**Enabling HTTPS For exacqVision Enterprise Manager:**

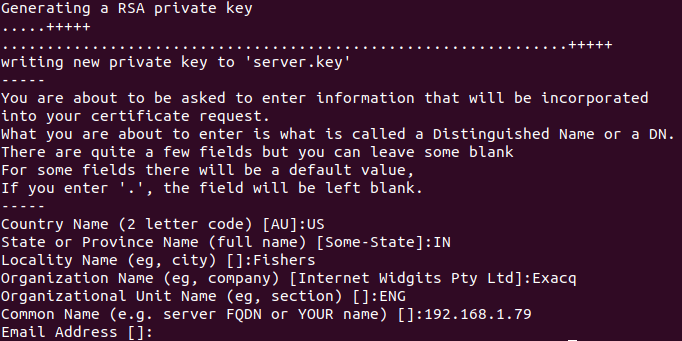
For a trusted certificate, it is recommended that you purchase a third-party intermediate certificate from one of many online providers.

These steps will detail how to create a self-signed certificate:

**CREATING A SELF-SIGNED SSL CERTIFICATE**

**Command:** sudo openssl req -new -x509 -sha256 -days 365 -nodes -out server.crt -keyout server.key

You will be prompted with a series of questions.:



* Use data specific to your site.
* Items can be left blank with the exception of Common Name
* Common Name (e.g. server FQDN or YOUR name) should be the IP address of EM Server

**Summary of above command:**

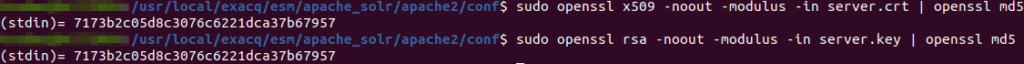
* Generates a self-signed SSL/TLS certificate (server.crt) and its associated private key (server.key).
* The certificate is valid for 365 days and uses the SHA-256 algorithm for signing.
* The certificate is not encrypted with a passphrase (-nodes), making it suitable for automated server use.
* Both the certificate and the private key are saved in the current directory (or the directory you run the command from).

**Validate the Cert and Key files:**

sudo openssl x509 -noout -modulus -in /usr/local/server.crt | openssl md5

sudo openssl rsa -noout -modulus -in /usr/local/server.key | openssl md5

Verify the md5 hashes match, if they DO NOT then see the troubleshooting section below before proceeding.



**OBTAINING A THIRD-PARTY CERTIFICATE**

If you are planning to acquire a third-party certificate from a trusted provider, you may need to provide them with a Certificate Signing Request (CSR) file.

You may use our tool at the following URL to generate a CSR file.   <https://exacq.com/support/gencsr/>

Enter all the fields click on the ‘Submit’ button to download the ZIP file. Inside this ZIP file is the CSR file and RSA key to give to your certificate provider.

If you purchased a chained certificate, be sure to download the appropriate intermediate bundle.

Once you have downloaded the files from your provider:

* Rename the .crt file to ‘server.crt’.
* Rename the .key file to ‘server.key’.
* If you have a chained certificate, rename the chain file to ‘server-ca.crt’.

Place the renamed files from your Certificate Authority (CA) into the following directory:

* Windows: C:\Program Files\exacqVision\EnterpriseManager\apache\conf\
* Linux:  /etc/evapache/

**TIPS**

When purchasing an SSL certificate, many providers offer an Intermediate Bundle, or additional certificates that must be present to link your certificate to a root certification authority. Usually the provider will have documentation on how to accomplish this with Apache, but it is a good idea to ask them before or during the purchasing process. Exacq is **not** responsible for making your certificates capable of working with Apache.

It is possible to combine all the intermediate certificates that a provider may give you into one file. Consult your provider for more information.

**Python Uvi corn Server to Start the Https server and redirect to HTTPS:**