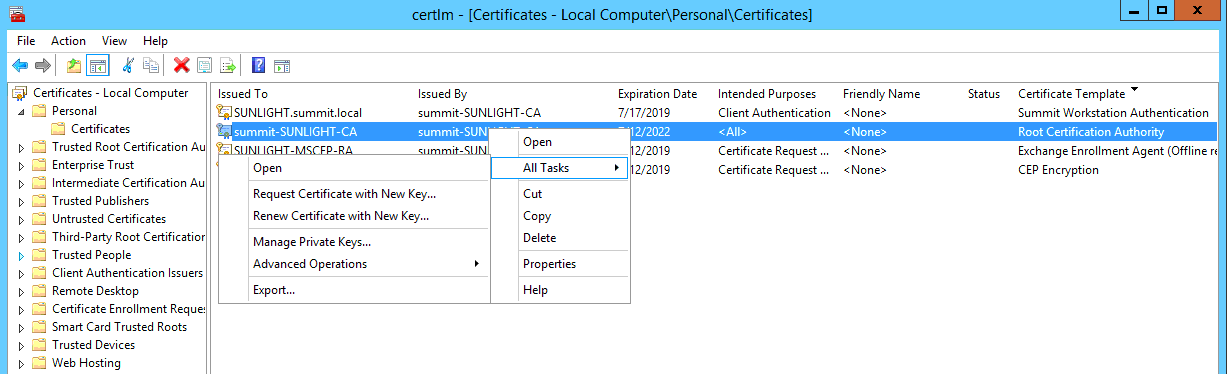
Summit VPN Certificate management.

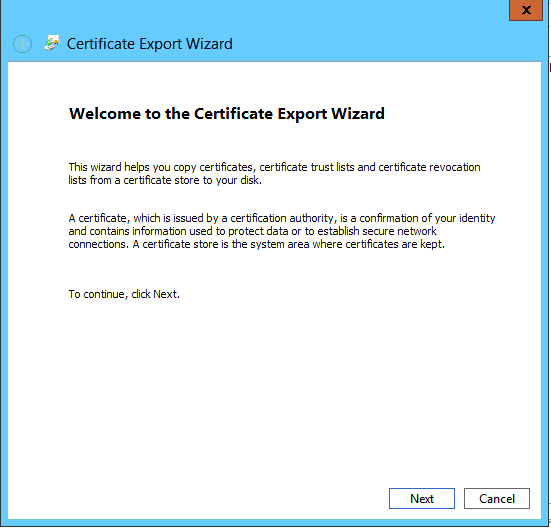
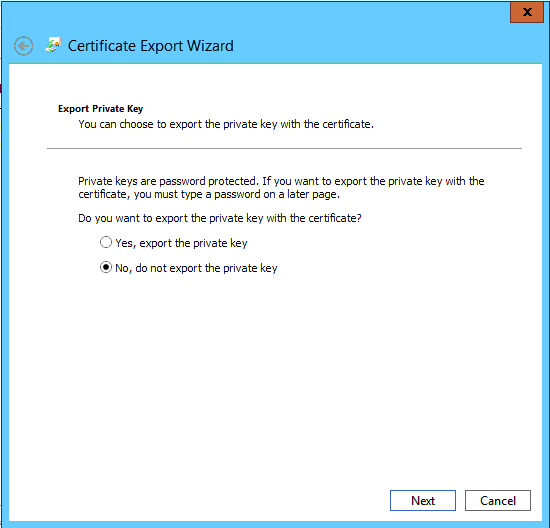
The Summit Anyconnect policy is configured to authenticate based on Certificate and Username/Password. Active Directory is the source for the username and password. Sunlight.summit.local is the server with the Certificate Authority role utilized for the certificates used for the VPN Authentication.

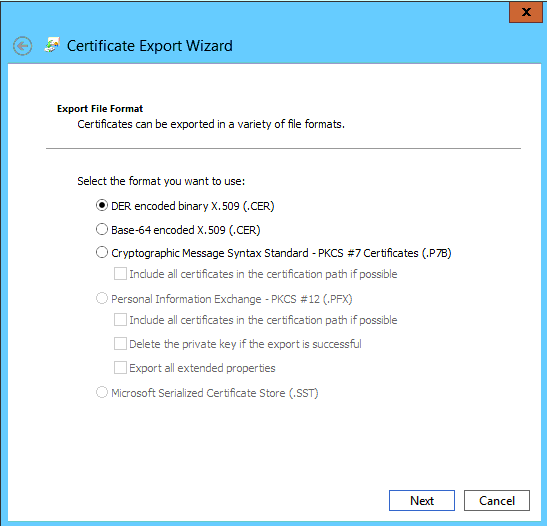
Certificates are automatically issued for workstations that are members of the domain by the current CA installed on Sunlight.summit.local.

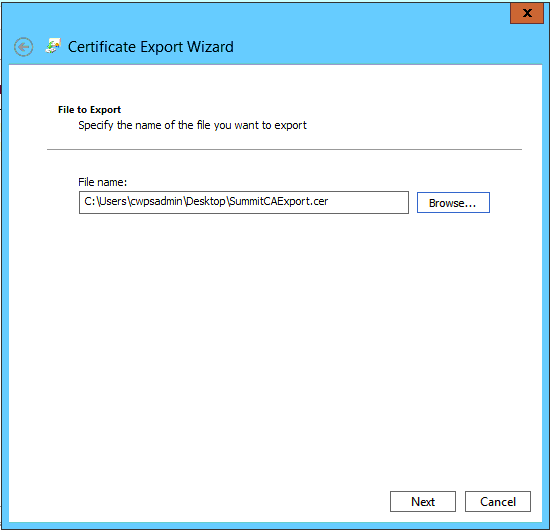
Clients will need both the CA certificate and an identity certificate signed by the CA installed in order to authenticate to the Anyconnect VPN policy.

The CA Certificate can be downloaded from the CA server for client installation.

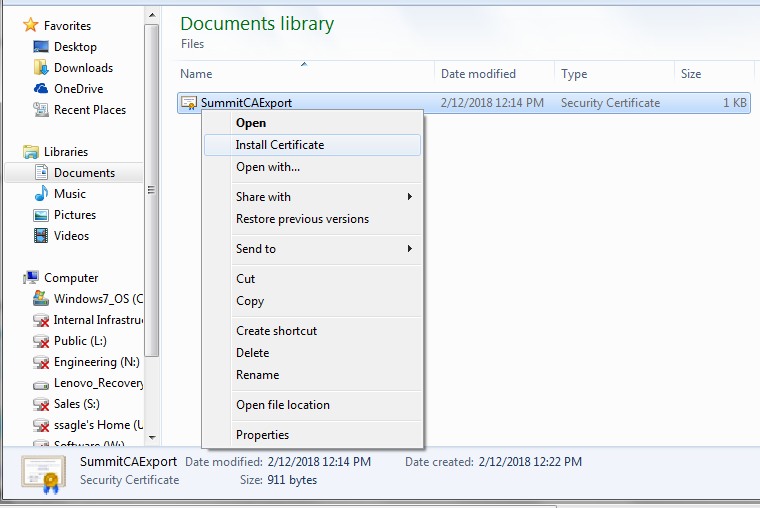
1. Connect to Sunlight and launch the Certification Authority MMC  
   
2. Navigate to Certificates > Personal > Certificates, highlight the summit-SUNLIGHT-CA certificate, right click > All Tasks > Export  
   

1. Click Next  
   
2. Select - No, do not export the private key and click next.  
   

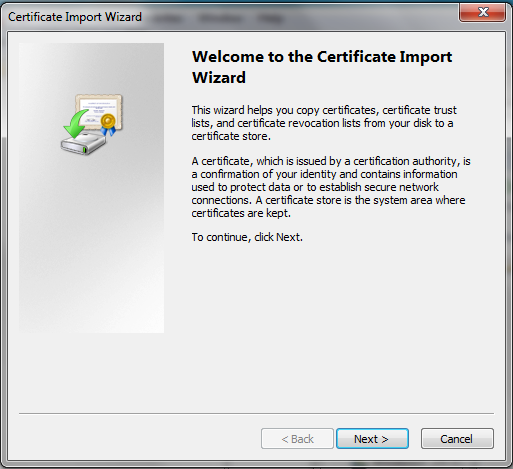
1. Select DER encoded binary X.509 (.CER) and click next  
   
2. Identify where to export the certificate and click Next then click Finish.

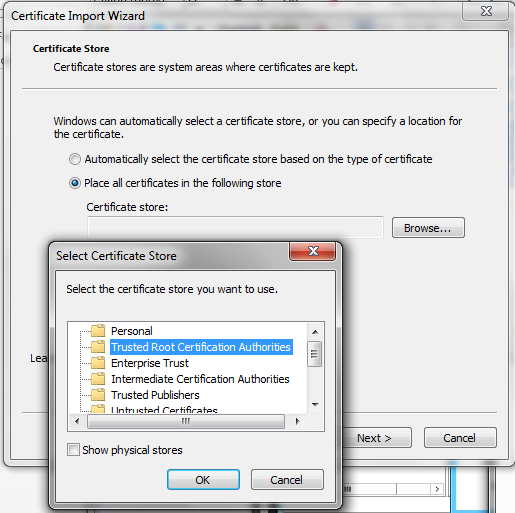


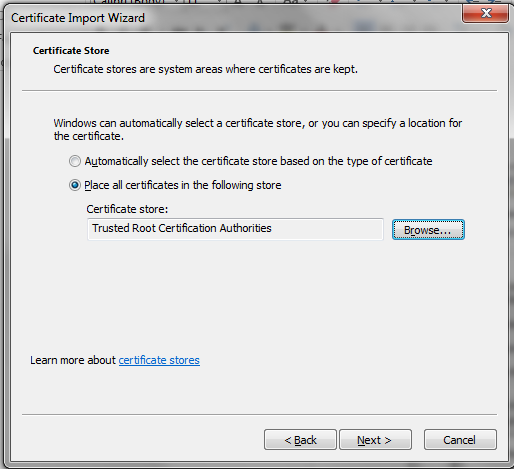
1. Copy the exported certificate to the workstation that needs access to the VPN.
2. Right click > Install Certificate



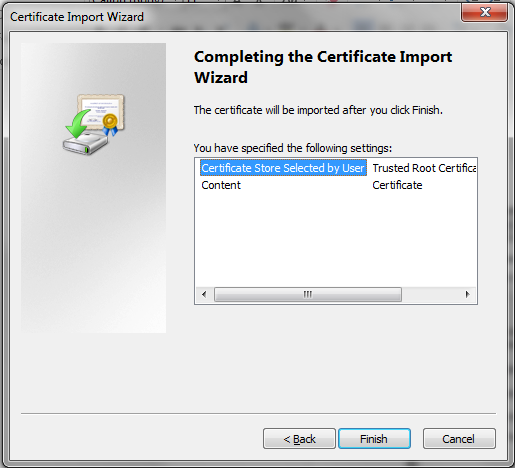
1. Click next



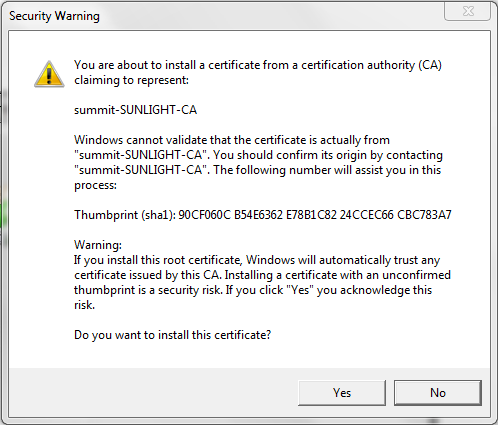
1. Select Place all certificates in the following store and click Browse. Select Trusted Root Certification Authorities and click OK
2. Click Next



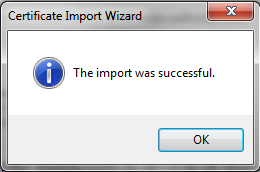
1. Click Finish



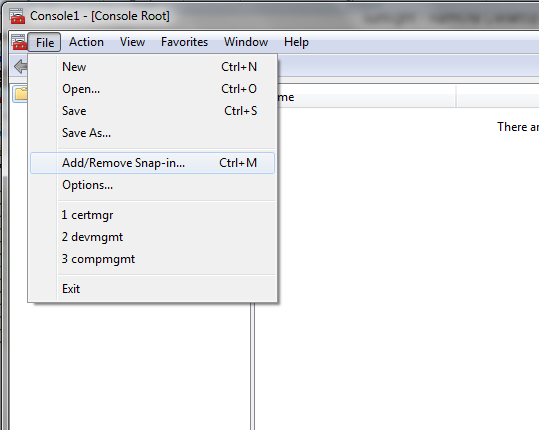
1. Click Yes



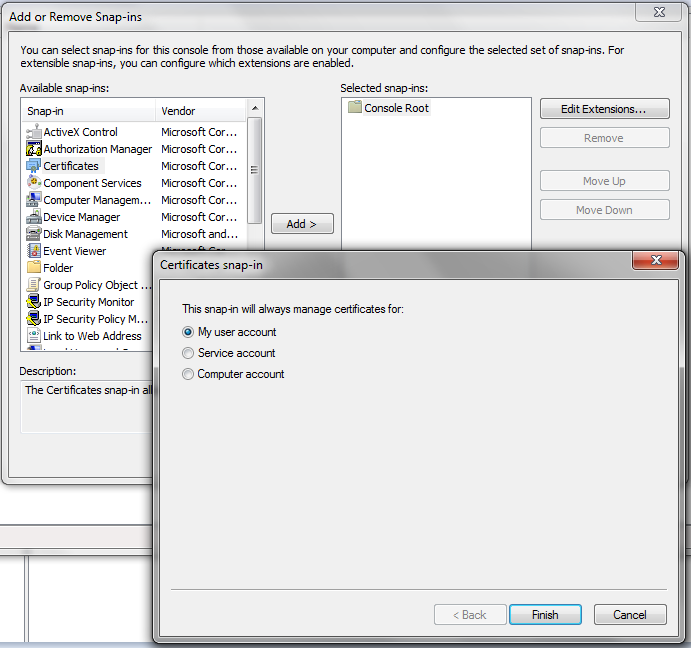
1. Click OK

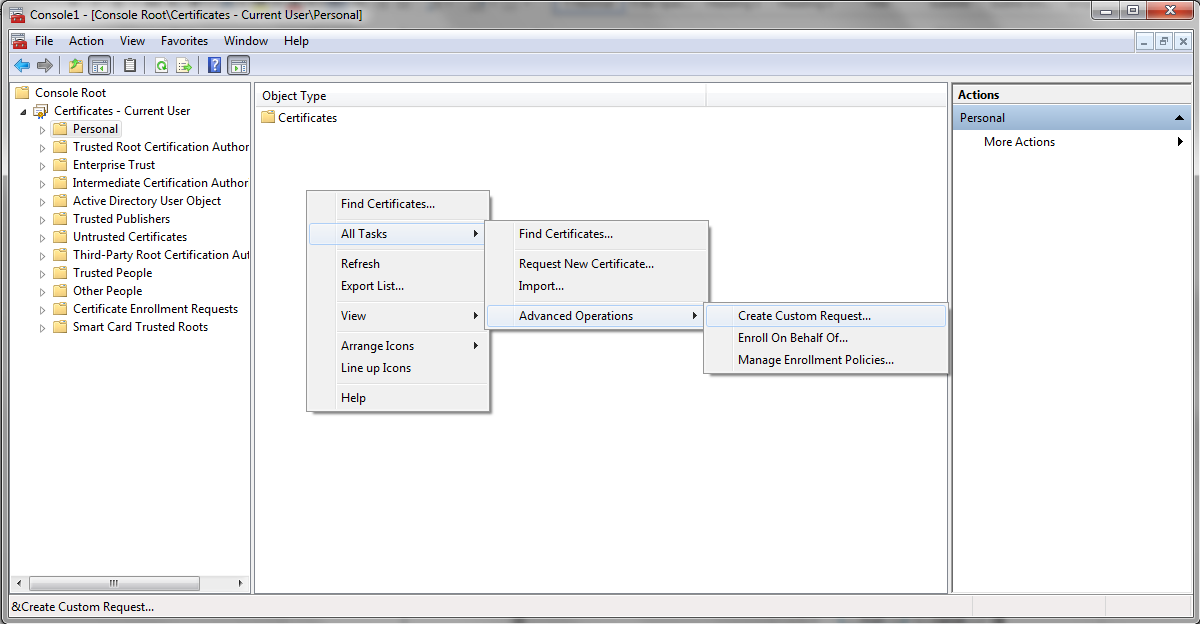


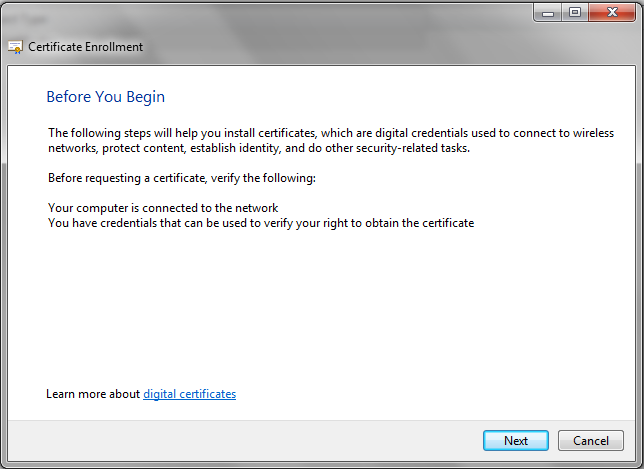
1. Create a CSR for the workstation. Launch MMC and select File Add/Remove Snap-in



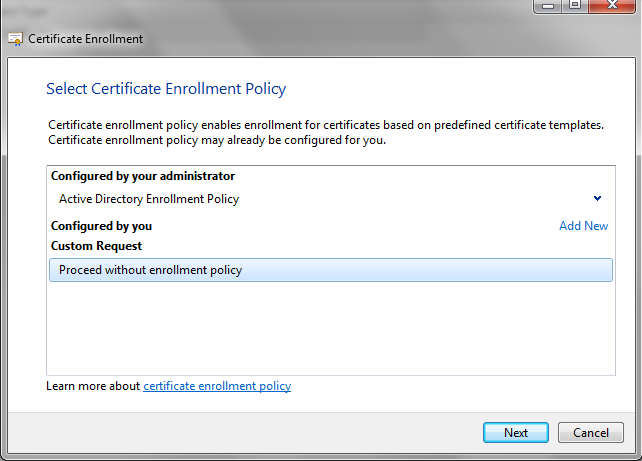
1. Select Certificates, click Add, Select My User Account and click Finish then OK

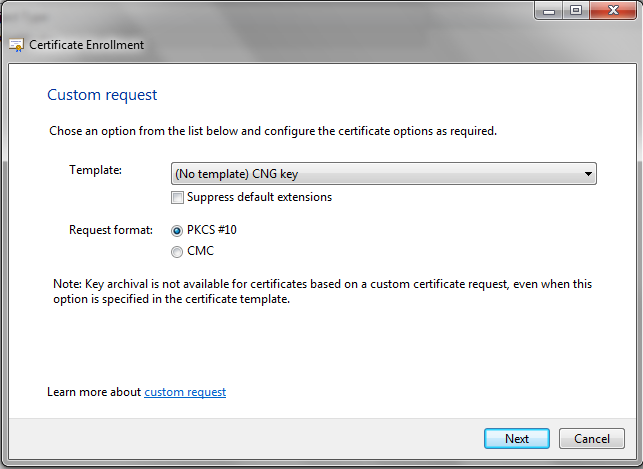


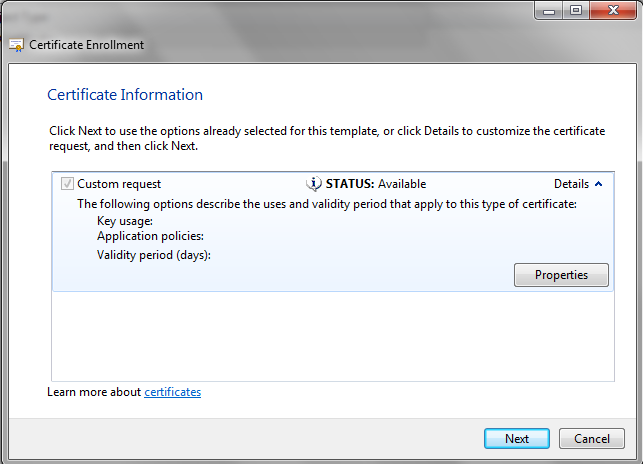
1. Select Personal, Right click the center pane, select All Tasks > Advanced Options > Create Custom Request
2. Click Next

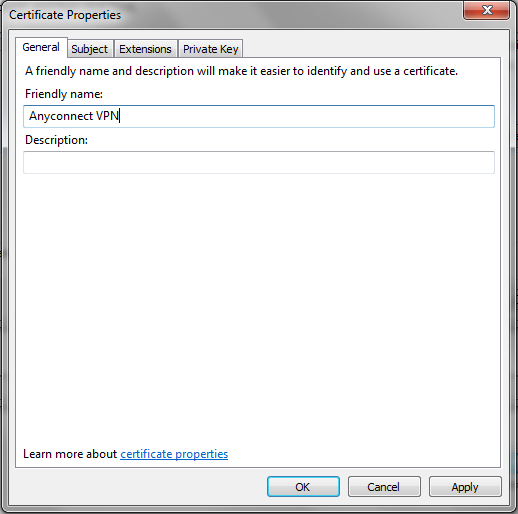


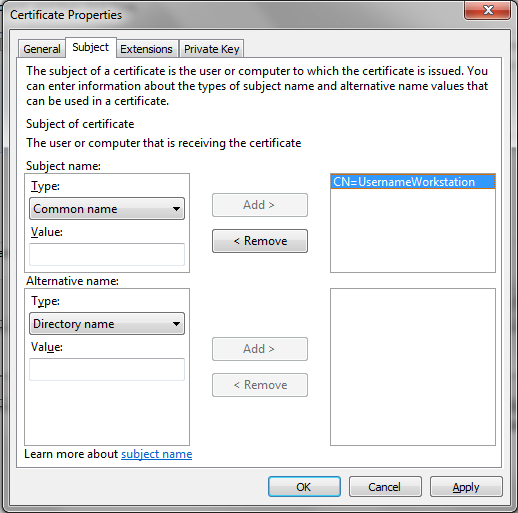
1. Select Proceed without enrollment policy and click Next.



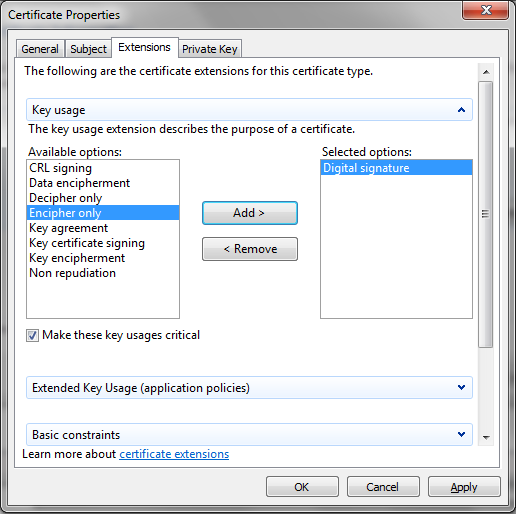
1. No template, PKCS #10 > Next
2. Expand Details and click Properties

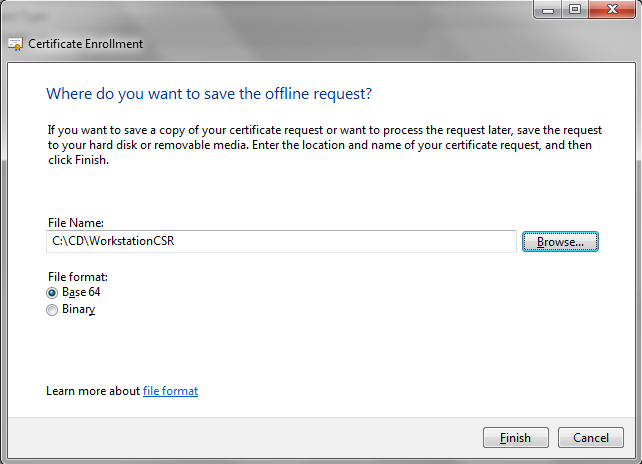


1. On the General Tab enter Friendly Name 
2. On the Subject Tab add a Common name and any additional identifying attributes for the client CSR.

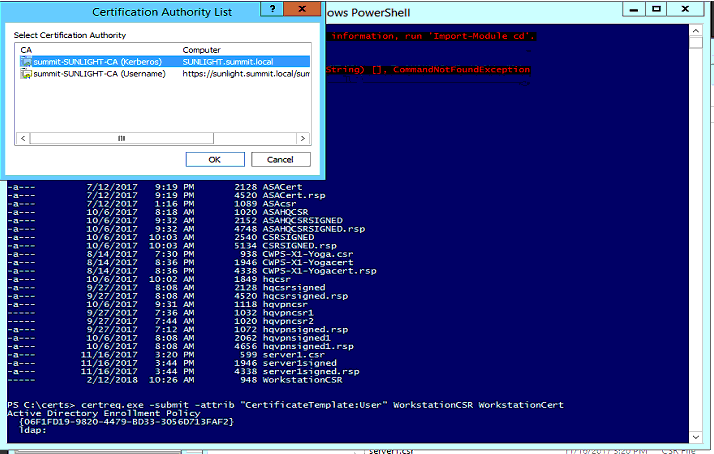


1. On the Extensions Tab, click the Key Usage option and add Digital Signature to the selected options.

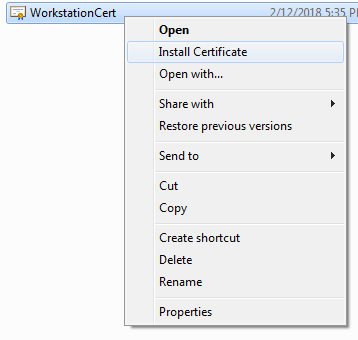


1. Click OK then Next. Select a location to save the CSR export and click Finish
2. Copy the CSR file to sunlight c:\certs
3. Sign the CSR in powershell with the certreq command

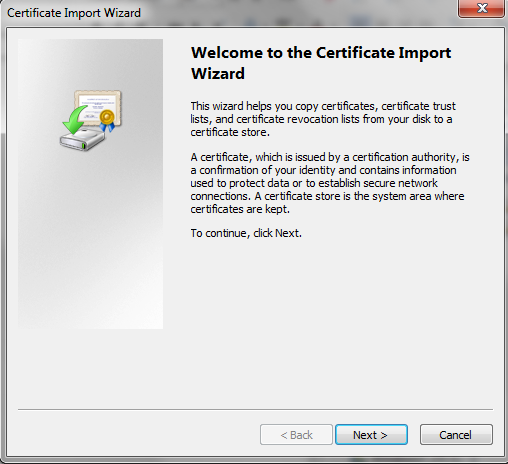
Ex: certreq.exe -submit -attrib "CertificateTemplate:User" WorkstationCSR WorkstationCert  
When prompted, highlight summit-SUNLIGHT-CA (Kerberos) and click OK



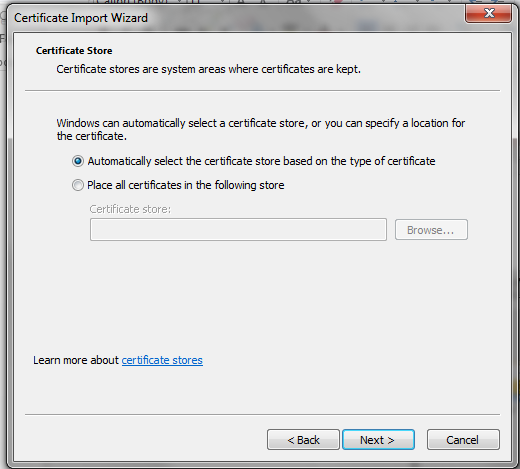
1. Copy WorkstationCert back to the user computer. On the workstation, Right click > Install Certificate



1. Click Next



1. Click Next



1. Click Finish and OK

