Procedure for Improving the Start Behavior of Applications on a SIMATIC PCS 7 Installation

SIMATIC PCS 7

https://support.industry.siemens.com/cs/ww/de/view/87057037

Siemens Industry Online Support

This entry originates from the Siemens Industry Online Support. The conditions of use specified there apply (www.siemens.com/nutzungsbedingungen).

Security Notes

Siemens offers products and solutions with industrial security functions which support the secure operation of plants, solutions, machines, devices and/or networks. They are important components in a comprehensive industrial security concept. The Siemens products and solutions continue to be developed under this aspect. Siemens recommends that you keep yourself regularly informed about product updates.

For the safe operation of Siemens products and solutions it is necessary to take appropriate security measures (cell protection concept, for example) and to integrate each component in an overall industrial security concept which is state of the art. This should also cover the third-party products used. Additional information about industrial security is available at: http://www.siemens.com/industrialsecurity.

In order to keep yourself informed about product updates, we recommend subscribing to our product-specific newsletter. Additional information about this is available at http://support.industry.siemens.com.

Contents

1 Overview

In more recent versions of SIMATIC PCS 7 delays or even abortion of the start may occur when starting SIMATIC and operating system applications used by Siemens software.
This concerns, for example, the PCS 7 Web Option for OS, WinCC Calendar Option, Batch Control Center (BCC) and Batch Recipe Editor.

This behavior can occur under the following conditions:

- The computer has no enabled network connection.
- The computer has no access to the internet, in particular to
  - Windows Update
  - URLs which refer to the CRLs of certificates in the certificates

Details about the behavior

Microsoft have made security-relevant improvements in more recent versions of their products. These include the checking of digital signatures of the installed software and drivers for the operating system. Siemens also puts a digital signature on its SIMATIC applications to ensure the trustworthiness and authenticity of its applications. Here, when these applications are run, certificates are also checked for validity.
These checks might require network access to URLs, CAs, CTLs and CRLs which are either in the local network or in the internet. If these network addresses are not reached, then the behavior described might occur.

The following scenarios lead to start delays or abortion of the start of SIMATIC and operating system applications.

1. CTL non existent

   A check is made whether a certificate was issued by a trustworthy CA. If the Root Certificate of that CA is not available locally, a query is made at Microsoft over the internet. If this is not possible, the start is delayed or aborted.

2. CRL not accessible

   The URL of a CRL is given in a certificate or in a root certificate. If this cannot be accessed via the network, the start is delayed or aborted.

Note

On Windows systems, in the event display, in the "Application and Services Protocols", in the "Ready for Operation Protocol" of the Microsoft Windows CAPI2 service, you can check whether one of the scenarios described above is on the corresponding plant computer. You enable this protocol beforehand in the actions of the MMC or in the pop-up menu of the protocol. If this protocol contains error messages, the possible causes can be found in the details of the messages.

2 Solution

2.1 CTL Non Existent

The following measures are comparable with a central Patch Management Server, with which all the required and current CTLs are provided. In this way you can also check for updates of the certificates.

1. Installation and use of a WSUS Patch Management Server

   Click the link to find and download released Microsoft Patches ("Security Patches" and "Critical Patches") for SIMATIC PCS 7:
   http://support.automation.siemens.com/WW/view/en/18490004

   Link to the SIMATIC Process Control System PCS 7 Patch Management and Security Updates:
   http://support.automation.siemens.com/WW/view/en/38621083

2. Installation of the Microsoft Security Update "KB2813430" on all plant computers

   With this Security Update (not available for Windows XP, Windows Server 2003) Microsoft has changed some options and the way of processing with regard to CTLs and CRLs. This update has been available at Microsoft through the Windows Update Mechanisms (through a WSUS, for example) since June 2013 and it is included in the list of the Security Patches released for SIMATIC PCS 7. Download the update here and install it on all plant computers.
   Link to the download: http://support.microsoft.com/kb/2813430/en-us

3. Downloading of the CTLs to the WSUS using the "CertUtil" application

   For this refer to the documentation (see link) in the chapter "Configure a file or web server to download the CTL files". Store the downloaded CTLs on the WSUS in a directory that can be accessed via a new virtual website you configure. In this way you can make them also available to the plant computers in the future.
   Link to the documentation:
   http://technet.microsoft.com/en-us/library/dn265983.aspx#BKMK_PrepServer

4. Local usage of the CTLs on the WSUS server

   Establish a group policy to make the downloaded CTLs available locally for the WSUS. For this refer to the documentation (see link) in the chapter "Redirect the Microsoft Automatic Update URL for a disconnected environment". Here you can use one of the web pages you have configured or the local directory on the WSUS.
   Link to the documentation: https://technet.microsoft.com/en-us/library/dn265983.aspx#BKMK_both

5. Daily update of the CTLs on the web server of the WSUS using "CertUtil"

   On the WSUS, use the Task Scheduler to configure a task that is to be executed daily which ensures that the CertUtil command is started. You can use a script to do this, for example. This updates the CTLs and makes them available on the locally configured web page.
   Help on the topic of the Task Scheduler: https://technet.microsoft.com/en-us/library/cc766428.aspx

6. Downloading and daily updating of the CTLs on the plant computers

   On the WSUS, use the Task Scheduler to configure a task that is to be executed daily which ensures that the latest CTLs are downloaded from the web server of the WSUS and made available in a locally configured directory. You can use a script to do this, for example. Start the script initially so that the configuration described in the next step functions without error.
   Help on the topic of the Task Scheduler: http://technet.microsoft.com/en-us/library/cc766428.aspx

7. Configuration of the plant computers by GPO

   Establish a group policy on the plant computers to make the CTLs downloaded from the WSUS available locally. Follow the steps in the documentation (see link) in the chapter "Redirect the Microsoft Automatic Update URL for a disconnected environment". Configure the local directory that is used for the download of the CTLs by the described tasks.
   Link to the documentation: http://technet.microsoft.com/en-us/library/dn265983.aspx#BKMK_both

Note If the CTLs are stored only on the WSUS, there might be start delays as soon as the WSUS can no longer be reached.

2.2 CRL Not Accessible

Proceed as follows on PCS 7 computers which use their own CRLs (when using client certificates, for example).

- Enable CRL check in the Internet Explorer
  Go to "Options > Internet Option > Advanced > Security" and select the setting "Check for publisher's certificate revocation".
- URL call timeout
  Via a group policy you configure how long the system attempts to reach a certificate link or CRL link.
  On the systems considered you start the local group policy editor (gpedit.msc) with administrator rights. Alternatively you create a corresponding group policy for an OU in an available Active Directory domain.
  Then you configure the following policy under "Policies for local computer > Computer configuration > Windows Settings > Security Settings > Policies for Public Keys > Settings for Checking the Certificate Path > Network Call":
  1. Define this Policy Setting: "on"
  2. Automatic update of certificates in the Microsoft Program for root certificates (recommended): "on"
  3. Default value for URL call timeout (in seconds): "1" (minimum)
  4. Default value for cumulated call timeouts for the path check (in seconds): "1" (minimum)

Link to the Online Help "Increase the option for timeout":
http://technet.microsoft.com/en-us/library/cc771429.aspx

3 List of Abbreviations

Table 3-1

Abbreviation	Long form	Meaning
URL	Uniform Resource Locator	Address of a web server
CA	Certification Authority	A trusted entity that issues certificates and thus declares that the person, computer or organization requesting the certificate meets the criteria of specific guidelines.
CTL	Certificate Trust List	A predefined list of elements signed by a trusted entity. A certificate trust list can be varied, for example, a list of hashes of certificates or a list of file names. All the elements in the list are authenticated and approved by the trusted signing entity.
CRL	Certificate Revocation List	A document managed and published by a certification authority. It lists certificates issued by the certification authority that are no longer valid.
	Root Certificate	A certificate of a self-signed certification authority that identifies a certification authority. It is called a root certificate because it is the certificate for the root certification authority. The root certificate must sign its own certificate of the certification authority, because there is no higher certification authority.