

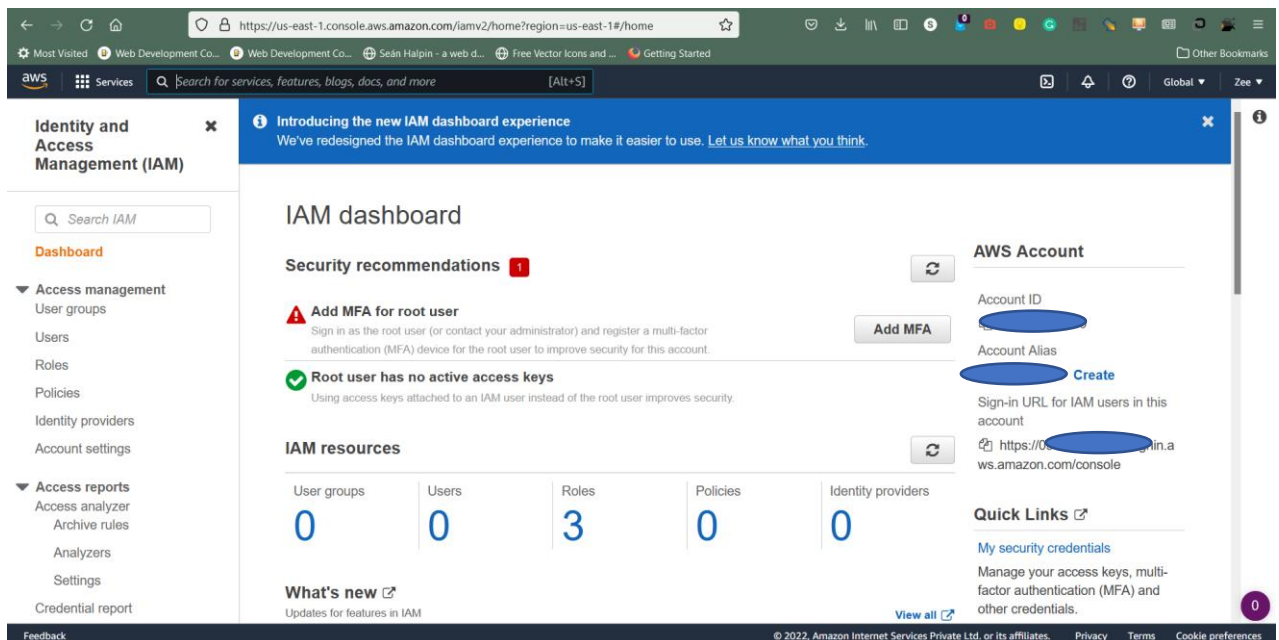
Practical 7

Aim: Perform IAM (Identity and Access Management) Operations in AWS.

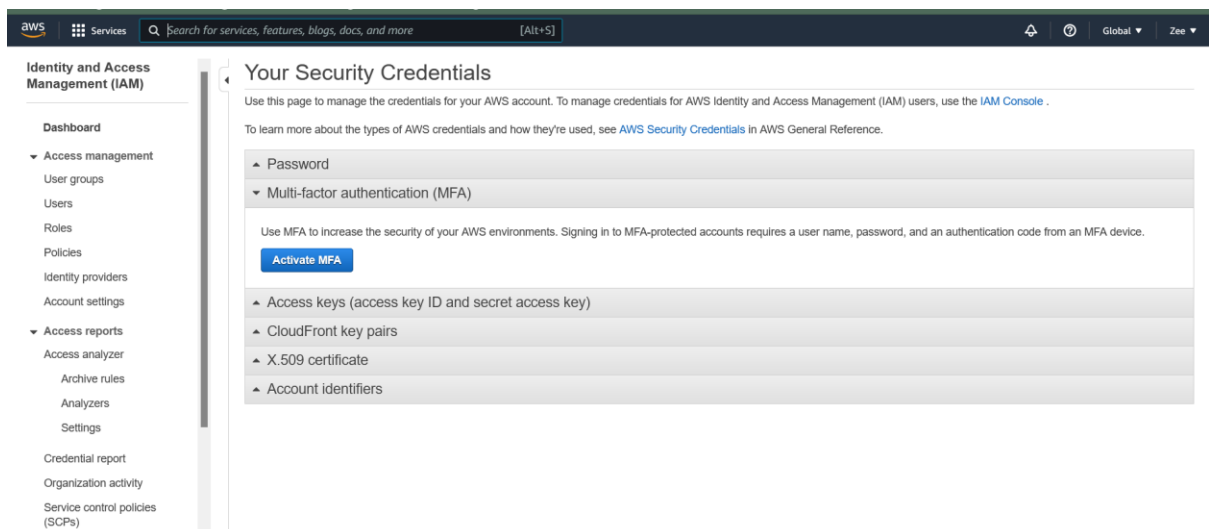
A) MFA

Steps:

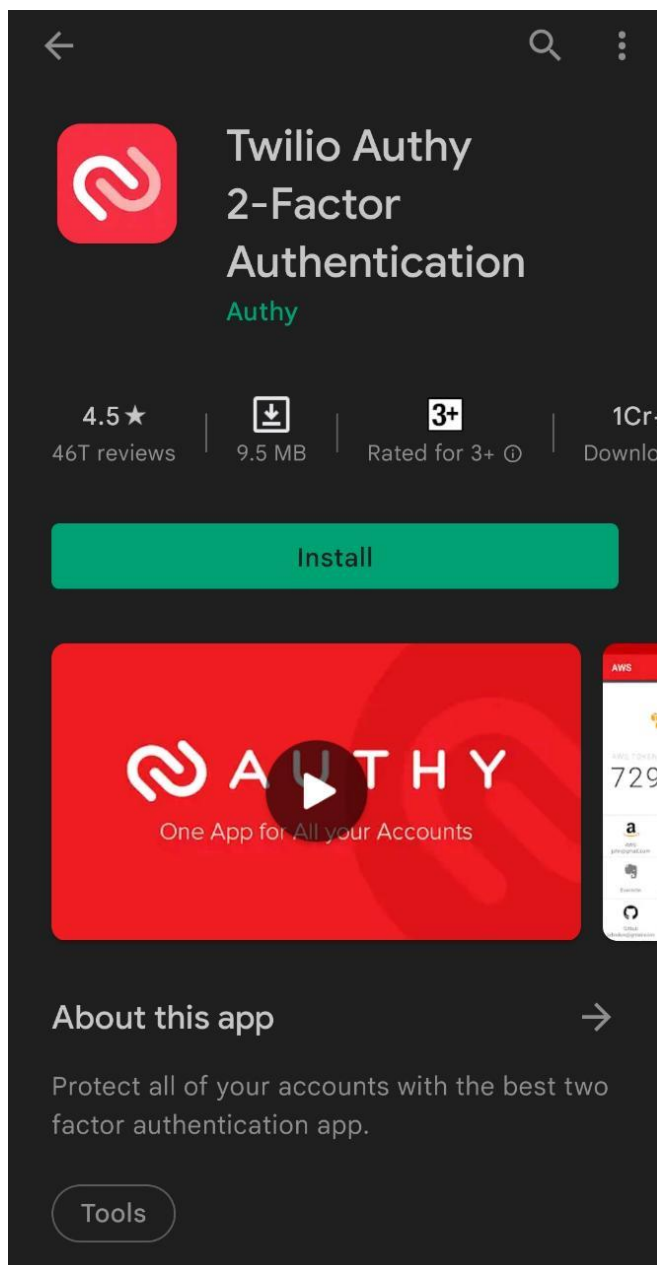
- 1) Log in to your Aws Console.
- 2) Search AWS inside search bar.
- 3) On IAM Dashboard Click-On Add MFA



4) Click on Activate MFA



5) Install Authy From Android Play Store



6) Scan QR Code from Authy.

7) Enter 2 consecutive MFA codes.

Set up virtual MFA device

1. Install a compatible app on your mobile device or computer

See a [list of compatible applications](#)

2. Use your virtual MFA app and your device's camera to scan the QR code

Show QR code

Alternatively, you can type the secret key. [Show secret key](#)

3. Type two consecutive MFA codes below


Cancel

Previous

Assign MFA

8) Click on Assign MFA

Set up virtual MFA device



Alternatively, you can type the secret key. [Show secret key](#)

3. Type two consecutive MFA codes below

MFA code 1

769518

MFA code 2

794041

Cancel

Previous

Assign MFA

Identity and Access Management (IAM)

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#).

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

Password
 Multi-factor authentication (MFA)

Use MFA to increase the security of your AWS environments. Signing in to MFA-protected accounts requires a user name, password, and an authentication code from an MFA device.

Device type	Serial number	Actions
Virtual	arn:aws:iam::[redacted]:mfa-device	Manage

Access keys (access key ID and secret access key)
 CloudFront key pairs
 X.509 certificate
 Account identifiers

9) Multifactor Authentication has been successfully implemented.

Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address: zeewithz@gmail.com

MFA code

[Submit](#)

[Troubleshoot MFA](#)

[Cancel](#)

Amazon Lightsail

Lightsail is the easiest way to get started on AWS

[Learn more »](#)

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

English

Identity and Access Management (IAM)

Introducing the new IAM dashboard experience
We've redesigned the IAM dashboard experience to make it easier to use. [Let us know what you think.](#)

IAM dashboard

Security recommendations

- ✓ **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

User groups	Users	Roles	Policies	Identity providers
0	0	3	0	0

What's new
Updates for features in IAM [View all](#)

AWS Account

Account ID: [redacted]

Account Alias: [redacted] [Create](#)

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

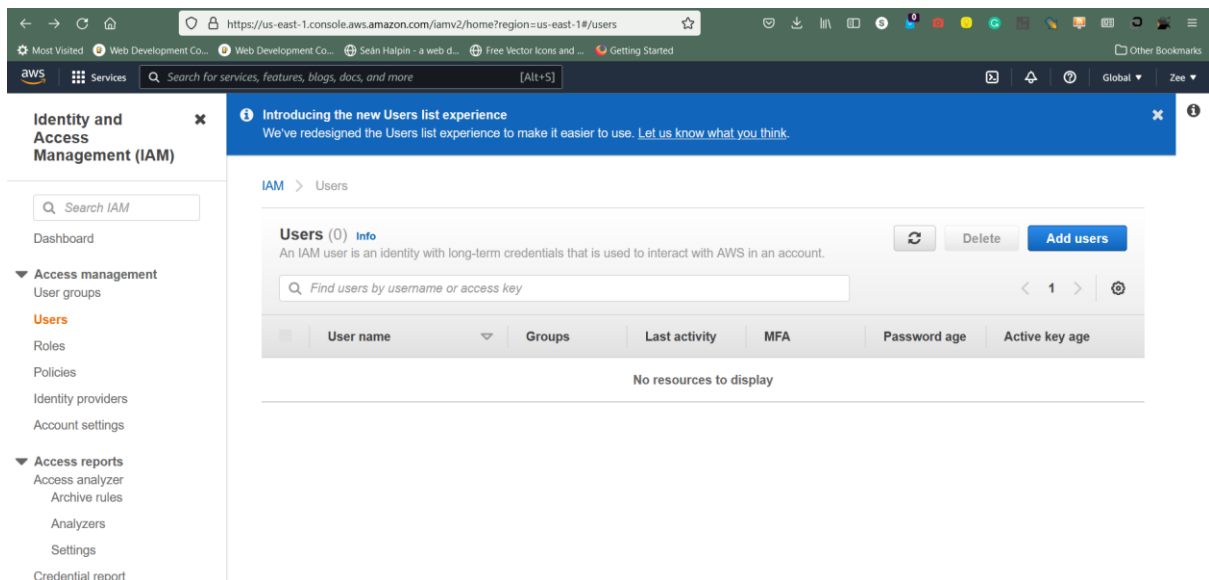
Quick Links

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

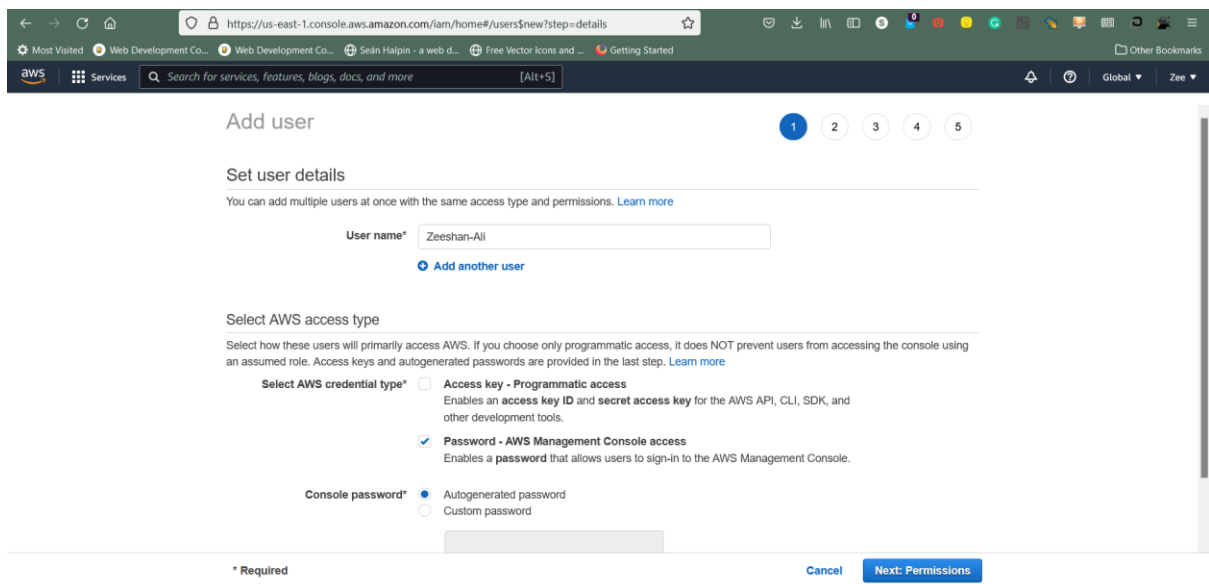
B) Create users

Steps:

1) Click-On Add Users



2) Add User Name



3) Set Permissions

← → ↻ 🏠 🔒 https://us-east-1.console.aws.amazon.com/iam/home#/users\$new?step=permissions&login=...

Most Visited Web Development Co... Web Development Co... Seán Halpin - a web d... Free Vector Icons and ... Getting Started


aws Services 🔍 Search for services, features, blogs, docs, and more [Alt+S]


Global Zee


Add user

1 2 3 4 5

▼ Set permissions

 Add user to group

 Copy permissions from existing user

 Attach existing policies directly

Get started with groups

You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. [Learn more](#)

Create group

► Set permissions boundary

Cancel Previous **Next: Tags**

▼ Set permissions boundary

Set a permissions boundary to control the maximum permissions this user can have. This is an advanced feature used to delegate permission management to others. [Learn more](#)

- ☒ Create user without a permissions boundary
- ☐ Use a permissions boundary to control the maximum user permissions

Cancel Previous **Next: Tags**

4) Add Tags

← → ↻ 🏠 🔒 https://us-east-1.console.aws.amazon.com/iam/home#/users\$new?step=tags&login=&userNa=...

Most Visited Web Development Co... Web Development Co... Seán Halpin - a web d... Free Vector Icons and ... Getting Started

aws Services 🔍 Search for services, features, blogs, docs, and more [Alt+S]

Global Zee

Add user

1 2 3 4 5

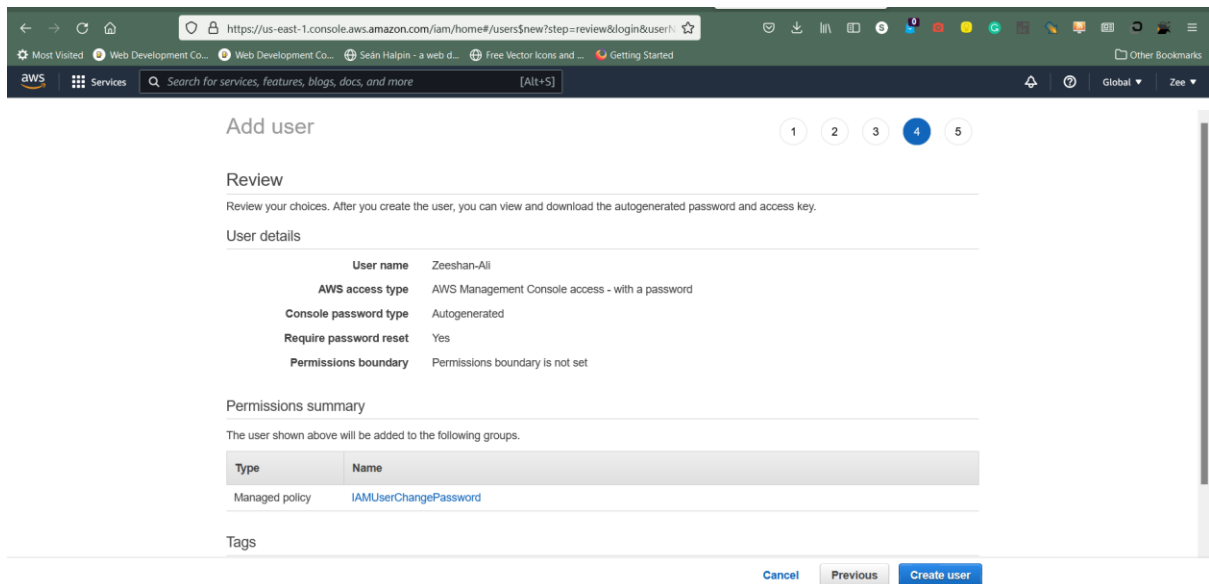
Add tags (optional)

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](#)

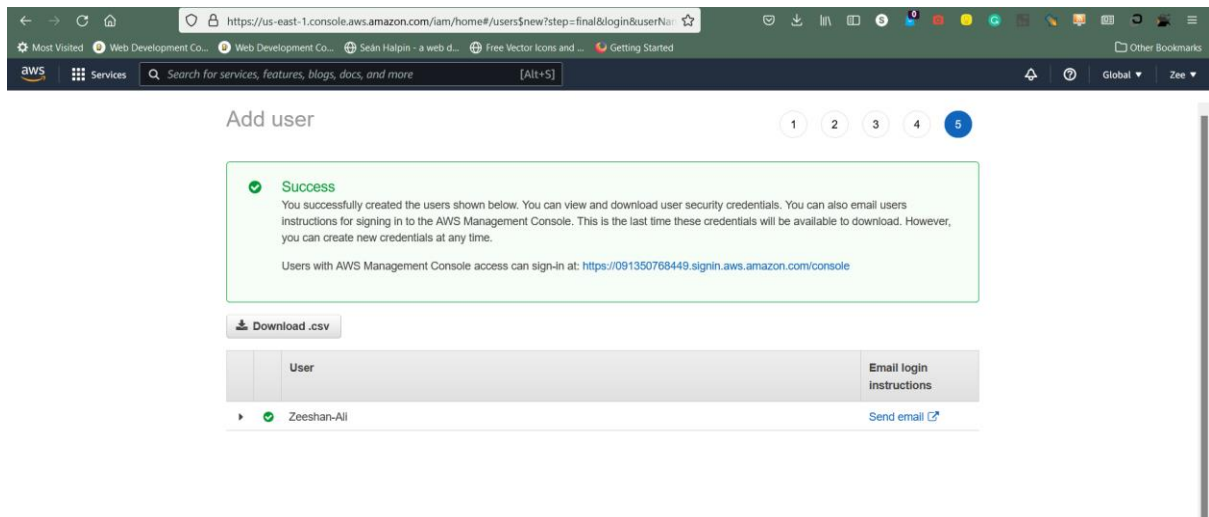
Key	Value (optional)	Remove
Web-Development	Fullstack	✕
Add new key		

You can add 49 more tags.

5) Click-On Create User



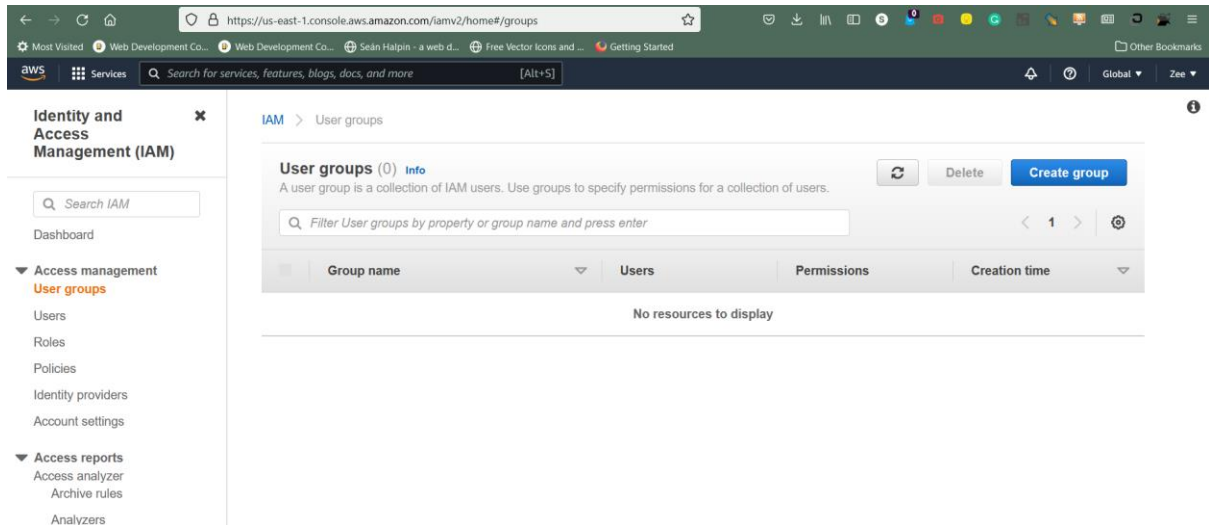
6) User has been created successfully



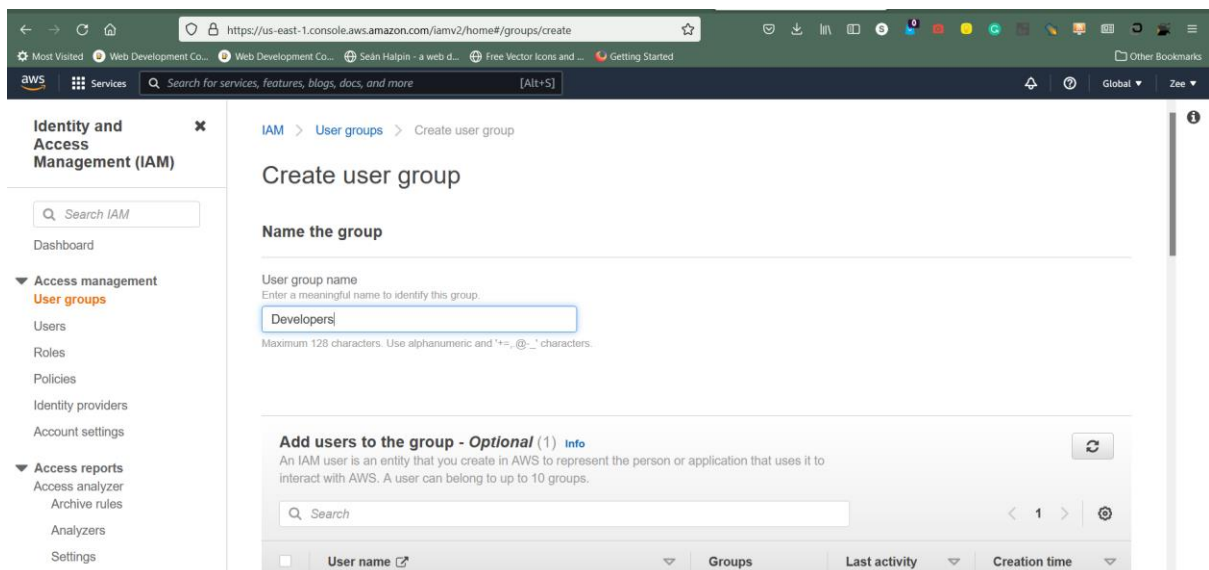
C) User Groups

Steps:

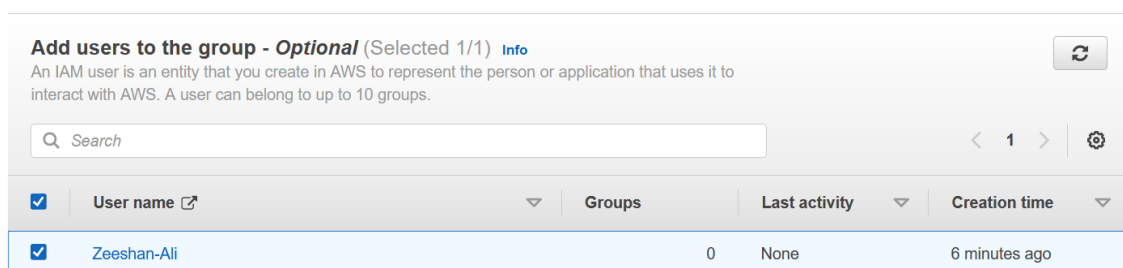
1) Click-On Create Groups.



2) Assign names to the group.



3) Add Users to the group.



5) Click-On create group.

Attach permissions policies - *Optional* (Selected 3/746)

[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.

< 1 2 3 4 5 6 7 ... 38 >

Policy name

Type

Description

<input checked="" type="checkbox"/>	AWSDirectConnectReadOnlyAccess	AWS managed	Provides read only ac
<input checked="" type="checkbox"/>	AmazonGlacierReadOnlyAccess	AWS managed	Provides read only ac
<input checked="" type="checkbox"/>	AWSMarketplaceFullAccess	AWS managed	Provides the ability to
<input type="checkbox"/>	AWSSSODirectoryAdministrator	AWS managed	Administrator access f
<input type="checkbox"/>	AWSIoT1ClickReadOnlyAccess	AWS managed	Provides read only ac

6) User group generated.

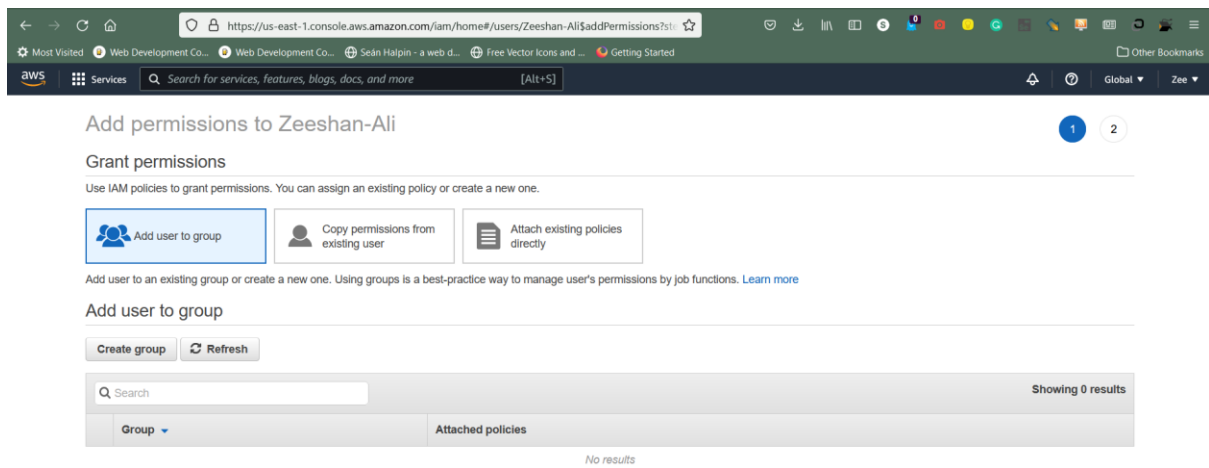
The screenshot displays the AWS IAM console interface. At the top, a green banner confirms the creation of the 'Developers' user group, with a 'View group' button. The left-hand navigation pane shows the 'Access management' section expanded, with 'User groups' selected. The main content area, titled 'User groups (1) Info', provides a description of user groups and a search filter. Below this is a table listing the existing user group:

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	Developers	1	Defined	Now

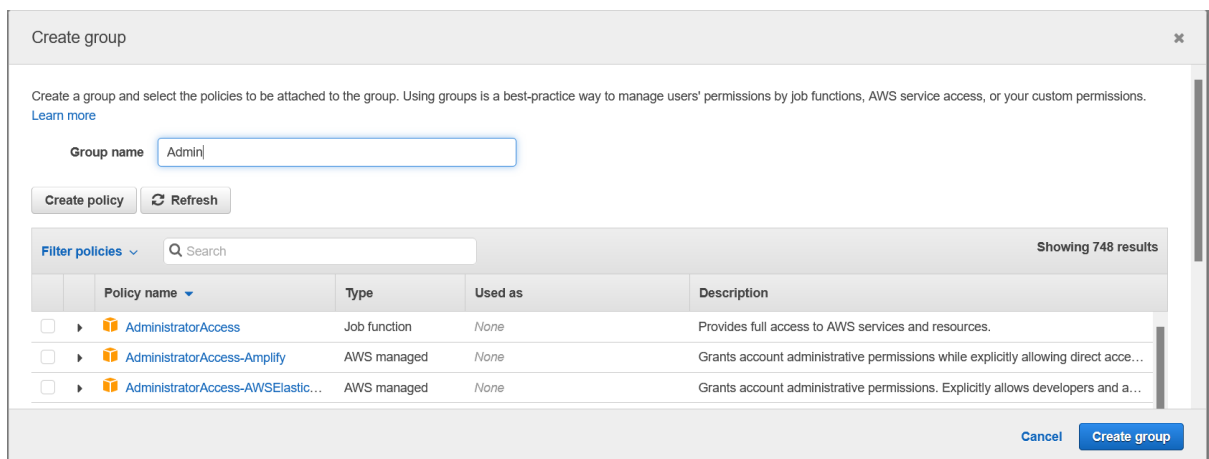
D) Create Policies

Steps:

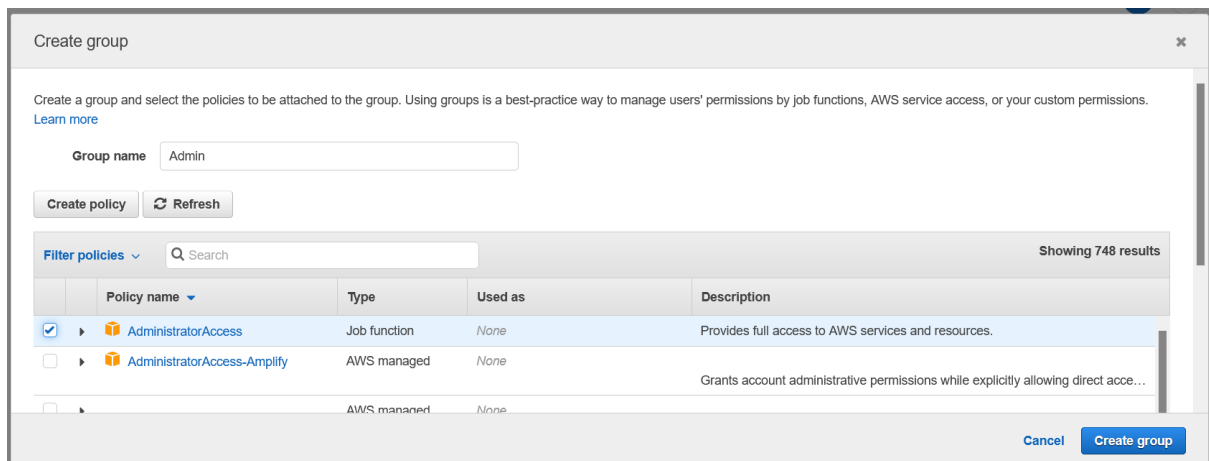
1) Click-On user you want to update policies for



2) Create a Group



3) Add policies for the group.



4) Click On Generate Policy.

Permissions

Groups (2)

Tags (1)


Security credentials

Access Advisor

▼ Permissions policies (5 policies applied)


Add permissions

Add inline policy

Policy name ▼	Policy type ▼
Attached directly	
▶  IAMUserChangePassword	AWS managed policy ✕
Attached from group	
Show 4 more	

▶ Permissions boundary (not set)

▼ Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#) 

Share your [feedback](#) and help us improve the policy generation experience.

Generate policy

Conclusion: IAM operation executed successfully.