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**
with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken.

CAUTION
without a safety alert symbol, indicates that property damage can result if proper precautions are not taken.

**NOTICE**
indicates that an unintended result or situation can occur if the relevant information is not taken into account.

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.
# Table of contents

1 Preface......................................................................................................................................................... 5

2 Virus scanner administration........................................................................................................................ 7
   2.1 Introduction....................................................................................................................................7
   2.2 Definitions......................................................................................................................................8
   2.3 Using virus scanners..................................................................................................................... 9
   2.4 Basic virus scanner architecture..................................................................................................10

3 Configuration.............................................................................................................................................. 11
   3.1 Introduction..................................................................................................................................11
   3.2 Overview of the OS functions and modules................................................................................ 12
   3.3 OS functions and modules.......................................................................................................... 13
      3.3.1 Installation................................................................................................................................... 13
      3.3.2 General information.....................................................................................................................13
      3.3.3 Anti-Virus..................................................................................................................................... 13
      3.3.4 Behavior Monitor......................................................................................................................... 15
      3.3.5 Device Control............................................................................................................................. 15
      3.3.6 Smart Protection.......................................................................................................................... 16
      3.3.7 Updates....................................................................................................................................... 16
Preface

This documentation describes the settings to be changed from Trend Micro OfficeScan 10.6 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

Systems tested. 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 how to discover and make effective as comprehensively as possible the best possible compromise currently known between the target, virus and damage software, and ensure a time response that is as deterministic as possible for the PCS 7 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 virus scanner installation.

Skills 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.

Scope of the documentation

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

NOTICE

Note that certain virus scanners are only enabled 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/lisapi.dll?
func=cslib.csinfo&objid=2334224&objAction=csOpen&nodeid0=10806846&lang=de&siteid=csius&aktprim=0&extranet=standard&viewreg=WW)
2.1 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.
2.2 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.
2.3 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.
2.4 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.
3.1 Introduction

Additional functions above and beyond the traditional virus scanner are released for the first time with Trend Micro OfficeScan(OS) 10.6. The following configurations relate to the version of OS managed centrally which is configured using the OS Web Console. 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.
3.2 Overview of the OS functions and modules

OS has functions (can be configured via the OS Web Console)

- Anti-Virus
- Firewall
- Behavior Monitor
- Device Control
- Smart Protection
- Cisco NAC
- 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 (with reservations)
- 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 Reputation; exchanging data with third parties is not recommended.
- Cisco NAC – This involves system-specific settings that cannot be checked.

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

3.3.1 Installation

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

<table>
<thead>
<tr>
<th>Installation/Setup</th>
<th>Enable Trend Micro Smart Feedback</th>
<th>Uncheck</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation/Setup</td>
<td>Enable Firewall</td>
<td>Uncheck</td>
</tr>
</tbody>
</table>

Installing "Cisco NAC Server" is not recommended.

3.3.2 General information

All computers that have OfficeScan-Clients must be configured on the server as Internal Clients.

3.3.3 Anti-Virus

The following configurations relate to a default installation.

**Networked Computers – Global Client Settings**

<table>
<thead>
<tr>
<th>Scan Settings</th>
<th>Do not scan files in the compressed file if the size exceeds</th>
<th>Set to 1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Settings</td>
<td>In compressed file, scan only the first</td>
<td>Set to 100000</td>
</tr>
<tr>
<td>Alert Settings</td>
<td>Display a notification message if the client computer needs a restart to load a kernel mode driver</td>
<td>Uncheck</td>
</tr>
</tbody>
</table>

**Networked Computers – Client Management**

<table>
<thead>
<tr>
<th>Settings -&gt; Scan Settings -&gt; Scan Methods</th>
<th>Conventional scan</th>
<th>Select</th>
</tr>
</thead>
</table>
### 3.3 OS functions and modules

<table>
<thead>
<tr>
<th>Settings -&gt; Scan Settings -&gt; Real-time Scan</th>
<th>All scannable files</th>
<th>Select</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings-&gt; Target-&gt; Files to Scan</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Settings-&gt; Scan Settings-&gt; Real-time Scan</th>
<th>Scan compressed files</th>
<th>Set to 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings-&gt; Target-&gt; Scan Settings</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Settings-&gt; Scan Settings-&gt; Real-time Scan</th>
<th>Scan OLE objects</th>
<th>Set to 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings-&gt; Target-&gt; Scan Settings</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Settings-&gt; Scan Settings-&gt; Real-time Scan</th>
<th>Use the same action for all virus/malware types</th>
<th>Select</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings-&gt; Action-&gt; Virus/Malware</td>
<td>Set 1st &quot;Clean&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set 2nd &quot;Quarantine&quot;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Settings-&gt; Scan Settings-&gt; Real-time Scan</th>
<th>Display a notification message on the client computer when virus/malware is detected</th>
<th>Uncheck</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings-&gt; Action-&gt; Virus/Malware</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Settings-&gt; Privileges and other Settings-&gt; Privileges-&gt; Proxy Setting Privileges</th>
<th>Allow the client user to configure proxy settings</th>
<th>Uncheck</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings-&gt; Privileges and other Settings-&gt; Component Update Privileges</td>
<td>Perform &quot;Update Now!&quot;</td>
<td>Uncheck</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Settings-&gt; Privileges and other Settings-&gt; Other Settings-&gt; Update Settings</th>
<th>Enable scheduled update</th>
<th>Uncheck</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings-&gt; Privileges and other Settings-&gt; Other Settings-&gt; Update Settings</td>
<td>Clients can update components but not upgrade the client program or deploy hot fixes</td>
<td>Uncheck</td>
</tr>
</tbody>
</table>
3.3.4 **Behavior Monitor**

The following configurations relate to a default installation.

No changes required.

**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 then careful consideration should be given as whether the user wishes to have this option 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.

<table>
<thead>
<tr>
<th>Settings -&gt; Behavior Monitor Settings</th>
<th>Enable Malware Behavior Blocking</th>
<th>Uncheck</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display a notification when a program is blocked</td>
<td>Uncheck</td>
<td></td>
</tr>
<tr>
<td>Display a notification message if the client computer needs a restart to finish cleaning infected files</td>
<td>Uncheck</td>
<td></td>
</tr>
</tbody>
</table>

3.3.5 **Device Control**

The following configurations relate to a default installation.

The recommendation is only to use Device Control, in order to prevent the use of USB devices for example.

**Networked Computers – Client Management**

<table>
<thead>
<tr>
<th>Settings -&gt; Device Control Settings -&gt; Internal Clients-&gt; Notification</th>
<th>Display a notification message on the client computer when OfficeScan detects unauthorized device access</th>
<th>Uncheck</th>
</tr>
</thead>
</table>
3.3 OS functions and modules

3.3.6 Smart Protection

The following configurations relate to a default installation.

Smart Protection – Integrated Server

<table>
<thead>
<tr>
<th>Integrated Smart Protection Server Server</th>
<th>Enable File Reputation Service</th>
<th>Uncheck</th>
</tr>
</thead>
</table>

3.3.7 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 –Networked Computers-Automatic Update

<table>
<thead>
<tr>
<th>Updates –Networked Computers-Automatic Update</th>
<th>Initiate component update on clients immediately after the OfficeScan server downloads a new component</th>
<th>Uncheck</th>
</tr>
</thead>
</table>

| 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

<table>
<thead>
<tr>
<th>Automatic Update (Networked Computers)-&gt; Schedule-based Update</th>
<th>Weekly, every</th>
<th>Set to a day of your choice</th>
</tr>
</thead>
</table>