

CONFIGURAZIONE XAMPP + SSL (HTTPS)

a cura di Anna Marchese

Questa guida consente di configurare Xampp per Windows 7, con il protocollo https (ovvero connessione sicura o protetta). Io ho installato Xampp sul mio hard disk esterno per cui farò riferimento a questa directory (G:\) in cui ho scaricato il pacchetto di Xampp (file .zip anziché l'installer).

Effettua una copia di backup dei 3 file di configurazione di Apache (httpd.conf , php.ini , httpd_ssl.conf) che trovi in:

1. G:\xampp\apache\conf\httpd.conf
2. G:\xampp\apache\conf\extra\httpd-ssl.conf
3. G:\xampp\php\php.ini

I STEP (CREAZIONE DEL CERTIFICATO)

Apri una finestra DOS da Start → Digita cmd → Esegui come amministratore.

Digita **cd ** in modo tale da trovarti su C:\ se hai installato Xampp in C. Io ho eseguito il comando **G:** per portarmi in **G:**

A questo punto vai nella directory **bin** con il comando **cd G:\xampp\apache\bin** come mostrato nell'immagine sottostante:



```
Amministratore: C:\Windows\System32\cmd.exe
Microsoft Windows [Versione 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.

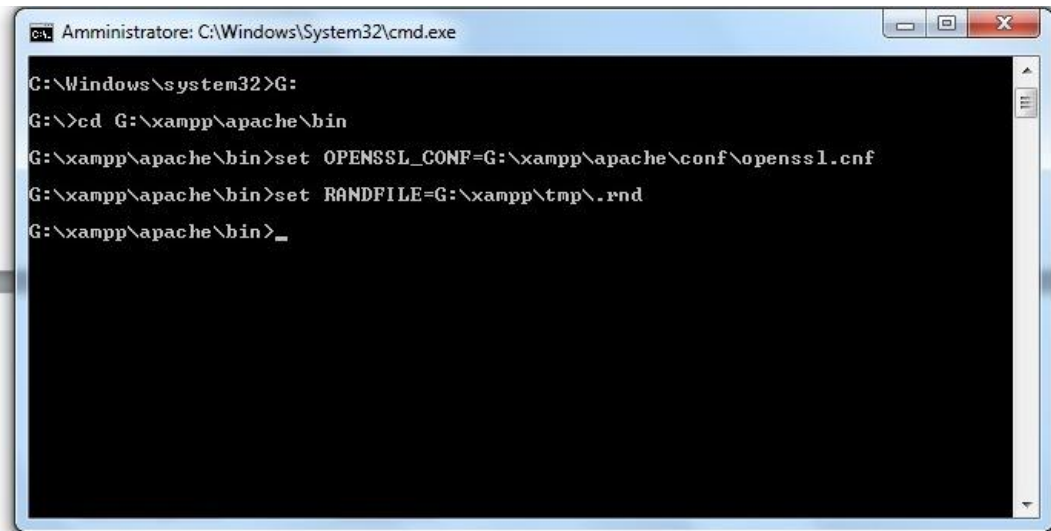
C:\Windows\system32>G:
G:\>cd G:\xampp\apache\bin
G:\xampp\apache\bin>
```

Figura1

Setta le seguenti variabili d'ambiente:

```
set OPENSSL_CONF=G:\xampp\apache\conf\openssl.cnf
```

```
set RANDFILE=C:\Windows\Temp\.rnd
```



```
Amministratore: C:\Windows\System32\cmd.exe
C:\Windows\system32>G:
G:\>cd G:\xampp\apache\bin
G:\xampp\apache\bin>set OPENSSL_CONF=G:\xampp\apache\conf\openssl.cnf
G:\xampp\apache\bin>set RANDFILE=G:\xampp\tmp\rnd
G:\xampp\apache\bin>_
```

Figura2

Adesso puoi creare un certificato con firma digitale.

Lancia openssl.exe digitando **openssl** dalla directory in cui ti trovi.

Digitare la seguente riga per creare una chiave criptata a 1024 bits:

genrsa -des3 -out server.key 1024

Dopo l'esecuzione vi verrà chiesto di inserire una password a vostra scelta (2 volte, per evitare errori di digitazione), come mostrato nella figura sottostante:



```
C:\Windows\system32\cmd.exe - openssl
OpenSSL> genrsa -des3 -out server.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
OpenSSL>
```

Figura3

Adesso crea una copia di questa chiave (1) e dopo genera la chiave in uscita (2), ottenuta dalla copia stessa. Questa operazione ci evita di inserire la password nella successiva fase.

1. Posizionati in **G:\xampp\apache\bin** e digita il seguente comando:

copy server.key server.key.org

2. Lancia di nuovo **openssl** e da qui il comando:

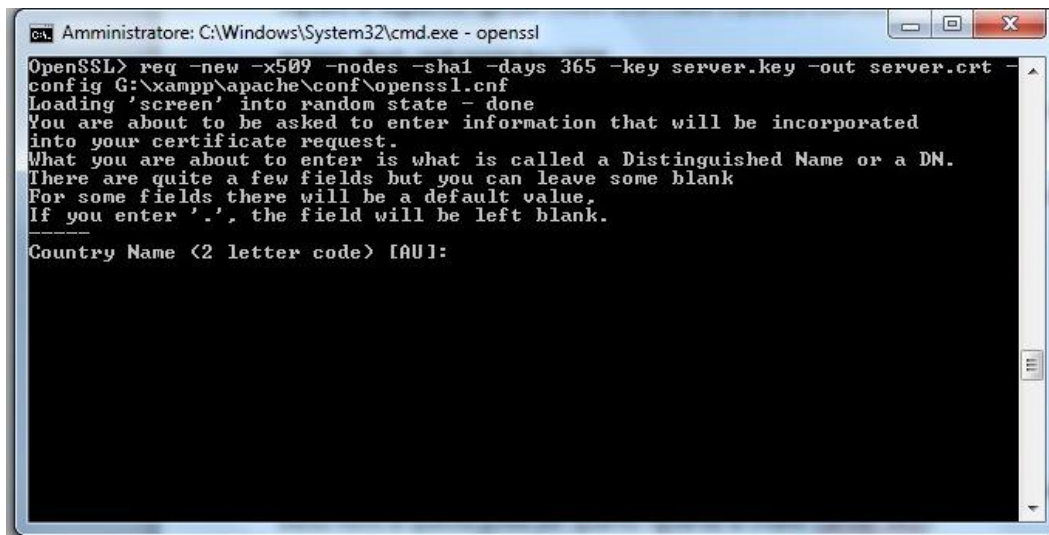
rsa -in server.key.org -out server.key

L'ultima operazione da fare per creare il certificato è digitare la seguente riga, supponendo di aver usato gli stessi nomi di questa guida per quanto riguarda la chiave (server.key):

req -new -x509 -nodes -sha1 -days 365 -key server.key -out server.crt -config G:\xampp\apache\conf\openssl.cnf

L'attributo days sta ad indicare il tempo di validità del certificato: fra 1 anno scadrà e occorrerà farne uno nuovo.

A questo punto dopo l'esecuzione del comando verranno chieste alcune cose. Per ciascuna si può continuare a cliccare invio senza inserire alcun valore. L'unico da inserire è il parametro **localhost** quando si chiede il Common Name.



```
Amministratore: C:\Windows\System32\cmd.exe - openssl
OpenSSL> req -new -x509 -nodes -sha1 -days 365 -key server.key -out server.crt -
config G:\xampp\apache\conf\openssl.cnf
Loading 'screen' into random state - done
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]:
```

Figura4

Dopo questa operazione la creazione del certificato che ti servirà per l'esecuzione del protocollo HTTPS è terminata. Nella directory **G:\xampp\apache\bin** avrai i due file (server.key e server.crt).

II step (COPIA DEI DUE FILE NELLA DIRECTORY G:\xampp\apache\conf)

Crea due directory nel percorso **G:\xampp\apache\conf** denominate **ssl.crt** e **ssl.key**.

Copia il file server.key nella directory ssl.key e il file server.crt nella directory ssl.crt

Se già esistenti, sovrascrivili.

III step (MODIFICA FILE HTTPD.CONF E PHP.INI)

1. Vai in **G:\xampp\apache\conf** e cerca nel file httpd.conf la linea di codice:

```
#LoadModule ssl_module modules/mod_ssl.so
```

rimuovi il commento (#) per abilitare l'istruzione.

2. Sempre nel file httpd.conf cerca la riga:

```
#include conf/extra/httpd-ssl.conf
```

Rimuovi il commento (#) e copiala in basso dopo la fine del codice </ifModule>

Salva le modifiche apportate al file httpd.conf

3. Apri il file **php.ini** che si trova nella directory **G:\xampp\php** e cerca la linea di codice:

```
;extension=php_openssl.dll
```

Elimina il commento (;) per abilitare l'istruzione.

Salva le modifiche apportate al file php.ini

IV step (MODIFICA DEL FILE HTTPD_SSL.CONF)

Vai nella directory **G:\xampp\apache\conf\extra** e apri **httpd_ssl.conf**. Cerca il seguente blocco di codice:

```
<VirtualHost _default_:443>

    # General setup for the virtual host

    DocumentRoot "/xampp/htdocs"

    ServerName www.example.com:443

    ServerAdmin admin@example.com

    ErrorLog "/xampp/apache/logs/error.log"

    TransferLog "/xampp/apache/logs/access.log"
```

Modificalo come segue:

```
<VirtualHost _default_:443>

    # General setup for the virtual host

    DocumentRoot "my_documentRoot"

    ServerName localhost:443

    ServerAdmin admin@example.com

    ErrorLog "/xampp/apache/logs/error.log"

    TransferLog "/xampp/apache/logs/access.log"
```

dove my_documentRoot è il nome della directory che hai scelto come DirectoryRoot. Il resto può restare com'è o puoi modificare, ad esempio, il ServerAdmin, ErrorLog e TransferLog.

Nello stesso file cerca ora le righe:

```
SSLCertificateFile "conf/ssl.crt/server.crt"
```

e

SSLCertificateKeyFile "conf/ssl.key/server.key"

Accertati che siano scritte così e non siano commentate. In caso contrario, modificate e/o decommenta.

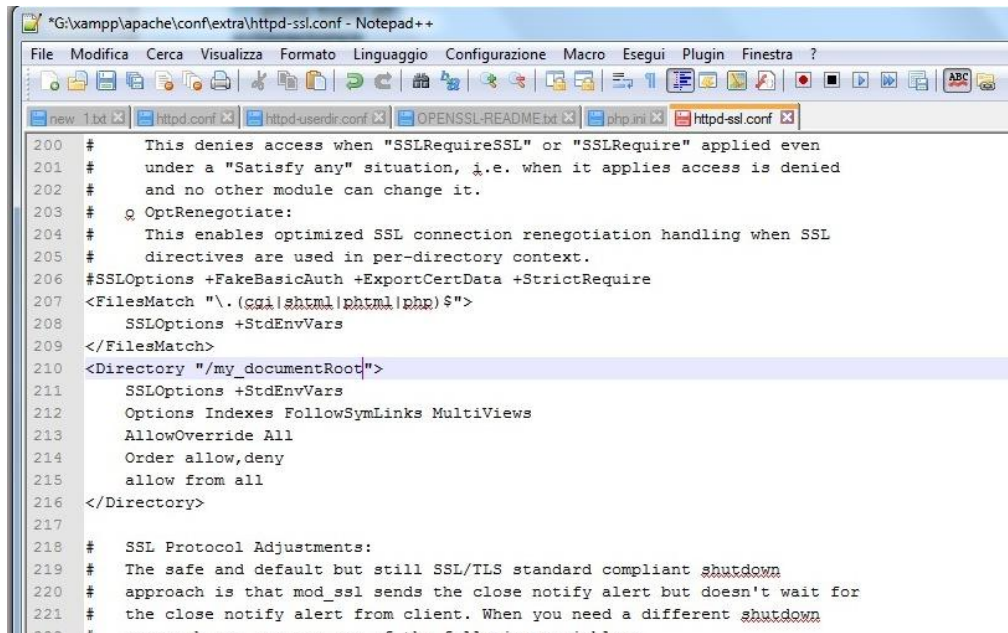
Cerca questo blocco di codice:

```
<FilesMatch "\.(cgi|shtml|phtml|php)$">  
    SSLOptions +StdEnvVars  
</FilesMatch>  
  
<Directory "/xampp/apache/cgi-bin">  
    SSLOptions +StdEnvVars  
</Directory>
```

E modificalo in

```
<FilesMatch "\.(cgi|shtml|phtml|php)$">  
    SSLOptions +StdEnvVars  
</FilesMatch>  
  
<Directory "/my_documentRoot">  
    SSLOptions +StdEnvVars  
  
    Options Indexes FollowSymLinks MultiViews  
  
    AllowOverride All  
  
    Order allow,deny  
  
    allow from all  
  
</Directory>
```

Salvate il file **httpd_ssl.conf** con le modifiche apportate.



```
*G:\xampp\apache\conf\extra\httpd-ssl.conf - Notepad++
File Modifica Cerca Visualizza Formato Linguaggio Configurazione Macro Esegui Plugin Finestra ?
new 1.txt httpd.conf httpd-userdir.conf OPENSLL-README.txt php.ini httpd-ssl.conf
200 # This denies access when "SSLRequireSSL" or "SSLRequire" applied even
201 # under a "Satisfy any" situation, i.e. when it applies access is denied
202 # and no other module can change it.
203 # OptRenegotiate:
204 # This enables optimized SSL connection renegotiation handling when SSL
205 # directives are used in per-directory context.
206 #SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
207 <FilesMatch "\.(cgi|sh|html|php)$">
208     SSLOptions +StdEnvVars
209 </FilesMatch>
210 <Directory "/my_documentRoot">
211     SSLOptions +StdEnvVars
212     Options Indexes FollowSymLinks MultiViews
213     AllowOverride All
214     Order allow,deny
215     allow from all
216 </Directory>
217
218 # SSL Protocol Adjustments:
219 # The safe and default but still SSL/TLS standard compliant shutdown
220 # approach is that mod_ssl sends the close notify alert but doesn't wait for
221 # the close notify alert from client. When you need a different shutdown
222 # approach you can use the following directives:
```

V step (VERIFICA DEL LAVORO SVOLTO E RIAVVIO XAMPP)

Da Start → esegui cmd come amministratore. Posizionati in **G:\xampp\apache\bin** ed esegui il comando **httpd -t**

Se è visualizzato “Syntax OK” il codice non ha errori.

Riavvia i servizi di XAMPP e controlla digitando <https://localhost> se il server risponde in maniera positiva.