While Debian and Red Hat have some similarities they are still very different with regards to setting up the configuration.

Create the directory where Apache will retrieve the key and certificate.

mkdir -p /etc/ssl/localcerts

Generate the root certificate with key.

openssl req -new -x509 -days 365 -nodes -out /etc/ssl/localcerts/apache.pem -keyout /etc/ssl/localcerts/apache.key

Use the key to create a certificate.

openssl req -x509 -new -set_serial 1 -key apache.key -out apache.crt

Protect the keys by applying the following permissions.

*chmod 600 /etc/ssl/localcerts/apache**

Install the module is required by using package installer. To view current modules installed enter: *apachectl -M*

yum install mod_ssl

Note the following modules as a result of apachectl -M:
rewrite_module (shared)
ssl_module (shared)

Bind the http port 80 to all interfaces:

Listen 80

The following is the virtual host entry that can either be entered at the bottom of the httpd.conf file or as noted in the “conf.d” directory as a text file with an extension of .conf:

*<VirtualHost *:80>*
DocumentRoot /var/www/lssdb
ServerName www.lssdb.com
</VirtualHost>

** Depending on the Apache 2 package version a second virtual host entry will be required. In our test case the yum installation created the vhost file.*

*<VirtualHost *:443>*
SSLEngine On
SSLCertificateFile /etc/ssl/localcerts/apache.crt
SSLCertificateKeyFile /etc/ssl/localcerts/apache.key
DocumentRoot /var/www/lssdb
ServerName www.lssdb.com
</VirtualHost>

When using a package installer version of "mod_ssl" a ssl.conf file is loaded at /etc/httpd/conf.d/ssl.conf. To use this file edit the following items:

```
##
## SSL Virtual Host Context
##

<VirtualHost _default_:443>
# General setup for the virtual host, inherited from global configuration
DocumentRoot "/var/www/lssdb"

#   Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/ssl/localcerts/apache.crt

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/ssl/localcerts/apache.key

</VirtualHost>
```

The systemctl utility can be used to start, stop, and retrieve status for apache web server. The following commands will start the server and display it's status:

systemctl start httpd
systemctl restart httpd
systemctl status httpd

To run the httpd service on start up enter "systemctl enable httpd.service" and then review the list of services with "systemctl list-unit-files".

After completing the setup and for debugging tips the following are useful commands:

Apachectl configtest

View the apache error log, enter the following command:
tail *-f /var/log/httpd/error_log*

The system log has been changed and requires the *journalctl* command. To see all system message then enter:

Journalctl –f
Journalctl –f –u httpd

Note the second journal control command will display the apache log messages.

The iptables configuration is located in /etc/systemconfig/iptables. This folder will contain configuration settings and when disabled, there are only directives. There are basically two files “iptable.conf “ and “ip6table.conf” that contains the rules.