

# PROJECT 9: WORKING WITH IAM

## Task 1: Creating a user 'Aranabb' without permission-IAM password policy check

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with options like Dashboard, Access management, Groups, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, and Credential report. The main content area is titled 'Summary' for the user 'Aranabb'. It displays the User ARN as 'arn:aws:iam::477487505631:user/Aranabb', Path as '/', and Creation time as '2020-10-23 16:29 UTC+0530'. Below this, there are tabs for Permissions, Groups, Tags, Security credentials, and Access Advisor. The 'Permissions' tab is active, showing 'Permissions policies (1 policy applied)'. A table lists the attached policies: 'IAMUserChangePassword' (AWS managed policy) and 'Permissions boundary (not set)'. There are buttons for 'Add permissions' and 'Add inline policy'.



You must change your password to continue

AWS account 477487505631

IAM user name Aranabb

Old password .....

New password .....

Retype new password .....

Confirm password change

Sign in using root user email

English

Terms of Use Privacy Policy © 1996-2020, Amazon Web Services, Inc. or its affiliates.

The screenshot shows the AWS Management Console with the 'New EC2 Experience' toggle. A blue banner at the top says 'Welcome to the new EC2 console! We're redesigning the EC2 console to make it easier to use and improve performance. We'll release new screens periodically. We encourage you to try them and let us know when can make improvements. To switch between the old console and the new console, use the New EC2 Experience toggle.' Below this is the 'Resources' section, which lists various Amazon EC2 resources in the Asia Pacific (Mumbai) Region. Each resource has a yellow 'API Error' icon next to it. The resources listed are: Instances, Dedicated Hosts, Volumes, Security groups, Load balancers, Elastic IPs, Snapshots, Key pairs, Placement groups, and Running instances. On the right side, there is a section for 'Account attributes' with links to 'Supported platforms', 'Default VPC', 'Settings', 'EBS encryption', 'Zones', 'Default credit specification', and 'Console experiments'.

## Task 2: Creating a user 'Mahan' without IAM password policy and permission

The screenshot shows the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' menu is visible, with 'Users' selected. The main content area displays the 'Summary' page for user 'Mahan'. The user's ARN is 'arn:aws:iam::477487505631:user/Mahan', the path is '/', and the creation time is '2020-10-23 16:47 UTC+0530'. The 'Permissions' tab is active, showing a message: 'Get started with permissions. This user doesn't have any permissions yet. Get started by adding the user to a group, copying permissions from another user, or attaching a policy directly. Learn more'. There is an 'Add permissions' button and a link to 'Add inline policy'. Below this, it states 'Permissions boundary (not set)'.

The screenshot shows the AWS S3 console interface. On the left, the 'Amazon S3' menu is visible, with 'Buckets' selected. The main content area displays a message: 'We've temporarily re-enabled the previous version of the S3 console while we continue to improve the new S3 console experience. Switch to the new console.' Below this, the 'S3 buckets' section is shown. A search bar is present, and there are buttons for 'Create bucket', 'Edit public access settings', 'Empty', and 'Delete'. A red error banner is displayed with the message 'Error: Access Denied'. Below the error banner, there is a table with columns for 'Bucket name', 'Access', 'Region', and 'Date created'. The table is currently empty.

## Task 3: Create a user 'Ravi' with S3 full access

The screenshot shows the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' menu is visible, with 'Users' selected. The main content area displays the 'Summary' page for user 'Ravi'. The user's ARN is 'arn:aws:iam::477487505631:user/Ravi', the path is '/', and the creation time is '2020-10-23 16:56 UTC+0530'. The 'Permissions' tab is active, showing a message: 'Permissions policies (1 policy applied)'. There is an 'Add permissions' button and a link to 'Add inline policy'. Below this, a table lists the attached policies. The table has columns for 'Policy name' and 'Policy type'. The policy 'AmazonS3FullAccess' is listed as an 'AWS managed policy'. Below the table, it states 'Permissions boundary (not set)'.

aws Services

Amazon S3

Buckets

Batch Operations

Access analyzer for S3

Account settings for Block Public Access

Feature spotlight

Access S3-backed file shares on premises and reduce local storage costs using AWS Storage Gateway. [Learn more](#)

Amazon S3

While we continue to improve the new version of the S3 console, you can temporarily switch to the previous console experience for buckets. To help us improve the experience, give feedback.

Buckets (1)

Buckets are containers for data stored in S3. [Learn more](#)

Find buckets by name

Name	Region	Access	Creation date
dns555	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	October 23, 2020, 17:00 (UTC+05:30)

#### Task 4: Create a group 'HRs' with EC2 full access

aws Services

Identity and Access Management (IAM)

Dashboard

Access management

Groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

IAM > Groups > HRs

Summary

Group ARN: [arn:aws:iam::477487505631:group/HRs](#)

Users (in this group): 0

Path: /

Creation Time: 2020-10-23 17:04 UTC+0530

Users Permissions Access Advisor

Managed Policies

The following managed policies are attached to this group. You can attach up to 10 managed policies.

[Attach Policy](#)

Policy Name	Actions
<a href="#">AmazonEC2FullAccess</a>	<a href="#">Show Policy</a>   <a href="#">Detach Policy</a>   <a href="#">Simulate Policy</a>

Inline Policies

#### Task 5: Add user to a group and check if user policy and group policy is reflecting on the user

aws Services

Identity and Access Management (IAM)

Dashboard

Access management

Groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Service control policies

Users > Ravi

Summary

User ARN: [arn:aws:iam::477487505631:user/Ravi](#)

Path: /

Creation time: 2020-10-23 16:56 UTC+0530

Permissions Groups (1) Tags Security credentials Access Advisor

Permissions policies (2 policies applied)

[Add permissions](#) [Add inline pol](#)

Policy name	Policy type
Attached directly	
<a href="#">AmazonS3FullAccess</a>	AWS managed policy
Attached from group	
<a href="#">AmazonEC2FullAccess</a>	AWS managed policy from group HRs

Permissions boundary (not set)

aws Services ▾

New EC2 Experience  
Tell us what you think

EC2 Dashboard **New**

Events **New**

Tags

Limits

▼ Instances

**Instances** **New**

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts **New**

Welcome to the new instances experience!  
We're redesigning the EC2 console to make it easier to use. To switch between the old console and the new console, use the New EC2 Experience toggle above the navigation panel. We'll release updates continuously based on customer feedback.

Instances Info

Filter instances

1

Name	Instance ID	Instance state	Instance type	Status check	Alarm Status	Availability zone	Public IPv
You do not h							

Select an instance above

aws Services ▾

Amazon S3

Buckets

Batch Operations

Access analyzer for S3

Account settings for Block Public Access

Feature spotlight 3

Successfully created bucket "aws435"  
To upload files and folders, or to configure additional bucket settings choose [View details](#).

Access S3-backed file shares on premises and reduce local storage costs using AWS Storage Gateway. [Learn more](#)

Amazon S3

While we continue to improve the new version of the S3 console, you can temporarily [switch to the previous console experience](#) for buckets. To help us improve the experience, [give feedback](#).

Buckets (1)

Buckets are containers for data stored in S3. [Learn more](#)

Find buckets by name

Name	Region	Access	Creation date
aws435	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	October 23, 2020, 17:19 (UTC+05:30)

## Task 6: Copy policies from existing user

aws Services ▾

Add user

1 2 3 4 5

▼ Set permissions

Add user to group

**Copy permissions from existing user**

Attach existing policies directly

Select an existing user from which to copy policies and group membership.

Copy permissions from existing user

Showing 5 results

User name	Groups	Attached policies
<input type="radio"/> Aranabb	None	IAMUserChangePassword
<input type="radio"/> Dipa	HRs	AmazonS3FullAccess
<input type="radio"/> Hiru	HRs	None
<input type="radio"/> Mahan	None	None
<input checked="" type="radio"/> Ravi	HRs	AmazonS3FullAccess

Cancel Previous Next: Tags


## Task 7: Add user to group in the process of creating a user


aws Services ▾


add user

1 2 3 4 5

▼ Set permissions

 Add user to group

 Copy permissions from existing user

 Attach existing policies directly

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](#)

Add user to group

Create group Refresh

Search Showing 1 result

Group ▾	Attached policies
✓ HRS	AmazonEC2FullAccess

aws Services ▾

Identity and Access Management (IAM)

Dashboard

▼ Access management

Groups

**Users**

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Users > Sachin

Summary Delete user

User ARN `arn:aws:iam::477487505631:user/Sachin`

Path /

Creation time 2020-10-23 17:37 UTC+0530

Permissions Groups (1) Tags Security credentials Access Advisor

▼ Permissions policies (1 policy applied)

Add permissions Add inline poli

Policy name ▾	Policy type ▾
Attached from group	
▶ AmazonEC2FullAccess	AWS managed policy from group HRS

▶ Permissions boundary (not set)

## Task 8: Setting Password Policy

aws Services ▾

Set password policy

A password policy is a set of rules that define complexity requirements and mandatory rotation periods for your IAM users' passwords. [Learn more](#)

Select your account password policy requirements:

☒ Enforce minimum password length

characters

☒ Require at least one uppercase letter from Latin alphabet (A-Z)

☒ Require at least one lowercase letter from Latin alphabet (a-z)

☒ Require at least one number

☒ Require at least one non-alphanumeric character (!@#\$%^&\*()\_+ = []{}|'')

☒ Enable password expiration

Expire passwords in  day(s)

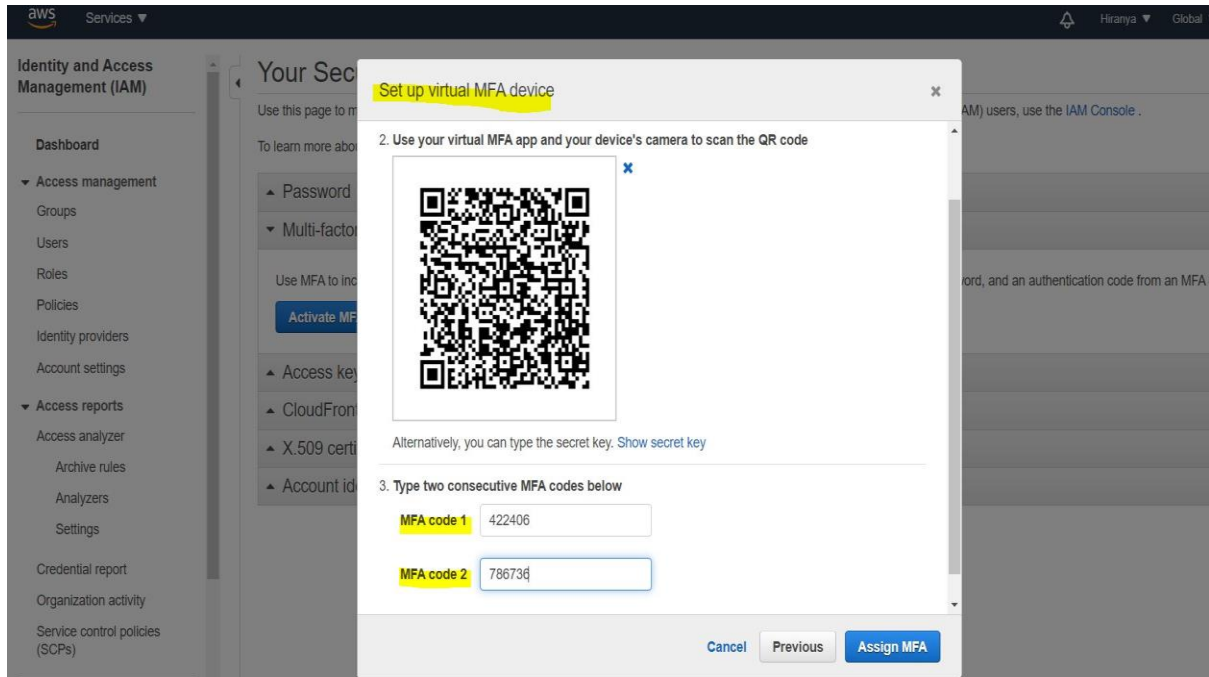
☒ Password expiration requires administrator reset

☒ Allow users to change their own password

☐ Prevent password reuse

Cancel Save changes

## Task 9: Enabling MFA and using a MFA device



### 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: hbhuyan09@gmail.com

MFA code

818213

Submit

[Troubleshoot MFA](#)

[Cancel](#)

## Build Mobile and Web Apps Fast

Add authentication and data syncing with AWS Amplify in just a few lines of code

[LEARN MORE](#)

