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.
# Table of contents

1  Security information ..............................................................................................................................5  
2  Preface ................................................................................................................................................7  
3  Configuration ........................................................................................................................................9  

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Introduction</td>
<td>9</td>
</tr>
<tr>
<td>3.2</td>
<td>Notice</td>
<td>9</td>
</tr>
<tr>
<td>3.3</td>
<td>Overview of SEP modules and functions</td>
<td>10</td>
</tr>
<tr>
<td>3.4</td>
<td>SEP modules and functions</td>
<td>11</td>
</tr>
<tr>
<td>3.4.1</td>
<td>General information</td>
<td>11</td>
</tr>
<tr>
<td>3.4.2</td>
<td>Virus and Spyware Protection</td>
<td>11</td>
</tr>
<tr>
<td>3.4.3</td>
<td>Intrusion Prevention</td>
<td>13</td>
</tr>
<tr>
<td>3.4.4</td>
<td>Host Integrity</td>
<td>13</td>
</tr>
<tr>
<td>3.4.5</td>
<td>Application and Device Control</td>
<td>13</td>
</tr>
<tr>
<td>3.4.6</td>
<td>LiveUpdate</td>
<td>13</td>
</tr>
<tr>
<td>3.4.7</td>
<td>Network Application Monitoring</td>
<td>14</td>
</tr>
</tbody>
</table>
Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines, and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens’ products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit:
https://www.siemens.com/industrialsecurity

Siemens’ products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer’s exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
Security information
This documentation describes the settings of Symantec Endpoint Protection (SEP) that need to be changed for use in an industrial plant.

The configuration represents an extract of the settings from SEP which were used in the compatibility test with PCS 7 and WinCC.

Important information about this whitepaper

Note

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 currently known, best-possible compromise between the objective of maximizing the detection and neutralization of virus software and malware and guaranteeing a highly deterministic time behavior of the PCS 7 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 virus scanner installation.

Required knowledge

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.

In addition, readers should be familiar with the PCS 7 & WinCC security concept.

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

Scope of the documentation

This documentation applies to process control systems that are realized with the corresponding PCS 7 or WinCC product version.

Note

Note that certain virus scanners are only approved for certain product versions. Additional information is available on the Internet at the following address:

Compatibility tool (https://www.siemens.com/kompatool)
3.1 Introduction

Symantec Endpoint Protection (SEP) activates additional functions going beyond the traditional virus scanner. The following configurations refer to the centrally managed SEP variant, which is configured using the SEP Manager. 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.

3.2 Notice

The following setting is essential for stable operation of PCS 7.

Under "Clients->My Company->Policies->External Communication Settings:

<table>
<thead>
<tr>
<th>Client Submission</th>
<th>Send anonymous data to Symantec</th>
<th>Uncheck</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Queries</td>
<td>Allow Insight lookups for thread detection</td>
<td>Uncheck</td>
</tr>
</tbody>
</table>

When this option is active, the virus scanner attempts to contact Symantec Server directly on the Internet during each file scan. There is a significant delay if the virus scanner cannot reach the server. This makes the stable operation of PCS 7 impossible.

All other check boxes under Submission Settings should also be cleared so that no internal information, even if it is anonymous, is sent to Symantec. The other options do not have a negative effect on PCS 7, however.

Client Restart

Clients should never be restarted automatically. You should disable an automatic restart in two places.

Under "Clients->My Company->Policies->General:

<table>
<thead>
<tr>
<th>Restart Settings</th>
<th>Restart method</th>
<th>No restart</th>
</tr>
</thead>
</table>

Generate a new policy under Install Packages->Client Install Settings:

<table>
<thead>
<tr>
<th>Restart Settings</th>
<th>Restart method</th>
<th>No restart</th>
</tr>
</thead>
</table>
3.3 Overview of SEP modules and functions

SEP has the following configurable modules that can be configured with policies (available in the SEP under "Policies"):

- Virus and Spyware Protection
- Firewall
- Intrusion Prevention
- Application and Device Control
- Host Integrity
- LiveUpdate
- Exceptions

Additional settings (available in the SEP Manager under Clients > Policies > Location-independent Policies and Settings):

- Custom Intrusion Prevention
- System Lockdown
- Network Application Monitoring

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

- Virus and Spyware Protection
- Intrusion Prevention
- Device Control
- Host Integrity (provisional)
- LiveUpdate
- Network Application Monitoring

The following modules and settings 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.
- Application Control – This involves computer-specific settings that cannot be checked.
- Exceptions – This involves system-specific settings that cannot be checked.
- Custom Intrusion Prevention – This involves plant-specific settings that cannot be checked.
- System Lockdown – This involves computer-specific settings that cannot be checked.

For this reason, no policies should be assigned for these modules and the settings should not be switched "On". Any use of modules and settings which are not recommended is the user's own responsibility.
3.4 SEP modules and functions

3.4.1 General information

The options for the policies which have to be configured have no locks next to them. We recommend that you “close” all locks (by clicking on them). This guarantees that the configuration of the virus scan client cannot be changed locally.

For the same reason we recommend that you, under Clients-> Policies-> Location-specific Settings-> Client User Interface Control Settings: Click Server Control and Customize and clear all the check boxes except for "Display the client" and "Display the notification area icon".

3.4.2 Virus and Spyware Protection

The following configurations relate to a newly created Default Policy.

<table>
<thead>
<tr>
<th>Windows Settings-&gt; Scheduled Scans-&gt; Scans-&gt;Administrator-Defined Scans</th>
<th>Daily Scheduled Scan</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Settings-&gt; Protection Technology-&gt; Auto-Protect-&gt; Actions-&gt; Actions-&gt; Actions (for &quot;Malicious&quot; and &quot;Security Risks&quot;)</td>
<td>First action</td>
<td>Leave alone (log only)</td>
</tr>
<tr>
<td>Windows Settings-&gt; Protection Technology-&gt; Auto-Protect-&gt; Actions-&gt; Remediation</td>
<td>Terminate processes automatically</td>
<td>Uncheck</td>
</tr>
<tr>
<td>Windows Settings-&gt; Protection Technology-&gt; Auto-Protect-&gt; Actions-&gt; Remediation</td>
<td>Stop services automatically</td>
<td>Uncheck</td>
</tr>
<tr>
<td>Windows Settings-&gt; Protection Technology-&gt; Auto-Protect-&gt; Notifications-&gt; Notifications</td>
<td>Display the Auto-Protect result dialog on the infected computer</td>
<td>Uncheck</td>
</tr>
<tr>
<td>Windows Settings-&gt; Protection Technology-&gt; Download Protection-&gt; Download Insight</td>
<td>Enable Download Insight to detect potential risk in downloaded files based on file reputation</td>
<td>Uncheck</td>
</tr>
<tr>
<td>Windows Settings-&gt; Protection Technology-&gt; Download Protection-&gt; Actions-&gt; Malicious files</td>
<td>First action</td>
<td>Leave alone (log only)</td>
</tr>
</tbody>
</table>
### Configuration

#### 3.4 SEP modules and functions

| Windows Settings-> Protection Technology-> Download Protection-> Actions-> Unproven files | Specify action for unproven files | Leave alone (log only) |
| Windows Settings-> Protection Technology-> Download Protection-> Notifications-> Notifications | Display a notification message on the infected computer | Uncheck |
| Windows Settings-> Protection Technology-> SONAR-> SONAR Settings | Enable SONAR | Uncheck |
| Windows Settings-> Email Scans-> Internet Email Auto-Protect-> Scan Details | Enable Internet Email Auto-Protect | Uncheck |
| Windows Settings-> Email Scans-> Microsoft Outlook Auto-Protect-> Scan Details | Enable Microsoft Outlook Email Auto-Protect | Uncheck |
| Windows Settings-> Email Scans-> Lotus Notes Email Auto-Protect-> Scan Details | Enable Lotus Notes Email Auto-Protect | Uncheck |
| Windows Settings-> Advanced Options-> Global Scan Options | Display notifications about detections | Uncheck |
| Windows Settings-> Advanced Options-> Quarantine-> General-> When New Virus Definitions Arrive | Specify how client computers handle items in the Quarantine | Do Nothing |
| Windows Settings-> Advanced Options-> Quarantine-> General-> Quarantined Items | Allow client computers to manually submit quarantined items… | Uncheck |
| Windows Settings-> Advanced Options-> Quarantine-> Cleanup-> Repaired Files | Enable automatic deleting of backup files | Uncheck |
| Windows Settings-> Advanced Options-> Quarantine-> Cleanup-> Backup Files | Enable automatic deleting of repaired files | Uncheck |
3.4 SEP modules and functions

### 3.4.3 Intrusion Prevention

The following configurations relate to a newly created Default Policy.

No changes required.

### 3.4.4 Host Integrity

Using "Host Integrity" you can monitor the configuration and the behavior of computers. This monitoring has to be configured specifically for the plant. Care should be taken to ensure that no dialog boxes or messages appear on the local client.

### 3.4.5 Application and Device Control

The following configurations relate to a newly created Default Policy.

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

All check boxes should be cleared under "Application Control".

### 3.4.6 LiveUpdate

The following configurations relate to a newly created Default Policy.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Settings-&gt; Advanced Options-&gt; Quarantine-&gt; Cleanup-&gt; Quarantined Files</td>
<td>Enable automatic deleting of quarantined files that could not be repaired</td>
</tr>
<tr>
<td>Windows Settings-&gt; Advanced Options-&gt; Miscellaneous-&gt; Notifications-&gt; Notifications</td>
<td>Display error messages with a URL to a solution</td>
</tr>
<tr>
<td>Windows Settings-&gt; Schedule-&gt; Live-Update Scheduling</td>
<td>Enable LiveUpdate Scheduling</td>
</tr>
<tr>
<td>Windows Settings-&gt; Advanced Settings-&gt; User Settings</td>
<td>Allow the user to manually launch LiveUpdate</td>
</tr>
</tbody>
</table>
3.4 SEP modules and functions

### 3.4.7 Network Application Monitoring

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

The setting "Network Application Monitoring" is under "Clients-> My Company-> Policies-> Location-independent Policies and Settings-> Network Application Monitoring".

The inheritance settings have to be changed here, depending on the company and network topology.

<table>
<thead>
<tr>
<th>Network Application Monitoring</th>
<th>Enable network application monitoring</th>
<th>Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Application Monitoring</td>
<td>When an application change is detected</td>
<td>Allow and Log</td>
</tr>
</tbody>
</table>

| Windows Settings-> Advanced Settings-> User Settings | Allow the user to modify HTTP, HTTPS, or FTP proxy settings for LiveUpdate | Uncheck |