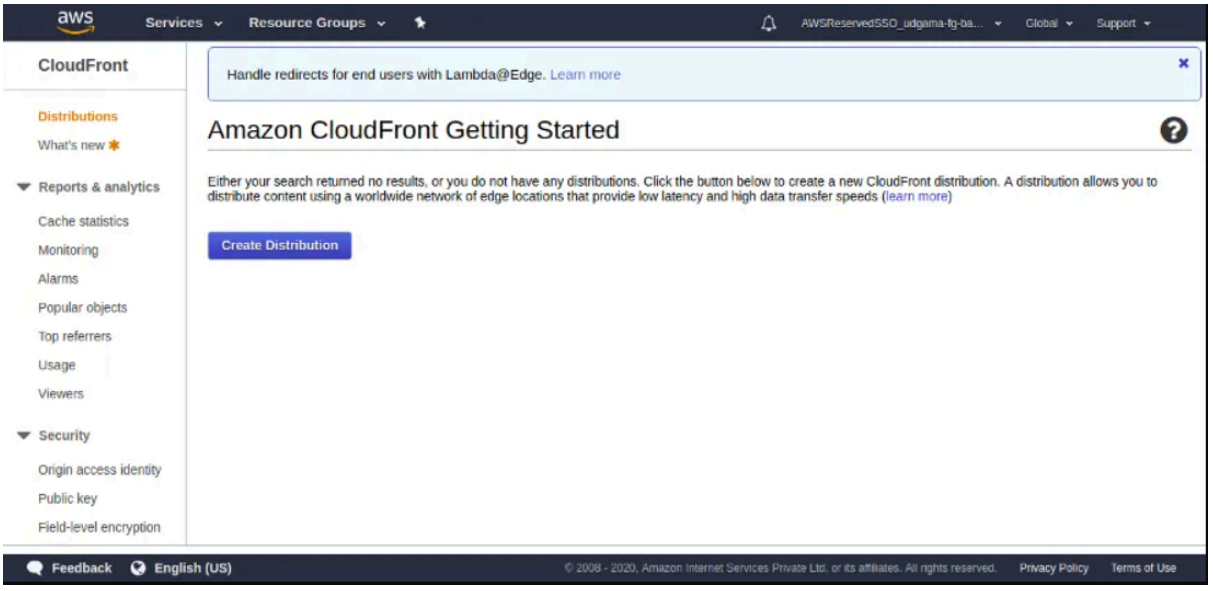
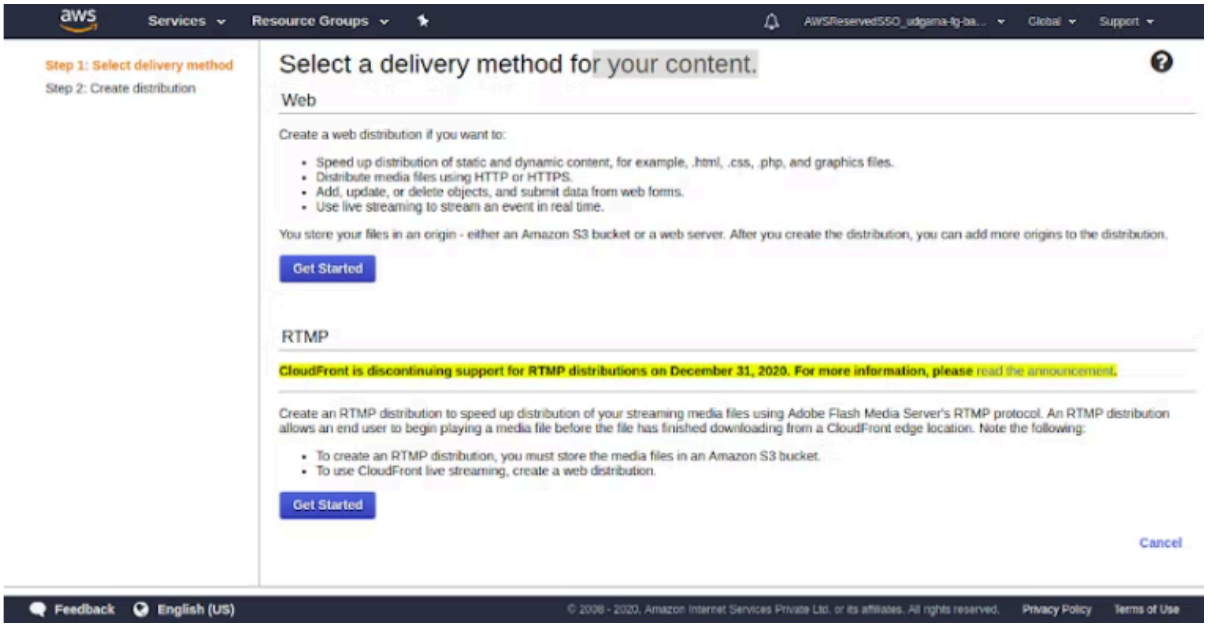
Let’s start the creation of CloudFront distribution.

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**.



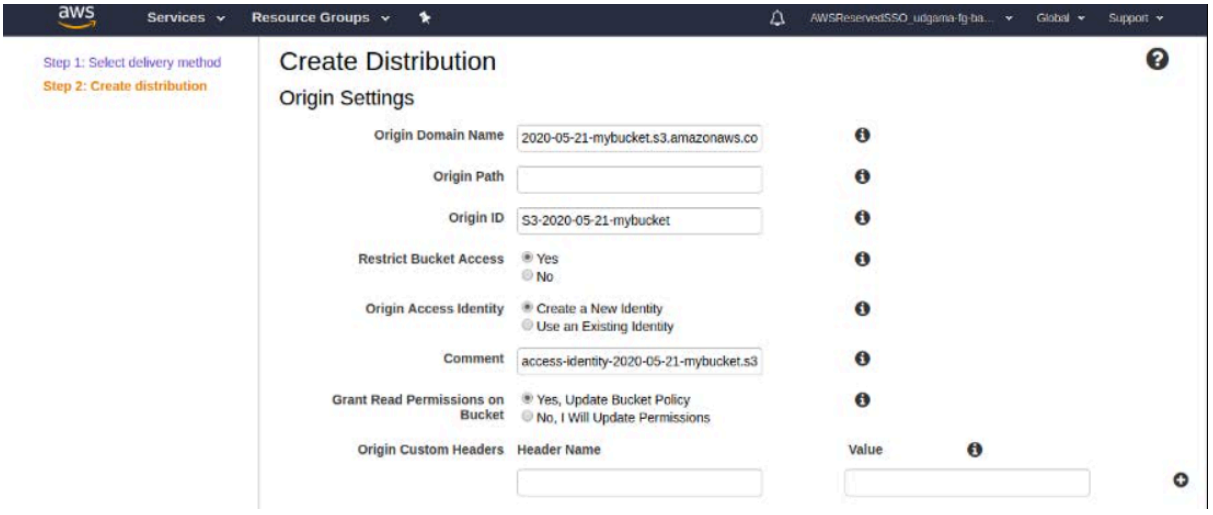
- Under **Web** click **Get Started**.



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

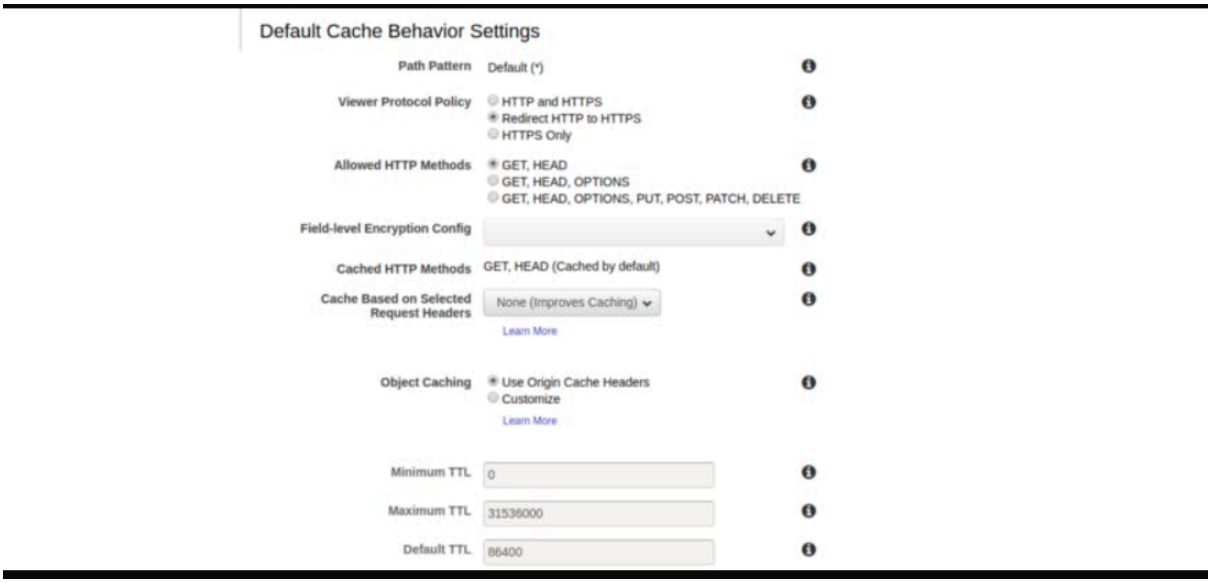
Note: I already created S3 bucket in AWS so If you don't have any website on S3 bucket then plz create it first

- 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.

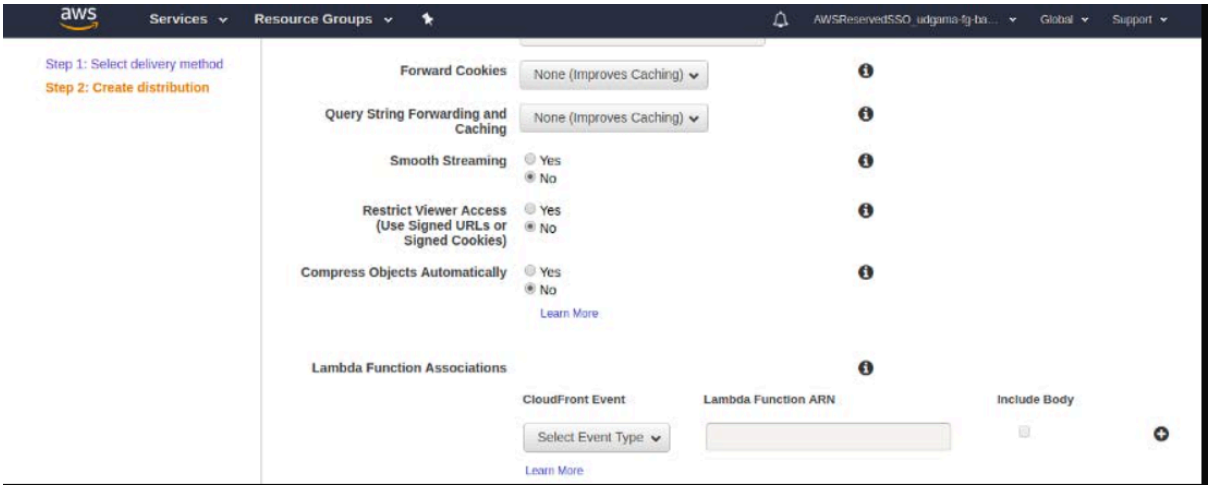


- For the **Default Cache Behavior Settings** section:
- Under **Viewer Protocol Policy** select option **Redirect HTTP to HTTPS**.
- For **Allowed HTTP Methods** choose **GET, HEAD**.
- Leave **Field-level Encryption Config** blank.
- Leave **GET, HEAD (Cached by default)** for **Cached HTTP Methods**.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

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

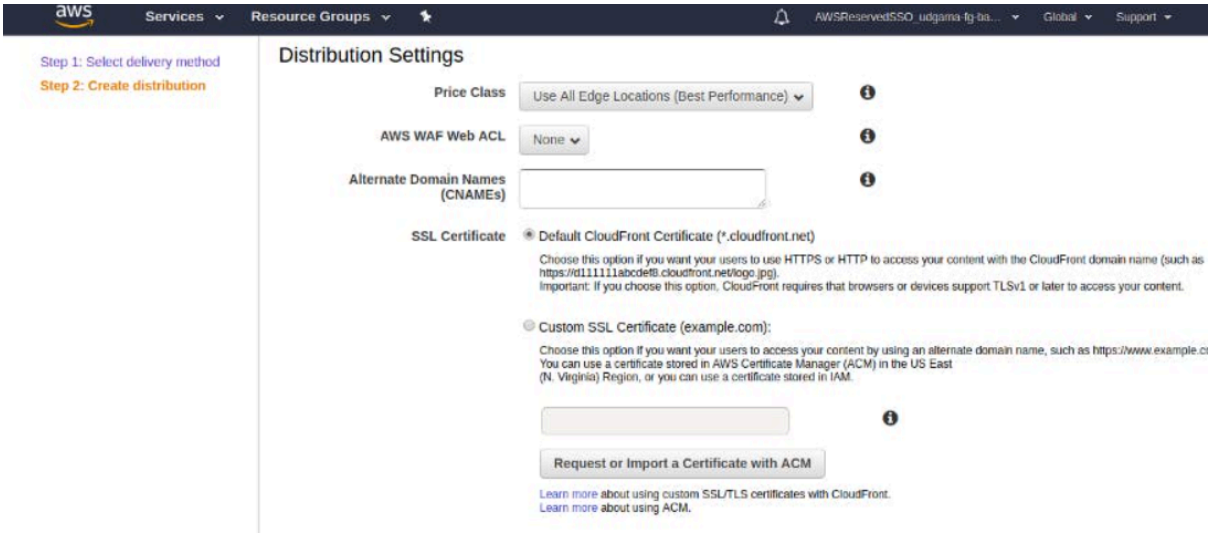


- Under **Forward Cookies** leave it as **None (Improves Caching)**.
- Also for **Query String Forwarding and Caching** leave as **None (Improves Caching).**
- For **Smoothing streaming** select **No**.
- For **Restrict Viewer Access (Use Signed URLs or Signed Cookies)** select **No**.
- Leave **Compress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

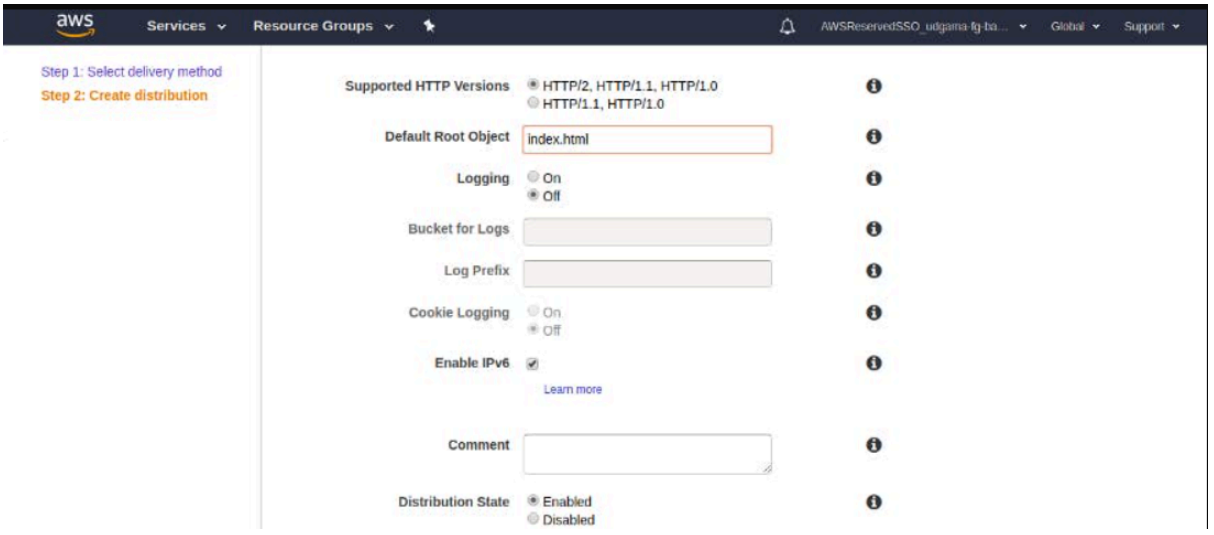


- Scroll down to **Distribution Settings**.
- For **Price Class** leave the default **Use All Edge Locations (Best Performance)**.

- 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.**



- 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**.



- 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.

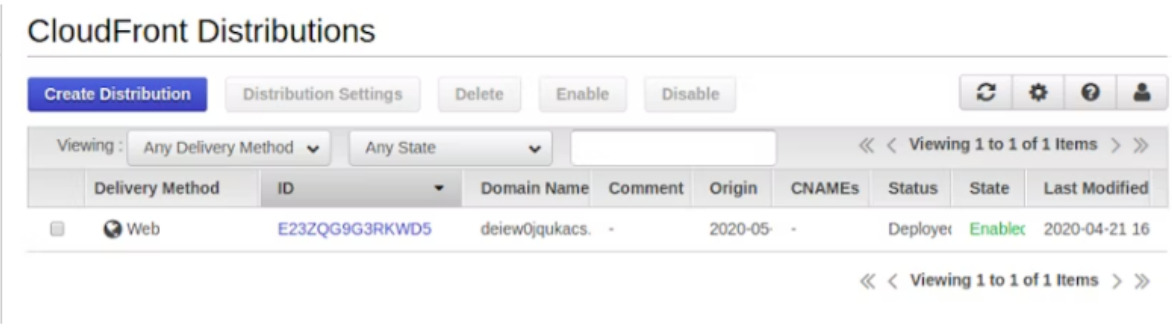
403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: 19484A9BACAAF49F
- HostId: a8203GKQUo4VWzqCuJVhQ4o+V1LF2e+6++rv+lX8i8fE0ZlSh2mT8nIMA2pKUwb9H78DimGbYr8=

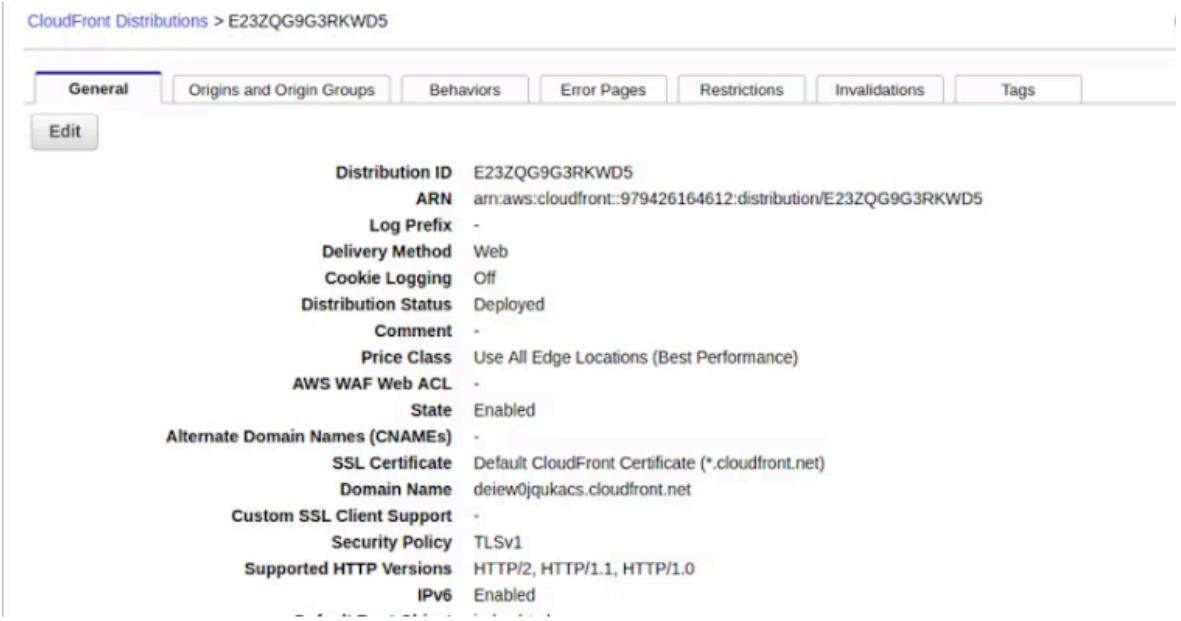
An Error Occurred While Attempting to Retrieve a Custom Error Document

- Code: AccessDenied
- Message: Access Denied

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



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



THAT'S ALL