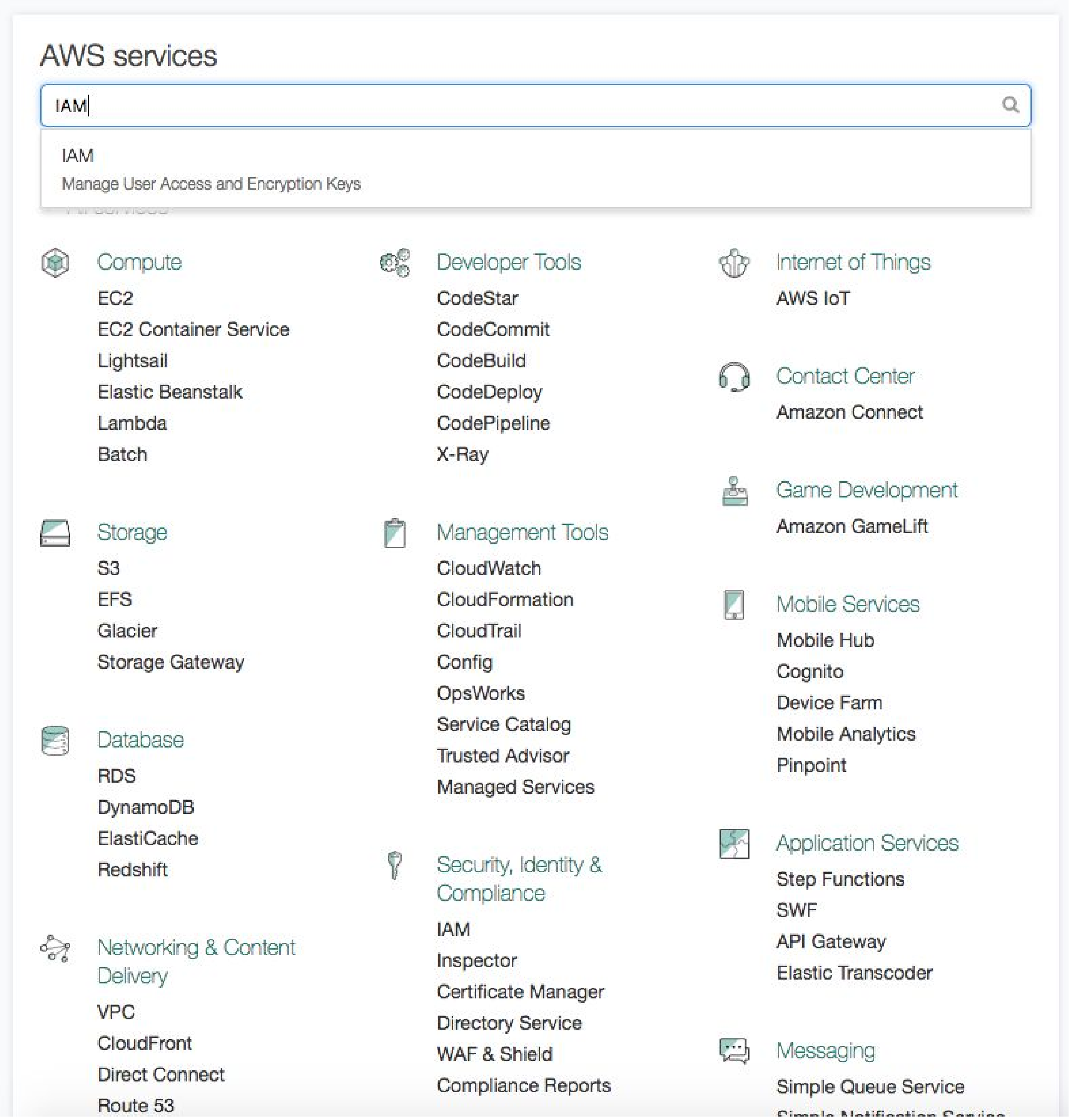
Getting Started with AWS

Create AWS IAM User Access Key and Secret Key

- ➔ Log in to **aws.amazon.com** with your login credentials.
- ➔ Search for IAM service and click on it.

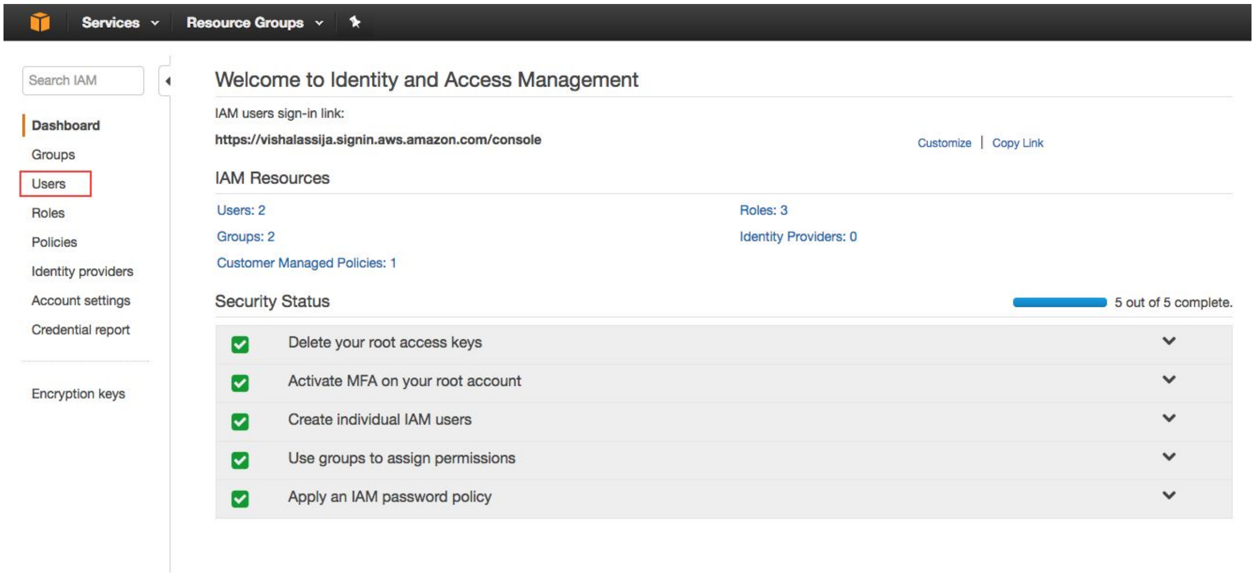


AWS services

IAM

IAM
Manage User Access and Encryption Keys

- ➔ Under IAM screen tap on ‘Users’ option.



Welcome to Identity and Access Management

IAM users sign-in link:
https://vishalassija.signin.aws.amazon.com/console

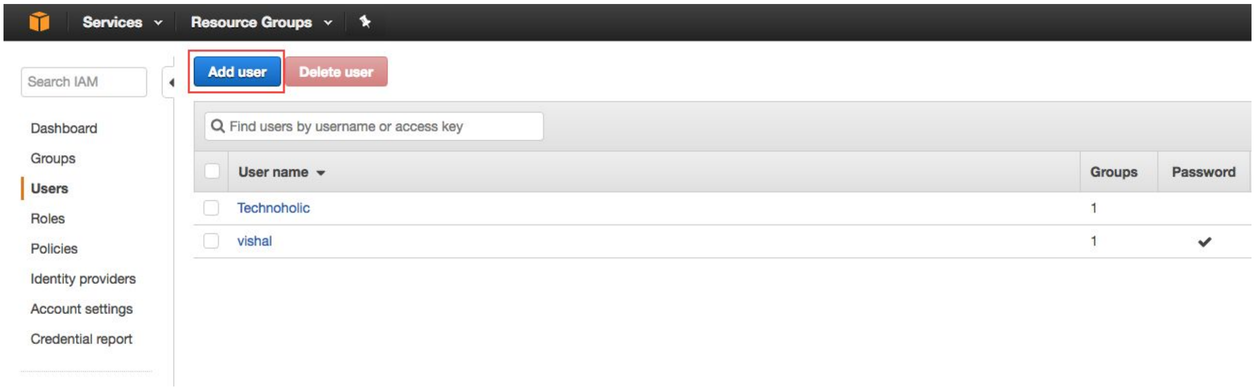
IAM Resources

Users: 2	Roles: 3
Groups: 2	Identity Providers: 0
Customer Managed Policies: 1	

Security Status — 5 out of 5 complete.

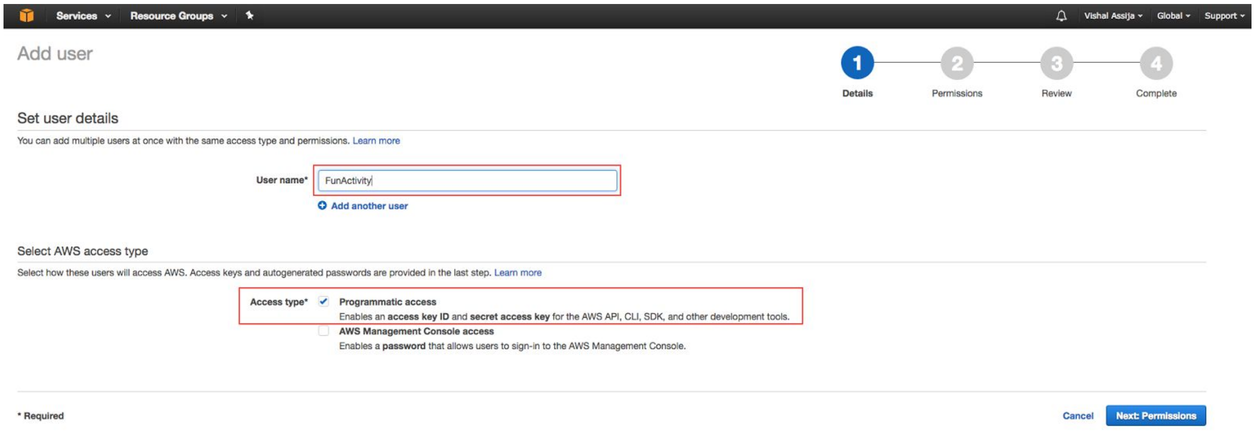
- ☑ Delete your root access keys
- ☑ Activate MFA on your root account
- ☑ Create individual IAM users
- ☑ Use groups to assign permissions
- ☑ Apply an IAM password policy

➔ Now click on ‘Add User’ button.



□	User name	Groups	Password
□	Technoholic	1	
□	vishal	1	✓

➔ Enter username and Make sure you mark Programmatic Access.



Add user

Set user details

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

User name* FunActivity

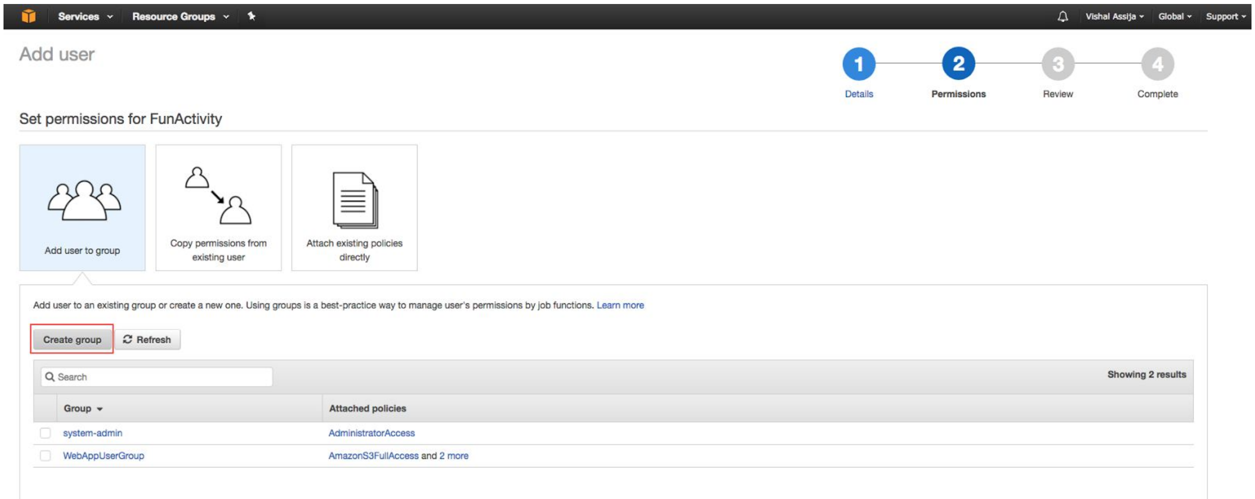
Select AWS access type

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.

* Required

➔ Create a new group for user to be added.



Add user

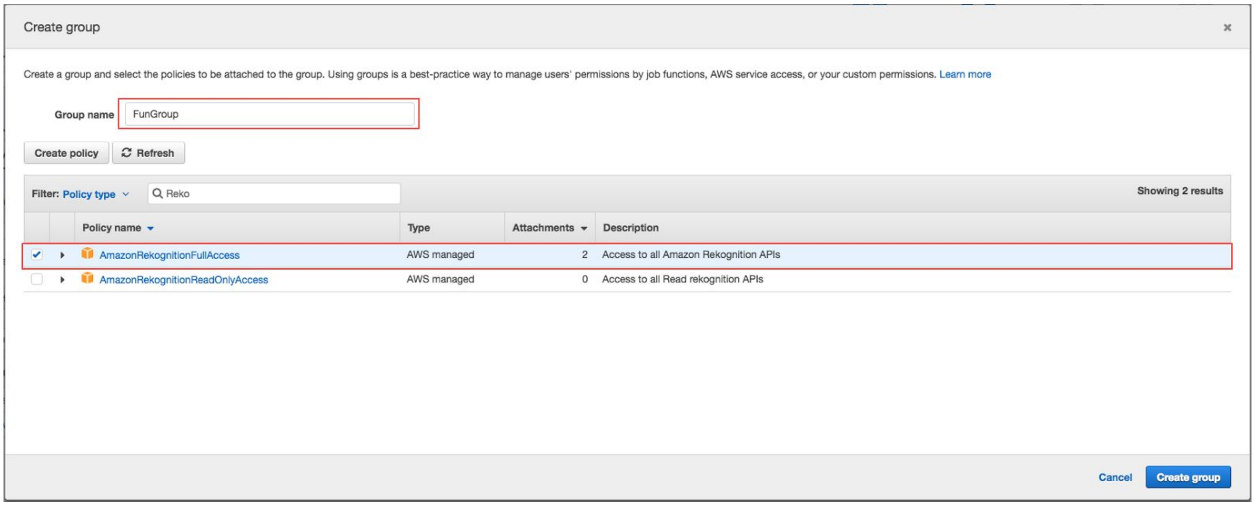
Set permissions for FunActivity

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

Showing 2 results

	Group	Attached policies
□	system-admin	AdministratorAccess
□	WebAppUserGroup	AmazonS3FullAccess and 2 more

- ➔ Give group a name and make sure you have associated following two policies with group:
  - ◆ RekognitionFullAccess
  - ◆ PollyFullAccess



Create group

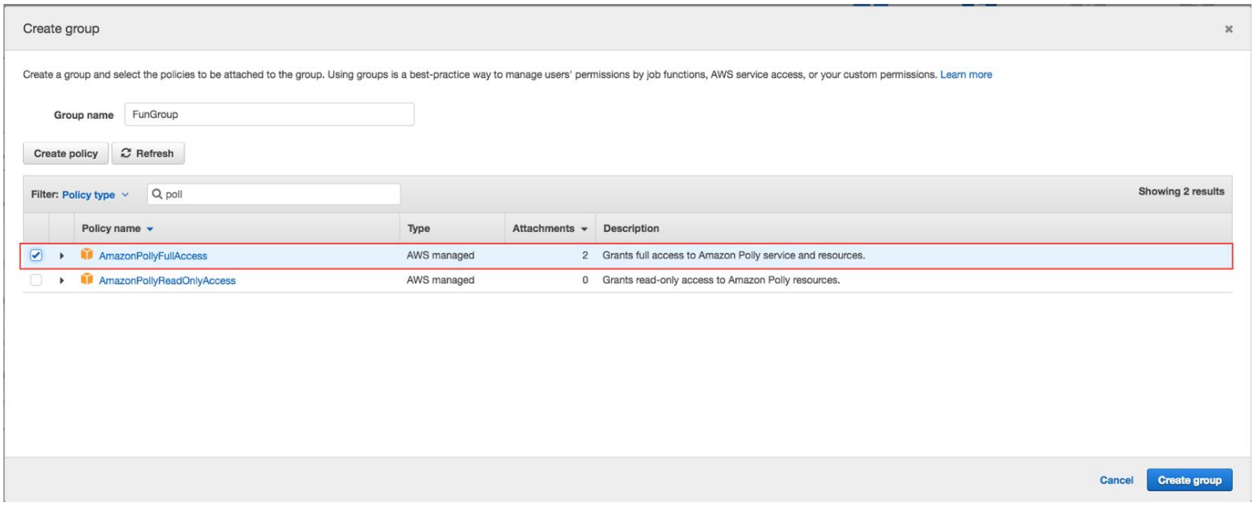
Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Learn more

Group name: FunGroup

Filter: Policy type: Reko

Showing 2 results

	Policy name	Type	Attachments	Description
☑	AmazonRekognitionFullAccess	AWS managed	2	Access to all Amazon Rekognition APIs
□	AmazonRekognitionReadOnlyAccess	AWS managed	0	Access to all Read rekognition APIs



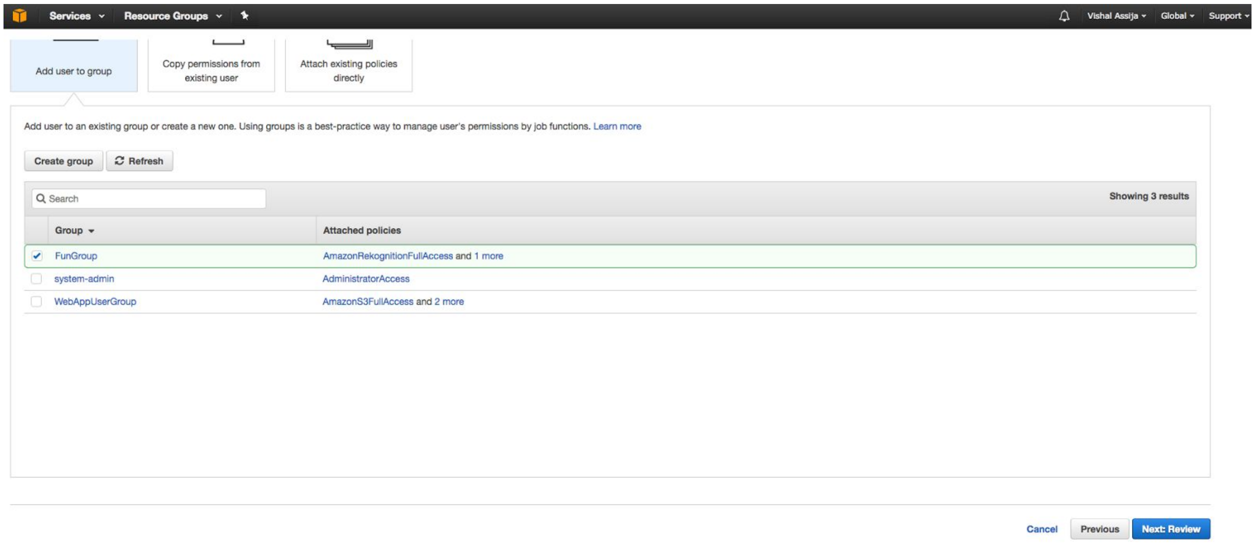
Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Learn more

Group name: FunGroup

Filter: Policy type — poll — Showing 2 results

		Policy name	Type	Attachments	Description
☑	▸	AmazonPollyFullAccess	AWS managed	2	Grants full access to Amazon Polly service and resources.
□	▸	AmazonPollyReadOnlyAccess	AWS managed	0	Grants read-only access to Amazon Polly resources.

➔ Once you have selected both the policies tap on ‘Create Group’ button.


Services
Resource Groups
Vishal Assija
Global
Support
Add user to group
Copy permissions from existing user
Attach existing policies directly

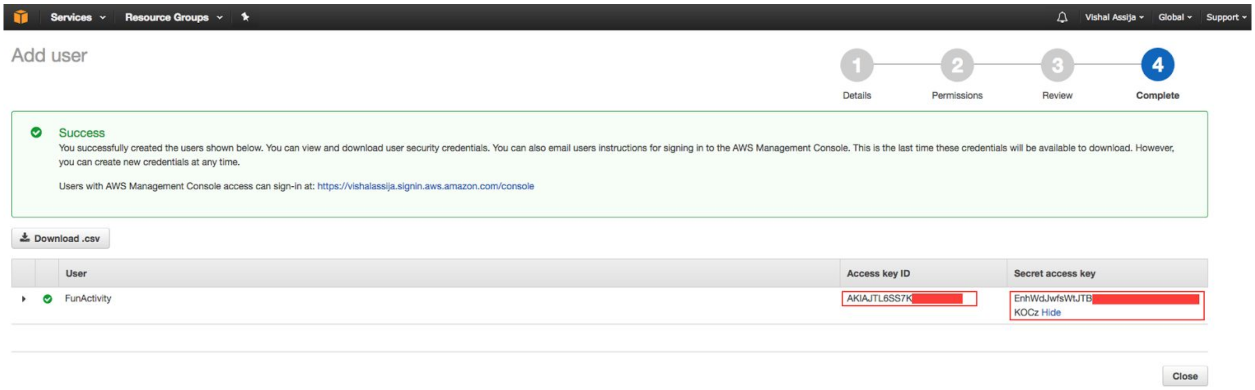
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Showing 3 results

	Group	Attached policies
☑	FunGroup	AmazonRekognitionFullAccess and 1 more
□	system-admin	AdministratorAccess
□	WebAppUserGroup	AmazonS3FullAccess and 2 more

➔ So once you selected the newly created group, tap on Next button to review all the things that you have done so far. And hit create button.

P.S. Please make sure to download newly created user Access Key and Secret Key as .csv file or copy from the screen that you will see after you hit create. (Since after that you will not be able recover them and you need to follow the whole process again.)



Add user

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://vishalassija.signin.aws.amazon.com/console

		User	Access key ID	Secret access key
▸	✓	FunActivity	AKIAJTL6SS7K[redacted]	EnhWdJwfsWtJTB[redacted] KOCz Hide