

IAM Resources Task

IAM (Identity and Access Management) is a service in AWS that helps you decide who can use your AWS account and what they can do.

1. User: Individual identities

User Creation steps-

The screenshot shows the AWS IAM 'Create user' console. The breadcrumb navigation at the top reads 'IAM > Users > Create user'. On the left, a vertical list of steps is shown: Step 1 (Specify user details, selected), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password). The main content area is titled 'Specify user details' and contains two sections: 'User details' and 'Console password'.

User details

User name

Gunjan

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.

XXXXXXXXXX123

- 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.

Information: 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

Attach Permission to the user

IAM > Users > Create user

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. [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.

Permissions policies (1391) [Create policy](#)

Choose one or more policies to attach to your new user.

Filter by Type: All types

Search:

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AccessAnalyzerServiceRolePolicy	AWS managed	0

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 Gurjan	Console password type Custom password	Require password reset No
---------------------	--	------------------------------

Permissions summary

Name	Type	Used as
No resources		

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](#)

You can set MFA to user(optional)

IAM > Users

Search IAM

Dashboard

Access management

User groups

Users

Users (4) [Info](#)

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

Search

<input type="checkbox"/>	User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Access key ID
<input type="checkbox"/>	Gurjan	/	0	-	-	Now	-	-

[Delete](#) [Create user](#)

Why do we need Access Key for a user?

- Because **applications, scripts, or CLI (Command Line Interface)** cannot type passwords like humans.
- Access keys act like a **username + password pair** for software/programs.

Create Access key for user. You can create only 2 keys of single user

English ▼ Preferences ▼ Contact Us Feedback

You can access user through CLI

```
Command Prompt
Microsoft Windows [Version 10.0.26100.4946]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sjain403>aws configure
AWS Access Key ID [*****P4MD]: AKIA3VYGS47WFRADW5YR
AWS Secret Access Key [*****KaZn]: bAHHTUwZLEw7QvthkEQCE4EPtryKlyGHHp0R0
Default region name [None]:
Default output format [None]:

C:\Users\sjain403>aws s3 ls
2025-08-23 11:46:17 mentore-solution01

C:\Users\sjain403>
```

2. User Groups: A collection of users.

Create user group

Name the group

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

Add users to the group - Optional (2/4) [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.

<input checked="" type="checkbox"/>	User name	Groups	Last activity	Creation time
<input checked="" type="checkbox"/>	Gunjan	0	None	2 minutes ago
<input type="checkbox"/>	Sakshi	1	None	10 days ago
<input checked="" type="checkbox"/>	Test	1	12 days ago	12 days ago
<input type="checkbox"/>	Test02	0	12 days ago	12 days ago

Attach permissions policies - Optional (1/1076) [Info](#)

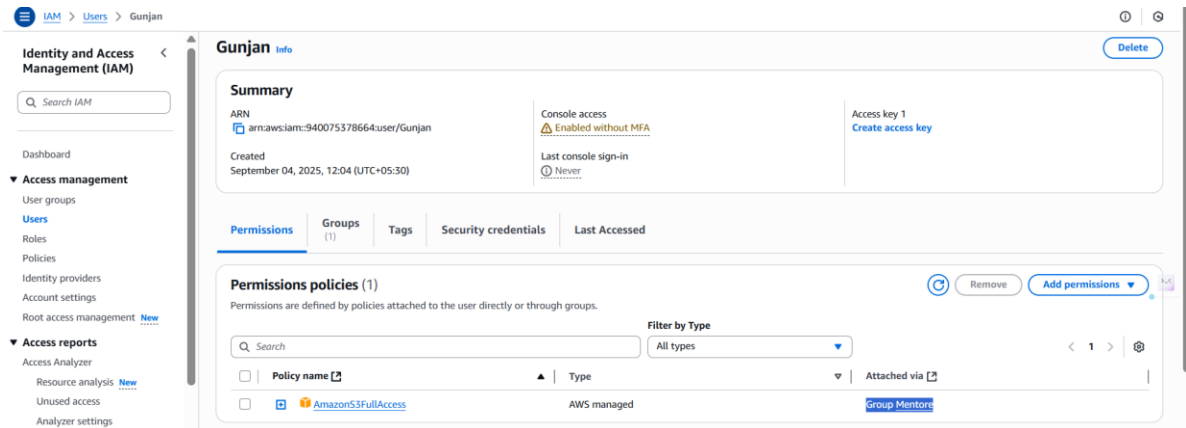
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type: S3Full (1 match)

<input checked="" type="checkbox"/>	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	Permissions policy (3)	Provides full access to all buckets via t...

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

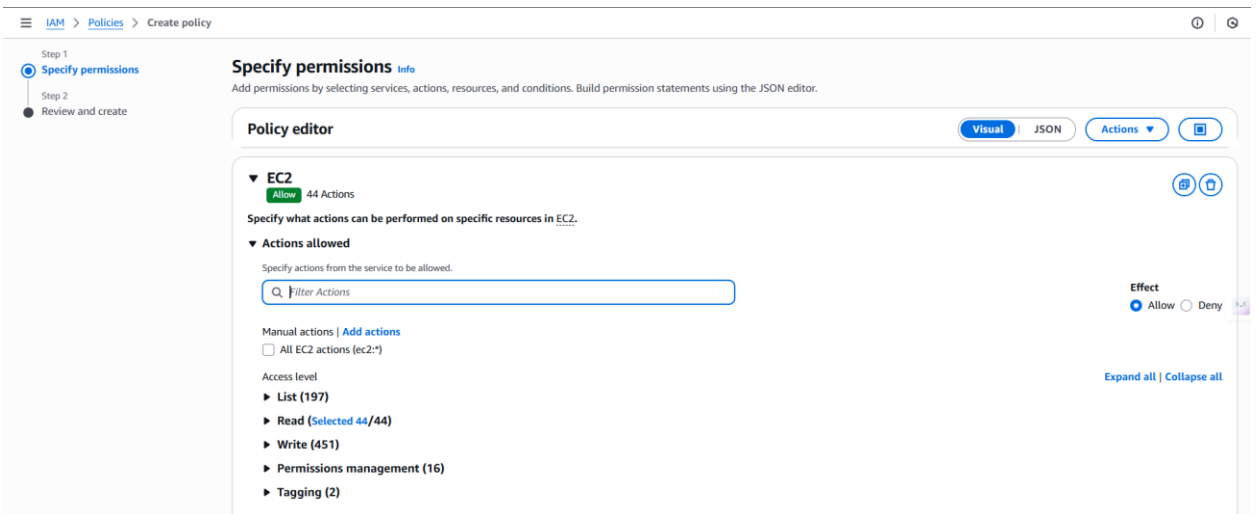
You can see user is added in group and having group permissions



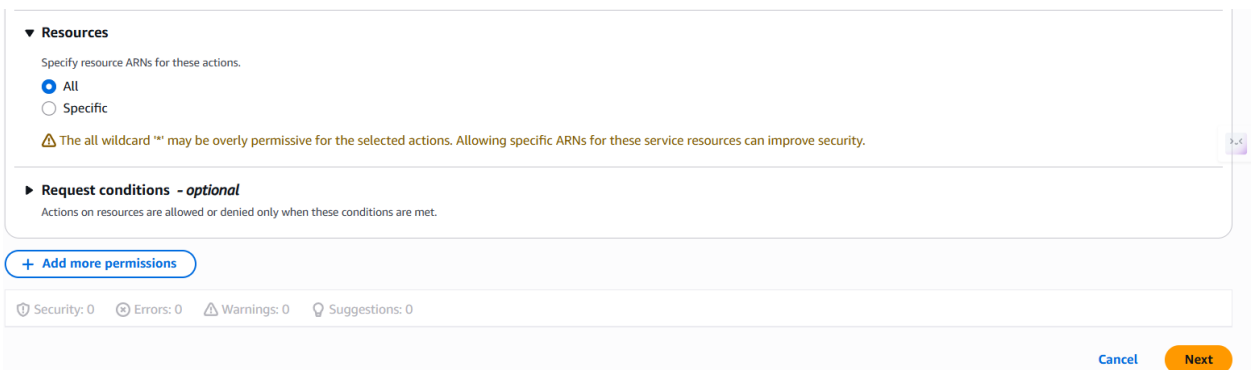
3. Policies: Rules that define what a user, group, or role can do.

You can create policy for any service

Here is 2 ways to create policy -1. Visual 2. JSON



You can create policy for all resource or specific resource.



4. Roles: Temporary identities with permissions, usually for applications or services.

4. Roles: Temporary identities with permissions, usually for applications or services.

Step 1

● Select trusted entity

Step 2

● Add permissions

Step 3

● **Name, review, and create**

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

Test-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 letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+, @, ^, [], #, \$, %, *, ~, =, -

IAM
Roles
Test-role

Identity and Access Management (IAM)

Dashboard
Access management
Users
Policies
Identity providers
Account settings
Root access management
Access reports
Resource analysis
Unused access
Analyzer settings
Credential report
Organization activity

Role Test-role created.
View role
Delete

Test-role

Allows EC2 instances to call AWS services on your behalf.

Summary

Creation date
September 04, 2025, 20:06 (UTC+05:30)

Last activity
-

ARN
arn:aws:iam::940075378664:role/Test-role

Maximum session duration
1 hour

Instance profile ARN
arn:aws:iam::940075378664:instance-profile/Test-role

Permissions
Trust relationships
Tags
Last Accessed
Revoke sessions

Permissions policies (1)

You can attach up to 10 managed policies.

Filter by Type
All types

Policy name	Type	Attached entities
<input type="checkbox"/> <input type="checkbox"/> AmazonEC2FullAccess	AWS managed	1

Create EC2 Instance

EC2 > Instances > Launch an instance

Take a walkthrough Do not show me this message again.

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

Test

Add additional tags

Application and OS Images (Amazon Machine Image) Info

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose [Browse more AMIs](#).

Search our full catalog including 1000s of application and OS images

Summary

Number of instances Info

1

Software Image (AMI)

Canonical, Ubuntu, 24.04, amd64...[read more](#)

ami-0a716d3f3b16d290c

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Cancel Launch instance

Preview code

EC2 > Instances > Launch an instance

On-Demand Linux base pricing: 0.0108 USD per Hour
On-Demand Windows base pricing: 0.02 USD per Hour
Additional costs apply for AMIs with pre-installed software

Key pair (login) Info

You can use a key pair to securely connect to your instance.

Key pair name - required

Select

Network settings Info

Network Info

vpc-03bf2f3813ecfe793

Subnet Info

Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

TestInstance01

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ RSA
RSA encrypted private and public key pair

☐ ED25519
ED25519 encrypted private and public key pair

Private key file format

☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

Cancel Create key pair

Click on connect

EC2 > Instances

EC2

Dashboard

AWS Global View

Events

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

Instances (1/1) Info

Last updated less than a minute ago

Connect

Instance state

Actions

Launch instances

Find Instance by attribute or tag (case-sensitive)

All states

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
<input checked="" type="checkbox"/>	Test	i-077c3f4b8136b5f45	Running	t3.micro	Initializing	View alarms +

i-077c3f4b8136b5f45 (Test)

Details

Status and alarms

Monitoring

Security

Networking

Storage

Tags

Instance summary Info

Instance ID

i-077c3f4b8136b5f45

Public IPv4 address

51.21.192.139 | [open address](#)

Private IPv4 addresses

172.31.32.232

Connect [Info](#)

Connect to an instance using the browser-based client.


EC2 Instance Connect

Session Manager

SSH client

EC2 serial console


Instance ID

 i-014c249fde0d345de (Test)

Connection type

☒ Connect using a Public IP
Connect using a public IPv4 or IPv6 address


☐ Connect using a Private IP
Connect using a private IP address and a VPC endpoint

☒ Public IPv4 address
 16.171.0.54

☐ IPv6 address
—

Username

Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ec2-user.

 ec2-user

