

## Create a New IAM User

1. Create a new IAM user with programmatic access.

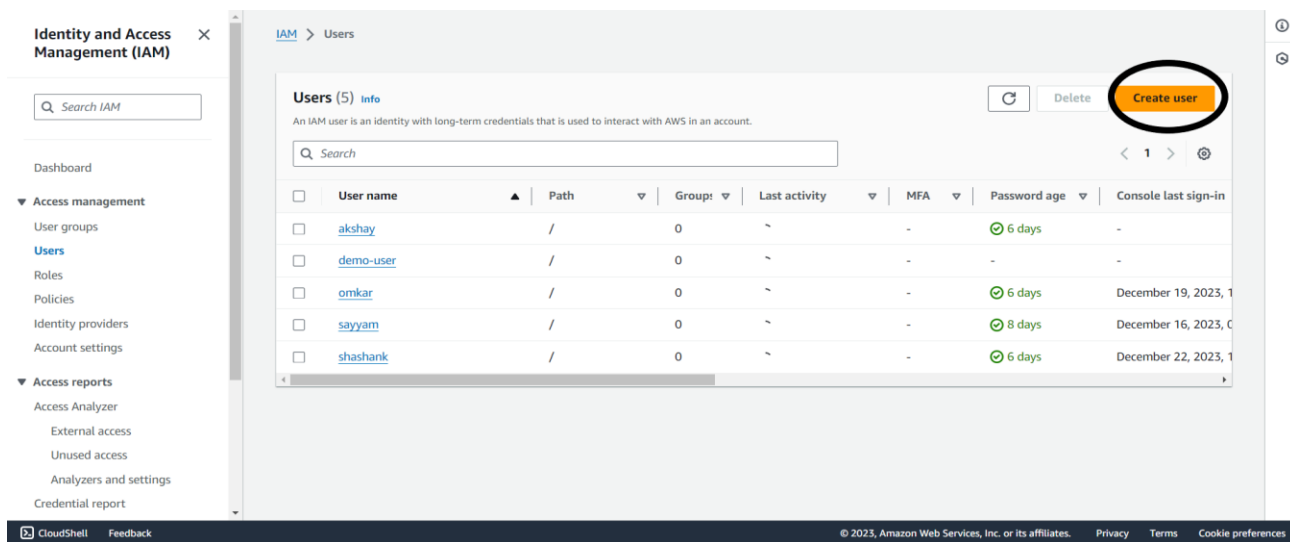
Assign appropriate permissions to the user based on their role or responsibilities.

Generate and securely provide the user's access key and secret access key.

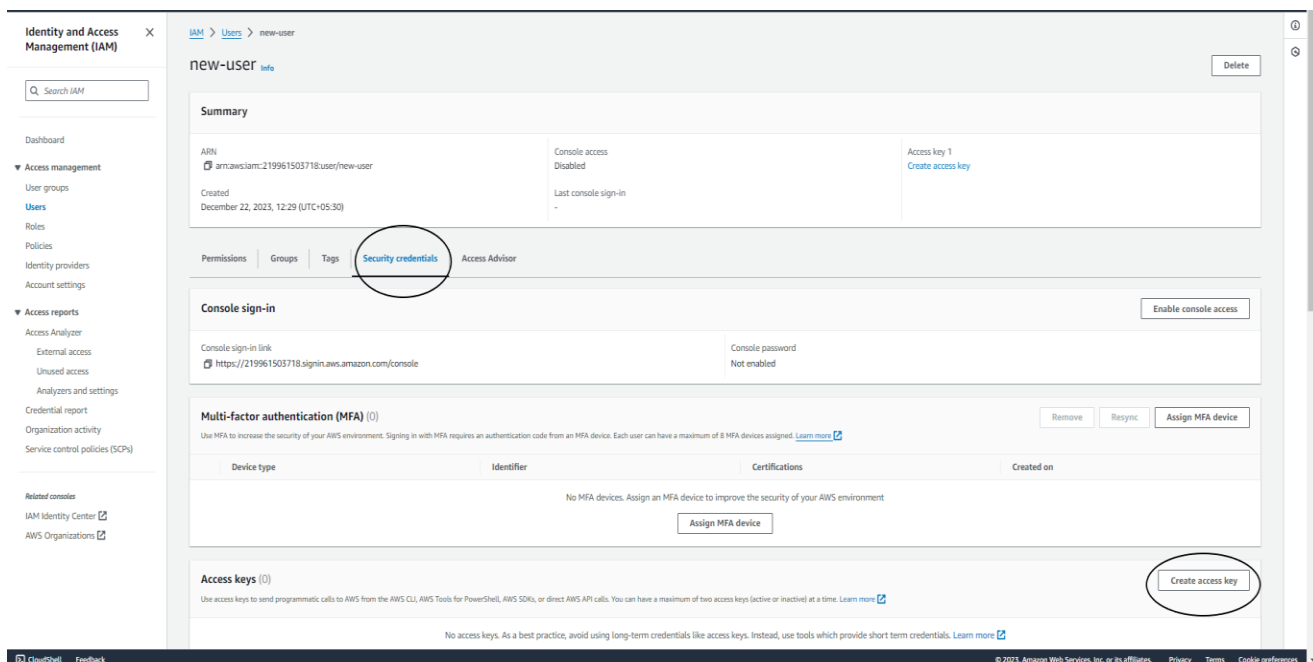
Configure IAM Roles:

Create a IAM user-:

Step 1- Go to IAM services and create user.



Step 2- Go to the security credentials to create access key and secret key.



## Step 3- Select the use case. (Select Cli)

IAM > Users > new-user > Create access key

Step 1  
Access key best practices & alternatives

Step 2 - optional  
Set description tag

Step 3  
Retrieve access keys

### Access key best practices & alternatives [info](#)

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

**Use case**

- ☒ **Command Line Interface (CLI)**  
You plan to use this access key to enable the AWS CLI to access your AWS account.
- ☐ **Local code**  
You plan to use this access key to enable application code in a local development environment to access your AWS account.
- ☐ **Application running on an AWS compute service**  
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.
- ☐ **Third-party service**  
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.
- ☐ **Application running outside AWS**  
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.
- ☐ **Other**  
Your use case is not listed here.

**Alternatives recommended**

- Use [AWS CloudShell](#), a browser-based CLI, to run commands. [Learn more](#)
- Use the [AWS CLI V2](#) and enable authentication through a user in IAM Identity Center. [Learn more](#)

**Confirmation**

☒ I understand the above recommendation and want to proceed to create an access key.

Cancel **Next**

CloudShell Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

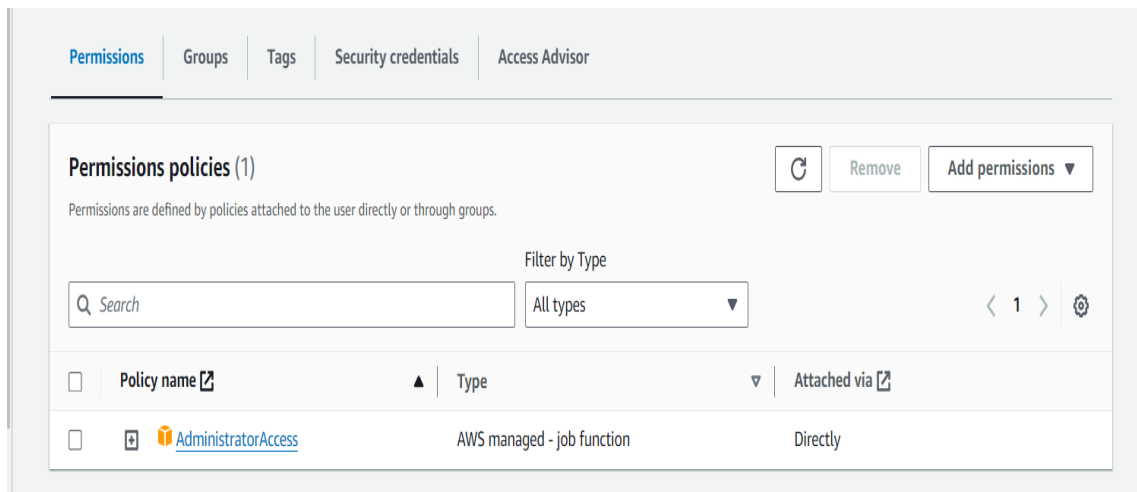
## Step 4- Then search cloud shell in search bar of the console and log in the console.

```
aws CloudShell

ap-south-1

[cloudshell-user@ip-10-132-90-83 ~]$ aws iam get-user --user-name new-user
{
  "User": {
    "Path": "/",
    "UserName": "new-user",
    "UserId": "AIDATGMV2F7TOF46EB7MT",
    "Arn": "arn:aws:iam::219961503718:user/new-user",
    "CreateDate": "2023-12-22T06:59:38+00:00"
  }
}
[cloudshell-user@ip-10-132-90-83 ~]$
```

## Step 5- Attach or remove policy.

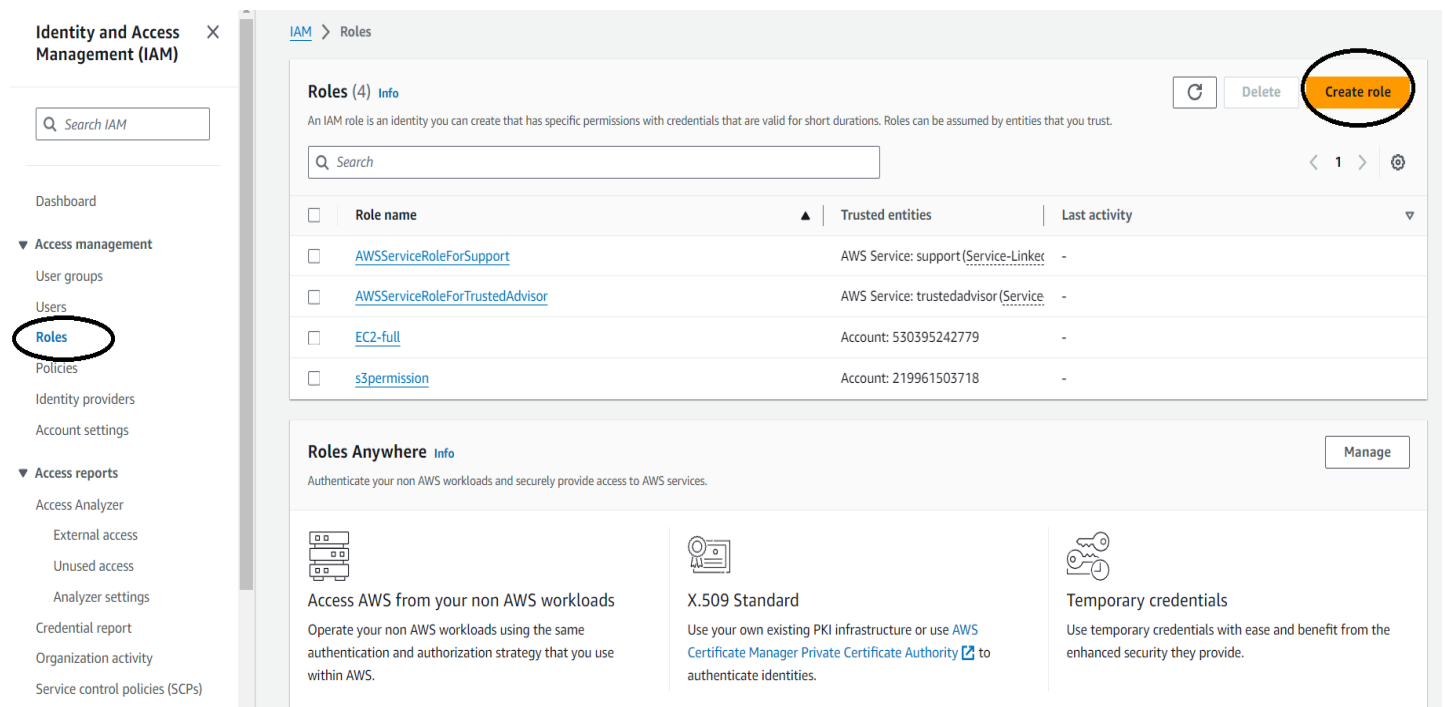


**2.Create an IAM role for EC2 instances or Lambda functions with specific permissions.**

**Attach policies to the role that grant necessary permissions to access AWS resources.**

**Assign the role to EC2 instances or Lambda functions.**

**Step 1- Go to the IAM services inside the IAM services click on the role for creating the role.**



**Step 2- Select AWS service which is in present in trusted entity and after that select use case as EC2**

[IAM](#) > [Roles](#) > Create role

Step 1  
Select trusted entity

Step 2  
Add permissions

Step 3  
Name, review, and create

## Select trusted entity [Info](#)

**Trusted entity type**

☒ **AWS service**  
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ **AWS account**  
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ **Web identity**  
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ **SAML 2.0 federation**  
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ **Custom trust policy**  
Create a custom trust policy to enable others to perform actions in this account.

**Use case**  
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case  
EC2

Choose a use case for the specified service.  
Use case

☒ **EC2**  
Allows EC2 instances to call AWS services on your behalf.

☐ **EC2 Role for AWS Systems Manager**  
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

☐ **EC2 Spot Fleet Role**  
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

☐ **EC2 - Spot Fleet Auto Scaling**  
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

☐ **EC2 - Spot Fleet Tagging**

**Step 3- After this select the permission that you have to apply (EC2 full access in this case)**

[IAM](#) > [Roles](#) > Create role

Step 1  
[Select trusted entity](#)

Step 2  
Add permissions

Step 3  
Name, review, and create

## Add permissions [Info](#)

**Permissions policies (1/906)** [Info](#)

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

Filter by Type

Q ec2 X All types 30 matches

| <input type="checkbox"/>            | Policy name  | Type        | Description                                |
|-------------------------------------|--|-------------|--|
| <input type="checkbox"/>            | <a href="#">AmazonEC2ContainerRegistryFullAccess</a>   | AWS managed | Provides administrative access to Ama...   |
| <input type="checkbox"/>            | <a href="#">AmazonEC2ContainerRegistryPowerUser</a>    | AWS managed | Provides full access to Amazon EC2 Co...   |
| <input type="checkbox"/>            | <a href="#">AmazonEC2ContainerRegistryReadOnly</a>     | AWS managed | Provides read-only access to Amazon E...   |
| <input type="checkbox"/>            | <a href="#">AmazonEC2ContainerServiceAutoscaleRole</a> | AWS managed | Policy to enable Task Autoscaling for A... |
| <input type="checkbox"/>            | <a href="#">AmazonEC2ContainerServiceEventsRole</a>    | AWS managed | Policy to enable CloudWatch Events fo...   |
| <input type="checkbox"/>            | <a href="#">AmazonEC2ContainerServiceforEC2Role</a>    | AWS managed | Default policy for the Amazon EC2 Rol...   |
| <input type="checkbox"/>            | <a href="#">AmazonEC2ContainerServiceRole</a>          | AWS managed | Default policy for Amazon ECS service ...  |
| <input checked="" type="checkbox"/> | <a href="#">AmazonEC2FullAccess</a>                    | AWS managed | Provides full access to Amazon EC2 via...  |
| <input type="checkbox"/>            | <a href="#">AmazonEC2ReadOnlyAccess</a>                | AWS managed | Provides read only access to Amazon E...   |
| <input type="checkbox"/>            | <a href="#">AmazonEC2RoleforAWSCodeDeploy</a>          | AWS managed | Provides EC2 access to S3 bucket to do...  |

**Step 4- Click next permission after this go to the EC2 services select instance select instance then start it. When the instance start running go to**

## action->security->modify role

EC2 Dashboard X

EC2 Global View

Events

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Successfully started i-0fa32b0ea0584de5a X

Instances (1/1) Info

Find Instance by attribute or tag (case-sensitive)

| <input checked="" type="checkbox"/> | Name            | Instance ID         | Instance state | Instance type | Status check | Alarm status |
|-------------------------------------|-----------------|---------------------|----------------|---------------|--------------|--------------|
| <input checked="" type="checkbox"/> | shubham-inst... | i-0fa32b0ea0584de5a | Running        | t2.micro      | -            | No alarms    |

Connect

View details

Manage instance state

Instance settings

Networking

Security

Image and templates

Monitor and troubleshoot

Change security groups

Get Windows password

Modify IAM role

Launch instances

ic IPv4 DNS

13-232-69-1

## Step 5- Select the role and click update IAM role

EC2 > Instances > i-0fa32b0ea0584de5a > Modify IAM role

### Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID

i-0fa32b0ea0584de5a (shubham-instance)

IAM role

Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

ec2-full-access ▼

[Create new IAM role](#)

Cancel

Update IAM role

## 3.Implement Multi-Factor Authentication (MFA):

Enable MFA for IAM users to provide an additional layer of security.

**Guide users on how to set up MFA devices (such as virtual MFA apps or hardware tokens).**

**Test the MFA configuration to ensure it functions correctly.**

**Create IAM Policies:**

**Step 1- To enable MFA go IAM services->user->security credentials->assign MFA device**

The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with sections like 'Identity and Access Management (IAM)', 'Access management', 'Access reports', and 'Related consoles'. The main content area is titled 'shashank-test' and includes a 'Delete' button. Below the title is a 'Summary' section with details about the user's ARN, console access status (Enabled without MFA), and last sign-in. A tabbed interface below the summary shows 'Permissions', 'Groups (1)', 'Tags', 'Security credentials' (which is circled in red), and 'Access Advisor'. The 'Security credentials' tab displays 'Permissions policies (1)' and a table with one policy: 'AmazonS3ReadOnlyAccess', which is AWS managed and attached directly. There are also buttons for 'Remove' and 'Add permissions'.

| Policy name            | Type        | Attached via |
|------------------------|-------------|--------------|
| AmazonS3ReadOnlyAccess | AWS managed | Directly     |

**Step 2- Select MFA device**

[IAM](#) > [Users](#) > [shashank-test](#) > Assign MFA device

Step 1  
Select MFA device

Step 2  
Set up device

## Select MFA device [Info](#)


### 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.

☐  **Security Key**  
Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.

☐  **Hardware TOTP token**  
Authenticate using a code displayed on a hardware Time-based one-time password (TOTP) token.

## Set up device-

### 1. Install authenticator app

**Download and install an authenticator app on your mobile device.**

### 2. Scan QR code or enter key

**Use app to scan the QR code displayed in IAM console or manually enter the secret configuration key.**

### 3. Enter verification code

**The app will generate a time-based verification code. Enter this code in IAM console to confirm activation.**

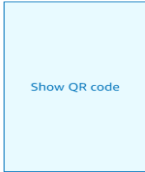
IAM > Users > shashank-test > Assign MFA device

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 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 Fill in two consecutive codes from your MFA device.  
MFA code 1:   
MFA code 2:

Cancel Previous **Add MFA**

**4. Write a custom IAM policy that allows or denies specific actions on AWS resources.**

**Associate the policy with the appropriate IAM users, groups, or roles.**

**Test the policy to verify that the desired access control is enforced.**

**Use IAM Groups:**

**Step 1- Go to IAM policies to create policy -> Create policy**


IAM > Policies








**Policies (1167) Info**

A policy is an object in AWS that defines permissions.

Filter by Type

Search  All types

1 2 3 4 5 6 7 ... 59 > 

|                       | Policy name  | Type                       | Used as                | Description                                |
|-----------------------|--|----------------------------|------------------------|--|
| <input type="radio"/> |  <a href="#">AccessAnalyzerServiceRolePolicy</a>  | AWS managed                | None                   | Allow Access Analyzer to analyze resou...  |
| <input type="radio"/> |  <a href="#">AdministratorAccess</a>              | AWS managed - job function | Permissions policy (6) | Provides full access to AWS services an... |
| <input type="radio"/> |  <a href="#">AdministratorAccess-Amplify</a>      | AWS managed                | None                   | Grants account administrative permissi...  |
| <input type="radio"/> |  <a href="#">AdministratorAccess-AWSElasti...</a> | AWS managed                | None                   | Grants account administrative permissi...  |
| <input type="radio"/> |  <a href="#">AlexaForBusinessDeviceSetup</a>      | AWS managed                | None                   | Provide device setup access to AlexaFo...  |
| <input type="radio"/> |  <a href="#">AlexaForBusinessFullAccess</a>       | AWS managed                | None                   | Grants full access to AlexaForBusiness ... |
| <input type="radio"/> |  <a href="#">AlexaForBusinessGatewayEve...</a>    | AWS managed                | None                   | Provide gateway execution access to A...   |



## Step 2- Write JESON code for policy (S3 list access grand)

**Specify permissions** [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

**Policy editor**

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Statement1",
6       "Effect": "Allow",
7       "Action": [
8         "s3:ListAccessGrants"
9       ],
10      "Resource": []
11    }
12  ]
13 }
```

**Edit statement** Remove

**Statement1**

**Add actions**

All services > S3

☐ All actions (s3:\*)

**Access level - list**

- ☒ ListAccessGrants [Info](#)
- ☐ ListAccessGrantsInstances [Info](#)
- ☐ ListAccessGrantsLocations [Info](#)
- ☐ ListAccessPoints [Info](#)
- ☐ ListAccessPointsForObjectLambda [Info](#)

## Step 3- Attach policy to the user

**Add permissions**

**Review**

The following policies will be attached to this user. [Learn more](#)

**User details**

User name  
shashank-test

**Permissions summary (1)** < 1 >

| Name <a href="#">🔗</a>                 | Type        | Used as            |
|--|-------------|--------------------|
| <a href="#">AmazonS3ReadOnlyAccess</a> | AWS managed | Permissions policy |

Cancel Previous Add permissions

## Step 4- After attaching the policy user added into the group

Users (1) | Permissions | Access Advisor


**Users in this group (1)** Refresh Remove Add users

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

Search

| <input type="checkbox"/> | User name <a href="#">↗</a>   | ▲ Groups | Last activity ▼ | Creation time ▼ |
|--------------------------|-------------------------------|----------|-----------------|-----------------|
| <input type="checkbox"/> | <a href="#">shashank-test</a> | 1        | 18 minutes ago  | 35 minutes ago  |

**Step 5- After adding into the group check the policy the error occurs due to incomplete access of S3**



**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

Cancel
Create bucket

**5.Create an IAM group and assign permissions to it.**

**Add IAM users to the group to manage their access collectively.**

**Remove users from the group when their access requirements change.**

**Implement IAM Access Analyzer:**

**Step 1- Create an IAM group go to the IAM console->user group->create user group->name the group (demo group)->add users to the groups->attach permission policies**

Identity and Access Management (IAM)

Q Search IAM

Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies (SCPs)
Related services
IAM Identity Center
AWS Organizations

IAM > User groups > Create user group

Create user group

Name the group

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

Add users to the group - Optional (1/77) 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.

Q Search

| User name     | Groups | Last activity  | Creation time  |
|---------------|--------|----------------|----------------|
| alishay       | 0      | None           | 7 days ago     |
| Alshay-test   | 0      | None           | 41 minutes ago |
| anbar         | 0      | 59 minutes ago | 6 days ago     |
| anvaram       | 0      | 7 days ago     | 9 days ago     |
| shashank      | 0      | 1 hour ago     | 7 days ago     |
| shashank-test | 1      | 13 hours ago   | 13 hours ago   |
| User01        | 0      | 13 hours ago   | 13 hours ago   |

Attach permissions policies - Optional (1/306) 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.

Q id

Filter by Type: All types 10 matches

| Policy name                          | Type        | Used as                | Description   |
|--------------------------------------|-------------|------------------------|---|
| AmazonQMSRedshiftRole                | AWS managed | None                   | Provides access to manage S3 settings for Redshift endpoints for DMS.   |
| AmazonS3FullAccess                   | AWS managed | Permissions policy (8) | Provides full access to all buckets via the AWS Management Console.   |
| AmazonS3ObjectLambdaExecutionRole... | AWS managed | None                   | Provides AWS Lambda functions permissions to interact with Amazon S3 Object Lambda. Also grants Lambda permissions to write to CloudWatch Logs. |
| AmazonS3OutpostsFullAccess           | AWS managed | None                   | Provides full access to Amazon S3 on Outposts via the AWS Management Console.   |
| AmazonS3OutpostsS3Access             | AWS managed | None                   | Provides read only access to Amazon S3 on Outposts via the AWS Management Console.  |
| AmazonS3OutpostsOnlyAccess           | AWS managed | Permissions policy (1) | Provides read only access to all buckets via the AWS Management Console.  |

## Step 2- Removing users from the group

Go to -Access group members->select user->remove users

Identity and Access Management (IAM)

Q Search IAM

Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies (SCPs)

IAM > User groups > demo-group

demo-group info

Summary

User group name

demo-group

Creation time

December 23, 2023, 09:27 (UTC+05:30)

ARN

arn:aws:iam::219961503718:group/demo-group

Users (1)

Permissions

Access Advisor

Users in this group (1/1)

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

Q Search

| User name     | Groups | Last activity | Creation time |
|---------------|--------|---------------|---------------|
| shashank-test | 2      | 13 hours ago  | 13 hours ago  |

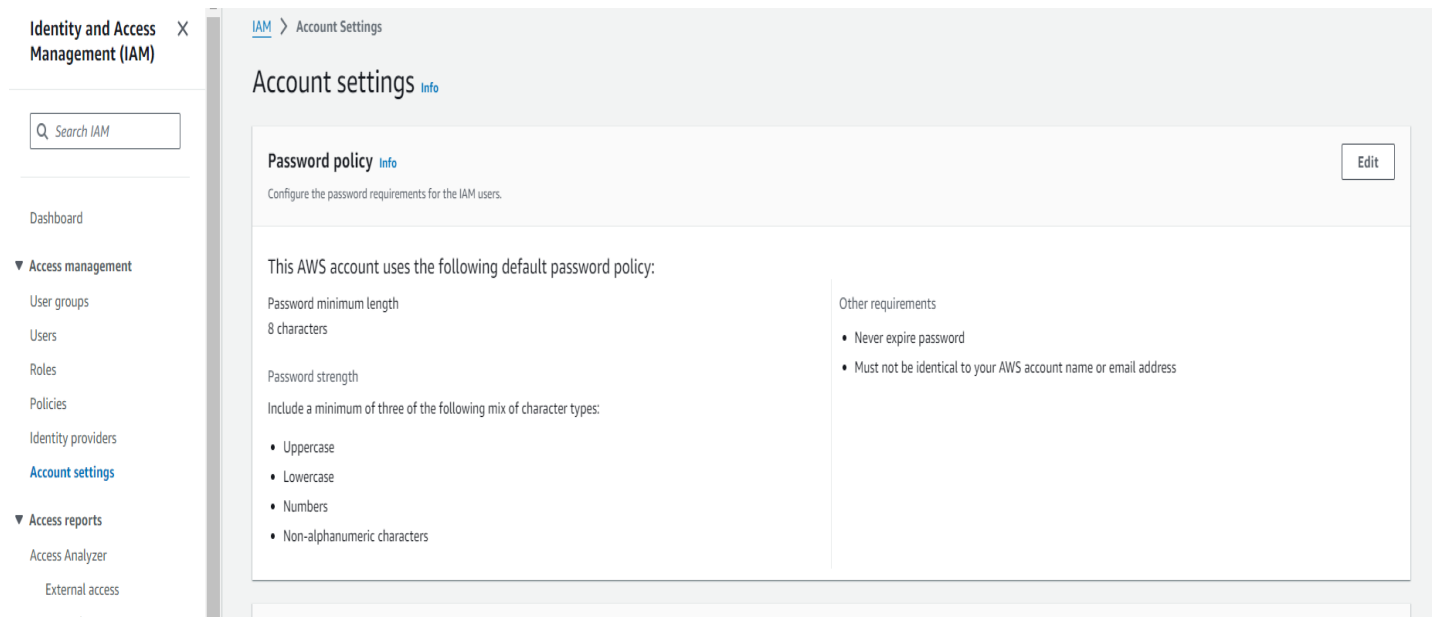
## 6. Define and enforce password policies for IAM users.

Set requirements such as minimum password length, complexity, and expiration.

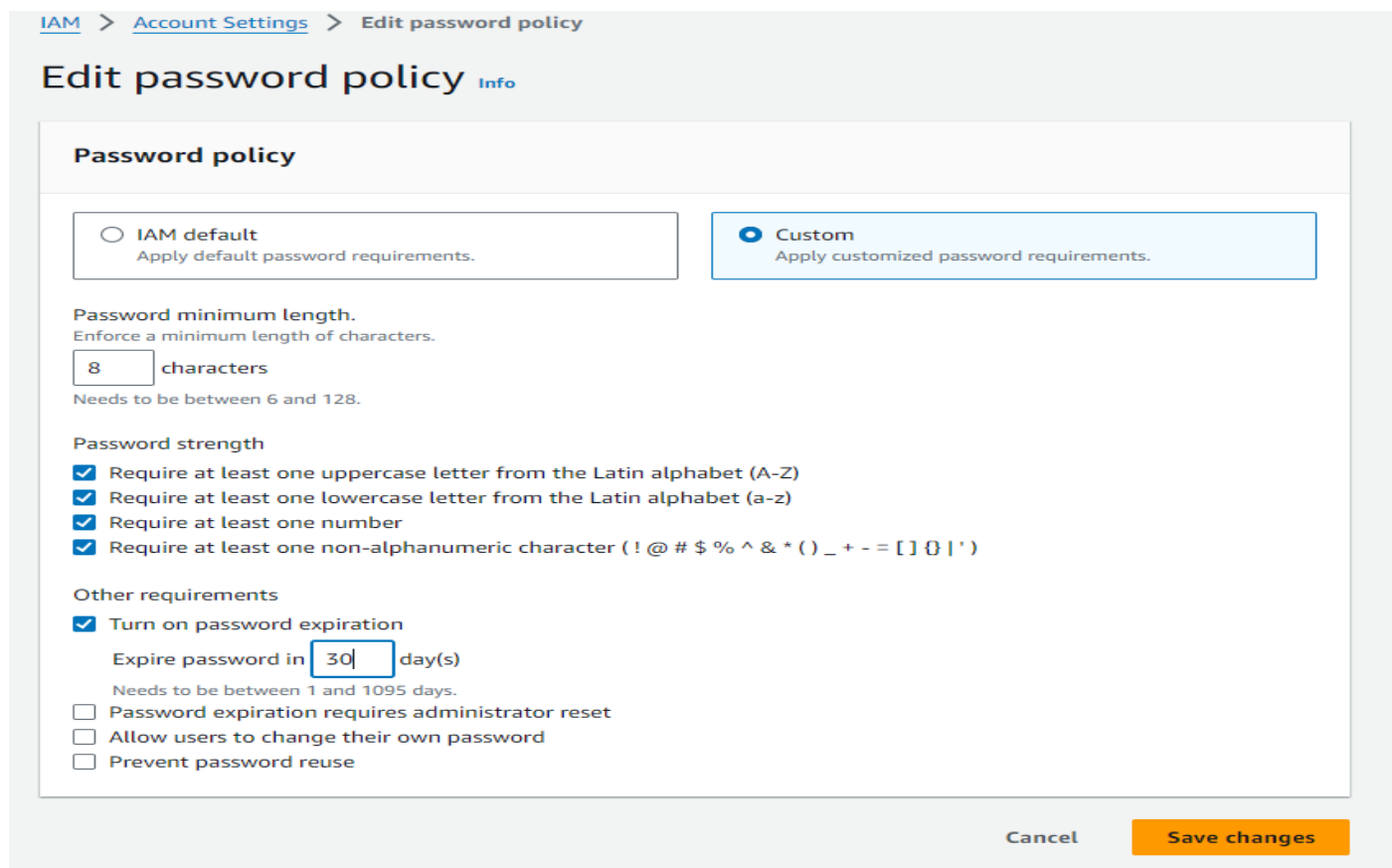
Regularly remind users to update their passwords according to the policy.

Step 1- To set policy for the password go to the

## –IAM console-> account setting->password policy->edit



**Step 2- After entering the edit option click on ->custom (configure as per requirement) click on save changes. To apply new password policy.**



**7.Create user Shubham.shubham can only launch ec2 instance in Mumbai**

## Region

**Step 1- For creating the new user go to the IAM console ->user-> create user  
->specify user details->user name(in our case user name is shubham)**

IAM > Users > Create user

Step 1  
Specify user details

Step 2  
Set permissions

Step 3  
Review and create

### Specify user details

#### User details

User name

shubham

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.

**i** 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- select – provide user access to AWS management console**

**Select- i want to create an IAM user**

**Go to console password->Select custom password->next**

IAM > Users > Create user

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

shubham

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.

**i** 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:  
shubham-demo@123

☒ Show password

☒ Users must create a new password at next sign-in - Recommended  
Users automatically get the [IAM:UserChangePassword](#) policy to allow them to change their own password.

**i** 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 3- Attach the policy**

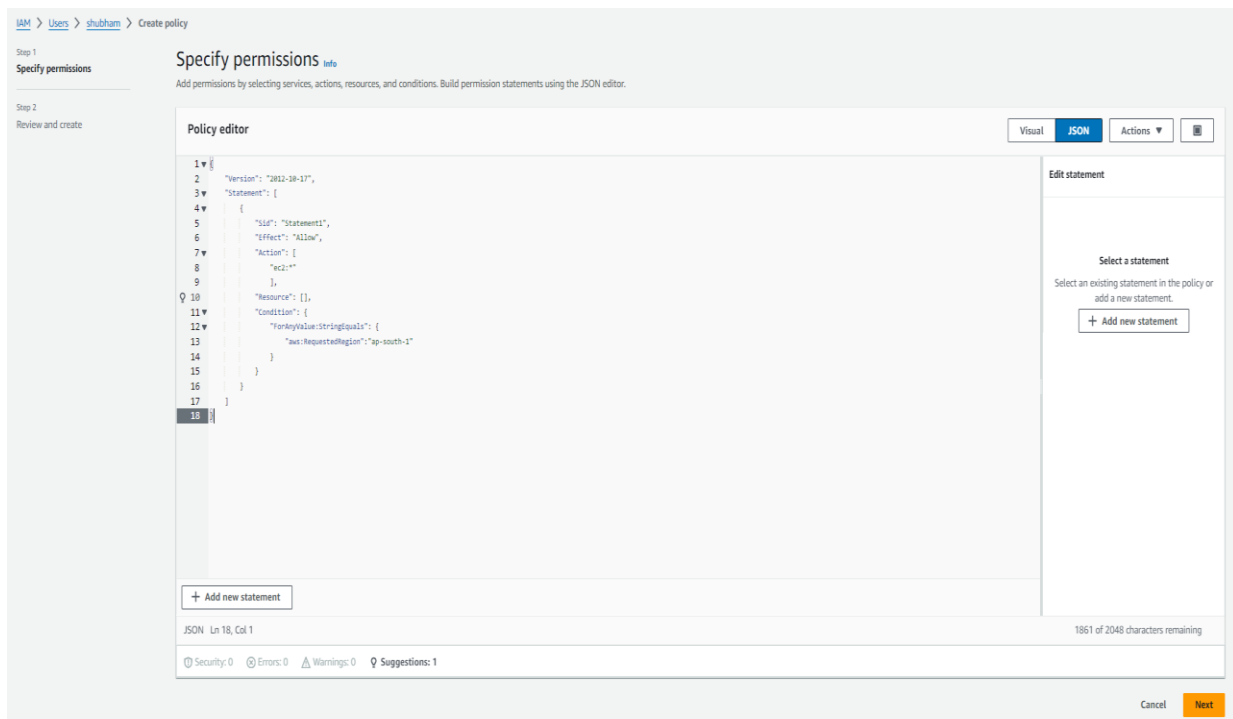
**Click on user which is present in IAM console**

**Select the user(in our case shubham)**

**Go to permission policy and click on add permission then click on create inline policy**

**Click next and**

**Add policy to it**



**8.Scenario: You are a DevOps engineer responsible for managing AWS resources for your company's e-commerce application. Your company uses S3 to store**

product images, and you need to grant specific permissions to different teams within your organization.

**Task:** Your task is to set up IAM users and policies to manage access to the S3 buckets containing product images. Here are the steps you need to follow:

**Create IAM Groups:**

Create two IAM groups: "Marketing" and "Developers."

**Create IAM Policies:**

Create an IAM policy called "MarketingAccess" that allows read-only access to the S3 bucket containing product images. Attach this policy to the "Marketing" group.

Create an IAM policy called "DevAccess" that allows both read and write access to the same S3 bucket. Attach this policy to the "Developers" group.

**Create IAM Users:**

Create two IAM users: "Shubham" and "Deepak"

Add "Shubham" to the "Marketing" group and "Deepak" to the "Developers" group.

**Configure S3 Bucket Permissions:**

Configure the S3 bucket containing product images with a bucket policy that allows read-only access for the "Marketing" group and read/write access for the "Developers" group.

**Testing:**

Log in to the AWS Management Console as "Shubham" (Marketing team) and verify that he can only read the product images from the S3 bucket.

Log in to the AWS Management Console as "Deepak" (Developers team) and verify that he can both read and write product images to the S3 bucket.

## Documentation:

### Step 1- create S3 bucket

#### Go to S3 console


click on ->Create bucket

Select->AWS Region

Click on ->create bucket

[Amazon S3](#) > [Buckets](#) > Create bucket

## Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#) 


### General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1 ▼

Bucket name [Info](#)

new-demo-bucket-new


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

### ► Advanced settings

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

Cancel [Create bucket](#)

### Step 2- Creating an IAM group for marking

#### Go to the IAM console



**Click on user group**

**Click on create group for marketing and developers**

**Name the group(marketing and for second group developers)**

The image displays two screenshots of the AWS IAM console's 'Create user group' page. Both screenshots show the left-hand navigation pane with 'Identity and Access Management (IAM)' selected, and a search bar labeled 'Search IAM'. The main content area is titled 'Create user group' and includes a breadcrumb trail: 'IAM > User groups > Create user group'.

**Top Screenshot:** The 'Name the group' section shows the 'User group name' field with the text 'Marketing' entered. Below the field, a note states: 'Maximum 128 characters. Use alphanumeric and '+', '@', '-' characters.'

**Bottom Screenshot:** This screenshot shows the same page after the 'Marketing' group has been created. A green success banner at the top reads 'Marketing user group created.' with a 'View group' button. The 'User group name' field now contains the text 'Developers'.

**Step 3- Create IAM policies Marketing Access**

**Go to IAM console**

**Click on policies**

**Click on create policy**

**Choose JSON type for the creation of policy**


**Enter the name as marketing access**

**Click on create**

Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

Visual JSON Actions 

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Statement1",
6       "Effect": "Allow",
7       "Action": [
8         "s3:GetObject"
9       ],
10      "Resource": [
11        "arn:aws:s3:::product-image"
12      ]
13    }
14  ]
}
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

+ Add new statement

JSON Ln 14, Col 1

6000 of 6144 characters remaining

🛡️ Security: 0 🚫 Errors: 0 ⚠️ Warnings: 0 💡 Suggestions: 0

Cancel **Next**

**Step 4- Create IAM policies Developer Access**

**Go to IAM console**

**Click on policies**

**Click on create policy**

**Choose JSON type for the creation of policy**

**Enter the name as Developer access**

**Click on create**

## Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

**Policy editor**

VisualJSONActions

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Statement1",
6       "Effect": "Allow",
7       "Action": [
8         "s3:GetObject",
9         "s3:PutObject"
10      ],
11      "Resource": [
12        "arn:aws:s3::product-image"
13      ]
14    }
15  ]
}
```

+ Add new statement

**Edit statement**

Select a statement  
Select an existing statement in the policy or add a new statement.

+ Add new statement

## Step 5- Attach the policies to groups

Click on IAM console

Click on user group

Select marketing

Go to permission add permission

Attach policy

[IAM](#) > User groups

**User groups (1/5)** [Info](#)

Delete>Create group

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

☐

Akshay-group

0

Defined

9 days ago

☐

demo-group

1

Defined

6 hours ago

☐

Developers

0

Not defined

32 minutes ago

☒

Marketing

0

Not defined

32 minutes ago

☐

shashank-test-group

1

Not defined

20 hours ago

## Attach permission policies to Marketing

▶ Current permissions policies (0)

## Other permission policies (1/908)

You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.

Q marketing X Filter by Type All types 1 match < 1 > ⚙

| <input checked="" type="checkbox"/> | Policy name                     | Type             | Used as | Description |
|-------------------------------------|---------------------------------|------------------|---------|-------------|
| <input checked="" type="checkbox"/> | <a href="#">MarketingAccess</a> | Customer managed | None    | -           |

Cancel

Attach policies

## Step 6- Same for the Developer

## Attach permission policies to Developers

▶ Current permissions policies (0)

## Other permission policies (1/908)

You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.

Q deve X Filter by Type All types 4 matches < 1 > ⚙

| <input type="checkbox"/>            | Policy name   | Type             | Used as | Description                                  |
|-------------------------------------|---|------------------|---------|--|
| <input type="checkbox"/>            | <a href="#">AmazonCognitoDeveloperAuthenticatedIdentities</a> | AWS managed      | None    | Provides access to Amazon Cognito APIs t...  |
| <input type="checkbox"/>            | <a href="#">AWSCodeBuildDeveloperAccess</a>                   | AWS managed      | None    | Provides access to AWS CodeBuild via the ... |
| <input type="checkbox"/>            | <a href="#">AWSProtonDeveloperAccess</a>                      | AWS managed      | None    | Provides access to the AWS Proton APIs a...  |
| <input checked="" type="checkbox"/> | <a href="#">DeveloperAccess</a>                               | Customer managed | None    | -  |

Cancel

Attach policies

## Step 7- Create IAM user

Go to IAM console

Click to users

Create shubham user

Click next

Add permission select marketing

Click next

# Click create user

IAM > Users > Create user

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

shubham

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.

SHUBHAM@123

- 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 ( ! @ # \$ % ^ & \* ( ) \_ + - { } | ' )

☒ 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](#)

Cancel

Next

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.

User groups (1/5)

☐

Alshay-group

0

[AmazonEC2FullAccess](#), [AmazonS3FullAccess](#) and 2 more

2023-12-13 (9 days ago)

☐

demo-group

1

[AmazonS3FullAccess](#)

2023-12-23 (7 hours ago)

☐

Developers

0

[DeveloperAccess](#)

2023-12-23 (44 minutes ago)

☒

Marketing

0

[MarketingAccess](#)

2023-12-23 (44 minutes ago)

☐

shashank-test-group

1

-

2023-12-22 (20 hours ago)

Set permissions boundary - optional

Cancel

Previous

Next

## Step 8- Create IAM user for developer

## Go to IAM console

## Click to users

## Click create user

Cancel Next

[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.

User groups (1/5)

☐

Group name

▲

☐

Users

▼

☐

Attached policies

▼

☐

Created

▼

|                                     |                                     |   |   |                             |
|-------------------------------------|-------------------------------------|---|---|-----------------------------|
| <input type="checkbox"/>            | <a href="#">Aishay-group</a>        | 0 | <a href="#">AmazonEC2FullAccess</a> , <a href="#">AmazonS3FullAccess</a> and 2 more | 2023-12-13 (9 days ago)     |
| <input type="checkbox"/>            | <a href="#">demo-group</a>          | 1 | <a href="#">AmazonS3FullAccess</a>  | 2023-12-23 (7 hours ago)    |
| <input checked="" type="checkbox"/> | <a href="#">Developers</a>          | 0 | <a href="#">DeveloperAccess</a>   | 2023-12-23 (46 minutes ago) |
| <input type="checkbox"/>            | <a href="#">Marketing</a>           | 0 | <a href="#">MarketingAccess</a>   | 2023-12-23 (47 minutes ago) |
| <input type="checkbox"/>            | <a href="#">shashank-test-group</a> | 1 | -   | 2023-12-22 (20 hours ago)   |

► Set permissions boundary - optional

Cancel

Previous

Next

## Step 9- Testing for shubham user

Shubham (marketing team) and he only have read only permission so it fail to create bucket and upload the files

Services

[Alt+S]

Global

Shubham1 @ th

Amazon S3

> Buckets

▼ Account snapshot

View Storage Lens dashboard

Last updated: Dec 21, 2023 by Storage Lens. Metrics are generated every 24 hours. Metrics don't include directory buckets. [Learn more](#)

|               |              |                     |   |
|---------------|--------------|---------------------|---|
| Total storage | Object count | Average object size | You can enable advanced metrics in the "default-account-dashboard" configuration. |
| 26.0 B        | 1            | 26.0 B              |   |

General purpose buckets

Directory buckets

General purpose buckets (5) [Info](#)

< 1 >

| Name  | AWS Region                       | Access  | Creation date                           |
|---|----------------------------------|---|---|
| <input type="radio"/> <a href="#">b12345y</a> | Asia Pacific (Mumbai) ap-south-1 | <a href="#">Bucket and objects not public</a> | December 22, 2023, 19:56:32 (UTC+05:30) |

Upload failed  
View details below.

## Upload: status

Close

The information below will no longer be available after you navigate away from this page.

### Summary

Destination  
s3://taskbucket122

Succeeded  
0 files, 0 B (0%)

Failed  
1 file, 1.9 KB (100.00%)

In case of Deepak(Developer team) and he have read and write permission  
So he create bucket and uplaod the files

Amazon S3 > Buckets > taskbucket122

## taskbucket122

Objects

Properties

Permissions

Metrics

Management

Access Points

### Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Copy S3 URI Copy URL Download Open Delete Actions Create folder  
Upload

Find objects by prefix

Show versions

< 1 >

|  | Name          | Type | Last modified                              | Size    | Storage class |
|--|---------------|------|--|---------|---------------|
|  | products.html | html | December 22, 2023,<br>18:37:35 (UTC+05:30) | 22.0 KB | Standard      |

Upload succeeded  
View details below.

## Upload: status

Close

The information below will no longer be available after you navigate away from this page.

### Summary

Destination  
s3://taskbucket122

Succeeded  
1 file, 1.2 KB (100.00%)

Failed  
0 files, 0 B (0%)