

Identity and Access Management (IAM) Dashboard

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access Analyzer
- External access
- Unused access

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.  
[Add MFA](#)
- Root user has no active access keys  
Using access keys attached to an IAM user instead of the root user improves security.

AWS Account

Account ID  
339712971313

Account Alias  
[Create](#)

Sign-in URL for IAM users in this account  
<https://339712971313.signin.aws.amazon.com/console>

Quick Links

[My security credentials](#)  
Manage your access keys, multi-factor

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	4	0	0

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Identity and Access Management (IAM) Create user group

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access Analyzer
- External access
- Unused access

Create user group

Name the group

User group name  
Enter a meaningful name to identify this group.  
  
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.

< 1 > ⚙

User name	Groups	Last activity	Creation time
No resources to display			

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access Analyzer
- External access
- Unused access

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 30 matches

	Policy name	Type	Used as	Description
<input type="checkbox"/>	AmazonEC2Contai...	AWS managed	None	Provides administrative access to Amazon EC2
<input type="checkbox"/>	AmazonEC2Contai...	AWS managed	None	Provides full access to Amazon EC2
<input type="checkbox"/>	AmazonEC2Contai...	AWS managed	None	Provides read-only access to Amazon EC2
<input type="checkbox"/>	AmazonEC2Contai...	AWS managed	None	Policy to enable Task Autoscaling for Amazon EC2
<input type="checkbox"/>	AmazonEC2Contai...	AWS managed	None	Policy to enable CloudWatch Events for Amazon EC2
<input type="checkbox"/>	AmazonEC2Contai...	AWS managed	None	Default policy for the Amazon EC2
<input type="checkbox"/>	AmazonEC2Contai...	AWS managed	None	Default policy for Amazon ECS service
<input checked="" type="checkbox"/>	AmazonEC2FullAcc...	AWS managed	None	Provides full access to Amazon EC2
<input type="checkbox"/>	AmazonEC2ReadO...	AWS managed	None	Provides read only access to Amazon EC2
<input type="checkbox"/>	AmazonEC2Rolefo...	AWS managed	None	Provides EC2 access to S3 bucket to

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access Analyzer
- External access
- Unused access

Developer user group created. View group

IAM > User groups

User groups (1) Info

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

Search

	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	Developer	0	Loading	Now

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access Analyzer
- External access
- Unused access

Developer user group created.

View group

<input type="checkbox"/>	AmazonEC2Contai...	AWS managed	None	Provides read-only access to Amazon
<input type="checkbox"/>	AmazonEC2Contai...	AWS managed	None	Policy to enable Task Autoscaling fo
<input type="checkbox"/>	AmazonEC2Contai...	AWS managed	None	Policy to enable CloudWatch Events
<input type="checkbox"/>	AmazonEC2Contai...	AWS managed	None	Default policy for the Amazon EC2 F
<input type="checkbox"/>	AmazonEC2Contai...	AWS managed	None	Default policy for Amazon ECS servi
<input type="checkbox"/>	AmazonEC2FullAcc...	AWS managed	Permissions policy (1)	Provides full access to Amazon EC2
<input checked="" type="checkbox"/>	AmazonEC2ReadQ...	AWS managed	None	Provides read only access to Amazon
<input type="checkbox"/>	AmazonEC2Rolefo...	AWS managed	None	Provides EC2 access to S3 bucket to
<input type="checkbox"/>	AmazonEC2Rolefo...	AWS managed	None	Provides EC2 limited access to S3 bu
<input type="checkbox"/>	AmazonEC2Rolefo...	AWS managed	None	Default policy for the Amazon EC2 F
<input type="checkbox"/>	AmazonEC2Rolefo...	AWS managed	None	This policy will soon be deprecated.
<input type="checkbox"/>	AmazonEC2RolePo...	AWS managed	None	Managed policy for the Amazon Lau
<input type="checkbox"/>	AmazonEC2SpotFl...	AWS managed	None	Policy to enable Autoscaling for Am

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access Analyzer
- External access
- Unused access

Operation user group created.

View group

IAM > User groups

User groups (2) Info

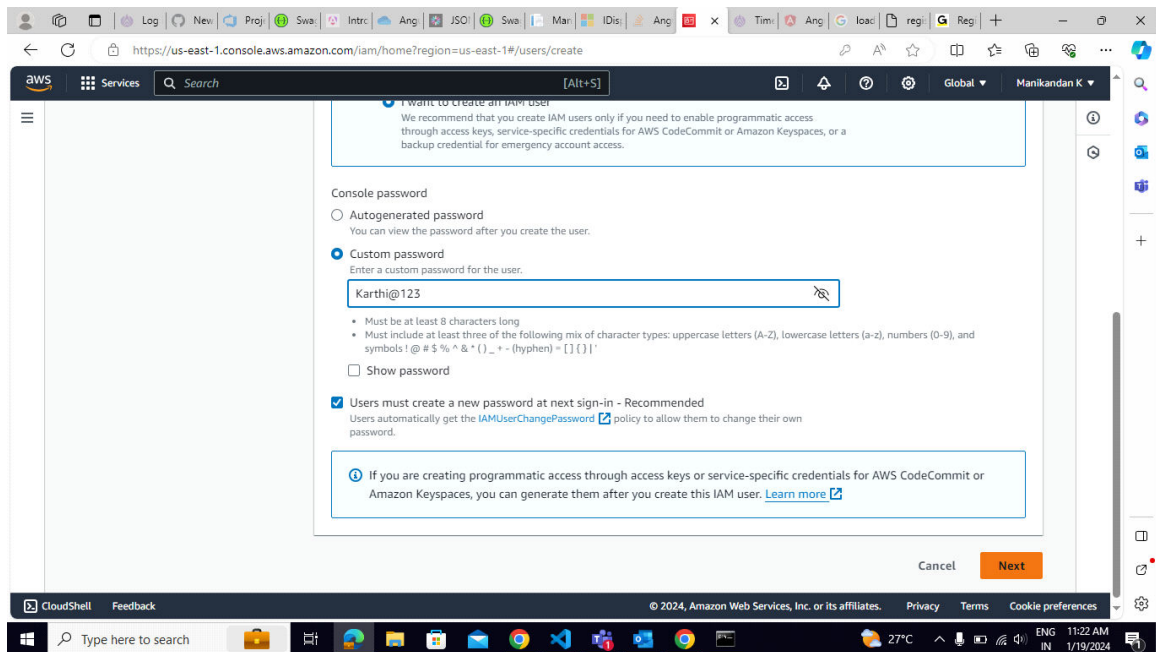
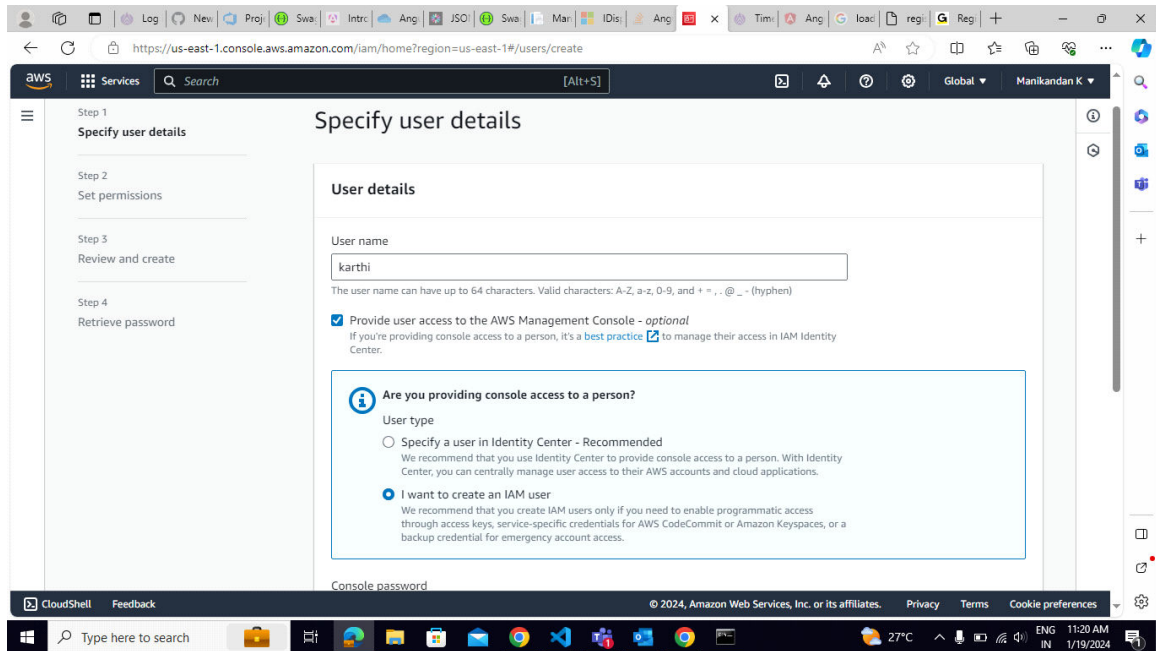
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Search

< 1 >

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	Developer	Loading	Loading	1 minute ago
<input type="checkbox"/>	Operation	Loading	Loading	Now

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



Step 3  
Review and create

Step 4  
Retrieve password

☒ 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)

< 1 > ⚙

<input checked="" type="checkbox"/>	Group name	Users	Attached policies	Created
<input checked="" type="checkbox"/>	<a href="#">Developer</a>	0	<a href="#">AmazonEC2FullAccess</a>	2024-01-19 (3 mi...)
<input type="checkbox"/>	<a href="#">Operation</a>	0	<a href="#">AmazonEC2ReadOnlyA...</a>	2024-01-19 (2 mi...)

▶ Set permissions boundary - optional

Cancel Previous Next

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 1  
Specify user details

Step 2  
Set permissions

Step 3  
Review and create

Step 4  
Retrieve password

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

IAM > Users > Create 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

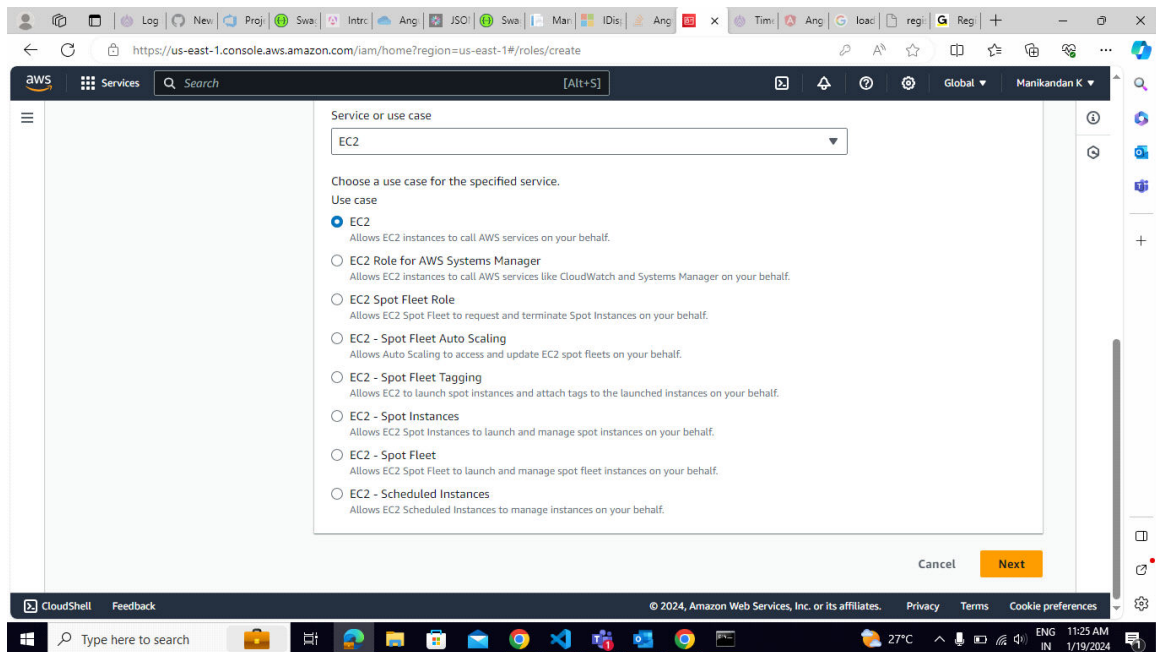
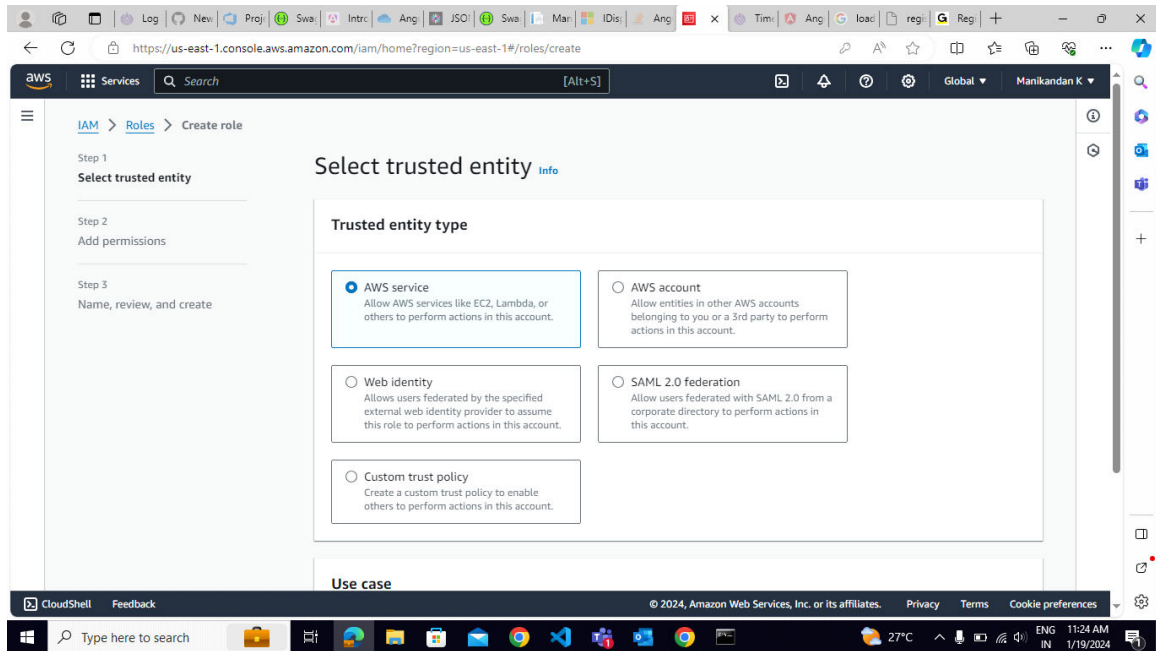
Console sign-in URL  
<https://339712971313.signin.aws.amazon.com/console>

User name  
karthi

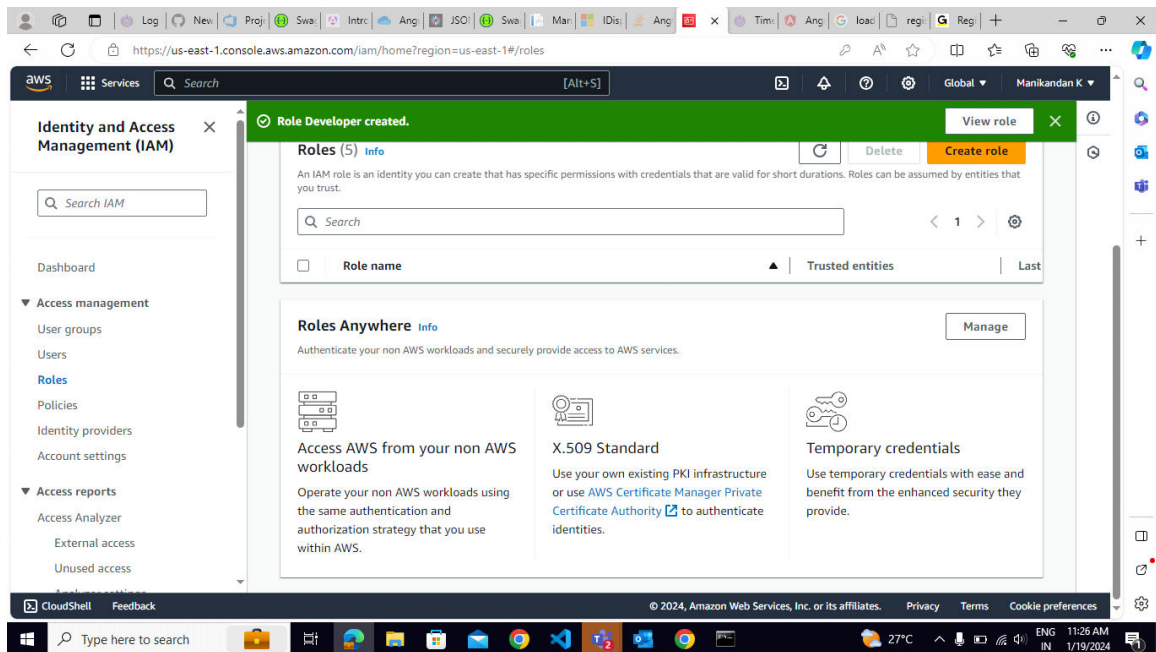
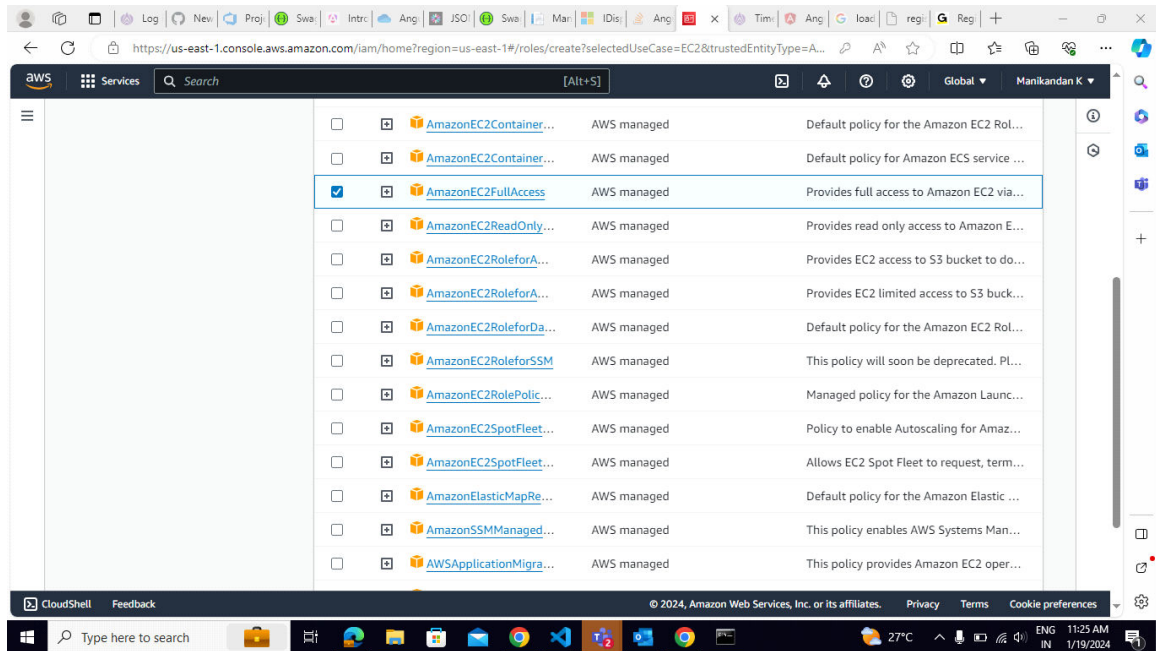
Console password  
\*\*\*\*\* Show

Cancel Download .csv file Return to users list

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences







LogNewProjSwaIntrcAngJSOSwaMarIDistAng

TimAngloacregReg

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

ServicesSearch[Alt+S]

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

IAM > Roles

Roles (5) Info

RefreshDeleteCreate role

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

☐

Role name

Trusted entities

Last

☐

[AWSServiceRoleForRDS](#)

AWS Service: rds (Service-Linked Rol

28 m

☐

[AWSServiceRoleForSupport](#)

AWS Service: support (Service-Linker

-

☐

[AWSServiceRoleForTrustedAdvisor](#)

AWS Service: trustedadvisor (Service

-

☐

[Developer](#)

AWS Service: ec2

-

☐

[rds-monitoring-role](#)

AWS Service: monitoring\_rds

16 h

Roles Anywhere Info

Manage

Authenticate your non AWS workloads and securely provide access to AWS services.

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

Type here to search

27°C

ENG  
IN

11:26 AM  
1/19/2024



