DEPARTMENT OF COMPUTER ENGINEERING

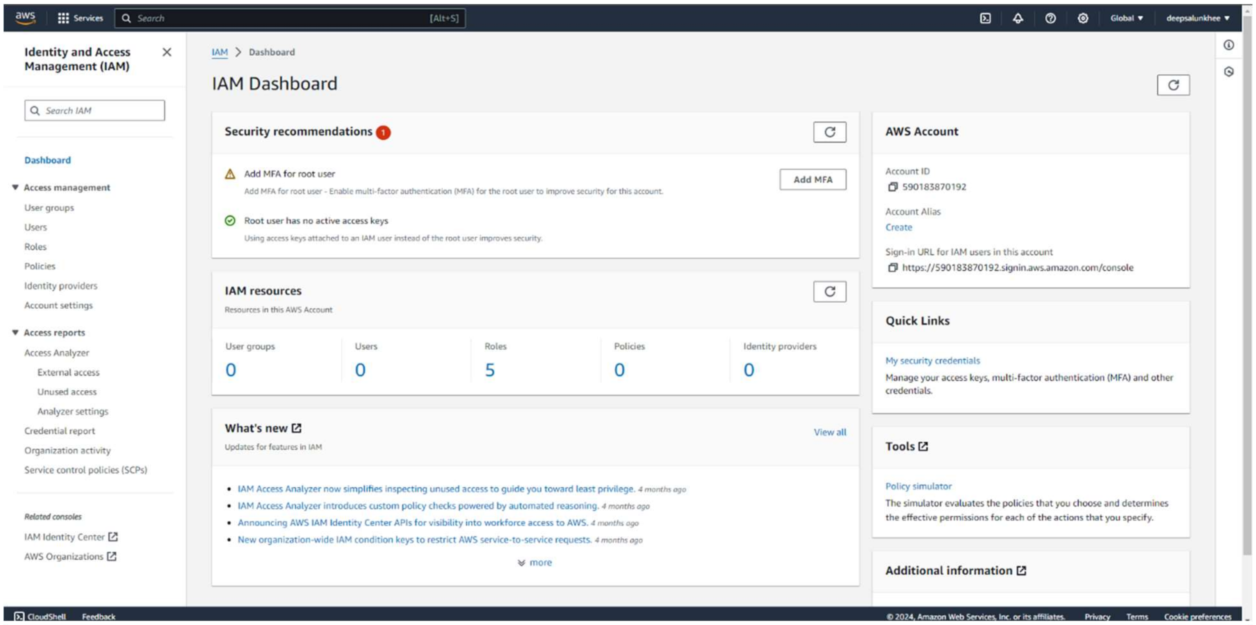
Semester	T.E. Semester VI – Computer Engineering
Subject	Cloud Computing
Subject Professor In-charge	Prof. Divya Nimbalkar
Assisting Teachers	Prof. Divya Nimbalkar

Student Name	Deep Salunkhe
Roll Number	21102A0014
TE Division	A

Title: Implementation of AWS IAM

Implementation:

Creation of IAM users and permission assignment. Check if the given permissions are effective



IAM Dashboard

Security recommendations 1

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.

Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources
Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	5	0	0

What's new
Updates for features in IAM

- IAM Access Analyzer now simplifies inspecting unused access to guide you toward least privilege. *4 months ago*
- IAM Access Analyzer introduces custom policy checks powered by automated reasoning. *4 months ago*
- Announcing AWS IAM Identity Center APIs for visibility into workforce access to AWS. *4 months ago*
- New organization-wide IAM condition keys to restrict AWS service-to-service requests. *4 months ago*

AWS Account

Account ID
590183870192

Account Alias
Create

Sign-in URL for IAM users in this account
https://590183870192.signin.aws.amazon.com/console

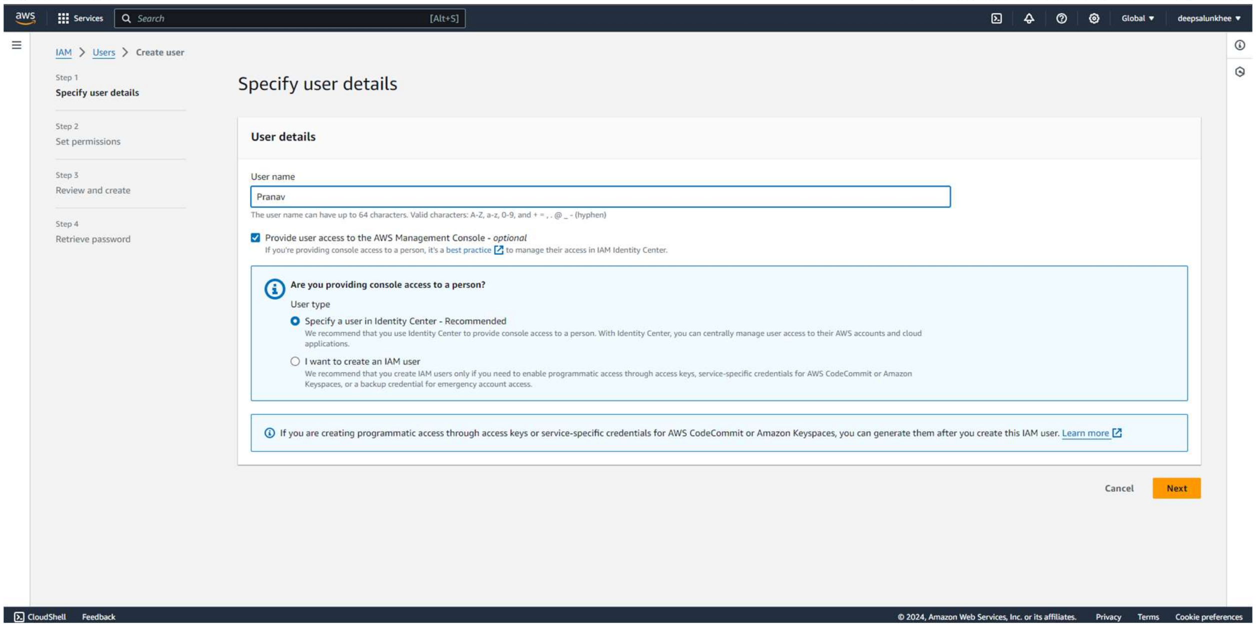
Quick Links

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.

Additional information



Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Specify user details

User details

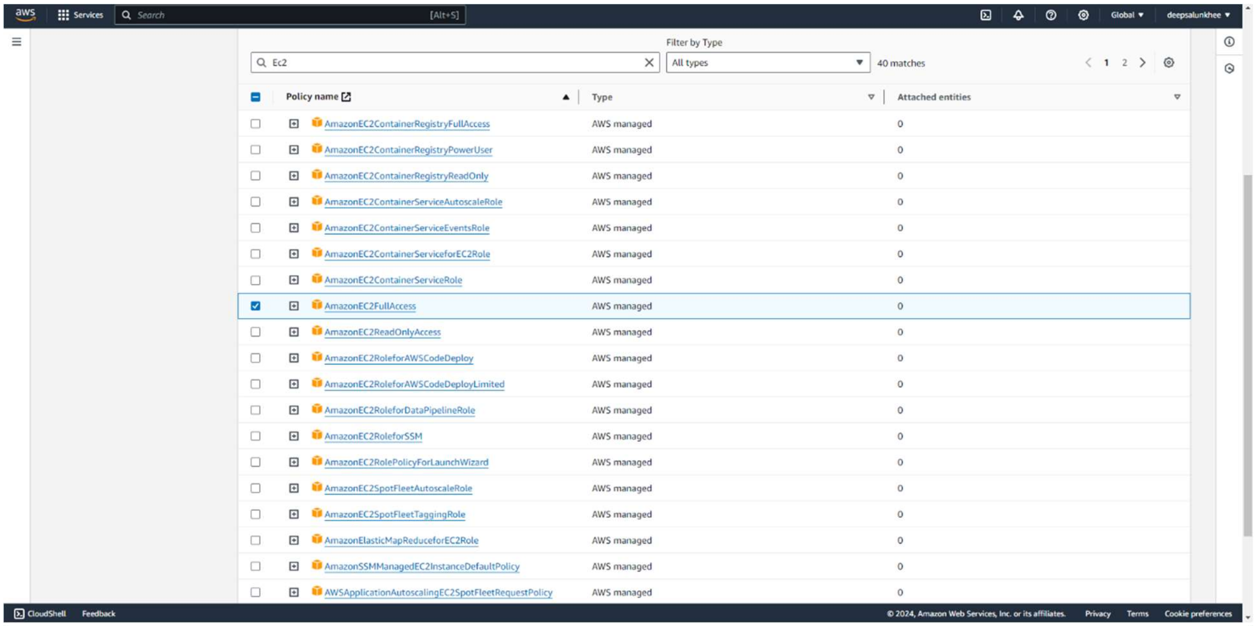
User name: Pranav

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.

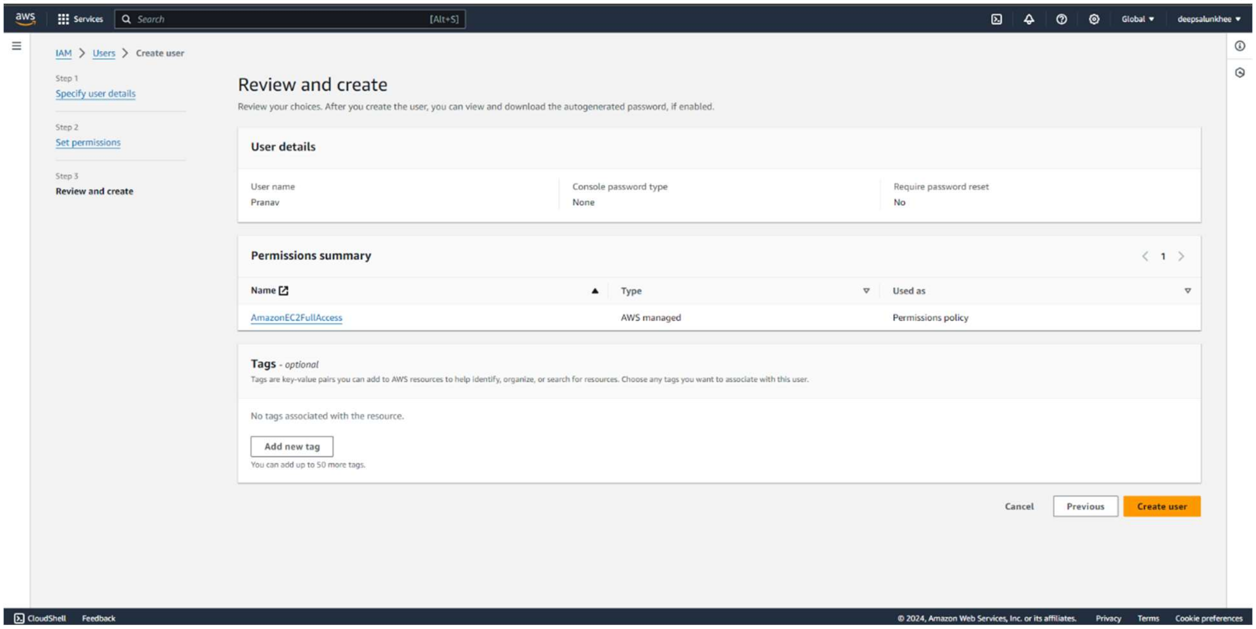
If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more



Filter by Type

Ec2 | All types | 40 matches | 1 2

☐	Policy name	Type	Attached entities
☐	AmazonEC2ContainerRegistryFullAccess	AWS managed	0
☐	AmazonEC2ContainerRegistryPowerUser	AWS managed	0
☐	AmazonEC2ContainerRegistryReadOnly	AWS managed	0
☐	AmazonEC2ContainerServiceAutoscaleRole	AWS managed	0
☐	AmazonEC2ContainerServiceEventsRole	AWS managed	0
☐	AmazonEC2ContainerServiceforEC2Role	AWS managed	0
☐	AmazonEC2ContainerServiceRole	AWS managed	0
☑	AmazonEC2FullAccess	AWS managed	0
☐	AmazonEC2ReadOnlyAccess	AWS managed	0
☐	AmazonEC2RoleforAWSCodeDeploy	AWS managed	0
☐	AmazonEC2RoleforAWSCodeDeployLimited	AWS managed	0
☐	AmazonEC2RoleforDataPipelineRole	AWS managed	0
☐	AmazonEC2RoleforSSM	AWS managed	0
☐	AmazonEC2RolePolicyForLaunchWizard	AWS managed	0
☐	AmazonEC2SpotFleetAutoscaleRole	AWS managed	0
☐	AmazonEC2SpotFleetTaggingRole	AWS managed	0
☐	AmazonElasticMapReduceforEC2Role	AWS managed	0
☐	AmazonSSMManagedEC2InstanceDefaultPolicy	AWS managed	0
☐	AWSApplicationAutoscalingEC2SpotFleetRequestPolicy	AWS managed	0



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
Pranav	None	No

Permissions summary

Name	Type	Used as
AmazonEC2FullAccess	AWS managed	Permissions policy

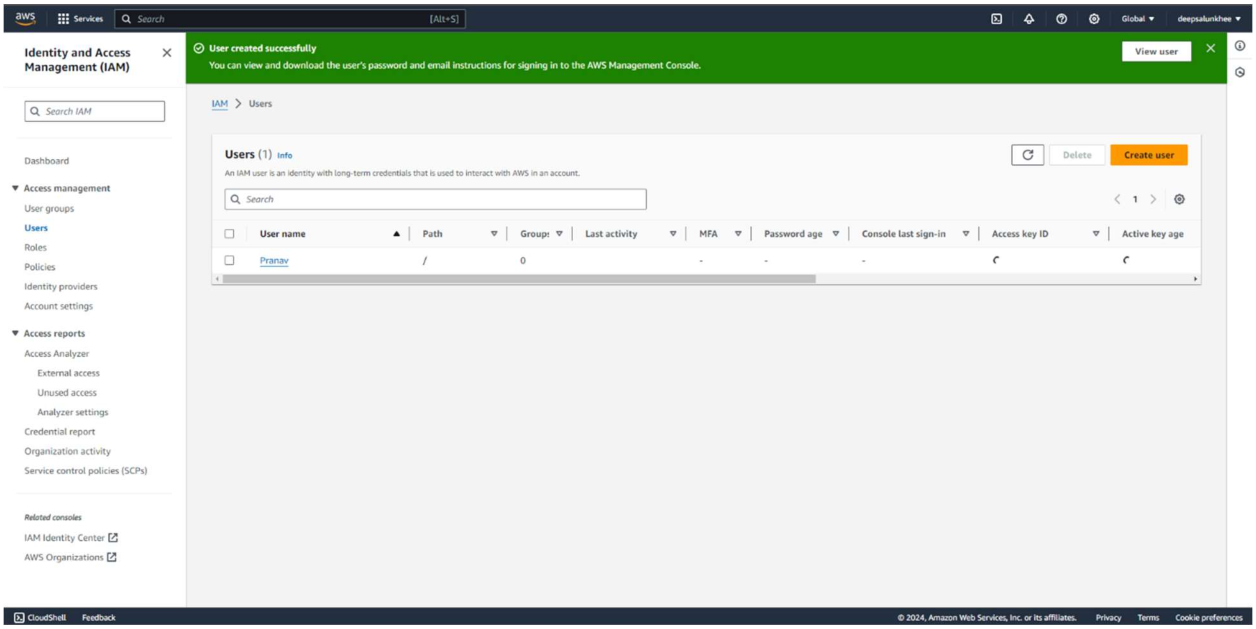
Tags - *optional*

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

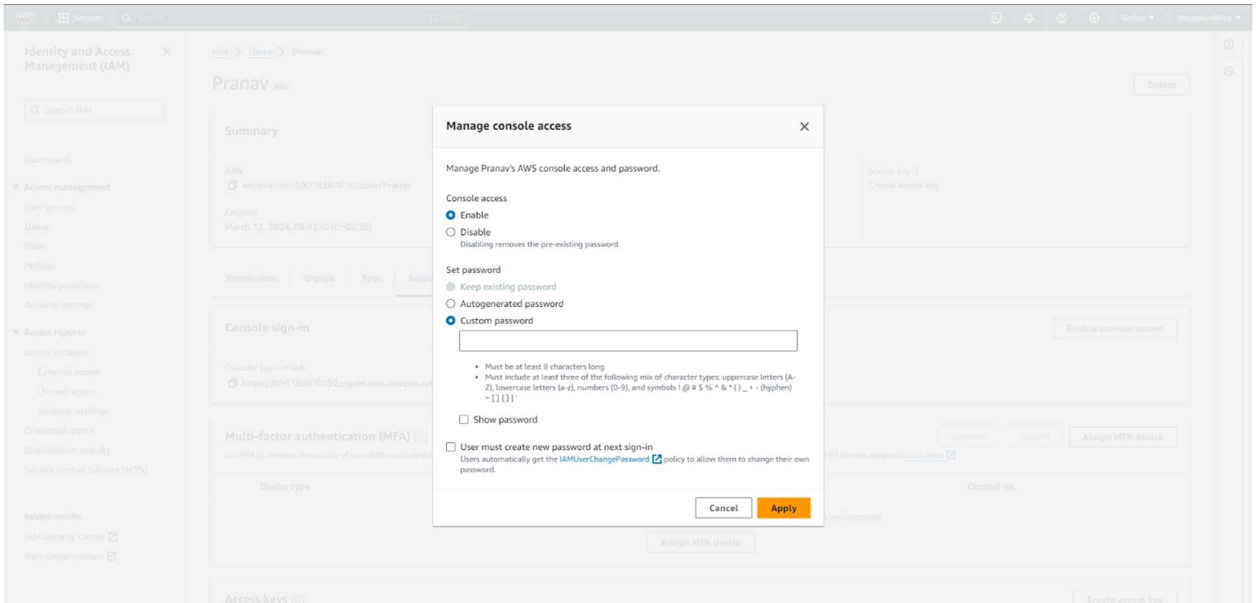
You can add up to 50 more tags.



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

Users (1)
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
□	Pranav	/	0		-	-	-		



Manage Pranav's AWS console access and password.

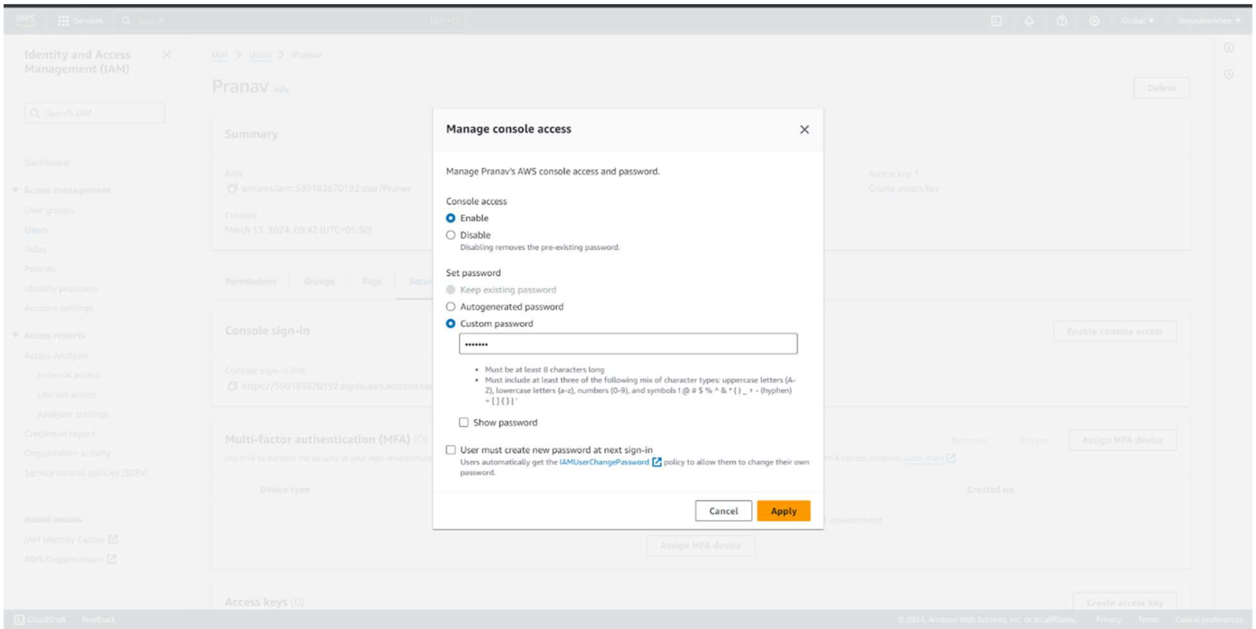
Console access
● Enable
○ Disable
Disabling removes the pre-existing password.

Set password
○ Keep existing password
○ Autogenerated password
● Custom password

- 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

□ User must create new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.



Manage console access

Manage Pranav's AWS console access and password.

Console access

● Enable

○ Disable

Disabling removes the pre-existing password.

Set password

○ Keep existing password

○ Autogenerated password

● Custom password

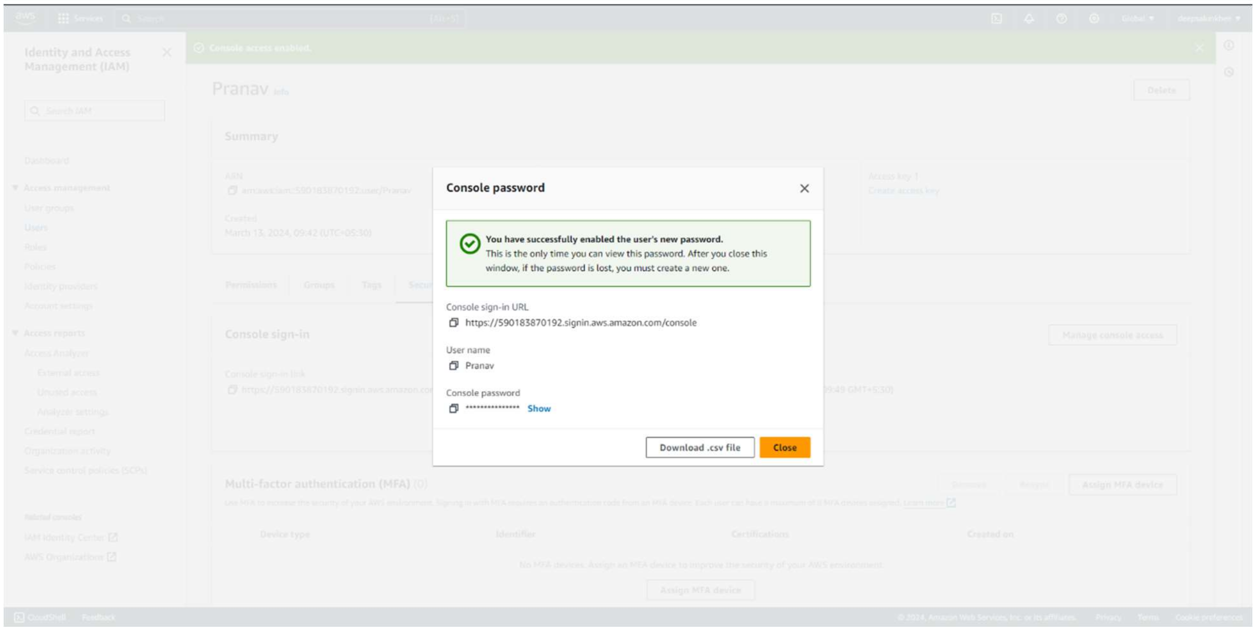
•••••••

- 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

□ User must create new password at next sign-in

Users automatically get the IAMUserChangePassword policy to allow them to change their own password.



Console access enabled.

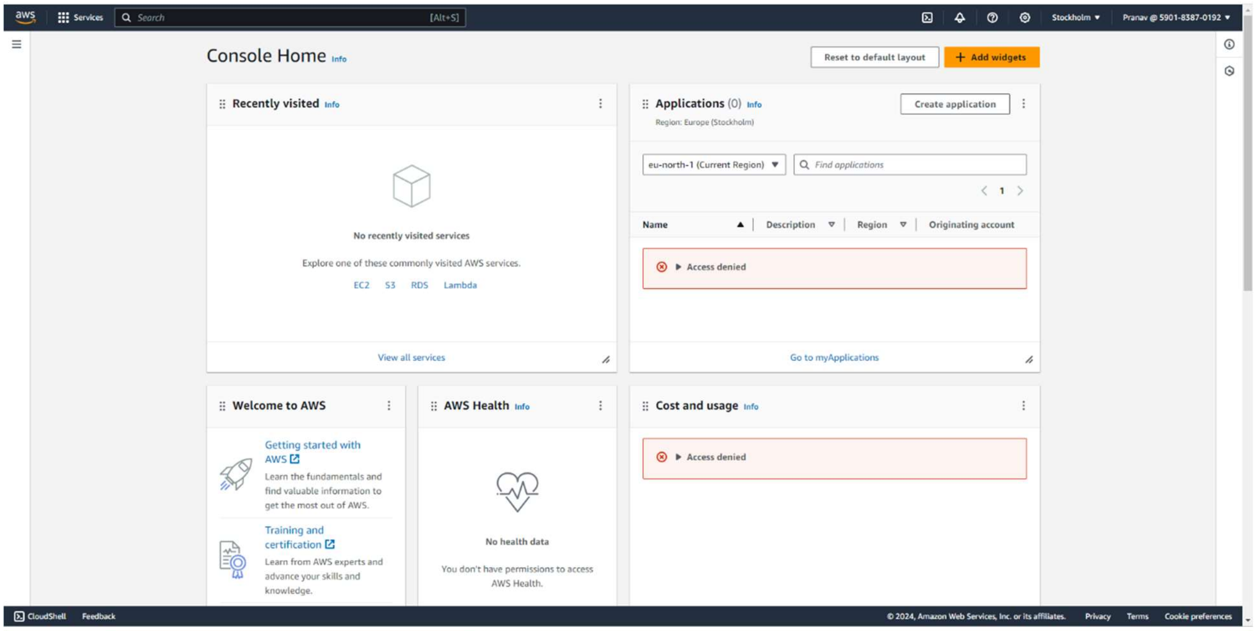
Console password

You have successfully enabled the user's new password.
This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.

Console sign-in URL
https://590183870192.signin.aws.amazon.com/console

User name
Pranav

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



No recently visited services

Explore one of these commonly visited AWS services.

Access denied

Learn the fundamentals and find valuable information to get the most out of AWS.

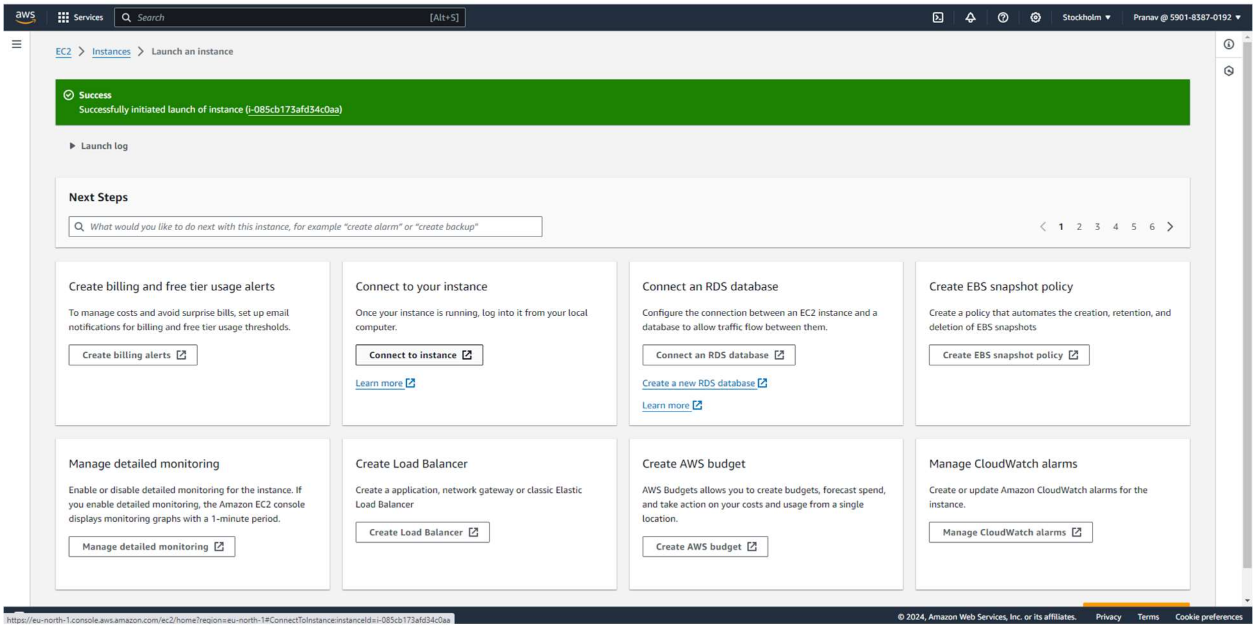
Learn from AWS experts and advance your skills and knowledge.

No health data

You don't have permissions to access AWS Health.

Access denied

© 2024, Amazon Web Services, Inc. or its affiliates.



Success
Successfully initiated launch of instance (i-085cb173afd34c0aa)

What would you like to do next with this instance, for example "create alarm" or "create backup"

Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.

Connect to your instance
Once your instance is running, log into it from your local computer.

Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.

Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots

Manage detailed monitoring
Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.

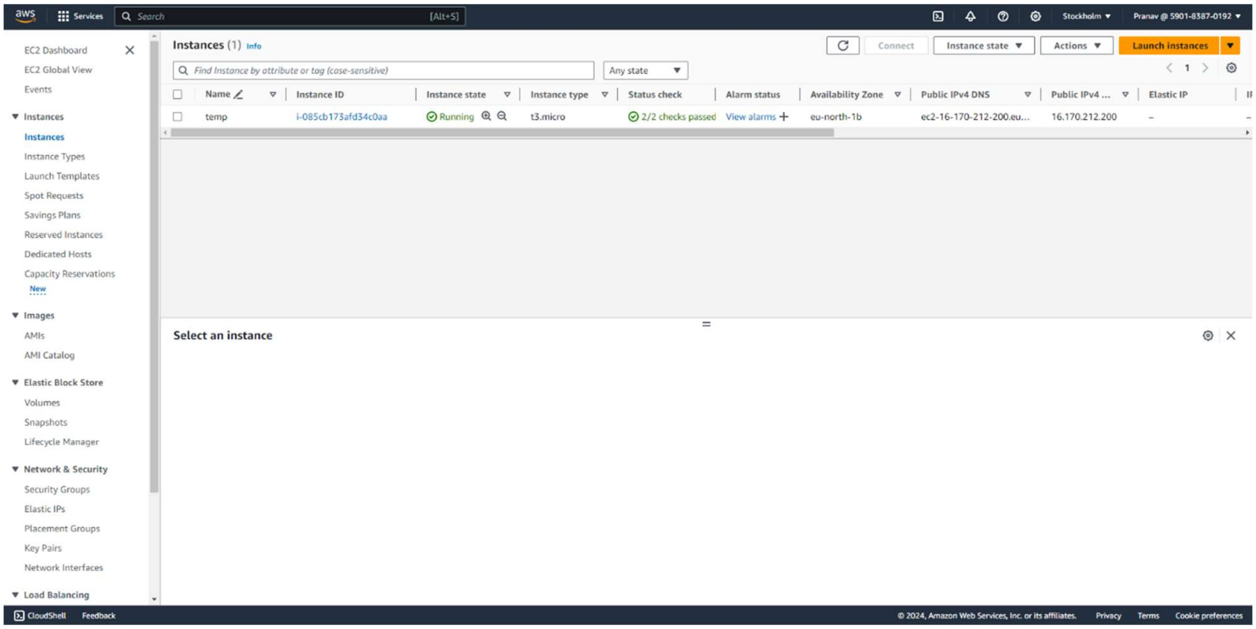
Create Load Balancer
Create a application, network gateway or classic Elastic Load Balancer

Create AWS budget
AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location.

Manage CloudWatch alarms
Create or update Amazon CloudWatch alarms for the instance.

https://eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#ConnectToInstance:instanceId=i-085cb173afd34c0aa

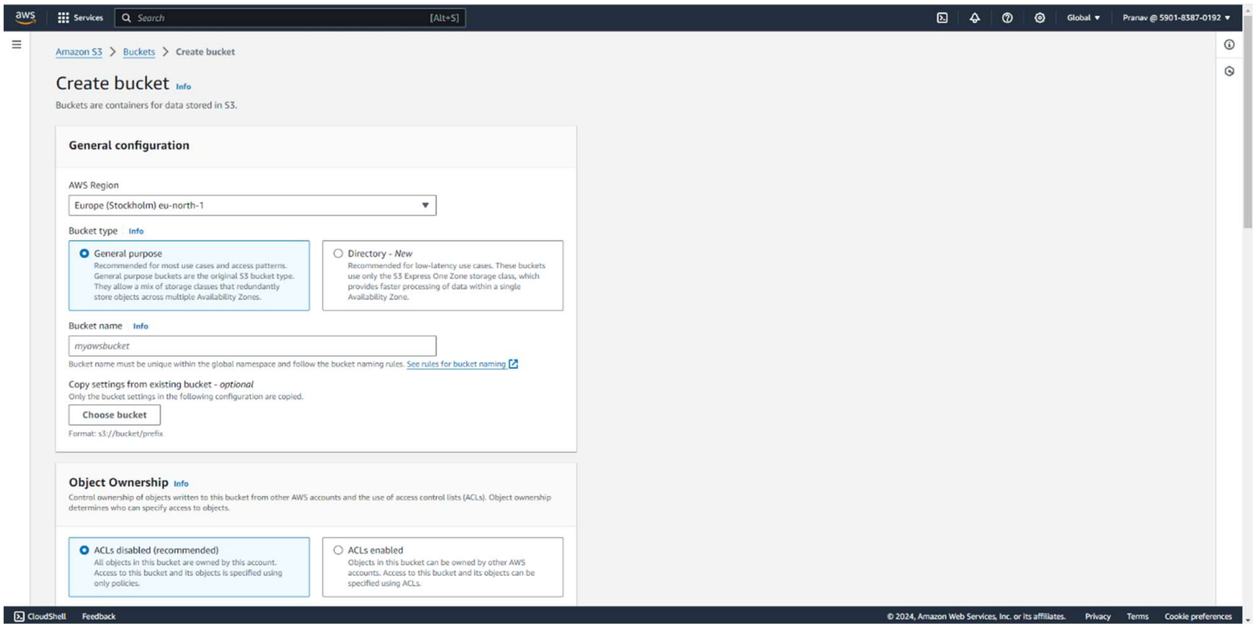
© 2024, Amazon Web Services, Inc. or its affiliates.



Instances (1) Info

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
□	temp	i-085cb173afd34c0aa	Running	t3.micro	2/2 checks passed	View alarms +	eu-north-1b	ec2-16-170-212-200.eu...	16.170.212.200	–

Select an instance



Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region: Europe (Stockholm) eu-north-1

Bucket type Info

● General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

○ Directory - *New*
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name Info: *myawsbucket*

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

Choose bucket

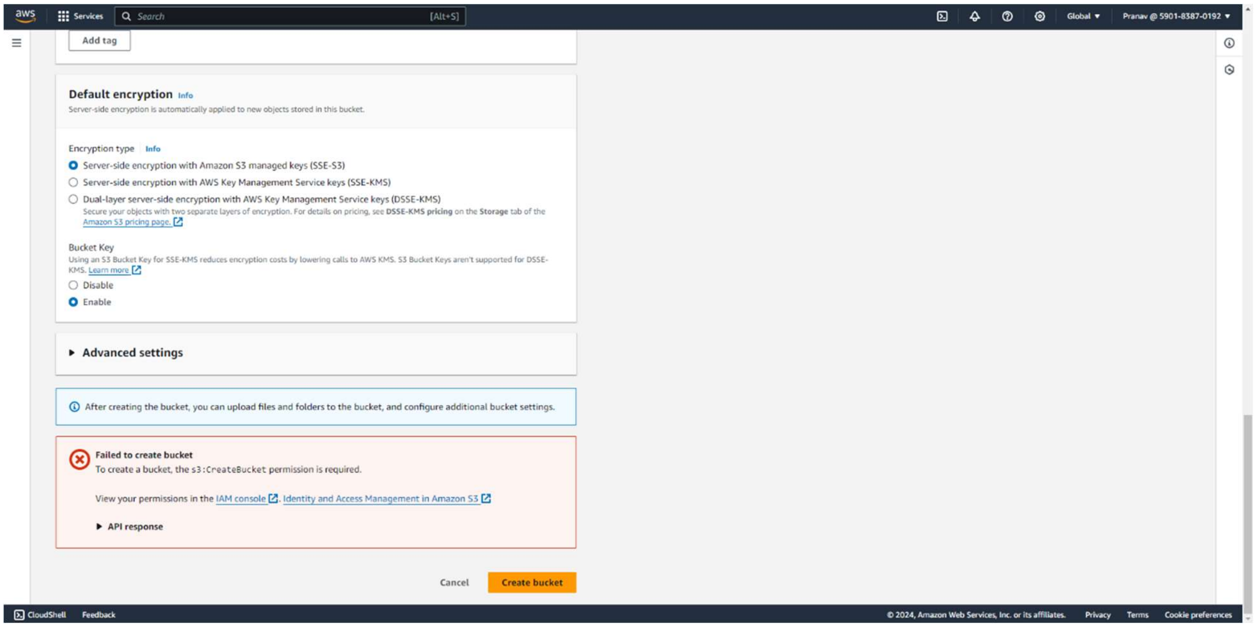
Format: s3://bucket/prefix

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

● ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

○ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.



Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type | Info

● Server-side encryption with Amazon S3 managed keys (SSE-S3)

○ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more

○ Disable

● Enable

▸ **Advanced settings**

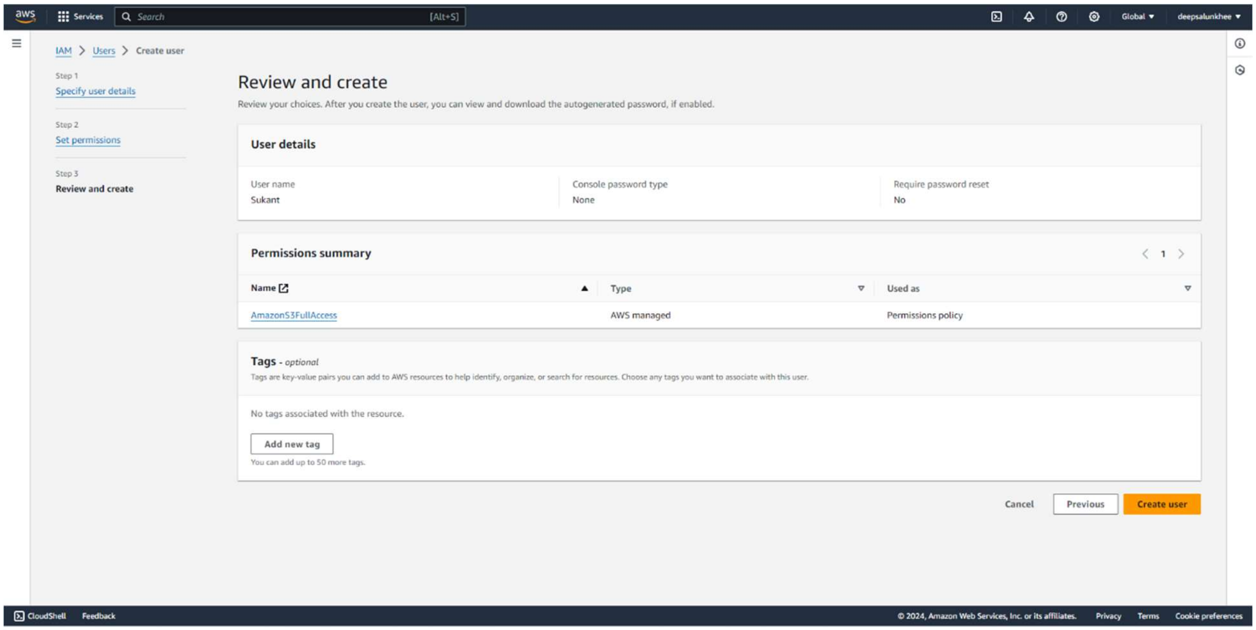
ⓘ After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

ⓧ **Failed to create bucket**
To create a bucket, the `s3:CreateBucket` permission is required.

View your permissions in the IAM console. Identity and Access Management in Amazon S3

▸ **API response**

Changing the authentication mechanism to change the password setting policy



IAM > Users > Create user

Step 1 Specify user details

Step 2 Set permissions

Step 3 Review and create

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
Sukant	None	No

Permissions summary

Name	Type	Used as
AmazonS3FullAccess	AWS managed	Permissions policy

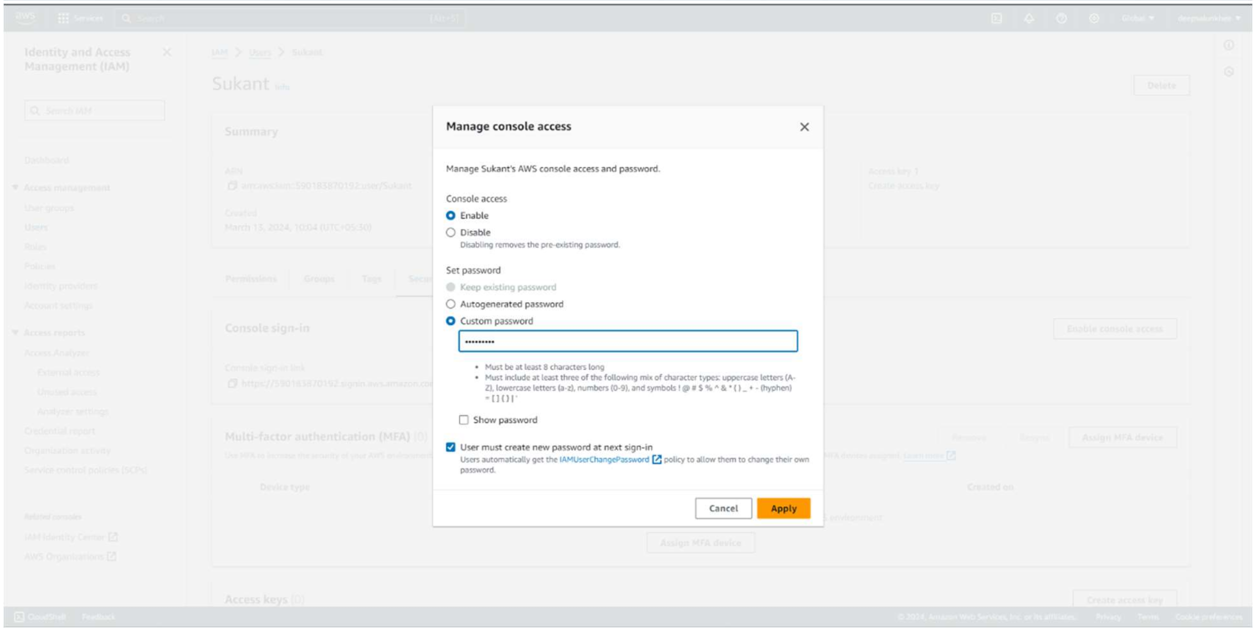
Tags - *optional*

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.



Manage console access

Manage Sukant's AWS console access and password.

Console access

● Enable

○ Disable
Disabling removes the pre-existing password.

Set password

○ Keep existing password

○ Autogenerated password

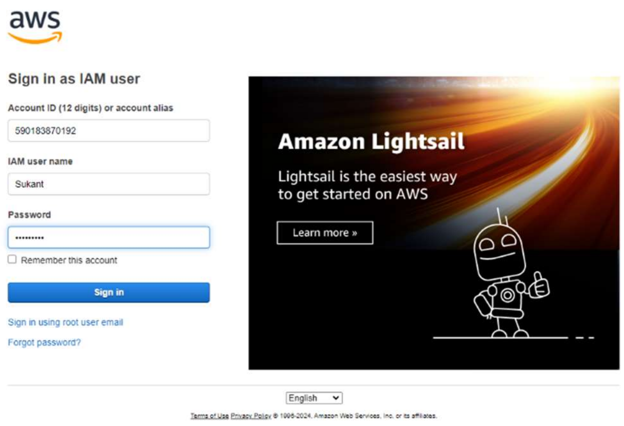
● Custom password

•••••••••

- 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

☑ User must create new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.



Sign in as IAM user

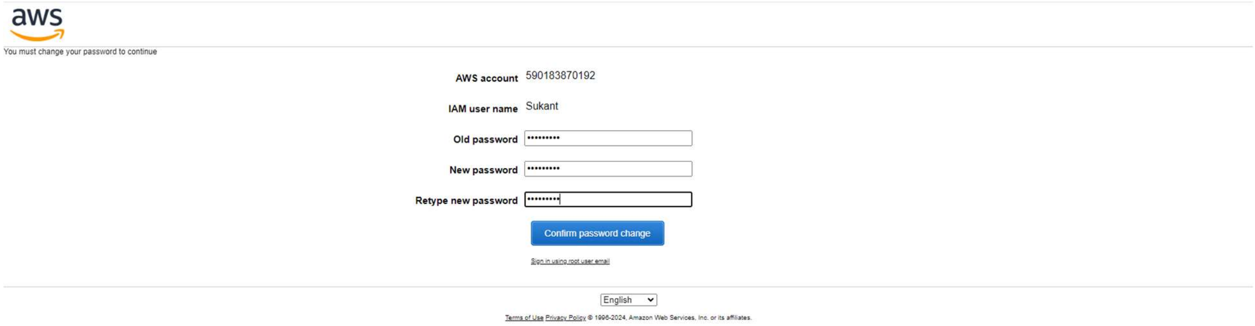
Account ID (12 digits) or account alias: 590183870192

IAM user name: Sukant

Password: •••••••••

☐ Remember this account

aws
Sign in
Sign in using root user email
Forgot password?
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »
English
Terms of Use Privacy Policy © 1996-2024, Amazon Web Services, Inc. or its affiliates.



You must change your password to continue

AWS account: 590183870192

IAM user name: Sukant

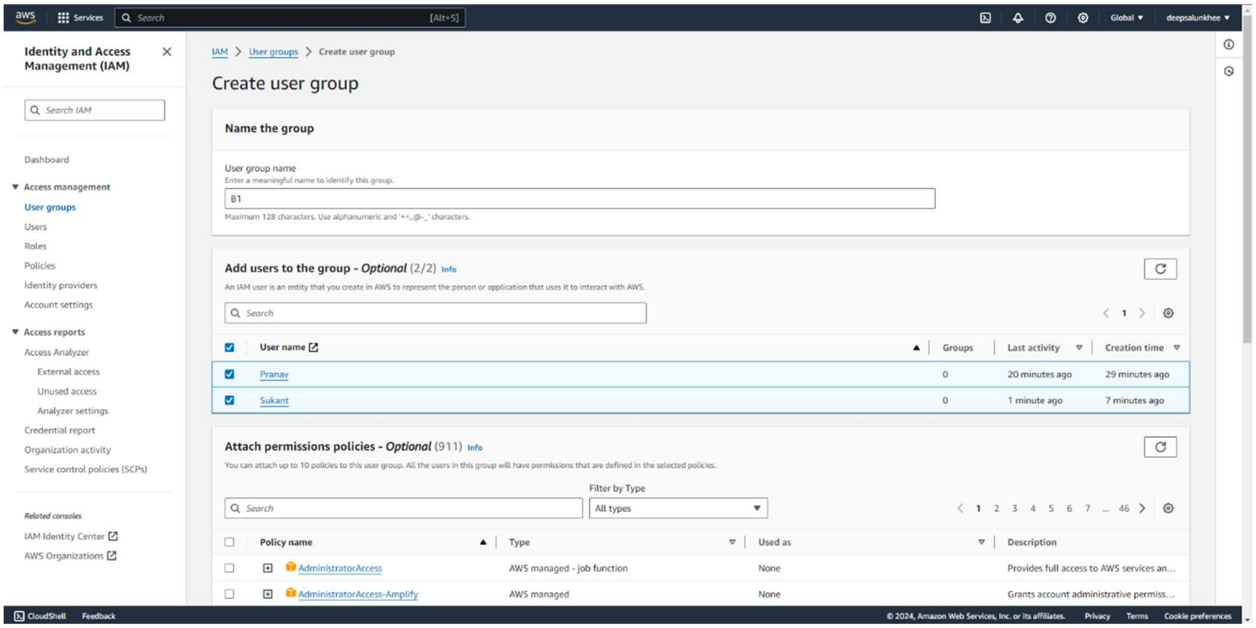
Old password: •••••••••

New password: •••••••••

Retype new password: •••••••••

aws
Confirm password change
Sign in using root user email
English
Terms of Use Privacy Policy © 1996-2024, Amazon Web Services, Inc. or its affiliates.

- Creation of User group and assignment of permission through user group



IAM > User groups > Create user group

Create user group

Name the group

User group name
Enter a meaningful name to identify this group.
B1
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (2/2) 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
☑	Pranav	0	20 minutes ago	29 minutes ago
☑	Sukant	0	1 minute ago	7 minutes ago

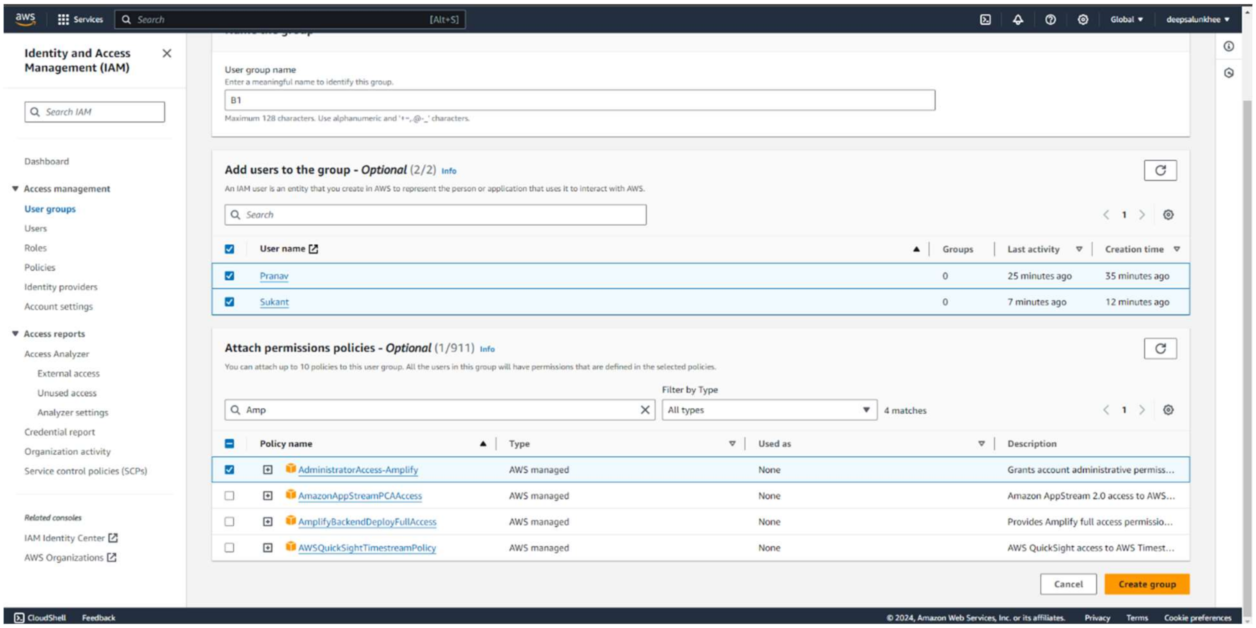
Attach permissions policies - *Optional* (911) Info

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

< 1 2 3 4 5 6 7 ... 46 >

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



User group name
Enter a meaningful name to identify this group.
B1
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (2/2) 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
☑	Pranav	0	25 minutes ago	35 minutes ago
☑	Sukant	0	7 minutes ago	12 minutes ago

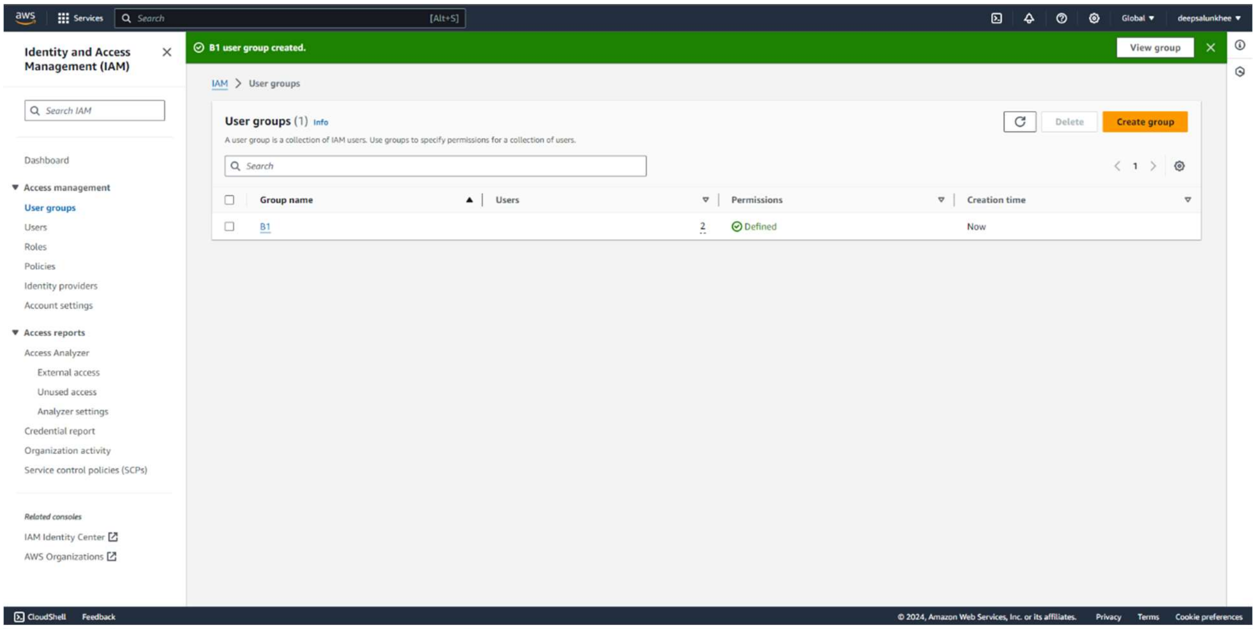
Attach permissions policies - *Optional* (1/911) Info

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: Amp
Filter by Type: All types
4 matches

▬	Policy name	Type	Used as	Description
☑	AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permiss...
□	AmazonAppStreamPCAAccess	AWS managed	None	Amazon AppStream 2.0 access to AWS...
□	AmplifyBackendDeployFullAccess	AWS managed	None	Provides Amplify full access permissio...
□	AWSQuickSightTimestreamPolicy	AWS managed	None	AWS QuickSight access to AWS Timest...

Cancel | Create group

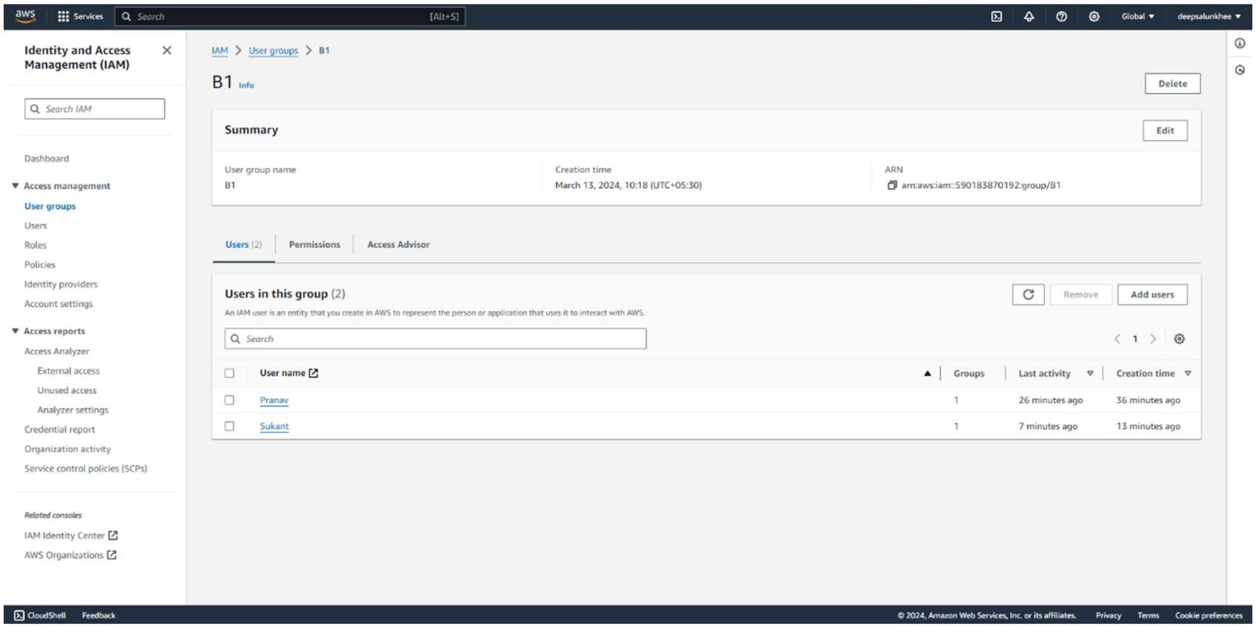


B1 user group created.

User groups (1) Info

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
□	B1	2	Defined	Now



B1 Info

Summary

User group name: B1

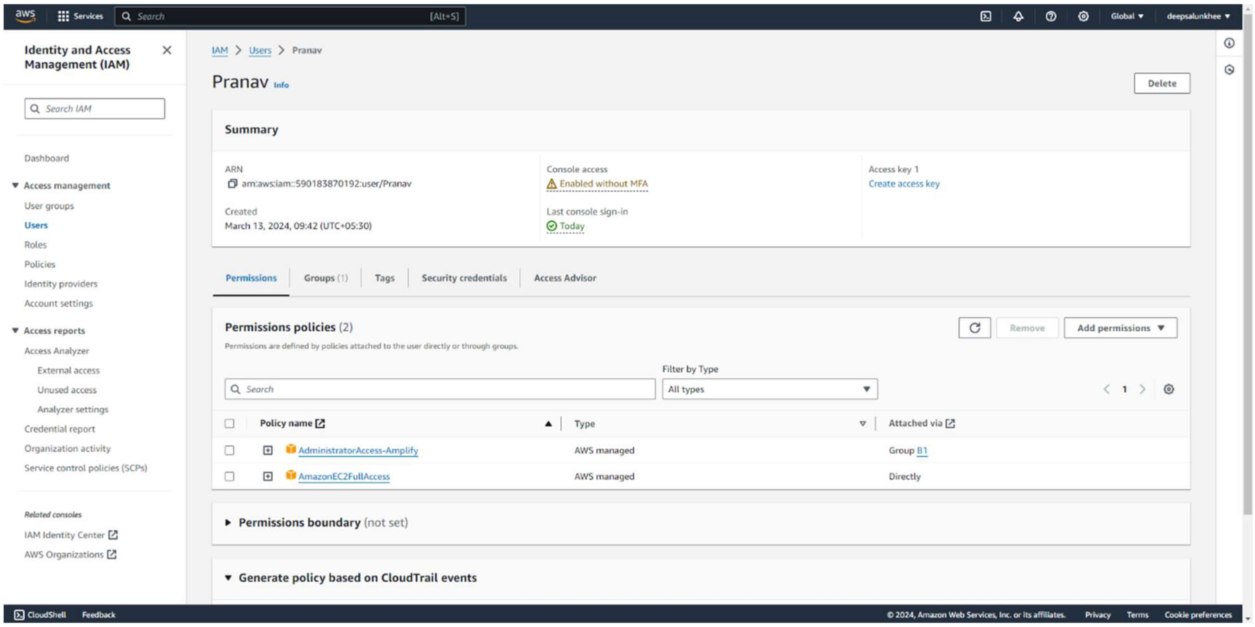
Creation time: March 13, 2024, 10:18 (UTC+05:30)

ARN: arn:aws:iam::590183870192:group/B1

Users in this group (2)

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
□	Pranav	1	26 minutes ago	36 minutes ago
□	Sukant	1	7 minutes ago	13 minutes ago



Pranav

Summary

ARN
arn:aws:iam::590183870192:user/Pranav

Created
March 13, 2024, 09:42 (UTC+05:30)

Console access
Enabled without MFA

Last console sign-in
Today

Access key 1
Create access key

Permissions policies (2)

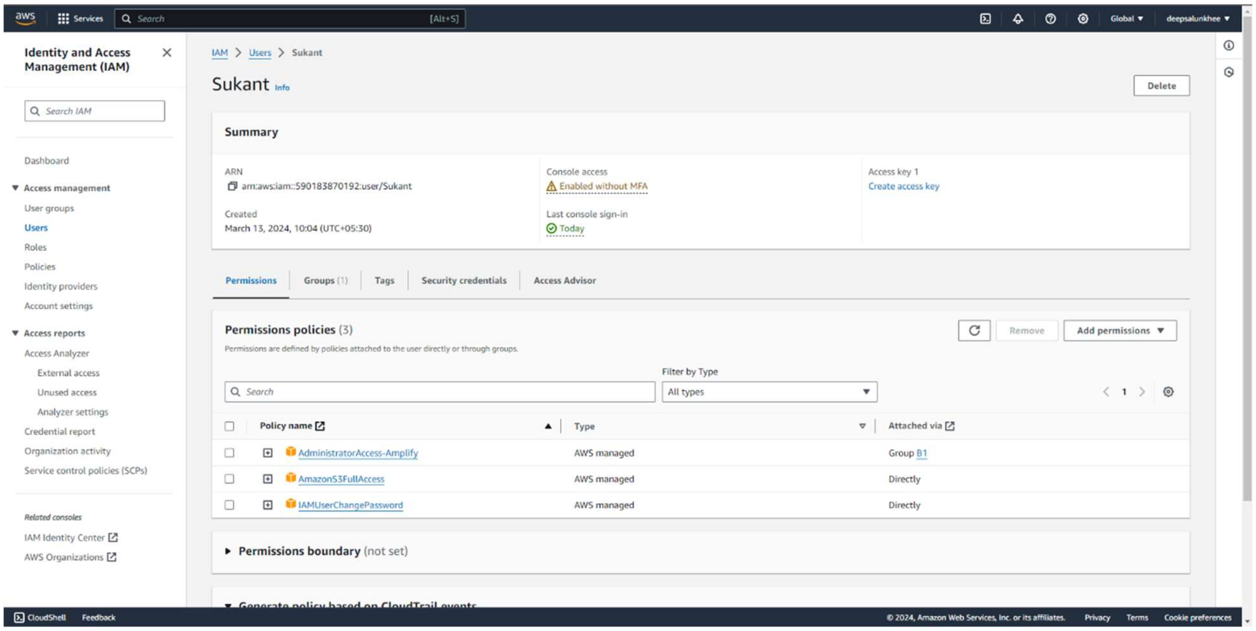
Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: All types

Policy name	Type	Attached via
AdministratorAccess-Amplify	AWS managed	Group B1
AmazonEC2FullAccess	AWS managed	Directly

▸ Permissions boundary (not set)

▾ Generate policy based on CloudTrail events



Sukant

Summary

ARN
arn:aws:iam::590183870192:user/Sukant

Created
March 13, 2024, 10:04 (UTC+05:30)

Console access
Enabled without MFA

Last console sign-in
Today

Access key 1
Create access key

Permissions policies (3)

Permissions are defined by policies attached to the user directly or through groups.

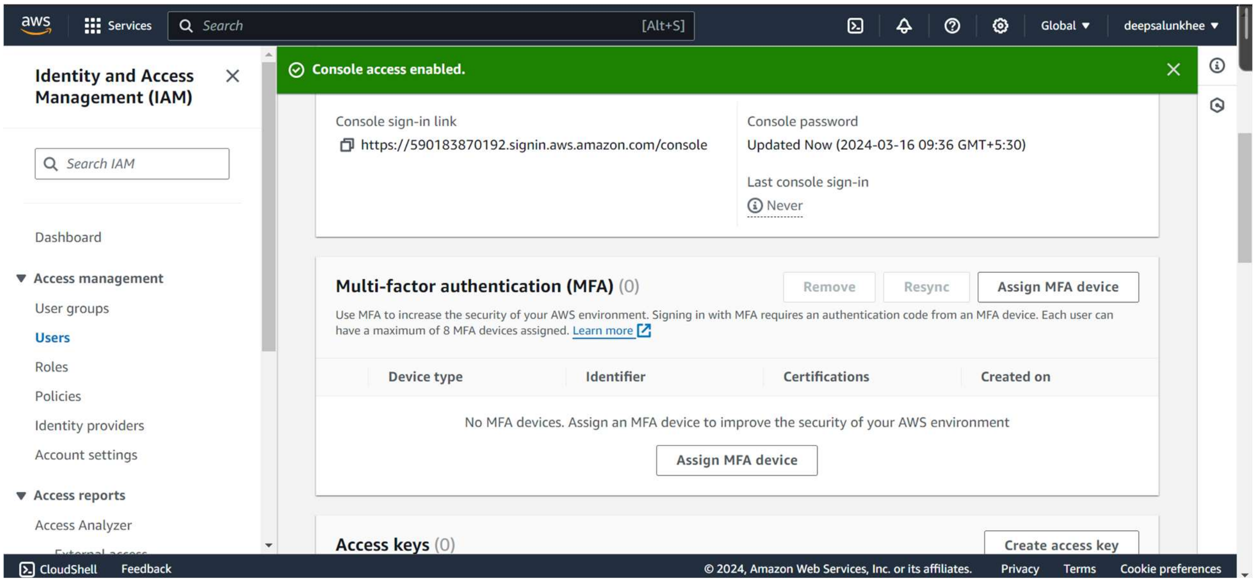
Filter by Type: All types

Policy name	Type	Attached via
AdministratorAccess-Amplify	AWS managed	Group B1
AmazonS3FullAccess	AWS managed	Directly
IAMUserChangePassword	AWS managed	Directly

▸ Permissions boundary (not set)

▾ Generate policy based on CloudTrail events

Changing the authentication mechanism to enable Multifactor authentication



Console access enabled.

Console sign-in link
https://590183870192.signin.aws.amazon.com/console

Console password
Updated Now (2024-03-16 09:36 GMT+5:30)

Last console sign-in
Never

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

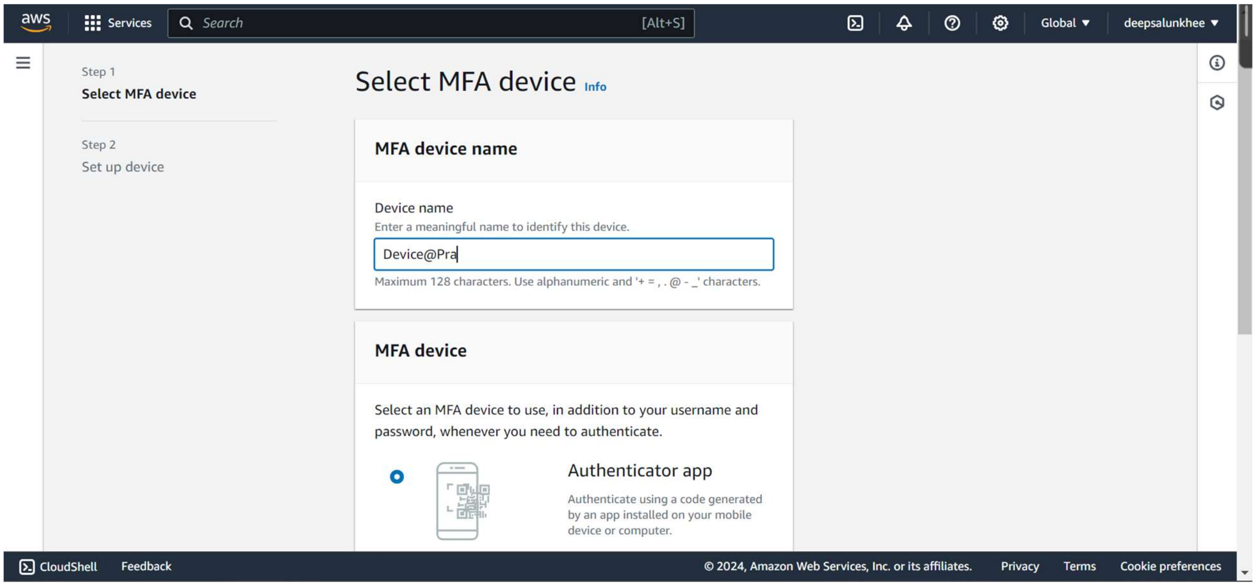
Device type	Identifier	Certifications	Created on

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

Assign MFA device

Access keys (0)

Create access key



Select MFA device Info

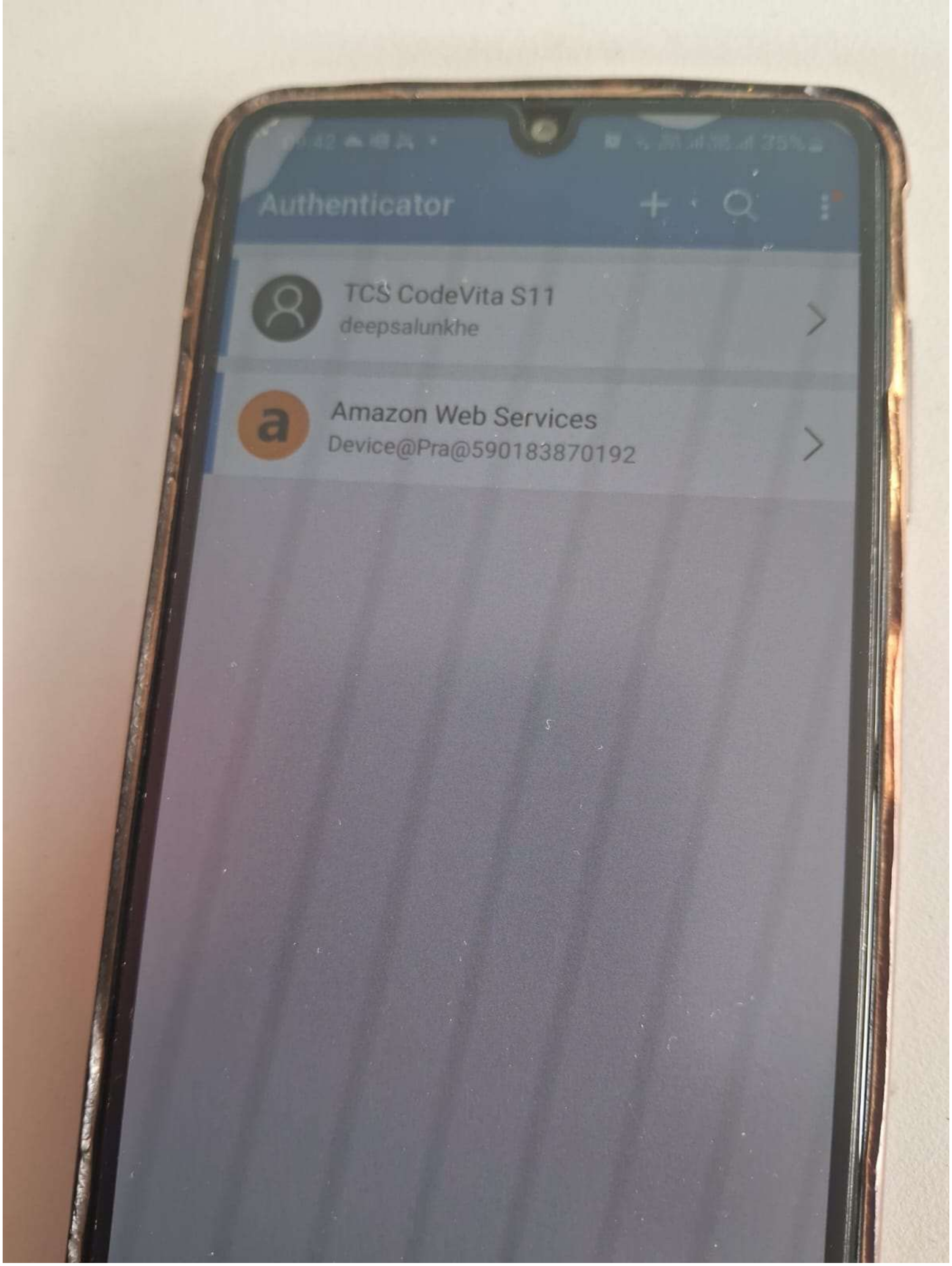
MFA device name

Device name
Enter a meaningful name to identify this device.
Device@Pra
Maximum 128 characters. Use alphanumeric and '+ = , . @ - _' characters.

MFA device

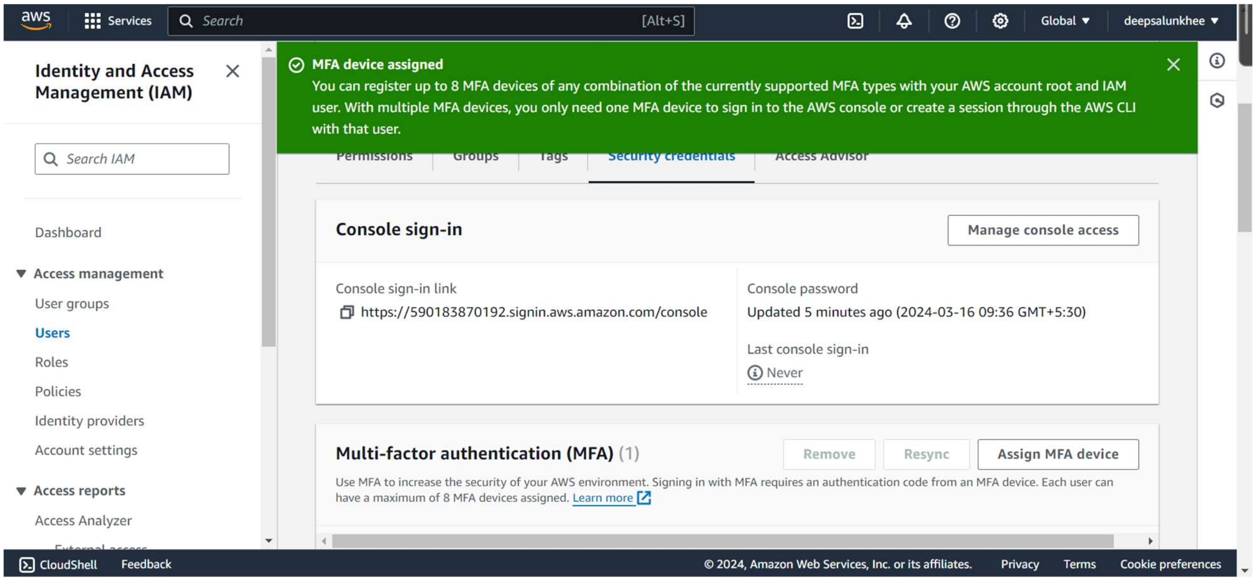
Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.

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



TCS CodeVita S11
deepsalunkhe

Amazon Web Services
Device@Pra@590183870192



MFA device assigned

You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. 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.

Console sign-in

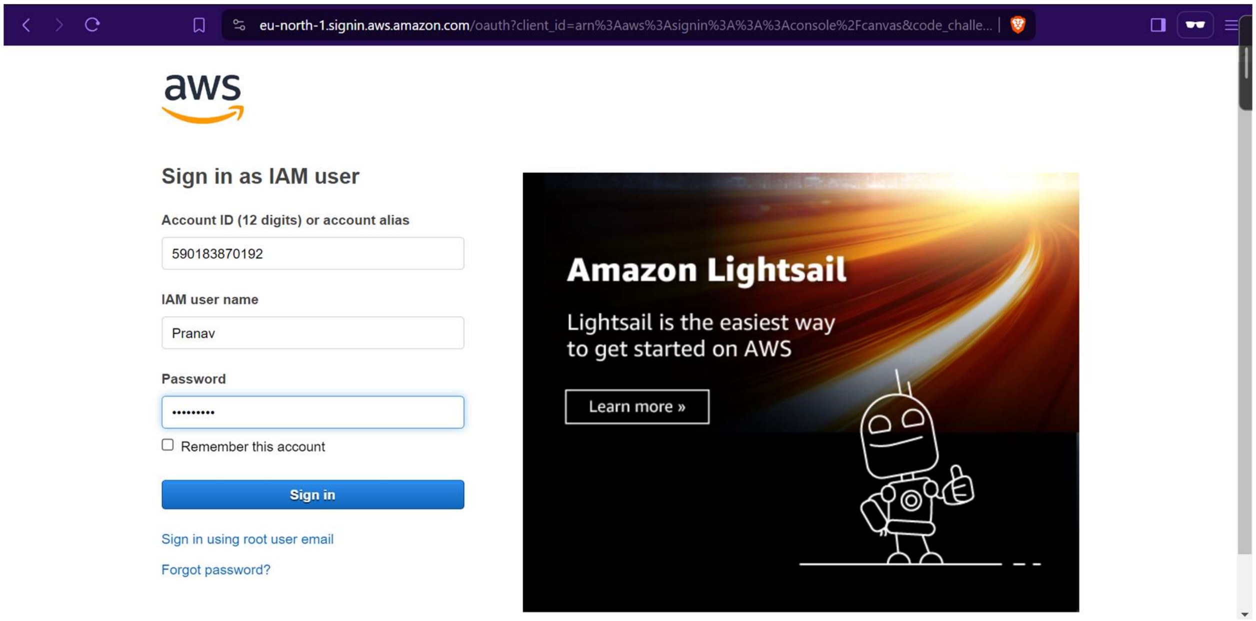
Console sign-in link
https://590183870192.signin.aws.amazon.com/console

Console password
Updated 5 minutes ago (2024-03-16 09:36 GMT+5:30)

Last console sign-in
Never

Multi-factor authentication (MFA) (1)

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



eu-north-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challe...
aws
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »

Sign in as IAM user

Account ID (12 digits) or account alias
590183870192

IAM user name
Pranav

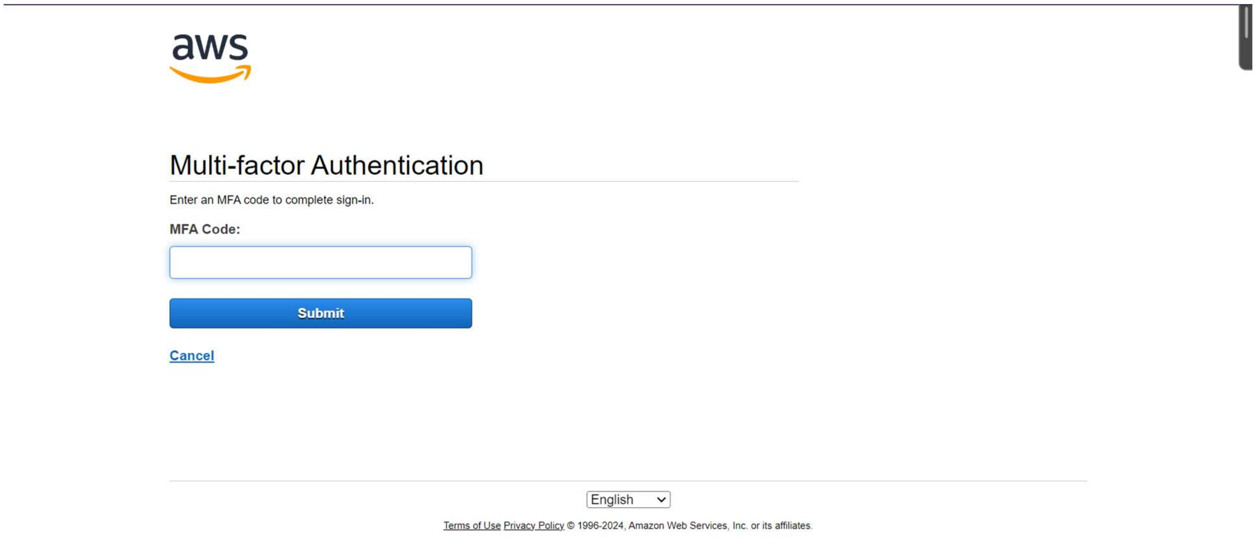
Password
•••••••••

□ Remember this account

Sign in

Sign in using root user email

Forgot password?

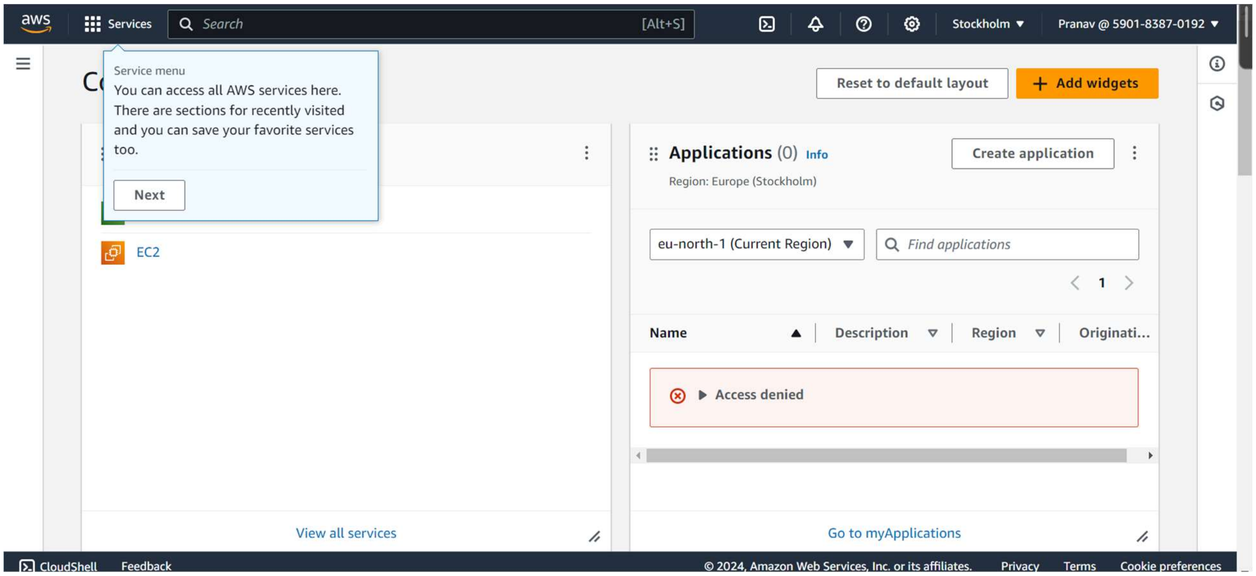


Multi-factor Authentication

Enter an MFA code to complete sign-in.

MFA Code:

Terms of Use Privacy Policy © 1996-2024, Amazon Web Services, Inc. or its affiliates.



Service menu

You can access all AWS services here. There are sections for recently visited and you can save your favorite services too.

Applications (0)

Region: Europe (Stockholm)

eu-north-1 (Current Region)

Name ▲	Description ▽	Region ▽	Originati...
Access denied			

© 2024, Amazon Web Services, Inc. or its affiliates.