EXPLORE DIGITAL SKILLS

Set Up Your Everyday IAM User Account

Train Overview

In this train, you will learn how to create an IAM user account with full administrator privileges for daily use. This will help to protect your root user account from any unauthorised access.

We will cover the following topics:

01 AWS Identity Access Management(IAM) service.

02 IAM User Authentication

03 IAM Groups

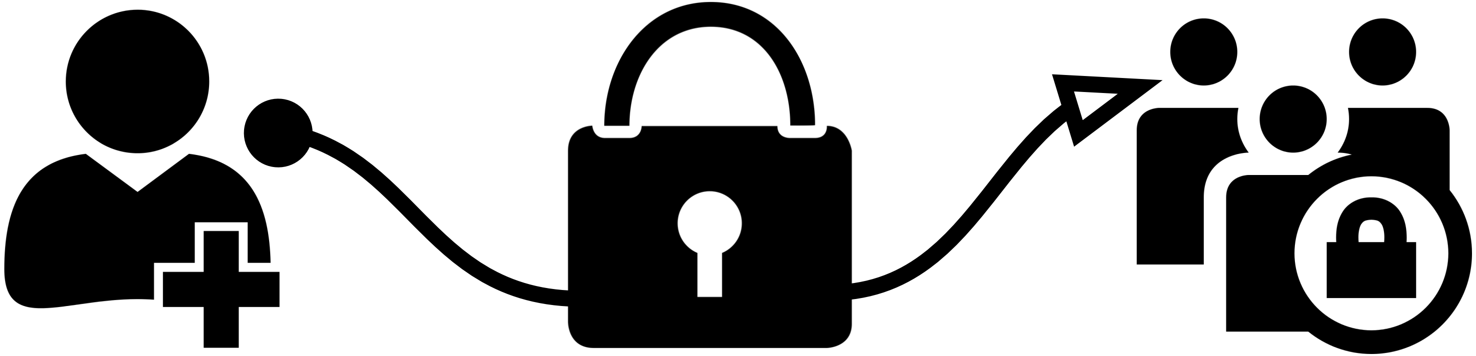
04 IAM Policies

Root User vs IAM User Access

In AWS there are root users and IAM users. A root user is for the person that created the AWS account (the account owner), and the root user creates the IAM user. The root user can create an IAM administrator to manage IAM users.

The **Root User** account will allow full access to all resources in the account. If the root user account belongs to a company that uses AWS Organizations then access can be limited with a service control policy (SCP).

An **IAM User** account can be used to securely control access to AWS services and resources for all users in your AWS account. Each user can have unique credentials created for them which define who has access to which resources.



EXPLORE DIGITAL SKILLS

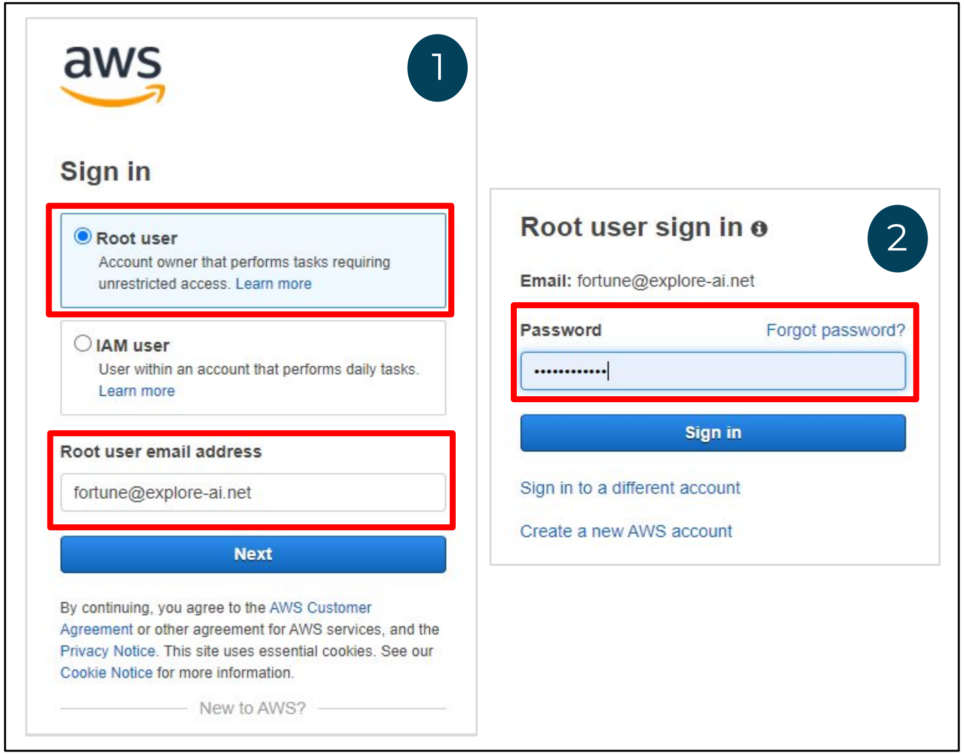
Creating IAM user account

Creating an **IAM user** with **administrator permissions** to use for everyday AWS tasks is a great way to keep your account secure. To do this you need to sign in to your AWS account using Root user authentication.

1. Start off by selecting the Root radio button followed by inputting your registered AWS **Root user email address** and click the next button.

2. On the next screen type in your **Password** then click Sign in

There are specific tasks such as changing AWS account settings, restoring IAM user permissions, activating IAM access to the Billing and Cost Management console and even closing the AWS account.



Sign in

● Root user
Account owner that performs tasks requiring unrestricted access. Learn more

○ IAM user
User within an account that performs daily tasks. Learn more

Root user email address: fortune@explore-ai.net

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

New to AWS?

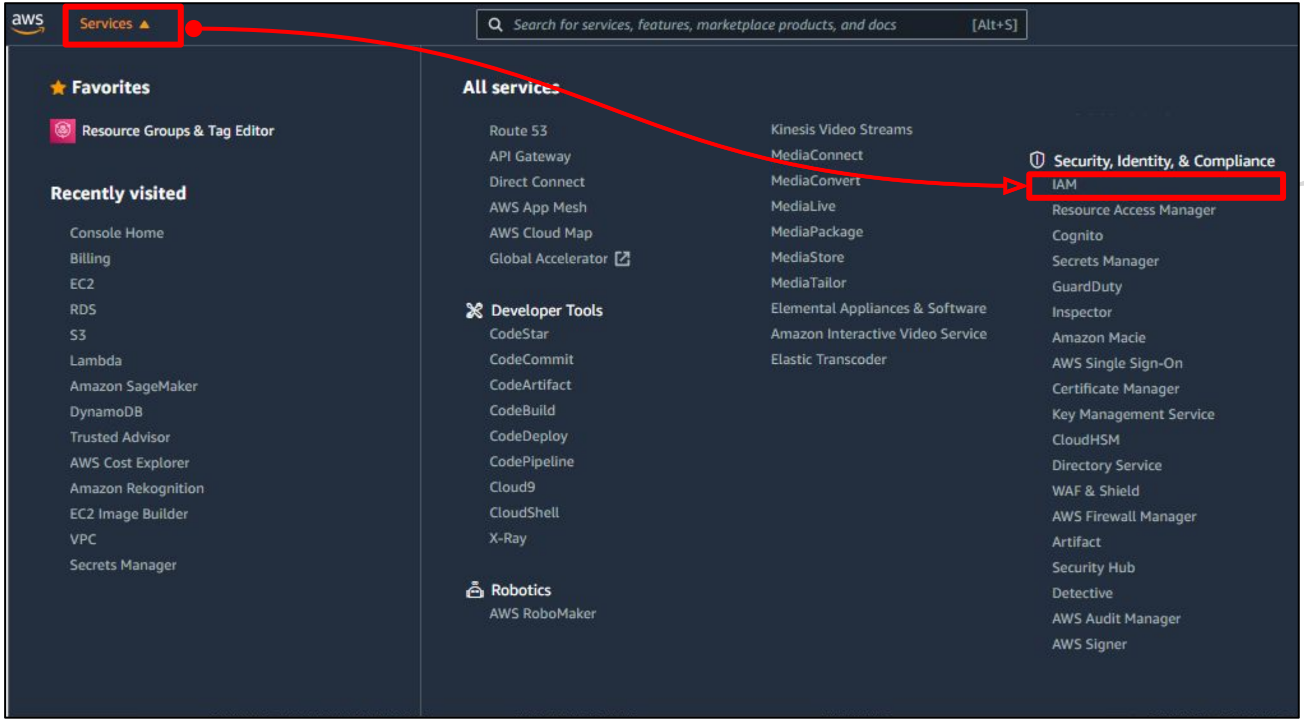
Root user sign in

Email: fortune@explore-ai.net

Password: ············

Creating an IAM User Account

To access the AWS IAM service you can use the drop-down menu on the top left corner of your AWS Management console. The IAM service is located in the Security, Identity, and Compliance category.



aws Services ▲

Search for services, features, marketplace products, and docs [Alt+S]

★ Favorites

- Resource Groups & Tag Editor

Recently visited

- Console Home
- Billing
- EC2
- RDS
- S3
- Lambda
- Amazon SageMaker
- DynamoDB
- Trusted Advisor
- AWS Cost Explorer
- Amazon Rekognition
- EC2 Image Builder
- VPC
- Secrets Manager

All services

- Route 53
- API Gateway
- Direct Connect
- AWS App Mesh
- AWS Cloud Map
- Global Accelerator

Developer Tools

- CodeStar
- CodeCommit
- CodeArtifact
- CodeBuild
- CodeDeploy
- CodePipeline
- Cloud9
- CloudShell
- X-Ray

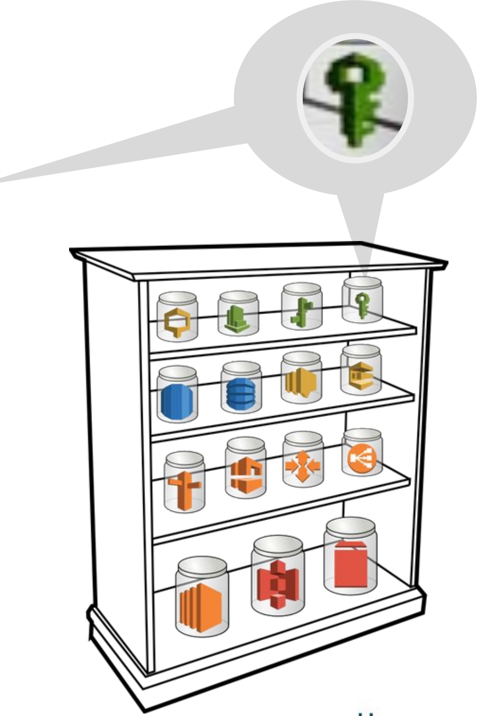
Robotics

- AWS RoboMaker

- Kinesis Video Streams
- MediaConnect
- MediaConvert
- MediaLive
- MediaPackage
- MediaStore
- MediaTailor
- Elemental Appliances & Software
- Amazon Interactive Video Service
- Elastic Transcoder

Security, Identity, & Compliance

- IAM
- Resource Access Manager
- Cognito
- Secrets Manager
- GuardDuty
- Inspector
- Amazon Macie
- AWS Single Sign-On
- Certificate Manager
- Key Management Service
- CloudHSM
- Directory Service
- WAF & Shield
- AWS Firewall Manager
- Artifact
- Security Hub
- Detective
- AWS Audit Manager
- AWS Signer



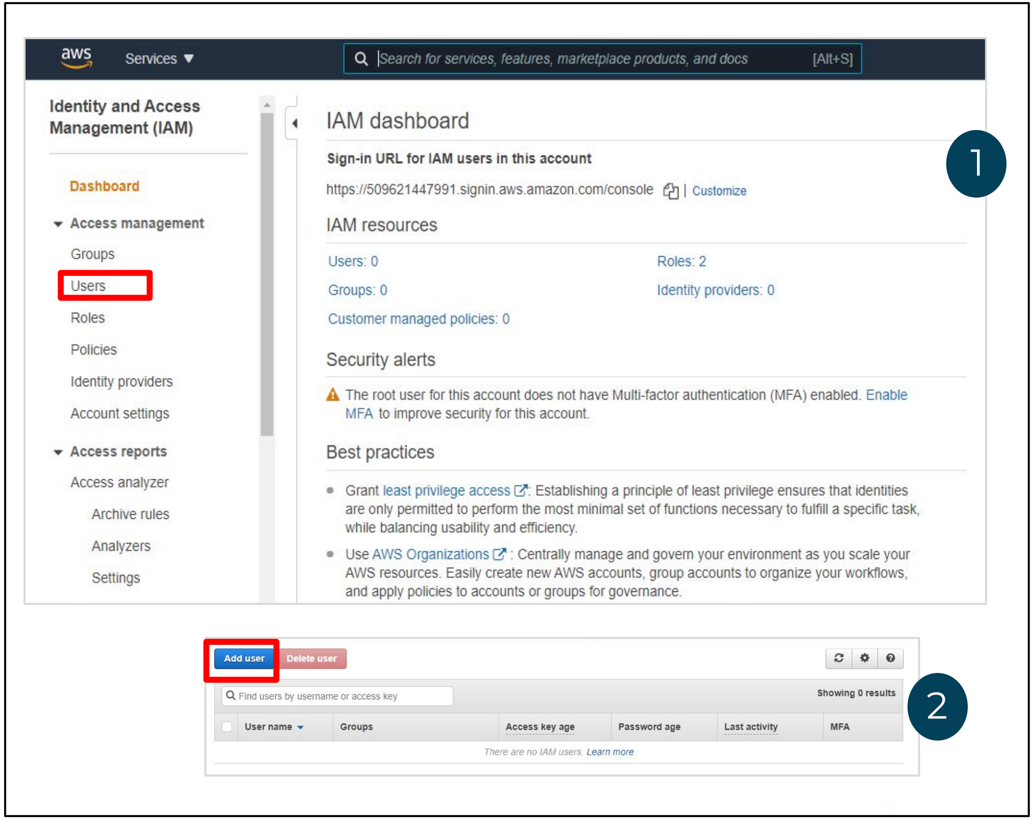
EXPLORE DIGITAL SKILLS

AWS IAM Dashboard

The IAM Dashboard is a simple interface that you can use to manage resources and features of the IAM service. This page will be populated with information about the **Sign-in URL** form. The IAM **Users**, **Groups**, **Roles** and other Identity and Access Management resource information are tracked and managed on this screen. On the left of the screen, you will be able to navigate to any of the resources available in the IAM dashboard this is known as the navigation pane.

1. Now to create a new IAM user click **Users** to be switched to the user view of the dashboard.

2. Click on the **Add User** button to be redirected to the add user page.



IAM dashboard

Sign-in URL for IAM users in this account

https://509621447991.signin.aws.amazon.com/console | Customize

IAM resources

Users: 0	Roles: 2
Groups: 0	Identity providers: 0
Customer managed policies: 0	

Security alerts

⚠ The root user for this account does not have Multi-factor authentication (MFA) enabled. Enable MFA to improve security for this account.

Best practices

- Grant least privilege access: Establishing a principle of least privilege ensures that identities are only permitted to perform the most minimal set of functions necessary to fulfill a specific task, while balancing usability and efficiency.
- Use AWS Organizations : Centrally manage and govern your environment as you scale your AWS resources. Easily create new AWS accounts, group accounts to organize your workflows, and apply policies to accounts or groups for governance.

Find users by username or access key — Showing 0 results

□	User name ▾	Groups	Access key age	Password age	Last activity	MFA

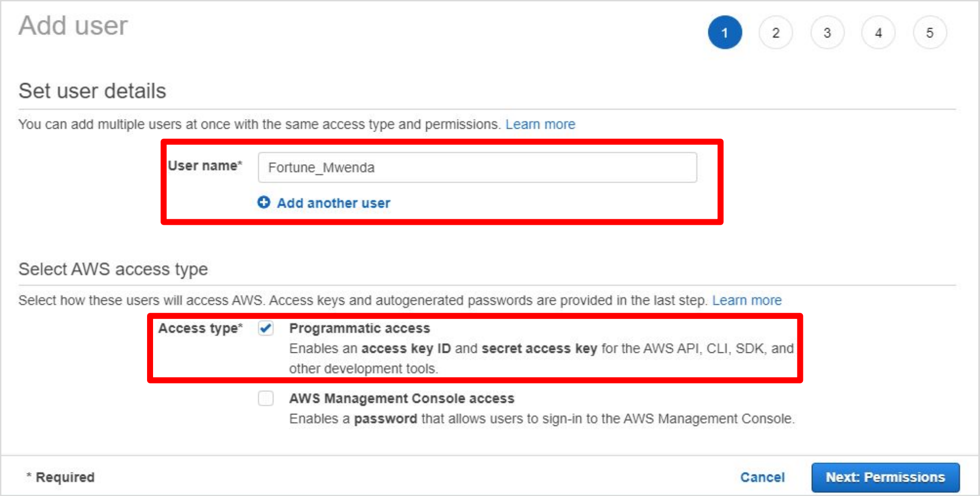
There are no IAM users. Learn more

Configuring IAM User Account Details

To configure your IAM user permissions you start by creating a User name, it is also possible to create multiple users that will share the same permissions.
Then choose the Access type you want your new account to have. In this train, we will select both **Programmatic access** and AWS **Management Console access**

Programmatic access uses an **access key** and **secret access key** combination for access through development tools such as the AWS CLI, API and SDK. AWS Management Console access enables **User name** and **password access** that can be used to access your AWS services on a web browser. You can choose to set a custom password or let AWS auto-generate a password for you.

Click on “Next: Permissions” to continue.



Add user

Set user details

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

User name* Fortune_Mwenda

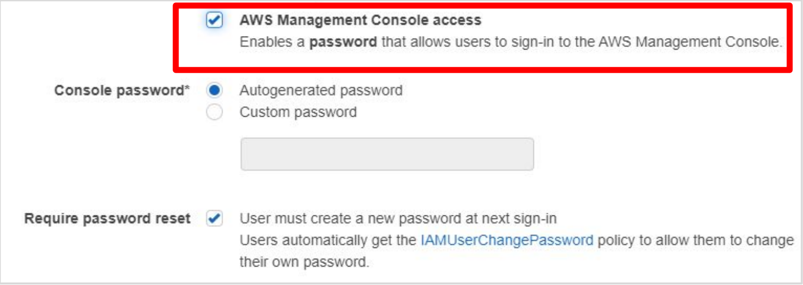
Select AWS access type

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



☑ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ● Autogenerated password
○ Custom password

Require password reset ☑ User must create a new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

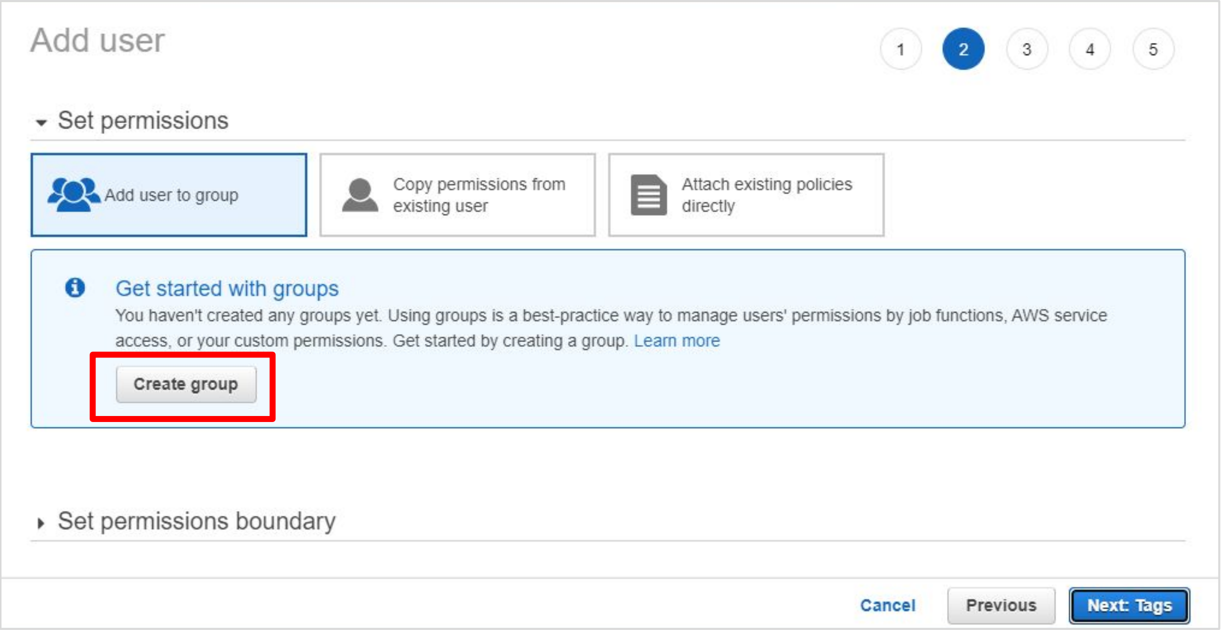
Configuring IAM User Permissions

When you set permissions for your IAM user you will have 3 options to choose from. For this train we will add our user to a group, this will allow you to create new groups to manage user permissions based on the policies that are attached to those groups.

Add user to a group will allow you to add your user(s) to a new group or existing groups

If you have already created an IAM user you can Copy permissions from existing users

You can even attach existing policies directly to the IAM user account



Add user

Set permissions

Get started with groups

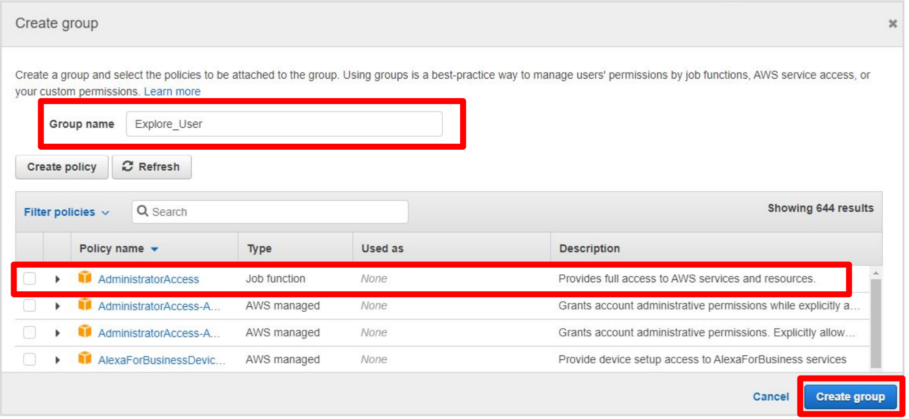
You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. Learn more

Set permissions boundary

1
2
3
4
5
Add user to group
Copy permissions from existing user
Attach existing policies directly
Create group
Cancel
Previous
Next: Tags

Create an IAM Group and Associate Policies

Creating a group is a simple as providing a **Group name** and choosing which policies you want to attach to the group. For your IAM account select the **AdministratorAccess** policy for full access to AWS services.



Create group ×

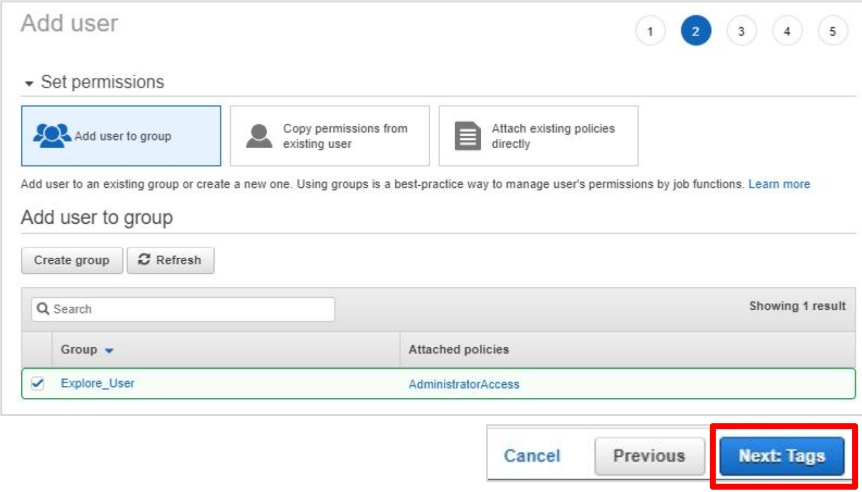
Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Learn more

Group name: Explore_User

Showing 644 results

		Policy name	Type	Used as	Description
□	▸	AdministratorAccess	Job function	None	Provides full access to AWS services and resources.
□	▸	AdministratorAccess-A...	AWS managed	None	Grants account administrative permissions while explicitly a...
□	▸	AdministratorAccess-A...	AWS managed	None	Grants account administrative permissions. Explicitly allow...
□	▸	AlexaForBusinessDevic...	AWS managed	None	Provide device setup access to AlexaForBusiness services

Once you have created a group with administrator access permissions select the group and add a user to the group. At this point, you are basically done with the main requirements for setting up an IAM user. Click on the **Next: Tags** button to continue.



Add user

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 1 result

	Group	Attached policies
☑	Explore_User	AdministratorAccess

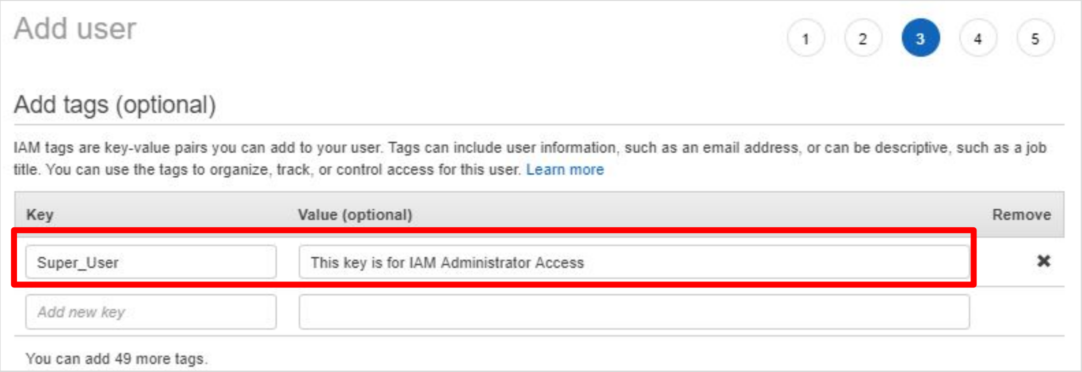
Adding IAM Tags

Adding tags is optional but it can be a useful way to keep track of the IAM user account that you create. Tagging is supported by many AWS services as a tool for identifying and organizing your AWS resources.

You can use tagging to describe the user permissions and user type. Tags are key-value pairs custom attribute labels.

A tag has two parts:

1. **Key** - Case sensitive title (e.g admin_user, dev_user) the choice is yours.
2. **Value** - An optional field, however omitting this field is the same as using an empty string. The value is also case-sensitive.



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
Super_User	This key is for IAM Administrator Access	✖
Add new key		

You can add 49 more tags.

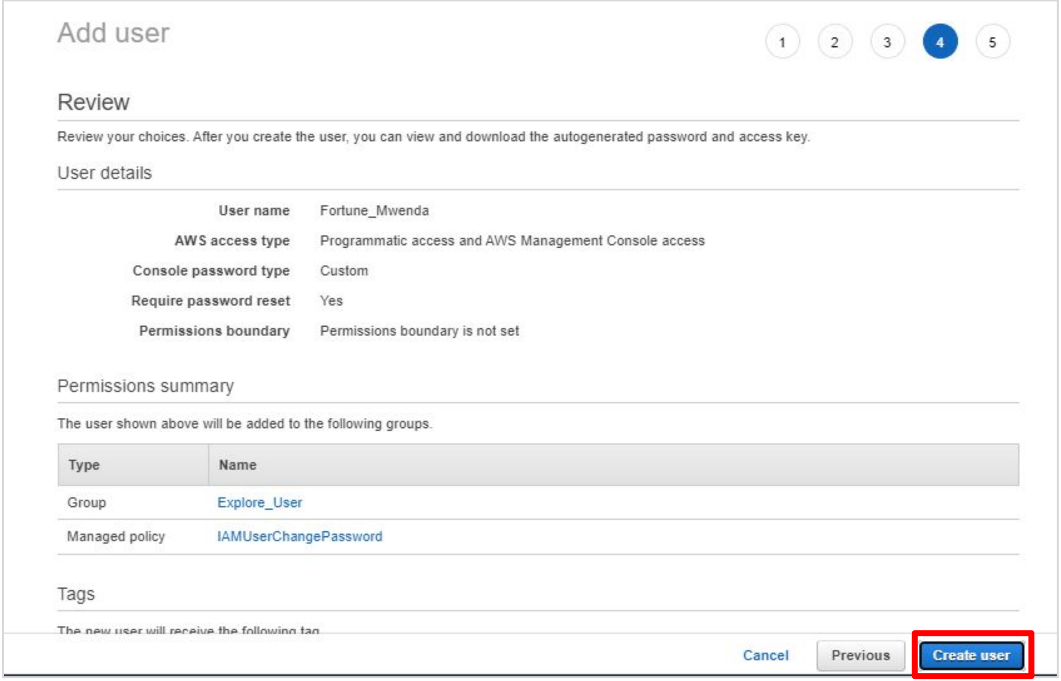
Review Account Settings

Finally, it is time to review the configurations you have set for your new IAM account. You can navigate back from this page to make any changes if you need to.

Ensure that your account has:

- Both programmatic and AWS Management Console **access types**
- There are no **permission boundaries** set.
- And your account is **associated with a group** that has **full administrator access permission**.

If your IAM account meets these conditions you can click the **Create user** button to complete the creation of your IAM account.



Add user

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	Fortune_Mwenda
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

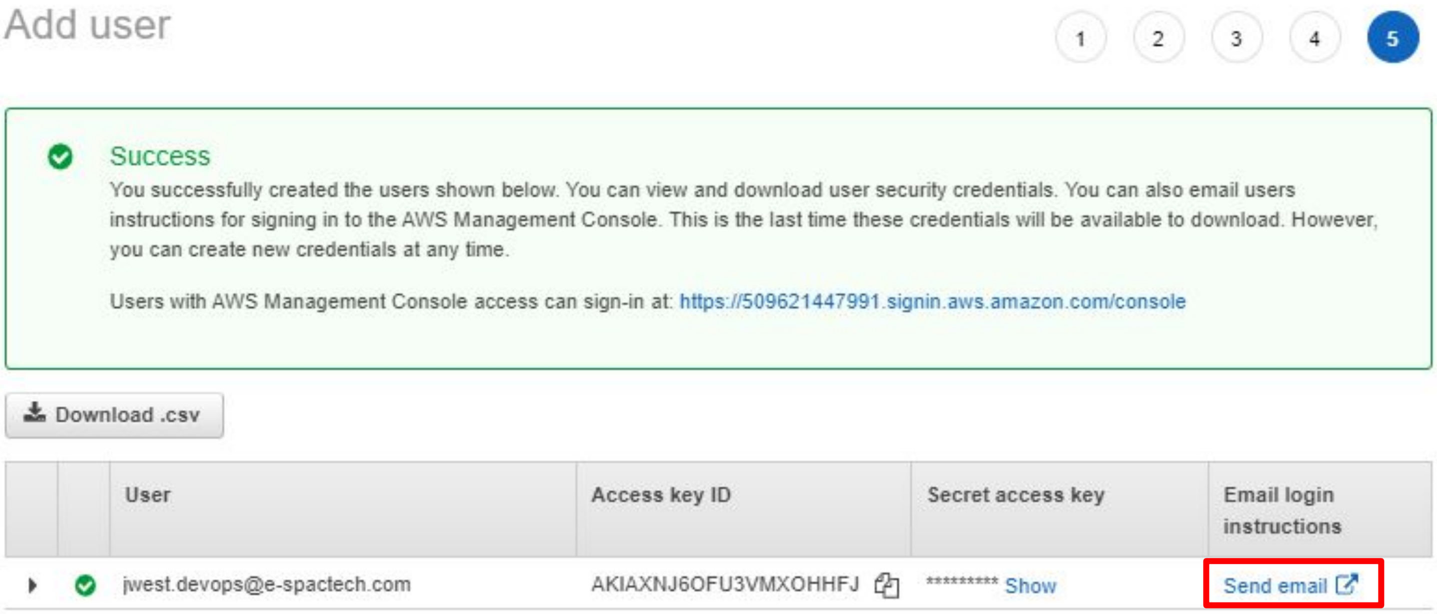
Type	Name
Group	Explore_User
Managed policy	IAMUserChangePassword

Tags

The new user will receive the following tag

Your IAM User Account Credentials

Congratulations! You know have an IAM user account to use in AWS. This account should be used to access AWS in place of your root user account whenever possible as this will help to improve your security in the cloud. The is an option to send login details to your email use this link to get **login instructions sent to your email**.



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://509621447991.signin.aws.amazon.com/console

		User	Access key ID	Secret access key	Email login instructions
▸	✓	jwest.devops@e-spactech.com	AKIAXNJ6OFU3VMXOHHFJ	********* Show	Send email

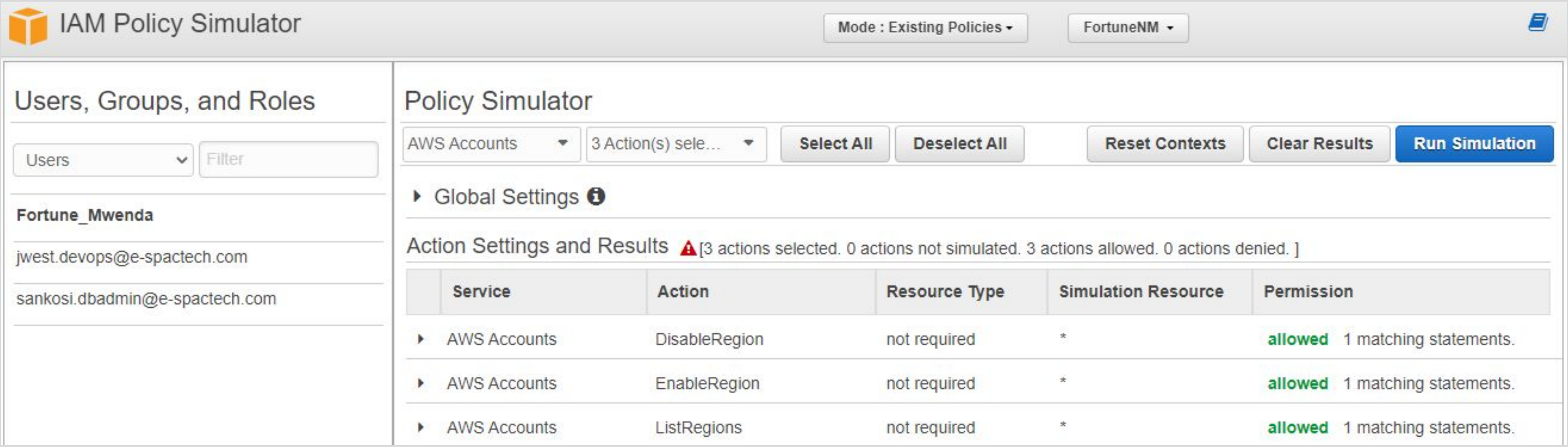
Conclusion

- In this train we've learned how to:
  - Access the AWS Identity Access Management(IAM) service.
  - Navigate the AWS IAM Dashboard to create a new IAM user.
  - Configure IAM user account details
  - Configure IAM user permissions
  - Create an IAM group and associate policies
  - Get your IAM user account credentials and login instructions

- Once you're comfortable with your new AWS IAM account you can use it to create a new IAM user account with minimum privileges for the resources you need.

Appendix

While signed in with your AWS account You can simulate an IAM user policy using the IAM Policy Simulator. To try it out you just select an **IAM User** and the **IAM Policies** you want to check and the actions you want the policy simulator to check. You can also simulate **IAM Group** and **Roles** policies.



Fortune_Mwenda

jwest.devops@e-spactech.com

sankosi.dbadmin@e-spactech.com

Action Settings and Results [3 actions selected. 0 actions not simulated. 3 actions allowed. 0 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
AWS Accounts	DisableRegion	not required	*	allowed 1 matching statements.
AWS Accounts	EnableRegion	not required	*	allowed 1 matching statements.
AWS Accounts	ListRegions	not required	*	allowed 1 matching statements.