0)

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

No resources to display

Choose the users to be added to the respective group.



IAM > User groups > DevTeam > Add users

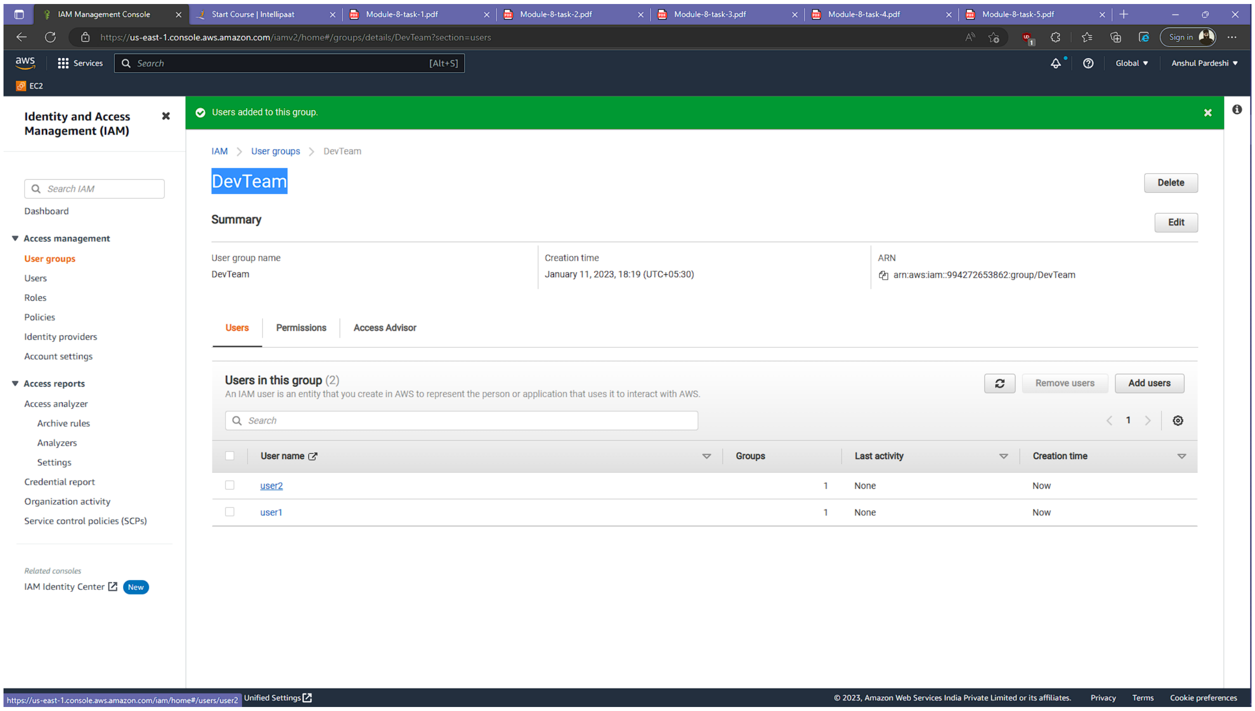
Add users to DevTeam Info

Other users in this account (Selected 2/4)

	User name	Groups	Last activity	Creation time
☑	user1	0	None	Now
☑	user2	0	None	Now
□	user3	0	None	Now
□	user4	0	None	Now

Cancel | Add users

Another group.



Users added to this group.

IAM > User groups > DevTeam

DevTeam

Delete

Summary Edit

User group name: DevTeam

Creation time: January 11, 2023, 18:19 (UTC+05:30)

ARN: arn:aws:iam::994272653862:group/DevTeam

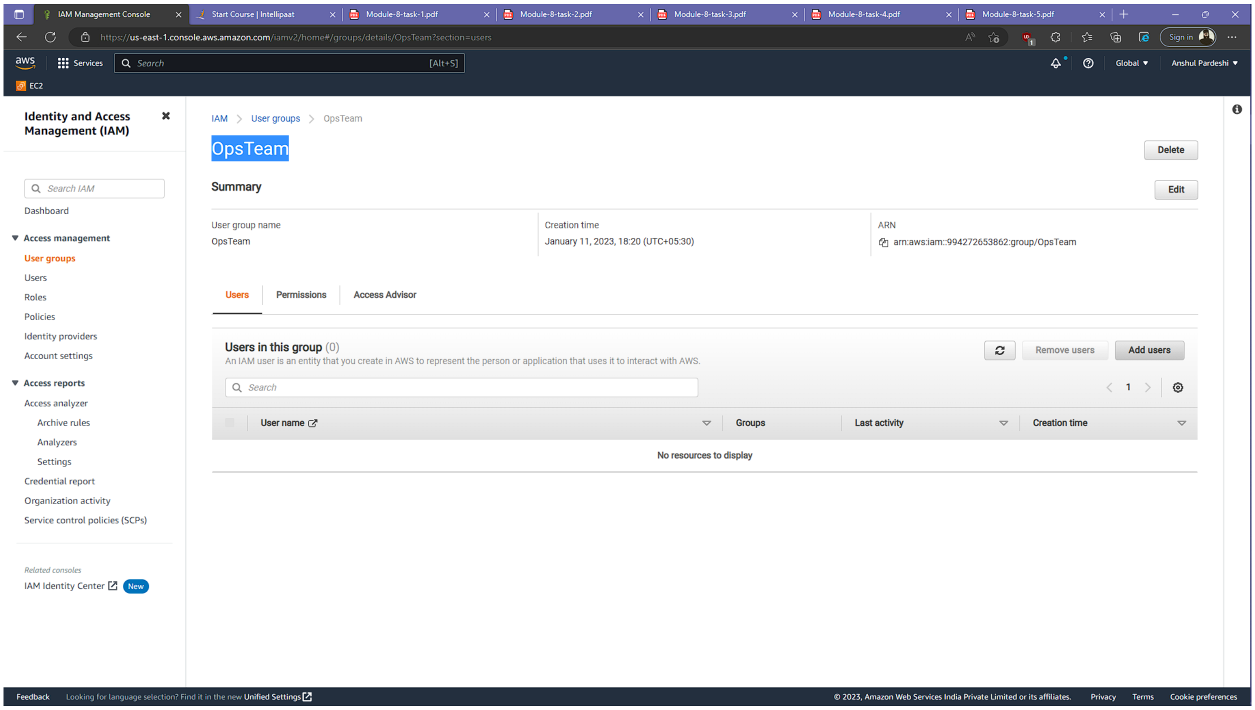
Users | Permissions | Access Advisor

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.

Remove users | Add users

	User name	Groups	Last activity	Creation time
□	user2	1	None	Now
□	user1	1	None	Now



https://us-east-1.console.aws.amazon.com/iamv2/home#/groups/details/OpsTeam?section=users

IAM > User groups > OpsTeam

OpsTeam

Summary

User group name	Creation time	ARN
OpsTeam	January 11, 2023, 18:20 (UTC+05:30)	arn:aws:iam::994272653862:group/OpsTeam

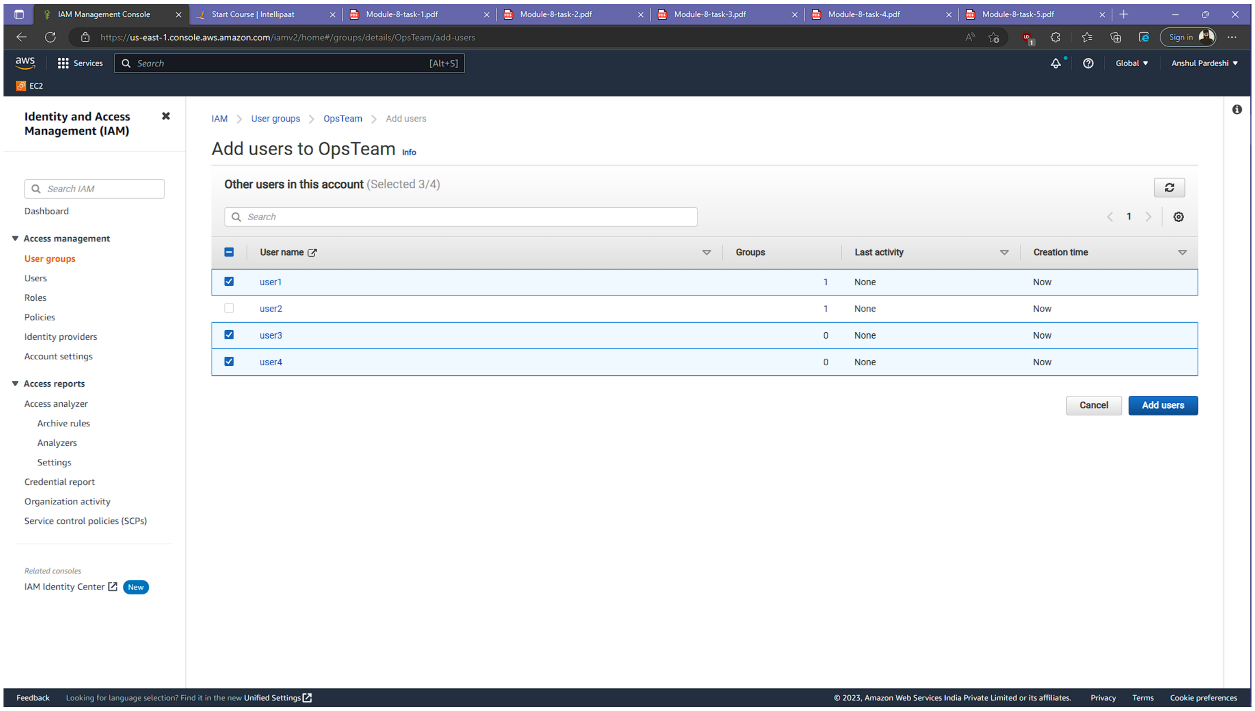
Users in this group (0)

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

No resources to display

Choose the users.



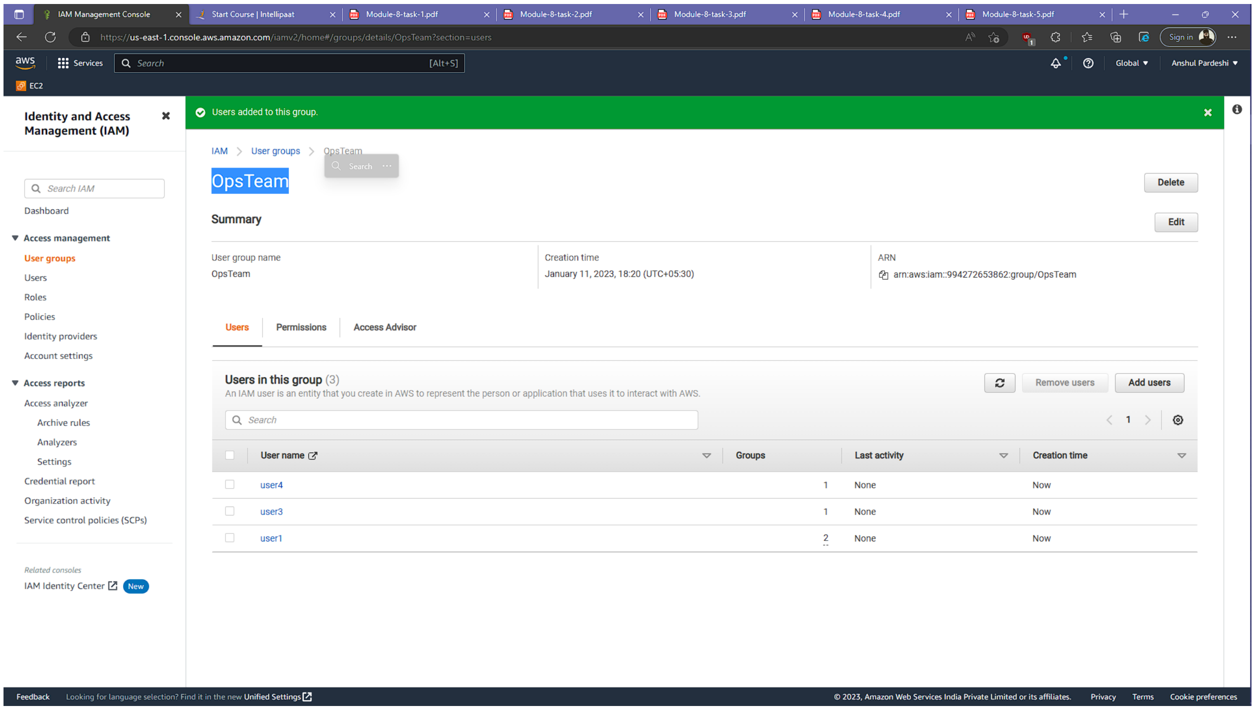
https://us-east-1.console.aws.amazon.com/iamv2/home#/groups/details/OpsTeam/add-users

IAM > User groups > OpsTeam > Add users

Add users to OpsTeam Info

Other users in this account (Selected 3/4)

	User name	Groups	Last activity	Creation time
☑	user1	1	None	Now
□	user2	1	None	Now
☑	user3	0	None	Now
☑	user4	0	None	Now



Users added to this group.

OpsTeam

Summary

User group name: OpsTeam

Creation time: January 11, 2023, 18:20 (UTC+05:30)

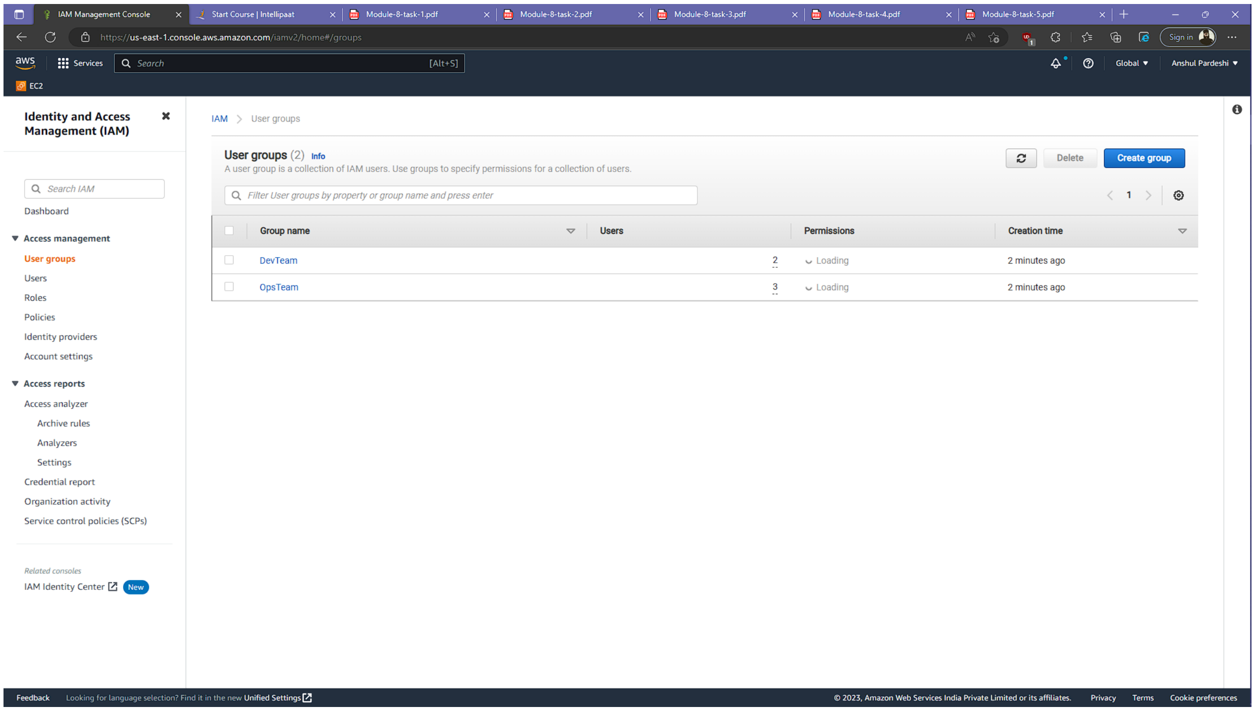
ARN: arn:aws:iam::994272653862:group/OpsTeam

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
user4	1	None	Now
user3	1	None	Now
user1	2	None	Now

Groups have been created according to respective users.



User groups (2)

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
DevTeam	2	Loading	2 minutes ago
OpsTeam	3	Loading	2 minutes ago