

0 0



≡ IAM > Users > Mode-staff1 > Create access key

Step 1

Access key best practices & alternatives

Step 2 - optional

Set description tag

Step 3

Retrieve access keys

# Access key best practices & alternatives Info

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

#### Use case

Command Line Interface (CLI)

You plan to use this access key to enable the AWS CLI to access your AWS account.

O Local code

You plan to use this access key to enable application code in a local development environment to access your

Application running on an AWS compute service

You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

O Third-party service

You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

Application running outside AWS

You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.

O Other

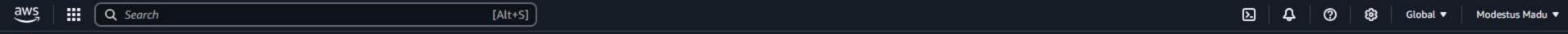
Your use case is not listed here.

### ⚠ Alternatives recommended

- Use AWS CloudShell, a browser-based CLI, to run commands. Learn more
- Use the AWS CLI V2 and enable authentication through a user in IAM Identity Center. Learn more [2]

#### Confirmation

I understand the above recommendation and want to proceed to create an access key.



Step 1 Access key best practices & alternatives Step 2 - optional

■ IAM > Users > Mode-staff1 > Create access key

Set description tag

Step 3

O Retrieve access keys

# Set description tag - optional Info

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

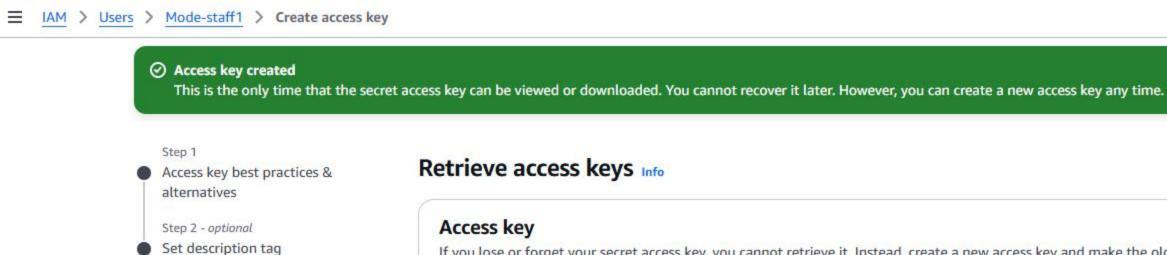
Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: \_ .: / = + - @

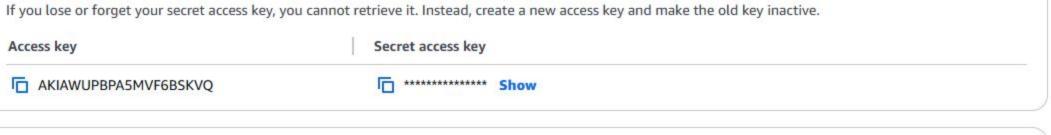
Description tag value Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later. Access key

> Previous Create access key Cancel

0 0







## 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

Step 3

Retrieve access keys

① **③**