

## Generating CSRs for 3rd Party Certificates

### Tools Required

- **OpenSSL**
  - <https://slproweb.com/products/Win32OpenSSL.html>
- **Helper pages**
  - <https://www.digicert.com/easy-csr/openssl.htm> will generate the openssl command to create the CSR and private key for the certificate obtained from a trusted certificate authority.
  - <https://www.sslshopper.com/article-most-common-openssl-commands.html> shows common commands. The command to be used is the last in the list with modifications.

### Introduction

Customers coming online with Qlik Sense want to use certificates issued by trusted certificate authorities like Symantec, Digicert, GoDaddy, and others. While the QMC does have a certificate export function, the only capability is exporting the Qlik Sense generated self-signed certs. To generate a CSR, you need to use an additional tool like OpenSSL.

### Certificate Requirements

Certificates that are known to work well with Qlik Sense have the following attributes:

- Must contain a Private Key
- Certificates that are x509 version 3. More information including filename extensions under <https://en.wikipedia.org/wiki/X.509>
- Use signature algorithm sha256RSA
- Use signature hash algorithm sha256
- Signed by a valid, and os/browser configured, CA
- Are valid according to date restrictions (valid from/valid to)
- Key in format CryptoAPI (not in CNG)

See [Qlik Sense: Compatibility Information for third-party SSL certificates to use with HUB/QMC](#).

Also note that the certificate must include the ProviderType (24) Microsoft Enhanced RSA and AES Cryptographic Provider. See how to convert the provider under [SHA-256 and Converting the Cryptographic Service Provider Type](#).

### OpenSSL Installation

1. Download the x64 version of OpenSSL. You can obtain a Windows ready copy from [Shining Light Productions](#)
2. Transfer the installation file to the Qlik Sense server. Perform the installation.  
In our example, we use the installation path c:\openssl
3. Open a command line window and change directories to c:\openssl\bin. Keep the window open.



## Digicert's OpenSSL Command Line Generator

1. Navigate to here in web browser: <https://www.digicert.com/easy-csr/openssl.htm>
2. When presented with the form fill in the fields:

Certificate Details

Common Name:

Organization:

Department:

City:

State / Province:

Country:

Key Size:

Field	Value	Description
Common Name	*.example.com	The fully qualified hostname of the server that will use the certificate. Wildcards for hostnames accepted on fully qualified names. e.g. myserver.example.com or *.example.com
Organization	Company Friendly name	Company Friendly name
Department	Optional, the department using the certificate	Optional, the department using the certificate
City	Optional, the city for the certificate	Optional, the city for the certificate
State	Required, the state the company is headquartered	Required, the state the company is headquartered
Country	Required, the country the company is headquartered	Required, the country the company is headquartered
Key Size	RSA 2048, Leave at this value.	RSA 2048, Leave at this value.

3. After filling out the CSR tool, click the generate button. An OpenSSL command will replace the entry form.

Certificate Details

Common Name:

Organization:

Department:

City:

State / Province:

Country:

Key Size:

Information

Now just copy and paste this command into a terminal session on your server. Your CSR will be written to myserver\_example\_com.csr.

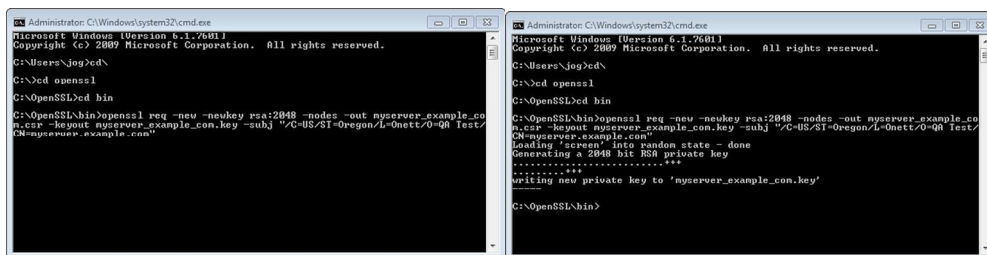
```

openssl req -new -newkey rsa:2048 -nodes -out myserver_example_com.csr -keyout myserver_example_com.key -subj /C=US/ST=Oregon/L=Ornett/O=QA Test/CN=myserver.example.com

```

## Generate the CSR

1. Copy the command line and place it in the command window opened earlier. Observe the reference to the csr file after the -out command and private key after the -keyout command. Hit the enter key.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

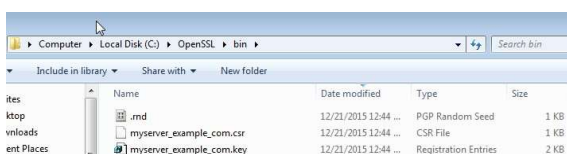
C:\Users\jog>cd
C:\>cd openssl
C:\OpenSSL>cd bin
C:\OpenSSL\bin>openssl req -new -newkey rsa:2048 -nodes -out myserver_example.com.csr -keyout myserver_example_com.key -subj "/C=US/ST=Oregon/L=Onett/O=QA Test/myserver.example.com"

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\jog>cd
C:\>cd openssl
C:\OpenSSL>cd bin
C:\OpenSSL\bin>openssl req -new -newkey rsa:2048 -nodes -out myserver_example.com.csr -keyout myserver_example_com.key -subj "/C=US/ST=Oregon/L=Onett/O=QA Test/myserver.example.com"
Loading random state - done
Generating a 2048 bit RSA private key
.....+...
Writing new private key to 'myserver_example_com.key'

C:\OpenSSL\bin>
```

2. The CSR and private key will be generated in the openssl\bin directory because we didn't specify a path to output in the files.



3. At this point, it's time to send the CSR to the trusted certificate authority. The method for providing the CSR differs by vendor, please identify how to supply the CSR and upload it to the CA.
4. When the CA receives the CSR, the certificates will be generated. Typically, an email address is required for certificate ownership. This is where the certificate will likely be sent if distributed via email. Other CAs like goDaddy allow certificate owners to download the certificate.

## Adding the Private Key to the Certificate

1. Once the certificate is obtained, the private key needs to be added to it in order for Qlik Sense to use it for server authentication and certification. To perform this action, use OpenSSL again to create a pkcs12 certificate file containing the certificate and the private key.
2. Copy the obtained certificate to the openssl\bin folder.
3. In the command line, we will tell OpenSSL to:
  - Use the .crt file as a source for the .pfx
  - Output a .pfx
  - Include the key (-inkey)
  - Specify the Microsoft Enhanced RSA and AES Cryptographic Provider (-CSP)

### Example Command:

```
openssl pkcs12 -export -in certificateFromCAProvider.crt -out certificate.pfx -inkey myserver_example_com.key -CSP "Microsoft Enhanced RSA and AES Cryptographic Provider"
```

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\jog>cd\
C:\>cd openssl
C:\OpenSSL>cd bin
C:\OpenSSL\bin>openssl req -new -newkey rsa:2048 -nodes -out myserver_example.com.csr -keyout myserver_example_con.key -subj "/C=US/ST=Oregon/L=0nett/O=QA Test/CN=myserver.example.com"
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+++++
writing new private key to 'myserver_example_con.key'

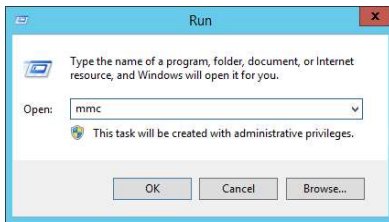
C:\OpenSSL\bin>openssl pkcs12 -export -out certificate.pfx -inkey myserver_example_con.key -in certificateFromCA.crt

```

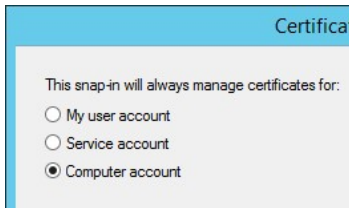
- Running this command will request a password for the new file and generate the pfx file in the openssl\bin folder. Now import the certificate for use with Qlik Sense.

## Import a 3rd Party Certificate for Use with Qlik Sense Server

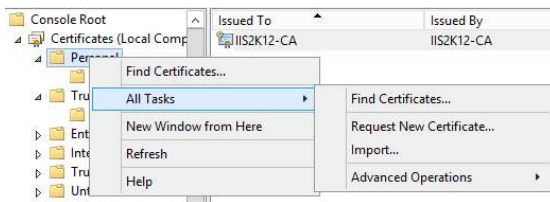
- Launch the MMC.



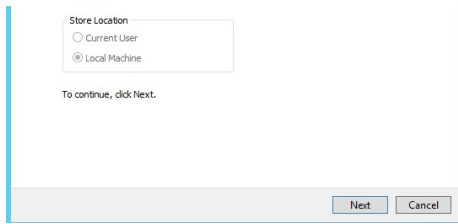
- When the MMC opens go to File|Add/Remove Snap-in.
- Click on the Certificates snap-in on the left side list box and click the add button.
- Choose Computer account and click Next.



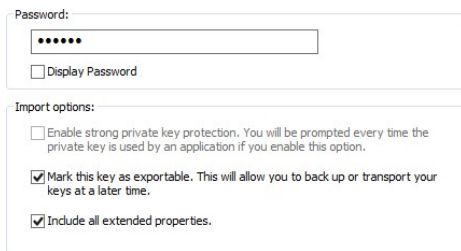
- Leave Local computer selected and click Finish.
- Click OK to go back to the MMC. The Local computer certificate store opens
- Right click on the Personal folder and choose Import.



- Because we have specified the location to import a certificate, the store location choice is greyed out.
- Click Next.



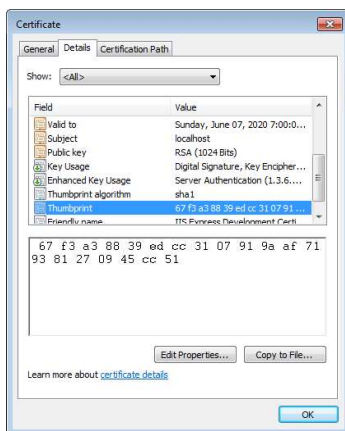
10. Browse to the location of the certificate containing private key (the pfx file) and
11. Click Next.
12. Enter the password set during certificate merge process.



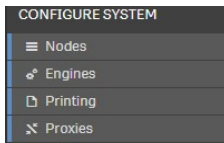
13. Prompted with the Certificate store to place the certificate, make sure the radio button is highlighted for Place all cert... and the store is Personal.
14. Click Next.



15. Click Finish and the certificate will be imported.
16. Double click on the imported certificate and choose details.
17. Navigate down the list and click on Thumbprint.



18. Copy the thumbprint with spaces from the textbox.
19. Browse to the Qlik Sense Management Console.
20. Click on the Proxies menu item.



21. Choose the appropriate proxy to input the thumbprint to use the 3rd party certificate. Click edit to open the proxy settings.
22. Click on the security option and enter the thumbprint (with spaces) in the textbox. Click Apply. The QMC will ask to restart. Please click the Restart QMC button. You may be required to refresh the browser as well.

For detailed information on how to apply a 3<sup>rd</sup> party certificate, see: [How to change the certificate used by the Qlik Sense Proxy.](#)