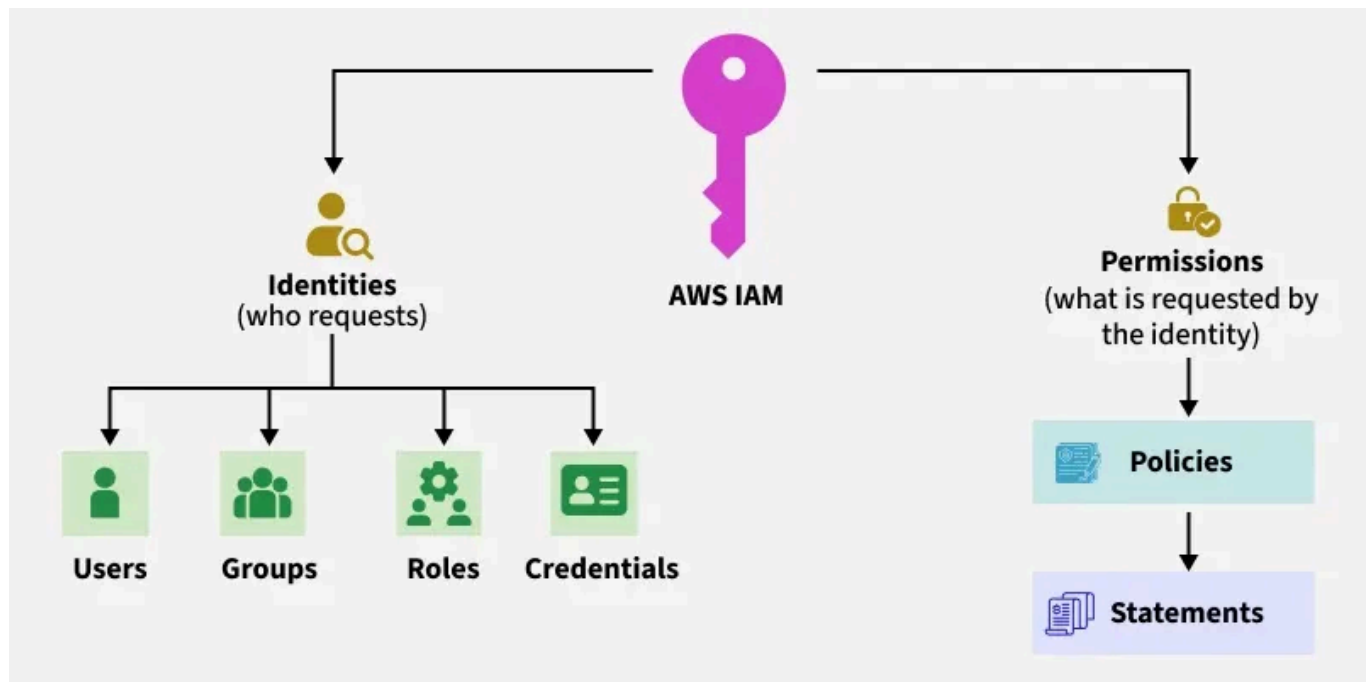


# IAM(Identity Access Management)

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. With IAM, you can manage permissions that control which AWS resources users can access. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources. IAM provides the infrastructure necessary to control authentication and authorization for your AWS accounts.



-> For owner account have a full permission

-> for IAM user have zero permission

**how to create a IAM :**

go to user and create user

The screenshot shows the 'Specify user details' step of the AWS IAM 'Create user' process. The left sidebar shows a progress bar with four steps: Step 1 (Specify user details), 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 the following sections:

- User details**
  - User name**: A text input field. Below it, a note states: '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**  
In addition to console access, users with SignInLocalDevelopmentAccess permissions can use the same console credentials for programmatic access without the need for access keys.
- Console password**
  - ☒ **Autogenerated password**  
You can view the password after you create the user.
  - ☐ **Custom password**  
Enter a custom password for the user.  
Below this is a password input field with a strength indicator.
    - 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.

A blue information box at the bottom states: '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](#)'

set permission

The screenshot shows the 'Set permissions' step of the AWS IAM 'Create user' process. The left sidebar shows a progress bar with four steps: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password). The main content area is titled 'Set permissions' and contains the following sections:

- 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 (1440)**  
Choose one or more policies to attach to your new user.  
Below this is a search bar and a 'Filter by Type' dropdown menu. A table lists available policies with columns for 'Policy name', 'Type', and 'Attached entities'.

Policy name	Type	Attached entities
<a href="#">AccessAnalyzerServiceRolePolicy</a>	AWS managed	0
<a href="#">AccountManagementFromVercel</a>	AWS managed	0
<a href="#">AdministratorAccess</a>	AWS managed - job function	0
<a href="#">AdministratorAccess-Amplify</a>	AWS managed	0
<a href="#">AdministratorAccess-AWSElasticBeanstalk</a>	AWS managed	0
<a href="#">AIOpsAssistantIncidentReportPolicy</a>	AWS managed	0
<a href="#">AIOpsAssistantPolicy</a>	AWS managed	0
<a href="#">AIOpsConsoleAdminPolicy</a>	AWS managed	0
<a href="#">AIOpsOperatorAccess</a>	AWS managed	0
<a href="#">AIOpsQuickSetupAccess</a>	AWS managed	0

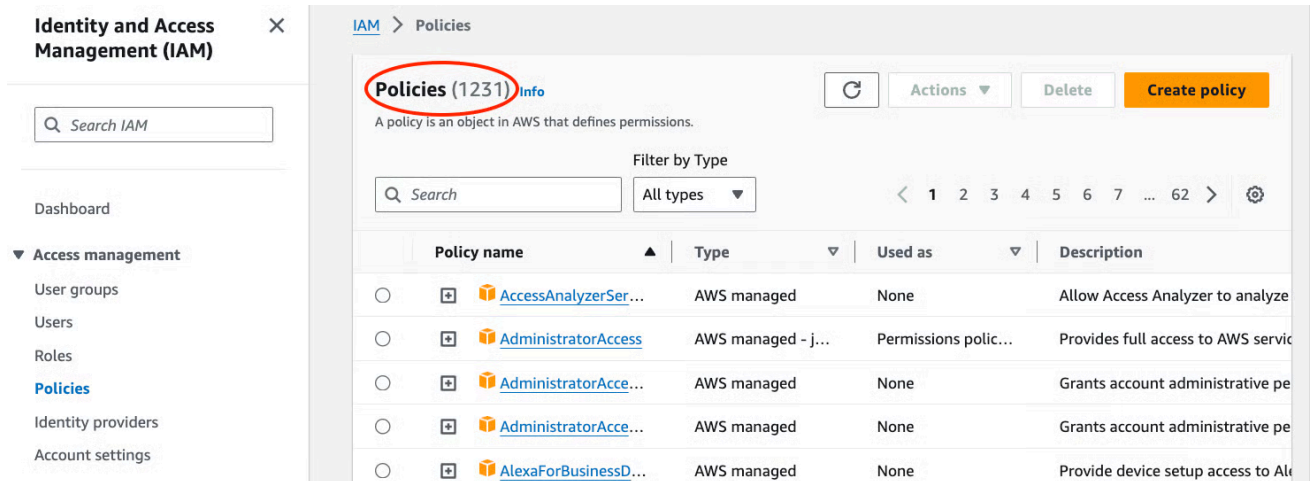
using this create the user.

## Creating and attaching policies to users, groups, and roles:

Creating and attaching policies to users, groups, and roles in AWS is pretty straightforward.

### Creating a policy:

- To create a policy, click “Policies” in the IAM console left-hand menu and click “Create Policy.”
- You can define your policy using the visual editor or the JSON tab. The visual editor is easier if you’re not familiar with JSON. For example, to create a policy that allows read-only access to S3, you can select the “S3 service” and then choose the “read-only” actions.
- Once you’ve defined the policy, click “Review policy.” Then, give your policy a name and description and click “Create policy.” At this point, your custom policy should be created.



## Attaching policies to users

- If you want to attach a policy to a user, go to “Users” in the IAM console and select the user to whom you want to attach the policy.
- Click on the “Permissions” tab and then click “Add permissions.”

Select “Attach policies directly,” find the policy you created (or any existing policy you want to attach) and choose it.

[IAM](#) > [Users](#) > [Administrator](#) > Add permissions

Step 1  
**Add permissions**

Step 2  
Review

## Add 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, inline policies, and any existing permissions boundaries 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 (1234)

Filter by Type

Search:  21 matches

<input type="checkbox"/>	Policy name <a href="#">↗</a>	Type	Atta...
<input type="checkbox"/>	 <a href="#">AmazonDMSRedshiftS3Role</a>	AWS managed	0
<input type="checkbox"/>	 <a href="#">AmazonS3FullAccess</a>	AWS managed	8

- Go to “Roles” in the IAM console and select the role to which you want to attach a policy.
- Click on the “Permissions” tab and then click “Add permissions.” This step is slightly different from what we’ve encountered previously. You’re shown the current permission policies and the complete list of other policies you can attach.