How To Create a SSL Certificate on Apache for CentOS 6

Authored by: ***ASPHostServer Administrator*** *[asphostserver@gmail.com]*
Saved From: *http://faq.asphosthelpdesk.com/article.php?id=237*

A SSL certificate is a way to encrypt a site's information and create a more secure connection. Additionally, the certificate can show the virtual private server's identification information to site visitors. Certificate Authorities can issue SSL certificates that verify the virtual server's details while a self-signed certificate has no 3rd party corroboration.

Step One—Install Mod SSL

In order to set up the self signed certificate, we first have to be sure that Apache and Mod SSL are installed. You can install both with one command:

```
yum install mod_ssl
```

Step Two—Create a New Directory

Next, we need to create a new directory where we will store the server key and certificate

```
mkdir /etc/httpd/ssl
```

Step Three—Create a Self Signed Certificate

When we request a new certificate, we can specify how long the certificate should remain valid by changing the 365 to the number of days we prefer. As it stands this certificate will expire after one year.

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/httpd/ssl/apache.key -out /etc/httpd/ssl/apache.crt
```

With this command, we will be both creating the self-signed SSL certificate and the server key that protects it, and placing both of them into the new directory.

This command will prompt terminal to display a lists of fields that need to be filled in.

The most important line is "Common Name". Enter your official domain name here or, if you don't have one yet, your site's IP address.

```
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]:US
State or Province Name (full name) [Some-State]:New York
Locality Name (eg, city) []:NYC
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Awesome Inc
Organizational Unit Name (eg, section) []:Dept of Merriment
Common Name (e.g. server FQDN or YOUR name) []:example.com
Email Address []:webmaster@awesomeinc.com
```

Step Four—Set Up the Certificate

Now we have all of the required components of the finished certificate.The next thing to do is to set up the virtual hosts to display the new certificate.

Open up the SSL config file:

```
vi /etc/httpd/conf.d/ssl.conf
```

Find the section that begins with <VirtualHost _default_:443> and make some quick changes.

Uncomment the DocumentRoot and ServerName line and replace example.com with your DNS approved domain name or server IP address (it should be the same as the common name on the certificate):

```
 ServerName example.com:443
```

Find the following three lines, and make sure that they match the extensions below:

```
SSLEngine on
SSLCertificateFile /etc/httpd/ssl/apache.crt
SSLCertificateKeyFile /etc/httpd/ssl/apache.key
```

Your virtual host is now all set up! Save and Exit out of the file.

Step Five—Restart Apache

You are done. Restarting the Apache server will reload it with all of your changes in place.

```
/etc/init.d/httpd restart
```

In your browser, type https://youraddress to view the new certificate.