Resolving Windows Certificate Errors for Synopsys Products

Windows-based products signed by the Synopsys Sign utility require certain certificates. If these certificates are expired or missing, immediately after installation you will receive an error regarding the expired or missing certificates, and you will not be able to start the tool. (For Synopsys Common Licensing, you will not receive any installation error, but you will not be able to start the SCL / snpslmd vendor daemon.)

The information in this document will help you install the required certificates so that you may use your Synopsys products.

This document contains the following sections:

Required Certificates

Windows-based products (including SCL) signed by Synopsys require these certificates:

• Sectigo RSA Time Stamping
• USERTrust RSA Certification Authority
• UTN-USERFirst-Object
• VeriSign Class 3 Public Primary Certification Authority - G5
• VeriSign Universal Root Certification Authority

Downloading the Required Certificates

To resolve any certificate errors regarding missing or expired certificates, you must download and install / update the required certificates. These certificates may be obtained from the links below:

• Sectigo RSA Time Stamping:
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt

• USERTrust RSA:
http://www.tbs-x509.com/USERTrustRSACertificationAuthority.crt

• UTN-USERFirst-Object (Comodo):
https://support.comodo.com/index.php?/comodo/Knowledgebase/Article/View/961/0/kmcs-utn-userfirst-object

• VeriSign (DigiCert) certificates:
https://www.websecurity.digicert.com/theme/roots

IMPORTANT: These security certificates must be installed **only** as trusted root certificates.

NOTE: For the Verisign certificates, do **NOT** click or double-click the download links at the DigiCert page. Instead, right-click the desired "Root Download Link:" and choose "Save Link As" as or "Save Target As", then click Save to download the *.pem file to your download directory.

Installing the Required Certificates

1. If you have downloaded Verisign (DigiCert) certificates, rename the downloaded *.pem files to be *.cer files. Right-click each *.pem file, choose Rename, then give the file a **.cer** extension. For example, "VeriSign-Universal-Root-Certification-Authority.**cer**".)

2. Right-Click a downloaded certificate and choose either **Install Certificate > Open** or **Install CRL**. The Certificate Import Wizard will start.

3. Click Next, then Click Install Certificate.

4. Under Store Location, choose Local Machine, then click Next.

5. Choose Place All Certificates in the following Store.

6. Under Certificate Store:, click Browse.

7. Choose Trusted Root Certification Authorities and click OK.

8. Click Next. Verify that the Trusted Root Certification Authorities store is selected and click Finish.

9. You will see a message that the Import was successful; click OK.

10. Repeat steps 2 through 10 if you have additional certificates to install.

11. After you are finished installing the missing certificates, start your tool; it should start normally. (You may need to set SNPSLMD_LICENSE_FILE.)

12. If this machine is an SCL license server machine, run *whatscl.exe --check-cert* from the command line, to make sure the certificates are properly installed:

C:\Synopsys\SCL\2018.06-SP1\win32\bin> **whatscl.exe --check-cert**

Deleting Expired Certificates

This procedure is only required if, after installing the required certificates, the Windows tool continues to give you the message that a certificate is expired. To delete expired certificates:

1. Click Start and type "MMC".

2. Click MMC to open the Microsoft Management Console (MMC).

3. Click File > Add / Remove Snap In.

4. Under "Available Snap-Ins:", double-click Certificates.

5. Select Computer Account and click Next.

6. Select Local Computer > Finish.

7. At the bottom of the screen, click OK to exit the Snap-In window.

8. Under Console Root, expand the Certificates list by clicking ">".

9. Click Trusted Root Certificates > Certificates.

10. Locate and select the expired certificate you wish to **delete**. (For example, you might select an expired UTN-USERFirst-Object certificate.)

11. Click Action > Delete, then select **Yes** to delete the expired certificate.

Exporting Certificates

If the Windows machine where the tool (or SCL server) is installed does not have access to the Internet, you can export the required certificates from another machine with Internet access. To export one or more installed certificates:

1. Login to the machine that has the certificates installed.

2. Click Start and type “MMC”.

3. Click MMC to open the Microsoft Management Console (MMC).

4. Click File > Add / Remove Snap In.

5. Under "Available Snap-Ins:", double-click Certificates.

6. Select Computer Account and click Next.

7. Select Local Computer > Finish.

8. At the bottom of the screen, click OK to exit the Snap-In window.

9. Under Console Root, expand the Certificates list by clicking ">".

10. Click Trusted Root Certificates > Certificates.

11. Locate and select the certificate(s) you wish to export.
(Press and hold down the Ctrl key to select more than one certificate.)

12. Click Action > All Tasks > Export to start the Certificate Export Wizard.

13. Click Next.

14. If you have chosen to export one certificate,
choose "DER encoded binary X.509 (.CER)", then click Next and go to step 16.

15. If you have chosen to export multiple certificates, choose
"Personal Information Exchange - *PKCS* #12 (.PFX)",
then click Next. a. For PFX export files, security is required.

b. Choose "Group or User names (recommended)" -OR-
choose "Password:" and type and confirm your password.

c. Click Next.

16. In the File to Export screen, click Browse.

17. Choose the folder and filename and then click Save. Do **NOT** type any extension.

18. Click Next, then click Finish.

19. Click OK when you see the dialog that the export was successful.

20. If needed, transfer the saved file to a shared folder or to a USB stick.

21. To transfer the exported certificate file to another machine, follow the procedure under Importing Certificates (see next section).

Importing Certificates

1. Login to the machine that is missing the certificates.

2. Click Start and type “MMC”.

3. Click MMC to open the Microsoft Management Console (MMC).

4. Click File > Add / Remove Snap In.

5. Under "Available Snap-Ins:", double-click Certificates.

6. Select Computer Account and click Next.

7. Select Local Computer > Finish.

8. At the bottom of the screen, click OK to exit the Snap-In window.

9. Under Console Root, expand the Certificates list by clicking ">".

10. Click Trusted Root Certificates > Certificates.

11. Click Action > All Tasks > Import to start the Certificate Import Wizard.

12. Click Next.

13. To the right of File Name, click Browse to access the shared (exported) certificate file.

a. To import a single *.cer file, browse to and select the *.cer or *.crt file.

b. To import a *.pfx file, click the Down Arrow to the right of File name and choose "Personal Information Exchange (*.pfx; *.p12)".

14. Click Open, then Click Next.

15. If requested, enter the password and click Next.

16. Under "Certificate store:", verify Trusted Root Certification Authorities is chosen. (If not, click Browse to choose this option.)

17. Click Next, then click Finish.

18. Click OK when you see the dialog that the export was successful.

19. After you are finished importing (installing) the missing certificates, start your Synopsys tool. Providing it can get a license (you may need to set SNPSLMD_LICENSE_FILE), the tool should start normally, with no certificate error.

20. For an SCL license server machine (only) rerun *whatscl.exe --check-cert* to make sure the certificates are properly installed.

Updated February 4, 2021