

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:

🦳 Internet Communication setting:			
Turn off Automatic Root	Setting	State	
Certificates Update	Turn off handwriting recognition error reporting	Not configured	
Edit policy setting	🖹 Turn off Windows Customer Experience Improvement Progr	Not configured	
Luic poncy security	📔 Turn off Automatic Root Certificates Update	Enabled	
Requirements:	🖹 Turn off printing over HTTP	Not configured	
At least Windows XP Professional	🖹 Turn off downloading of print drivers over HTTP	Not configured	
family with SP1	🖹 Turn off Windows Update device driver searching	Not configured	
	🖹 Turn off Event Viewer "Events.asp" links	Not configured	
Description:	🖹 Turn off Help and Support Center "Did you know?" content	Not configured	
Specifies whether to automatically	🖹 Turn off Help and Support Center Microsoft Knowledge Bas	Not configured	
Windows IIndate Web site.	🖹 Turn off Internet Connection Wizard if URL connection is ref	Not configured	
	🖻 Turn off Registration if URL connection is referring to Micro	Not configured	

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 <u>https://digicert.tbs-certificats.com/DigiCertTrustedRootG4.crt</u> 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.c <u>rt</u> to download the specified file. This file should be installed into the *Current User* \rightarrow *Intermediate Certification Authorities* certificate repository as described below, if it is not already installed.

• Use the link

https://cacerts.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA3842021C A1.crt to download the specified file. This file should be installed into the *Current User* \rightarrow *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.



 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.

Open File	- Security W	/arning	×
Do you	want to ope	en this file?	
	Name:	ertTrustedG4RSA4096SHA256TimeStampingCA.cr	t
E,	Publisher:	Unknown Publisher	
	Type:	Security Certificate	
	From:	C:\Users\Bill.Gascoyne\Downloads\DigiCertTruste	
		Open Cancel	
< Alwa	ys ask before	e opening this file	
!	While files potentially do not ope	from the Internet can be useful, this file type can harm your computer. If you do not trust the source, n this software. <u>What's the risk?</u>	



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

<u>द</u> ि Ce	rtificate	,	×
Genera	al Details Cer	tification Path	
1	ertifica	te Information	
T	his certificate • Allows data • 2.23.140.1 • 2.16.840.1	is intended for the following purpose(s): a to be signed with the current time .4.2 .114412.7.1	
	Issued to:	DigiCert Trusted G4 RSA4096 SHA256 TimeStamping CA	
	Issued by:	DigiCert Trusted Root G4	
	Valid from	3/22/2022 to 3/22/2037	
		Install Certificate Issuer Statement	
		ОК	



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**.

← 🛃 Certificate Import Wizard

welcome to the certificate import wizar	Wel	come to	the	Certificate	Import	Wizard
---	-----	---------	-----	-------------	--------	--------

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location	
O Current User	
O Local Machine	

To continue, click Next.

Next	Cancel



Certificate Import Wizard	×
	Welcome to the Certificate Import Wizard
	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
	To continue, dick Next.
	< Back Next > Cancel

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...**.

Certificate stores are system areas	where certificates are kept.
Windows can automatically select a othe certificate.	certificate store, or you can specify a location for
O Automatically select the certifi	icate store based on the type of certificate
O Place all certificates in the follo	owing store
Certificate store:	
	Browse

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

Next

Cancel





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

← 🛿 🐓 Certificate Import Wizard

Completing	the	Certificate	Import	Wizard
------------	-----	-------------	--------	--------

The certificate will be imported after you click Finish.

You have specified the following settings:

 Certificate Store Selected by User
 Trusted Root Certification Authorities

 Content
 Certificate

Finish	Cancel	

9. Click Finish.



Security	Warning	×
4	You are about to install a certificate from a certification authority (CA) claiming to represent:	
	Sectigo RSA Time Stamping CA	
	Windows cannot validate that the certificate is actually from "Sectigo RSA Time Stamping CA". You should confirm its origin by contacting "Sectigo RSA Time Stamping CA". The following number will assist you in this process:	
	Thumbprint (sha1): 02D65B95 E28370C1 570095FA 88F923DD 937FAD8F	
	Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.	
	Do you want to install this certificate?	
	Ver	
	Yes No	

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.

Certificate Import Wizard	×
The import was successful.	
ОК	

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**.