

Project 2: IAM

Task 1: Creating users without permissions-IAM password policy check.

Ss1: user summary with all tab information

The screenshot displays the AWS IAM Management Console interface. The left-hand navigation pane is expanded to show the 'Users' section under 'Identity and Access Management (IAM)'. The main content area is titled 'Summary' and shows details for a user named 'AWS-Test'. The user's ARN is 'arn:aws:iam::618639665310:user/AWS-Test', the path is '/', and the creation time is '2020-10-23 17:34 UTC+0530'. Below this, the 'Permissions' tab is selected, showing 'Permissions policies (1 policy applied)'. A table lists the policy 'IAMUserChangePassword' as an 'AWS managed policy'. The 'Access Advisor' tab is also visible. The bottom of the screen shows the Windows taskbar with various application icons and the system clock indicating 17:48 on 23/10/2020.

Task 2: Creating users without the IAM password policy.

Ss2: user summary with all tab information

This screenshot is identical to the one above, showing the AWS IAM Management Console 'Summary' page for the user 'AWS-Test'. It displays the same user details (ARN, path, creation time) and the 'Permissions' tab with the 'IAMUserChangePassword' policy. The interface elements, including the navigation pane and the Windows taskbar at the bottom, are consistent with the previous image.

Task 3: Create a user with S3 full access.

Ss3: User summary

The screenshot shows the AWS IAM Management Console interface. The left sidebar contains the navigation menu with sections like Dashboard, Access management, Access reports, and Credential report. The main content area is titled 'Summary' and displays details for a user named 'AWS-Test'. The user's ARN is 'arn:aws:iam::618639665310:user/AWS-Test', the path is '/', and the creation time is '2020-09-29 17:01 UTC+0530'. The 'Permissions' tab is selected, showing 'Permissions policies (2 policies applied)'. A table lists the attached policies: 'AmazonS3FullAccess' and 'IAMUserChangePassword', both are AWS managed policies. There is also a 'Permissions boundary (not set)' section.

Policy name	Policy type
AmazonS3FullAccess	AWS managed policy
IAMUserChangePassword	AWS managed policy

Task4: Create a group with ec2 full access.

Ss4: group summary

The screenshot shows the AWS IAM Management Console interface. The left sidebar contains the navigation menu. The main content area is titled 'Summary' and displays details for a group named 'developer'. The group's ARN is 'arn:aws:iam::618639665310:group/developer', the path is '/', and the creation time is '2020-10-23 18:17 UTC+0530'. The 'Permissions' tab is selected, showing 'Managed Policies'. A table lists the attached policy: 'AmazonEC2FullAccess'. Below the table, there are links to 'Show Policy', 'Detach Policy', and 'Simulate Policy'.

Policy Name	Actions
AmazonEC2FullAccess	Show Policy Detach Policy Simulate Policy

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

Ss5: user summary with permissions

The screenshot shows the AWS IAM console interface. The left sidebar contains the 'Identity and Access Management (IAM)' 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 displays the 'Permissions' tab for the user 'AWS-Admin'. It shows the User ARN as 'arn:aws:iam::618639665310:user/AWS-Admin', Path as '/', and Creation time as '2020-09-29 17:01 UTC+0530'. Below this, there are tabs for 'Permissions', 'Groups (1)', 'Tags', 'Security credentials', and 'Access Advisor'. The 'Permissions' tab is active, showing 'Permissions policies (2 policies applied)'. There are two buttons: 'Add permissions' and 'Add inline policy'. A table lists the attached policies:

Policy name	Policy type
Attached directly	
IAMUserChangePassword	AWS managed policy
Attached from group	
AmazonEC2FullAccess	AWS managed policy from group developer
Permissions boundary (not set)	

Ss6: login as this user show that this policy is in effect

The screenshot shows the AWS IAM console interface. The left sidebar is the same as in the previous screenshot. The main content area displays the 'Users' tab. At the top, there is a red error message box that says: 'You need permissions. You do not have the permission required to perform this operation. Ask your administrator to add permissions. Learn more'. Below the error message, there are buttons for 'Add user' and 'Delete user'. A search bar is present with the text 'Find users by username or access key'. Below the search bar, there is a table with columns: 'User name', 'Groups', 'Access key age', 'Password age', 'Last activity', and 'MFA'. The table is currently empty, showing 'Showing 0 results'.

Task 6: Copy policies from the existing user.

Ss7: attach user summary of the user from which you create a new user.

The screenshot shows the AWS IAM Management Console. The left sidebar contains the 'Identity and Access Management (IAM)' 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' and shows details for a user with the ARN 'arn:aws:iam::618639665310:user/AWS-Test'. The user's path is '/' and creation time is '2020-09-29 17:01 UTC+0530'. Below this, the 'Permissions' tab is selected, showing 'Permissions policies (3 policies applied)'. A table lists the attached policies:

Policy name	Policy type
AmazonS3FullAccess	AWS managed policy
AdministratorAccess	AWS managed policy
IAMUserChangePassword	AWS managed policy

Ss8: login as this user show that this policy is in effect.

The screenshot shows the AWS S3 Management Console. The left sidebar contains the 'Amazon S3' menu with options like Buckets, Batch operations, Access analyzer for S3, Block public access (account settings), and Feature spotlight. The main content area shows a notification about the S3 console experience. Below this, the 'S3 buckets' section is displayed, showing a search bar and a table of buckets:

Bucket name	Access	Region	Date created
elasticbeanstalk-ap-south-1-618639665310	Objects can be public	Asia Pacific (Mumbai)	Sep 22, 2020 5:50:07 PM GMT+0530

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

The screenshot shows the AWS IAM Management Console interface. The top navigation bar includes the AWS logo, 'Services', and user information (pankubhole78@gmail.com). The main content area is titled 'Set user details' and includes a 'User name' field with the value 'test' and a link to 'Add another user'. Below this is the 'Select AWS access type' section, which has two checked options: 'Programmatic access' and 'AWS Management Console access'. The 'Console password' section has 'Custom password' selected. At the bottom of this section are 'Cancel' and 'Next: Permissions' buttons.

The second screenshot shows the 'Review' step. It displays a summary of the user details: 'User name' is 'Test', 'AWS access type' is 'Programmatic access and AWS Management Console access', 'Console password type' is 'Custom', 'Require password reset' is 'Yes', and 'Permissions boundary' is 'Permissions boundary is not set'. Below this is a 'Permissions summary' section showing that the user will be added to the 'Testing' group. At the bottom of this section are 'Cancel', 'Previous', and 'Create user' buttons.

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* test [Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type*

- ☒ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- ☒ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password*

- ☐ Autogenerated password
- ☒ Custom password

* Required [Cancel](#) [Next: Permissions](#)

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	Test
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	Testing

[Cancel](#) [Previous](#) [Create user](#)

Task8: setting a password policy

Ss9: password policy screen

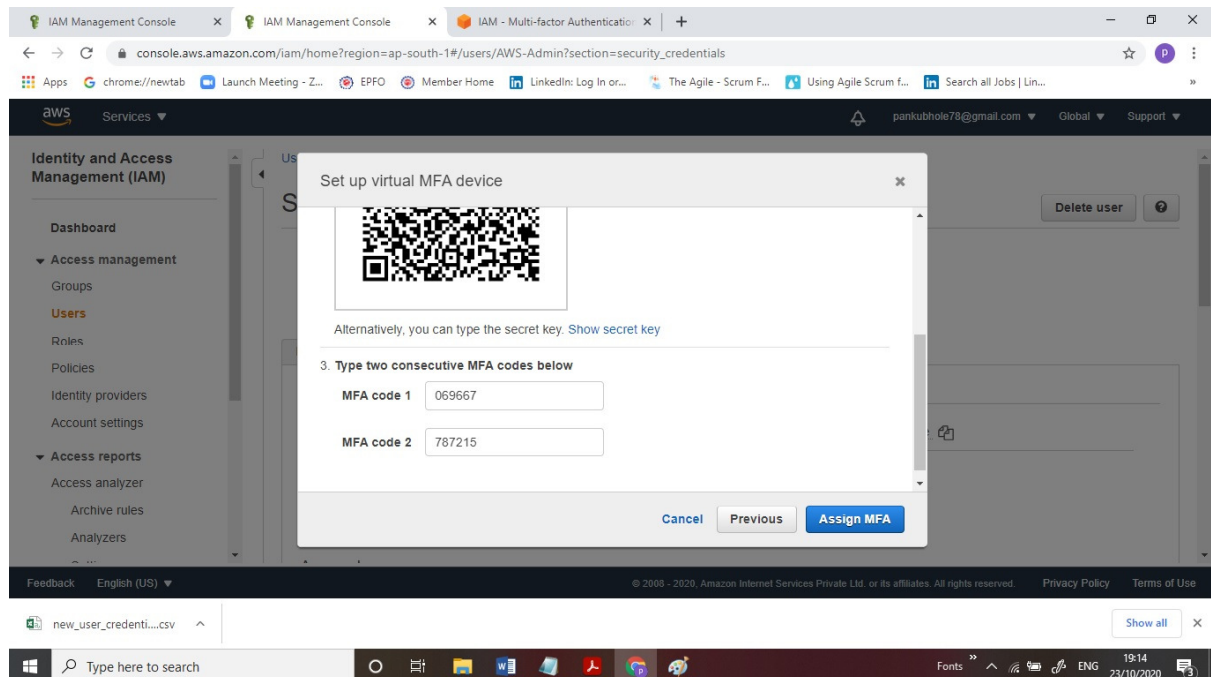
The screenshot shows the 'Modify password policy' page in the AWS IAM console. The page title is 'Modify password policy'. Below the title, there is a brief explanation: 'A password policy is a set of rules that define complexity requirements and mandatory rotation periods for your IAM users' passwords. [Learn more](#)'. The main section is 'Select your account password policy requirements:'. It contains several checkboxes and input fields: 'Enforce minimum password length' (checked) with a value of '6' characters; 'Require at least one uppercase letter from Latin alphabet (A-Z)' (unchecked); 'Require at least one lowercase letter from Latin alphabet (a-z)' (unchecked); 'Require at least one number' (unchecked); 'Require at least one non-alphanumeric character (!@#\$%^&*()_+-=[]{}|)'' (unchecked); 'Enable password expiration' (checked) with an expiration period of '90' day(s); and 'Password expiration requires administrator reset' (unchecked). At the bottom right of the form are 'Cancel' and 'Save changes' buttons. The footer of the console shows 'Feedback', 'English (US)', and copyright information for 2008-2020 Amazon Internet Services Private Ltd. or its affiliates. The browser's taskbar at the bottom shows various application icons and the system clock at 19:00 on 23/10/2020.

Ss10: login as the user and show password incompatibility error

The screenshot shows the 'Sign in as IAM user' page in the AWS IAM console. The page title is 'Sign in as IAM user'. Below the title, there is a message: 'Your authentication information is incorrect. Please try again.' The form contains three input fields: 'Account ID (12 digits) or account alias' with the value '610639665310'; 'IAM user name' with the value 'Test'; and 'Password' (empty). Below the password field is a blue 'Sign in' button. At the bottom left of the form are links for 'Sign in using root user email' and 'Forgot password?'. On the right side of the page is a large promotional banner for 'AWS Storage Day Virtual Event' with the text 'Join us on November 10th to learn what's new across the AWS Storage portfolio' and a 'REGISTER NOW' button. The footer of the console shows 'Feedback', 'English (US)', and copyright information for 2008-2020 Amazon Internet Services Private Ltd. or its affiliates. The browser's taskbar at the bottom shows various application icons and the system clock at 19:00 on 23/10/2020.

Task 9: Enabling MFA and using an MFA device

Ss11: enable MFA



Ss12: login screen for MFA

