

AWS IAM Tasks Document

Overview

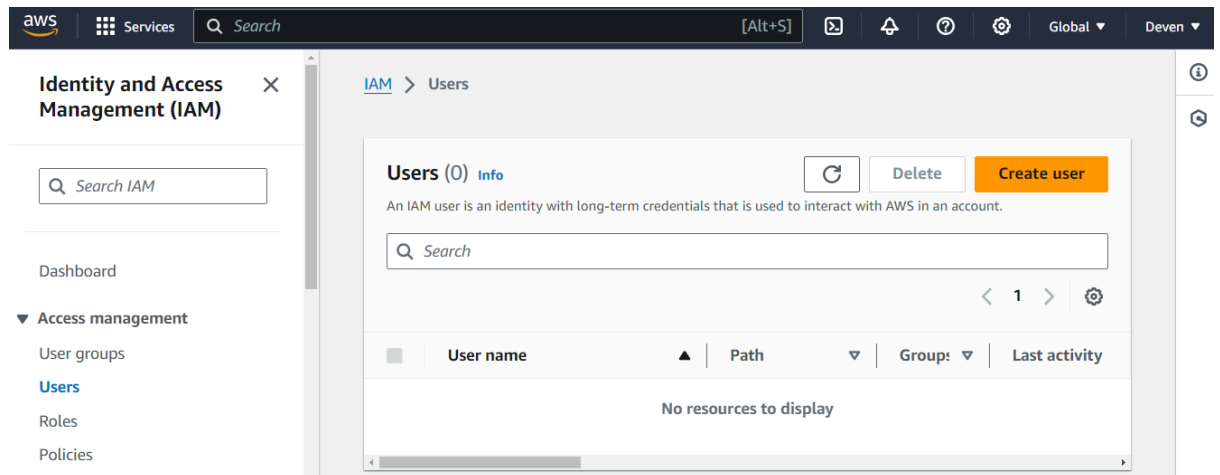
This document outlines the steps required to create IAM users, roles, and policies in AWS, including custom policies and user groups.

1. Create a User in IAM

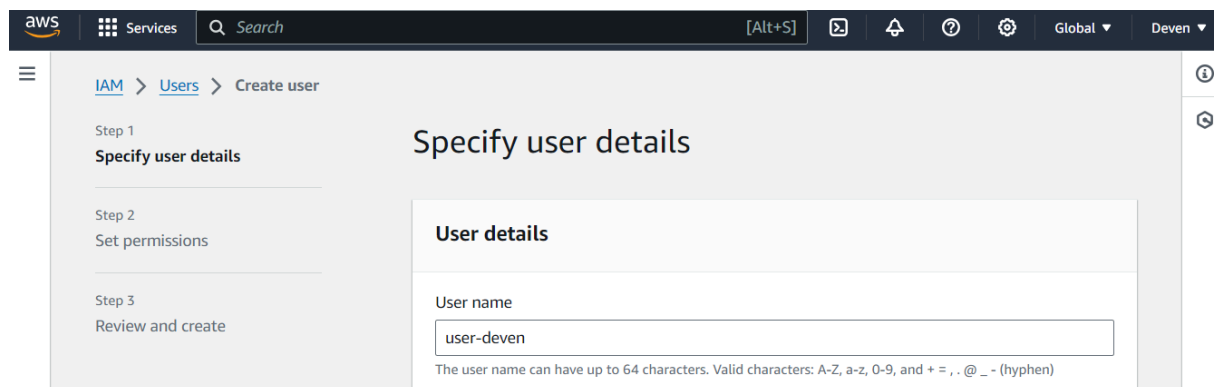
User Name: `user-deven`

Steps:

1. Go to **IAM > Users > Add user**.



2. Enter the user name `user-deven`.



3. Select **Programmatic access** and/or **AWS Management Console access** as required.

User name

user-deven

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.

4. Set a password if AWS Management Console access is selected.

Console password

☐ Autogenerated password
You can view the password after you create the user.

☒ Custom password
Enter a custom password for the user.

.....

- 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.

5. Click **Next: Permissions**.

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.

6. Click **Next: Tags** (optional) and then **Next: Review**.

The screenshot shows the AWS IAM console 'Create user' wizard at the 'Review and create' step. The left sidebar shows the progress: 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 'Review and create' and includes a sub-header 'Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.'

User details

User name user-deven	Console password type Custom password	Require password reset Yes
-------------------------	--	-------------------------------

Permissions summary

Name	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional

7. Click **Create user**.

The screenshot shows the AWS IAM console 'Create user' wizard at the 'Retrieve password' step. A green banner at the top states 'User created successfully' with a 'View user' button. The left sidebar shows the progress: 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 'Retrieve password' and includes a sub-header '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 [\[Link\]](#)

Console sign-in URL
<https://980921736064.signin.aws.amazon.com/console>

User name
user-deven

Console password
***** [Show](#)

Buttons: Cancel, Download .csv file, Return to users list

2. Create IAM Policies

2.1 Custom Policy for EC2 Instances and IAM Services

Policy Name: `EC2AndIAMFullAccessPolicy`

Description: Provides access to EC2 instances and all services in IAM.

Policy JSON:

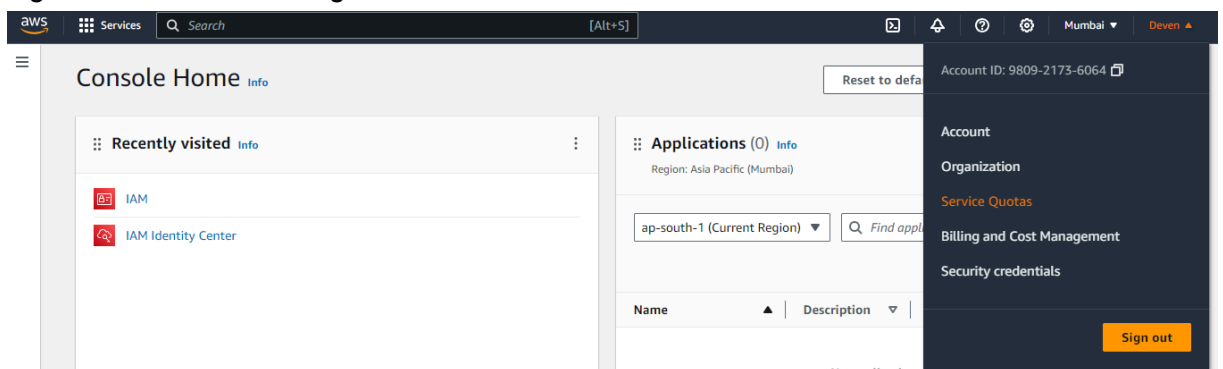
json

Copy code

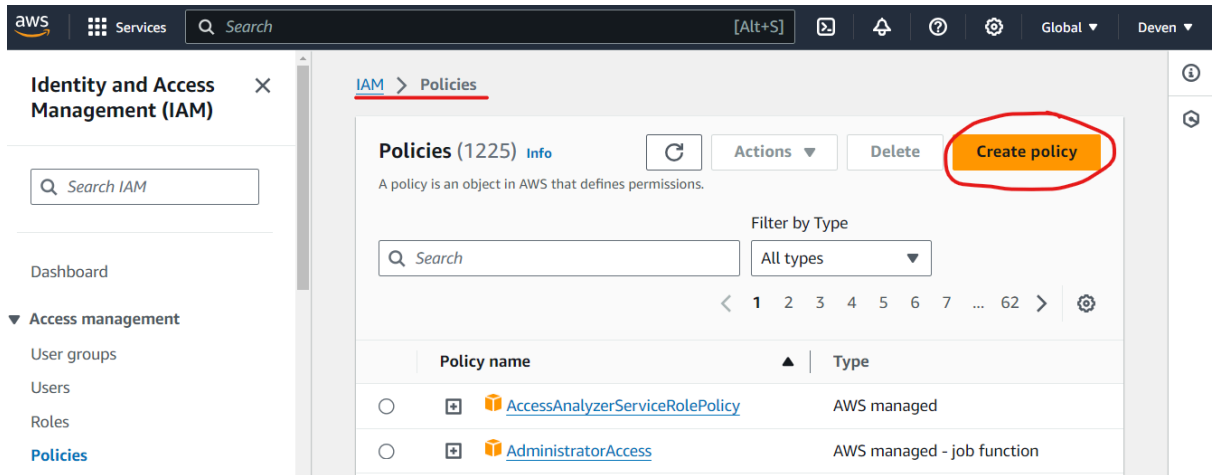
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:RunInstances",
        "ec2:DescribeVolumes",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:CreateTags",
        "ec2>DeleteTags"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:*"
      ],
      "Resource": "*"
    }
  ]
}
```

Steps:

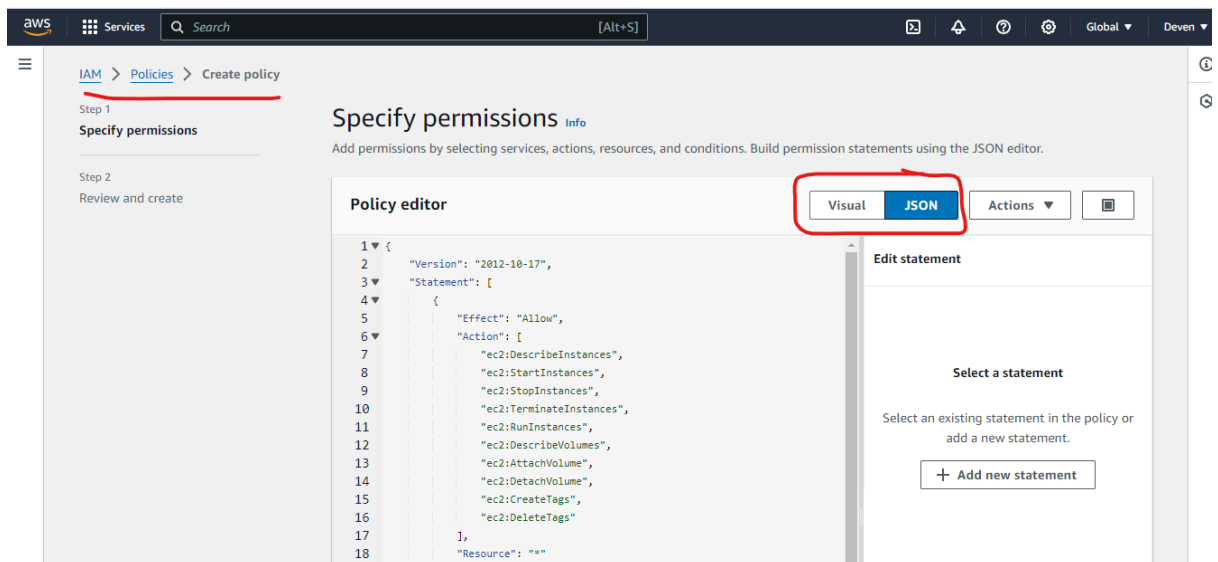
1. Sign in to the AWS Management Console.



2. Navigate to **IAM > Policies > Create policy**.



3. Switch to the **JSON** tab and paste the above policy JSON.



Note: Policy can be created using visual option easy to use

4. Click **Next: Tags** (optional) and then **Next: Review**.

```
11     "ec2:RunInstances",
12     "ec2:DescribeVolumes",
13     "ec2:AttachVolume",
14     "ec2:DetachVolume",
15     "ec2:CreateTags",
16     "ec2:DeleteTags"
17   ],
18   "Resource": "*"
19 },
20 {
21   "Effect": "Allow",
22   "Action": [
23     "iam:*"
24   ],
25   "Resource": "*"
26 }
27 ]
28 }
```

JSON Ln 7, Col 14 5805 of 6144 characters remaining

Security: 1 Errors: 0 Warnings: 1 Suggestions: 0

Check for new access

Cancel **Next**

5. Name the policy **EC2AndIAMFullAccessPolicy** and provide a description.

Review and create [Info](#)

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and '+-._@-' characters.

Description - optional
Add a short explanation for this policy.

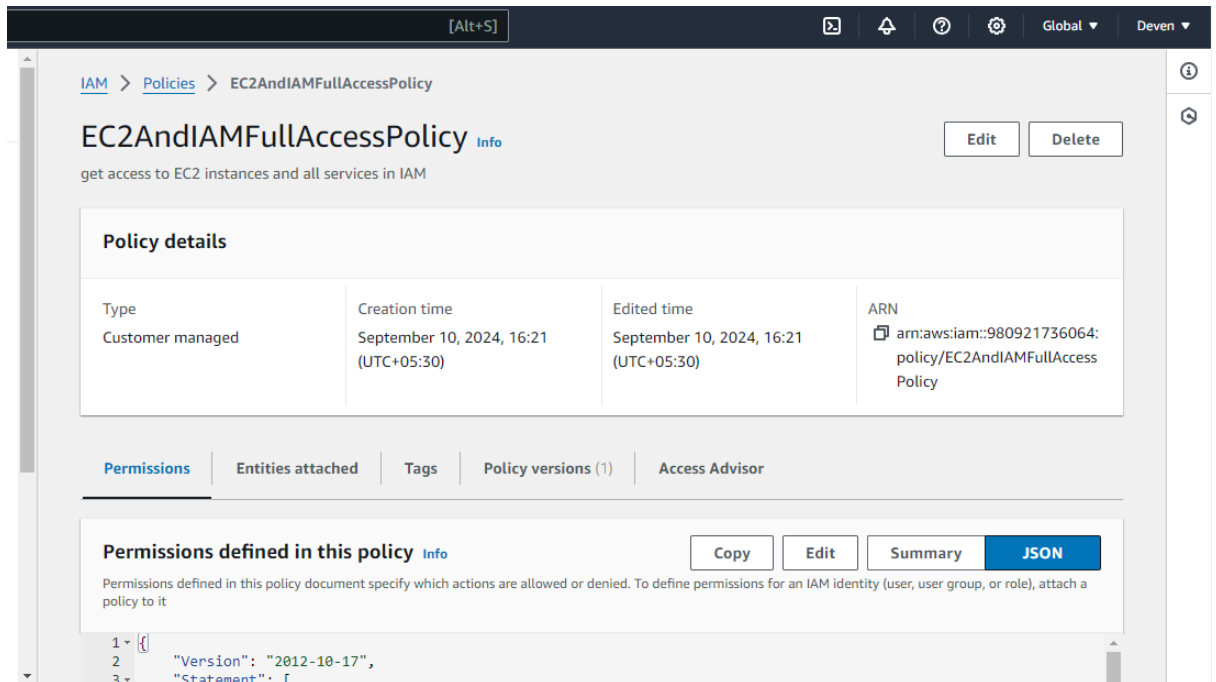
Maximum 1,000 characters. Use alphanumeric and '+-._@-' characters.

Search

Allow (2 of 421 services) ☐ Show remaining 419 services

Service	Access level	Resource	Request condition
EC2	Full: Tagging Limited: List, Write	All resources	None
IAM	Full access	All resources	None

6. Click **Create policy**.



2.2 Custom Policy for EC2 Services and IAM Users

Policy Name: EC2AndIAMUsersAccessPolicy

Description: Provides access to all EC2 services and IAM users.

Policy JSON:

json

Copy code

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "ec2:*"  
      ],  
      "Resource": "*"   
    },  
    {  
      "Effect": "Allow",  
      "Action": [  
        "iam:*"  
      ],  
      "Resource": "*"   
    }  
  ]  
}
```

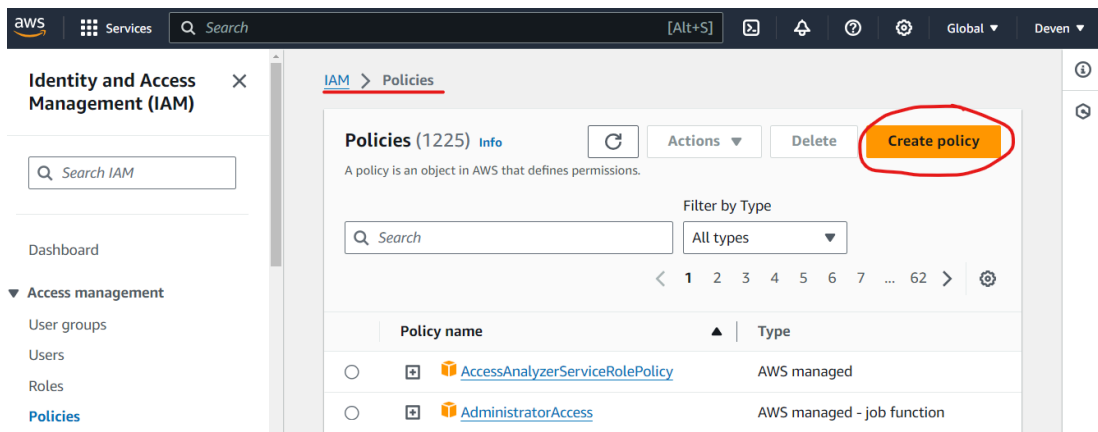
```

    "iam:ListUsers",
    "iam:GetUser"
  ],
  "Resource": "*"
}
]
}

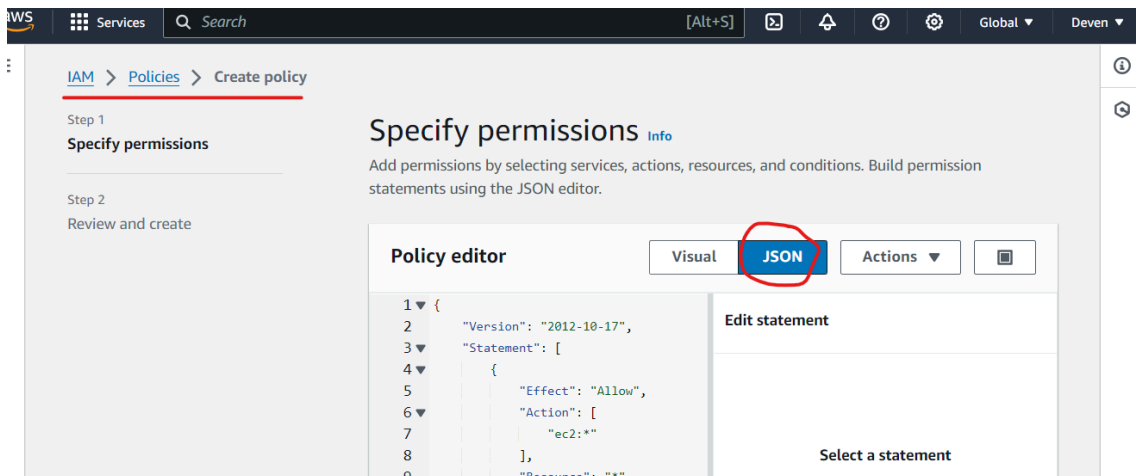
```

Steps:

1. Navigate to **IAM > Policies > Create policy**.



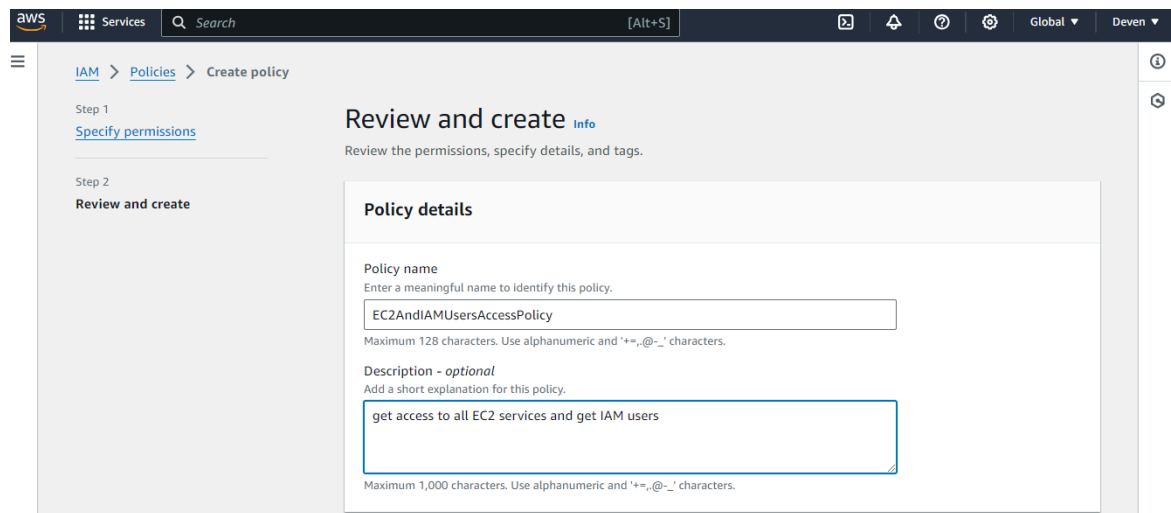
2. Switch to the **JSON** tab and paste the above policy JSON.



3. Click **Next: Tags** (optional) and then **Next: Review**.

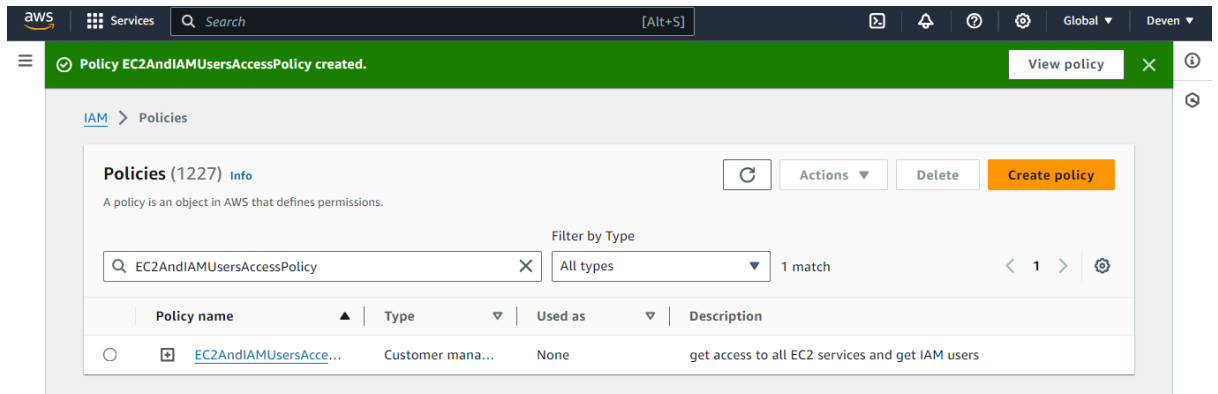


4. Name the policy **EC2AndIAMUsersAccessPolicy** and provide a description.



Allow (2 of 421 services)				Show remaining 419 services
Service	Access level	Resource	Re	
EC2	Full access	All resources	No	
IAM	Limited: List, Read	All resources	No	

5. Click **Create policy**.



3. Create a User Group

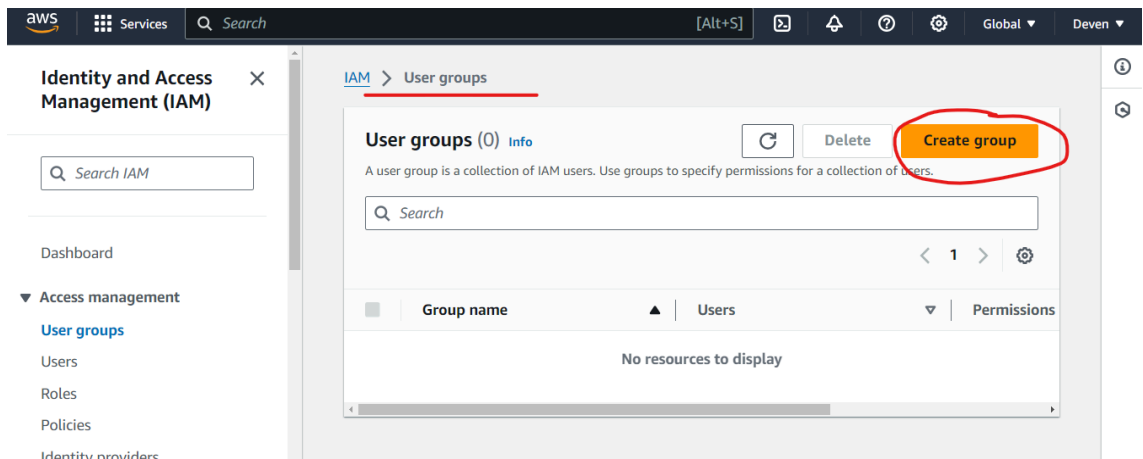
Group Name: **EC2AndIAMUsersGroup**

Policies Attached:

- **EC2AndIAMFullAccessPolicy**
- **EC2AndIAMUsersAccessPolicy**

Steps:

1. Go to **IAM > User groups > Create group**.



2. Enter the group name **EC2AndIAMUsersGroup**.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

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

IAM > User groups > Create user group

Create user group

Name the group

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

EC2AndIAMUsersGroup

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.

Search

< 1 > ⚙

3. Search for and select both **EC2AndIAMFullAccessPolicy** and **EC2AndIAMUsersAccessPolicy**. Then click **Create user group**

Attach permissions policies - Optional (2/949) 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

Search

Customer mana... 2 matches

< 1 > ⚙

<input checked="" type="checkbox"/>	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	EC2AndIAMFullAccess...	Customer man...	None	get access to EC2 instances and all ser...
<input checked="" type="checkbox"/>	EC2AndIAMUsersAcce...	Customer man...	None	get access to all EC2 services and get I...

Cancel Create user group

4. Click **Create group**.

aws Services Search [Alt+S]

EC2AndIAMUsersGroup 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

< 1 > ⚙

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	EC2AndIAMUsersGroup	0	Defined	1 minute ago

Create group

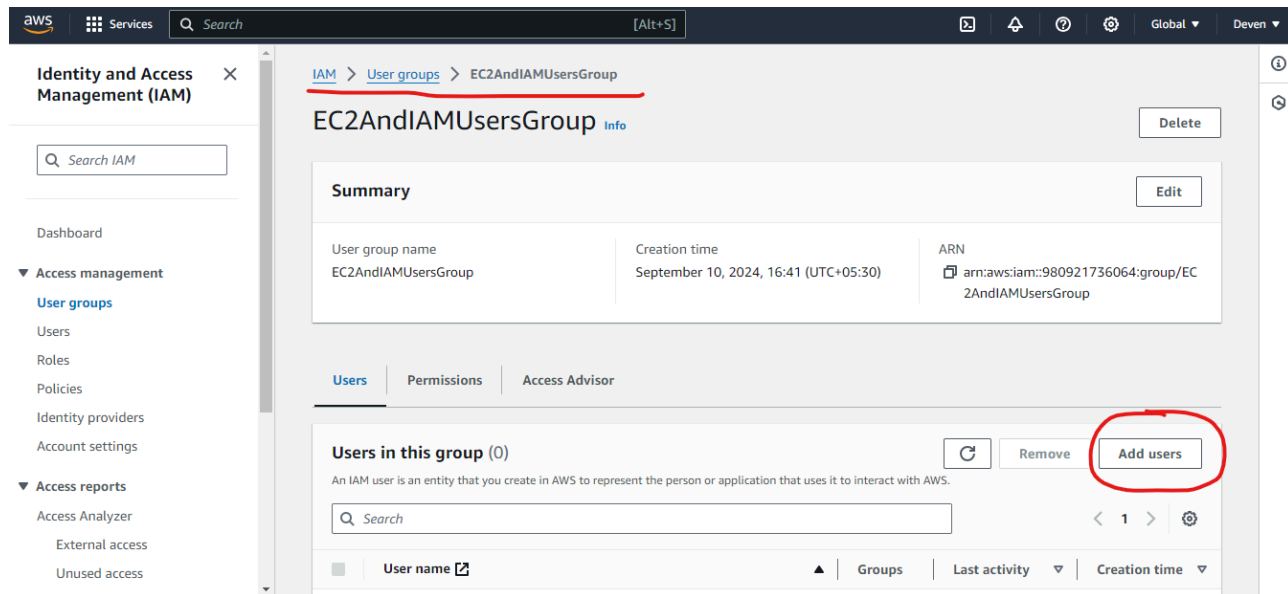
4. Assign User to Group

User Name: **user-deven**

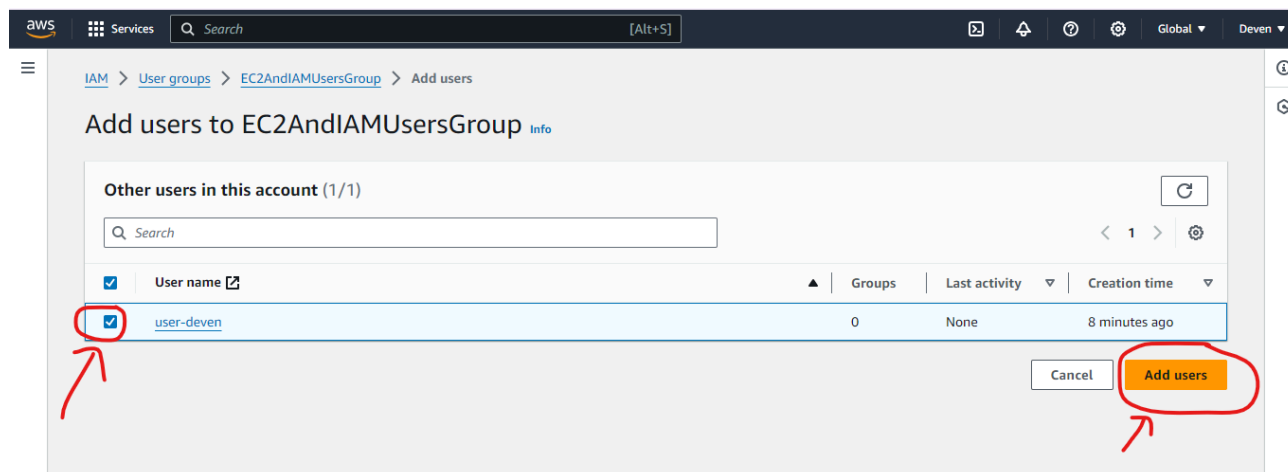
Group Assigned: **EC2AndIAMUsersGroup**

Steps:

1. Go to **IAM > User groups > EC2AndIAMUsersGroup** and click add user



2. Select the user from list (**user-deven**) and click add users



3. User added to the group.

The screenshot shows the AWS IAM console with a green notification bar at the top stating "1 user added to this group." Below this, the "Summary" tab for the "EC2AndIAMUsersGroup" is visible. The "Users (1)" tab is selected, showing a table with one user: "user-deven". The user's creation time is "September 10, 2024, 16:41 (UTC+05:30)" and their last activity is "10 minutes ago".

User name	Groups	Last activity	Creation time
user-deven	1	None	10 minutes ago

The screenshot shows the "user-deven" user details page. The "Permissions policies (3)" section is expanded, showing three policies: "EC2AndIAMFullAccessPolicy", "EC2AndIAMUsersAccessPolicy", and "IAMUserChangePassword". The "EC2AndIAMUsersAccessPolicy" is highlighted with a red box, and its "Attached via" column shows it is attached to the "Group EC2AndIAMUsersGroup".

Policy name	Type	Attached via
EC2AndIAMFullAccessPolicy	Customer managed	Group EC2AndIAMUsersGroup
EC2AndIAMUsersAccessPolicy	Customer managed	Group EC2AndIAMUsersGroup
IAMUserChangePassword	AWS managed	Directly

5. Login Verification

1. Provide the user with the AWS Management Console URL for sign-in (find this under **Dashboard > IAM Users Sign-In Link**).

The screenshot shows the "IAM Dashboard" in the AWS IAM console. A notification at the top right states "Sign-in URL copied". Below this, the "AWS Account" section shows the "Account ID" as "980921736064" and the "Account Alias" as "amazon.com/console". The "IAM users in this account" section shows a list of users, with "user-deven" highlighted. The "Quick Links" section includes a link to "My security credentials".

2. Have **user-deven** log in using the provided credentials.

eu-north-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=IT-rw9OYpHdIfwR9fbphm-WkgQh-i...

aws

Sign in as IAM user

Account ID (12 digits) or account alias

980921736064

IAM user name

user-deven

Password

☐ Remember this account

Sign in

[Sign in using root user email](#)

[Forgot password?](#)

Amazon Lightsail

Lightsail is the easiest way to get started on AWS

[Learn more »](#)

aws

You must change your password to continue

AWS account 980921736064

IAM user name user-deven

Old password *****

New password *****

Retype new password *****

Confirm password change

[Sign in using root user email](#)

English

[Terms of Use](#) [Privacy Policy](#) © 1996-2024. Amazon Web Services, Inc. or its affiliates.

3. Verify that **user-deven** can access EC2 instances and view IAM users as expected.

Search [Alt+S] Mumbai user-deven @ 9809-2173-6064

Account ID: 9809-2173-6064
IAM user: user-deven

Account

Organization

Service Quotas

Billing and Cost Management

Security credentials

Switch role Sign out

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
1	1	2	2	0

What's new

Updates for features in IAM

[View all](#)