



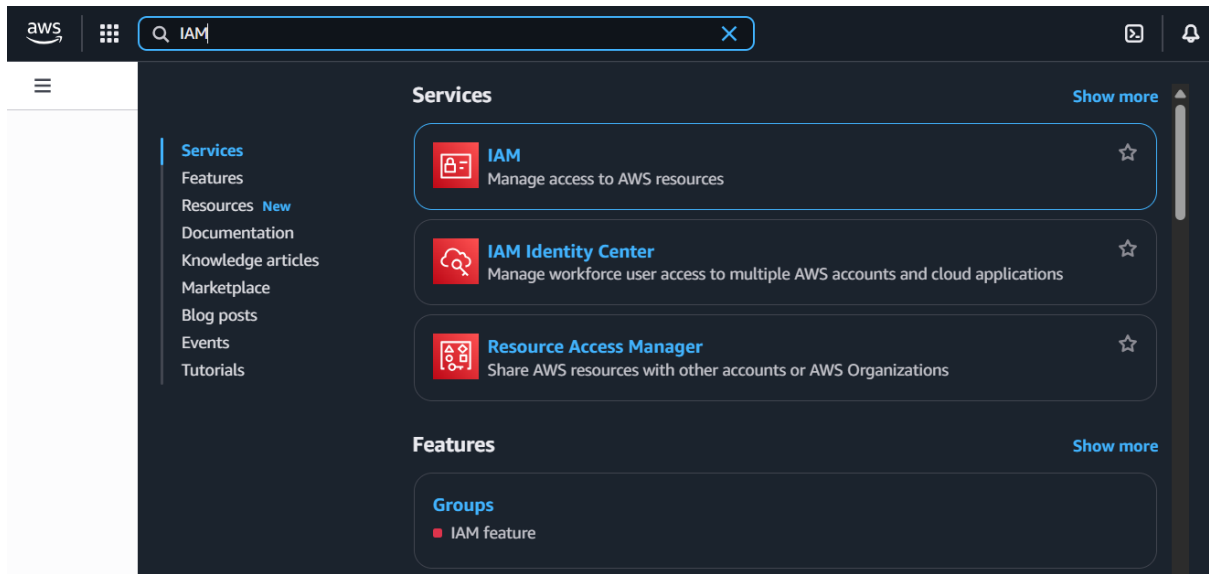
Day 19

“CLOUD SECURITY”

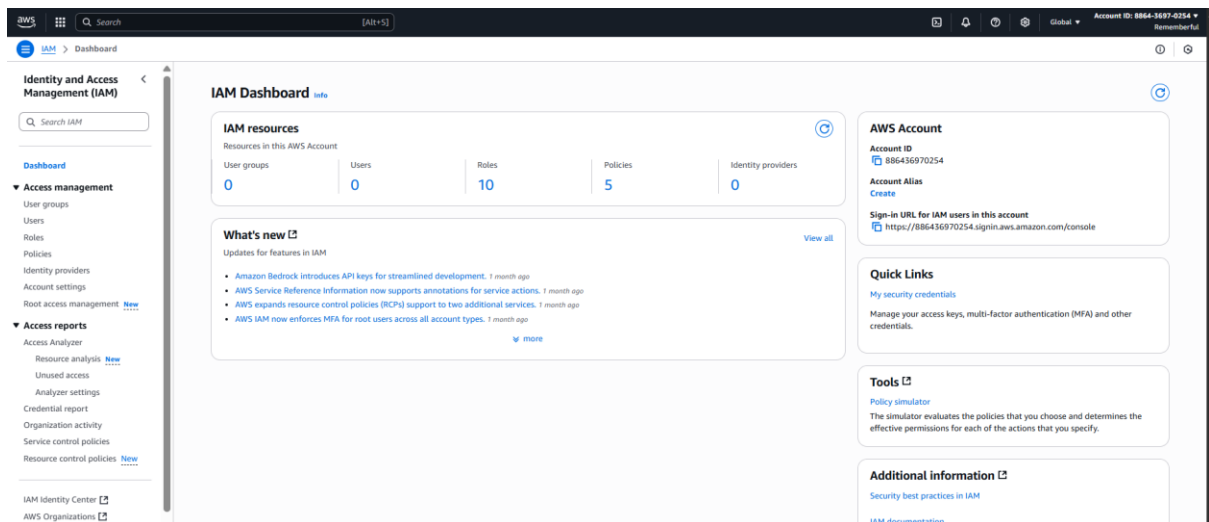
Implementing AWS IAM:

Steps:

Open the AWS console, and search for IAM in the Search bar of AWS:



Click on it to open, following screen will appear:



On the dashboard of your left, click on the “User Groups”:

Identity and Access Management (IAM)

 Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

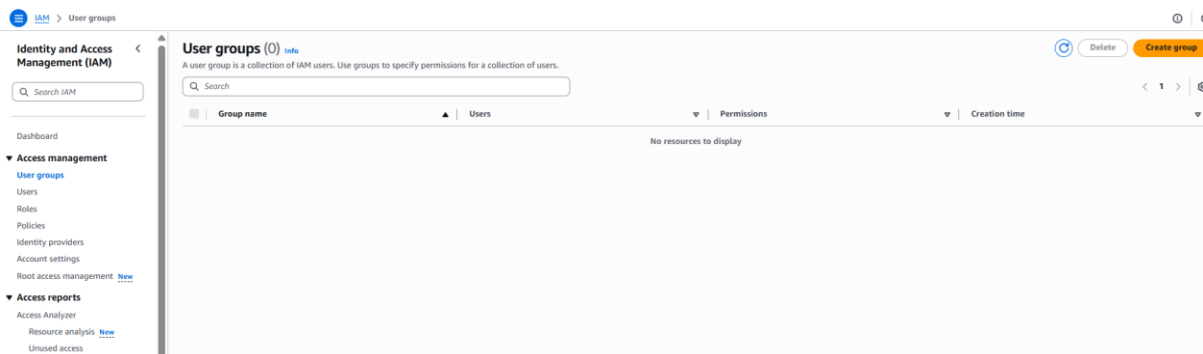
Policies

Identity providers

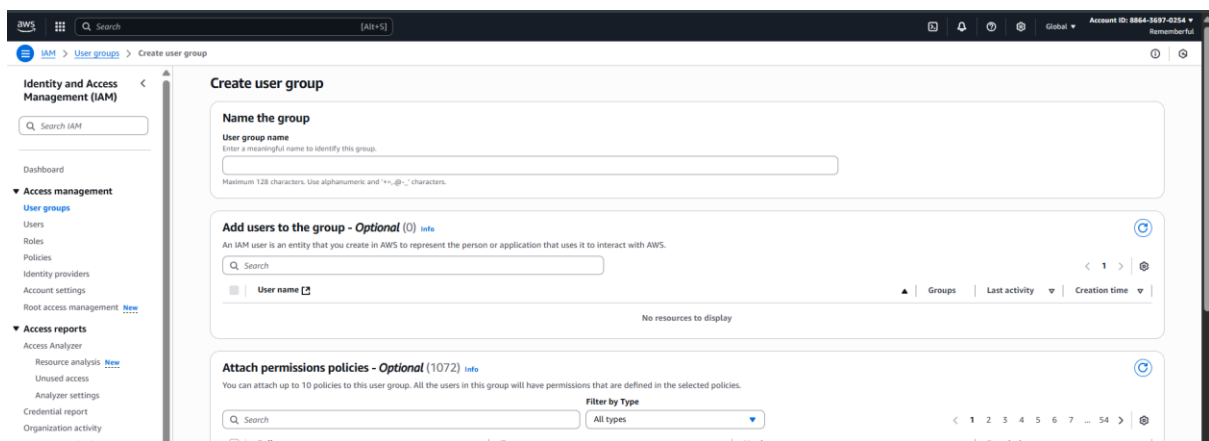
Account settings

Root access management [New](#)

Following screen will appear:



Now, to create the group, click on the “Create group” button: following screen will appear.



Fill it as per the need:

The screenshot shows the 'Create user group' page in the AWS IAM console. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and IAM Identity Center. The main content area is titled 'Create user group' and includes three sections: 'Name the group' with a 'User group name' field containing 'Training_group'; 'Add users to the group - Optional (0)' with a search bar and a table showing no resources; and 'Attach permissions policies - Optional (1/1072)' with a search bar and a table of policies. The table lists 'IAMUserChangePassword' and 'IAMUserSSHKeys' as 'AWS managed' policies. At the bottom right, there are 'Cancel' and 'Create user group' buttons.

Then click on the “orange” button at the bottom, the group will be created:

The screenshot shows the 'User groups' page in the AWS IAM console. A green banner at the top states 'Training_group user group created.' with a 'View group' button. Below the banner, the 'User groups (1)' section shows a table with one entry: 'Training_group'. The table columns are 'Group name', 'Users', 'Permissions', and 'Creation time'. The 'Training_group' row shows 'Defined' permissions and 'Now' creation time. At the bottom right, there are 'Delete' and 'Create group' buttons.

Now, click on the “users” from the dashboard at left: following screen will appear.

The screenshot shows the 'Users' page in the AWS IAM console. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and IAM Identity Center. The main content area is titled 'Users (0)' and includes a search bar and a table with columns: 'User name', 'Path', 'Group', 'Last activity', 'MFA', 'Password age', 'Console last sign-in', 'Access key ID', 'Active key age', and 'Access key last use'. The table shows no resources. At the bottom right, there are 'Delete' and 'Create user' buttons.

Click on the “create user” button: following screen will appear.

The screenshot shows the 'Create user' page in the AWS IAM console. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and IAM Identity Center. The main content area is titled 'Specify user details' and includes a 'User details' section with a 'User name' field. Below the field, there is a checkbox for 'Provide user access to the AWS Management Console - optional'. At the bottom right, there are 'Cancel' and 'Next' buttons.

Fill that form accordingly:

User details

User name
Alice

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +, -, @, _ (hyphen).

☒ **Provide user access to the AWS Management Console - optional**
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

Are you providing console access to a person?

User type
☐ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
☒ **I want to create an IAM user**
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password
☐ Autogenerated password
You can view the password after you create the user.
☒ **Custom password**
Enter a custom password for this user:
 xxxxxxxxxxxx
 • Must be at least 8 characters long
 • Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % & * () _ + - { } | ~ [] ' "
☐ Show password

☒ **Users must create a new password at next sign-in - Recommended**
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

Next

Click on the “Next” button: following screen will appear.

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.

User groups (1)

Search

Group name	Users	Attached policies	Created
<input checked="" type="checkbox"/> Training_group	0	DatabaseAdministrator and IAMUserChg...	2025-08-09 (4 minutes ago)

Set permissions boundary - optional

Next

Select the group:

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.

User groups (1/1)

Search

Group name	Users	Attached policies	Created
<input checked="" type="checkbox"/> Training_group	0	DatabaseAdministrator and IAMUserChg...	2025-08-09 (4 minutes ago)

Set 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](#)

☐ Use a permissions boundary to control the maximum permissions
You can select one of the existing permissions policies to define the boundary.

Next

Click on “Next” button: following screen will appear.

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 Alice	Console password type Custom password	Require password reset Yes
--------------------	--	-------------------------------

Permissions summary

Name	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy
Training_group	Group	Permissions group

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](#)

Fill it accordingly:

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 Alice	Console password type Custom password	Require password reset Yes
--------------------	--	-------------------------------

Permissions summary

Name	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy
Training_group	Group	Permissions group

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.

Key	Value - optional	
Department	Training	Remove

[Add new tag](#)
You can add up to 49 more tags.

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

Click on the “create user” button: following confirmation will occur.

User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console. [View user](#)

Retrieve password
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

[Email sign-in instructions](#)

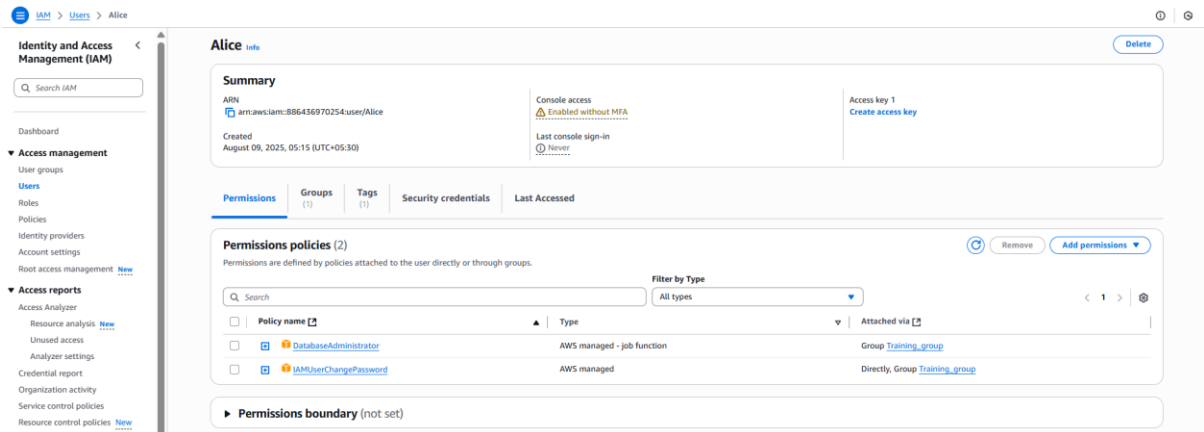
Console sign-in URL
<https://886436970254.signin.aws.amazon.com/console>

User name
Alice

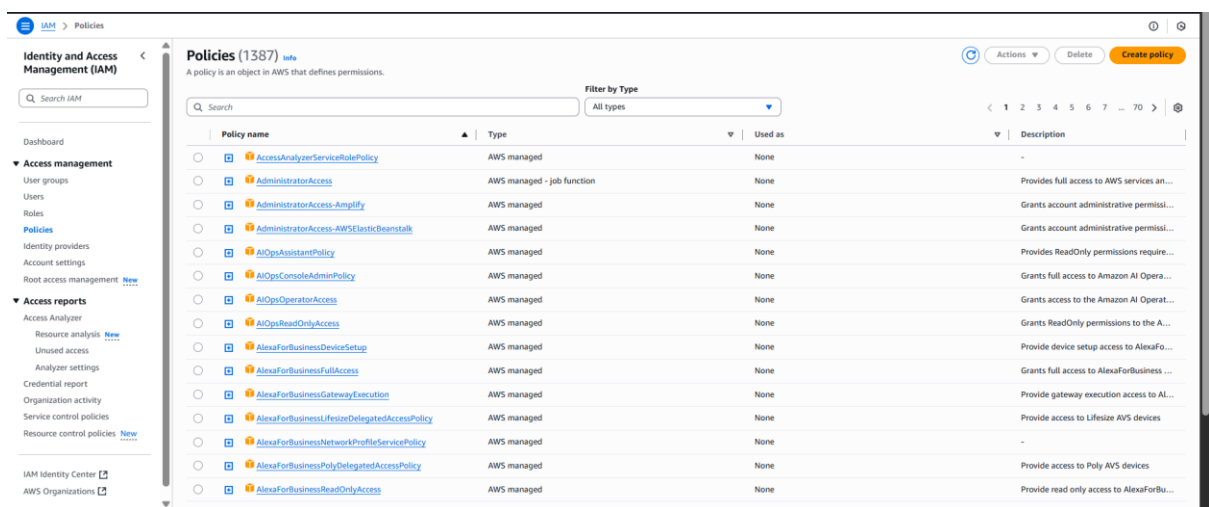
Console password
XXXXXXXXXX [Show](#)

[Cancel](#) [Download .csv file](#) [Return to users list](#)

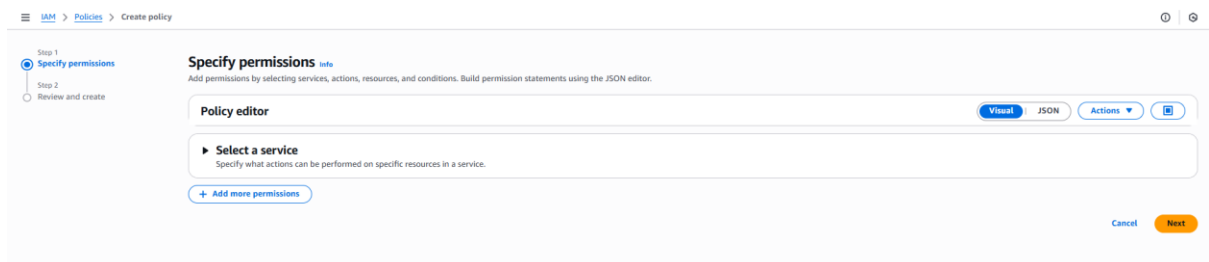
Next attach a policy to the user. Select the user to which you want to attach policy to: click on the “Alice”



Now, to create policies by ourselves, click on the “policies” at the left dashboard: following screen will appear.



Click on the “Create Policy” button: following screen will appear.



Click on the “Select a service” section: and select the service.

Step 1 **Specify permissions**
Step 2 Review and create

Specify permissions info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor Visual JSON Actions

▼ **Select a service**
Specify what actions can be performed on specific resources in a service.

Service
Choose a service
Filter services

Commonly used services

- Auto Scaling
- CloudFront
- EC2
- IAM
- Lambda
- RDS
- S3
- SNS

Other services

- Access Analyzer
- Account
- Articulate

Cancel **Next**

Then under the “Action allowed” select as needed:

Step 1 **Specify permissions**
Step 2 Review and create

Specify permissions info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor Visual JSON Actions

▼ **CloudFront** 41 Actions

Specify what actions can be performed on specific resources in [CloudFront](#).

▼ **Actions allowed**
Specify actions from the service to be allowed.
Filter Actions

Manual actions | [Add actions](#)
☐ All CloudFront actions (cloudfront:*)

Access level
► **List (37)**

▼ **Read (Selected 41/41)**

☒ All read actions

<input checked="" type="checkbox"/> DescribeFunction <small>info</small>	<input checked="" type="checkbox"/> DescribeKeyValueStore <small>info</small>	<input checked="" type="checkbox"/> GetAnycastIpList <small>info</small>
<input checked="" type="checkbox"/> GetCachePolicy <small>info</small>	<input checked="" type="checkbox"/> GetCachePolicyConfig <small>info</small>	<input checked="" type="checkbox"/> GetCloudFrontOriginAccessIdentity <small>info</small>
<input checked="" type="checkbox"/> GetCloudFrontOriginAccessIdentityConfig <small>info</small>	<input checked="" type="checkbox"/> GetConnectionGroup <small>info</small>	<input checked="" type="checkbox"/> GetConnectionGroupByRoutingEndpoint <small>info</small>
<input checked="" type="checkbox"/> GetContinuousDeploymentPolicy <small>info</small>	<input checked="" type="checkbox"/> GetContinuousDeploymentPolicyConfig <small>info</small>	<input checked="" type="checkbox"/> GetDistribution <small>info</small>
<input checked="" type="checkbox"/> GetDistributionConfig <small>info</small>	<input checked="" type="checkbox"/> GetDistributionTenant <small>info</small>	<input checked="" type="checkbox"/> GetDistributionTenantByDomain <small>info</small>
<input checked="" type="checkbox"/> GetFieldLevelEncryption <small>info</small>	<input checked="" type="checkbox"/> GetFieldLevelEncryptionConfig <small>info</small>	<input checked="" type="checkbox"/> GetFieldLevelEncryptionProfile <small>info</small>
<input checked="" type="checkbox"/> GetFieldLevelEncryptionProfileConfig <small>info</small>	<input checked="" type="checkbox"/> GetFunction <small>info</small>	<input checked="" type="checkbox"/> GetInvalidation <small>info</small>

Effect
☒ Allow ☐ Deny

[Expand all](#) | [Collapse all](#)

As per the requirement, Decide the “Resources” and “Request conditions - optional”.

▼ **Resources**
Specify resource ARNs for these actions.
☒ All
☐ Specific
⚠ The all wildcard "*" may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

▼ **Request conditions - optional**
Actions on resources are allowed or denied only when these conditions are met.

☐ **User is MFA Authenticated**
Filters access if MFA was used to validate the temporary security credentials that made the request.

☐ **Requested from IP**
Filters access by the requester's IP address.

[+ Add another condition](#)

[+ Add more permissions](#)

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Cancel **Next**

Click on the “Next” button: following screen will appear.

Review and create [info](#)

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and "+,=,_,@,-" characters.

Description - optional
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and "+,=,_,@,-" characters.

Permissions defined in this policy [info](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Allow (1 of 447 services) [Show remaining 446 services](#)

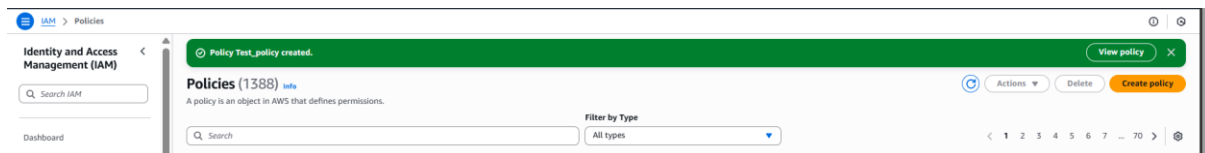
Service	Access level	Resource	Request condition
CloudFront	Full: Read	All resources	aws:MultiFactorAuthPresent Bool [true]

Add tags - optional [info](#)

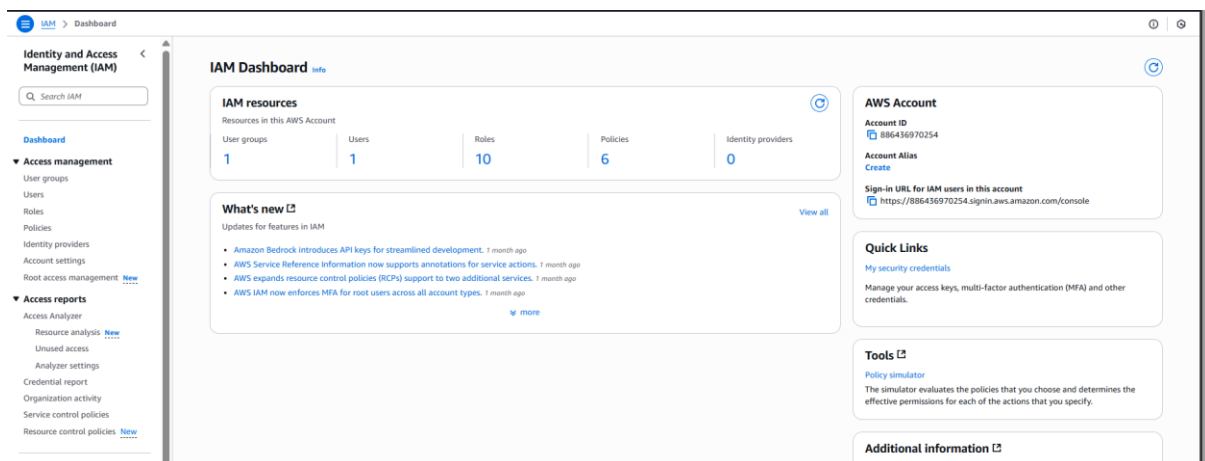
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

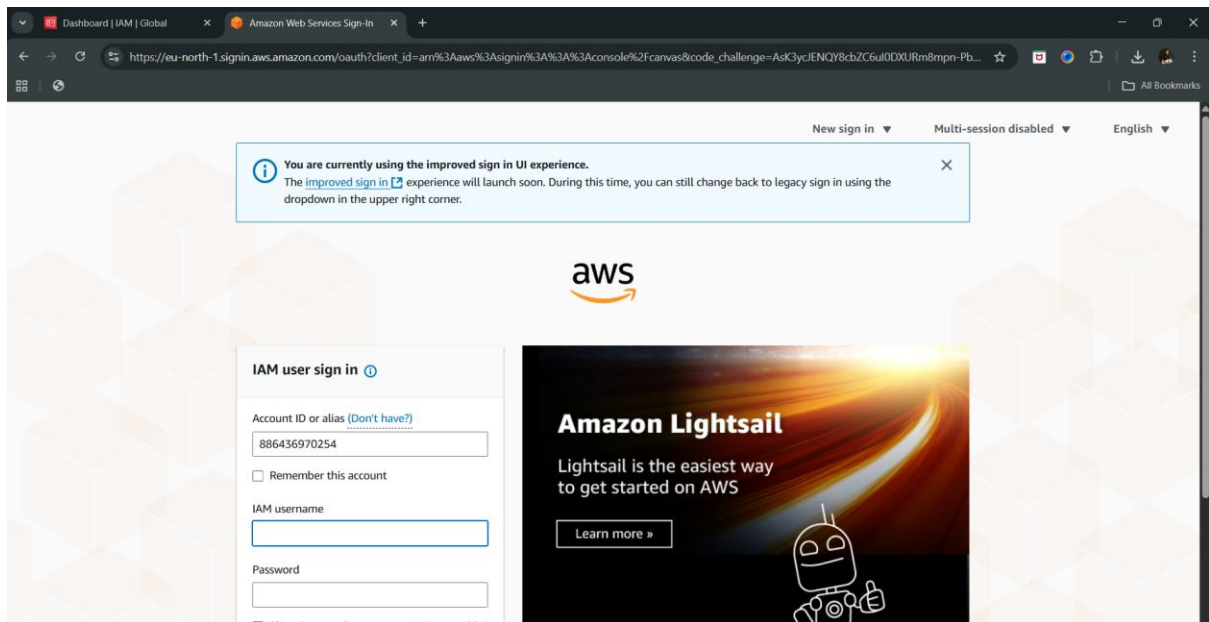
Fill it and click on the “Create Policy” button: following confirmation will appear.



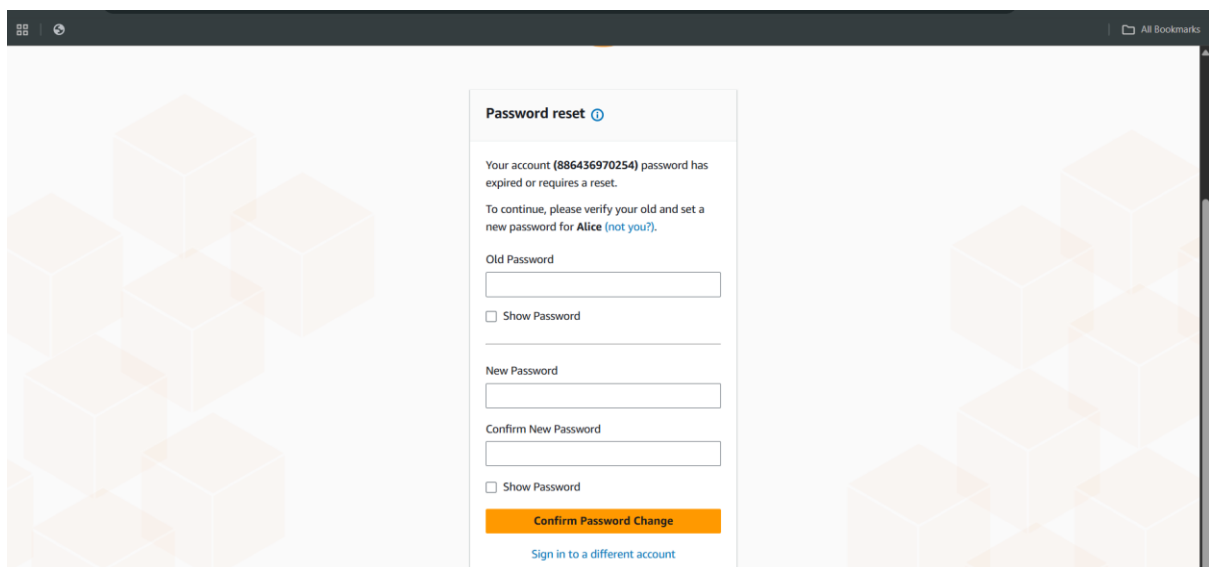
Now, to access this IAM user: click on the “dashboard” at left panel. You will be able to see a link.



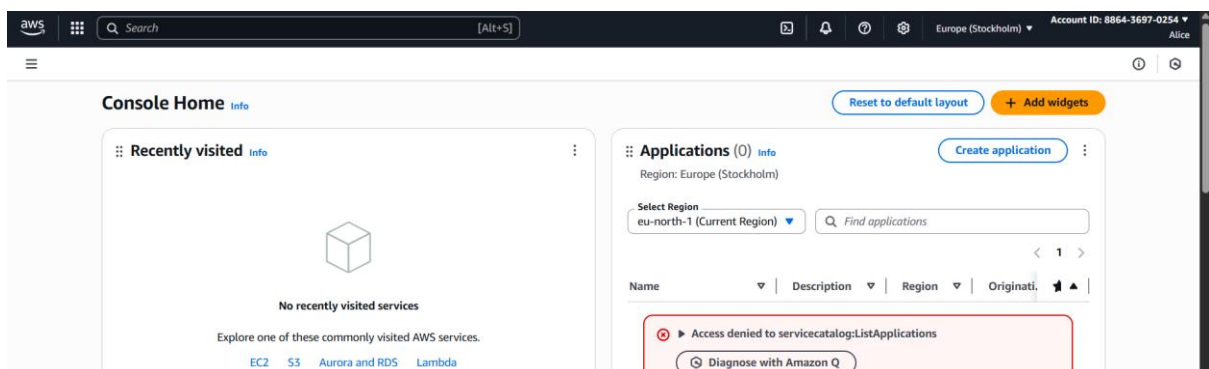
Copy and paste it in a new tab: following window appears.



Enter the credentials which we had created recently, and click on sign-in. Following screen will appear:



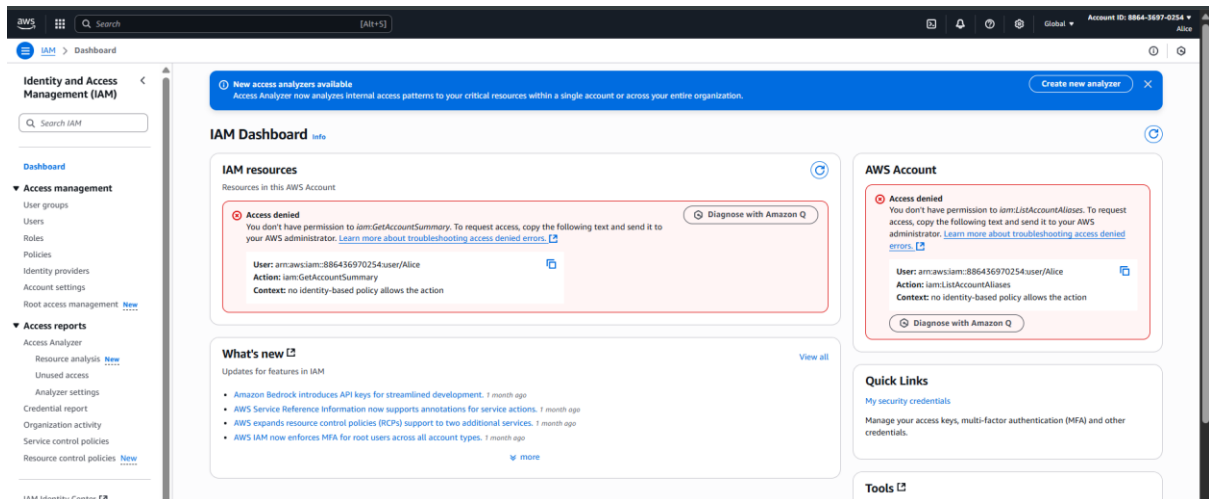
Change the password, and sign in: following screen appear.



We can also cross check:



To verify the permissions: open the IAM



Clearly, it is working as expected. Now, delete all these resources to avoid any cost.

--The End--