SIEMENS

Configuration 2

SIMATIC

Process Control System PCS 7 Symantec Endpoint Protection 11.0 Configuration

Commissioning Manual

08/2009 A5E02634984-01

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.

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 corresponding 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 for the specific task, 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:

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 adhered to. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of the 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 Industry Sector Postfach 48 48 90026 NÜRNBERG GERMANY A5E02634984-01 @ 08/2009

Table of contents

1	Using virus scanners				
	1.1	Preface	5		
	1.2 1.2.1 1.2.2 1.2.3 1.2.4	Using virus scanners Introduction Definitions and information Principle structure of the virus scanner architecture Using antivirus software	6 6 7 8		
2	Configur	ation	9		
	2.1	Introduction	9		
	2.2	Client Modules	9		
	2.3	Policies	9		
	2.4	Virus Definition Manager	.10		
	2.5 2.5.1 2.5.2 2.5.3 2.5.4 2.5.5 2.5.6 2.5.7	File System Auto-Protect File System Auto-Protect File System Email Protection Antispyware Protection – TruScan Proactive Threat Scans Quarantine settings Report Submission settings Miscellaneous settings	.12 .12 .12 .18 .19 .21 .23 .24		
	2.6	Client Administrator and Tamper Protection Options	.28		
	2.7	Endpoint Console Firewall Settings	.31		
	2.8	Endpoint Intrusion Detection Settings	.33		

Using virus scanners

1.1 Preface

Important information about this whitepaper

The compatibility of the virus scanners recommended for PCS 7 and WinCC has been tested with the systems. The recommended settings for these virus scanners have been chosen to ensure 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 currently known, best possible compromise between the target, virus and damage software, and ensure an as determinable as possible time response of the PCS 7 control system can be achieved 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 virus scanner installation.

Required knowledge

This documentation is aimed at anyone who is involved in configuring, commissioning and operating 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.

NOTICE

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

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

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

1.2 Using virus scanners

1.2 Using virus scanners

1.2.1 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 cannot protect a process control system against hostile attacks.

The security concept PCS 7 / WinCC is available on the Internet under:

http://support.automation.siemens.com

Virus scanners should comply with the requirements described in the security concepts of PCS 7 / WinCC.

1.2.2 Definitions and information

Basic principle

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

Virus scanners

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

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 through 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 deploys them on the virus scan clients.

1.2 Using virus scanners

1.2.3 Principle structure of the virus scanner architecture

A virus scan server receives its virus signatures from the update server of the respective virus scan manufacturer in the Internet or from an upstream virus scan server and manages its virus scan clients.

Remote access to the virus scan server is available via web console.



1.2 Using virus scanners

1.2.4 Using antivirus software

Information for configuration of local virus scanners

• Integrated firewall of the virus scanner

The local Windows firewall is used as of PCS 7 V7.0 and configured with the SIMATIC Security Control (SSC) component. The firewalls integrated in the virus scanners are therefore not installed.

- Manual scan (manual scan, on demand scan) A manual scan should never be performed on virus scan clients during process mode (runtime). This should take place at regular intervals, e.g. during maintenance, on all computers of the system.
- Automatic scan (auto-protect, on-access scanning) With automatic scanning, it is sufficient to check the incoming data traffic.
- Scheduled scan (planned search, on demand scan) A scheduled scan should never be performed on virus scan clients during process mode (runtime).
- Displaying messages

To ensure that process mode is not inhibited, no messages should be displayed on the virus scan clients.

• Drives

To avoid overlapping scanning of network drives, only local drives are scanned.

• E-mail scan

Scanning of e-mail can be disabled except on the engineering station which receives e-mails.

• Division into groups

Organize your virus scan clients in groups.

• Deployment of the virus signature (pattern update)

The deployment of the virus signatures to the virus scan clients is performed by the upstream virus scan server. Test the virus signatures in a test system before deploying them in process mode to ensure that work correctly. Distribute the virus signatures manually to the respective groups.

• Update the virus scan engine

Do not conduct the virus scan engine update in runtime as these updates will probably require you to restart the virus scan client.

Note on installation

The software installation must be carried out from a virus-free storage location (e.g. from a file server with its own virus scanner or from a certified DVD). During the software installation, automatic changes are often carried out in the operating system. An enabled virus scanner must not obstruct or falsify the software installation.

Configuration

2.1 Introduction

Symantec Endpoint Protection 11.0 by Symantec is the successor to Norton Antivirus 10.2. Only version 11.0 of the Symantec Endpoint Protection virus scanner has been approved for some versions of PCS 7. The settings described below that have changed in comparison to the standard version were tested for PCS7.

Approved virus scanners for the following PCS 7 versions

You can find the latest overview of the virus scanners authorized for a PCS 7 version at the following Internet address: http://support.automation.siemens.com/WW/view/en/10154608

2.2 Client Modules

The only module that needs to be enabled in the "Deployment Wizard" dialog is "Antivirus and Antispyware Protection". The following client modules should be disabled:

- Email Protection
- Network Threat Protection
- Proactive Threat Protection

These client modules should also be disabled on the management server.

2.3 Policies

Client groups (computer groups) can be assigned different settings.

The settings for client groups are defined by policies. Each program component (antivirus, firewall, updates, etc.) has its own policy, which has to be defined in the Endpoint Protection Manager Console.

2.4 Virus Definition Manager

Updates

The following distinctions should be noted:

- Management server updates are set as local properties of a computer.
- Client updates are defined as a "policy".

Server update settings in the "Site Properties" dialog box

• Menu Admin > Servers > Edit Site Properties > "LiveUpdate" tab "Frequency" option button: Continuously

Symant	ec Endpoint Protection Manager Co	nsole 🔽	
🔘 Syr	mantec™ Endpoint Protectio	on Man	
Monitors Eleme Monitors Reports Elecies	View Servers Servers	Site N Site I Replin Creat	General Log Settings LiveUpdate Database Download Schedule Specify when you want LiveUpdate to run. Frequency: Continuously Every 4 + hours Daily Weekly Select download start time window Start: 12 : 00 PM End: 12 : 00 AM Every: Tuesday Image: Select download Content Types to Download The following product updates and signatures will be downloaded. Change Selection Client updates Antivirus and antispyware definitions Image: Selection Change Selection Languages to Download Updates and signatures will be downloaded for the following languages. Image: Selection
Admin	Tasks	24. Juni 24. Juni 24. Juni 24. Juni	English Change Selection LiveUpdate Source Servers Using default Symantec LiveUpdate server Using default Symantec LiveUpdate server Edit Source Servers Disk Space Management for Downloads Number of content revisions to keep: 3 Ive Store client packages unzipped to provide better network performance for upgrades Ive Store client packages unzipped to provide better network performance for upgrades
	Install Packages	24. Juni	OK Cancel Help ye

Client update settings in the "Site Properties" dialog box

 Menu Policies > Live Update Policy > "Server Settings" tab "Use the default management server" check box: Selected

🛑 LiveUpdate Policy	×							
🚕 LiveUpdate	Server Settings							
Policy	Internal or External LiveUpdate Server							
Overview	Select the source server that will be used by this policy to retrieve updates. If both the default management server and a							
Schedule	LiveUpdate server are selected, the client computer will retrieve updates from both servers.							
Advanced Settings	Use a LiveUpdate server							
	Ise the default Sumanter Livel Indate server							
	C Use a specified internal Livel Indete server							
	Name Address Addr							
	Crown Underte Dravidae							
	If the local network has a client designated as the Group Llodate Provider, clients will pull their updates from this local							
	computer rather than one of the LiveUpdate servers. If the Group Update Provider, clients will plui their updates from this local server selected above will be used.							
	Use the Group Update Provider as the default LiveUpdate server Group Update Provider							
	Group Update Provider: <none assigned=""></none>							
	Third Party Management							
	Instead of getting content directly from the management server or LiveUpdate server, you can use third party tools. See the Administrator's Guide for more information.							
	Enable third party content management							
	OK Cancel Help							

Only enabled update options can serve as a source for updates. Clients are not updated if both update options are disabled.

When both update options are enabled, clients only obtain updates from the "Management Server".

For manual deployment of the virus definition files, enable this check box only for deploying virus definition files. The deployment of the virus definition files is performed automatically when this check box is selected.

Check the deployment in the log.

2.5 File System Auto-Protect

2.5.1 File System Auto-Protect

This option was known as "Client Auto-Protect" in ealier versions of Symantec antivirus software.

2.5.2 File System

File System Auto-Protect settings in the "Scan Details" dialog box

Menu Policies > Antivirus and Antispyware > File System Auto-Protect > "Scan Details" tab

- "Enable File System Auto-Protect" check box: Selected
- "Block security risks from being installed" check box: Cleared
- "Network Settings" check box: Cleared
- "Check floppies for boot viruses when accessed" check box: Selected

WAntivirus and Antispyware Policy							
Antivirus and Antispyware	File System Auto-Protect						
Policy	Scan Details Actions Notifications Advanced						
Overview	Enable File System Auto-Protect						
Administrator-defined Scans	Scamping						
File System Auto-Protect	Scanning						
Internet Email Auto-Protect	Specify what files or processes are scanned by Auto-Protect.						
Microsoft Outlook Auto-Protect	File types:						
Lotus Notes Auto-Protect	🍐 💿 Scan all files						
TruScan Proactive Threat Scans	C Scan only selected extensions: Select Extensions						
Quarantine	Determine file types by examining file contents						
Submissions							
Miscellaneous	Additional options:						
	i Scan for security risks						
	Block security risks from being installed						
	Advanced Scanning and Monitoring						
	Network Settings						
	Specify network options for scanning files on remote computers.						
	Network: Network Settings						
	Floppy Settings						
	Specify options for scanning floppies.						
	Check floppies for boot viruses when accessed						
	When a boot virus is found:						
	Leave alone (log only)						
	OK Cancel Help						

File System Auto-Protect settings in the "Advanced Scanning and Monitoring" dialog box

Menu Policies > Antivirus and Antispyware > File System Auto-Protect > "Scan Details" tab > Advanced Scanning and Monitoring...

- "Scan when a file is modified" option button: Selected
- "Scan when a file is backed up" check box: Selected
- "Delete newly created infected files if the action is 'Leave alone (log only)" check box: Cleared

WAdvanced Scanning and Monitoring					
Scan Files When					
Specify activities that trigger automatic scans.					
C Scan when a file is accessed or modified					
Scan when a file is modified					
Scan when a file is backed up					
Other Options					
Delete newly created infected files if the action is 'Leave alone (log only)'					
Preserve file times					
Bloodhound(TM) Detection Settings					
Configure Bloodhound(TM) detection to scan files for suspicious behavior.					
Enable Bloodhound(TM) heuristic virus detection					
Level of protection to use: Default					
OK Cancel Help					

File System Auto-Protect settings in the "Actions" dialog box

Menu Policies > Antivirus and Antispyware > File System Auto-Protect > "Actions" tab

- Selection in "First action" drop-down list: Leave alone (log only) This selection also applies to "Non-macro virus" and "Security Risks"
- "Back up files before attempting to repair them" check box: Cleared
- "Terminate processes automatically" check box: Cleared
- "Stop services automatically" check box: Cleared

🖤 Antivirus and Antispyware Policy						×
Antivirus and Antispyware	File System Auto-Protect					
Policy	Scan Details	Actions	Notifications	Advanced]	
Overview	Actions					
Administrator-defined Scans	Constitution of the					
File System Auto-Protect	Detection Actions for: Macro virus					
Internet Email Auto-Protect	Macro virus	IS	Holions for.			
Microsoft Outlook Auto-Protect	Non-macro	virus	Specify first a	nd second actio	ons for detections	
Lotus Notes Auto-Protect	Adware	:KS	of this type of	risk.		
TruScan Proactive Threat Scans	Dialers Heak Tes	le.	First action:	<u>a</u> F	eave alone (log only) 🗾	
Quarantine	Joke Prog	yram s	If first action fails: 🙈 Quarantine risk			
Submissions	Other Remote 4	locess				
Miscellaneous	Spyware	,				
	Remediation Select remediation actions for the scan. Image: Back up files before attempting to repair them Image: Back up files before attempting to repa					
					ОК	Cancel Help

File System Auto-Protect settings in the "Notifications" dialog box

Menu Policies > Antivirus and Antispyware > File System Auto-Protect > "Notifications" tab

- "Display a notification message on the infected computer" check box: Cleared
- "Display the Auto-Protect results dialog on the infected computer" check box: Cleared



File System Auto-Protect settings in the "Advanced" dialog box

Menu Policies > Antivirus and Antispyware > File System Auto-Protect > "Advanced" tab

- "Check floppies when the computer shuts down" check box: Cleared
- "Enable after..." check box: Cleared
- "Wait until the computer is restarted" option button: Selected

🛡 Antivirus and Antispyware Policy	<u>×</u>					
Antivirus and Antispyware	File System Auto-Protect					
Policy	Scan Details Actions Notifications Advanced					
Overview	Startun and Shitrdown					
Administrator-defined Scans	Sherifu startun and shutdown ontions					
File System Auto-Protect	specify startup and shutdown options.					
Internet Email Auto-Protect	Load Auto-Protect when:					
Microsoft Outlook Auto-Protect	Computer starts					
Lotus Notes Auto-Protect	O Symantec Endpoint Protection starts					
TruScan Proactive Threat Scans	Check floppies when the computer shuts down					
Quarantine	Auto-Protect Reloading and Enablement					
Submissions	Sherifu Auto-Protect load ortions					
Miscellaneous						
·	When Auto-Protect must be reloaded:					
	V vvair unim me computer is restarted					
	Additional Options					
	Configure options for the file cache and Risk Tracer.					
	File Cache Risk Tracer					
	OK Cancel Help					

File System Auto-Protect settings in the "File Cache" dialog box

Menu Policies > Antivirus and Antispyware > File System Auto-Protect > "Advanced" tab > "File Cache..." dialog



File System Auto-Protect settings in the "Risk Tracer" dialog box

Menu **Policies > Antivirus and Antispyware > File System Auto-Protect >** "Advanced" tab > "Risk Tracer..." dialog

🔍 Risk Tracer					
Risk Tracer					
Specify Risk Tracer options. Risk Tracer can identify the source of network-based virus infections.					
🙆 🗖 Enable Risk Tracer					
Resolve the source computer IP address					
Poll for network sessions every:					
10000 milliseconds (1 to 30000)					
OK Cancel Help					

2.5.3 Email Protection

E-mail virus protection is not necessary in a PCS 7 environment because the options for Internet Email, Microsoft Outlook and Lotus Notes are disabled.

Menu Policies > Antivirus and Antispyware Policy >

Make these setting in the following tabs:

- "Internet Email Auto-Protect" tab
- "Microsoft Outlook Auto-Protect" tab
- "Lotus Notes Auto-Protect" tab

Setting

• "Internet Email Auto-Protect" check box: Cleared

WAntivirus and Antispyware Policy							
Antivirus and Antispyware	Internet Email Auto-Protect						
Policy	Scan Details Actions Notifications Advanced						
Overview							
Administrator-defined Scans							
File System Auto-Protect	Scanning						
Internet Email Auto-Protect	Specify which files will be scanned.						
Microsoft Outlook Auto-Protect							
Lotus Notes Auto-Protect	File types:						
TruScan Proactive Threat Scans	Scan al files						
Quarantine	O Scan only selected extensions: Select Extensions						
Submissions							
Miscellaneous	🖀 🗹 Scan files inside compressed files						
	OK Cancel Help						

2.5.4 Antispyware Protection – TruScan Proactive Threat Scans

Introduction

Antispyware protection is not necessary because it is performed by other applications; all settings need to be disabled.

TruScan Proactive Threat Scans settings in the "Scan Details" dialog box

Menu Policies > Antivirus and Antispyware Policy > TruScan Proactive Threat Scans > "Scan Details" tab

- "Scan for trojans and worms" check box: Cleared
- "Scan for keyloggers" check box: Cleared

🛑 Antivirus and Antispyware Policy	×					
Antivirus and Antispyware	TruScan Proactive Threat Scans					
Policy	Scan Details Notifications Scan Frequency					
Overview	Scanning					
Administrator-defined Scans						
File System Auto-Protect						
Internet Email Auto-Protect	Scan for trojans and worms					
Microsoft Outlook Auto-Protect	Use defaults defined by Symantec					
Lotus Notes Auto-Protect	The When a trojan or worm is detected within the sensitivity threshold:					
TruScan Proactive Threat Scans						
Quarantine	Sensitivity: 1 100					
Submissions						
Miscellaneous						
	Market Set and the Symmetric Symmetric Symmetric Symmetry Symmetric Symmetry Sym					
	🎦 When a keylogger is detected within the sensitivity threshold: 🛛 💽					
	🎦 Sensitivity: 💿 Low 🔿 High					
	Detecting Commercial Applications Specify what action to take when a scan detects a commercial application that can be used for malicious purposes.					
	When a commercial keylogger is detected:					
	When a commercial remote control application is detected:					
	OK Cancel Help					

TruScan Proactive Threat Scans settings in the "Notifications" dialog box

Menu Policies > Antivirus and Antispyware Policy > TruScan Proactive Threat Scans > "Notifications" tab

• "Display a message when there is a detection" check box: Cleared

🛡 Antivirus and Antispyware Policy							×
Antivirus and Antispyware	TruScan Proactive Threat Scans						
Policy	Scan Details	Notifications	Scan Frequency				
Overview							
Administrator-defined Scans	Notification	ns					
File System Auto-Protect	Specify how	to notify about scar	results.				
Internet Email Auto-Protect		🗌 Display a messag	e when there is a detec	tion			
Microsoft Outlook Auto-Protect		Prompt before ter	minating a process				
Lotus Notes Auto-Protect	<u></u>	Prompt before sto	pping a service				
TruScan Proactive Threat Scans							
Quarantine							
Submissions							
Miscellaneous							
					ОК	Cancel	Help

2.5.5 Quarantine settings

Quarantine settings in the "General" dialog box

Menu Policies > Antivirus and Antispyware Policy > Quarantine > "General" tab

• "Do nothing" option button: Selected

🛞 Antivirus and Antispyware Policy		×
Antivirus and Antispyware	Quarantine	
Policy	General Cleanup	
Overview	When New Virus Definitions Arrive	
Administrator-defined Scans	Specify how client computers handle tems in the Quarantine	.
File System Auto-Protect		
Internet Email Auto-Protect	O Automatically repair and restore files in Quarantine silently	
Microsoft Outlook Auto-Protect	C Repair files in Quarantine silently without restoring	
Lotus Notes Auto-Protect	C Prompt user	
TruScan Proactive Threat Scans	Do nothing	
Quarantine	Local Quarantino Ontione	
Submissions		.
Miscellaneous	specify whether to use the default quarantine folder or a custom quarantine folder.	
	O Use the default quarantine folder	
	C Specify the quarantine folder:	
	Browse	
	OK Cancel He	lp

Quarantine settings in the "Cleanup" dialog box

Menu Policies > Antivirus and Antispyware Policy > Quarantine > "Cleanup" tab

- "Enable automatic deleting of repaired files" check box: Cleared
- "Enable automatic deleting of backup files" check box: Cleared
- "Enable automatic deleting of quarantined files that could not be repaired" check box: Cleared

Antivirus and Antispyware Policy	<u>×</u>
Antivirus and Antispyware	Quarantine
Policy	General Cleanup
Administration defined Conne	Repaired Files
	Sets the number of days to keep repaired files before they are automatically removed from the computer.
File System Auto-Protect	Enable automatic deleting of repaired files
Internet Email Auto-Protect	
Microsoft Outlook Auto-Protect	
Lotus Notes Auto-Protect	Delete oldest files to limit folder size at: 50 MB
TruScan Proactive Threat Scans	Backup Files
Quarantine	Sets the number of days to keep backup files before they are automatically removed from the computer.
Submissions	Enable automatic deleting of backup files
Miscellaneous	
	Delete oldest files to limit folder size at: 50 MB
	Quarantined Files
	Sets the number of days to keep quarantined files before they are automatically removed from the computer.
	Enable automatic deleting of quarantined files that could not be repaired
	Delete after: 30 🖨 days
	Delete oldest files to limit folder size at: 50 MB
	OK Cancel Help

2.5.6 Report Submission settings

A client cannot sent a report; it can only log it for the server (Log only). "Report Submissions" therefore must be disabled.

Submissions settings

Menu Policies > Antivirus and Antispyware Policy > Submissions

- "Allow client computers to submit processes detected by scans" check box: Cleared
- "Allow client computers to submit threat detection rates" check box: Cleared
- "Allow client computers to manually submit quarantined items to Symantec Security Response" check box: Cleared

🛑 Antivirus and Antispyware Policy	X					
Antivirus and Antispyware	Submissions					
Policy	TruScan Proactive Threat Scans					
Overview	Specify whether client computers automatically send information to Symantec Security Response about processes that					
Administrator-defined Scans	are detected by TruScan proactive threat scans.					
File System Auto-Protect	Allow client computers to submit processes detected by scans					
Internet Email Auto-Protect	Percentage of client computers allowed to submit: 100					
Microsoft Outlook Auto-Protect						
Lotus Notes Auto-Protect	Detection Rates					
TruScan Proactive Threat Scans	Specify whether client computers automatically send information to Symantec Security Response about threat detection					
Quarantine	rates that are determined by Auto-Protect and manual scans.					
Submissions	Allow client computers to submit threat detection rates					
Miscellaneous	Percentage of client computers allowed to submit: 100					
1	Our sufficient Manua					
	Specify how quarantined items on client computers are submitted to Symantec Security Response. Client computers can submit items directly to Symantec or to a Quarantine Server, which scans the items before sending them to Symantec					
	I Allow client computers to manually submit quarantined items to Symantec Security Response					
	Allow client computers to automatically submit quarantined items to a Quarantine Server					
	Server name:					
	Port: 33					
	Retry: 600 🖨 seconds					
	OK Cancel Help					

2.5.7 Miscellaneous settings

Settings in the "Miscellaneous" tab

Menu Policies > Antivirus and Antispyware Policy > Miscellaneous > "Miscellaneous" tab

- Selection in "Disable Windows Security Center" drop-down list: Never
- Selection in "Display antivirus events within Windows Security Center" drop-down list: **Disable**



Settings in the "Log Handling" tab

Menu Policies > Antivirus and Antispyware Policy > Miscellaneous > "Log Handling" tab

• Selection in "Show" drop-down list: All antivirus and antispyware events The settings should correspond to those in the figures below.

🔘 Antivirus and Antispyware Policy	×
Antivirus and Antispyware	Miscellaneous
Policy	Miscellaneous Log Handling Notifications
Overview	Antivirus and Antispyware Log Event Filtering
Administrator-defined Scans	All events checked will be sent from the client to the management server
File System Auto-Protect	
Internet Email Auto-Protect	Show: All antivirus and antispyware events
Microsoft Outlook Auto-Protect	File backed up/restored to/from Quarantine
Lotus Notes Auto-Protect	File forwarded to Quarantine Server
TruScan Proactive Threat Scans	File forwarded to Symantec
Quarantine	File not scanned
Submissions	☑ Scan aborted
Miscellaneous	☑ Scan started
·	✓ Scan stopped
	Security Risk detection operation
	Log Retention
	Select the time period to retain antivirus and antispyware logs.
	Delete loos older than:
	Log Event Aggregation
	Specify how often client computers send aggregated events to the server.
	Send aggregated events every: 5 🖨 minutes
	OK Cancel Help

2.5 File System Auto-Protect

- File backed up/restored to/from Quarantine
- File forwarded to Quarantine Server
- File forwarded to Symantec
- 🔲 File not scanned
- 🗹 Scan aborted
- 🗹 Scan started
- 🔽 Scan stopped
- Security Risk detection operation
- 🗹 Security Risk side effect repair failed
- 🗹 Security Risk side effect repair pending
- ☑ Security Risk side effect repaired successfully
- TruScan proactive threat detection known
- TruScan proactive threat detection permitted
- TruScan proactive threat scanning is not supported on this platform
- Client running without virus definitions
- New virus definitions assigned
- ☑ Virus definition rollback
- Virus definition update information
- Antivirus installed
- Configuration change
- 🗹 Uninstall
- ☑ Uninstall rolled back
- Error loading services
- Service shutdown
- 🗹 Service startup
- Services loaded
- 🔽 Services unloaded

Settings in the "Notifications" tab

Menu Policies > Antivirus and Antispyware Policy > Miscellaneous > "Notifications" tab

- "Display a warning when definitions are outdated" check box: Cleared
- "Display a warning when Symantec Endpoint Protection is running without virus definitions" check box: **Cleared**
- "Display error messages with a URL to a solution" check box: Cleared

🛞 Antivirus and Antispyware Policy	
Antivirus and Antismavare	Miscellaneous
	Miscellaneous Log Handling Notifications
Overview	Notifications
Administrator-defined Scans	Configure different types of patifications
File System Auto-Protect	Display a warping when definitions are outdated
Internet Email Auto-Protect	
Microsoft Outlook Auto-Protect	Warn after: 14 🚽 days
Lotus Notes Auto-Protect	Display a warning when Symantec Endpoint Protection is running without virus definitions
TruScan Proactive Threat Scans	Warn after: 2 🚔 remediation attempts Warning
Quarantine	Display error messages with a URL to a solution
Submissions	Display the LIRL to a Symantec Technical Support Knowledge Base article.
Miscellaneous	
	Display a custom onc. pp.//www.symantec.com/techsupp/serviet/#roductivessages
	Customize Error Message
	OK Cancel Help

2.6 Client Administrator and Tamper Protection Options

2.6 Client Administrator and Tamper Protection Options

You can find the general settings below.

Menu Clients > "Policies" tab > General Settings



Configuration

2.6 Client Administrator and Tamper Protection Options

Security and privileges settings

Menu Clients > "Policies" tab > General Settings > "Security Settings" tab

- "Require a password to stop the client service" check box: Cleared
- "Require a password to uninstall the client" check box: Cleared
- Enter password

🔲 General Settings for Global	×
General Settings Security Settings Tamper Protection	_
Client Password Protection	
Require a password to open the client user interface Password:	
Require a password to stop the client service Confirm password:	
Require a password to import or export a policy	
Require a password to uninstall the client	
- Coourity Pottingo	
Block all traffic until the firewall starts and after the firewall stops	
Eaching accurate communications between the menogramment convex and eligible humaing digital contrification	
for authentication	
OK Cancel Help	

Tamper Protection settings

Menu Clients > "Policies" tab > General Settings > "Tamper Protection" tab

- "Protect Symantec security software from being tampered with or shut down" check box: **Selected**
- Selection in "Actions to take..." drop-down list: Log the event only
- "Display a notification message when tampering is detected" check box: Cleared

🔘 General Setting	s for Global				×
General Settings	Security Settings	Tamper Protection			
Actions to	antec security software fi ake if an application attem	rom being tampered with o pts to tamper with or shut	or shut down down Symante	ec security softw	vare:
Log the ev	ent only		_		
🗎 🗖 Displa	/ a notification message w	hen tampering is detected	i:		
Target: [T Event Info: ActionTak Actor Proc	C TAMPER PROTECTION A argetPathname] [SystemEvent] [EntityTyp en: [ActionTaken] ess: [ActorProcessName] eFound]	e]] (PID [ActorProcessID])			
			ОК	Cancel	Help

Configuration

2.7 Endpoint Console Firewall Settings

2.7 Endpoint Console Firewall Settings

Because Endpoint ignores the functions of the firewall, all of the configured rules need to be disabled.

Firewall Policy - Rules

Menu Policies > Firewall Policy > "Rules" tab

• ALL check boxes of the firewall rules: Cleared

Firewall	Rules										Maximize \	Mindow
Policy	Rules	N	otifications	1								
verview												
ules	Firewal	I RUI	es									
mart Traffic Filtering	Firewall	rules	allow, block, a	nd log netwo	rk traffic. You car	n add higher priority	rules above	the blue	line in the ta	able below. Th	ose rules c	annot be
raffic and Stealth Settings		Inhe	erit Firewall Rule	es from Parer	nt Group							
	No	En	. Na	ne	Severity	Application	Host	Time	Service	Adapter	Screen.	. Action
	1		🔄 Block IPv6	i.	10-Minor	📩 Any	📩 Any	📩 Any	🔗 Ethe	🔛 All Ada	📩 Any	🔘 Bloc
	2		🛅 Block IPv6	over IPv4	10-Minor	📩 Any	📩 Any	📩 Any	🤣 UDP:	🔛 All Ada	📩 Any	🔘 Bloc
	3		🛅 Block IPv6	over IPv4	10-Minor	📩 Any	📩 Any	📩 Any	🔗 IP:[41]	🔛 All Ada	📩 Any	🔘 Bloc
	4		🛅 Allow frag	gmented pa	10-Minor	📩 Any	📩 Any	📩 Any	🔗 IP:[fr	🔛 All Ada	📩 Апу	Allo
	5		🛅 Allow wir	eless EAPOL	10-Minor	📩 Any	📩 Any	📩 Any	🔗 Ethe	🔛 All Ada	📩 Any	🔘 Allo
	6		C Allow MS	Remote Ac	.10-Minor	📑 wanarp.s	📩 Any	📩 Any	📩 Any	🔛 All Ada	📩 Any	Allo
	7	Г	管 Block loca	l file sharing	10-Minor	📩 Any	📩 Any	📩 Any	TCP:	🔛 All Ada	📩 Any	O Bloc
	8		R Block Ren	ote Admini	10-Minor	* Anv	* Anv	* Anv	TCP	All Ada	* Any	O Bloc
	9	E	Allow all a	nnlications	10-Minor	Ā.	* Any	* Any	* Any	All Ada	* Any	O Allo
	10	Γ	ि Allow ping	;, pong and	.10-Minor	📩 Any	* Any	📩 Any	CMP	🖼 All Ada	* Any	O Allo
	11		Allow VPI	N	5-Major	📩 Any	📩 Any	📩 Any	 VPN VPN VPN VPN VPN VPN VPN VPN VPN 	🔛 All Ada	📩 Any	 Allo
	12		🚊 Allow all d	ther IP traffic	15-Information	📩 Any	📩 Any	📩 Any	💮 IP:	🔛 All Ada	📩 Any	O Allo
	13	Г	🔄 Don't log k	proadcast a	15-Information	📩 Any	Local:	📩 Any	📩 Any	🖼 All Ada	📩 Апу	O Bloc
	14	Г	🔁 Block all o	ther traffic	15-Information	📩 Any	📩 Any	📩 Any	📩 Any	🔛 All Ada	📩 Any	🔘 Bloc
						[Add Rule		Add Bla	nk Rule	Delet	e
		_										

2.7 Endpoint Console Firewall Settings

Menu Policies > Firewall Policy> "Smart Traffic Filtering" tab

- "Enable Smart DHCP" check box: Cleared
- "Enable Smart DNS" check box: Cleared
- "Enable Smart WINS" check box: Cleared

Firewall Policy		×
Firewall	Smart Traffic Filtering	Maximize Window
Firewall Policy Overview Rules Smart Traffic Filtering Traffic and Stealth Settings	Smart Traffic Filtering Image: Comparison of the second	Maximize Window
	ОК	Cancel Help

Configuration 2.8 Endpoint Intrusion Detection Settings

2.8 Endpoint Intrusion Detection Settings

Symantec Endpoint Protection is not used for intrusion detection in PCS 7. All associated functions are therefore disabled.

"Settings" tab

Menu Policies > Intrusion Prevention Policy > "Settings" tab

- "Enable Intrusion Prevention" check box: Cleared
- "Enable denial of service detection" check box: Cleared
- "Enable port scan detection" check box: Cleared
- "Enable excluded hosts" check box: Cleared
- "Automatically block an attacker's IP address" check box : Cleared

Intrusion Prevention Policy		×
Untrusion Prevention Policy Intrusion Prevention Policy Overview Settings Exceptions	Settings Intrusion Prevention C Enable Intrusion Prevention Automatically detects and blocks network attacks.	×
	Active Response Active Response Automatically block an attacker's IP address Number of seconds during which to block the IP address: 600 seconds	
	OK Cancel He	ql