Forescout

Digital Signing of Windows Portable Executable Files

Technical Note

Version 2.0

As of May 25, 2017

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.forescout.com/support/

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Resources page on the Forescout website for additional technical documentation: https://www.forescout.com/company/resources/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

2019-12-17 11:32

Table of Contents

Scope

This document describes changes which affect all Forescout plugins and modules that contain Windows executables and were released after May 25, 2017. This includes, but is not limited to:

- HPS Inspection Engine
- Windows Applications
- Hardware Inventory
- IOC Scanner
- Microsoft SMS/SCCM

About Portable Executable (PE) Files

Microsoft has defined the PE file format as a container for executables and object files. The Forescout platform makes use of various Windows executables, including the SecureConnector executable, the Forescout Remote Inspection service (fsprocsvc), and various other utility .EXE and .VBS files.

This document describes changes to the algorithms that the Forescout platform uses for certificate-based signing of files distributed in the PE format.

Certificate Based Signing of Executable Code

Code signing is used to ensure the authenticity and integrity of the code. When executables are signed by a certificate chain of a trusted issuer, entities that run the code can validate that:

- The code being run was provided by the company that signed it – in this case, Forescout.
- The code has not been tampered with since its release.

Code signing supports transparent background interaction between the Forescout platform and endpoints in the following ways:

- ***At the browser level***, browsers perform multiple checks on applications that users download, including reputation and potentially anti-malware checks. One of these checks looks at whether the application was signed by a trusted source. Browsers apply various types of these checks when end users download SecureConnector through their browsers. Appropriately signed code satisfies these checks without end user interaction.
- ***At the endpoint OS level***, Windows itself performs checks on executables when running them. Depending on the version of Windows and the security level set, users receive warnings when running an executable which is not signed or not signed with a valid certificate. The warning prompts the user to make a conscious decision as to whether they want to go ahead and run the

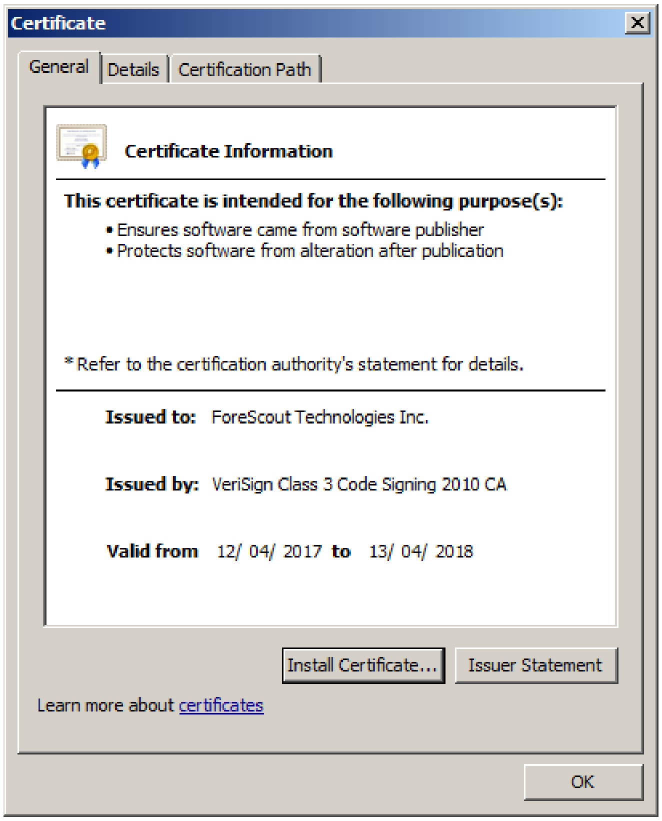
executable. Correctly signing such files with valid certificates, especially in the case of files that were downloaded from the web, helps avoid this warning.

- ***At the endpoint policy/application whitelist level***, for security reasons, some system administrators lock down their desktops and laptops to ensure that only whitelisted executables are run. One strong method of whitelisting requires that executables are signed by one of a number of approved certificates. Depending on your implemented policies and plugin configuration, the Forescout platform may run scripts and utility executables on your Windows endpoints to retrieve properties and perform actions.

Current Code Signing Practice (as of May 25, 2017)

Forescout utilizes two different types of digital certificates for code signing of Windows executables:

1. A Verisign (Symantec)-issued SHA-1 digital certificate with a SHA-1 root certificate.



Certificate Information

This certificate is intended for the following purpose(s):

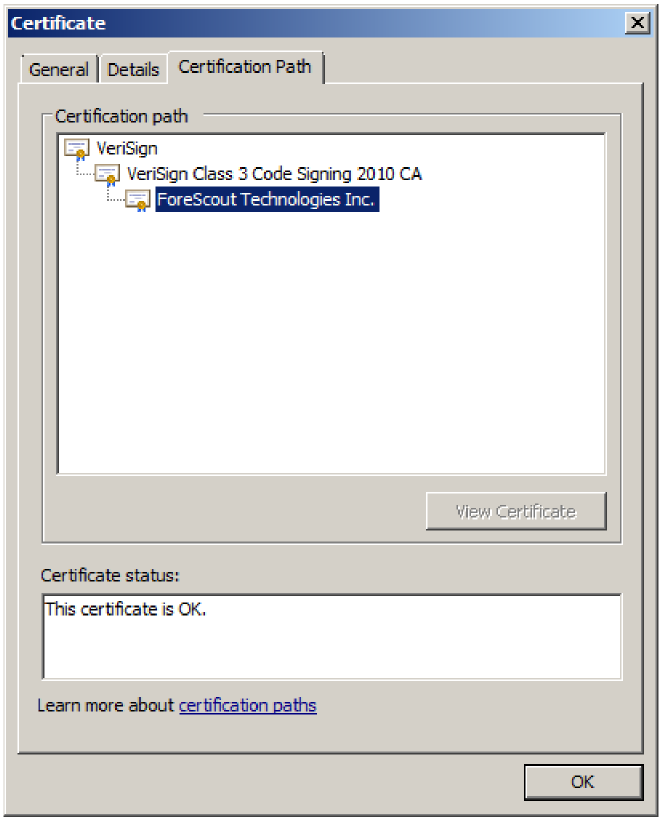
- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

Issued to: ForeScout Technologies Inc.

Issued by: VeriSign Class 3 Code Signing 2010 CA

Valid from 12/ 04/ 2017 **to** 13/ 04/ 2018



Certification path

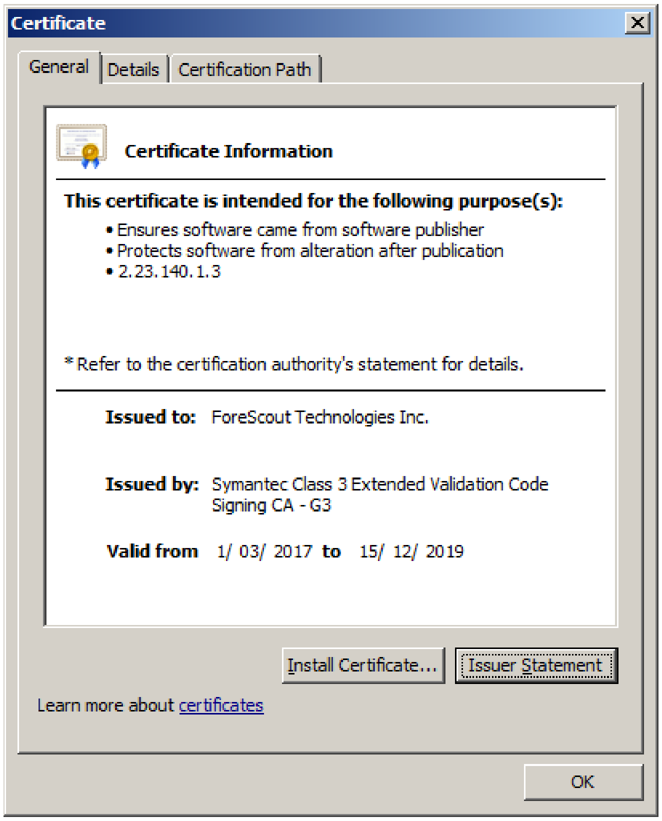
- VeriSign
  - VeriSign Class 3 Code Signing 2010 CA
    - ForeScout Technologies Inc.

Certificate status:

This certificate is OK.

Learn more about certification paths

2. A Symantec-issued SHA-256 digital certificate with a SHA-256 root certificate.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication
- 2.23.140.1.3

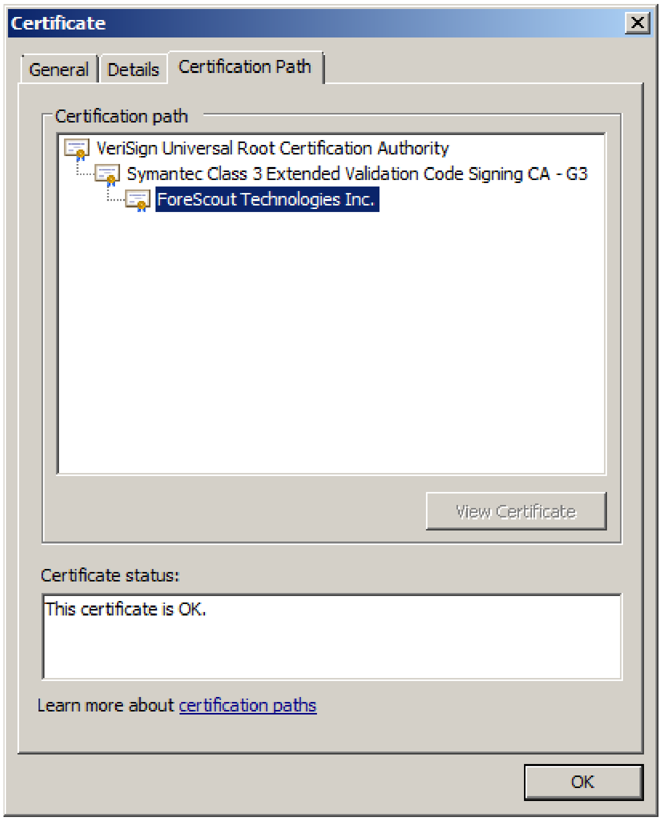
* Refer to the certification authority's statement for details.

Issued to: ForeScout Technologies Inc.

Issued by: Symantec Class 3 Extended Validation Code Signing CA - G3

Valid from 1/ 03/ 2017 **to** 15/ 12/ 2019

Learn more about certificates



Certificate

General | Details | Certification Path

Certification path

VeriSign Universal Root Certification Authority
  Symantec Class 3 Extended Validation Code Signing CA - G3
    ForeScout Technologies Inc.

Certificate status:

This certificate is OK.

Learn more about certification paths

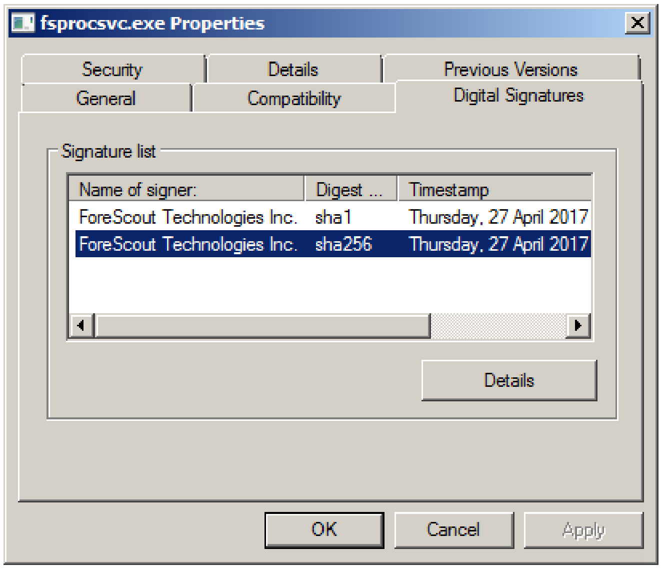
Forescout maintains multiple instances of each certificate type, yet they all have the same common names as shown above. The differences between the certificates are only in the form of the validity dates and the serial numbers.

All Windows PE files included with the Forescout platform (including Forescout plugins and modules) are digitally signed as described in the following table.

File type	Certificate	Signature Digest Algorithm
EXE	SHA-1	SHA-1
	SHA-256	SHA-256
VBS	SHA-256	SHA-1
MSI	SHA-256	SHA-1

Dual signing of .EXE files ensures that Microsoft Authenticate trusts the executable when it is downloaded by endpoints running any recent or legacy version of

Windows. To verify dual signing, right-click on the file, select **Properties** and then view the **Digital Signatures** tab. You should see the following:



Name of signer:	Digest ...	Timestamp
ForeScout Technologies Inc.	sha1	Thursday, 27 April 2017
ForeScout Technologies Inc.	sha256	Thursday, 27 April 2017

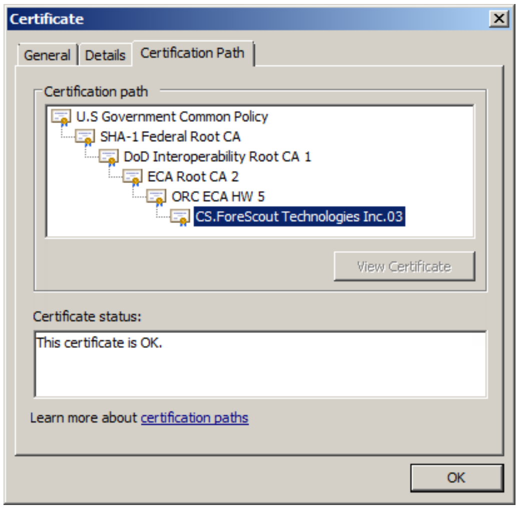
Since VBS files cannot be dual signed, Forescout signs all VBS files with the SHA-256 based certificate. MSI installer packages use the singing method applied to VBS files. Older versions of Windows which do not support SHA-256 cannot verify this signature, and consider such files unsigned. To run Forescout VBS scripts and MSI installers, endpoints in your environment that still run these versions of Windows must not have a security policy that prevents running unsigned scripts.

Appendix - History of Changes to Forescout Code Signing of Windows Executables

This section describes the background for previous changes to the code signing procedure used by Forescout, and describes changes for specific files.

Code Distributed Prior to October 25, 2016

All relevant Windows files were signed by a code signing certificate issued to Forescout. Files are signed by one of two certificates, issued either to “CS.Forescout Technologies Inc.02” or “CS.Forescout Technologies Inc.03”. Depending on the certificate used to sign the files, the certificate chain looks like one of the following:

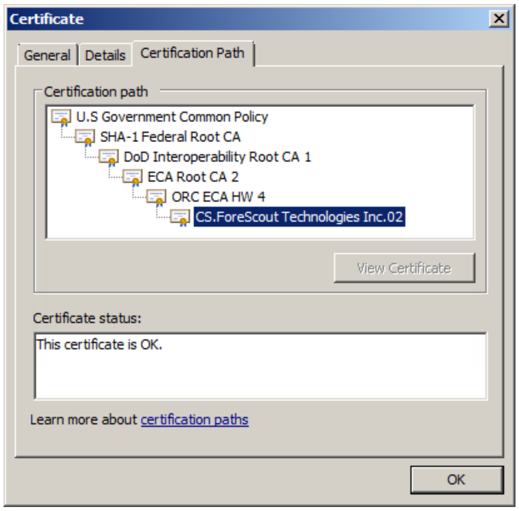


U.S Government Common Policy
SHA-1 Federal Root CA
DoD Interoperability Root CA 1
ECA Root CA 2
ORC ECA HW 5
CS.ForeScout Technologies Inc.03

Certificate status:

This certificate is OK.

Learn more about certification paths



U.S Government Common Policy
SHA-1 Federal Root CA
DoD Interoperability Root CA 1
ECA Root CA 2
ORC ECA HW 4
CS.ForeScout Technologies Inc.02

Certificate status:

This certificate is OK.

Learn more about certification paths

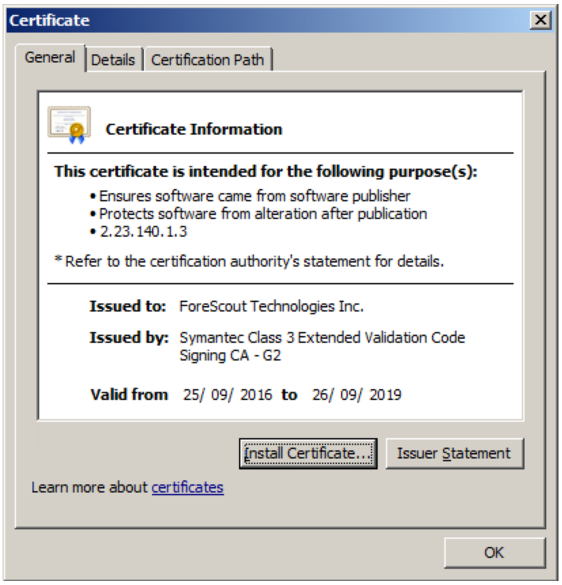
These certificates are SHA-1 based certificates and the digital signatures are SHA-1 based.

Code Distributed Between October 25, 2016, and May 25, 2017

Due to increasing attacks on the SHA-1 algorithm, SHA-1 certificates were no longer considered secure. Industry best practices recommended the use of SHA-256 based certificates.

During 2016, Microsoft began actively discouraging the use of SHA-1 certificates for code signing, but held off full deprecation of SHA-1 in order to support older Windows operating systems that cannot work with SHA-256 certificates. Similarly, Forescout wished to continue support for these legacy systems, including Windows XP and Windows Server 2003.

Forescout introduced the use of a second code signing certificate for signing PE files. The new certificate is SHA-256 based and issued to “Forescout Technologies Inc.” This certificate has a SHA-1 root certificate.



Certificate Information

This certificate is intended for the following purpose(s):

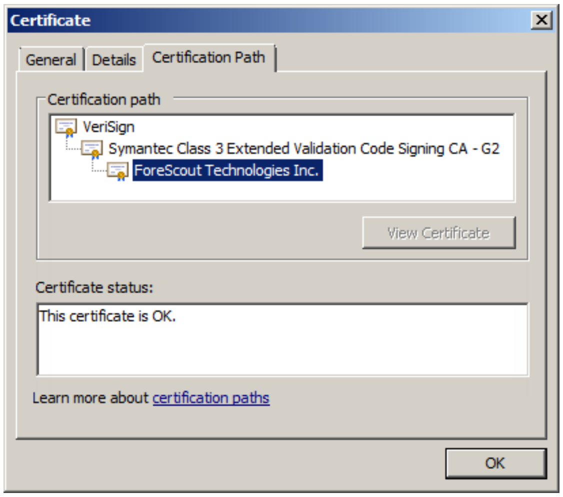
- Ensures software came from software publisher
- Protects software from alteration after publication
- 2.23.140.1.3

* Refer to the certification authority's statement for details.

Issued to: ForeScout Technologies Inc.

Issued by: Symantec Class 3 Extended Validation Code Signing CA - G2

Valid from 25/ 09/ 2016 **to** 26/ 09/ 2019



Certification path

- VeriSign
  - Symantec Class 3 Extended Validation Code Signing CA - G2
    - ForeScout Technologies Inc.

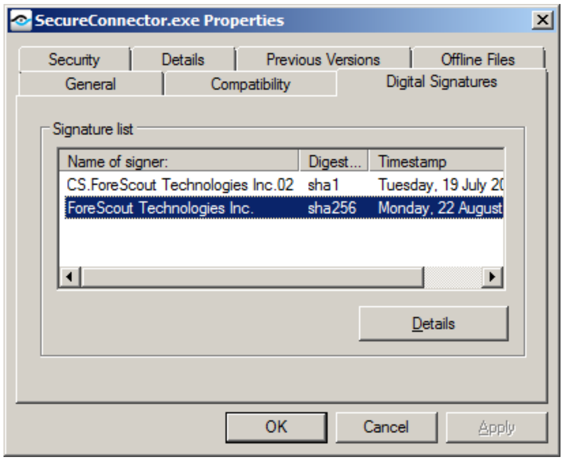
Certificate status:

This certificate is OK.

Between October 25, 2016 and May 25, 2017, Forescout code containing .EXE and .VBS files were signed as follows:

.EXE Files

.EXE files were dual signed by two separate code signing certificates. The first signature utilized the original SHA-1 code-signing certificate described above. The second signature utilized the new SHA-256 digital certificate. To verify dual signing, right-click on the file, select **Properties** and then view the **Digital Signatures** tab. You should see the following:



Name of signer:	Digest...	Timestamp
CS.ForeScout Technologies Inc.02	sha1	Tuesday, 19 July 20
ForeScout Technologies Inc.	sha256	Monday, 22 August

.VBS Files

VBS files cannot be dual-signed, therefore Forescout signs all VBS files with the SHA-256 based certificate. Older versions of Windows which do not support SHA-256 cannot verify the signature, and such scripts are considered unsigned. To run Forescout VBS scripts, endpoints in your environment that still run these versions of Windows must not have a security policy that prevents running unsigned scripts.

References

1. Windows Enforcement of SHA1 Certificates - https://social.technet.microsoft.com/wiki/contents/articles/32288.windows-enforcement-of-sha1-certificates.aspx
2. Windows Script Host 5.6 (with references to digitally signing scripts) - https://msdn.microsoft.com/en-us/library/ms974613.aspx and https://technet.microsoft.com/en-us/library/ee176795.aspx
3. Introduction to Code Signing - https://msdn.microsoft.com/en-us/library/ms537361(v=vs.85).aspx

Additional Forescout Documentation

For information about other Forescout features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

Access documentation downloads from the Forescout Resources Page, or one of two Forescout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** – Product Updates Portal
- ***Flexx Licensing Mode*** – Customer Portal

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Forescout Resources Page

The Forescout Resources page provides links to the full range of technical documentation.

To access the Forescout Resources page:

- Go to https://www.Forescout.com/company/resources/, select **Technical Documentation,** and search for documents.

Product Updates Portal

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer Portal:

- Go to https://Forescout.force.com/support/ and select **Downloads**.

Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

🗎 *If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.*

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context-sensitive *Help* buttons to access information about tasks and topics quickly.

Forescout Administration Guide

- Select **Forescout Help** from the **Help** menu.

Plugin Help Files

- After installing the plugin, select **Tools** > **Options** > **Modules**, select the plugin, and then select **Help**.

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).