Setup AWS S3 static website hosting using SSL (ACM)

medium.com/@sbuckpesch/setup-aws-s3-static-website-hosting-using-ssl-acm-34d41d32e394

February 24, 2017

Sebastian Buckpesch
I write about AWS and cloud topics. I'm interested in User experience, Web, Internet of things and Automation. Portfolio: https://buckpesch.io/

Feb 24, 2017

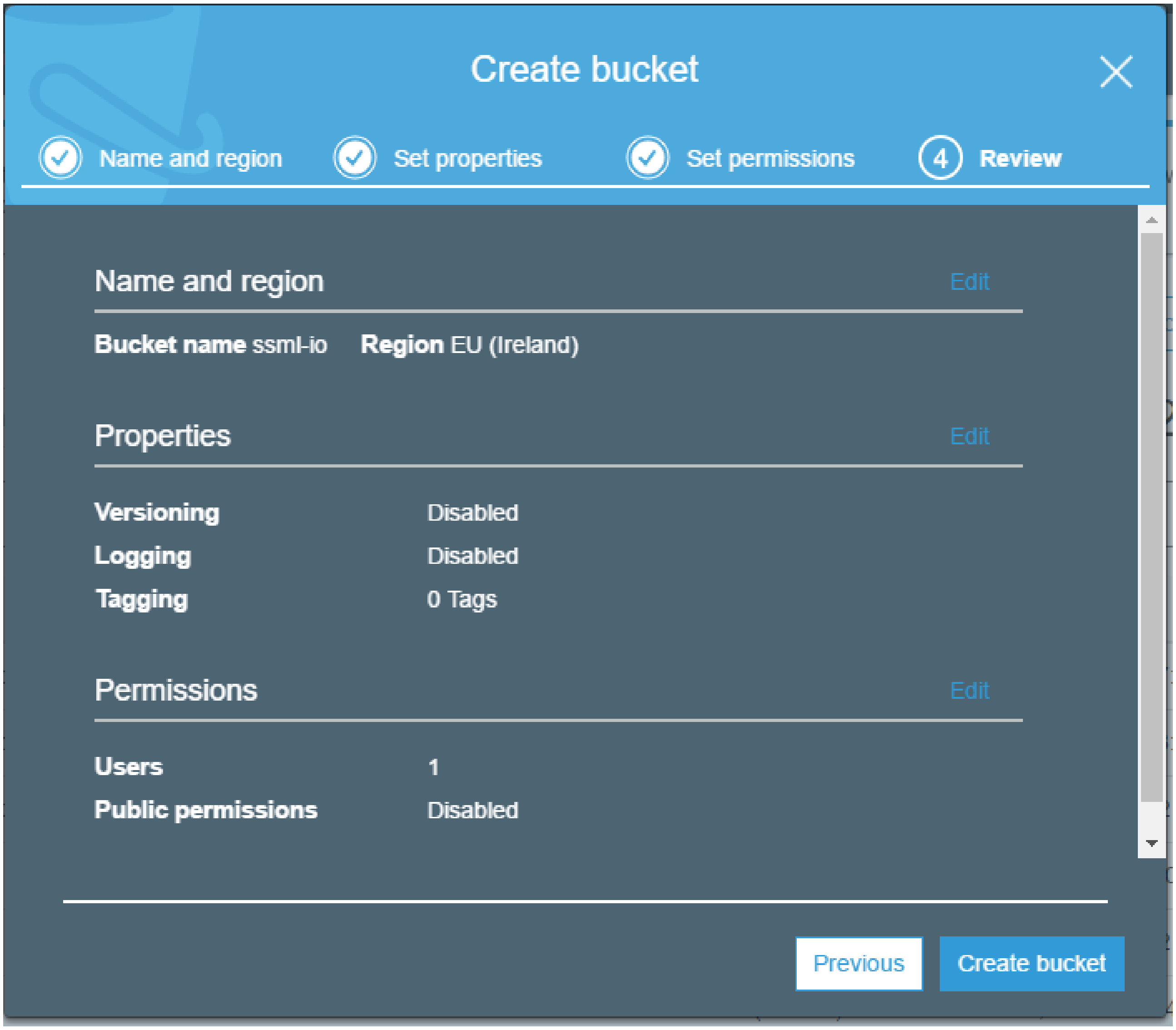
I registered a new domain (ssml.io) and I want to use it to host a static website using S3 and Cloudfront. For this website I want an SSL connection using a AWS Certificate Manager certificate.

To finish this setup you have to go through these steps:

- Create an S3 bucket and upload your index.html file
- Create a cloudfront distribution pointing to this S3 bucket
- Setup Domain MX records using SES to receive the SSL certificate domain validation email
- Request a new SSL certificate in region *us-east-1* (!)
- Assign the certificate to your Cloudfront distribution

I assume that you already have a (new) domain registered in Route 53 with no A or MX records setup.

1) Create a new S3 bucket for your static files



Name and region

Bucket name ssml-io **Region** EU (Ireland)

Properties

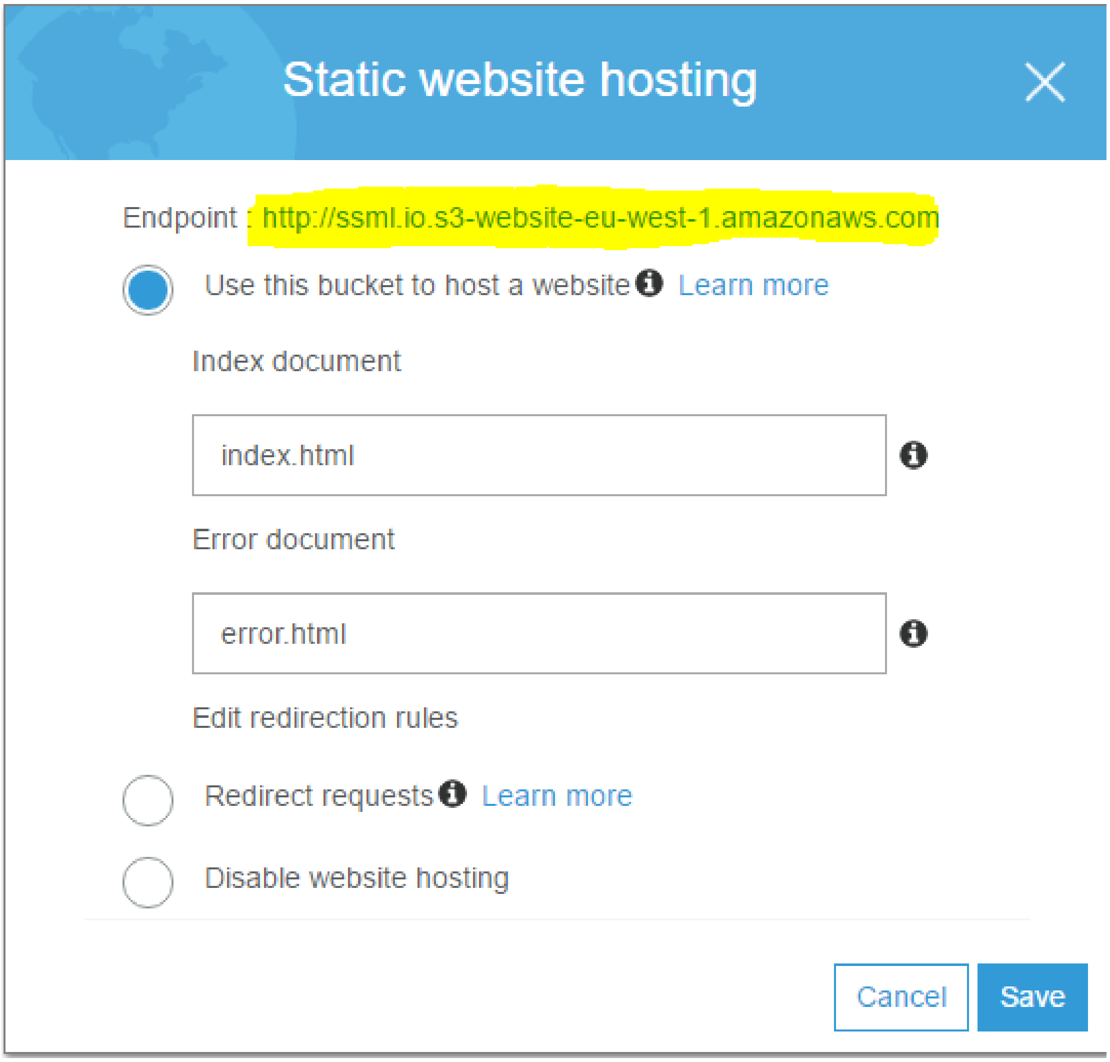
Versioning Disabled
Logging Disabled
Tagging 0 Tags

Permissions

Users 1
Public permissions Disabled

Create a new S3 bucket using the default settings

Open the buckets properties and activate “Static website hosting”. Make note of the Endpoint URI.



Static website hosting

Endpoint : http://ssml.io.s3-website-eu-west-1.amazonaws.com

● Use this bucket to host a website Learn more

Index document

index.html

Error document

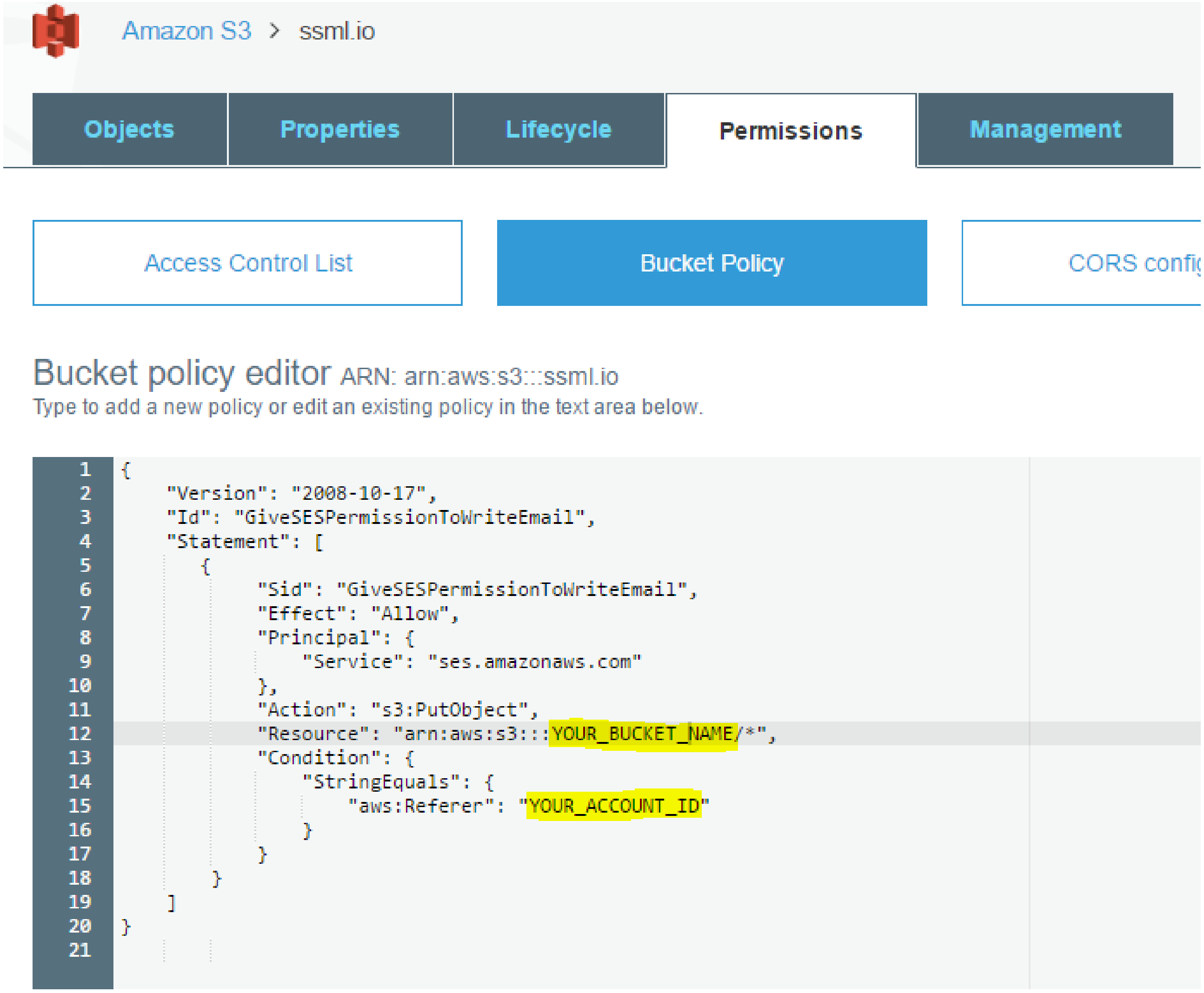
error.html

Edit redirection rules

○ Redirect requests Learn more

○ Disable website hosting

To save emails on your bucket from SES later, you need to grant permissions to SES to write to your bucket. Add the following bucket policy and replace *YOUR_BUCKET_NAME* and *YOUR_ACCOUNT_ID* with your corresponding values.



Bucket policy editor ARN: arn:aws:s3:::ssml.io

Type to add a new policy or edit an existing policy in the text area below.

```
{
    "Version": "2008-10-17",
    "Id": "GiveSESPermissionToWriteEmail",
    "Statement": [
        {
            "Sid": "GiveSESPermissionToWriteEmail",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::YOUR_BUCKET_NAME/*",
            "Condition": {
                "StringEquals": {
                    "aws:Referer": "YOUR_ACCOUNT_ID"
                }
            }
        }
    ]
}
```

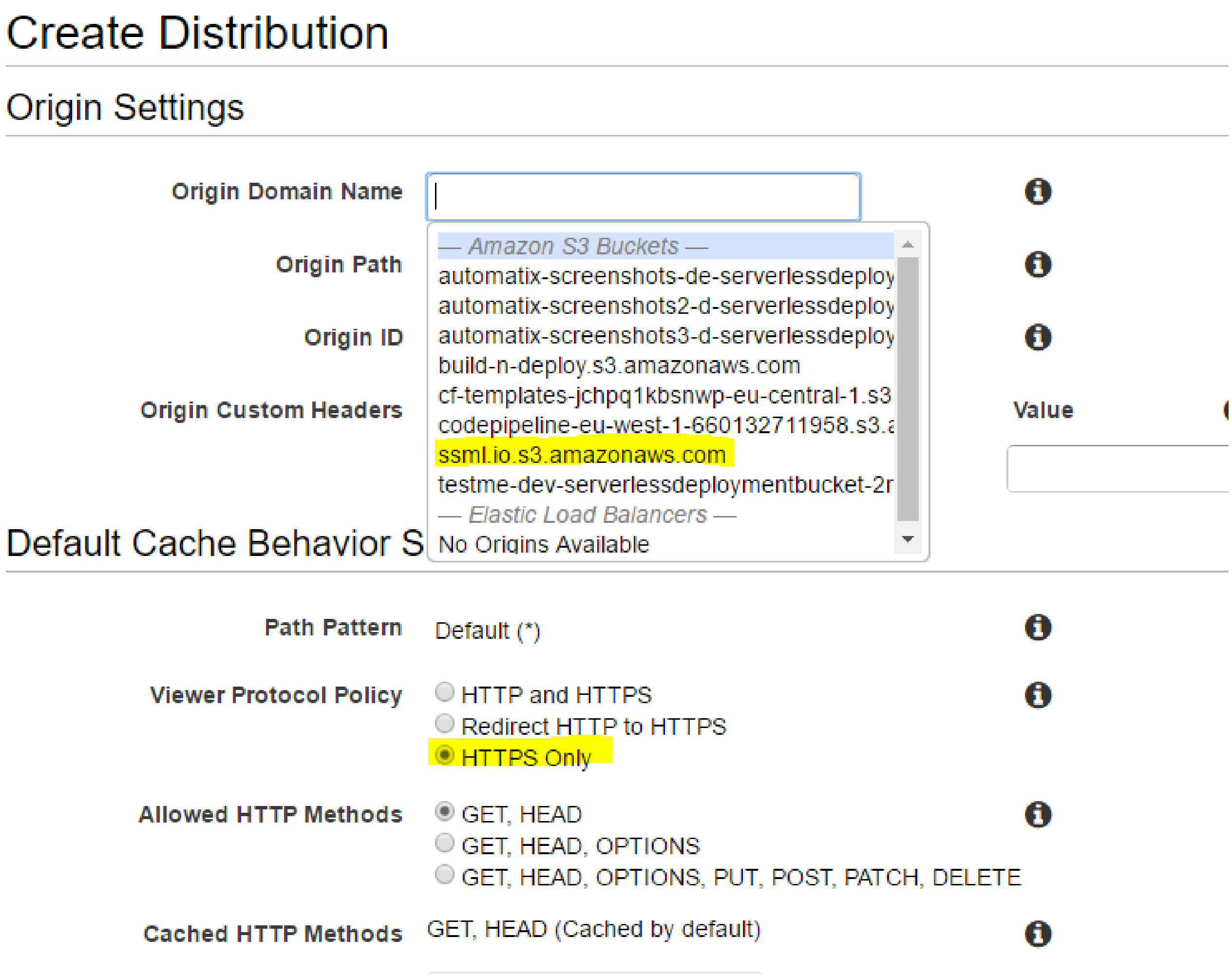
```
{
  "Version": "2012-10-17",
  "Id": "GiveSESPermissionToWriteEmail",
  "Statement": [
    {
      "Sid": "GiveSESPermissionToWriteEmail",
      "Effect": "Allow",
      "Principal": {
        "Service": "ses.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::ssml.io/*",
      "Condition": {
        "StringEquals": {
          "aws:Referer": "123456789012"
        }
      }
    }
  ]
}
```

Save the policy, upload your index.html file and your are done.

2) Create a cloudfront distribution using a custom CNAME

SSL certificates can only be assigned to cloudfront distributions, so we need to create one to enable SSL for our static website.

Create a new Web distribution and select your S3 bucket as*Origin Domain Name*. Select HTTPS Only for *Viewer Protocol Policy*.



Create Distribution

Origin Settings

Origin Domain Name: |

— Amazon S3 Buckets —
automatix-screenshots-de-serverlessdeploy
automatix-screenshots2-d-serverlessdeploy
automatix-screenshots3-d-serverlessdeploy
build-n-deploy.s3.amazonaws.com
cf-templates-jchpq1kbsnwp-eu-central-1.s3
codepipeline-eu-west-1-660132711958.s3.a
ssml.io.s3.amazonaws.com
testme-dev-serverlessdeploymentbucket-2r
— Elastic Load Balancers —
No Origins Available

Origin Path

Origin ID

Origin Custom Headers — Value

Default Cache Behavior S

Path Pattern: Default (*)

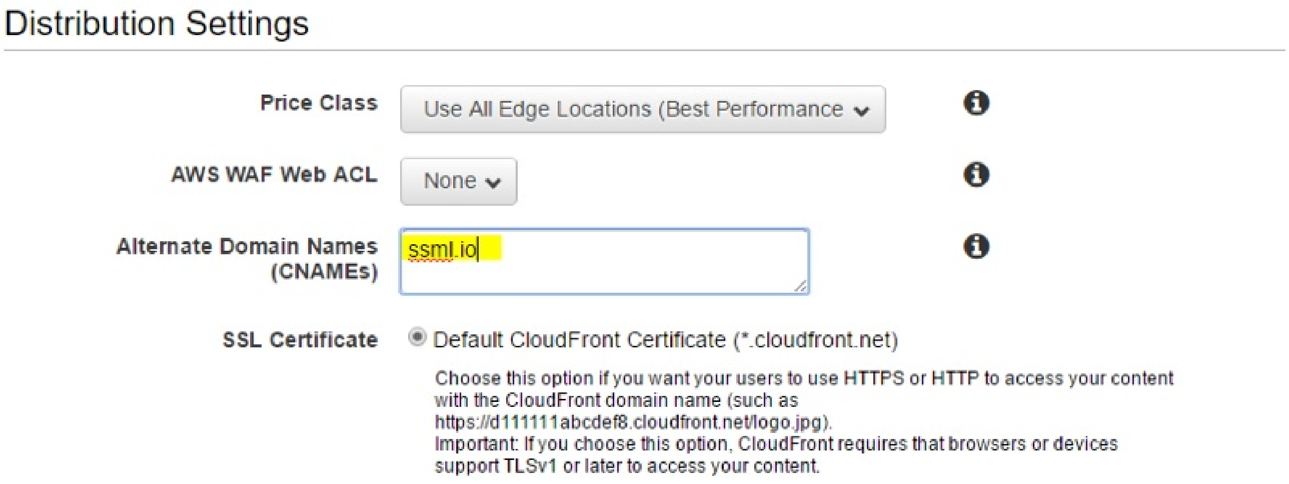
Viewer Protocol Policy:
○ HTTP and HTTPS
○ Redirect HTTP to HTTPS
● HTTPS Only

Allowed HTTP Methods:
● GET, HEAD
○ GET, HEAD, OPTIONS
○ GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Cached HTTP Methods: GET, HEAD (Cached by default)

Select the S3 bucket as origin and set the viewer protocol to HTTPS only

In the Distribution Settings section enter your domain name you want to host your static files on (My site is https://ssml.io). Do not change the SSL Certificate settings for now, as we did not setup our email address to receive the domain validation email for our certificate request.



Distribution Settings

Price Class: Use All Edge Locations (Best Performance

AWS WAF Web ACL: None

Alternate Domain Names (CNAMEs): ssml.io

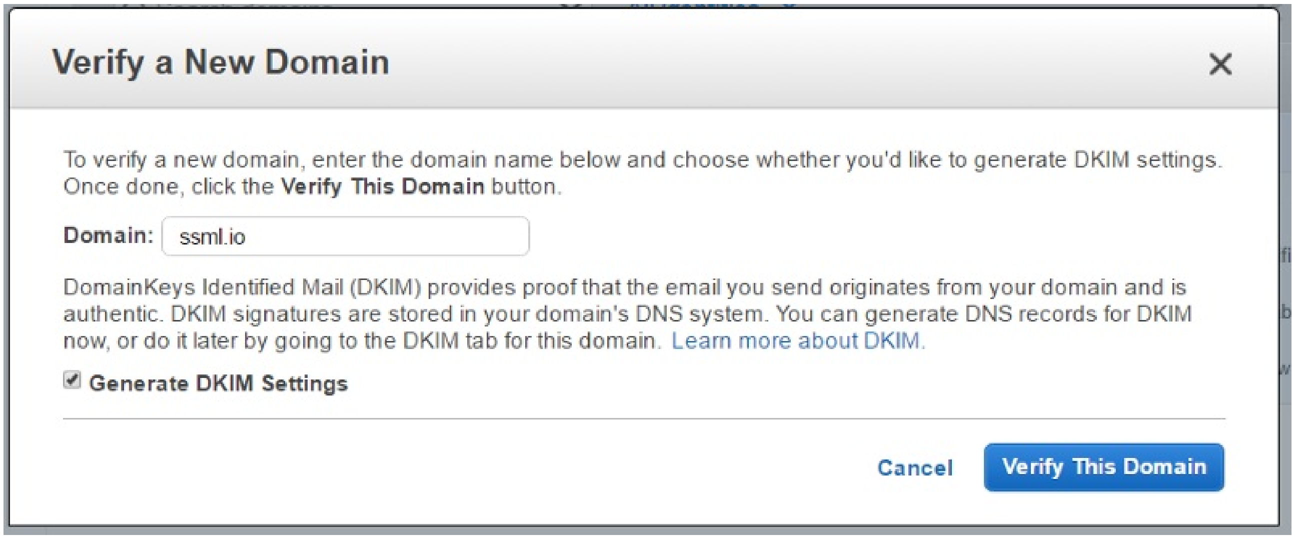
SSL Certificate: ● Default CloudFront Certificate (*.cloudfront.net)

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://d111111abcdef8.cloudfront.net/logo.jpg).
Important: If you choose this option, CloudFront requires that browsers or devices support TLSv1 or later to access your content.

Beside that keep all the default settings and click “Create distribution”. Grab a cup of coffee or two and wait until the distribution is created………

3) Setup Route53 MX records using SES to forward emails to S3

Go to AWS SES and verify a new domain. Generate DKIM Settings as well.



Verify a New Domain

To verify a new domain, enter the domain name below and choose whether you'd like to generate DKIM settings. Once done, click the **Verify This Domain** button.

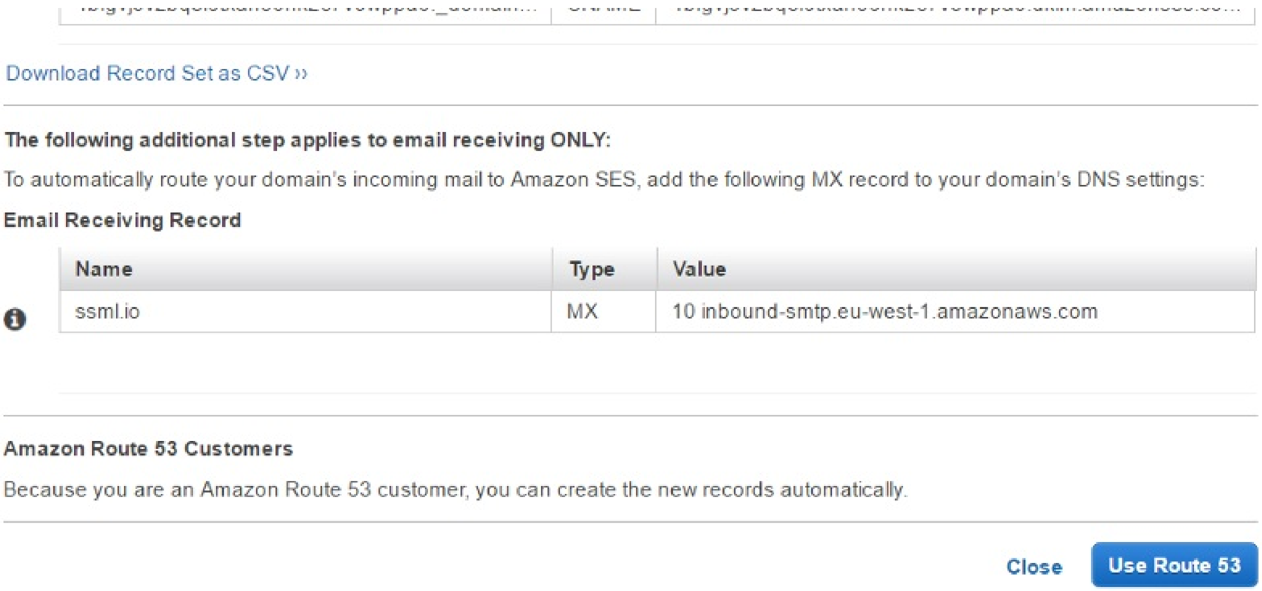
Domain: ssml.io

DomainKeys Identified Mail (DKIM) provides proof that the email you send originates from your domain and is authentic. DKIM signatures are stored in your domain's DNS system. You can generate DNS records for DKIM now, or do it later by going to the DKIM tab for this domain. Learn more about DKIM.

☑ Generate DKIM Settings

Generate DKIM Settings for your domain to verify your email domain

Click “Use Route53” to setup all necessary Domain Records in Route53. Amazon is handling everything for you :-)



Download Record Set as CSV ››

The following additional step applies to email receiving ONLY:

To automatically route your domain's incoming mail to Amazon SES, add the following MX record to your domain's DNS settings:

Email Receiving Record

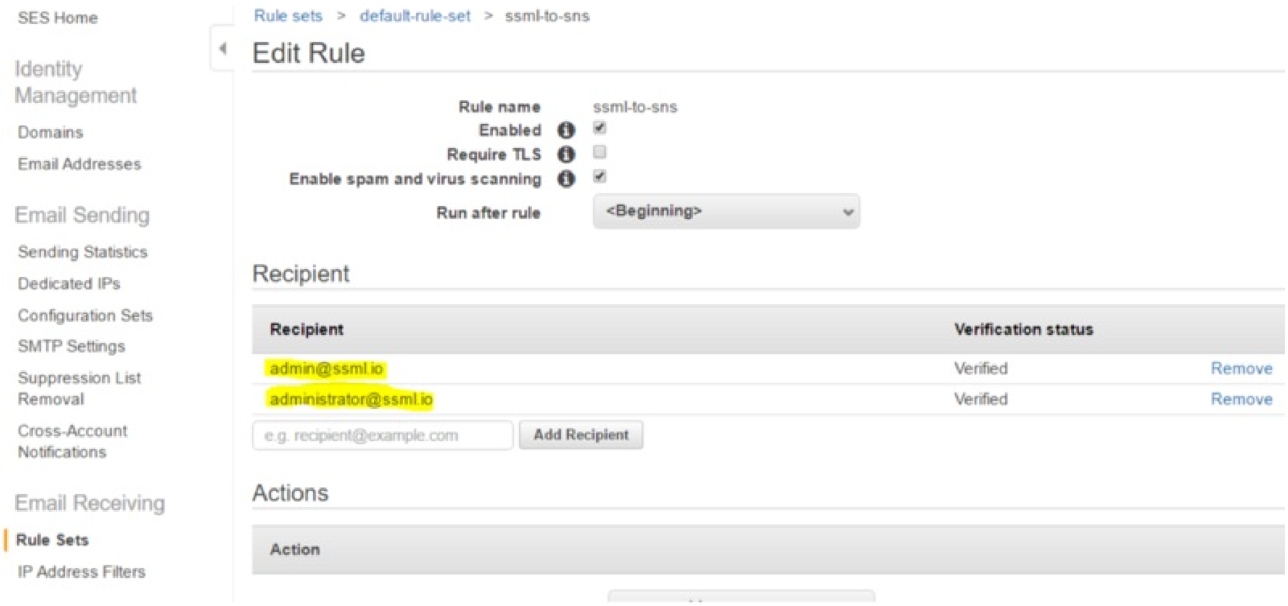
Name	Type	Value
ssml.io	MX	10 inbound-smtp.eu-west-1.amazonaws.com

Amazon Route 53 Customers

Because you are an Amazon Route 53 customer, you can create the new records automatically.

AWS helps yout to setup all your domain records to verify a email sending and receiving domain

In the left navigation head to “Rule sets”, create a new one and a new “Rule”. Enter *administrator@yourdomain.com* to the receipients as this email address is used by default to receive SSL certificate domain verification emails.



Rule sets > default-rule-set > ssml-to-sns

Edit Rule

Rule name: ssml-to-sns

Enabled ☑

Require TLS ☐

Enable spam and virus scanning ☑

Run after rule: <Beginning>

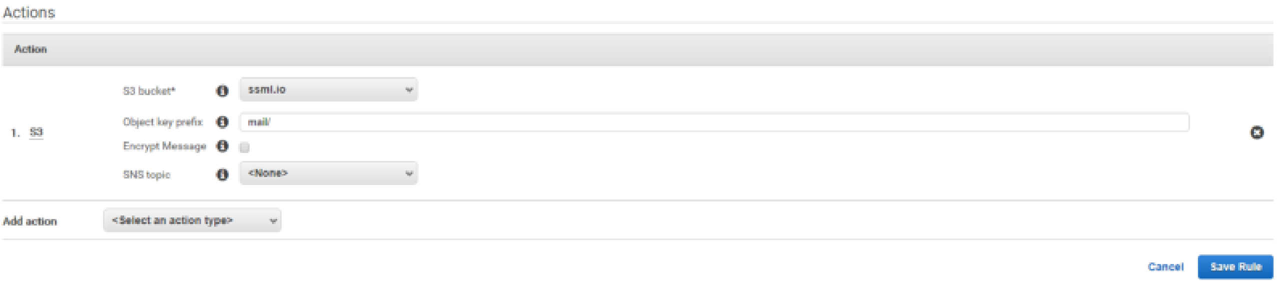
Recipient

Recipient	Verification status	
admin@ssml.io	Verified	Remove
administrator@ssml.io	Verified	Remove

Actions

Action

In the bottom part of the rule settings define a S3 Rule to save incoming email to a ‘folder’ in your bucket.



Actions

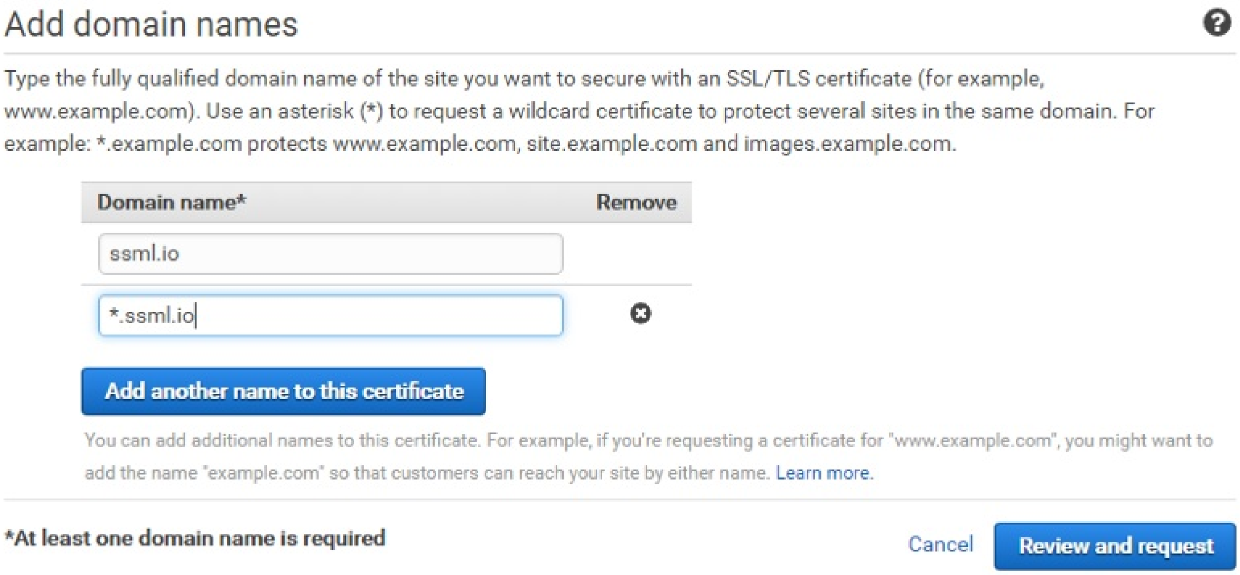
Action	
1. S3	S3 bucket*: ssml.io Object key prefix: mail/ Encrypt Message: □ SNS topic: <None>
Add action	<Select an action type>

Save incoming email to a S3 bucket

4) Request a free SSL certificate using AWS Certificate Manager (former ACM)

> Cloudfront only accepts certificates hosted in region us-east-1. **Switch to that region NOW**.

Enter one or more domain names, you want to create a SSL certificate for. You can even use a wildcard.



Add domain names

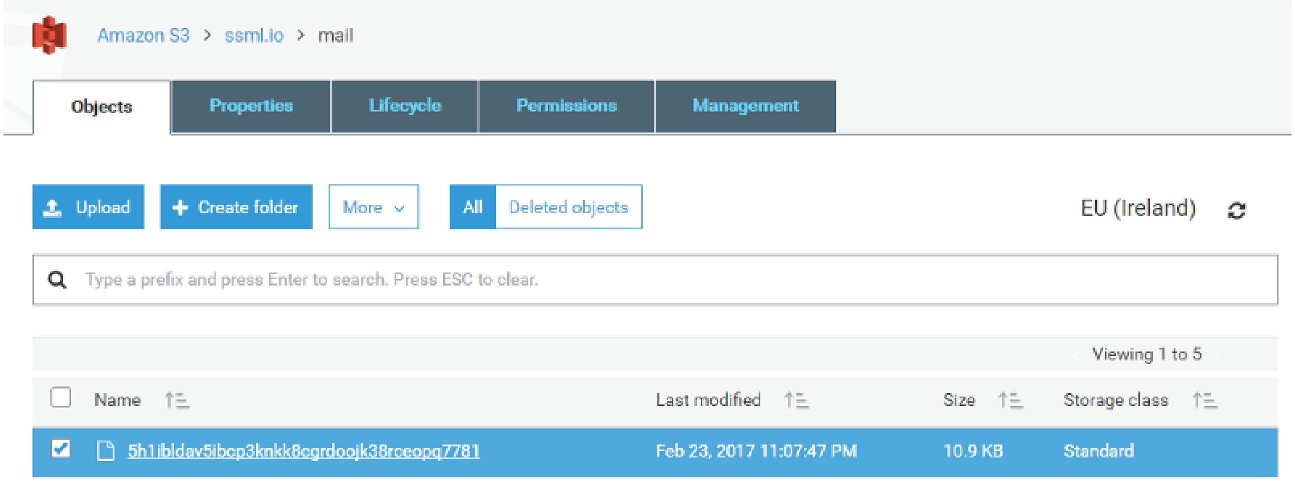
Type the fully qualified domain name of the site you want to secure with an SSL/TLS certificate (for example, www.example.com). Use an asterisk (*) to request a wildcard certificate to protect several sites in the same domain. For example: *.example.com protects www.example.com, site.example.com and images.example.com.

Domain name*	Remove
ssml.io	
*.ssml.io	⊗

You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name. Learn more.

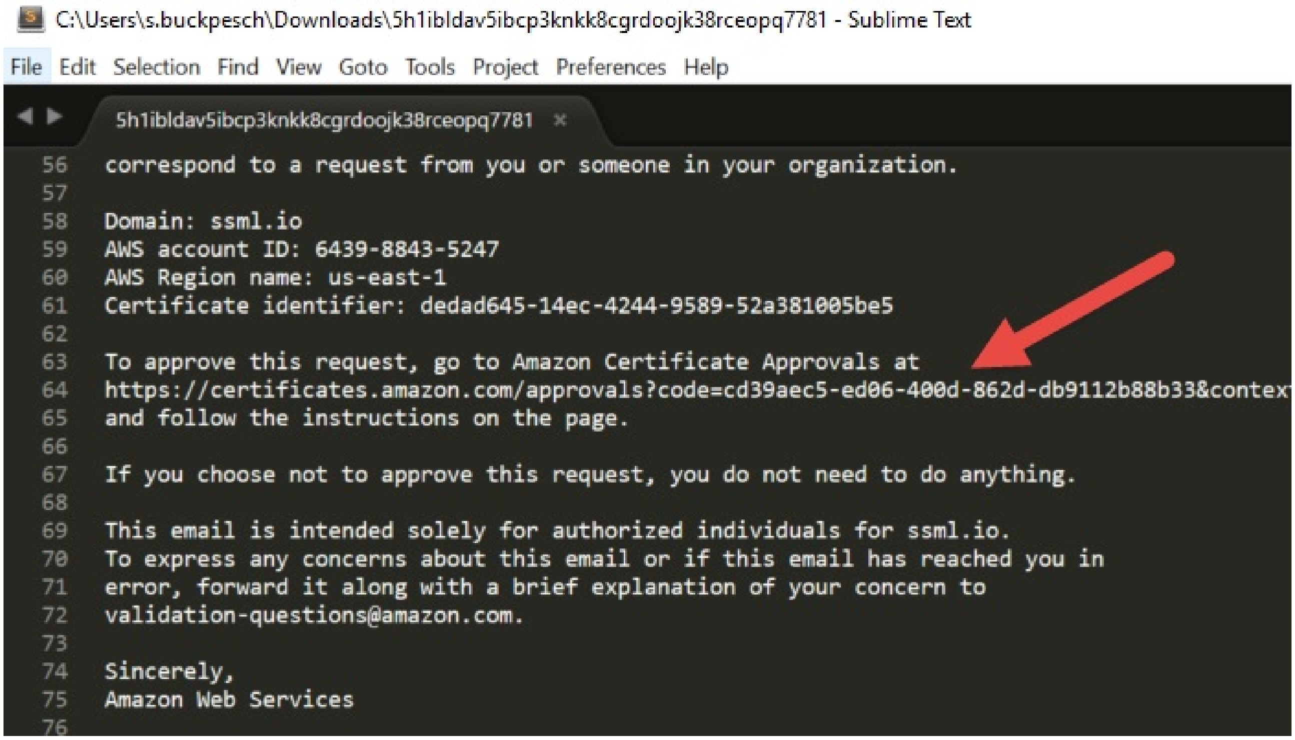
*At least one domain name is required

Now you should have a new email on your S3 bucket containing the verification link. Download the email file open it in your favorite text editor and copy the verification link to your browser.



Viewing 1 to 5

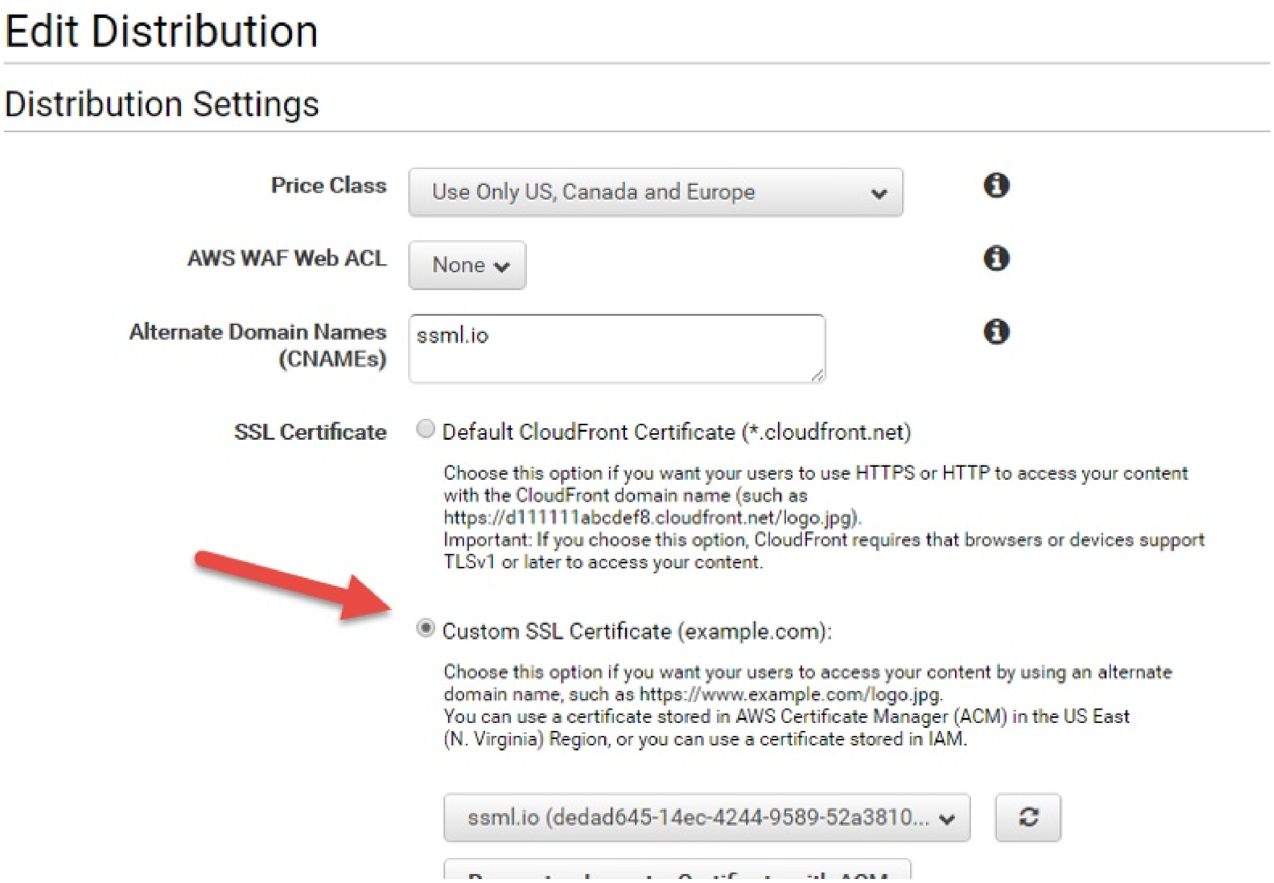
□	Name	Last modified	Size	Storage class
☑	5h1ibldav5ibcp3knkk8cgrdoojk38rceopq7781	Feb 23, 2017 11:07:47 PM	10.9 KB	Standard


C:\Users\s.buckpesch\Downloads\5h1ibldav5ibcp3knkk8cgrdoojk38rceopq7781 - Sublime Text
File Edit Selection Find View Goto Tools Project Preferences Help
5h1ibldav5ibcp3knkk8cgrdoojk38rceopq7781

```
correspond to a request from you or someone in your organization.

Domain: ssml.io
AWS account ID: 6439-8843-5247
AWS Region name: us-east-1
Certificate identifier: dedad645-14ec-4244-9589-52a381005be5

To approve this request, go to Amazon Certificate Approvals at
https://certificates.amazon.com/approvals?code=cd39aec5-ed06-400d-862d-db9112b88b33&contex
and follow the instructions on the page.

If you choose not to approve this request, you do not need to do anything.

This email is intended solely for authorized individuals for ssml.io.
To express any concerns about this email or if this email has reached you in
error, forward it along with a brief explanation of your concern to
validation-questions@amazon.com.

Sincerely,
Amazon Web Services
```

5) Assign the SSL certificate to your Cloudfront distribution

You’re almost done. Go back to Cloudfront and edit your distribution. Now you should be able to select your brand new SSL certificate.



Edit Distribution

Distribution Settings

Price Class: Use Only US, Canada and Europe

AWS WAF Web ACL: None

Alternate Domain Names (CNAMEs): ssml.io

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://d111111abcdef8.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/logo.jpg.
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.

ssml.io (dedad645-14ec-4244-9589-52a3810...

Select a SSL certificate from AWS Certificate Manager

Congratulations. You’re done :-) Check it out: https://ssml.io