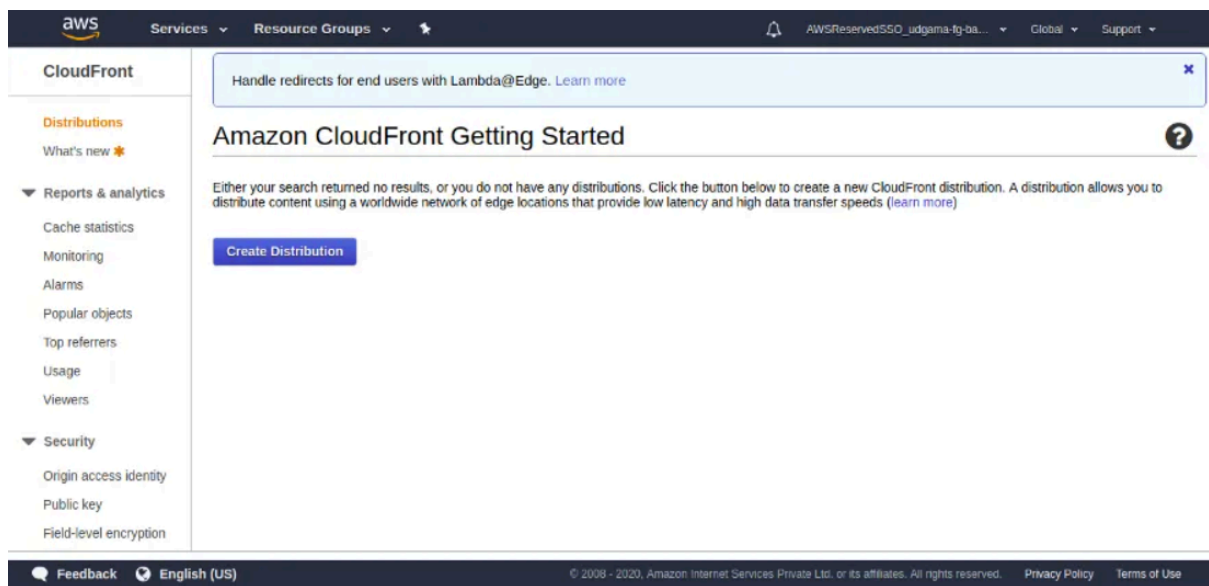


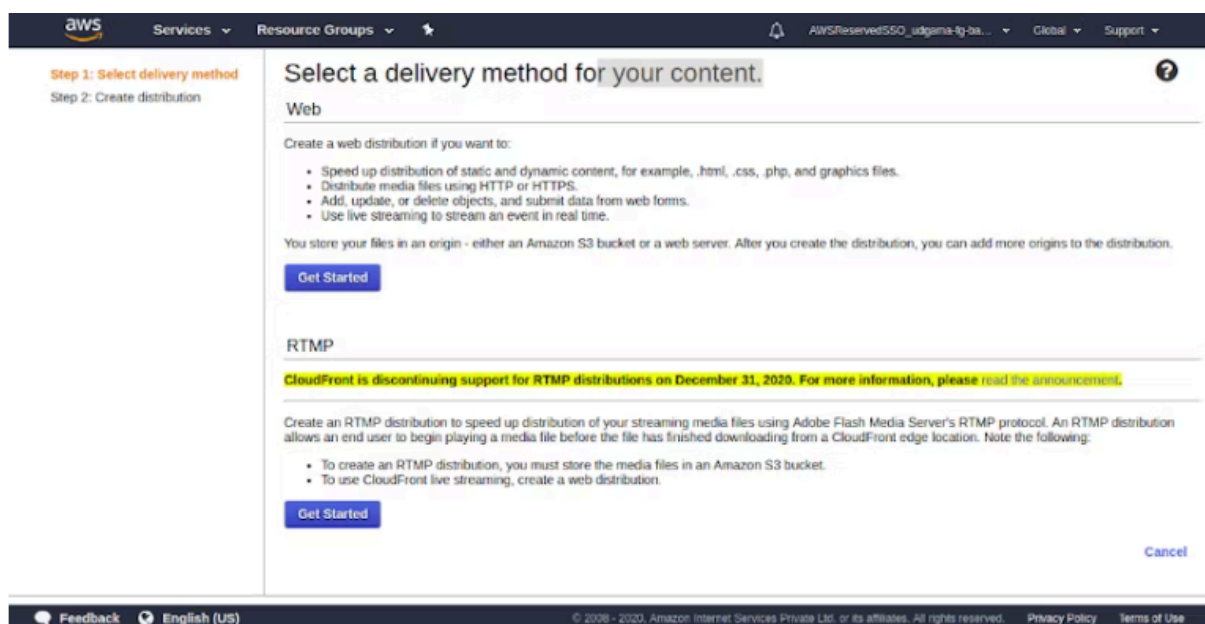
Let's start the creation of CloudFront distribution.

1. Steps for creating a CloudFront distribution

- Sign in to the AWS Management Console and in the **Find Services**, you can see a search box in that type cloud and choose **CloudFront**.
- You should **Global** for the region at the top right.
- Click **Create Distribution**.



- Under **Web** click **Get Started**.



- For **Origin Domain Name** once you place the cursor in there you should see your available S3 buckets.

Note: I already created S3 bucket in AWS so If you don't have any website on S3 bucket then plz create it first

- Pick the website bucket you created.
- If it's not listed type it in: e.g
2020-05-21-mybucket.s3.amazonaws.com that is nothing but your bucket name.
- Leave **Origin Path** blank.
- The **Origin ID** should have been pre-populated when you choose your bucket.
- Click **Yes** to **Restrict Bucket Access**.
- Under **Origin Access Identity** select **Create a New Identity**.
- It will pre-populate the **Comment** and append the bucket name.
- For **Grant Read Permissions** on Bucket choose options **Update Bucket Policy**. [This will update the bucket policy for us].
- Leave the **Origin Custom Headers** blank.

The screenshot shows the 'Create Distribution' page in the AWS console. The 'Origin Settings' section is visible, containing the following fields and options:

- Origin Domain Name:** 2020-05-21-mybucket.s3.amazonaws.com
- Origin Path:** (empty)
- Origin ID:** S3-2020-05-21-mybucket
- Restrict Bucket Access:** ☒ Yes, ☐ No
- Origin Access Identity:** ☒ Create a New Identity, ☐ Use an Existing Identity
- Comment:** access-identity-2020-05-21-mybucket.s3
- Grant Read Permissions on Bucket:** ☒ Yes, Update Bucket Policy, ☐ No, I Will Update Permissions
- Origin Custom Headers:** A table with columns 'Header Name' and 'Value', both currently empty.

- For the **Default Cache Behavior Settings** section:
- Under **Viewer Protocol Policy** select option **Redirect HTTP to HTTPS**.
- For **Allowed HTTP Methods** choose **GET, HEAD**.
- Leave **Field-level Encryption Config** blank.
- Leave **GET, HEAD (Cached by default)** for **Cached HTTP Methods**.
- For **Cache Based on Selected Request Headers** leave it as the default **none (Improves Caching)**.

- For **Object Caching** also leave it as the default **Use Origin Cache Headers**

Default Cache Behavior Settings

Path Pattern	Default (*)	?
Viewer Protocol Policy	<input type="radio"/> HTTP and HTTPS <input checked="" type="radio"/> Redirect HTTP to HTTPS <input type="radio"/> HTTPS Only	?
Allowed HTTP Methods	<input checked="" type="radio"/> GET, HEAD <input type="radio"/> GET, HEAD, OPTIONS <input type="radio"/> GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE	?
Field-level Encryption Config	(empty dropdown)	?
Cached HTTP Methods	GET, HEAD (Cached by default)	?
Cache Based on Selected Request Headers	None (Improves Caching)	?
	Learn More	
Object Caching	<input checked="" type="radio"/> Use Origin Cache Headers <input type="radio"/> Customize	?
	Learn More	
Minimum TTL	0	?
Maximum TTL	31536000	?
Default TTL	86400	?

- Under **Forward Cookies** leave it as **None (Improves Caching)**.
- Also for **Query String Forwarding and Caching** leave as **None (Improves Caching)**.
- For **Smoothing streaming** select **No**.
- For **Restrict Viewer Access (Use Signed URLs or Signed Cookies)** select **No**.
- Leave **Compress Objects Automatically** as **No**.
- Leave **Lambda Function Associations** as the default.

Distribution Settings

Forward Cookies	None (Improves Caching)	?
Query String Forwarding and Caching	None (Improves Caching)	?
Smooth Streaming	<input type="radio"/> Yes <input checked="" type="radio"/> No	?
Restrict Viewer Access (Use Signed URLs or Signed Cookies)	<input type="radio"/> Yes <input checked="" type="radio"/> No	?
Compress Objects Automatically	<input type="radio"/> Yes <input checked="" type="radio"/> No	?
	Learn More	
Lambda Function Associations	(empty)	?
CloudFront Event	<input type="text" value="Select Event Type"/>	
Lambda Function ARN	<input type="text"/>	
Include Body	<input type="checkbox"/>	
	Learn More	

- Scroll down to **Distribution Settings**.
- For **Price Class** leave the default **Use All Edge Locations (Best Performance)**.

- We will not be using WAF, so for **AWS WAF Web ACL**, leave it as **None**.
- Leave **Alternate Domain Names (CNAMEs)** blank.
- We will also use the **Default CloudFront Certificate** for **SSL Certificate**.

Distribution Settings

Price Class: Use All Edge Locations (Best Performance) ⓘ

AWS WAF Web ACL: None ⓘ

Alternate Domain Names (CNAMEs): ⓘ

SSL Certificate:

- ☒ Default CloudFront Certificate (*.cloudfront.net)

Choose this option if you want your users to use HTTPS or HTTP to access your content with the CloudFront domain name (such as https://d111111abcdeffs.cloudfront.net/logo.jpg). Important: If you choose this option, CloudFront requires that browsers or devices support TLSv1 or later to access your content.

- ☐ Custom SSL Certificate (example.com):

Choose this option if you want your users to access your content by using an alternate domain name, such as https://www.example.com. You can use a certificate stored in AWS Certificate Manager (ACM) in the US East (N. Virginia) Region, or you can use a certificate stored in IAM.

Request or Import a Certificate with ACM ⓘ

[Learn more about using custom SSL/TLS certificates with CloudFront.](#)
[Learn more about using ACM.](#)

- For **Supported HTTP Versions** leave as **HTTP/2,HTTP/1.1,HTTP/1.0**.
- Under **Default Root Object** type **index.html**.
- We can leave **Logging** set to **Off**.
- Leave **Enable IPv6** checked.
- Finally set the **Distribution State** to **Enabled**.

aws

Services

Resource Groups

AWSReservedSSO_udgama-fg-bo...

Global

Support

Step 1: Select delivery method

Step 2: Create distribution

Supported HTTP Versions

☒ HTTP/2, HTTP/1.1, HTTP/1.0

☐ HTTP/1.1, HTTP/1.0

Default Root Object

Logging

☐ On

☒ Off

Bucket for Logs

Log Prefix

Cookie Logging

☐ On

☒ Off

Enable IPv6

☒

[Learn more](#)

Comment

Distribution State

☒ Enabled

☐ Disabled

- Click **Create Distribution**.

- Click on **Distributions** at the top left to see the status of CloudFront distribution being built or not.
- This can take 15–20 minutes to complete.

2. Restrict our S3 bucket policy to Cloud Front

- Click **Services** at the top left and type in S3 or select it from History.
- Click on your Bucket name **2024-mm-dd-xx-mybucket**.

IMPORTANT: Your bucket will have a different name.

- Click **Permissions**.
- Select **Bucket Policy**.
- We can see that CloudFront has added what we call an “Origin Access Identity” to the policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AddPerm",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::2020-05-21-mybucket/*"
    },
    {
      "Sid": "2",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity E2V8GJ8FKJPGFQ"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::2020-05-21-mybucket/*"
    }
  ]
}
```

- Remove the public s3 section so it looks like following

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "2",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
        Identity E2V8GJ8FKJPGFQ"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::2020-05-21-mybucket/*"
    }
  ]
}
```

- This will only allow our specific CloudFront distribution access to our S3 bucket which is what we want.
- Click **Save**.

3. Steps for testing that we successfully locked down S3 from public view

- Browse to your S3 endpoint:
Example: <http://2020-05-21-mybucket.s3-website-us-east-1.amazonaws.com>
- You will see a **403 Forbidden** because we removed public access from the bucket policy.

403 Forbidden






- Code: AccessDenied
- Message: Access Denied
- RequestId: 19484A9BACAAAF49F
- HostId: a8203GKQUo4VWzqCuJVhQ4o+V1LF2e+6++rv+IX8i8fE0ZlSh2mT8nIMA2pKUwb9H78DimGbYr8=

An Error Occurred While Attempting to Retrieve a Custom Error Document


- Code: AccessDenied
- Message: Access Denied

- Click on the **CloudFront distribution ID**. (The blue hyperlink)

CloudFront Distributions

Create Distribution	Distribution Settings	Delete	Enable	Disable	   				
Viewing :	Any Delivery Method ▾	Any State ▾			« < Viewing 1 to 1 of 1 Items > »				
	Delivery Method	ID ▾	Domain Name	Comment	Origin	CNAMEs	Status	State	Last Modified
	Web	E23ZQG9G3RKWD5	deiew0jukacs.	-	2020-05-	-	Deployer	Enabled	2020-04-21 16
« < Viewing 1 to 1 of 1 Items > »									

- Copy the URL under **Domain Name**.

CloudFront Distributions > E23ZQG9G3RKWD5	
General Origins and Origin Groups Behaviors Error Pages Restrictions Invalidations Tags	
	
Distribution ID	E23ZQG9G3RKWD5
ARN	arn:aws:cloudfront::979426164612:distribution/E23ZQG9G3RKWD5
Log Prefix	-
Delivery Method	Web
Cookie Logging	Off
Distribution Status	Deployed
Comment	-
Price Class	Use All Edge Locations (Best Performance)
AWS WAF Web ACL	-
State	Enabled
Alternate Domain Names (CNAMEs)	-
SSL Certificate	Default CloudFront Certificate (*.cloudfront.net)
Domain Name	deiew0jukacs.cloudfront.net
Custom SSL Client Support	-
Security Policy	TLSv1
Supported HTTP Versions	HTTP/2, HTTP/1.1, HTTP/1.0
IPv6	Enabled

THAT'S ALL