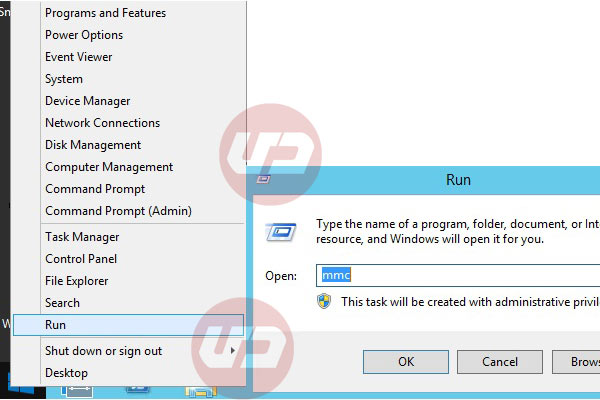
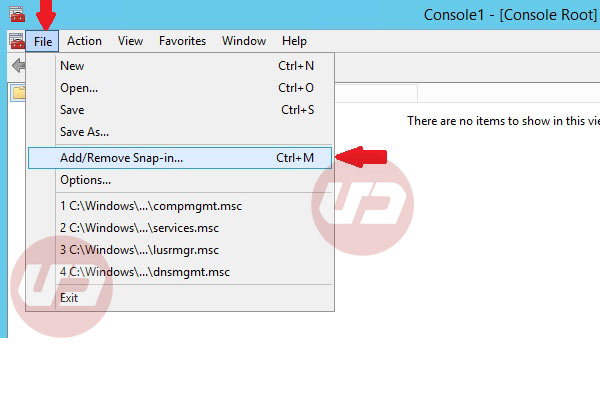
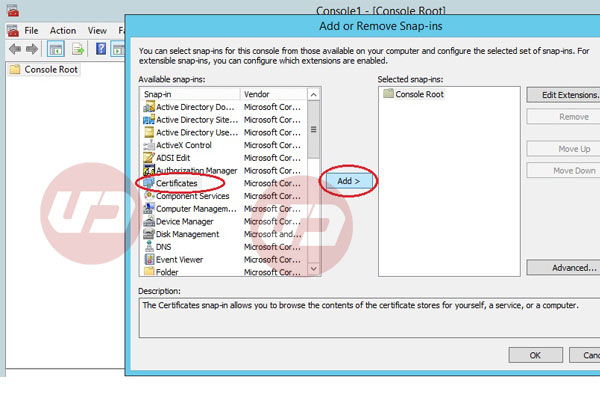
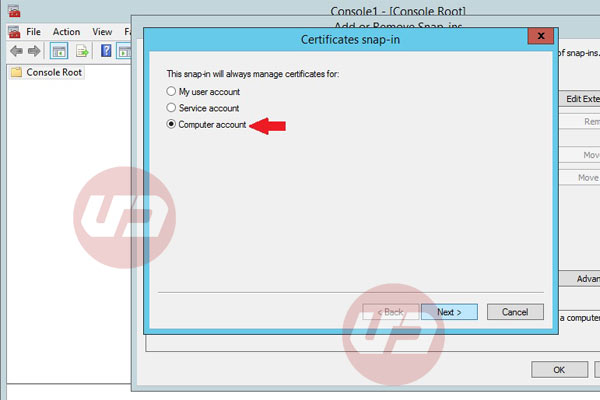
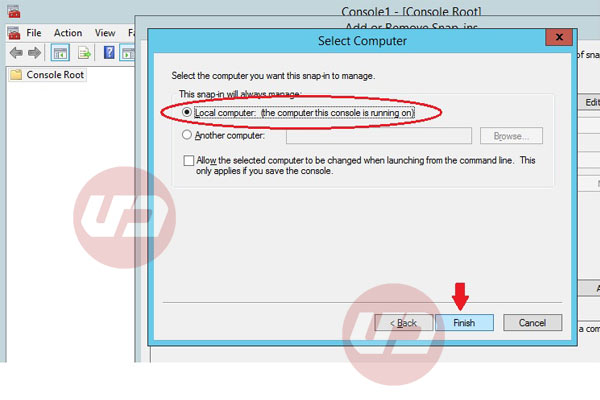
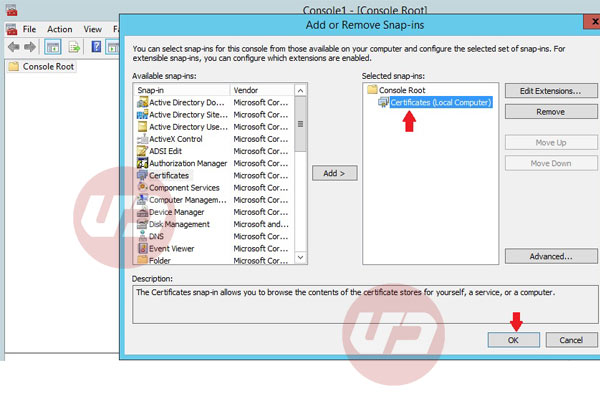
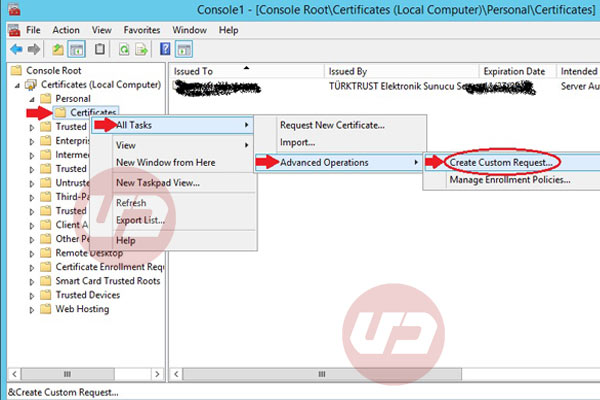
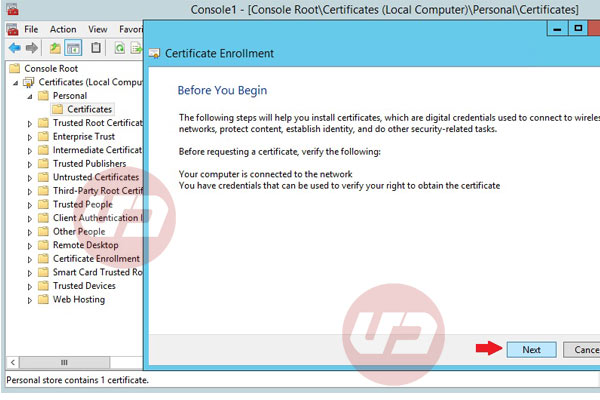
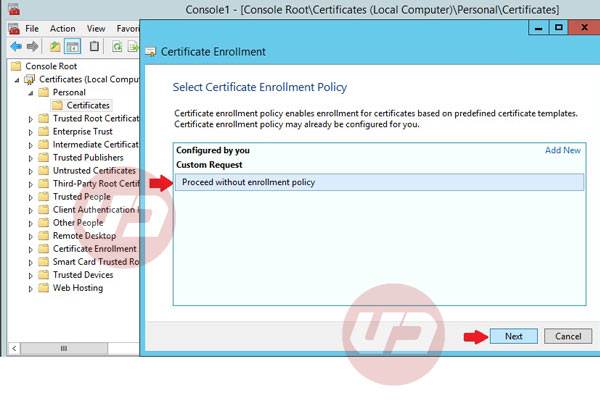
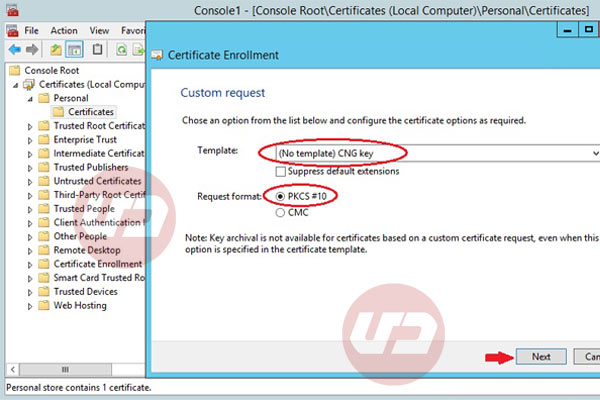
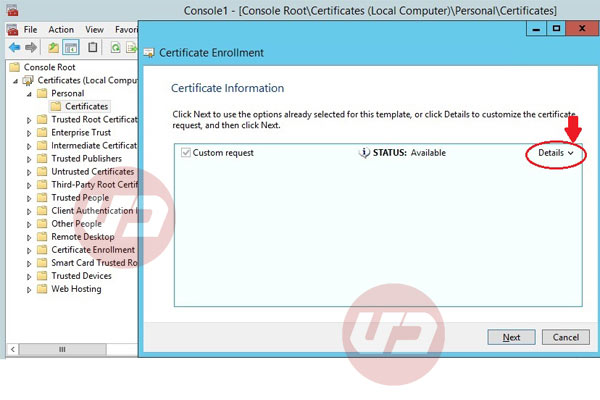
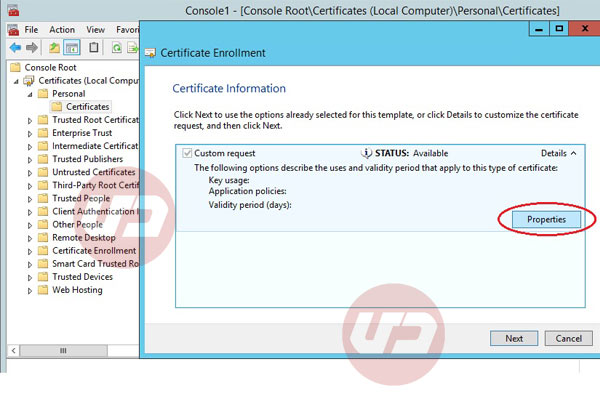
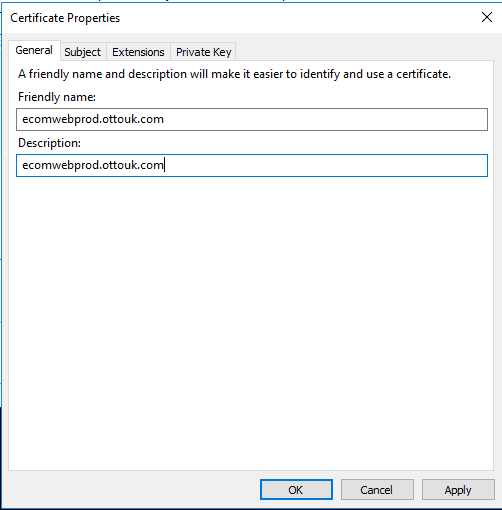
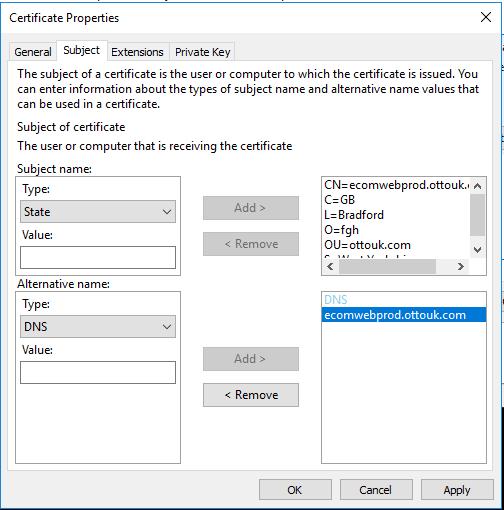
Create Certificate request SHA256

To start:  
  
RUN > MMC > FIle> Add Remove Snap -In... > Certificates > Add  
(This screen shots are from windows server 2012 R2 but win 2003 and 2008 have same steps)  
  
  
Type MMC on RUN  
  
  
From File> Add/Remove Snap-in...  
  
  
  
Select Certificates from left panel and click Add button  
  
  
  
By click on Add button Certificate Snap-in window will pop-up. Select Computer account > Next  
  
  
In Select Computer window select Local Computer(the computer this console is running on) >Finish  
  
  
  
in Add or Remove Snap-ins window select added Certificates snap-in and press OK.  
  
  
  
Under Console Root select Personal> Certificates(right click)> All Tasks> Advanced Operations> Create custom request...  
  
  
  
  
In Certificate Enrollment window select Next  
  
  
  
Select Proceed without enrollment policy on Select Certificate Enrollment Policy page> Next  
  
  
  
in Custom request windows select (No Template)CNG key and PKCS#10 format and select Next  
  
  
  
In Certificate Information page select Details to expand box  
  
  
  
After clicking Details properties will appear select it.  
  
  
  
  
In Certificate Properties > General tab for friendly name add domain you need SSL for that for example if you are creating CSR for www.day.ir type this on Description and friendly name.

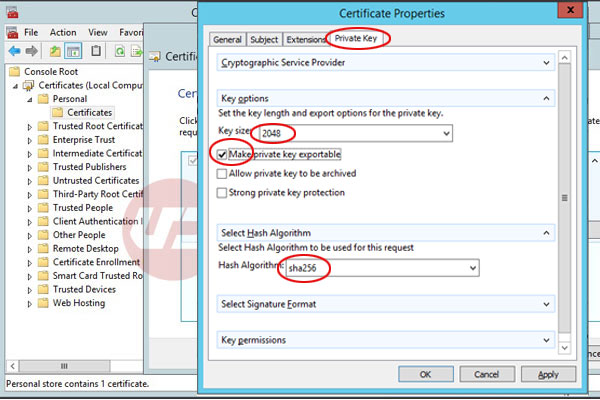
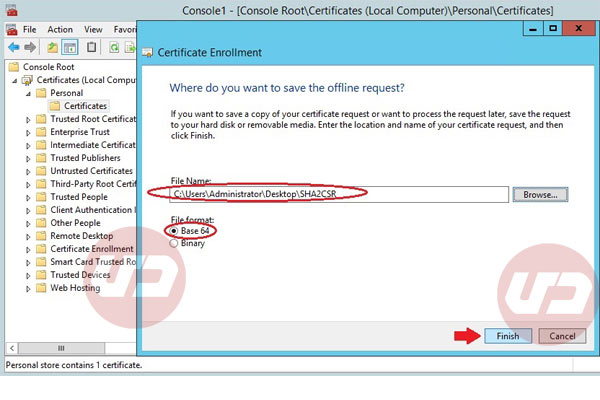
Add FQDN………. IE: ecomwebdev.ottouk.com  
  
  
  
  
In certificate properties Subject tab on Subject name from left panel under Type select the types your CA need from you. usually the item I introducing you are necessary, after selecting item should fill value and Add to right panel, the item you may need:  
Common name: CN is your domain name for example CN=ecomwebdev.ottouk.com  
Organization: O is your company name: for example O=fgh  
Organization Unit OU is name of unit in your company that related to SSL for example: OU= ottouk  
Locality: L your city for example L=Bradford  
State: S your State in your country for example: S=West Yorkshire  
Country: C for example C=GB

# Wildcard Certificate

Friendly Name = \*.ottouk.com

For a Wildcard certificate CN=\*.ottouk.com

No Alternate name needed.

SAN  
You cal also have **SAN** Subject Alternative Name if your  issuer CA support it.for example if you don't add www on Alternative Name your SSL will not cover https://www.yourdomain.com and it will just use for http://yourdomain.com  
  
  
This part is why we are here, in Private Key tab select Key Options and change **Key size** to **2048** or bigger.On Select Hash Algorithm change **Hash Algorithm** to **sha256** click OK and Next.  
Selecting **Make private key exportable** will help to backup installed certificate in future for move to new server or any problem  
  
  
  
Where do you want to save the offline request? select destination and from file format select Base 64> **Finish**.  
Now you can check your CSR on:   
<https://ssltools.digicert.com/checker/views/csrCheck.jsp>