

# create IAM user in AWS to Secure Root User?

As the root user runs sensitive operations in AWS, creating an extra authentication layer helps you secure your account more effectively.

Creating an IAM user in [AWS](#) is vital for implementing [AWS security best practices](#). The unrestricted access of the root user makes it susceptible to malicious attacks. Here are some reasons to create an IAM user.

- This user can be assigned specific permissions for resource management, reducing the risk of unauthorized changes.

- IAM users also promote segregation of duties and accountability by assigning access levels based on roles.
- It strengthens account security and mitigates potential damage from compromised credentials.
- Adding users through IAM enables centralized access management, streamlining onboarding and offboarding processes and reducing lingering access risks.

## How to create IAM user in AWS

Creating an IAM user in AWS ensures better control and accountability over cloud resources, minimizing potential risks for organizations.

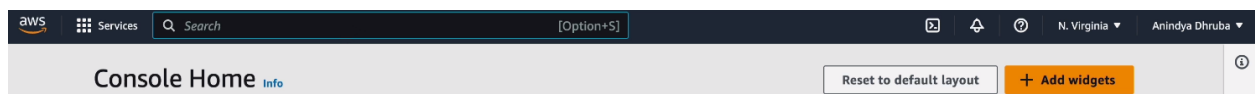
In three steps, you can create an IAM user in AWS.

1. Navigate to IAM from the root user's dashboard
2. Add user
3. Login with the new user credentials

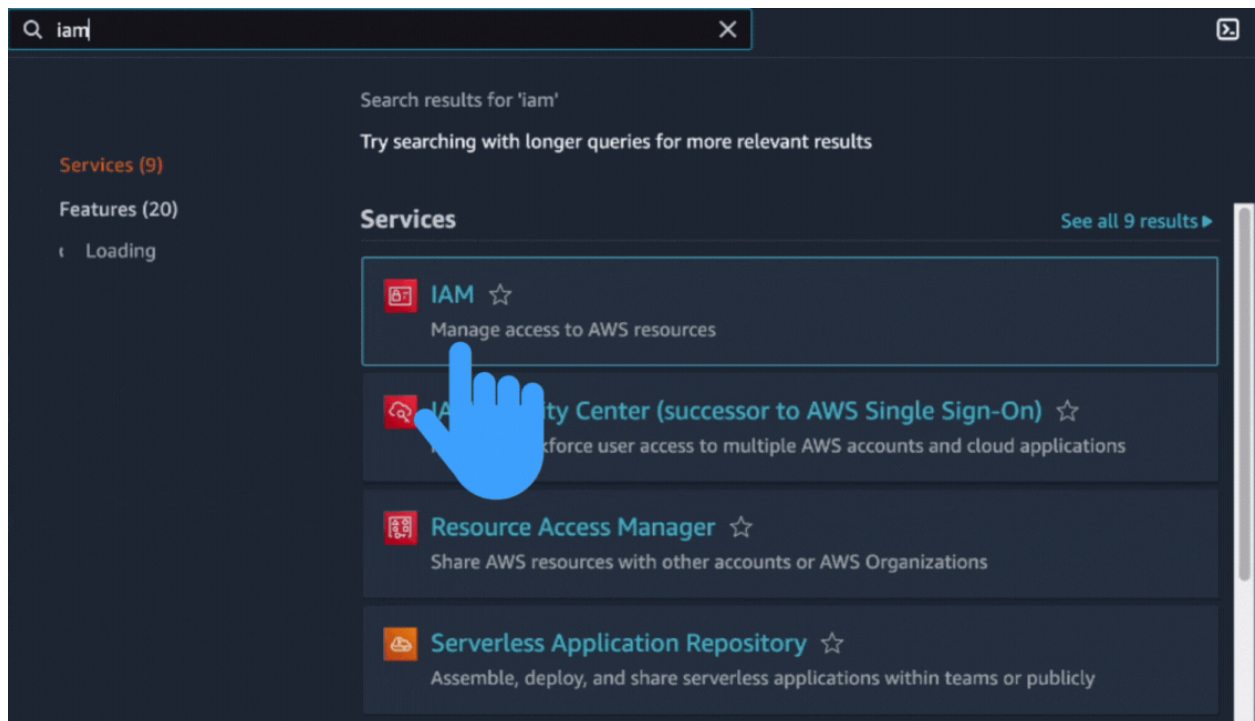
Here is a video tutorial on **how to create IAM user in AWS** to assist you through the entire process.

## **1** Navigate to IAM from the root user's dashboard

The Console home has a search bar like the one below.

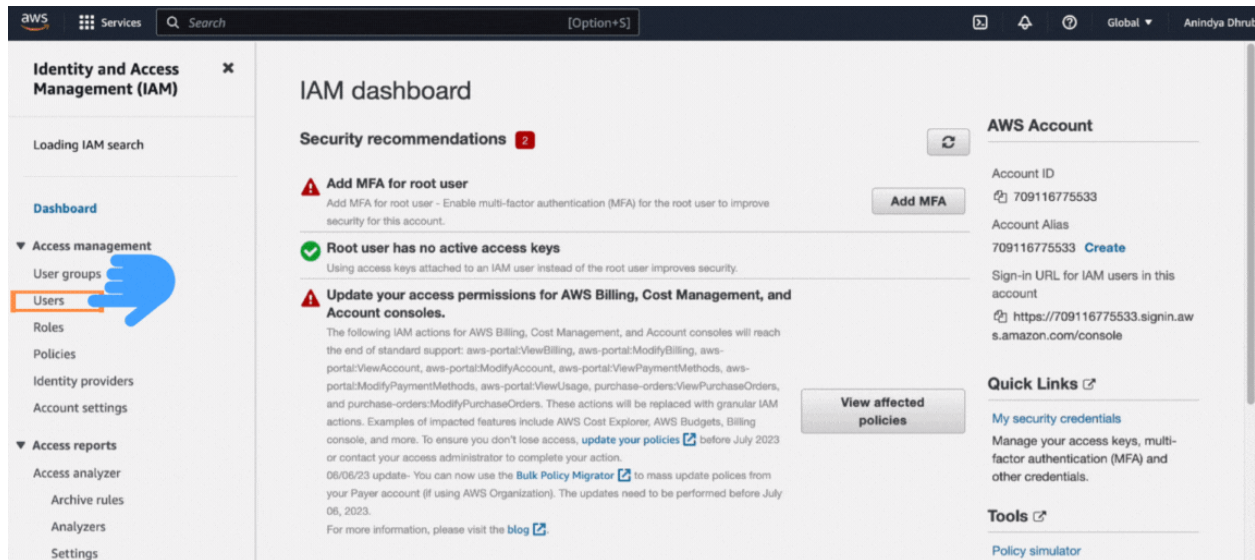


Insert the text “iam” in the search bar, and select the IAM service as shown below.



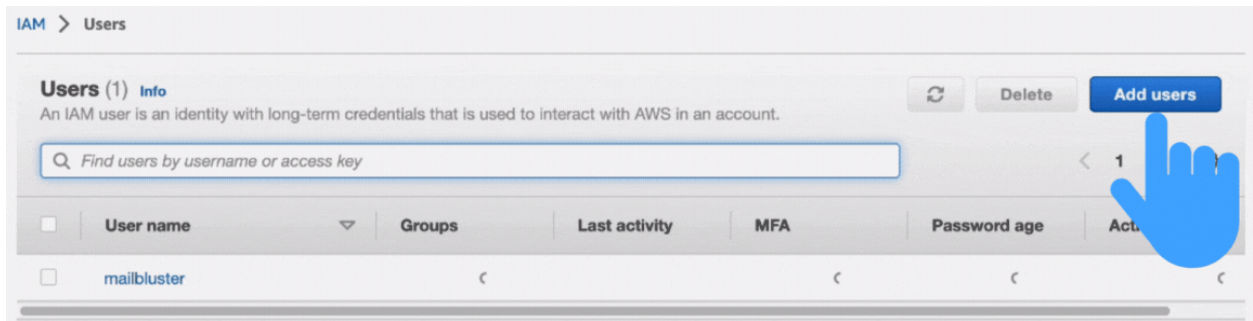
Now, you are on the Identity and Access Management dashboard.

Click on the “Users” section on the left side of the page.



## 1 Add User

You will find the “Add users” button. Click on that as shown in the screenshare.



A section like the one below will appear to you.

Here, you must insert the desired “user name” you want and then click on the “Next” button.

## Specify user details

### User details

User name

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + =, \_ - (hyphen)

☐ Provide user access to the AWS Management Console - *optional*  
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspace, you can generate them after you create this IAM user. [Learn more](#)

Cancel Next

A section named “Set permission” will appear.

Click on the “Attach policies directly.”

## 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.

Scrolling down a bit, you will find a section like the one shown below.

In the search bar, type “sqs,” and then click on the AmazonSQSFullAccess.

**Permissions policies (1/1106)**  
Choose one or more policies to attach to your new user.

Filter by Type

Search: sqs 3 matches

	Policy name	Type	Attached entities
<input checked="" type="checkbox"/>	AmazonSQSFullAccess	AWS managed	1
<input type="checkbox"/>	AmazonS3OutpostsFullAccess	AWS managed	0
<input type="checkbox"/>	AWSLambdaQueueExecutionRole	AWS managed	0



This time, you will see the section named “Review and create.”

Simply click on the “Create user” button on the bottom-right side of the page.

## 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	Console password type	Require password reset
my-user	None	No

### Permissions summary

< 1 >

Name 	Type	Used as
<a href="#">AmazonSQSFullAccess</a>	AWS managed	Permissions policy

### Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.


Add new tag

You can add up to 50 more tags.

Cancel

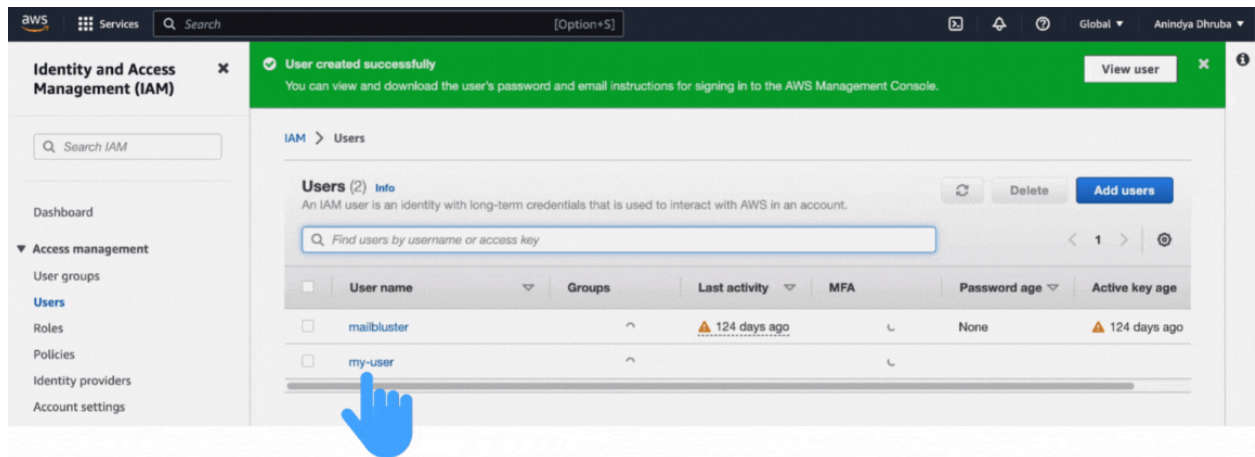
Previous

Create user



At this time, you will see the user you just created. In our case, we named the user as “my-user.”

Just click on it.



Click on the “Security credentials” from your new user’s section below.

IAM > Users > my-user


## my-user [Info](#)

Delete

### Summary

ARN arn:aws:iam::709116775533:user/my-user	Console access	Access key 1 Not enabled
Created July 03, 2023, 11:39 (UTC+06:00)	Last console sign-in	Access key 2 Not enabled

[Permissions](#) | [Groups](#) | [Tags](#) | [Security credentials](#) | [Access Advisor](#)



The “Console sign-in” section has a button named “Enable console access.”

Click on that button.

Permissions

Groups

Tags

Security credentials

Access Advisor

Console sign-in

Enable console access

Console sign-in link

Console password

https://709116775533.signin.aws.amazon.com/console

Not enabled

Multi-factor authentication (MFA) (0)

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](#)

Remove

Resync

Assign MFA device

Device type

Identifier

Certifications

Created on

No MFA devices. Assign an MFA device to improve the security of your AWS environment

Assign MFA device

After that, a section will appear to you. You can enable the console access from here, like the one shown below.

**Manage console access** [X]

Manage my-user's AWS console access and password.

Console access

☐ Enable

☒ Disable

Disabling removes the pre-existing password.

Cancel Apply

After clicking on “Enable,” you will find the “Set password” section. Here, you can select an auto-generated or custom password.

In our case, we have selected “Autogenerated password.”

After selecting, click on the “Apply” button.

## Manage console access

Manage my-user's AWS console access and password.

Console access

☒ Enable

☐ Disable

Disabling removes the pre-existing password.

Set password

☐ Keep existing password

☒ Autogenerated password

☐ Custom password

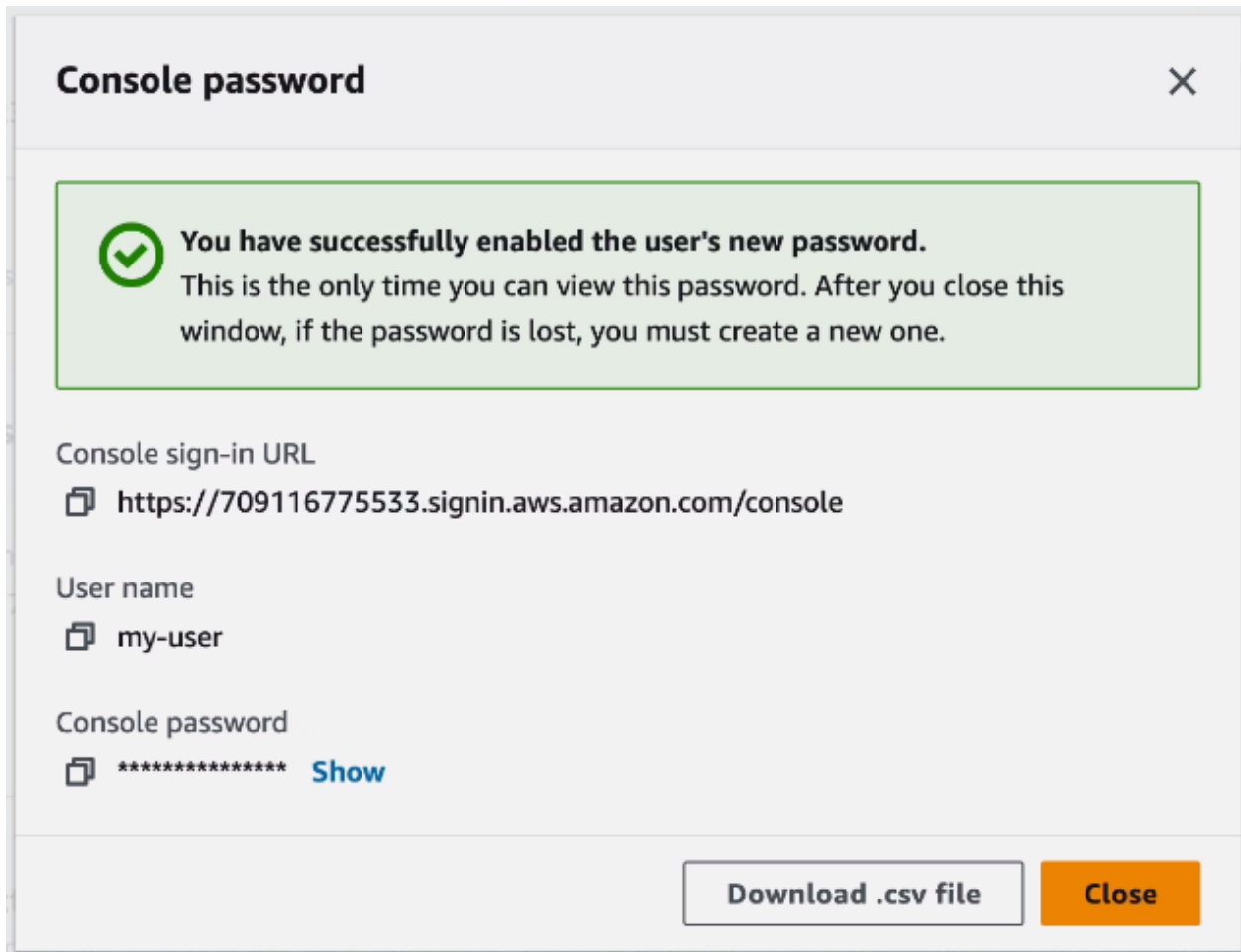
☐ User must create new password at next sign-in

Users automatically get the [IAMUserChangePassword](#) policy their own password.

Cancel

Apply

You will now get the Console Sign-in URL, User name, and Console password.



## 1 Login with new user credential

Copy the Console sign-in URL, and then paste it into a new tab.



You will find the IAM sign-in section like the one shown below.

In the “Account ID” field, insert your 12-digit ID from the Console Sign-in URL.