Utilization of Whitelisting with McAfee Application Control in a PCS 7- / WinCC environment

SIMATIC PCS 7 and WinCC

https://support.industry.siemens.com/cs/ww/en/view/88653385

Siemens Industry Online Support

Warranty and liability

Note

The Application Examples are not binding and do not claim to be complete with respect to the configuration, equipment and any eventualities. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible in ensuring that the described products are correctly used. These Application Examples do not relieve you of the responsibility to use safe practices with respect to application, installation, operation and maintenance. When using these Application Examples, you acknowledge that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time without prior notice. If there are any deviations between the recommendations provided in these Application Examples and other Siemens publications – e.g. catalogs – the contents of the other documents have priority.

We do not accept any liability for the information contained in this document.

Any claims against us – for whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in case of mandatory liability, e.g. under the German Product Liability Act ("Produkthaftungsgesetz"), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of substantial contractual obligations ("wesentliche Vertragspflichten"). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.

Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of Siemens Industry Sector.

Security infor-mation

Siemens offers products and solutions with industrial security functions, which support the secure operation of systems, solutions, machines, devices and/or networks. They are important components of a holistic Industrial Security Concept. The Siemens products and solutions undergo continuous development with this concept in mind. Siemens recommends to stay informed about product updates on a regular basis.

For the safe operation of products and solutions from Siemens, it is necessary to take suitable protective measures (e.g. cell protection concept) and to integrate each component into an overall IT security concept which corresponds to the state-of-the-art IT technology. Any third-party products that may be in use must also be taken into account. You will find more information about Industrial Security under http://www.siemens.com/industrialsecurity.

Please register for our product-specific newsletter to ensure that you will always be informed about product updates. Detailed technical information can be found at http://support.automation.siemens.com.

Table of contents

Warranty and liability **2**

1 Preface **4**

2 Whitelisting **5**

2.1 Introduction 5
2.2 McAfee Application Control 6

3 Compatibility **7**

4 Administration **8**

4.1 General procedure 8
4.2 Local administration of McAfee Application Control 8
4.3 Central administration via McAfee ePolicy Orchestrator Server (ePO) 9

5 Use of McAfee Application Control with PCS 7 and WinCC **10**

5.1 Installation preparations 10
5.2 Installation and Configuration 11
5.2.1 Local administration 11
5.2.2 Central administration via ePO 13

6 Update installation **14**

6.1 Local administration 15
6.2 Central administration via ePO 15

7 Special characteristics for PCS 7 and WinCC **16**

7.1 Installing updates, hotfixes and patches 16
7.2 SIMATIC Batch 17
7.3 PUDManager 17
7.4 SIMATIC WinCC 17
7.5 Simultaneous use of Symantec Endpoint Protection and McAfee Application Control 17

8 History **18**

1 Preface

Purpose of the entry

This entry describes the installation, utilization, and recommended settings for McAfee Application Control (component of the McAfee Integrity Control product) in the SIMATIC PCS 7 and WinCC environment.

NOTICE

Please note that McAfee Integrity Control only releases the functionality of the whitelisting (McAfee Application Control) for certain product versions of SIMATIC PCS 7 and WinCC.

More information is available on the Internet at:
https://www.siemens.com/kompatool

Required knowledge

This documentation is intended for persons involved in project planning, commissioning and servicing of automation systems using SIMATIC PCS 7 or WinCC.

Administration knowledge and IT techniques for Microsoft Windows operating systems are required.

Validity

This documentation applies for process control systems that are realized with SIMATIC PCS 7 or WinCC.

It applies across versions, valid starting with PCS 7 V6.1 SP4 and WinCC starting with V7.0 SP1.

2 Whitelisting

2.1 Introduction

The utilization of whitelisting technologies in a process control system is only effective when they are part of a comprehensive security concept. The sole use of whitelisting technologies cannot comprehensively protect a process control system against malware attacks.

As a matter of principle, we therefore recommend adhering to the Security Concept PCS 7 / WinCC and PCS 7 Compendium Part F, which are available on the Internet via the following link:

http://support.automation.siemens.com

Whitelisting in conjunction with the above referenced security concept is an additional security measure (additional layer of defense) in order to counteract the increasing risk of attacks.

In principle, the whitelisting approach is based on a mistrust of all applications except those that have been tested and classified as trustworthy. This means, a positive list is maintained (whitelist). This positive list contains the applications that have been classified as harmless and that can safely be run on the computer system.

The principle of whitelisting is the exact opposite of blacklisting, which works with a list of "non-trustworthy" applications (negative list = blacklist). An example for blacklisting is a conventional virus scanner, which works with a blacklist, the virus patterns. Since the number of "non-trustworthy" applications increases constantly, this blacklist must be adjusted on a regular basis. This means for example that the current blacklist (virus patterns) must be available for the virus scanner at all times. The virus scanner can only recognize applications as malware when they are listed on this blacklist.

Since whitelisting works with a positive list, a constant adaptation to new threats in the form of malware is not necessary. This minimizes the administration and updating expense.

2.2 McAfee Application Control

McAfee Application Control can be used to block the start of unauthorized or unknown applications on servers and workstations. After the installation activation of McAfee Application Control, all executable applications and files are protected against modification. Contrary to simple whitelisting concepts, McAfee Application Control uses a dynamic trustworthiness model. This makes the lengthy, manual updating of lists of approved applications obsolete. Updates of authorized applications in the list can be integrated in different ways:

- through trustworthy users (user)
- through trustworthy manufacturers (certificate)
- through a trustworthy directory
- through a binary file
- through updaters (updating programs, e.g. Windows Update or virus scanners)

Furthermore, McAfee Application Control offers functions that monitor the main memory, provide protection against buffer overflow, and protect files that are running in the main memory.

NOTICE

McAfee Application Control is a component of McAfee Integrity Control. McAfee Integrity Control includes the components McAfee Application Control and McAfee Change Control.

In the SIMATIC PCS 7 and WinCC environment, only the functionality of the whitelisting (McAfee Application Control) has been approved.

For this reason, this documentation focuses exclusively on this functionality.

Siemens customers obtain McAfee Application Control as a separate software from McAfee or its distributors.

3 Compatibility

An overview of which version of SIMATIC PCS 7 and WinCC is compatible with which versions of McAfee Application Control can be found on the following website:

http://www.siemens.com/kompatool

4 Administration

The administration of McAfee Application Control can be carried out in different ways:

- Locally on a computer system (standalone)
- Centrally via the administration software McAfee ePolicy Orchestrator (ePO)

The decision concerning local or central administration should be made based on the number of systems that are to be maintained. Similarly to an Active Directory domain, the central administration should be used starting with about 10 systems that require administration.

4.1 General procedure

Independent from the administration type (locally or centrally), the following recommended procedures should be carried out directly following the installation of the operating system and SIMATIC PCS 7/WinCC:

1. Installation of McAfee Application Control on a PC
2. Execution of the "Solidify" on this PC
   This process searches all connected local drives for executable files and enters them in the whitelist. The duration of this procedure depends on the data volume and the performance of the computer and can last several hours. With up-to-date hardware, this should last about 20-30 minutes.
3. Activation of McAfee Application Control
4. Computer restart

All executable files that were found during the scan (exe, com, dll, bat, etc.) are now protected against modifications (renaming, deletion, moving within the file path, etc.). From this point on, new and therefore for the system unknown applications can no longer be executed.

4.2 Local administration of McAfee Application Control

The local administration takes place exclusively via the command line. The respective commands are self-explanatory. Furthermore, McAfee offers extensive product documentation. McAfee Application Control allows the administration via script.

4.3 Central administration via McAfee ePolicy Orchestrator Server (ePO)

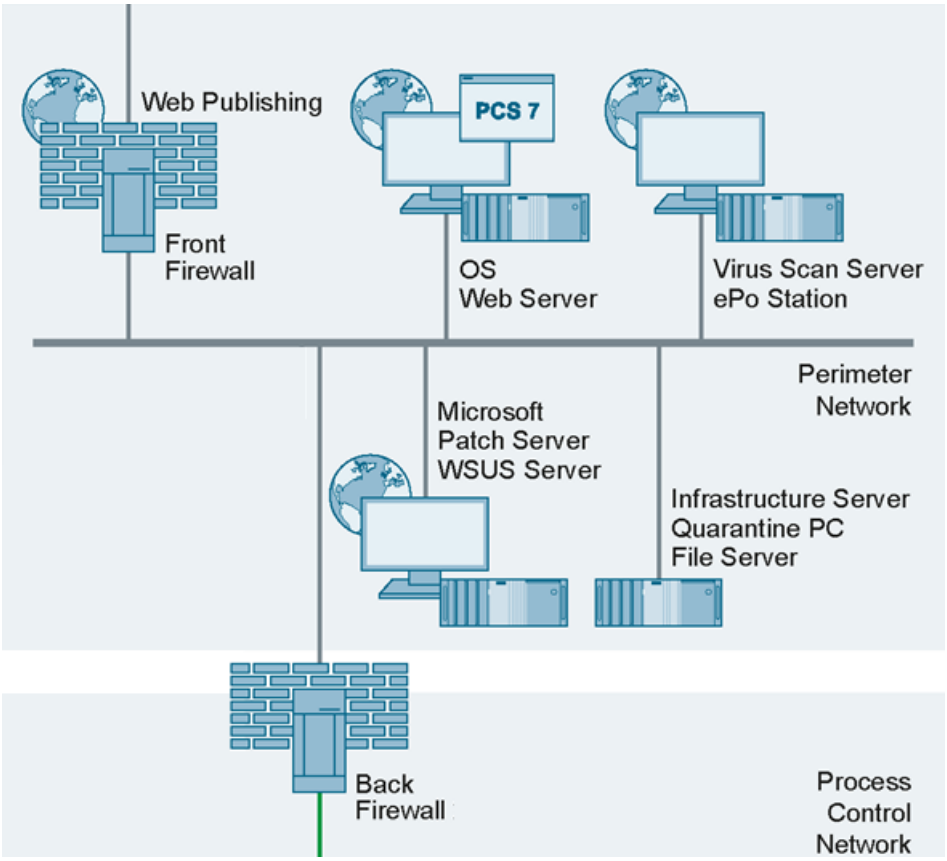
The central administration of the whitelisting (installation, configuration, and monitoring of the clients) takes place via the McAfee ePolicy Orchestrator (ePO) application, a management tool that can administrate all McAfee products but also provides many network management and network monitoring functionalities of which some are free of charge.

All local McAfee Application Control commands and options are also remotely available via the ePO. On one hand via predefined tasks and on the other via remote command line prompts. In comparison to the local administration, the ePO application provides improved monitoring and more clearly structured event management.

The McAfee ePO administration software needs to be installed on its own computer with up-to-date hardware and a respectively compatible, McAfee-approved Windows Server operating system. If the system already has an infrastructure computer (e.g. WSUS, VirusScan server), McAfee ePO can be installed there as well (upon verification of the compatibility).

NOTICE McAfee ePO must not be installed on a SIMATIC PCS 7 or WinCC computer or an active directory domain controller.

Figure 4–1: Architecture example for McAfee ePolicy Orchestrator



5 Use of McAfee Application Control with PCS 7 and WinCC

The following describes information and special characteristics in conjunction with the use of McAfee Application Control in the SIMATIC PCS 7 and WinCC environment.

5.1 Installation preparations

The following steps need to be followed during the installation and implementation of McAfee Application Control:

1. Setup of the system based on the recommendations of the Security Concept PCS 7 and WinCC in order to keep the risk presented by malware programs during the integration of McAfee Application Control as low as possible. http://support.automation.siemens.com/WW/view/en/60119725
2. Installation and configuration of the operating system
3. Installation of the required programs and components
4. Installation of all available security updates for the operating system and the program/components
5. Installation of a virus scanner including security updates and the newest, available virus signature files
6. If possible, isolation of the connection to external/third-party networks (e.g. on the front firewall)
7. Execution of a complete virus scan of the computer
8. Installation of McAfee Application Control either locally or via ePO
9. Execution of the "Solidify" process for all local hard drives and partitions
10. Activation of McAfee Application Control
11. Computer restart

5.2 Installation and Configuration

5.2.1 Local administration

No special characteristics must be taken into consideration during the use of McAfee Application Control with SIMATIC PCS 7 or WinCC. The standard installation for the system recommended by McAfee can be used.

The corresponding recommendations can be found in the McAfee manuals and Bests Practices Guides under the following link:(filter based on "Application and Change Control"):

https://mysupport.mcafee.com/eservice/productdocuments.aspx?strPage=2

Installation procedure

For the local installation of McAfee Application Control on a computer system, proceed as follows:

1. Execute the operating system-specific setup for McAfee Application Control and follow the instructions of the installation program. All default settings can be accepted. No changes or adjustments are necessary.
2. Open the McAfee Application Control command line via "Start > Programs > McAfee > Solidifier > McAfee Solidifier command line“
3. Execute the "Solidify" command for all hard drives and partitions
   To do so, enter the following command on the solidify her command line:

   "**sadmin solidify**" or "**sadmin so**"

   All partitions and local hard drives of the computer system will be scanned for executable files (applications) such as for example exe, com, bat, dll. etc., but also for Java, Active X control elements, scripts, etc. Files found during the scan will be signed by McAfee Application Control for future use and will be authorized and added to the whitelist. This also includes the protection against a subsequent change such as e.g. deletion or renaming**.**
   After the finalization of the "solidification", the Solidifier command line indicates how many data files per partition or hard drive or scans were scanned and how many files were authorized during this process.
4. After the "solidification", you must activate the McAfee Application Control.
   To do so, enter the following prompt on the solidifier command line:

   "**sadmin enable**"

Note The actual activation of the whitelisting via McAfee Application Control takes place only after restarting the computer.

CAUTION	**McAfee Application Control whitelisting with Windows Server 2016** When using McAfee Application Control whitelisting with Windows Server 2016, Windows logon may no longer work properly. The screen flashes on the logon screen and it does not allow you to log on. To avoid this behavior, add a skip list for the winlogon.exe . Add the skiplist command locally on the system by recovering the CLI mode or implement it from ePO if the system is being managed. Use the following command: **"sadmin attr add -c winlogon.exe"** More information can be found here: mcafee.com/KB92977

5. Restart the computer
6. After the restart you can query the current status of the whitelisting by entering the following prompt on the solidifier command line:

"**sadmin status**"

7. The output should show an active "solidifier".
8. Now, the computer system, meaning all applications on the computer, is protected against modifications, such as for example deletion or renaming. Furthermore, only the applications that were added to the whitelist can be executed.

How you can execute intentional modifications or application updates on a system that is protected in this manner is described in Chapter 6 „Update installation".

Protection of the configuration against modifications

McAfee Application Control can be protected by a password so that a local administrator can no longer switch off or configure McAfee Application Control.

The setup takes place on the solidifier command line via the prompt

"**sadmin passwd**".

The protection is active after entering the password two times.

After that, modifications of the configuration of the whitelist are only possible after entering this password (including for a local administrator).

Help for additional commands of the "solidifier"

Additional prompts and the respective help information can be displayed on the "solidifier" command line using the following prompts:

"**sadmin help**" and "**sadmin help-advanced**"

5.2.2 Central administration via ePO

No special characteristics must be taken into consideration during the use of McAfee Application Control with SIMATIC PCS 7 or WinCC. The standard installation recommended by McAfee for the system can be used.

The corresponding recommendations can be found in the McAfee manuals and Bests Practices under the following link: (filter based on "Application and Change Control"):

https://mysupport.mcafee.com/eservice/productdocuments.aspx?strPage=2

Installation of the ePO server

Installation and configuration of the McAfee ePolicy Orchestrator (ePO) is set up as follows:

1. Installation of the McAfee ePolicy Orchestrator
2. Installation of the Solidcore Extension Package
3. Installation of the license for Solidcore or McAfee Application Control

The standard settings recommended by McAfee for the installations of these products can be used.

Installation of McAfee Solidcore clients

The installation of the McAfee Solidcore Agents on the clients is structured in the following steps:

1. Adding of the Solidcore Agent Deployment Package to the ePO repository
2. Adding the client systems in the ePO console
3. Installation of the Solidcore Agent on the clients
4. Activation of the Solidcore Agent on the clients

Here, you can proceed as recommended and described by McAfee.

Activation of the Solidcore Agent on the clients

When the Solidcore Agent has been installed on all clients, you must activate McAfee Application Control (Solidcore) on the clients. However, prior to the activation, just like with the local administration, a "solidify" prompt must be executed in order to generate the whitelist for the corresponding system.

The "solidify" and activation of the whitelist on the clients is initiated via a client task. This client task needs to be generated on the ePO server, as described by McAfee, (creating the whitelist, force restart, and immediate execution of the task).

Additional client tasks

In a similar manner, additional client tasks can be created in order to control the Solidcore Agent on the client.

For example, you can activate the Solidcore Agent on the client/s via a deactivate or activate task. For that purpose, select the respective clients task type, as described by McAfee, and configure it.

6 Update installation

Only authorized applications can be executed on a computer protected by McAfee Application Control. However, under certain circumstances it becomes necessary that new applications need be installed on a computer or that an update or hotfix must be installed for existing and therefore authorized applications.

Examples for such a scenario:

- Installation of Microsoft security updates or additional important updates as part of a patch management
- Installation of new, current virus patterns or the updating of the virus scan engine
- Installation of hotfixes/updates for SIMATIC products
- Subsequent installation of diagnostic tools

There are different options or different procedures in McAfee Application Control to subsequently authorize new applications:

- through trustworthy users
- through trustworthy publishers of applications
- through a trustworthy directory
- through a binary file
- through updaters (updating programs, e.g. Windows Update, virus scanners)

The option that is most frequently used is the utilization of updating programs, the so-called "Updaters".

"Updater" or programs with which already registered files can be changed without additional administration from McAfee Application Control or new files can be added to the "whitelist". This is necessary for example in order to upload Windows updates via a WSUS patch server or to update the virus patterns of a virus scanner.

The procedure depends on how you administrate the system.

NOTICE For security reasons, limit the list of updaters to the selection required for the operation of the system.

During installation of SIMATIC PCS 7 or WinCC Updates, the information in Chapter 0 must be adhered to.

6.1 Local administration

For the local administration of McAfee Application Control, there is an updater for the configuration, such as for example for Windows update (patch management) or virus scanners, which regularly update the system, a batch file called

"**finetune.bat**"

This batch file can be executed via the McAfee Application Control command line. The self-explanatory script assists with the release of programs for updates, such as for example Windows Update client. At the same time, updaters can be added or removed with the following parameters and the respective designation of the updater.

"**add**' or "**remove**"

The predefined updaters are listed without specification of a parameter.

In order to display the list of authorized updating programs, enter the following prompt on the McAfee Application Control command line:

"**sadmin updaters list**"

6.2 Central administration via ePO

The configuration of updating programs is significantly easier in the administrative interface of the ePO. On the one hand the reason for that can be found in the graphics, on the other hand because McAfee provides default templates in order to release frequently used functions and programs. For example, templates for Windows Updates and the three virus scanners approved by Siemens are available.

In order to add an updating program (updater) to a client via McAfee ePO, proceed as described by McAfee. During this process, a guideline is generated, approved and allocated, utilizing previously created updater templates. You can also define your own updaters and add them to a guideline.

7 Special characteristics for PCS 7 and WinCC

7.1 Installing updates, hotfixes and patches

Service packs, updates, hotfixes and patches from SIMATIC PCS 7 or WinCC can only be installed during completed runtime and the activation of the update mode of McAfee Application Control (AC).

The following procedure is recommended for the uploading of SIMATIC PCS 7 or WinCC:

1. Power down and close all PCS 7 or WinCC applications
2. Computer restart

NOTICE If Autologin and Autostart have been configured for SIMATIC PCS 7 or WinCC systems, they must be deactivated prior to the restart.

3. Switching on update mode of AC via:

   "**sadmin bu**

   Depending on the system centrally via the ePO through a task or locally on the respective PC.
4. Installing of PCS 7 or WinCC update
5. Computer restart
6. Start the complete, updated PCS 7 or WinCC application
7. Activate the Autologin and Autostart if those have been deactivated previously
8. Terminating update mode of AC via

   "**sadmin eu**'

   Depending on the system centrally via the ePO through a task or locally on the respective PC.

7.2 SIMATIC Batch

The following information must be adhered to for the printing of protocols with templates:

Note

The application "ReportingServicesService.exe" has to be added as an updater to the McAfee Application Control on each master and standby server (centrally via the ePO or locally on the PC). Please note the McAfee documentation.

7.3 PUDManager

In order to use the PUDManager, consider the following note:

NOTE

The application "PudManHelpViewer.exe" has to be added as an updater to the McAfee Application Control on every PCS 7 computer (centrally via the ePO or locally on the PC). Please note the McAfee documentation.

7.4 SIMATIC WinCC

In order the WinCC help is also available in runtime mode and no alarm is triggered by the activation/deactivation of runtime, consider the following note:

Note

The application “hh_wincc.exe” has to be added as an exception to the McAfee Application Control (centrally via the ePO or locally on the PC). Please note the McAfee documentation.

7.5 Simultaneous use of Symantec Endpoint Protection and McAfee Application Control

Symantec Endpoint Protection and McAfee Application Control both provide a "Memory Protection" function. These two functions are incompatible with each other. Therefore, when operating both products together on one system, the "Memory Protection" function of one product must be disabled.

NOTE

Please refer to the manufacturer's instructions to learn how to disable the function:

- McAfee: Internet link (https://kc.mcafee.com/corporate/index?page=content&id=KB81465)
- Symantec: Internet link (https://support.symantec.com/de_DE/article.HOWTO125353.html)

8 History

Table 8–1

Version	Date	Change
V1.0	02/2014	First edition
V1.1	12/2014	Chapter “Special characteristics for PCS 7 and WinCC”
V1.2	07/2018	Adding the chapter "Simultaneous use of Symantec Endpoint Protection and McAfee Application Control"
V1.2.1	08/2020	Adding a warning note in chapter 5.2