How to Enable HTTPS on Apache running Ubuntu 12.04

1. Generate a Self Signed Cert

```
# sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
<KeyName>.key -out <CertName>.crt
```

Place these files in a logical location. I personally placed them in the following location:
`/etc/ssl/certs/myCert.crt`
`/etc/ssl/private/myKey.key`

2. Modify the following files

- File: `/etc/apache2/httpd.conf`
  This file should be empty by default. Add the following lines.

  ```
  ServerName localhost
  ```

- File: `/etc/apache2/ports.conf`
  add to the file:

  ```
  NameVirtualHost *:443
  Listen 443
  ```

  Note: Apache can listen on multiple ports. Ex. You can open port 80(http) and have the http service running in parallel with port 443(https).

  I personally commented everything else out on this file except the above script.

  ERROR: If you get an error:
  (98)Address already in use: make_sock: could not bind to address [::]:443

  Then, it means that there is a conflict on port 443. Most likely you have a multiple entry on this file. Ensure that there are only one entry per port#.

- File: `/etc/apache2/sites-available/default`

  ```
  <VirtualHost *:443>
      SSLEngine on
      SSLCertificateFile /etc/ssl/certs/myCert.crt
      SSLCertificateKeyFile /etc/ssl/private/myKey.key
  ```

- File: `/etc/apache2/sites-available/default-ssl`
  Changed from:

```
<VirtualHost _default_:443>
```

  Changed to:

```
<VirtualHost *:443>
```

3. Restart this Apache

```
# sudo /etc/init.d/apache2 restart
```

Or

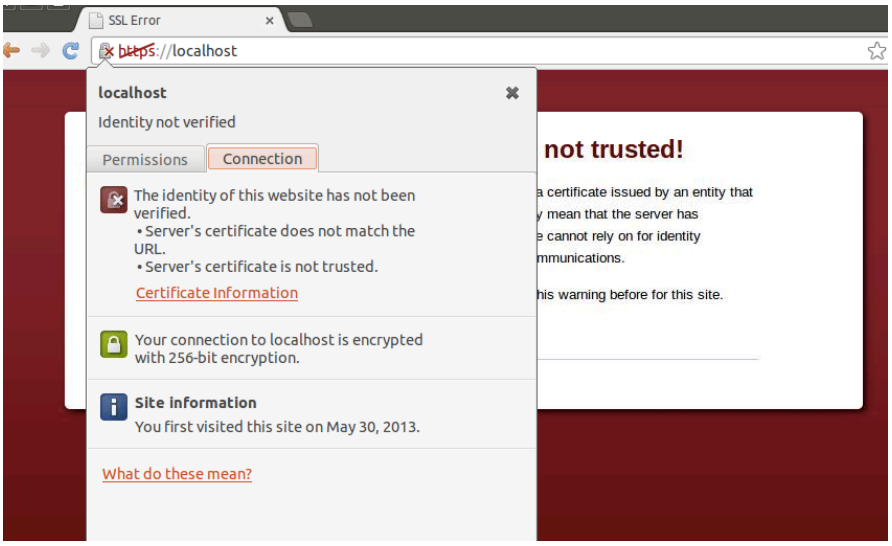
```
# sudo /etc/init.d/apache2 stop
# sudo /etc/init.d/apache2 start
```

4. Browser Connection via HTTPS

You will get a notification of if you want to accept the certificate or not.
You created and signed the certificate, so you know this certificate/website is good. Accept the certificate and enjoy your website.

If you see this "SSL Certificate not trusted" screen from a financial institute, ecommerce or a major cloud service such as Google, Yahoo!, Amazon, etc, then **you are in the wrong website**. It is a possible DNS spoofing or some other attack. **Do not accept the certificate and enter the website**.

There are Certificate Authority (CA) that verify the validity of the certificate such as VeriSign (Wiki: <http://en.wikipedia.org/wiki/Certificate_authority#Providers>). Major websites will register their certificate with these CA. For example, when you go to https://google.com, you will not be prompted with the "SSL Certificate not trusted" notification even when the connection is https. This is because Google has registered their certificate with the CA and your browser recognizes that Google's certificate is a valid certificate.



5. Troubleshooting

If you get an error message:

"Invalid command 'SSLEngine', perhaps miss spelled or defined by a module not included"

You need to enable **mod_ssl**

```
# sudo a2enmod ssl
# sudo /etc/init.d/apache2 restart
```

Source:

Error fix for "a23nmod ssl":
<http://www.emreakkas.com/linux-tips/invalid-command-sslengine-enabling-ssl-on-ubuntu-server#comment-9236>

How to create a certificate:
<http://www.sslshopper.com/article-how-to-create-and-install-an-apache-self-signed-certificate.html>

How to setup HTTPS on Apache:
<http://www.sslshopper.com/apache-server-ssl-installation-instructions.html>