

IAM

The image shows two screenshots of the AWS IAM console. The top screenshot is the IAM Dashboard, and the bottom screenshot is the 'Assign MFA device' wizard.

IAM Dashboard

The dashboard shows the following security recommendations:

- 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.

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	6	0	0

Assign MFA device

Step 1: Select MFA device

Select MFA device

MFA device name

Device name
Enter a meaningful name to identify this device.

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.

The screenshot displays the AWS IAM console interface for assigning a Multi-Factor Authentication (MFA) device to a user. The browser address bar shows the URL: `https://us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/security_credentials/mfa`. The left sidebar contains the navigation menu with sections like 'Access management', 'Access reports', and 'Access keys'. The main content area is titled 'Set up device' and includes a 'Step 2: Set up device' indicator. The 'Authenticator app' section provides instructions for installing a compatible application (e.g., Google Authenticator, Duo Mobile, or Authy) and scanning a QR code. A 'Show QR code' button is visible. Below the instructions, a green notification banner states 'MFA device assigned' with a close button. The 'Account details' section shows the user's name 'Bhuvana Thangaraj', email address 'bhuvana.thangaraj@aspiresys.com', and AWS account ID '471112545897'. The 'Multi-factor authentication (MFA) (1)' section includes a table with one entry: 'Virtual' device type, identifier 'arn:aws:iam::471112545897:mfa/Bhuvana', and 'Now' created on. The 'Access keys (0)' section is also visible at the bottom.

Set up device Info

Step 1
[Select MFA device](#)

Step 2
Set up device

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 [Show QR code](#) 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](#)

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. [Learn more](#)

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
Bhuvana Thangaraj

Email address
bhuvana.thangaraj@aspiresys.com

AWS account ID
471112545897

Canonical user ID
3d72adc8573baa5142396677a3448949114750c8f8a4e4a5d432aa7c45569f50

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](#)

Device type	Identifier	Certifications	Created on
<input type="radio"/> Virtual	arn:aws:iam::471112545897:mfa/Bhuvana	Not Applicable	Now

Access keys (0) [Create access key](#)

The image displays three sequential screenshots of the AWS IAM console interface, illustrating the steps to create a new user group and attach policies.

Top Screenshot: User groups overview
The 'User groups (0)' page is shown. It includes a search bar, a 'Create group' button, and a table with columns: Group name, Users, Permissions, and Creation time. The message 'No resources to display' is present.

Middle Screenshot: Create user group
The 'Create user group' page is shown. The 'Name the group' section has a text input field containing 'Glitters'. The 'Add users to the group - Optional (0)' section is also visible, showing a search bar and a table with columns: User name, Groups, Last activity, and Creation time. The message 'No resources to display' is present.

Bottom Screenshot: Policy selection
The 'Attach policies' page is shown. A search bar contains 'ec2', and the filter is set to 'All types' with 30 matches. A table lists available policies with columns: Policy name, Type, Used as, and Description. The policy 'AmazonEC2FullAccess' is selected.

Policy name	Type	Used as	Description
AmazonEC2Contai...	AWS managed	None	Provides administrative access to
AmazonEC2Contai...	AWS managed	None	Provides full access to Amazon EC
AmazonEC2Contai...	AWS managed	None	Provides read-only access to Ama
AmazonEC2Contai...	AWS managed	None	Policy to enable Task Autoscaling
AmazonEC2Contai...	AWS managed	None	Policy to enable CloudWatch Ever
AmazonEC2Contai...	AWS managed	None	Default policy for the Amazon EC
AmazonEC2Contai...	AWS managed	None	Default policy for Amazon ECS se
AmazonEC2FullAcc...	AWS managed	None	Provides full access to Amazon EC
AmazonEC2ReadO...	AWS managed	None	Provides read only access to Ama
AmazonEC2Rolefo...	AWS managed	None	Provides EC2 access to S3 bucket

The image displays three sequential screenshots of the AWS IAM console interface, illustrating the process of managing users and groups.

Screenshot 1: User groups (1) Info
This screenshot shows the 'User groups' page in the IAM console. A green notification banner at the top states 'Glitters user group created.' with a 'View group' link. The page title is 'User groups (1) Info'. Below the title, there is a search bar and a table listing the user groups. The table has columns for 'Group name', 'Users', 'Permissions', and 'Creation time'. One group, 'Glitters', is listed with a warning icon and 'Loading' status. The left sidebar shows the 'Identity and Access Management (IAM)' navigation menu with options like Dashboard, Access management, Access reports, and Account settings.

Screenshot 2: Users (0) Info
This screenshot shows the 'Users' page in the IAM console. A notification banner at the top reads 'Ready to streamline human access to AWS and cloud apps?' with a 'Manage workforce users' link. Below this, there is a section titled 'Users (0) Info' with a search bar and a table listing users. The table has columns for 'User name', 'Path', 'Group', 'Last activity', 'MFA', and 'P'. The table is currently empty, displaying 'No resources to display'. The left sidebar is the same as in the first screenshot.

Screenshot 3: Create user | IAM | Global
This screenshot shows the 'Create user' page in the IAM console. The page title is 'Create user | IAM | Global'. The left sidebar shows the 'Create user' steps: Step 1: Set permissions, Step 2: Review and create, Step 3: Retrieve password, and Step 4: Retrieve password. The main content area is titled 'User details' and includes a 'User name' field with the value 'Monisha'. Below this, there is a checkbox labeled 'Provide user access to the AWS Management Console - optional' which is checked. A blue box contains information about 'Are you providing console access to a person?' with two options: 'Specify a user in Identity Center - Recommended' and 'I want to create an IAM user'. The bottom of the page shows the AWS logo, 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc.

The image displays three sequential screenshots of the AWS IAM console's 'Create user' wizard, showing the steps to create a user named 'Monisha'.

Step 1: Specify user details

User details

User name: Monisha

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.

☐ 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](#)

Cancel Next

Step 2: Set permissions

☒ 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

1

<input checked="" type="checkbox"/>	Group name	Users	Attached policies	Created
<input checked="" type="checkbox"/>	Glitters	0	AmazonEC2FullAccess	2024-01-19 (...)

[Set permissions boundary - optional](#)

Cancel Previous Next

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
Monisha	None	No

Permissions summary

1

Name	Type	Used as
Glitters	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

The image displays three sequential screenshots of the AWS IAM console interface, illustrating the process of creating a user and managing roles.

Top Screenshot: Review and create user

- User name:** Monisha
- Console password type:** None
- Require password reset:** No
- Permissions summary:** A table showing the user is associated with the **Glitters** group, which is a **Permissions group**.
- Tags - optional:** A section for adding tags, currently showing "No tags associated with the resource."
- Buttons:** Cancel, Previous, and Create user.

Middle Screenshot: User created successfully

- Notification:** A green banner stating "User created successfully" with a "View user" link.
- Message:** "You can view and download the user's password and email instructions for signing in to the AWS Management Console."
- Buttons:** Dismiss and Manage workforce users.
- Users (1) Info:** A section showing the user **Monisha** with a search bar and a table of users.

Bottom Screenshot: Roles (6) Info

- Roles (6) Info:** A section showing a list of roles with a search bar and a table of roles.
- Roles:** A table listing roles such as **AWSServiceRoleForRDS**, **AWSServiceRoleForSSO**, **AWSServiceRoleForSupport**, **AWSServiceRoleForTrustedAdvisor**, and **rds-monitoring-role**.
- Buttons:** Create role and Manage.

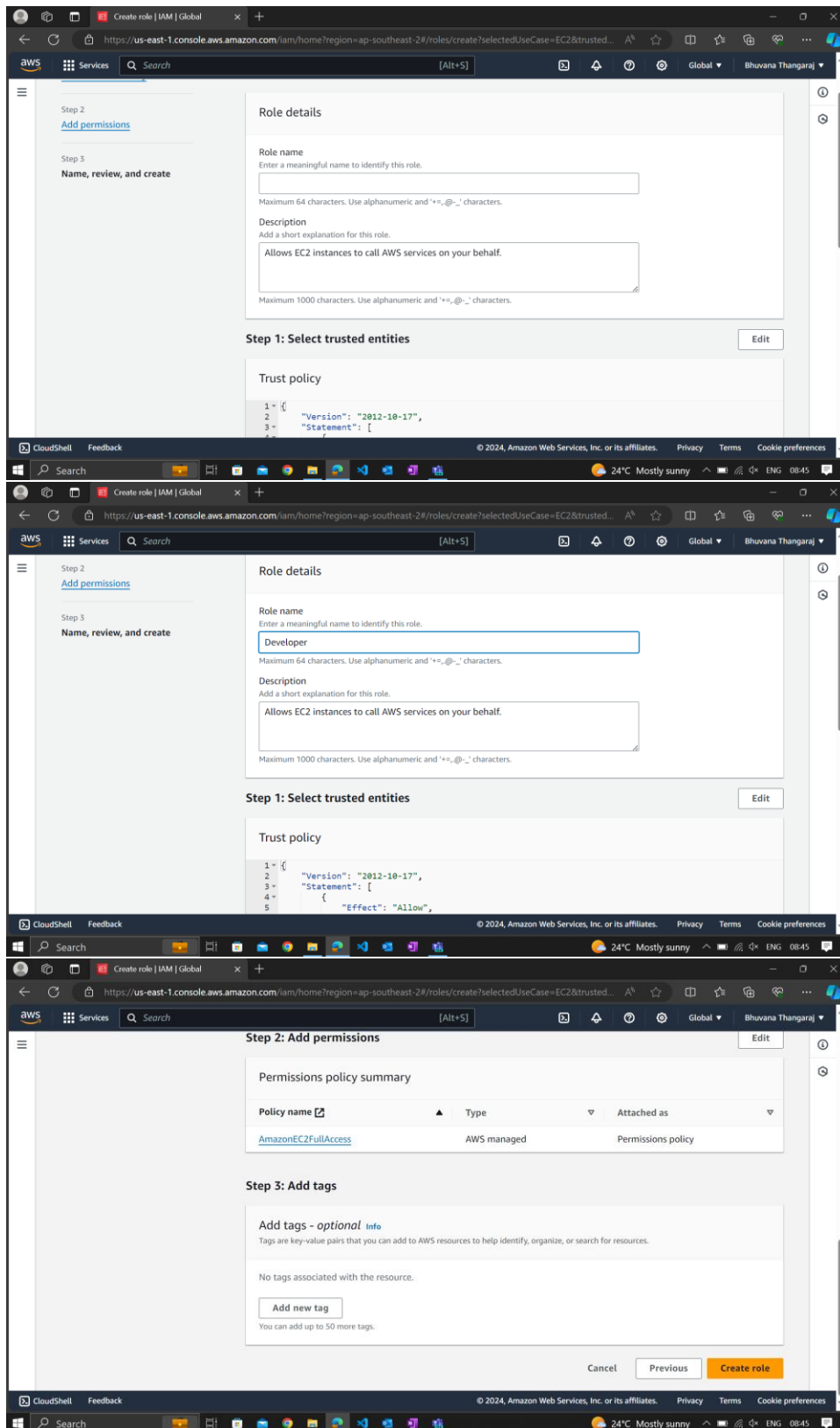
The image displays three sequential screenshots of the AWS IAM console, illustrating the process of creating a new role for EC2 instances.

Screenshot 1: Create role | IAM | Global
The URL is `https://us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/roles/create`. The page shows the "Create role" wizard. On the left, it indicates "Step 3: Name, review, and create". The main content area has several radio button options: "AWS service" (selected), "AWS account", "Web identity", "SAML 2.0 federation", and "Custom trust policy". Below these is a "Use case" section with a description: "Allow an AWS service like EC2, Lambda, or others to perform actions in this account." and a "Service or use case" dropdown menu.

Screenshot 2: Choose a use case for the specified service.
The URL is `https://us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/roles/create`. The "Service or use case" dropdown is set to "EC2". A list of use cases is shown, with "EC2" selected. The list includes: "EC2", "EC2 Role for AWS Systems Manager", "EC2 Spot Fleet Role", "EC2 - Spot Fleet Auto Scaling", "EC2 - Spot Fleet Tagging", "EC2 - Spot Instances", "EC2 - Spot Fleet", and "EC2 - Scheduled Instances". Each use case has a brief description of its permissions.

Screenshot 3: Selecting a policy.
The URL is `https://us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/roles/create/selectedUseCase=EC2&trusted...`. This screen shows a list of policies that can be attached to the role. The policies are listed in a table with columns for the policy name, whether it is AWS managed, and a brief description. The policy "AmazonEC2FullAccess" is selected with a checkmark.

Policy Name	Managed By	Description
AmazonEC2Contai...	AWS managed	Policy to enable Task Autoscaling for A...
AmazonEC2Contai...	AWS managed	Policy to enable CloudWatch Events fo...
AmazonEC2Contai...	AWS managed	Default policy for the Amazon EC2 Rol...
AmazonEC2Contai...	AWS managed	Default policy for Amazon ECS service ...
AmazonEC2FullAcc...	AWS managed	Provides full access to Amazon EC2 via...
AmazonEC2ReadO...	AWS managed	Provides read only access to Amazon E...
AmazonEC2Rolefo...	AWS managed	Provides EC2 access to S3 bucket to do...
AmazonEC2Rolefo...	AWS managed	Provides EC2 limited access to S3 buck...
AmazonEC2Rolefo...	AWS managed	Default policy for the Amazon EC2 Rol...
AmazonEC2Rolefo...	AWS managed	This policy will soon be deprecated. PL...
AmazonEC2RolePo...	AWS managed	Managed policy for the Amazon Launc...
AmazonEC2SpotFl...	AWS managed	Policy to enable Autoscaling for Amaz...
AmazonEC2SpotFl...	AWS managed	Allows EC2 Spot Fleet to request, term...



The image displays three sequential screenshots of the AWS IAM console, illustrating the process of creating a new role. The browser window shows the URL `https://us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/roles/create?selectedUseCase=EC2&trustedEntity=...`.

Step 1: Select trusted entities

Role details

Role name
Enter a meaningful name to identify this role.
Maximum 64 characters. Use alphanumeric and `*+_-.` characters.

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and `*+_-.` characters.

Trust policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonEC2FullAccess	AWS managed	Permissions policy

Step 3: Add tags

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.

[Add new tag](#)
You can add up to 50 more tags.

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

The image displays two screenshots of the AWS IAM console, specifically the 'Roles' page in the 'us-east-1' region.

Top Screenshot: The 'Role Developer created.' notification is visible at the top. The 'Roles Anywhere' section is highlighted, showing options to 'Access AWS from your non AWS workloads', 'X.509 Standard', and 'Temporary credentials'. The left sidebar shows the 'Identity and Access Management (IAM)' navigation menu.

Bottom Screenshot: The 'Roles (7)' list is displayed, showing a table of roles and their trusted entities. The roles listed are:

Role name	Trusted entities
AWSServiceRoleForOrganizations	AWS Service: organizations (Service-Linked Role)
AWSServiceRoleForRDS	AWS Service: rds (Service-Linked Role)
AWSServiceRoleForSSO	AWS Service: sso (Service-Linked Role)
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)
Developer	AWS Service: ec2
rds-monitoring-role	AWS Service: monitoring.rds

The screenshot displays the AWS IAM console interface. The top section shows the 'Delete Developer?' dialog box, which prompts the user to confirm the deletion of the 'Developer' role. The dialog includes a table with the role name and last activity, a note about activity data retention, and a confirmation field where 'Developer' has been entered. The bottom section shows the 'User groups' page, which displays a message indicating that the user 'Monisha' and the user group have been successfully deleted. The console also shows the 'User groups (0)' list, which is currently empty.

Delete Developer?

Delete **Developer** permanently? This will also delete all its inline policies and any attached instance profiles.

Role name	Last activity
Developer	-

Note: Recent activity usually appears within 4 hours. Data is stored for a maximum of 365 days, depending when your region began supporting this feature. [Learn more](#)

This action cannot be undone.

To confirm deletion, enter the role name in the text input field.

[Cancel](#) [Delete](#)

User "Monisha" deleted.

User group deleted.

User groups (0) [info](#) [Refresh](#) [Delete](#) [Create group](#)

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			