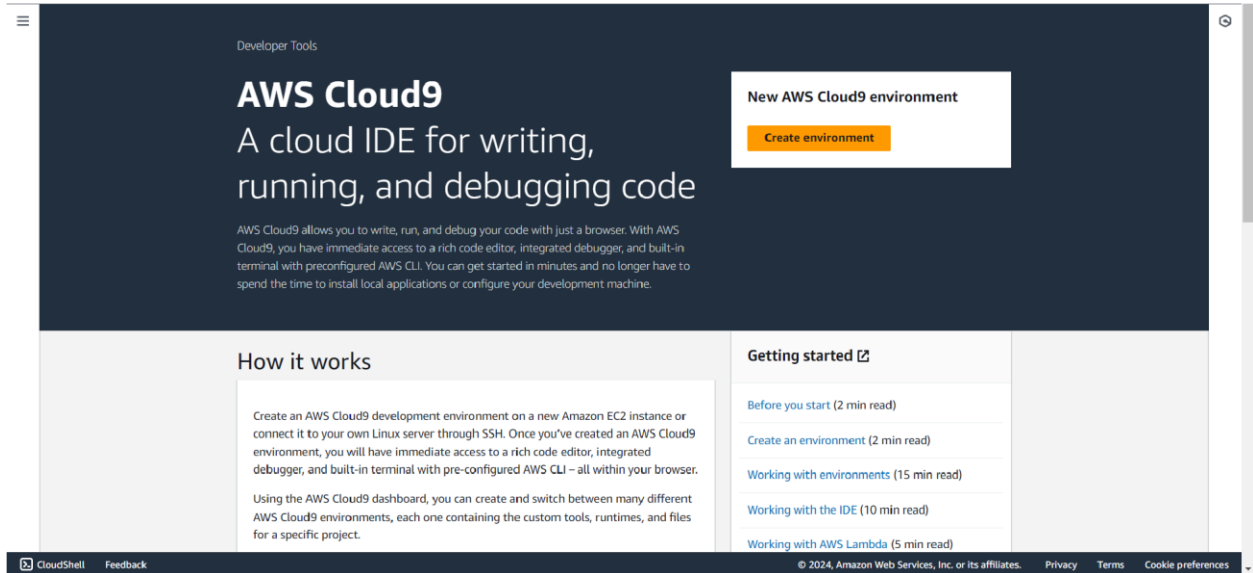
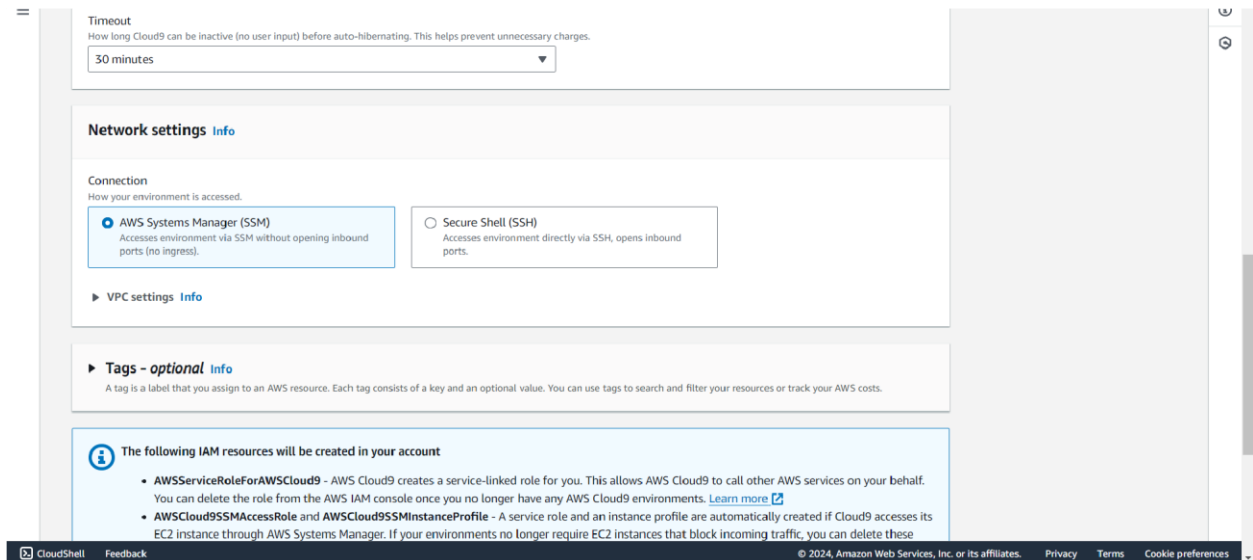


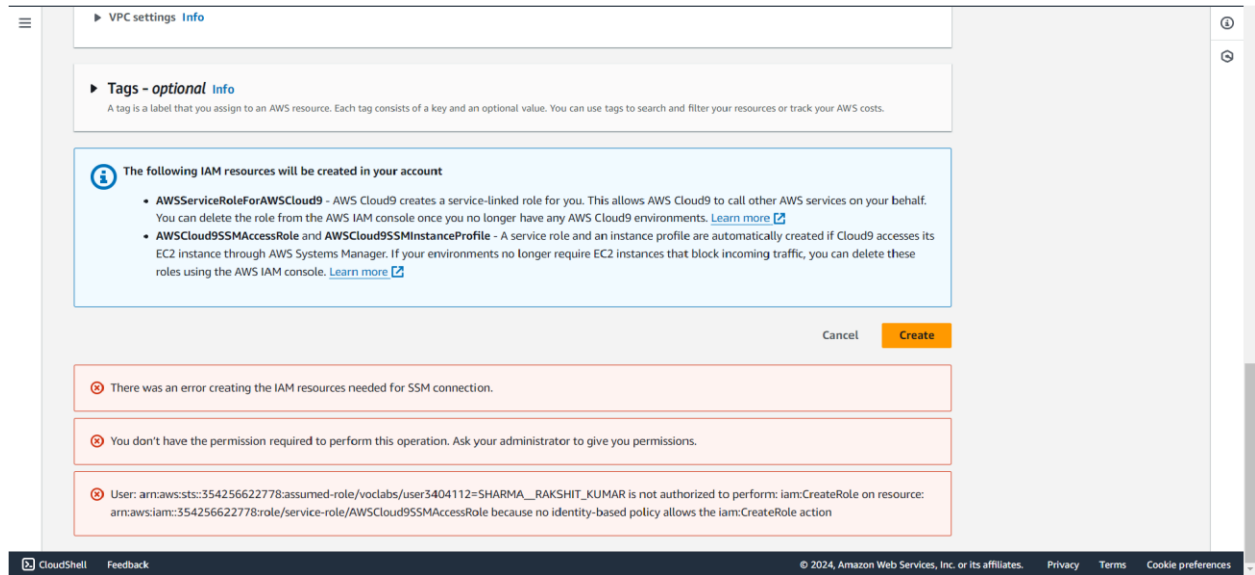
## Experiment 1B: IAM and cloud9

1. Open the AWS account and search for Cloud9.

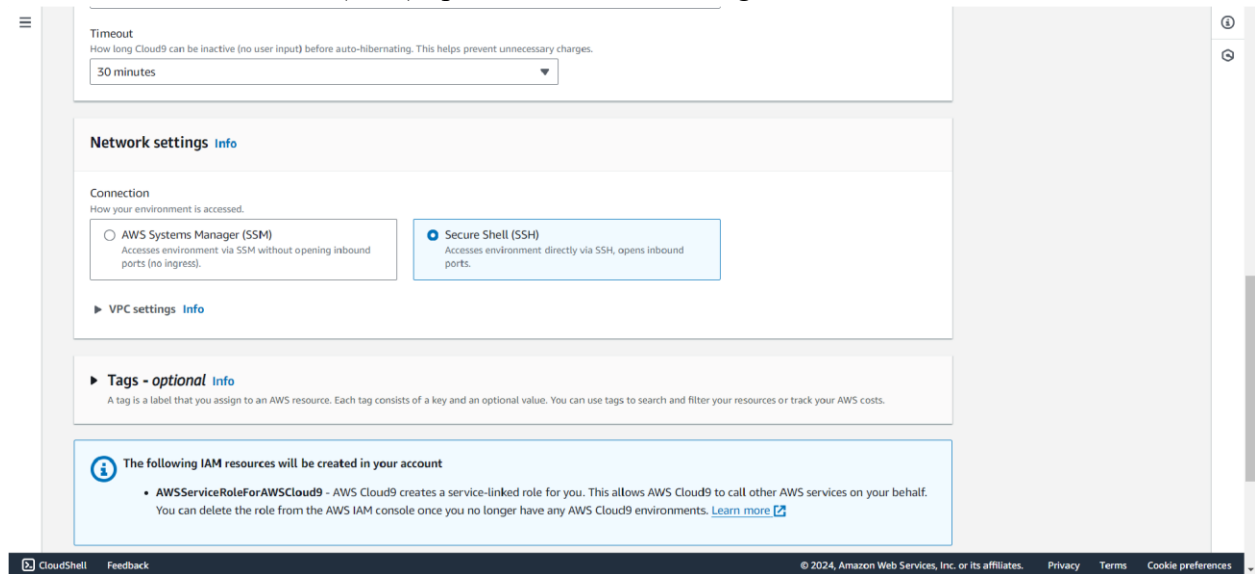


2. Enter the name and other required configuration for creating an environment. In network settings, using the AWS system manager gives an error while creating the environment

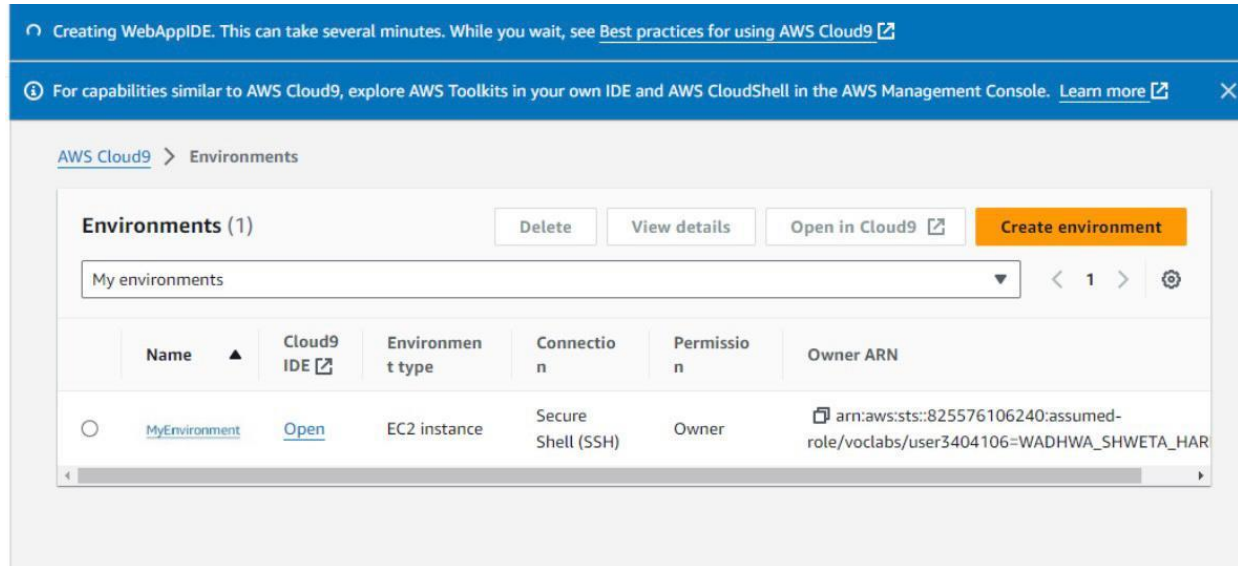




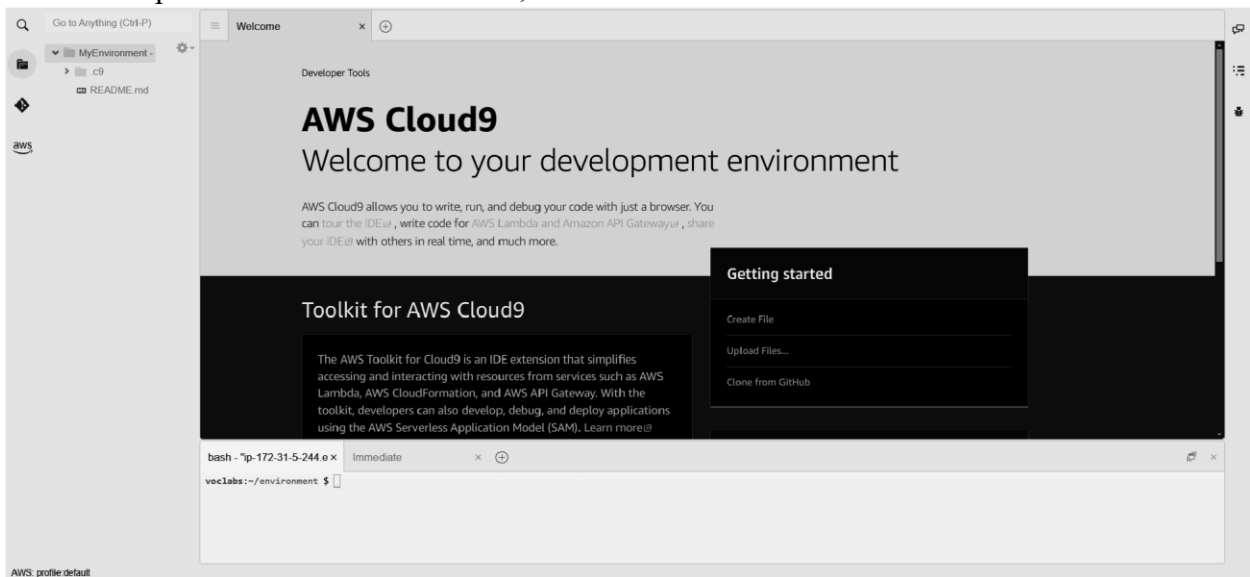
### 3. Select the Secure Shell (SSH) option in Network settings



### 4. Once all configurations are set, click on 'Create Environment' to initiate the Cloud9 environment.

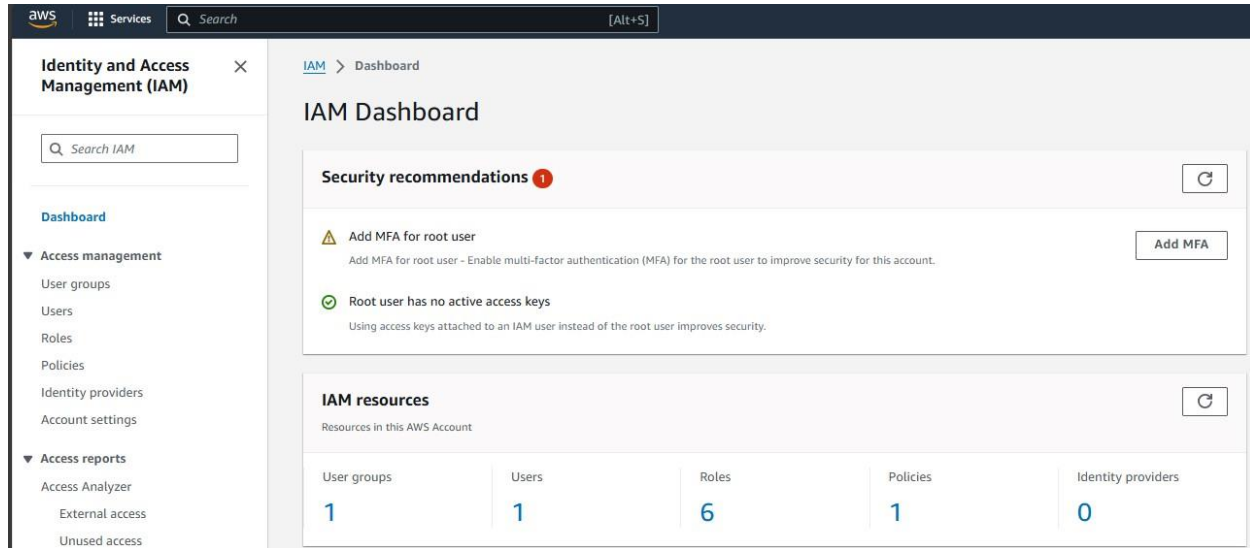


5. To open the Cloud9 environment, click on the environment name.



## IAM user creation steps

1. Login to your AWS account and search for IAM under services.



2. From the left-hand panel, select 'Users' and click on the 'Create User' button. Enter the desired username.



3. If no existing user group is available, click 'Add User to Group'

The screenshot shows the 'Set permissions' step in the AWS IAM console. The left sidebar indicates the current step is 'Set permissions'. The main content area is titled 'Set permissions' and includes a sub-header 'Permissions options'. There are three radio button options: 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. Below these options is a section for 'Set permissions boundary - optional'. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

**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.

► **Set permissions boundary - optional**

Cancel Previous **Next**

4. Create a new user group by providing a name and selecting the necessary policies.

The screenshot shows the 'Create user group' page in the AWS IAM console. The left sidebar indicates the current step is 'Create user group'. The main content area is titled 'Create user group' and includes a sub-header 'Name the group'. There is a text input field for 'User group name' with the value 'sample group'. Below this is a section for 'Add users to the group - Optional (1/1)' with a search bar and a table of users. The table has columns for 'User name', 'Groups', and 'Last activity'. Below this is a section for 'Attach permissions policies - Optional (945)' with a search bar, a 'Filter by Type' dropdown, and a table of policies. The table has columns for 'Policy name', 'Type', 'Used as', and 'Description'. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

**Create user group**

**Name the group**

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

**Add users to the group - Optional (1/1)** 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

<input checked="" type="checkbox"/>	User name	Groups	Last activity
<input checked="" type="checkbox"/>	sample	0	None

**Attach permissions policies - Optional (945)** 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.

Search

Filter by Type: All types

<input type="checkbox"/>	Policy name	Type	Used as	Description
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	None	Provides full ac
<input type="checkbox"/>	AdministratorAccess-Amplify	AWS managed	None	Grants account
<input type="checkbox"/>	AdministratorAccess-AWSElasticBeans...	AWS managed	None	Grants account
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	None	Provide device :

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

5. After the user group is created, select the group name and proceed by clicking 'Next' to finalize user creation .

myweb-app-group user group created.

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)**

Search

< 1 > ⌵

<input type="checkbox"/>	Group name	Users	Attached policies	Created
<input type="checkbox"/>	myweb-app-group	0	-	2024-08-08 (Now)

► Set permissions boundary - optional

Cancel Previous **Next**

6. Review all configuration details, ensure no steps were missed, and then click the 'Create User' button

IAM > Users > Create user

Step 1  
Specify user details

Step 2  
Set permissions

Step 3  
**Review and create**

### 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 sample	Console password type None	Require password reset No
---------------------	-------------------------------	------------------------------

**Permissions summary**

< 1 >

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.

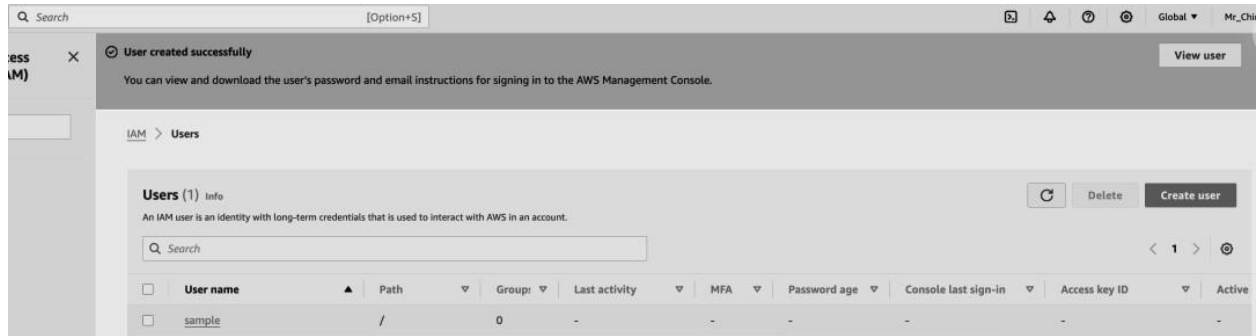
No tags associated with the resource.

**Add new tag**

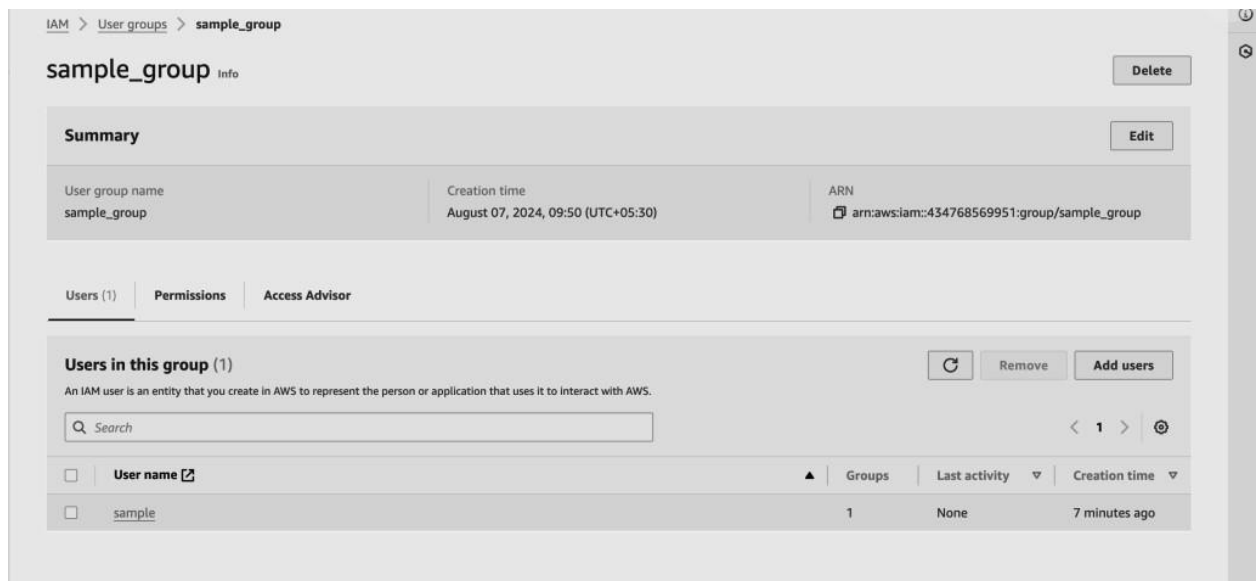
You can add up to 50 more tags.

Cancel Previous **Create user**

7. Upon successful user creation, a confirmation message will appear. If needed, download the CSV file to store the password securely.



8. After the user is created, go to the 'User Groups' tab, select the appropriate group, and navigate to the 'Permissions' tab. Click on 'Add Permissions' and attach the relevant policy.



9. Search for the "AWSCloud9EnvironmentMember" policy and attach it.

