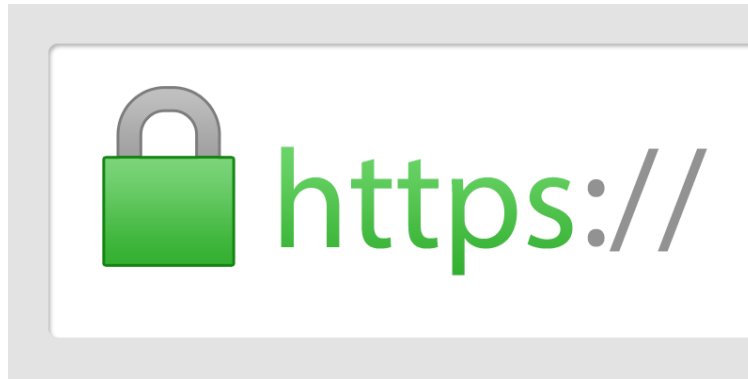


[Sign In](#)[Get started](#)Adnan Sabanovic [Follow](#)Dec 7, 2017 · 4 min read · [Listen](#)

How to Quickly add SSL certificate to Laravel on EC2 AWS



Secure site

There are many advantages of having an SSL certificate issued for your site. From a technical standpoint, your site is more secure and Google will love you more (meaning your SEO won't get worse), to a personal standpoint where you tend to trust more to sites having that HTTPS in front of their domain.

...

Web Hosting Recommendation

Many people have asked me about the hosting I am using. To be honest I tried different hosting accounts from shared, VPS and dedicated. In case you want some really affordable hosting I recommend [Bluehost](#). I am also hosting some of my Laravel projects right there on this \$3.95 shared account and it works great.



My recommendation for the best affordable web hosting. [Click here to jump right there!](#)

...

Continue ...

There were a lot of resources online, but most of them were by specific certificate agencies, explaining things from their end and then relating to AWS documentation for further action.

This article can really be about any application because the setup is almost completely server side. Only one tiny thing is related to Laravel, which is the path to its index.php file.

I will give you simple steps and explanations on how to set up your HTTPS quickly and painless.

SSL certificates range from \$5 to more than \$1200 per year and this is all about





1. Domain validation — They will just check your domain and possibly the WHOIS records, and make sure that your email is a valid one. It can be done within a few minutes and is generally a cheaper way to obtain a certificate. Ideal for startups and small companies.

2. Organization validation — This can take up to a few days. The agency will have to examine your organization/company papers to validate that you are a real, registered business.

3. Extended validation — This is the highest level where the agency will dig into your government records (in addition to doing the previous two validations). Once you are validated, your browser bar will turn into green, having your company name right before your address bar.

OK, now when you are familiar with how it works, let's see how we can install it on the server.

Instead of typing all the steps, I will refer to an article that will get you up to 80% of what you need to do

<https://www.domainsatretail.com/blog/security/simplest-way-use-ssl-certificates-amazon-ec2-ubuntu-server/>. Make sure you create those folders in `/etc/apache2/ssl`.

For transferring your files from your computer to your server, you can use `scp` command. Here is an example:

```
scp -i ~/.ssh/your_aws_key.pem /Users/adnan/Desktop/my_certs/*  
ubuntu@ec2-***-***-116-*.us-west-  
2.compute.amazonaws.com:/var/www/your-site
```

We are connecting with `ubuntu` user so it won't have privileges to store files inside `/etc/apache2/ssl` so let's just move it somewhere where `ubuntu` has a permission to create files and then log into your server, and `mv` your certificates as `root` to your `ssl` folder.

After you have received your certificate (Example: `my_certificate.crt`) and a



Once you have it, locate your hosts file. In case you just run a single EC2 (Without a load balancer) you can look for `/etc/apache2/sites-available` folder. In there you will have two files, `000-default.conf` and `default-ssl.conf`. The first one will have your `<VirtualHost *:80>` information and the second one, `default-ssl.conf` will hold your `<VirtualHost *:443>` host with port 443 for HTTPS.

Open up the second one, `default-ssl.conf` with `sudo vim default-ssl.conf` and change your DocumentRoot to your Laravel `public/` folder which could be something like `/var/www/your-site/public` and add the following lines after it:

```
SSLEngine on

SSLCertificateFile /etc/apache2/ssl/your_certificate.crt

SSLCertificateKeyFile /etc/apache2/ssl/private/your_key.key

SSLCertificateChainFile /etc/apache2/ssl/your_certificate.ca-bundle
```

Make sure you save the file before exiting.

After that we want to enable the instance to read from this file. Type the following:

```
sudo a2enmod ssl
sudo a2ensite default-ssl
sudo /etc/init.d/apache2 restart
```

If you have set your Inbound Rules from your EC2 Security group to allow traffic from 443 port (HTTPS) you should now type <https://your-site.com> and be able to load the site with https.

There is one more tiny thing to do here. We want to redirect all HTTP to HTTPS traffic and we can do that by opening the file we mentioned before `000-default.conf` and add the following lines right before the closing tags of

```
<VirtualHost *:80>
```

```
RewriteEngine On

RewriteRule ^(.*)$ https://%{HTTP_HOST}%1 [R=301,L]
```

And that's it.

Congratulations, you have successfully setup your site to load through HTTPS.

Follow me on [Twitter](#)

Add me on [LinkedIn](#)

[Sign In](#)[Get started](#)

Just a tech guy involved in mastering life using mental and physical discipline.
Journaling about productivity, personal development and overall growth. #Life

Love podcasts or audiobooks? Learn on the go with our new app.


[Try Knowable](#)

Recommended from Medium

 Ravi Chandra

Free Central Logging, Monitoring, and Analytics with ELK Stack



 Antonio Bulgaro


Cisco tutorial: How to optimize HSRP



 William Hard... in AWS in Plain En...


How to Implement Least Privilege Permissions Using the AWS IAM Access Analyzer




 Deeheem Ansari

Unemployment at a time of COVID-19: for developers fresh out of college



 Adil Abdullah

Services/API deployment in IIB 10

 Kavindu Abeywickrama


Job Roles related to the Database Management



 Chase

Download In @PDF Practical Oracle E-Business Suite: An Implementation and...



 Nandhini Rajaguru

Let me start with a small story.



[About](#) [Help](#) [Terms](#) [Privacy](#)

