May need CSR (Certificate signing request) generated before SSL can be applied.

# Certificate signing request.

<https://www.digicert.com/easy-csr/openssl.htm>

# Certificate Decoder

<https://www.sslshopper.com/certificate-decoder.html>

# Check CSR

<https://www.digicert.com/ssltools/view-csr/>

# To extract private key from PFX :

openssl pkcs12 -in ssl.pfx -out priv.key -nocerts -nodes

# To extract .crt from PFX : # Export client certificate

openssl pkcs12 -in keystore.p12 -out certificate.pem -nodes -nokeys -clcerts

**Export CA certificate chain**

openssl pkcs12 -in keystore.p12 -out intermediate.pem -nodes -nokeys -cacerts

**Use private key and PEM to generate .PFX file**

openssl pkcs12 -export -out certificate.pfx -inkey private\_key.pem -in certificate.pem

**Use client and intermediate certificate and private key to generate .PFX file**

openssl pkcs12 -in certificate.pem -certfile intermediate.pem -inkey private.key -export -out certificate.p12

# Compare the keys

Below will compare the md5 hash, if it matches use the private key and certificate file.

openssl pkey -in privateKey.key -pubout -outform pem | sha256sum

openssl x509 -in certificate.crt -pubkey -noout -outform pem | sha256sum

If on reverse proxy – need to go to /etc/httpd.d/conf.d and edit .conf file with update directory path of SSL key , .crt and bundle crt files

Check logs here  -  /var/log/httpd/error\_log

Restart the httpd service

sudo service httpd stop

sudo service httpd start

sudo service httpd status

\*\*NOTE \*\*  I have seen where reverse proxy has NGINX installed, please check this also.

cd /etc/nginx/conf.d

s nginx -t

s service nginx reload