Confirming that Macrium download is genuine

We are often asked from concerned customers if our installers have been infected with malware, or if third parties have included toolbars and additional download items to our installer.

We take the provenance of our downloads seriously. If you believe that a download has been compromised, please contact us immediately, after finding that any of the following checks fail.

The following steps will enable to you confirm that the file you downloaded is byte for byte, the one created by our build process.

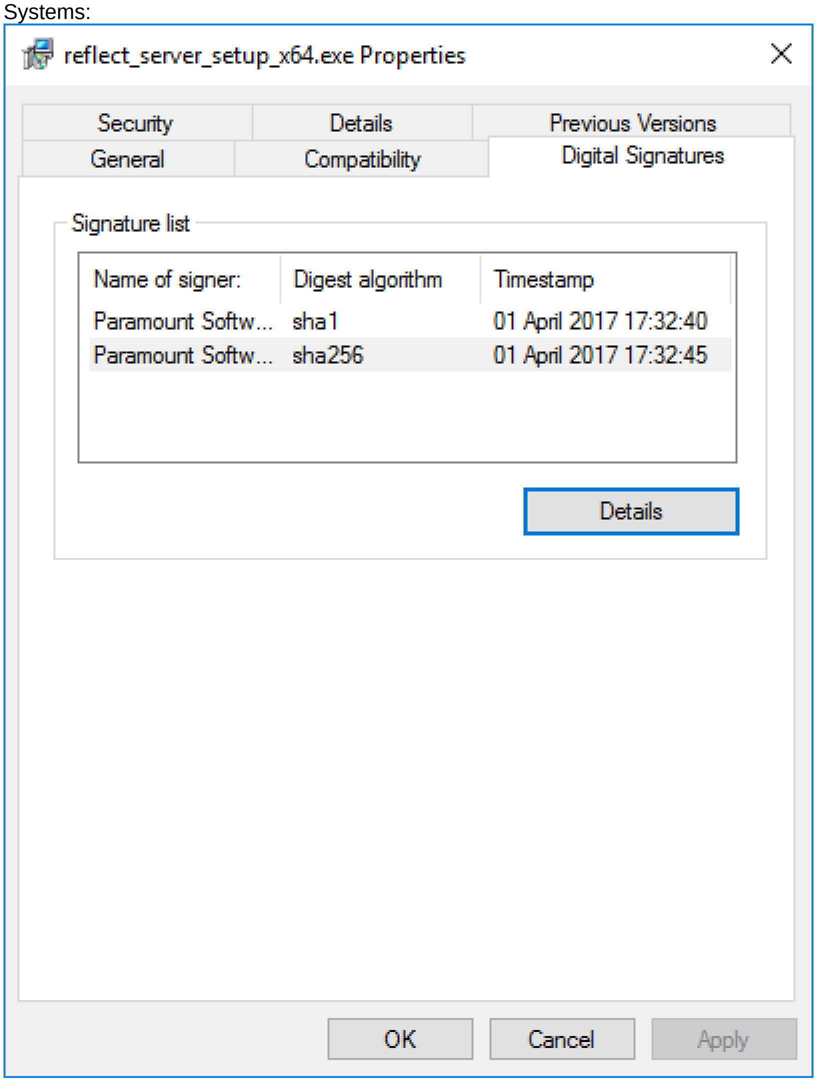
If any of the checks below fail, then the file is not to be trusted; please re-download using only links on www.macrium.com

You can read more about code signing and the assurance it confers here.
http://msdn.microsoft.com/en-us/library/ie/ms537361%28v=vs.85%29.aspx

1. Right click on the downloaded file, and chose properties:

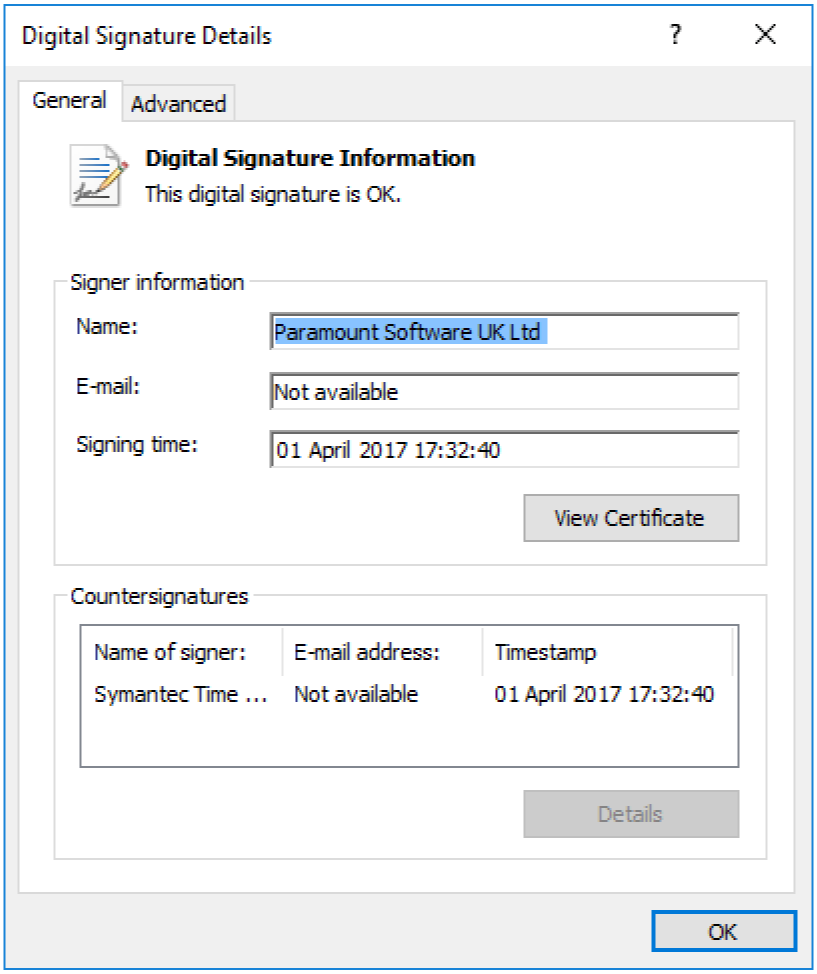
    a. Check that the file has a digital signature (if not, the digital signature tab is not present).

    b. Select **digital signatures tab.**
    There will be two signatures, sha1 and sha256. Having two signatures ensures complete coverage for all Windows Operating Systems:



Name of signer:	Digest algorithm	Timestamp
Paramount Softw...	sha1	01 April 2017 17:32:40
Paramount Softw...	sha256	01 April 2017 17:32:45

    c. Check the digital signatures are valid, **Click details** on both certificates.



Digital Signature Details

Digital Signature Information

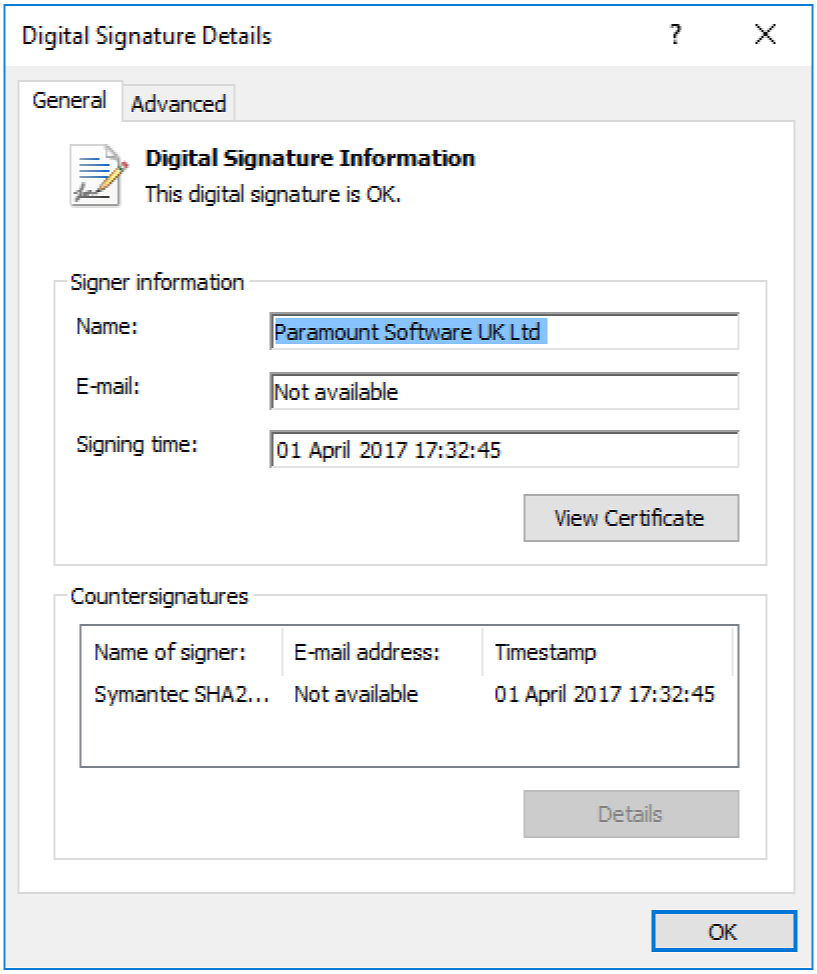
This digital signature is OK.

Signer information

Name:	Paramount Software UK Ltd
E-mail:	Not available
Signing time:	01 April 2017 17:32:40

Countersignatures

Name of signer:	E-mail address:	Timestamp
Symantec Time ...	Not available	01 April 2017 17:32:40



Digital Signature Information
This digital signature is OK.

Signer information

Name: Paramount Software UK Ltd

E-mail: Not available

Signing time: 01 April 2017 17:32:45

Countersignatures

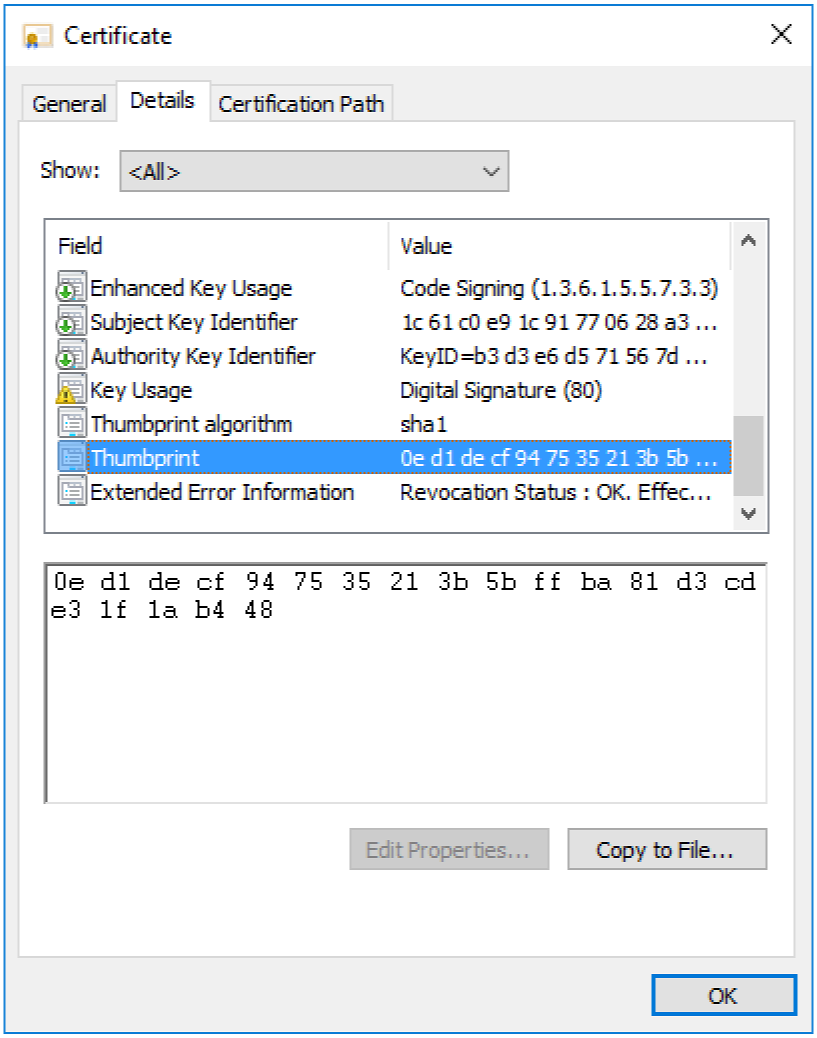
Name of signer:	E-mail address:	Timestamp
Symantec SHA2...	Not available	01 April 2017 17:32:45

2. Verify the code signing, confirming that the file hasn't been modified and then resigned with a certificate that resembles ours:

    a. Click **view certificate button.**

    b. Click **details** tab.

        i. The thumbprint for the sha1 certificate should be: 0e d1 de cf 94 75 35 21 3b 5b ff ba 81 d3 cd e3 1f 1a b4 48 and

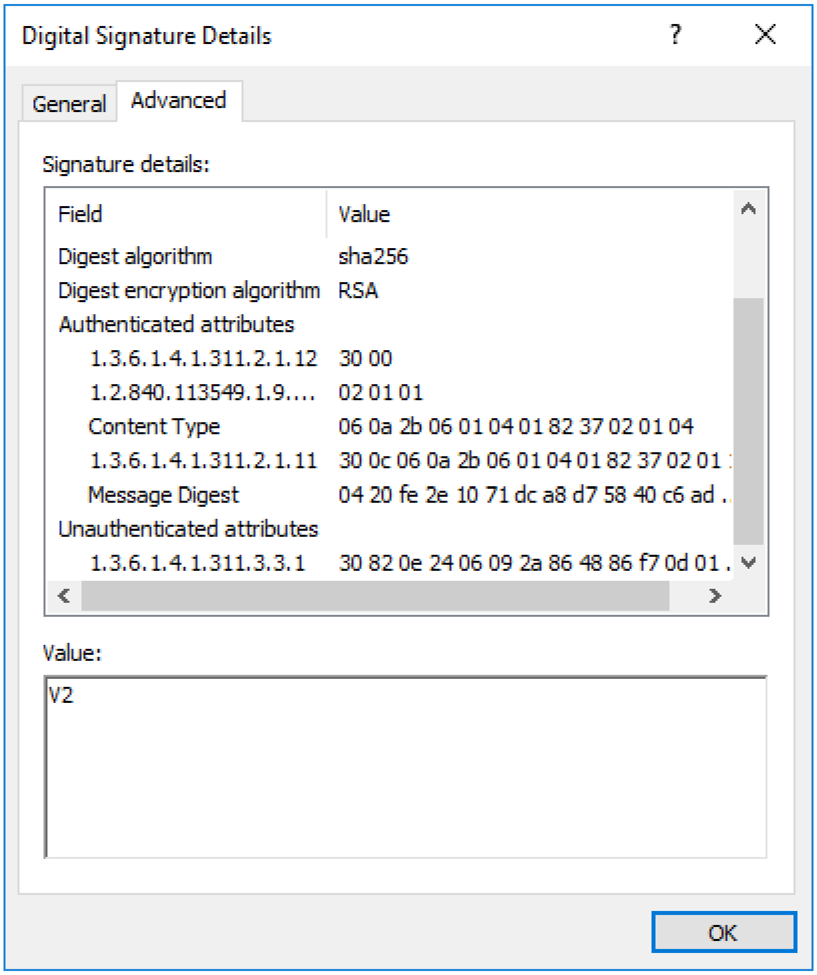


Show: <All>

Field	Value
Enhanced Key Usage	Code Signing (1.3.6.1.5.5.7.3.3)
Subject Key Identifier	1c 61 c0 e9 1c 91 77 06 28 a3 ...
Authority Key Identifier	KeyID=b3 d3 e6 d5 71 56 7d ...
Key Usage	Digital Signature (80)
Thumbprint algorithm	sha1
Thumbprint	0e d1 de cf 94 75 35 21 3b 5b ...
Extended Error Information	Revocation Status : OK. Effec...

```
0e d1 de cf 94 75 35 21 3b 5b ff ba 81 d3 cd
e3 1f 1a b4 48
```

ii. The sha256 certificate should look the same as below:



Signature details:

Field	Value
Digest algorithm	sha256
Digest encryption algorithm	RSA
Authenticated attributes	
1.3.6.1.4.1.311.2.1.12	30 00
1.2.840.113549.1.9....	02 01 01
Content Type	06 0a 2b 06 01 04 01 82 37 02 01 04
1.3.6.1.4.1.311.2.1.11	30 0c 06 0a 2b 06 01 04 01 82 37 02 01 :
Message Digest	04 20 fe 2e 10 71 dc a8 d7 58 40 c6 ad .
Unauthenticated attributes	
1.3.6.1.4.1.311.3.3.1	30 82 0e 24 06 09 2a 86 48 86 f7 0d 01 .

Value:

V2