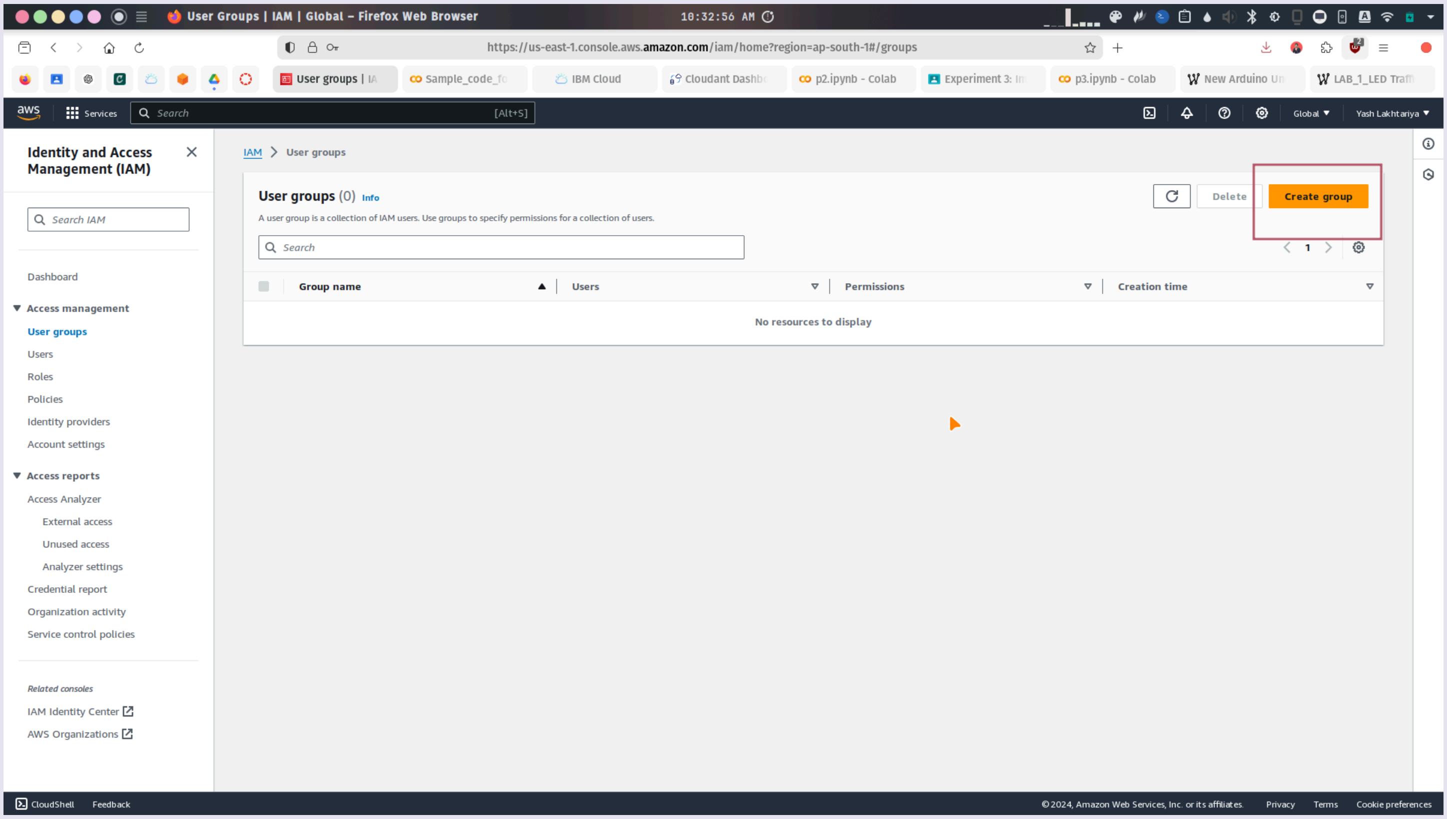
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 71
CCE Practical 4

Scenario : Demonstrate the use of Identity and Access Management services using proper configuration for various IAM Users Roles and Policies User wise.

Tasks to be completed :

- **Create an IAM users like DevOps, Solution Architect.**
- **Manage User roles and policies using Identity and Access Management (IAM).**
- **Create an MFA for all users.**

Screenshots and steps :

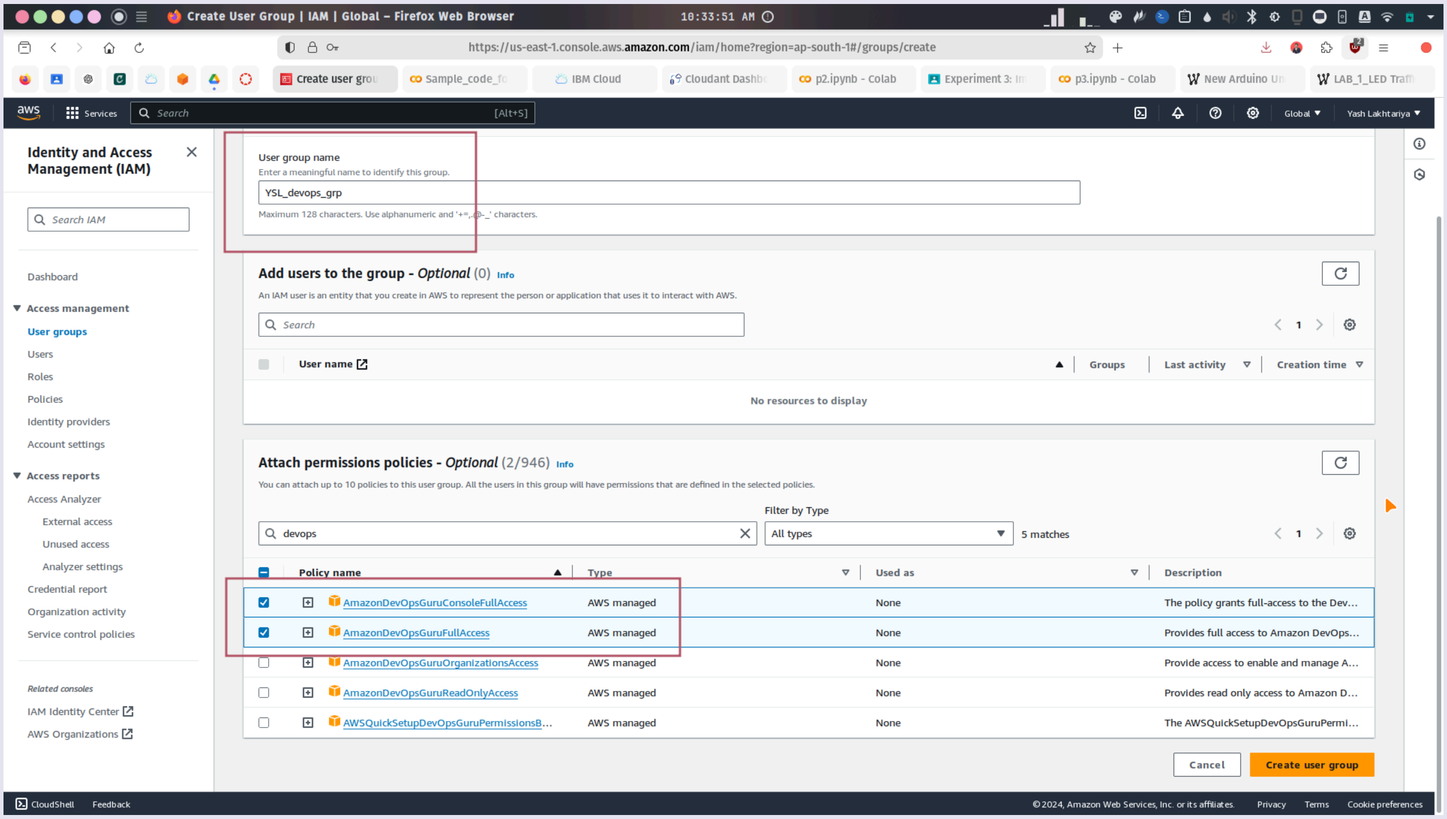


A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Group name	Users	Permissions	Creation time

No resources to display

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CCE Practical 4



User group name
Enter a meaningful name to identify this group.
YSL_devops_grp
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (0) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

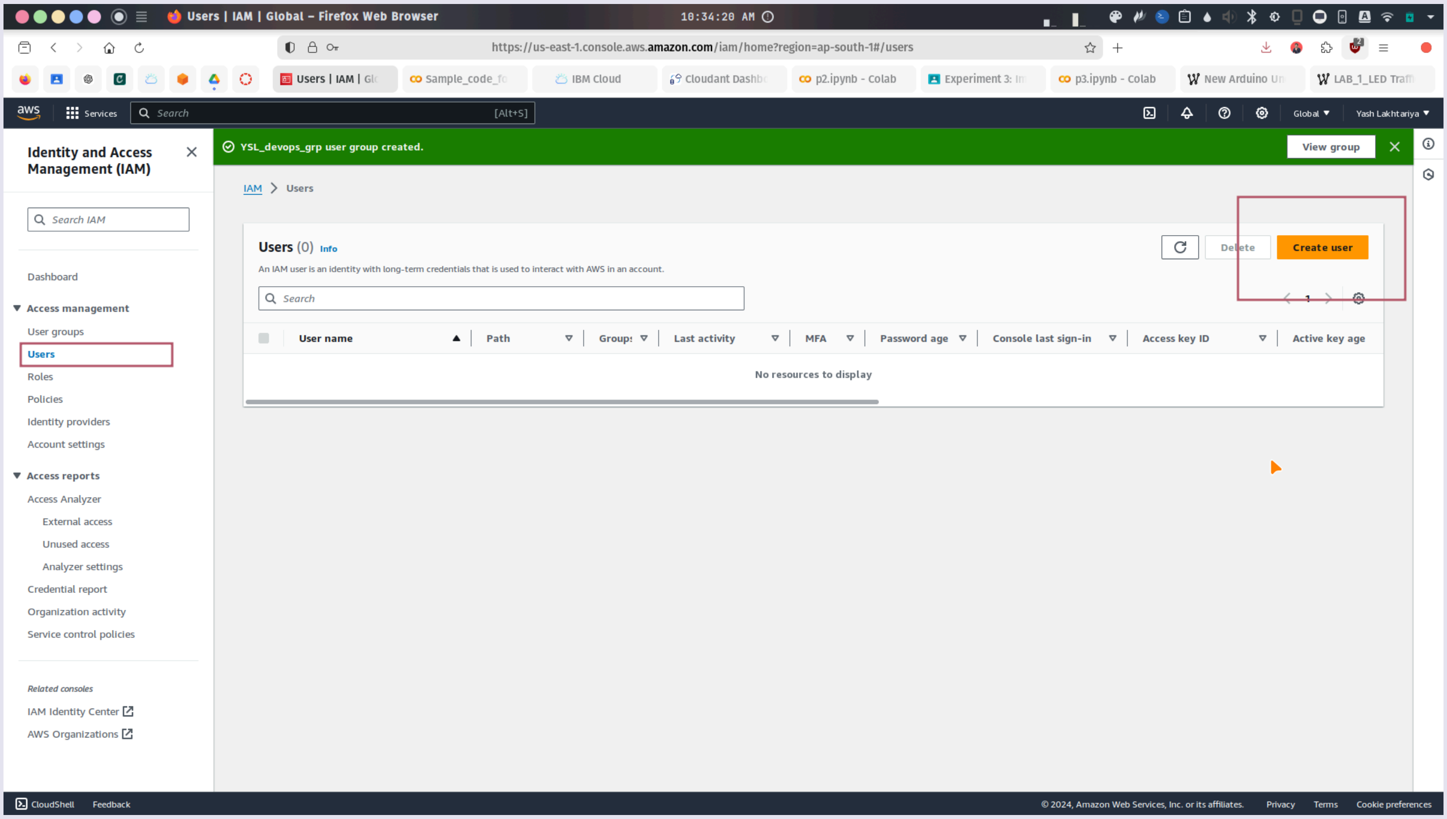
User name	Groups	Last activity	Creation time
No resources to display			

Attach permissions policies - *Optional* (2/946) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Search: devops — Filter by Type: All types — 5 matches

	Policy name	Type	Used as	Description
☑	AmazonDevOpsGuruConsoleFullAccess	AWS managed	None	The policy grants full-access to the Dev…
☑	AmazonDevOpsGuruFullAccess	AWS managed	None	Provides full access to Amazon DevOps…
□	AmazonDevOpsGuruOrganizationsAccess	AWS managed	None	Provide access to enable and manage A…
□	AmazonDevOpsGuruReadOnlyAccess	AWS managed	None	Provides read only access to Amazon D…
□	AWSQuickSetupDevOpsGuruPermissionsB…	AWS managed	None	The AWSQuickSetupDevOpsGuruPermi…



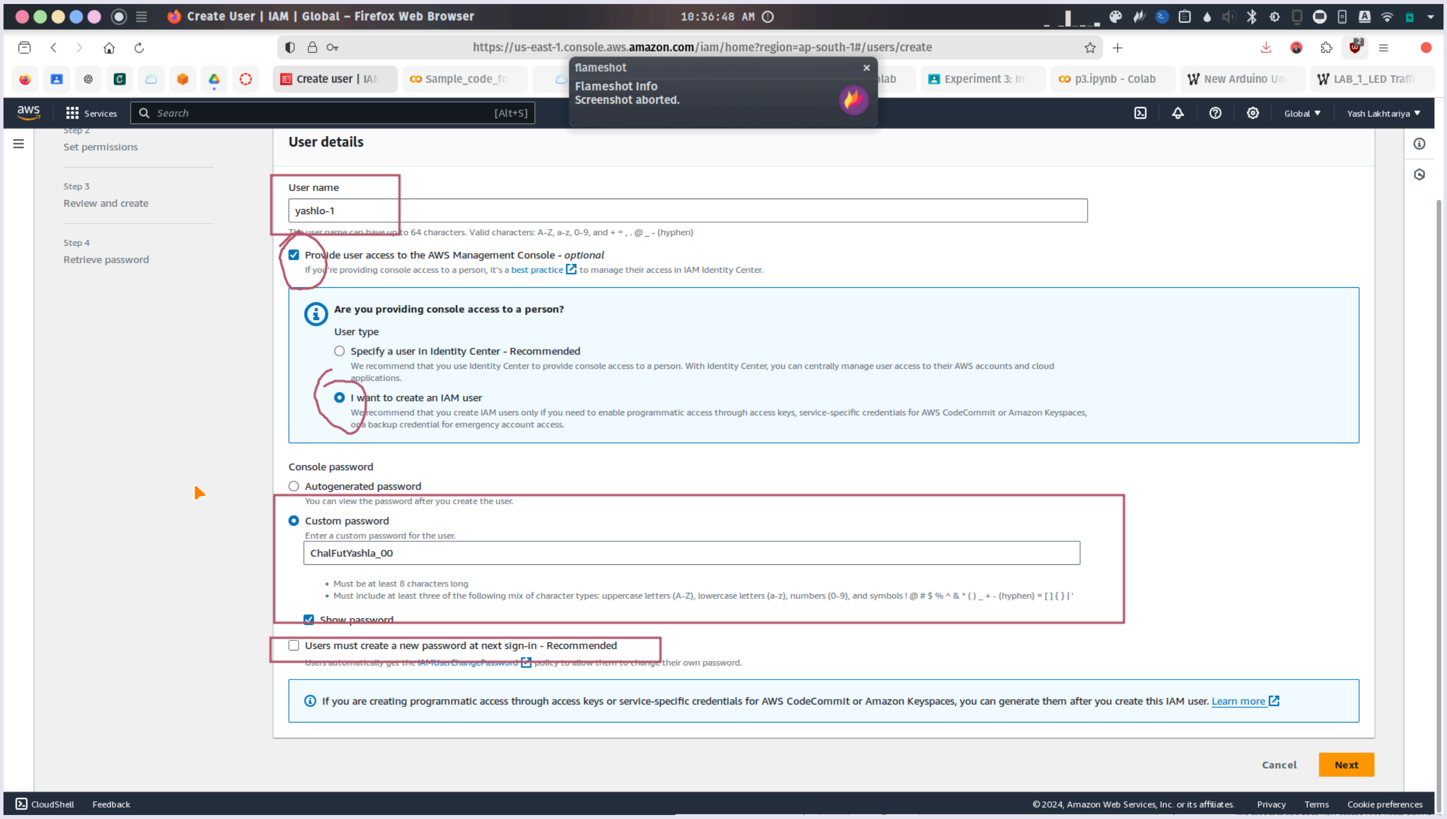
YSL_devops_grp user group created.

Users (0) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Group:	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age
No resources to display								

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 71
CCE Practical 4



flameshot
Flameshot Info
Screenshot aborted.

User details

User name

yashlo-1

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 the user.

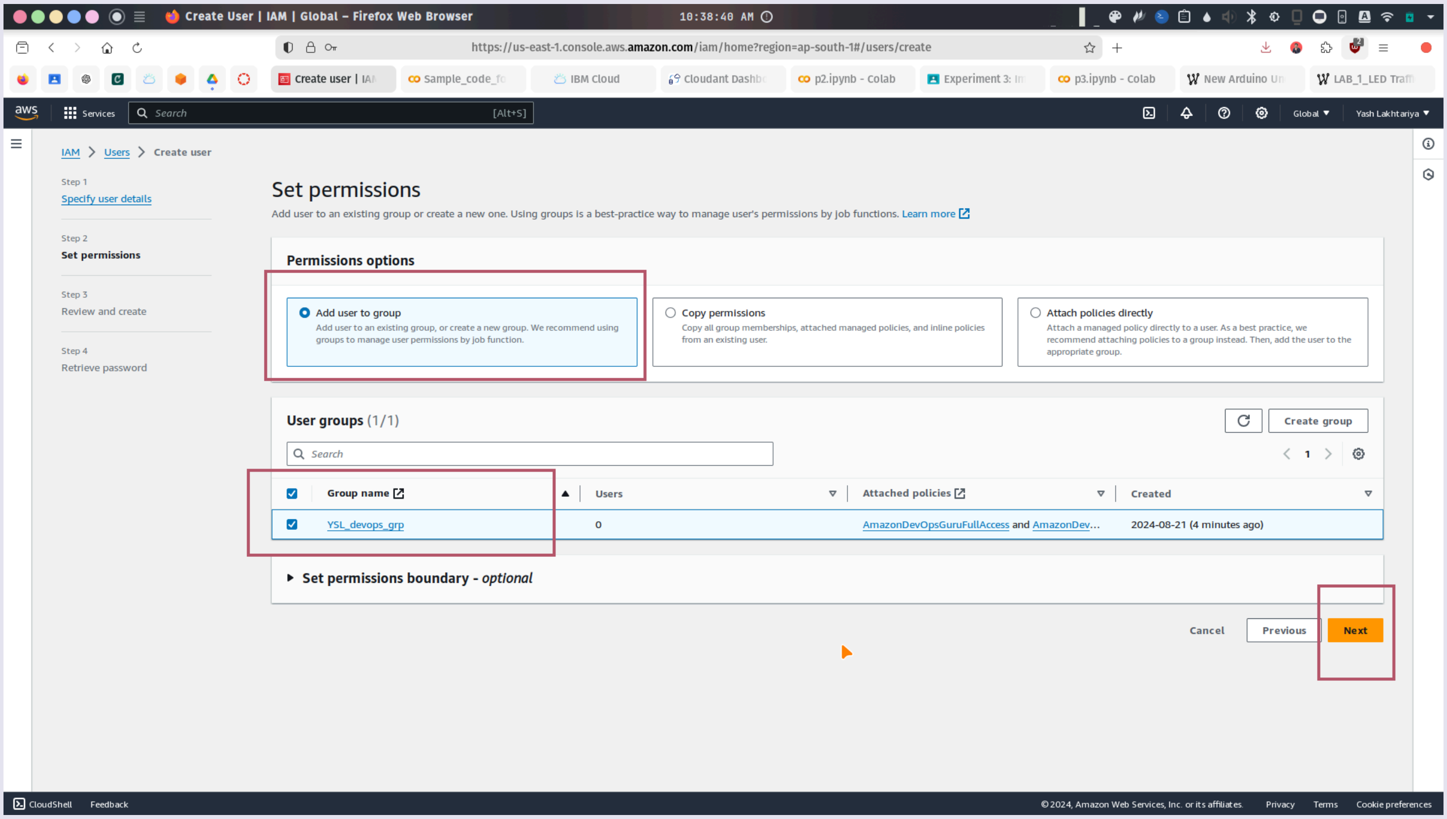
ChalFutYashla_00

- 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 ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

☑ 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.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more



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.

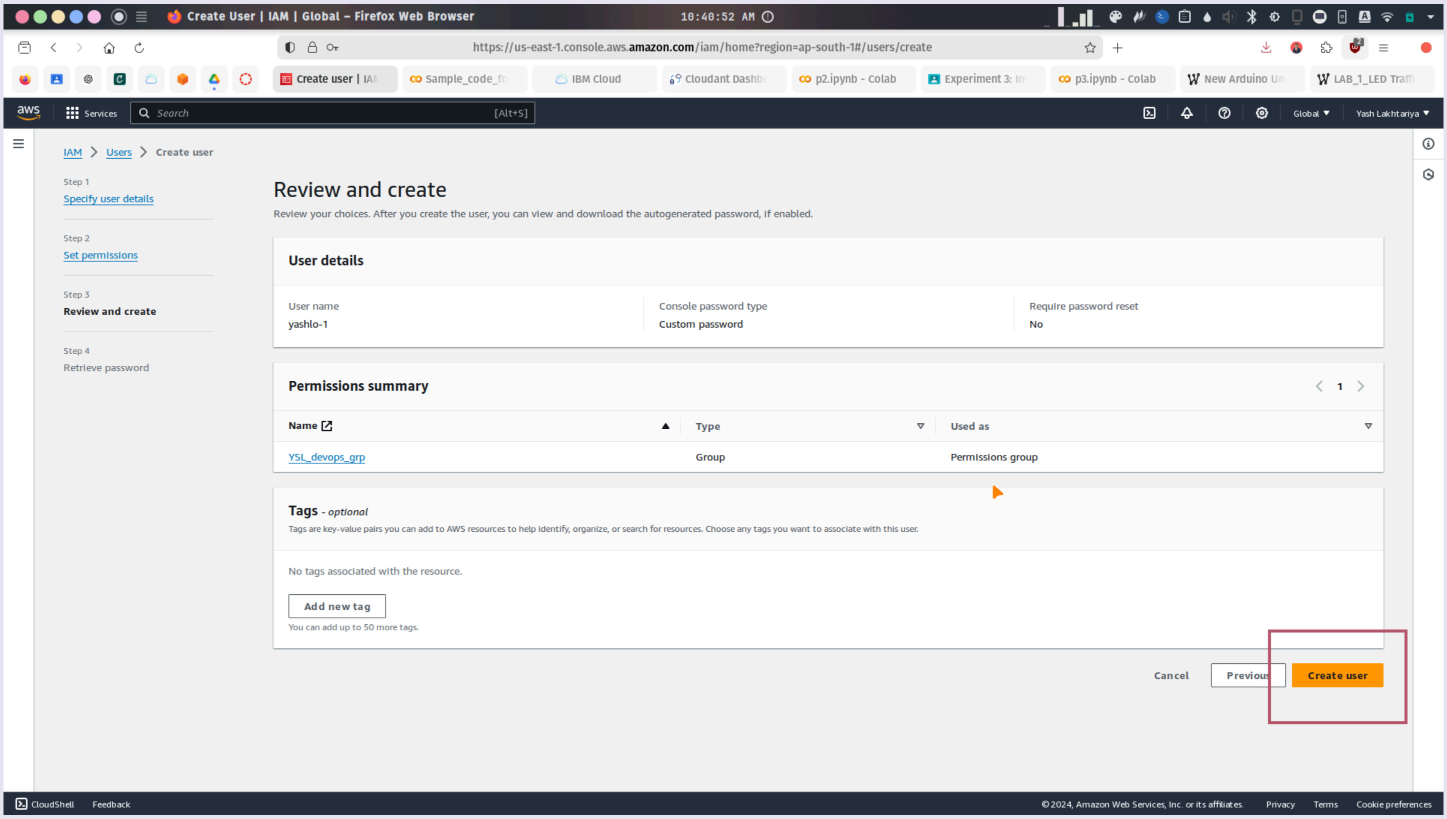
○ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1/1)

☑	Group name	Users	Attached policies	Created
☑	YSL_devops_grp	0	AmazonDevOpsGuruFullAccess and AmazonDev...	2024-08-21 (4 minutes ago)

▸ Set permissions boundary - *optional*

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CCE Practical 4



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	Console password type	Require password reset
yashlo-1	Custom password	No

Permissions summary

Name	Type	Used as
YSL_devops_grp	Group	Permissions group

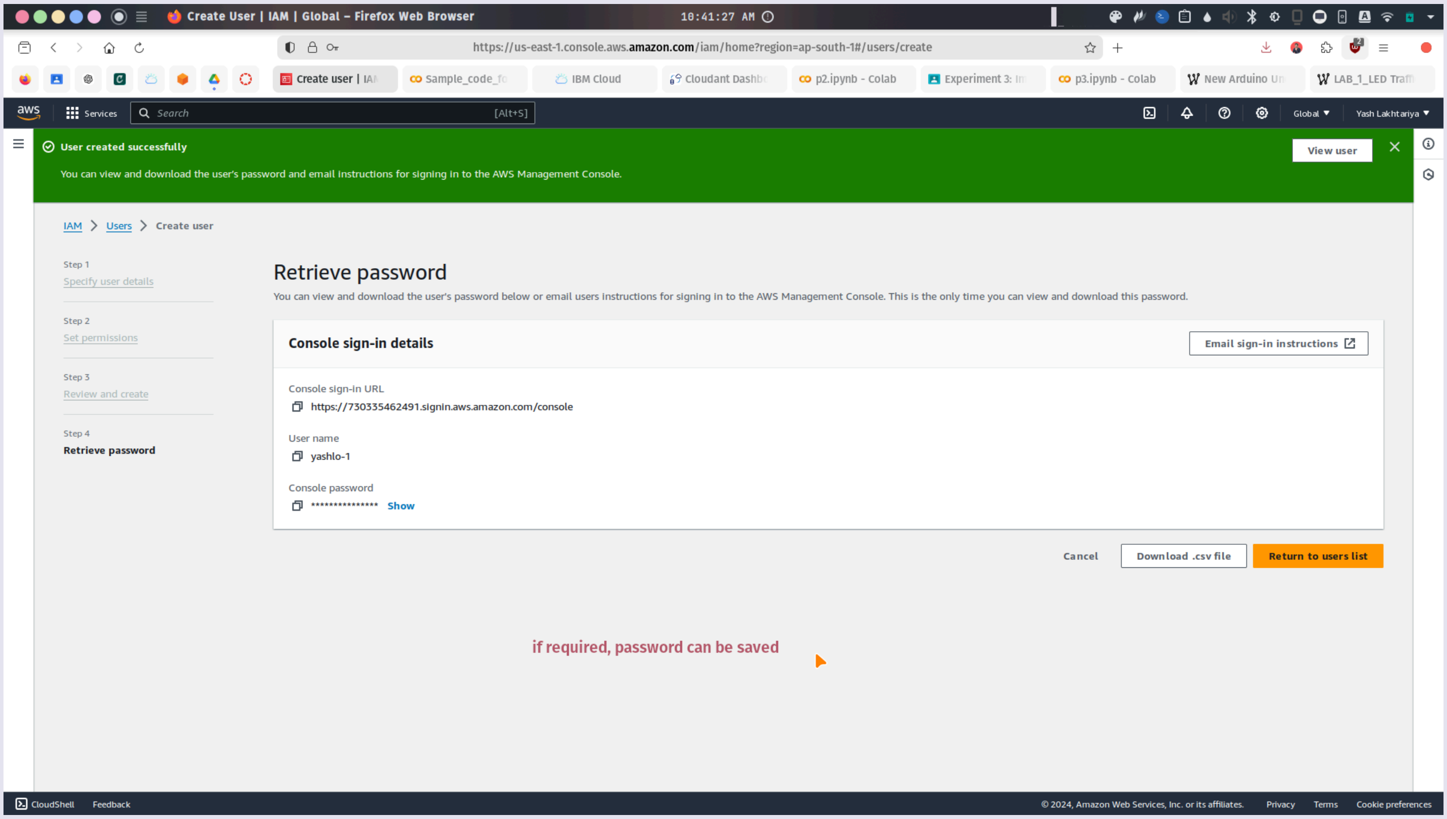
Tags - *optional*

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.



User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

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

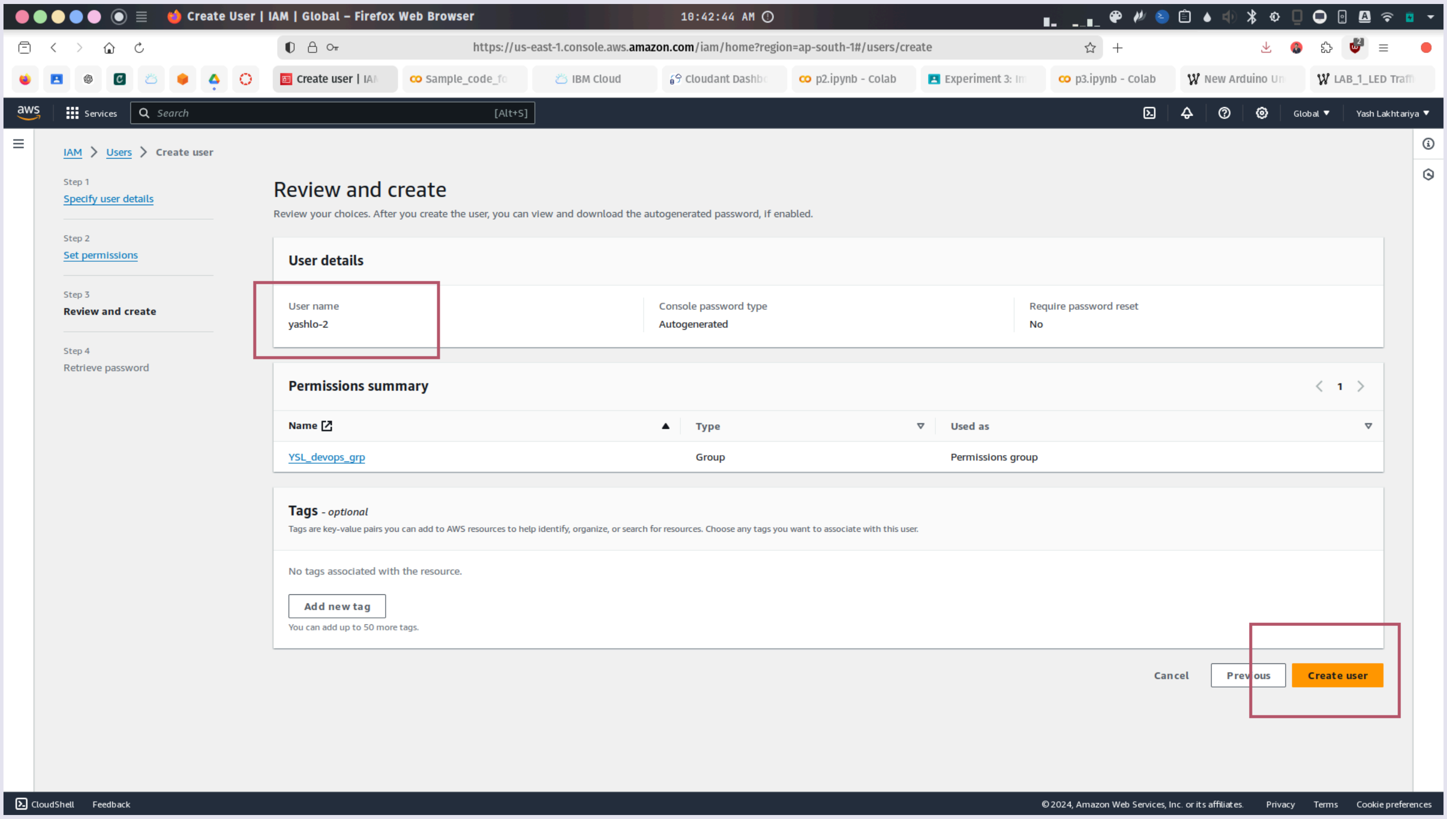
Console sign-in URL
https://730335462491.signin.aws.amazon.com/console

User name
yashlo-1

Console password
*************** Show

if required, password can be saved

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 71
CCE Practical 4



Create User | IAM | Global – Firefox Web Browser 10:42:44 AM

https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create

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	Console password type	Require password reset
yashlo-2	Autogenerated	No

Permissions summary

Name	Type	Used as
YSL_devops_grp	Group	Permissions group

Tags - *optional*

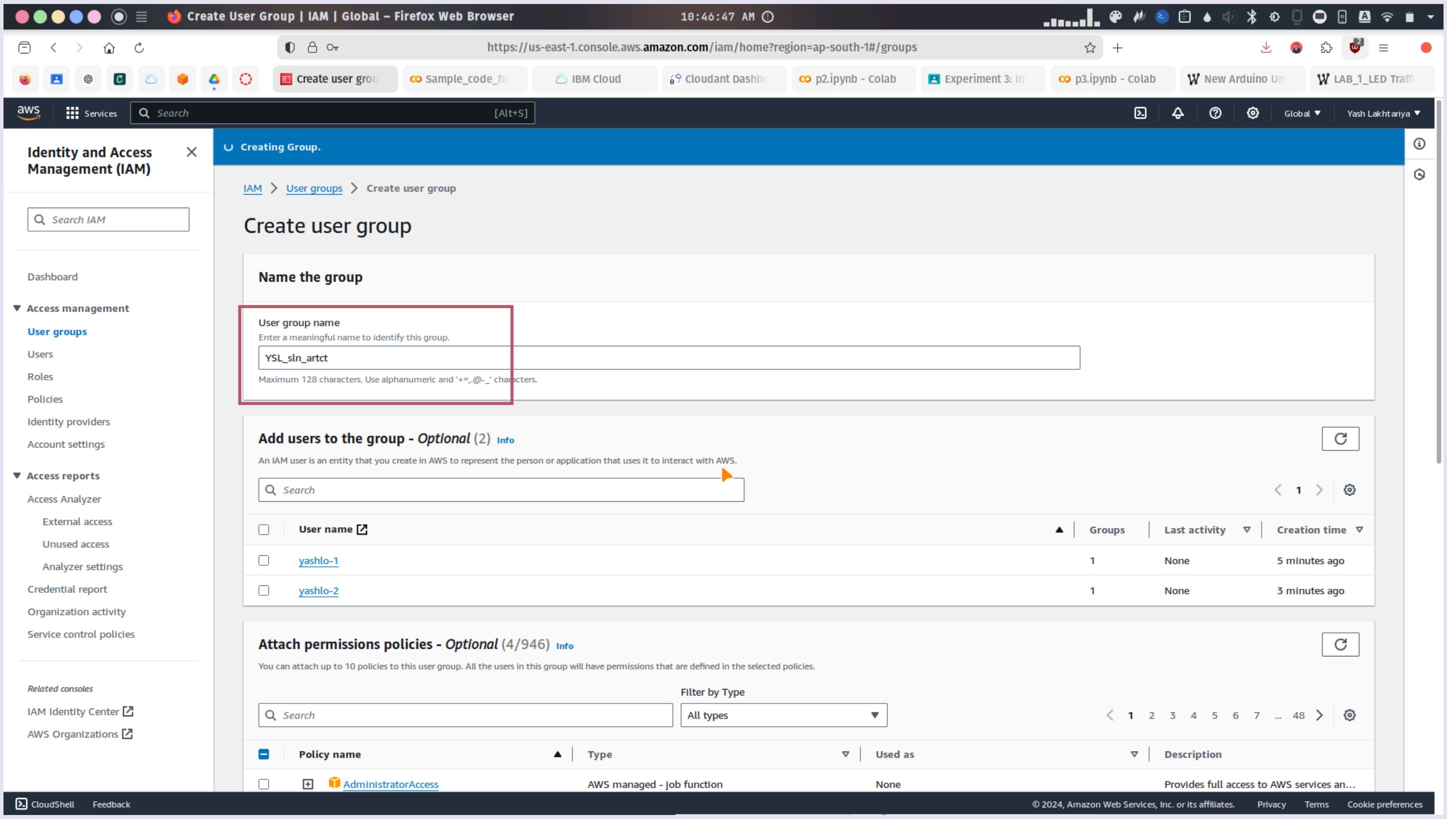
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Previous Create user



Create User Group | IAM | Global – Firefox Web Browser 10:46:47 AM

https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups

Identity and Access Management (IAM)

Creating Group.

IAM > User groups > Create user group

Create user group

Name the group

User group name
Enter a meaningful name to identify this group.
YSL_sln_artct
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (2) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

	User name	Groups	Last activity	Creation time
□	yashlo-1	1	None	5 minutes ago
□	yashlo-2	1	None	3 minutes ago

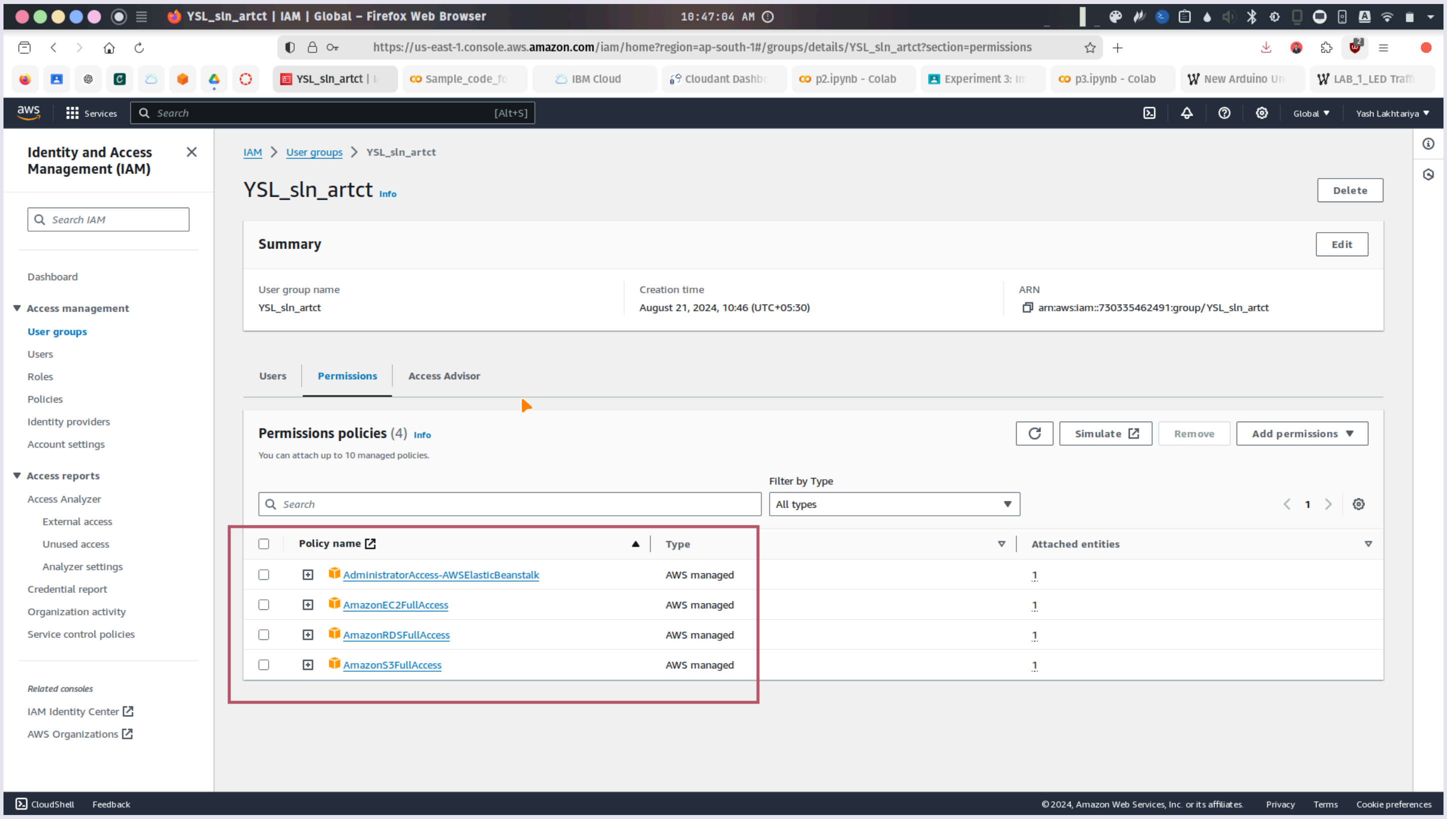
Attach permissions policies - *Optional* (4/946) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type: All types

	Policy name	Type	Used as	Description
□	AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 71
CCE Practical 4



YSL_sln_artct

Summary

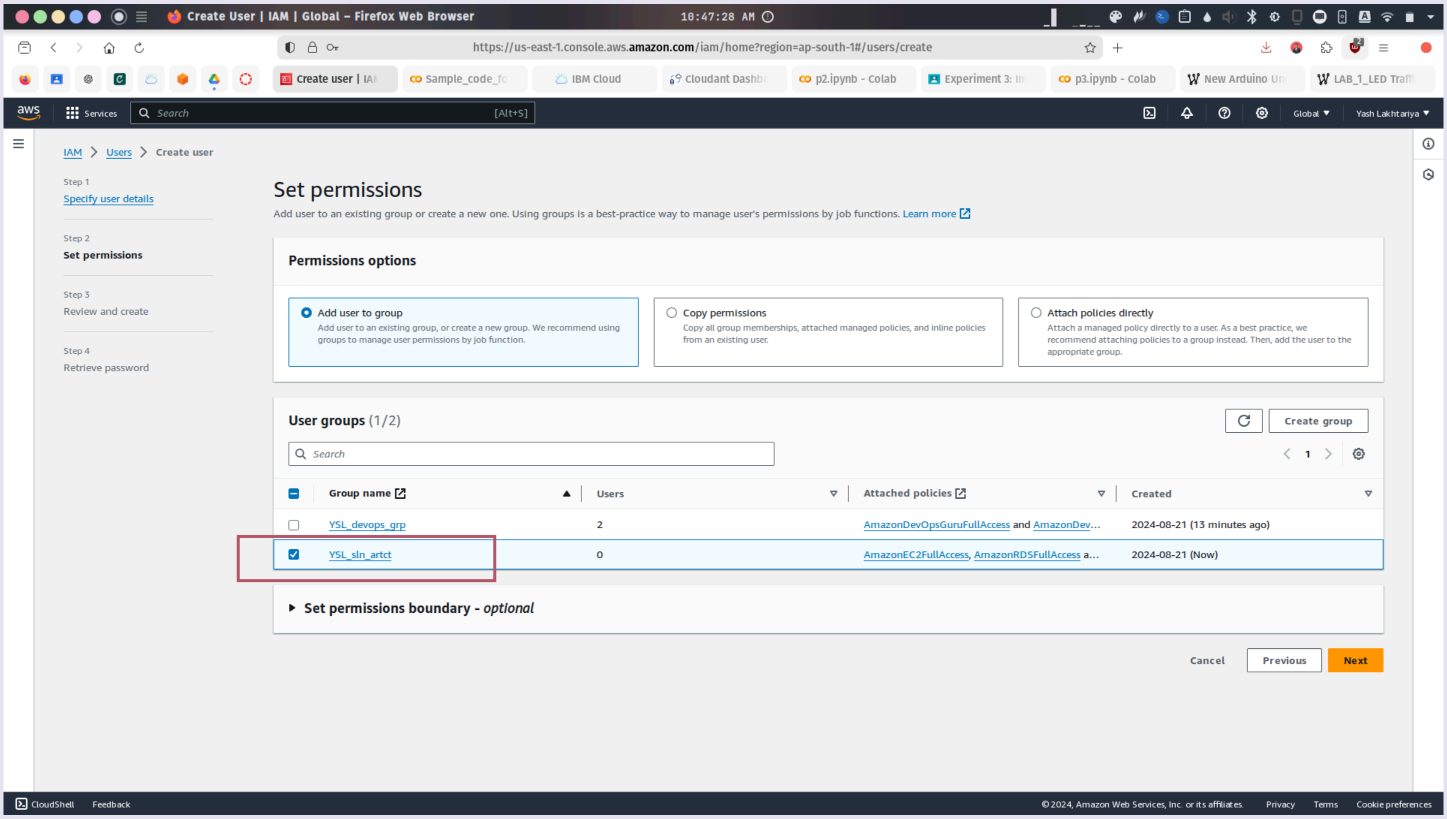
User group name	Creation time	ARN
YSL_sln_artct	August 21, 2024, 10:46 (UTC+05:30)	arn:aws:iam::730335462491:group/YSL_sln_artct

Permissions policies (4)

You can attach up to 10 managed policies.

Filter by Type: All types

□	Policy name	Type	Attached entities
□	AdministratorAccess-AWSElasticBeanstalk	AWS managed	1
□	AmazonEC2FullAccess	AWS managed	1
□	AmazonRDSFullAccess	AWS managed	1
□	AmazonS3FullAccess	AWS managed	1



Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

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.

Permissions options

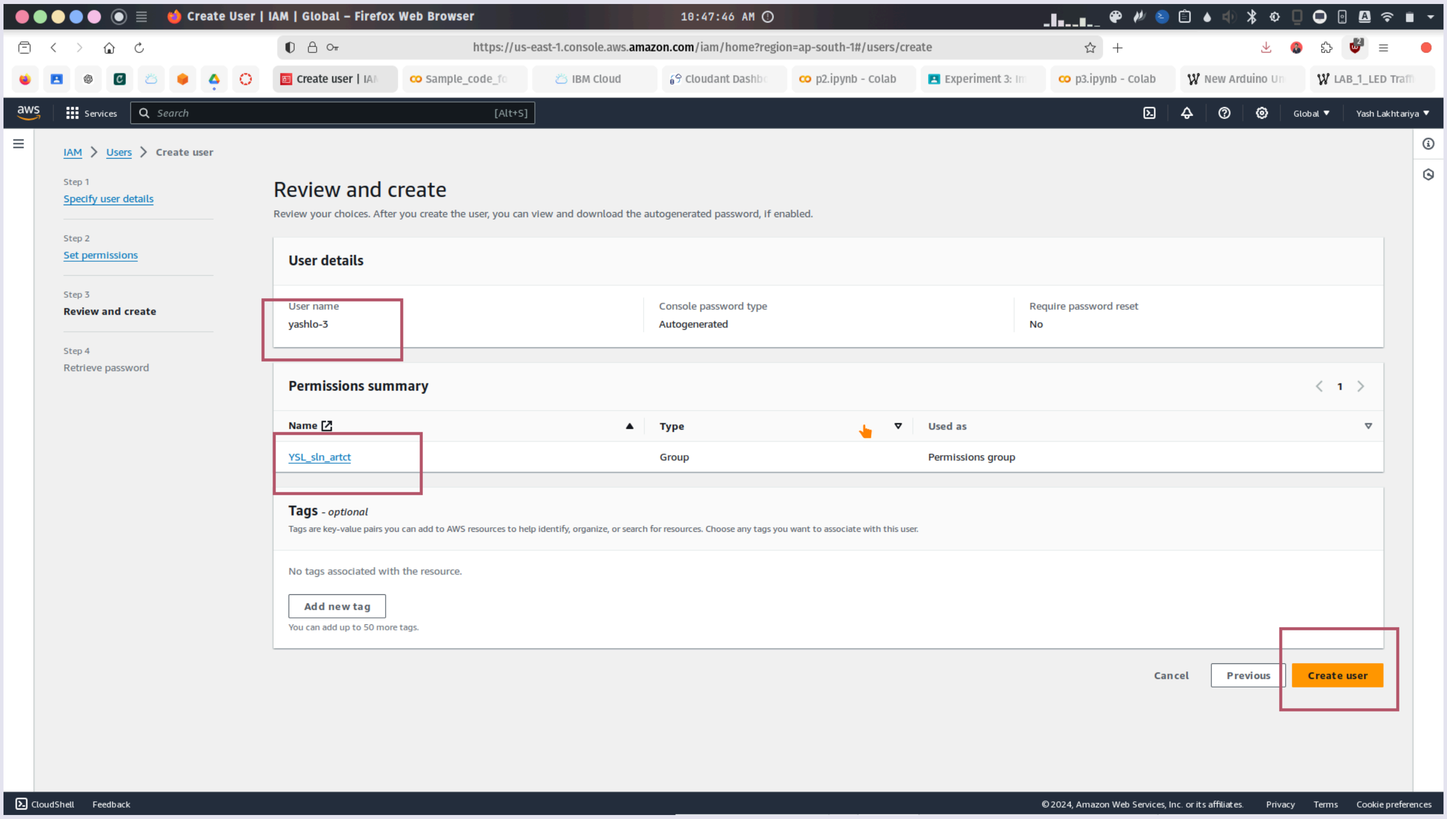
- ● Add user to group — Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- ○ Copy permissions — Copy all group memberships, attached managed policies, and inline policies from an existing user.
- ○ Attach policies directly — Attach 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 (1/2)

□	Group name	Users	Attached policies	Created
□	YSL_devops_grp	2	AmazonDevOpsGuruFullAccess and AmazonDev...	2024-08-21 (13 minutes ago)
☑	YSL_sln_artct	0	AmazonEC2FullAccess, AmazonRDSFullAccess a...	2024-08-21 (Now)

▸ **Set permissions boundary - *optional***

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CCE Practical 4



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	Console password type	Require password reset
yashlo-3	Autogenerated	No

Permissions summary

Name	Type	Used as
YSL_sln_artct	Group	Permissions group

Tags - *optional*

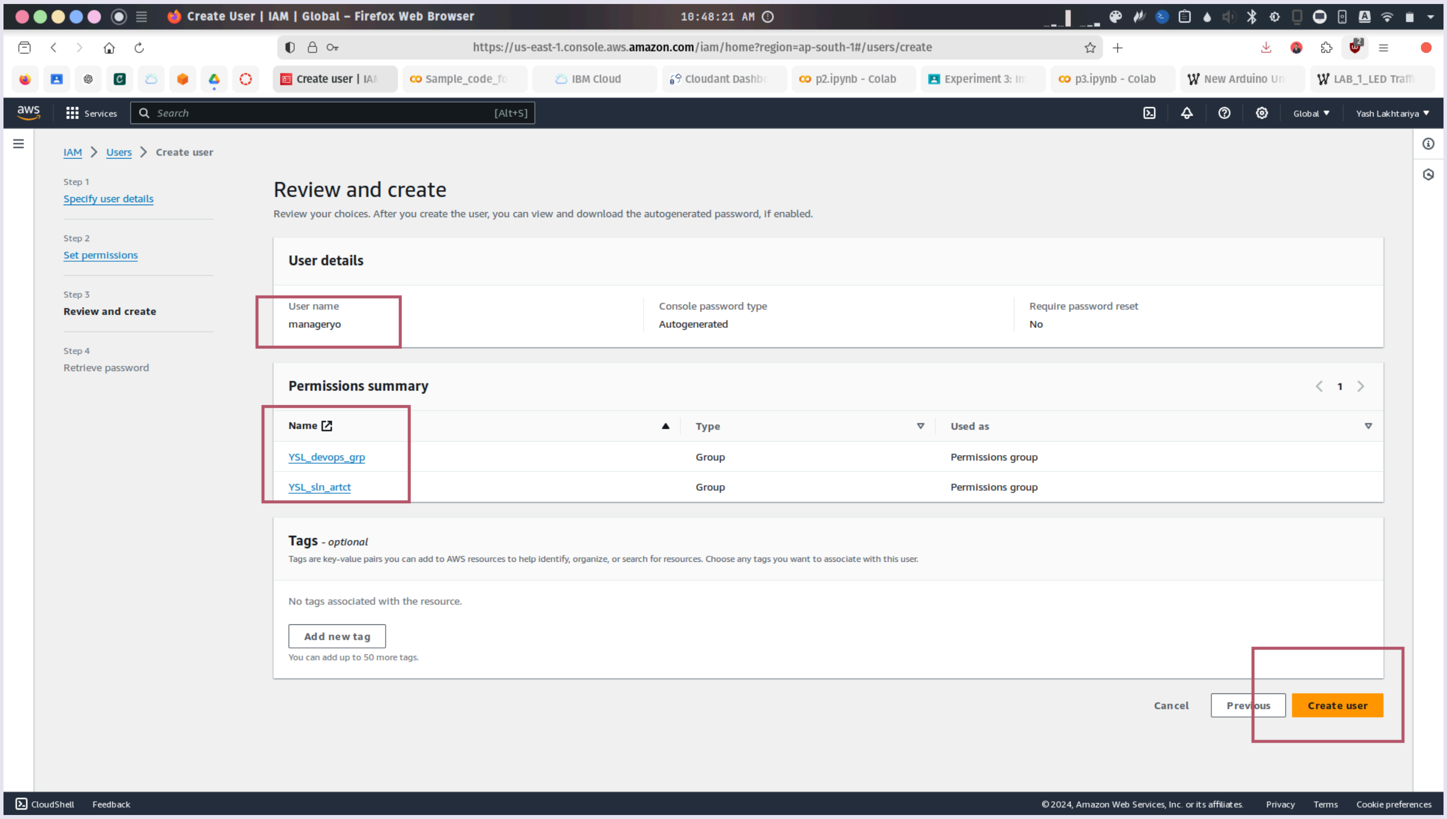
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Previous **Create user**



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	Console password type	Require password reset
manageryo	Autogenerated	No

Permissions summary

Name	Type	Used as
YSL_devops_grp	Group	Permissions group
YSL_sln_artct	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.

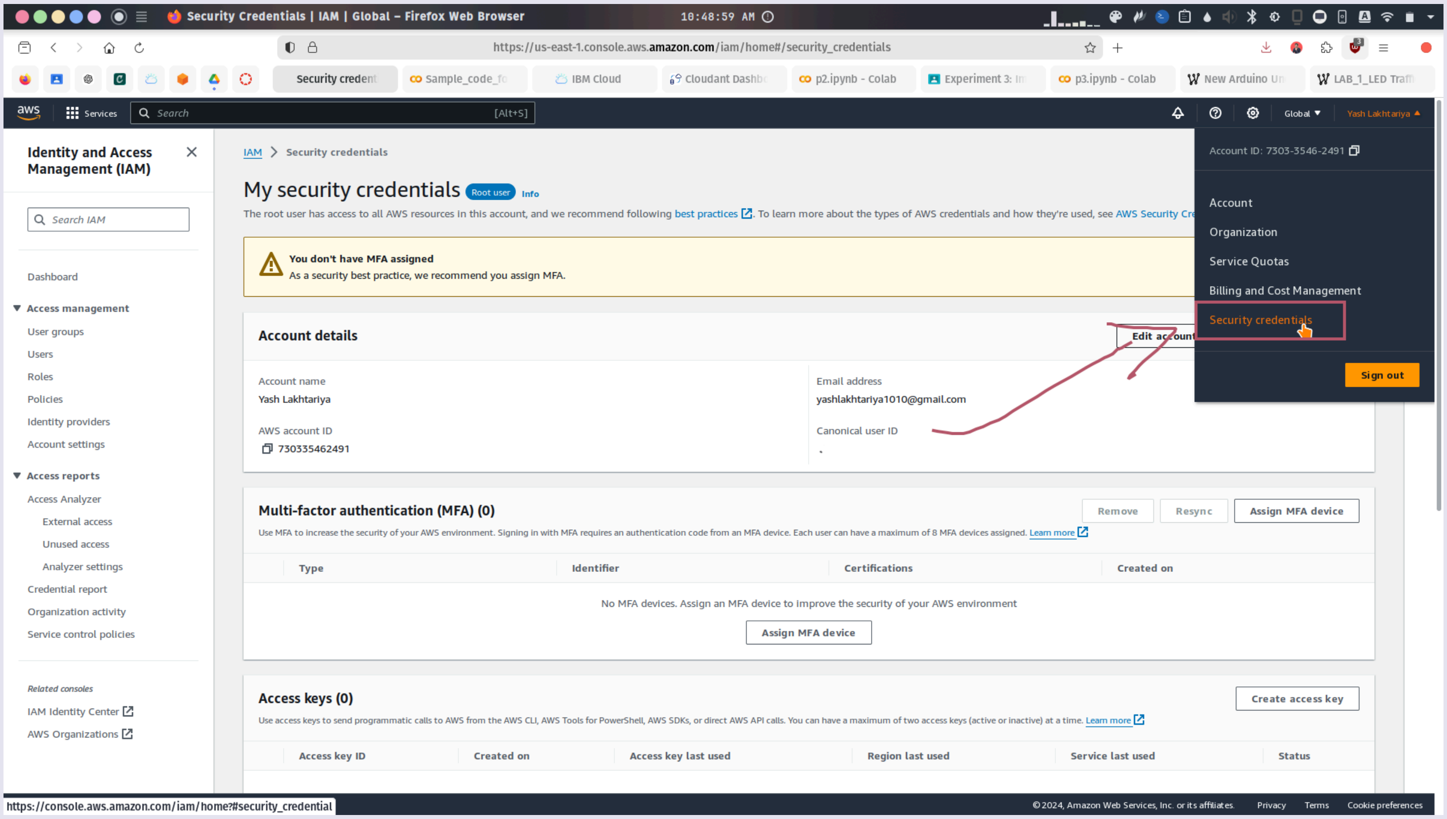
No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Previous **Create user**

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CCE Practical 4



IAM > Security credentials

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 Cre

You don't have MFA assigned
As a security best practice, we recommend you assign MFA.

Account details

Edit account

Account name
Yash Lakhtariya

Email address
yashlakhtariya1010@gmail.com

AWS account ID
730335462491

Canonical user ID
.

Multi-factor authentication (MFA) (0)

Remove Resync Assign MFA device

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

Type	Identifier	Certifications	Created on

No MFA devices. Assign an MFA device to improve the security of your AWS environment

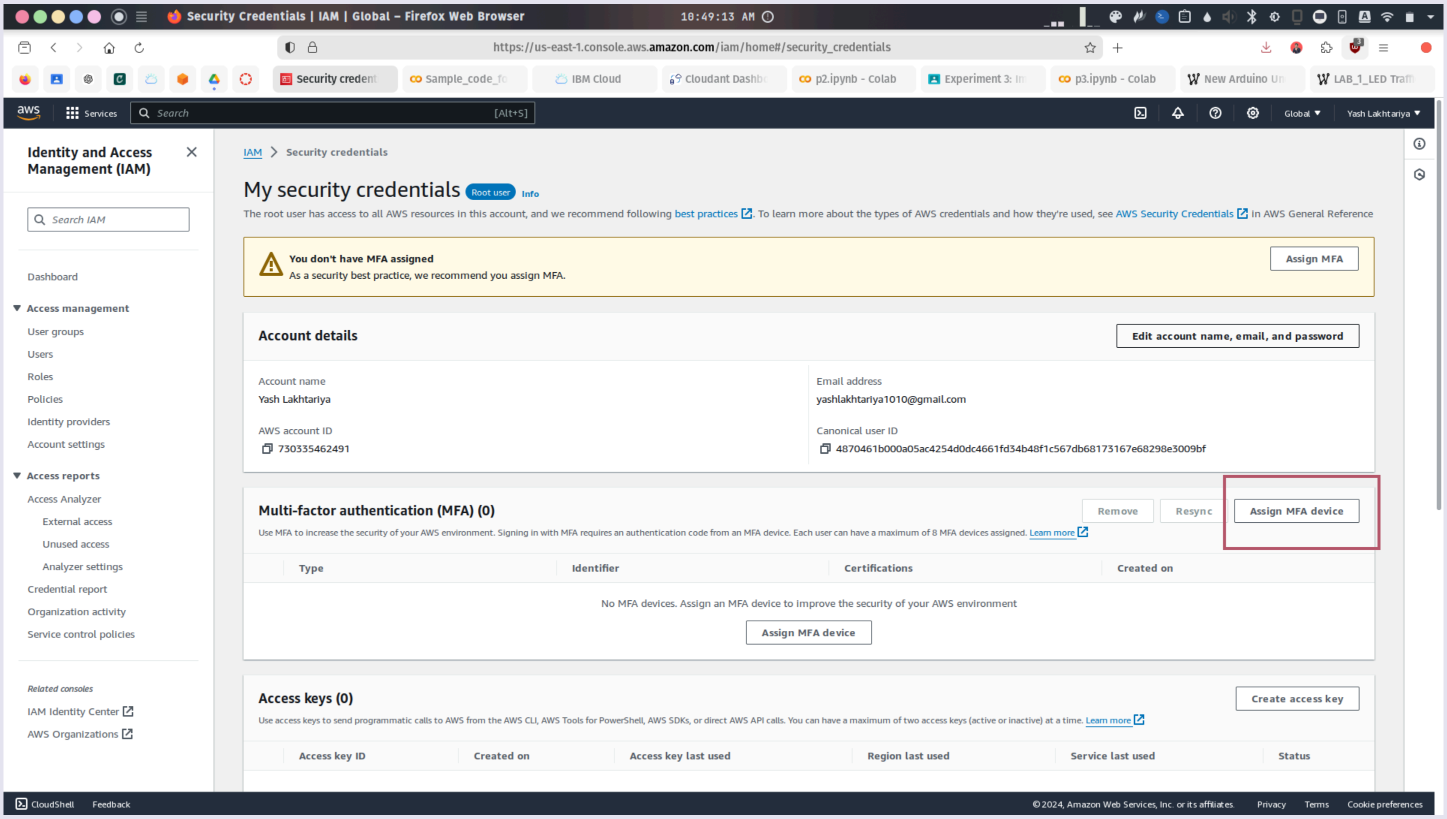
Assign MFA device

Access keys (0)

Create access key

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more

Access key ID	Created on	Access key last used	Region last used	Service last used	Status



IAM > Security credentials

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

You don't have MFA assigned
As a security best practice, we recommend you assign MFA.

Assign MFA

Account details

Edit account name, email, and password

Account name
Yash Lakhtariya

Email address
yashlakhtariya1010@gmail.com

AWS account ID
730335462491

Canonical user ID
4870461b000a05ac4254d0dc4661fd34b48f1c567db68173167e68298e3009bf

Multi-factor authentication (MFA) (0)

Remove Resync Assign MFA device

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

Type	Identifier	Certifications	Created on

No MFA devices. Assign an MFA device to improve the security of your AWS environment

Assign MFA device

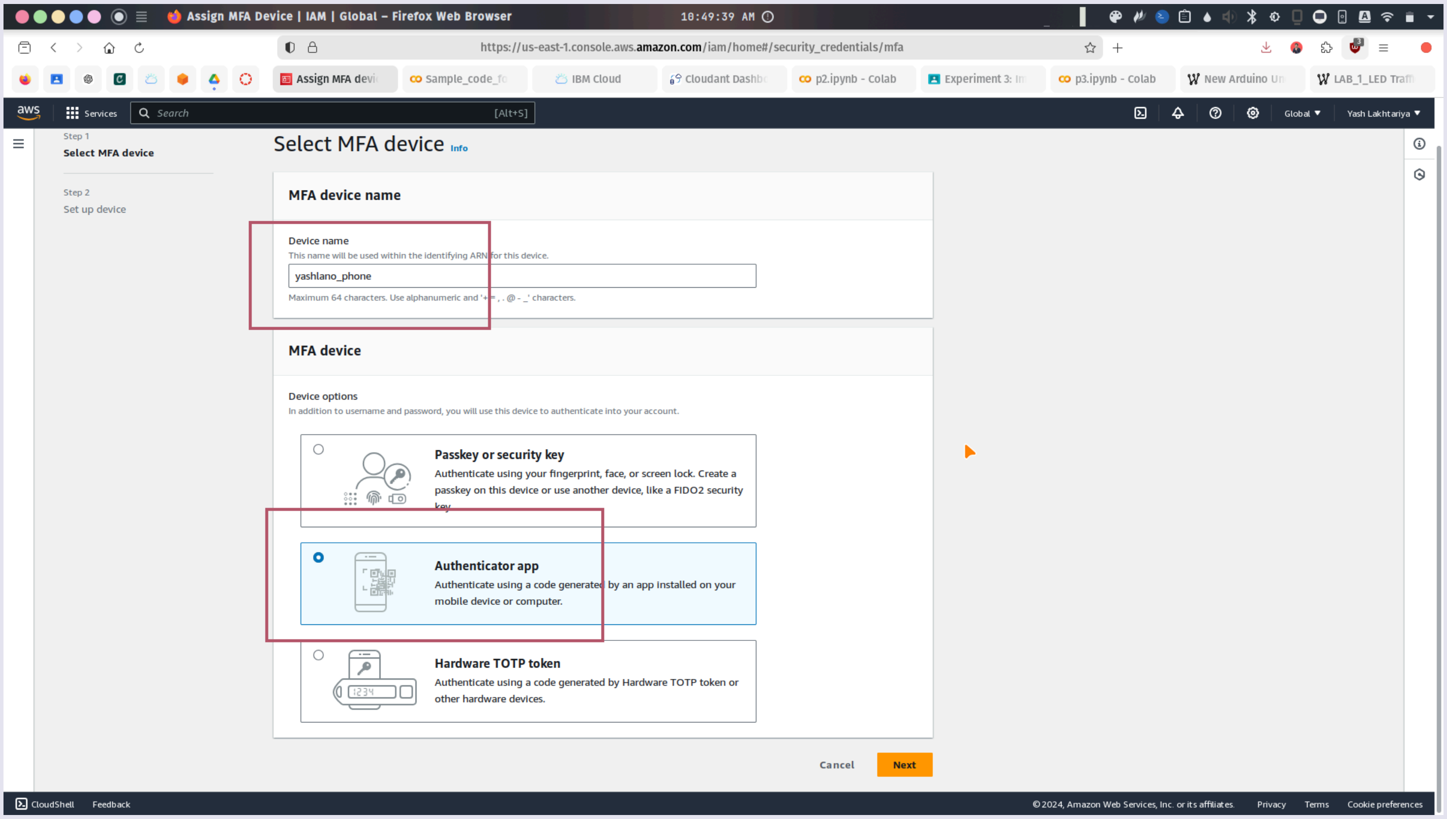
Access keys (0)

Create access key

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more

Access key ID	Created on	Access key last used	Region last used	Service last used	Status

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 71
CCE Practical 4



Step 1
Select MFA device

Step 2
Set up device

Select MFA device Info

MFA device name

Device name
This name will be used within the identifying ARN for this device.
yashlano_phone
Maximum 64 characters. Use alphanumeric and '+ = , . @ - _' characters.

MFA device

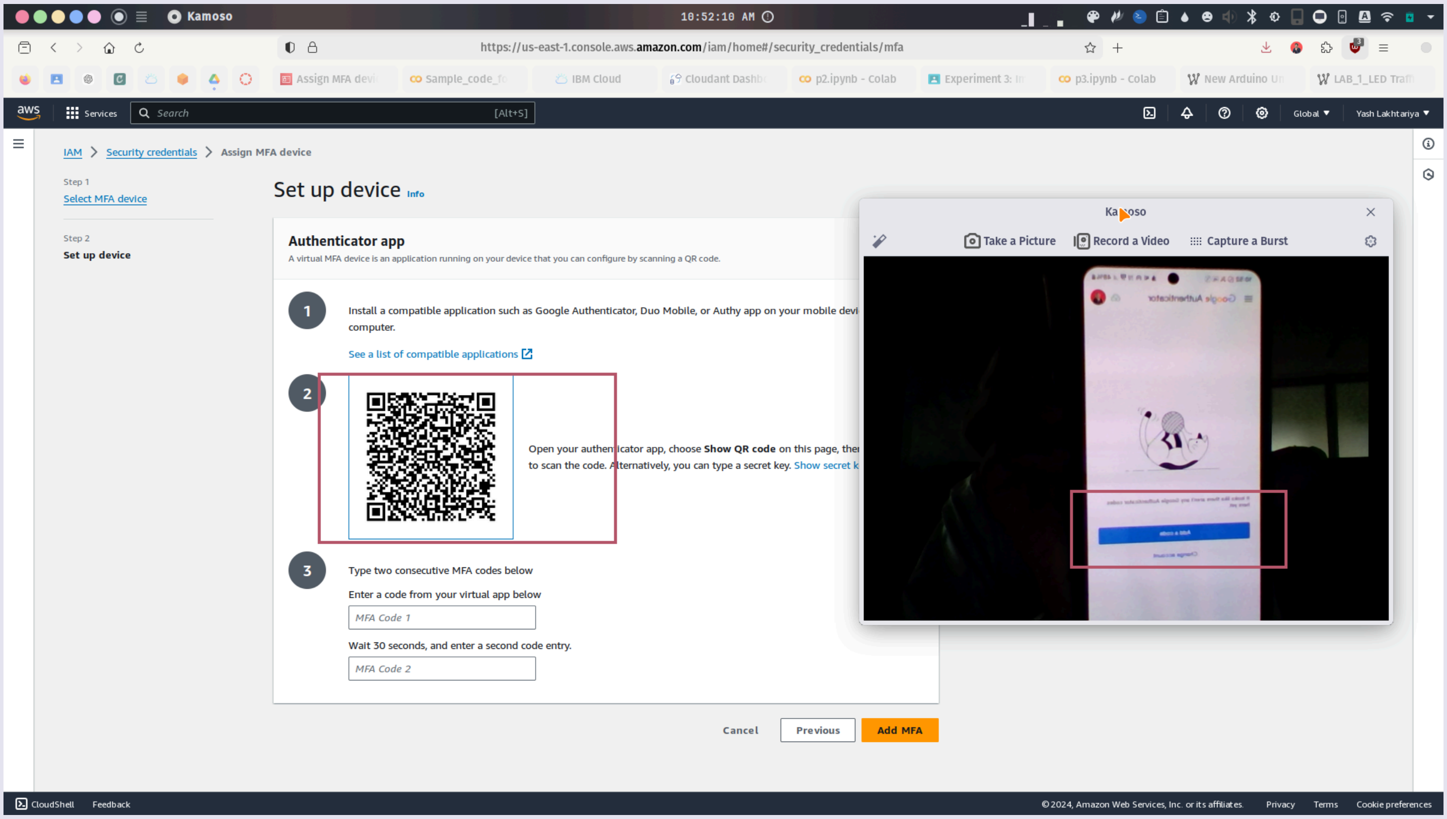
Device options
In addition to username and password, you will use this device to authenticate into your account.

○ **Passkey or security key**
Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.

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

○ **Hardware TOTP token**
Authenticate using a code generated by Hardware TOTP token or other hardware devices.

Cancel Next



IAM > Security credentials > Assign MFA device

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.

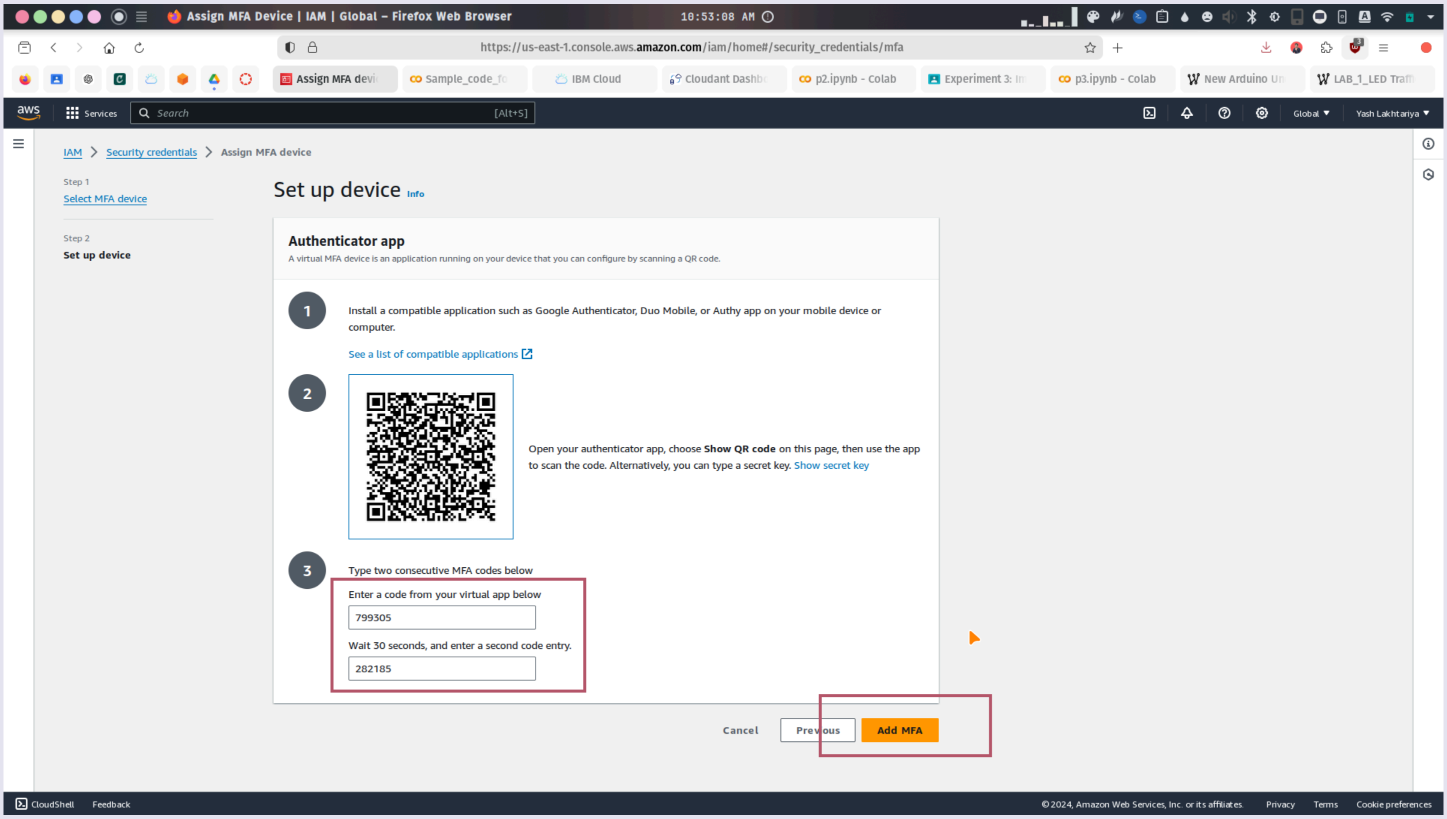
1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile devi computer.
See a list of compatible applications

2 Open your authenticator app, choose **Show QR code** on this page, then to scan the code. Alternatively, you can type a secret key. Show secret k

3 Type two consecutive MFA codes below
Enter a code from your virtual app below
MFA Code 1
Wait 30 seconds, and enter a second code entry.
MFA Code 2

Cancel Previous Add MFA

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CCE Practical 4


Assign MFA Device | IAM | Global — Firefox Web Browser
10:53:08 AM
https://us-east-1.console.aws.amazon.com/iam/home#/security_credentials/mfa
Services
Search [Alt+S]
Global
Yash Lakhtariya
IAM > Security credentials > Assign MFA device
Step 1
Select MFA device
Step 2
Set up device
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

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 Type two consecutive MFA codes below

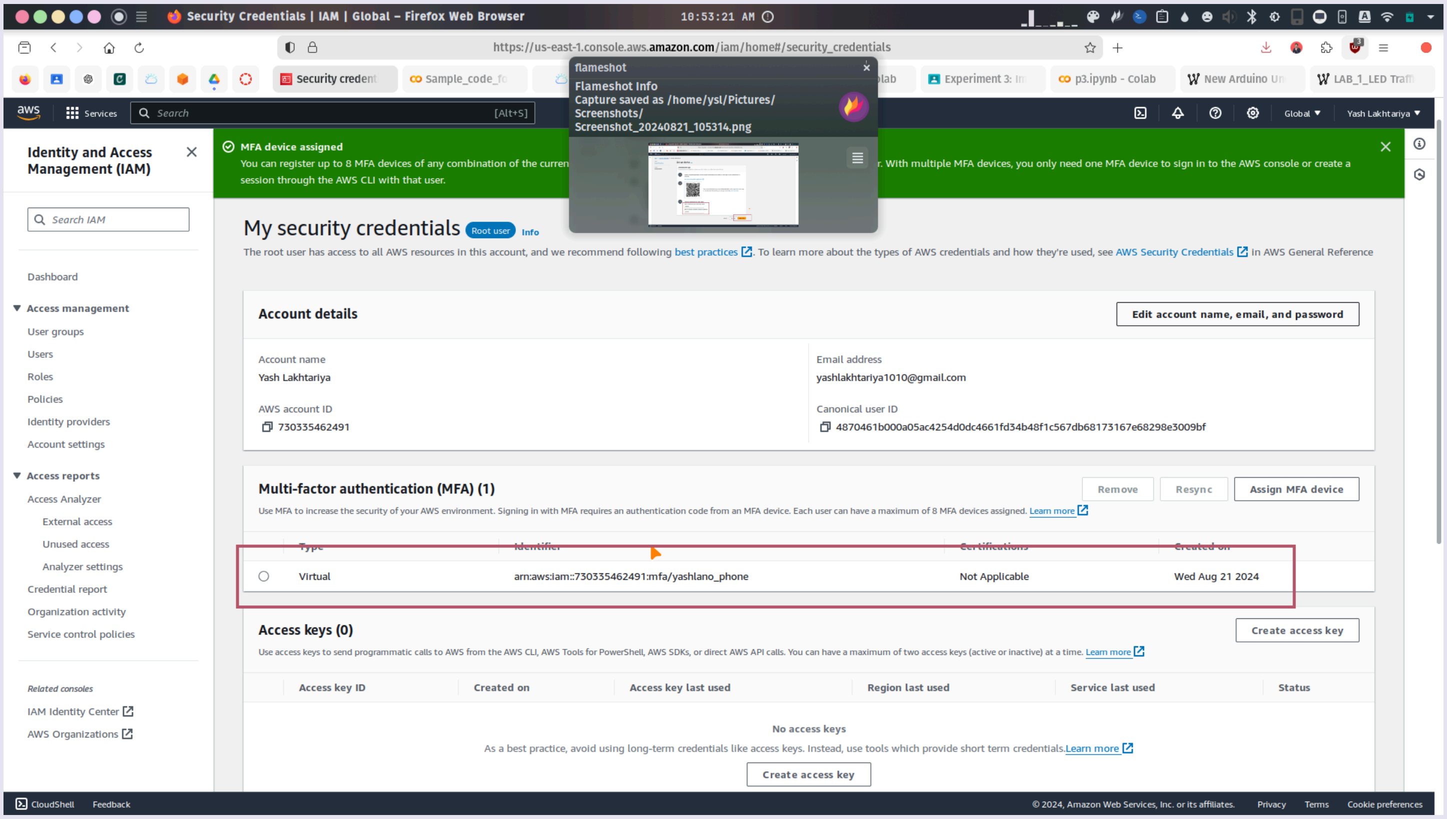
Enter a code from your virtual app below

799305

Wait 30 seconds, and enter a second code entry.

282185

Cancel | Previous | Add MFA



flameshot

Flameshot Info
Capture saved as /home/ysl/Pictures/Screenshots/Screenshot_20240821_105314.png

MFA device assigned

You can register up to 8 MFA devices of any combination of the curren[...]. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

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

Account details | Edit account name, email, and password

Account name
Yash Lakhtariya

Email address
yashlakhtariya1010@gmail.com

AWS account ID
730335462491

Canonical user ID
4870461b000a05ac4254d0dc4661fd34b48f1c567db68173167e68298e3009bf

Multi-factor authentication (MFA) (1) | Remove | Resync | Assign MFA device

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

	Type	Identifier	Certifications	Created on
○	Virtual	arn:aws:iam::730335462491:mfa/yashlano_phone	Not Applicable	Wed Aug 21 2024

Access keys (0) | Create access key

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more

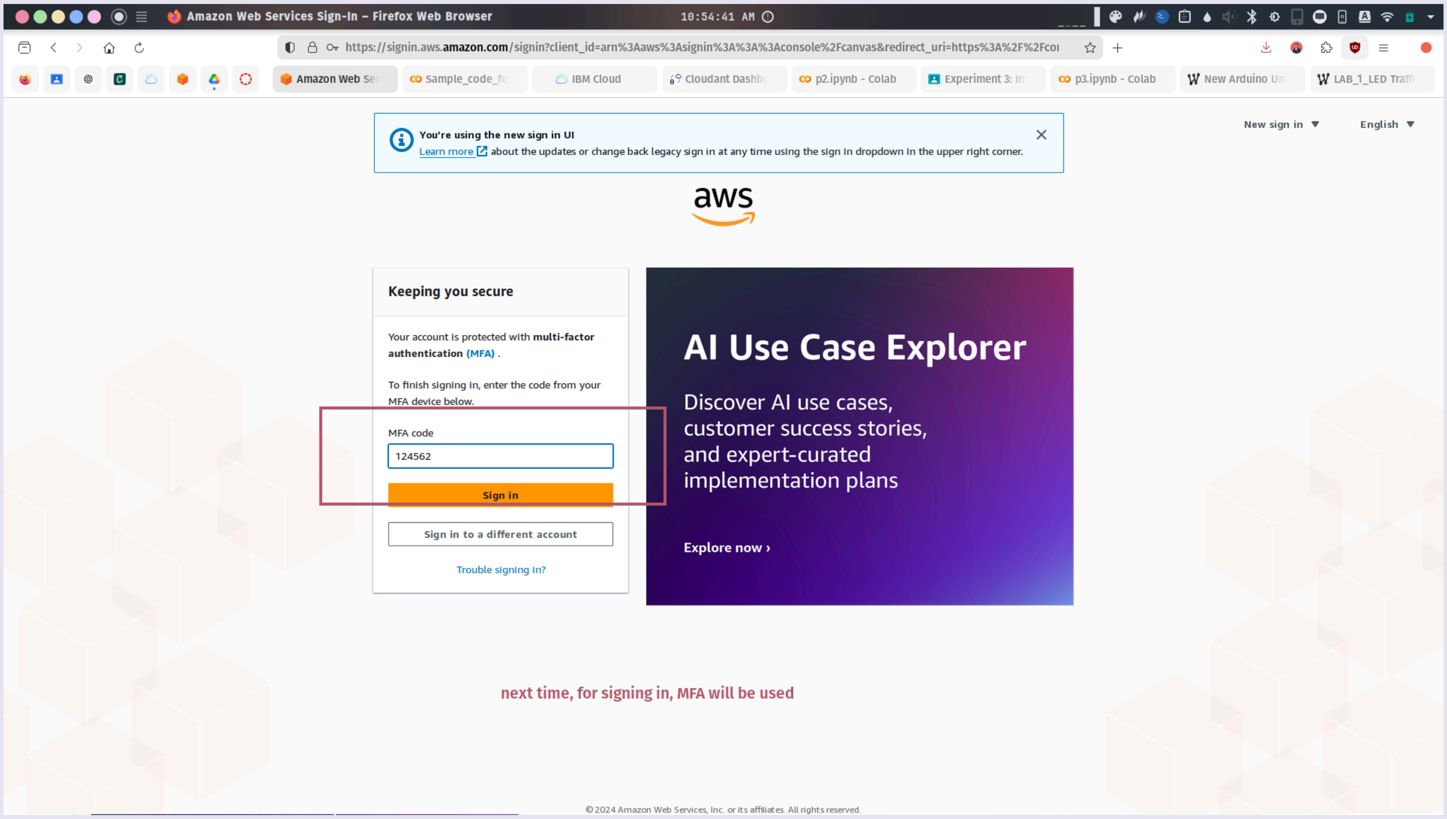
Access key ID	Created on	Access key last used	Region last used	Service last used	Status

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

Create access key

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CCE Practical 4


Amazon Web Services Sign-In — Firefox Web Browser
10:54:41 AM
https://signin.aws.amazon.com/signin?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&redirect_uri=https%3A%2F%2Fcon
Amazon Web Se
Sample_code_fo
IBM Cloud
Cloudant Dashb
p2.ipynb - Colab
Experiment 3: Im
p3.ipynb - Colab
New Arduino Un
LAB_1_LED Traff
New sign in ▼
English ▼
aws

You're using the new sign in UI

Learn more about the updates or change back legacy sign in at any time using the sign in dropdown in the upper right corner.

Keeping you secure

Your account is protected with **multi-factor authentication (MFA)** .

To finish signing in, enter the code from your MFA device below.

MFA code: 124562

Sign in
Sign in to a different account
Trouble signing in?
AI Use Case Explorer
Discover AI use cases, customer success stories, and expert-curated implementation plans
Explore now ›

next time, for signing in, MFA will be used

©2024 Amazon Web Services, Inc. or its affiliates. All rights reserved.