

## Module 1: Introduction to AWS

---

### Demo Document 2

**edureka!**

**edureka!**

© Brain4ce Education Solutions Pvt. Ltd.

## A) Explore Console and Create S3 Bucket via Console

- Enter the below URL to start using console

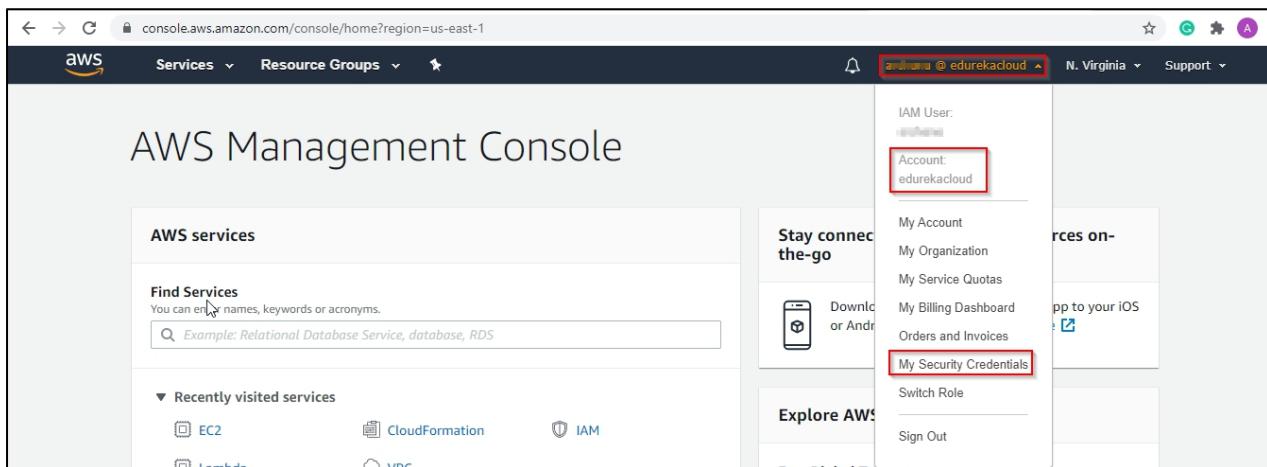
<https://aws.amazon.com/console/>

The screenshot shows the AWS Management Console homepage. At the top, there's a navigation bar with links for Services, Resource Groups, and Support. Below the navigation is a search bar with the URL "console.aws.amazon.com/console/home?region=us-east-1". The main content area is titled "AWS Management Console". On the left, there's a sidebar titled "AWS services" with sections for "Recently visited services" (EC2, CloudFormation, IAM, Lambda, VPC) and "All services" (Compute, Blockchain, Security, Identity, & Compliance, Lightsail, Amazon Managed Blockchain, IAM, Lambda, Batch, Satellite, Ground Station, Resource Access Manager, Cognito, Elastic Beanstalk). To the right, there are several promotional boxes: one for connecting to AWS resources on-the-go (with a link to the AWS Console Mobile App), one for "Explore AWS" with "Free Digital Training" and "AWS Certification" options, and another for staying connected to AWS products and services.

- Choose the desired region

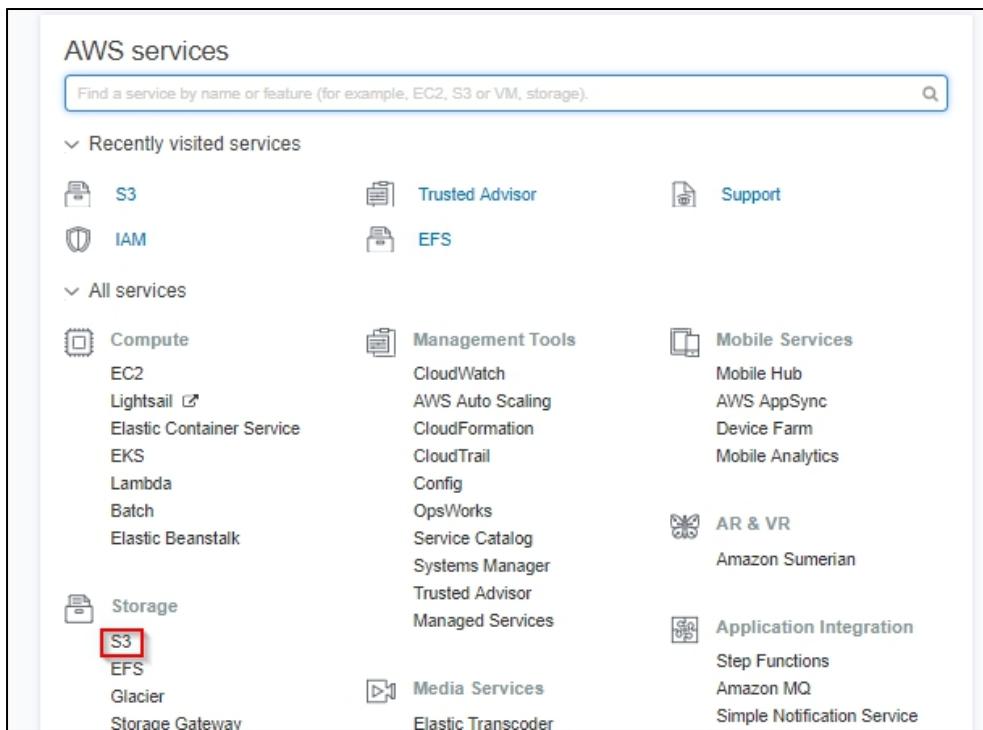
This screenshot is similar to the previous one, showing the AWS Management Console homepage. However, the "N. Virginia" region is highlighted in a red box in the top navigation bar. The rest of the interface is identical to the first screenshot, including the AWS services sidebar and promotional sections.

- In case, if you want to log-out or get the account details

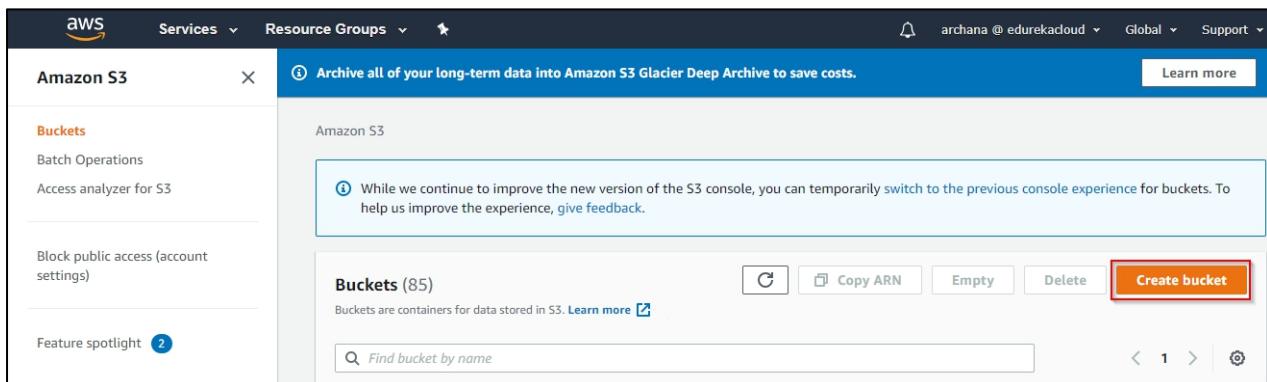


Now lets see how to configure S3 bucket via console:

**Step 1:** Sign in to the AWS Management Console and open the Amazon S3.

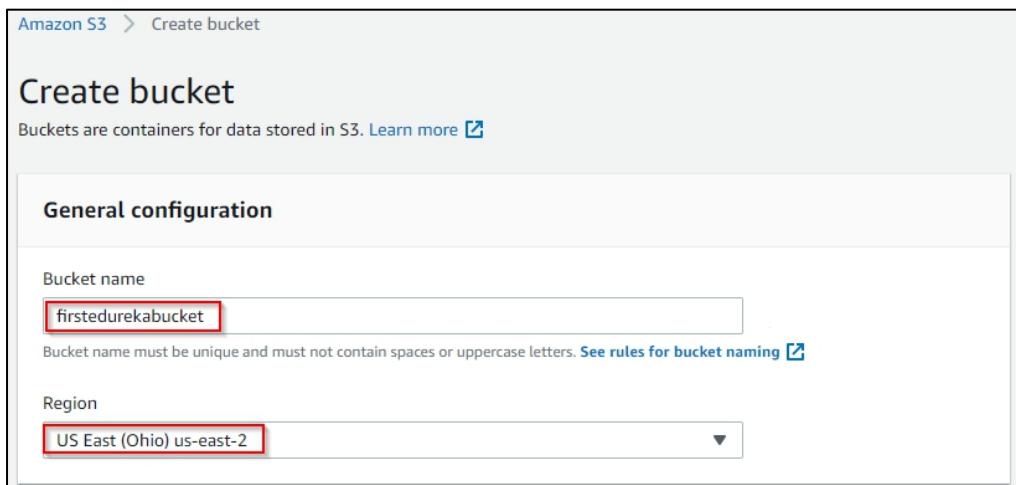


## Step 2: Choose Create Bucket.



The screenshot shows the AWS S3 service page. On the left, there's a sidebar with options like 'Buckets', 'Batch Operations', 'Access analyzer for S3', 'Block public access (account settings)', and 'Feature spotlight'. The main area is titled 'Amazon S3' and shows a message about archiving long-term data into Amazon S3 Glacier Deep Archive. Below this, there's a note about switching to the previous console experience for buckets. A table lists 'Buckets (85)' with columns for actions like 'Copy ARN', 'Empty', 'Delete', and a prominent orange 'Create bucket' button. A search bar at the bottom allows finding buckets by name.

**Step 3:** In the Bucket name space, type a unique name for your new bucket, as demonstrated below. Create your bucket name while ensuring that the name is unique across all existing bucket names in Amazon S3. Specify the AWS Region.



The screenshot shows the 'Create bucket' configuration page. It has a header 'Amazon S3 > Create bucket' and a sub-header 'Create bucket'. Below that is a note about buckets being containers for data stored in S3. The main section is 'General configuration' with two fields: 'Bucket name' containing 'firstedurekabucket' (which is highlighted with a red box) and 'Region' set to 'US East (Ohio) us-east-2' (also highlighted with a red box). There are also tabs for 'Advanced configuration' and 'Tags'.

- Make sure you uncheck block all public access, to make your bucket publicly accessible.  
Then click on **Create bucket**

**Block all public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- Block public access to buckets and objects granted through new access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

**⚠ Turning off block all public access might result in this bucket and the objects within becoming public**  
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

I acknowledge that the current settings might result in this bucket and the objects within becoming public.

### Step 4: From the list of buckets, select the bucket Your Bucket.

**✓ Successfully created bucket "firstedurekabucket"**  
To upload files and folders, or to configure additional bucket settings such as Bucket Versioning, tags, and default encryption, choose [View details](#).

**ⓘ S3 Replication lets you simply copy objects from one S3 bucket to another.** [Learn more](#)

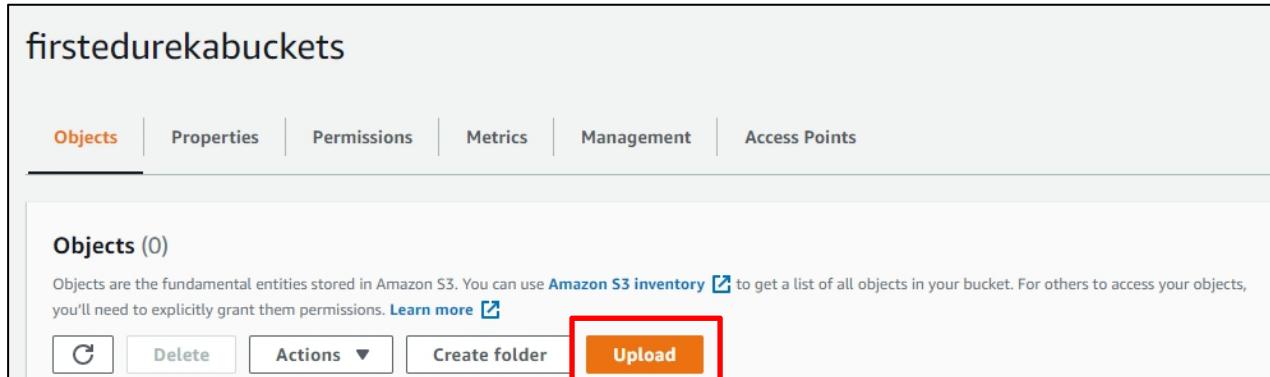
Amazon S3

**Buckets (86)**

Buckets are containers for data stored in S3. [Learn more](#)

Name	Region	Access	Creation date
<a href="#">fir</a> firstedurekabucket	US East (Ohio) us-east-2	Bucket and objects not public	June 11, 2020, 15:27 (UTC+05:30)

**Step 5:** Upload the file in the created bucket



**Step 6:** Click on **Upload**.

**Files and folders (1 Total, 12.7 KB)**

All files and folders in this table will be uploaded.

	Name	Folder	Type	Size
<input type="checkbox"/>	cloud-computing.png	-	image/png	12.7 KB

**Destination**

Destination  
s3://firstedurekabuckets

**Destination details**

The following bucket settings impact new objects stored in the specified destination.

Bucket Versioning When enabled, multiple variants of an object can be stored in the bucket to easily recover from unintended user actions and application failures. <a href="#">Learn more</a>	Default encryption When enabled, new objects stored in this bucket are automatically encrypted. <a href="#">Learn more</a>	Object Lock When enabled, objects in this bucket might be prevented from being deleted or overwritten for a fixed amount of time or indefinitely. <a href="#">Learn more</a>
<span style="color: red;">⚠</span> Disabled	Disabled	Disabled

⚠ We recommend that you enable Bucket Versioning to help protect against unintentionally overwriting or deleting objects. [Learn more](#)

[Enable Bucket Versioning](#)

▶ Additional upload options

Cancel Upload

### Step 7: Open the document (uploaded file).

**Files and folders (1 Total, 12.7 KB)**

	Name	Folder	Type
<input checked="" type="checkbox"/>	cloud-computing.png	-	image/png

### Step 8: Go to **Permissions** and make available to public and check **Everyone** on the left and **Read object** on the right and hit **Save**.

Amazon S3 > firstedurekabuckets > cloud-computing.png

### cloud-computing.png

[Copy S3 URI](#) [Object actions ▾](#)

Properties	Permissions	Versions
<b>Access control list (ACL)</b> Grant basic read/write permissions to AWS accounts. <a href="#">Learn more</a>		
<a href="#">Edit</a>		
Grantee	Object	Object ACL
Object owner Canonical ID: <a href="#">059ce661fb1e647fa98415c4469fe0f097e37ff5ba7c6816bb6d1490d5f2cd33</a>	Read	Read, Write
Everyone (public access) Group: <a href="#">http://acs.amazonaws.com/groups/global/AllUsers</a>	-	-
Authenticated users group (anyone with an AWS account) Group: <a href="#">http://acs.amazonaws.com/groups/global/AuthenticatedUsers</a>	-	-

Amazon S3 > firstedurekabuckets > cloud-computing.png > Edit access control list

### Edit access control list

**Access control list (ACL)**  
Grant basic read/write permissions to AWS accounts. [Learn more](#)

Grantee	Objects	Object ACL
Object owner Canonical ID: <a href="#">059ce661fb1e647fa98415c4469fe0f097e37ff5ba7c6816bb6d1490d5f2cd33</a>	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Everyone (public access) Group: <a href="#">http://acs.amazonaws.com/groups/global/AllUsers</a>	<input checked="" type="checkbox"/> <span style="color: red;">⚠ Read</span>	<input type="checkbox"/> Read <input type="checkbox"/> Write
Authenticated users group (anyone with an AWS account) Group: <a href="#">http://acs.amazonaws.com/groups/global/AuthenticatedUsers</a>	<input type="checkbox"/> Read	<input type="checkbox"/> Read <input type="checkbox"/> Write

**⚠️** When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.

[Learn more](#)

I understand the effects of these changes on this object.

**Access for other AWS accounts**

No other AWS accounts associated with the resource.

[Add grantee](#)

**Specified objects**

Name	Type	Last modified	Size
<a href="#">cloud-computing.png</a>	png	March 16, 2021, 19:22:00 (UTC+05:30)	12.7 KB

[Cancel](#) Save changes

**Step 9:** Go back to **Properties** and click on **Make Public**.

**cloud-computing.png**

[Copy S3 URI](#) [Object actions](#)

[Download actions](#)

[Download](#) [Download as](#)

[Edit actions](#)

[Rename object](#) [Edit storage class](#) [Edit server-side encryption](#) [Edit metadata](#) [Edit tags](#) Make public

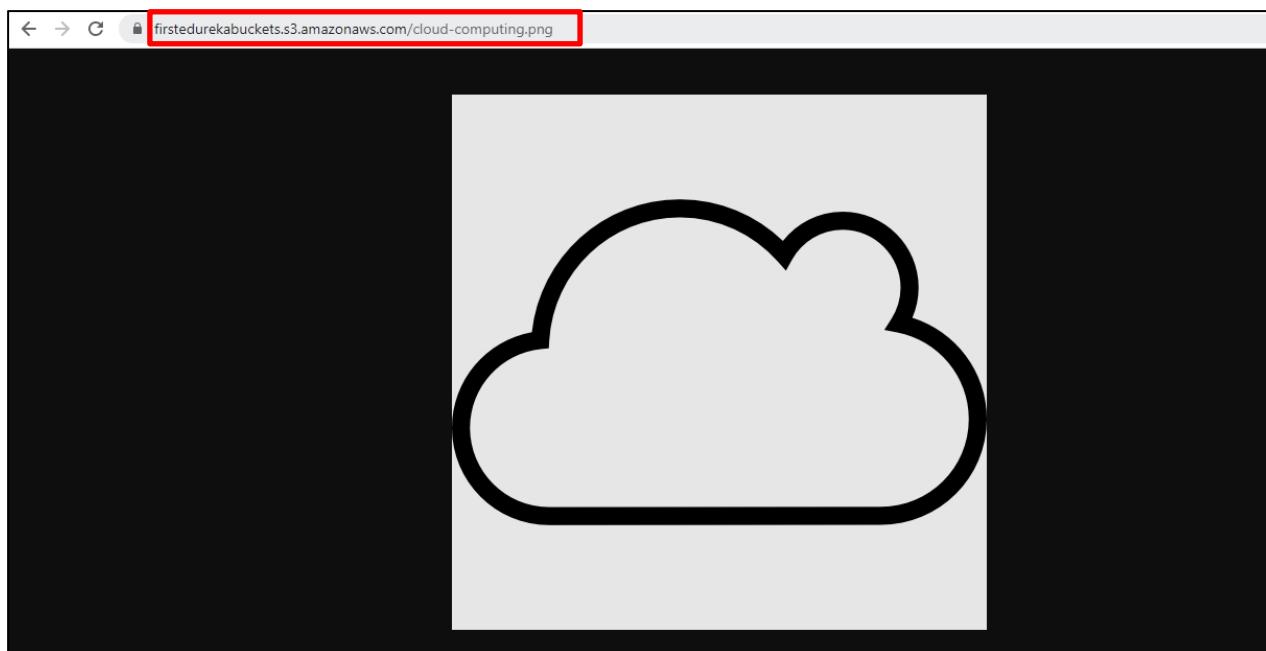
**Properties** [Permissions](#) [Versions](#)

**Object overview**

Owner	S3 URI
Shubhialive	<a href="#">s3://firstedurekabuckets/cloud-computing.png</a>
AWS Region	Amazon resource name (ARN)
US East (N. Virginia) us-east-1	<a href="#">arn:aws:s3:::firstedurekabuckets/cloud-computing.png</a>
Last modified	Entity tag (Etag)
March 16, 2021, 19:22:00 (UTC+05:30)	<a href="#">688a47b1c212c61c3a1c68997df5e7ce</a>
Size	

Properties	Permissions	Versions
<b>Object overview</b>		
Owner	S3 URI	
Shubhialive	<a href="s3://firstedurekabuckets/cloud-computing.png">s3://firstedurekabuckets/cloud-computing.png</a>	
AWS Region	Amazon resource name (ARN)	
US East (N. Virginia) us-east-1	<a href="arn:aws:s3::firstedurekabuckets/cloud-computing.png">arn:aws:s3::firstedurekabuckets/cloud-computing.png</a>	
Last modified	Entity tag (Etag)	
March 16, 2021, 19:22:00 (UTC+05:30)	<a href="688a47b1c212c61c3a1c68997df5e7ce">688a47b1c212c61c3a1c68997df5e7ce</a>	
Size	Object URL	
12.7 KB	<a href="https://firstedurekabuckets.s3.amazonaws.com/cloud-computing.png">https://firstedurekabuckets.s3.amazonaws.com/cloud-computing.png</a>	
Type		
png		

**Step 10:** Copy the link and paste it in the address bar of a browser



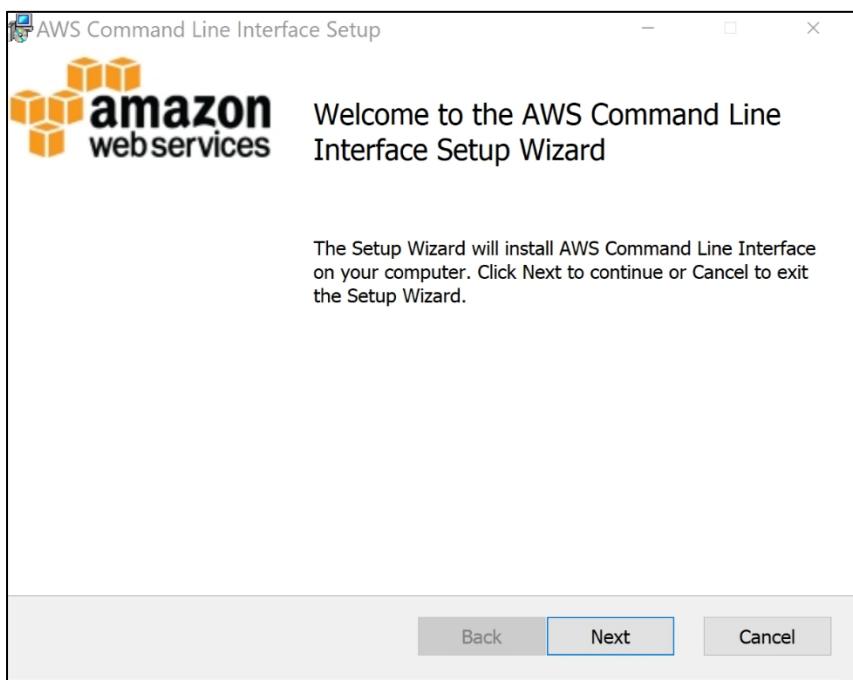
## B) Configure AWS CLI and Create S3 Bucket via CLI

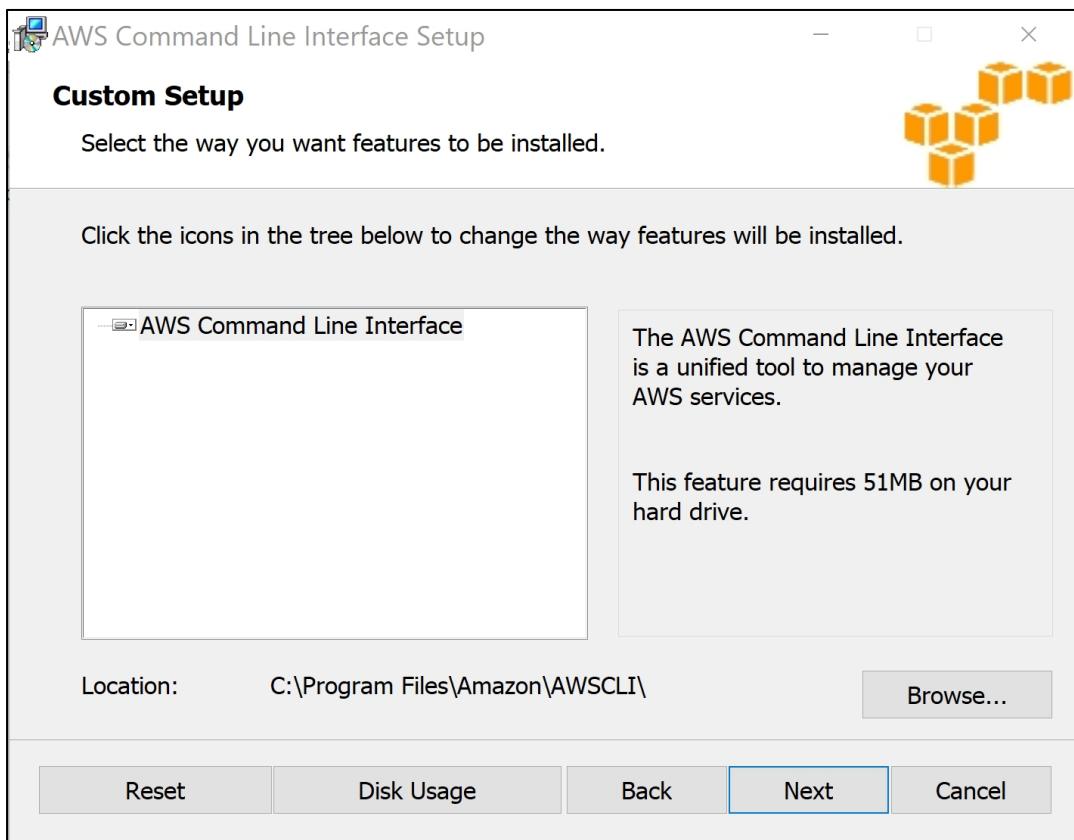
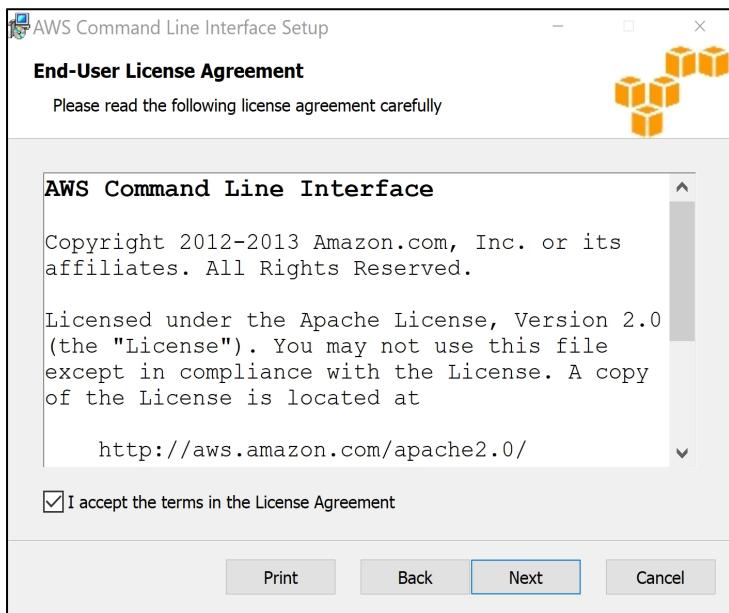
**Step 1:** Download the appropriate MSI installer based on your operating system (32/64 bit) from one of the following links.

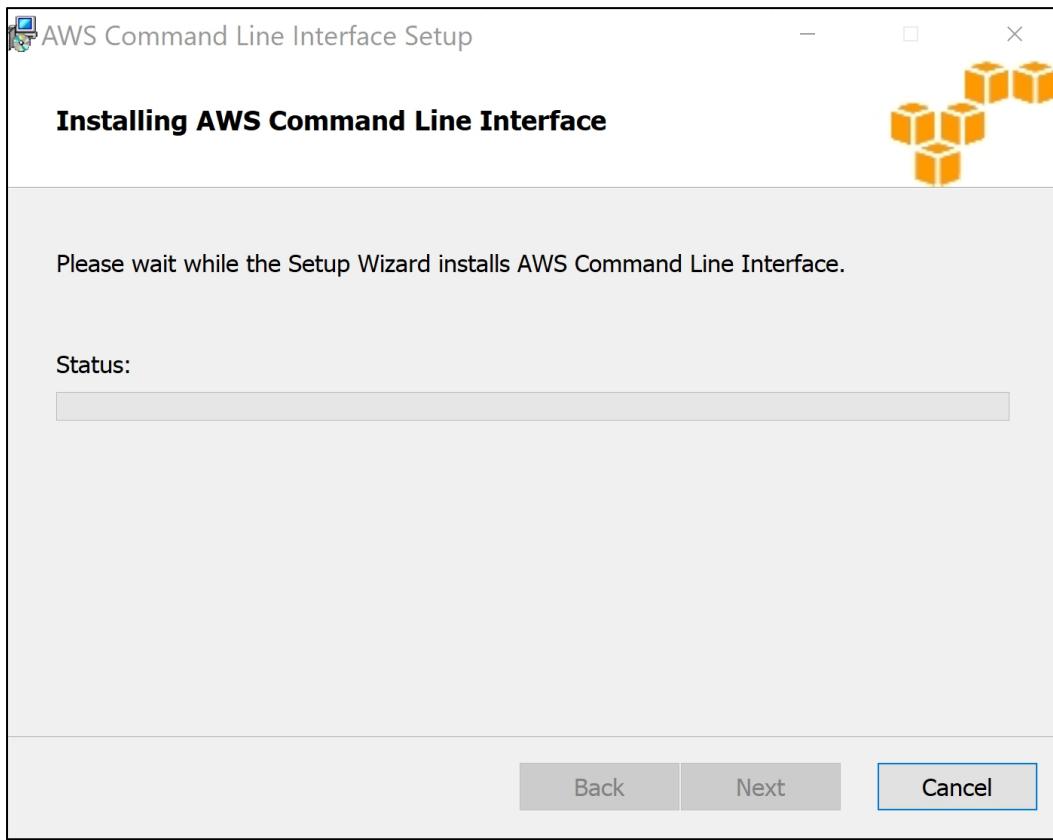
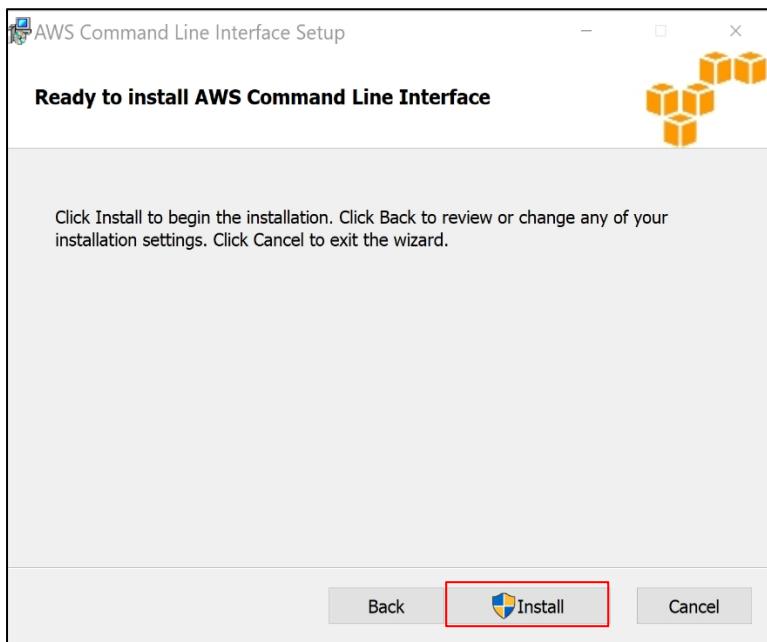
<https://s3.amazonaws.com/aws-cli/AWSCLI64.msi>

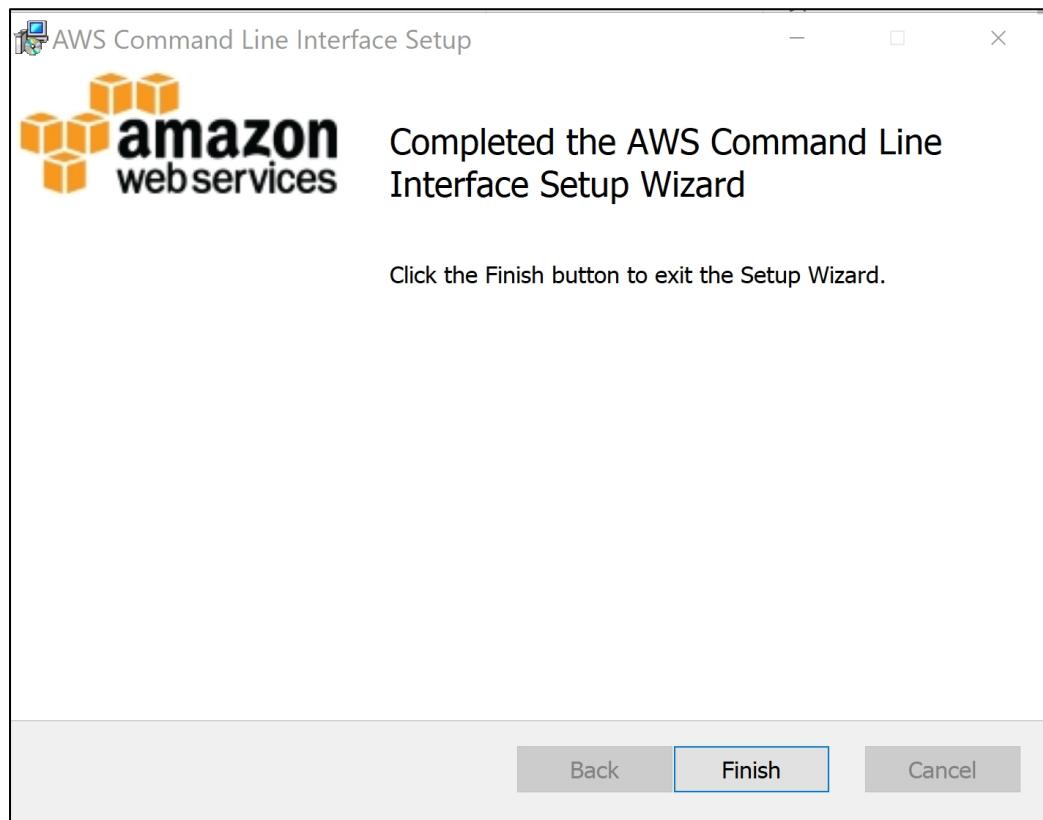
<https://s3.amazonaws.com/aws-cli/AWSCLI32.msi>

**Step 2:** Run the downloaded MSI installer and install it by following the below screenshots.



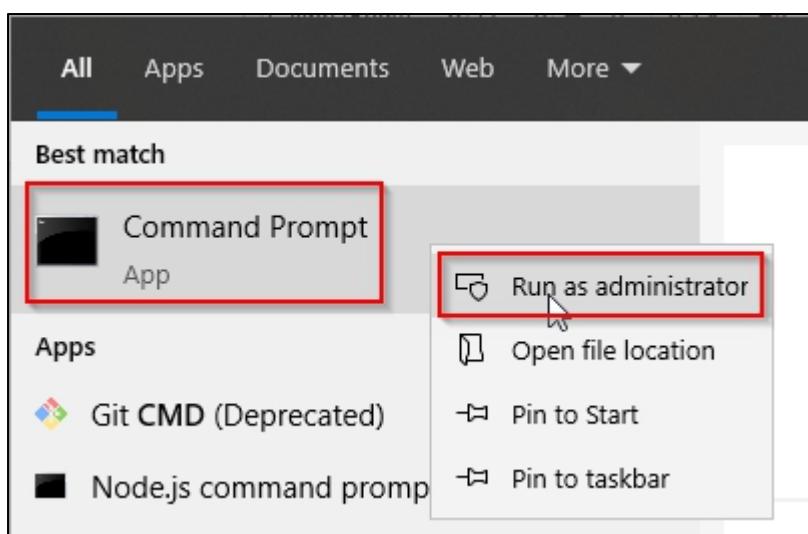


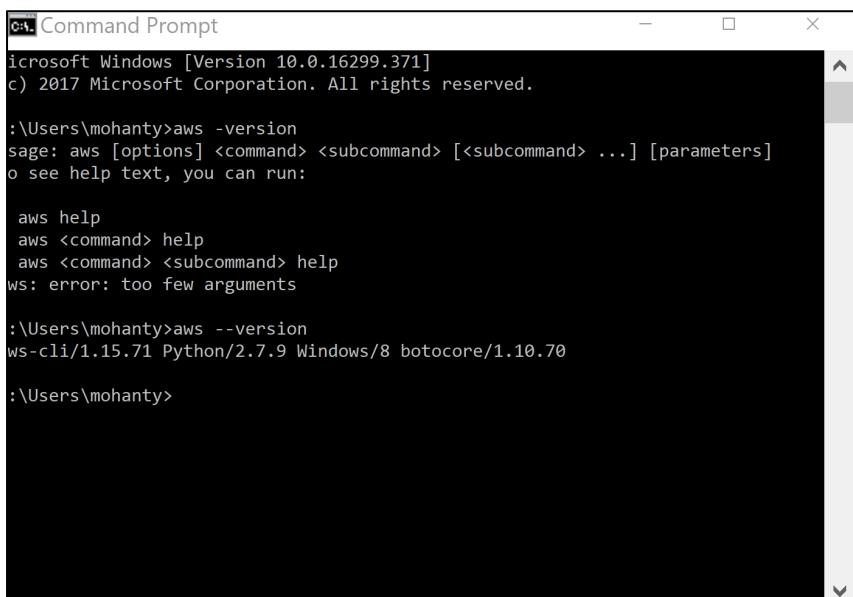




**Step 3:** Open **Command Prompt** and verify the AWS version using the below command

```
aws --version
```





```
c:\ Command Prompt
Microsoft Windows [Version 10.0.16299.371]
c) 2017 Microsoft Corporation. All rights reserved.

:\Users\mohanty>aws -version
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
o see help text, you can run:

aws help
aws <command> help
aws <command> <subcommand> help
ws: error: too few arguments

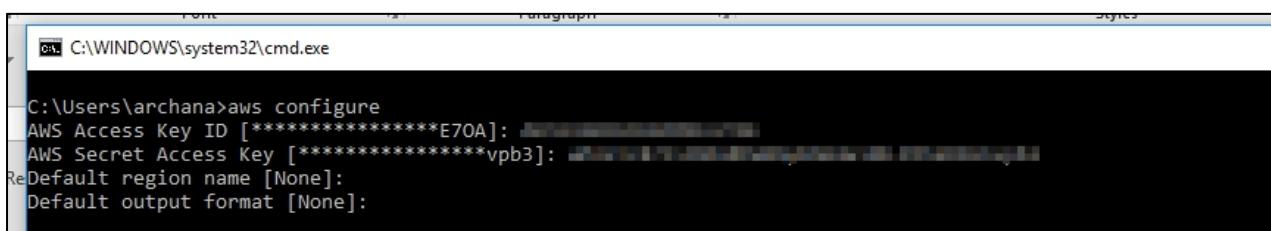
:\Users\mohanty>aws --version
ws-cli/1.15.71 Python/2.7.9 Windows/8 botocore/1.10.70

:\Users\mohanty>
```

**Step 4:** Connect to your AWS account using command:

*aws configure*

Enter Access Key ID and Secret Access key.

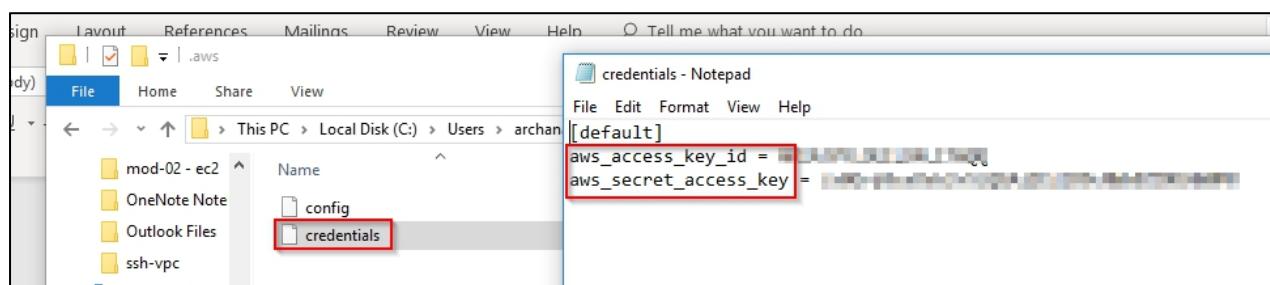
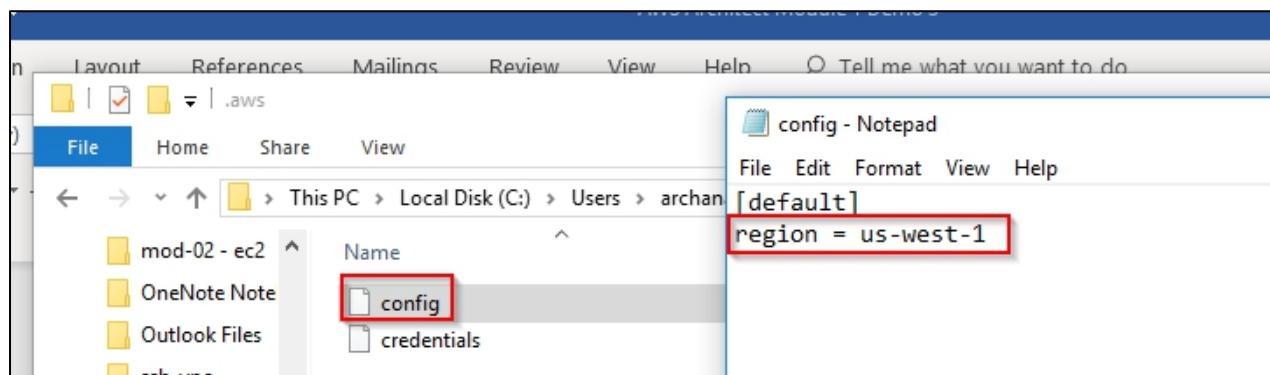


```
C:\WINDOWS\system32\cmd.exe

C:\Users\archana>aws configure
AWS Access Key ID [*****E70A]: *****
AWS Secret Access Key [*****vpb3]: *****
Default region name [None]:
Default output format [None]:
```

**Note:** If you want to reconfigure your credentials, you can use the below path:

C:\Users\user-name\.aws



**Step 5:** Create a bucket using the following command:

```
aws s3 mb s3://edureka13
```

```
C:\Users\archana>aws s3 mb s3://edureka13
make_bucket: edureka13
```

## Conclusion

You have successfully created an S3 bucket and added the file in the bucket using console and CLI.