S3Media LinkSafe™ Lite

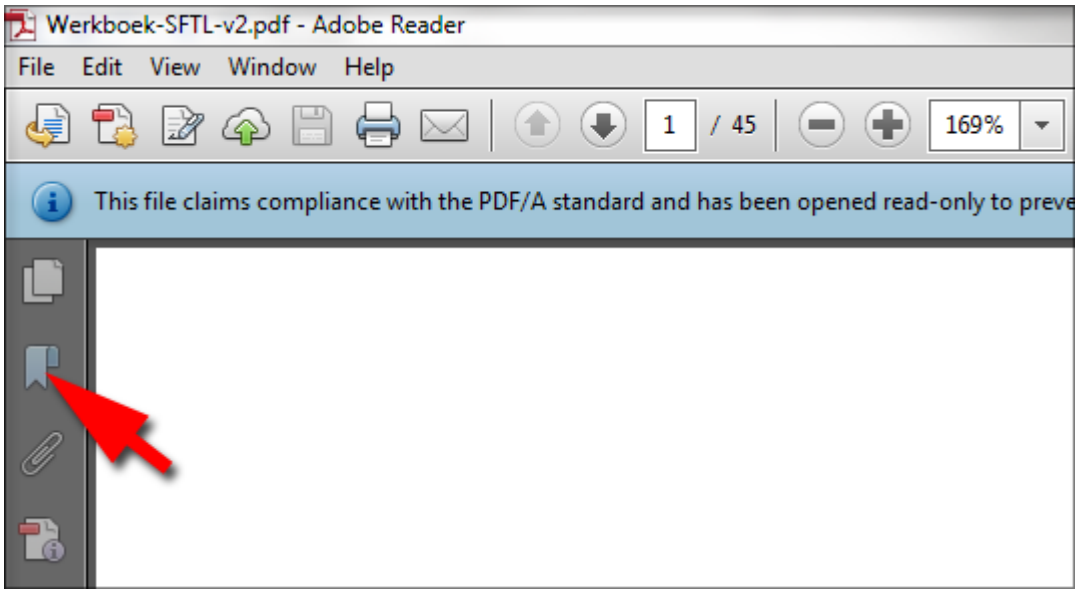
How to Tutorial: setting up web distributions - 17 January 2015 - for users of S3Media LinkSafe Lite

S3Media LinkSafe™ Lite is a free plugin for WordPress 3.x and 4.x featuring protected download links via S3 Amazon/CloudFront. Like S3Media Stream™ and S3Media Stream™ Enterprise, it works with *expiring URLs*, also called *signed URLs*.
An excellent tool if you offer paid or free documentation, games, webinars, applications, downloadable videos and audios or any file type you can think of via your WordPress site.

For example: you have a PDF, an audio, or any file type you want to share with your visitors but you do not want anyone to send that link via email or published on another site (a technique called 'leeching').
Then, S3Media LinkSafe™ Lite is the solution, because the links are only valid for a short period of time. Therefore, copying those links makes no sense.

To make this plugin work, you have to configure your S3 Amazon account before you can use it. In this tutorial we show you how to set up your bucket, create a private web distribution, upload your files using the AWS console and check/correct the permissions. Although this may sound complicated, with the easy step by step approach, you find it not so difficult.

This PDF has bookmarks. Best show the bookmarks for easy navigation in the document since it uses a lot of screenshots. You can show bookmarks by clicking on the ribbon in the left hand pane:



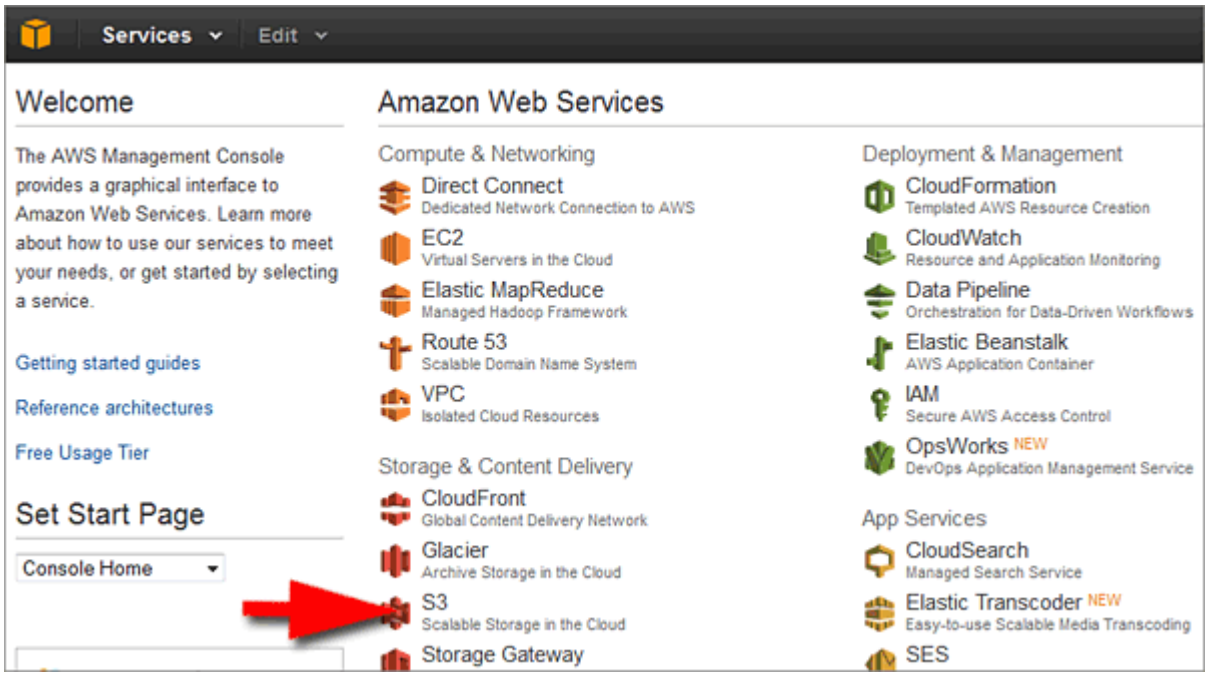
Setup a bucket using the AWS console

Basically, a bucket is a folder in which you can place files. Buckets can also contains directories(formerly called *folders*), making it possible to create a logical structure if you serve various file types. In this tutorial we do not go deeper into directories but work directly in the bucket to keep it simple.

Please note that the interface of the AWS console changes faster than you can drop your head, but generally they contain minor layout changes, like different colors or buttons or added functionality. Normally, you should be able to work it out with the included screenshots. If you notice dramatic changes, please let us know.

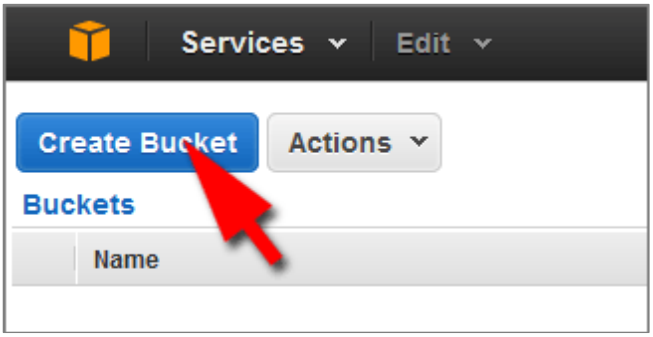
If you have already a bucket in your S3 account, you can skip this section and go to: **Create a Private Download CloudFront Distribution**, otherwise proceed creating your bucket:

First, you need to create a bucket. For this, you go to https://console.aws.amazon.com/console and login with your Amazon account credentials. You get now the following screen after login:

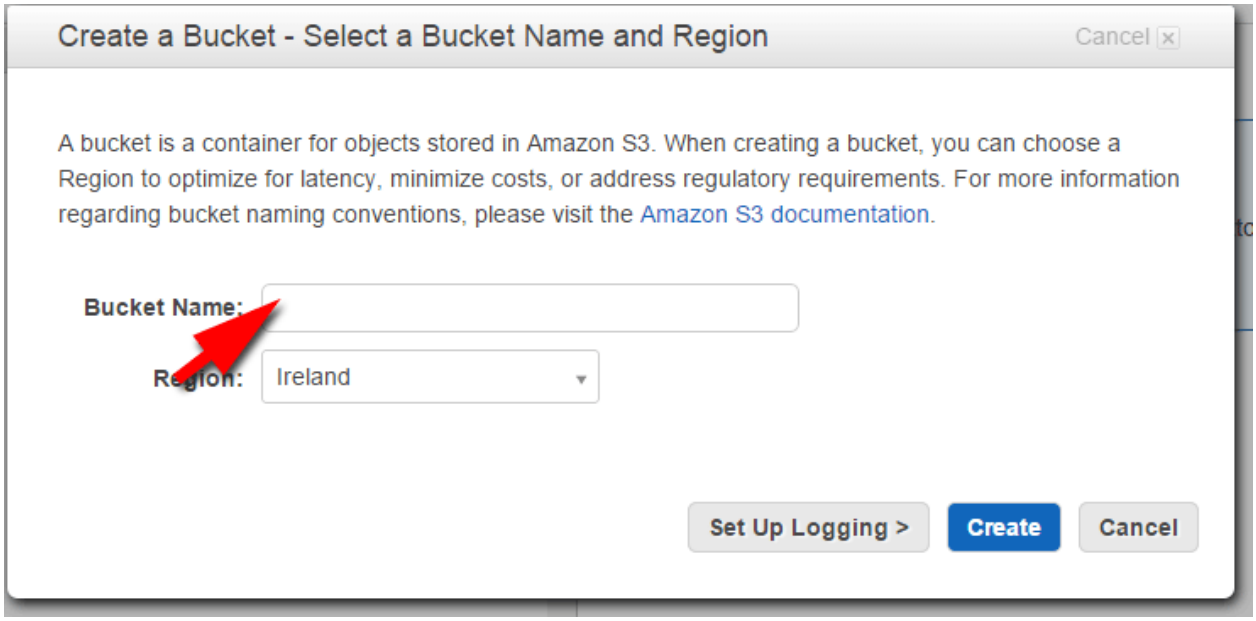


In that screen you select **S3**:

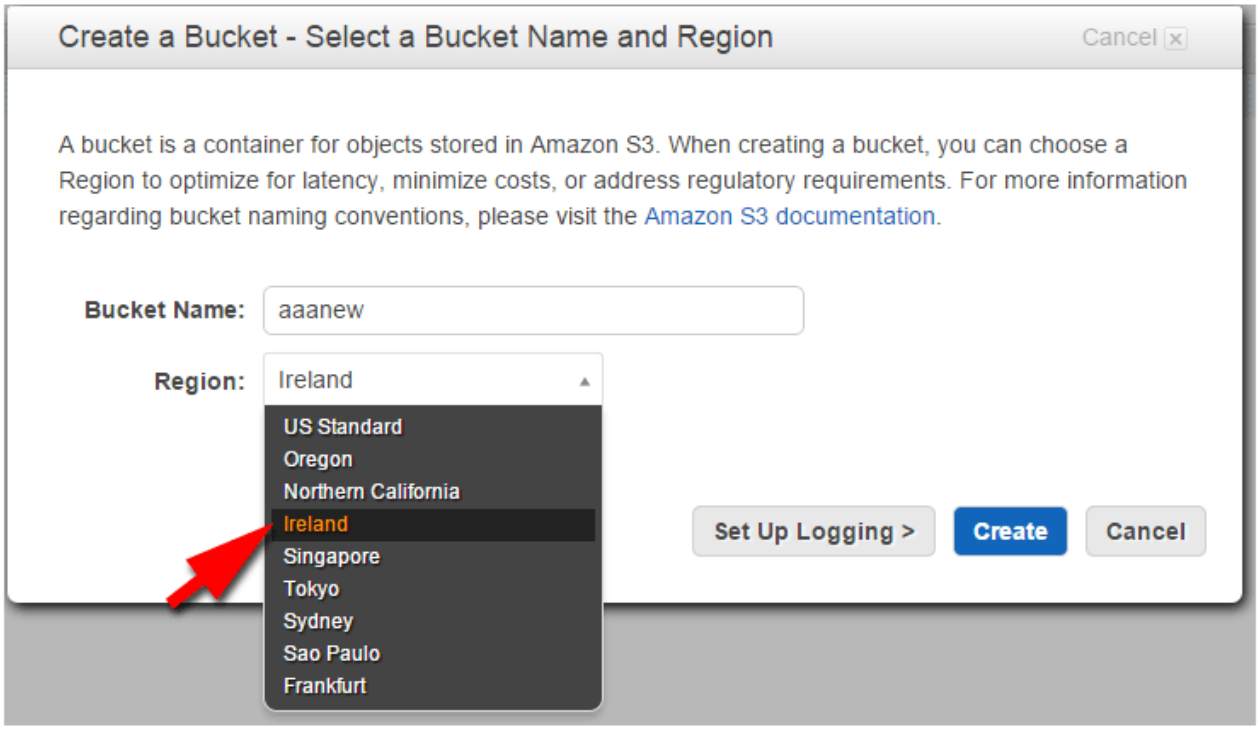
In the next screen, click on **Create Bucket**:



A dialog box pops up and there you type the name of your bucket in the **Bucket Name** field:



This name has to be unique all over the AWS network. Then, you select the region you want to store the bucket:

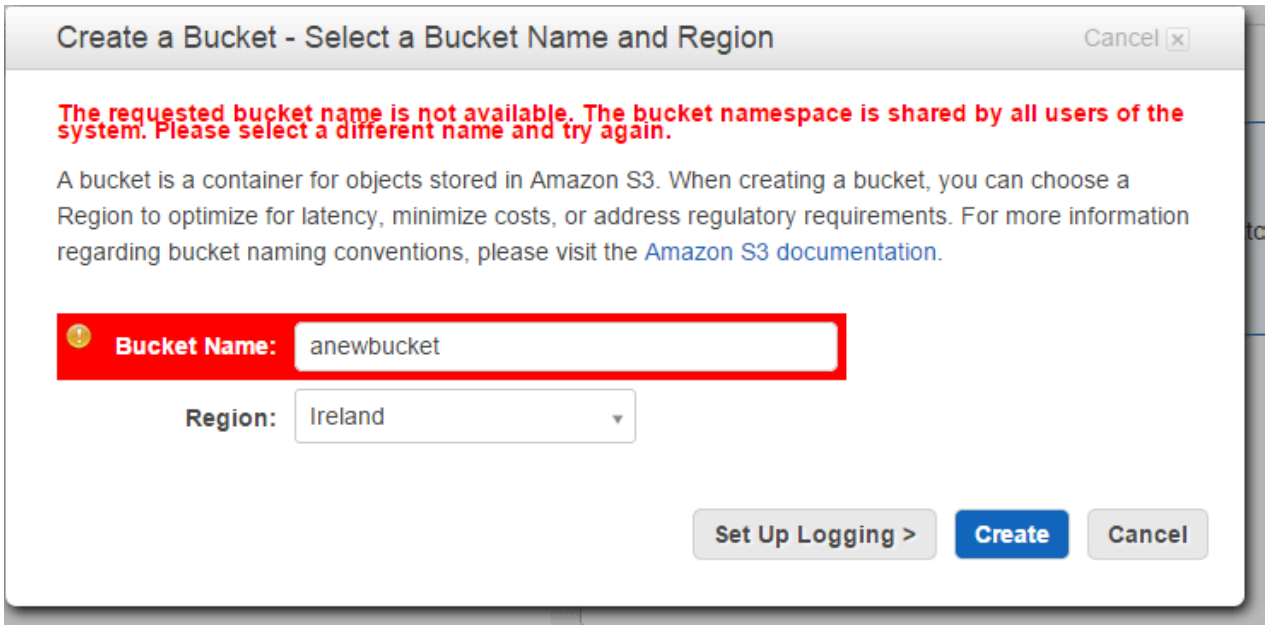


For instance, if you live in Europe, or your audience resides primarily in Europe, you may select Ireland. When you plan only to work with Download distributions, the region does not really matter for the audience, since those files are served from a server closest to your audience. But for you, to upload media to the bucket, this makes a difference in speed, so best chose a location closest to you.

When you have done that, you may setup logging to track your files, but you can always do that later. It is best to create a separate bucket for logging because it creates many files and it would become difficult to scroll through the list finding your media.

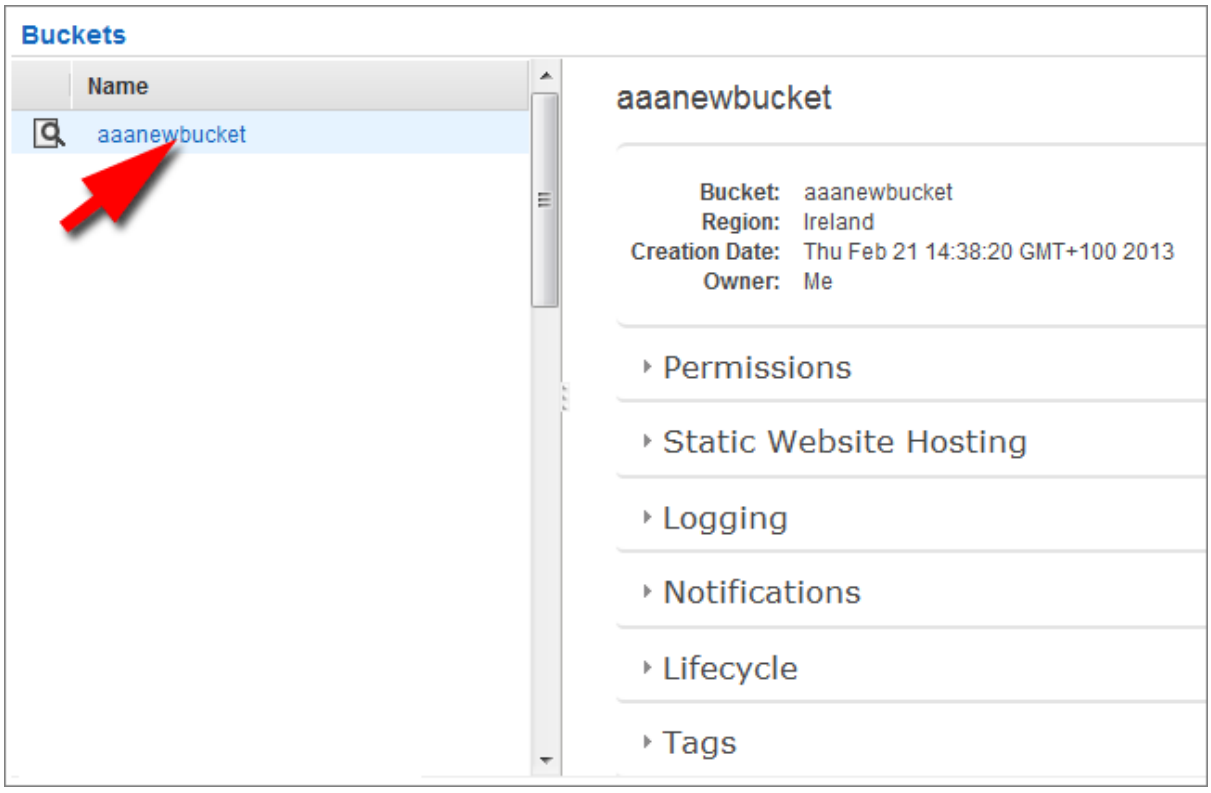
Click on the **Create** button.

If you get an error message like this:



It means the bucket exists already. Simply choose another name. As time goes by, you may find that many names have already been taken. Some marketing gurus find the name important for promotional reasons, but to be honest, it does not really matter that much since this name is seldom shown on the frontend of your site. Besides, if you find the name important, it is possible to use a CNAME for a bucket or distribution, consisting of a domain name, but this is quite advanced and we will not discuss it here.

Click on the **Create** button. Now you will see your bucket listed on the left with its properties on the right:



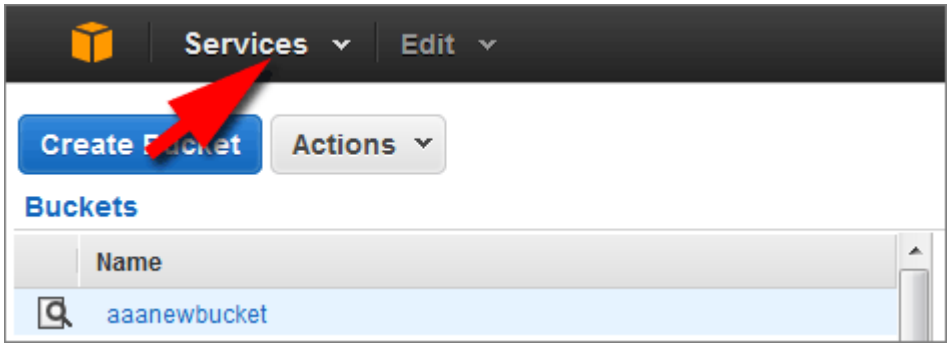
Default, the bucket is generated with the permissions (ACL settings) set to **private**, so you do not need to change this, we are done here.

In the next section, we are going to setup the **CloudFront Web distribution** for your bucket. You may disregard that section if you only plan to work with an audience in your country. In this case, skip to the **Uploading files** section.

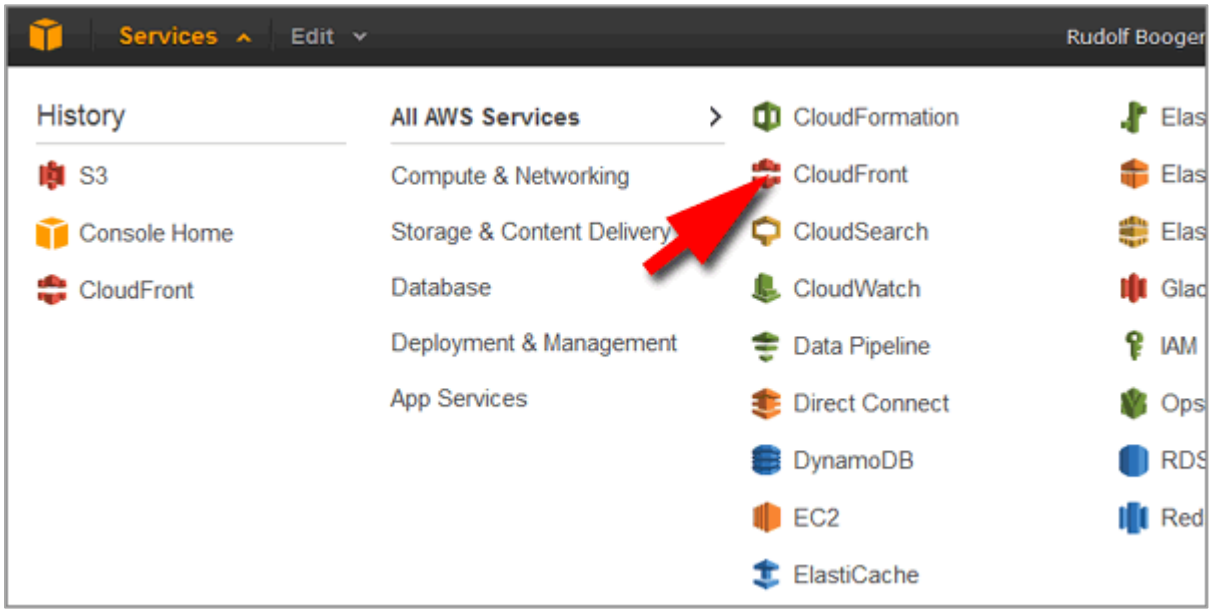
However, if you expect to get an international audience, CloudFront is the way to go because this service works with the edge servers all over the globe, therefore your audience gets your files from the server closest to his/her area.

Create a Private Web Distribution with CloudFront

Click on Services in the top left to leave the S3 console and select CloudFront:

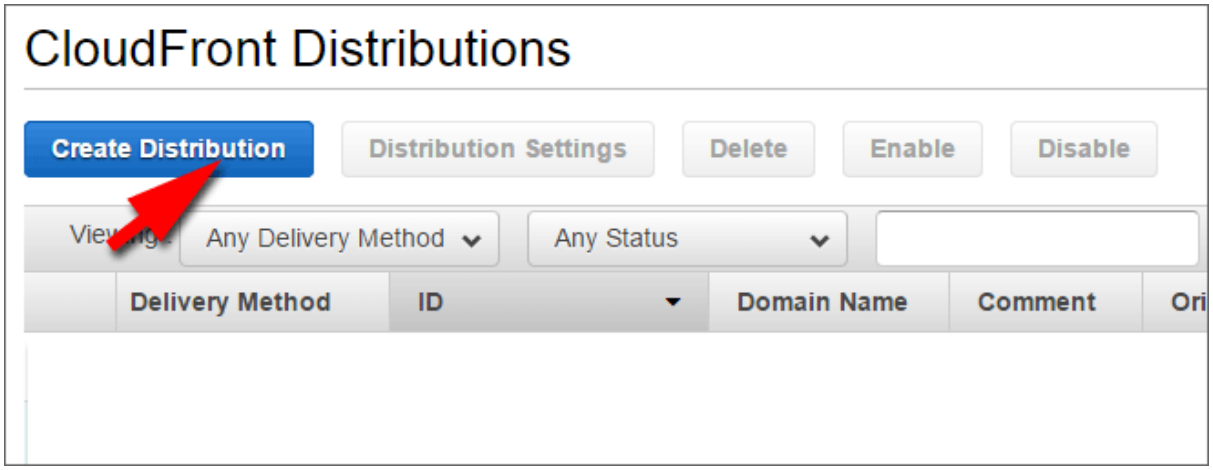


As soon as you click this link, all services are shown. Locate **CloudFront** and click on it:

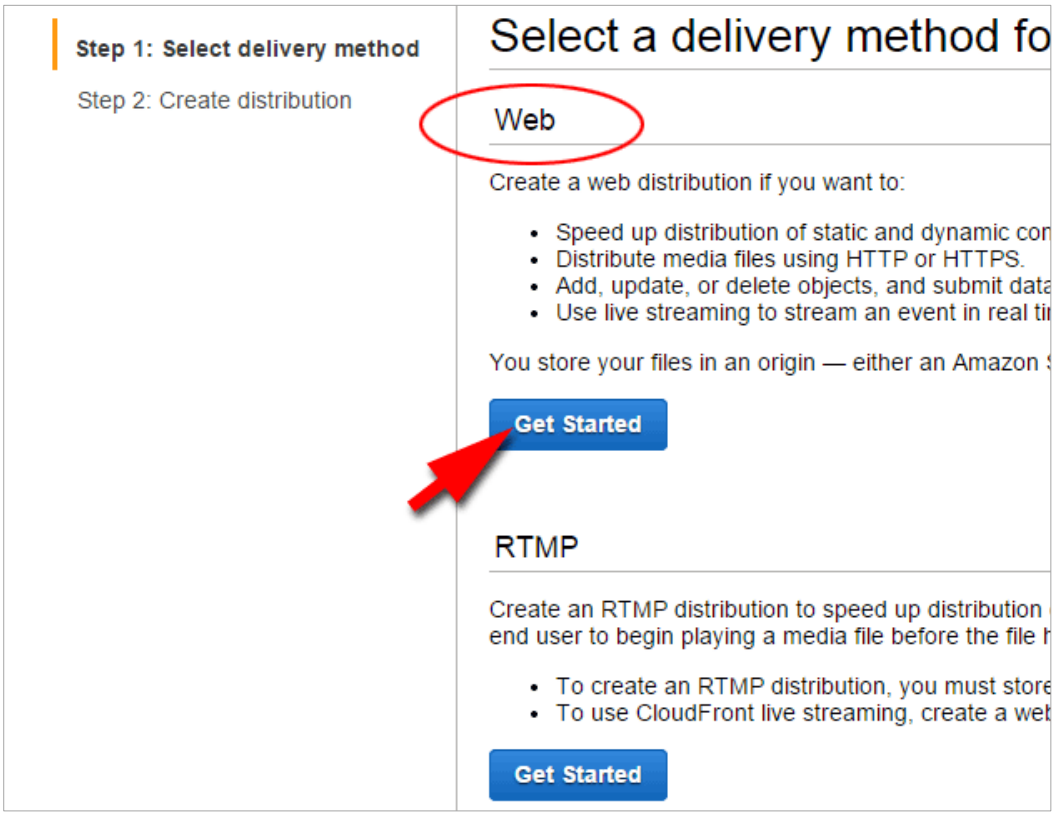


The next time you can select **S3** and **CloudFront** in the History list on the left. But the first time, it shows only **Console Home**. In your case it may show **S3** as well.
After selection the CloudFront console opens. You also directly access it via this link:
https://console.aws.amazon.com/cloudfront/home/

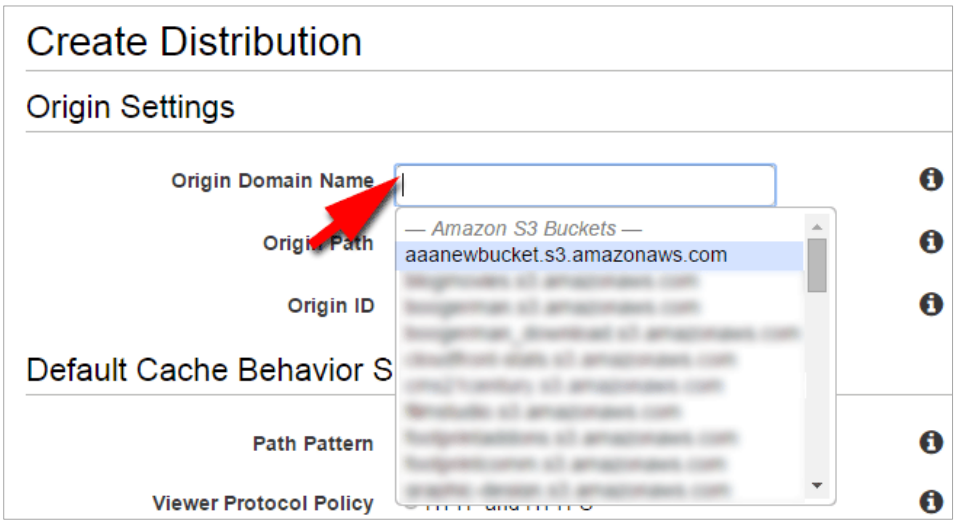
When you are in the CloudFront Console, you see on the left a Help panel, on the right a list of existing distributions, if any. To create a distribution, click on the **Create Distribution** button:



The next screen shows the options. Default, a **Web** Distribution is selected; this is what we need here. There are also **RTMP** (Streaming) distributions but that is meant to stream video and audio. S3Media LinkSafe does not support this feature, but S3Media Stream™ does.
Make sure you select a **Web** distribution (formerly called *download* distribution):

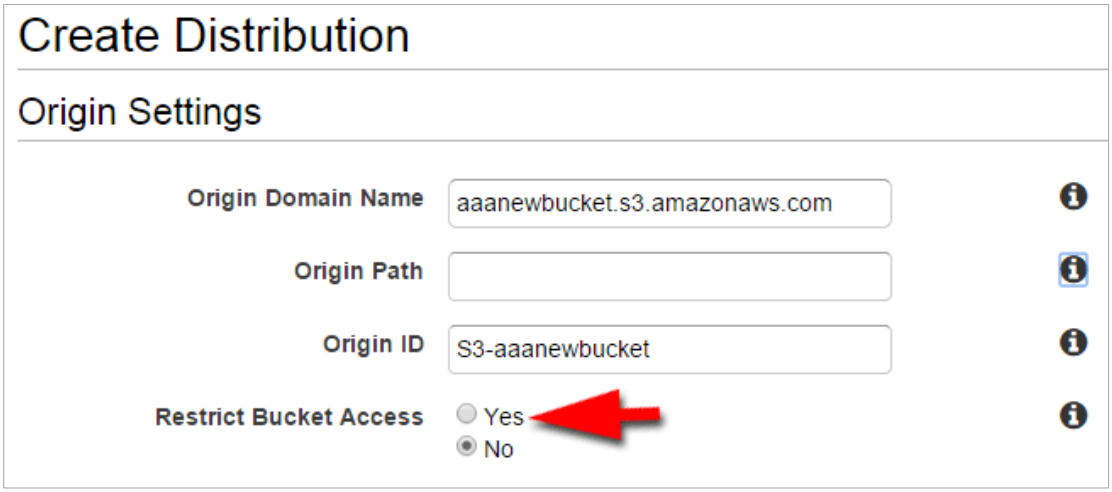


Then click the **Get Started** button. In the next screen, you see a range of settings. First, we need to select the bucket we use this download distribution on. When you click in the **Origin Domain** field, it changes to a dropdown list with all the buckets in your S3 account:

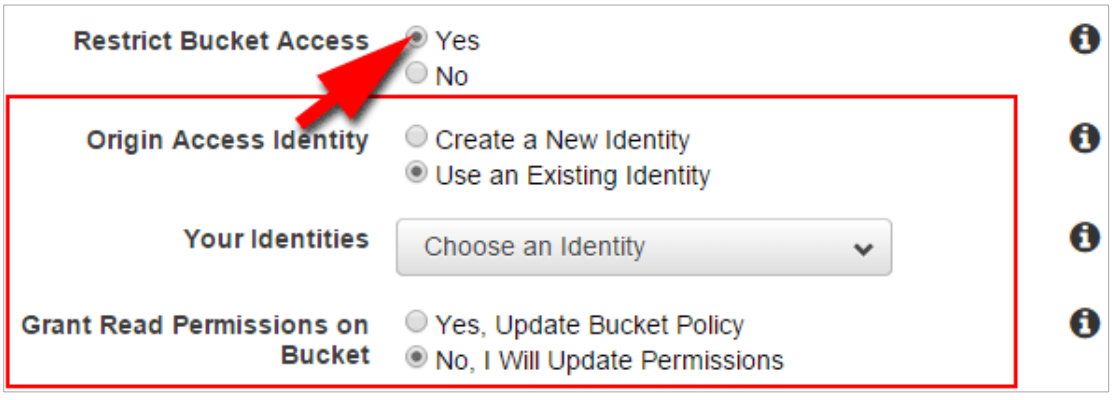


Select the name of your bucket from that list. Notice that the interface changes and shows more options.

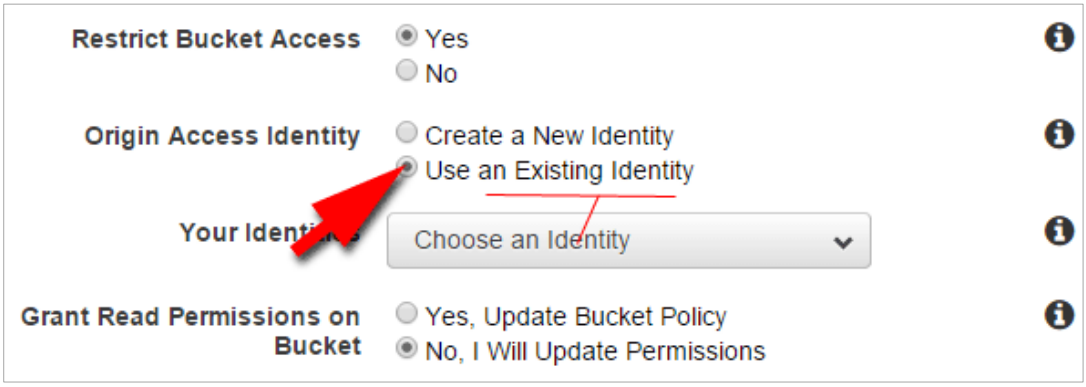
Origin Path restricts the distribution to a directory (formerly called *folder*). You can leave this empty.
Origin ID is already filled in, generally you do not need this.
Now we move down to **Restrict Bucket Access**:



Default, it is set to **No**, which means create a public download distribution, but we don't want that since we want to keep our files private to protect them from theft or unauthorized sharing.
Select **Yes.** As soon as you do that, a new list of options appear directly underneath:

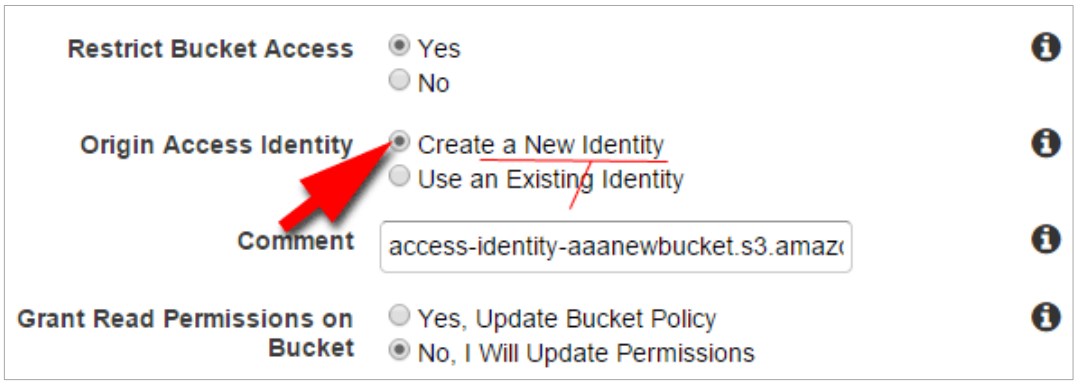


For the **Origin Access Identity**, which we need for private downloads to be able to serve them; you can either select an existing identity or create a new one. Default it is set to **Use Existing Identity**. If you have already one, select it from the dropdown list called **Your Identities**, just below the radio buttons:

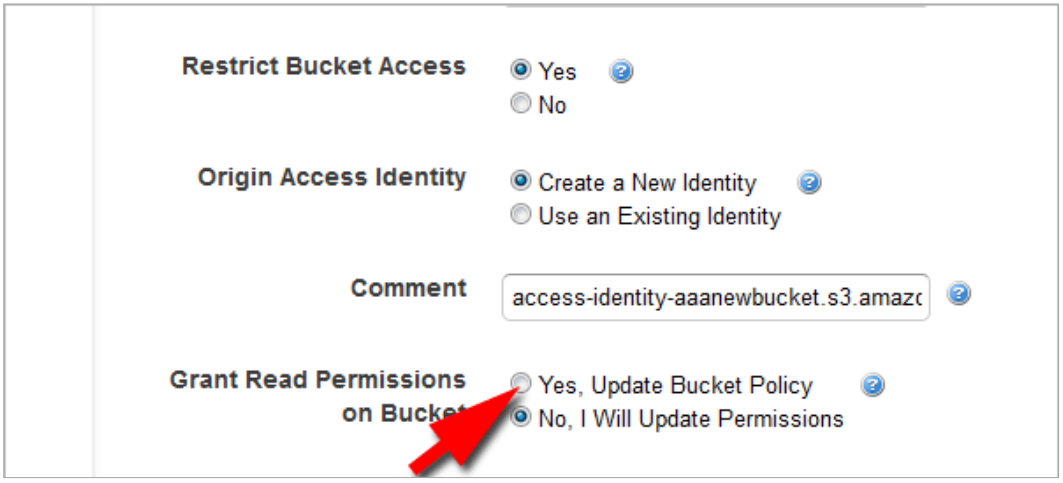


To keep it easy to maintain, you best use the same identity for all your distributions.
If this is the first time, select **Create a New Identity**.

The dropdown list for **Choose an Identity** is now replaced by a **Comment** box. In this box, you can write a comment about this identity or you can leave it as is:

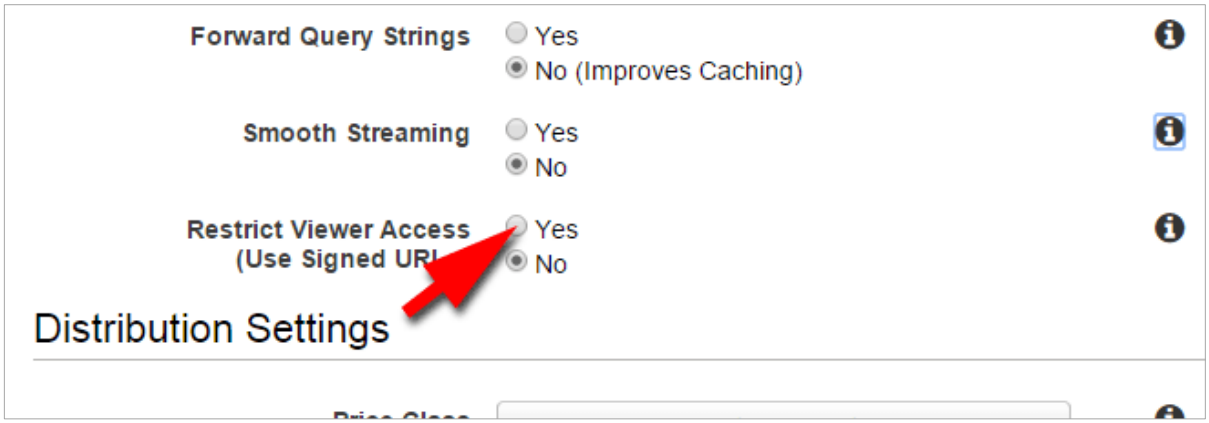


Moving down, we have to set **Grant Read Permissions on Bucket**. Default this is set to **No, I will Update Permissions**, but it is better to select **Yes, Update Bucket Policy**, because this ensures that all items you upload to the bucket will inherit the permissions you set in this panel automatically:

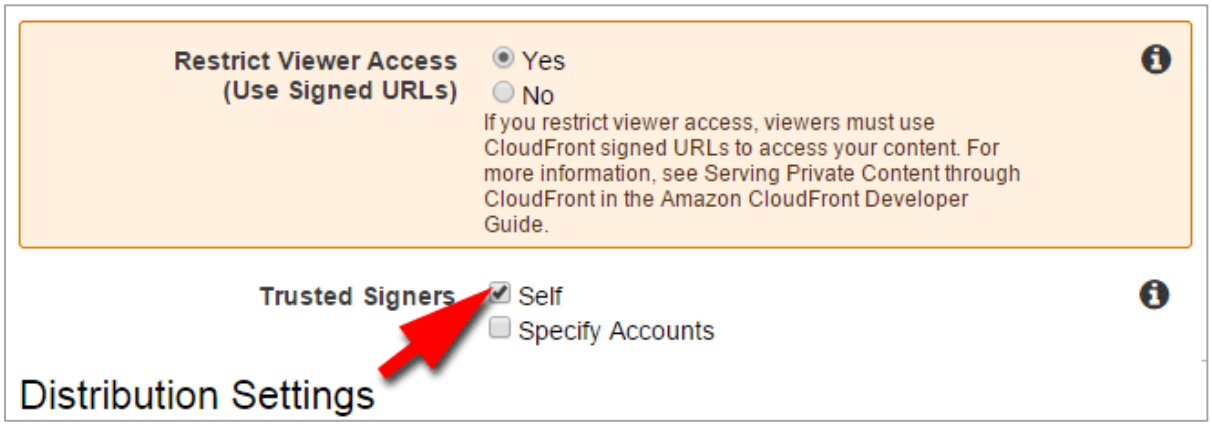


Even if there was no bucket policy for your bucket yet, it will be created by this action. The bucket policy will be a real time saver for you. In the past, you either had to write a bucket policy yourself, or to add **the CloudFront Access Identity** manually per item which is very time consuming.

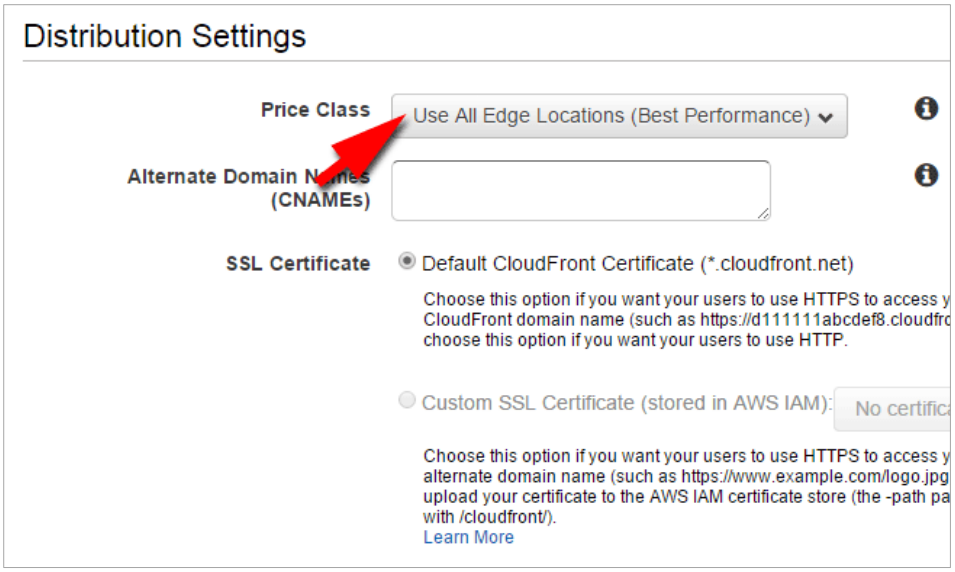
Now, scroll down to **Default cache behavior** settings.
The only important setting in there is **Restrict Viewer Access (Use Signed URLs)**. You can leave the rest in between as is. Select **Yes**. This means that viewer cannot access your content without using a signed URL, also called an *Expiring URL* (in other words: a time limited link to your media):



As soon as you select **Yes**, two more options show up under the radio buttons. Make sure that for **Trusted Signers**, you select **Self** (this is you):



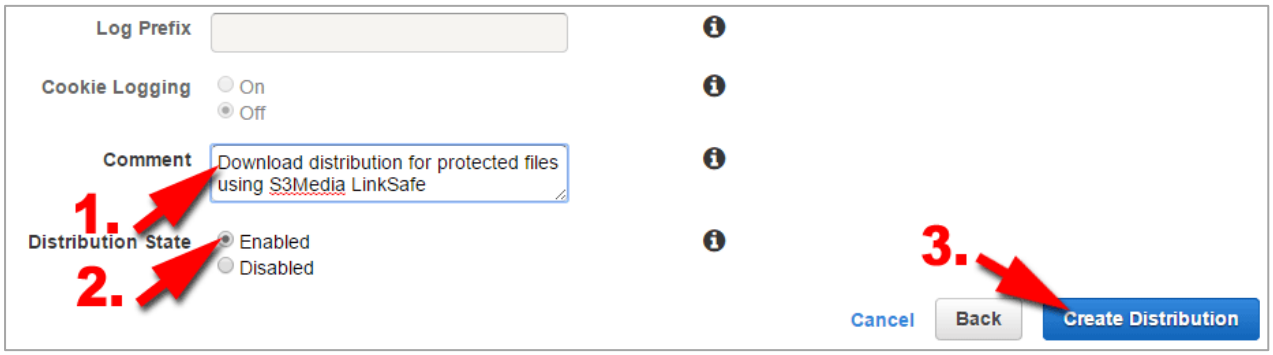
Then, when we move down, you see a **Price Class** dropdown list for your Web distribution:



Here you can limit the locations your distribution is available to. When your site is meant for a worldwide audience, you may want to set it to **Use All Edge Locations**. Otherwise, you may restrict it to the areas related to your target audience. The price difference lies in the amount of Edge locations used. For instance, if you limit this to **US and Europe**, visitors from Asia or Australia won't be able to view/download your content. This will reduce the costs because the content will not be copied to Edge servers outside US and Europe. However, generally **Use All Edge Locations** gives best performance and the pricing difference is minor. Various customers of S3Media Stream™ reported problems with restricted distributions.

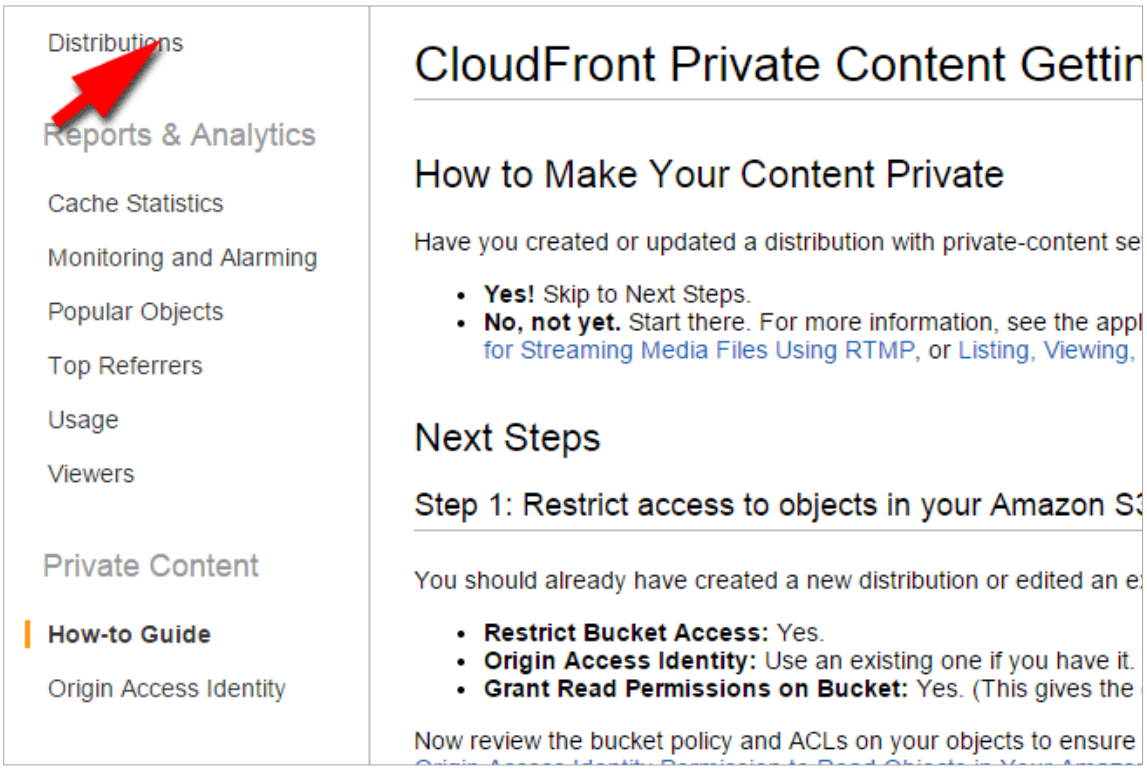
SSL Certificate can be left alone, unless you know what you are doing. It is not covered in this tutorial.

When you selected the right option for your situation, scroll down to the bottom. There you see a range of options related to logging and CNAMES, but for now we leave that alone.
You want to fill in the comment (1.) box as a reminder for the purpose of this download distribution, like this:

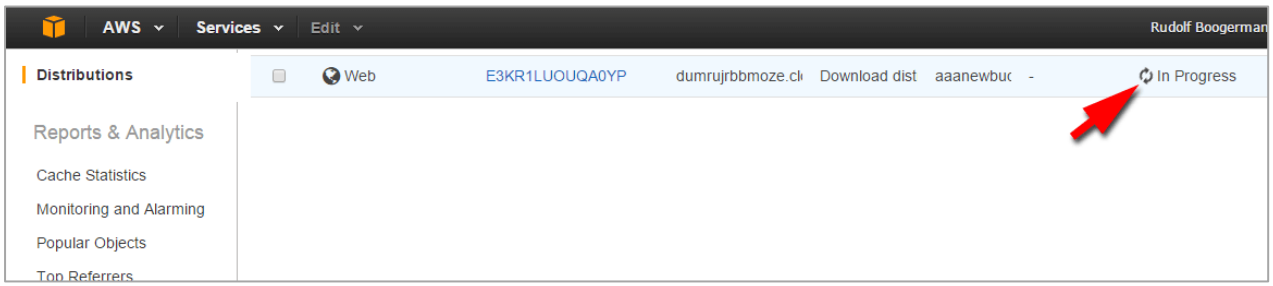


Then, make sure **Distribution State** is enabled (2)Then click the **Create distribution** button(3).

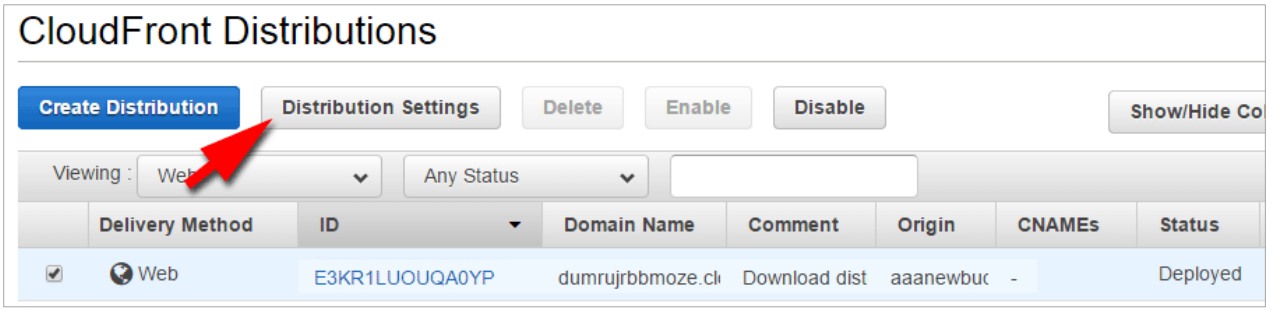
In the next screen, you are redirected to the **How to Guide** for further fine tuning, but in principle, you do not need this and the documentation can be somewhat confusing. Feel free to explore it, but to check whether what you did was correct, you best click on the link **Distributions**, in the left hand pane:



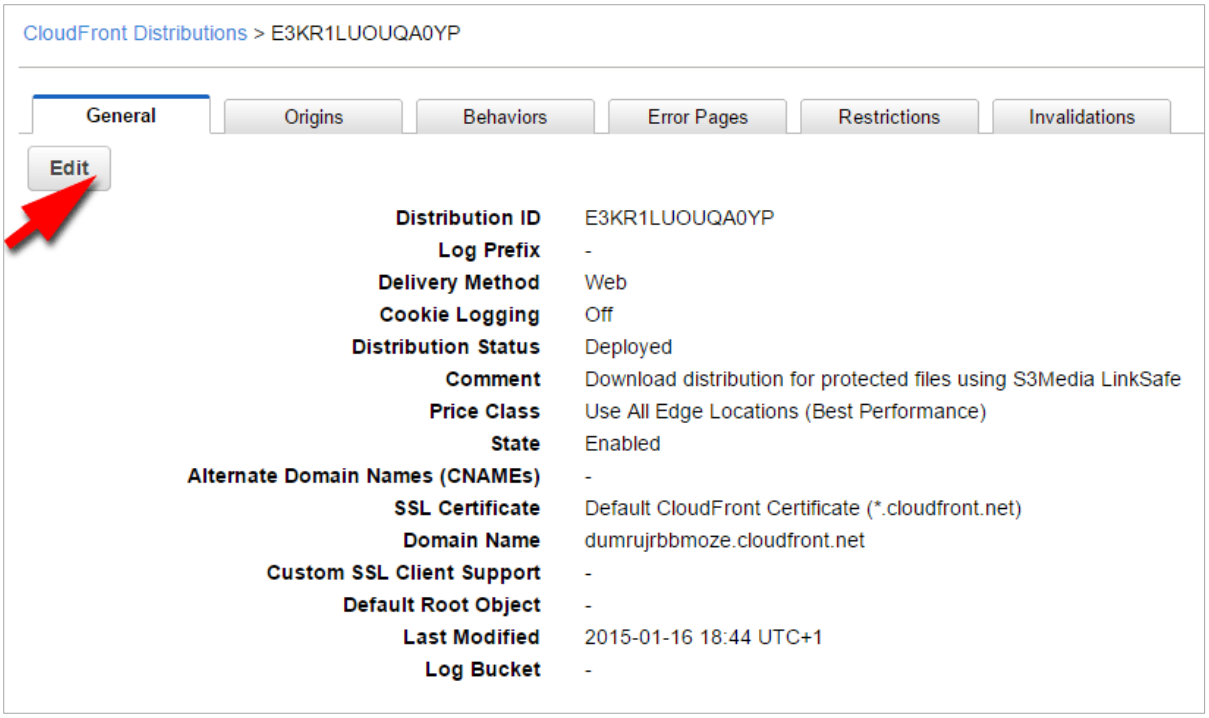
In the next screen you get a list of your distributions:



Since you just created the web distribution, the Status will be **In Progress**. This means the distribution cannot be used yet. This **Status** updates automatically and it takes about 15-20 minutes. When it says **Deployed**, you can review your settings by selecting the distribution using the checkbox next to the distribution:



Then, click the **Distribution Settings** button.
If it looks more or less like this, everything is in order, otherwise click Edit to change update the settings:



You can also use this section to set the **CloudFront Access Identity** for other existing **Web Distributions** which do not have a **CloudFront Access Identity** assigned or are not set to private yet.
It follows the same process as described in the **Web Distribution Settings** higher up in this tutorial.

So, later on, you can go directly to https://console.aws.amazon.com/cloudfront/home and select the checkbox next to the distribution you are interested to access the **Distribution Settings** Panel.

Resume of what we did and what it means

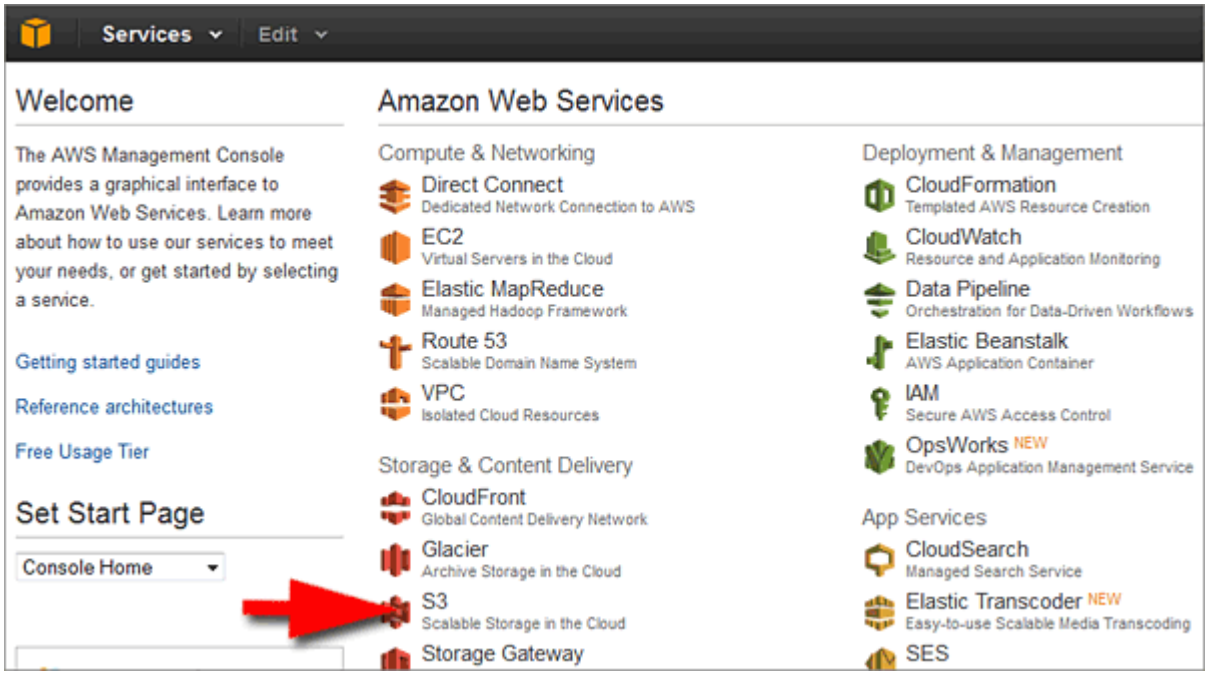
1. We created a **Bucket**
2. added a private **Web Distribution** (formerly called **Download distribution**)on that selected bucket.
3. we created or selected a **CloudFront Origin Access Identity** and assigned it to the **web distribution.**

1. Needs no explanation, you can't serve content without a bucket.

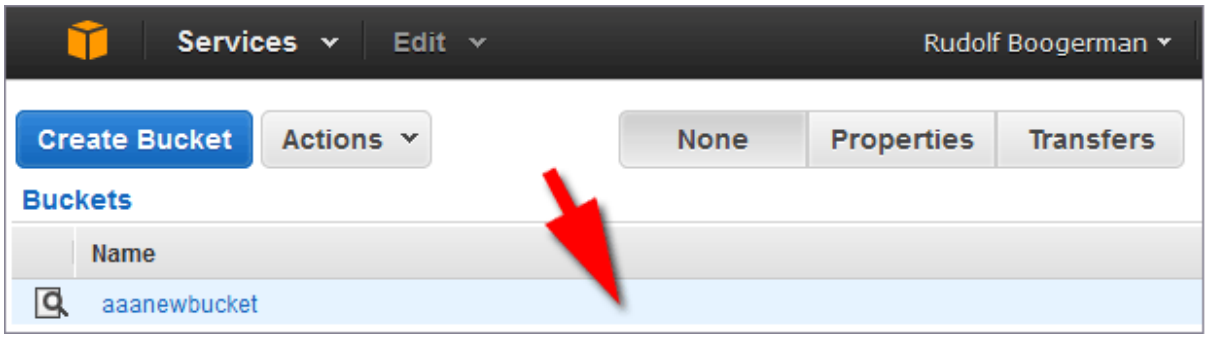
2. This is quite simple as well; we created the opportunity to download files via the Edge servers of CloudFront, enabling faster download for international visitors.

3. Needs a bit of explanation. With regular S3 buckets or public web distributions, you have four ACL settings. But with private distributions (including streaming distributions), you need a fifth one, telling AWS that it is allowed to serve private content via the **Trusted Signer**, which is you.
So, we created that fifth element via the option **Create New Origin Access Identity** in the **Create Distribution** process, and by selecting the **Yes, Update bucket policy** options in that process, we created a bucket policy with the correct permissions.

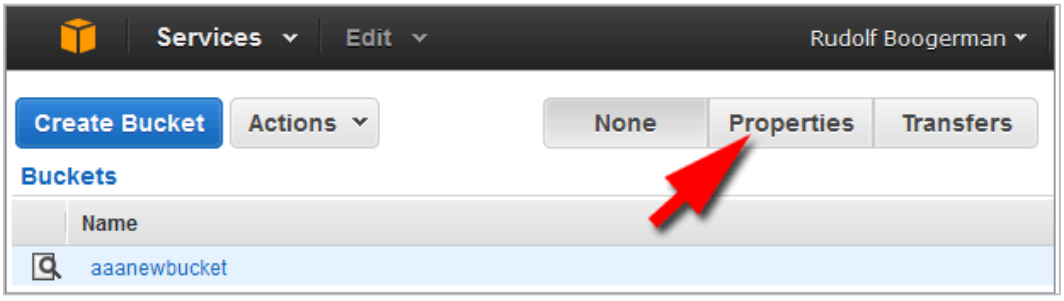
However, you need to check if that bucket policy is indeed created before you upload files.
Go to **Services** again at the top left menu bar and select **S3**:



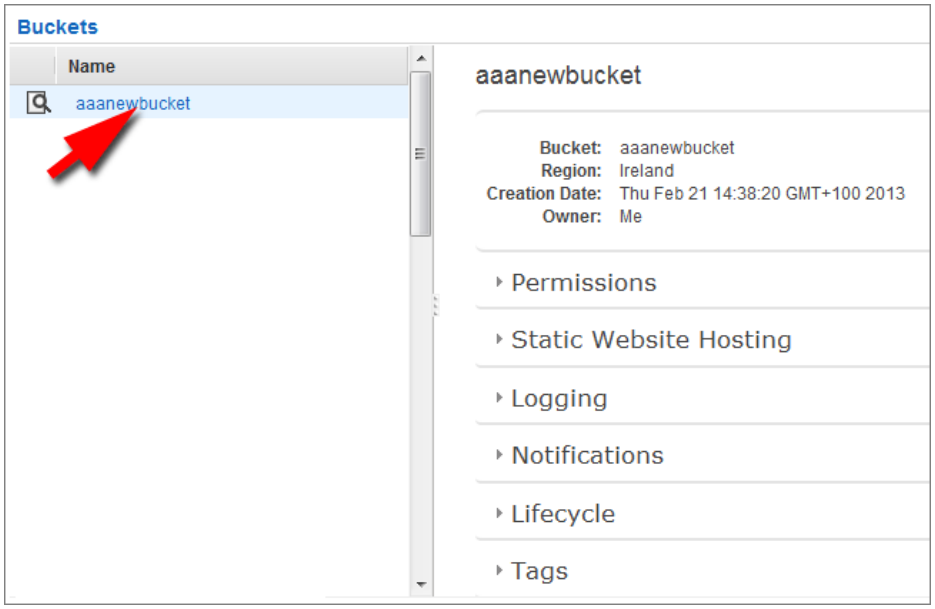
Once in the **S3** panel, select your bucket in the list. There are two ways to click on a bucket, either the text link or the light blue bar itself. If you click on the link, it will show the list of contents in your bucket. However, since there is no content yet, this makes no sense. Instead, we only have to select the bucket, therefore we just click on the blue bar when we hover over the bucket list area, like this:



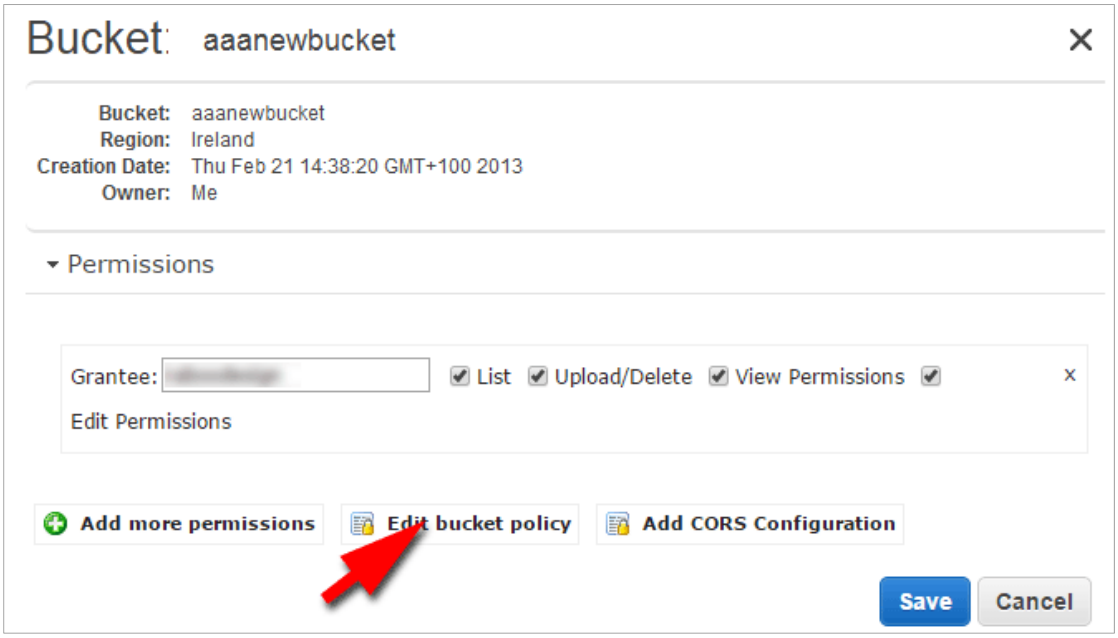
With the bucket selected, we click on the **Properties** button at the top right:



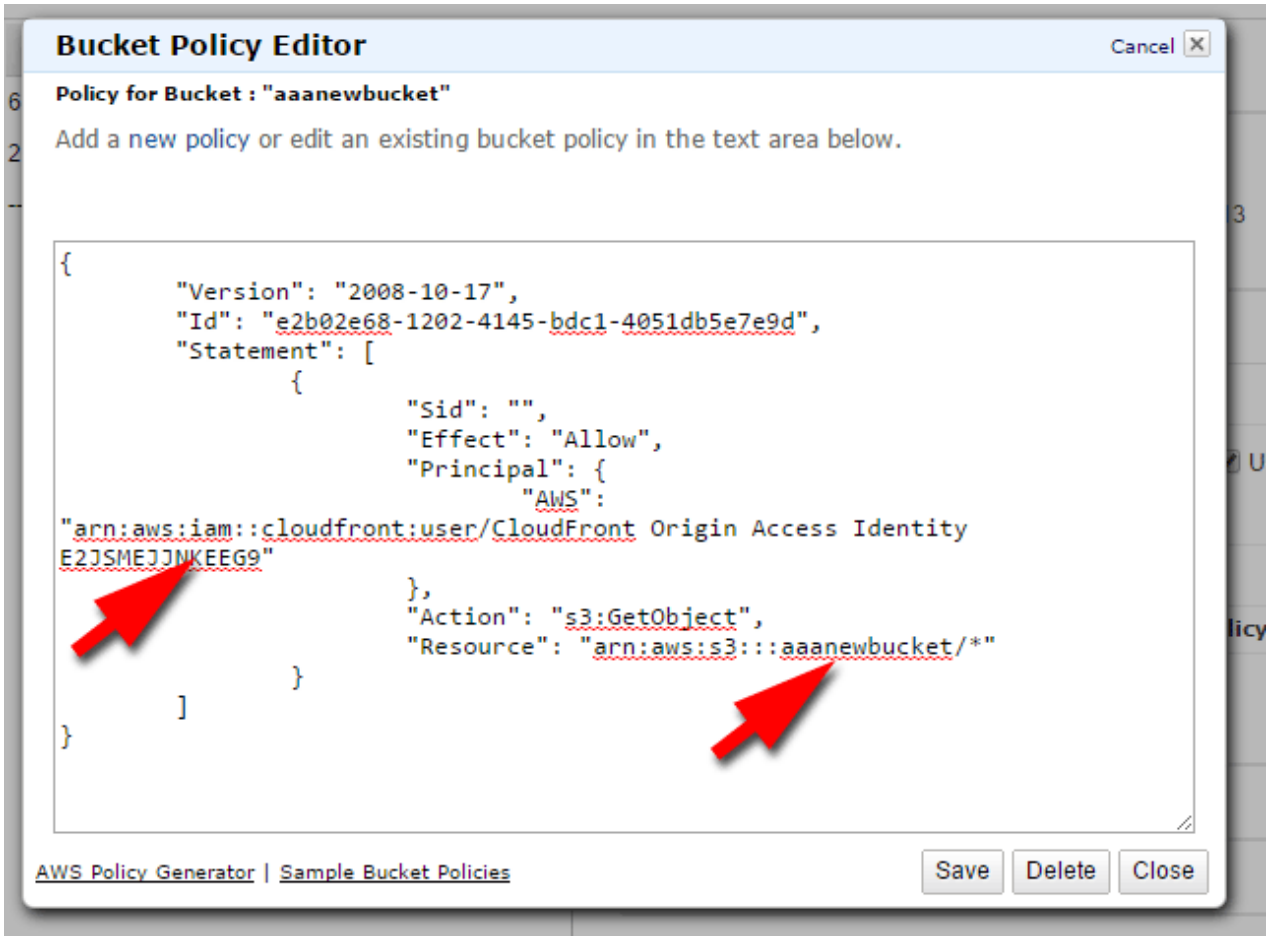
This brings up the properties panel with various options. We are primarily interested in the **Permissions**:



When you click on **Permissions**, an accordion flap out will open showing you the permissions settings:



If you see an option below like **Edit bucket policy**, it means the update bucket function succeeded to create the bucket policy. Click on that option to view the result:



If it looks more or less like this, you are good to go. Note the **CloudFront Origin Access Identity** and the **bucket name** in the bucket policy. This policy makes sure that all files you upload will be accessible via expiring links.
At the same time, they remain inaccessible via other methods.

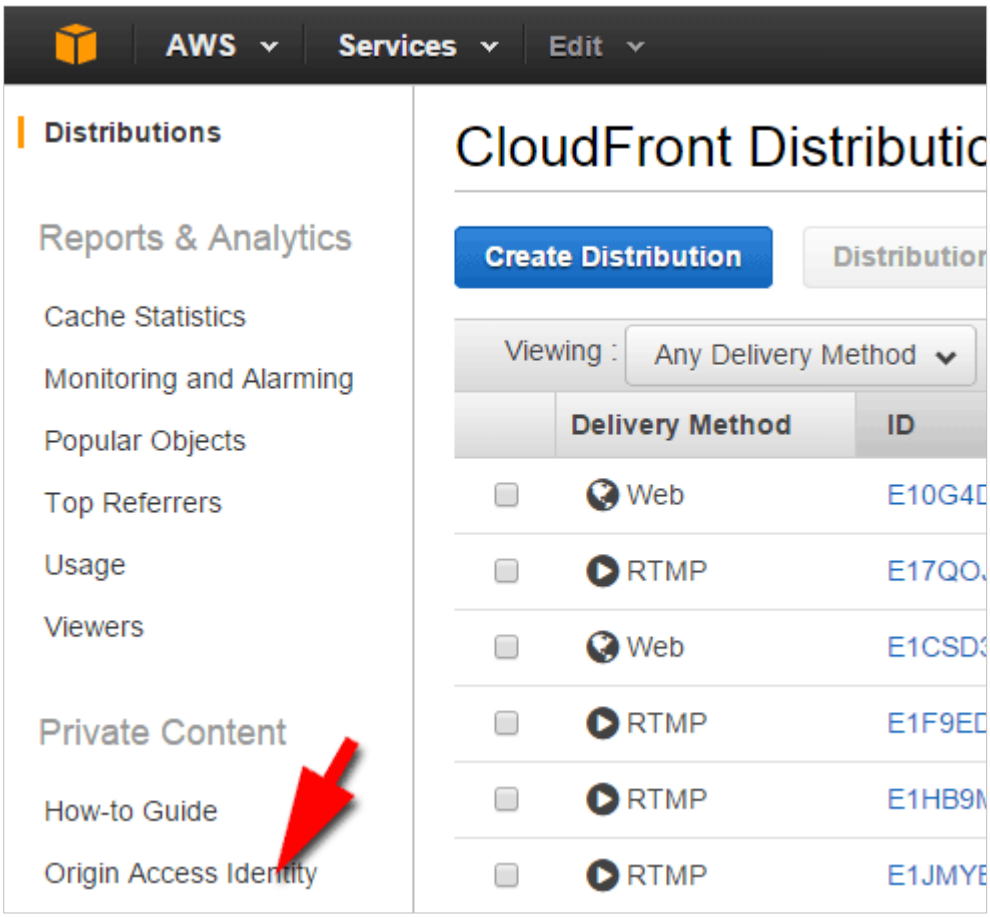
If, for some unknown reason, there is no bucket policy, you need to create it yourself.
In the bucket properties, click on the link **Add bucket policy** at the bottom.

In the policy editor copy and paste the template below:

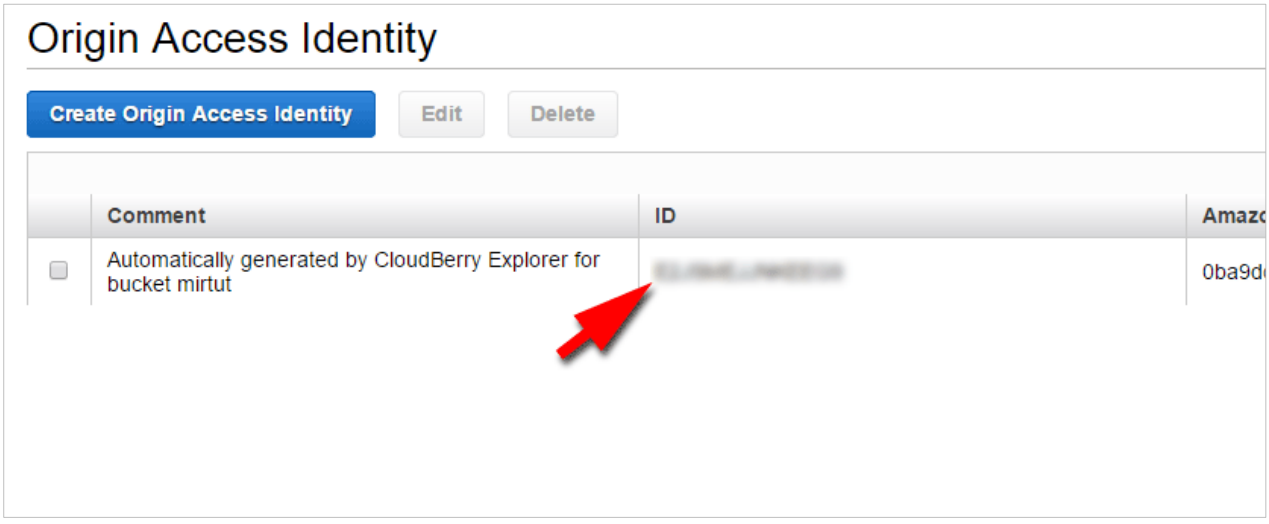
```
{
        "Version": "2008-10-17",
        "Id": "e2b02e68-1202-4145-bdc1-4051db5e7e9d",
        "Statement": [

              {
        "Sid": "",
        "Effect": "Allow",
        "Principal": {
             "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity E2JSMEJJNKEEG9"
              },
         "Action": "s3:GetObject",
         "Resource": "arn:aws:s3:::aaanewbucket/*"}]}
```

And change the red parts into your own, then paste it in the policy editor. You can find the CloudFront **Origin Access Identities** on the left hand pane in the CloudFront service (open this is a second tab, so that you can switch between the bucket policy and Origin Access identity list):

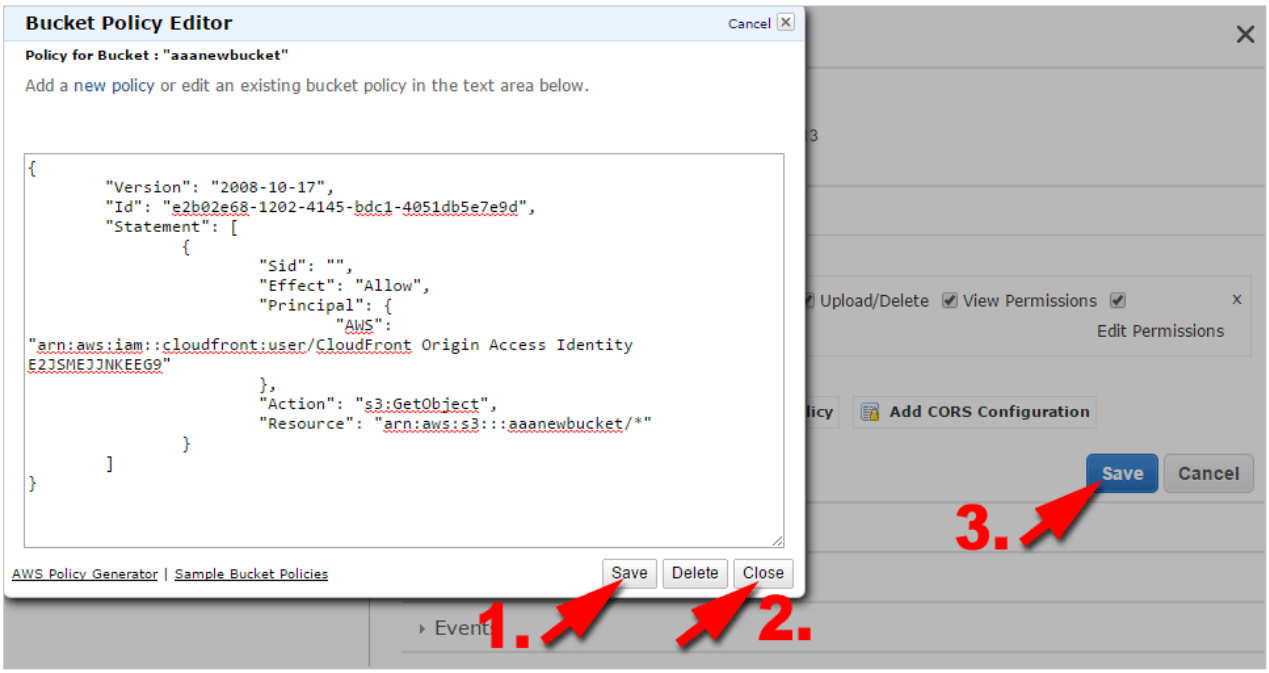


In the list copy the access identity in the column **ID**:



Then paste this ID in the bucket policy and change the bucket name to your own.

Save the policy(1):



Close the window(2) Then, click the blue **Save** button(3).

You are ready to go now.

In the past, you had to create a new Grantee, but this is no longer needed. The bucket policy takes care of everything.

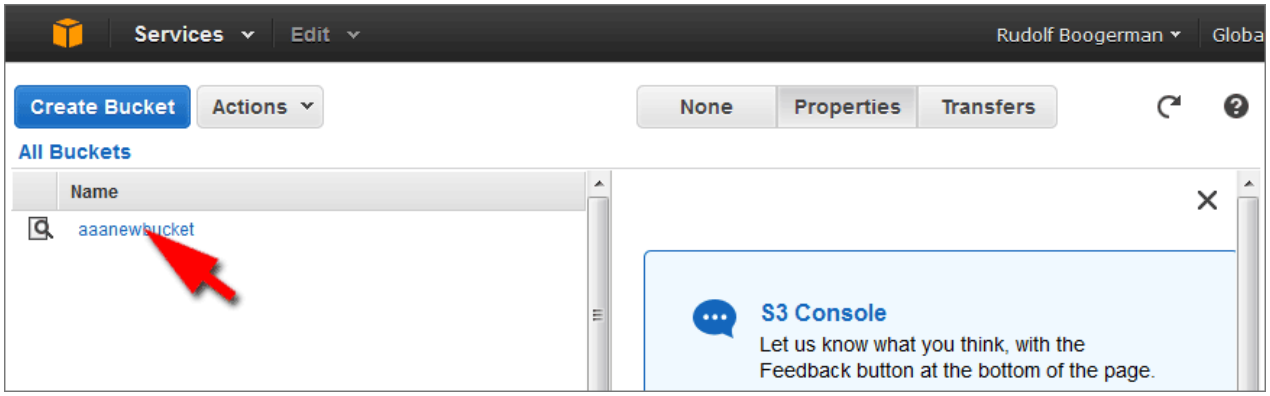
What we basically did was to prepare the bucket to automatically assign the correct permissions for the files you are going to upload. In the past, you had to set this manually for each file in the console, but thanks to the bucket policy, this is automated.

See the next part for uploading files:

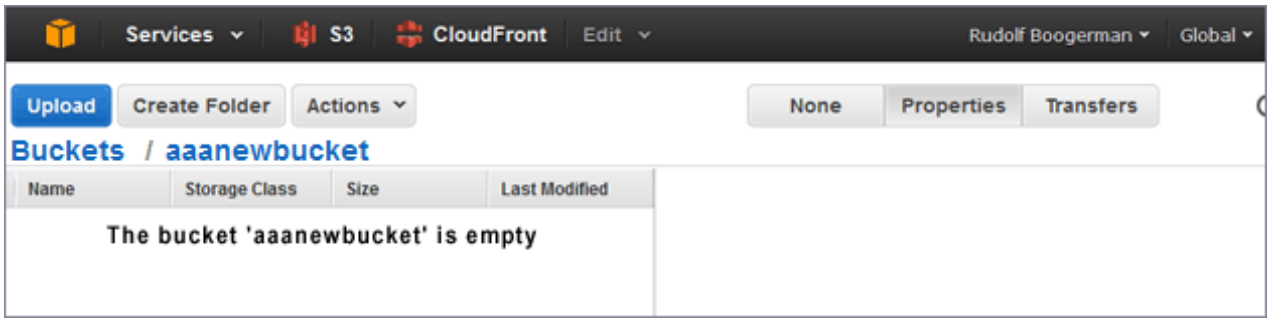
Upload files

Now we are ready to upload files. Whether you work with the bucket itself or with download distributions, all files are uploaded to the bucket itself or in a folder within a bucket.

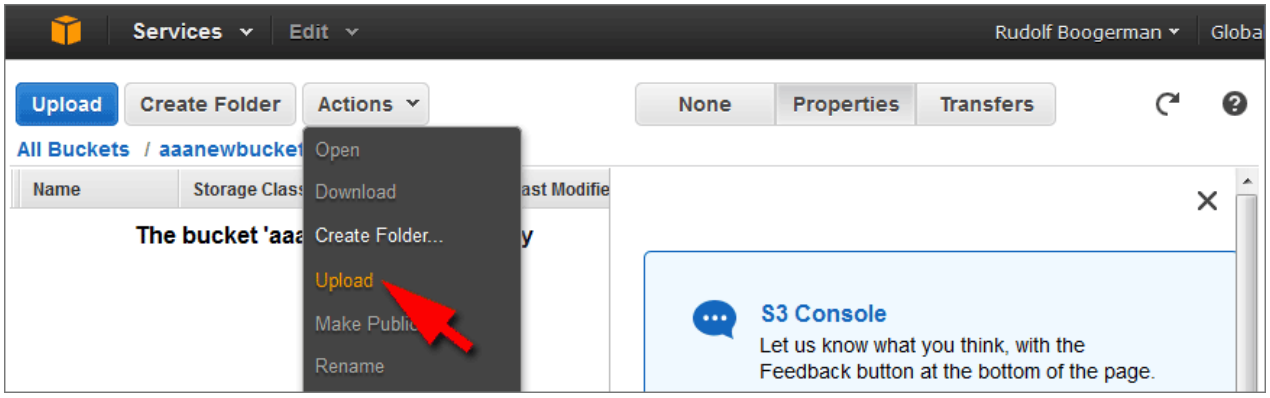
Make sure you are in the **S3** panel and this time click on the link of your bucket:



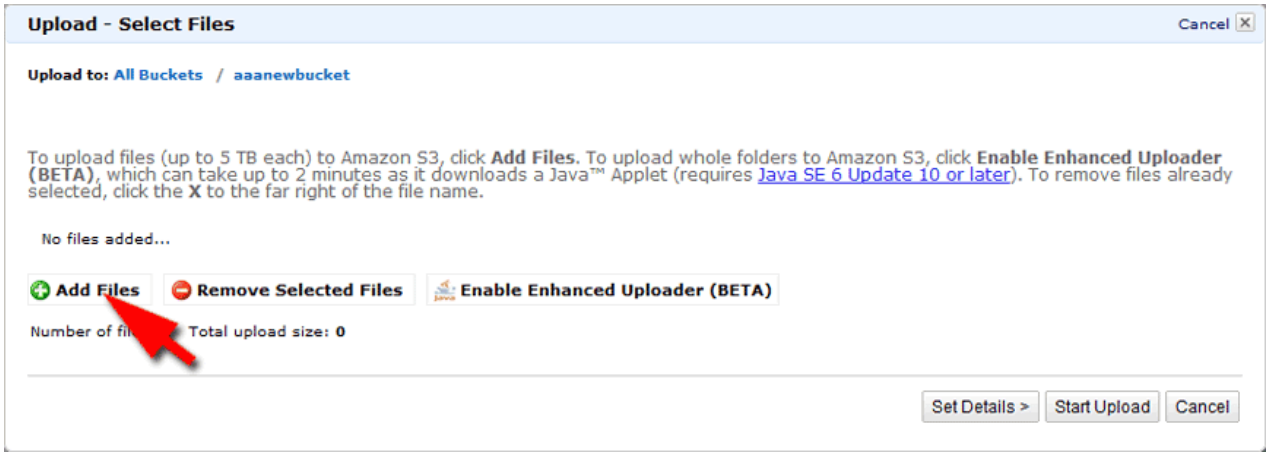
If the bucket is still empty, it will show in the panel:



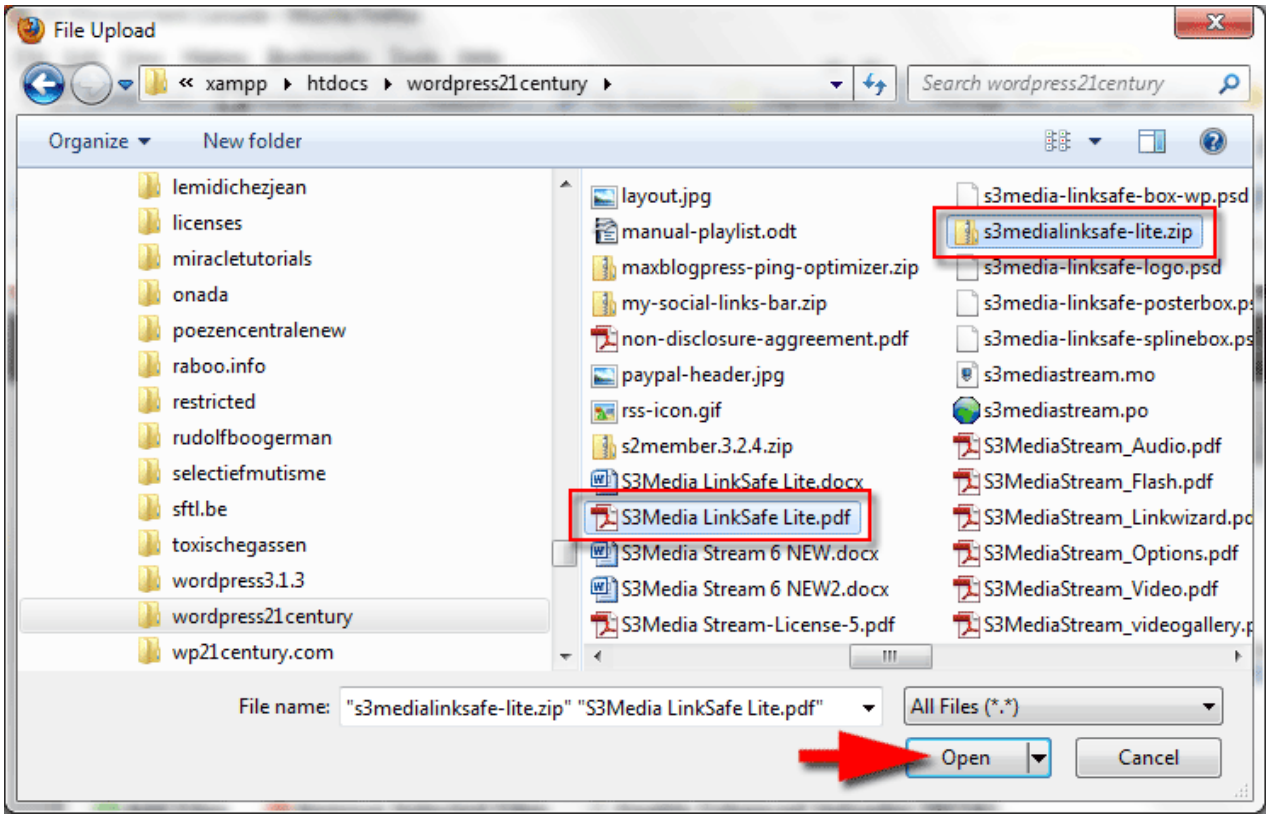
Note that there is a **Create folder** button to add a folder in the bucket, but as said before, weleave that alone. Now, we are going to the button **Actions** and select **Upload Files**:



Or you can click the big blue **Upload** button on the left depending on your preference. A popup window will show up with several options. You can add files, delete files and upload a complete folder. In this tutorial we are going to upload just a couple of files, so click on **Add files**:

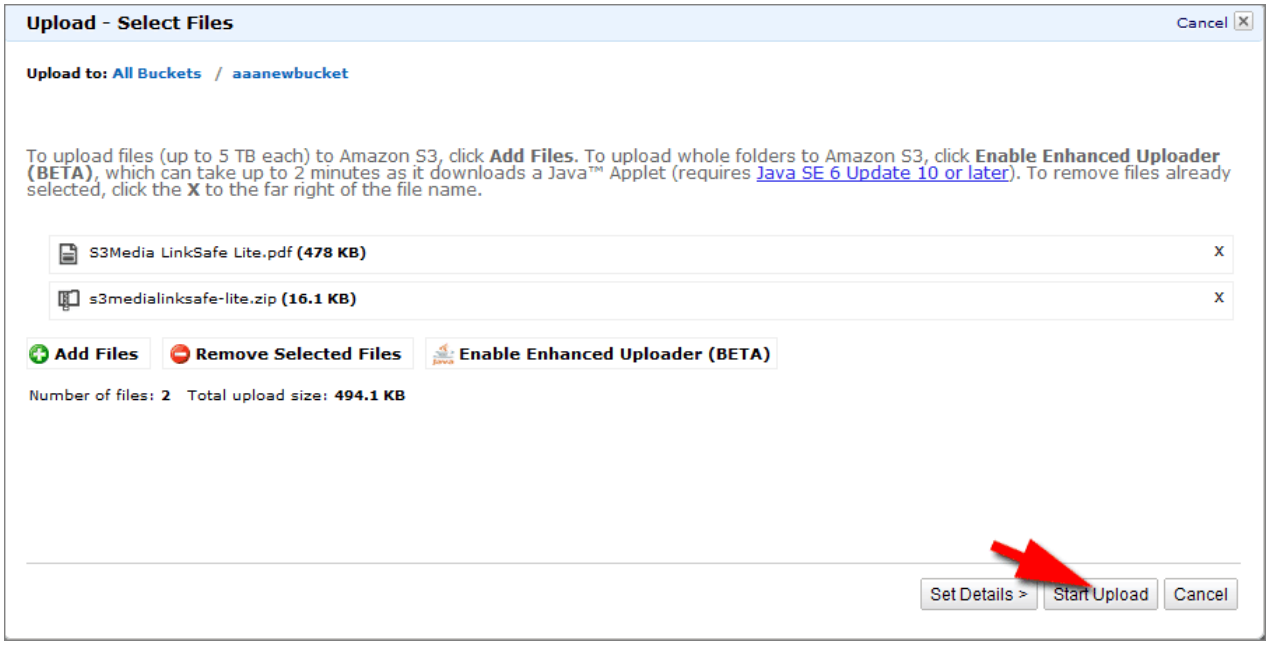


This opens the file browser of your computer. How that looks depends on your operating system, the screenshot below shows it in Windows 7, but they all behave more or less the same:

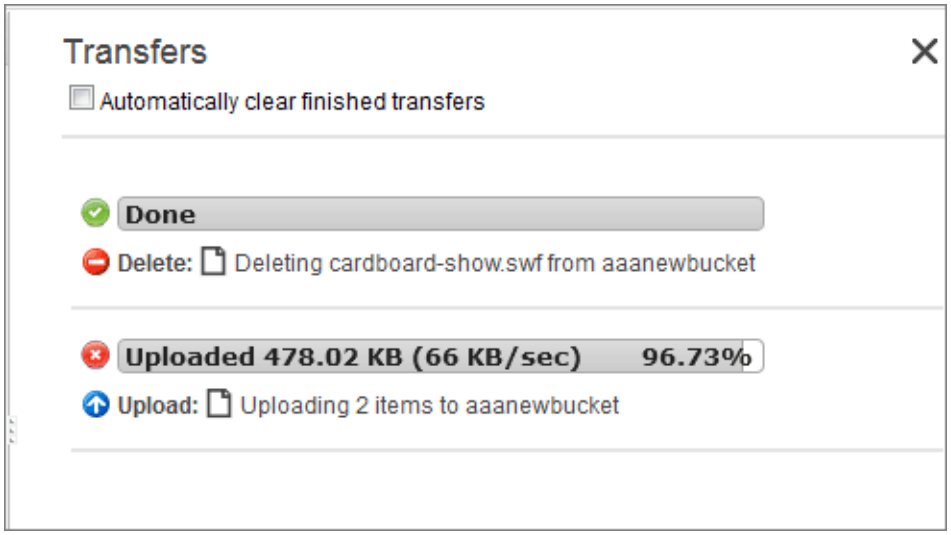


You can select one or more files. When you are done selecting, click **Open**

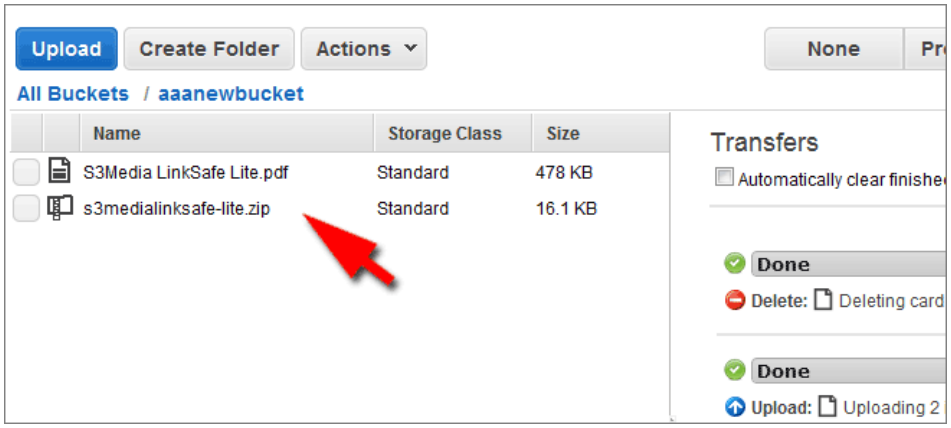
Here we see the selected files:



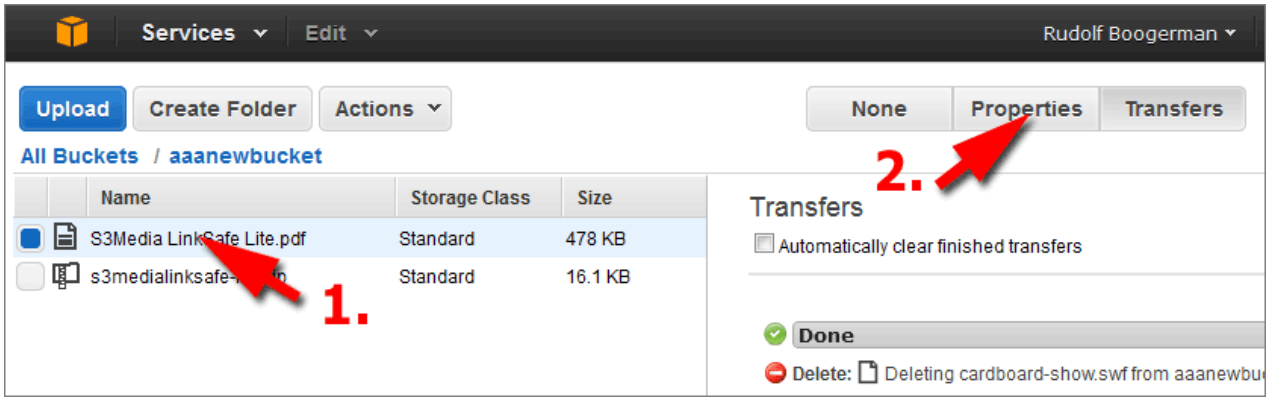
Click the Start **Upload** button to upload the files. In the right hand pane you see the file transfer in action. Depending on the size of your files this can take a while:



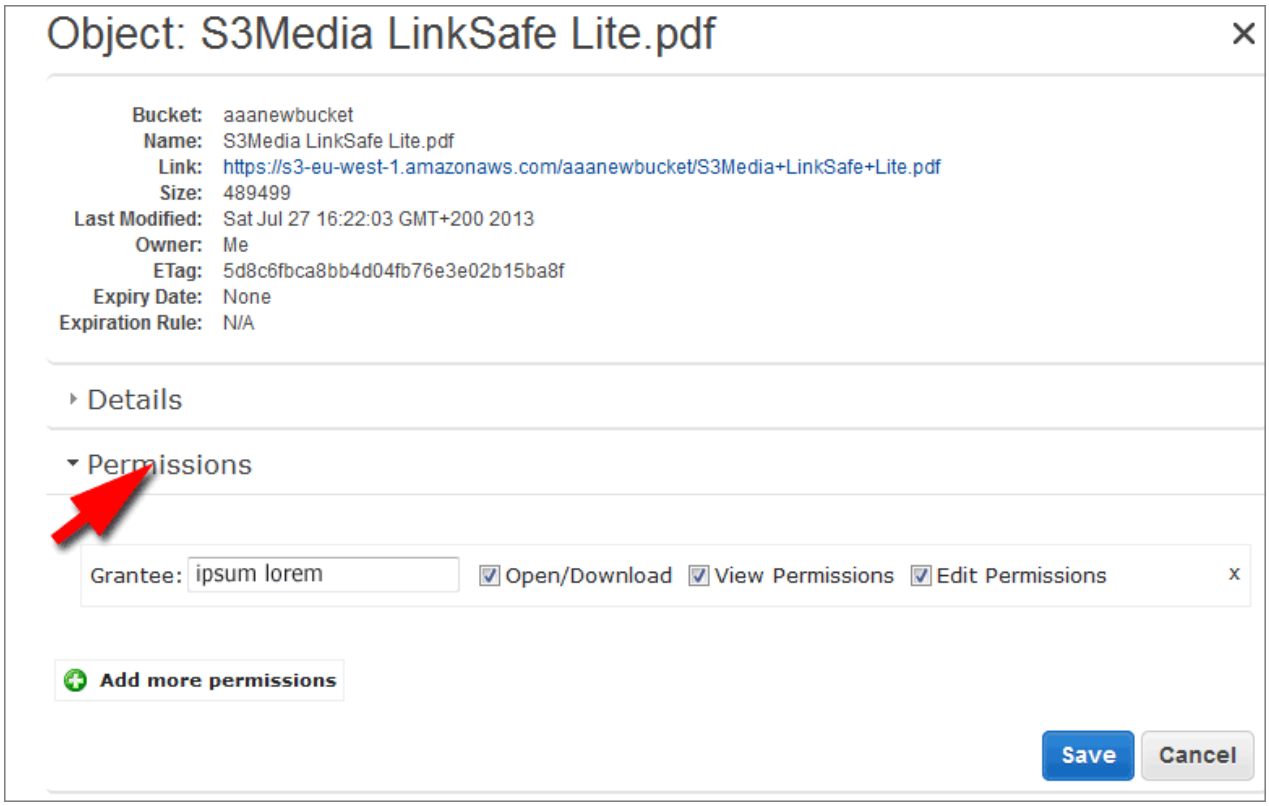
When the upload is finished, your files show up in the left hand pane:



To make sure the permission settings are as they should, let us have a look. Click on one of those files(1). A blue icon appears on the left of the selected file:



Click on the **Properties** button(2) to show the details of the selected file in the right hand pane. Click the **Permissions** link to check those settings:



For those of you who plan to use the bucket itself to serve protected files, this setting is perfect. Only the owner, presented here as the Grantee *ipsum lorem*, has full access to the files. No one else can view those files unless you use a plugin like S3Media LinkSafe™ Lite to create protected links for visitors.
Note: In your case, the owner grantee will have another name; ipsum *lorem* is just an example.

For **CloudFront Web distributions**, you may recall that we had the Web distribution setup in a way that it would inherit the correct permissions, including the **Trusted Signer** grantee. Yet, there is no trace of this here. This is no problem , the *bucket policy* takes care of access to distributions. In the past, each object needed a grantee set to **view/download**.

There are client applications which work much faster than the AWS console but they are platform dependent. For Windows, you can download CloudBerry Explorer and for Mac there is Cyberduck. Cyberduck exists for Windows also but we recommend CloudBerry Explorer as it is a better choice.

Using S3Media LinkSafe Lite

With the hardest part over, you are now ready to use S3Media LinkSafe™ Lite. There is a tutorial available on the website. We decided not to create PDF for this since changes will be made from time to time, so we deemed it better to make this a live document:

http://www.wp21century.com/how-to-use-s3media-linkafe-lite/

In case you struggle with setting up your bucket, we provide a service to configure it for you. See Premium support / Intervention AWS setup for more details.

Also check out our commercial plugin to protect videos and audios for coaches and professionals: S3Media Stream™