**Secure Nginx with Let's Encrypt on Ubuntu**

**Let’s Encrypt is a Certificate Authority (CA) that provides an easy way to obtain and install free TLS/SSL certificates, thereby enabling encrypted HTTPS on web servers. It simplifies the process by providing a software client, Certbot, that attempts to automate most (if not all) of the required steps. Currently, the entire process of obtaining and installing a certificate is fully automated on both Apache and Nginx.**

**Prerequisites**

* A fully registered domain name. This tutorial will use **abhiz.tk** throughout. You can get one for free on **Freenom**, or use the domain registrar of your choice.
* Both of the following DNS records set up for your server
* An A record with abhiz.tk pointing to your server’s public IP address.
* An A record with www.abhiz.tk pointing to your server’s public IP address.
* Nginx installed.

**The first step to using Let’s Encrypt to obtain an SSL certificate is to install the Certbot software on your server.**

**First, add the repository.**

add-apt-repository ppa:certbot/certbot

**You’ll need to press ENTER to accept.**

**Then, update the package list to pick up the new repository’s package information.**

sudo apt-get update

**And finally, install Certbot’s Nginx package with apt-get.**

sudo apt-get install python-certbot-nginx

**Certbot is now ready to use, but in order for it to configure SSL for Nginx, we need to verify some of Nginx’s configuration.**

vi /etc/nginx/sites-available/abhiz.tk.conf

. . .

*server\_name abhiz.tk www.abhiz.tk;*

. . .

**Then, verify the syntax of your configuration edits.**

sudo nginx -t

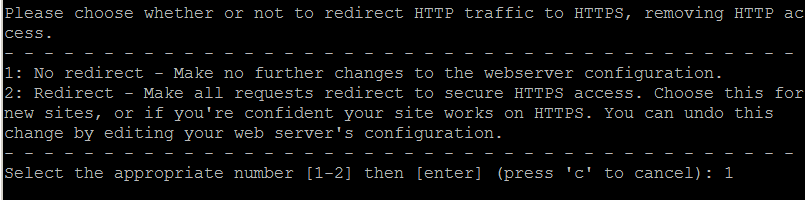
systemctl reload nginx

**Obtaining an SSL Certificate**

certbot --nginx -d abhiz.tk -d www.abhiz.tk

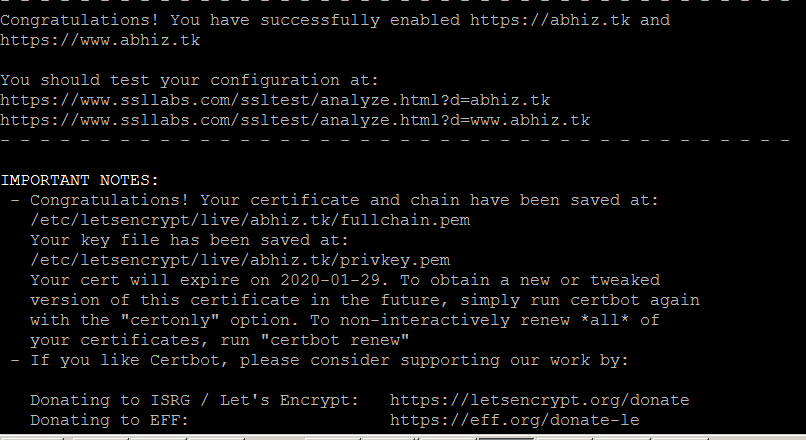
**you will be prompted to enter an email address and agree to the terms of service. After doing so, certbot will communicate with the Let’s Encrypt server, then run a challenge to verify that you control the domain you’re requesting a certificate for**.

**If that’s successful, certbot will ask how you’d like to configure your HTTPS settings.**

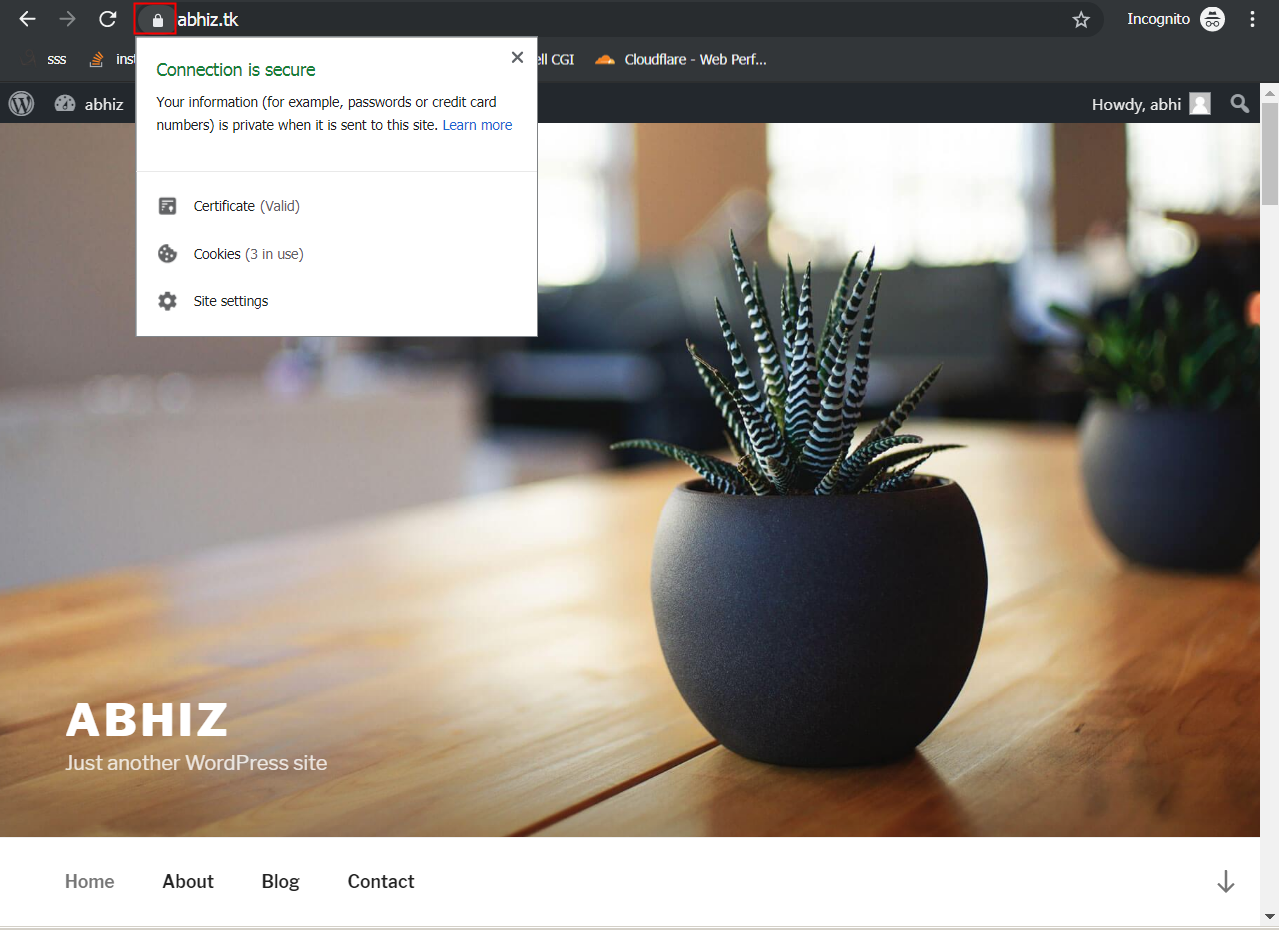


**Select your choice then hit ENTER. (recommended 1)**

**certbot will wrap up with a message telling you the process was successful and where your certificates are stored:**

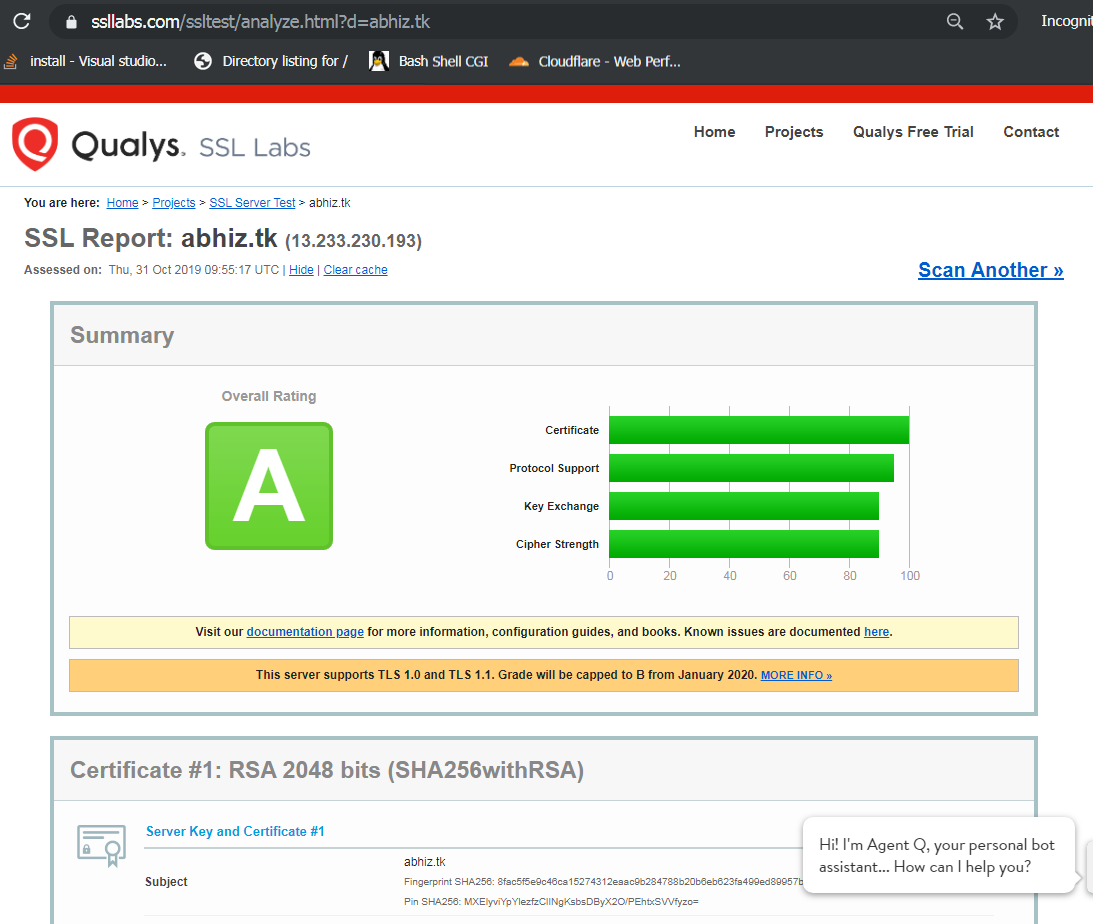
****

**Your certificates are downloaded, installed, and loaded. Try reloading your website using https:// and notice your browser’s security indicator.**

****

**To verify the status of your SSL Certificate visit the following link.**

https://www.ssllabs.com/ssltest/analyze.html?d=abhiz.tk&latest

****

**Secure Apache with Free Let’s Encrypt SSL Certificate on Ubuntu**

**In order to install Let’s Encrypt software on your server you need to have git package installed on your system.**

sudo apt-get -y install git

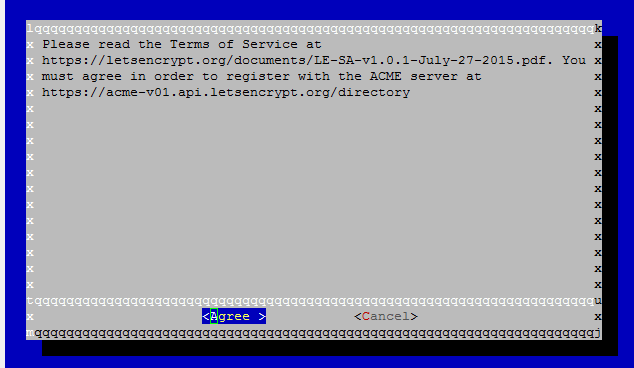
**clone Let’s Encrypt git repository.**

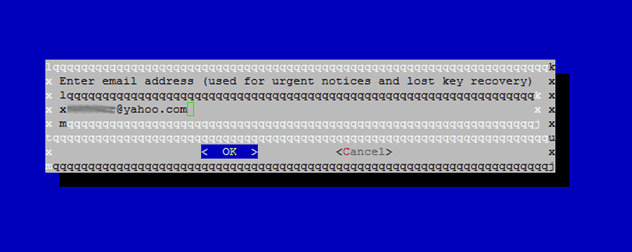
git clone https://github.com/letsencrypt/letsencrypt

**Generate a SSL Certificate for Apache**

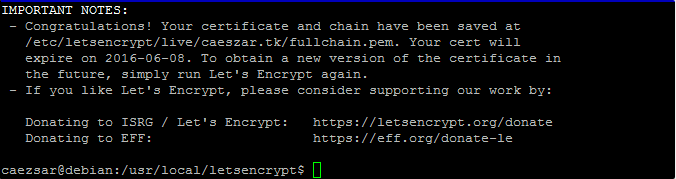
./letsencrypt-auto --apache -d saezar.tk -d www.saezar.tk

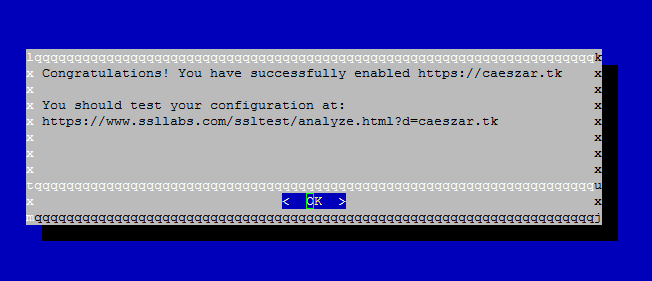
**Agree the license, enter an email address for recovery and choose whether clients can browse your domain using both HTTP protocols (secure and insecure) or redirect all non-secure requests to HTTPS.**

****

****

**After the installation process finishes successfully a congratulation message is displayed on your console informing you about the expiration date and how you can test the configuration as illustrated on the below screenshots.**





**after that you have to restart apache.**

systemctl restart apache2

**thats it.**