

Cloud Plus Plus Services



Install and configure AWS CLI for an IAM user.

Step 1: Download the AWSCLI tool to manage services from console:

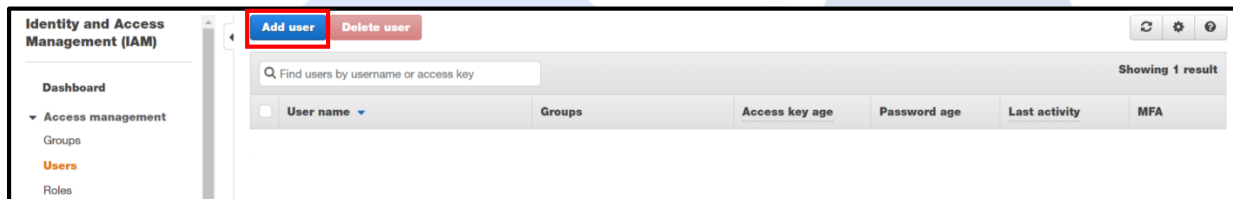
<https://s3.amazonaws.com/aws-cli/AWSCLI64.msi>

Install the downloaded file.

Note: If you have an existing IAM User with programmatic access and Full S3 Access permissions, go to **Step 8**.

Step 2: Go to **IAM** service dashboard. In the left side panel, click on **Users** under **Access management**.

Click on **Add User**.



Step 3: In Set User Details, Give the name as **S3User**. Check the box for **Programmatic access**. This provides the user access to development tools such as CLI.

Click on **Next: Permissions** in bottom right corner.

Add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* ☒ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☐ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

* Required

[Cancel](#) [Next: Permissions](#)

Cloud Plus Plus Services



Step 4: Under **Set Permissions**, click on **Attach existing policies directly**.

In the Filter policy search box, search for S3 full access and select **AmazonS3FullAccess** from the drop down searched policies.

Add user

1 2 3 4 5

▼ Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

Create policy

Filter policies ▼ Showing 1 result

	Policy name ▼	Type	Used as
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	Permissions policy (2)

Cancel Previous **Next: Tags**

Click on **Next: Tags** in bottom right corner.

Step 5: Add a tag with **Key: Name** and **Value: S3User**. Click on **Next: Review** in bottom right corner.

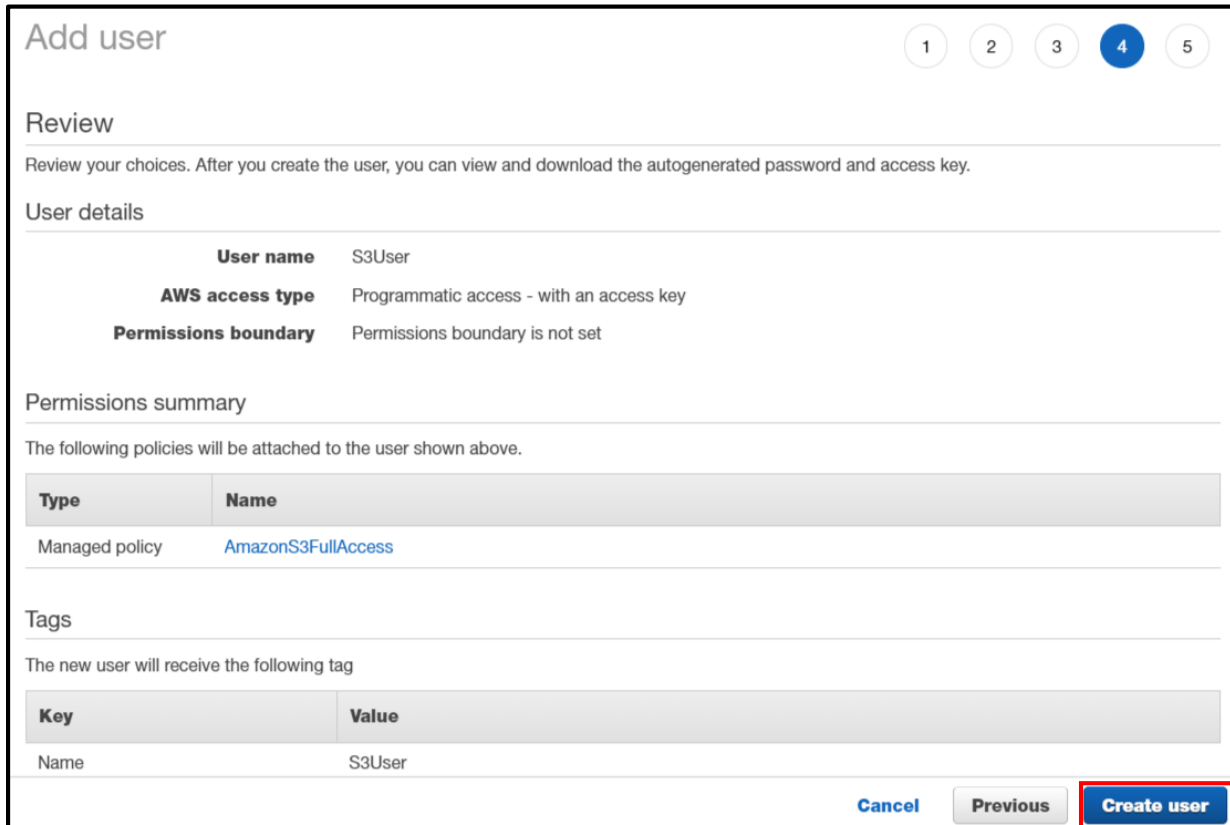
Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
Name		
	S3User	

Cancel Previous **Next: Review**

Step 6: Click On **Create User** after reviewing the details.



Add user

1 2 3 **4** 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	S3User
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AmazonS3FullAccess


Tags

The new user will receive the following tag

Key	Value
Name	S3User

[Cancel](#) [Previous](#) [Create user](#)

Step 7: On this step, click on **Download .csv** button. A .csv file compatible with MsExcel will get downloaded on your local drive.



[Download .csv](#)

User	Access key ID	Secret access key
<input checked="" type="checkbox"/> S3User	AKIATR GXU2KWHWZWYJHE	***** Show

[Close](#)

Save this file in a secure location for further use and correspondence.

Go to **IAM** dashboard and confirm that the user has been created.



Dashboard

[Add user](#) [Delete user](#)

Find users by username or access key

Showing 2 results

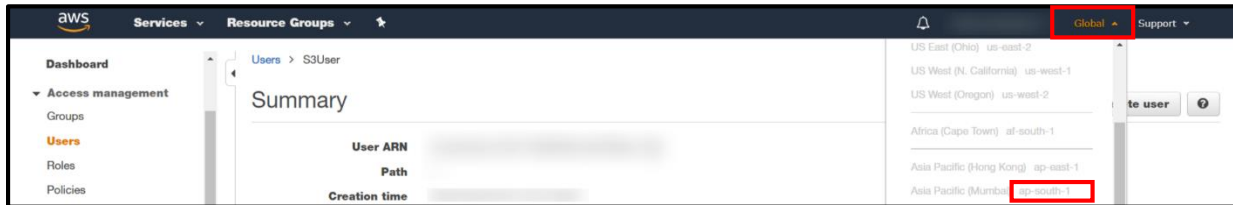
User name	Groups	Access key age	Password age	Last activity	MFA
<input type="checkbox"/> S3User	S3Developers	None	None	None	Not enabled

Cloud Plus Plus Services



Step 8: Find the **Global** drop down on your AWS console top bar and copy the alias of region name. The region name is usually the name of region that you are operating from. E.g. **ap-south-1** in this case.

Store it in a text file.



Step 9: Open Command Prompt.

Type in the command: **aws configure**

Copy the **Access key ID** from .csv file and paste it here for **AWS Access Key ID**.

Similarly copy the **Secret access key** and paste it here for **AWS Secret Access Key**.

Give the **Default region name** that we stored in Step 8, **ap-south-1** in this case.

Give **Default output format** as **text**.

```
D:\>cd \Cloud-plusplus\AWSCLI

D:\Cloud-plusplus\AWSCLI>aws configure
AWS Access Key ID : AKIATRQXU2KWHWZJHE
AWS Secret Access Key : B7/zpi4Qo+222UkJ8qHUZjRBaKky+s6Dth0ImSSo
Default region name : ap-south-1
Default output format : text
```

Step 10: This step is to test whether the User can access S3 services through AWS CLI commands.

To create a bucket enter following command:

aws s3 mb s3://mybucket753159

Here mybucket753159 is a random name chosen for your bucket.

You may have to try this command again if your required bucket name is already being used by some other AWS user.

Cloud Plus Plus Services



```
D:\Cloud-plusplus\AWSCLI>aws s3 mb s3://mybucket753159
make_bucket: mybucket753159

D:\Cloud-plusplus\AWSCLI>
```

If you observe **make_bucket: (name of your bucket)** as output, your bucket has been successfully created for this particular s3 user using the access and policies you chose for the user.

Step 11: Go to **S3** services from AWS console and click on **Buckets** to check that the bucket has been created.

Bucket name	Access	Region	Date created
mybucket753159	Objects can be public	Asia Pacific (Mumbai)	

Note: Delete the S3 bucket and the IAM user if you no longer need to use them.

Cloud++
Your trusted partner for
cloud enablement

Cloud Plus Plus Services



Document Created by	Version
Parag Deshpande	02-Oct-2020
Parag Deshpande	06-Sep-2020

CLOUD ++

Your trusted partner for
cloud enablement