SIEMENS

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.

⚠ 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 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:

⚠ 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 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

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

1.2.1 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

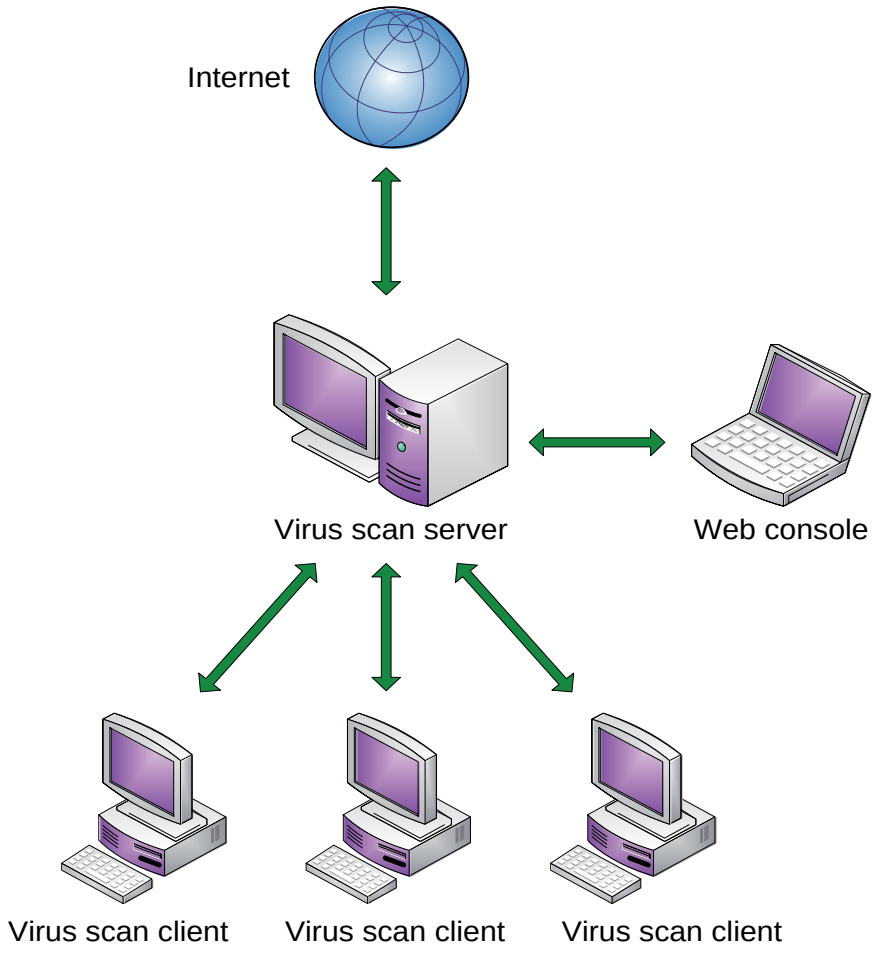
The virus scan client is a computer which is examined for viruses and managed by the virus server.

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.

1.2.3 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.



1.2.4 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

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

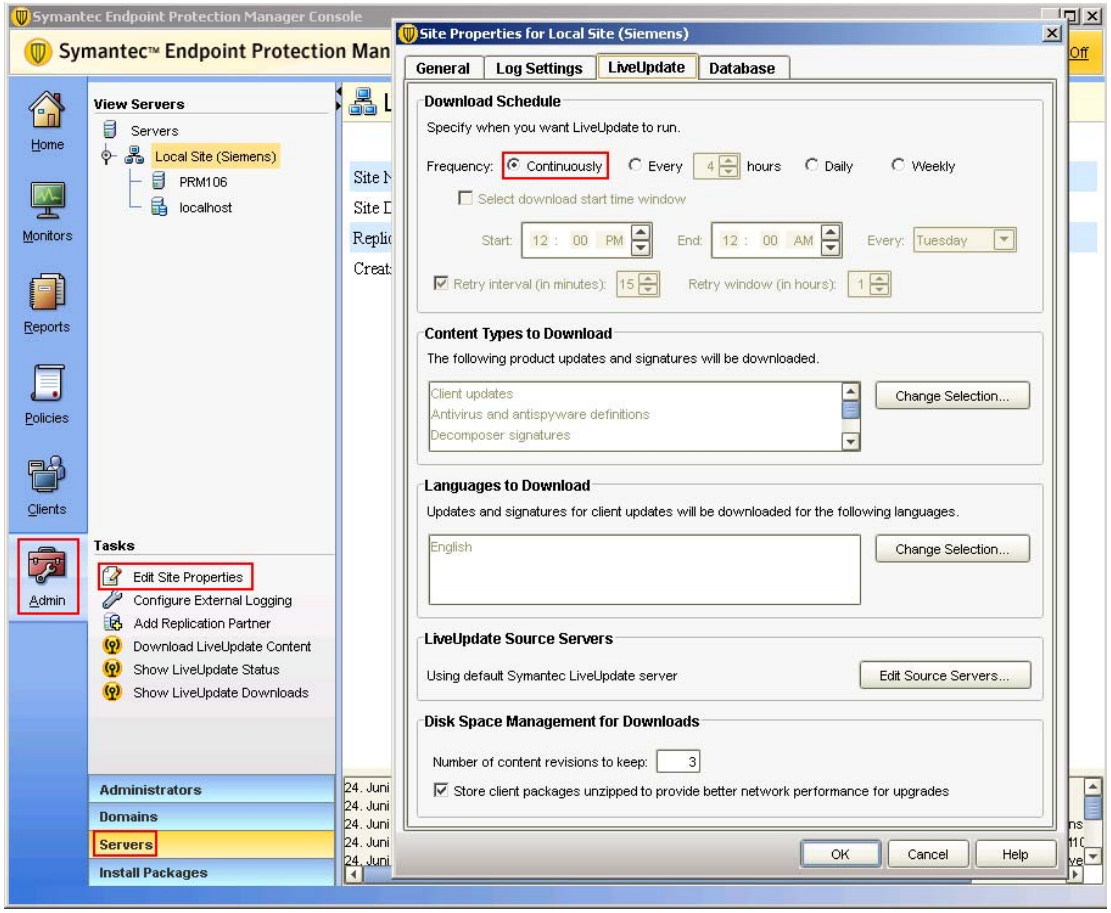
Updates

The following distinctions should be noted:

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

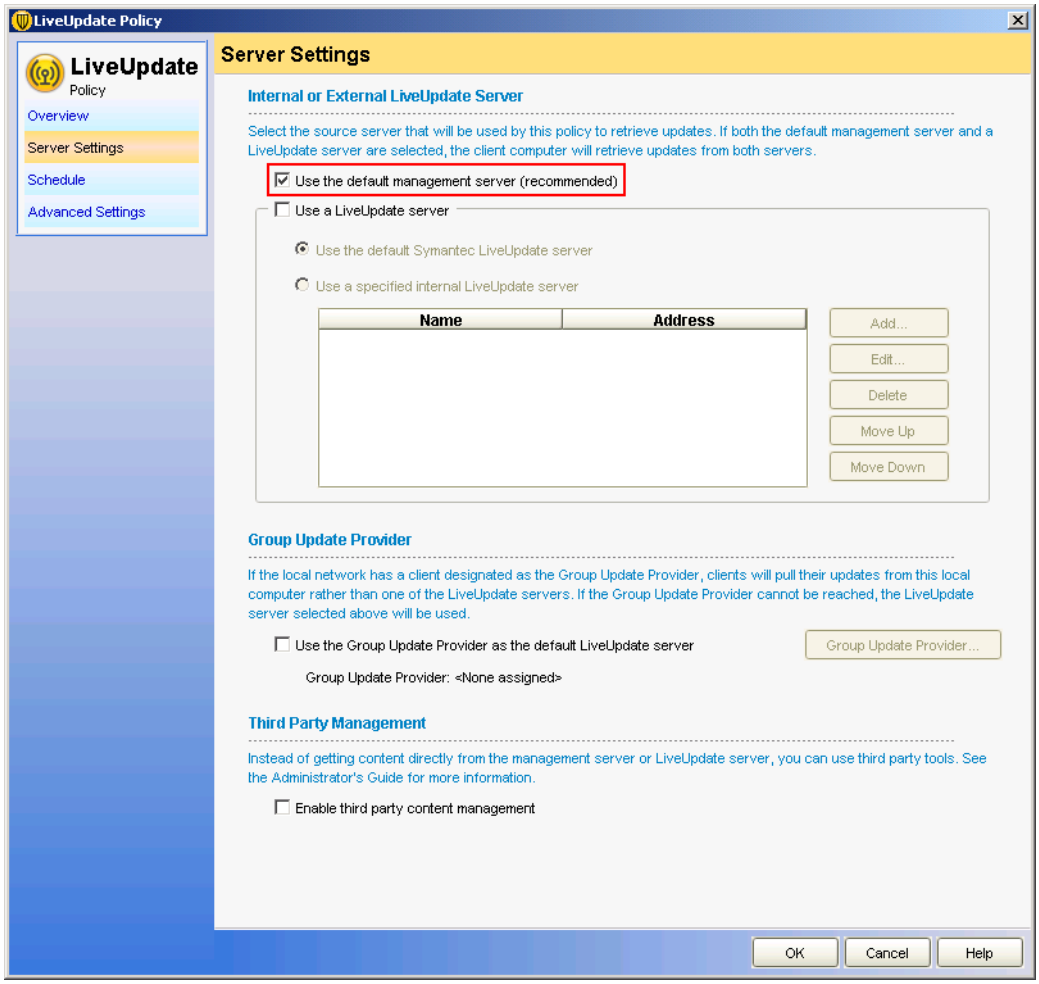
Server update settings in the "Site Properties" dialog box

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



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



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

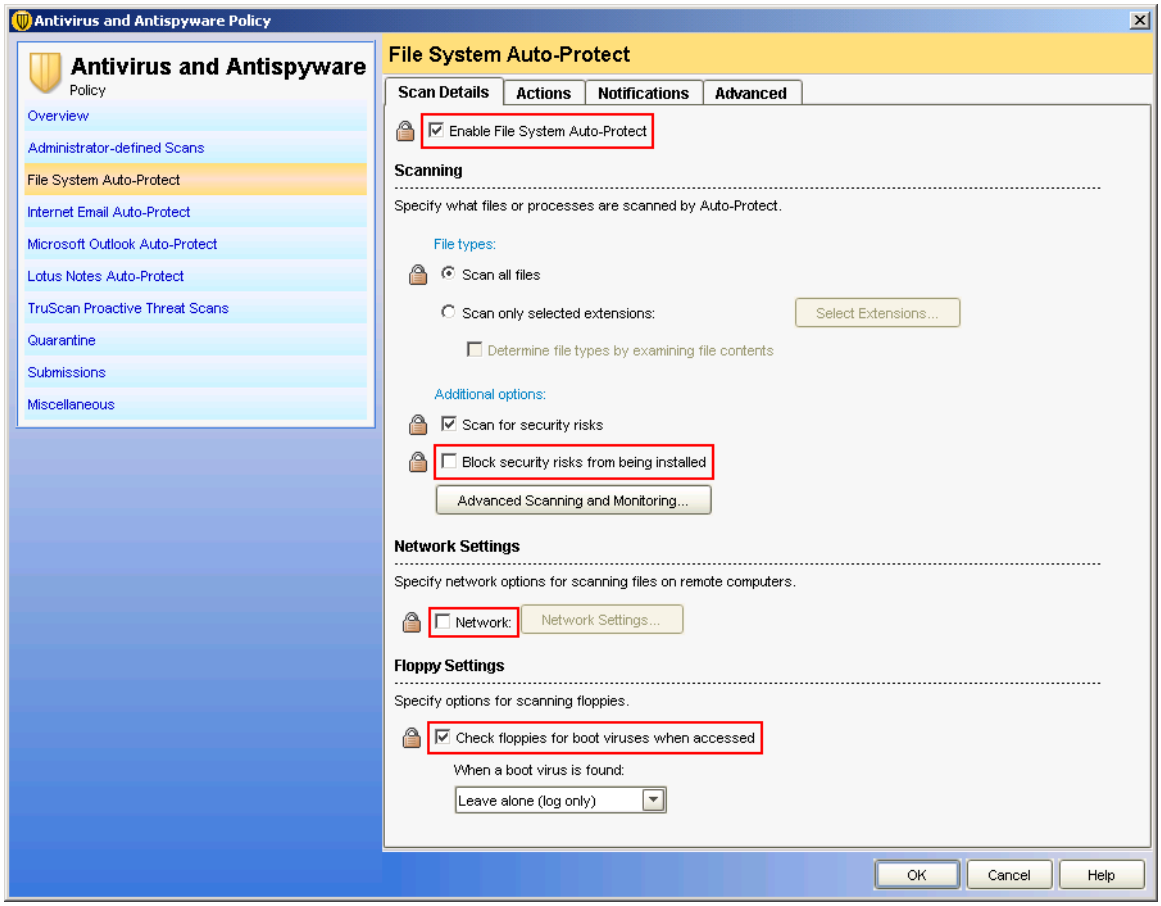
This option was known as "Client Auto-Protect" in ealier versions of Symantec antivirus software.

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

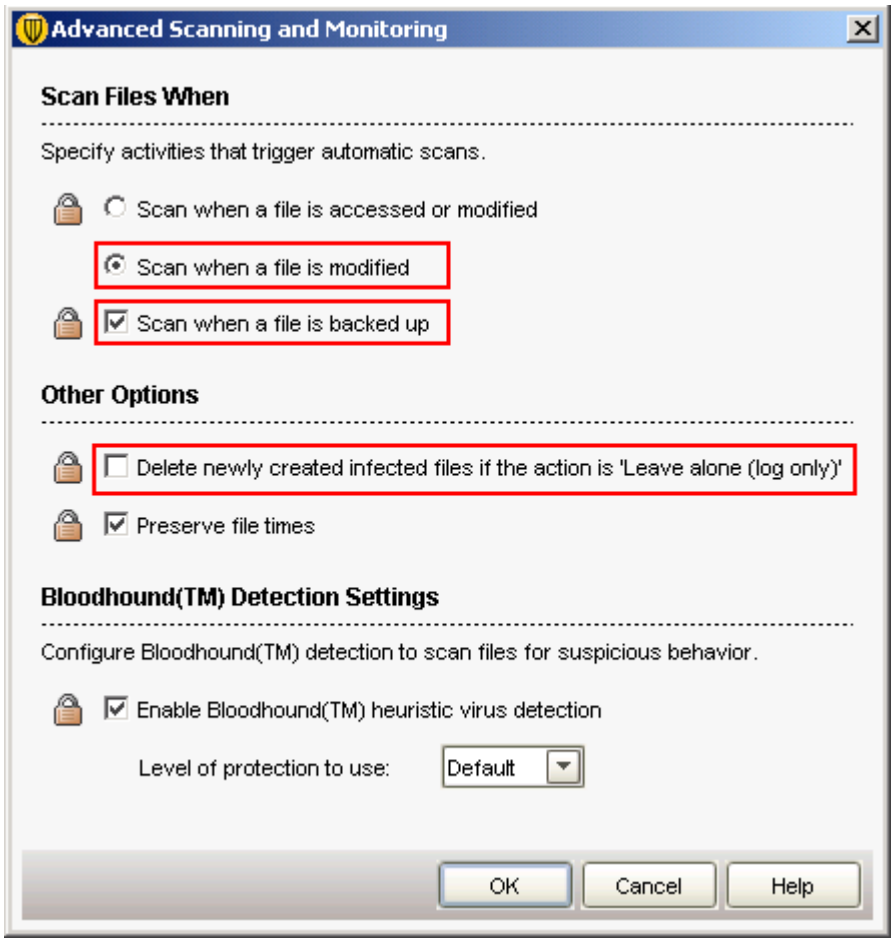
- "Enable File System Auto-Protect" check box: **Selected**
- "Block security risks from being installed" check box: **Cleared**
- "Network Settings" check box: **Cleared**
- "Check floppies for boot viruses when accessed" check box: **Selected**



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…**

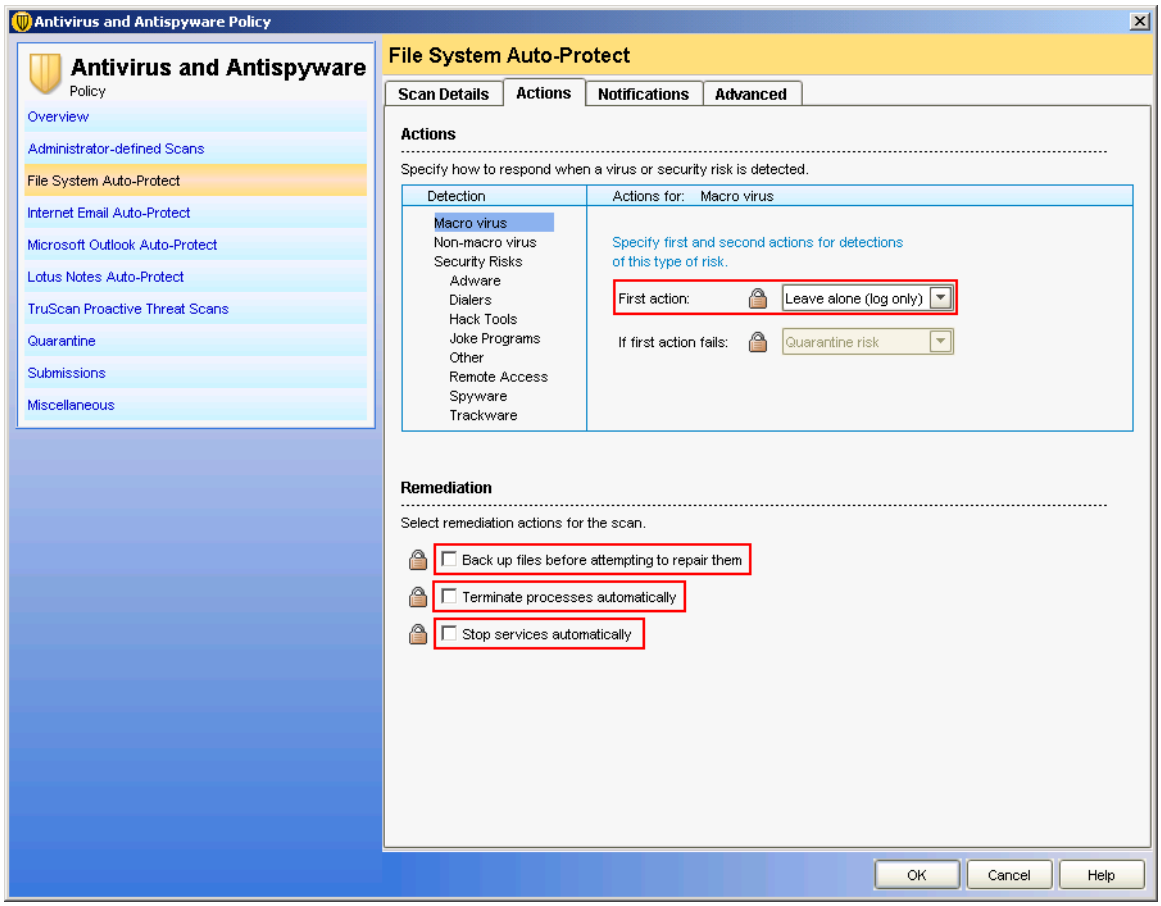
- "Scan when a file is modified" option button: **Selected**
- "Scan when a file is backed up" check box: **Selected**
- "Delete newly created infected files if the action is 'Leave alone (log only)" check box: **Cleared**



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

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

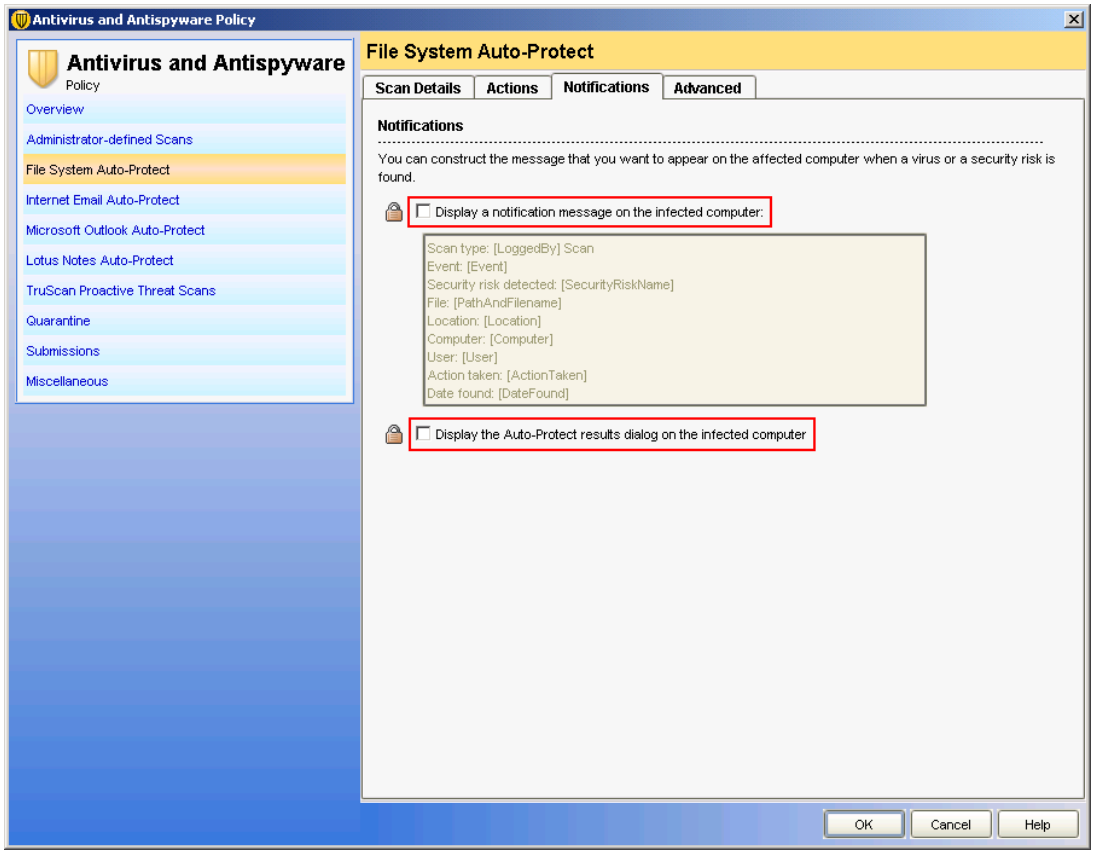
- Selection in "First action" drop-down list: **Leave alone (log only)**
  This selection also applies to "Non-macro virus" and "Security Risks"
- "Back up files before attempting to repair them" check box: **Cleared**
- "Terminate processes automatically" check box: **Cleared**
- "Stop services automatically"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



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

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

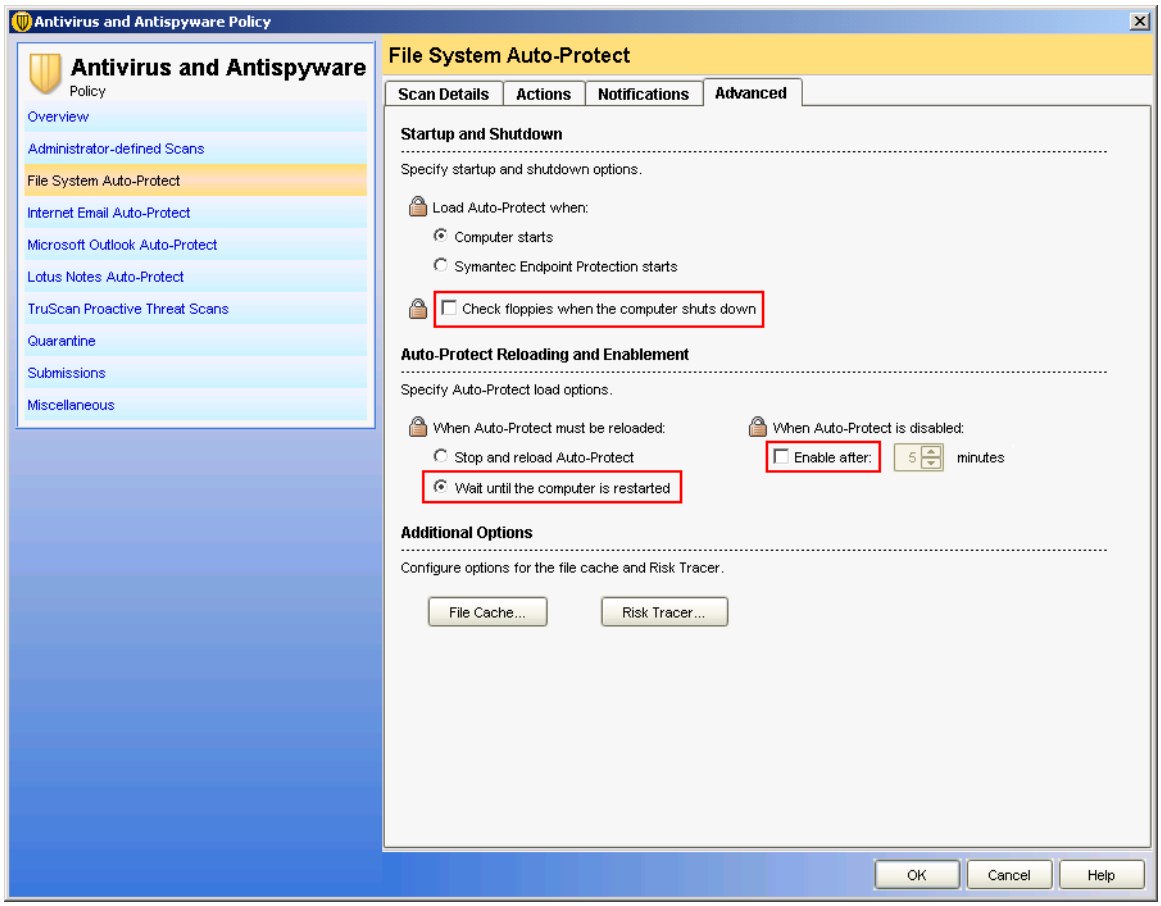
- "Display a notification message on the infected computer" check box: **Cleared**
- "Display the Auto-Protect results dialog on the infected computer" check box: **Cleared**



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

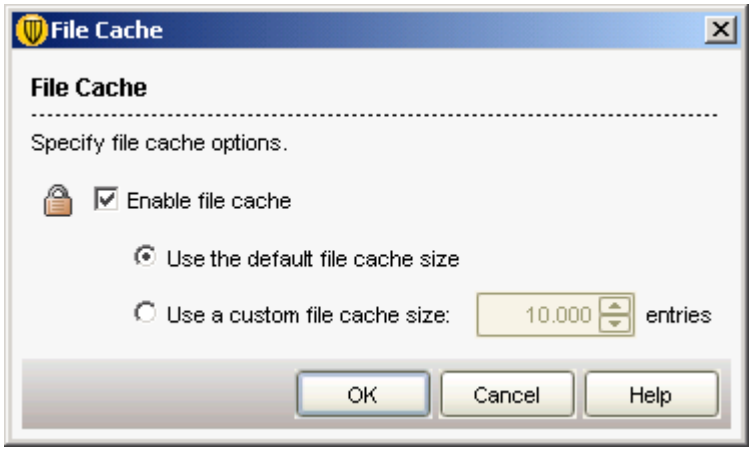
Menu **Policies > Antivirus and Antispyware > File System Auto-Protect >** "Advanced" tab

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



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

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.

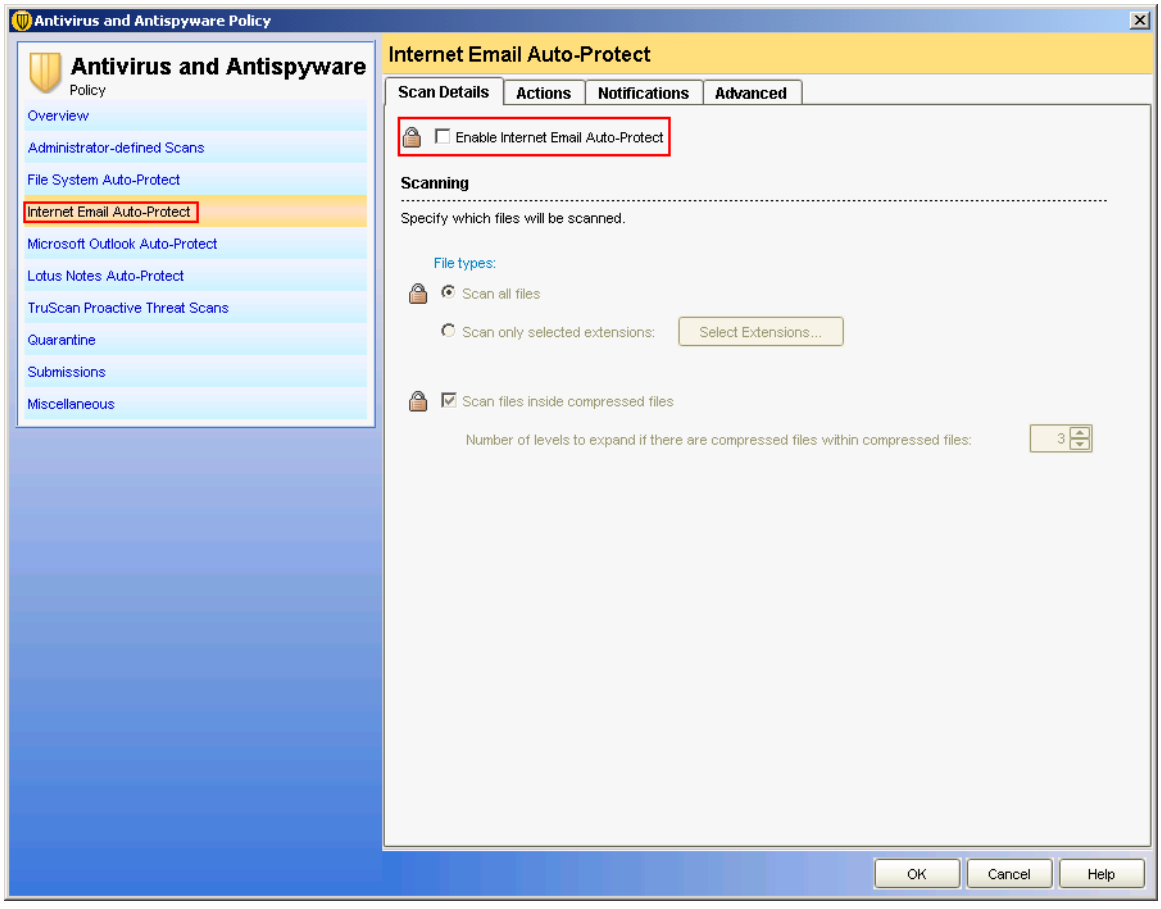
Menu **Policies > Antivirus and Antispyware Policy >**

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**



2.5.4 Antispyware Protection – TruScan Proactive Threat Scans

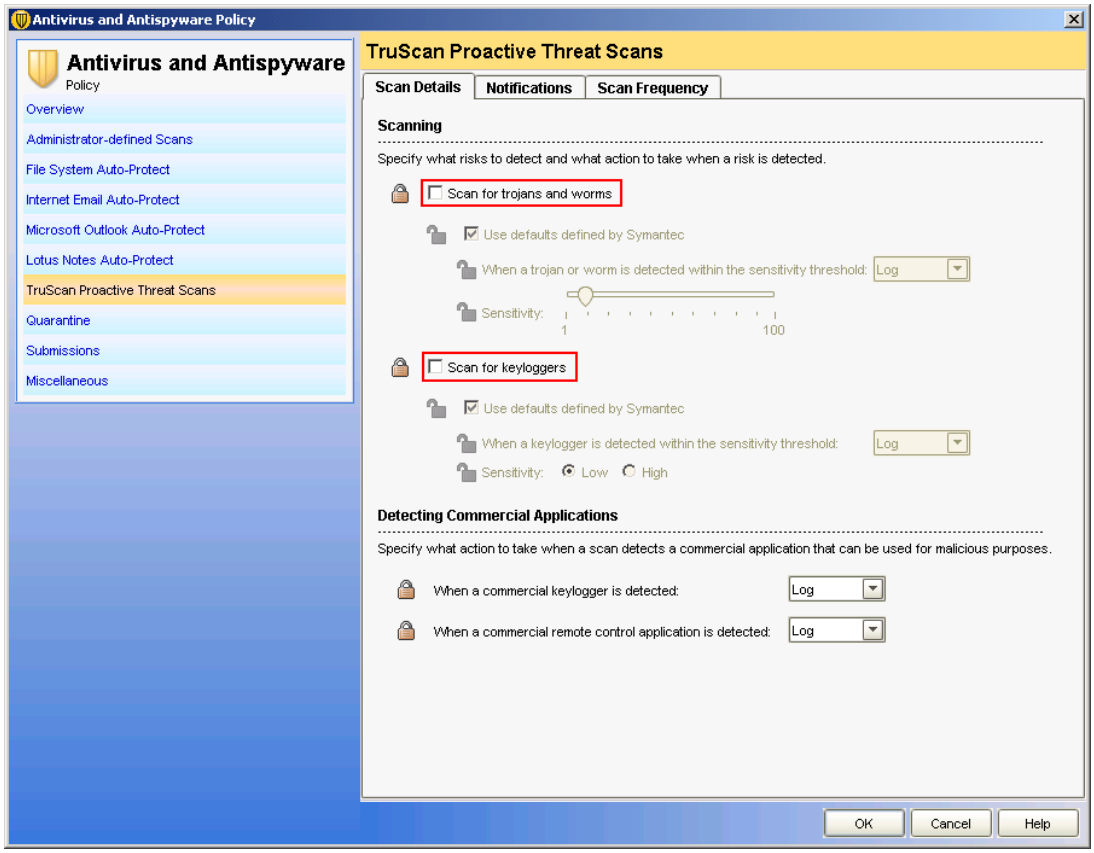
Introduction

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

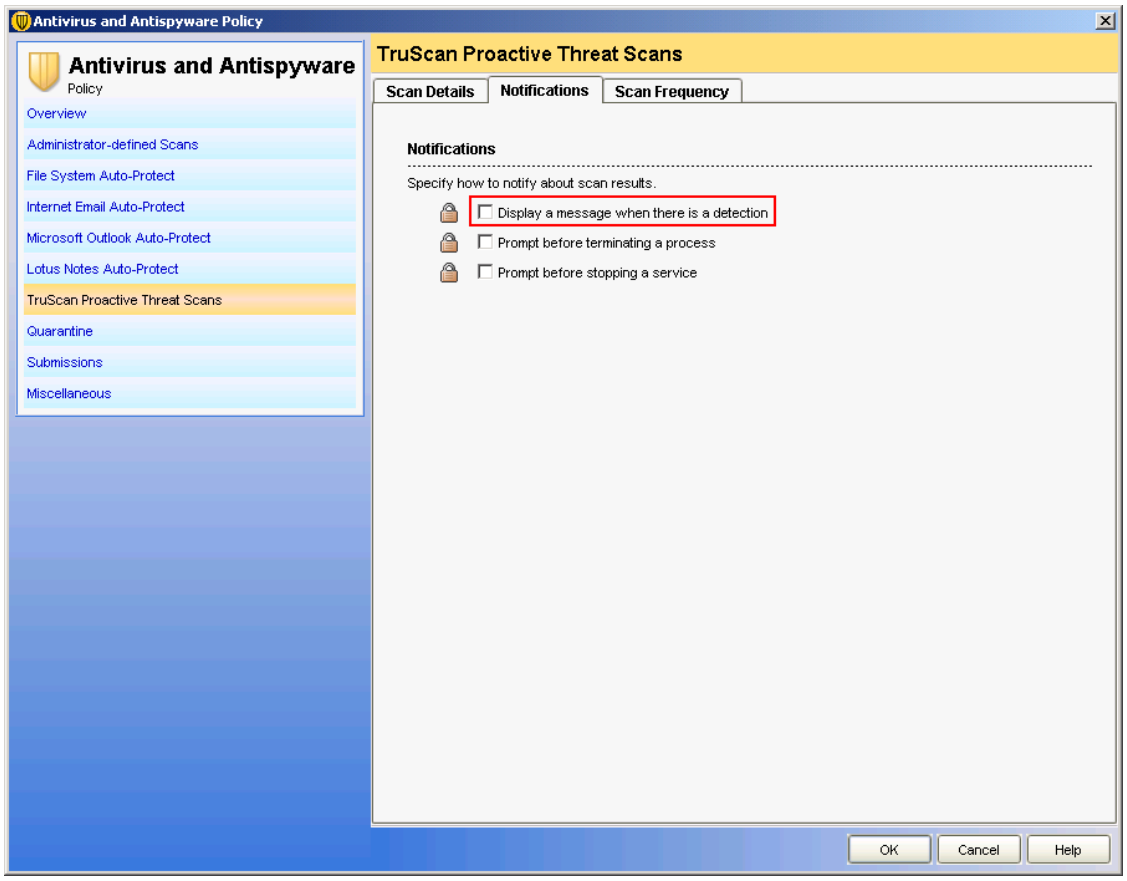
- "Scan for trojans and worms" check box: **Cleared**
- "Scan for keyloggers" check box: **Cleared**



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**

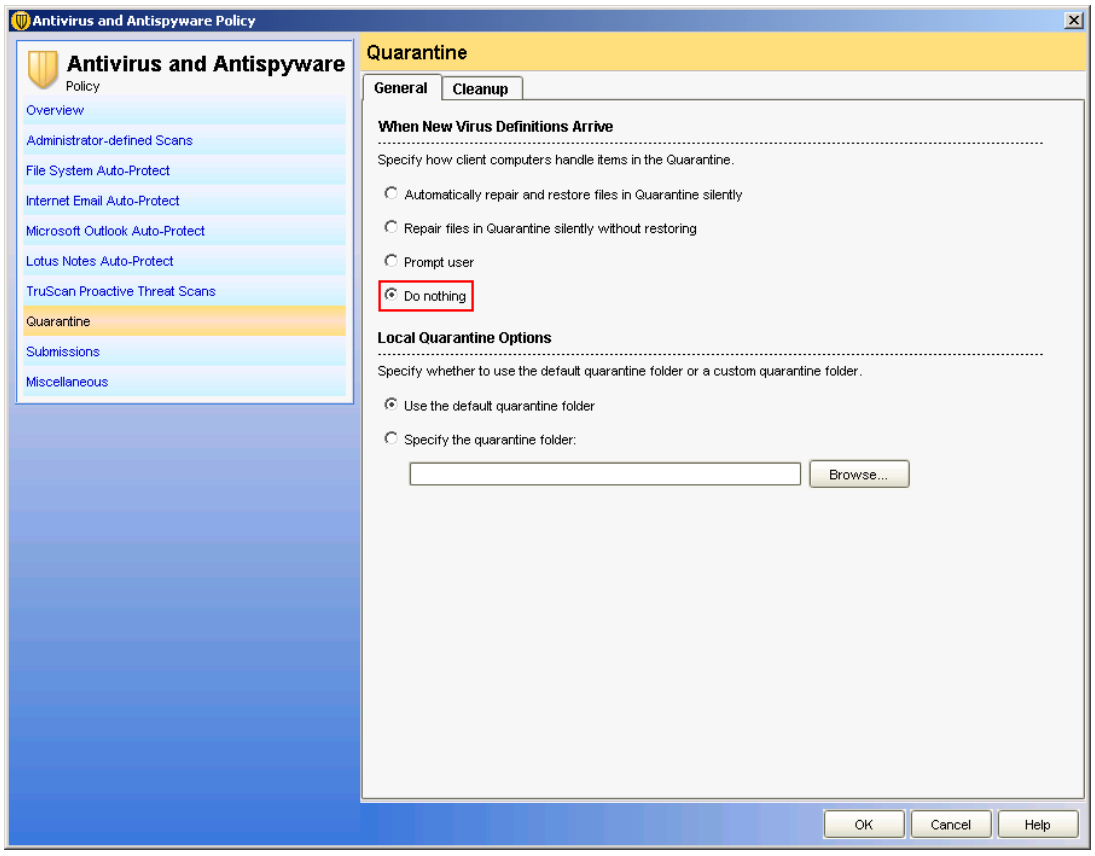


2.5.5 Quarantine settings

Quarantine settings in the "General" dialog box

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

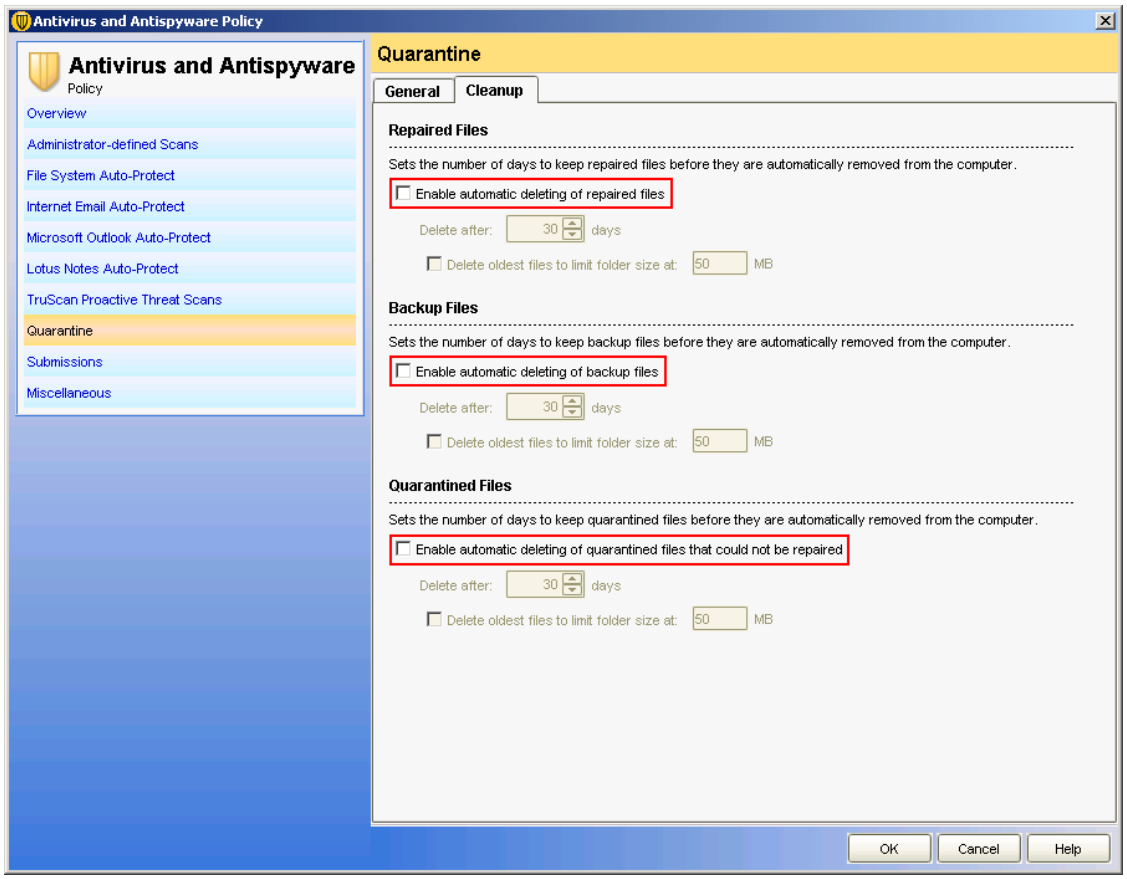
- "Do nothing" option button: **Selected**



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**



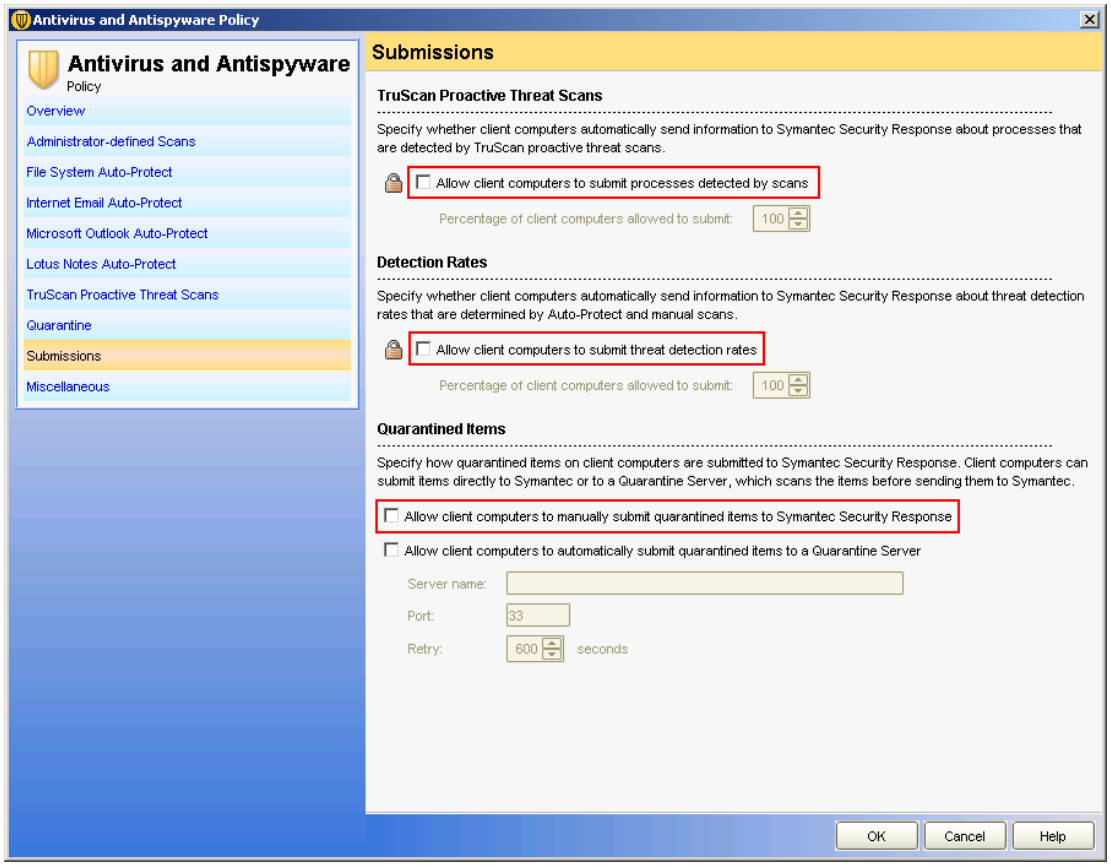
2.5.6 Report Submission settings

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

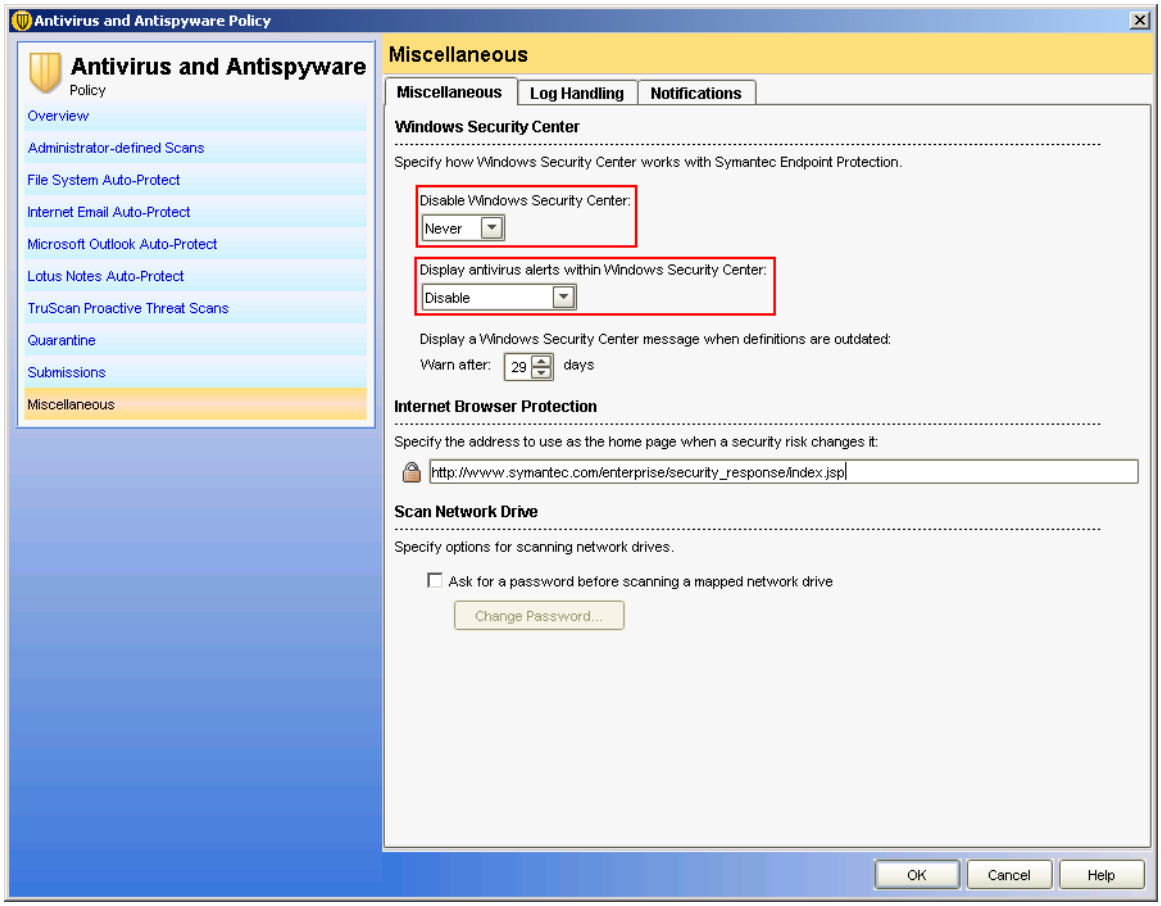


2.5.7 Miscellaneous settings

Settings in the "Miscellaneous" tab

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

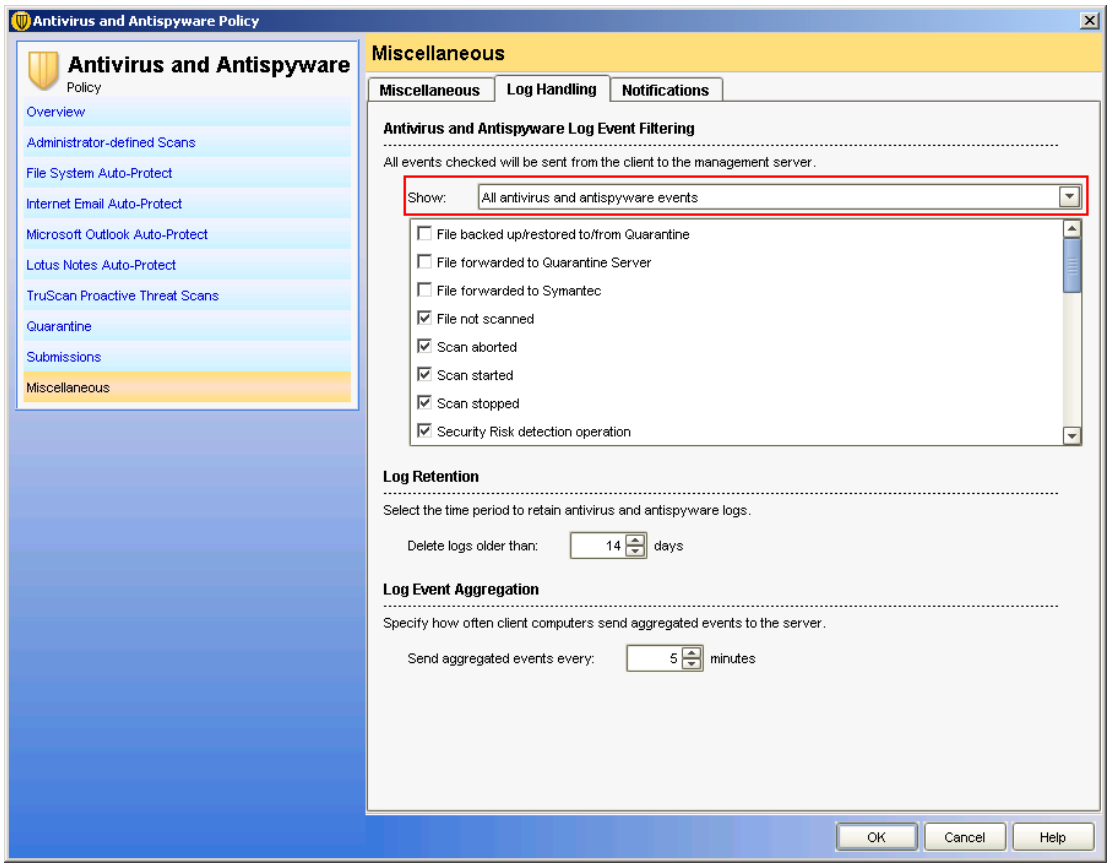
- Selection in "Disable Windows Security Center" drop-down list: **Never**
- Selection in "Display antivirus events within Windows Security Center" drop-down list: **Disable**

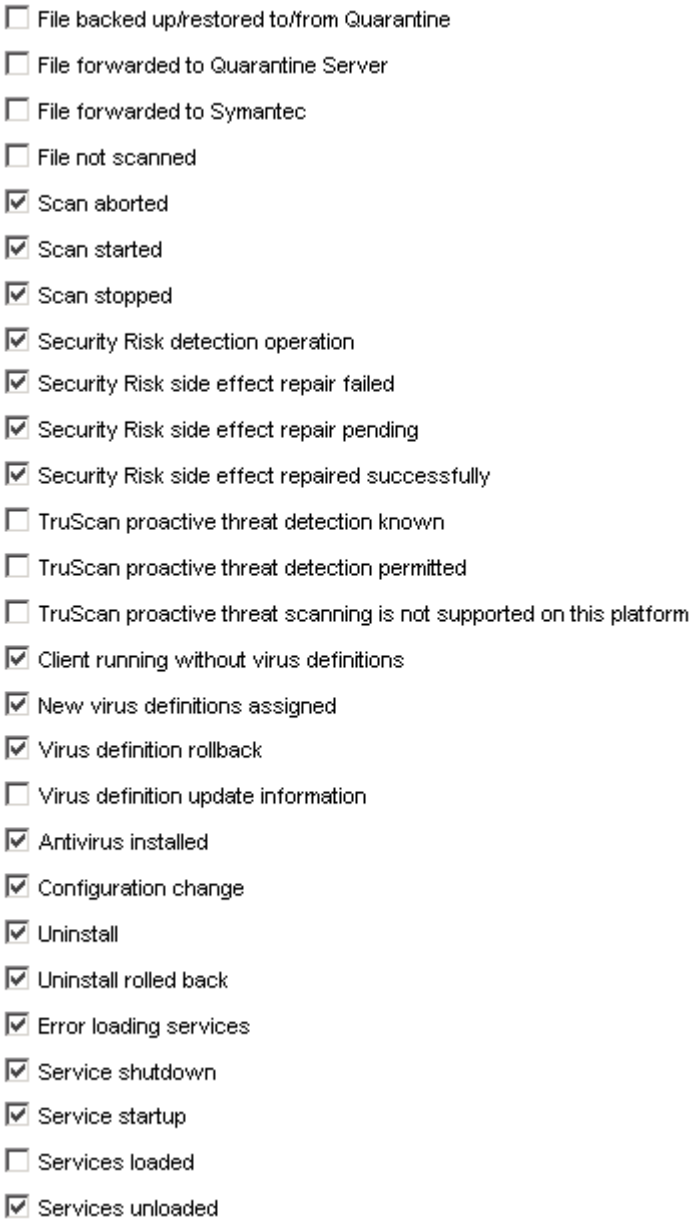


Settings in the "Log Handling" tab

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.

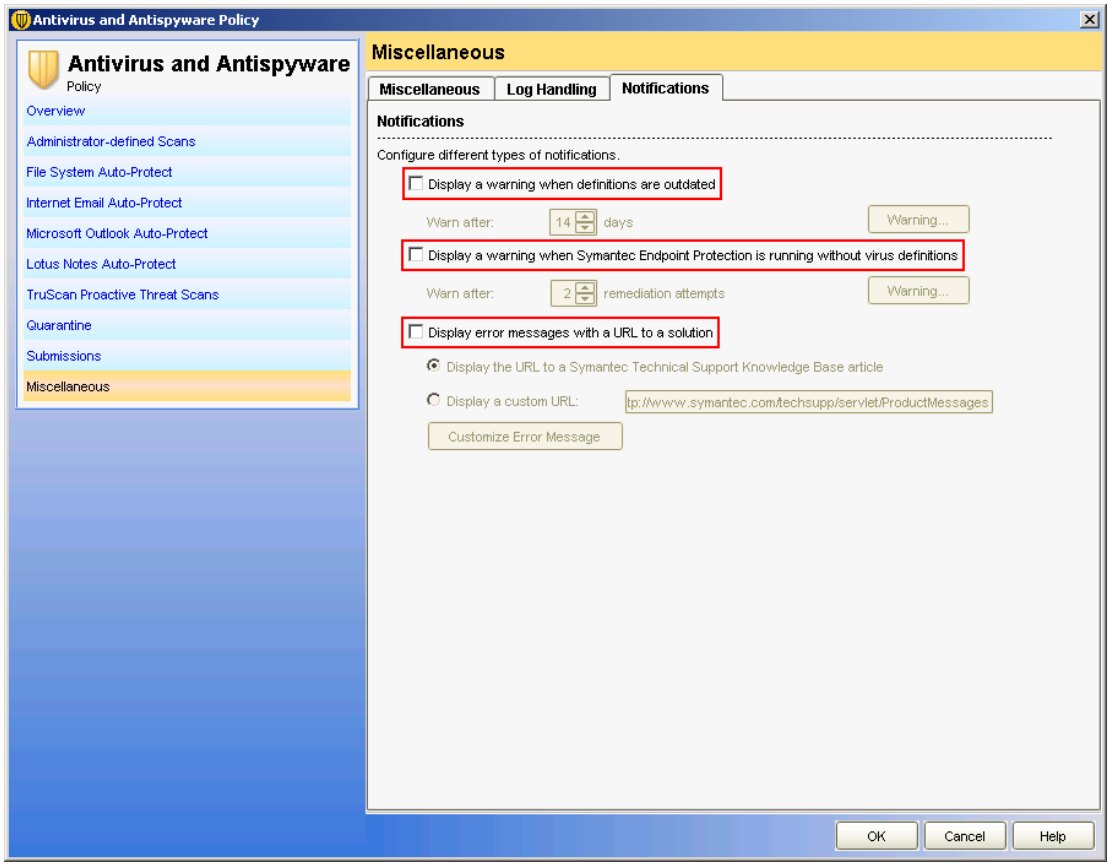



File backed up/restored to/from Quarantine
File forwarded to Quarantine Server
File forwarded to Symantec
File not scanned
Scan aborted
Scan started
Scan stopped
Security Risk detection operation
Security Risk side effect repair failed
Security Risk side effect repair pending
Security Risk side effect 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

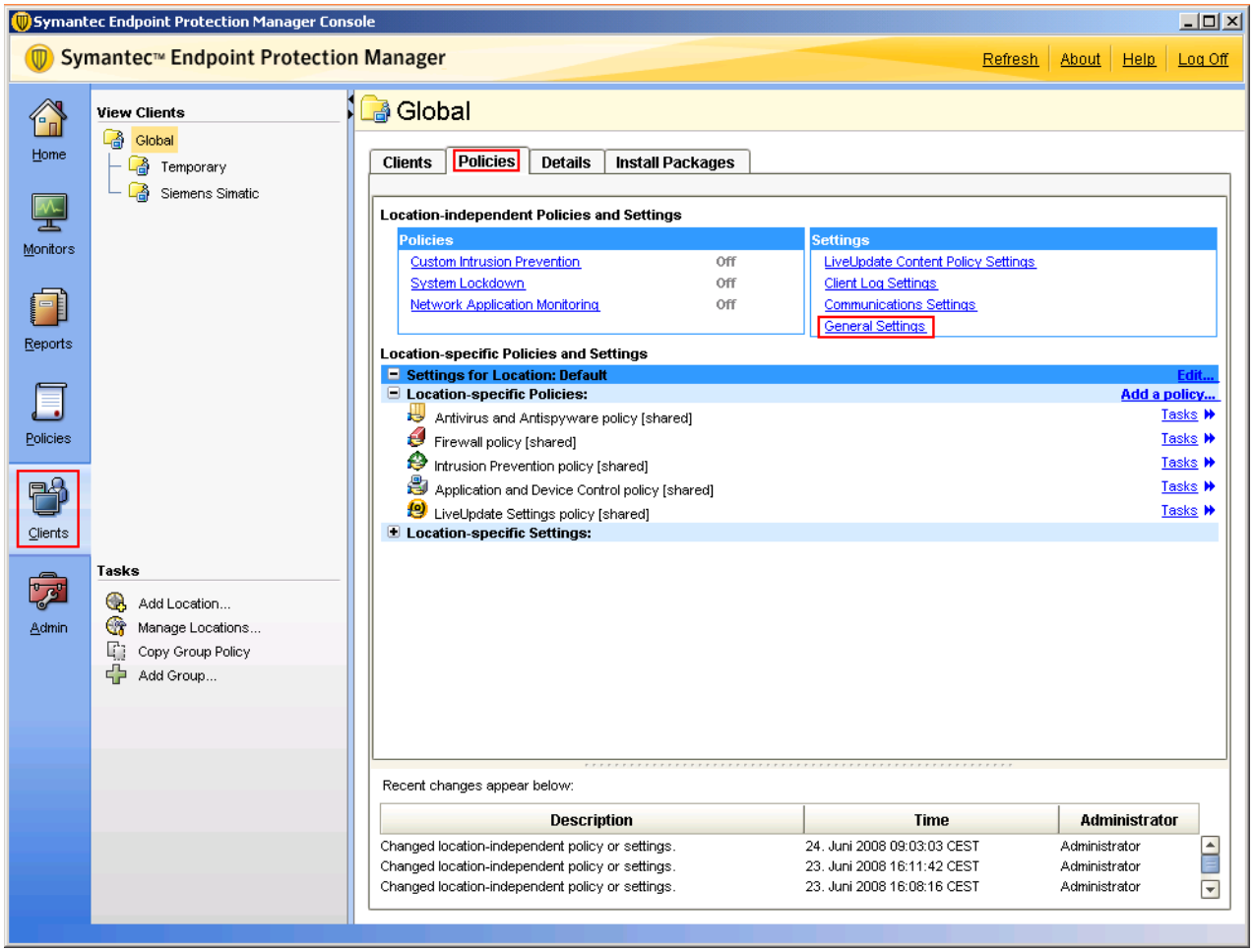
- "Display a warning when definitions are outdated" check box: **Cleared**
- "Display a warning when Symantec Endpoint Protection is running without virus definitions" check box: **Cleared**
- "Display error messages with a URL to a solution" check box: **Cleared**



2.6 Client Administrator and Tamper Protection Options

You can find the general settings below.

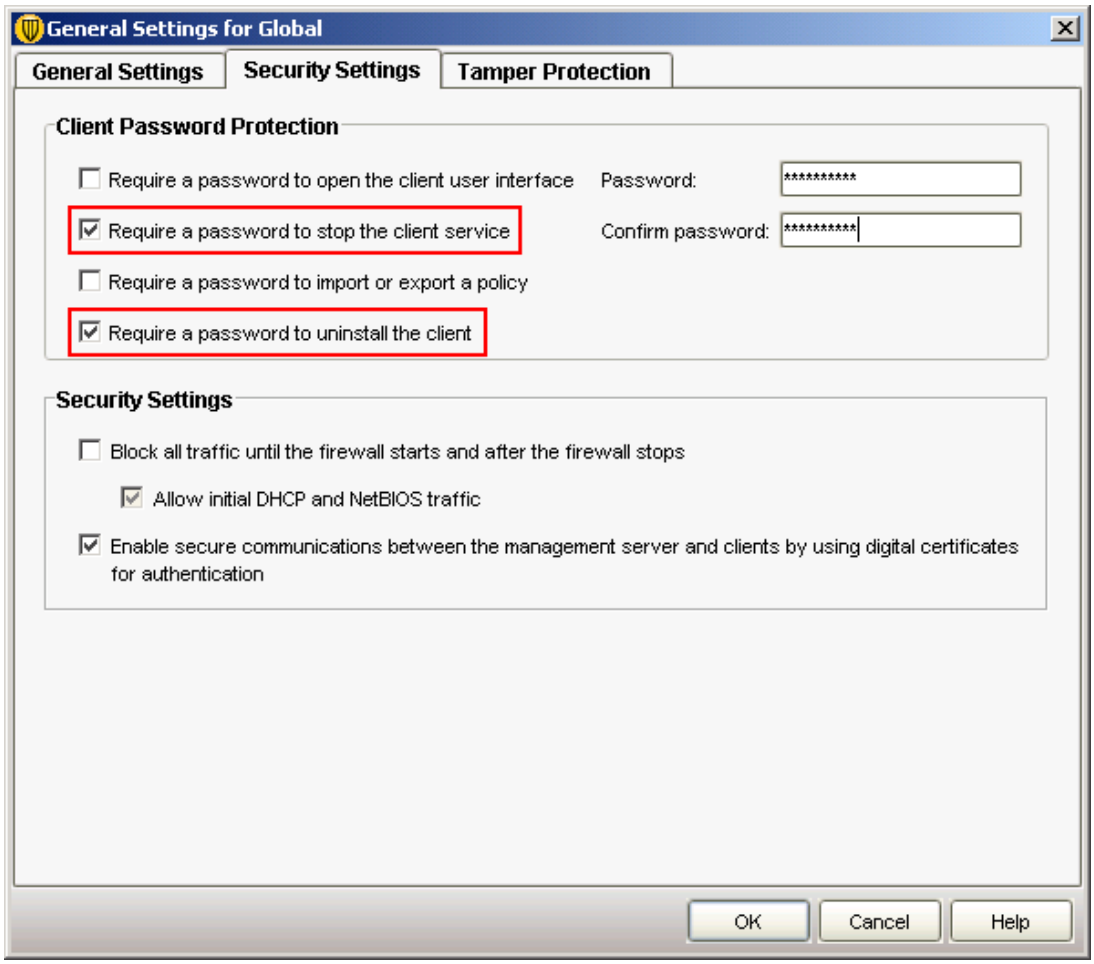
Menu Clients > "Policies" tab > General Settings



Security and privileges settings

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

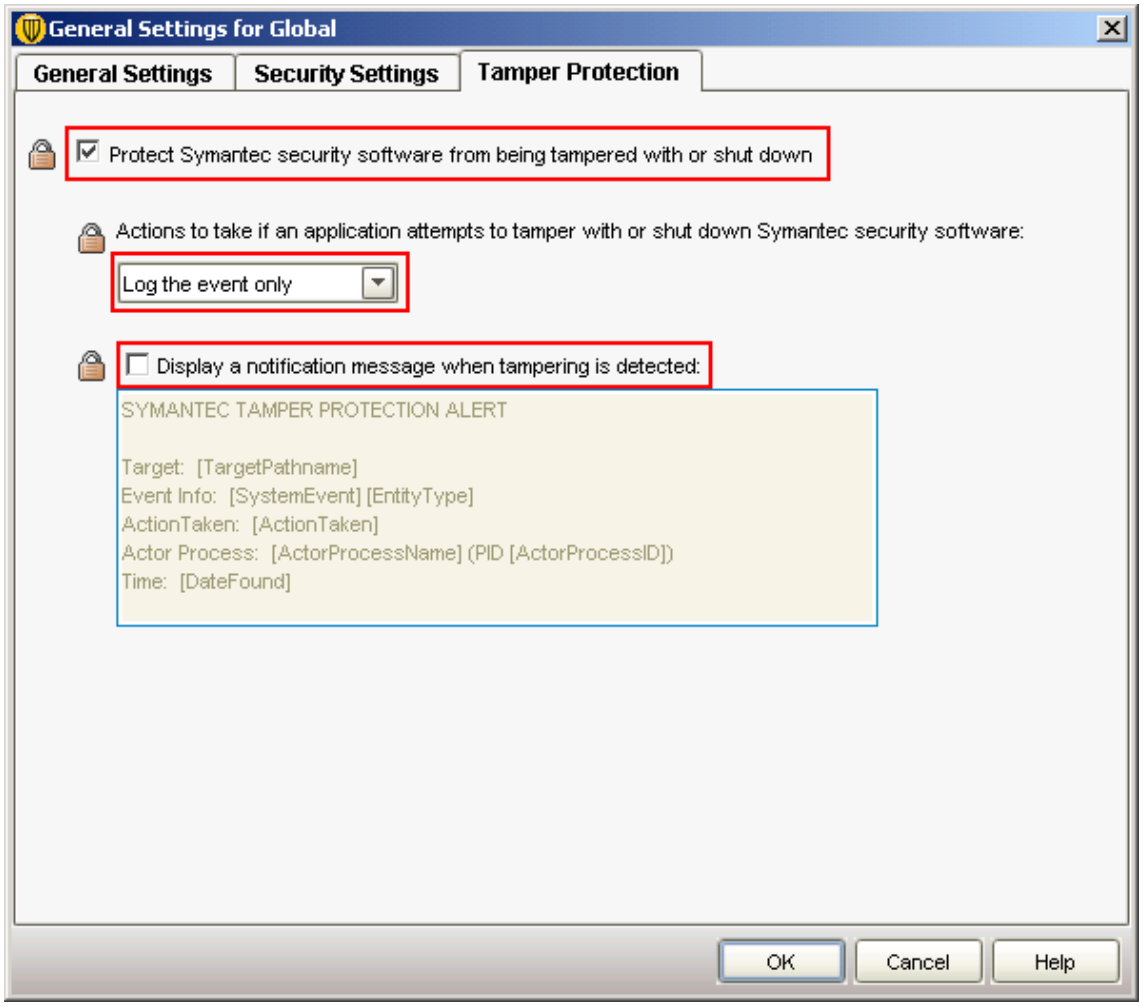
- "Require a password to stop the client service" check box: **Cleared**
- "Require a password to uninstall the client" check box: **Cleared**
- Enter password



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**



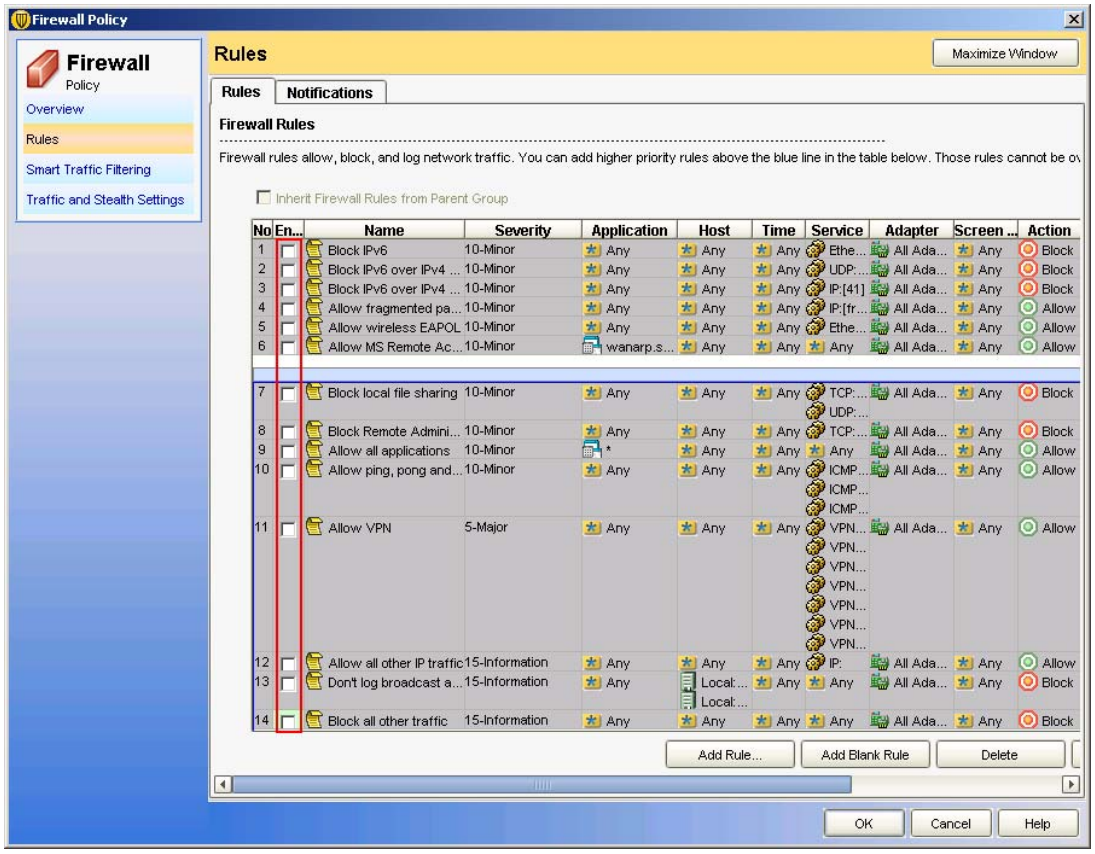
2.7 Endpoint Console Firewall Settings

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

Firewall Policy - Rules

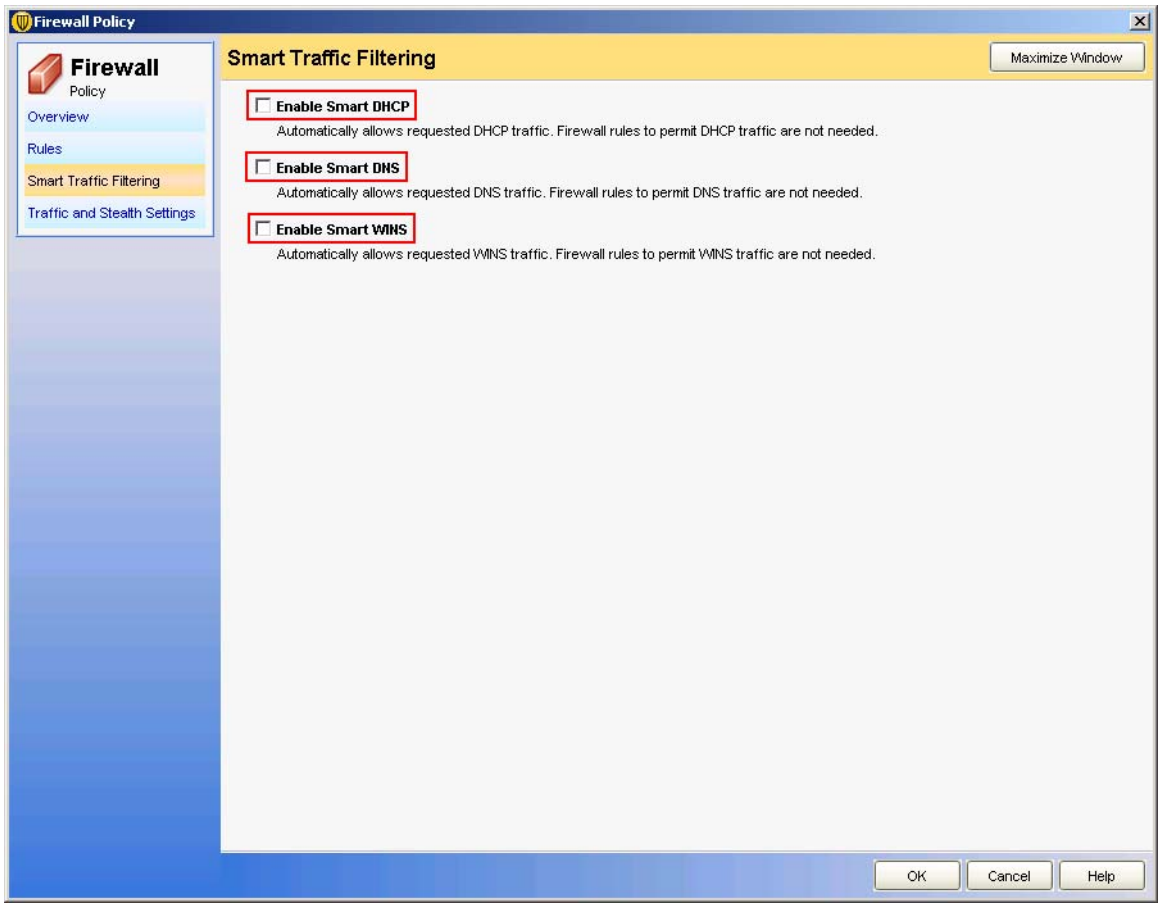
Menu **Policies > Firewall Policy >** "Rules" tab

- ALL check boxes of the firewall rules: **Cleared**



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**



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**