

1. Login to AWS console
2. Search for IAM → Users → Create User → give username as terraform and click Next button

IAM > Users > Create user

Step 1
 Specify user details
 Step 2
 Set permissions
 Step 3
 Review and create

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.

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

Cancel Next

3. In set permissions screen select “Attach policies directly” → Search for AdministratorAccess and select it → scroll down and click on next button

Specify user details
 Step 2
 Set permissions
 Step 3
 Review and create

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.

Permissions policies (1/1317)

Choose one or more policies to attach to your new user. [Create policy](#)

Filter by Type: All types

Search

Policy name	Type	Attached entities
<input type="checkbox"/> AccessAnalyzerServiceRoleP...	AWS managed	0
<input checked="" type="checkbox"/> AdministratorAccess	AWS managed - job function	1
<input type="checkbox"/> AdministratorAccess-Amplify	AWS managed	0

4. Finally click on Create User.
5. You will see terraform user in user list → click on terraform user → click on “Security Credential” tab

Permissions
Groups
Tags
Security credentials
Last Accessed

Console sign-in

Console sign-in link
<https://575046702235.signin.aws.amazon.com/console>

Console password
Not enabled

Enable console access

Multi-factor authentication (MFA) (0)

Remove
Resync
Assign MFA device

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](#)

Type	Identifier	Certifications	Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment			

Assign MFA device

Access keys (0)

Create access key

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more](#)

- In Access keys section → Create access key → select Command line interface (CLI) → check confirmation check box → click on Next button

Step 1
Access key best practices & alternatives
Step 2 - optional
Set description tag
Step 3
Retrieve access keys

Set description tag - optional

The description for this access key will be attached to this user as a tag and shown alongside the access key.

Description tag value
Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.

terraform user with access key

Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . : / = + - @

Cancel
Previous
Create access key

- Optionally give description and click on Create access key

Access key created
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

Step 1
Access key best practices & alternatives
Step 2 - optional
Set description tag
Step 3
Retrieve access keys

Retrieve access keys

Access key
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIAVL3UKSNYMETO4HG	***** Show

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [best practices for managing AWS access keys](#).

Download .csv file
Done

- Copy Access key and Secret access key and click on Done

9. Open command prompt → type “aws configure” command
 - a. Provide AWS Access key Id (Access key)
 - b. AWS Secret Access Key (Secret access key)
 - c. Default region name (us-east-1)
 - d. Default output format (press enter to default value)
10. Now, use terraform for creating resources in AWS (Note. You need terraform install on machine)