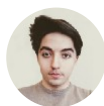




"A man wearing a watch typing on a MacBook" by Brad Neathery on Unsplash

Node + Express + LetsEncrypt : Generate a free SSL certificate and run an HTTPS server in 5 minutes or less



David Mellul [Follow](#)

Apr 22, 2018 · 4 min read

At the time of writing [my last article](#) I had a lot of hardships dealing with SSL certificates generated with LetsEncrypt (**certbot** actually).

I couldn't find a step by step tutorial just working like expected, thus I decided to write my own according to what worked for me.

***Side note:** Most often, your host will provide a one-click solution to setup and renew SSL certificates on your server. But if like me you're working on a VPS, you'll have to deal with it manually.*

. . .

What you actually came for

First, you need those few things:

- A server running on a linux distribution with root access (via SSH)
- NodeJS: <https://nodejs.org/en/>
- Express: `npm install express`
- Certbot

To install certbot, copy-paste those lines in a terminal :

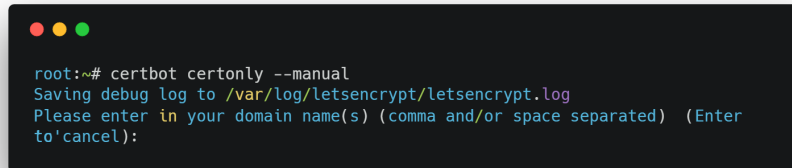
```
$ sudo add-apt-repository ppa:certbot/certbot
```

```
$ sudo apt-get update
```

```
$ sudo apt-get install certbot
```

Second, you will generate an SSL certificate with certbot :

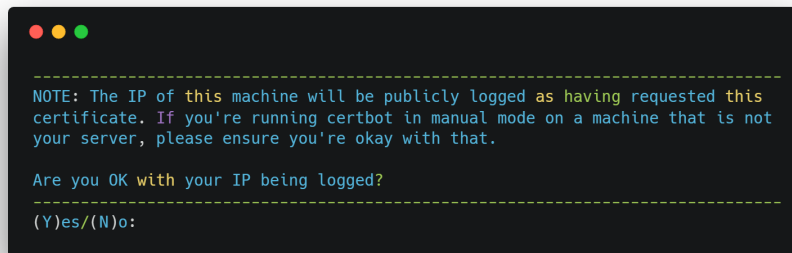
```
$ certbot certonly --manual
```

A terminal window with a dark background and three colored window control buttons (red, yellow, green) in the top-left corner. The text inside the terminal is as follows:

```
root:~# certbot certonly --manual
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Please enter in your domain name(s) (comma and/or space separated) (Enter
to 'cancel):
```

This picture has been generated with carbon, I like this tool very much (thanks Mr. Turin)

Type your domain name(s) without the protocol part. For instance:
yourdomain.com or even **muchdomain.verysite**.

A terminal window with a dark background and three colored window control buttons in the top-left corner. The text inside the terminal is as follows:

```
-----
NOTE: The IP of this machine will be publicly logged as having requested this
certificate. If you're running certbot in manual mode on a machine that is not
your server, please ensure you're okay with that.

Are you OK with your IP being logged?
-----
(Y)es/(N)o:
```

Type **Y** then **ENTER**.

A terminal window with a dark background and three colored window control buttons in the top-left corner. The text inside the terminal is as follows:

```
-----
Make sure your web server displays the following content at
http://yourdomain.com/.well-known/acme-challenge/a-string before continuing:

a-challenge

[You don't care about what's next]
-----
Press Enter to Continue
```

Note two things :

- **a-string** : The name of the file you have to create, right now. Just create it, we'll take care of the directories later.

- **a-challenge:** Open the file you just created and put this challenge string into it. Nothing else, just this challenge string.

Now, don't continue. You need to run a web server with Node & Express.

Keep your terminal opened somewhere

- **Create a directory with the name you want**, e.g : server
- **In this directory, create a JS file which will run your server.**
Keep it empty for the moment as I'll provide you with a ready-to-copy/paste source code.
- In this directory, create two directories : `.well-known` , and inside this one, create : `acme-challenge` .
- In the directory : `acme-challenge` place the file you created before : **a-string**

This is what you should have :

```
\server
----\.well-known
-----\acme-challenge
-----a-string
----server.js
```

Important: Actually the filename isn't **a-string**, it is a long alphanumeric string. For security purposes I can't show you mine. Same goes for **a-challenge**...

You're almost done !

Use your favorite code editor and copy-paste this code :

```
1  // Dependencies
2  const express = require('express');
3
4  // Configure & Run the http server
5  const app = express();
6
7  app.use(express.static(__dirname, { dotfiles: 'allow'
8
```

To verify that everything is fine, open up your browser and navigate to :
<http://yourdomain.com/.well-known/acme-challenge/a-string>

Your browser should download your challenge file. If it's not the case, take everything back from the start. Don't touch your shell, restart from directory & file creation.

If everything is okay, go back to your shell and type ENTER.

```
Press Enter to Continue
Waiting for verification...
Cleaning up challenges
Generating key (2048 bits): /etc/letsencrypt/keys/0002_key-certbot.pem
Creating CSR: /etc/letsencrypt/csr/0002_csr-certbot.pem

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at
  /etc/letsencrypt/live/yourdomain.com/fullchain.pem. Your cert
  will expire on 2018-07-21. To obtain a new or tweaked version of
  this certificate in the future, simply run certbot again. To
  non-interactively renew *all* of your certificates, run "certbot
  renew"
- If you like Certbot, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
  Donating to EFF: https://eff.org/donate-le
```

Hooray, one last step and you're done !!

Copy-paste the following code and you'll have a fresh HTTPS server running.

```
1  // Dependencies
2  const fs = require('fs');
3  const http = require('http');
4  const https = require('https');
5  const express = require('express');
6
7  const app = express();
8
9  // Certificate
10 const privateKey = fs.readFileSync('/etc/letsencrypt/live/yourdomain.com/privatekey.pem');
11 const certificate = fs.readFileSync('/etc/letsencrypt/live/yourdomain.com/fullchain.pem');
12 const ca = fs.readFileSync('/etc/letsencrypt/live/yourdomain.com/chain.pem');
13
14 const credentials = {
15     key: privateKey,
16     cert: certificate,
17     ca: ca
18 };
19
20 app.use((req, res) => {
21     res.send('Hello there !');
22 });
23
```

Navigate to : <https://yourdomain.com>, you should see “Hello there !”.

Well done, you've reached the end of this tutorial.

Last words:

- You might encounter errors, restart the tutorial from the beginning and overall don't forget to modify **yourdomain.com** with your actual domain name. Same goes for **a-string** and **a-challenge**.
- If nothing works, let me apologize. StackOverflow will be your best friend.
- This tutorial aims to make you use the manual method so that you have control over almost everything. In my case, this is the only solution that has worked.

. . .

Thanks for reading

I hope this tutorial was helpful enough.

You can check my last article here : [Creating a chatbot to book film tickets—Part 2](#)

Feel free to reach out to me at **david.mellul@outlook.fr**.

I'm opened to suggestions & requests for future articles, cya ☕ 😊



"Cappuccino in a white mug with white foam art on a wooden table" by wu yi on Unsplash