How to create a Self-Signed SSL Certificate on Ubuntu 18.04

Published on: 16 January 2020

Apache Security SSL Ubuntu

Contents

SSL Self-Signed certificates are self-signed certificates that are mainly used in development on our local machine or our remote server, when there is no certificate available from an external certification authority.

These self-signed certificates are rarely used for production in particular because they do not guarantee an adequate level of reliability, as they are not verified by a Certification Authority.

On the other hand, if you are interested in obtaining a free SSL certificate issued by an external certification authority, you can follow our guide on How to secure Apache with Let's Encrypt and Ubuntu 18.04.

First, connect to your server via an SSH connection. If you haven't done so yet, following our guide is recommended to connect securely with SSH. In case of a local server, go to the next step and open the terminal of your server.

Creating a private key

First of all, create a private key to make your public certificate.

To create a private key, use the OpenSSL client:

```
$ sudo openssl genrsa -aes128 -out private.key 2048
```

N.B. This command is used to specify the creation of a private key with a length of 2048 bits which will be saved in the private.key file.

```
Generating RSA private key, 2048 bit long modulus

....+++

...................+++

e is 65537 (0x010001)

Enter pass phrase for privata.key:

Verifying - Enter pass phrase for private.key:
```

You will be asked to protect the key with a password.

Creating a Certificate Signing Request (CSR)

After generating your private key, create a certificate signing request (CSR) which will specify the details for the certificate.

```
$ sudo openssl req -new -days 365 -key private.key -out request.csr
```

OpenSSL will ask you to specify the certificate information that have to be completed in this way:

```
You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]: IT

State or Province Name (full name) [Some-State]: Lazio

Locality Name (eg, city) []: Rome

Organization Name (eg, company) [Internet Widgits Pty Ltd]: My Society

Organizational Unit Name (eg, section) []: Security

Common Name (e.g. server FQDN or YOUR name) []: example.it

Email Address []: mymail@email.com
                Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []: An optional company name []:
```

You will be asked to protect the certificate request with a password.

The request.csr file with n all the useful information entered will be created for the generation of the certificate.

Generating the SSL Certificate

At this point, proceed with the generation of the certificate:

```
$ sudo openssl x509 -in request.csr -out certificate.crt
-req -signkey private.key -days 365
```

Where :

- for the -in parameter specify the certificate signing request
- for the parameter -out specify the name of the file that will contain the certificate
- for the -signkey parameter specify your private key
- for the parameter -days specify the number of days of validity of the certificate that is going o be created

Insert the password of private.key.

If the creation procedure was carried out correctly", this writing will be displayed on the screen:

```
Signature ok
```

followed by the certificate details specified above.

Finally, the certificate.crt file is ready to be used in different ways, such as to protect the connection to a web server.

Cloud Backup

Learn more ❯

Database as a Service

Learn more ❯

Cloud Object Storage

Learn more ❯

Domain Center

Learn more ❯

Jelastic Cloud

Learn more ❯