SIEMENS

SIMATIC

Process Control System PCS 7 Trend Micro OfficeScan configuration (V11.0 SP1)

Commissioning Manual

03/2016

A5E37491480-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 Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E37491480-AA
Ⓟ 04/2016 Subject to change

Table of contents

Security information 1

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. You can find more information about industrial security under: http://www.siemens.com/industrialsecurity

To stay informed about product updates as they occur, sign up for a product-specific newsletter. You can find additional information on this at: http://support.automation.siemens.com.

Preface 2

This documentation describes the settings to be changed for Trend Micro OfficeScan 11.0 SP1 for use in an industrial plant. The configuration represents an extract of the settings from Trend Micro OfficeScan which were used in the compatibility test with PCS 7 and WinCC.

Important information about this whitepaper

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

These recommendations describe the best possible compromise currently known between the aim of discovering and disabling viruses and malware, and the aim of ensuring a time response that is as deterministic as possible for the process control system 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 the 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.

Required knowledge

This documentation is aimed at persons involved in the engineering, commissioning, and servicing of automation systems with SIMATIC PCS 7 or WinCC. Knowledge of administration and IT techniques for Microsoft Windows operating systems is assumed. In addition, readers should be familiar with the PCS 7 & WinCC security concept.

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

http://support.industry.siemens.com/cs (https://support.industry.siemens.com/cs/ww/en/view/60119725)

Scope 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.industry.siemens.com/cs (https://support.industry.siemens.com/cs/ww/en/view/2334224)

Virus scanner administration 3

3.1 Introduction

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.

3.2 Definitions

Virus scanners

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

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.

3.3 Using virus scanners

The use of a virus scanner should never inhibit runtime of a plant. 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.

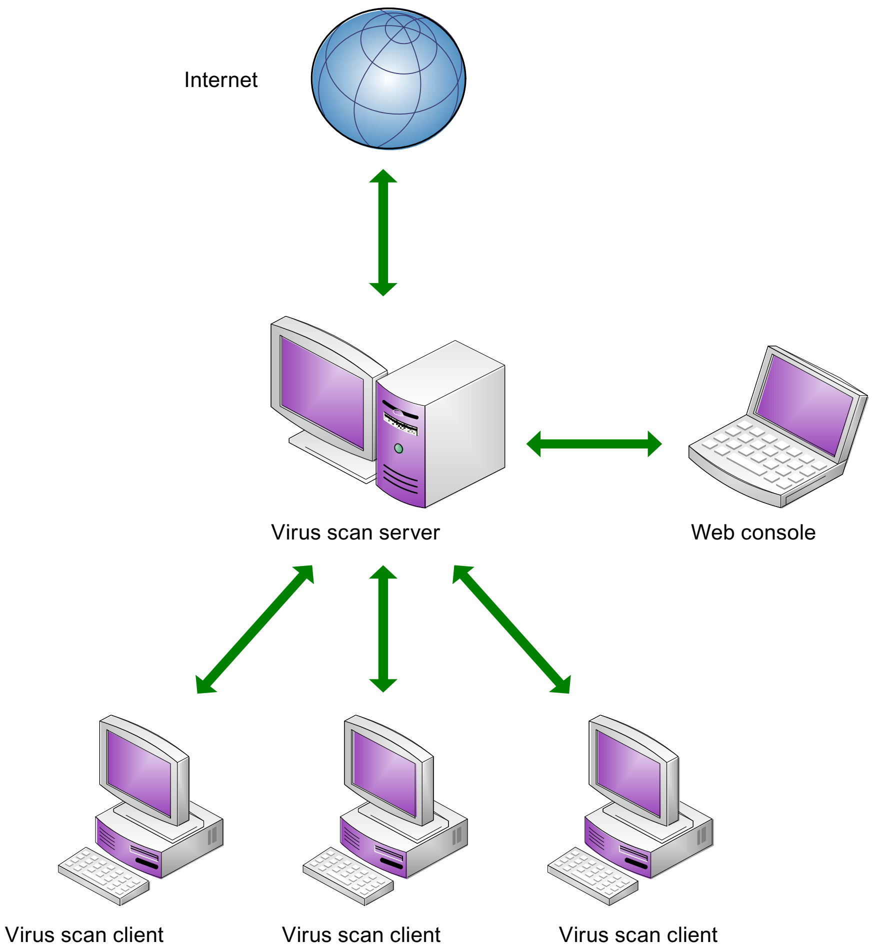
The following requirements are therefore set for virus scanners when used in industrial environments:

- When using a Security Suite (virus scanner plus options) then 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 sending data or reports to virus scanner manufacturers where a virus is found.
- It must be possible to divide the virus scan clients in a centrally managed virus scanner architecture into groups and this must be configurable.
- 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.
- Where a virus is detected a message must be generated in all cases but a file action must not be executed compulsorily (e.g. delete, block, move).
- All messages must be logged on the virus scanner server.
- The virus scan 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 scan clients should be configured in such a way that only the local drives of the virus scan 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.

3.4 Basic virus scanner architecture

A basic virus scanner architecture as illustrated in the following image 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 scan 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.

Trend Micro OfficeScan configuration 4

4.1 Introduction

Additional functions above and beyond the classic virus scanner are released with Trend Micro OfficeScan (TMOS) V11.0 SP1. The following configurations relate to the centrally managed version of TMOS as of version 11.0 SP1, which is configured using the TMOS Web Console. The use of a local, non-managed installation is allowed, but is not described. In addition, only an English installation is referred to. All the configurations described are deviations from the default configurations, i.e. any settings not described are not changed.

4.2 TMOS functions

TMOS provides the following functions (can be configured via the TMOS Web Console)

- Anti-Virus
- Firewall
- Behavior Monitor
- Device Control
- Smart Protection
- Updates

The following modules and settings are recommended and are tested for compatibility for use in a PCS 7 and WinCC environment:

- Anti-Virus
- Behavior Monitor (conditionally)
- Device Control
- Updates

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

- Firewall – Only the Windows Firewall is released for use with PCS 7 and WinCC as this is configured automatically depending on the product installed.
- Smart Protection – File and Web Reputation; exchanging data with third parties is not recommended.

Any use of modules and settings which are not recommended is the user's own responsibility.

4.2.1 Installation

The following options must be configured during the installation; all other options may retain the default configuration.

Installation/Setup	Install integrated Smart Protection Server	No. ...

Installation/Setup	Enable Trend Micro Smart Feedback	Uncheck

Installation/Setup	Enable Firewall	Uncheck

Installation/Setup	Anti Spyware Assessment Feature	No. ...

Installation/Setup	Enable webreputation policy	Uncheck

4.2.2 General information

All OfficeScan clients must be configured on the server as "Internal Clients".

4.2.3 Anti-Virus

The following configurations relate to a default installation.

Agents – Global Agent Settings

Scan Settings	Do not scan files in the compressed file if the size exceeds	Set to 1000
Scan Settings	In compressed file, scan only the first	Set to 100000
Scan Settings	Clean/Delete infected files within compressed files	Uncheck
Behavior Monitoring Settings	Monitor newly encountered programs downloaded through HTTP…	Uncheck
Alert Settings	Display a notification message if the client computer needs a restart to load a kernel mode driver	Uncheck

Agents – Agent Management

Settings -> Scan Settings -> Scan Methods	Conventional scan	Select
Settings-> Scan Settings-> Real-time Scan Settings-> Target-> User Activity on Files	Created/modified	Select
Settings -> Scan Settings -> Real-time Scan Settings-> Target-> Files to Scan	All scannable files	Select
Settings-> Scan Settings-> Real-time Scan Settings-> Target-> Files to Scan	Scan the boot sector of the USB storage device after plugging in	Check
Settings-> Scan Settings-> Real-time Scan Settings-> Target-> Files to Scan	Scan all files in removable storage device after plugging in	Check
Settings-> Scan Settings-> Real-time Scan Settings-> Target-> Files to Scan	Quarantine malware variants detected in memory	Check
Settings-> Scan Settings-> Real-time Scan Settings-> Target-> Scan Settings	Scan compressed files	Set to 6
Settings-> Scan Settings-> Real-time Scan Settings-> Target-> Scan Settings	Scan OLE objects	Set to 10
Settings-> Scan Settings-> Real-time Scan Settings-> Action-> Virus/Malware	Use the same action for all virus/malware types	Select Set 1st "Clean" Set 2nd "Quarantine"
Settings-> Scan Settings-> Real-time Scan Settings-> Action-> Spyware/Grayware	Deny access	Select
Settings-> Scan Settings-> Real-time Scan Settings-> Action-> Spyware/Grayware	Display a notification on endpoints when spyware/grayware is detected	Uncheck
Settings-> Scan Settings-> Real-time Scan Settings-> Action-> Virus/Malware	Display a notification message on the client computer when virus/malware is detected	Uncheck
Settings-> Privileges and other Settings-> Privileges-> Proxy Setting Privileges	Allow the client user to configure proxy settings	Uncheck
Settings-> Privileges and other Settings-> Privileges-> Component Update Privileges	Perform "Update Now!"	Uncheck
Settings-> Privileges and other Settings-> Other Settings-> Update Settings	Clients download updates from the Trend Micro ActiveUpdate Server	Uncheck
Settings-> Privileges and other Settings-> Other Settings-> Update Settings	Enable scheduled update	Uncheck

Settings-> Privileges and other Settings-> Other Settings-> Web Reputation Settings	Display a notification when a web site is blocked	Uncheck
Settings-> Privileges and other Settings-> Other Settings-> Behavior Monitoring Settings	Display a notification when a program is blocked	Uncheck
Settings-> Privileges and other Settings-> Other Settings-> C&C Contact Alert Settings	Display a notification when a C&C callback is detected	Uncheck
Settings-> Privileges and other Settings-> Other Settings-> Restart Notification	Display a notification message if the client computer needs a restart to finish cleaning infected files	Uncheck

4.2.4 Behavior Monitor

The following configurations relate to a default installation.

Networked Computers – Client Management

Behavior Monitor attempts to block malware based on the known behavior of harmful software. As it is only possible to block and not merely to report the malware, the user should give careful consideration as to whether this option should be activated. There is always a risk that known malware functions as harmless software and that there is therefore a false positive for this. A risk analysis for this situation is recommended.

If the option is to be used then nothing must be changed in the configuration.

If Behavior Monitor is not to be used then the following change must be made to the configuration.

Settings -> Behavior Monitor Settings	Enable Malware Behavior Blocking	Uncheck

4.2.5 Device Control

The following configurations relate to a default installation.

The use of Device Control is recommended if, for example, the use of USB devices is prevented.

Networked Computers – Client Management

Settings -> Device Control Settings -> Internal Clients-> Notification	Display a notification message on the client computer when OfficeScan detects unauthorized device access	Uncheck

4.2.6 Smart Protection

The following configurations relate to a default installation.

No changes required.

4.2.7 Updates

The following configurations relate to a default installation.

The settings for reaching the Trend Micro Update Server on the Internet or a higher-level update server must be adapted to the relevant network topology.

Updates – Agents - Automatic Update

Automatic Update (Networked Computers)-> Event-trigerred Update	Initiate component update on clients immediately after the OfficeScan server downloads a new component	Uncheck
Automatic Update (Networked Computers)-> Event-triggered Update	Let clients initiate component update when they restart and connect to the OfficeScan server (roaming clients are excluded)	Uncheck

Since is not possible to deactivate the "Schedule-based Update", select:

Automatic Update (Networked Computers)-> Schedule-based Update	Weekly, every	Set to a day of your choice