SIEMENS

SIMATIC

Process Control System PCS 7 Configuration McAfee VirusScan Enterprise 8.8 - White Paper

Application manual

08/2012
A5E31308835-AA

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E31308835-AA
℗ 11/2014 Subject to change

Copyright © Siemens AG 2012.
All rights reserved

Table of contents

Preface

1

Important information about this whitepaper

Systems tested. The recommended settings for these virus scanners have been chosen to ensure that the reliable real-time mode of PCS 7 is not adversely affected by the virus scanner software.

These recommendations describe how to discover and make effective as comprehensively as possible the best possible compromise currently known between the target, viruses and malicious software, and ensure a PCS 7 control system time response that is as deterministic as possible in all operating phases.

If you choose different settings for the virus scanner, this could have negative effects on the real-time behavior.

Purpose of this documentation

This documentation describes the recommended settings for virus scanner software in combination with PCS 7 and WinCC, following the installation of the virus scanner.

The following basic knowledge is required

This documentation is aimed at persons involved in the engineering, commissioning, and operation of automated systems based on SIMATIC PCS 7 or WinCC. Knowledge of administration and IT techniques for Microsoft Windows operating systems is assumed.

Validity of the documentation

The documentation applies to process control systems equipped with the respective product version of PCS 7 or WinCC.

Note

Note that certain virus scanners are only approved for certain product versions.

Additional information is available on the Internet at the following address:

http://support.automation.siemens.com (http://support.automation.siemens.com/WW/view/en/10154608)

Virus scanner administration 2

Using virus scanners in a process control system is only effective when they are part of a comprehensive security concept. A virus scanner alone generally cannot protect a process control system from security threats.

2.1 Definitions

Virus scanners

A virus scanner is software that detects, blocks or eliminates known harmful program routines (computer viruses, worms and similar malware).

Scan engine (scanner module)

The scan engine is a component of the virus scanner software that can examine data for harmful software.

Virus signature file (virus pattern file or virus definition file)

This file provides the virus signatures to the scan engine, which uses it to search data for harmful software.

Virus scan client

The virus scan client is a computer which is examined for viruses and managed by the virus server.

Virus scan server

The virus scan server is a computer which centrally manages virus scan clients, loads virus signature files and distributes them on the virus scan clients.

Security Suite

Program suites usually sold by former virus scanner manufacturers that provide further security functionalities in addition to traditional virus scanner functions, such as IPS, Application Control, Firewall, etc.

2.2 Using virus scanners

The use of a virus scanner should never inhibit the plant's process mode. The following two examples illustrate the problems that arise in automation through the use of virus scanners:

- A virus infected computer cannot be switched off by a virus scanner if in doing so control is lost over the production process or a plant can no longer be operated in a safe condition.
- Even a virus infected project file, e.g. a database archive, cannot be automatically suspended, blocked or deleted if there is no longer any ability to trace important measured values by doing so.

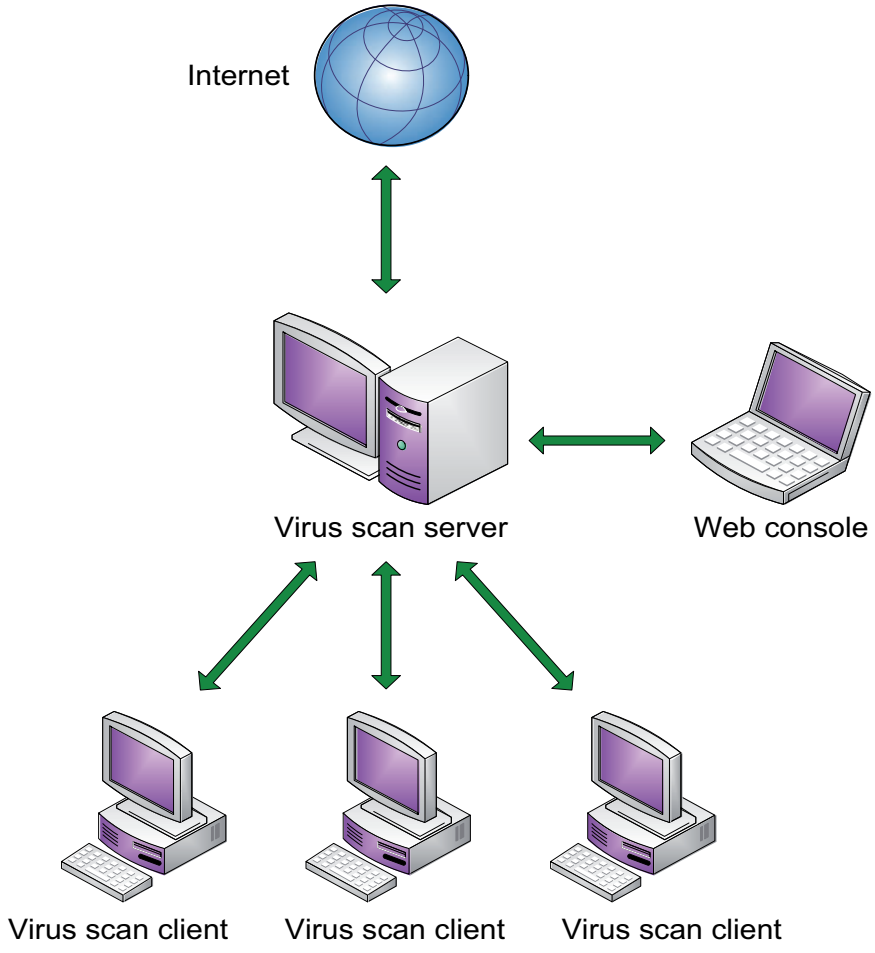
The following requirements are therefore set for virus scanners when used in industrial environments:

- When using a Security Suite (virus scanner plus options), all options that go beyond the functions of a traditional virus scanner must be capable of being deactivated, e.g. firewall, e-mail scan.
- It must be possible to deactivate the sending of data or reports to virus scanner manufacturers when a virus is found.
- In a centrally managed virus scanner architecture, it must be possible to divide the virus scanner clients into groups and to configure these clients.
- It must be possible to disable automatic distribution of virus signatures.
- It must be possible to distribute virus signatures manually and on a group basis.
- Manual and group-based file and system scans must be possible.
- When a virus is detected, a message must be generated in all cases but a file action (e.g. delete, block, move) must not necessarily be executed.
- All messages must be logged on the virus scanner server.
- The virus scanner clients must be configured in such a way that no message is displayed on them that could hide the more important process information.
- For performance reasons the virus scanner clients should be configured in such a way that only the local drives of the virus scanner clients are scanned in order to prevent overlapping scans on network drives.
- For performance reasons the virus scan clients should be configured in such a way that only the incoming data traffic is checked, provided that all data available locally has already been checked once.

2.3 Basic virus scanner architecture

A basic virus scanner architecture as illustrated in the following illustration is recommended for implementing the requirements stated in the "Using virus scanners" chapter.

The virus scan server receives its virus signatures from the update server of the respective virus scanner manufacturer on the Internet or from an upstream virus scan server and manages its virus scan clients. Administrative access to the virus scanner server is possible via a Web console or similar device.



Depending on the manufacturer it may also be possible to use multiple virus scan servers which can be arranged in parallel or in a hierarchy.

Configuration of McAfee VirusScan Enterprise 3

3.1 Introduction

Additional functions beyond the traditional virus scanner are released for the first time with McAfee VirusScan Enterprise (VSE) 8.8. The following configurations relate to the version of the VSE managed centrally which is configured using the McAfee ePolicy Orchestrator (ePO). In addition, only an English installation is referred to. All the configurations described are deviations from the default configurations, which means any settings not described are not changed.

3.2 VSE Functions

VSE has the following functions that can be configured with policies (available in the ePO under "Policy Catalog"):

- "Access Protection"
- "Alert"
- "Buffer Overflow Protection"
- "General Options"
- "On Delivery Email Scan"
- "On-Access Default Processes"
- "On-Access General"
- "On-Access High-Risk Processes"
- "On-Access Low-Risk Processes"
- "Quarantine Manager"
- "Unwanted Programs"

For use in a PCS 7 and WinCC environment, the following functions and settings are recommended and are tested for compatibility:

- "Access Protection" (conditional)
- "Alert"
- "Buffer Overflow Protection"
- "General Options"
- "On-Access Default Processes"
- "On-Access General"
- "Quarantine Manager"
- "Unwanted Programs"

The following functions are not recommended and are not checked in the compatibility test:

- "On Delivery Email Scan" – The use of e-mail programs is not recommended on PCS 7 and WinCC computers.
- "On-Access High-Risk Processes" – This function is a refinement of the "On-Access General" function. We recommend that you configure all PCS 7 and WinCC computers the same way and that you treat all data equally.
- "On-Access Low-Risk Processes" – This function is a refinement of the "On-Access General" function. We recommend that you configure all PCS 7 and WinCC computers the same way and that you treat all data equally.

This means you should not assign any policies to this function. The user is fully responsible for any use of functions and settings which are not recommended.

3.2.1 General

We recommend that you use the same policies for all PCS 7 and WinCC computers and that you make the same settings for the workstation and servers.

3.2.2 Access Protection

The following configurations refer to a new policy derived from the McAfee Default Policy.

Only the McAfee Default settings are checked for compatibility. Any change is system-specific and cannot be analyzed.

This setting should only be used by administrators with sound network and security knowledge and in systems that have their own security administration.

3.2.3 Alert

The following configurations refer to a new policy derived from the McAfee Default Policy.

No changes required.

3.2.4 Buffer Overflow Protection

The following configurations refer to a new policy derived from the McAfee Default Policy.

Buffer Overflow Protection

Buffer overflow settings-> Enable buffer overflow protection	Warning mode	Select

Client system warning	Show the messages dialog box when a buffer overflow is detected	Uncheck

3.2.5 General Options

The following configurations refer to a new policy derived from the McAfee Default Policy.

Display Options

System tray icon	Show the system tray icon with minimal menu options	Select

Console options	Allow this system to make remote console connections to other systems	Uncheck

Console options	Disable default AutoUpdate task schedule	Select

Console options	Enable splash screen	Uncheck

Password Options

User interface password	Password protection for all items listed	Select; choose a password

3.2.6 On-Access Default Processes

The following configurations refer to a new policy derived from the McAfee Default Policy.

Scan Items

Scan files	When reading from disk	Uncheck

Scan files	Opened for backup	Uncheck

Compressed files	Scan inside archives (e.g. .ZIP)	Check

Compressed files	Decode MINE encoded files	Check

Actions

When a thread is found	If the first action fails, then perform this action	Deny access to files

When an unwanted program is found	If the first action fails, then perform this action	Deny access to files

3.2.7 On-Access General

The following configurations refer to a new policy derived from the McAfee Default Policy.

General

Artemis (Heuristic network check for suspicious files	Sensitivity level	Disabled

ScriptScan

ScriptScan Exceptions	Processes	Add bfmappersrvx.exe

Blocking

Block the connection	Block the connection when a threatened file is detected in a shard folder	Uncheck

Messages

User messages	Show the messages dialog box when a threat is detected and display the specified text in the message	Uncheck

Actions available to user	Remove message from the list	Uncheck

Actions available to user	Clean files	Uncheck

3.2.8 Quarantine Manager

The following configurations refer to a new policy derived from the McAfee Default Policy.

No changes required.

3.2.9 Unwanted Programs

The following configurations refer to a new policy derived from the McAfee Default Policy.

No changes required.

3.2.10 Pattern Updates

The distribution of patten updates and other updates is not configured with the McAfee VirusScan Policies but with the "Product Update" Client Tasks of the McAfee Agent. We recommend to update the pattern time-delayed. More detailed information is available in the "Detail document Virus scanner administration" security concept.