

Module 2: Security Management in AWS

Demo Document 1

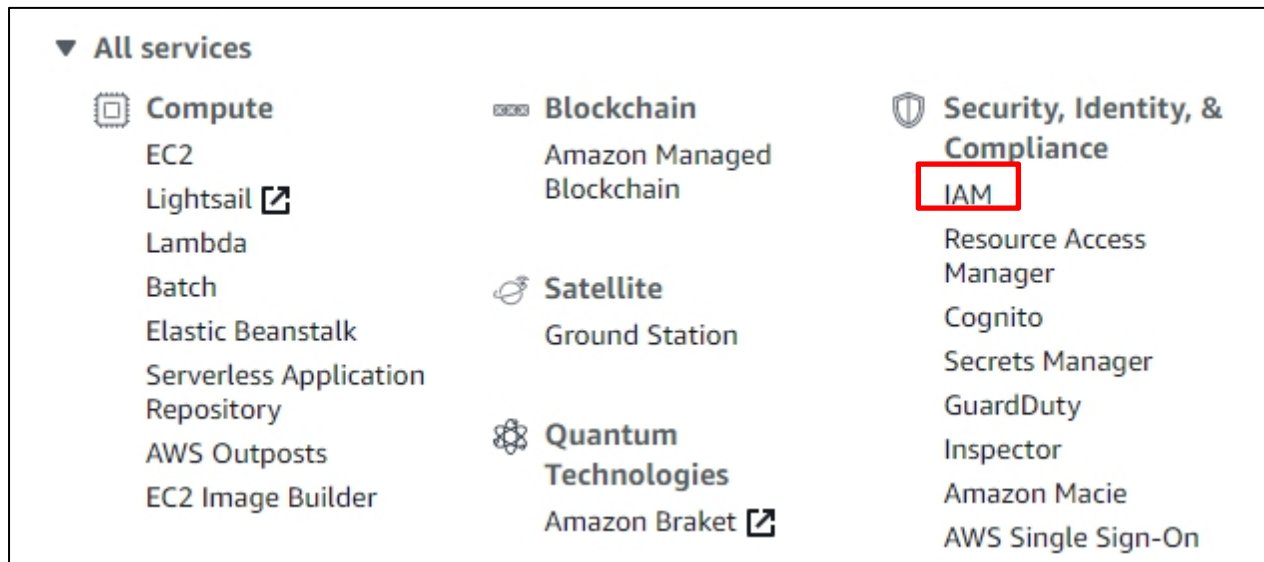
edureka!

edureka!

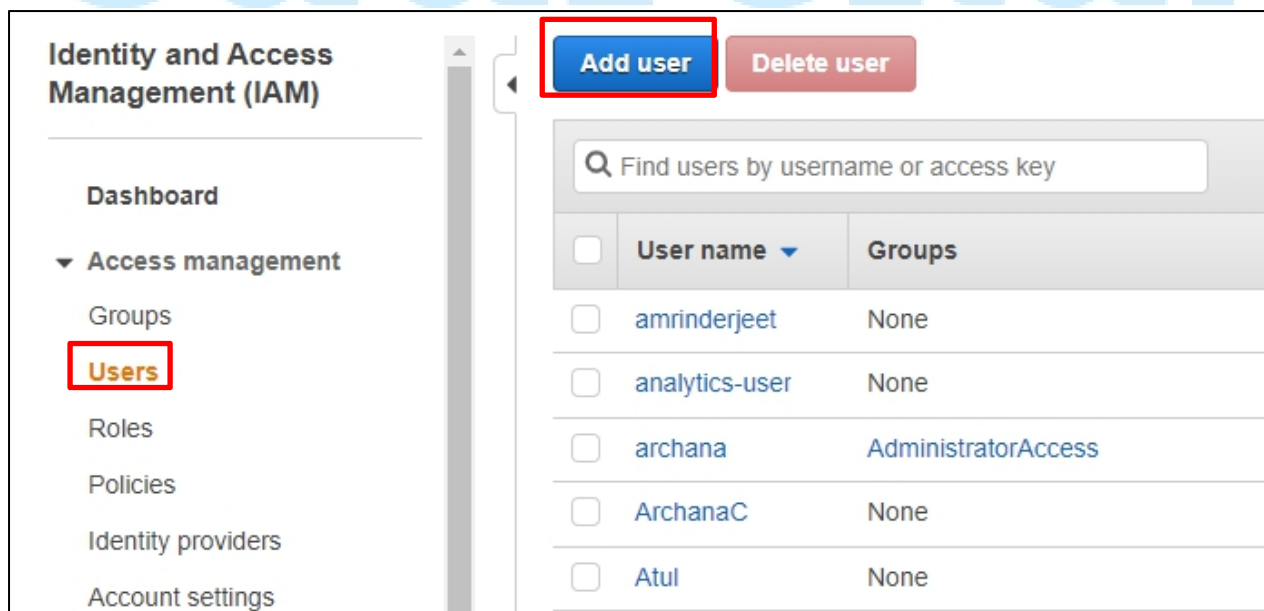
© Brain4ce Education Solutions Pvt. Ltd.

Creating New User to Log in to AWS Management Console

Step 1: Go to the AWS Management Console. Under the Security, Identity, and Management category, click on **IAM**.



Step 2: Go to **Users** and click on **Add user**.



Step 3: Enter the **User name** and fill the following details and click on **Next**.

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

Archana

[Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type*

☐

Programmatic access
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.

☒

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

☒ User must create a new password at next sign-in

Step 4: Now click on **Create group**.

▼ Set permissions

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

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](#)

Add user to group

Showing 14 results

Group	Attached policies
<input type="checkbox"/> devops	AmazonEC2FullAccess and 6 more
<input type="checkbox"/> admin	AmazonS3FullAccess
<input type="checkbox"/> AdministratorAccess	AdministratorAccess
<input type="checkbox"/> AdministratorAccess1	AdministratorAccess

Step 5: Enter the field with the group name and attach the **policy**. Click on **Create group**.

Add user

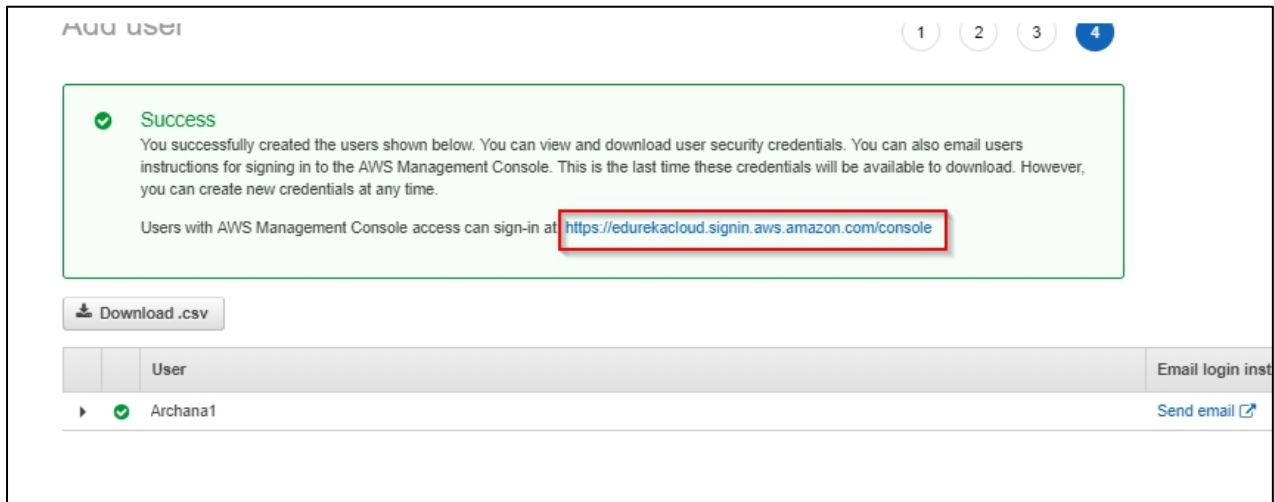
Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions b

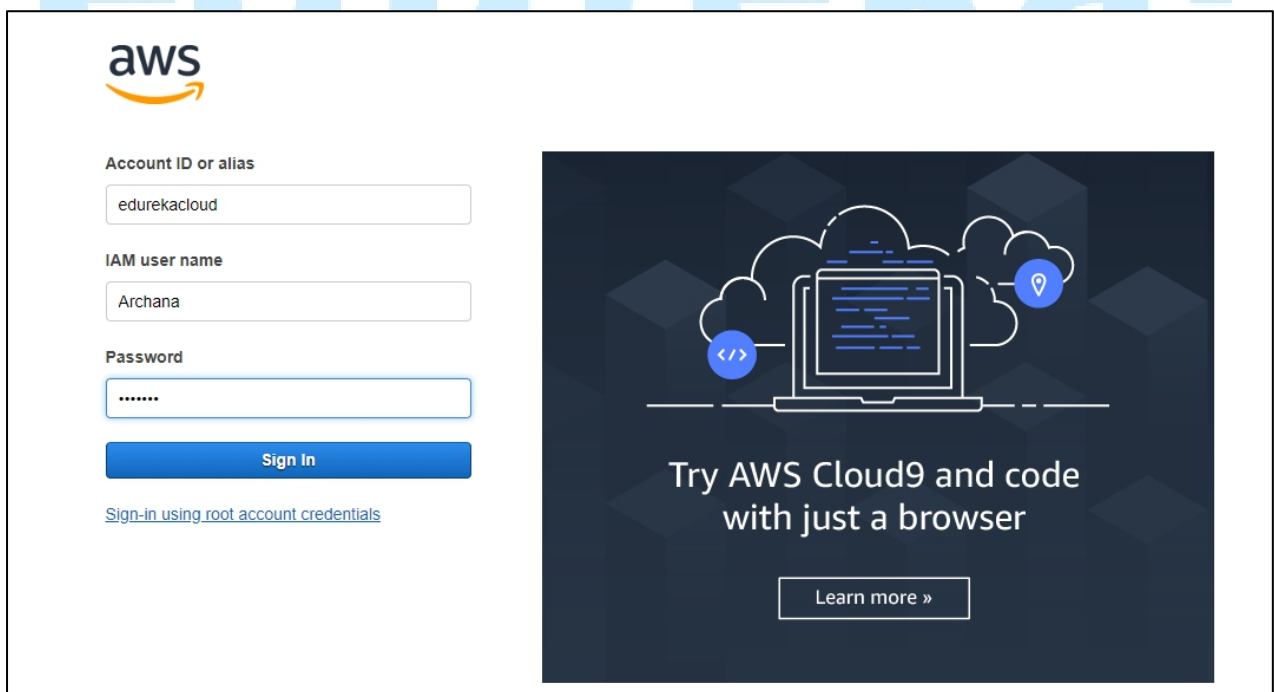
Group name

	Policy name	Type	Used as
<input checked="" type="checkbox"/>	AdministratorAccess	Job function	Permissions policy (24)
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS managed	None

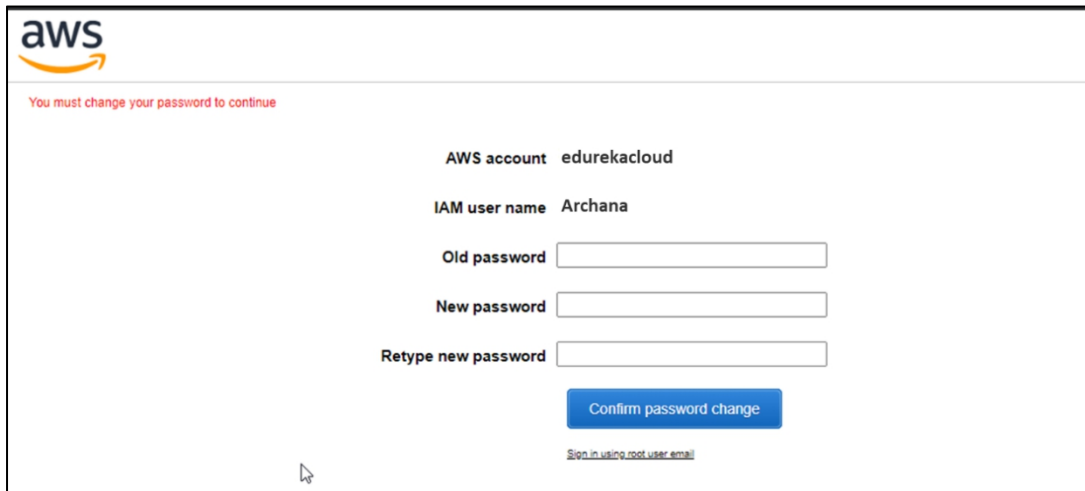
Step 6: Attach the group to **User** and copy the URL when you complete it successfully.



Step 7: Paste the URL in a browser and enter the created user-name and password to sign in to the AWS account.



Step 8: Fill the required details, configure the new password and click on ***confirm password change***.



The screenshot shows the AWS IAM console interface for changing a password. At the top left is the AWS logo. Below it, a red message states: "You must change your password to continue". The page displays the following information and fields:

- AWS account:** edurekacloud
- IAM user name:** Archana
- Old password:** [Text input field]
- New password:** [Text input field]
- Retype new password:** [Text input field]
- Confirm password change:** [Blue button]
- [Sign in using root user email](#) [Link]

Conclusion:

We have successfully created an **IAM user** to log in to the AWS Management Console.