

MFA AND ROLES

The screenshot shows the AWS Console Home page. At the top right, there is a yellow box containing the text "MFA AND ROLES". Below the header, there are several sections: "Recently visited" (Billing, EC2, Elastic Beanstalk, AWS Cost Explorer, VPC, Lambda, DynamoDB, IAM, S3, CodePipeline), "Welcome to AWS" (Getting started with AWS, Training and certification, What's new with AWS?), "AWS Health" (Open issues), and "Cost and usage" (Current month costs, Top costs for current month). At the bottom, there are links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

Login to your account.

The screenshot shows the AWS Account page. On the left, there is a sidebar with links: Account, Organization, Service Quotas, Billing Dashboard, and Security credentials. At the bottom of the sidebar is a "Sign out" button. The main content area is currently empty.

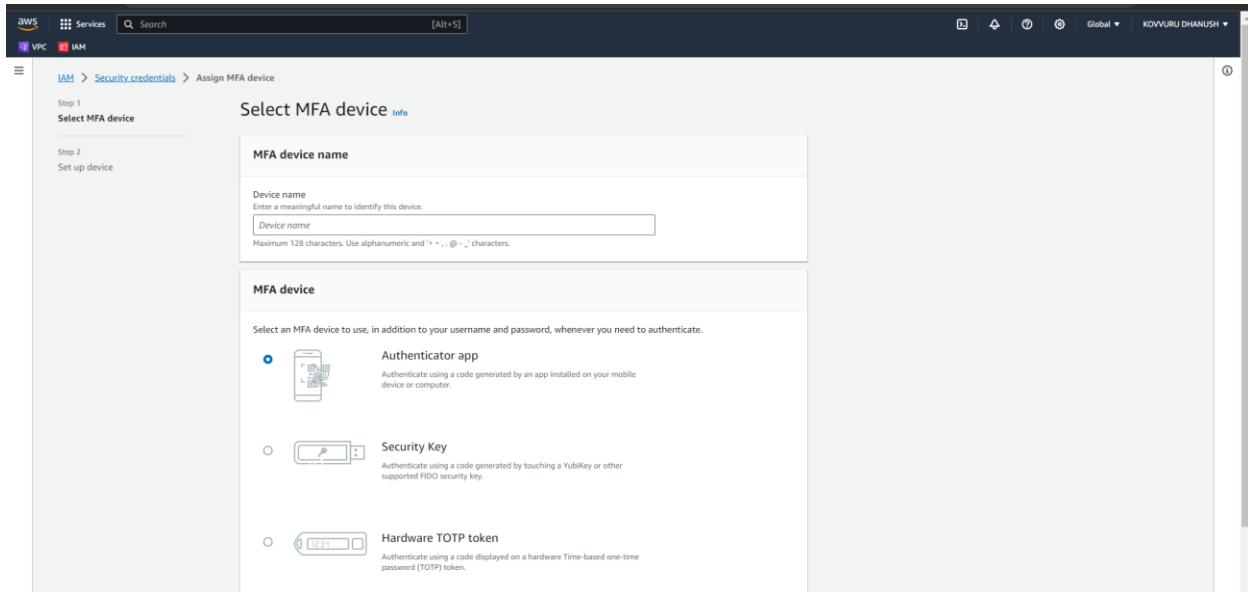
Click on security credentials.

The screenshot shows the AWS Identity and Access Management (IAM) service. In the left sidebar, under 'Access management', the 'User groups' option is selected. The main content area displays the 'My security credentials' page for the 'Root user'. A prominent yellow warning box at the top states: 'You don't have MFA assigned. As a security best practice, we recommend you assign MFA.' To the right of this message is a blue 'Assign MFA' button. Below the warning, there's a section titled 'Account details' with fields for 'Account name' (empty), 'Email address' (empty), 'AWS account ID' (empty), and 'Canonical user ID' (empty). Further down, a section for 'Multi-factor authentication (MFA)' shows '(0)' and includes 'Remove', 'Resync', and 'Assign MFA device' buttons. At the bottom of the page, there are links for 'CloudShell', 'Feedback', and copyright information: '© 2023, Amazon Web Services India Private Limited or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.



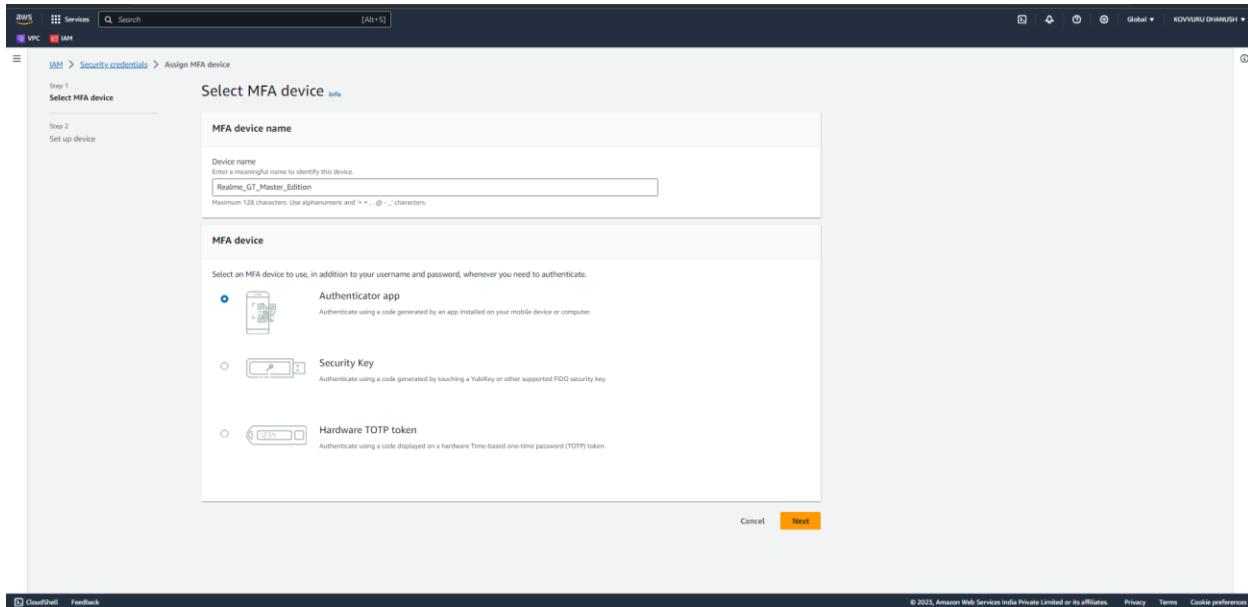
Check here it is asking us to assign MFA as we are root user as per AWS recommendations it is asking us to ASSGIN MFA.

NOW Click on Assign MFA.

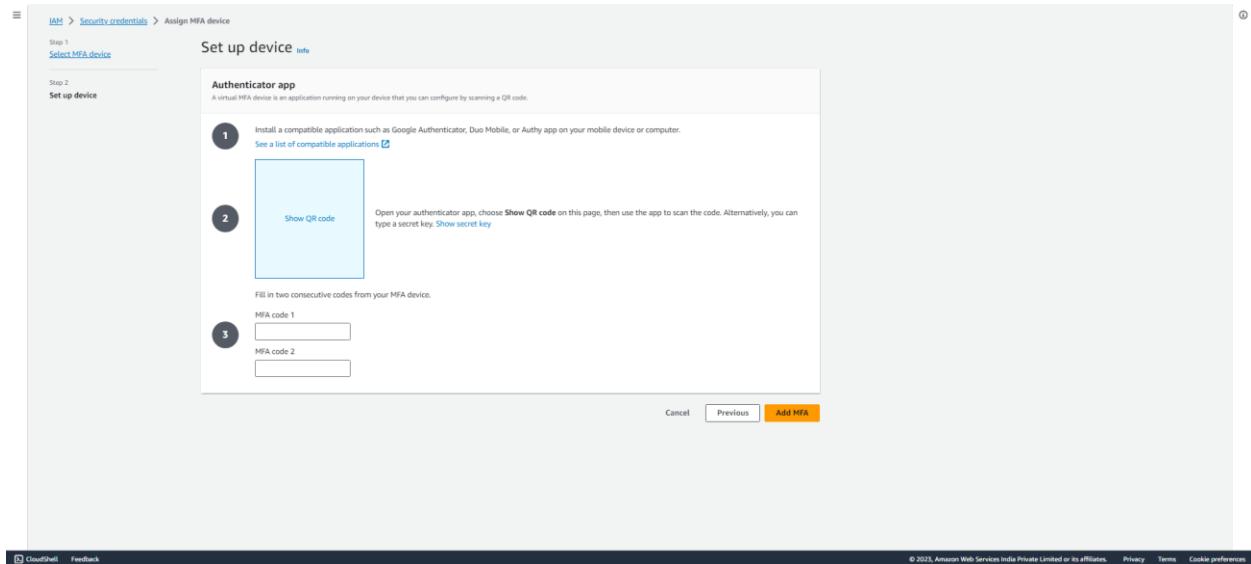


Then you will be landed on this page.

Here it is asking us to provide the device name, here in my case Realme GT Master Edition.



Now click on next.



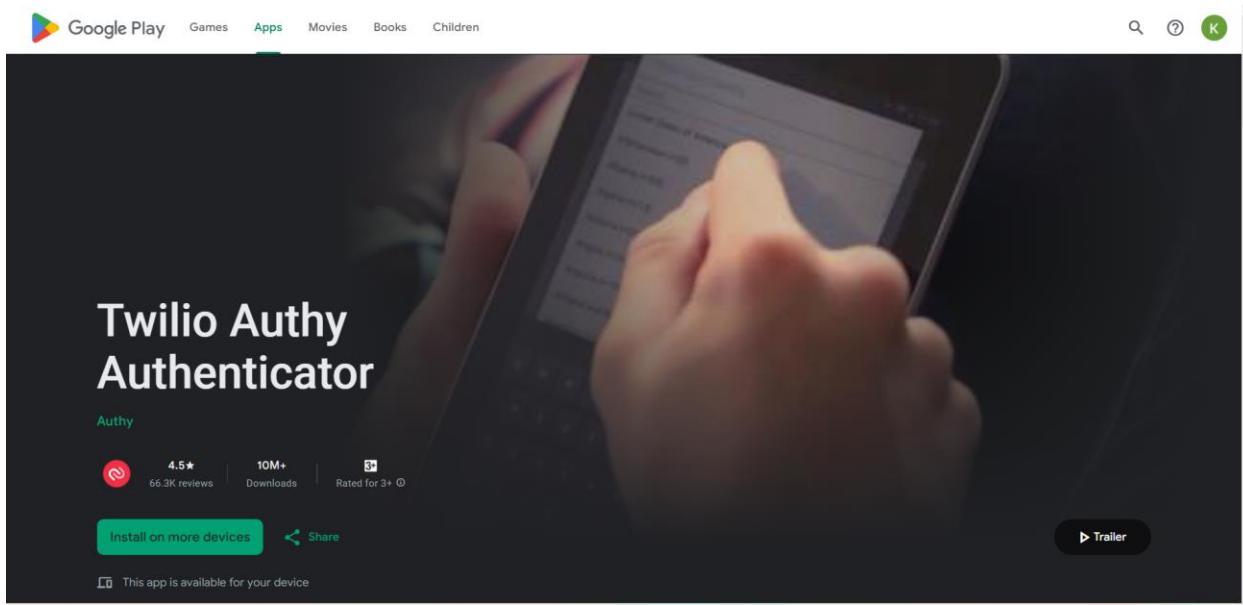
Click on see a list of compatible applications.

Android	Twilio Authy Authenticator , Duo Mobile , Microsoft Authenticator , Google Authenticator , Symantec VIP
iOS	Twilio Authy Authenticator , Duo Mobile , Microsoft Authenticator , Google Authenticator , Symantec VIP

Here my device is Android, so these are the compatible applications if yours's IOS then download anyone.

Here I'm using Twilio Authy Authenticator.

So, click on Twilio Authy Authenticator.



Open your mobile and download the Authy Authenticator.

[←](#)



**Twilio Authy
Authenticator**

Authy

[Uninstall](#) [Open](#)

What's new • [→](#)
Last updated 11 Sept 2023

App improvements

Rate this app
Tell others what you think

[Write a review](#)

App support [▼](#)

Switch accounts to become a beta tester

This app is associated with a different account, kovurudhanush@gmail.com.
To get beta updates for this app, first switch to that account in Play Store and join the beta.

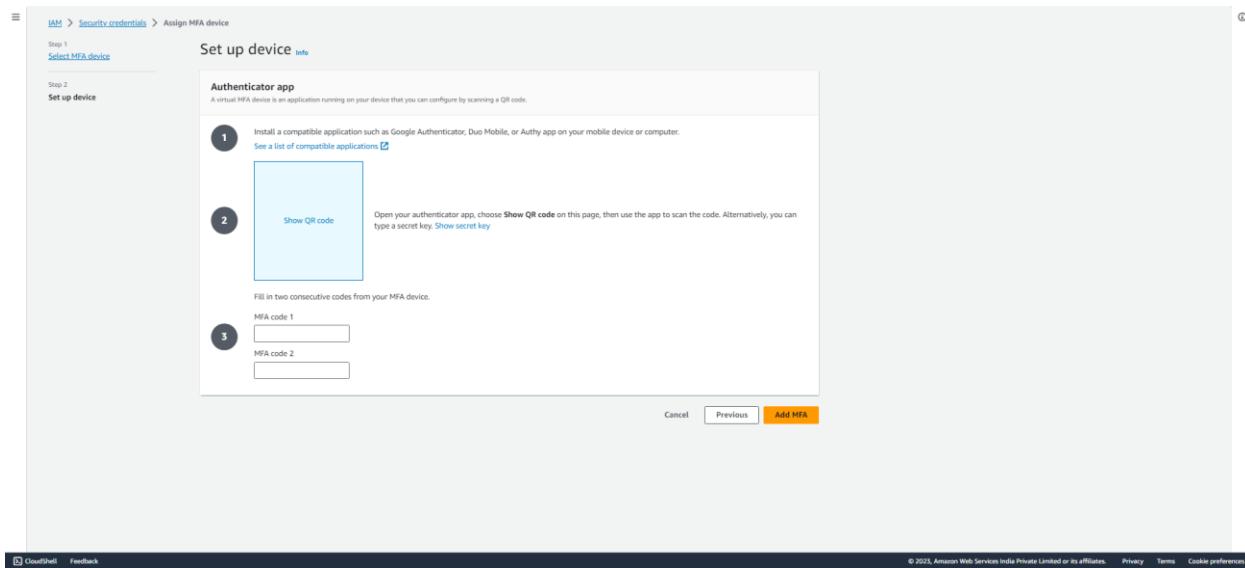


here in my case, it is already installed.

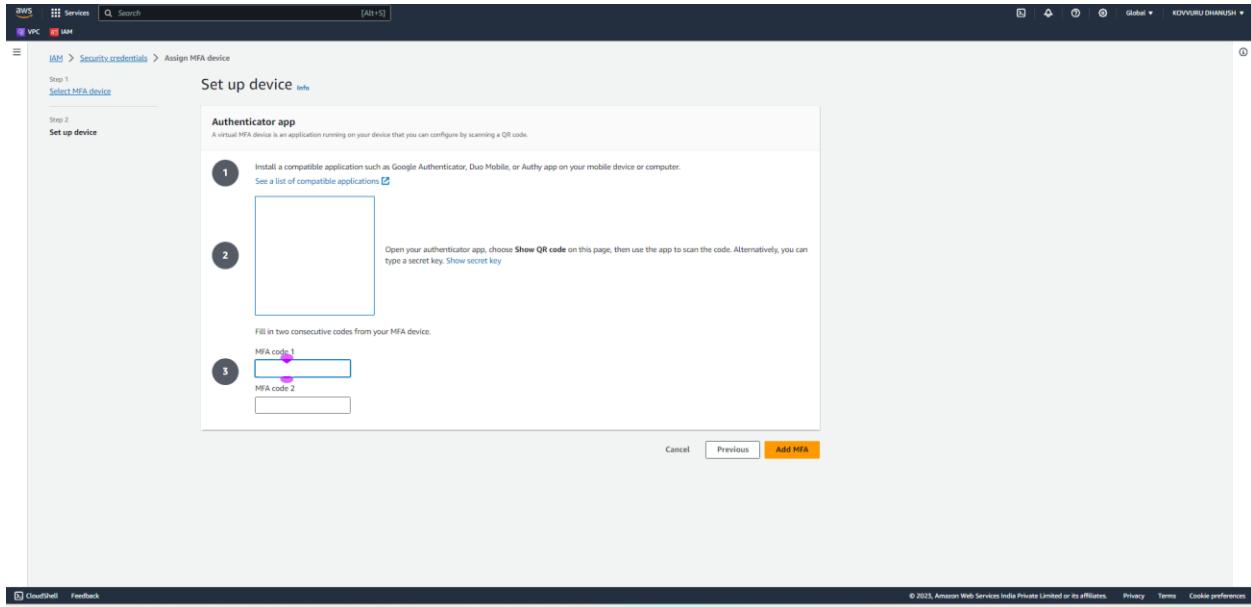
After the installation open the App.

Click on add Account.

Next click on scan QR Code.



Click on show QR Code.



After scanning we need to add MFA Code 1,2 and click on Add MFA.

The screenshot shows the 'My security credentials' page in the AWS IAM console. A green success message at the top indicates that an MFA device has been assigned. The 'Multi-factor authentication (MFA)' section lists one device: a virtual device with the identifier 'arn:aws:iam::280694802344:mfa/Realme_GT_Master_Edition'. The 'Access keys' section is also present at the bottom of the page.

Here MFA is added successfully.

aws

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

Next

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? [Create a new AWS account](#)

ANALYTICS

Run OpenSearch without managing clusters

Deliver search and log analytics without provisioning and adjusting resources

[Learn more >](#)



Enter your email.

aws

Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address: kovurudhanush@gmail.com

MFA code

Submit

[Troubleshoot MFA](#)

[Cancel](#)

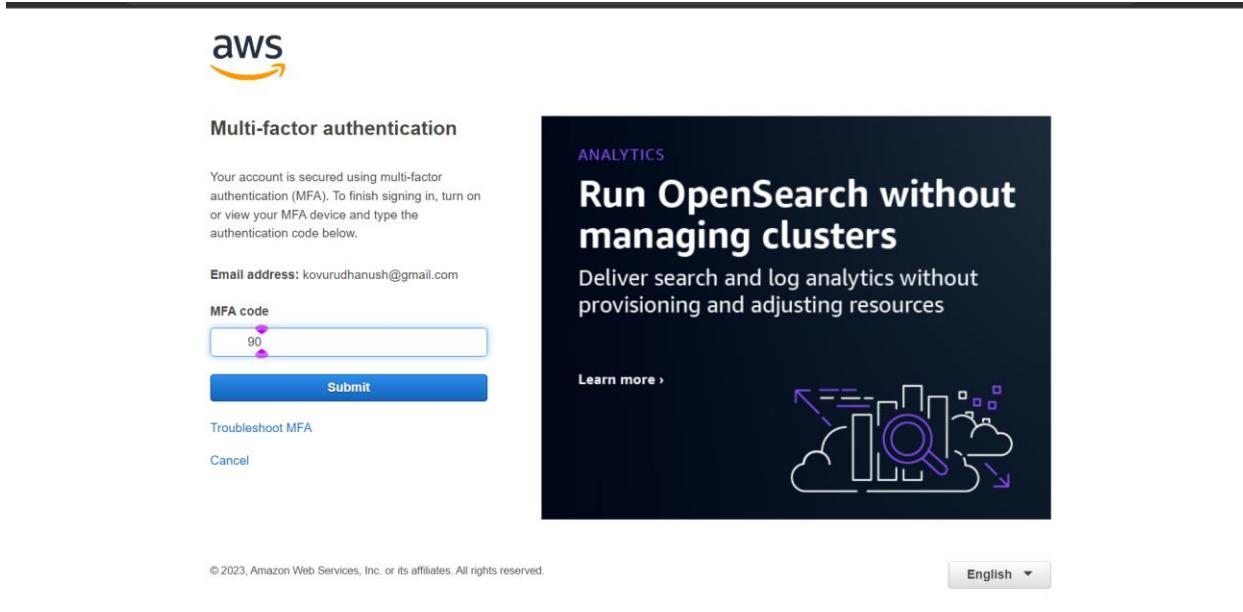
ANALYTICS

Run OpenSearch without managing clusters

Deliver search and log analytics without provisioning and adjusting resources

[Learn more >](#)





© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

English ▾

The image shows the AWS Console Home screen. At the top, there is a navigation bar with the AWS logo, 'Services' (selected), a search bar, and account information (KOVVURU DHANUSH). Below the navigation bar is a 'Console Home' section with a 'Recently visited' list containing links to Billing, EC2, Elastic Beanstalk, AWS Cost Explorer, VPC, Lambda, DynamoDB, IAM, S3, and CodePipeline. There are buttons for 'Reset to default layout' and '+ Add widgets'. At the bottom, there are links for CloudShell, Feedback, and various legal and preference links.

Now I have log into my account successfully.

← 🔎 ⋮

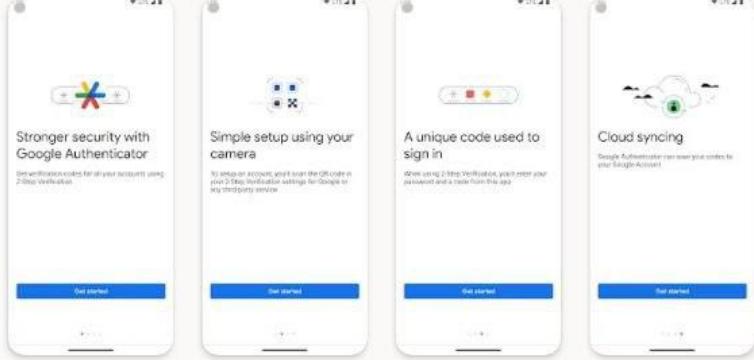
 Google
Authenticator

Google LLC

3.9 ★
452K reviews ⓘ |  7.0 MB |  Rated for 3+

Install

Install on phone. More devices available.



About this app →

Enable 2-step verification to protect your account from hijacking.

Tools

Data safety →

Safety starts with understanding how developers collect and share your data. Data privacy and security

Google Play Games Apps Movies Books Children

Google Authenticator

Google LLC

3.9★ 467K reviews 100M+ Downloads Rated for 3+

Install Share Add to wishlist

This app is available for your device



App support More by Google LLC →

More by Google LLC →

Google Pay: Secure UPI payment Google LLC 4.4★

IAM > Security credentials > Assign MFA device

Step 1 Select MFA device

Step 2 Set up device

Select MFA device

MFA device name

Device name
Enter a meaningful name to identify this device.
 Maximum 128 characters. Use alphanumeric and '-' characters.

MFA device

Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.

Authenticator app
Authenticate using a code generated by an app installed on your mobile device or computer.

Security Key
Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.

Hardware TOTP token
Authenticate using a code displayed on a hardware Time-based one-time password (TOTP) token.

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

IAM > Security credentials > Assign MFA device

Step 1 Select MFA device

Step 2 Set up device

Select MFA device

MFA device name

Device name
Enter a meaningful name to identify this device.
 Maximum 128 characters. Use alphanumeric and '+' '-' characters.

MFA device

Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.

Authenticator app
Authenticate using a code generated by an app installed on your mobile device or computer.

Security Key
Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.

Hardware TOTP token
Authenticate using a code displayed on a hardware Time-based one-time password (TOTP) token.

Cancel **Next**

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Click on next.

IAM > Security credentials > Assign MFA device

Step 1 Select MFA device

Step 2 Set up device

Set up device

Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
[See a list of compatible applications](#)

2 Show QR code

Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. [Show secret key](#)

3 Fill in two consecutive codes from your MFA device.

MFA code 1

MFA code 2

Cancel **Previous** **Add MFA**

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Now click on show QR Code and add MFA 1, 2 .

Step 1
Select MFA device

Step 2
Set up device

Set up device Info

Authenticator app
A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
[See a list of compatible applications](#)

2 Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. [Show secret key](#)

3 Fill in two consecutive codes from your MFA device.

MFA code 1
616783

MFA code 2
659444

Cancel Previous Add MFA

Step 1
Select MFA device

Step 2
Set up device

Set up device Info

Authenticator app
A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
[See a list of compatible applications](#)

2 Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. [Show secret key](#)

3 Fill in two consecutive codes from your MFA device.

MFA code 1
616783

MFA code 2
659444

Cancel Previous Add MFA

The screenshot shows the 'My security credentials' section of the AWS IAM console. It includes fields for Account name, Email address, AWS account ID, Canonical user ID, and a table for Multi-factor authentication (MFA) devices. The MFA device listed is 'Virtual' with identifier 'arn:aws:iam::280694802344:mfa/My_REALME_GT_MASTER_EDITION'. There is a table for Access keys and another for CloudFront key pairs.

Now done.

IAM ROLES

The screenshot shows the AWS Console Home page. It features a 'Recently visited' section with links to Billing, EC2, Elastic Beanstalk, AWS Cost Explorer, VPC, Lambda, DynamoDB, IAM, S3, and CodePipeline. To the right, there are three 'Welcome to AWS' widgets: 'Getting started with AWS' (with a rocket icon), 'Training and certification' (with a graduation cap icon), and 'What's new with AWS?' (with a lightbulb icon). At the bottom, there are sections for 'AWS Health' and 'Cost and usage'.

Login to your account.

The screenshot shows the AWS search interface with the query 'IAM'. The results are categorized into 'Services' and 'Features'.

Services (10)

- Documentation (48,487)
- Marketplace (675)
- Blogs (1,649)
- Events (12)
- Tutorials (2)

Features (20)

- IAM ★** Manage access to AWS resources
- IAM Identity Center ☆** Manage workforce user access to multiple AWS accounts and cloud applications
- Resource Access Manager ☆** Share AWS resources with other accounts or AWS Organizations
- AWS App Mesh ☆** Easily monitor and control microservices

Features (See all 20 results)

- Groups** IAM feature

Current month costs: Top costs for current month

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

In Search bar type IAM.

The screenshot shows the IAM Dashboard with the following details:

IAM resources

User groups	Users	Roles	Policies	Identity providers
1	1	5	4	0

What's new

- IAM Roles Anywhere is now available in the AWS GovCloud (US) Regions. 2 weeks ago
- AWS Identity and Access Management provides action last accessed information for more than 140 services. 3 weeks ago
- IAM roles last used and last accessed information available in AWS GovCloud (US) Regions. 4 weeks ago
- IAM Roles Anywhere credential helper adds support for O5 certificate stores. 2 months ago

AWS Account

Account ID: 280694802344
Account Alias: Create
Sign-in URL for IAM users in this account: https://280694802344.signin.aws.amazon.com/console

Quick Links

My security credentials: Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Click on Roles.

The screenshot shows the AWS IAM Roles page. On the left, there's a sidebar with navigation links like Dashboard, Access management, Roles, Access reports, and more. The main area displays a table of roles:

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service)	-

Below the table, there are three sections: "Roles Anywhere" (with icons for SSO, X.509, and Temporary credentials), "Access AWS from your non AWS workloads" (with a brief description), and "X.509 Standard" (with a brief description). At the bottom right, there are links for "Manage" and "Create role".

Click on create Role.

The screenshot shows the "Select trusted entity" step of the "Create role" wizard. It has three tabs: Step 1 (Select trusted entity), Step 2 (Add permissions), and Step 3 (Name, review, and create). The Step 1 tab is active. It includes a "Trusted entity type" section with four options:

- AWS service: Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- AWS account: Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- Web identity: Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- SAML 2.0 federation: Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- Custom trust policy: Create a custom trust policy to enable others to perform actions in this account.

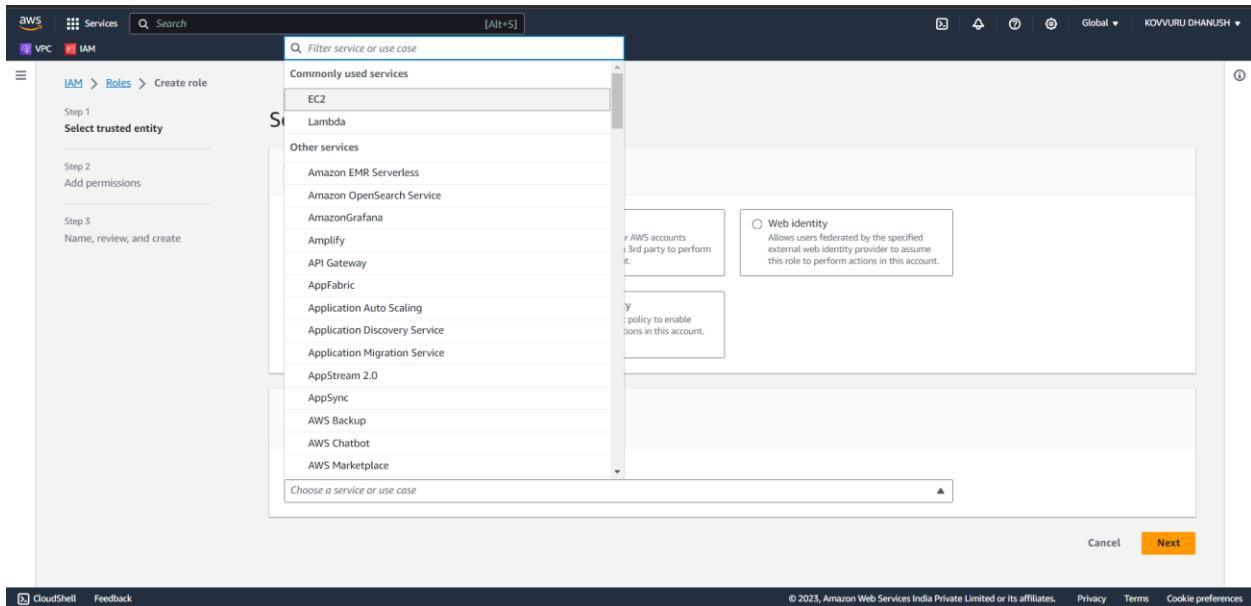
Below this is a "Use case" section with a note: "Allow an AWS service like EC2, Lambda, or others to perform actions in this account." A dropdown menu for "Service or use case" is shown, with the placeholder "Choose a service or use case". At the bottom right are "Cancel" and "Next" buttons.

Click on AWS Service.

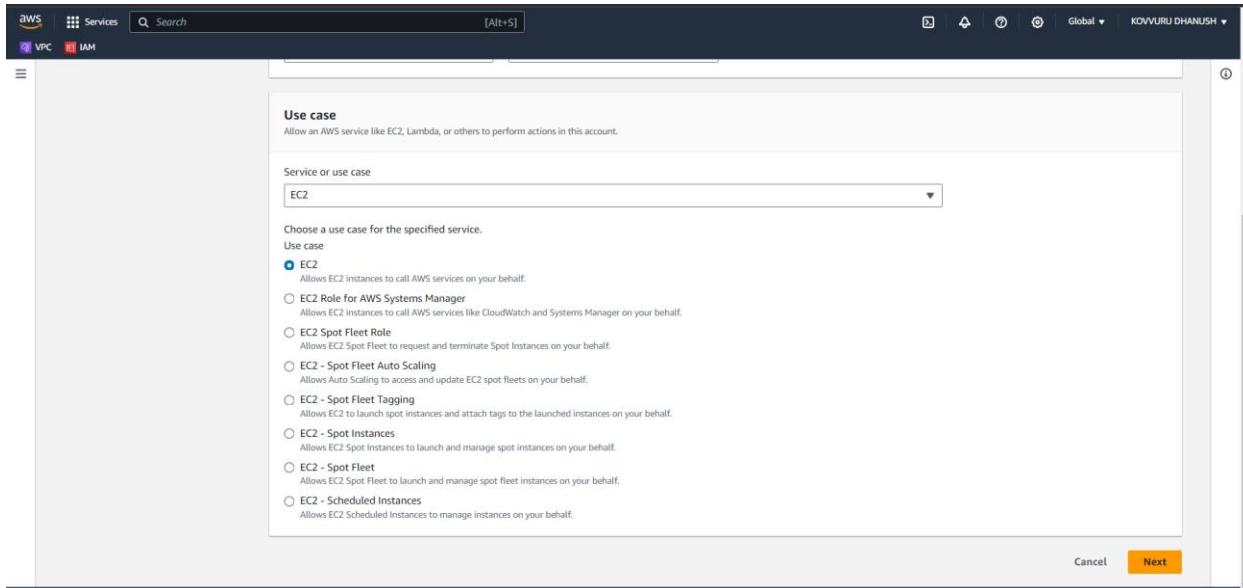
AWS service

Allow AWS services like EC2, Lambda, or others to perform actions in this account.

Read this.

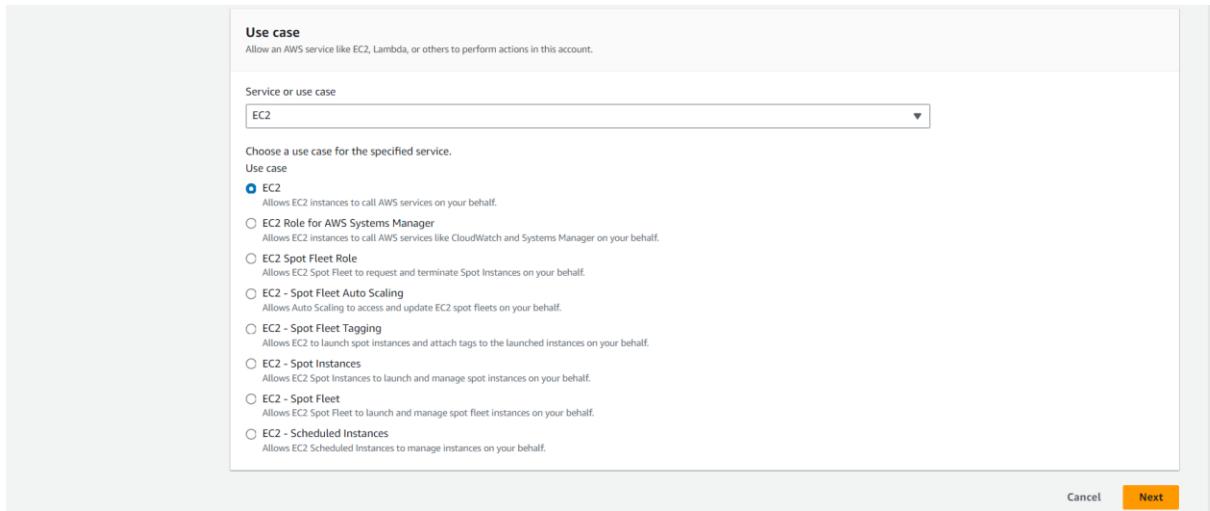


Here in the use case select EC2 .



Here select EC2 ->Allows you to call AWS Services on your behalf.

Here while discussing EC2, I will share what is meant by Spot Fleet and spot instances and I will share minimum 6 posts on EC2 only in detailed and simple.



Click on next.

The screenshot shows the AWS IAM 'Add permissions' step. The top navigation bar includes 'Services' and 'Search'. The main area has three steps: 'Select trusted entity', 'Add permissions', and 'Name, review, and create'. The 'Add permissions' step is active, titled 'Add permissions'. Below it, a sub-section titled 'Permissions policies (886)' says 'Choose one or more policies to attach to your new role.' A search bar and a 'Filter by Type' dropdown are present. The table lists 45 policies, each with a checkbox, policy name, type (AWS managed), and a brief description. Policies listed include 'AdministratorAccess', 'AmazonAPIGatewayAdministrator', and various Alexa and Amazon AppFlow policies.

Here in permissions, we need to attach policy why this role and what to do.

Here we attach one policy for the roles.

This screenshot continues from the previous one, showing the 'Add permissions' step. The search bar now contains 'ec2'. The table lists 29 matches for 'AmazonEC2FullAccess'. The row for 'AmazonEC2FullAccess' is selected, indicated by a blue border around the checkbox and the row itself. Other policies listed include 'AmazonEC2ContainerRegistryFullAccess', 'AmazonEC2ContainerRegistryPowerUser', and 'AmazonEC2ContainerServiceAutoscaleRole'.

Here I gave full permission to EC2 mean EC2 Full Access.

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

Add permissions

Permissions policies (2/886) Info

Choose one or more policies to attach to your new role.

Policy name	Type	Description
AmazonEC2ReadOnlyAccess	AWS managed	Provides read only access to Amazon EC2 via the AWS Management Console.

Set permissions boundary - optional

Cancel Previous Next

Here If I want to give read only Access, I can Give Access to just read mean I can't create the Instance or I can't do any changes I have permissions that is just to read.

Here for security reasons, I'm giving only one permission that is just to read EC2 Instance.

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

Add permissions

Permissions policies (2/886) Info

Choose one or more policies to attach to your new role.

Policy name	Type	Description
AmazonEC2ReadOnlyAccess	AWS managed	Provides read only access to Amazon EC2 via the AWS Management Console.

Set permissions boundary - optional

Cancel Previous Next

So, select the permission and attach it to the role.

The screenshot shows the 'Create role' wizard in the AWS IAM console. The current step is 'Name, review, and create'. The role details section shows the role name 'EC2ReadOnlyPermission' and a description: 'Allow EC2 instances to call AWS services on your behalf.' Below this is the 'Trust policy' section, which contains the following JSON policy:

```

1 "Version": "2012-10-17",
2 "Statement": [
3     {
4         "Effect": "Allow",
5         "Action": [
6             "sts:AssumeRole"
7         ],
8         "Principal": [
9             "*"
10        ],
11        "Service": [
12            "ec2.amazonaws.com"
13        ]
14    }
15 ]

```

Below the trust policy is the 'Permissions policy summary' section, which lists the policy name 'AmazonEC2ReadOnlyAccess' and its type 'AWS managed'. The 'Attached as' dropdown is set to 'Permissions policy'. The final section is 'Step 3: Add tags', which currently has no tags added.

Here if you observer I gave permission to read EC2 Instances only.

This screenshot shows the same 'Create role' wizard as the previous one, but the JSON policy document in the 'Trust policy' section is identical to the one shown in the first screenshot.

```

1 "Version": "2012-10-17",
2 "Statement": [
3     {
4         "Effect": "Allow",
5         "Action": [
6             "sts:AssumeRole"
7         ],
8         "Principal": [
9             "*"
10        ],
11        "Service": [
12            "ec2.amazonaws.com"
13        ]
14    }
15 ]

```

Here this is called JSON Policy we will see what is meant by version, Statement, Effect, Action and Service in simple.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "sts:AssumeRole"  
            ],  
            "Principal": {  
                "Service": [  
                    "ec2.amazonaws.com"  
                ]  
            }  
        }  
    ]  
}
```

Here we will look into this Syntax and what it is meant in detailed.

Version:

This specifies the version of the policy language being used. In this case, it's using the version released on October 17, 2012.

Statement:

This is an array of statements. Each statement defines a single permission or rule.

Effect:

This determines whether the permissions are granted or denied. In this case, it's set to "Allow", which means it allows the specified action.

Action:

This specifies the action or actions that are allowed. In this case, it allows the action "sts:AssumeRole". This action allows an entity (in this case, an EC2 instance) to assume a specified IAM role.

Principal:

Think like this policy applies to EC2 instances.

Screenshot of the AWS IAM Role creation wizard:

- Step 1: Name, review, and create**
 - Role details**
 - Role name:** EC2RoleForReadOnlyPermission
 - Description:** Allows EC2 instances to call AWS services on your behalf.
 - Step 1: Select trusted entities**
 - Trust policy (JSON code shown)
- Step 2: Add permissions**
 - Permissions policy summary
 - Policy name: **AmazonEC2ReadOnlyAccess**
 - Type: AWS managed
 - Attached as: Permissions policy
- Step 3: Add tags**
 - Add tags - optional
 - No tags associated with the resource.
 - Add new tag

Bottom right: Cancel, Previous, Create role, Next, Done, Create policy.

Click on create Role.

Success message: **Role EC2RoleForReadOnlyPermission created.**

Roles (3) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service)	-
EC2RoleForReadOnlyPermission	AWS Service: ec2	-

Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

Now role has created successfully.

The screenshot shows the AWS IAM Roles page. At the top, it displays the role name "EC2RoleForReadOnlyPermission" with a "Delete" button. Below the title, a summary table provides details like creation date (October 08, 2023), ARN (arn:aws:iam::280694802344:role/EC2RoleForReadOnlyPermission), and instance profile ARN (arn:aws:iam::280694802344:instance-profile/EC2RoleForReadOnlyPermission). The "Permissions" tab is selected, showing one policy attached: "AmazonEC2ReadOnlyAccess". Other tabs include "Trust relationships", "Tags", "Access Advisor", and "Revoke sessions". At the bottom, there are buttons for "Edit", "Simulate", "Remove", and "Add permissions".

Here check the permission policies.

Check this below link for further information.

<https://docs.aws.amazon.com/aws-managed-policy/latest/reference/AmazonEC2ReadOnlyAccess.html>

This screenshot is identical to the one above, showing the "Permissions" tab for the "EC2RoleForReadOnlyPermission" role. It displays one attached policy, "AmazonEC2ReadOnlyAccess". The interface includes search, filter, and pagination controls at the top right.

Here if we want further permissions, we can edit the permissions mean we can add permissions.

Now role has created successfully.

AWS CLI and Console Access

Use this link to download CLI.

Download and run the AWS CLI MSI installer for Windows (64-bit):

<https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html>

<https://awscli.amazonaws.com/AWSCLIV2.msi>

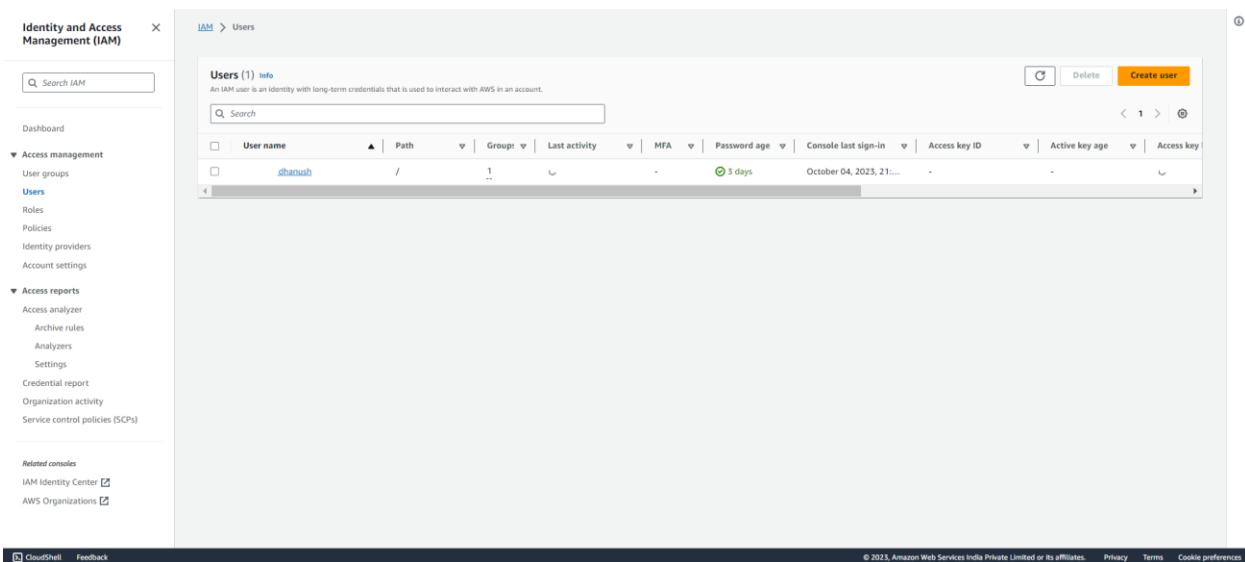
After Downloading successfully.



To check if it is downloaded successfully or not.

```
waws --version
aws-cli/2.13.4 Python/3.11.4 Windows/10 exe/AMD64 prompt/off
```

Here in my case, it is downloaded successfully.



The screenshot shows the AWS Identity and Access Management (IAM) service interface. On the left, there's a navigation sidebar with options like 'Dashboard', 'Access management' (which is expanded to show 'User groups', 'Users', 'Roles', 'Policies', 'Identity providers', and 'Account settings'), 'Access reports' (with 'Access analyzer', 'Archive rules', 'Analyzers', and 'Settings'), and 'Related consoles' (with links to 'IAM Identity Center' and 'AWS Organizations'). The main content area is titled 'Users (1) info' and contains a table with one row. The table columns are: User name, Path, Groups, Last activity, MFA, Password age, Console last sign-in, Access key ID, Active key age, and Access key. The single user listed is 'dhanush'. The 'Create user' button is visible at the top right of the table.

Here if you remember in my previous post, I created IAM User, and we gave permission Administrator Access right so by using CLI we will create S3 bucket via CLI when I'm sharing posts regarding S3 .

But now we will see via CLI how many users that are present in my account.

So, here we need the Access key and Secret Access key.

The screenshot shows the AWS search interface with the query 'IAM' entered in the search bar. The results are categorized into 'Services' and 'Features'. Under 'Services', there are 10 results: IAM (Manage access to AWS resources), IAM Identity Center (Manage workforce user access to multiple AWS accounts and cloud applications), Resource Access Manager (Share AWS resources with other accounts or AWS Organizations), and AWS App Mesh (Easily monitor and control microservices). Under 'Features', there are 20 results: Groups (IAM feature). A sidebar on the right displays 'AWS Fundamentals' and 'AWS certification' sections.

In search bar type IAM.

The screenshot shows the IAM Users section. The left sidebar includes options like Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), Access reports (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs)), and Related consoles (IAM Identity Center, AWS Organizations). The main area displays a table titled 'Users (1) info' with one entry:

User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age	Access key
kovvuru_dhanush	/		Oct 04, 2023		3 days	October 04, 2023, 21...			

Come to the Users section.

Identity and Access Management (IAM)

kovvuru_dhanush

Summary

ARN: arn:aws:iam::280694802344:user/kovvuru_dhanush

Created: October 04, 2023, 21:18 (UTC+05:30)

Console access: Enabled without MFA

Last console sign-in: 3 days ago

Access key 1: Create access key

Permissions | Groups (1) | Tags | Security credentials | Access Advisor

Permissions policies (1): AdministratorAccess

Generate policy based on CloudTrail events

Generate policy

No requests to generate a policy in the past 7 days.

Identity and Access Management (IAM)

kovvuru_dhanush

Summary

ARN: arn:aws:iam::280694802344:user/kovvuru_dhanush

Created: October 04, 2023, 21:18 (UTC+05:30)

Console access: Enabled without MFA

Last console sign-in: 3 days ago

Access key 1: Create access key

Permissions | Groups (1) | Tags | Security credentials | Access Advisor

Console sign-in

Console sign-in link: [Manage console access](#)

Multi-factor authentication (MFA) (0): Assign MFA device

Device type Identifier Certifications Created on

Assign MFA device

Click on security credentials.

Access keys (0): Create access key

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 [\[link\]](#)

Create access key

Click on the create Access key.

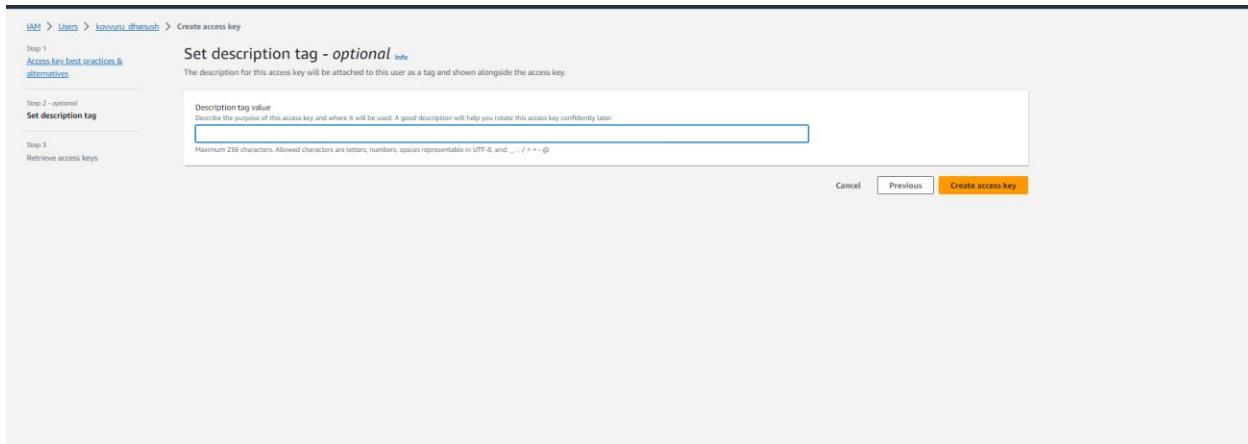
The screenshot shows the AWS IAM 'Create access key' wizard. It is on Step 1: Access key best practices & alternatives. The 'Command Line Interface (CLI)' option is selected. Other options include Local code, Application running on an AWS compute service, Third-party service, Application running outside AWS, and Other. A note at the bottom says 'Your use case is not listed here.' At the bottom right are 'Cancel' and 'Next' buttons.

Here we need to access via CLI.

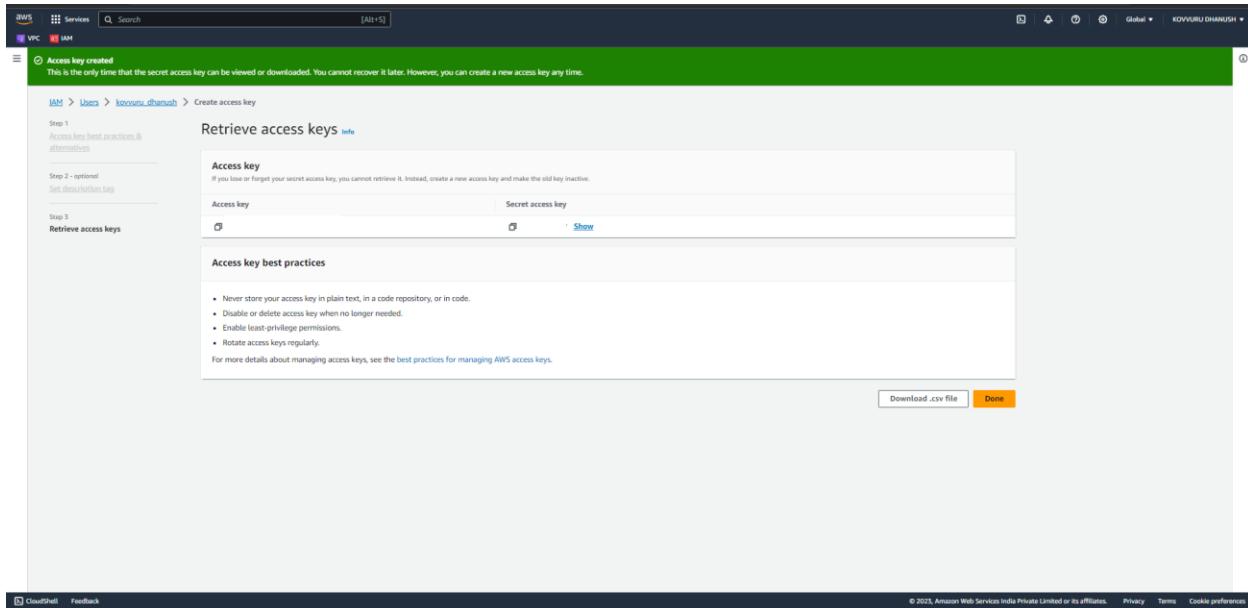
So, select CLI(Command Line Interface).

The screenshot shows the AWS IAM 'Create access key' wizard. It is on Step 1: Access key best practices & alternatives. The 'Command Line Interface (CLI)' option is selected. An 'Alternatives recommended' section lists using AWS CloudShell or AWS CLI V2. A 'Confirmation' section has a checked checkbox for 'I understand the above recommendation and want to proceed to create an access key.' At the bottom right are 'Cancel' and 'Next' buttons.

Now click on next.



Now click on the create Access key.



Now Access key and Secret Access key was generated Successfully.

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
[Get temporary key](#)

Step 3
[Retrieve access keys](#)

Retrieve access keys [Info](#)

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.

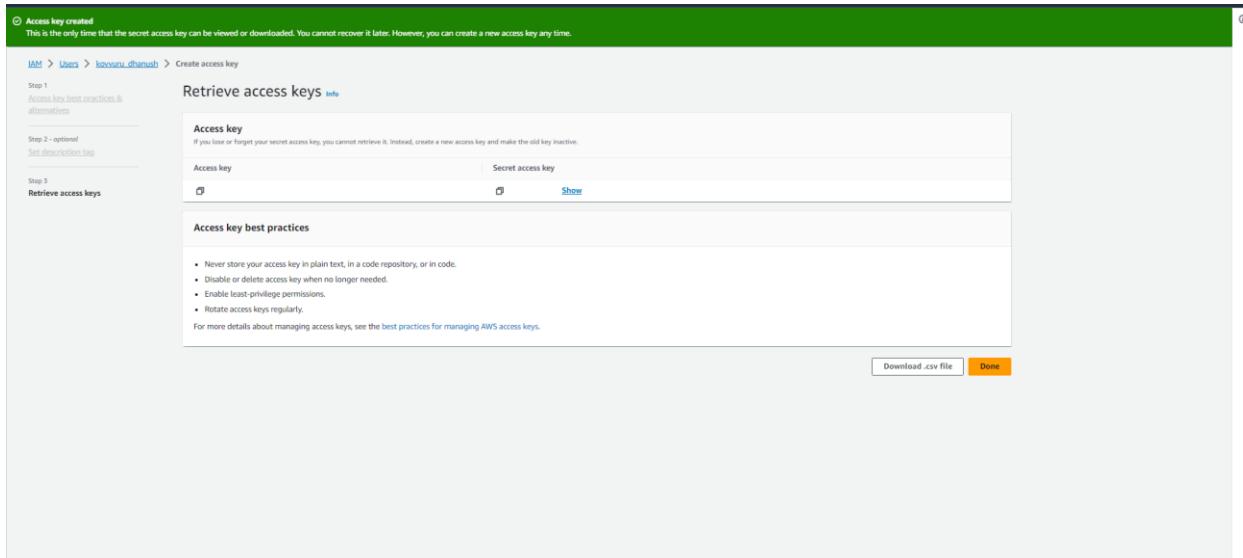
Access key	Secret access key
View	View Show

Access key best practices

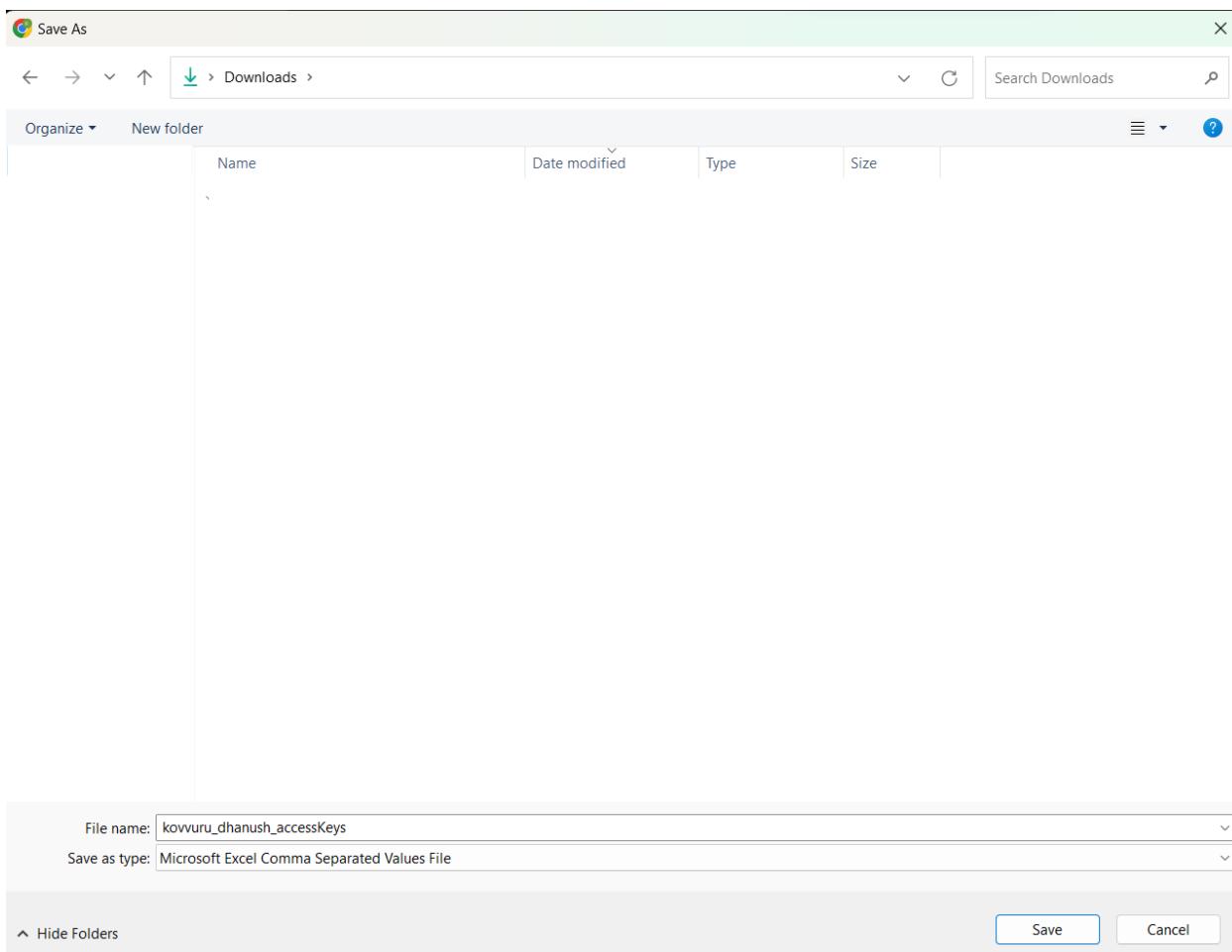
- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the best practices for managing AWS access keys.

[Download .csv file](#) [Done](#)



Click on Download .csv file.



Download it to your system.



Today

- [kovvuru_dhanush_accessKeys.csv](#)

blob:https://us-east-1.console.aws.amazon.com/0e2c85ee-efcd-4aca-bedf-470a6d1f6...

[Show in folder](#)

- [AWS Certified Cloud Practitioner \(retired\).pdf](#)

https://www.certmetrics.com/amazon/public/download_score_report.aspx?d=202310...

[Show in folder](#)

See Downloaded Successfully.

The screenshot shows the AWS IAM Access Key creation interface. At the top, there's a green banner stating "Access key created" with the note: "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." Below this, the breadcrumb navigation shows: IAM > Users > kovvuru_dhanush > Create access key. The main form is titled "Retrieve access keys" and contains fields for "Access key" (with a "Generate" button) and "Secret access key" (with a "Show" link). A sidebar on the left lists steps: Step 1 (Access key best practices), Step 2 (optional: Set expiration tag), and Step 3 (Retrieve access keys). A section titled "Access key best practices" lists several guidelines. At the bottom right are "Download .csv file" and "Done" buttons. The footer includes links for CloudShell, Feedback, and various AWS terms like Global, IAM, VPC, and Lambda.

Now click on done.

The screenshot shows the AWS IAM Access Keys page. It displays a single access key named "AKIAUCWVWY6UGGF26Y7Y". The key has the following details:

Key	Description	Status	Created	Last used service
AKIAUCWVWY6UGGF26Y7Y	-	Active	3 minutes ago	N/A

A "Create access key" button is located at the top right.

check the status it is active now.

Now open your CLI.

```
kovur>aws --version
aws-cli/2.13.4 Python/3.11.4 Windows/10 exe/AMD64 prompt/off
kovur>aws configure
AWS Access Key ID [*****cls]:
```

The aws configure command is used to set up the AWS Command Line Interface (CLI) with your AWS account credentials. It allows you to provide your AWS Access Key ID, Secret Access Key, default region, and default output format. This information is necessary for the CLI to communicate with your AWS account.

Now you have downloaded .csv file right open that and copy Access key and paste it on the console.

Now you have downloaded the .csv file, open it right and copy the Secret Access key and paste it on the console.

A screenshot of a Windows Command Prompt window titled "Command Prompt". The command "aws --version" is run, showing "aws-cli/2.13.4 Python/3.11.4 Windows/10 exe/AMD64 prompt/off". Then "aws configure" is run, prompting for AWS Access Key ID, AWS Secret Access Key, Default region name (set to "clear"), and Default output format (set to "None"). Finally, "aws iam list-users" is run, displaying a JSON response with a list of users, their User IDs, and ARNs. A callout box highlights the "here you get user name and user ID" portion of the JSON output.

```
kovur>aws --version
aws-cli/2.13.4 Python/3.11.4 Windows/10 exe/AMD64 prompt/off
kovur>aws configure
AWS Access Key ID [*****cls]
AWS Secret Access Key [*****leat]
Default region name [clear]: [REDACTED]
Default output format [None]: [REDACTED]

C:\Users\kovur>aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": "kovur",
      "UserId": "AIDAJKZPQW5HJL567890",
      "Arn": "arn:aws:iam::123456789012:user/kovur",
      "CreateDate": "2023-01-01T12:00:00Z",
      "PasswordLastUsed": null
    }
  ]
}
```

Add Access key and Secret Access Key here and Add region too.

here you get user name and user ID

See we have listed out IAM Users in my account.

Credentials Report

A screenshot of the AWS IAM "Credentials Report" page. The left sidebar shows navigation options like "Access management", "Access reports", and "Credential report" (which is selected). The main content area displays a "Credentials report of IAM users in this account" section with a "Download credentials report" button. A note indicates no report was created in the past 4 hours. Related consoles like "IAM Identity Center" and "AWS Organizations" are listed at the bottom.

Credentials report of IAM users in this account [Info](#)

The credentials report lists all your IAM users in this account and the status of their various credentials. After a report is created, it is stored for up to four hours.

Credentials report

[Download credentials report](#)

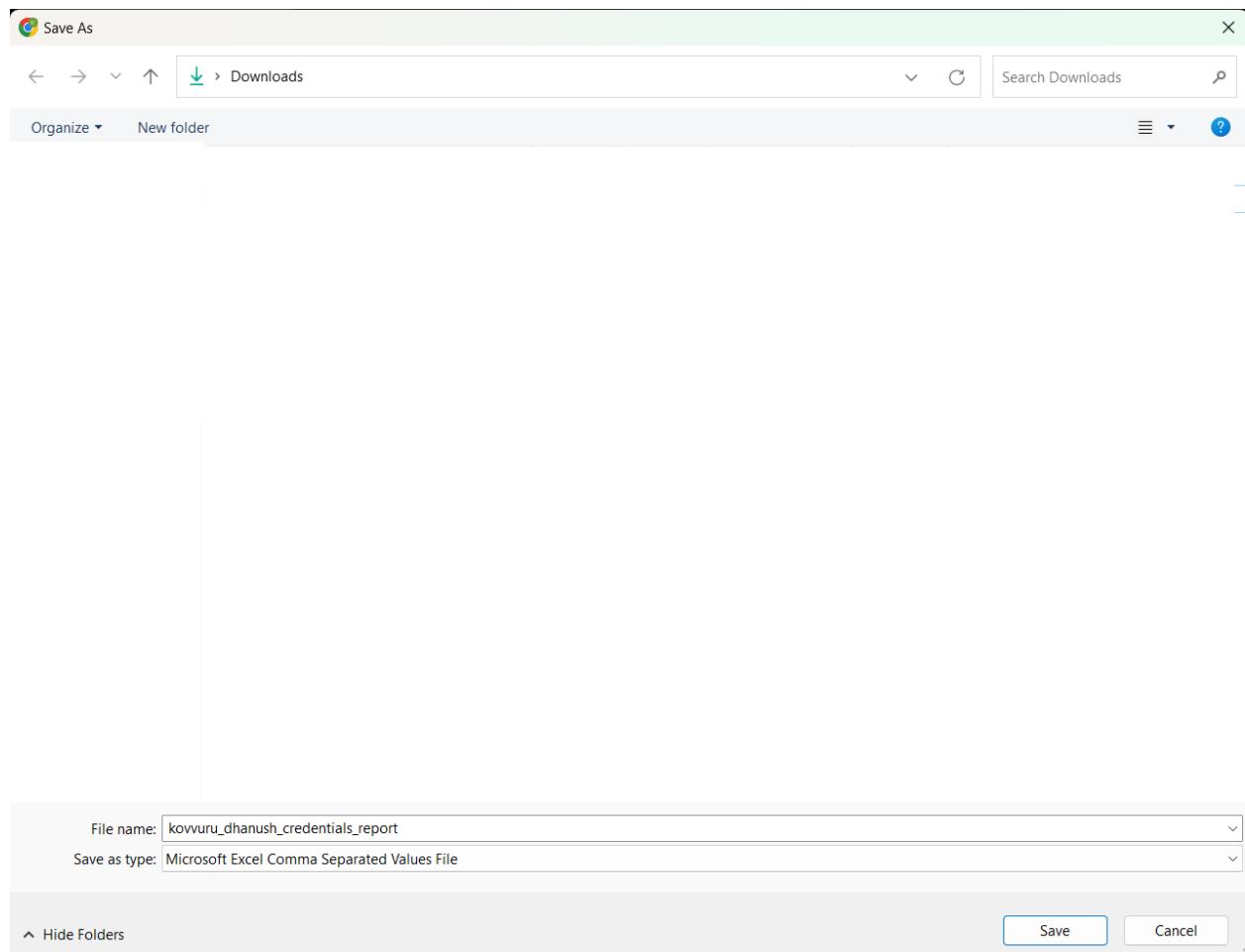
No report created in the past 4 hours. A new report will be created.

Related consoles

IAM Identity Center [\[\]](#)

AWS Organizations [\[\]](#)

Download credentials report.



[Download the credentials Report.](#)

A screenshot of Microsoft Excel showing a table titled "kovvuru_dhanush_credentials_report". The table has 26 columns and 26 rows. The columns are labeled from A to Z. Row 1 contains the column headers: "user", "arn", "user_creation_time", "password_expires", "password_last_used", "password_mfa_active", "access_kev1", "access_kev2", "access_kev3", "access_kev4", "access_kev5", "access_kev6", "access_kev7", "access_kev8", "access_kev9", "access_kev10", "access_kev11", "access_kev12", "access_kev13", "access_kev14", "access_kev15", "access_kev16", "access_kev17", "access_kev18", "access_kev19", "access_kev20", "access_kev21", "access_kev22", "access_kev23", "access_kev24", and "access_kev25". Row 2 contains the value "user". Rows 3 through 25 are empty.

1	user	arn	user_creation_time	password_expires	password_last_used	password_mfa_active	access_kev1	access_kev2	access_kev3	access_kev4	access_kev5	access_kev6	access_kev7	access_kev8	access_kev9	access_kev10	access_kev11	access_kev12	access_kev13	access_kev14	access_kev15	access_kev16	access_kev17	access_kev18	access_kev19	access_kev20	access_kev21	access_kev22	access_kev23	access_kev24	access_kev25
2																															
3																															
4																															
5																															
6																															
7																															
8																															
9																															
10																															
11																															
12																															
13																															
14																															
15																															
16																															
17																															
18																															
19																															
20																															
21																															
22																															
23																															
24																															
25																															
26																															

[Download the credentials report](#)

Thank You

