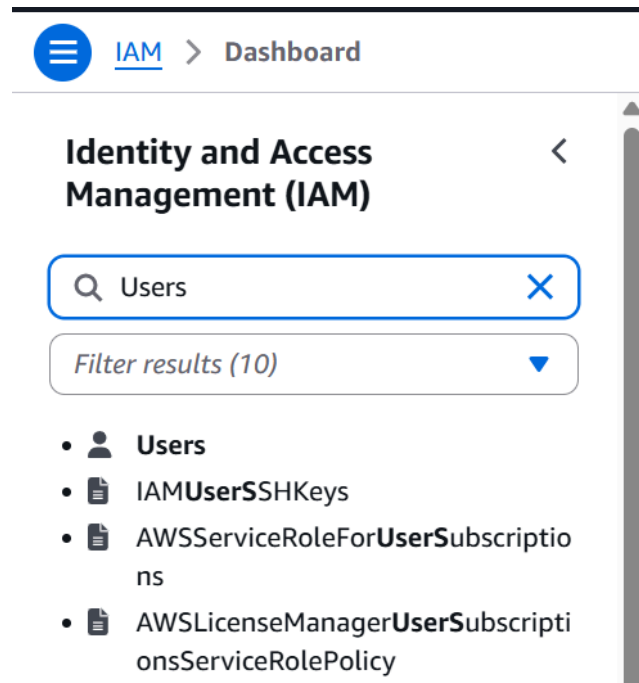


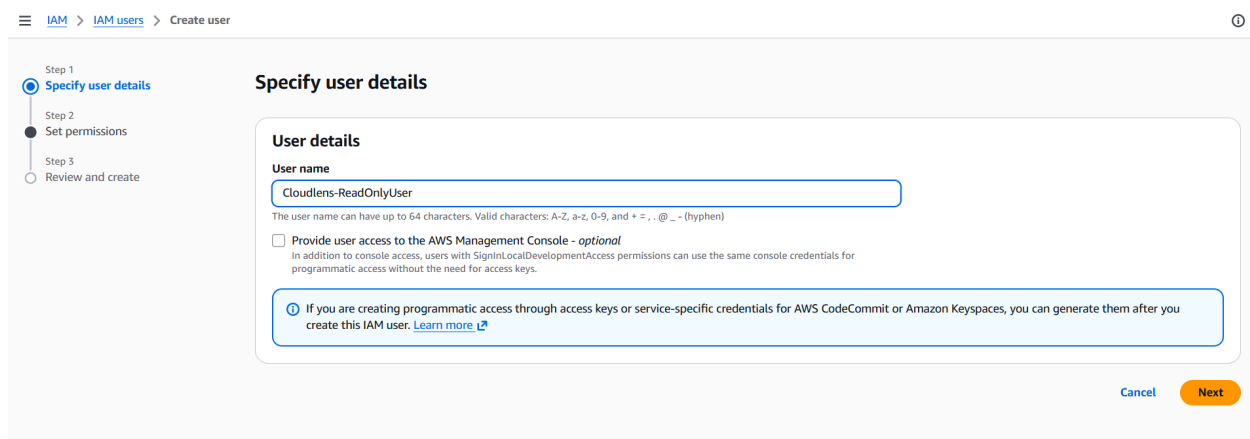


IAM Setup Guide: Connecting Your AWS Account to CloudLens

1. Sign into your AWS Management Console.
2. In the search bar or clicking on the 3x3 dot box, type or look for **IAM** in the service list.
3. Once the IAM page loads on the main dashboard, search for **Users** and select the option as seen below.



4. Click on **Create User**.
5. Enter in a name for this user like “Cloudlens-ReadOnly”, and **DO NOT** check “Provide user access to the AWS Management Console - *optional*”. Press next to continue.





- Next you will click on **Attach policies directly**, and then on the right side of the page click on **Create policy**. This will open up a new tab, and leave the existing tab open, that will continue on **Step 13**.

Step 1 Specify user details
Step 2 **Set permissions**
Step 3 Review and create

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.

Permissions policies (1587)
Choose one or more policies to attach to your new user.

[Create policy](#)

- Once in the Specify permissions page inside the new tab, click on **JSON** in the policy editor.
- Remove the existing code, and copy and paste this JSON file below into the policy editor tab, which will include the 4 actions of **"GetCostAndUsage"**, **"GetCostandUsageWithResources"**, **"GetCostForecast"**, and **"GetDimensionValues"**.

JSON FILE:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageWithResources",
        "ce:GetCostForecast",
        "ce:GetDimensionValues"
      ],
      "Resource": "*"
    }
  ]
}
```



IAM > Policies > Create policy

Step 1
Specify permissions
Step 2
Review and create

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       "Effect": "Allow",  
6       "Action": [  
7         "ce:GetCostAndUsage",  
8         "ce:GetCostAndUsageWithResources",  
9         "ce:GetCostForecast",  
10        "ce:GetDimensionValues"  
11      ]  
12      "Resource": "*"  
13    }  
14  ]  
15 }
```

Visual **JSON** Actions

Edit statement

Select a statement

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

+ Add new statement

9. Scroll to the bottom of the page once the JSON file is pasted, press **Next** to continue.
10. Next, assign a policy name like **"Cloudlens-ReadOnly"** for identification, you can also click on the Cost Explorer Service under the **Permissions Defined in this Policy** to confirm that the 4 actions were applied.

IAM > Policies > Create policy

Step 1
Specify permissions
Step 2
Review and create

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.

Permissions defined in this policy [Info](#) [Edit](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it (1)

Allow (1 of 476 services) ☒ Show remaining 475 services

Service	Access level	Resource	Request condition
Cost Explorer Service	Limited: Read	All resources	None

11. Scroll to the bottom of the page, and click **Create Policy**.
12. Now go back to the original tab under **IAM > CreateUsers > Set Permissions**, and refresh the Permissions policies, you should now see your newly created Cloudlens-ReadOnly.
13. Select the checkbox next to the policy name, and press **Next** to continue.



IAM > IAM users > Create user

Step 1 Specify user details
Step 2 Set permissions
Step 3 Review and create

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.

Permissions policies (1/1588) [Create policy](#)

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

Search: Cloudlens-ReadOnly Filter by Type: All types 1 match

Policy name	Type	Attached entities
☒ Cloudlens-ReadOnly-Test	Customer managed	0

► Set permissions boundary - optional

Cancel Previous Next

14. Review your details to make sure they are correct, and click on **Create User** to finish.

IAM > 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 Cloudlens-ReadOnly-Test	Console password type None	Require password reset No
--------------------------------------	-------------------------------	------------------------------

Permissions summary < 1 >

Name	Type	Used as
Cloudlens-ReadOnly-Test	Customer managed	Permissions policy

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

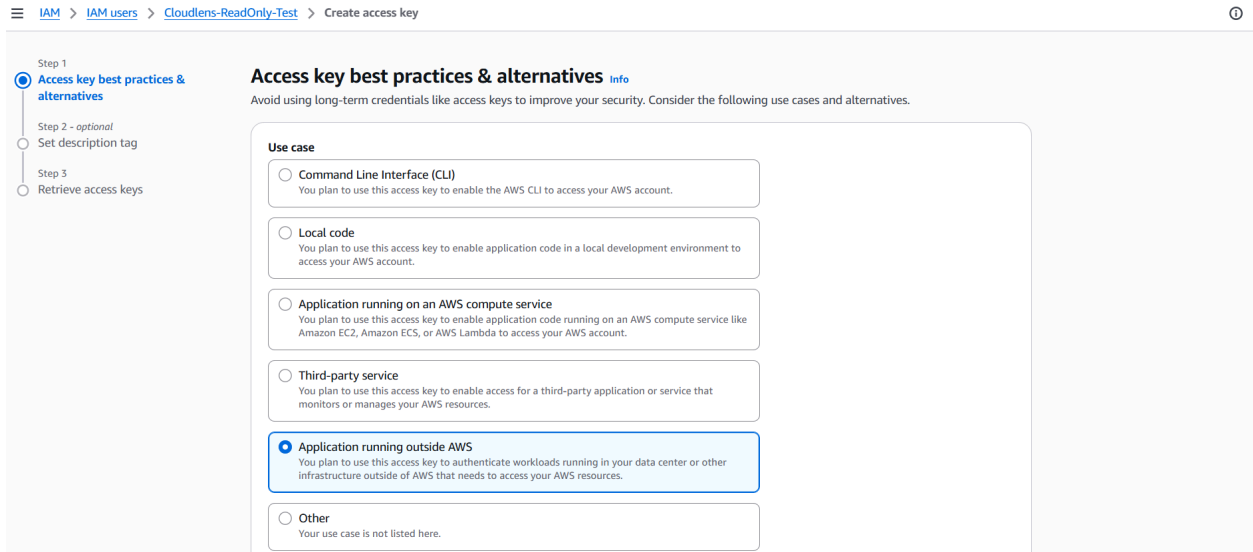
15. Head back to your **IAM Console** -> **Users** -> click on your newly created user (**Cloudlens-ReadOnly**).

16. Click on the **Security Credentials** tab.

17. Scroll down to **Access Keys**, and click on **create access key**.

18. Under Access key best practices and alternatives click on **Application running outside on AWS**, then click **Next**.

(Note: AWS may recommend using IAM Roles anywhere as a more secure alternative. The IAM user you are creating through this guide has no ability to modify, delete or access any of your AWS resources, it can only read billing data.)



IAM > IAM users > Cloudless-ReadOnly-Test > Create access key

⌵

This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

✕

Step 1

Access key best practices & alternatives

Step 2 - optional

Set description tag

Step 3

Retrieve access keys

Retrieve access keys

Info

Access key

If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key

Secret access key

Ⓞ

Show

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the best practices for managing AWS access keys.

Download .csv file

Done

20. You're now ready to connect your AWS account to Cloudlens. Click **Done** to return to the IAM Users homepage, and in Cloudlens head to **Settings -> AWS Accounts -> Add Account** to view your billing information.