**Create AWS Free Tier Account**

Contents

[**Important Notes** 2](#_Toc74849341)

[a) Create an AWS Account 3](#_Toc74849342)

[b) Navigate AWS Console (Optional) 7](#_Toc74849343)

[C) AWS Identity and Access Management (Bouns) 8](#_Toc74849344)

[1. Navigate to IAM 8](#_Toc74849345)

[2. Secure your AWS account based on best practices 8](#_Toc74849346)

[3. Enable MFA on your root account (Google Authenticator) 8](#_Toc74849347)

[4. Create individual IAM users 10](#_Toc74849348)

[5. Use groups to assign permissions 14](#_Toc74849349)

[6. Apply an IAM password policy 15](#_Toc74849350)

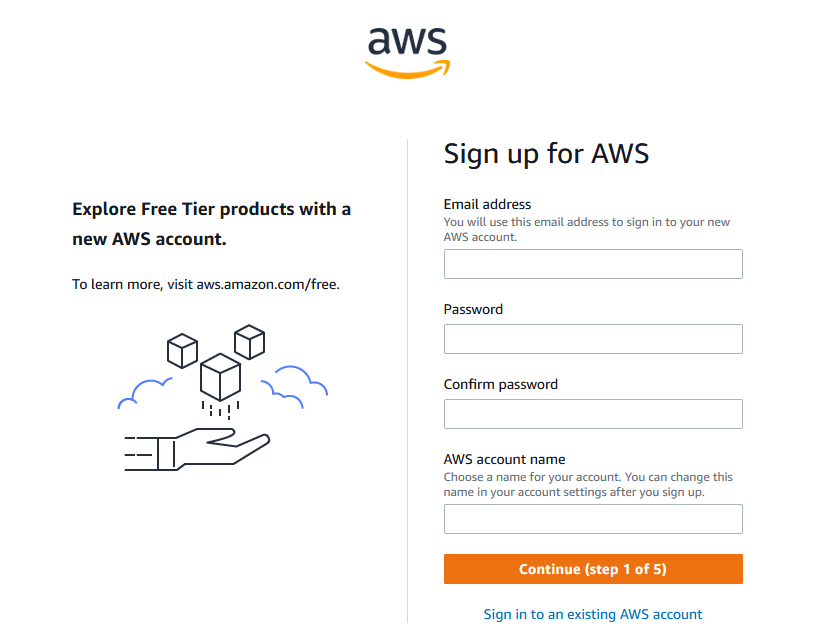
[7. Add the Admin user to the AdminGroup 16](#_Toc74849351)

# **Important Notes**

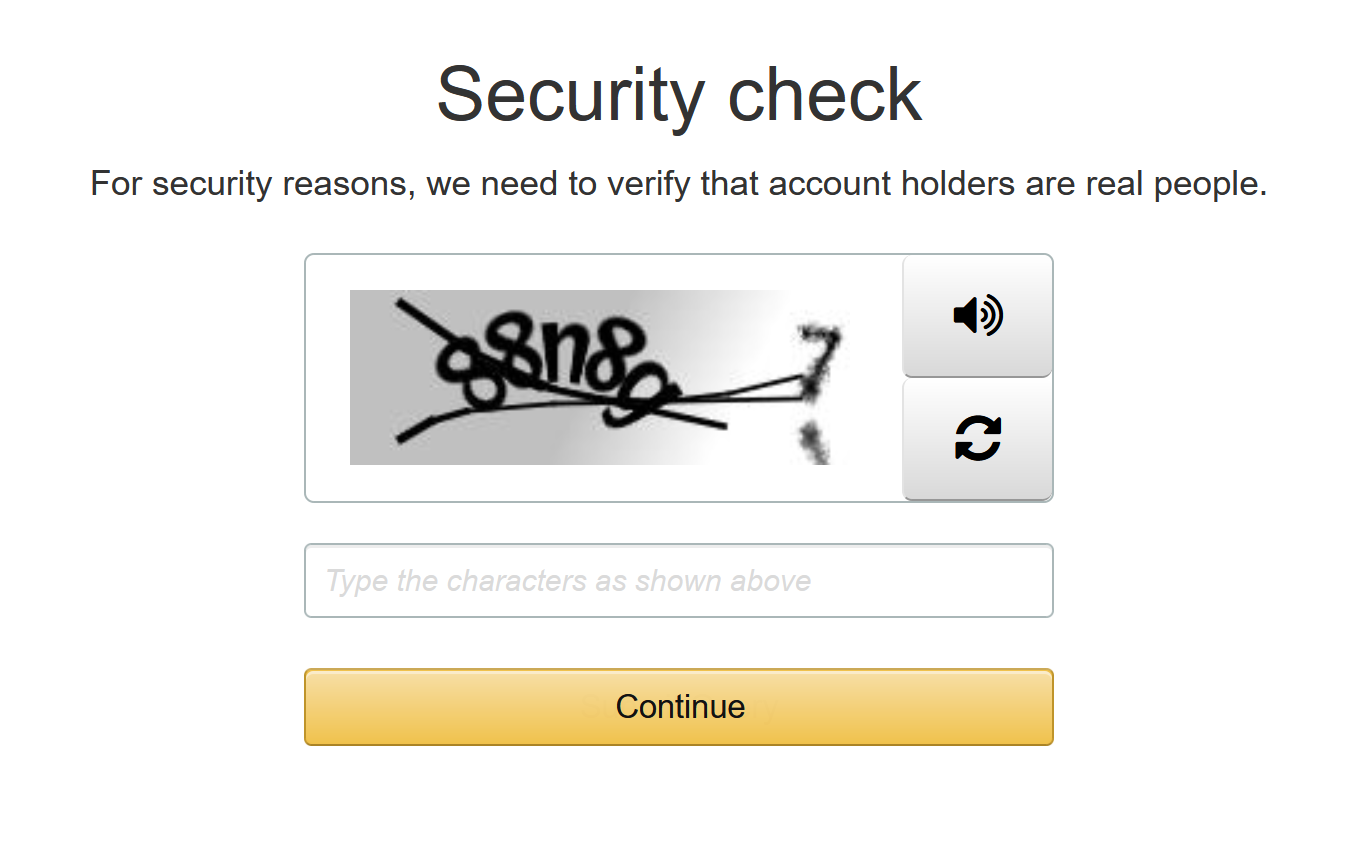
1. You must follow the instructions strictly to remain within the free tier.
2. You must not use a personal email subscribed early for the free tier because you will not be eligible. A workaround to use another email not used before or create a new one.
3. Suppose there is Active Directory Synchronization, Federation, Single-Sign-On (SSO) integration in place between your organization and public cloud providers (AWS). Most likely, you will not be able to use your organization's email for provisioning resources. Unless you are one of the administrators, please be careful and not use your organization's email.

# a) Create an AWS Account

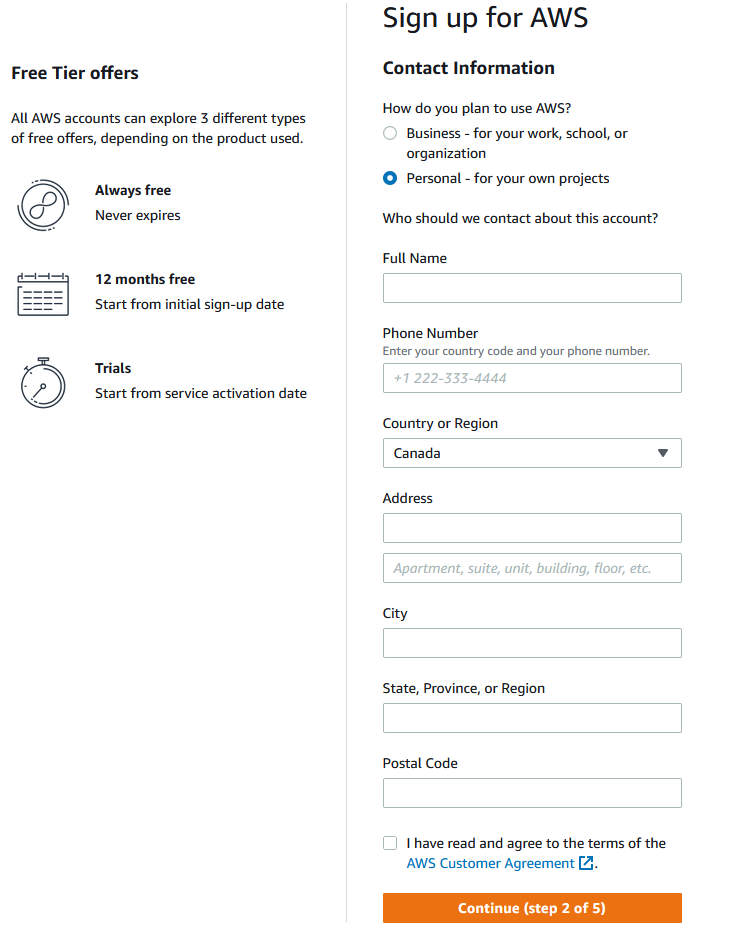
1. Open URL: <https://aws.amazon.com/getting-started/>
2. Click on **Create an AWS Account**
3. AWS Accounts include 12 months of free tier access for full offer terms, and free tier details visit <https://aws.amazon.com/free/>
4. Enter the following details: your email address, create a password and choose your preferred AWS account name. Click Continue



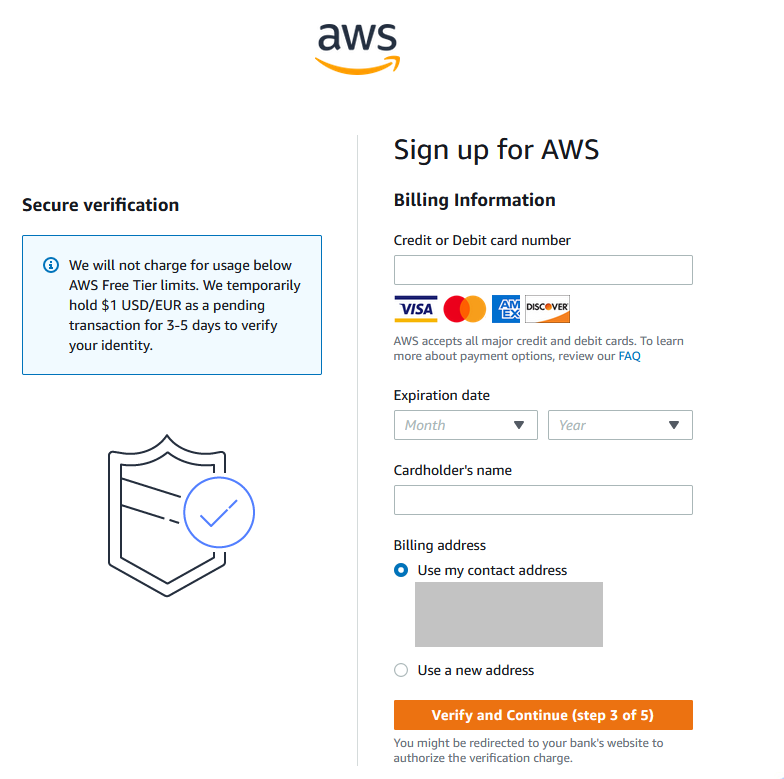
1. Complete the Security check. click Continue



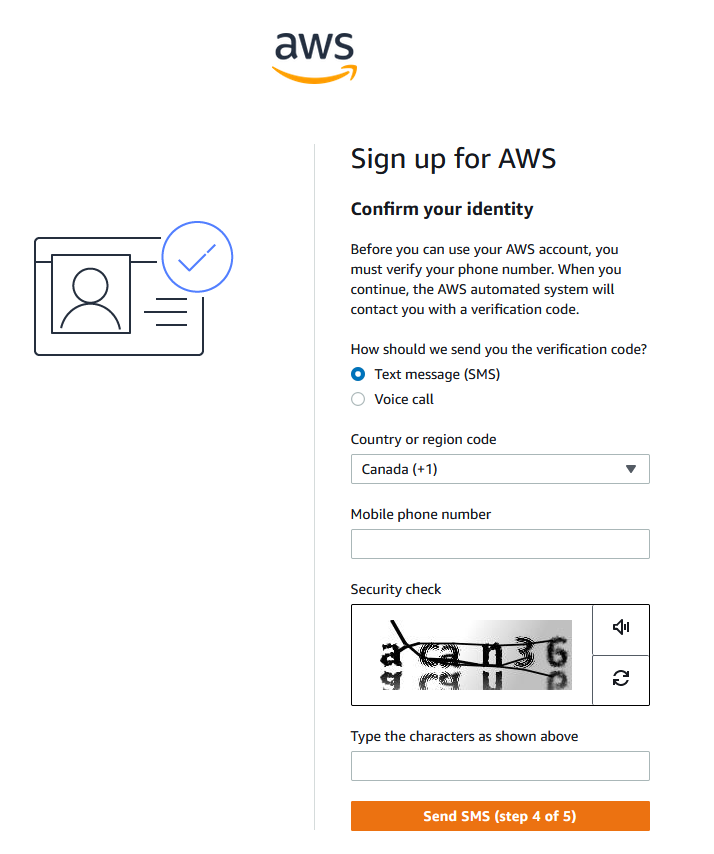
1. Complete the **Contact Information**
   * Select Account Type (Professional OR Personal) **Personal**
   * Enter your full name, phone number, country/region, address, city, state/province or region, postal code, read and accept AWS Customer Agreement

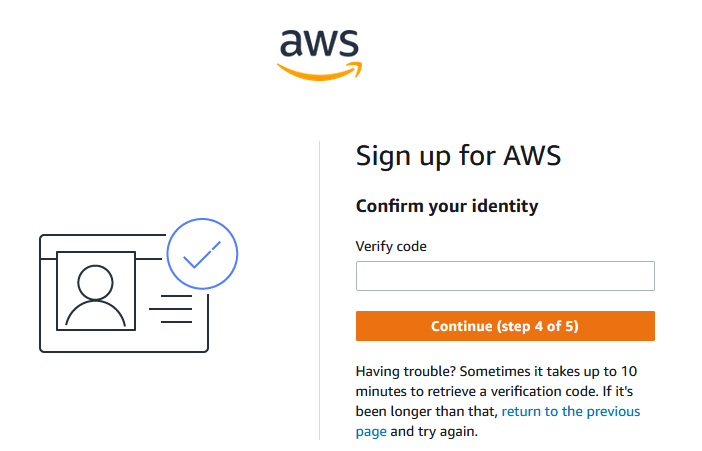


1. Complete the Payment Information (You need **Valid** Credit Card)

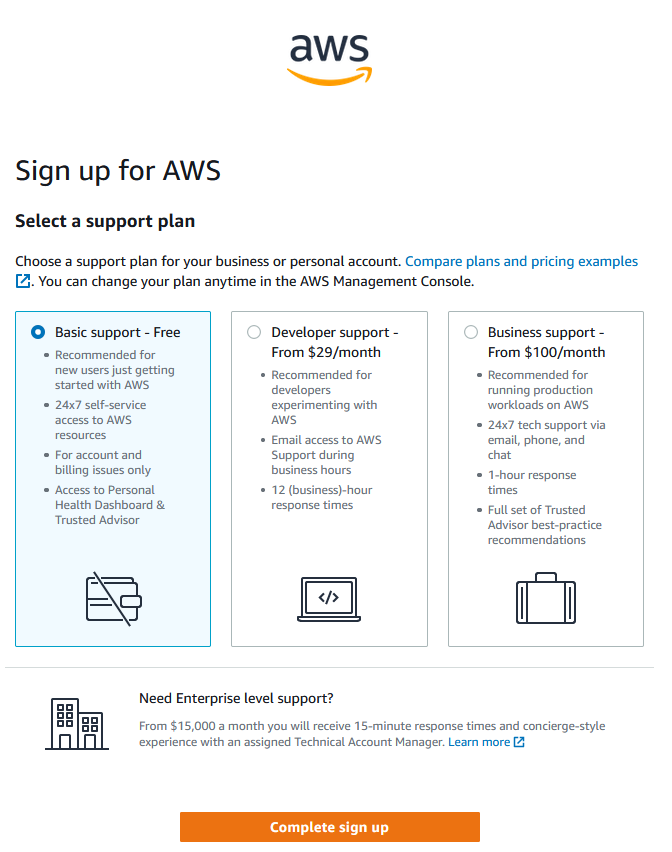


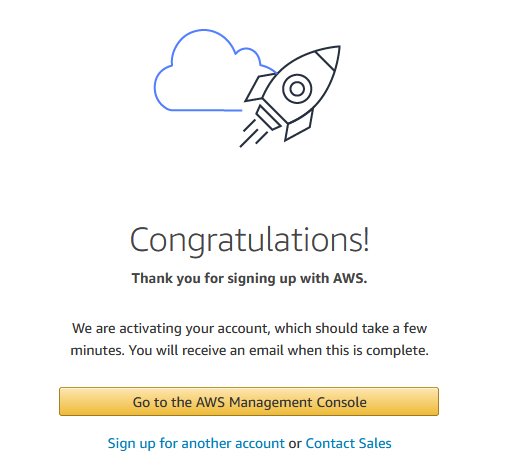
1. Confirm your identity. (Your identity has been verified successfully)



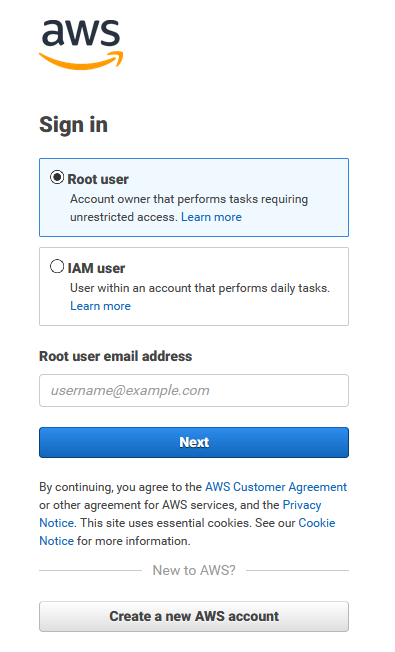
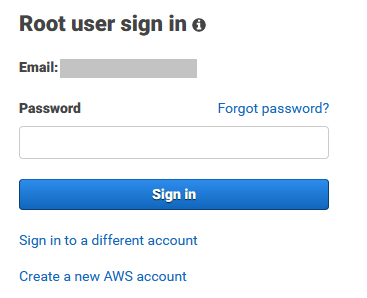
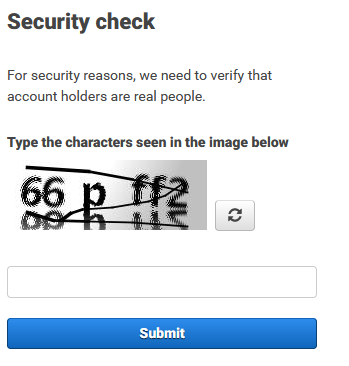


1. Select a support plan (select **Basic** for Free Tier)

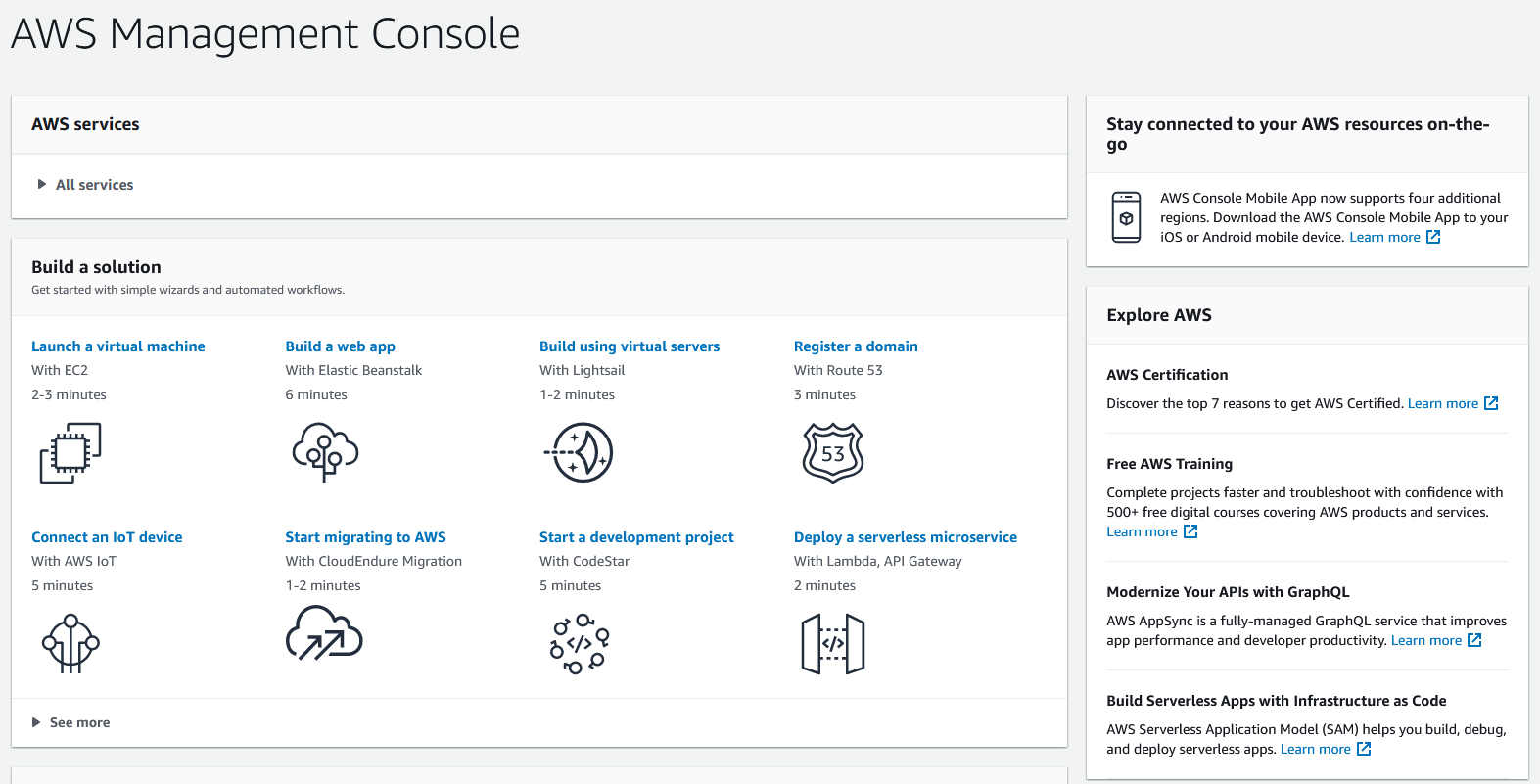




1. Sign in to the AWS console

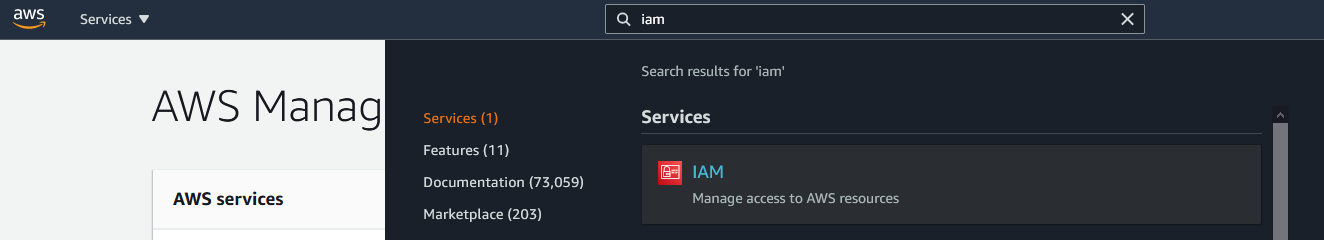
 

# b) Navigate AWS Console (Optional)

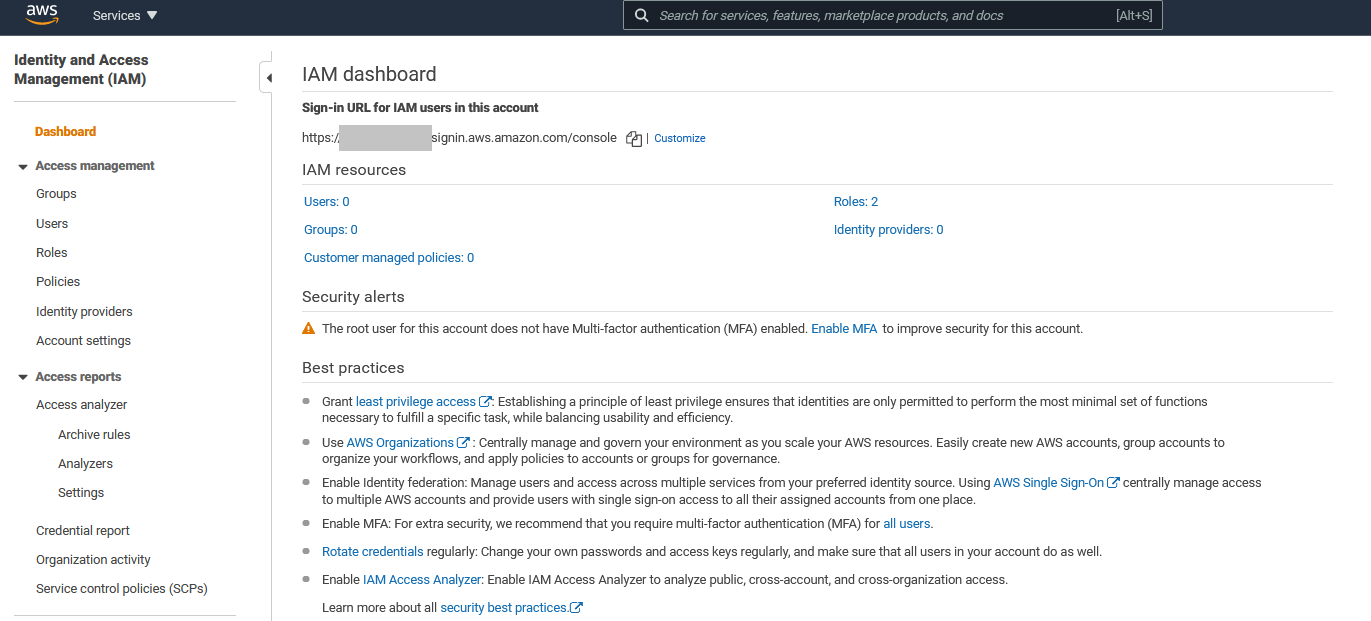


# C) AWS Identity and Access Management (Bouns)

## 1. Navigate to IAM

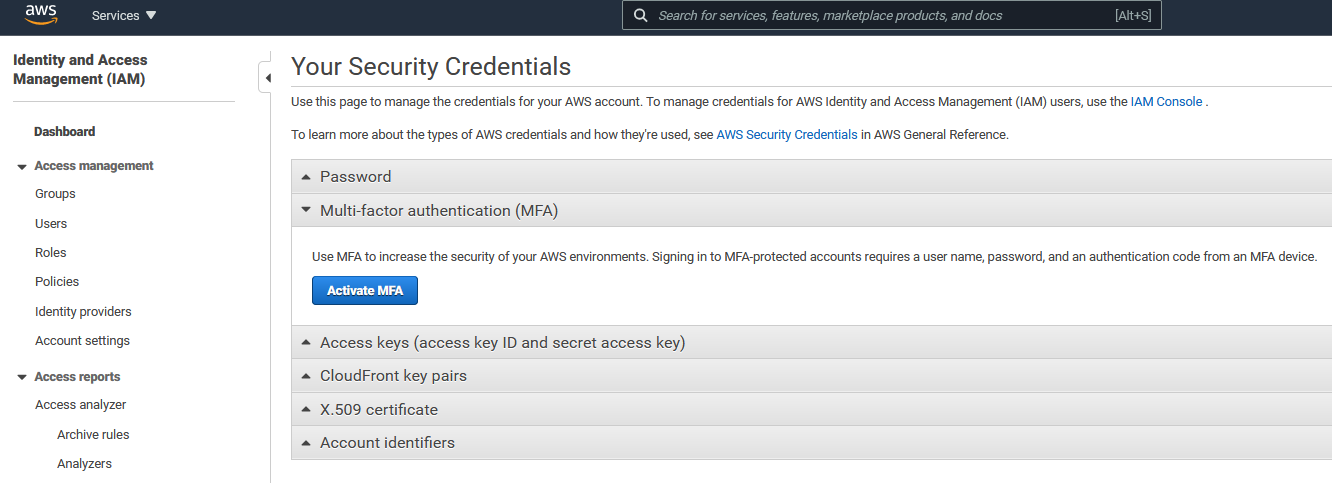


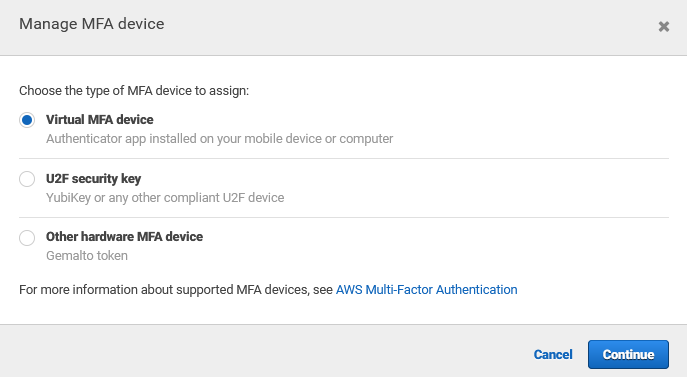
## 2. Secure your AWS account based on best practices



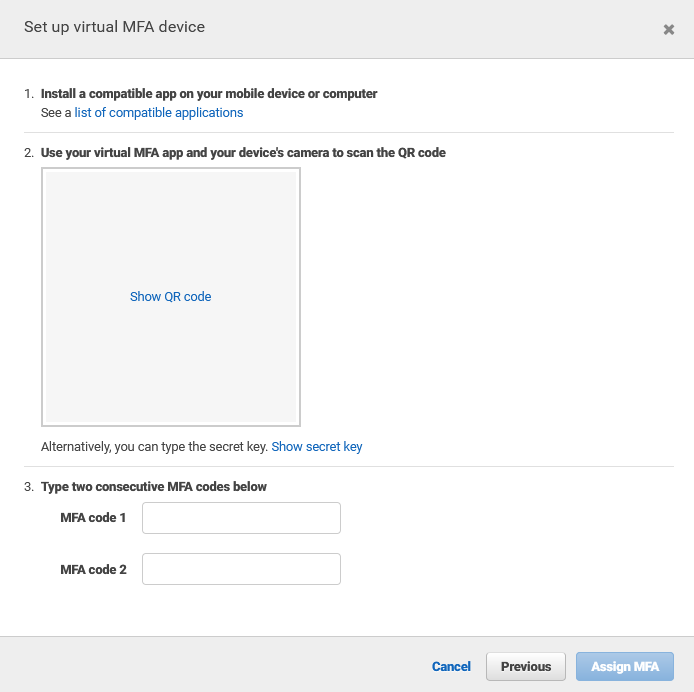
## 3. Enable MFA on your root account (Google Authenticator)

* 1. Click on Enable MFA Under Security alerts



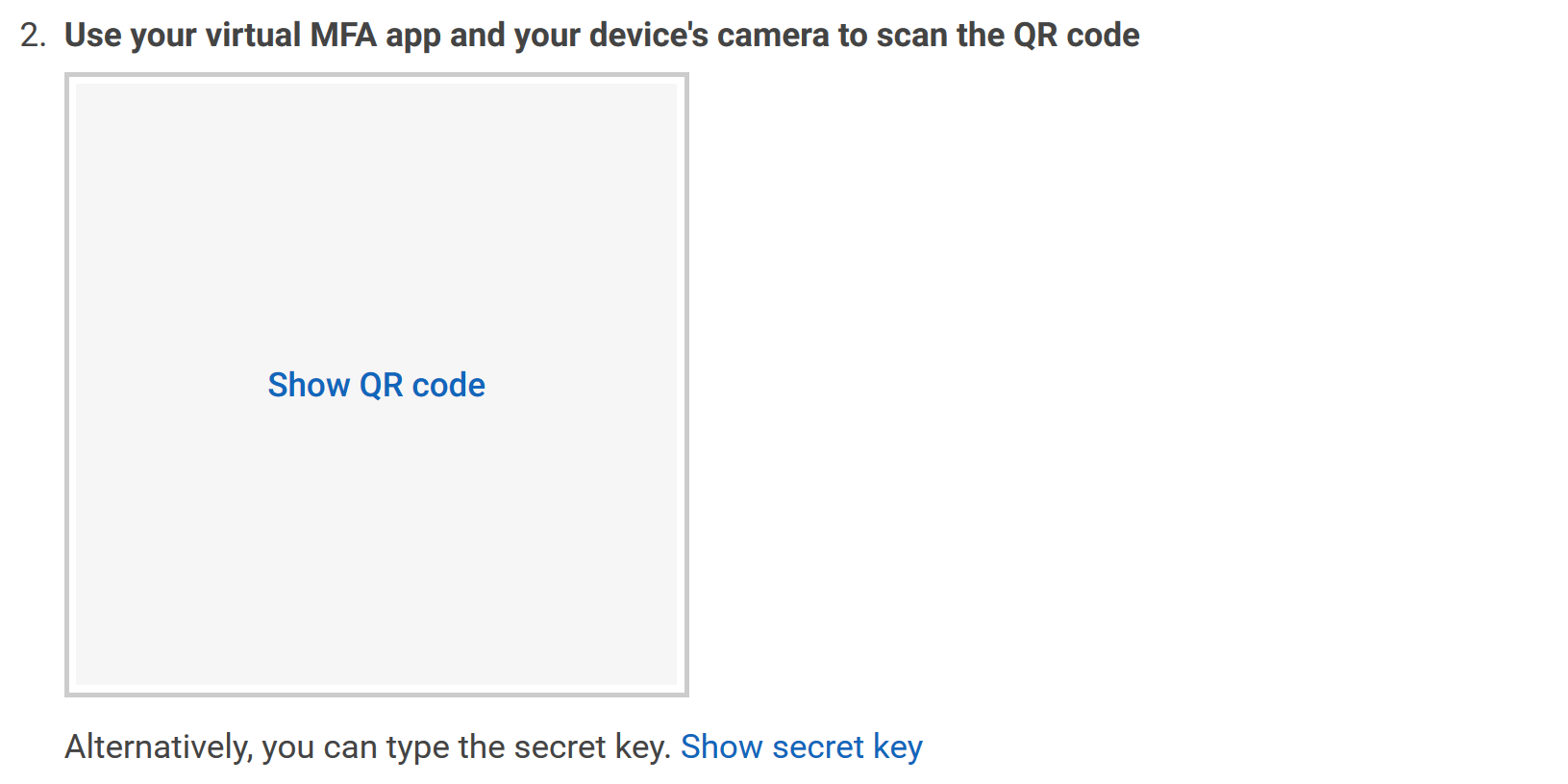


* 1. Set up virtual MFA device

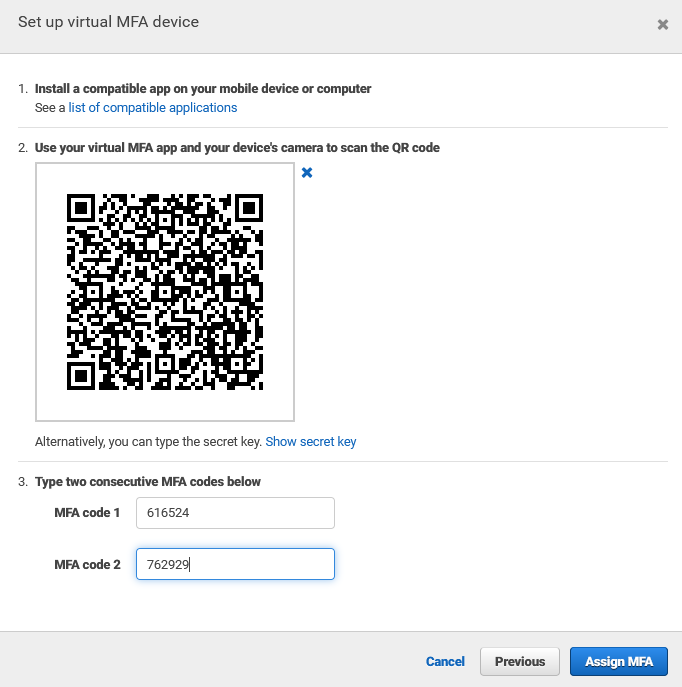


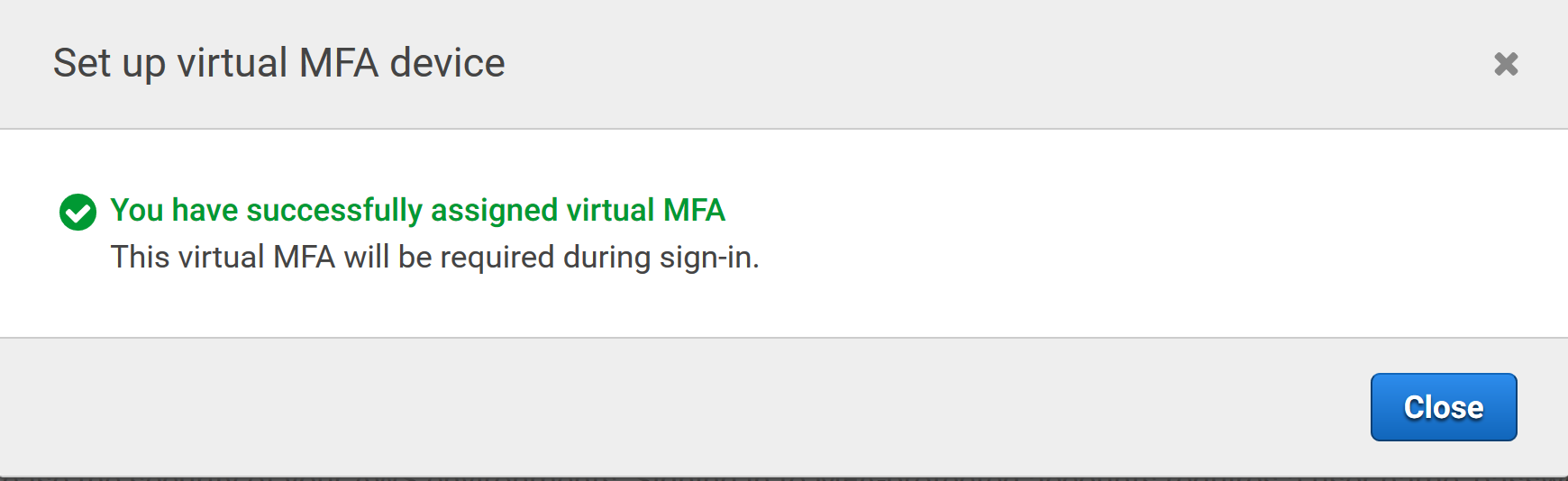
Install a compatible app on your mobile device or computer

See a [list of compatible applications](https://aws.amazon.com/iam/details/mfa/)

* 1. Use your virtual MFA app and your device's camera to scan the QR code 
  2. Type two consecutive MFA codes below

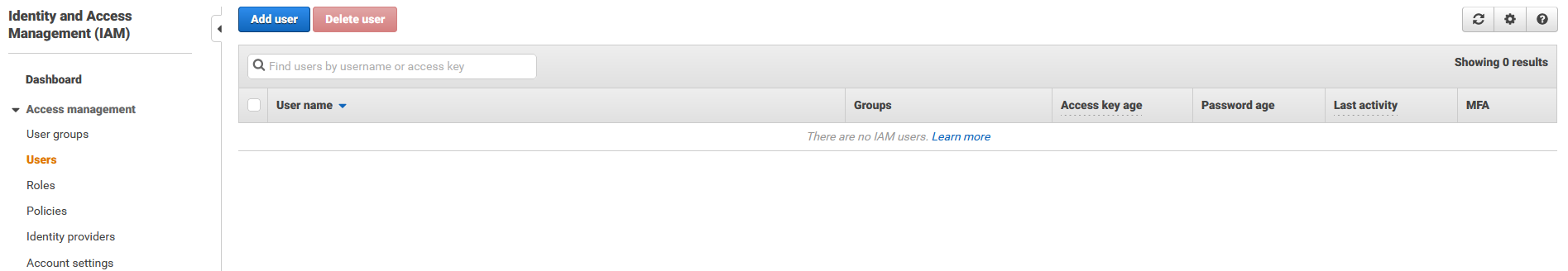






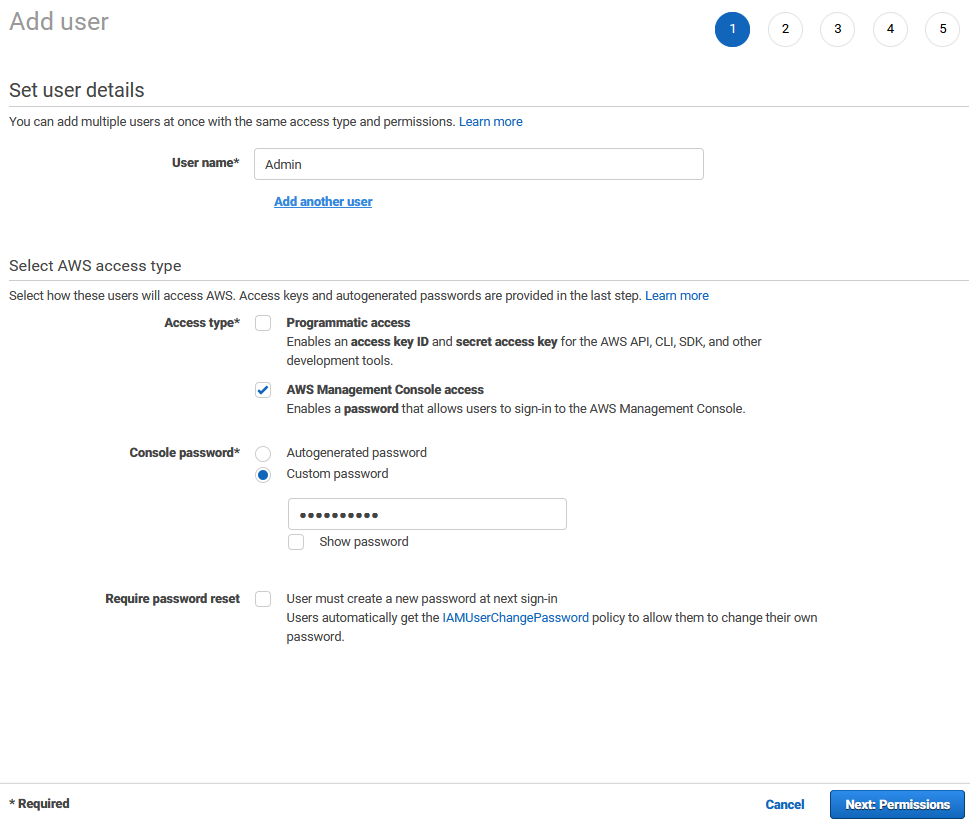
## 4. Create individual IAM users

* 1. Select Users under Access Management

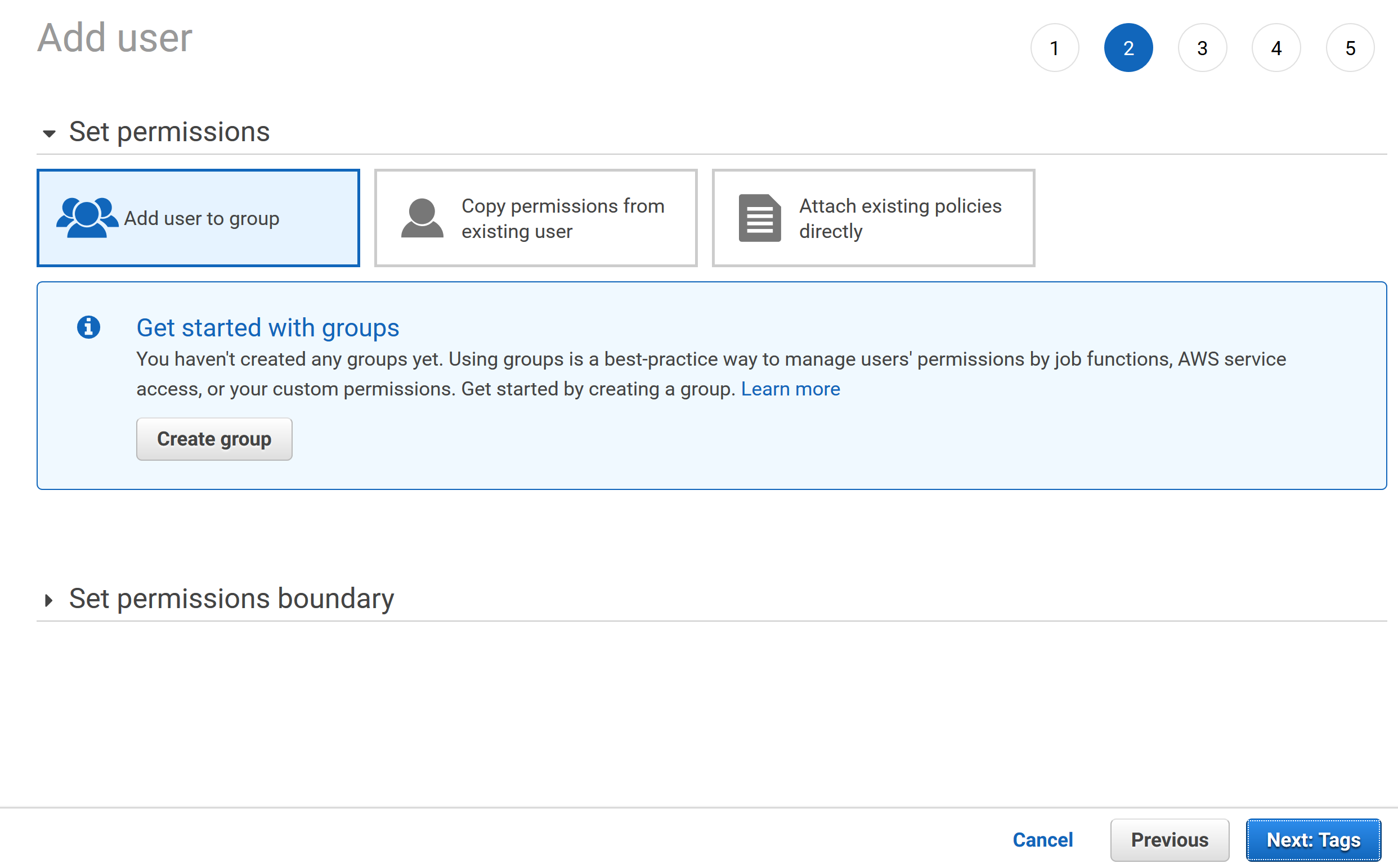


4.2. Add User

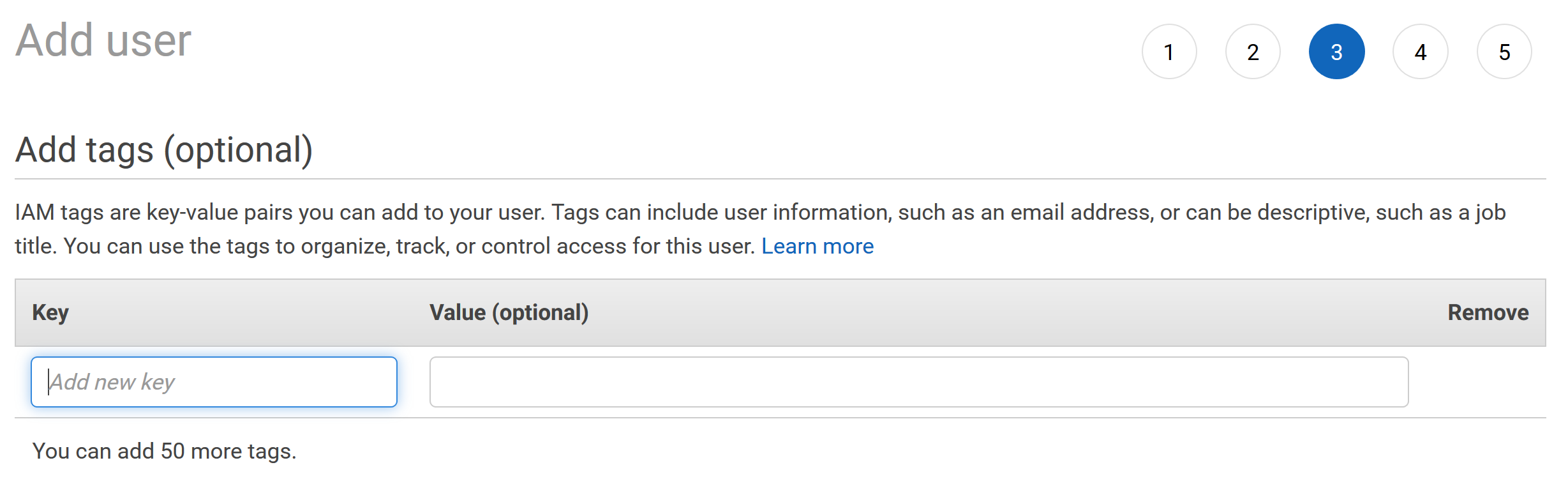
* + Set user details
    - User name: Admin
  + Select AWS access type:
    - Access type: Select AWS Management Console access
    - Console password: Select Custom password and insert a password
    - Require password reset: Unselect (User must create a new password at next sign-in)



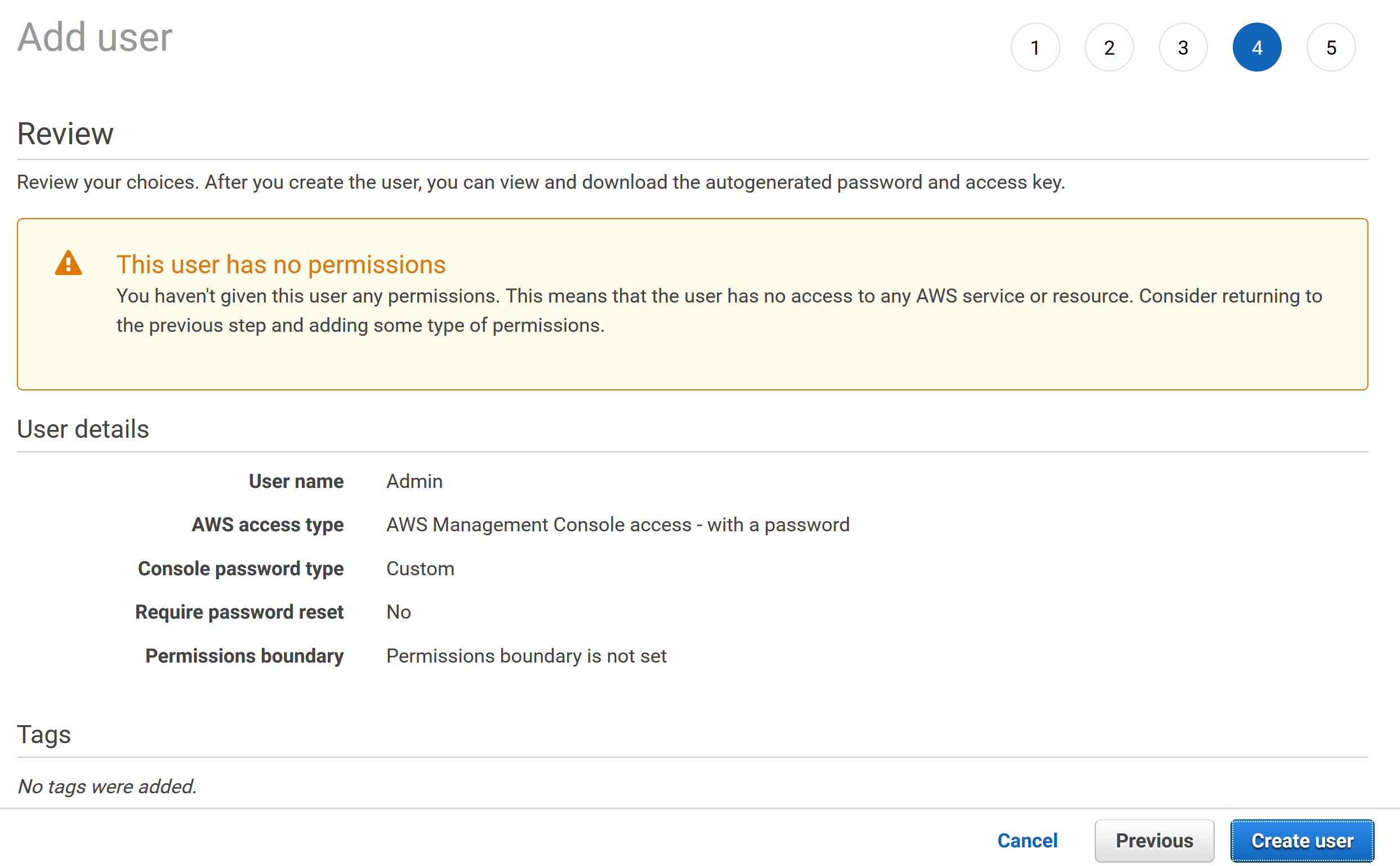
* + Set Permissions

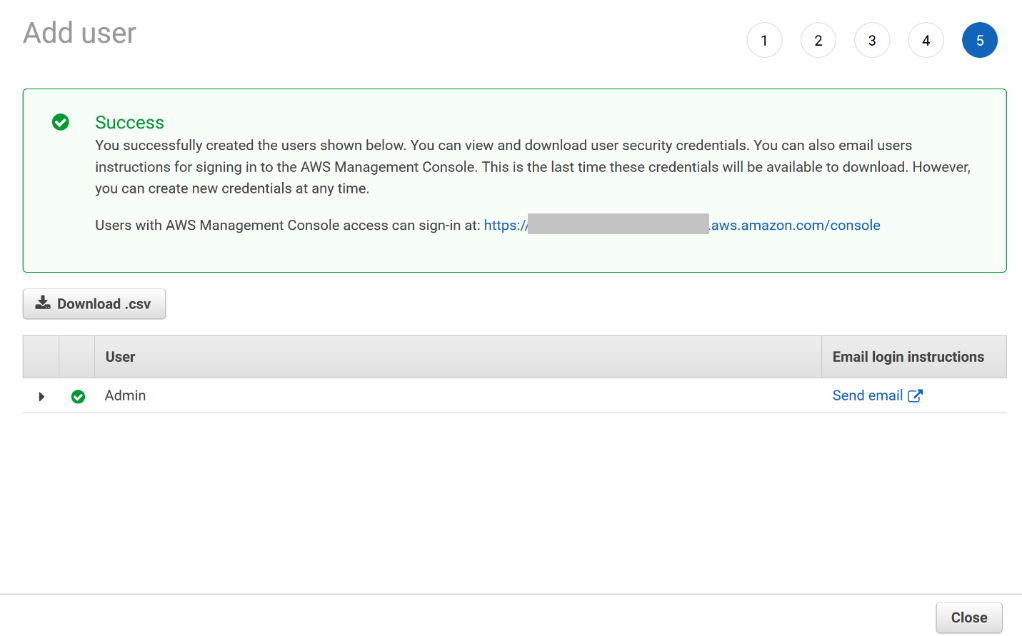


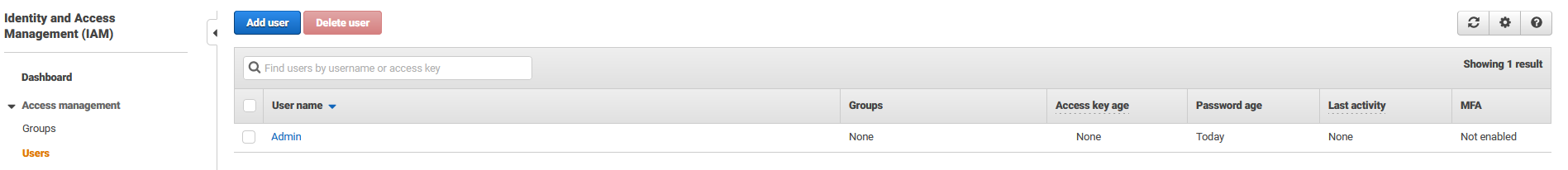
* + Add tags (optional)



* + Review

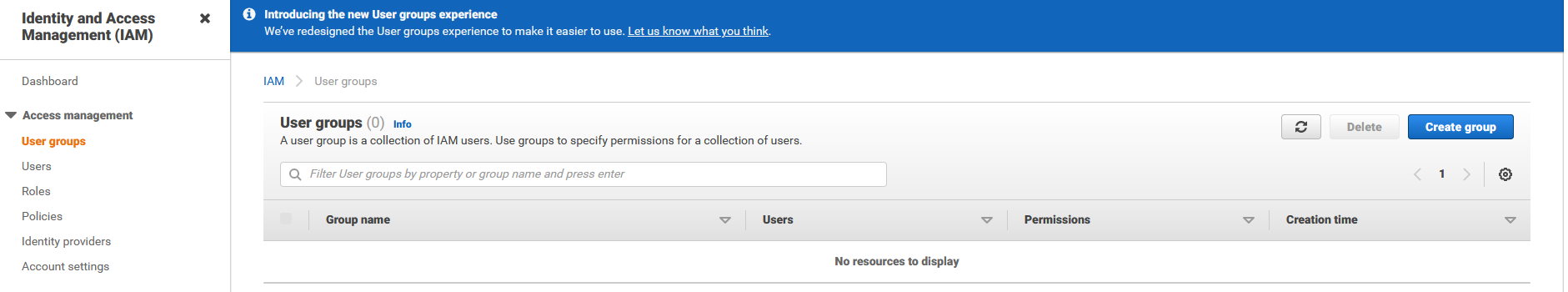






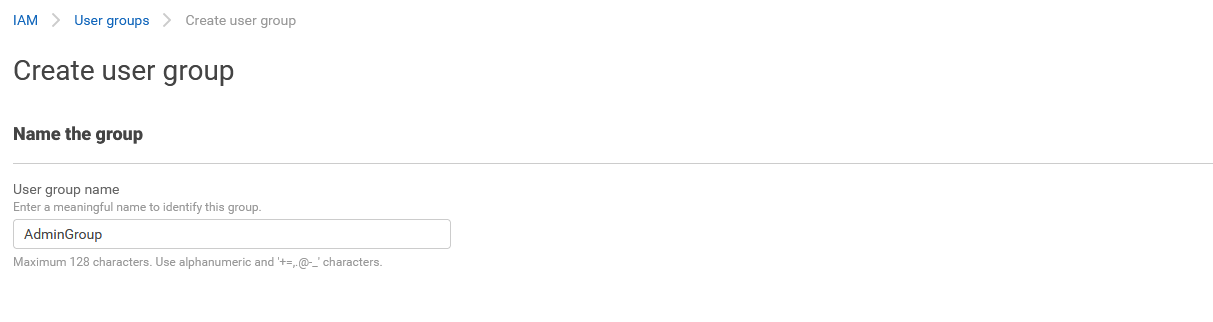
## 5. Use groups to assign permissions

* 1. Select Users under Access Management

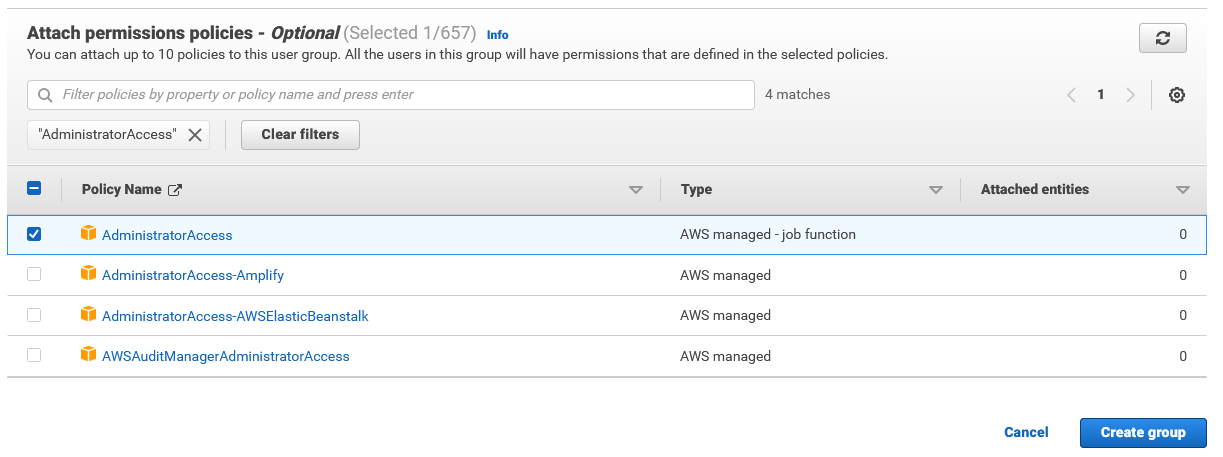


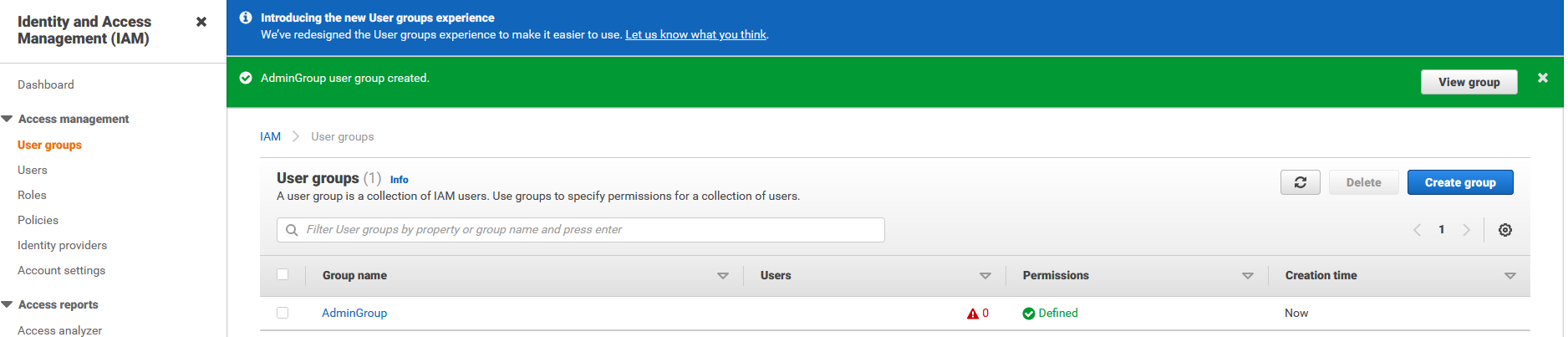
5.2. Create Group

* + Group Name: AdminGroup



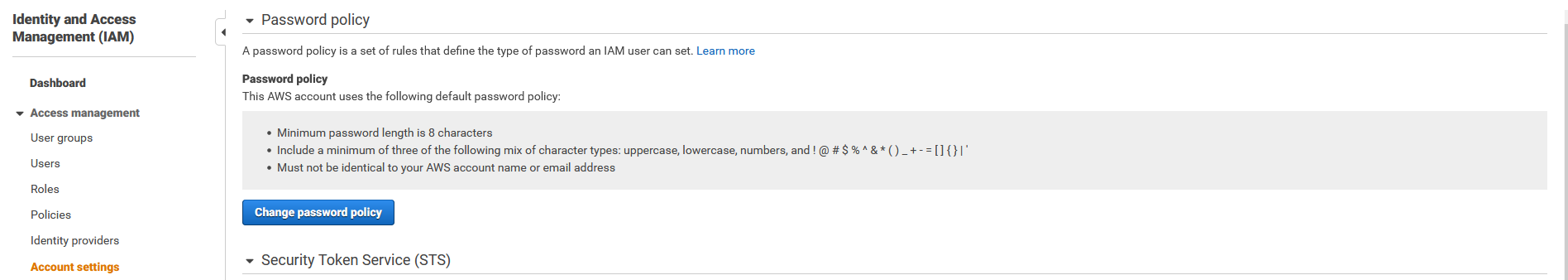
* + Attach Policy AdministratorAccess



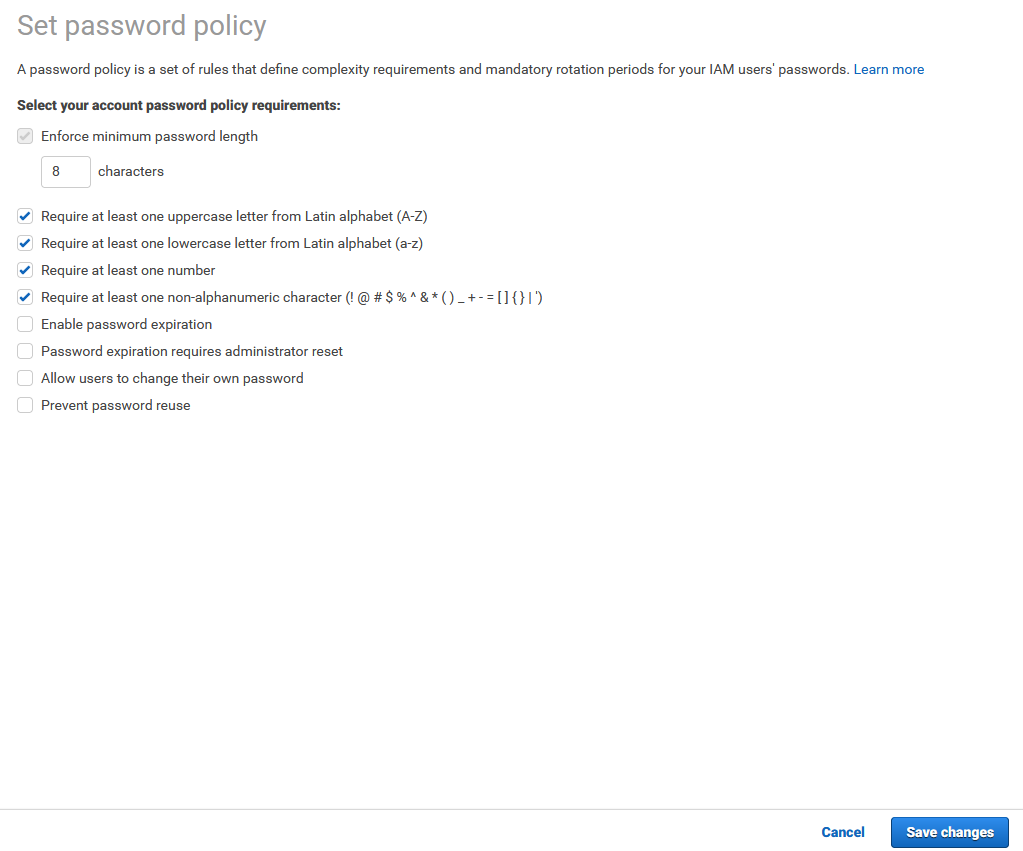


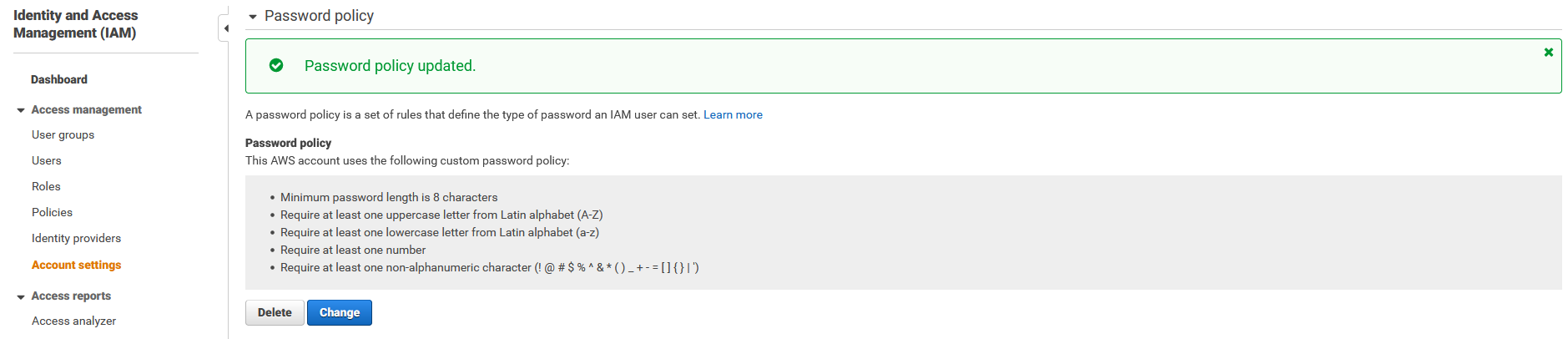
## 6. Apply an IAM password policy

* 1. Select Account Settings under Access Management



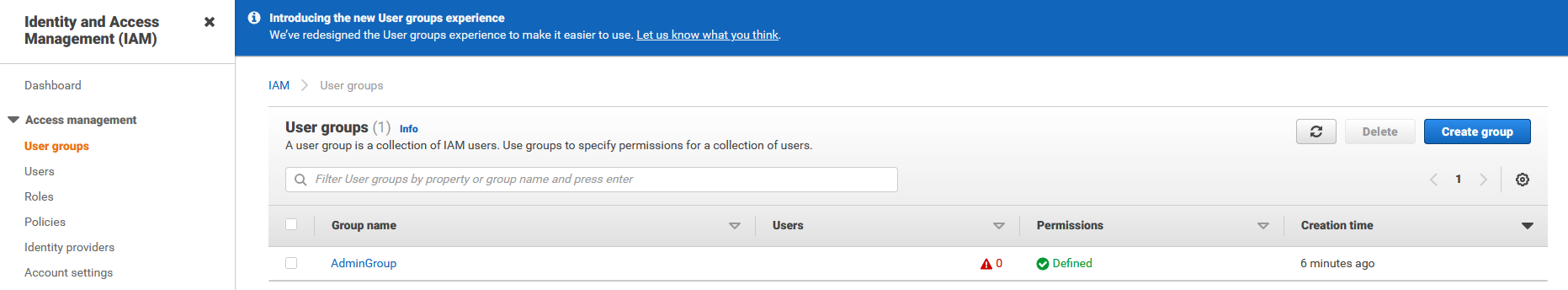
* 1. Select Change password policy



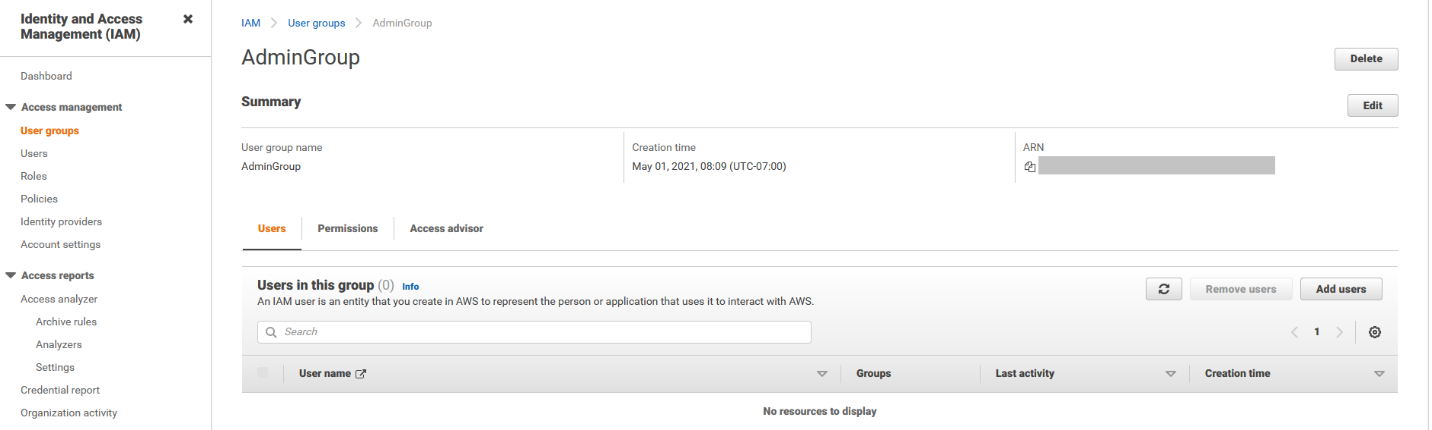


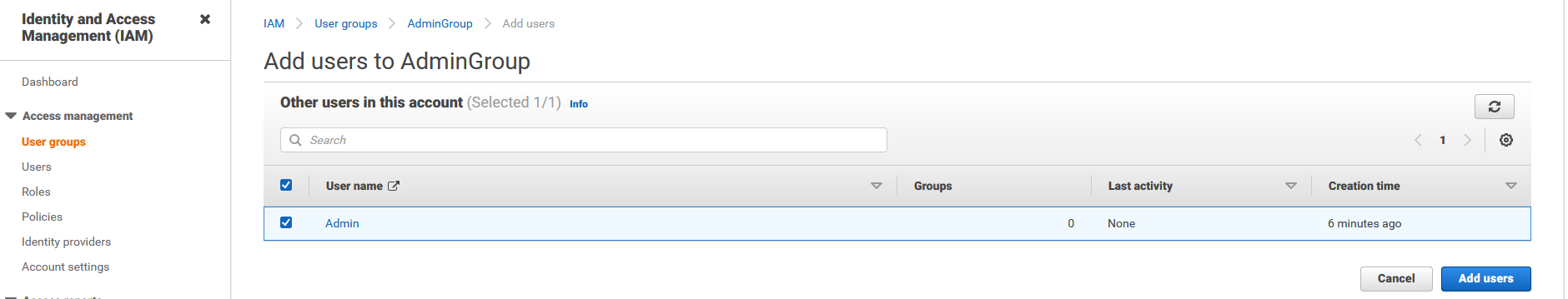
## 7. Add the Admin user to the AdminGroup

* 1. Click on the AdminGroup

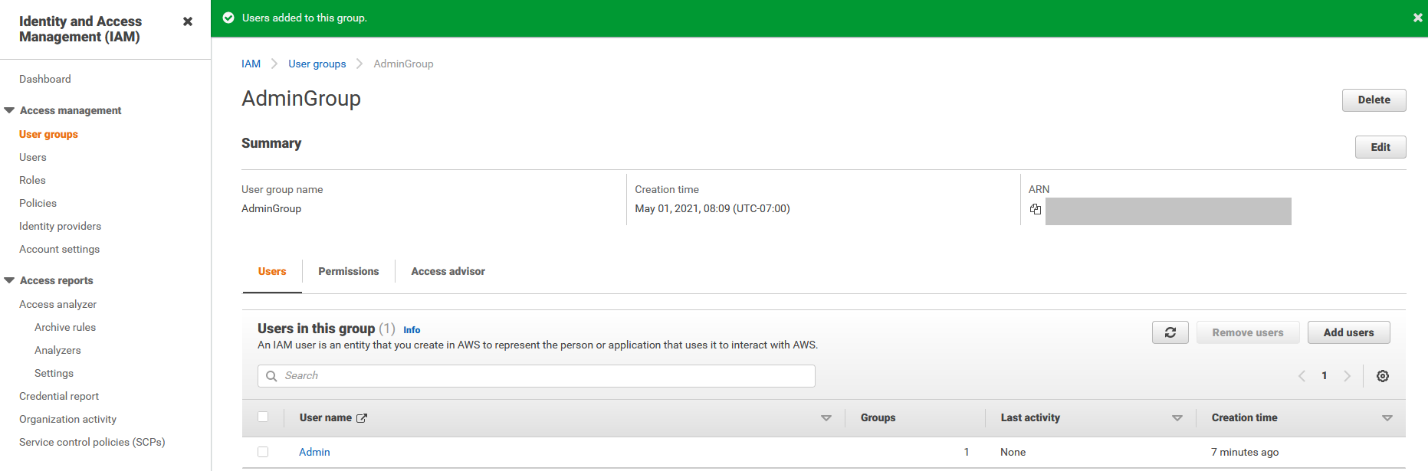


* 1. Click on the Add users and then select the User name **Admin**

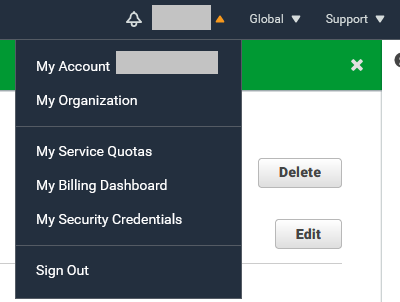




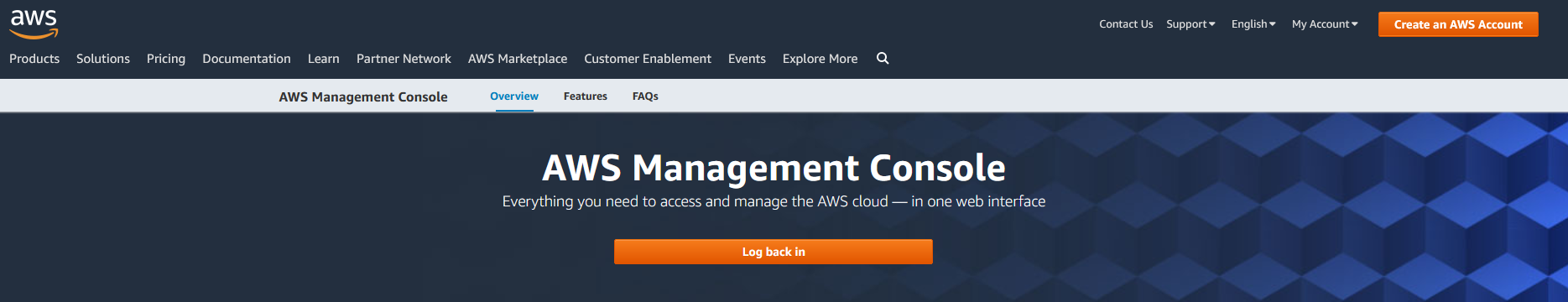
* 1. Click on Add Users



* 1. Take a not of you Account Number (My Account)



* 1. Now Sign out from the root user



* 1. Click Log back in
  2. Sing in with Admin user. You can also setup MFA for the Admin user following the same steps done previously for the root user

