Blue Pearl Software

Installing VVS without Automatic Root Certificate Updates

Introduction

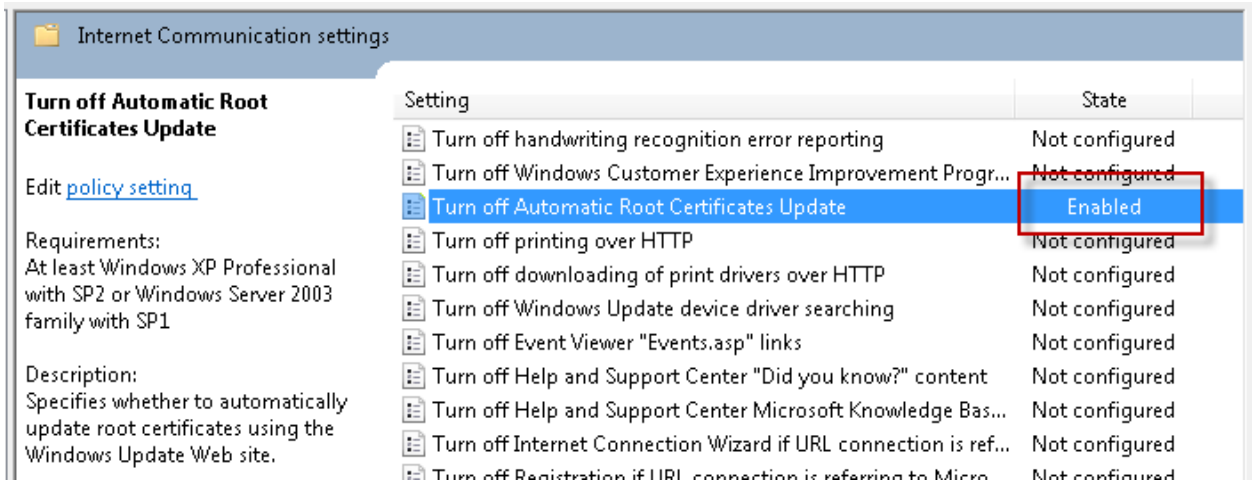
Some new users of Blue Pearl Software's **Visual Verification Suite** (VVS) working in environments with enhanced security configurations have encountered an issue with root certificate importation during installation. This paper provides a solution to that issue.

What are Certification Authorities and certificates?

A *Certification Authority* (or CA) is a third party that has been entitled to verify that someone is who they say they are. It does this by issuing *certificates* containing a digital signature. The authority must be trusted by both the subject (owner) of the certificate and the party relying upon the certificate. Such certificates are used within Windows installation software to verify that the installed programs come from reputable sources.

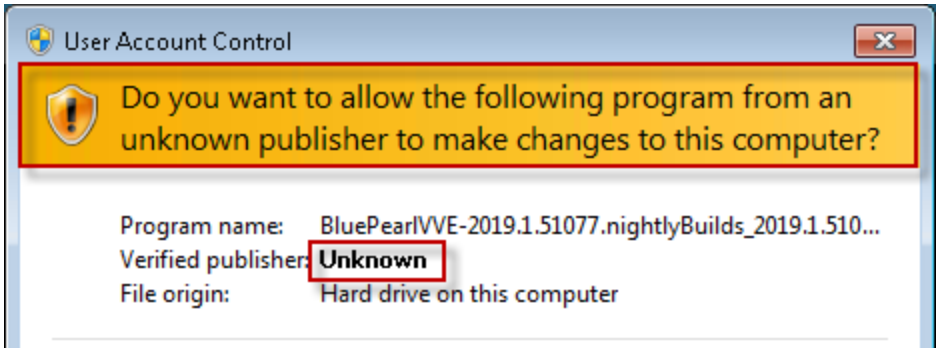
In accordance with established Microsoft suggested practices, BPSVVS installer uses an identification certificate issued by DigiCert to confirm when the software was compiled and packaged.

It would be impractical for a user's computer to have all the world's certificates prior to installing software from a new vendor for the first time, so most systems allow Automatic Root Certificate Updates. Some users, however, opt to enhance security by disabling this feature, as shown here:



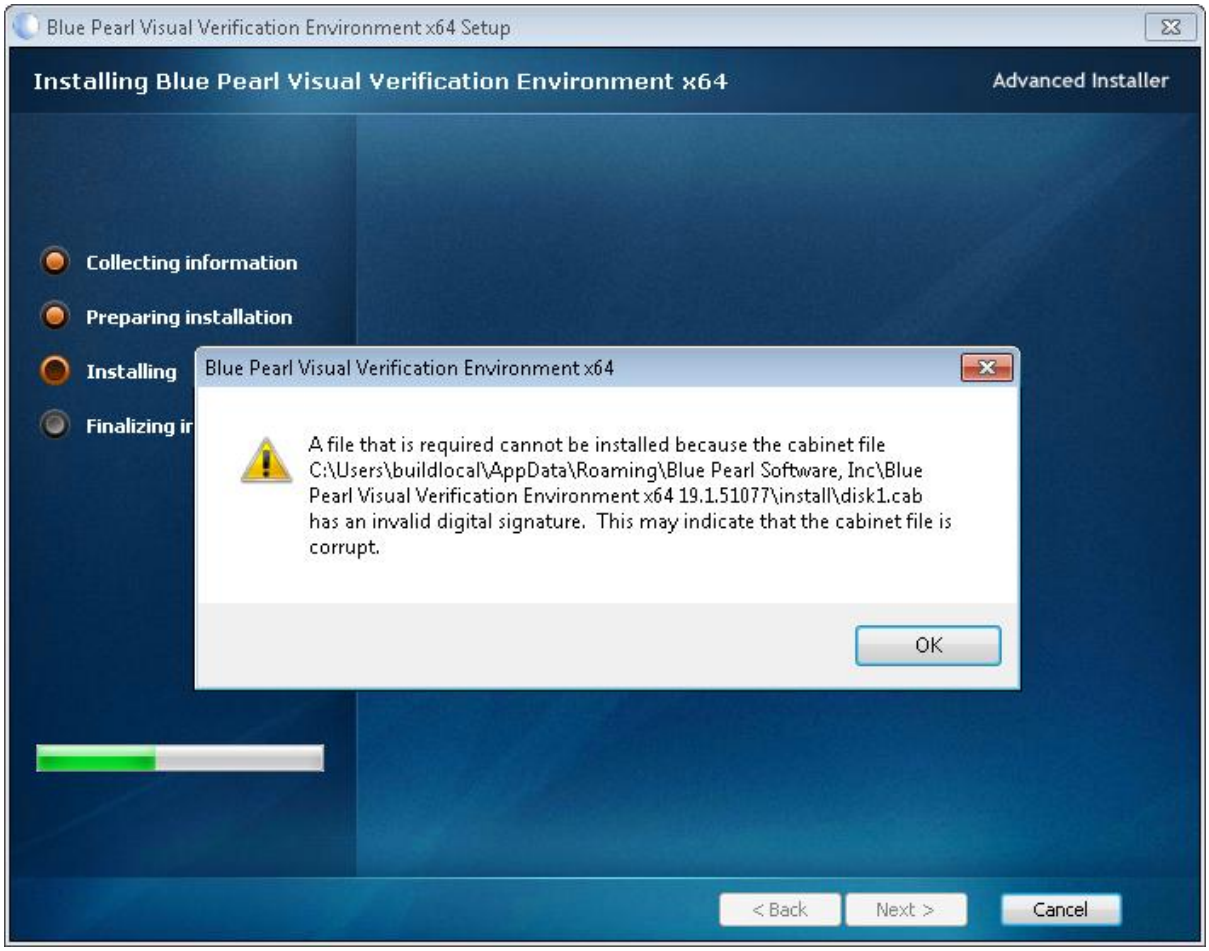
Most installations of Windows 10 already include the proper CA files, so for the most part this issue affects installations prior to Windows 10.

If you encounter a dialog box that looks like this while installing VVS:



where the *Verified publisher* is listed as **Unknown**, it means that your system does not trust the certificates supplied by Blue Pearl Software. Lack of Automatic Root Certificate Updates is one possible cause, but there may be others.

If you choose to proceed beyond this cautionary dialog, you may encounter another barrier that cannot be surmounted by the click of a button.



At this point a simple solution is to manually obtain copies of the required certificates and install them. The remainder of this White Paper provides instructions on how to do that.

Obtaining and installing the certificates

Download the three required files from the following URLs shown here:

- Use the link https://digicert.tbs-certificats.com/DigiCertTrustedRootG4.crt to download the required ".crt" file. This file should be installed into the *Current User → Trusted Root Certification Authorities* certificate repository as described below, if it is not already installed.

- Use the link https://cacerts.digicert.com/DigiCertTrustedG4RSA4096SHA256TimeStampingCA.crt to download the specified file. This file should be installed into the *Current User → Intermediate Certification Authorities* certificate repository as described below, if it is not already installed.

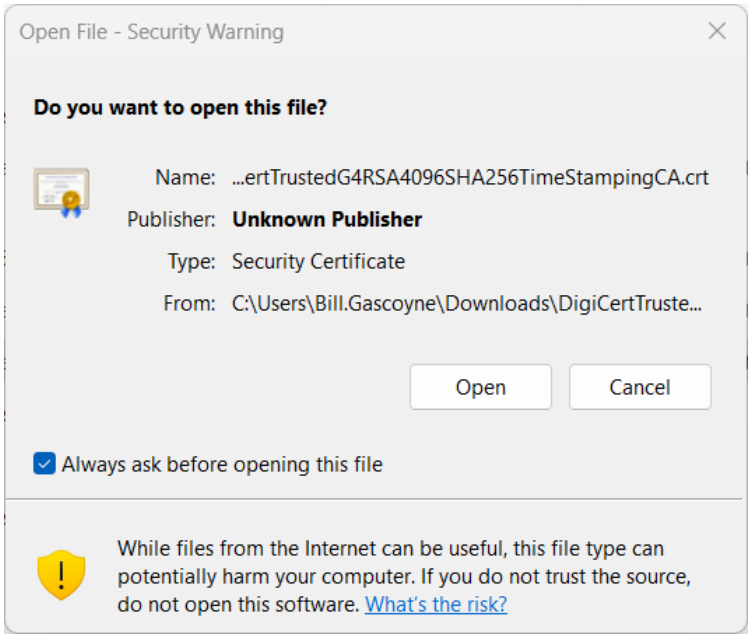
- Use the link https://cacerts.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA3842021CA1.crt to download the specified file. This file should be installed into the *Current User → Intermediate Certification Authorities* certificate repository as described below, if it is not already installed.

While the actual installation of VVS requires administrative privileges and/or granted rights for installing software onto a given Windows system, importing the relevant root CA certificates to their certificate repository can be done by an unprivileged account. A domain administrator should also be able to import these root CA certificates either into the domain certificate trust structure or onto specific computers' certificate repositories through whatever means that they deem prudent and secure.

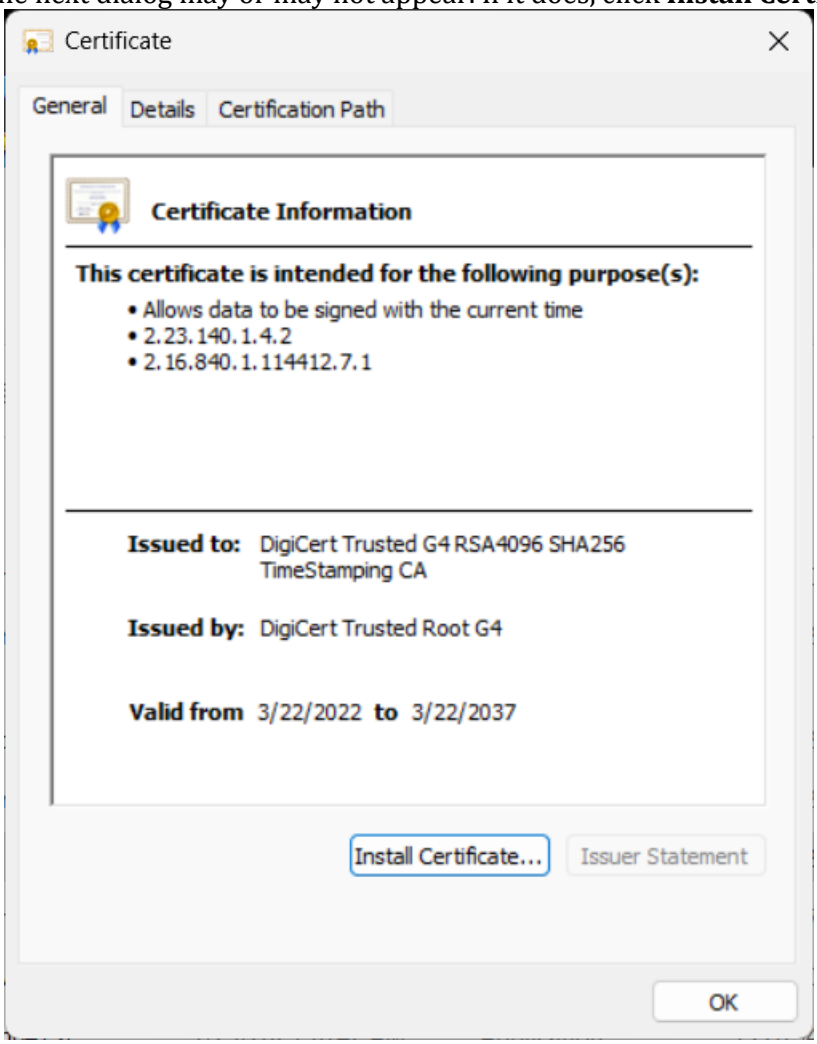
The following instructions are valid for Windows 7, 8, 10 and 11 on unprivileged accounts. Follow the same procedure for each of the certification files. The figures below are from Windows 11 (mostly identical to Windows 10) unless otherwise indicated.

1. Open Windows Explorer and navigate to one of the certification files.

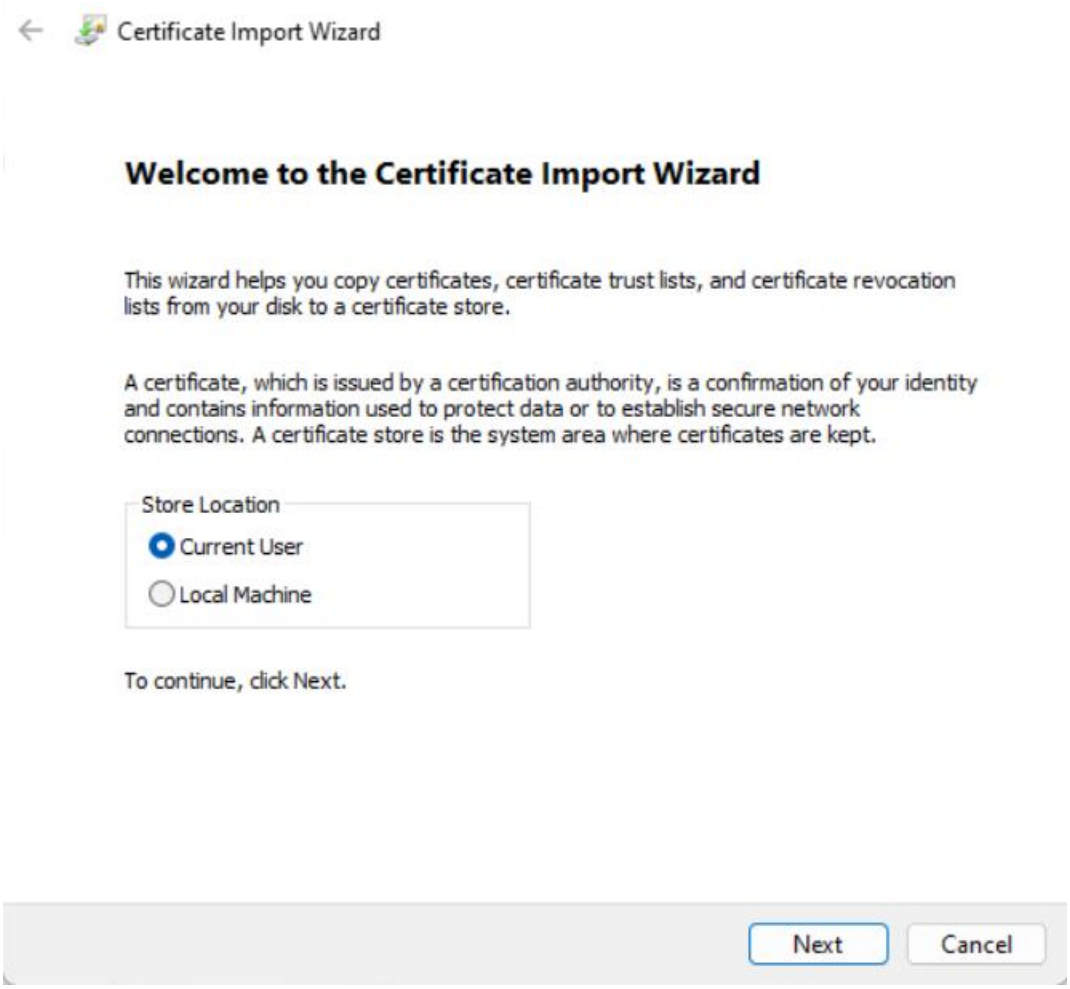
2. Right Mouse Click on the file and select **Install Certificate**. Alternatively, select **Open With → Crypto Shell Extensions**. If you get the **Open File – Security Warning** dialog as shown below, click **Open**.



3. The next dialog may or may not appear. If it does, click **Install Certificate…**.

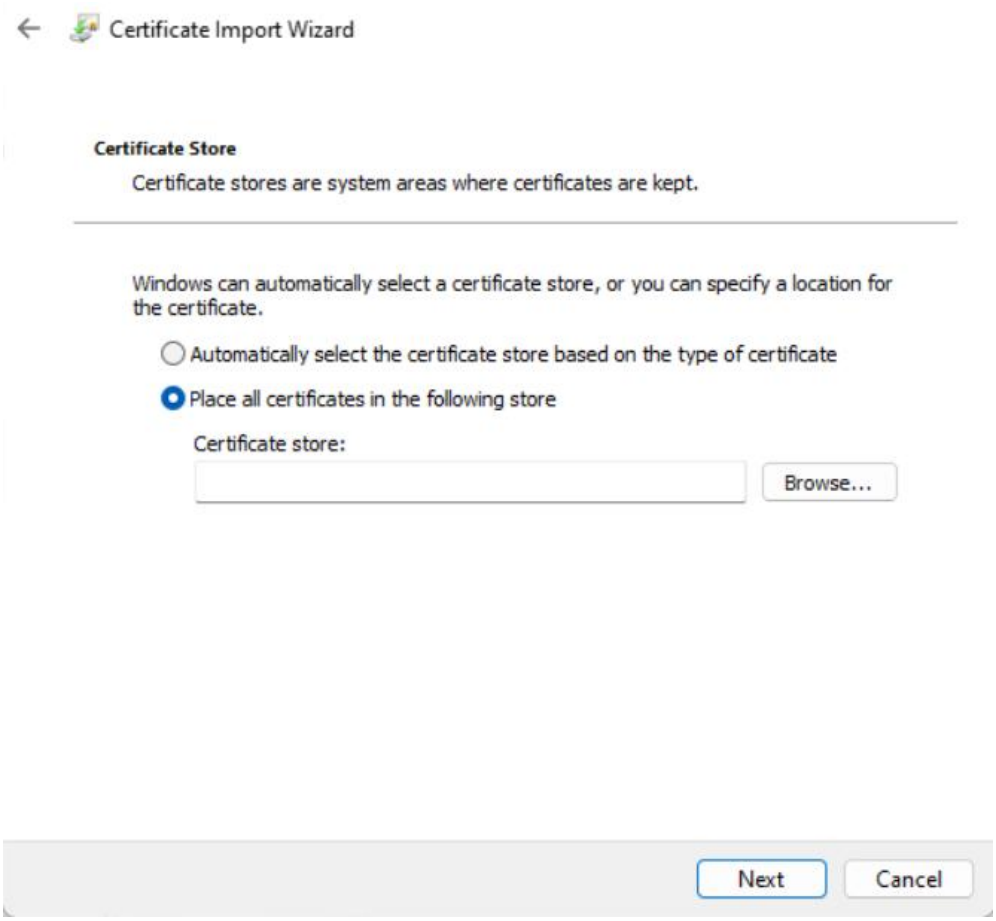


4. If (as seen in the first figure from Windows 11) the resulting dialog provides a choice between **Current User** and **Local Machine**, choose **Current User**.

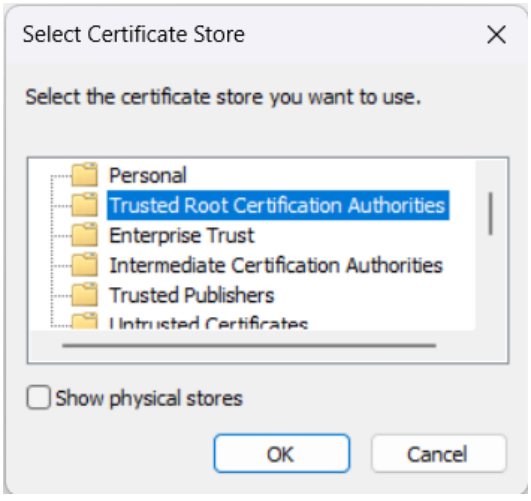


5. In either case (the other case illustrated in the second figure from Windows 7), click **Next**.

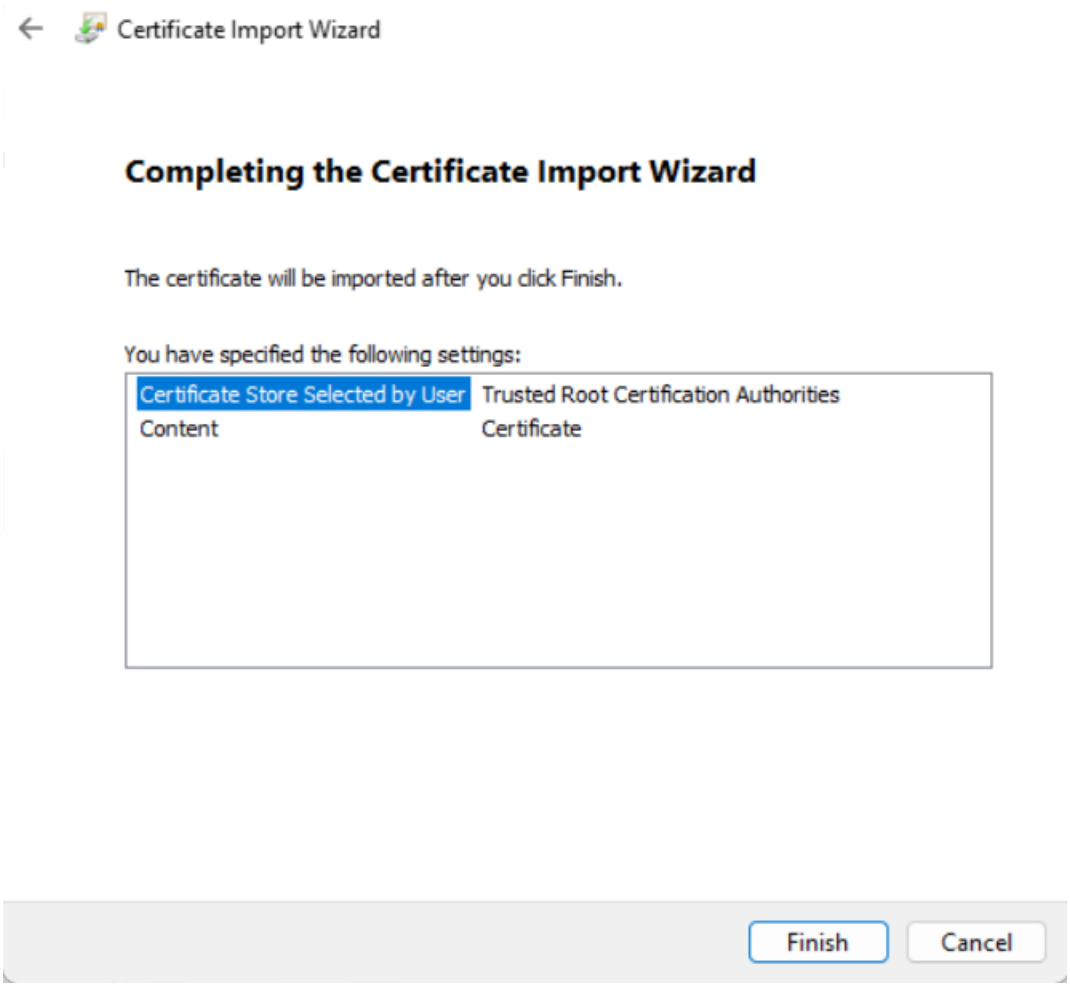
6. In the next dialog, select **Place all certificates in the following store** and then click **Browse…**.



7. In the **Select Certificate Store** dialog, select *Trusted Root Certification Authorities* or *Intermediate Certification Authorities* as indicated above, and then click **OK**.

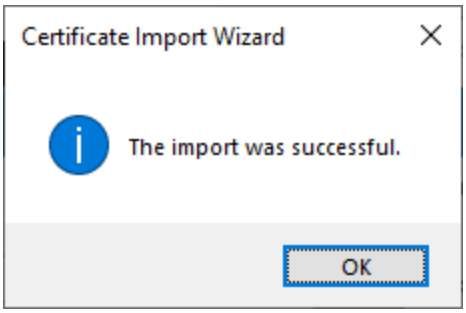


8. Back in the wizard, click **Next**.



9. Click **Finish**.

10. You may or may not see a warning similar to this. If you do, click **Yes** to give this certificate permission to validate any request made to it.



11. The import should be successful at this point, so click **OK**.

That concludes the installation. Remember to perform this procedure for all three certificate files as needed.

Conclusion

While enhanced computer security has its advantages and may in many cases be necessary, it does sometimes require additional effort, especially when it involves overriding automatic functions. We hope the descriptions and procedures provided here have been helpful in enabling you to access all the benefits of the **Blue Pearl Visual Verification Suite**.