

## Assignment 2:

### Setting up Custom Sign-in URL || MFA.

- Search for IAM in the management console.
- In the dashboard you can see the 12-digit pre-defined sign-in URL for the IAM users.
- Now to login with the URL you need Users. So, go to users and add a user.
- After the user has been added come back to the dashboard and copy the link seen at the beginning and paste it in a new browser.
- You can see the account id or alias automatically filled with the 12-digit number. If the user doesn't have the URL handy then it is very hard to remember the 12-digit code to log in to the console.

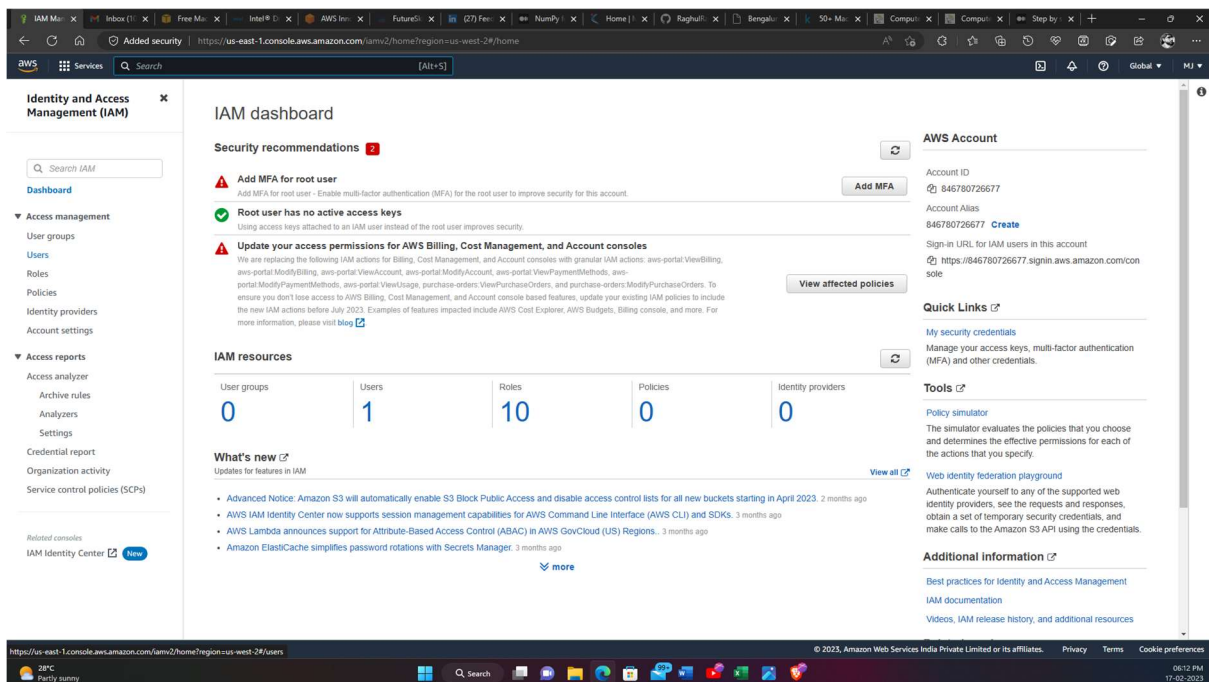
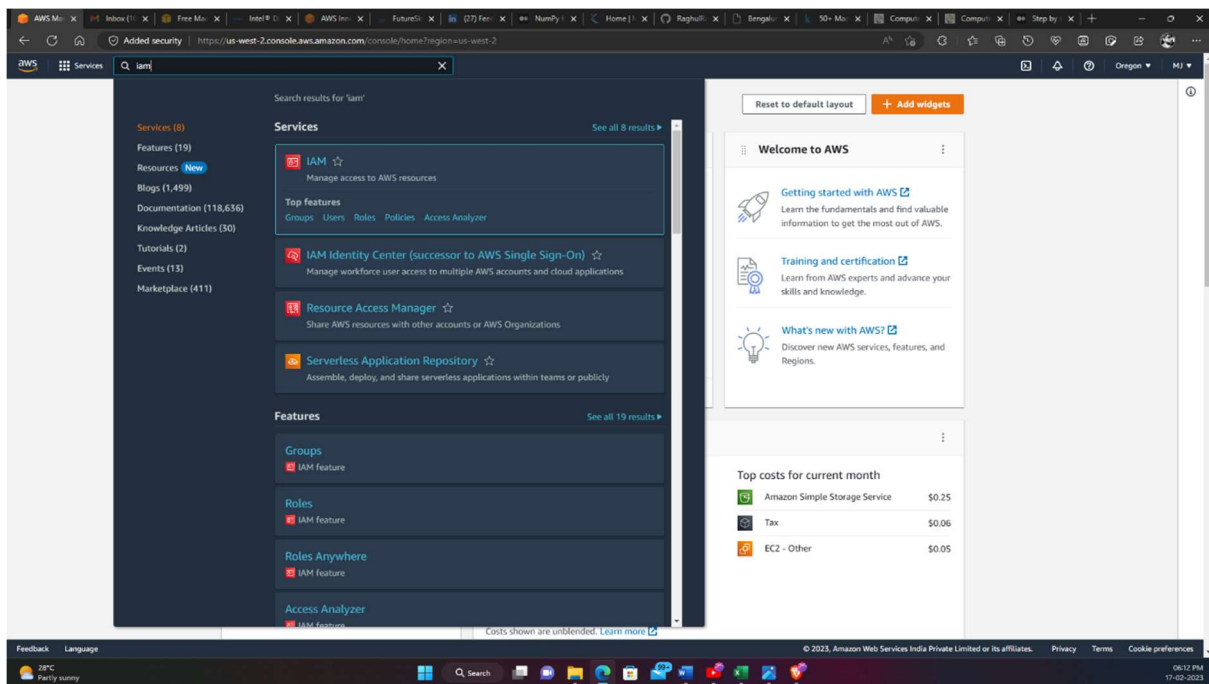
### Setting up custom URL

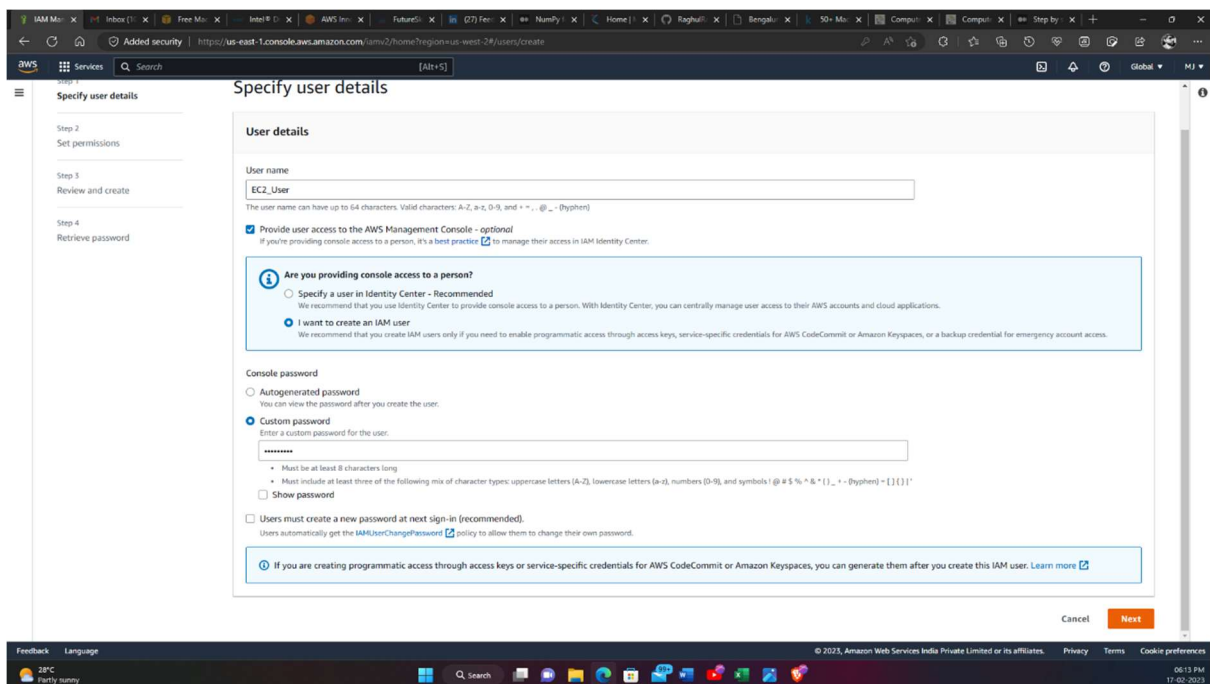
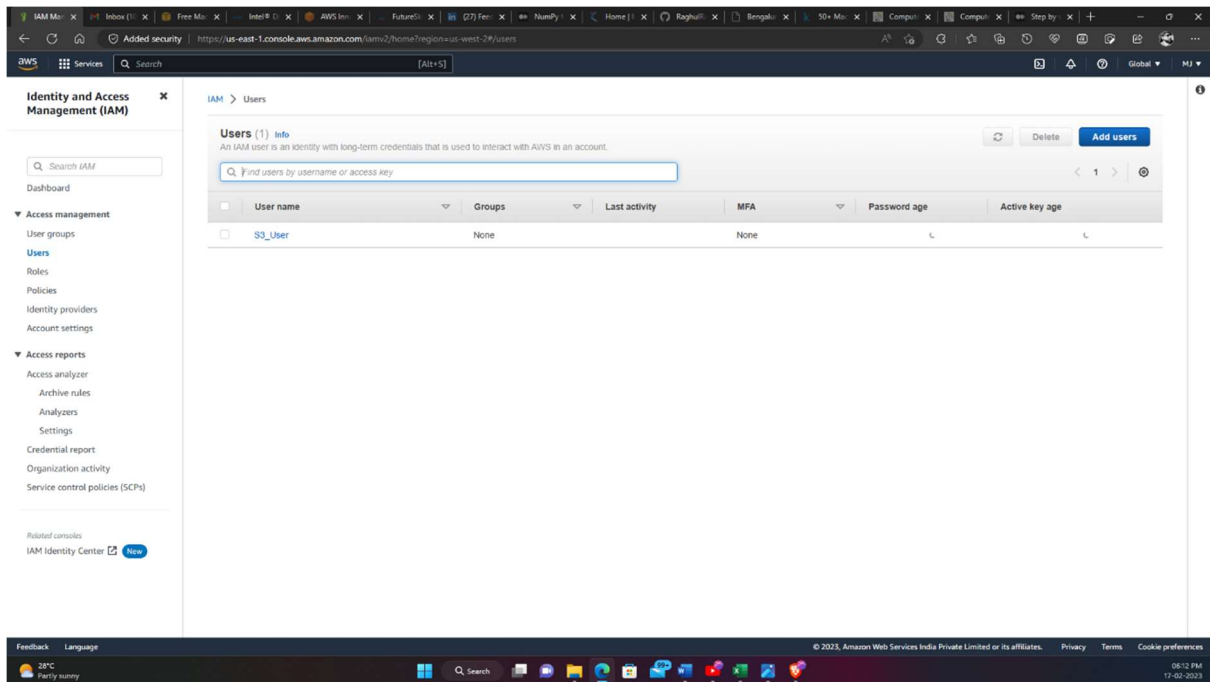
- So now go back to the IAM dashboard and click on create which is present next to the 12-digit in account alias.
- Remember you need to give a unique name for this and after saving the changes you can now see the URL has now changed.
- Copy the URL and paste it in the search box. Now, you can see the Account ID or Account alias as the name which you gave before.
- This is easy to remember and access for the IAM users.

### MFA

- To add MFA come back to the IAM dashboard and click on Add MFA.
- In the next page click on Assign MFA.
- Here we have 3 options, and we will be going with the authenticator app option.
- You can either use the google authenticator app for mobile or use the authenticator extension available in the browsers.
- Here we are using the extension. After adding the extension, we need to scan the QR code present in the screen and add the 2 consecutive codes that are generated to successfully add the authenticator.

- From next time when you login to the console you will be asked to enter the MFA code.





**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 (1/1045)**  
Choose one or more policies to attach to your new user.

Filter distributions by text, property or value  1 match

<input checked="" type="checkbox"/>	Policy name	Type	Attached entities
<input checked="" type="checkbox"/>	AmazonEC2FullAccess	AWS managed	0

**Permissions boundary - optional**  
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. [Learn more](#)

Services

Search

Alt+S

IAM > Users > Create user

Step 1  
Specify user details

Step 2  
Set permissions

Step 3  
**Review and create**

Step 4  
Retrieve password

## 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 EC2_User	Console password type Custom password	Require password reset No
-----------------------	--	------------------------------

### Permissions summary

< 1 >

Name	Type	Used as
AmazonEC2FullAccess	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.

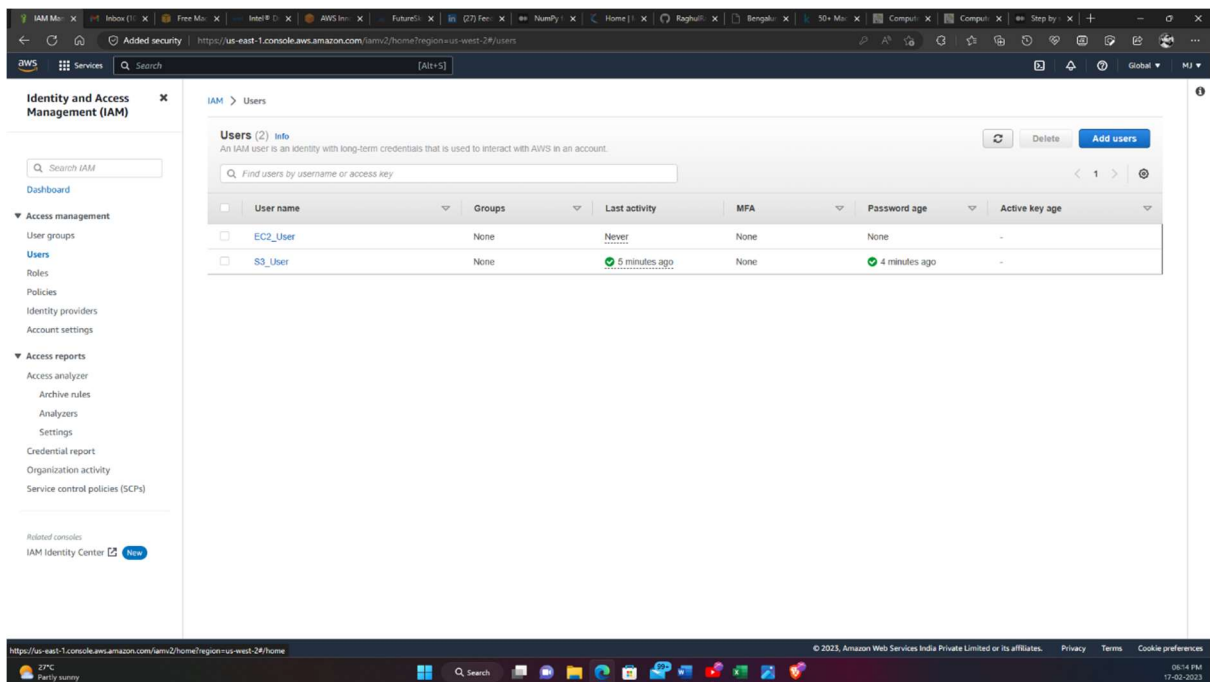
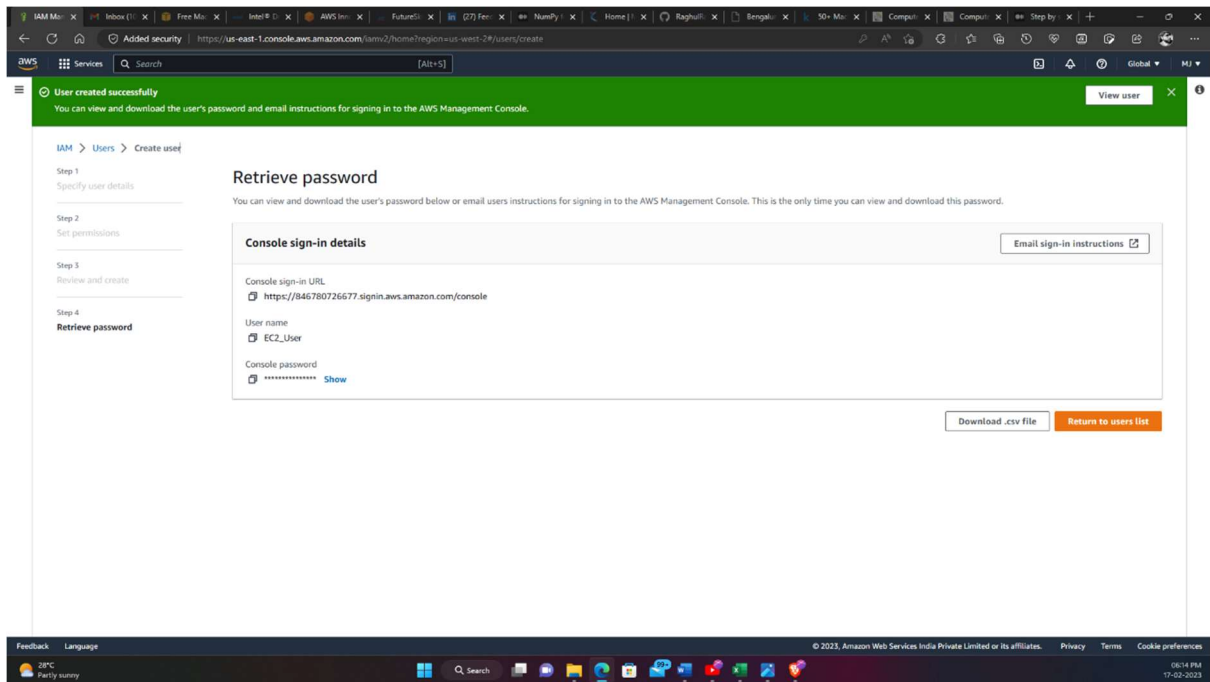
Add new tag

You can add up to 50 more tags.

Cancel

Previous

Create user



Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analysers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Related consoles

- IAM Identity Center

### IAM dashboard

#### Security recommendations

- Add MFA for root user**  
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.  
[Add MFA](#)
- Root user has no active access keys**  
Using access keys attached to an IAM user instead of the root user improves security.
- Update your access permissions for AWS Billing, Cost Management, and Account consoles**  
We are replacing the following IAM actions for Billing, Cost Management, and Account consoles with granular IAM actions: aws-portal:ViewBilling, aws-portal:ModifyBilling, aws-portal:ViewAccount, aws-portal:ModifyAccount, aws-portal:ViewPaymentMethods, aws-portal:ModifyPaymentMethods, aws-portal:ViewUsage, purchase-orders:ViewPurchaseOrders, and purchase-orders:ModifyPurchaseOrders. To ensure you don't lose access to AWS Billing, Cost Management, and Account console based features, update your existing IAM policies to include the new IAM actions before July 2023. Examples of features impacted include AWS Cost Explorer, AWS Budgets, Billing console, and more. For more information, please visit [blog](#).  
[View affected policies](#)

#### IAM resources

User groups	Users	Roles	Policies	Identity providers
0	2	10	0	0

#### What's new

Updates for features in IAM

- Advanced Notice: Amazon S3 will automatically enable S3 Block Public Access and disable access control lists for all new buckets starting in April 2023. 2 months ago
- AWS IAM Identity Center now supports session management capabilities for AWS Command Line Interface (AWS CLI) and SDKs. 3 months ago
- AWS Lambda announces support for Attribute-Based Access Control (ABAC) in AWS GovCloud (US) Regions. 3 months ago
- Amazon ElastiCache simplifies password rotations with Secrets Manager. 3 months ago

[View all](#)

#### AWS Account

Account ID: 846780726677

Account Alias

[Sign in URL Copied](#)

[Create](#)

IAM users in this account

[https://846780726677.signin.aws.amazon.com/console](#)

#### Quick Links

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

#### Tools

- [Policy simulator](#)  
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.
- [Web identity federation playground](#)  
Authenticate yourself to any of the supported web identity providers, see the requests and responses, obtain a set of temporary security credentials, and make calls to the Amazon S3 API using the credentials.

#### Additional information

- [Best practices for Identity and Access Management](#)
- [IAM documentation](#)
- [Videos, IAM release history, and additional resources](#)

Feedback Language

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

27°C Partly sunny 06:14 PM 17-02-2023

Amazon Web Services Sign-In

ap-northeast-1.signin.aws.amazon.com/oauth?client\_id=arn%3Aaws%3A%3A%3Aconsole%2Fcanvas&code\_challenge=LizYQKXog2L5zQQGaCDwU0Y787U3hjBUIclAGyxl&code\_challenge\_method=SHA-256&response\_type=code&redirect\_uri=https%3A%2F%2F...

## aws

### Sign in as IAM user

Account ID (12 digits) or account alias

846780726677

IAM user name

EC2\_User

Password

.....

☐ Remember this account

[Sign in](#)

[Sign in using root user email](#)

[Forgot password?](#)

## Amazon DocumentDB AllScale Clusters

Scale your document database to handle virtually any number of reads and writes

[LEARN MORE](#)

English

[Terms of Use](#) [Privacy Policy](#) © 1996-2023, Amazon Web Services, Inc. or its affiliates.

ap-northeast-1.signin.aws.amazon.com/oauth?client\_id=arn%3Aaws%3A%3A%3Aconsole%2Fcanvas&code\_challenge=LizYQKXog2L5zQQGaCDwU0Y787U3hjBUIclAGyxl&code\_challenge\_method=SHA-256&response\_type=code&redirect\_uri=https%3A%2F%2F...

27°C Sunset 06:15 PM 17-02-2023

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

## IAM dashboard

Security recommendations 2

- Add MFA for root user**  
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account. [Add MFA](#)
- Root user has no active access keys**  
Using access keys attached to an IAM user instead of the root user improves security.
- Update your access permissions for AWS Billing, Cost Management, and Account consoles**  
We are replacing the following IAM actions for Billing, Cost Management, and Account consoles with granular IAM actions: `aws-portal:ViewBilling`, `aws-portal:ModifyBilling`, `aws-portal:ViewAccount`, `aws-portal:ModifyAccount`, `aws-portal:ViewPaymentMethods`, `aws-portal:ModifyPaymentMethods`, `aws-portal:ViewUsage`, `purchase-orders:ViewPurchaseOrders`, and `purchase-orders:ModifyPurchaseOrders`. To ensure you don't lose access to AWS Billing, Cost Management, and Account console based features, update your existing IAM policies to include the new IAM actions before July 2023. Examples of features impacted include AWS Cost Explorer, AWS Budgets, Billing console, and more. For more information, please visit [blog](#). [View affected policies](#)

### IAM resources

User groups	Users	Roles	Policies	Identity providers
0	2	10	0	0

### AWS Account

Account ID: 846780726677

Account Alias: 846780726677 [Create](#)

Sign-in URL for IAM users in this account: <https://846780726677.signin.aws.amazon.com/console>

### Quick Links

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

### Tools

- [Policy simulator](#)  
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

Feedback Language

AH43 / NH44 / ... Construction

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

ENG US 06:16 PM 17-02-2023

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

## IAM dashboard

Security recommendations

- Add MFA for root user**  
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account. [Add MFA](#)
- Root user has no active access keys**  
Using access keys attached to an IAM user instead of the root user improves security.
- Update your access permissions for AWS Billing, Cost Management, and Account consoles**  
We are replacing the following IAM actions for Billing, Cost Management, and Account consoles with granular IAM actions: `aws-portal:ViewBilling`, `aws-portal:ModifyBilling`, `aws-portal:ViewAccount`, `aws-portal:ModifyAccount`, `aws-portal:ViewPaymentMethods`, `aws-portal:ModifyPaymentMethods`, `aws-portal:ViewUsage`, `purchase-orders:ViewPurchaseOrders`, and `purchase-orders:ModifyPurchaseOrders`. To ensure you don't lose access to AWS Billing, Cost Management, and Account console based features, update your existing IAM policies to include the new IAM actions before July 2023. Examples of features impacted include AWS Cost Explorer, AWS Budgets, Billing console, and more. For more information, please visit [blog](#). [View affected policies](#)

### IAM resources

User groups	Users	Roles	Policies	Identity providers
0	2	10	0	0

### AWS Account

Account ID: 846780726677

Account Alias: 846780726677 [Create](#)

Sign-in URL for IAM users in this account: <https://846780726677.signin.aws.amazon.com/console>

### Quick Links

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

### Tools

- [Policy simulator](#)  
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

Alias not created for this account.  
The account alias aws-user already exists.

### Create alias for AWS account 846780726677

Preferred alias

Must be not more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen).

New sign-in URL  
<https://assignment-aws-class.signin.aws.amazon.com/console>

**Info** IAM users will still be able to use the default URL containing the AWS account ID.

[Cancel](#) [Save changes](#)

Feedback Language

27°C Partly sunny

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

ENG US 06:17 PM 17-02-2023



Identity and Access Management (IAM)

Search IAM

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)

Alias assignment-aws-class created for this account.

### IAM dashboard

Security recommendations 2

- Add MFA for root user**  
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account. [Add MFA](#)
- Root user has no active access keys**  
Using access keys attached to an IAM user instead of the root user improves security.
- Update your access permissions for AWS Billing, Cost Management, and Account consoles**  
We are replacing the following IAM actions for Billing, Cost Management, and Account consoles with granular IAM actions: `aws-portal:ViewBilling`, `aws-portal:ModifyBilling`, `aws-portal:ViewAccount`, `aws-portal:ModifyAccount`, `aws-portal:ViewPaymentMethods`, `aws-portal:ModifyPaymentMethods`, `aws-portal:ViewUsage`, `purchase-orders:ViewPurchaseOrders`, and `purchase-orders:ModifyPurchaseOrders`. To ensure you don't lose access to AWS Billing, Cost Management, and Account console based features, update your existing IAM policies to include the new IAM actions before July 2023. Examples of features impacted include AWS Cost Explorer, AWS Budgets, Billing console, and more. For more information, please visit [blog](#).

[View affected policies](#)

### IAM resources

User groups	Users	Roles	Policies	Identity providers
0	2	10	0	0

**AWS Account**

Account ID: 846780726677

Account Alias: assignment-aws-class [Edit](#) | [Delete](#)

Sign-in URL for IAM users in this account: <https://assignment-aws-class.signin.aws.amazon.com/console>

**Quick Links**

- [My security credentials](#)  
Manage your access keys, multi-factor authentication (MFA) and other credentials.
- [Tools](#)
  - [Policy simulator](#)  
The simulator evaluates the policies that you choose and determines the

Feedback Language

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

27°C Partly sunny

AWS Management Console

Products Search

Overview Features FAQs

# AWS Management Console

Everything you need to access and manage the AWS Cloud — in one web interface

[Log back in](#)

**Free AWS Training**  
Advance your career with AWS Cloud Practitioner Essentials—a free, six-hour, foundational course

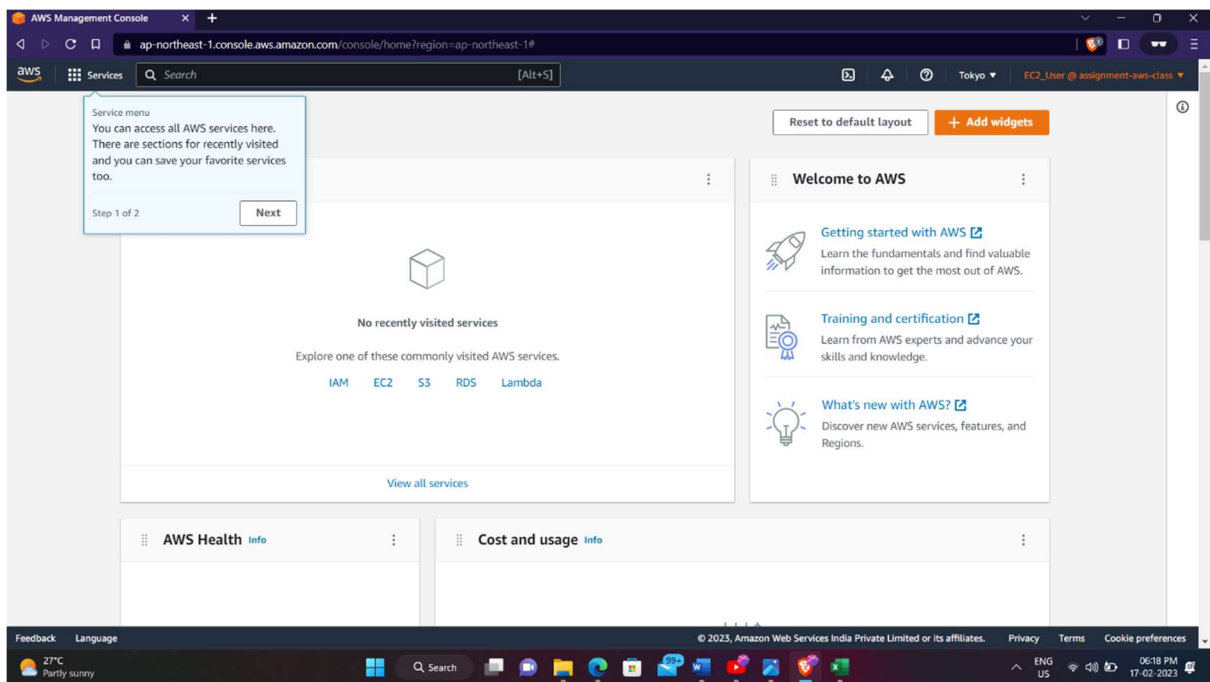
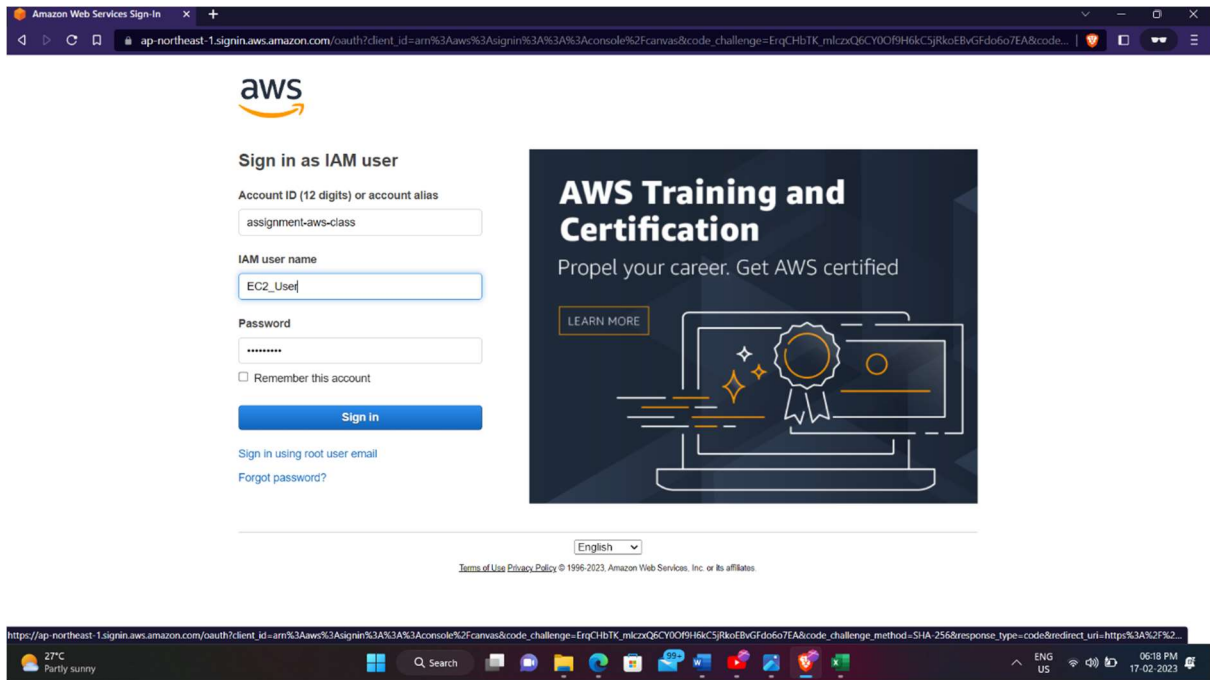
**AWS Certification**  
Propel your career forward with AWS Certification.

**7 Reasons to get AWS Certified**  
Discover the top 7 reasons to get AWS Certified

**AWS Training**  
Free digital courses to help you develop your skills

27°C Partly sunny





Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

## IAM dashboard

Security recommendations 2

- Add MFA for root user**  
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account. [Add MFA](#)
- Root user has no active access keys**  
Using access keys attached to an IAM user instead of the root user improves security.
- Update your access permissions for AWS Billing, Cost Management, and Account consoles**  
We are replacing the following IAM actions for Billing, Cost Management, and Account consoles with granular IAM actions: `aws-portal:ViewBilling`, `aws-portal:ModifyBilling`, `aws-portal:ViewAccount`, `aws-portal:ModifyAccount`, `aws-portal:ViewPaymentMethods`, `aws-portal:ModifyPaymentMethods`, `aws-portal:ViewUsage`, `purchase-orders:ViewPurchaseOrders`, and `purchase-orders:ModifyPurchaseOrders`. To ensure you don't lose access to AWS Billing, Cost Management, and Account console based features, update your existing IAM policies to include the new IAM actions before July 2023. Examples of features impacted include AWS Cost Explorer, AWS Budgets, Billing console, and more. For more information, please visit [blog](#). [View affected policies](#)

### IAM resources

User groups	Users	Roles	Policies	Identity providers
0	2	10	0	0

### AWS Account

Account ID: 846780726677

Account Alias: assignment-aws-class [Edit](#) [Delete](#)

Sign-in URL for IAM users in this account: <https://assignment-aws-class.signin.aws.amazon.com/console>

### Quick Links

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

### Tools

- [Policy simulator](#)  
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

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

27°C Partly sunny

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

## My security credentials (root user) Info

The root user has access to all AWS resources in this account, and we recommend following [best practices](#). To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

**MFA not activated for root user**  
The root user for this account does not have multi-factor authentication (MFA) activated. Activate MFA to improve security for this account. [Assign MFA](#)

### Account details

[Edit account name, email, and password](#)

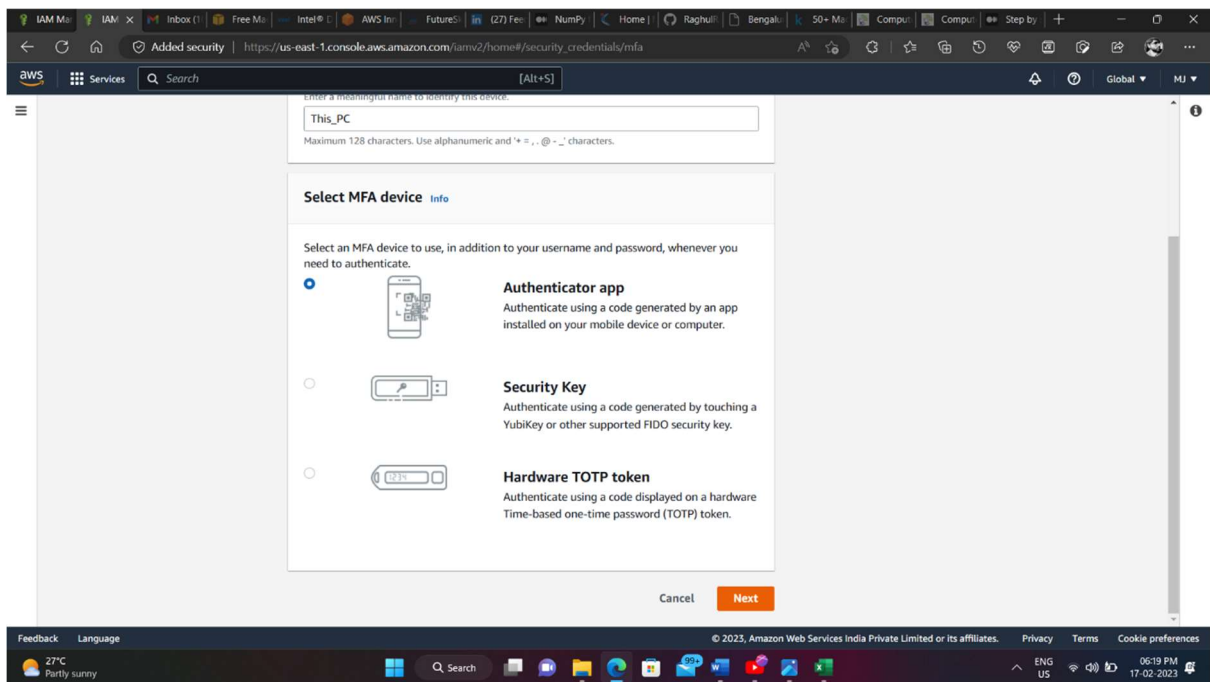
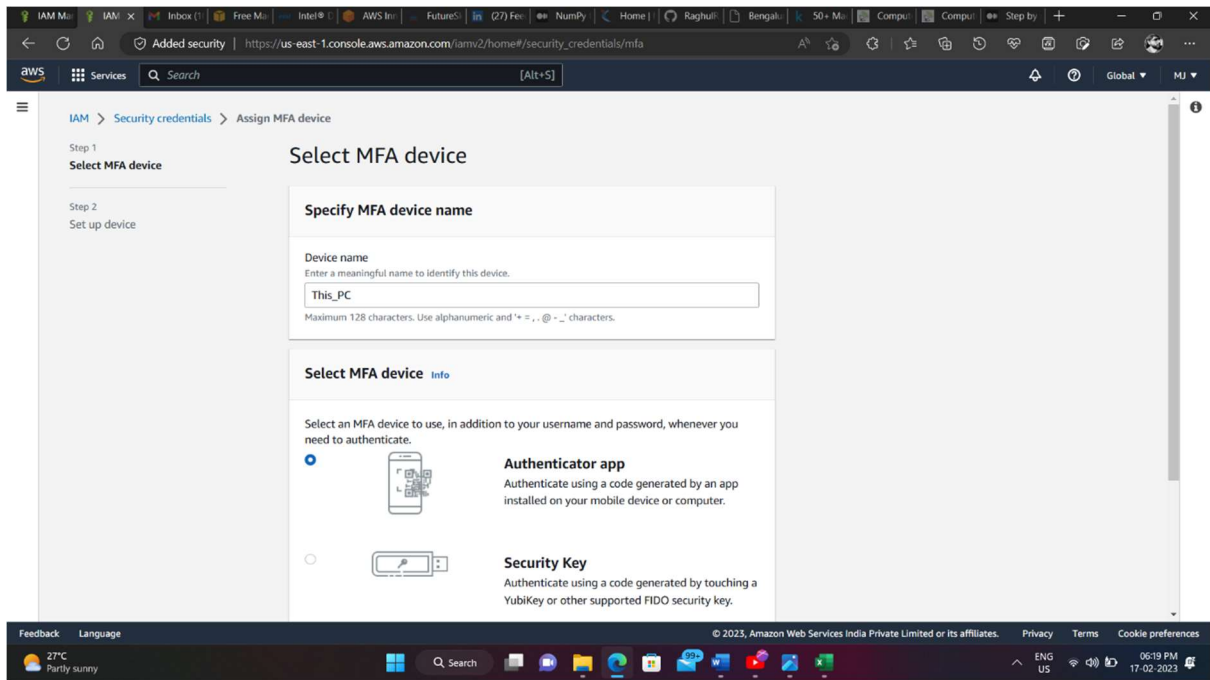
Account name MJ	Email address <a href="mailto:imjmanoj@gmail.com">imjmanoj@gmail.com</a>
AWS account ID 846780726677	Canonical user ID b0e9f4d1012b389c1cdc22f0c9e1afbd590277892a2de49b89640d2005e1f1a5

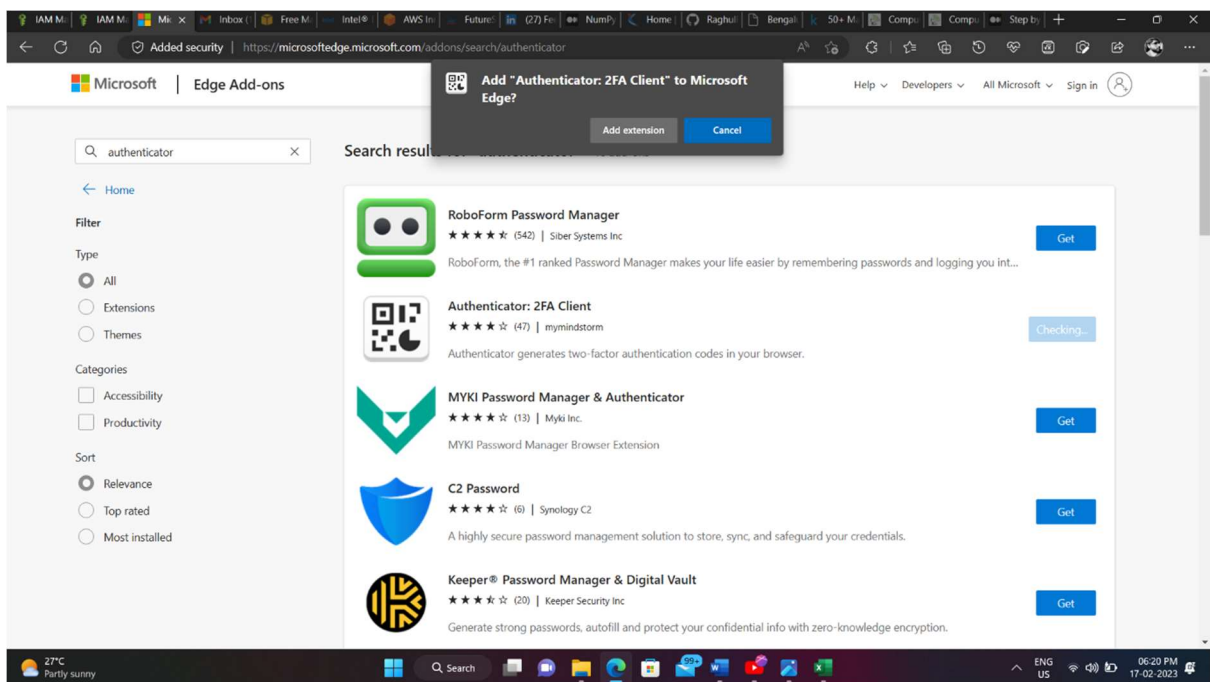
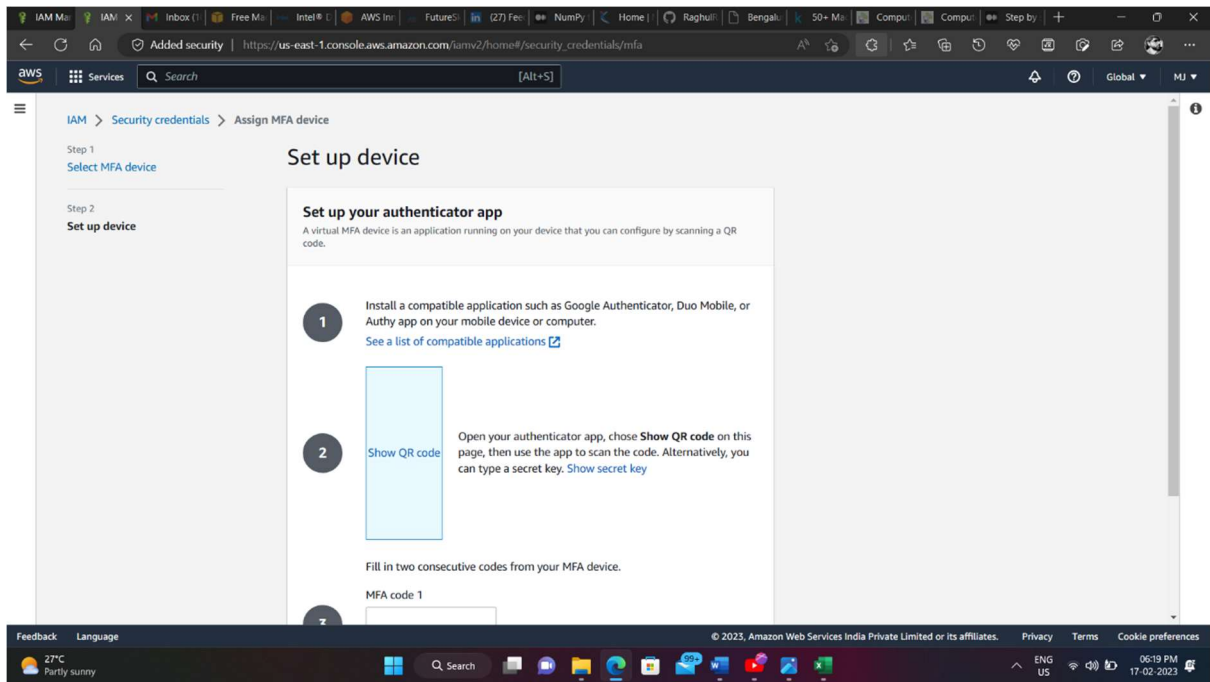
### Multi-factor authentication (MFA) (0)

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](#)

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

27°C Partly sunny





Microsoft | Edge Add-ons

Search results for "authenticator"

Filter

Type

- All
- Extensions
- Themes

Categories

- Accessibility
- Productivity

Sort

- Relevance
- Top rated
- Most installed

RoboForm Password Manager

★★★★★ (542) | Siber Systems Inc

RoboForm, the #1 ranked Password Manager makes your life easier by remembering passwords and logging you into...

Authenticator: 2FA Client

★★★★★ (47) | mymindstorm

Authenticator generates two-factor authentication codes in your browser.

MYKI Password Manager & Authenticator

★★★★★ (13) | Myki Inc.

MYKI Password Manager Browser Extension

C2 Password

★★★★★ (6) | Synology C2

A highly secure password management solution to store, sync, and safeguard your credentials.

Keeper® Password Manager & Digital Vault

★★★★★ (20) | Keeper Security Inc

Generate strong passwords, autofill and protect your confidential info with zero-knowledge encryption.

Authenticator: 2FA Client has been added to Microsoft Edge

Use this extension by selecting this icon.

- Manage your extensions by clicking Settings and more > Extensions.

See more

27°C Partly sunny

aws | Services | Search

Set up your authenticator app

A virtual MFA device is an application running on your device that you use to generate a code.

- 1 Install a compatible application such as Google Authenticator on your mobile device or computer. See a list of compatible applications
- 2 Show QR code
- 3 Fill in two consecutive codes from your MFA device.

MFA code 1

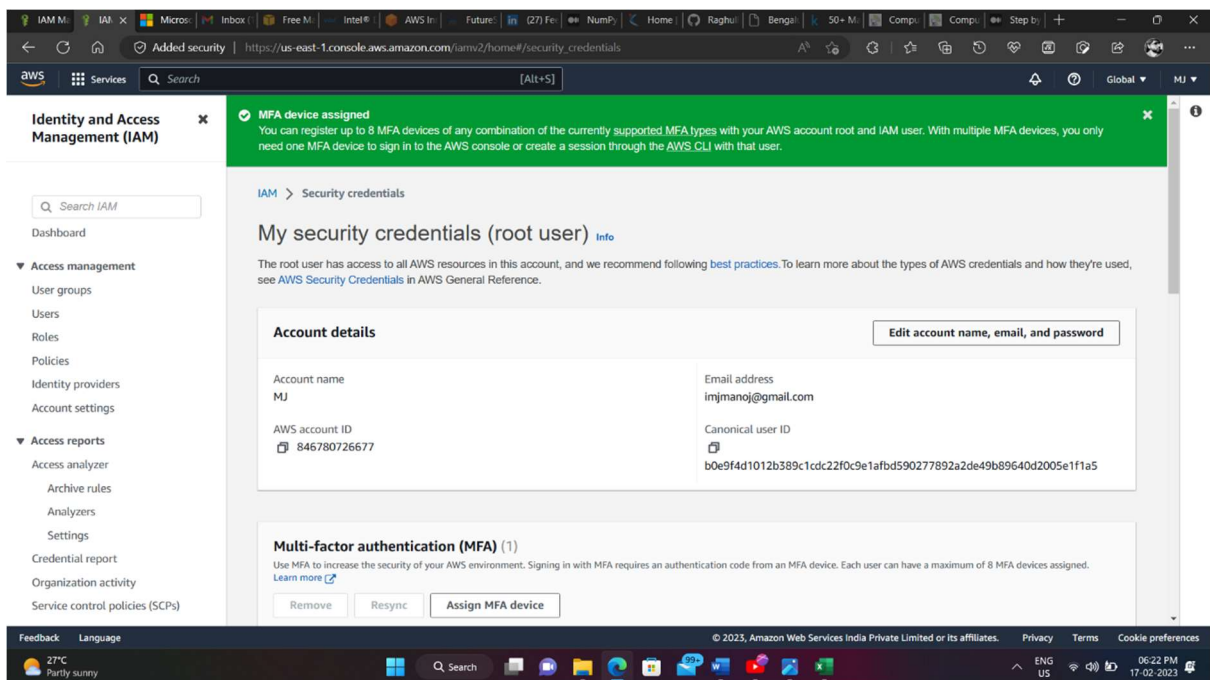
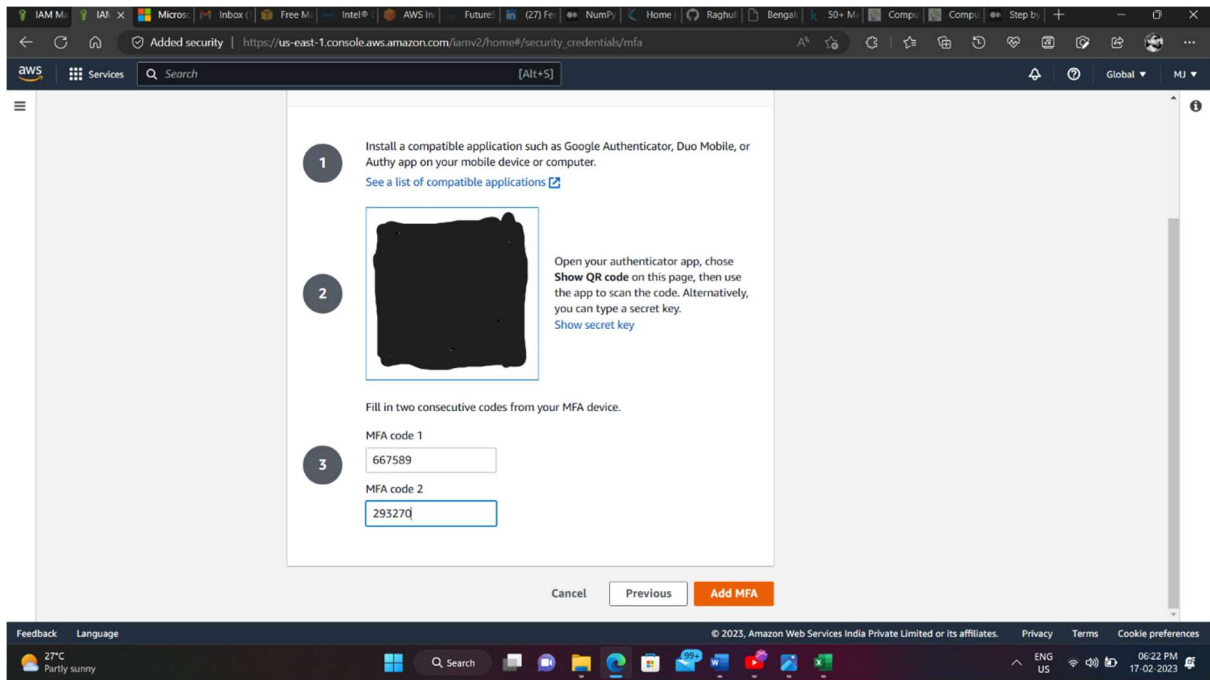
MFA code 2

Authenticator

No accounts to display. Add your first account now. [Learn more](#)

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

27°C Partly sunny





Am: X

Microso

Inbox (1)

Free Ma

Intel® I

AWS In

FutureS

(27) Fe

NumPy

Home |

Raghu

Bengal

50+ Ma

Compu

Compu

Step by

+

Added security | https://signin.aws.amazon.com/signin?redirect\_uri=https%3A%2F%2Fconsole.aws.amazon.com%2Fconso...

aws

Root user sign in

Email: imjmanoj@gmail.com

Password

Forgot password?

Sign in


Sign in to a different account

Create a new AWS account

AWS Training and Certification

Propel your career. Get AWS certified

LEARN MORE

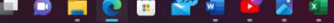


© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

English

27°C  
Partly sunny

Q Search



ENG  
US

06:23 PM  
17-02-2023

Am: X

Microso

Inbox (1)

Free Ma

Intel® I

AWS In

FutureS

(27) Fe

NumPy

Home |

Raghu

Bengal

50+ Ma

Compu

Compu

Step by

+

Added security | https://signin.aws.amazon.com/signin?redirect\_uri=https%3A%2F%2Fconsole.aws.amazon.com%2Fconso...

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: imjmanoj@gmail.com

MFA code

134332

Submit


Troubleshoot MFA

Cancel

AWS Training and Certification

Propel your career. Get AWS certified

LEARN MORE




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

English

27°C  
Partly sunny

Q Search



ENG  
US

06:23 PM  
17-02-2023