Solution ID : **SO29005**

Last Modified : **05/02/2018**

WSS

Code Signing Certificate Signing Request (CSR) Generation Instructions via MMC certificate snap-in using Microsoft Windows

Solution

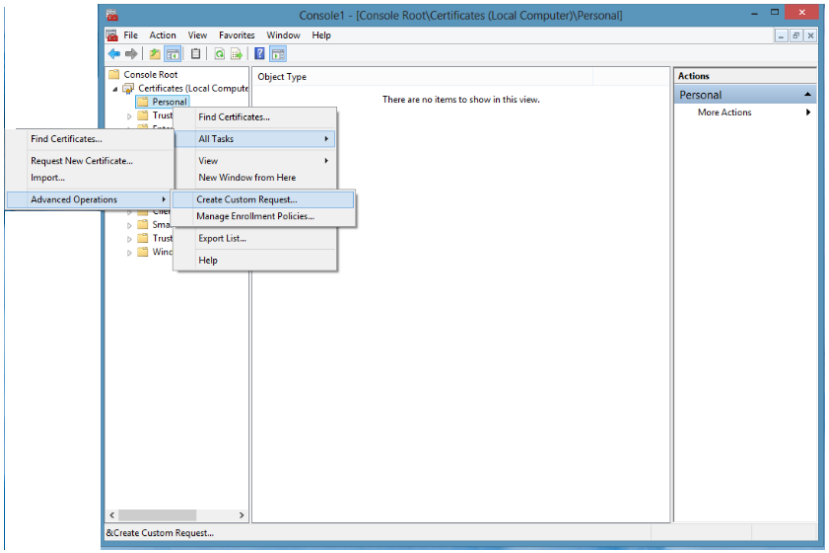
This document provides instructions for generating a Certificate Signing Request (CSR) on Microsoft Windows using the MMC console. If you are unable to follow these steps, Symantec recommends that you contact Microsoft Support.

Note: To generate a CSR, you will need to create a key pair for your windows computer. These two items are a digital certificate key pair and cannot be separated. If you lose your

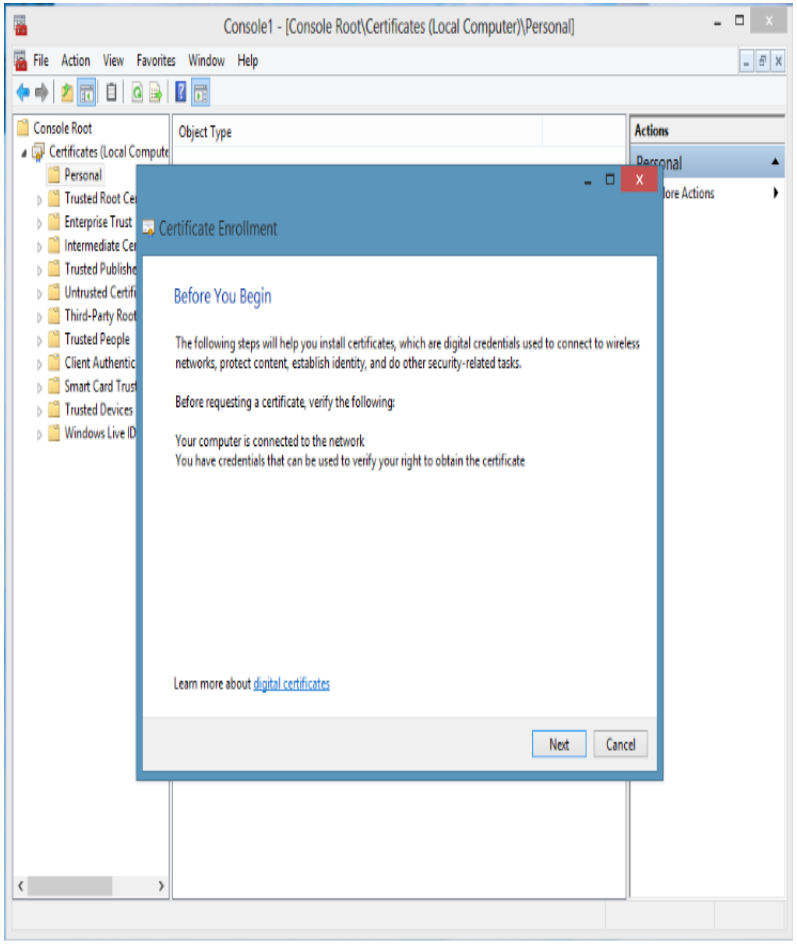
public/private key file and generate a new one, your code signing certificate will no longer match. You will have to replace the certificate then.

To generate a Certificate Signing Request (CSR) via a MMC certificate snap-in using Microsoft Windows, perform the following steps.

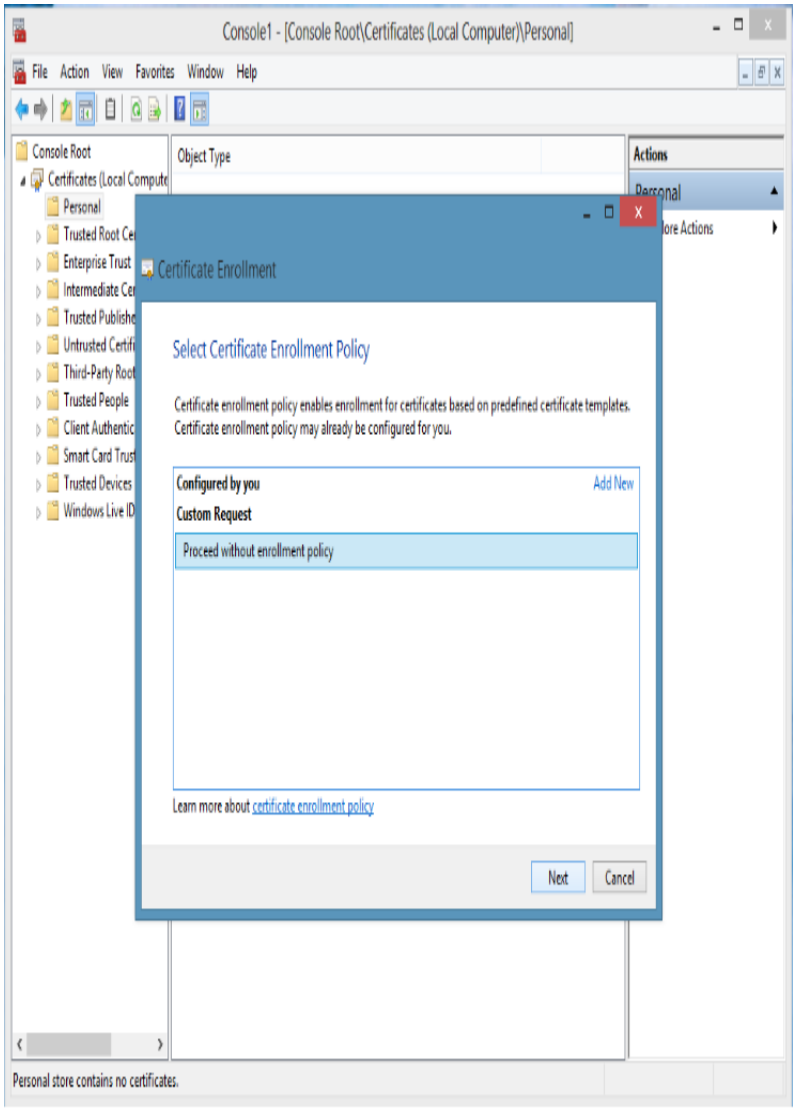
1. From Microsoft Windows, click **Start.**
2. In the Search programs and files field, type **mmc.**
3. Click **File** > **Add/Remove Snap-in.**
4. From the list of available snap-ins, select **Certificates.**
5. Click **Add.**
6. Select **Computer account.**
7. Click **Next.**
8. Select **Local computer** (the computer this console is running on).
9. Click **Finish.**
10. In the Add/Remove Snap-in window, click **OK.**
11. Save these console settings for future use.
12. Access your MMC snap in > right click the **Personal** folder.
13. Select **All Tasks** > **Advanced Operations** > **Create Custom Request.**


Console1 - [Console Root\Certificates (Local Computer)\Personal]
File Action View Favorites Window Help
Console Root
Certificates (Local Compute
Personal
Object Type
There are no items to show in this view.
Actions
Personal
More Actions
Find Certificates...
All Tasks
View
New Window from Here
Export List...
Help
Request New Certificate...
Import...
Advanced Operations
Create Custom Request...
Manage Enrollment Policies...
&Create Custom Request...

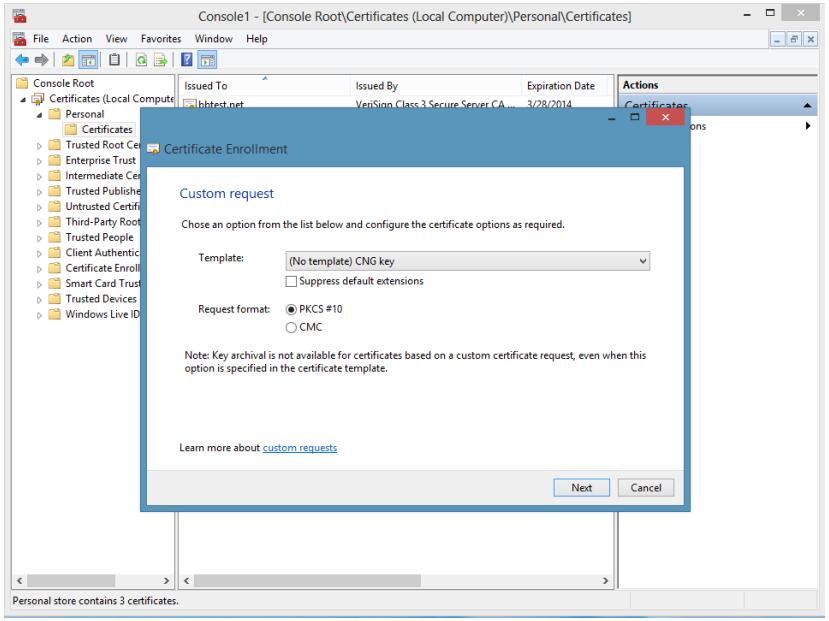
14. The CSR generation wizard will open > Click **Next.**



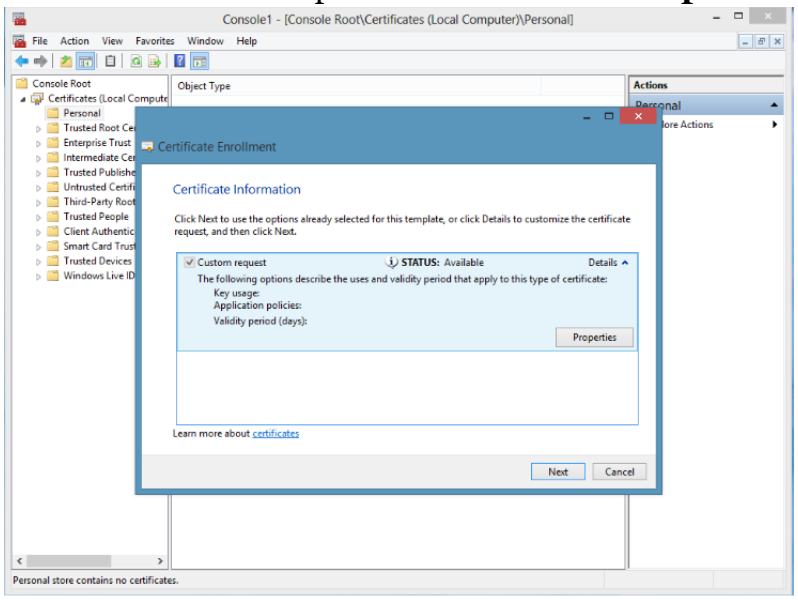
15. Select the option to **Proceed without enrollment policy** > Click **Next.**


Console1 - [Console Root\Certificates (Local Computer)\Personal]
File Action View Favorites Window Help
Console Root
Certificates (Local Compute
Personal
Trusted Root Ce
Enterprise Trust
Intermediate Ce
Trusted Publishe
Untrusted Certif
Third-Party Root
Trusted People
Client Authentic
Smart Card Trust
Trusted Devices
Windows Live ID
Object Type
Actions
Personal
More Actions
Certificate Enrollment
Select Certificate Enrollment Policy
Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates.
Certificate enrollment policy may already be configured for you.
Configured by you
Add New
Custom Request
Proceed without enrollment policy
Learn more about certificate enrollment policy
Next
Cancel
Personal store contains no certificates.

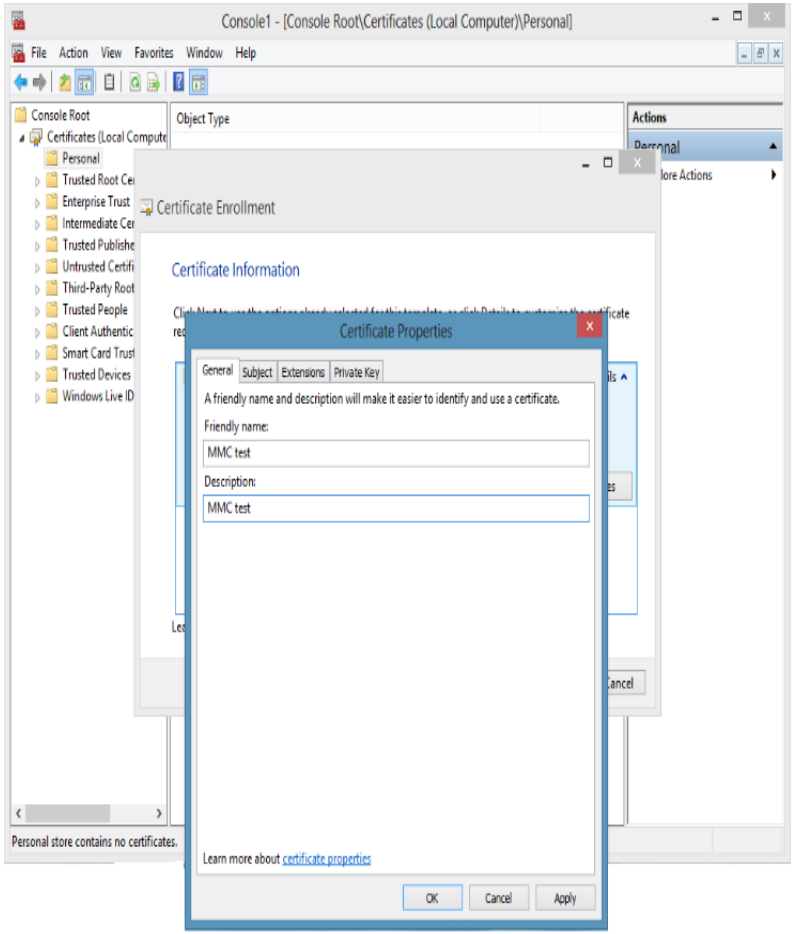
16. Click **Next** at the PKCS # 10 window.



17. From the **Details** drop down menu > Click **Properties.**



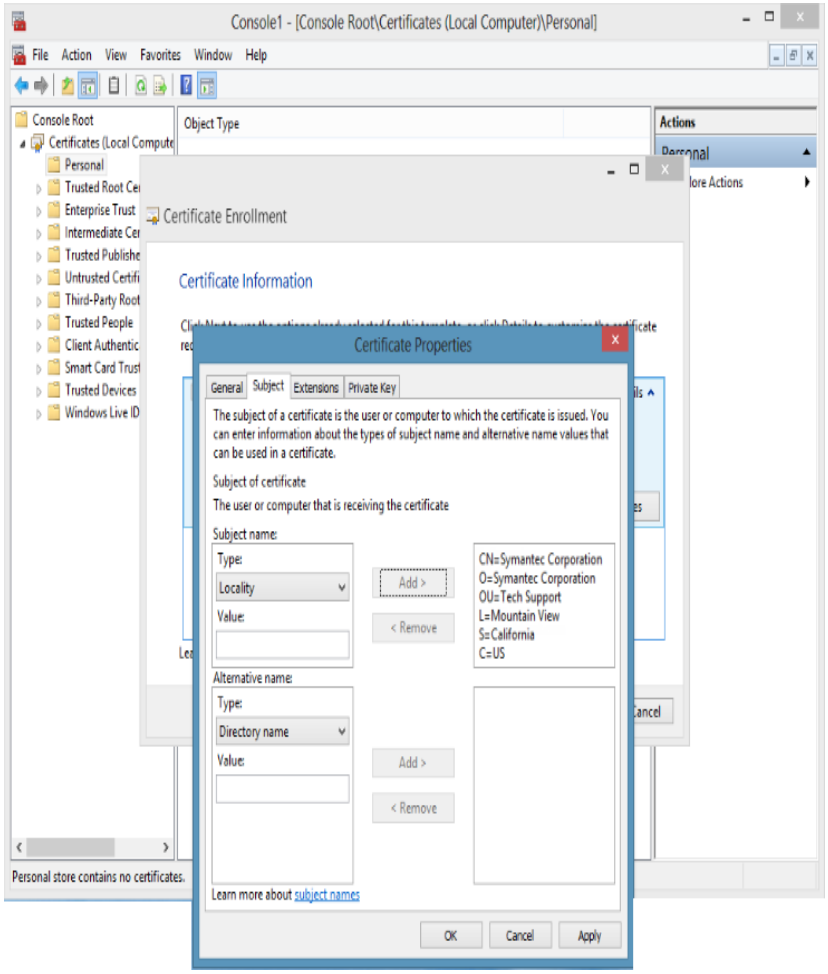
18. Enter a **Friendly Name** of your choosing.



19. Access the **Subject** tab > in the **Subject name: Type:** field add the following distinguish name values required for your CSR (**CN, O, OU, S, L and C**).

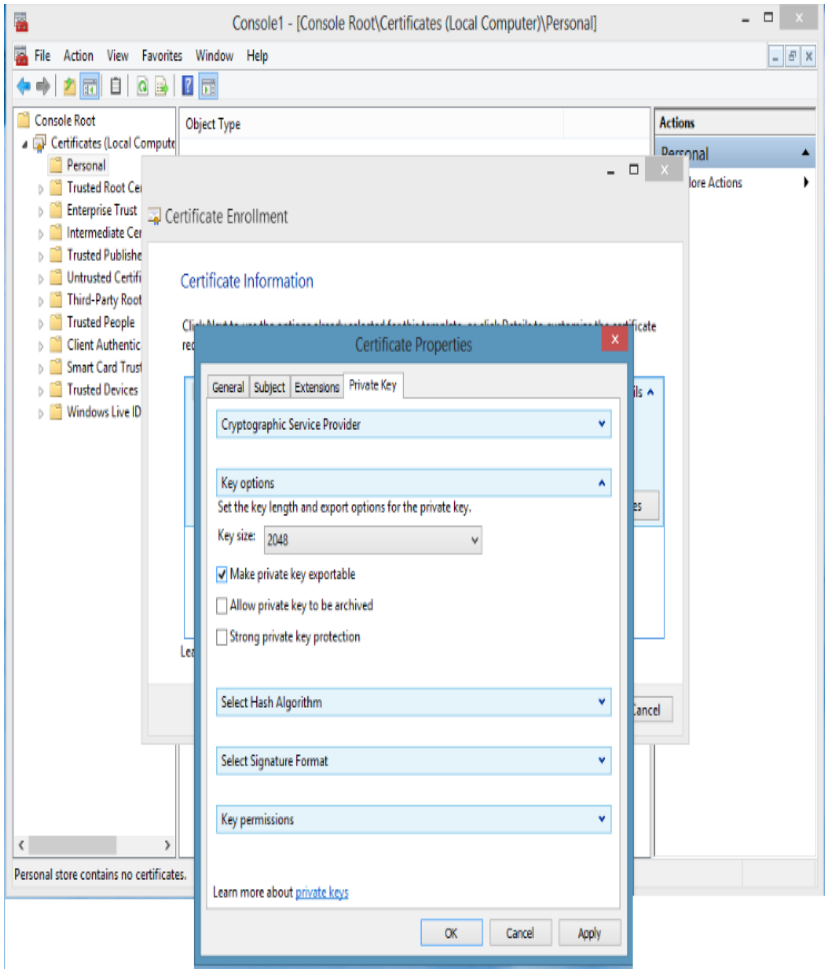
    Example:
    CN = **Common Name**: The registered organizational name that the certificate will be issued to and secure.
    O = **Organization**: The registered organizational name the certificate belongs to. If the company or department has an &, @, or any other symbol using the shift key in its name, the symbol must be spelled out or omitted, in order to enroll. For example: "XY & Z Corporation" would be

"XYZ Corporation" or "XY and Z Corporation".
OU = **Organizational Unit**: The department within the organization.
S = **State**: The business registered state or province. Do not abbreviate the state or province name, for example: California not CA.
L = **Locality**: The business registered location/city (not the actual server location).
C = **Country/region**: The two letter ISO country code.

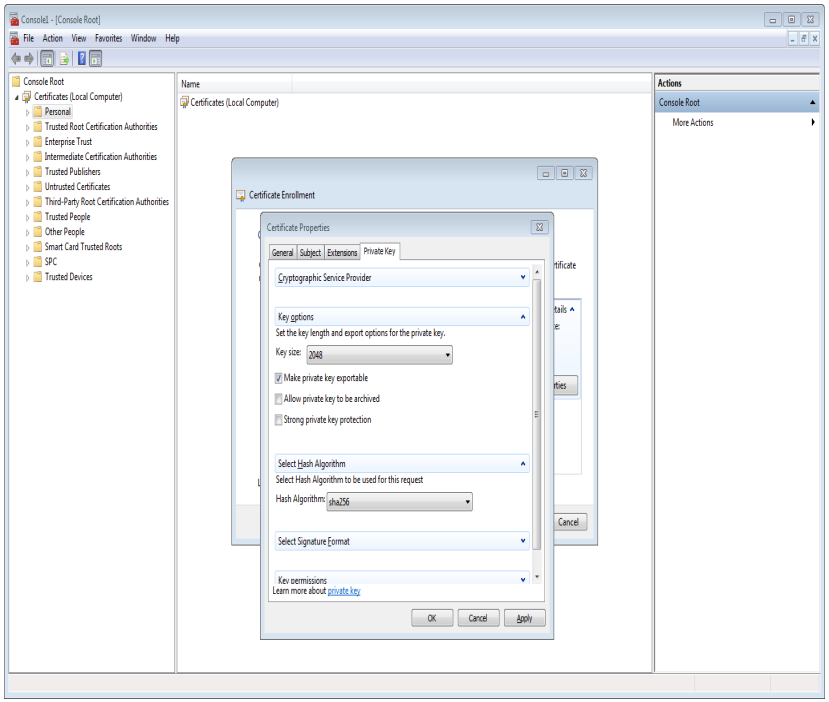


20. Click the **Private Key** tab > click the drop down for **Key options** > select **Key size: 2048** and check the option

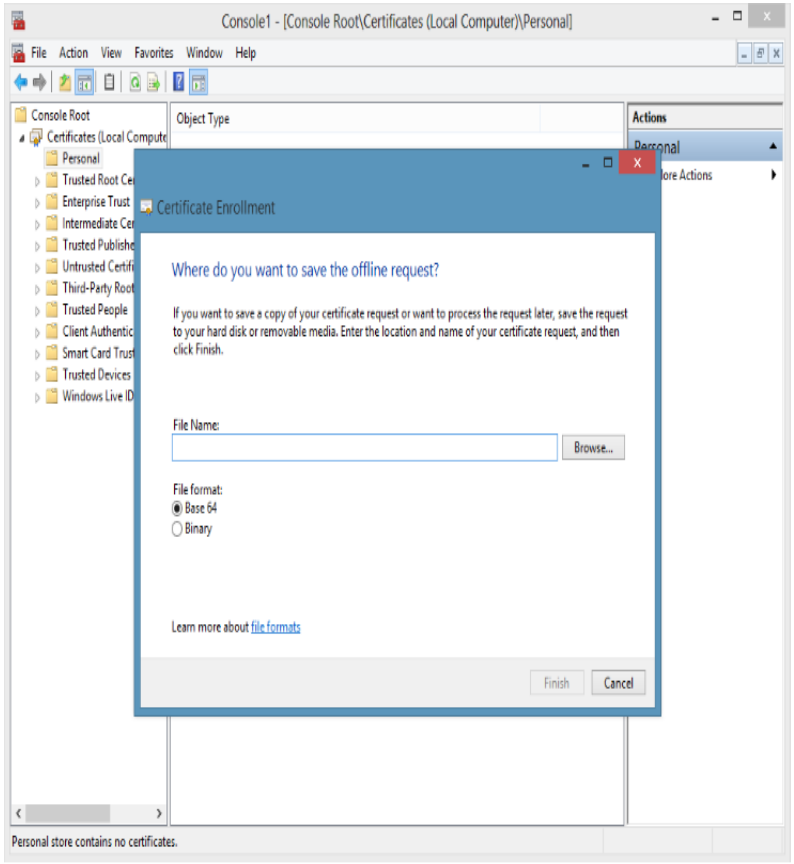
to **Make private key exportable** > Click **OK.**
Note: All code signing certificates must have a 2048 bit key size.



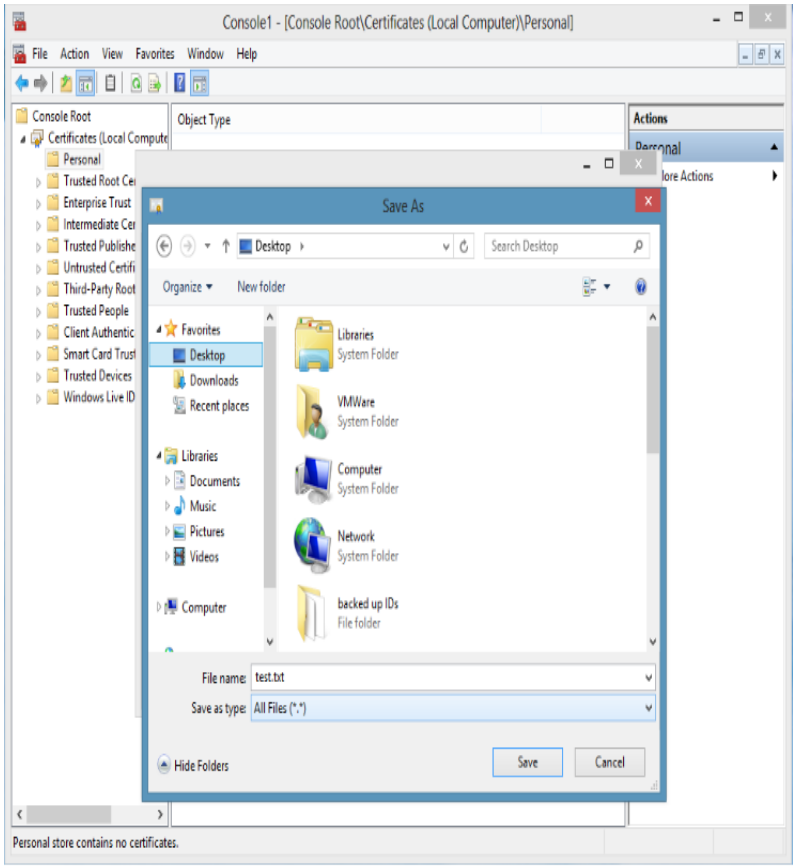
21. Click the drop down for **Select Hash Algorithm**, under Hash Algorithm select **sha256** > Click **OK**.


Console1 - [Console Root]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Other People
Smart Card Trusted Roots
SPC
Trusted Devices
Name
Certificates (Local Computer)
Actions
Console Root
More Actions
Certificate Enrollment
Certificate Properties
General Subject Extensions Private Key
Cryptographic Service Provider
Key options
Set the key length and export options for the private key.
Key size: 2048
Make private key exportable
Allow private key to be archived
Strong private key protection
Select Hash Algorithm
Select Hash Algorithm to be used for this request
Hash Algorithm: sha256
Select Signature Format
Key permissions
Learn more about private key
OK
Cancel
Apply
Cancel

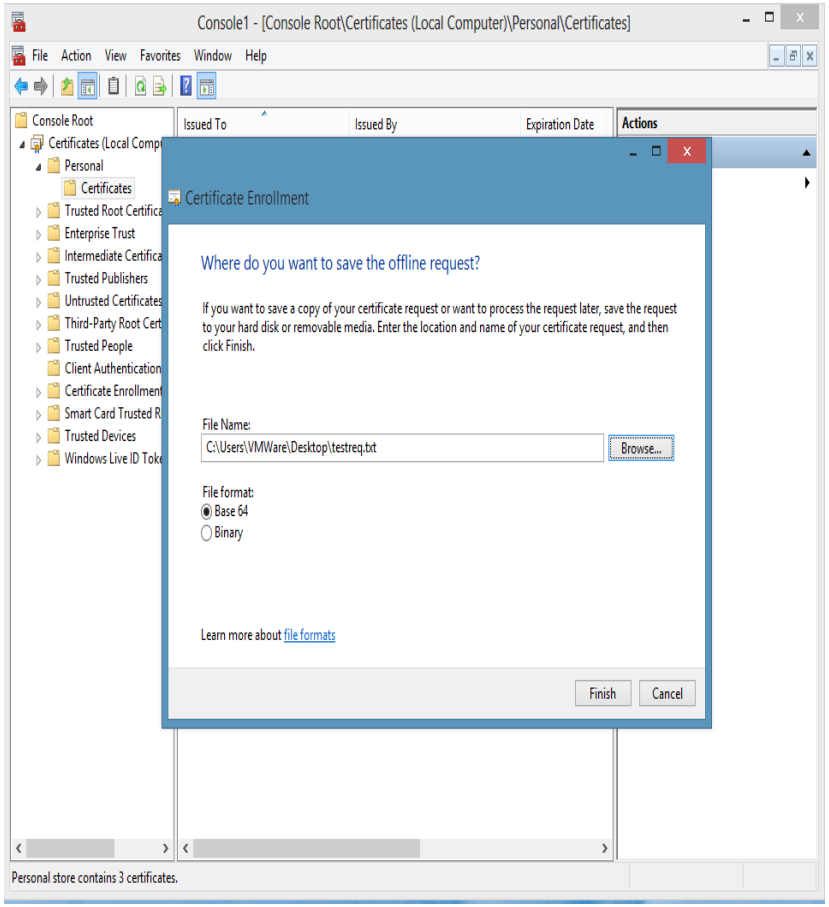
22. Click **Next** > Click **Browse.**



23. Select a location to save the CSR file. Enter a name for the file and click **Save.**


Console1 - [Console Root\Certificates (Local Computer)\Personal]
File Action View Favorites Window Help
Console Root
Certificates (Local Compute
Personal
Trusted Root Ce
Enterprise Trust
Intermediate Cer
Trusted Publishe
Untrusted Certifi
Third-Party Root
Trusted People
Client Authentic
Smart Card Trust
Trusted Devices
Windows Live ID
Object Type
Actions
Personal
lore Actions
Save As
Desktop
Search Desktop
Organize
New folder
Favorites
Desktop
Downloads
Recent places
Libraries
Documents
Music
Pictures
Videos
Computer
Libraries
System Folder
VMWare
System Folder
Computer
System Folder
Network
System Folder
backed up IDs
File folder
File name: test.txt
Save as type: All Files (*.*)
Hide Folders
Save
Cancel
Personal store contains no certificates.

24. Click **Finish.**



25. The CSR file will be present at the location you saved and can be used to request a code signing certificate.

To install a code signing certificate via MMC certificate snap-in using Microsoft Windows, click here (/content/digicertknowledgebase/en/us/solution/SO29171.html).