AWS IAM Tasks Document

Overview

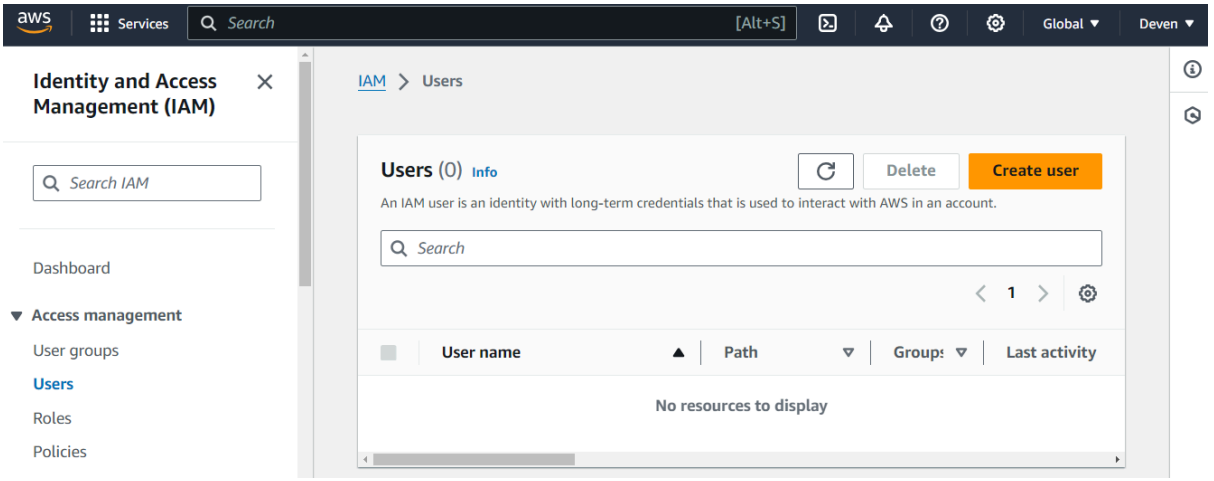
This document outlines the steps required to create IAM users, roles, and policies in AWS, including custom policies and user groups.

1. Create a User in IAM

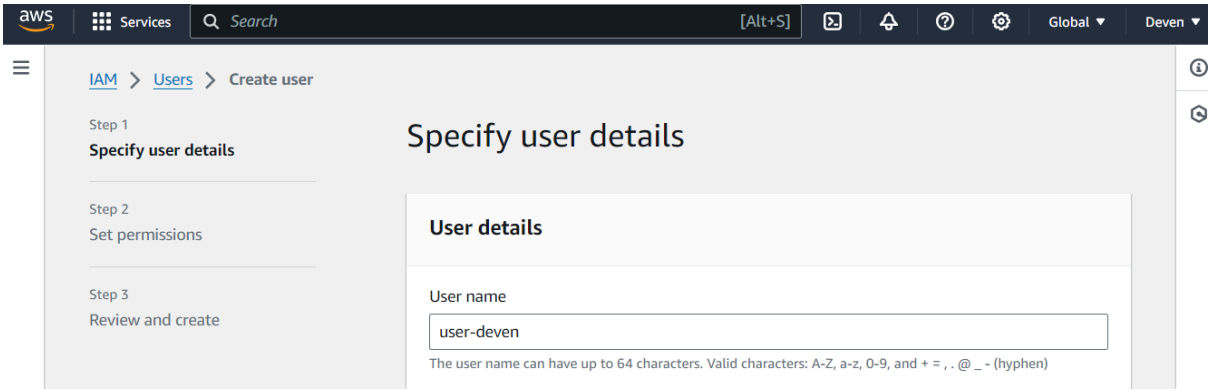
User Name: `user-deven`

Steps:

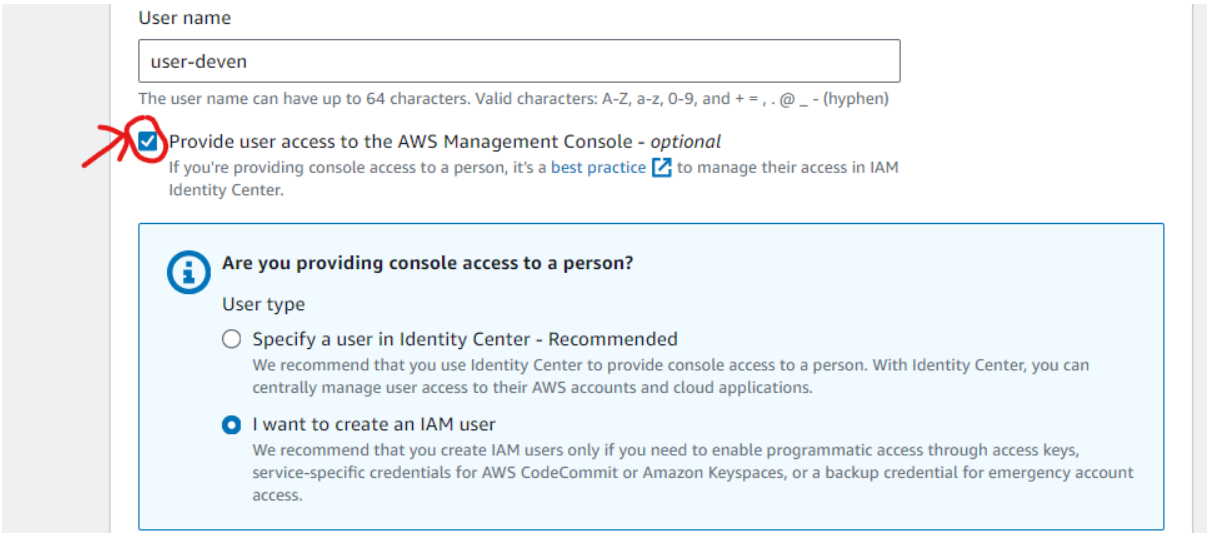
1. Go to **IAM** > **Users** > **Add user**.



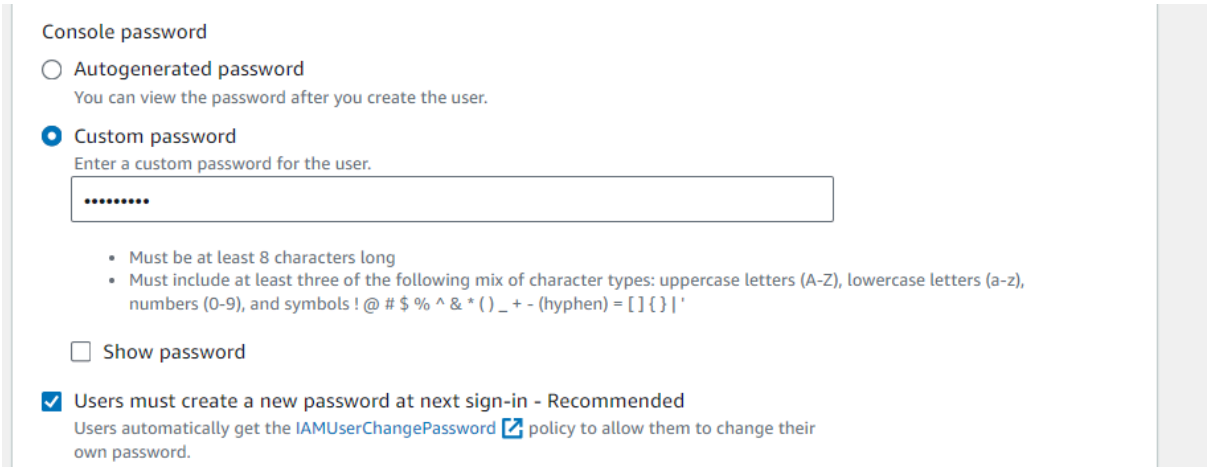
2. Enter the user name `user-deven`.



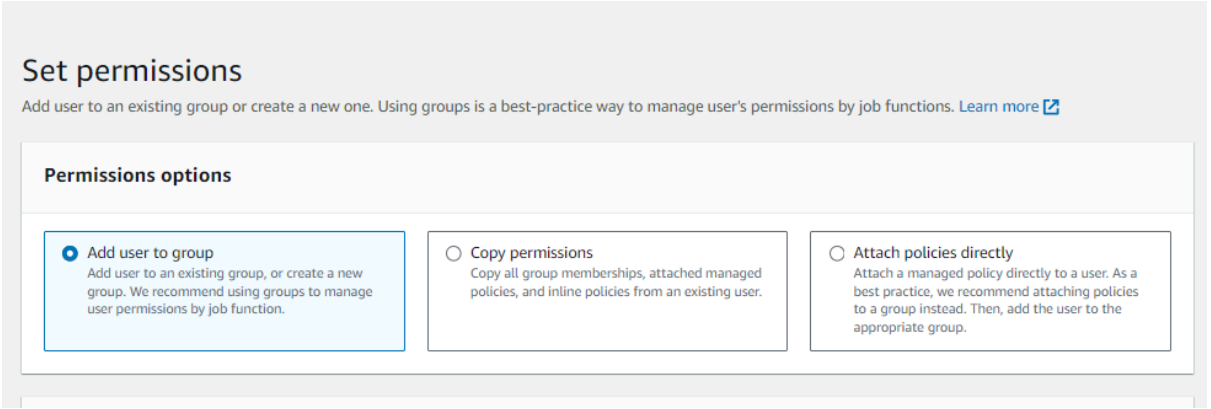
3. Select **Programmatic access** and/or **AWS Management Console access** as required.



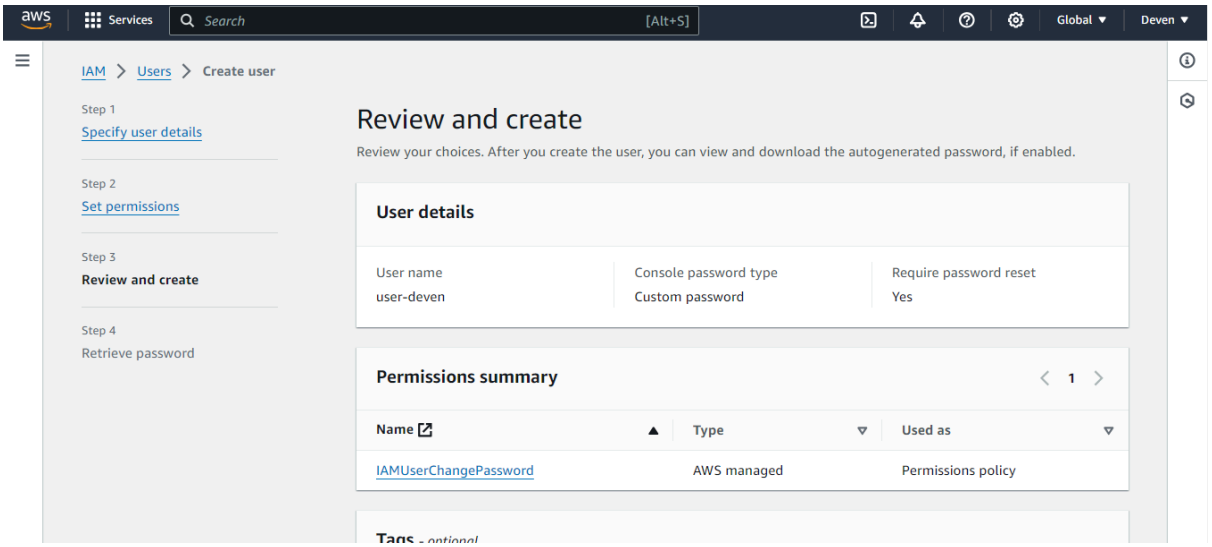
4. Set a password if AWS Management Console access is selected.



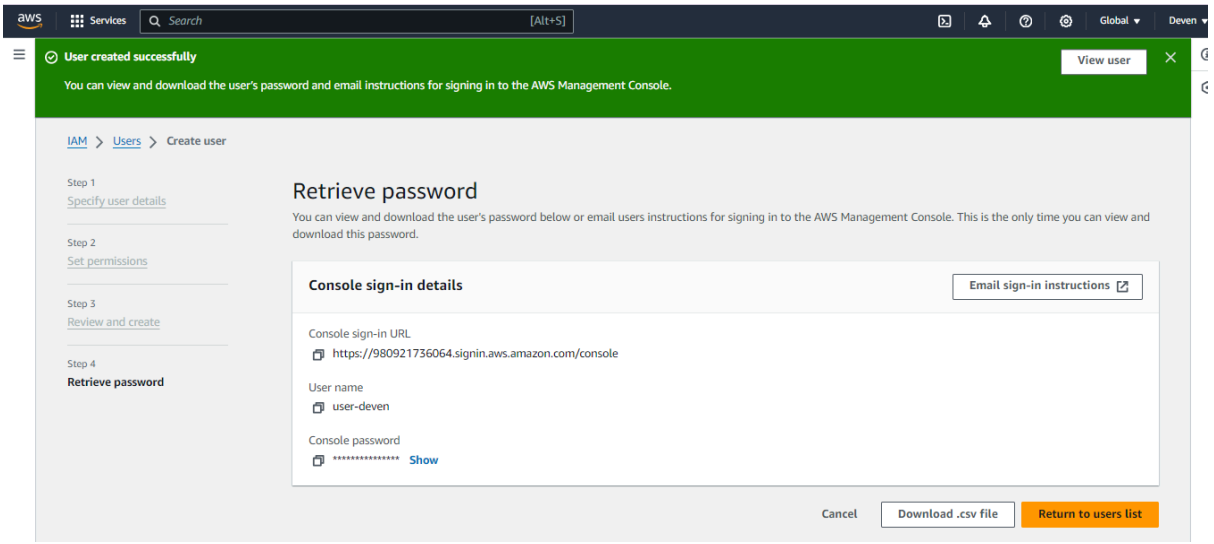
5. Click **Next: Permissions**.



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



7. Click **Create user**.



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:

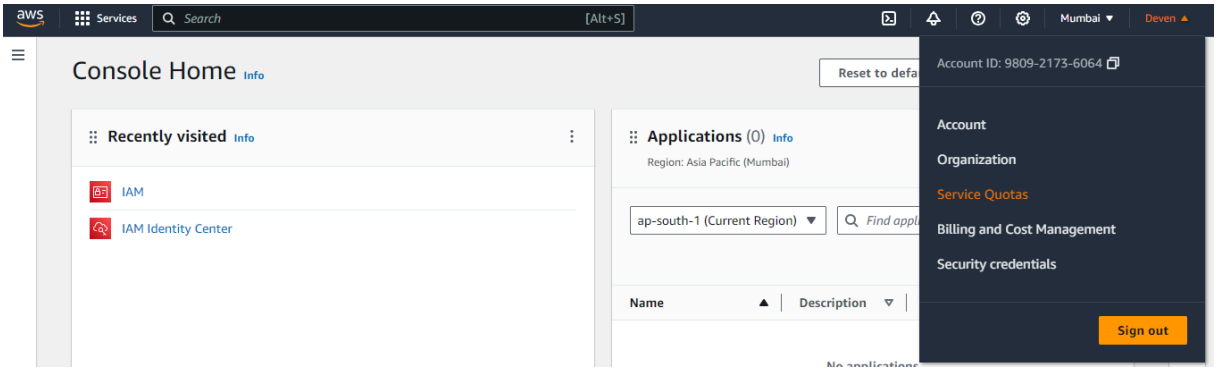
json

Copy code

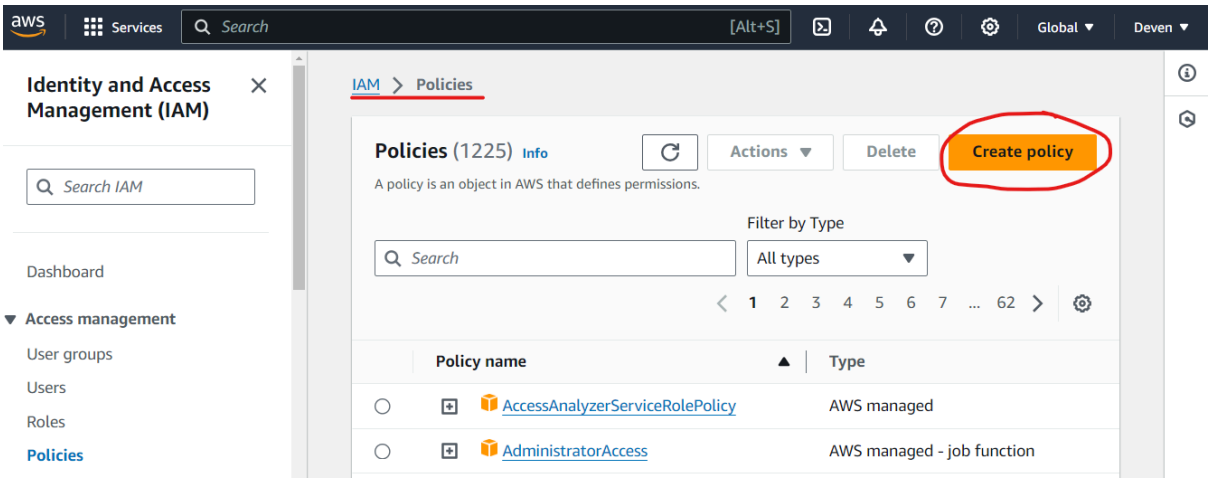
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:RunInstances",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

Steps:

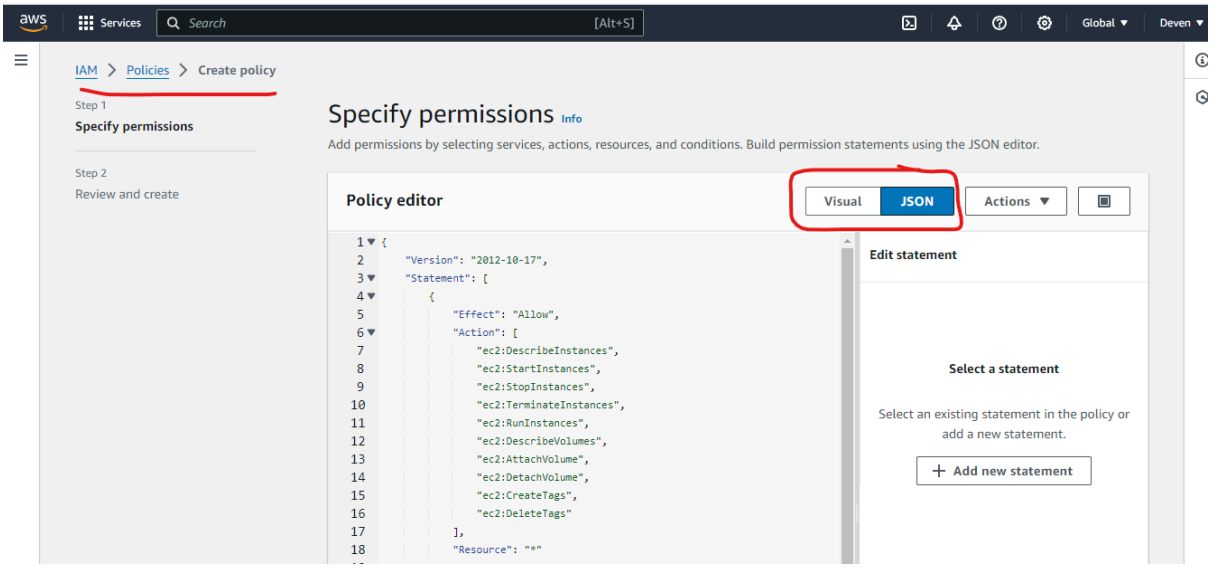
1. Sign in to the AWS Management Console.



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

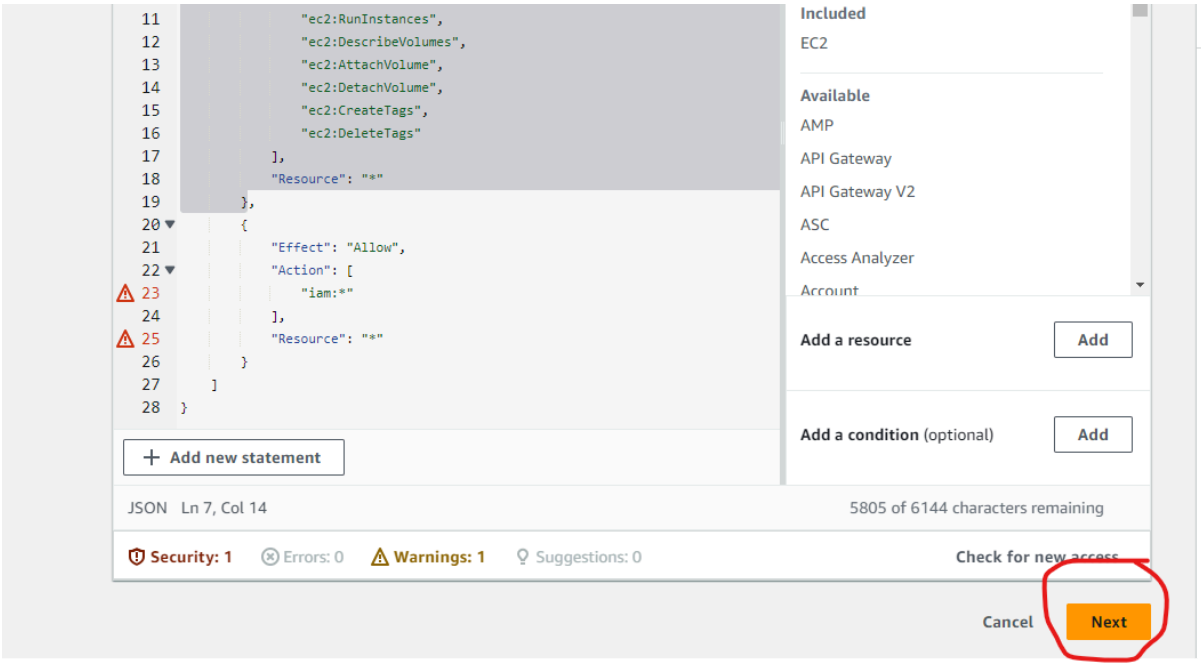


3. Switch to the **JSON** tab and paste the above policy JSON.

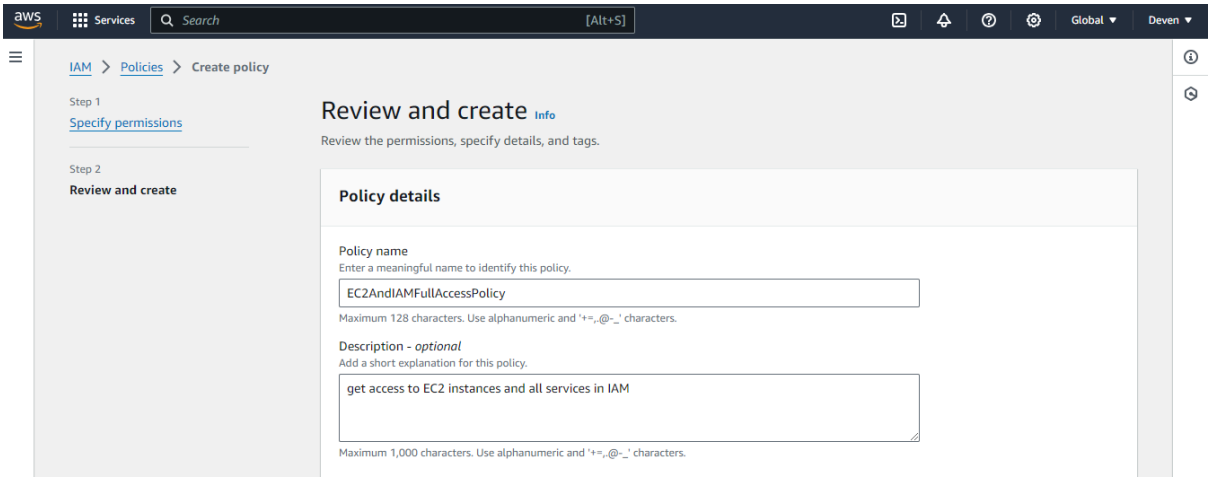


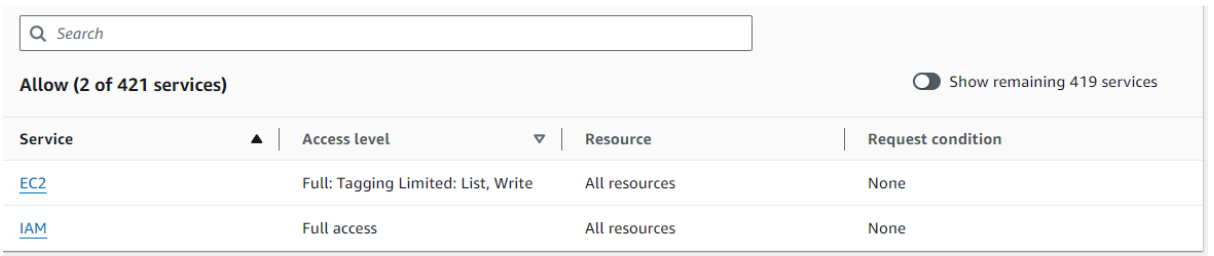
Note: Policy can be created using visual option easy to use

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

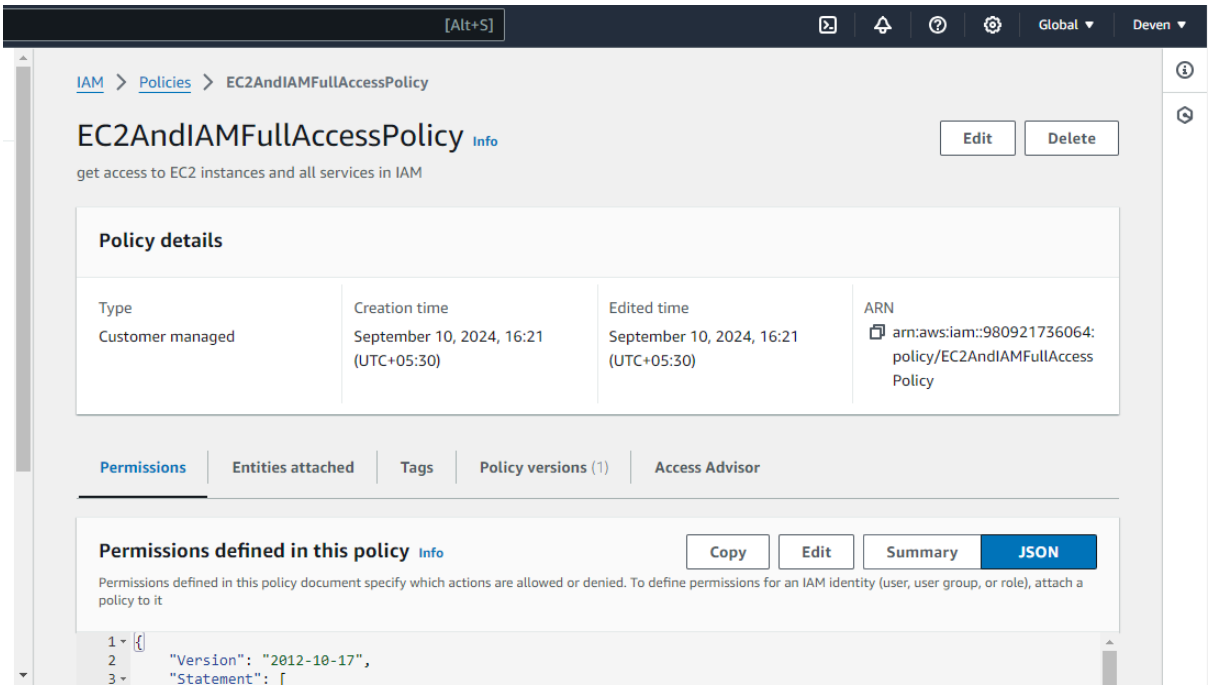


5. Name the policy `EC2AndIAMFullAccessPolicy` and provide a description.





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:

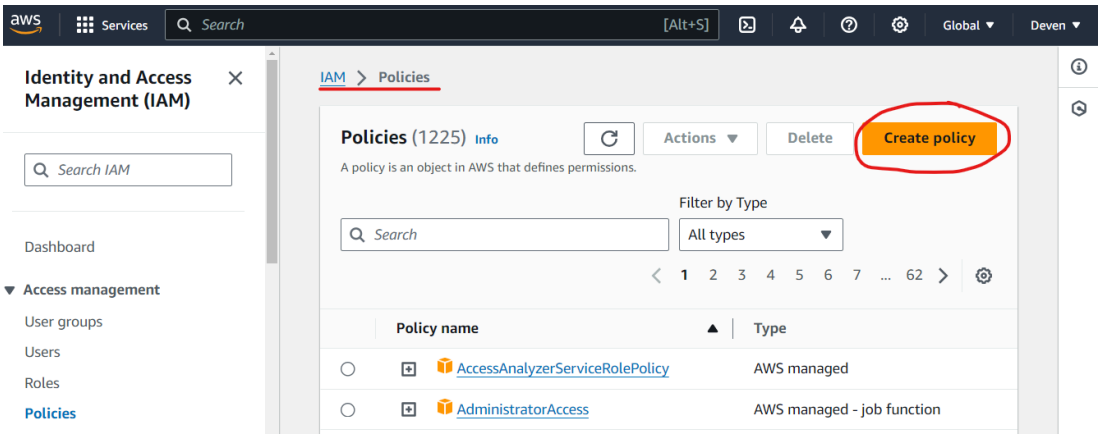
json
Copy code

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

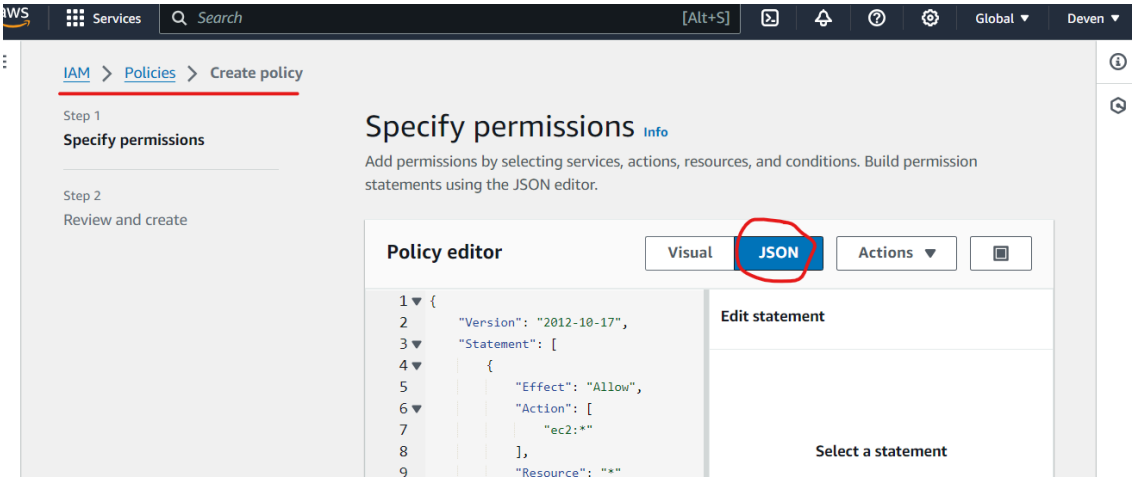
```
                "iam:ListUsers",
                "iam:GetUser"
            ],
            "Resource": "*"
        }
    ]
}
```

Steps:

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

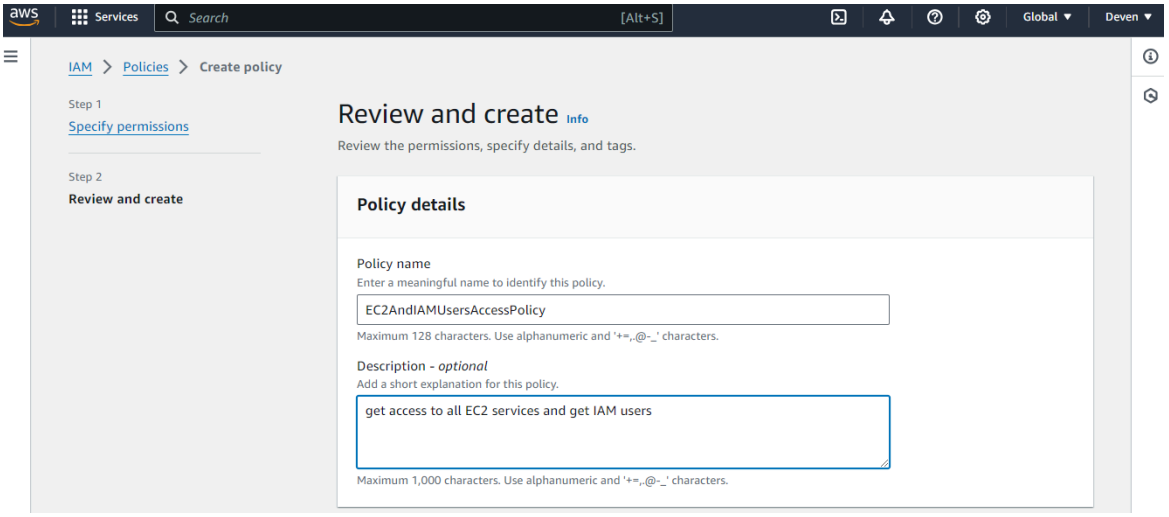


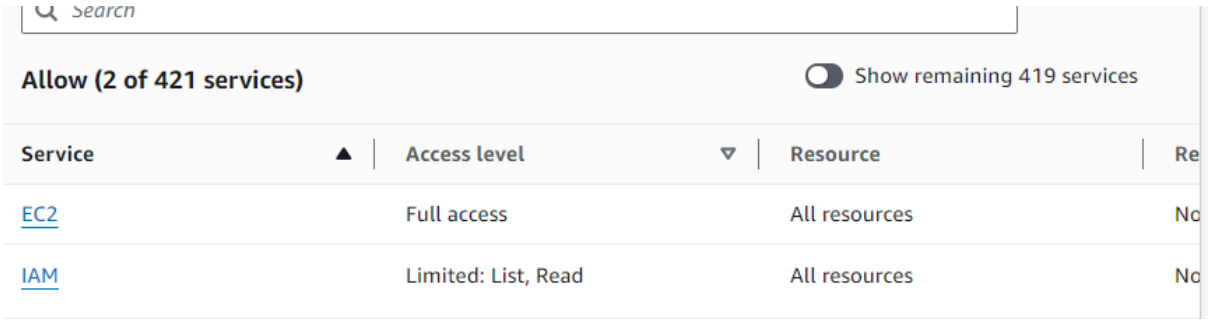
2. Switch to the **JSON** tab and paste the above policy JSON.



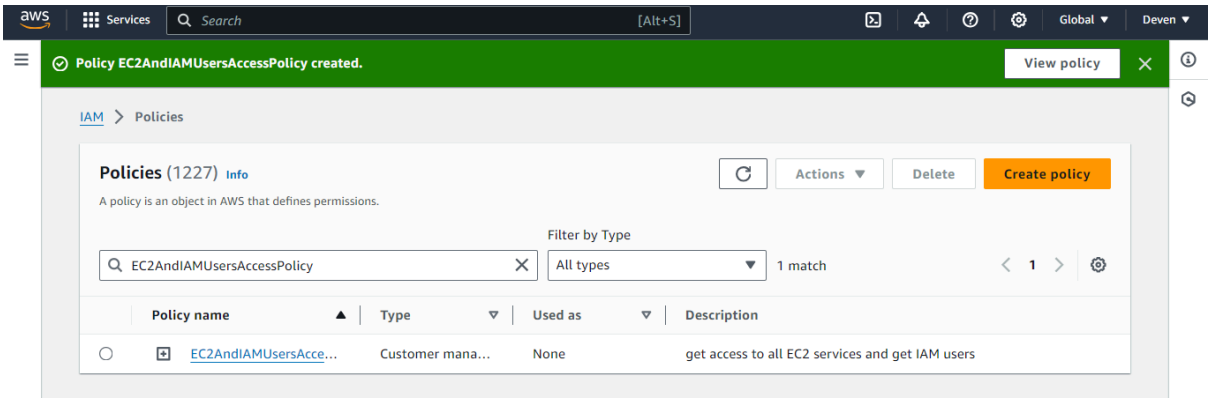
3. Click **Next: Tags** (optional) and then **Next: Review**.

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





5. Click **Create policy**.



3. Create a User Group

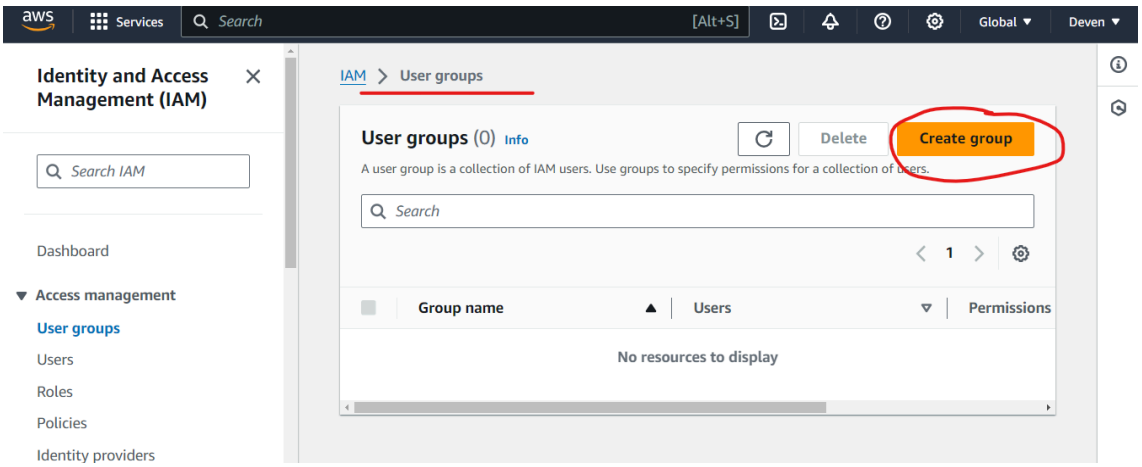
Group Name: `EC2AndIAMUsersGroup`

Policies Attached:

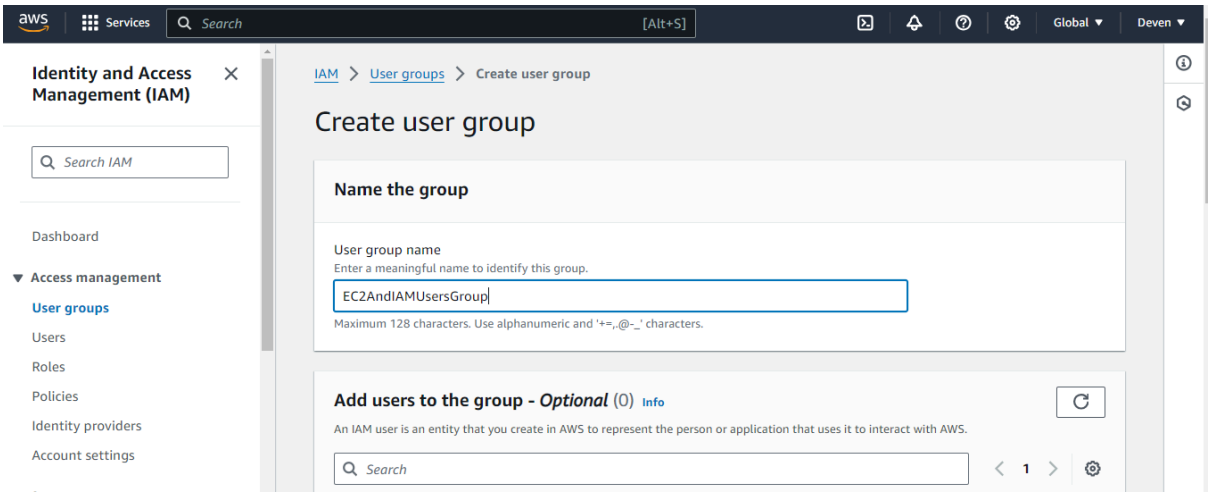
- `EC2AndIAMFullAccessPolicy`
- `EC2AndIAMUsersAccessPolicy`

Steps:

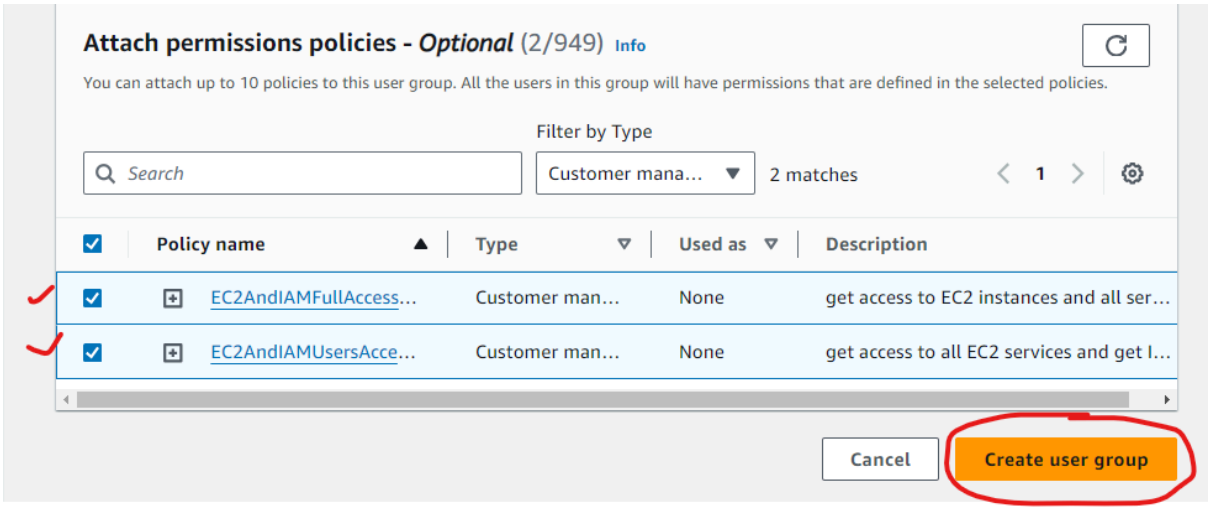
1. Go to **IAM** > **User groups** > **Create group**.



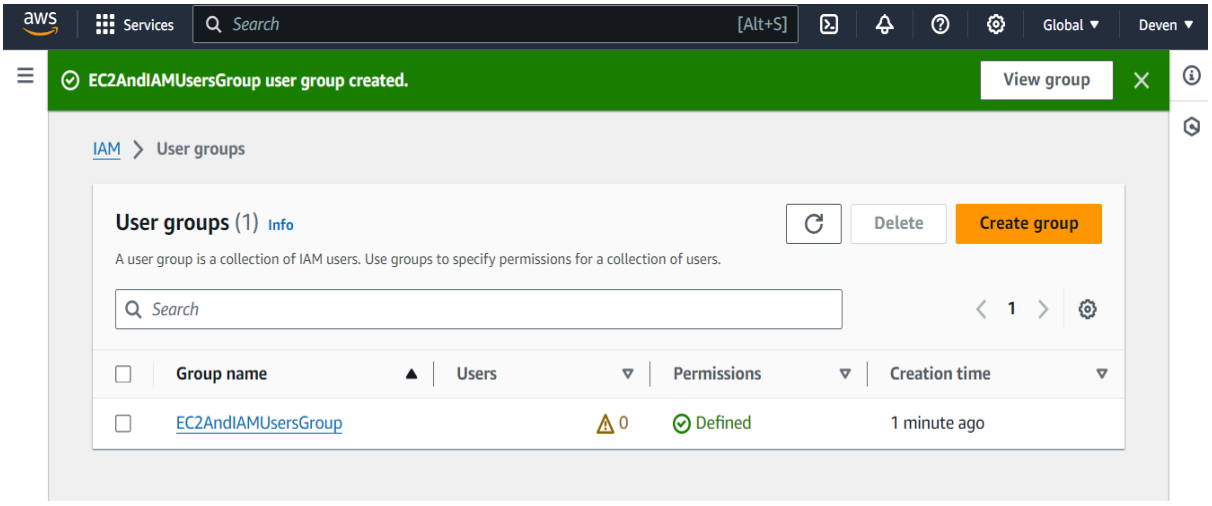
2. Enter the group name `EC2AndIAMUsersGroup`.



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



4. Click **Create group**.



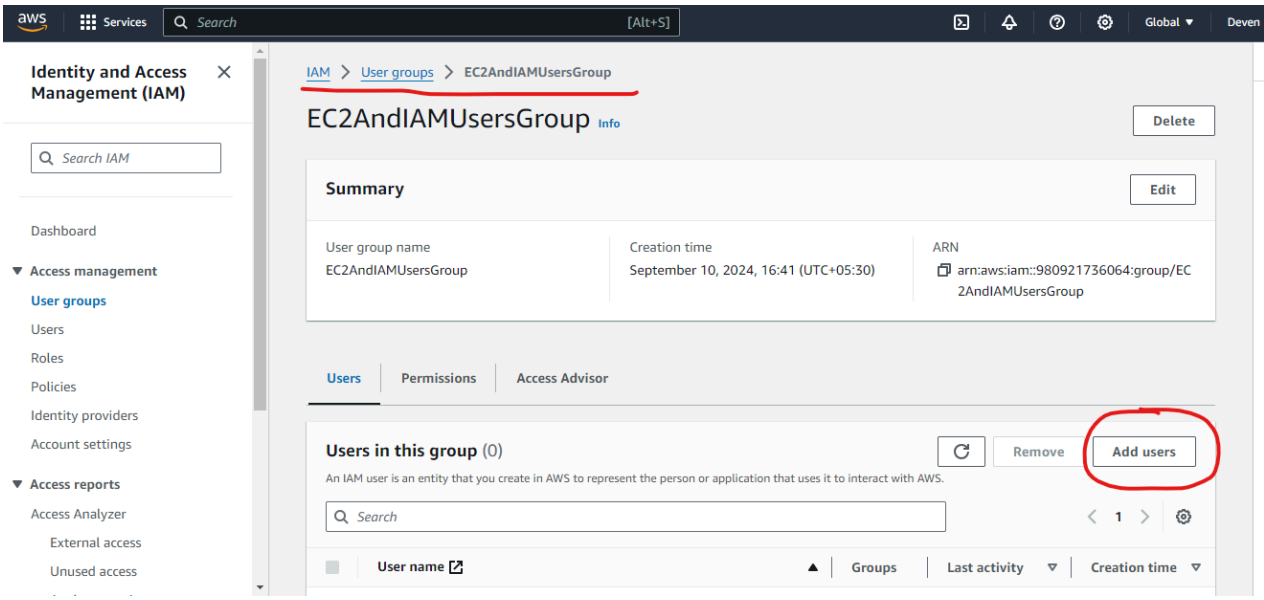
4. Assign User to Group

User Name: `user-deven`

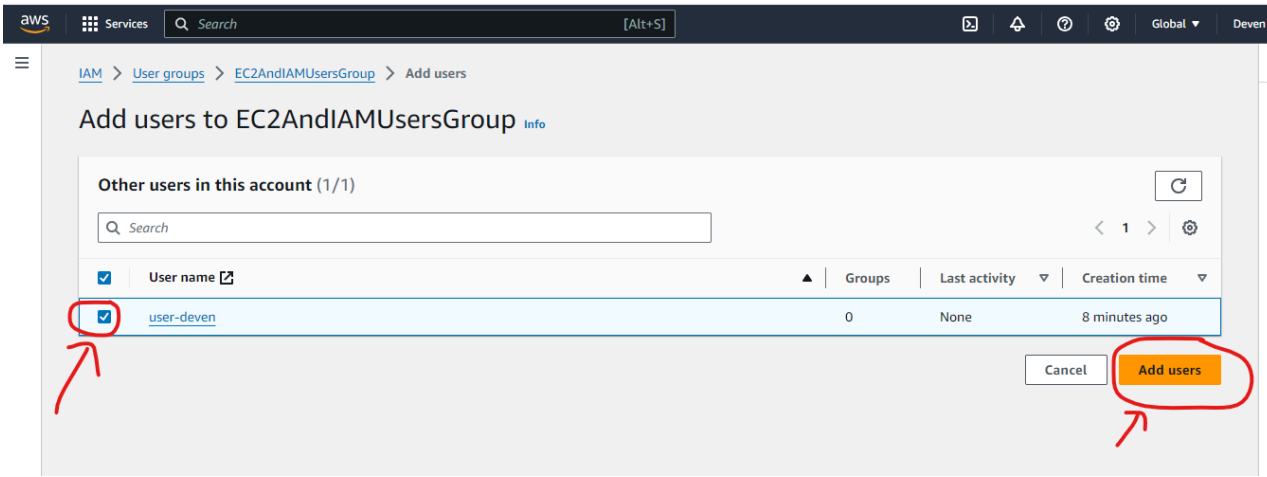
Group Assigned: `EC2AndIAMUsersGroup`

Steps:

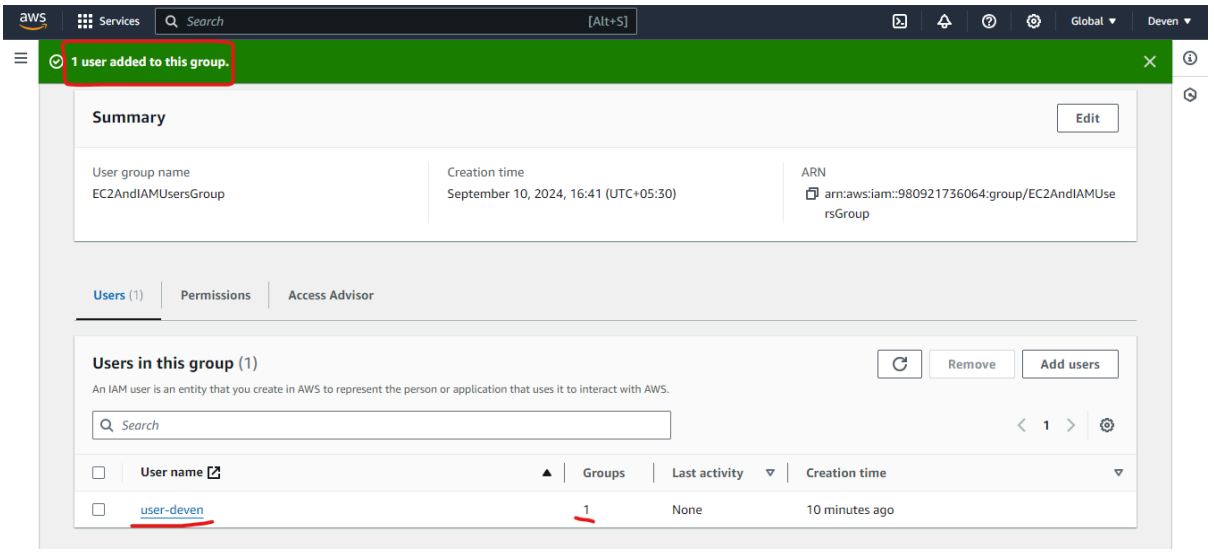
1. Go to **IAM >User groups>EC2AndIAMUsersGroup** and click add user

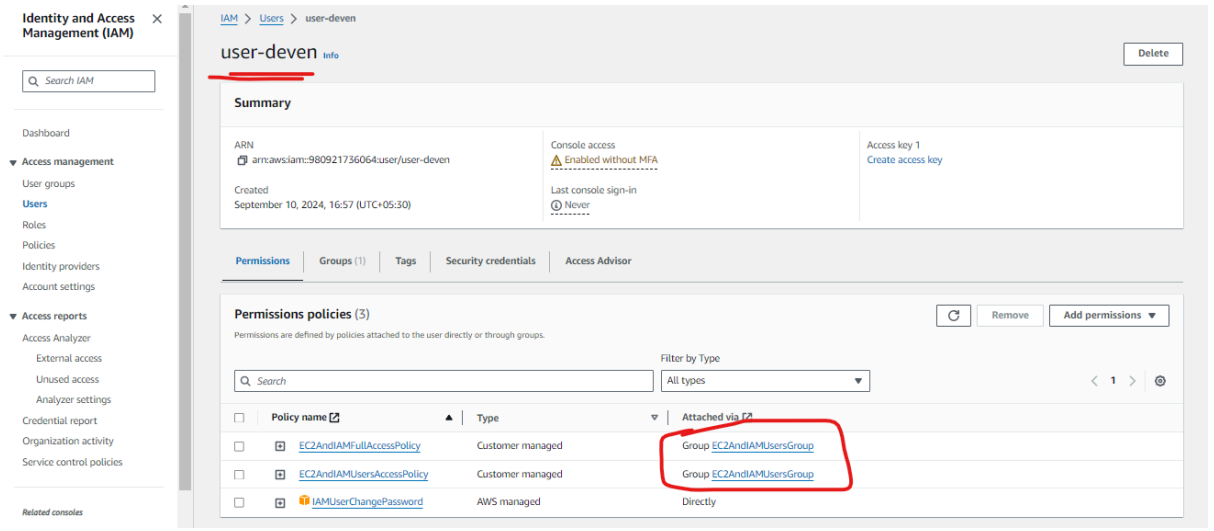


2. Select the user from list (`user-deven`) and click add users



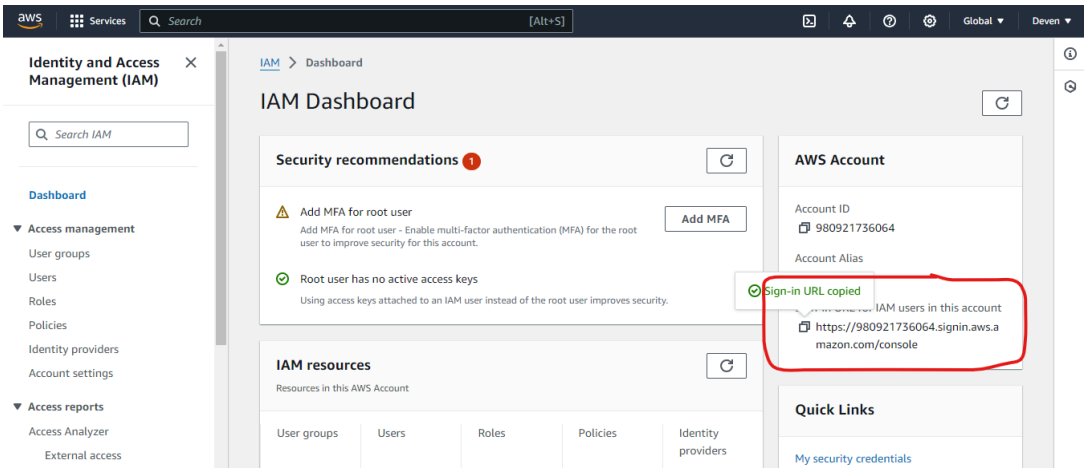
3. User added to the group.



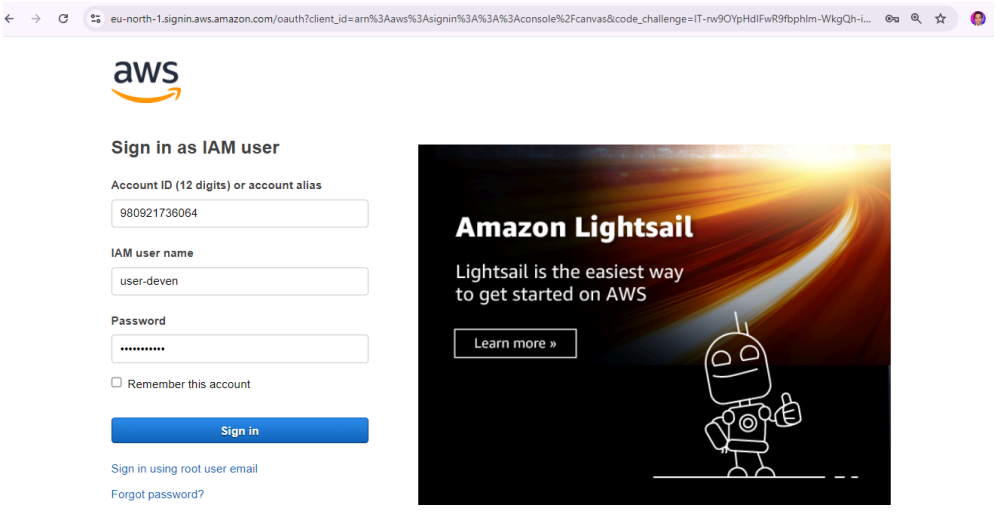


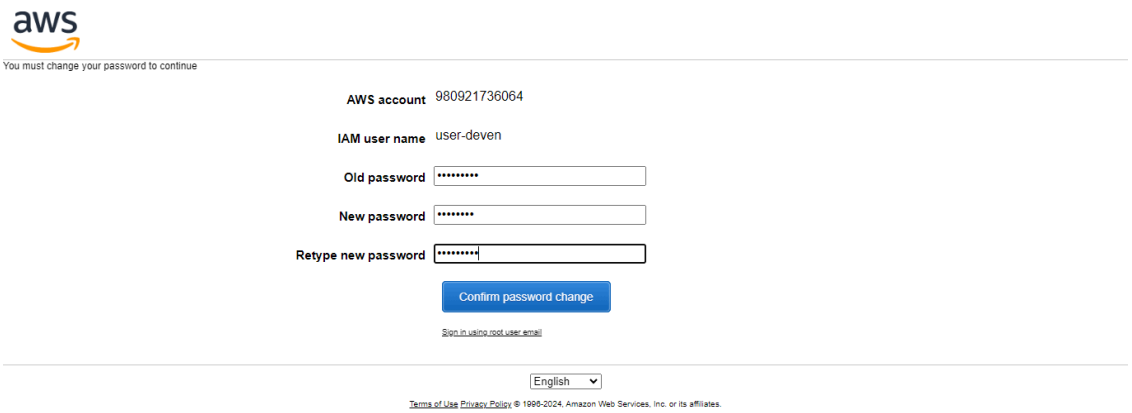
5. Login Verification

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



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





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