

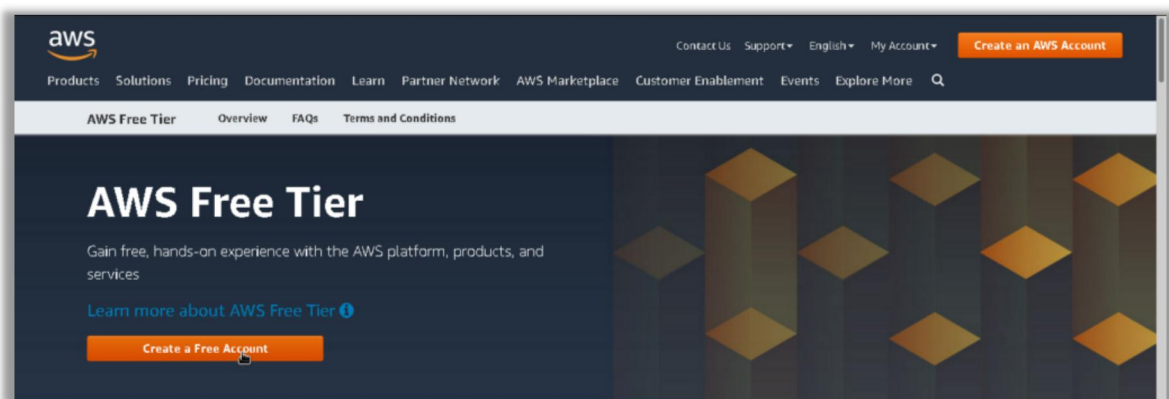
## Assignment: 01

Title: Create an account in AWS and configure the budget.

About Amazon Web Service: Amazon Web Services is one of the most emerging platforms offering services (by using all kind of technologies) that meets the need of any type of business. The AWS Free Tier automatically gets activated on each new AWS account. This lets the user explore all the AWS services free of cost up to specified limits for each service.

(a) Steps to create Amazon Web Service Account(AWS) account:

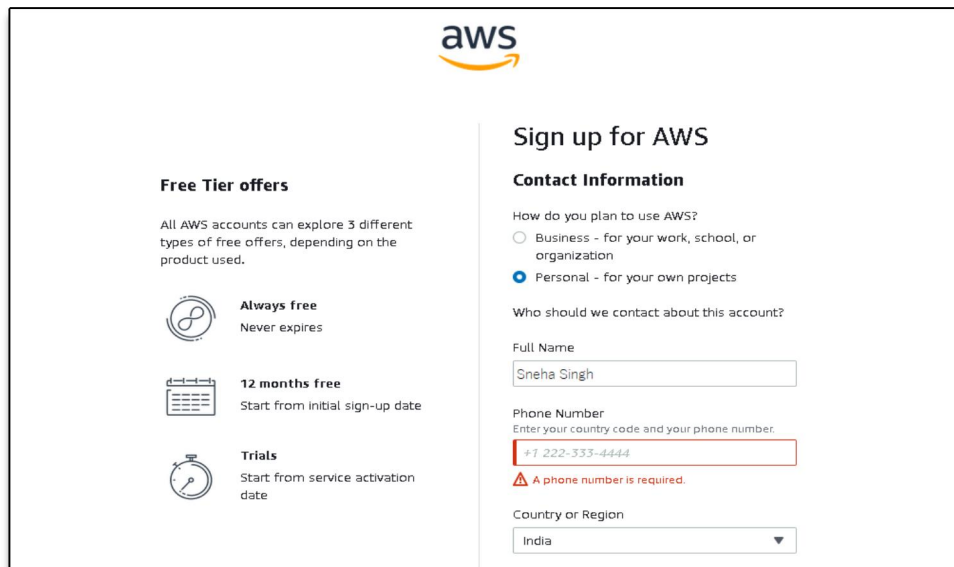
1. Visit the *AWS Free Tier webpage* & click on Create a free account option.



2. Provide your mail id that was never registered with Amazon AWS before then type a password and confirm it and give an *AWS account* name that you can also change after you sign up.

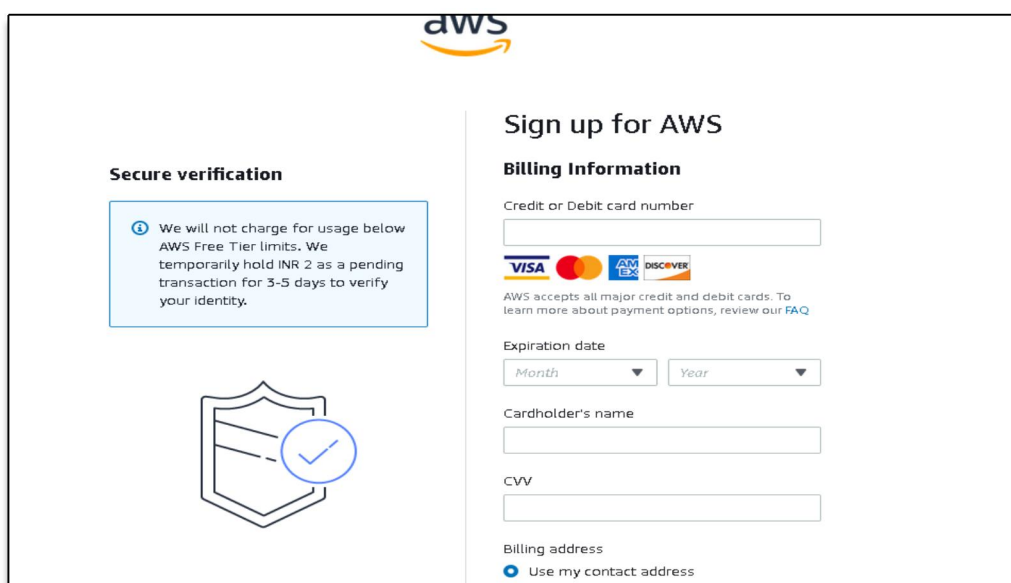
A screenshot of the AWS sign-up form. The form is titled 'Sign up for AWS' and includes fields for 'Email address', 'Password', 'Confirm password', and 'AWS account name'. The email address field contains 'kiya3928@gmail.com'. The password field is masked with dots. The confirm password field is also masked with dots. The AWS account name field contains 'Sneha Singh'. Below the form, there is a 'Continue (step 1 of 5)' button and a link 'Sign in to an existing AWS account'. On the left side of the form, there is a graphic showing a hand holding three cubes, with the text 'Explore Free Tier products with a new AWS account.' and a link 'To learn more, visit aws.amazon.com/free.'

3. Select your AWS type (Professional/ Personal), in our case we choose the **Personal** one , provide other details such as name, address, phone number, state, city, Accept the Terms and conditions and then click Create Account and Continue.



The screenshot shows the AWS sign-up page. On the left, under 'Free Tier offers', it lists three options: 'Always free' (Never expires), '12 months free' (Start from initial sign-up date), and 'Trials' (Start from service activation date). On the right, under 'Sign up for AWS', the 'Contact Information' section is active. It asks 'How do you plan to use AWS?' with radio buttons for 'Business' and 'Personal' (selected). It then asks 'Who should we contact about this account?' followed by input fields for 'Full Name' (Sneha Singh), 'Phone Number' (+1 222-333-4444), and 'Country or Region' (India). A red error message states 'A phone number is required.'

4. Lastly, you have to give the payment details so that after the trial is over they can charge you. After you are done with everything, your AWS Free Tier account will get activated. For the payment , all the credit cards except for RuPay are accepted. I have used my Airtel payments bank account card to complete the creation of my AWS account.

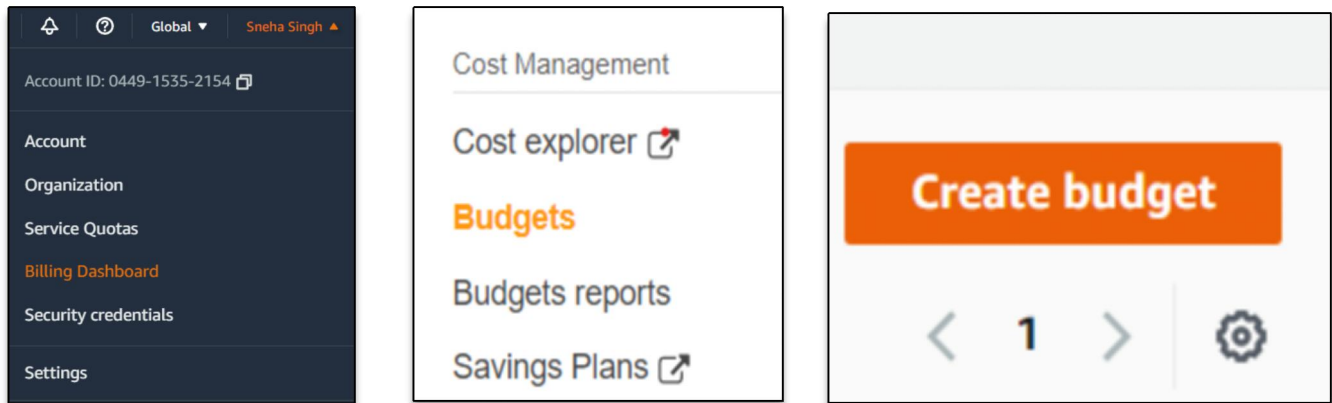


The screenshot shows the AWS sign-up page. On the left, under 'Secure verification', it states 'We will not charge for usage below AWS Free Tier limits. We temporarily hold INR 2 as a pending transaction for 3-5 days to verify your identity.' Below this is a shield icon with a checkmark. On the right, under 'Sign up for AWS', the 'Billing Information' section is active. It includes input fields for 'Credit or Debit card number', 'Expiration date' (Month and Year), 'Cardholder's name', and 'CVV'. Below these is a 'Billing address' section with a radio button for 'Use my contact address' (selected). Logos for VISA, Mastercard, AMEX, and DISCOVER are shown.

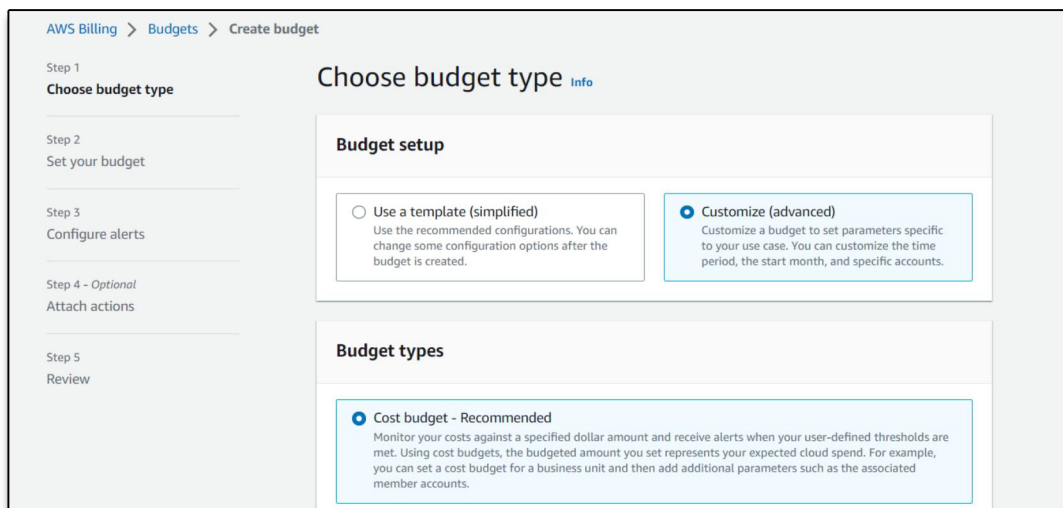
Now, we can easily log in to our AWS management console with our login credentials that is the email Id and password .

## (b) Steps to create and configure a budget :

1. Sign in to the AWS Management Console and open the AWS Cost Management console.
2. On the right side of the navigation bar, choose your account name, and choose **Billing Dashboard**, then on the left side under **Cost Management** choose **Budgets**.
3. At the top of the page, choose **Create budget**



4. Under **Budget setup**, choose **Customize (advanced)**.
5. Under **Budget types**, choose **Cost budget**. Then, choose **Next**.



6. Under **Details**, for **Budget name**, let's say **Budget-1** enter the name of your budget. Your budget name must be unique within your account. It can contain A-Z, a-z, spaces, and the following characters: `_./=+-%@`.
7. Under **Set budget amount**, for **Period**, choose how often you want the budget to reset the actual and forecasted spend. Select **Daily** for every day, **Monthly** for every month, **Quarterly** for every three months, or **Annually** for every year. We are choosing **Monthly**

**8. For Budget renewal type, choose *Recurring budget* for a budget that resets after the budget period. *Budgeted Amount - \$1.00* , Choose *Next*.**

The screenshot shows two panels from the AWS Budgets console. The left panel, titled 'Step 2: Set your budget', contains a sidebar with steps 2 through 5 and a main area with three steps: 'Step 1: Enter your budget details' (Define the budget name), 'Step 2: Set budget amount' (Select the period and whether you would like to have a fixed budget or to specify a budget plan, then enter your budget amount), and 'Step 3: Scope your budget - optional' (Add dimensions of data to narrow on a set of cost information). The 'Details' section shows a 'Budget name' field with the value 'B1'. The right panel, titled 'Set budget amount', shows the 'Period' set to 'Monthly', 'Budget renewal type' set to 'Recurring budget', 'Start month' set to 'Feb 2023', 'Budgeting method' set to 'Fixed', and 'Enter your budgeted amount (\$)' set to '1.00'.

**9. Choose *Add an alert threshold*.**

**10. Under *Set alert threshold*, for **Threshold**, enter the amount that must be reached for you to be notified. This can be either an absolute value or a percentage. For example, say you have a budget of 200 dollars. To be notified at 160 dollars (80% of your budget), enter **160** for an absolute budget or **80** for a percentage budget. We Choose *Percentage budget*.**

**11. Under *Notification preferences*, for **Email recipients**, enter the email addresses that you want the alert to notify. Separate multiple email addresses with commas. Review your budget settings, and then choose *Create budget*.**

The screenshot shows the 'Alert #1' configuration screen. It has a 'Remove' button in the top right. The 'Set alert threshold' section has a 'Threshold' field with the value '80' and a dropdown menu set to '% of budgeted amount'. The 'Trigger' section has a dropdown menu set to 'Actual'. A summary text states: 'Summary: When your actual cost is greater than 80.00% (\$0.80) of your budgeted amount (\$1.00), the alert threshold will be exceeded.' The 'Notification preferences' section has a text input field for 'Email recipients' with the value 'snehasinggh65@gmail.com'. Below this, there are links for 'Amazon SNS Alerts - Optional info' and 'AWS Chatbot Alerts'.

The budget has been created .  
And it can be observed in the  
the overview section of the  
Budgets as ***Budget-1***

The screenshot shows the 'Overview' section of the AWS Budgets console. It has a breadcrumb trail 'AWS Billing > Budgets > Overview'. The 'Overview' section has a search bar and a table with the following data:

	Name	Thresholds	Budget
<input type="checkbox"/>	Budget-1	OK	\$1.00

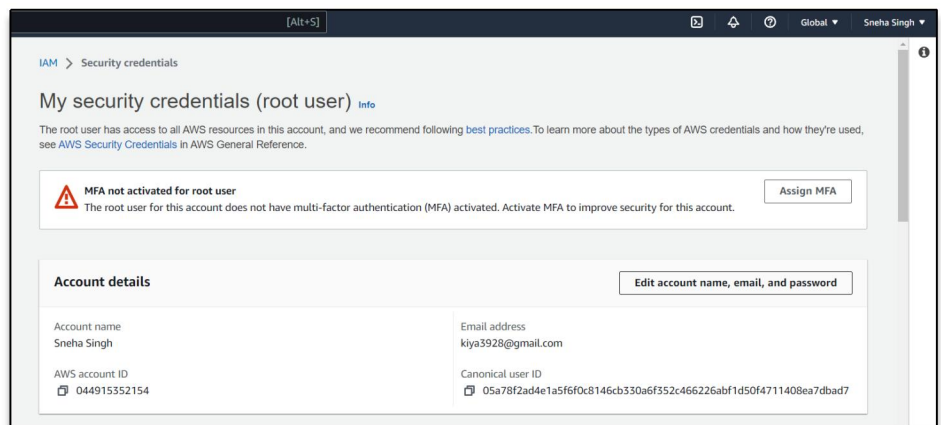
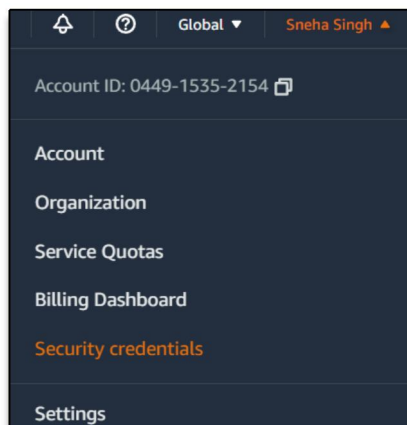
## Assignment: 02

### Title: Create MFA for authentication.

Multi - Factor authentication (MFA) :MFA adds extra security because it requires users to provide unique authentication from an AWS supported MFA mechanism in addition to their regular sign-in credentials when they access AWS websites or services. For increased security, we recommend that you configure multi-factor authentication (MFA) to help protect your AWS resources. You can enable MFA for the AWS account root user and IAM users. When you enable MFA for the root user, it affects only the root user credentials.

### Using multi-factor authentication (MFA) in AWS :

1. Sign in to the AWS Management Console.
2. On the right side of the navigation bar, choose your account name, and choose **Security credentials**. If necessary, choose **Continue to Security credentials**.
3. In the **Multi-Factor Authentication (MFA)** section, choose **Assign MFA device**.



4. In the wizard, type a **Device name** let it be **d1**, choose **Authenticator app**, and then choose **Next**.
5. It displays configuration information for the virtual MFA device, including a QR code graphic. The graphic is a representation of the secret configuration key that is available for manual entry on devices that do not support QR codes.



IAM > Security credentials > Assign MFA device

Step 1  
Select MFA device

### Select MFA device

**Specify MFA device name**

Device name  
Enter a meaningful name to identify this device.

Maximum 128 characters. Use alphanumeric and \* , . , @ , - , \_ characters.

Device name:

**Select MFA device** [Info](#)

Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.


☒ **Authenticator app**  
Authenticate using a code generated by an app installed on your mobile device or computer.

☐ **Security Key**  
Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.

Step 2  
Set up device

### Set up your authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1. Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.  
[See a list of compatible applications](#)
2.  Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key.  
[Show secret key](#)
3. Fill in two consecutive codes from your MFA device.

MFA code 1:

MFA code 2:

6. Open the virtual MFA app on the device.

7. To use the QR code to configure the virtual MFA device, from the wizard, choose **Show QR code**. Then follow the app instructions for scanning the code. For example, you might need to choose the camera icon or choose a command like **Scan account barcode**, and then use the device's camera to scan the QR code. We have used the **Google Authenticator** app for authentication.

8. The device starts generating six-digit numbers.

9. In the wizard, in the **MFA code 1** box, type the one-time password that currently appears in the virtual MFA device. Wait up to 30 seconds for the device to generate a new one-time password. Then type the second one-time password into the **MFA code 2** box. Choose **Add MFA**.

### Multi-factor authentication (MFA) (1)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned.  
[Learn more](#)

Device type	Identifier	Created on
<input checked="" type="radio"/> Virtual	arn:aws:iam::869659422847:mfa/D1	Now

The device is ready for use with AWS. For information about using MFA with the AWS Management Console.

Now, when we sign out of the console, everytime we log in again we need to enter the MFA code generated by the Authenticator app to successfully sign in to our AWS account.

## Assignment : 03

### Title : Create IAM user and thereby give full access of S3

**AWS Identity and Access Management (IAM):** It is a web service that helps you securely control access to AWS resources. With IAM, you can centrally manage permissions that control which AWS resources users can access. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

### Steps to create an IAM User :

#### A. Creating a user :

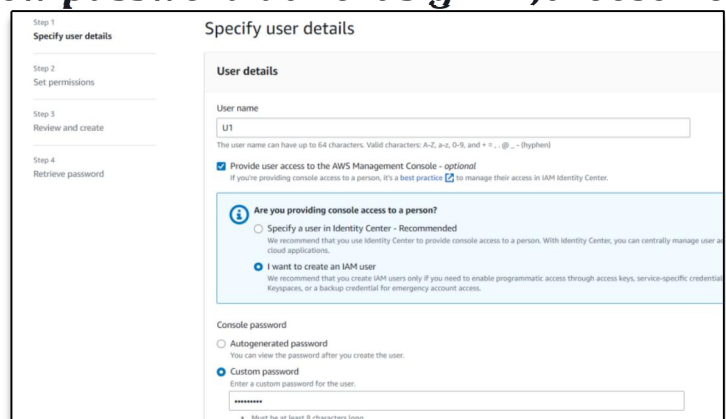
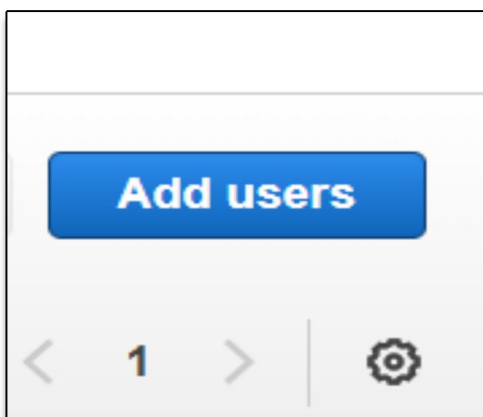
1. Sign in to the AWS Management Console and open the IAM console
2. In the navigation pane, choose **Users** and then choose **Add user**.
3. Type the user name for the new user , Lets say **U1**. This is the sign-in name for AWS.
4. Select the type of access this user will have.

We will go for **Console password**, choose one of the following:

**Auto-generated password** – The user gets a randomly generated password that meets the [account password policy](#).

**Custom password** – The user is assigned the password that you type in the box. We will assign a password we want to give for the IAM username.

5. Uncheck **Users must create a new password at next sign-in**, choose **Next**.



6. On the **Set permissions** page, specify how you want to assign permissions to this set of new users:

**Add user to group** – Choose this option if you want to assign the user to one or more groups that already have permissions policies. IAM displays a list of the groups in your account, along with their attached policies.

7. On the **Review and create** page, review all of the choices you made up to this point. When you are ready to proceed, choose **Create user**.

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.

[Get started with groups](#)  
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

Create group

Permissions boundary - optional  
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. [Learn more](#)

Cancel Previous Next

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: U1

Console password type: Custom password

Require password reset: No

Permissions summary

Name	Type	Used as
No resources		

8. To save the password, choose **Download.csv** and then save the file to a safe location. Choose **Return to users list**.

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://044915352154.signin.aws.amazon.com/console>

User name  
U1

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

Download .csv file Return to users list

### B. Creating a group and adding the user to it.

1. As the user U1 is created , Click on the **user U1**.

Users (1) Info

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

Find users by username or access key

User name	Groups	Last activity
U1	None	Never

2. On clicking U1 it will show all the summary , description and properties related to the User created. It will consist of tabs like **Permissions, Groups , Tags , Security credentials and Access advisor**. Choose **Groups** and then click on **Add user to groups**. Choose **Create group**.



3. Create user group window will appear , provide with a **User group name g1** lets say. In **permission policies** search for **S3** and select first two options , which means the group will provide full access for S3.

### U1

#### Summary

ARN  
arn:aws:iam::044915352154:user/U1

Created  
February 21, 2023, 01:19 (UTC+05:30)

Console access  
Enabled without MFA

Last console sign-in  
Never

Permissions

Groups

Tags

Security credentials

Access Advisor

#### User groups membership (0)

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

Remove

Add user to groups

Create user group

Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

User group name  
Enter a meaningful name to identify this group.  
g1  
Maximum 128 characters. Use alphanumeric and '+', '@', '-' characters.

Permissions policies (2/816)

Q s3

9 matches

< 1 >

<input type="checkbox"/>	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	AmazonD...	AWS managed	None	Provides access to ...
<input checked="" type="checkbox"/>	AmazonS3...	AWS managed	None	Provides full access ...
<input type="checkbox"/>	AmazonS3...	AWS managed	None	Provides AWS Lamb...

4.Complete the step and then the g1 appears in our user group list , Choose **Add user to group(s)**.

### Add user U1 to groups

Select which groups to add the user U1.

Other groups (1)

Q Search groups

☐

g1

1

AmazonDMSRedshiftS3Role and AmazonS...

2023-02-21 (Now)

Cancel

Add user to group(s)

5.The user U1 is added to group g1 and now we can login to the AWS console as IAM user using the username / login credentials of user U1.

### Users (1) Info

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

Q Find users by username or access key

< 1 >

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	U1	g1	Never	None	5 minutes ago	-

### Sign in as IAM user

Account ID (12 digits) or account alias  
https://044915352154.signin.aws.amazon.com

IAM user name  
U1

Password  
\*\*\*\*\*

☐ Remember this account

Sign in

Log in to your AWS account using the **account id, password and username** generated by the user U1 created , which were already saved in the .csv file, saved earlier. Now, you can continue using the AWS console as an **IAM user**.

N. Virginia U1 @ 0449-1535-2154

Account ID: 0449-1535-2154  
IAM user: U1

Account

Organization

Service Quotas

Billing Dashboard

Security credentials

Settings