How to Make Self Signed SSL Certificate Work in CPanel

Posted on March 25,2016 by admin

Tutorial Assumptions

- you have a website domain
- you have shared hosting using cPanel
- you are using a computer running Ubuntu

This isn't a perfect solution if you have a public facing website, but if you have a private website for yourself, your friends, your business, etc, this will be 'better than nothing' and at least give you encryption for your traffic. Most hosting companies probably sell 'real' SSL certificates which cost a certain amount per year. This may make sense if you don't have time to figure it out, or you don't have root control of your server, or if your server happens to suck and not be ubuntu. If these things happen, you should consider a hosting change ASAP because someone else is controlling your website. In my case, I'm financially challenged right now and I have a couple of personal domains I want to secure. Note that I have not yet, as of the date of posting this, figured out what to do for W.O.T. It is still showing 'not secure' because it's not https but I don't want to use a self-signed certificate because it will scare away most visitors before they start reading. The best looking solution moving forward, by the way, and I'm trying to plan all my future sites around it is Let's Encrypt which is supported by some major players but also playing ball with the EFF it looks like. However, if you don't have control over your terminal on your server and cannot issue commands, I'm not sure that it will work. I'm still investigating. This tutorial is using Greengeeks cheap shared hosting out of the USA. I remember having to contacts tech support to making this option available in cpanel so you might have to as well
Download and Install OpenSSL on your Ubuntu machine

I assume it would be this command although it has been a while. might have to search it out if this doesn't work: sudo apt-get install openssl
Navigate to a Nice Place with your Terminal and Create a Directory Where Your Certificates will be Stored

I gave these a file name of domain-name-ssl-certs, and I did it in my home directory for speed and ease
sudo mkdir domain-name-ssl-certs
Run the Command to Generate the Certificates

You will need to swap out the directory path in this command to the one that matches where you just created the above directory sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /directory/directory/domain-name-ssl-certs/apache.key -out /directory/directory/domain-name-ssl-certs/apache.crt It will ask you to fill out stuff and the most important is this one which links it to your actual domain:

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

Go to Cpanel back end and prepare to paste in some stuff where it should go

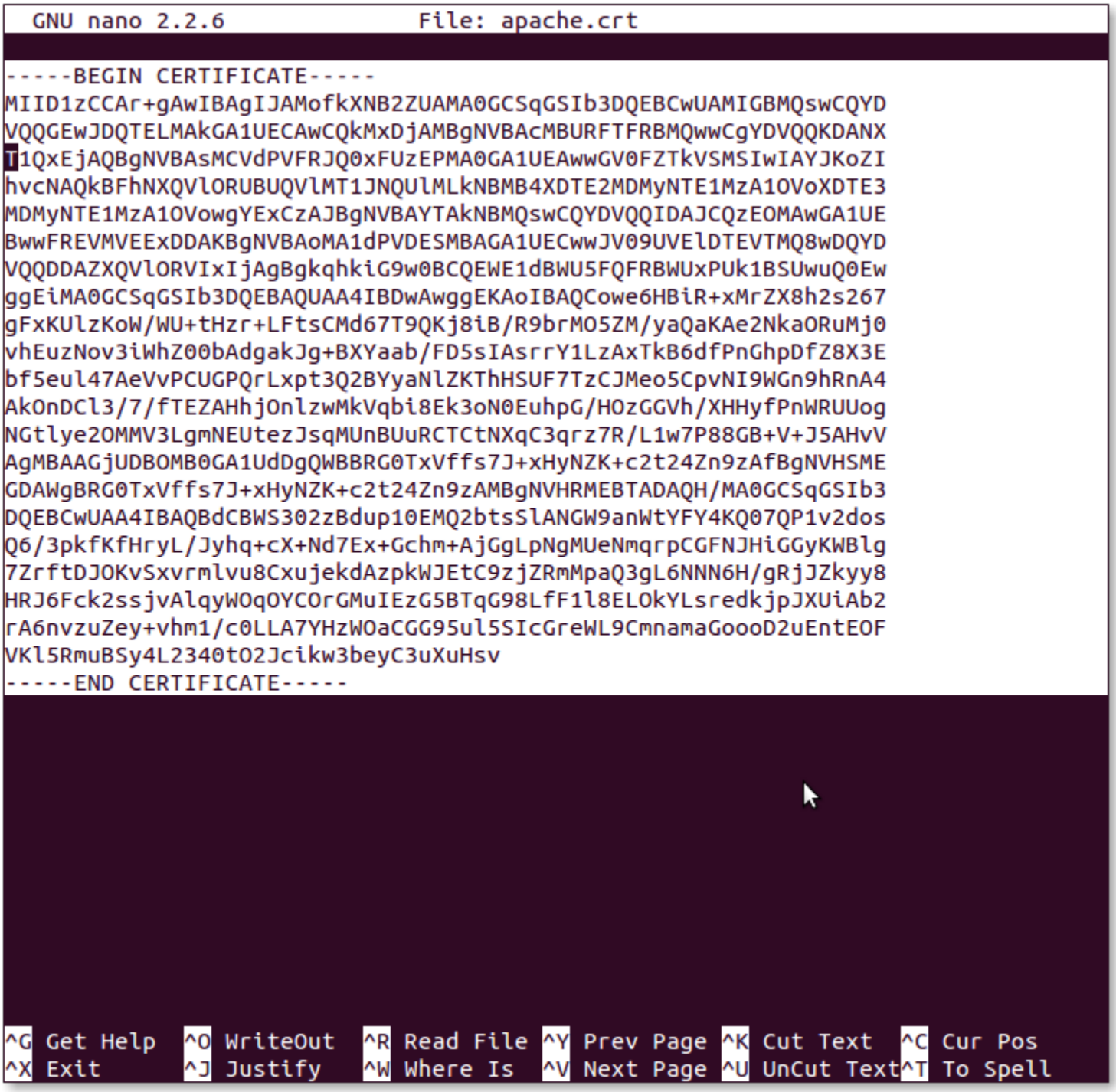
If you don't see the stuff I'm talking about in this section it may be because your hosting company doesn't want you to know you can do this because they want to sell you a $20 to $50/year 'real

certificate'. But if you are doing home-based stuff you need not spend. Make them make this function work or move to a company who will. In my cpanel it's under 'security' and 'SSL/TLS'. Click that.

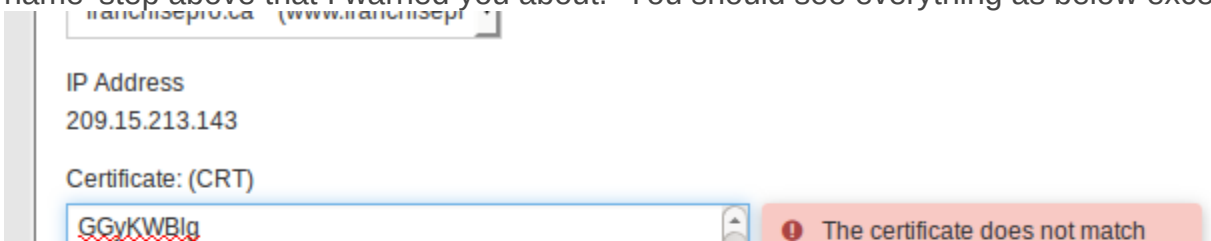
Install and Manage SSL for your site (HTTPS)

Go back to your terminal and open those .key and .crt files with a text editor like nano or gedit

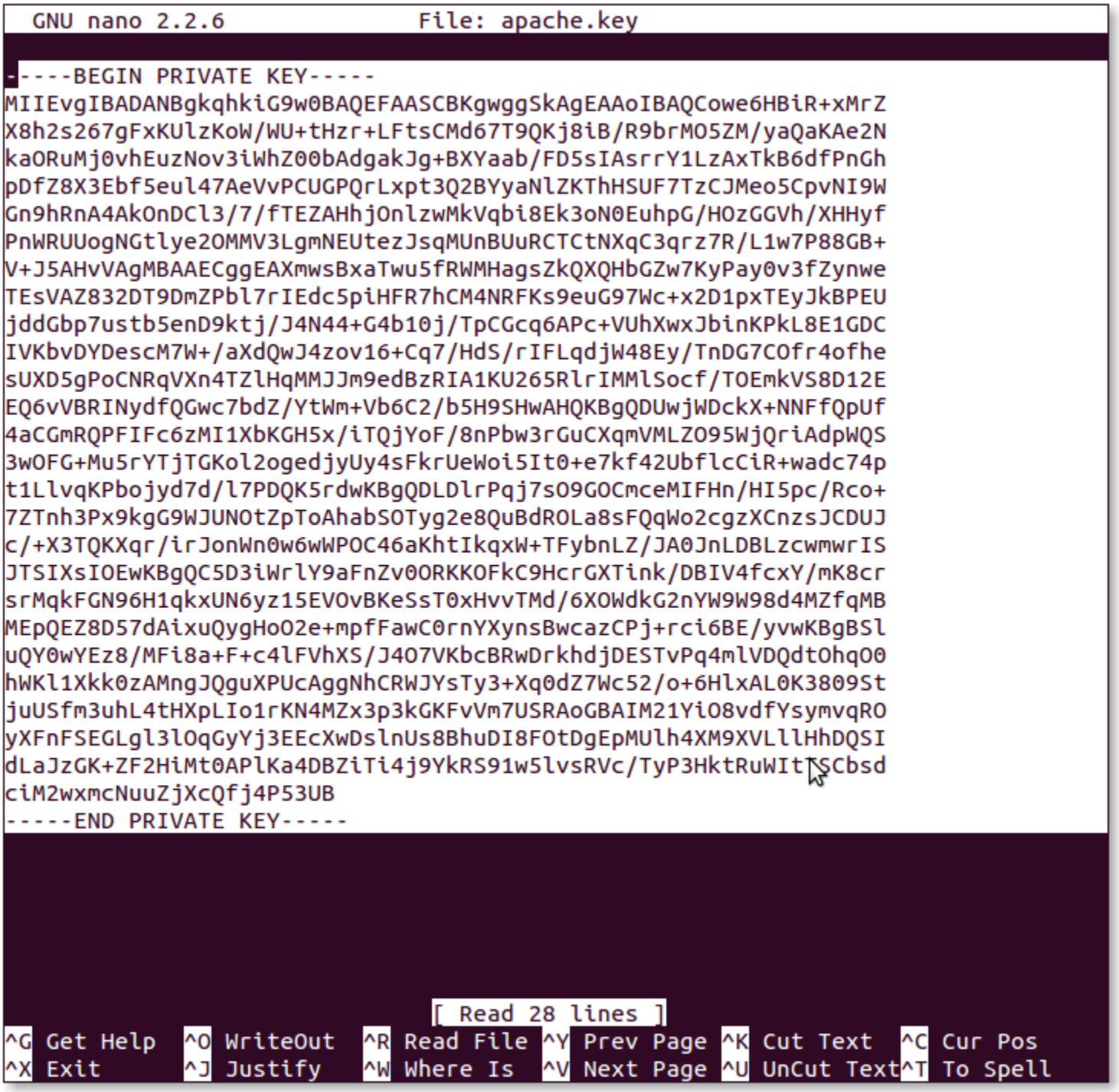
sudo nano apache.crt Select all the text after the --- of 'begin cert' and before the --- of 'end certificate' as follows.



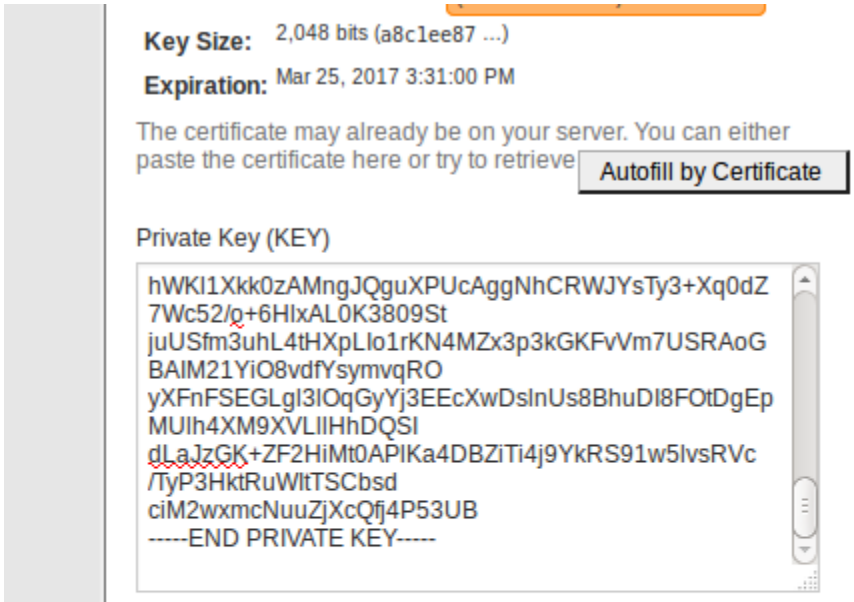
with the control and shift button down hit the 'c' button to copy it to the clipboard memory. Go back to your cPanel and paste it in the certificate field. If you get a warning that it doesn't match yoru domain it's because you didn't enter the domain correctly while you were creating the certificate in the 'Common name' step above that I warned you about. You should see everything as below except the red warning:



Open your Private Key that you generated and Copy/Paste it into your Cpanel sudo nano apache.key



control+shift+C it into this window in cPanel



good to go. Of course you will always get the 'this website is dangerous' warning the first time you visit it but whatever. Hope that helps. Now to try the same method with 'let's encrypt' and hopefully get rid of the 'dangerous' warnings, too!

Posted in:Technology,Tutorial,Ubuntu | Tagged:Certificates,Diy,Free,How To,Https,Key,Ssl,Tutorial,Ubuntu | With 1 comments