SoftControl

Endpoint Client 4.1.19

User's guide

Dear user!

SAFE 'N SEC Corporation thanks you for choosing SoftControl Endpoint Client. Specialists of the company do their best to make our software both meets the highest requirements in a field of information protection and be handy in use. We hope that SoftControl Endpoint Client will be helpful for you.

COPYRIGHT

This document is a property of the SAFE 'N SEC Corporation and can be used only for personal purposes. It is prohibited to reproduce parts of the document, make changes, share on network resources, distribute (including in translation) in hard- and soft-copy form, via communication channels and mass media or by any other means without prior written permission from the company and a reference to the source.

All the names used throughout this document are trademarks of it's respective owners.

LIABILITY LIMIT

Contents of the document may change without notice. SAFE 'N SEC Corporation doesn't bear responsibility for inaccuracies and/or errors in this document, and possible damage associated with it.

SAFE 'N SEC Corporation, 2017

Postal address:

127106 Russia, Moscow

Altufyevskoe shosse, 5/2

SAFE 'N SEC Corporation

Tel:

+7 (495) 967-14-51

Fax:

+ 7 (495) 967-14-52

E-mails:

Customer service: sns@safensoft.com

Sales team: sales@safensoft.com

Website: http://www.safensoft.com

Contents

1. Introduction

1.1. Purpose

SoftControl Endpoint Client (hereafter referred to as «SoftControl SysWatch») is intended for protection of Microsoft® Windows®-controlled workstations against unauthorized resource access.

1.2. Main features

SoftControl SysWatch is a proactive protection tool that belongs to the Host Intrusion Prevention System (HIPS) class. SoftControl SysWatch analyzes applications' activity and blocks dangerous operations which may cause system crash or the loss/damage of user's confidential information, provides protection from various types of malicious code, zero-day threats and other unauthorized actions of violators.

SoftControl SysWatch provides the following features:

▪ **Proactive protection** based on the patent pending V.I.P.O. (Valid Inside Permitted Operations) application control technique:

 ● Dynamic integrity control – detects unauthorized attempts to run processes and blocks them before a process can damage the system..

 ● Dynamic 'sandbox' execution – specially designated user account for potentially dangerous software provides system-level privilege controls to block malicious software activity;

 ● Dynamic resource control – controls applications permissions to access the file system, system registry keys and values, peripheral devices (USB drives, CD/DVD discs, LPT and COM ports) and network resources (firewall functions).

▪ **Automatic setup (system profile gathering)**: profiling the system to continue to monitor the integrity of the its initial state.

▪ **Incidents processing management**:

 ● classic (manual) mode, when the user makes a decision on whether to run or block applications;

 ● expert (automatic) mode, when the program makes a decision on whether to run or block applications, based on the current activity policy and incident processing settings.

▪ **Flexible set up of control rules**:

 ● creating private rules for certain applications;

- specifying the exceptions for the permissions to access the file system, registry, and USB drives (USB 'white list');

- selecting time intervals for the permissions to access the file system, registry, network resources, and USB drives.

- selecting user accounts that the permissions to access the file system, registry, network resources, and USB drives apply to.

- **Keeping application activity history**:

  - viewing the activity history for certain applications;

  - creating backup copies of the files that have been modified by the specified application, and restoring them when necessary.

- **Signature protection**: tools for the antivirus scanning of the system and neutralizing known malicious software (viruses, trojans, worms, spy programs, and so on), with the use of up-to-date signature bases.

- **Logging incidents and program statuses to reports**: saving the detailed information about the program work to text report files and WMI.

- **Self-protection system**:

  - password protecting the program interface and uninstaller;

  - disabling external access to the system service.

- **Saving and restoring program settings**: saving the backup copy of the program settings, so as to restore the settings if necessary.

- **Remote management**: if the program is used along with the SoftControl Service Center product, remote centralized management of the program, configuring and monitoring the protection state on the LAN endpoints are carried out remotely via administrative tools.

1.3. Notational conventions and terms

1.3.1. Notational conventions

Table 1 lists notational conventions used in this document.

Table 1. Notational conventions

Notation example	Description
ℹ	An important information, a note.
Condition	An execution condition, a note, or an example.

Notation example	Description
Update	− headers and acronyms; − names of buttons, links, menu items, and other program interface elements.
Control policy	− terms (definitions); − names of files and other objects; − messages displayed to user.
`C:\Program Files\SoftControl`	Paths to directories, files, or registry keys.
`%windir%\system32\msiexec.exe /i`	Source code, command and configuration file fragments.
<SoftControl SysWatchinstallation directory>	Fields with specific names to be replaced with actual values.
Appendix ⑦	Links to internal resources (document sections) with a specific page number, or links to external resources (URL).

1.3.2. List of acronyms

This documents uses the following acronyms:

- ❖ **CPU** – central processing unit;
- ❖ **GUI** – graphical user interface;
- ❖ **HDD** – hard disk drive;
- ❖ **LAN** – local area network;
- ❖ **OS** – operating system;
- ❖ **RAM** – random access memory;
- ❖ **SSD** – self-service device.

1.3.3. Glossary

Table 2. Glossary

Term	Description
Proactive protection	A series of measures to prevent harmful effects on the basis of prevention techniques.
Prevention techniques	The advanced data protection technologies based on the analysis of the activity on the user's computer. This can be the operation of any applications, OS services, user actions, external activity, etc. Unlike reactive techniques which are the basis of protections such as antivirus and personal firewalls, prevention techniques do not analyze an object

Term	Description
	code, but track the potentially dangerous actions the object performs. Therefore, SoftControl Endpoint Client does not require the bases of malicious code and their updates, which are necessary for traditional protections.
Control policy	A set of rules to monitor the application activity, analyze the applications, and to decide whether an application is malicious. It is the policy that determines what actions and sequence of actions should be considered as dangerous.
Activity control rule	A set of conditions that determine the application activity, and the actions that SoftControl Endpoint Client performs with respect to an application with such an activity. The conditions of a rule specify the control area and refine it (by specifying the object of the control, operation on the object, an application that performs the operation, etc.).
System profile	A collection of check sums of a portable executable modules (see 'The Portable Executable (PE) format') and paths to them in the system. It is a result of the automatic setup (profile gathering).
Installer flag	A special token that gives particular privileges for process to launch (see 'installation mode')
Installation mode	A process launch mode without restrictions when process and all its child processes are moved to the system profile if it's not there yet.
Reactive (signature) techniques	A mode of operation of antivirus software and intrusion detection systems. In this method, the program refers to the database of known viruses and checks whether some part of the code of the object being scanned corresponds to the known virus code (signature) in the database.
The Portable Executable (PE) format	A file format for executables, object code, DLLs and others used in 32-bit and 64-bit versions of Microsoft® Windows® operating systems.
Host	A computer device (workstation / server / self-service terminal) that connected to local area network or wide area network.

2. Hardware and software requirements

2.1. SoftControl SysWatch system requirements

Table 3. Minimal system requirements

OS	CPU frequency	RAM size	HDD free space
Workstations / servers: ▪ Microsoft® Windows® XP (SP2, SP3) x86 (32-bit) ▪ Microsoft® Windows® XP (SP2) x64 (64-bit) ▪ Microsoft® Windows® Server 2003 (SP2) x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® 10	800MHz	512MB	150MB + extra 120MB or more for antivirus database updates
▪ Microsoft® Windows® 10	800MHz	1024MB	
Workstations / servers: ▪ Microsoft® Windows® 7 (SP1) x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® 8 / 8.1 x86/x64 (32-bit/64-bit) ▪ Microsoft® Windows® Server 2008 R2 ▪ Microsoft® Windows® Server 2012 ▪ Microsoft® Windows® Server 2012 R2 ▪ Microsoft® Windows® 10 x86	1GHz	1024MB	
▪ Microsoft® Windows® 10 x64	1GHz	2048MB	
Self-service devices: ▪ Microsoft® Windows® XP Embedded (SP2, SP3) ▪ Microsoft® Windows® Embedded for Point of Service 1.0 ▪ Microsoft® Windows® 10 (without a display)	800MHz	256MB	
▪ Microsoft® Windows® 10 (with a display)	800MHz	512MB	
<u>Note</u>: all popular platforms with the above-mentioned operating systems are supported.			

3. Installing and setting up SoftControl SysWatch

SoftControl SysWatch can be installed onthe client hosts locally [11], as well as by one of the remote centralized [15] methods. Choosing the appropriate installation method depends on the specific application and is determined by the number of criteria such as the amount of the endpoints, network structure, security policy, and other features of the deployment environment.

This section also describes how to register SoftControl SysWatch on SoftControl Service Center [28].

3.1. Local installation

This method means local installation of the application copies on the each of the client hosts.

You can install SoftControl SysWatch locally in the following ways.

- standard mode (via GUI) [11];
- silent mode [14];
- silent mode with the help of configuration file [15].

3.1.1. Installing the component in standard mode

1) Run the *SoftControl_SysWatch.msi* installation package.

2) Click **Next** in the **SoftControl SysWatch Setup** window (fig. Running the installer [11]).

Figure 1. Running the installer

3) If you accept the terms, select **I accept the terms in the License Agreement** and click **Next**

(fig. License agreement [12]).

Figure 2. License agreement

4) Select a directory to install SoftControl SysWatch to (with the help of the **Change** button) and click **Next** (fig. Installation path [12]).
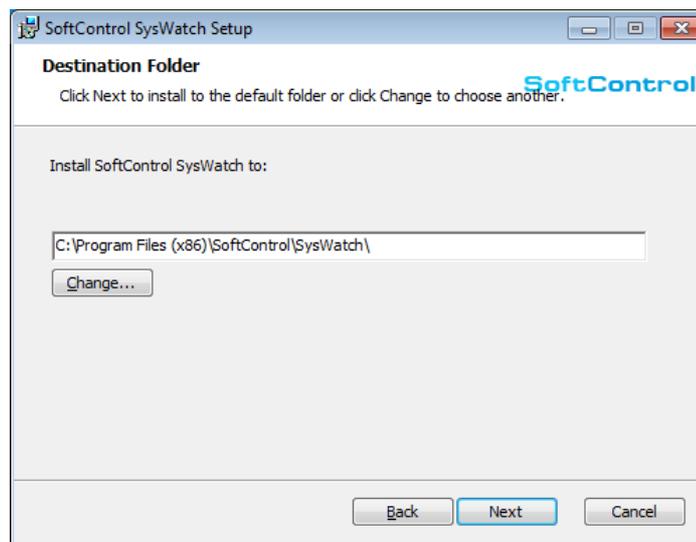
Figure 3. Installation path

5) By default, SoftControl SysWatch starts gathering system profile after installation (fig. Enabling profile collection [12]). As the process takes some time, you can deselect the option and run profile gathering later (see section Run on demand [46]).
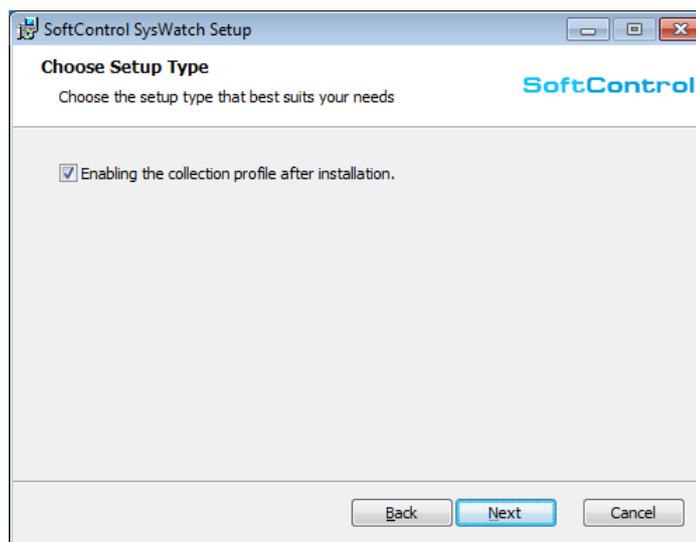
Рисунок 4. Enabling profile collection

6) Click **Install** (fig. Ready to install [13]).
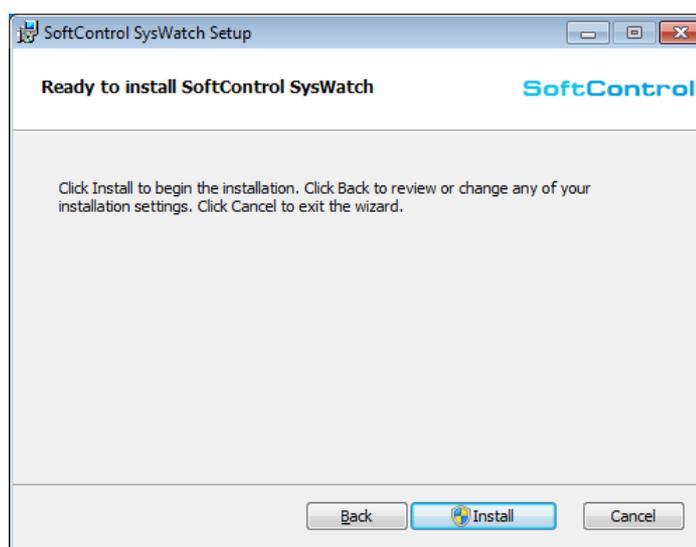
Figure 5. Ready to install

7) Wait until installation completes (fig. Installation progress [13]).
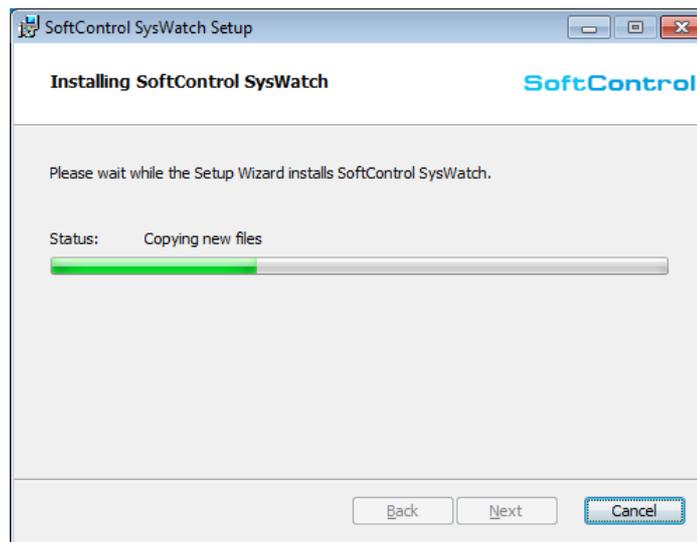
Figure 6. Installation progress

8) After the **Completed the SoftControl SysWatch Setup Wizard** message is displayed, click **Finish** (fig. Installation completes [14]).
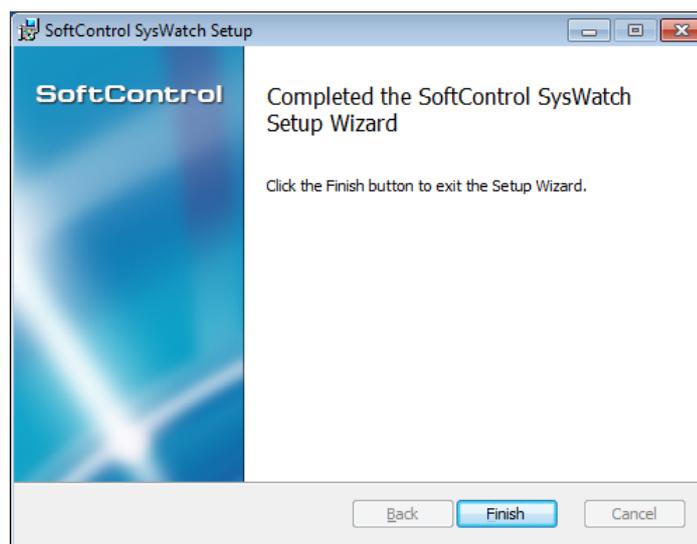
Figure 7. Installation completes

3.1.2. Installing the component in silent mode

Important: All steps require administrator privileges.

1) Copy the *SoftControl_SysWatch.msi* installation package to the `C:\Temp` directory of a client host.

2) Run Windows command prompt and enter the following command:

```
%windir%\system32\msiexec.exe /i "C:\Temp\SoftControl SysWatch.msi" /quiet
```

3.1.3. Installing the component in silent mode with the help of configuration file

<u>Important</u>: All steps require administrator privileges.

1) During silent installation, you can apply custom configuration (previously exported program settings [104]; *Storage.xmlc* in the example below) or configuration file with the settings of connection to the controlling server [39] (*ClientSettings.xmlc*), while keeping the default settings for the rest of configuration. Copy the *SoftControl_SysWatch.msi* installation package and the required configuration file to the `C:\Temp` directory of a client host.

2) Run Windows command prompt and enter the following command:

   for the configuration file with custom settings:

```
%windir%\system32\msiexec.exe /i "C:\Temp\SoftControl_SysWatch.msi" configfilename="C:\Temp\Storage.xmlc" /quiet
```

   for the configuration file with the connection settings:

```
%windir%\system32\msiexec.exe /i "C:\Temp\SoftControl_SysWatch.msi" tsconfig="C:\Temp\ClientSettings.xmlc" /quiet
```

   <u>Note</u>: In this case, SoftControl SysWatch switches to the Service Center management mode [38] automatically after installation.

3.2. Remote installation

Remote SoftControl SysWatch installation implies centrally managed installation of client applicationson the group of hosts that are integrated into a network. Choosing the installation method depends on the structure of network with the endpoints where client applications are to be deployed (a workgroup or a domain), and the administrative tools in use.

You can install SoftControl SysWatch remotely in the following ways.

- via domain group policy [16];
- via the remote installation utility [25];
- via third party administrative tools [28].

3.2.1. Installing via domain group policy

Note: The example below uses Microsoft® Windows® Server 2008 R2.

1) Open the **Server Manager** snap-in from the **Administrative Tools** section of the **Start** menu in the OS of the domain controller.

2) Go to the **Features** → **Group policy Management** → **Forest: <domain name>** → **Domains** → **<domain name>** section, invoke its context menu and select **New Organizational Unit** (fig. Creating new domain organizational unit [16]).
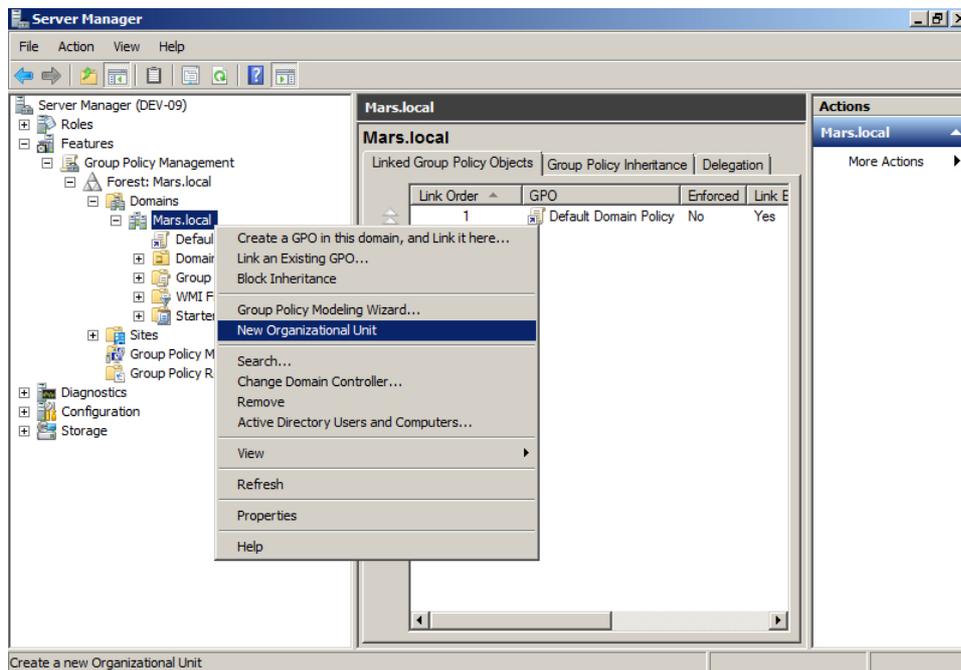
Figure 8. Creating new domain organizational unit

3) Enter **Name** of the unit in the **New Organizational Unit** dialog box and click **OK** (fig. Specifying the name of the organizational unit [16]).
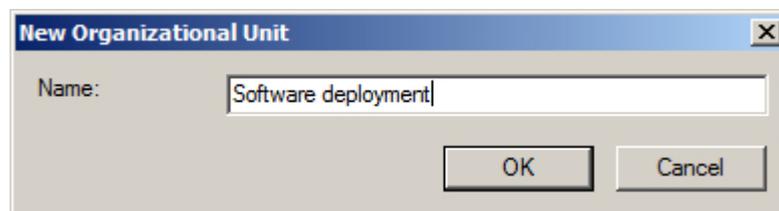
Figure 9. Specifying the name of the organizational unit

4) Invoke context menu of the created organizational unit in the **Features** → **Group policy Management** → **Forest: <domain name>** → **Domains** → **<domain name>** section and select **Create a GPO in this domain, and Link it here** (fig. Creating a new object of the group policy [16]).
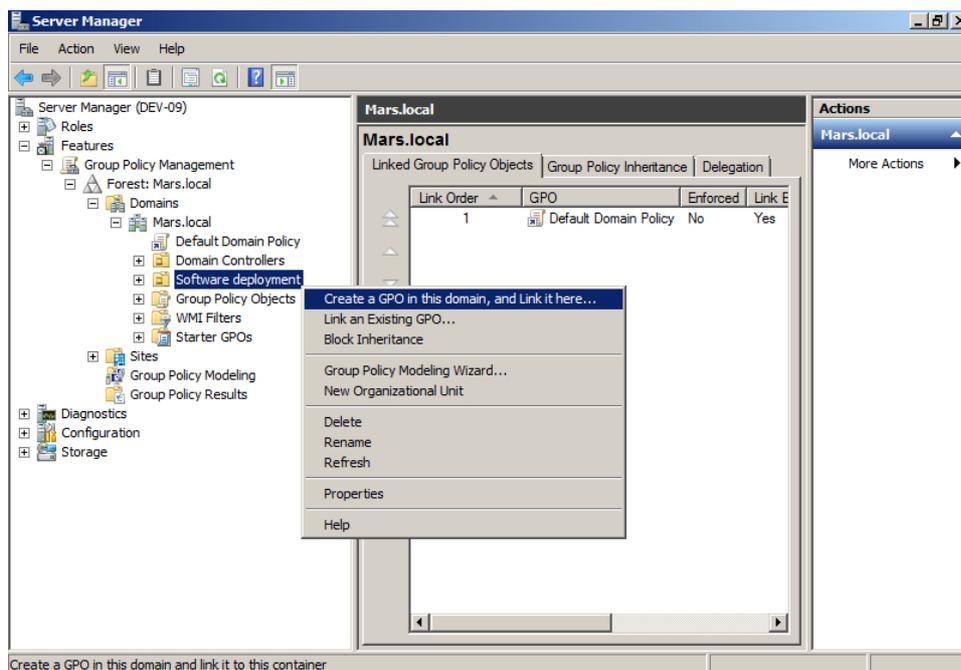
Figure 10. Creating a new object of the group policy

5) Enter **Name** of the new object in the **New GPO** dialog box and specify **Source Starter GPO**, if the new object should inherit properties from the pattern group policy, and then click **OK** (fig. Specifying the name and source starter GPO of new group policy[17]).
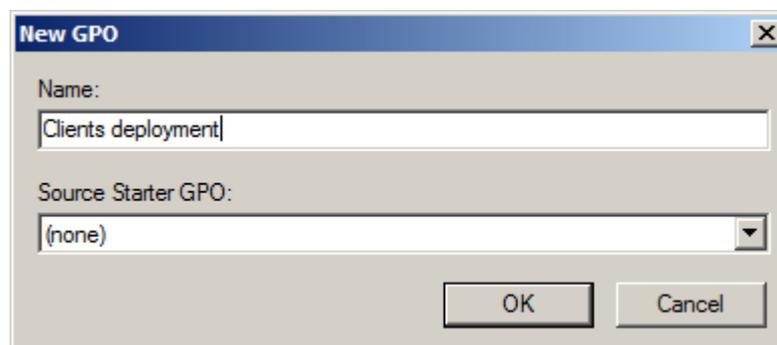
Figure 11. Specifying the name and source starter GPO of new group policy

6) Expand the created organizational unit, invoke the context menu of the created group policy object and select **Edit** (fig. Modifying group policy object[18]).

7) Go to the **Computer configuration** → **Policies** → **Software Settings** → **Software installation** section in the displayed **Group Policy Management Editor** snap-in window, invoke the context menu of the section and select **New** → **Package** (fig. Adding new installation package[18]).

8) Select the *SoftControl_SysWatch.msi* installation package which is in the network source

available to the client hosts you need to install the products to, and click **Open** (fig. Selecting the installation package [18]).
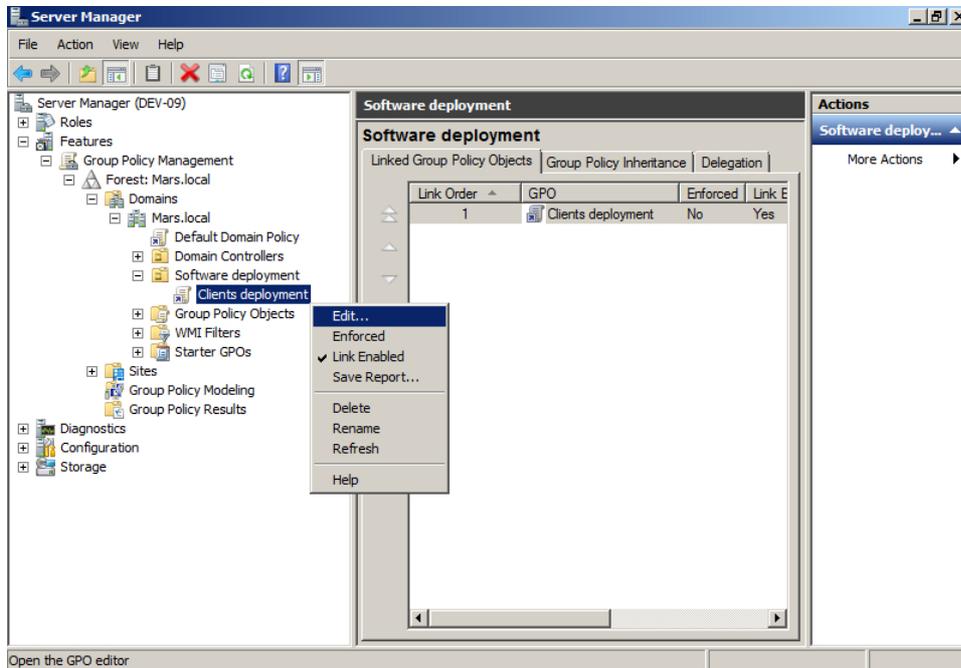
Figure 12. Modifying group policy object
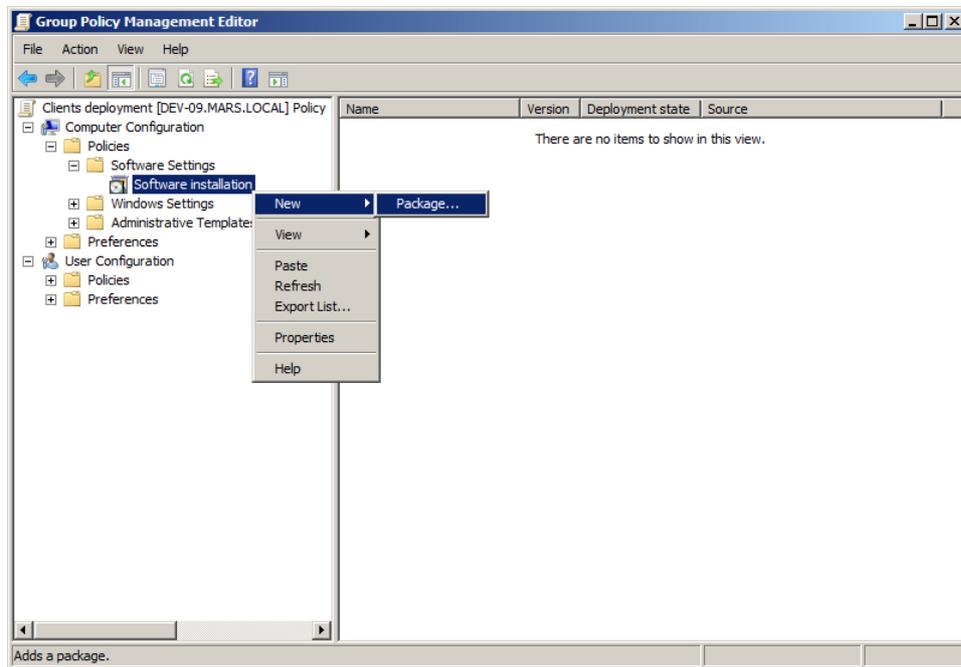
Figure 13. Adding new installation package
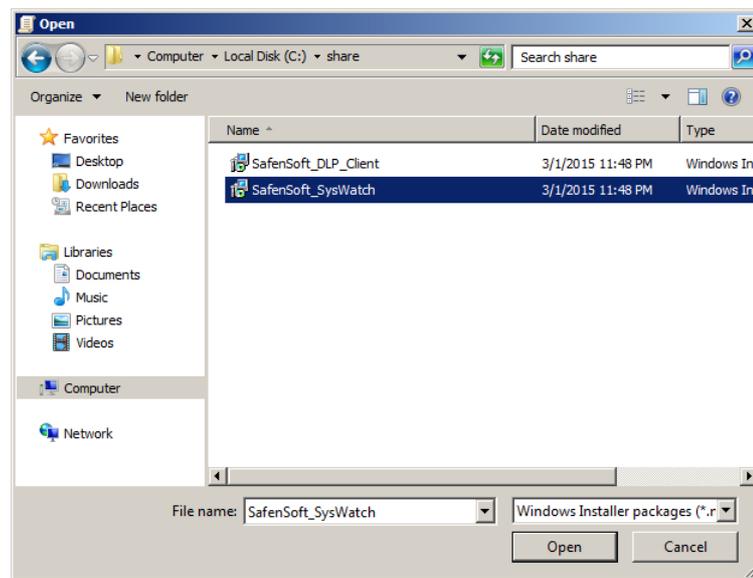
Figure 14. Selecting the installation package

9) If an alert is displayed, make sure that the selected installation package is available for the remote client hosts via network, and click **Yes** (fig. Alert when selecting the location of the installation package [19]).
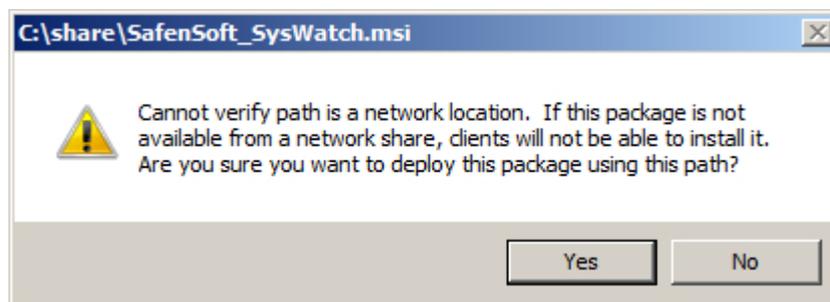
Figure 15. Alert when selecting the location of the installation package

10) Select the **Assigned** deployment method in the **Deploy Software** dialog box and click **OK** (fig. Selecting deployment method [19]).
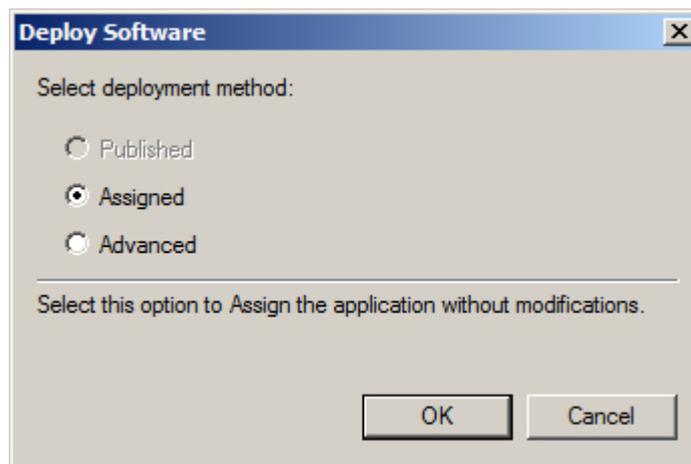
Figure 16. Selecting deployment method

11) Select the **Computer configuration** → **Policies** → **Software Settings** → **Software installation** section in the **Group Policy Management Editor** snap-in window, invoke the context menu of the section and select **Properties** (fig. Modifying properties of software deployment [20]).
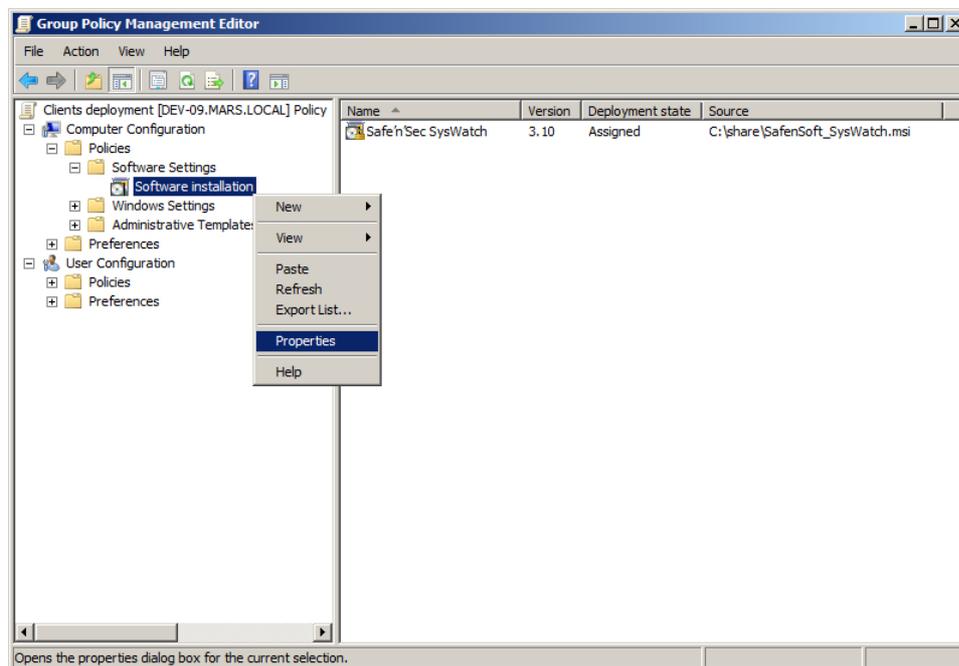
Figure 17. Modifying properties of software deployment

12) Switch to the **Advanced** tab of the **Software installation Properties** settings window, tick off **Uninstall the applications when they fall out of the scope of the management** if you need to remove applications when the specified group policy regarding the client hosts expires, and tick off **Make 32-bit X86 Windows Installer applications available to Win64 machines**, if

you plan to install onto the client hosts with 64-bit OS (fig. Properties of software deployment [21]).
To apply changes, click **OK**.
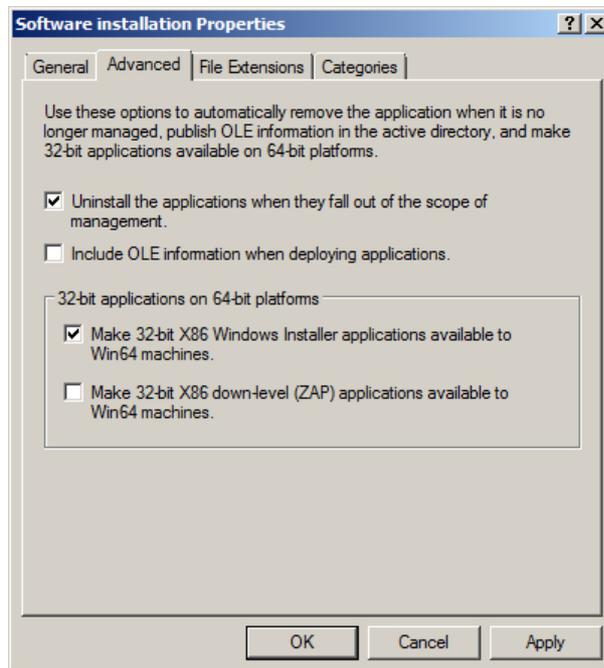
Figure 18. Properties of software deployment

13) Select the **Computer configuration** → **Policies** → **Software Settings** → **Software installation** section in the **Group Policy Management Editor** snap-in window, select the required application from the list on the right, invoke its context menu and select **Properties** (fig. Modifying the properties of the application deployment [21]).
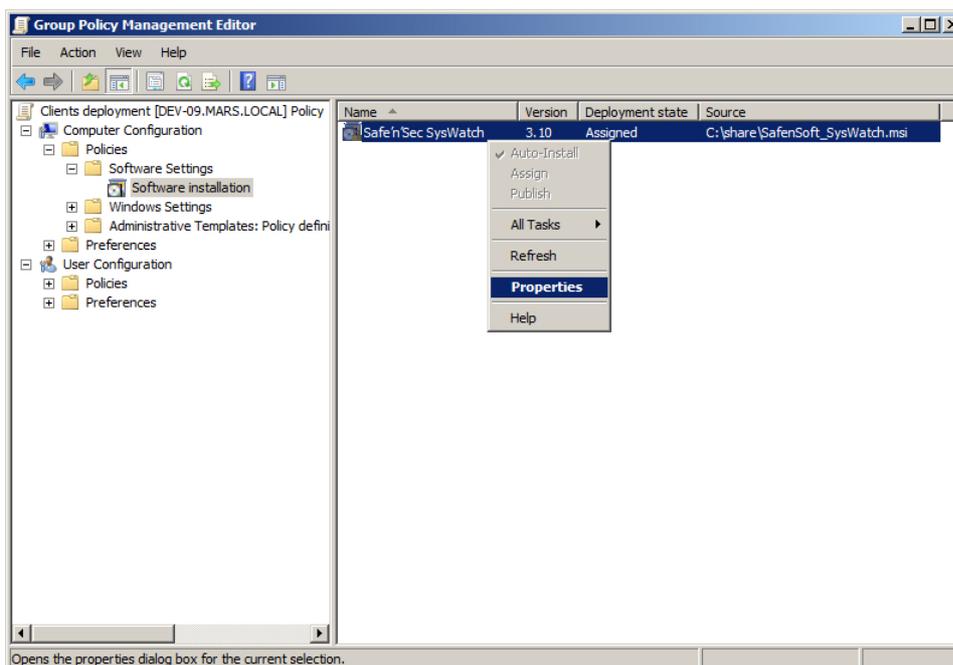
Figure 19. Modifying the properties of the application deployment

14) Switch to the **Deployment** tab of the displayed settings window and tick off **Uninstall this application when it falls out of the scope of the management** if you need to remove the application when the specified group policy regarding the client hosts expires (fig. Properties of the specific application deployment[22]).
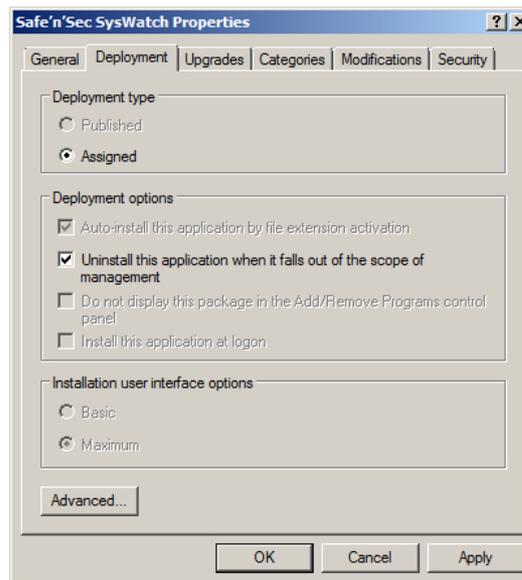
Figure 20. Properties of the specific application deployment

Click **Advanced** and tick off **Make this 32-bit X86 application available to Win64 machines** in the **Advanced deployment options** window, if you plan to install onto the client hosts with 64-bit OS (fig. Additional properties[22]). To apply changes, click **OK** in both settings window.
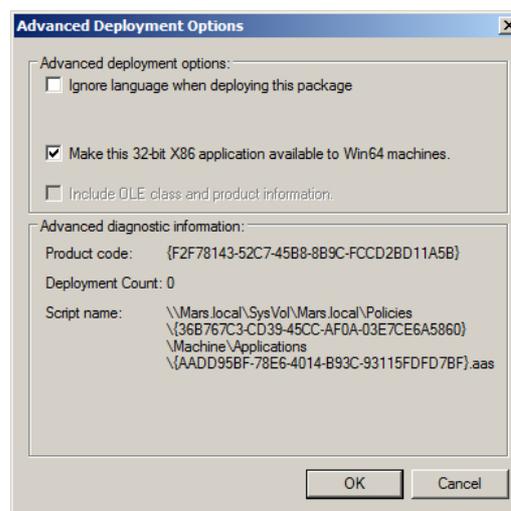
Figure 21. Additional properties

15) Close the **Group Policy Management Editor** and **Server Manager** snap-in windows and

open the **Active Directory Users and Computers** snap-in from the **Administrative Tools** section of the **Start** menu.

16) Expand the **<domain name>** section and select the **Computers** section (fig. List of the domain hosts [23]).
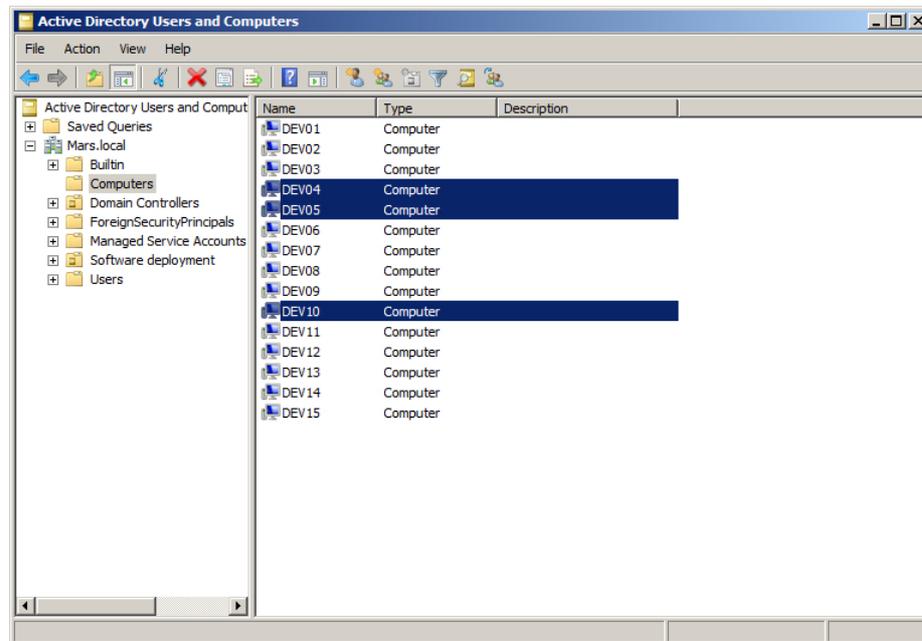
Figure 22. List of the domain hosts

17) Select the hosts that the client applications should be installed to and move them to the **Software deployment** section. Click **Yes** in the displayed alert window (fig. Alert when moving the hosts to another organizational unit [23]).
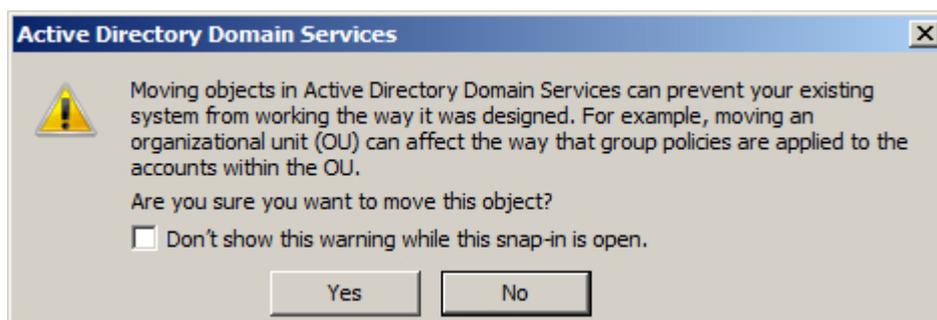
Figure 23. Alert when moving the hosts to another organizational unit

18) Open the **Software deployment** section and make sure that the required client hosts are in the list of the computers of the organizational unit (fig. List of the organizational unit hosts [23]).
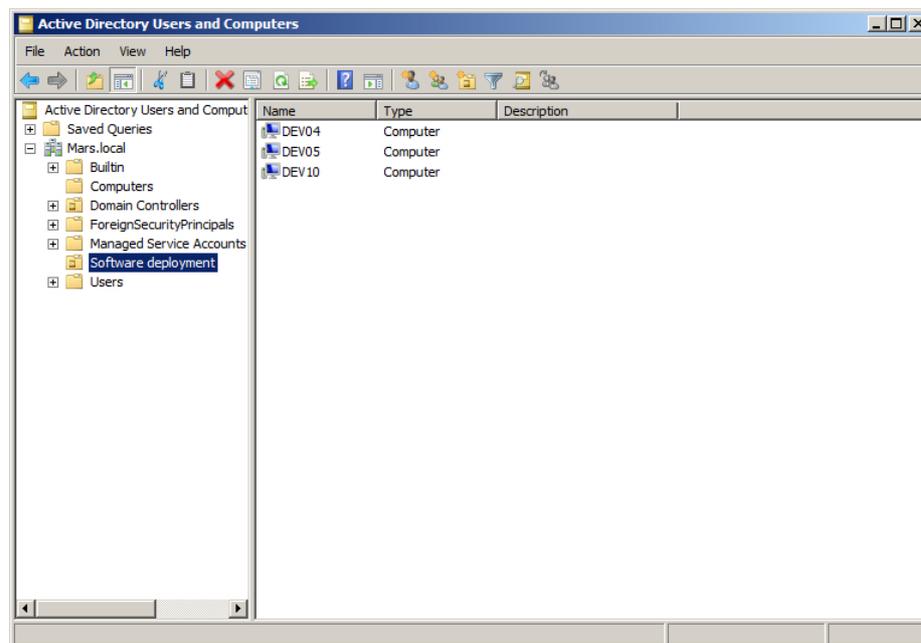
Figure 24. List of the organizational unit hosts

19) After the period of the group policy update update expires (the period depends on the Active Directory settings), the created policy is applied to the client hosts. Installation of the selected applications is performed after the next reboot of the client hosts. To apply the created group policy immediately, run Windows command prompt with the administrator privileges on a client host and enter the following command:

`gpupdate /force`

After the command executes, confirm system reboot by the *Y* command to apply the updated group policy (fig. Updating the group policy manually[24]).
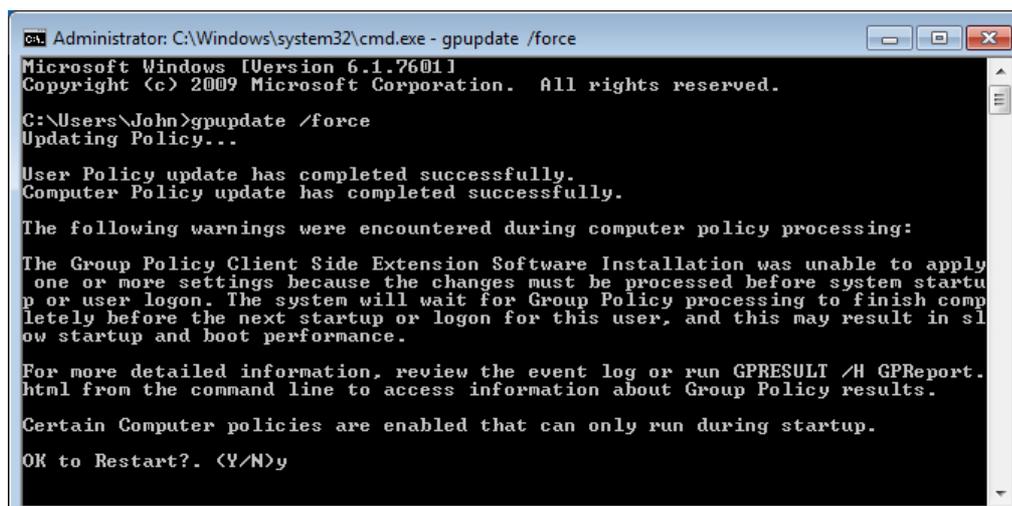
Figure 25. Updating the group policy manually

3.2.2. Installing via the remote installation utility

ℹ This installation method is designed for cases when installation via domain group policy is impossible, for example, if a network of protected endpoints is organized into a workgroup.

The *srvrimp.exe* command prompt utility is supplied along with SoftControl Service Center and is intended for remote installation of the SAFE 'N SEC Corporation client components. The utility is in the SoftControl Server component installation directory.

To install successfully, the remote hosts should meet the following conditions.

▽ **Installation conditions**

▪ User account with administrator privileges from the **Administrators** group exists on the server and remote endpoints. Login and password of such account should be the same on all the hosts.

▪ The following system services are running:

1) *Remote Registry*;

2) *Remote Procedure Call (RPC)*;

3) *Remote Procedure Call (RPC) Locator*;

4) *Windows Management Instrumentation*.

▪ The *Windows Installer* system service isn't disabled and isn't blocked.

▪ Shared resources *host*\C$ and *host*\ADMIN$ are open for Read, Write and Delete access.

Microsoft® Windows® XP, Microsoft® Windows® Server 2003:

1) Open the **Folder options** tool of the Windows Control panel.

2) Switch to the **View** tab.

3) Disable the **Use Simple File Sharing** option.

Microsoft® Windows® 7, Microsoft® Windows® Server 2008, Microsoft® Windows® 8, Microsoft® Windows® Server 2012:

1) Open the **Folder options** tool of the Windows Control panel.

2) Switch to the **View** tab.

3) Disable the **Use Sharing Wizard** option.

4) Open the **User Account Control Settings** tool of the Windows Control panel.

5) Disable user account control by moving the slider with the notification level to **Never notify**.

6) Open the following system registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`

7) Invoke the context menu of the above-mentioned key, select the **New → DWORD Value** command and enter the **LocalAccountTokenFilterPolicy** name for the created value.

8) Invoke the context menu of the created value, select the **Modify** command and enter **1** in the **Value data** field of the displayed window; then click **OK**.

9) Reboot the system to apply the changes.

▪ Common access is enabled with the following parameters.

Microsoft® Windows® 7, Microsoft® Windows® Server 2008:

1) Open **Network and Sharing Center** of the Windows Control panel.

2) Make sure that the host has the following network location: **Home network** or **Work network** for a workgroup, or **Domain network** for a domain. To change network type, click the link with name of the current network location.

3) Click **Change advanced sharing settings** and expand the profile of the current network location.

4) Select the **Turn on file and printer sharing** option in the **File and printer sharing** section.

5) Select the **Use user accounts and passwords to connect to other computers** option in the **HomeGroup Connections** section.

6) Click **Save changes**.

Microsoft® Windows® 8, Microsoft® Windows® Server 2012:

1) Double-click the network icon in the notification area.

2) Right-click the network name in the displayed list on the right and select **Turn sharing on or off**.

3) Select **Yes, turn on sharing and connect to devices**.

4) Open **Network and Sharing Center** of the Windows Control panel.

5) Click **Change advanced sharing settings** and expand the **Private** network profile.

6) Select the **Turn on file and printer sharing** option in the **File and printer**

sharing section.

7) Select the **Use user accounts and passwords to connect to other computers** option in the **HomeGroup Connections** section.

8) Click **Save changes**.

▪ Connection to the **File and Printer Sharing** service is enabled when Windows firewall is on.

Microsoft® Windows® XP, Microsoft® Windows® Server 2003:

1) Open Windows firewall.

2) Switch to the **Exceptions** tab.

3) Add to exceptions (tick off a checkbox at the rule) **File and Printer Sharing**.

Microsoft® Windows® 7, Microsoft® Windows® Server 2008, Microsoft® Windows® 8, Microsoft® Windows® Server 2012:

1) Open Windows firewall.

2) Open **Advanced settings**.

3) Select **Inbound Rules**.

4) Enable the **File and Printer Sharing (SMB-In)** for the profile of the network the host is located in.

▪ The following parameters are selected in the **Administrative Tools → Local Security Policy** tool of the Windows Control panel: **Local Policies → Security Options → Network access: Sharing and security model for local accounts → Classic - local users authenticate as themselves**.

▽ **Utility startup options**

Command line options for the remote installation utility are described in table 4.

Table 4. Srvrimp options

Option	Description
-h	Brief information about the utility options.
-i	Switch to the installation mode. Mandatory keys and their values should be specified as described below..
--login=<login>	Login of the user that have administrator privileges on the remote host.
--password=<password>	Password of the user that have administrator privileges on

Option	Description
	the remote host.
--client="<path to installer>"	Path to the SoftControl SysWatch installation package. If the file is in the utility execution folder, you can specify only the file name (without the quotes).
--config="<path to configuration file>"	Path to the configuration file with the settings of connection to the remote server. It's required to send automatic request for registration [28] on the SoftControl Server after the installation completes. If the file is in the utility execution folder, you can specify only the file name (without the quotes).
--hostnames=<name 1> <name 2>...<name N>	List of NetBIOS names of the remote hosts (separated with spaces) which the installation should be performed on.

You can also run the utility without specifying the key names, by placing the values in the following order:

```
srvrimp -i <login> <password> "<path to installer>" "<path to configuration file>" <name 1> <name 2>...<name N>
```

> ℹ If you need to install the client component on the server as well, run Windows command prompt with the administrator privileges and run the utility from it.

If installation is successful, the following message is displayed: _Installation successfully completed on host <name>_.

3.2.3. Installing via third party administrative tools

To install SoftControl SysWatch remotely, you can use third-party IT infrastructure management systems, for example, Microsoft® System Center Configuration Manager (hereafter referred to as MS SCCM). In this case, the installation method depends on the system in question and on the way in which the installation packages are distributed in this system.

3.3. Registration on the server

SoftControl SysWatch is a client component and can operates both in stand-alone and remote control from SoftControl Service Center modes. To connect SoftControl SysWatch to SoftControl Service Center, it's required to register it on SoftControl Server. To do so, take the following steps:

1) Switch SoftControl SysWatch to the remote management from the server [38] mode in the program settings.

2) Apply encrypted configuration file [39] with connection to the server settings.

3) Approve registration in SoftControl Admin Console on the **Client statuses** tab (see the

'SoftControl Service Center administrator's guide' document).

4. Working with SoftControl SysWatch locally

This section contains instructions of how to work with main SoftControl SysWatch functions locally.

4.1. SoftControl SysWatch interface

SoftControl SysWatch graphical user interface (GUI) consists of the following main elements.

- Program icon in the taskbar notification area [31] (item 1 in fig. below [30]);
- Context menu [31] (item 2 in fig. below [30]);
- Control panel [32] (item 3 in fig. below [30]).
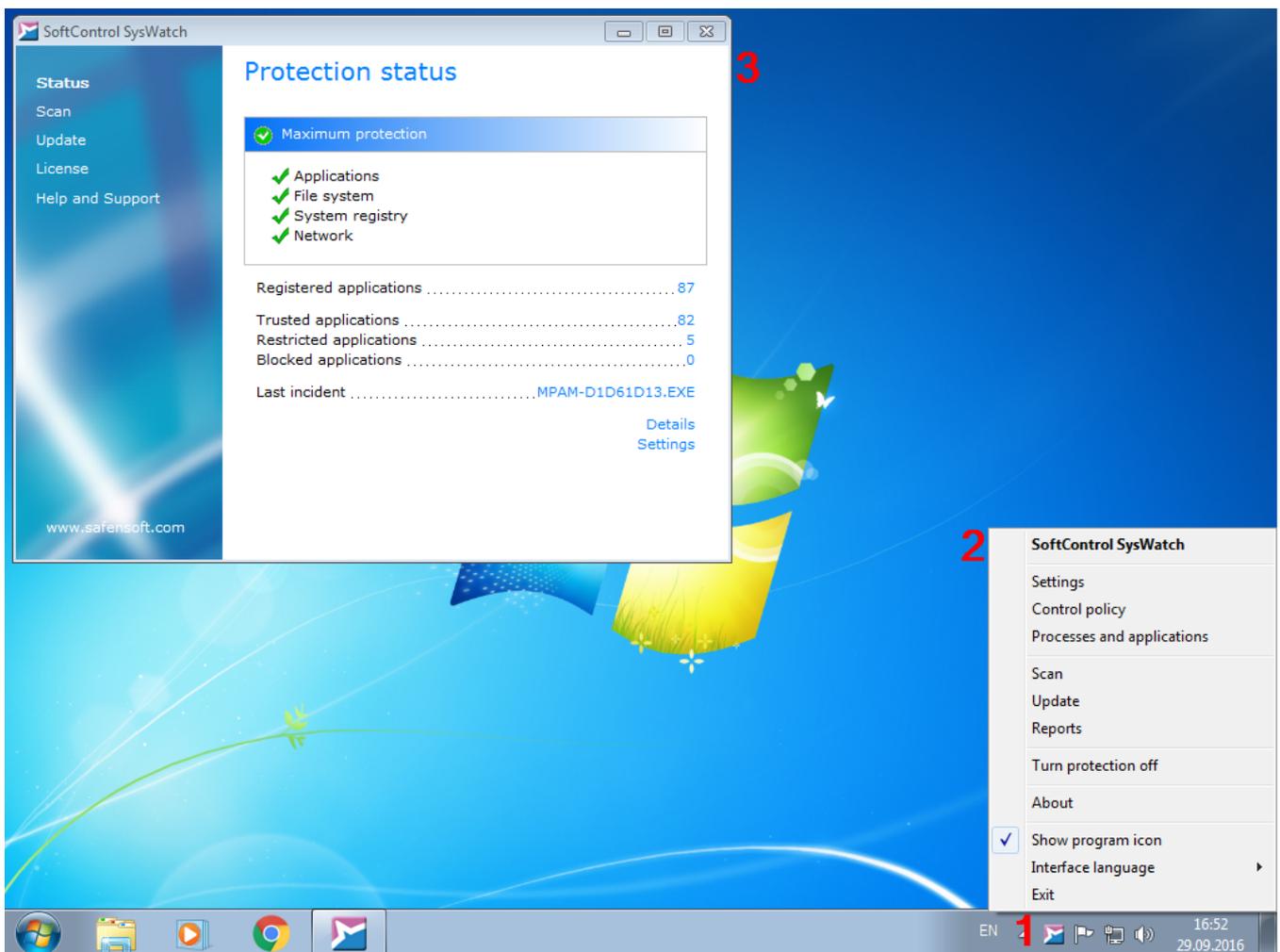
Figure 26. Elements of the program GUI

4.1.1. Program icon

After SoftControl SysWatch is installed, it displays its icon in the Windows taskbar notification area.

The icon indicates the program activity. It displays the protection status and displays a number of main operations that the application performs (table 5).

Table 5. Program statuses

Icon	Program status
	Protection is activated (at least one of the protection regions is under control).
	Protection is deactivated.
	Automatic setting or antivirus scanning is in progress.
	Software modules or antivirus bases update is in progress.

The icon also provides access to other main elements of the program interface: the context menu [31] and the control panel [32]:

- in order to activate the context menu, right-click the program icon;
- in order to activate the control panel, double-click the program icon.

4.1.2. Context menu

The context menu contains the items that provide quick access to the main settings and commands of SoftControl SysWatch. The menu is shown in fig. SoftControl SysWatch context menu [31], while table 6 lists the description of the items.

SoftControl SysWatch

Settings
Control policy
Processes and applications

Scan
Update
Reports

Turn protection off

About

√ Show program icon
Interface language ▶
Exit
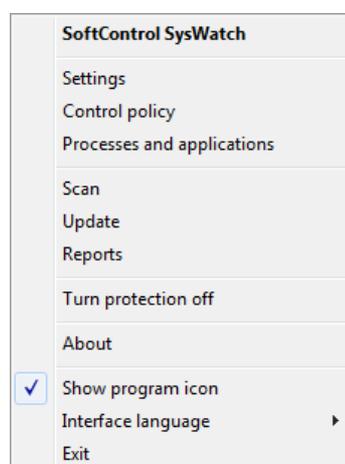
**Figure 27. SoftControl
SysWatch context menu**

Table 6. Description of the SoftControl SysWatch context menu items

Menu item	Action
SoftControl SysWatch	Open the **Status** tab of the program's control panel.
Settings	Open program settings.
Control policy	Open the **Common rules** tab of the **Control policy** window to view and modify the rules of the applications' access to computer resources and devices, as well to view and modify the rules of network activity.
Processes and applications	Open the **Processes and applications** tab of the **Control policy** windows to view and modify the rules of the applications' activity.
Scan	Open the **Scan** tab of the program's control panel.
Update	Open the **Update** tab of the program's control panel.
Reports	Open the directory with the reports.
Turn protection off/on	Change the protection activity status.
About	Open the SoftControl SysWatch general information window.
Show program icon	Switch off/on the program icon in the taskbar notification area.
Interface language	Select the program interface language.
Exit	Shutdown the program GUI (note that the SoftControl SysWatch interface module is deleted from RAM, but the protection module is still running).

4.1.3. Control panel

Control panel is the main SoftControl SysWatch window that comprises the **Status**, **Scan**, **Update**, **License**, and **Help and Support** tabs.

The **Status** tab displays current protection status (fig. The 'Status' tab [32]). See sections Applications activity control [49] and Control policy [65] for details on this tab.

Figure 28. The 'Status' tab

The **Scan** tab contains the tree of objects to be checked by antivirus on request (fig. The 'Scan' tab [33]). See section Antivirus scanning [87] for details.
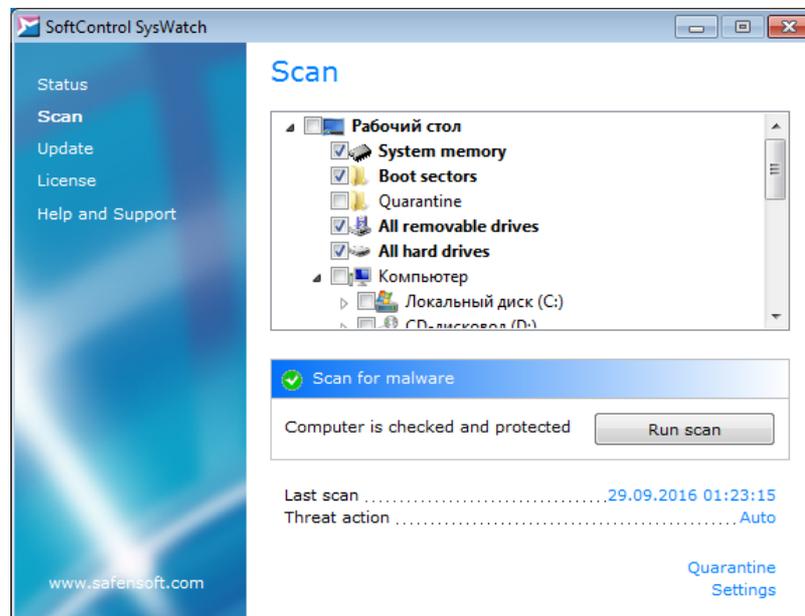
Figure 29. The 'Scan' tab

The **Update** tab indicates whether any updates of software modules and antivirus bases [111] are available (fig. The 'Update' tab [33]).
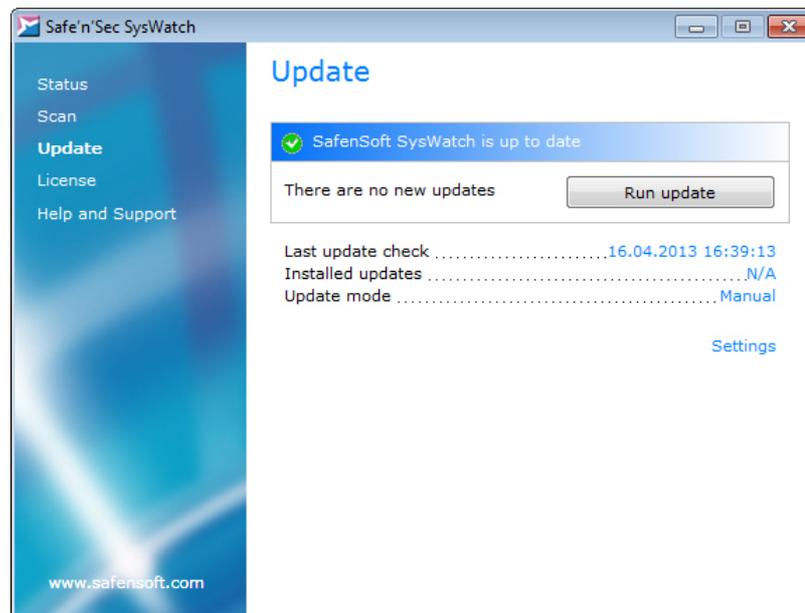
Figure 30. The 'Update' tab

The **License** tab contains information on the license key [40] that the program uses and the program components (fig. The 'License' tab [34]).

The **Help and Support** tab displays the version of the installed SoftControl SysWatch and information about the OS. By clicking **Open Help** on this tab you can invoke SoftControl SysWatch help. You can contact the company's customer support [126] through the website. The tab is shown in fig. The 'Help and Support' tab [34] .
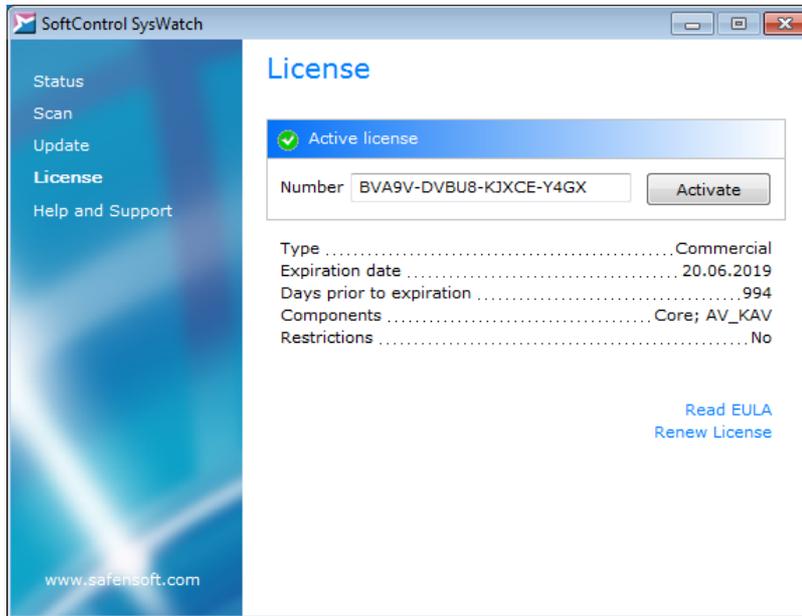
Figure 31. The 'License' tab
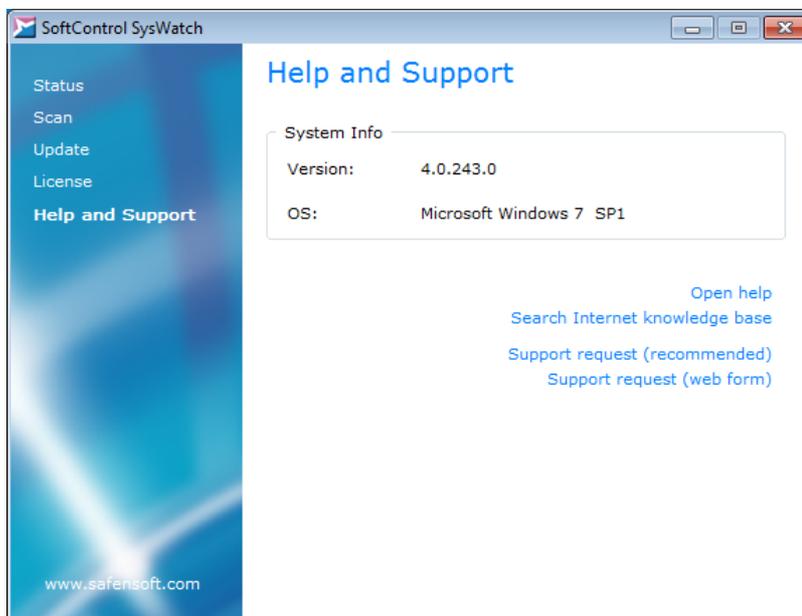
Figure 32. The 'Help and Support' tab

4.1.4. Interface settings

▽ **Setting up the interface**

To view and modify SoftControl SysWatch GUI parameters, open program settings and select **Settings** → **View** (fig. Interface settings [35]).

Select the required interface **Language** in the corresponding drop-down list:

- **English**;

- **Русский** (Russian).

Tick off **Show program icon in the taskbar notification area** to show the icon [31].
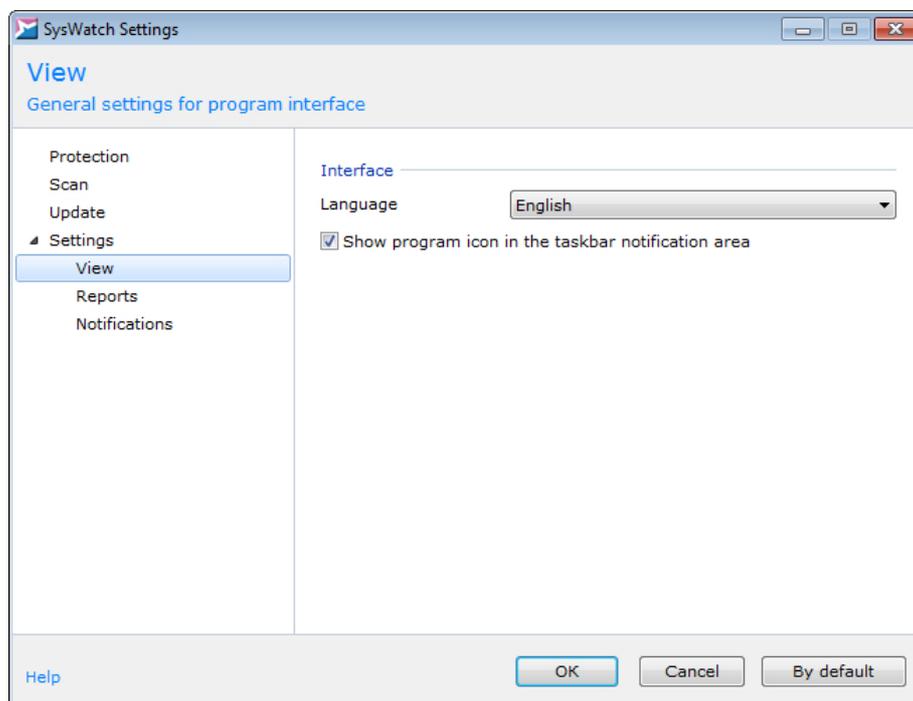
Figure 33. Interface settings

▽ **Setting up local notifications**

To specify how the SoftControl SysWatch user is notified about incidents and the program state, open program settings and select **Settings** → **Notifications** (fig. Local notifications settings [35]).
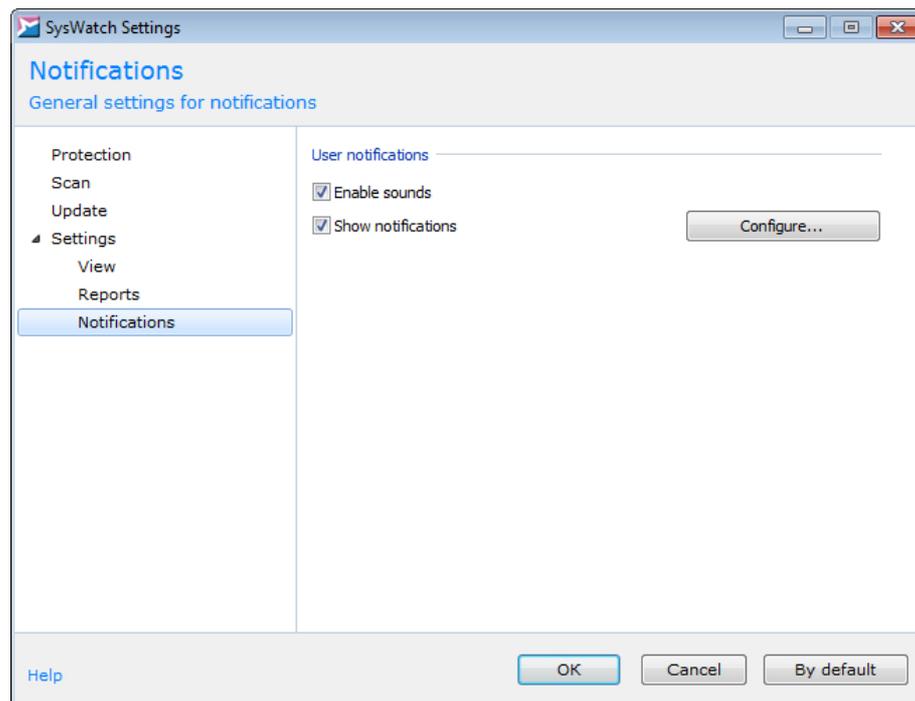
Figure 34. Local notifications settings

Tick off the **Enable sounds** checkbox if you need sound notifications about incidents.

To enable text and graphical notifications, tick off the **Show notifications** checkbox and click **Configure**. Select the required events in the **General settings for notifications** window (fig. Selecting event types for notifications [36]):

❑ **Protection status**;

❑ **Update**;

❑ **Scan for malware**;

❑ **Reports**;

❑ **Licensing**;

❑ **Application installation (uninstallation)**;

❑ **Program modules blocking**;

❑ **Restricting applications**.
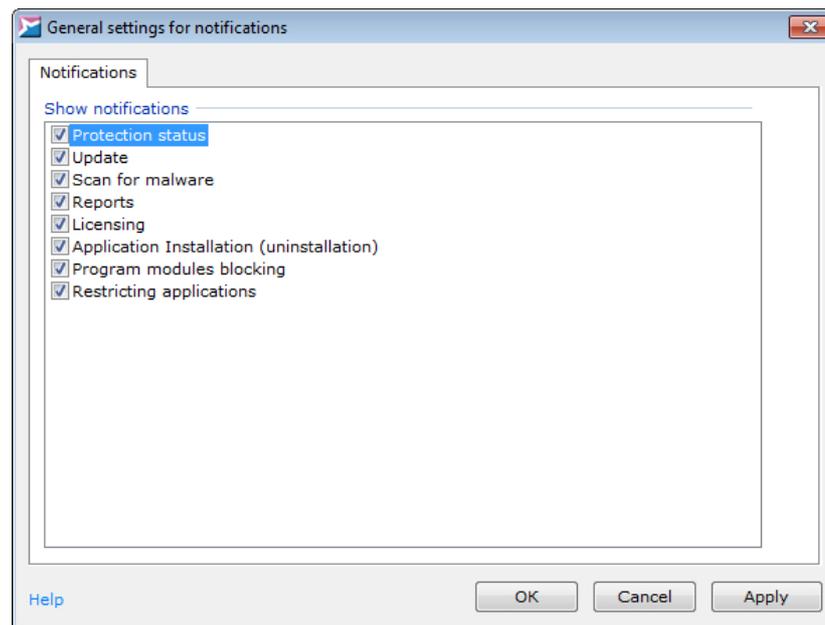
Figure 35. Selecting event types for notifications

Click **OK** to apply changes.

4.2. Management modes

SoftControl SysWatch can be managed in the following modes.

▪ Stand-alone mode ⁽³⁸⁾;

▪ Remote control from the server ⁽³⁸⁾.
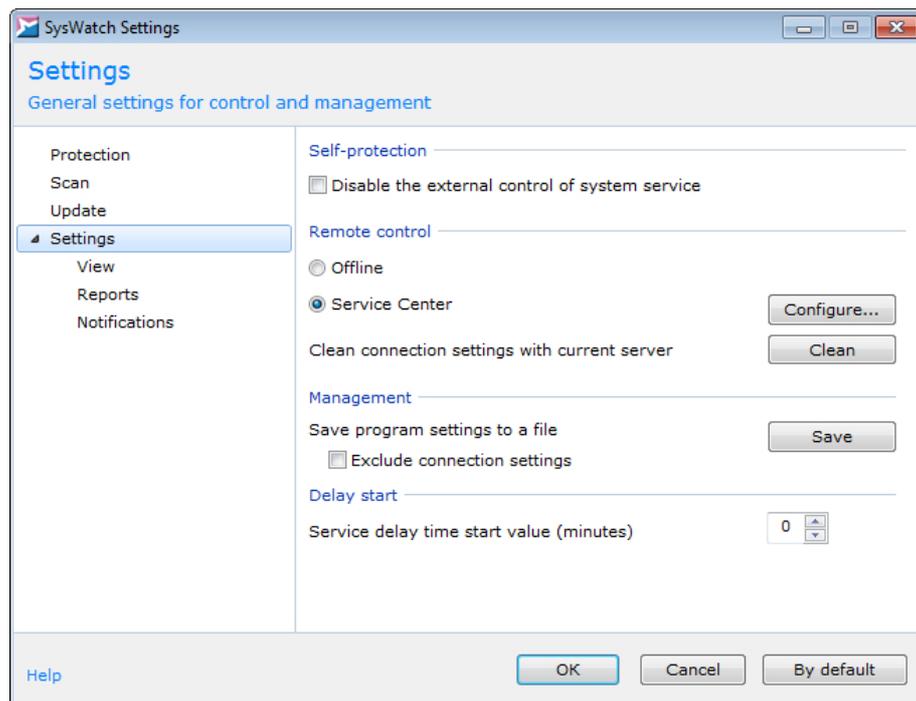
Figure 36. Setting up the program parameters

To set the management mode, open program settings and select the required option in the **Remote control** area of the **Settings** section (fig. Setting up the program parameters [37]). Click **OK** to apply changes.

4.2.1. Stand-alone mode

When SoftControl SysWatch operates in the stand-alone mode, the local user sets up the program, runs tasks and processes the incidents with the help of SoftControl SysWatch GUI.

To set this mode, select **Offline** in the program settings (fig. Setting up the program parameters [37]).

4.2.2. Remote control from the server

When SoftControl SysWatch is managed by the SoftControl Service Center administrative tools, the administrator sets up the program, runs tasks and monitors the incidents remotely. The detailed description of the process is given in 'SoftControl Service Center administrator's guide'.

To set this mode, select **Service Center** in the program settings (fig. Setting up the program parameters [37]) and click **Configure** to open the window with the server connection settings (fig. Server connection parameters [38]).
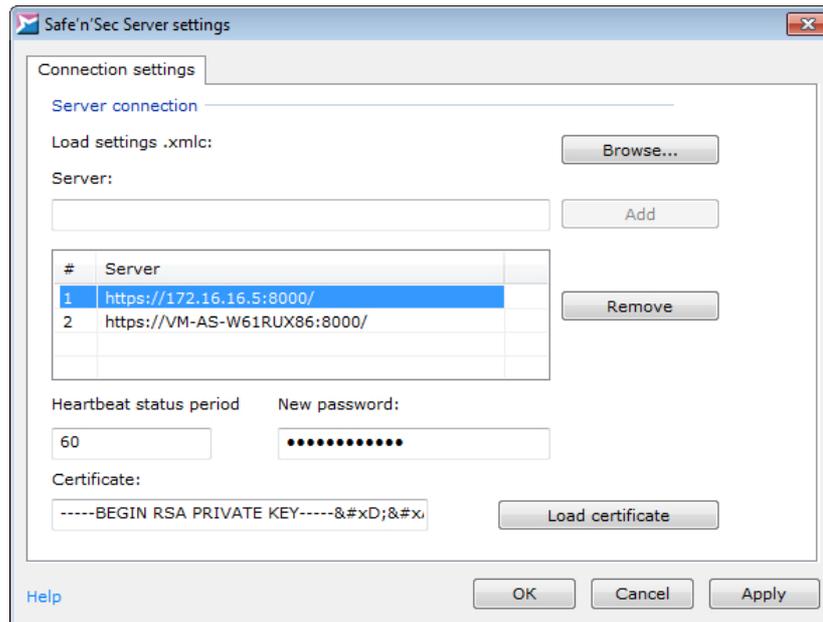
Figure 37. Server connection parameters

To apply client settings that have been specified on the server, perform the following steps.

1) Copy the *ClientSettings.xmlc* file (see 'SoftControl Service Center administrator's guide') to the hard drive of the client host.

2) Click **Browse** in the **SoftControl Server Settings** window (fig. Server connection parameters [38]).

3) In the displayed window, select *ClientSettings.xmlc* file you have copied and click **Open**.

SoftControl SysWatch sends the first request to the server as soon as the configuration file is applied. The received configuration is displayed in the **SoftControl Server Settings** window (fig. Server connection parameters [38]).

The **Server connection** area contains the list of the addresses which SoftControl SysWatch uses to connect to the controlling server (fig. Warning while cleaning the connection settings [40]). The list is specified by the administrator remotely from the SoftControl Admin Console management console. The list can also be modified manually through SoftControl SysWatch interface. To add an IP address to the list, enter the full address of the following form:

https://<server IP address or NetBIOS name>:<server connection port>/

to the **Server** field and click **Add**. To delete an IP address from the list, select it and click **Remove**. The list should contain at least one address; therefore, you cannot delete the only address.

Other connection settings are in the lower part of the **Server connection** area:

- **Heartbeat status period** is the interval between SoftControl SysWatch requests to the

controlling server (in seconds);

- **New Password** is the password for SoftControl SysWatch authentication on the controlling server (in seconds), with the certificate mentioned below;

- **Certificate** is the string representation of the certificate which is used to establish secure connection between SoftControl SysWatch and the controlling server.

All the parameters can be modified manually in the corresponding fields. To replace the certificate and leave other settings unchanged, click **Load certificate**, select the certificate file with the *.pem* extension in the displayed window and click **Open**.

If you want to disconnect SoftControl SysWatch from the current server, click **Clean** in the **Settings** section of the program settings (fig. <u>Setting up the program parameters</u>[37]). Select **Yes** in the displayed window (fig. <u>Warning while cleaning the connection settings</u>[40]).

SoftControl SysWatch automatically switches to the offline mode after the settings cleaning. To avoid the duplication of the client components when reconnecting to the same server, the administrator should remove this client component from the server via SoftControl Admin Console.
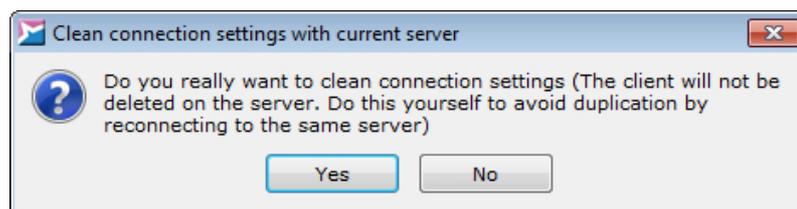
Figure 38. Warning while cleaning the connection settings

4.3. License key activation

Functionality of SoftControl SysWatch is determined by a license key. The license allows you to use the following components of the program as soon as it is installed:

- SoftControl SysWatch Core (Core) is the basic component of SoftControl SysWatch for executing proactive protection;

- Anti-Virus (AV_AV1) is an extra component that searches for viruses, trojan programs and other malicious objects (the BitDefender scanner);

- Anti-Virus (AV_KAV) is an extra component that searches for viruses, trojan programs and other malicious objects (the Kaspersky antivirus scanner);

For SoftControl SysWatch with the Kaspersky Antivirus engine, you also need a valid KAV license key (**.key*) that you should place to the following folder:

```
<SoftControl SysWatch installation directory>\Plugins\AV\KAV
```

- Anti-Virus (AV_AV3) is an extra component that searches for viruses, trojan programs and other malicious objects (the Commtouch antivirus scanner);
- Anti_Virus (AV-AV4) is an extra component that searches for viruses, trojan programs and other malicious objects (the Avira antivirus scanner).

Table 7 lists types of the SoftControl SysWatch licenses.

Table 7. Types of licenses

License	Description
Trial	The license key that is used to try the program out. Duration is 30 days. <u>Note</u>: the trial key can be used only once. Prolongation and reuse are impossible.
Commercial	The license key for full use of the program. The license properties and extra components are determined by the specific license keys.

To activate a license key locally, open the **License** tab of the SoftControl SysWatch <u>control panel</u> [32], enter the key to the **Number** field and click **Activate**. If activation is successful, the tab displays the *Active license* status.

30 days and 2 weeks before a key expires, as well as during the last week when the key is valid, the program notifies the user about it. The corresponding notification message is displayed in the mentioned days. After the license key expires, the **License** tab displays the *License has expired* status. SoftControl SysWatch remains fully functional except that <u>updates of software modules and antivirus bases</u> [111] are not possible.

We recommend that you prolong the program license in order to use new program functionality and the latest designs in the field of prevention techniques.

4.4. How SoftControl SysWatch works

The main purpose of the SoftControl SysWatch protection system is to preserve the integrity of the OS and all its components including software that has been installed by the user.

Immediately after installation, SoftControl SysWatch activates in the simple mode that allows you to monitor the start of unknown applications. This mode detects new software in the system and monitors how the executable modules are moved or modified.

When SoftControl SysWatch runs for the first time, it performs an <u>automatic setup</u> [43] which creates the basic system profile (the white list). After the automatic setup is successfully completed, SoftControl SysWatch activates the extended mode that is the program's regular mode and that

provides the most effective protection. When an unknown process attempts to run (executable component which is not in the system profile or which hasn't an installer flag), SoftControl SysWatch make decision according to the user's choice (in manual mode) or the selected options [52] (in automatic mode). As a result, the process is assigned to the one of the execution zones [56]:

- trusted;
- restricted;
- blocked.

For the process that are not blocked (trusted and restricted zone), control policy [65] rules apply that are common within each zone. The rules regulate access to file system, system registry and external devices, as well as network activity, process privileges and inter-process interaction. Besides, custom rules [62] can be assigned to each application.

SoftControl SysWatch divides the types of events that pose a security threat to the software environment (incidents) into the following main categories.

- unknown application launch;
- unknown installer launch;
- control policy violation.

Table 8 lists possible actions for the each category of incidents.

Table 8. Possible actions on incidents

Incident	Actions
Unknown application launching	• **Execute in a limited mode** The application runs under current user account or in the isolated environment ('sandbox') under the 'V.I.P.O.' user account with restricted rights. The application is not added to the system profilebut is moved to the restricted zone instead. The application can download additional modules that are not added to the system profile either. Even if this application is harmful and it installs some extra components, the system prevents them from loading. • **Scan and execute in a limited mode after** The application runs in limited mode, if no malicious code has been found during the antivirus scanning. Otherwise,the application is blocked. • **Execute in install mode** The application runs under current user account without restrictions or with reduced privileges. The application and all its child modules are moved to the system profile and the trusted zone. • **Scan and execute in install mode after** The application runs in installation mode, if no malicious code has been found during the antivirus scanning. Otherwise,the application is blocked. • **Block** (default) The application is blocked and moved to the blocked zone.
Unknown installer launching	• **Install** The installer runs under current user account without restrictions or with reduced privileges.

Incident	Actions
	The application and all its child modules are moved to the system profile and the trusted zone after installation. • **Scan and install after** The installer runs in installation mode, if no malicious code has been found during the antivirus scanning. Otherwise, the installer is blocked. • **Install in a limited mode** The installer runs under current user account or in the isolated environment («sandbox») under the 'V.I.P.O.' user account with restricted rights. The installer is not added to the system profile. The application and all its child modules are moved to the restricted zone after installation. • **Scan and install in a limited mode after** The installer runs in limited mode, if no malicious code has been found during the antivirus scanning. Otherwise, the installer is blocked. • **Block** (default) The installer is blocked and moved to the blocked zone.
Control policy violation	• **Allow** Allow a process to perform an action that meets the conditions of the specified control policy rule, once or for a session. • **Scan and allow after** Allow a process to perform an action that meets the conditions of the specified control policy rule once or for a session, if no malicious code has been found during the antivirus scanning. Otherwise, the action is blocked. • **Block** Do not allow the process to perform an action that meets the conditions of the specified control policy rule, once or for a session. • **Block and kill application** Do not allow the process to perform an action that meets the conditions of the specified control policy rule, and then kill the process, once or for a session.

4.5. Automatic setup (profile gathering)

Automatic setup, or profile gathering, is an important step to provide proactive protection of the system's software environment. Profile gathering starts automatically as soon as SoftControl SysWatch completes installation, except for silent installation with the help of the configuration file where this option is disabled or postponed start is selected[108]. It is presumed that system does not contain malware when profile gathering starts. Therefore, initial profile gathering is performed with the antivirus scan option[44] enabled, to make sure this condition is met. If ab object is not infected, its checksum is calculated and added to the profile. The objects are PE files.

Before you start profile gathering on demand[46], set up its parameters[44].

4.5.1. Profile gathering options

To set up the parameters of the profile gathering, open program settings and click **Configure** in the **Protection status** area of the **Protection** section (fig. Common protection settings [44]).
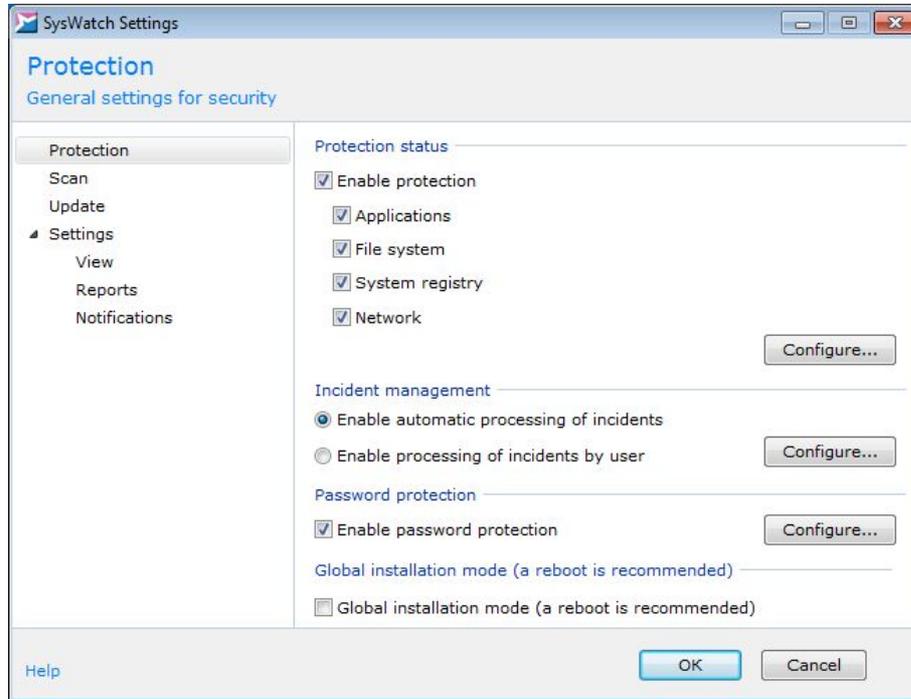
Figure 39. Common protection settings

Click **Settings** in the **System Profiling** tab of the **General settings for protection** window (fig. Profile gathering window [44]).
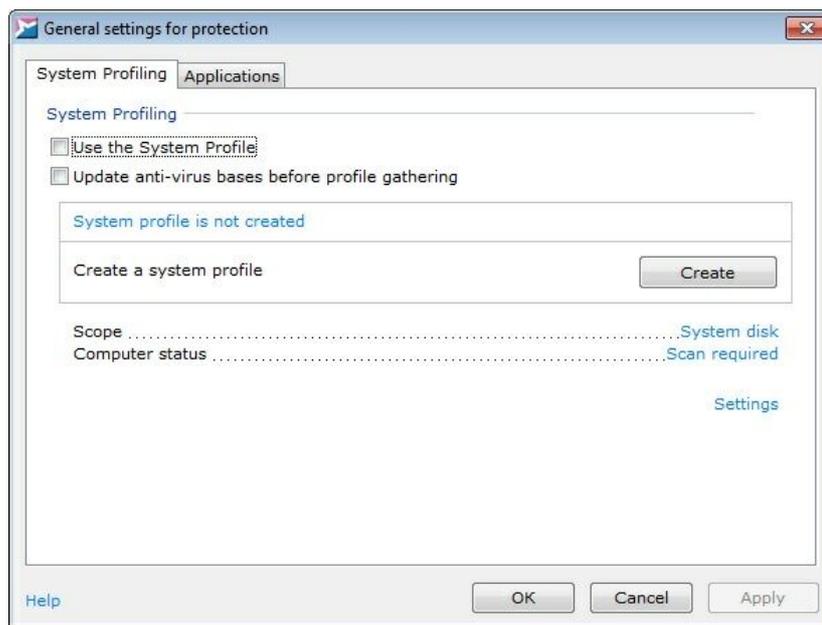
Figure 40. Profile gathering window

There are two options for the automatic setup in the **Computer state** area (fig. [Profile gathering options](#) [45]).

o **Scan required**

If you select this option, full automatic setup including antivirus scanning is performed. We recommend that you scan the computer during automatic setup if no antivirus software is installed in the system, and therefore, security vulnerabilities may exist.

o **Clean, scan is not required**

If you select this option, automatic setup is performed without antivirus scanning.

ℹ Full automatic setup requires more system resources and time than automatic setup without antivirus scanning.
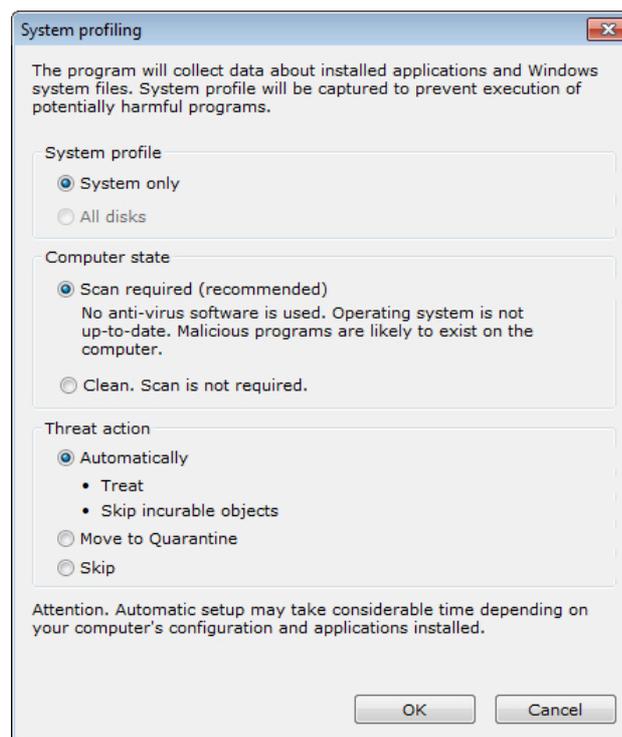
Figure 41. Profile gathering options

You can select the following actions on detecting the threats during antivirus scanning, in the **Threat action** area (available only for full automatic setup):

o **Automatically**:

• **Treat**

Neutralize the infected object.

• **Skip incurable objects**

Do not perform any operations with the infected object if it cannot be treated.

○ **Move to Quarantine**

Move the infected object to a special folder and do not allow it to run.

○ **Skip**

Don't perform any operations with the infected object.

4.5.2. Run on demand

▽ **Starting profile gathering**

To start profile gathering, click **Create** in the **System Profiling** tab of the **General settings for protection** window (fig. Profile gathering window [44]).

ℹ︎ We do not recommend that you install any software during automatic setup.

If you need to interrupt profile gathering, click **Stop** (fig. Profile gathering in progress [46]).
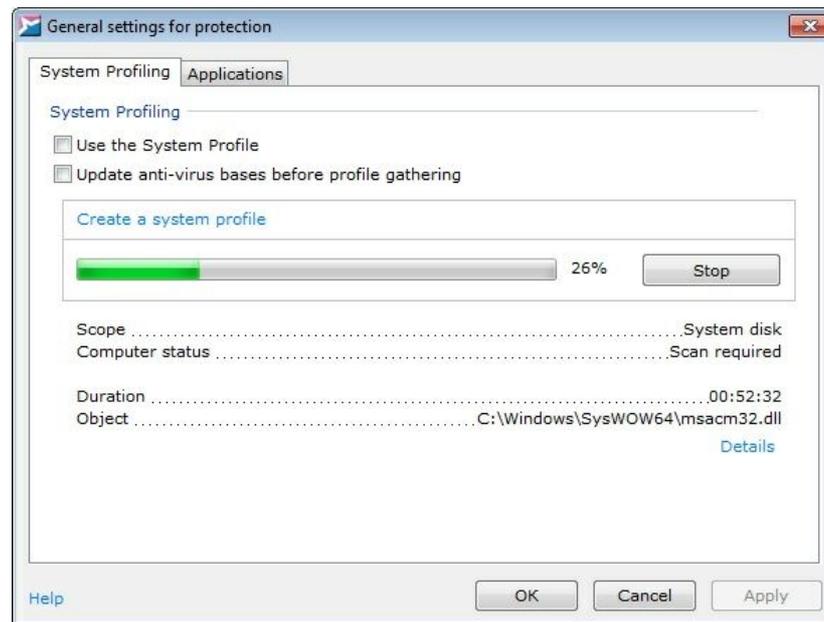
Figure 42. Profile gathering in progress

In the dialog box, select whether to save the collected data about the files so as to use it when profile gathering continues (fig. Choosing how to interrupt profile gathering [46]). By clicking **Yes** you will be able to continue profile gathering from where it was interrupted.
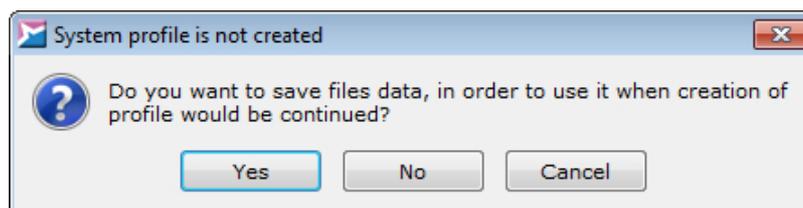
Figure 43. Choosing how to interrupt profile gathering

ℹ️ If the *safensec.exe* system service is interrupted during automatic setup, SoftControl SysWatch automatically resumes profile gathering after the service runs again. If the user stops profile gathering with the help of the corresponding button, SoftControl SysWatch does not resume profile gathering after the *safensec.exe* system service runs again. In this case, you should run automatic setup manually to continue it.

After profile gathering completes, the *System profile created* status is displayed and the **Use the System Profile** checkbox is ticked off: the program turns into the extended mode.

▽ Updating system profile

You can update system profile when necessary (for example, if a large number of software has been deployed without the installers, or SoftControl SysWatch protection was inactive). The full profile is not gathered during the update; instead, SoftControl SysWatch gathers data only about applications that have not been included in the profile when the update started. To perform the operation, click **Update** in the **System Profiling** tab of the **General settings for protection** window (fig. Running profile update [48]).

Figure 44. Running profile update

▽ Adding certain files to the profile

If you need to add only certain file or folder with files to the system profile, click the **Scope** string in the **System Profiling** tab of the **General settings for protection** window (fig. Running profile update [48]), select the corresponding option (**Add file** or **Add folder**), specify the required files and click **Open**. When the path to the required file or folder is displayed in the **Scope** string, click **Update**.

▽ Viewing profile gathering report

To view the detailed report about the performed profile gathering, click **Details** (fig. Running profile update [48]).

4.6. Applications activity control

Current protection status and the list of the control scopes are displayed in the **Status** tab of the program's control panel [32]. The tab also displays statistics about the total number of the registered processes, the number of applications in each of the execution zones [56] and the name of the process which caused the last incident. By default, protection is established over all control scopes (the *Maximum protection* status is displayed). You can enable or disable control for each of the scopes by left-clicking the scope name. The overall protection status then changes to *Limited protection* if you disable control for at least one scope, and to *Computer is not protected* if you disable control for all scopes. These features are duplicated in the program settings in the **Protection** section (fig. General protection settings [49]). SoftControl SysWatch controls the applications' activity when the **Applications** scope is ticked off.
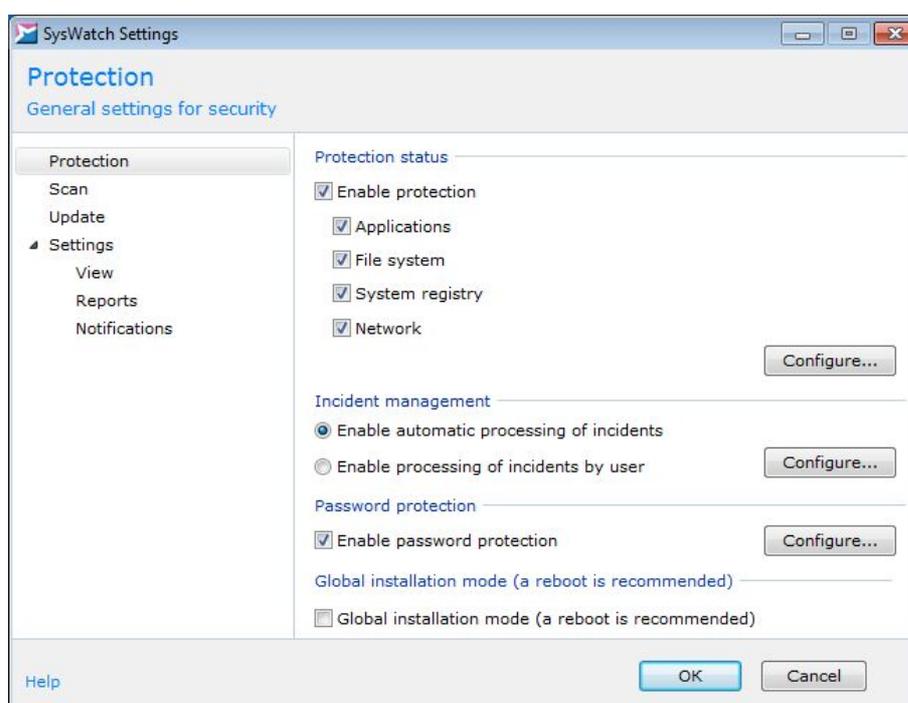
Figure 45. General protection settings

Below is the detailed information about the settings of the application activity control:

- activity control options [50];
- handling the process start incidents [51];
- application execution zones [56];
- properties of certain applications [59];

- <u>white list of certificates</u> (63).

4.6.1. Activity control options

To change additional activity control options, open the **Protection** section of the program settings, click **Configure** in the **Protection status** area (fig. <u>General protection settings</u> (49)), and go to the **Applications** tab of the **General settings for protection** window (fig. <u>Activity control options</u> (50)).

The **Applications** area contains the following options.

❑ **Save activity history of unknown applications on the first run**:

Automatically enable the <u>activity history saving option</u> (61) when an unknown application runs for the first time.

❑ **Disable script engine**:

Block the execution of untrustworthy scripts by the interpreters (except for the scripts that are signed by a valid digital signature or by a digital signature from the <u>white list of certificates</u> (63)).

❑ **Enable dll modules control**:

Monitor the Integrity of the dynamic-link libraries (DLL) that are used by the executable components.

❑ **Disable modification of portable executable files (except for installers)**:

Block modification of the PE files by untrustworthy processes (processes that do not have the installer flag). It allows reducing the risks of the system integrity violation.
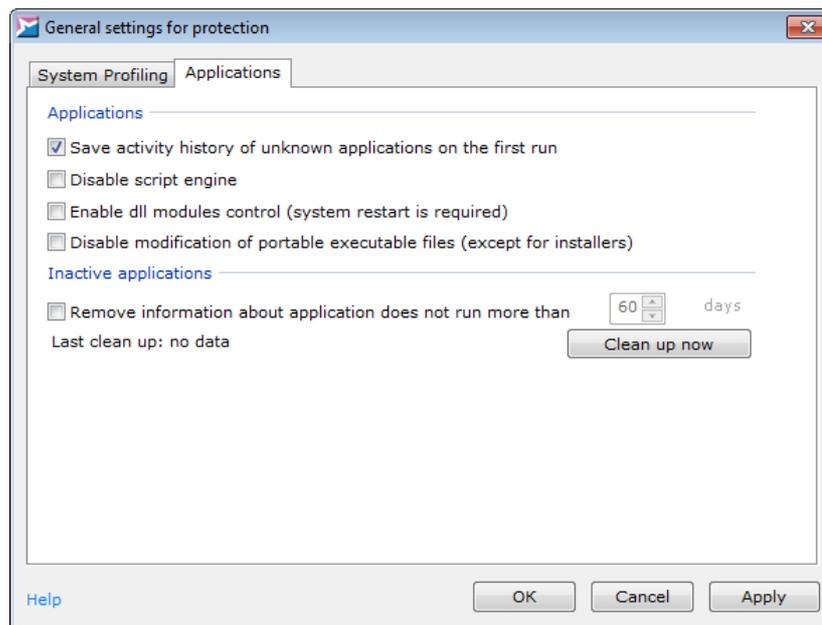
Figure 46. Activity control options

To delete entries about inactive applications from the SoftControl SysWatch database, tick off the **Remove information about application does not run more than** checkbox in the **Inactive applications** area and specify the required number of days. To delete data immediately, click **Clean up now**.

SoftControl SysWatch features global installation mode to support the execution of the multistage installers. When this mode is active, all processes run with the installer flag (education mode). To enable the mode, open the **Protection** section of the program settings and tick off **Global installation mode (a reboot is recommended)** (fig. General protection settings [49]). Besides, you can manage the global installation mode in silent mode, with the help of the changetpsmode extra utility [106].

4.6.2. Handling the process start incidents

Fig. below [51] shows the diagram of response to the incidents of unknown process start in the SoftControl SysWatch advanced mode.
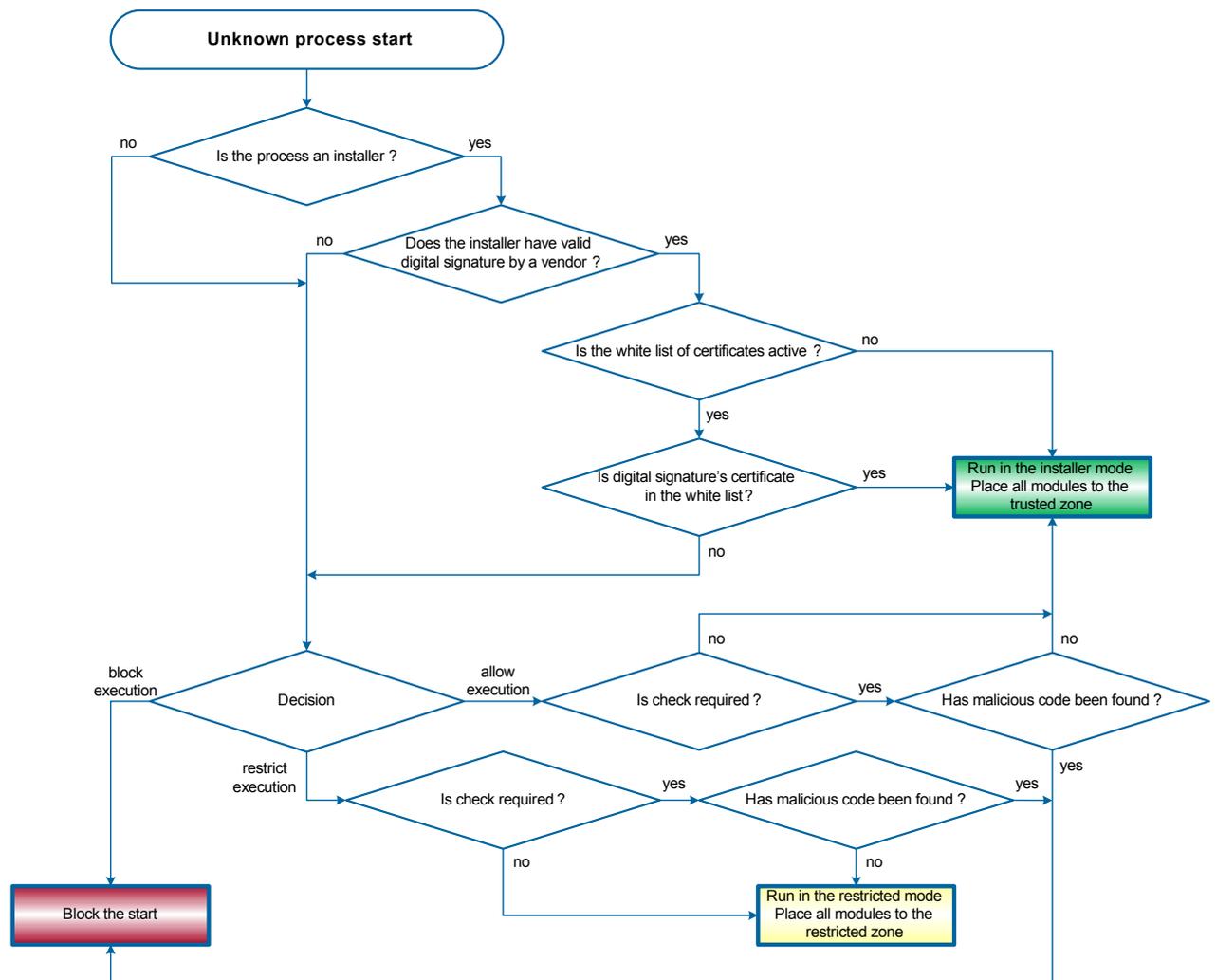
Figure 47. The scheme of the handling an unknown process start

The ginal *decision* (fig. above ^{51}) is made according to the incident processing mode:

- **Automatic**

SoftControl SysWatch makes a decision according to the incident processing parameters, without requests to the user. To select this mode and change its parameters, go the **Protection** section of the program settings, switch **Incident management** to **Enable automatic processing of the incidents** and click **Configure** (fig. General protection settings ^{49}). Select the required event type in the **Incident list** of the **Incidents management** window (fig. Setting up the incident processing ^{52}), and select an action that SoftControl SysWatch should perform when this event occurs. To confirm the selected settings, click **OK**. The full list of the incidents and possible actions is presented in table 8.
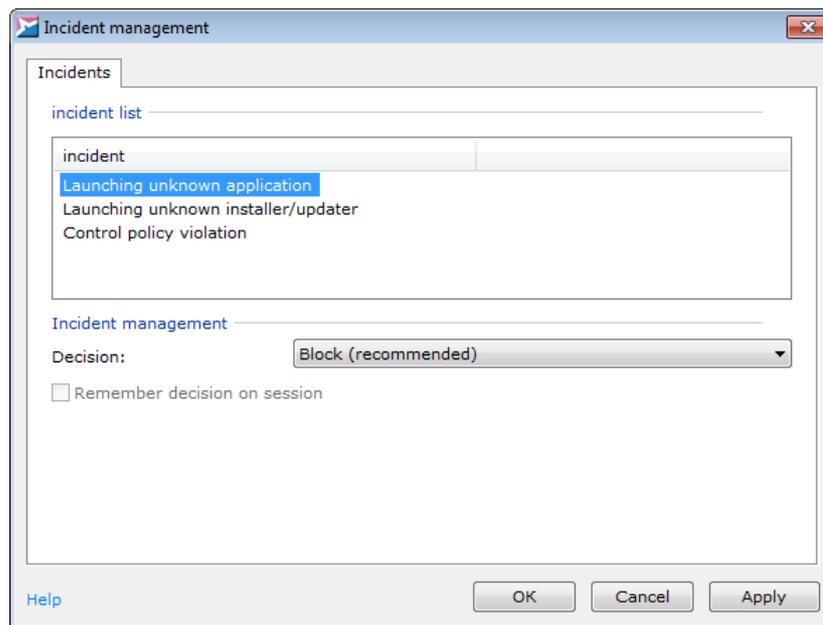
Figure 48. Setting up the incident processing

▪ **Manual**

SoftControl SysWatch makes a decision according to what the user selects in the dialog box. To select this mode, go to the **Protection** section of the program settings, switch **Incident management** to **Enable processing of incidents by user** and click **OK** (fig. General protection settings [49]).

▽ **Unknown application launching**

Fig. Warning for an unknown application [53] shows the warning that is displayed when an unknown application runs.

Figure 49. Warning for an unknown application

The **Alert - SoftControl SysWatch** window consists of two parts:

- Application description area. The area contains information about the unknown application: the name, the vendor, antivirus scan[87] result (you can check the application before you make the decision by clicking the **Scan** link and choosing **Scan...** in the context menu).

- Action selection area. The area contains possible actions when an unknown application runs:

  → **Execute**

    o **execute in a limited mode** – execute the application in the isolated environment ('sandbox') under the 'V.I.P.O.' user account with restricted rights;

    o **execute in install mode** – execute the application and add it to the system profile.

> ℹ We recommend that you select this action only if you are sure that it will not harm the system, or if the application is produced by a trusted vendor.

  → **Block** – block the execution of the application.

> ℹ We recommend that you select this action if the origin of the application is unknown, or if you have not authorized the application to run.

If you do not select an action in 5 minutes, SoftControl SysWatch blocks the application and closes the window with the warning.

▽ Unknown installer launching

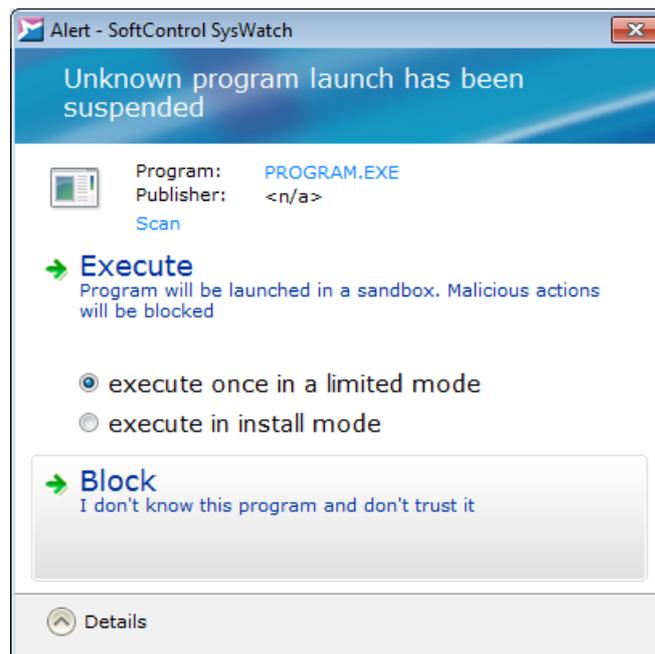Fig. <u>Warning for an unknown installer</u>[55] shows the warning that is displayed when an unknown installer runs.

The **Alert - SoftControl SysWatch** window consists of two parts:

- Application description area. The area contains information about the unknown installer: the name, the vendor, <u>antivirus scan</u>[87] result (you can check the installer before you make the decision by clicking the **Scan** link and choosing **Scan...** in the context menu).

- Action selection area. The area contains possible actions when an unknown installer runs:

  → **Execute** – execute the installer and add it and all the installed modules to the system profile;

ℹ️ We recommend that you select this action only if you are sure that it will not harm the system, or if the installer is produced by a trusted vendor.

  ❑ **run in a limited mode** – execute the installer in the isolated environment ("sandbox") under the 'V.I.P.O.' user account with restricted rights; do not add the installed modules to the system profile.

  → **Block** – block the execution of the installer.

ℹ️ We recommend that you select this action if the origin of the installer is unknown, or if you have not authorized the installer to run.

Figure 50. Warning window for unknown installer

If you do not select an action in 5 minutes, SoftControl SysWatch blocks the installer and closes the window with the warning.

4.6.3. Application execution zones

To view and modify the distribution of the applications among the execution zones, select **Processes and applications** in the SoftControl SysWatch context menu[31]. The **Processes and applications** tab of the **Control policy** window displays all applications (processes) registered by SoftControl SysWatch since it was installed (fig. Processes and applications[56]).
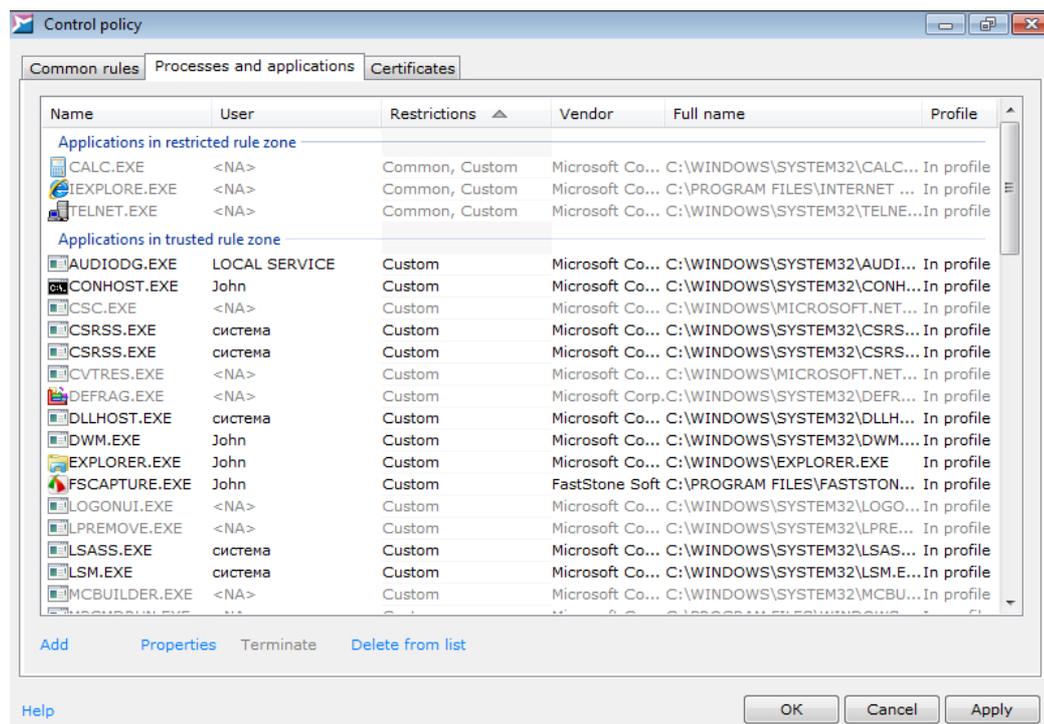
Figure 51. Processes and applications

Each application (process) is placed to one of the execution zones and has the following parameters.

- **Name** is the name of the executable file of the application.

- **User** is the user account that the application runs under.

- **Restrictions** are the set of restrictions and permissions that apply when the application runs:

  – **Custom** means the restrictions apply for a certain application.

  – **Common** means the restrictions apply for all applications in the execution zone.

  – **All blocked** means the application is blocked.

- **Vendor** is the application producer.

- **Full name** is the path to the executable file of the application.

- **Copyright** is the information about the application's copyright holder.

- **Description** is the brief description of the main feature.

- **File version** is the full version of the application's executable file.

- **Version** is the application (product) version.

- **Internal name** is the internal name from the application producer.

- **Original name** is the application name.

- **Product** is the software product that includes the application.

- **PID** is the process identifier in the system.

- **Status** is the application state:

  - **Running** means the active process; the application is currently running (the name is indicated in black);

  - inactive process; the application isn't currently running (the name is indicated in gray).

- **Delete application file on reboot** is the marker that indicates whether the application's executable file should be deleted after system reboot:

  - **No** means the application file is not deleted after reboot;

  - **Yes** means the application file is deleted after reboot.

- **Profile** is the marker that indicates whether the checksum of the application is in the system profile:

  - **In profile**;

  - **Not in profile**.

Possible actions in the applications list are as follows.

▽ **Adding/removing application from the list**

If there is no required application in the list, you can add it manually by clicking **Add** and specifying the path to the application. To perform the inverse operation, select the application and click the **Delete from list** link (or press **Delete** hot key). If this application isn't in the system profile, you should add it to the the profile[58] to run it with the required rights.

▽ **Adding/removing application from the system profile**

If you need to move an application to the system profile or delete it without updating the whole profile[48], right-click the required application to invoke the context menu and select one of the options:

  - **Add to profile**;

  - **Remove from profile**.

▽ **Changing application execution zone**

To move an application between the execution zones, right-click the required application to invoke the context menu and select one of the options (depending on the current execution zone):

- **Block application**;
- **Delete application from Trusted**;
- **Allow application**;
- **Trust to application**.

▽ **Terminating process**

If the application is running, you can interrupt the process by selecting the required application from the list and clicking **Terminate**. To **Delete application file on reboot**, invoke the context menu and select the corresponding command.

4.6.4. Properties of certain applications

SoftControl SysWatch allows you to specify the activity control rules for all applications, as well as to work with the options for certain applications. This includes specifying custom control policy rules. To do so, select the **Application properties** item in the process context menu on the [Processes and applications](56) tab.

▽ **Viewing detailed information on the application**

To view detailed information about the application, go to the **General** tab of the **Application properties** window (fig. [General information about the application](59)).
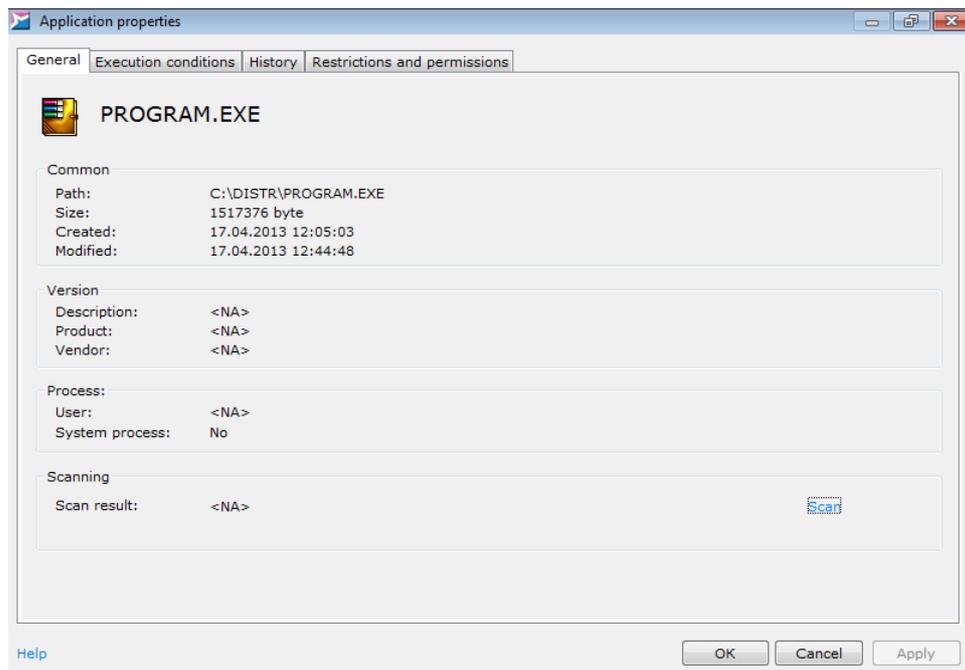
Figure 52. General information about the application

To check the application, click **Scan** and select **Scan...** in the context menu.

▽ **Specifying execution conditions**

To view and modify the current execution conditions of the application, go to the **Execution conditions** tab of the **Application properties** window (fig. Application execution conditions [60]).
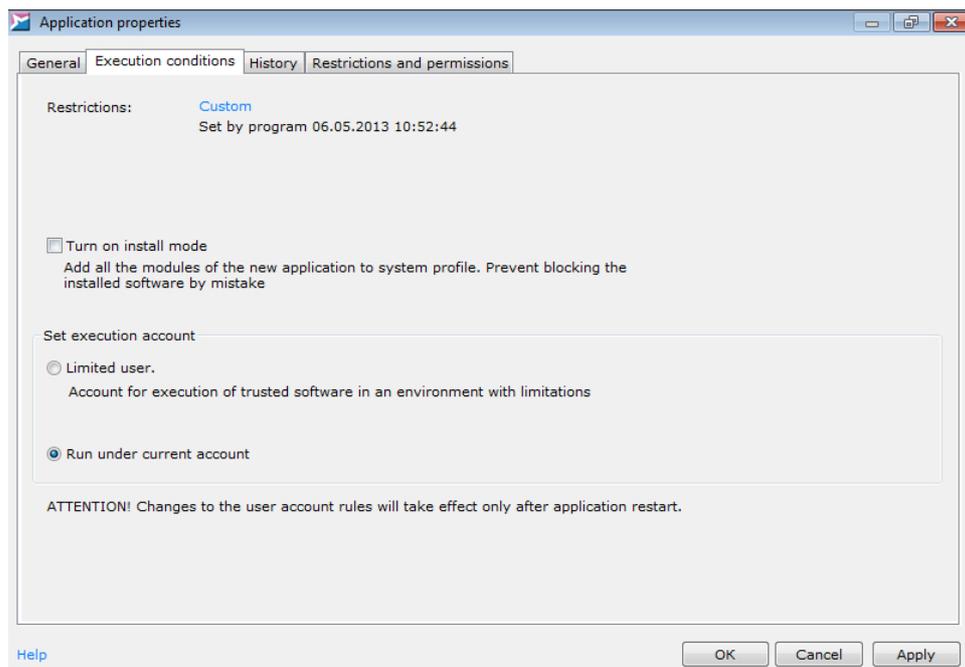

Figure 53. Application execution conditions

The tab displays the **Restriction** categories the application. To change them, click the link and select one of the commands (depending on the current execution zone):

- **Block application**;
- **Delete application from Trusted**;
- **Allow application**;
- **Trust to application**.

When the **Turn on install mode** option is selected, all program modules are added to the system profile. To activate the option, tick off the corresponding checkbox.

The **Set execution account** switch is responsible for selecting the user account which the application runs under:

- **Run under current account**: execute the process under current user account;
- **Limited user**: execute the process from the trusted zone under current user account but with reduced privileges;
- **Isolated user: V.I.P.O.**: execute the process from the restricted zone under the 'V.I.P.O.' user account with restricted rights.

▽ **Saving application activity history**

To view the activity of the application when accessing the file resources and the system registry, go to the **History** tab of the **Application properties** window (fig. Application activity history[61]).

Tick off **Save application history since...** to enable history saving. To update information on the tab, click **Refresh**.

Tick off **Create backup copies of objects for further recovery** to save copies of the objects that are modified by the application. To recover an object to the previous state, select the modification event in the list and click **Restore**.

Figure 54. Application activity history

▽ **Specifying custom rules**

To specify custom rules, go to the **Restrictions and permissions** tab of the **Application properties** window (fig. Custom restrictions of the application [62]) and select one of the control scopes:

- **File system**;
- **System Registry**;
- **Network**;
- **Process privileges**.

Actions on this tab are similar to specifying the common settings for:

- permissions to access file system [66];
- permissions to access system registry [70];
- network activity rules [78];
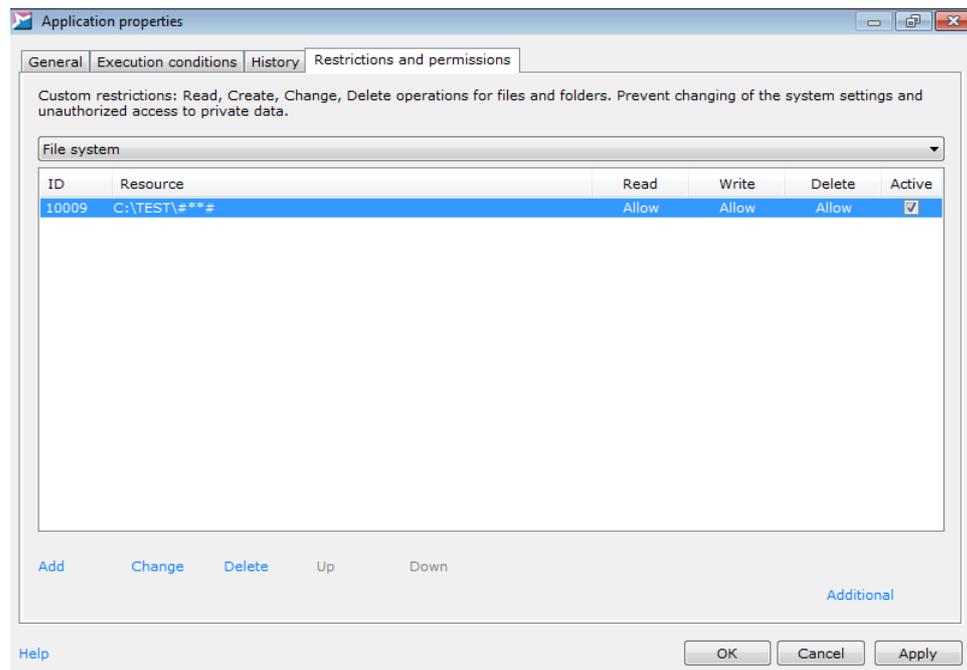- process privileges [83].

Figure 55. Custom restrictions of the application

Unlike common control rules, here you do not need to select the scope: a custom rule affects only the selected application. The priority of custom restrictions is higher than that of common restrictions: the restrictions of an application are checked at first, and then the general restrictions are checked. To view common rules that affect the execution zone which the application belongs to, select the **File system (common)**, **System Registry (common)** or **Network (common)** control scopes.

A standard set of custom restrictions can be included to the SoftControl SysWatch package; this set is created by the company experts as a result of the analysis of the application's actions.

To apply changes, click **OK** or **Apply**.

4.6.5. White list of certificates

When a process runs, SoftControl SysWatch heuristically determines whether it is an installer or a script. By default, if the process has a valid digital signature, it gets the installer flag. Besides, it is possible to check whether a digital signature certificate is in the white list. The white list of certificates is determined by user. Thus, certificate control in SoftControl SysWatch is used to restrict the start of the installers and the execution of scripts in the following cases.

- there is no digital signature;
- there is a digital signature with an expired certificate, and there is no signed timestamp;
- there is a digital signature of an unknown vendor or of a vendor whose digital signature has been stolen by a violator.

In each of these cases, there is a risk to infect the system being protected with a malware and violate the system's integrity.

To enable control over the white list of certificates, do the following actions.

1) Select **Processes and applications** in the SoftControl SysWatch context menu[31] and go to the **Certificates** tab of the **Control policy** window (fig. The white list of certificates [64]).
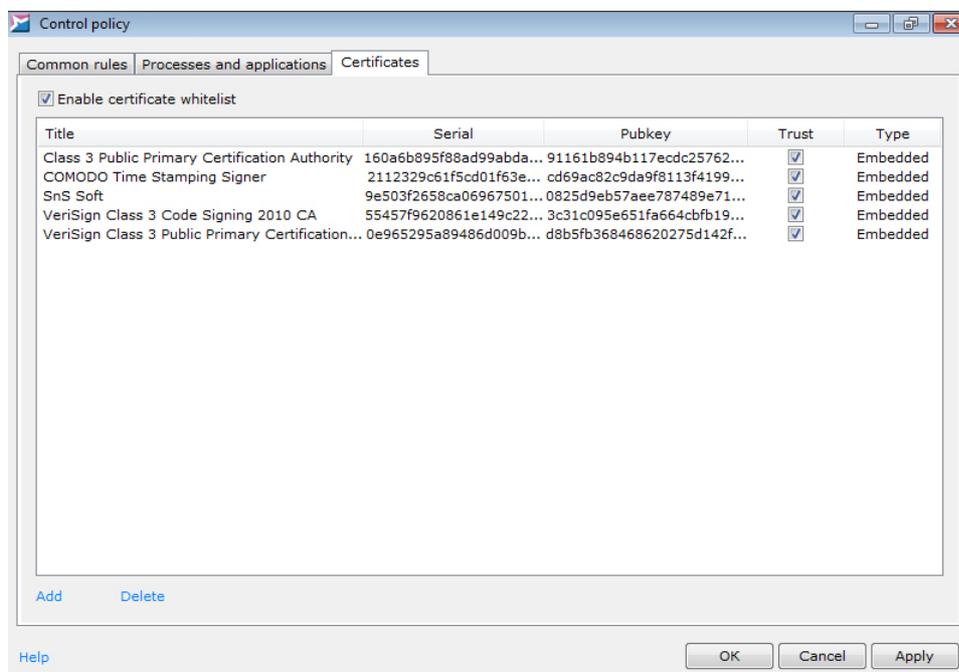

Figure 56. The white list of certificates

2) Tick off the **Enable certificate whitelist** checkbox to activate the white list.

3) The **Certificates** tab displays the list of certificates and their parameters. By default, SoftControl SysWatch contains the basic list of the certificates by trusted vendors. To add a new certificate to the list, click **Add** and specify an application, an installer or a script with a digital signature which certificate is to be included in the list and then click **Open**. Tick off boxes for the required certificates in the **Add** column of the displayed window and click **OK** (fig. Selecting the certificates to add [64]).
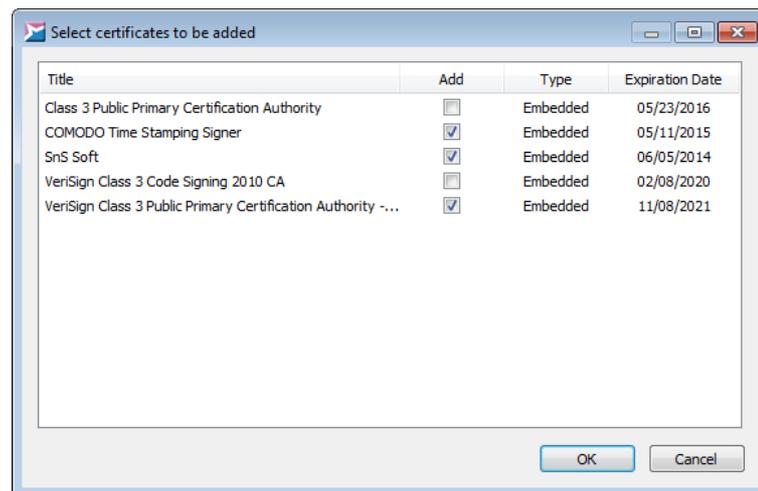
Figure 57. Selecting the certificates to add

4) Tick off the **Trust** column for the added certificates (fig. The white list of certificates [64]).

5) If you want to remove a certificate from the list of trusted certificates without deleting it, deselect checkbox in the **Trust** column. To delete a certificate from the list completely, select it and click the **Delete** link (fig. The white list of certificates [64]).

6) To apply changes, click **OK** or **Apply** (fig. The white list of certificates [64]).

4.7. Control policy

Current protection status and the list of the control scopes are displayed in the **Status** tab of the program's control panel [32]. Control policy of the applications' access to the system resources is active when the **File system**, **System Registry** and/or **Network** scopes are ticked off.

Below is the detailed information about the control policy settings for:

- permissions to access file system [66];
- permissions to access system registry [70];
- permissions to access devices and ports [75];
- network activity [78];
- process privileges [83];
- interprocess interaction [85].

4.7.1. Specifying permissions to access file system

The **File system** scope encompasses the access rules that deal with the file system objects:

- Reading a file or a folder;
- Writing to a file or to a folder (creating/changing a file or a folder);
- Deleting a file or a folder.

To view and modify control policy of the file system, select **Control policy** from the SoftControl SysWatch context menu[31], switch to the **Common rules** tab of the **Control policy** window and select **File system** from the drop-down list (fig. Control policy for the file system[66]).
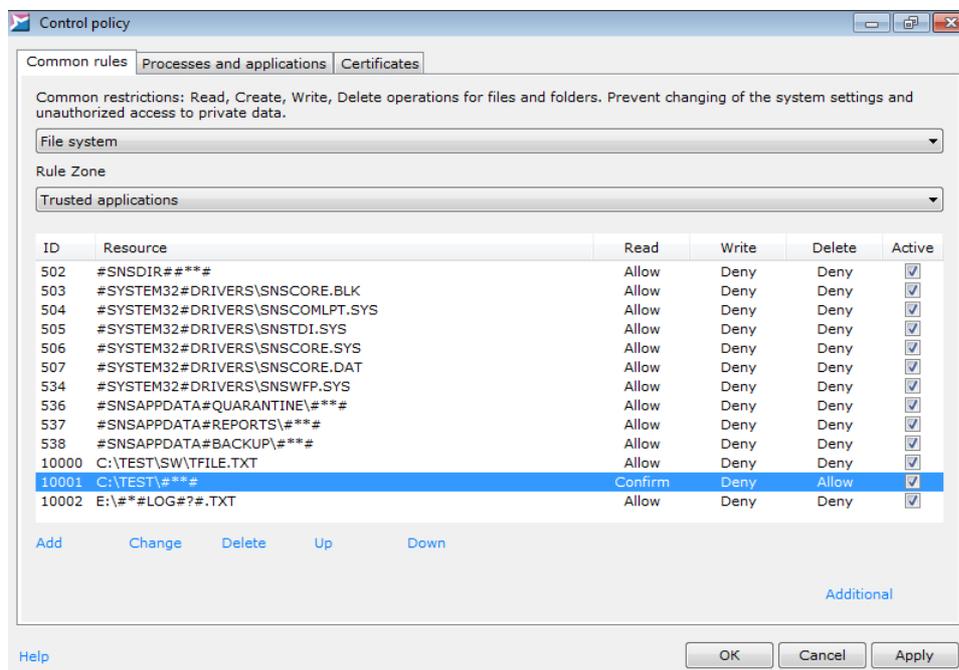

Figure 58. Control policy for the file system

Rules are divided into lists for applications from the following execution zones:

- **Trusted applications**;
- **Restricted applications**.

To switch between the lists, select the corresponding category from the **Rule Zone** drop-down list.

Each rule is an entry in the flat list and has a unique **ID**. The objects that the rule applies to are specified in the **Resource** column, while their permissions are specified in the **Read**, **Write**, and **Delete** columns. You can enable or disable the rule with the help of the **Active** checkbox.

If some rules have overlapping scopes, then the lowest rule in the list has the highest priority of execution. The rule position in the list can be changed by the **Up** and **Down** links.

<u>Example</u>: the rule with the **ID** 10001 which is shown in fig. <u>Control policy for the file system</u> [66], overrides the action of the rule with the **ID** 10000 because it is lower in the list.

▽ **Rule syntax**

A string in the **Resource** column is a path to the object or objects that the rule applies to. In this string, you can use masks to create a rule for the group of file system objects. For example, you can specify a rule for a folder and all objects inside it, or a rule for certain file types (extensions).

Below is the mask syntax:

#*# - the mask replaces any number of characters except for the '\' symbol (if the mask is placed at the end of the string, the rule affects only the root directory files);

##** - the mask replaces any number of characters (if the mask is placed at the end of the string, the rule affects the root directory files, subdirectories and files in the subdirectories);

#?# - the mask replaces exactly one character (any character).

<u>Example</u>: the rule with the **ID** 10002 (*E:\#*#log#?#.txt*) is shown in fig. <u>Control policy for the file system</u> [66]; the mask affects the following objects: the text files in the root directory of the *E* local drive that have the *log* sequence of letters in their names, any number of random characters before the indicated sequence, and one random character after it.

▽ **Creating a rule**

To create a rule, click **Add**.

Click **...** in the **Filesystem resource** window to select an object from the explorer or manually type a path to it in the **File or directory** field (fig. <u>Creating a rule for the file system object</u> [67]).
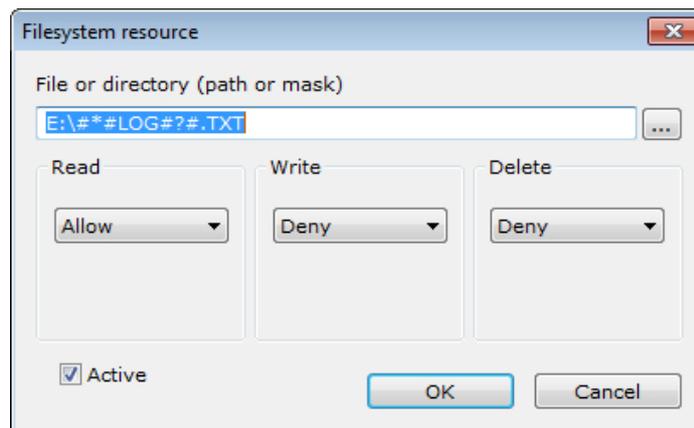
Figure 59. Creating a rule for the file system object

> ℹ️ When you add a folder via the explorer, the **#*#** mask [67] is added to folder automatically, i.e. the rule is specified for the folder and the files inside it.

Select the corresponding permissions to access an object, in the **Read**, **Write**, and **Delete** areas:

- **Allow** – allow the application to perform an operation with the object;
- **Deny** – do not allow the application to perform an operation with the object;
- **Confirm** – display the request when the operation with the object matches the rule condition.

To add the created rule to the list and make it active, tick off the **Active** checkbox and click **OK**.

▽ **Changing a rule**

To edit a rule, click **Change** and set up the rule parameters, as with the creation [67] of the rule.

▽ **Moving a rule between zones**

If you need to move a rule to the list for the applications from another execution zone, invoke the rule context menu and select one of the options:

- **All** – create a rule for both execution zones, if a rule is only in one list.
- **Restricted** – move a rule to the list for the restricted applications.
- **Trusted** – move a rule to the list for the trusted applications.

▽ **Additional rule parameters and exceptions**

By clicking **Additional** (either in the context menu or in the lower part of the window) you can specify the following additional rule parameters.

- **Users** – on this tab, you can specify user accounts the rule applies to (fig. Selecting user accounts [69]). By default, the rules apply to all the users.
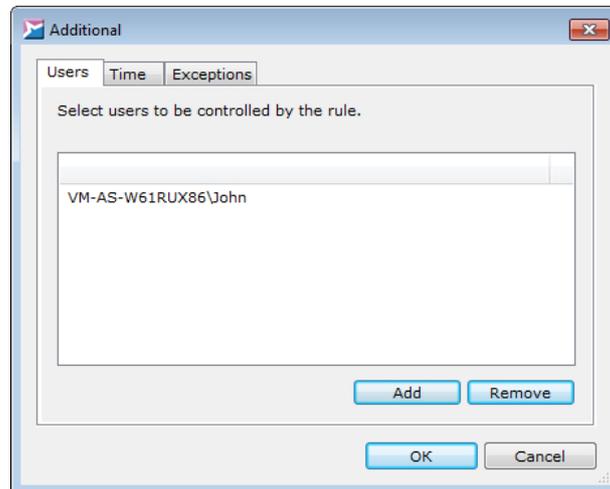

Figure 60. Selecting user accounts

- **Time** – on this, tab you can specify time intervals when the rule is valid (fig. Specifying time intervals [69]).
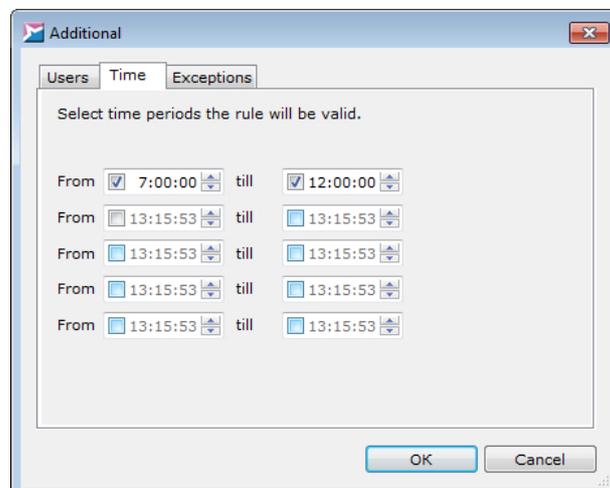

Figure 61. Specifying time intervals

> ℹ️ If you need to specify an interval that spans two days, you should divide it into two intervals (the first should end at 23:59:59, and the second should start at 0:00:00).

- **Exceptions** – on this tab, you can select applications the rule does not apply to (fig. Selecting applications - the exceptions [69]).
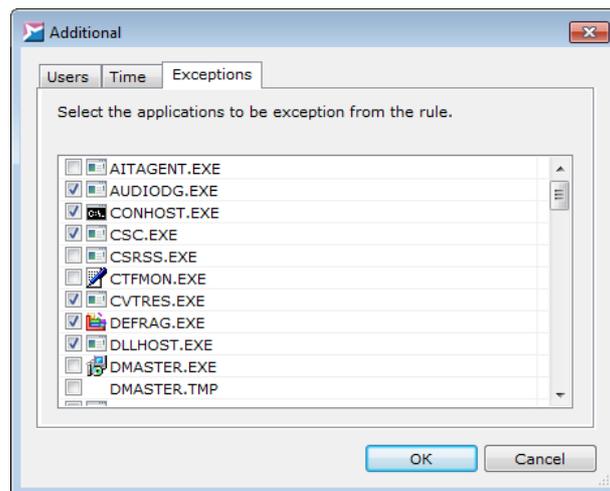
Figure 62. Selecting applications - the exceptions

> For the applications selected as exceptions, custom rule is created. The rule is displayed as read-only on the [Permissions and restrictions](62) tab in the application properties window.

Click **OK** to save the specified additional parameters.

▽ **Deleting a rule**

To delete a rule, press **Delete** and confirm the removal in the dialog box.

> SoftControl SysWatch contains the preset rules that apply to the system folders and the objects in the folders of the product components. Changing or deleting the preset rules may cause violation of the system integrity protection.

To apply changes, click **OK** or **Apply**.

4.7.2. Specifying permissions to access system registry

The **System registry** scope allows to create rules that control the access to the Windows System Registry:

- Writing to a registry key or to a value (creating/changing a key or a value);
- Deleting a registry key or a value.

To view and modify control policy for the system registry, select **Control policy** from the SoftControl SysWatch [context menu](31), switch to the **Common rules** tab of the **Control policy**

window and select **System Registry** from the drop-down list (fig. Control policy for the system registry[71]).
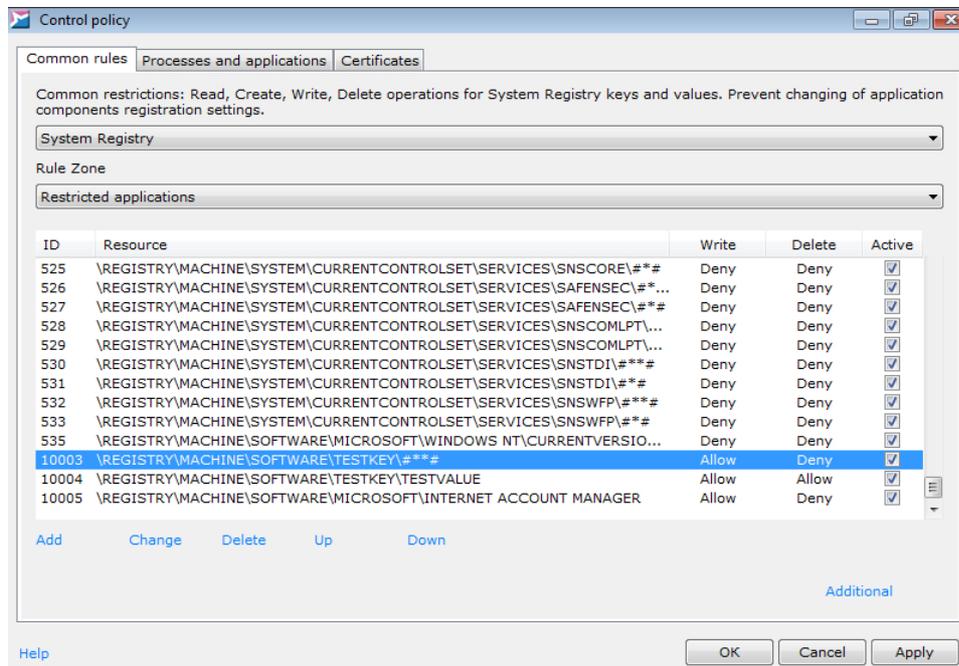

Figure 63. Control policy for the system registry

The rules are divided into lists for the applications from the following execution zones.

- **Trusted applications**;
- **Restricted applications**.

To switch between the lists, select the corresponding category from the **Rule Zone** drop-down list.

Each rule is an entry in the flat list and has a unique **ID**. The objects that the rule applies to are specified in the **Resource** column, their permissions are specified in the **Read**, **Write** and **Delete** columns. You can enable or disable the rule with the help of the **Active** checkbox.

If some rules have overlapping scopes, then the lowest rule in the list has the highest priority of execution. The rule position in the list can be changed by the **Up** and **Down** links.

Example: the rule with the **ID** 10004 which is shown in fig. Control policy for the system registry[71], overrides the action of the rule with the **ID** 10003 because it is lower in the list.

▽ **Rule syntax**

A string in the **Resource** column is a path to the object or objects that the rule applies to. In this string, you can use masks to create a rule for the group of system registry objects. For example, you can specify a rule for a registry key and all objects inside it.

Below is the masks syntax:

#*# - the mask replaces any number of characters except for the '\' symbol (if the mask is placed at the end of the string, the rule affects only key values);

#**# - the mask replaces any number of characters (if the mask is placed at the end of the string, the rule affects the key values, subkeys and subkey values);

#?# - the mask replaces exactly one character (any character).

Example: the rule with the **ID** 10003 (*\REGISTRY\MACHINE\SOFTWARE\TESTKEY \#**#*) is shown in fig. Control policy for the system registry [71]; the mask affects the following objects: the *TestKey* key, all its values, subkeys and subkey values.

▽ **Creating a rule**

To create a rule, click **Add**.

Select an object from the explorer in the **System registry resource** window or type its registry path in the field under the explorer (fig. Creating a rule for the system registry object [72]).
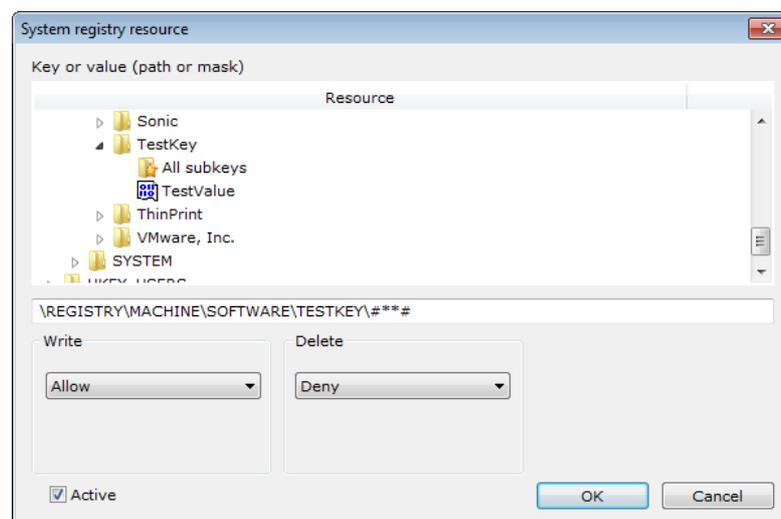
Figure 64. Creating a rule for the system registry object

Select the corresponding permissions to access an object, in the **Write**, and **Delete** areas:

- **Allow** – allow the application to perform an operation with the object;

- **Deny** – do not allow the application to perform an operation with the object;

- **Confirm** – display the request when the operation with the object matches the rule condition.

To add the created rule to the list and make it active, tick off the **Active** checkbox and click

OK.

▽ Changing a rule

To edit a rule, click **Change** and set up rule parameters, as with the creation[72] of the rule.

▽ Moving a rule between zones

If you need to move a rule to the list for the applications from another execution zone, invoke the rule context menu and select one of the options:

- **All** – create a rule for both execution zones, if a rule is located only in one list.
- **Restricted** – move a rule to the list for the restricted applications.
- **Trusted** – move a rule to the list for the trusted applications.

▽ Additional rule parameters and exceptions

By clicking **Additional** (either in the context menu or in the lower part of the window) you can specify the following additional rule parameters.

- **Users** – on this tab, you can specify user accounts the rule applies to (fig. Selecting user accounts[73]). By default, the rules apply to all the users.
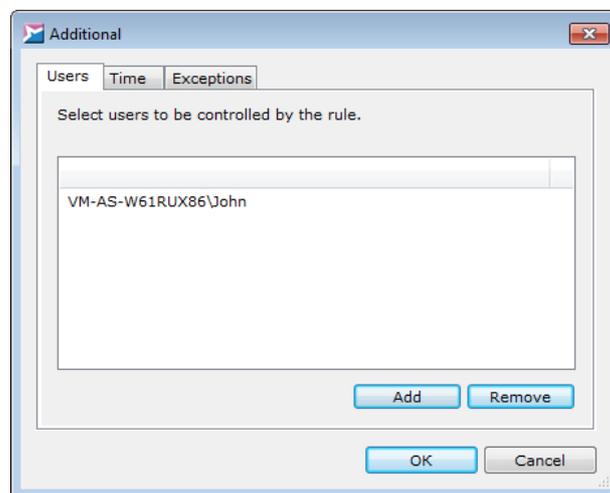

Figure 65. Selecting user accounts

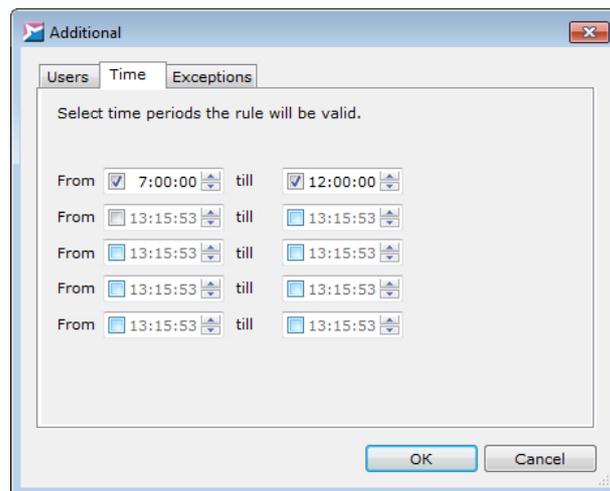- **Time** – on this, tab you can specify time intervals when the rule is valid (fig. Specifying time intervals[73]).

Figure 66. Specifying time intervals

ℹ️ If you need to specify an interval that spans two days, you should divide it into two intervals (the first should end at 23:59:59, and the second should start at 0:00:00).

• **Exceptions** – on this tab, you can select the applications the rule does not apply to (fig. Selecting applications - the exceptions [74]).
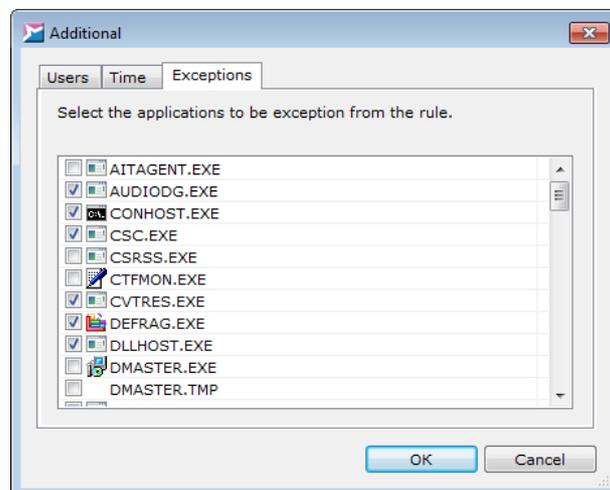

Figure 67. Selecting applications - the exceptions

ℹ️ For the applications selected as exceptions, custom rule is created. The rule is displayed as read-only on the Permissions and restrictions [62] tab in the application properties window.

Click **OK** to save the specified additional parameters.

▽ **Deleting a rule**

To delete a rule, press **Delete** and confirm the removal in the dialog box.

ℹ SoftControl SysWatch contains the preset rules that apply to the system registry keys and values that affects the operation of system and product components. Changing or deleting the preset rules may cause violation of the system integrity protection.

To apply changes, click **OK** or **Apply**.

4.7.3. Specifying permissions to access devices and ports

The **Devices** scope allows you to create rules that control the use of the following external devices and ports.

- USB devices;
- CD/DVD devices;
- LPT ports;
- COM ports.

To view and modify control policy for the devices, select **Control policy** from the SoftControl SysWatch context menu[31], switch to the **Common rules** tab of the **Control policy** window and select **Devices** from the drop-down list (fig. Control policy for the devices and ports[75]).
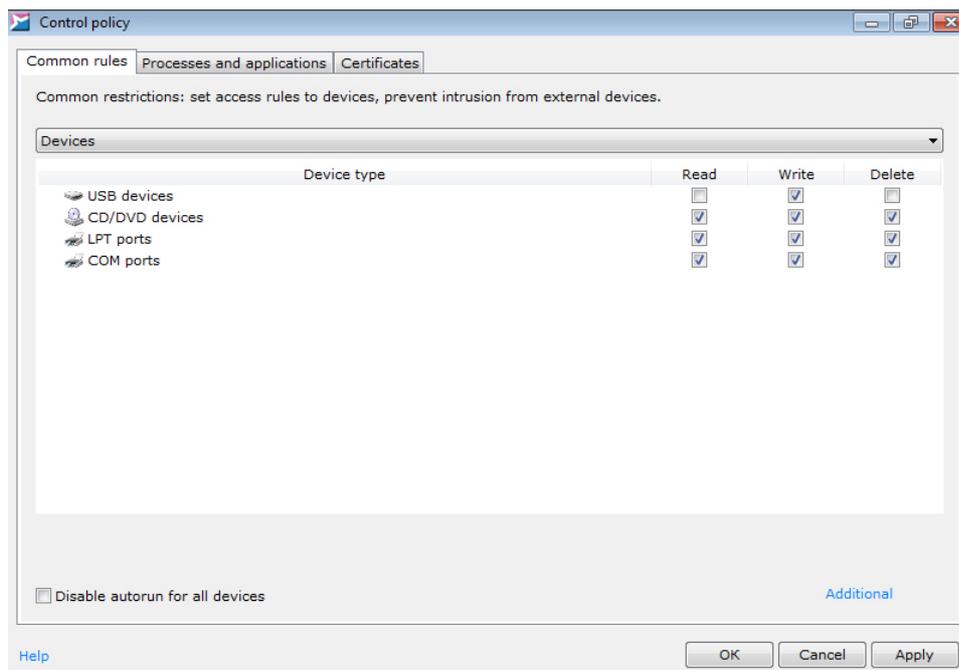

Figure 68. Control policy for the devices and ports

▽ **Specifying permissions to access USB devices**

To configure permissions to access USB devices, specify the permissions with the help of the corresponding checkboxes in the **Read**, **Write**, and **Delete** columns for the **USB devices** type.

By clicking **Additional** (either in the context menu or in the lower part of the window) you can specify the following additional options for the rule:

- **Users** – on this tab, you can specify user accounts the rule applies to (fig. Selecting user accounts ⁷⁶).

Figure 69. Selecting user accounts

- **Time** – on this tab, you can specify time intervals when the rule is valid (fig. Specifying time intervals ⁷⁶).

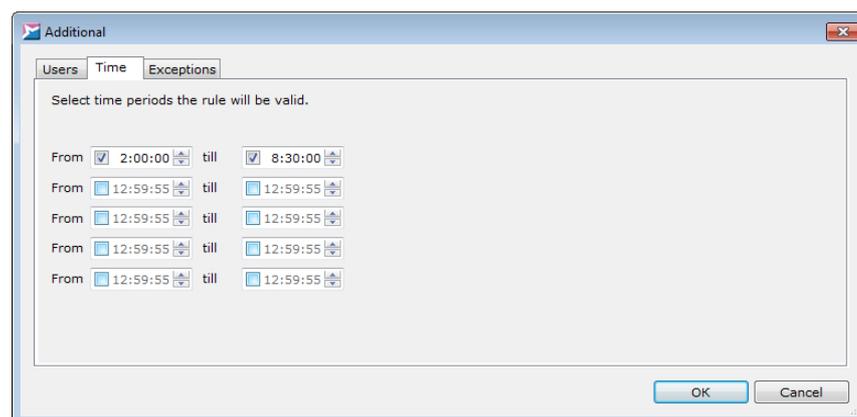**Figure 70. Specifying time intervals**

ℹ If you need to specify an interval that spans two days, you should divide it into two intervals (the first should end at 23:59:59, and the second should start at 0:00:00).

- **Exceptions** – on this tab, you can specify certain devices the rule does not apply to (fig. Selecting USB devices - the exceptions ⁷⁶).
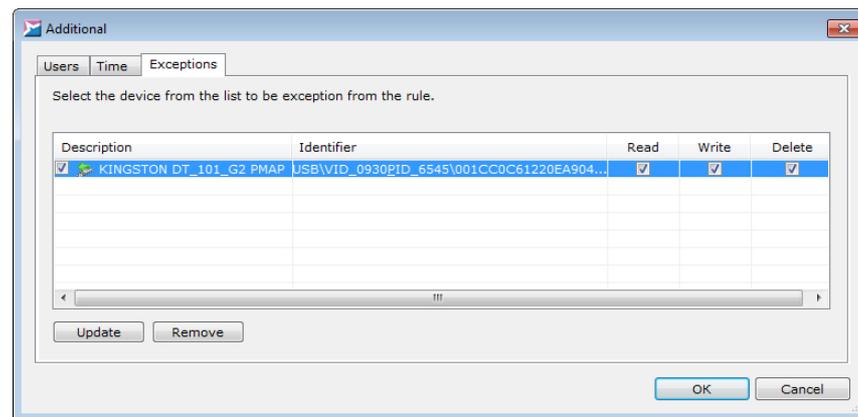
Figure 71. Selecting USB devices - the exceptions

In the USB devices 'white list', you can specify custom restrictions for each of the USB storage devices from the list, as with the common restrictions. To include a USB device into the white list, tick off the box with this device name in the **Description** tab. To refresh the list of USB devices, click **Update**. To delete a device from the list, select it and click **Remove**.

Click **OK** to save the specified additional parameters.

▽ **Blocking access to the CD/DVD devices**

To block access to the CD/DVD devices that are inserted into the optical drive of protected object, deselect any box in the **Write**, **Read** or **Delete** columns for the **CD/DVD devices** type (all the boxes are then deselected for this type).

▽ **Blocking autorun for all the devices**

To block autorun for USB and CD/DVD devices, tick off the **Disable autorun for all devices** checkbox.

▽ **Blocking access to the LPT ports**

To block access to the LPT ports of the protected object, deselect any box in the **Write**, **Read** or **Delete** columns for the **LPT ports** type (all the boxes are then deselected for this type).

ℹ You should additionally reboot the system to change the access rights.

▽ **Blocking access to the COM ports**

To block access to the COM ports of the protected object, deselect any box in the **Write**, **Read** or **Delete** columns for the **COM ports** type (all the boxes are then deselected for this type).

> ℹ You should additionally reboot the system to change the access rights.

To apply changes, click **OK** or **Apply**.

4.7.4. Specifying network activity rules

The **Network** scope allows you to create rules that monitor the network activity of the applications:

- Data receiving;
- Data sending.

To view and modify control policy for the network activity, select **Control policy** from the SoftControl SysWatch context menu[31], switch to the **Common rules** tab of the **Control policy** window and select **Network** from the drop-down list (fig. Control policy for the network activity[78]).
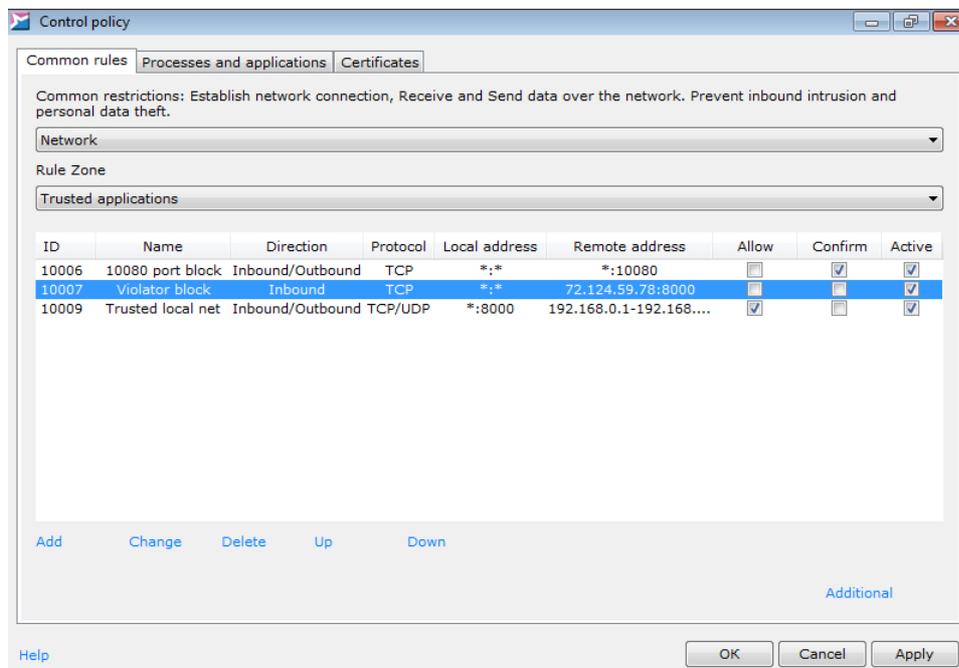

Figure 72. Control policy for the network activity

The rules are divided into lists for the applications from the following execution zones.

- **Trusted applications**;

- **Restricted applications**.

To switch between the lists, select the corresponding category from the **Rule Zone** drop-down list.

Each rule is an entry in the flat list and has a unique **ID**. Network connection parameters are specified in the following columns.

- **Name** is the rule name specified by the user.

- **Direction** is the direction of the network activity from the point of view of the connection initiator:

    – **Inbound** is the network connection initiated by the remote counterpart;

    – **Outbound** is the network connection initiated by the protected counterpart;

    – **Inbound/Outbound** is any direction.

- **Protocol** is the data transfer protocol:

    – **TCP**;

    – **UDP**;

    – **TCP/UDP** is either of these two.

- **Local address** is an IP address or a range of IP addresses of the local host that participate in the network connection. If the **Any address** option is selected during the [rule creation](79), then the '*' character is displayed before the ':' sign. If the **Any port** option is selected, then the '*' character is displayed after the ':' sign.

- **Remote address** is an IP address or a range of IP addresses of the remote host that participate in the network connection. If the **Any address** option is selected during the [rule creation](79), then the '*' character is displayed before the ':' sign. If the **Any port** option is selected, then the '*' character is displayed after the ':' sign.

Allowing or blocking the network connection with the specified parameters is managed by the checkbox in the **Allow** column. If it is assumed that the [user](80) processes the application network activity incidents, tick off the **Confirm** checkbox. You can enable or disable the rule with the help of the **Active** checkbox.

If several rules have overlapping scopes then the lowest rule in the list has the highest priority of execution. The position of the rule in the list can be changed by the **Up** and **Down** links.

▽ **Creating a rule**

To create a rule, click **Add**. Specify the required network connection parameters in the **Network resource** window (fig. Creating a network activity rule [80]).
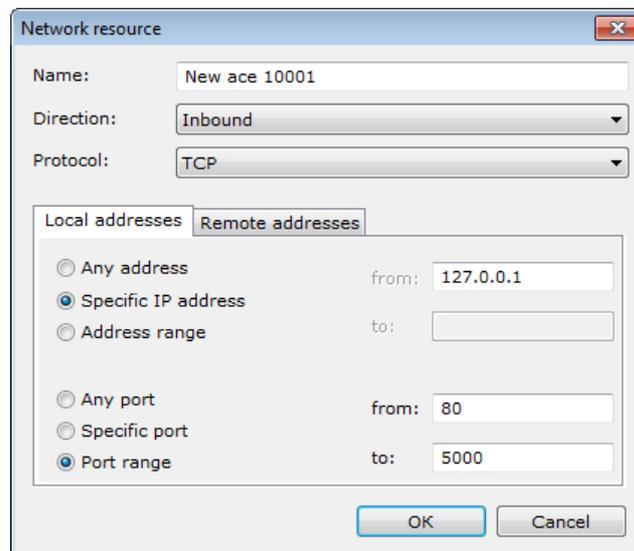
Click **OK** to add the created rule to the list.

Figure 73. Creating a network activity rule

▽ **Processing the network activity incidents manually**

Important: to enable this feature, activate manual incident processing. To do so, go the **Protection** section of the program settings, switch **Incident management** to the **Enable processing of incidents by user** state and click **OK**.

The warning that is displayed when the network connection parameters match the rule conditions is shown in fig. below [80].
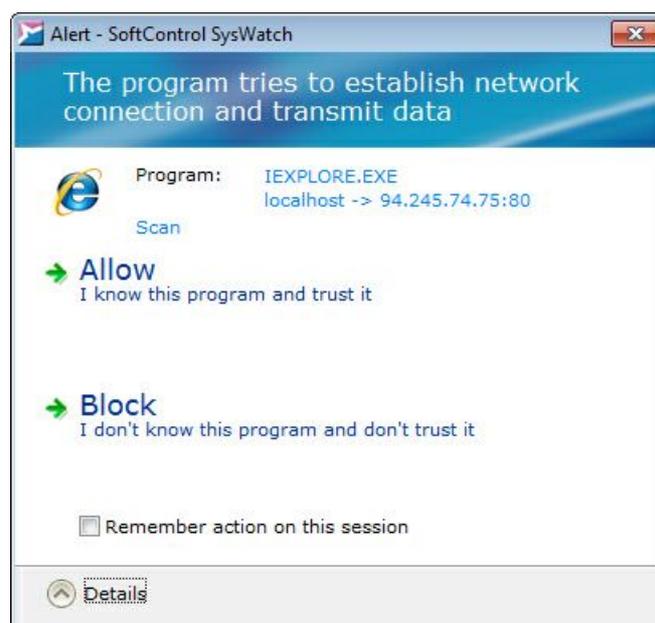
Figure 74. Warning for the network activity

The **Alert - SoftControl SysWatch** window consists of two parts:

- Network activity description area. The area displays information about the network connection being established: the name of the active application, terminal nodes to establish the connection, the direction of the connection, and antivirus scan [87] result (you can check the application before you make the decision, if the antivirus scanner and the corresponding program license [40] are available, by clicking the **Scan** link and selecting **Scan...** in the context menu).

- Action selection area. The area displays possible actions when an application tries to establish network connection:

  → **Allow** – allow the application to establish the connection;

  → **Block** – block network activity of the application;

  ❑ **Remember action on this section** – the decision applies to the rule until the end of current session.

If the action is not selected in 5 minutes, SoftControl SysWatch blocks the network activity and closes the window with the warning.

▽ **Changing the rule**

To edit a rule, click **Change** and set up the rule parameters, as with the creation [79] of the rule.

▽ **Moving a rule between zones**

If you need to move a rule to the list for the applications from another execution zone, invoke the rule context menu and select one of the options:

- **All** – create a rule for both execution zones, if the rule is located only in one list.
- **Restricted** – move the rule to the list for the restricted applications.
- **Trusted** – move the rule to the list for the trusted applications.

▽ **Additional rule parameters**

By clicking **Additional** (either in the context menu or in the lower part of the window) you can specify the following additional options for the rule.

- **Users** – on this tab, you can specify user accounts the rule applies to (fig. Selecting user accounts [81]). By default, the rules apply to all the users.
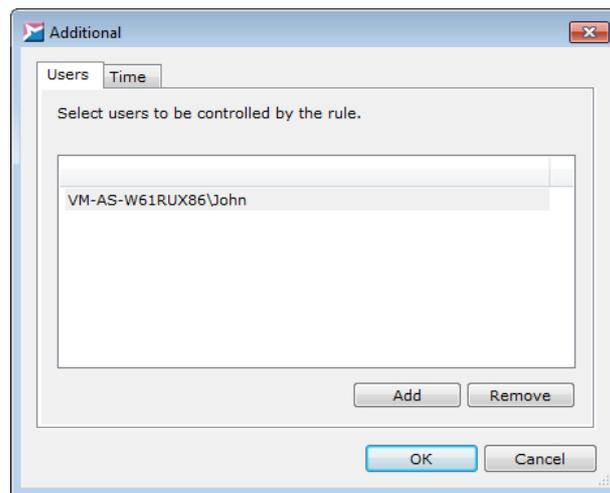
Figure 75. Selecting user accounts

- **Time** – on this tab, you can specify time intervals when the rule is valid (fig. Specifying time intervals [82]).
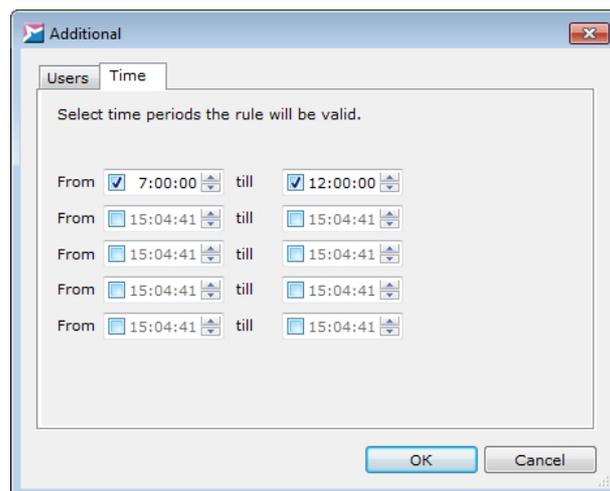

Figure 76. Specifying time intervals

> **i** If you need to specify an interval that spans two days, you should divide it into two intervals (the first should end at 23:59:59, and the second should start at 0:00:00).

Click **OK** to save the specified additional parameters.

▽ **Deleting a rule**

To delete a rule, press **Delete** and confirm the removal in the dialog box.

To apply changes, click **OK** or **Apply**.

4.7.5. Specifying process privileges

The **Process privileges** scope allows you to restrict the use of Windows privileges by the processes:

- Manage auditing and the security log;
- Back up files and directories;
- Restore files and directories;
- Change the system time;
- Shut down the system;
- Force shutdown from a remote computer;
- Take ownership of files or other objects;
- Debug programs;
- Modify firmware environment values;
- Profile the system performance;
- Profile a certain process;
- Increase scheduling priority;
- Load and unload device drivers;
- Create a pagefile;
- Adjust memory quotas for a process;
- Bypass cross-checking;
- Remove a computer from the docking station;
- Perform volume maintenance tasks;
- Impersonate a client after authentication;
- Create global objects.

Condition: the rules apply to all applications from the restricted zone.

To view and modify process privileges, select **Control policy** from the SoftControl SysWatch context menu [31], switch to the **Common rules** tab of the **Control policy** window and select **Process privileges** from the drop-down list (fig. Control policy for the process privileges [83]).
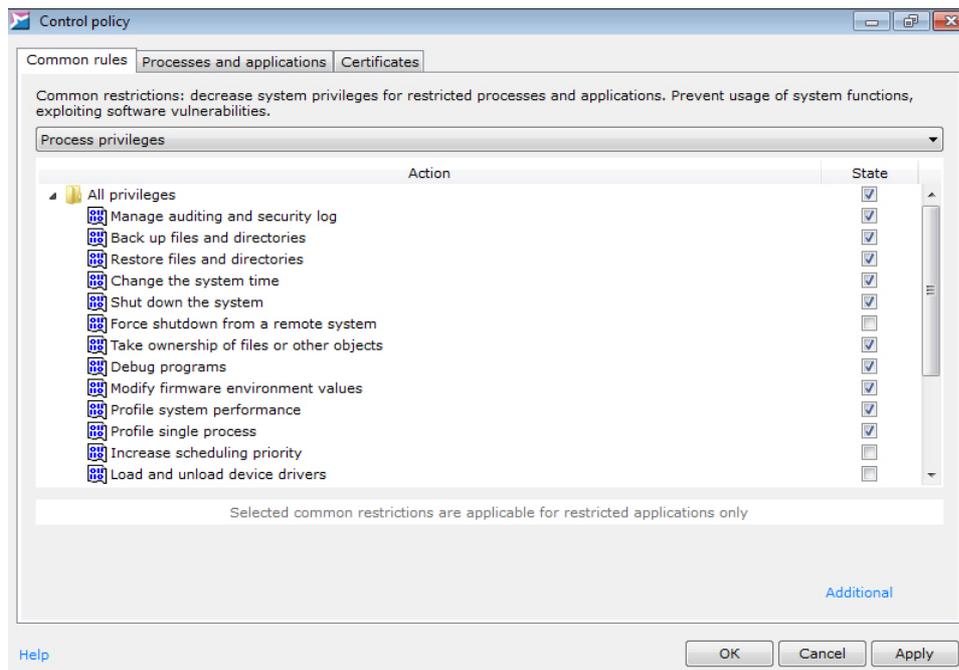
Figure 77. Control policy for the process privileges

▽ **Creating a rule**

By default, the applications (processes) have all the above-mentioned privileges; however, they can be limited by the OS. To restrict privileges manually, deselect checkboxes at the required privileges in the **State** column.

▽ **Additional rule parameters**

By clicking **Additional** (either in the context menu or in the lower part of the window) you can specify the following additional options for the rule:

- **Users** – on this tab, you can specify user accounts the rule applies to (fig. Selecting user accounts [84]). By default, rules apply to all the users.
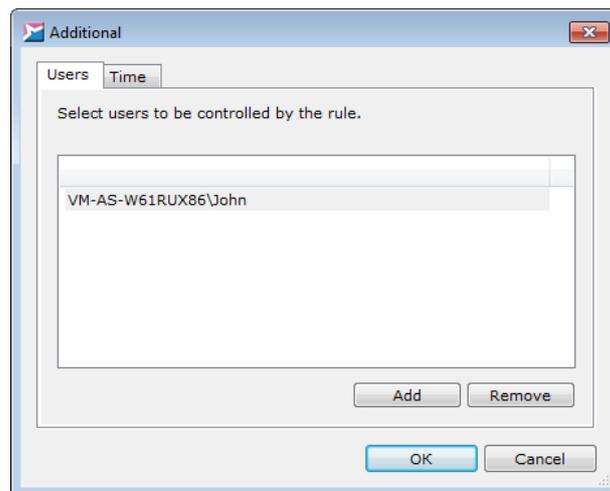
Figure 78. Selecting user accounts

- **Time** – on this tab, you can specify time intervals when the rule is valid (fig. Specifying time intervals [85]).
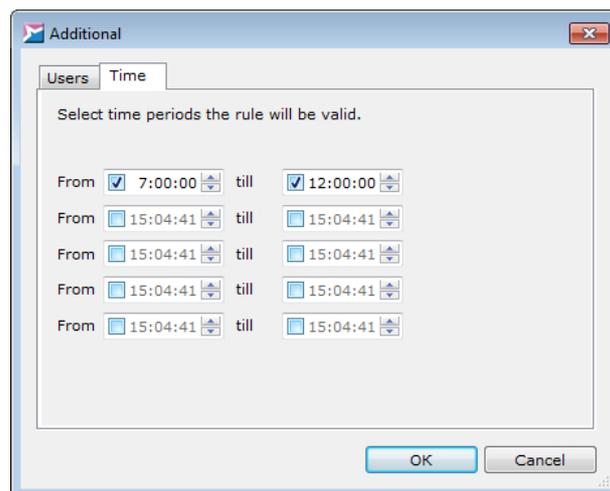

Figure 79. Specifying time intervals

> **i** If you need to specify an interval that spans two days, you should divide it into two intervals (the first should end at 23:59:59, and the second should start at 0:00:00).

Click **OK** to save the specified additional parameters.

To apply changes, click **OK** or **Apply**.

4.7.6. Specifying interprocess interaction

The **Interprocess interaction** scope allows you to set the following permissions for interprocess communication:

- Accessing the clipboard;

- Setting the hooks by an application;

- Accessingthe process and its threads from the outside.
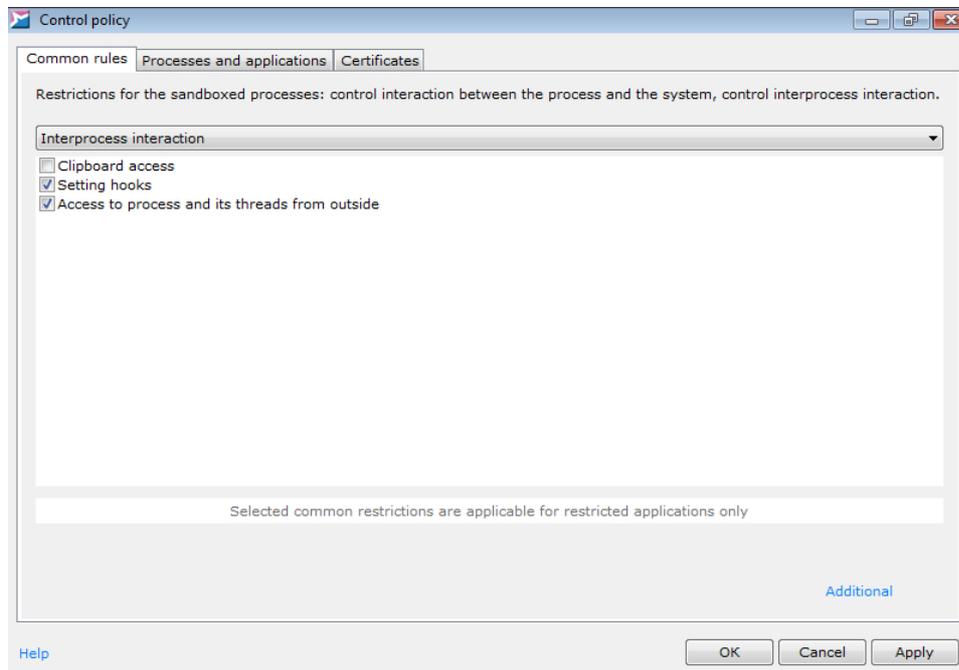
Figure 80. Control policy for the interprocess communication

Condition: the rules apply to the applications from the restricted zone that run under the 'V.I.P.O.' user account.

To view and modify the settings of the interprocess communication, select **Control policy** from the SoftControl SysWatch context menu[31], switch to the **Common rules** tab of the **Control policy** window and select **Interprocess interaction** from the drop-down list (fig. Control policy for the interprocess communication[86]).

▽ **Creating a rule**

By default, the applications from the restricted execution zone (that run under the 'V.I.P.O.' user account) do not have rights to perform the above-mentioned operations. To allow them to perform some interprocess communications, tick off the required checkboxes.

▽ **Additional rule parameters**

By clicking **Additional** (either in the context menu or in the lower part of the window) you can specify the following additional options for the rule:

- **Users** – on this tab, you can specify user accounts the rule applies to (fig. Selecting user accounts[86]). By default, rules apply to all the users.
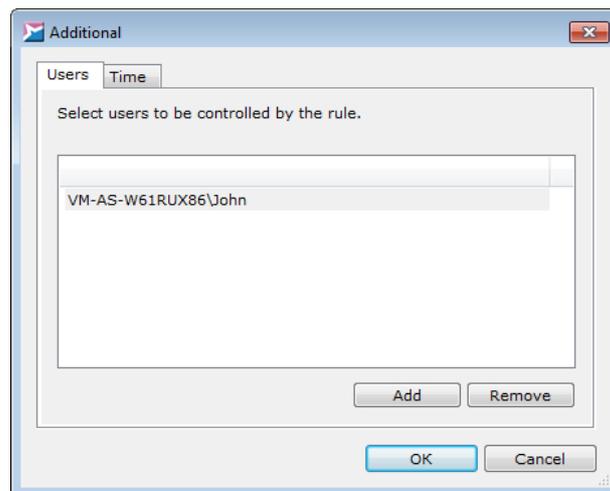
Figure 81. Selecting user accounts

- **Time** – on this tab you can specify time intervals when the rule is valid (fig. Specifying time intervals [87]).
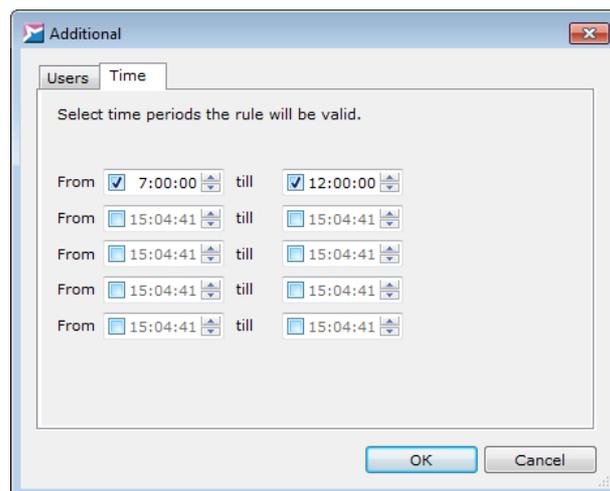

Figure 82. Specifying time intervals

> If you need to specify an interval that spans two days, you should divide it into two intervals (the first should end at 23:59:59, and the second should start at 0:00:00).

Click **OK** to save the specified additional parameters.

To apply changes, click **OK** or **Apply**.

4.8. Antivirus scanning

SoftControl SysWatch combines the features of both the prevention techniques and the reactive (signature) protection techniques. The basis of proactive protection is the application activity control [49]. The signature protection method of SoftControl SysWatch is implemented as an

antivirus scanner that uses a base of virus signatures (in order to use antivirus and spy databases, the appropriate license [40] is required).

The system can be infected by malware before SoftControl SysWatch installation. Full antivirus check of the system runs during automatic setup [43] by default. Otherwise,we recommend that you check the system by a third-party antivirus software, before you install SoftControl SysWatch.

During antivirus scanning, SoftControl SysWatch searches for malware with the help of:

- antivirus databases – SoftControl SysWatch searches for known viruses, trojan programs and other malicious objects;

- spyware databases – SoftControl SysWatch searches for known spy-programs;

i   To make the search for malicious code efficient, you need to update [111] the antivirus bases regularly. We recommend that you set up daily updates [111]. Daily updates are not required to prevent unauthorized activity of the applications.

In order to perform a scan, you need to:

1) Set up check parameters [89].
2) Specify the objects in the scan scope [92], such as the file system objects (logical drives and files), system memory, boot sectors, etc. By default, all the objects are included into the scope.
3) Start the check [92].
4) On the basis of the scan results [93], make a decision regarding the detected threats if they have not been neutralized.

We recommend that you perform scan:

- Immediately after SoftControl SysWatch installation, if there is no other antivirus software previously installed in the system.

- Each time when the application activity control [49] is disabled, and external storage devices (USB, CD, DVD etc.) are used or Internet connection is established.

4.8.1. Check options

Before you start antivirus check, you need to set up its parameters. To do so, open the **Scan** section of the program settings (fig. <u>Setting up check parameters</u> [89]).
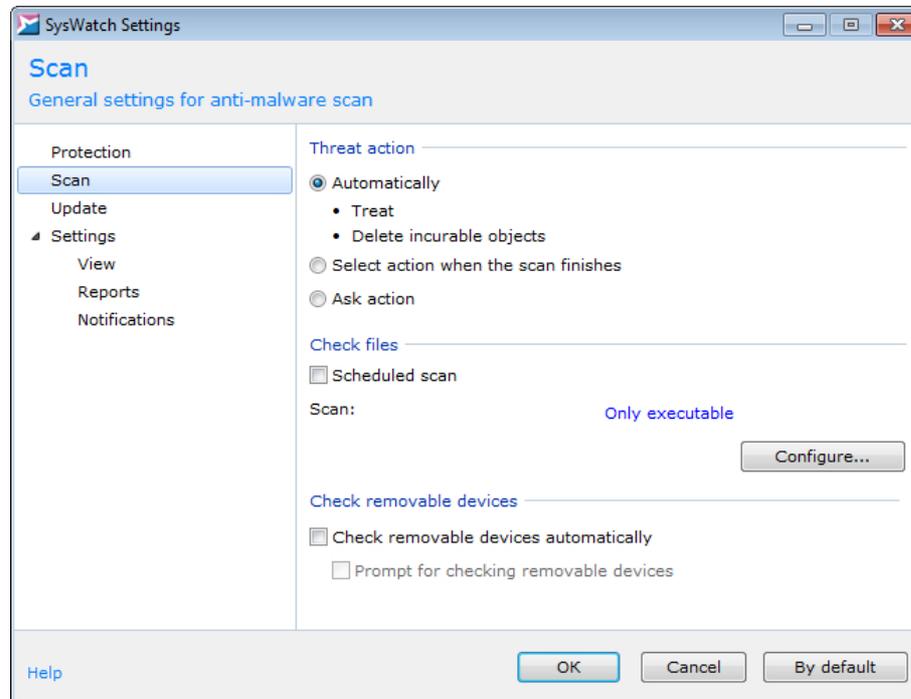
Figure 83. Setting up check parameters

▽ **Setting up response to a threat**

The **Threat action** area displays the following possible actions when threats are detected during the antivirus scanning:

o **Automatically**:

● **Treat**

Neutralize the infected object.

● **Delete incurable objects**

Delete the infected object if it cannot be treated.

o **Select action when the scan finishes**

After the check completes, the program prompts the user to select actions for all the detected threats.

o **Ask action**

The program prompts the user to select an action when a threat is detected.

▽ **Specifying file categories to scan and setting up the startup options**

The **Check files** area displays the categories of files analyzed by the antivirus scanner. Click **Configure** to modify the parameters.

There are the following options on the **Scan scope** tab of the **Advanced settings** window (fig. Check scope settings [90]):

- ○ **All files**

Scan all types of files except for the files that are not ticked off in the **Check compound files** area (the **Mail bases** and **Archives** checkboxes).

- ○ **Only executable**

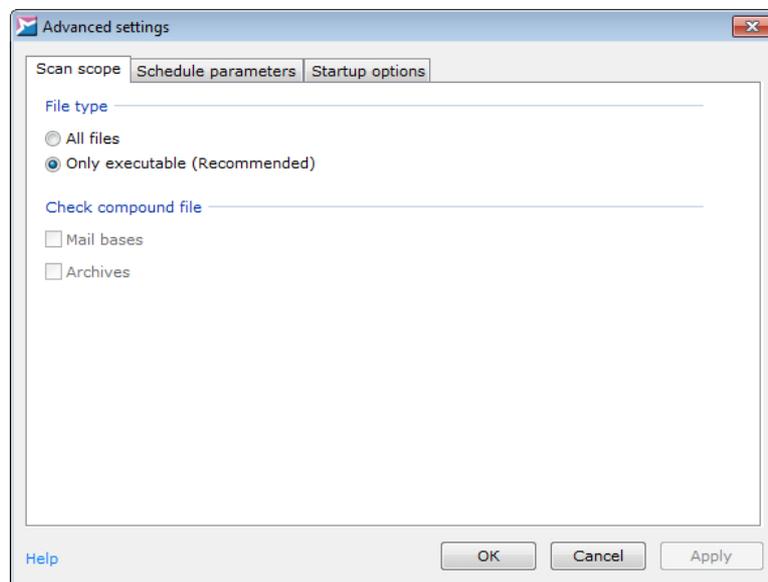Scan only PE files (**.exe, *.com*, etc.).

Figure 84. Check scope settings

Select user account to perform the scan, on the **Startup options** tab (fig. Additional check parameters [90]):

- ○ **Local System account**;
- ○ **This account:** specify credentials.

Tick off the **Preinitialize scanner** checkbox if it is required to initialize the antivirus engine every time the scan runs.
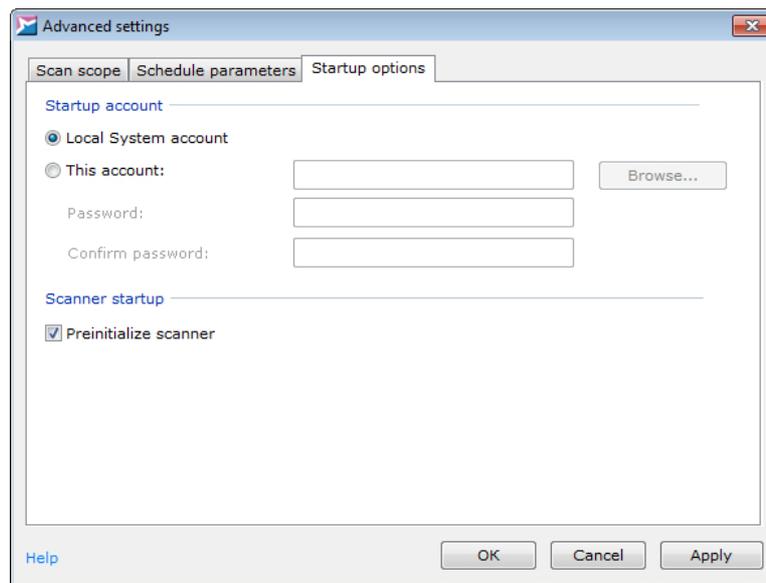
Figure 85. Additional check parameters

Click **OK** or **Apply** to apply settings.

▽ **Settings up scan schedule**

<u>Condition</u>: Only when SoftControl SysWatch is <u>controlled from the server remotely</u>[38].

To setting up the scan schedule parameters, click **Configure** in the **Check files** area.
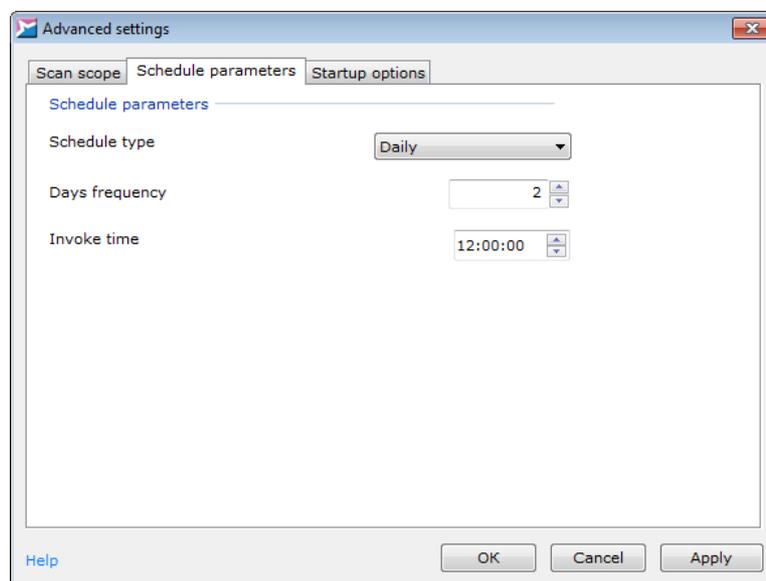

Figure 86. Scan schedule parameters

Switch to the **Schedule parameters** tab of the **Advanced settings** window and specify the frequency of the scan task in the **Days frequency** counter and time of the task start in *hh:mm:ss* format, in the **Invoke time** field (fig. <u>Scan schedule parameters</u>[91]).

▽ **Setting up automatic scan of removable storage devices**

Tick off the **Check removable devices automatically** checkbox in the **Check removable devices** area, if you need to start the antivirus scanning of the USB devices automatically when they connect. Tick off **Prompt for checking removable devices** to ask the user if the scan is required.

To apply changes, click **OK**.

4.8.2. Run on demand

In order to select a scan area and run the check, go the **Scan** tab of the SoftControl SysWatch control panel [32].

Hierarchical list of objects to be scanned contains the following elements.

- **System memory** – scan all running processes.

ℹ We recommend that you perform system memory scan each time the unknown processes that the user has not started appear in the system.

- **Boot sectors** – scan bootable sectors of the disks.
- **Quarantine** – scan the objects removed to quarantine.

ℹ We recommend that you rescan objects on quarantine after the antivirus base update [111] completes.

- **All removable drives** – scan all the file system objects on all removable drives.

ℹ We recommend that you scan the removable drives each time you plan to read or write files from or to such drives, or run a program from a removable media.

- **All hard drives** – scan all the file system objects on all hard drives.
- **My computer** – scan all the file system objects on all hard drives and external storage devices in the computer disc drives and ports.
- **Trash** – scan all the file system objects from the Recycle bin.
- **My documents** – scan user documents.
- **Desktop** – scan all available objects.

▽ **Running scan on demand**

Tick off the required objects and click **Run scan** to start the scan process.

The **Last scan** string indicates the date and time of the most recent check. The **Threat action** string displays the corresponding option [89].

If you click **Quarantine**, the folder opens that contains the files placed to quarantine.

▽ **Running scan in silent mode**

You can run antivirus scanning in silent mode with the help of changetpsmode additional command-line utility [106].

▽ **Viewing scan report**

To view detailed information about the check during the scan process, click **Details**. To open scan report [96] after the scan completes, click the link with the date and time of last check in the **Last scan** string.

4.8.3. Check results

When a malicious code is detected, SoftControl SysWatch determines its type (a virus, a trojan program, a spy program, etc.) and treats it in one of the following ways, according to the options for the response to a threat [89].

▽ **Selecting an action for a certain threat**

If the **Ask action** option is selected, SoftControl SysWatch prompts the user to select an action for each of the detected threats.

The window with the warning that is displayed when a threat is detected is shown in fig. Warning for an infected object [94].

The **SysWatch Alert** window consists of two parts:

• Threat description area. It contains information about the threat: object name, location, and description (possible type of malicious code according to the antivirus database).

• Action selection area. It contains possible actions for a detected threat:

→ **Treat** – disinfect or delete the infected object if it cannot be treated, or terminate the malicious process.

→ **Delete** – delete the infected object and terminate the malicious process;

→ **Move to Quarantine** – move the infected object to a special folder and block its execution.

→ **Skip** – do not perform any actions to treat the object.

❑ **Apply selected action for all objects** – apply the selected action to all subsequent threats in the current scan session.
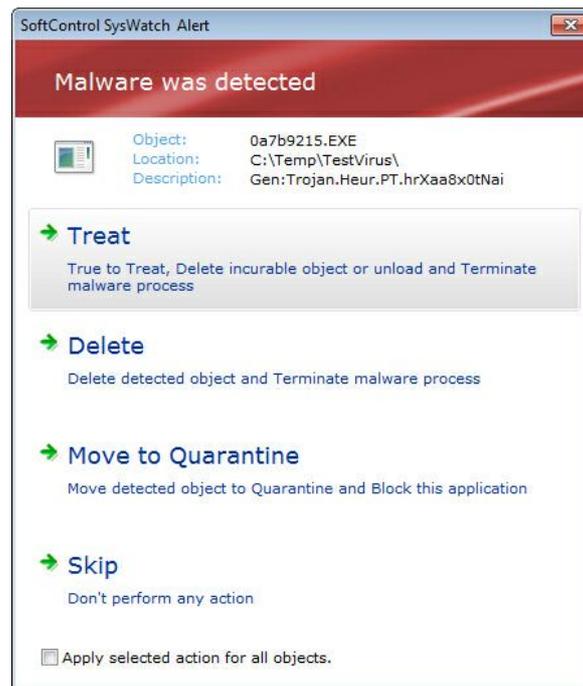

Figure 87. Warning for an infected object

▽ **Selecting action for all the threats when scan finishes**

If the **Select action when the scan finishes** option is selected, SoftControl SysWatch prompts the user to select an action for all threats found in the current scan session.

The **Detected threats** window with the list of the detected malicious objects and possible actions for them, is displayed after the scan and is shown in fig. Window with the detected threats [94].
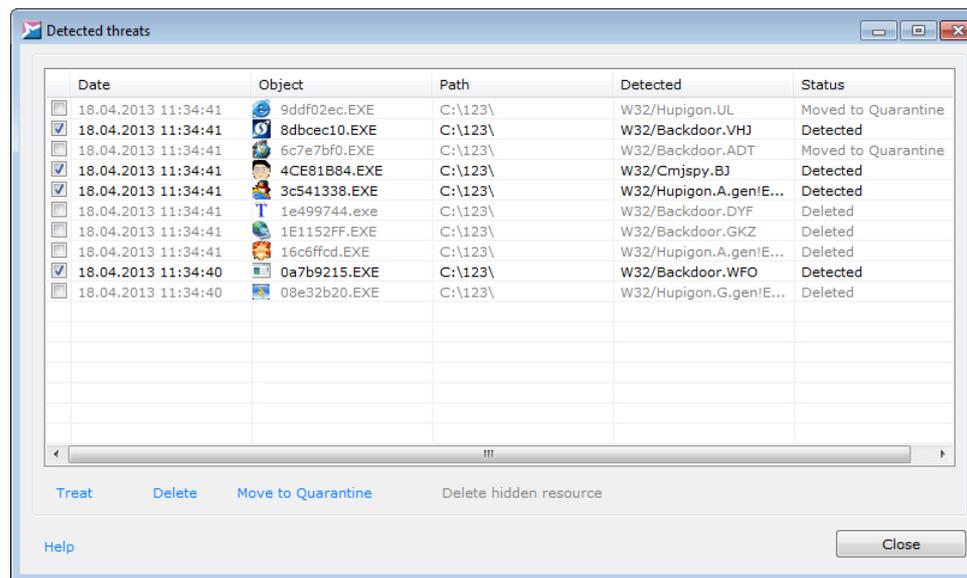
Figure 88. Window with the detected threats

The **Object**, the **Path** and the **Detected** columns display the information about the object that poses a threat: the name, location, and description (possible type of malicious code according to the antivirus database). The **Date** column shows the time of the threat detection, and the **Status** column shows current threat state.

Tick off the boxes for the objects that should be processed and click one of the links:

→ **Treat** – disinfect or delete the infected object if it cannot be treated, or terminate the malicious process.

→ **Delete** – delete the infected object and terminate the malicious process;

→ **Move to Quarantine** – move the infected object to a special folder and block its execution.

→ **Delete hidden resource** – remove a rootkit.

The color of the string with the selected object changes to gray after the actions are applied. The result of the action is displayed in the **Status** column.

Click **Close** after you finish working with the window.

▽ **Viewing the results of the automatic threat processing**

If the **Automatically** option is selected, SoftControl SysWatch processes the infected objects without requests to the user.

To view the check results, click the **Detected** link on the **Scan** tab of the SoftControl SysWatch control panel [32]. You can view the list of the threats and actions applied to them,

in the **Detected threats** window (fig. <u>Window with the detected threats</u> (94)).

Click **Close** after you finish working with the window.

If some of the threats remain unprocessed, the *Some threats have not been treated* status is displayed on the **Scan** tab of the SoftControl SysWatch <u>control panel</u> (32).

If all operations to neutralize threats are successful, the *Computer is checked and protected* status is displayed on the **Scan** tab of the SoftControl SysWatch <u>control panel</u> (32).

4.9. Reports

SoftControl SysWatch enables logging the security events and the program status and generating the reports of two types:

- <u>Text logs</u> (96);
- <u>Registering the events in Windows Management Instrumentation (WMI)</u> (98).

4.9.1. Text logs

Text logs are the main tool for retrospective analysis of the security events in the software environment. SoftControl SysWatch creates the following types of text logs:

- **System** log with the following data:
  - start and stop of the SoftControl SysWatch system service (*safensec.exe*);
  - service database initialization;
  - program name and version;
  - changes in the program status and settings;
  - incidents of the <u>application activity</u> (49) and their parameters: the name, the process and its identifier (PID), parent process module and its identifier (PPID), command line parameters, name of the loaded DLL module, account, execution zone, and status;
  - incidents of the <u>control policy</u> (65) violation and their parameters: the name, activity type, account, the program which is the source of the incident, the file being controlled, and the solution.
- **Profile gathering** log with the following data:
  - <u>profile gathering</u> (43) scope;
  - the list of the checked objects;

- profile gathering [43] results.

▪ **Scan** log with the following data:

- scan scope [92];

- settings for the response to a threat [89];

- scan results [93].

▪ **Update** log with information about the installed program updates [111].

▽ **Setting up report generating parameters**

To view and modify the log parameters, open program settings and select **Settings** → **Reports** (fig. Specifying the report parameters [97]).

To enable report generation, tick off **Enable reports** and select the types of the events to be logged:

❑ **Update**;

❑ **Scan**;

❑ **System**:

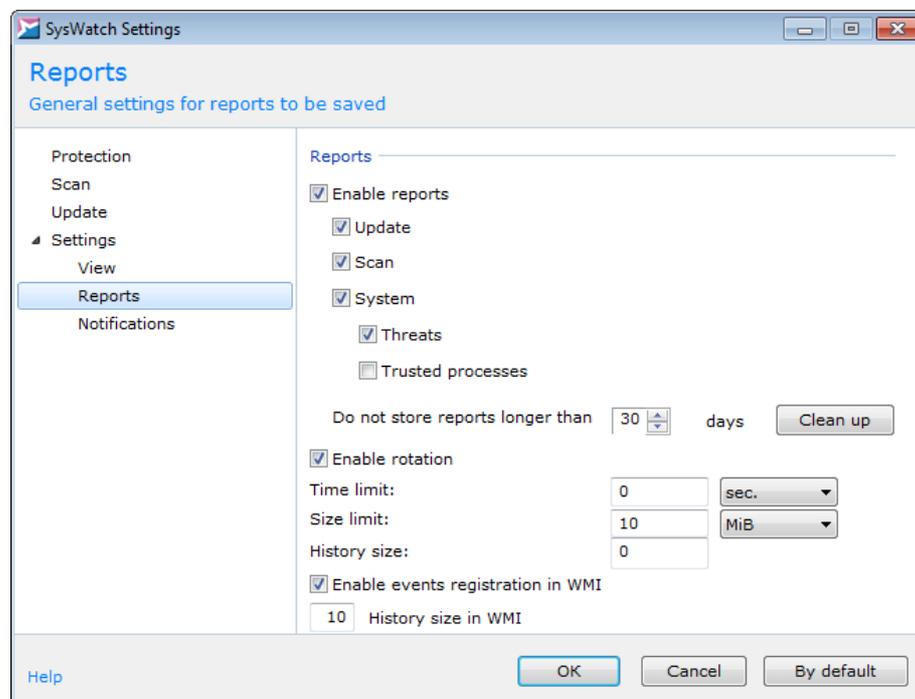   ❑ **Threats**;

     ❑ **Trusted processes**.

Figure 89. Specifying the report parameters

Specify the number of days during which the event history is stored, in the **Do not store**

reports longer than counter. To delete all report files, click **Clean up**.

SoftControl SysWatch supports program log rotation, which allows managing the size of the log file. Rotation allows the logs to be automatically divided into parts of the following type (all parts have identical parameters):

<report file name>.txt.<report part index>,

where the index of the latest log is always 1, and the index of the oldest log is the largest number.

To enable this option, tick off **Enable rotation** and specify the rotation parameters (one or several parameters):

- **Time limit**

Specify the time limit in this field. The log file is rotated after this period expires. Select a unit from the drop-down list (seconds, minutes, hours, or days).

- **Size limit**

Specify the file size limit in this field. The log is rotated when the specified size is exceeded. Select a unit from the drop-down list (bytes, KiB or MiB).

- **History size**

Specify the maximum number of the log file parts to be stored.

To apply changes, click **OK**.

Apart from the standard way to specify program settings with the help of GUI, you can perform this operation with the help of the configuration file [109].

▽ **Viewing the reports**

To view text logs, select **Reports** in the SoftControl SysWatch context menu [31]. In the displayed folder, open the text file with the name of the following type:

<report type>_<dd.mm.yy>_<hh.mm.ss.mmm>.txt.

4.9.2. Registering the events in WMI

SoftControl SysWatch can log information about the events and program status directly to the WMI objects as an aggregate. The feature allows you to obtain this information from the client hosts, in case of remote central administration, for example, with the help of MS SCCM.

Below is the description of the objects, the types of events and SoftControl SysWatch statuses.

An WMI object is called **SafenSoftService** for the *safensec.exe* system service, while it is called **SafenSoftScanner** for the *snsods.exe* antivirus scanner.

Table 9 lists the types of events for both objects.

Table 9. Types of events

Object	Types of events
SafenSoftService	• *InstallerAllow* – allow running an installer; • *InstallerBlock* – block the installer; • *ProcessAllow* – allow running a process; • *ProcessBlock* – block the process.
SafenSoftScanner	• *SuspectList* – suspicious object is detected; • *VirusList* – a virus is detected.

The above-mentioned types are the prefixes that are added before the attribute of the corresponding WMI object. Following a prefix is the _*Count* parameter (total number of the events of this type) or the _*Item0* - _*Item[N]* parameter, where [N] denotes the last N events (the amount specified in configuration).

> System scan errors are not registered in WMI.

Table 10 lists the types of the program status for both objects.

Table 10. Status types

Object	Types of statuses	Type	Value
SafenSoftService	• *AutoSetup* – automatic setup (profile gathering);	string	<status string>
	• *FilesystemControl* – file system protection;	Boolean	False ('0') - disabled True ('not 0') - enabled
	• *RegistryControl* – registry protection;	Boolean	
	• *NetworkControl* – network activity control;	Boolean	
	• *GlobalInstallationMode* – global installation mode;	Boolean	
	• *SystemScan* – system scan status;	string	<status string>
	• *Version* – version information.	string	<product name> <version number>
SafenSoftScanner	• *Version* – version information.	string	<product name> <version number>

Only profile gathering can switch *SystemScan* to all of the statuses mentioned below:

- *Scan is in progress*;

- *Scan has been interrupted by user*;

- *Scan has been completed. No threats have been detected*;

- *Scan has been completed. Threats have been detected*.

Antivirus scanning alone can only switch *SystemScan* to the following status:

- *Scan has been completed. Threats have been detected*.

To reset the '*Scan has been completed. Threats have been detected'* status, it is necessary to run profile gathering, and it should succeed (no malicious code should be detected).

An extra property with the *_LastChange* suffix is created for each attribute (except for the lists). The time of the attribute modification is added to to this property.

▽ **Setting up parameters of logging events to WMI**

To view and modify the parameters of the event logging into WMI, open the program settings and select **Settings** → **Reports** (fig. Specifying the report parameters [97]).

To enable the feature, tick off **Enable events registration in WMI** and specify **History size in WMI** in the corresponding field.

> **i** To avoid high system resource consumption, we recommend that you do not set the history size to more than 100 events; 10-50 events is the optimal value.

To apply changes, click **OK**.

Apart from the standard way to specify program settings with the help of GUI, you can perform this operation with the help of the configuration file [109].

▽ **Viewing registered events**

To view the above-mentioned objects in **Windows Management Instrumentation Tester**, make the following steps:

1) Run *wbemtest.exe* from the Microsoft® Windows®.

2) Click **Connect** and specify the *\\<URI>\root\cimv2* namespace in the upper input field of the **Connect** dialog box (*<URI>* is an IP address or a NetBIOS name of the client host with installed SoftControl SysWatch). To be able to work with a remote client host, you need the permissions to read and write from it. **WMI Control** provides such permissions.

3) Click **Connect**.

4) Click **Enum Classes** in the **IWbemServices** section.

5) Leave the field in the displayed dialog box empty and click **OK**.

6) Select **SafenSoftService** or **SafenSoftScanner** in the displayed list and double-click the selected object to open its properties.

7) Tick off **Hide system properties** in the displayed window.

8) Read the list of properties.

4.10. Setting up general program parameters

Below are the instructions on configuring the SoftControl SysWatch general parameters:

- system service self-protection[101];
- password protection[102];
- delayed start of the system service[103].

4.10.1. System service self-protection

To enable self-protection of the SoftControl SysWatch system service (*safensec.exe*), select the **Settings** section of the program settings and tick off **Disable the external control of system service** in the **Self-protection** area (fig. Setting up the program parameters[101]).
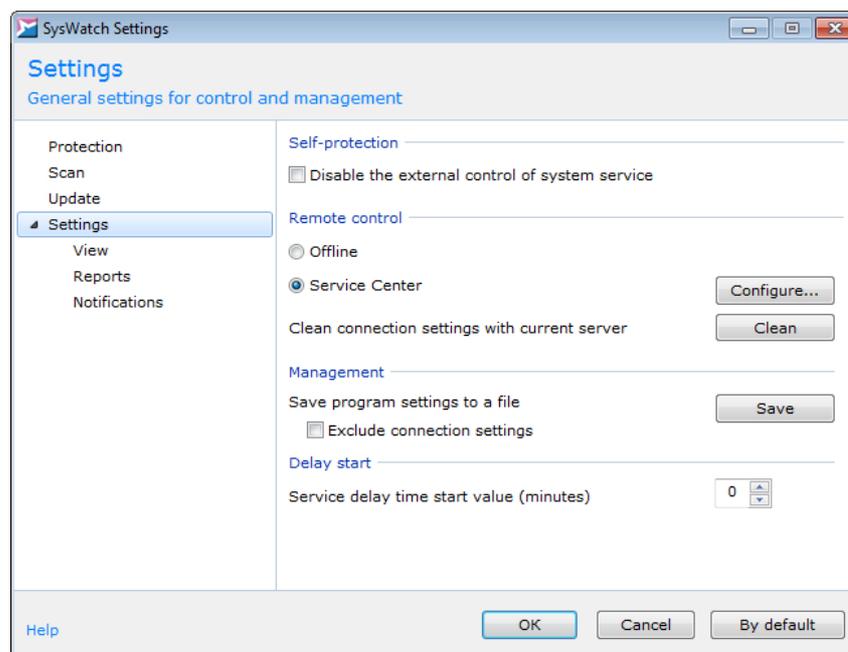
Figure 90. Setting up the program parameters

This option makes it impossible to force the SoftControl SysWatch system service to stop. To

confirm changes, click **OK**.

4.10.2. Password protection

To enable password protection, open the **Protection** section of the program settings, tick off **Enable password protection** and click **Configure** (fig. General protection options[102]).
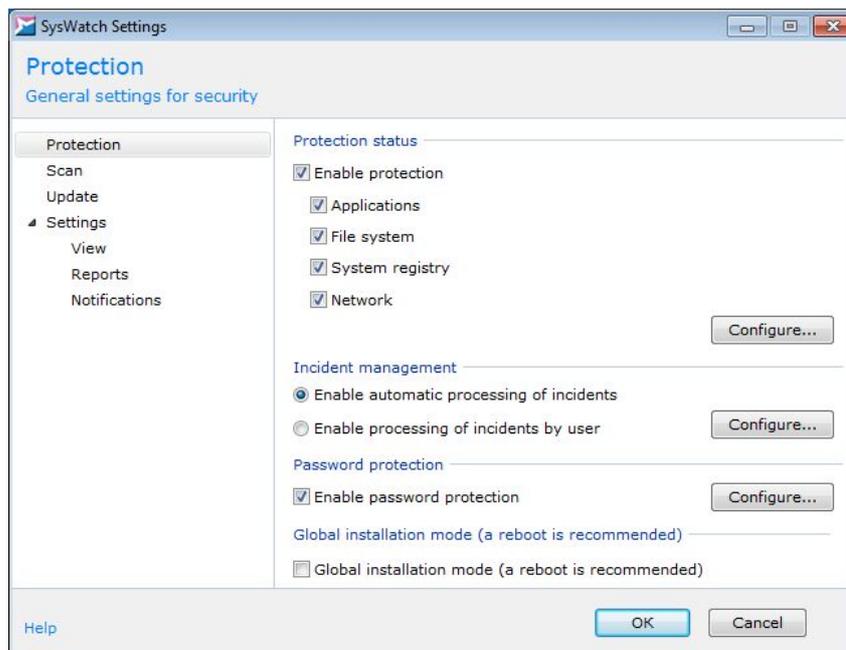

Figure 91. General protection options

Enter the current password (if it has been assigned previously), a new password and confirm it; then select the scope in the **Password protection settings** window (fig. Setting up password protection[102]):
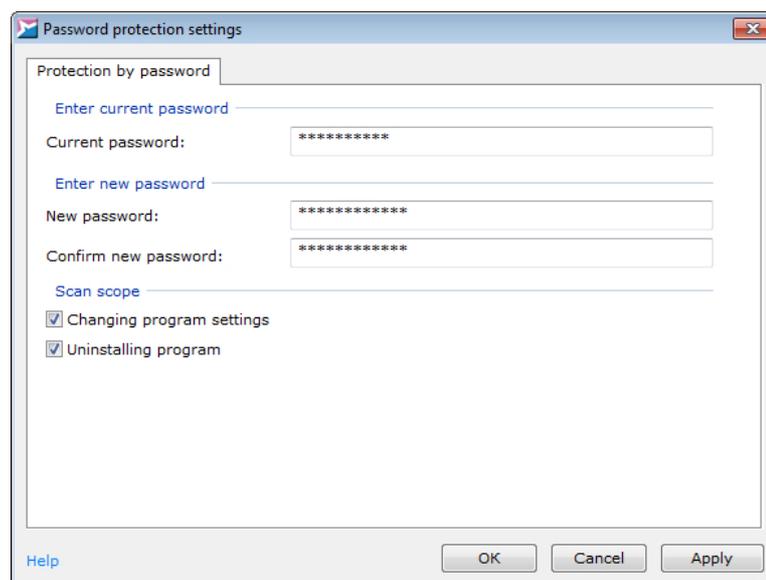

Figure 92. Setting up password protection

❑ **Changing program settings**

request the password when accessing SoftControl SysWatch control panel [32] and settings.

❑ **Uninstalling program**

request the password when uninstalling [120] SoftControl SysWatch.

ℹ The password should be at least 7 characters long.

To confirm changes, click **OK** in both settings window.

4.10.3. Delayed start of the system service

In SoftControl SysWatch, you can specify the interval for the delayed start of system service (*safensec.exe*). The option can be useful for low-speed systems (for example, SSD) when hardware and software initialization intervals overlap. In this case, some of the system devices or services may be initialized incorrectly during abnormal situations such as system reboot after power loss. Setting up the initialization time-outs allows you to avoid such situations.

To enable the option in SoftControl SysWatch, select the **Settings** section of the program settings and specify **Service delay time start value (minutes)** in the **Delay start** area (fig. Setting up the program parameters [103]).

When SoftControl SysWatch system service restarts next time, its loading is delayed for the specified value.
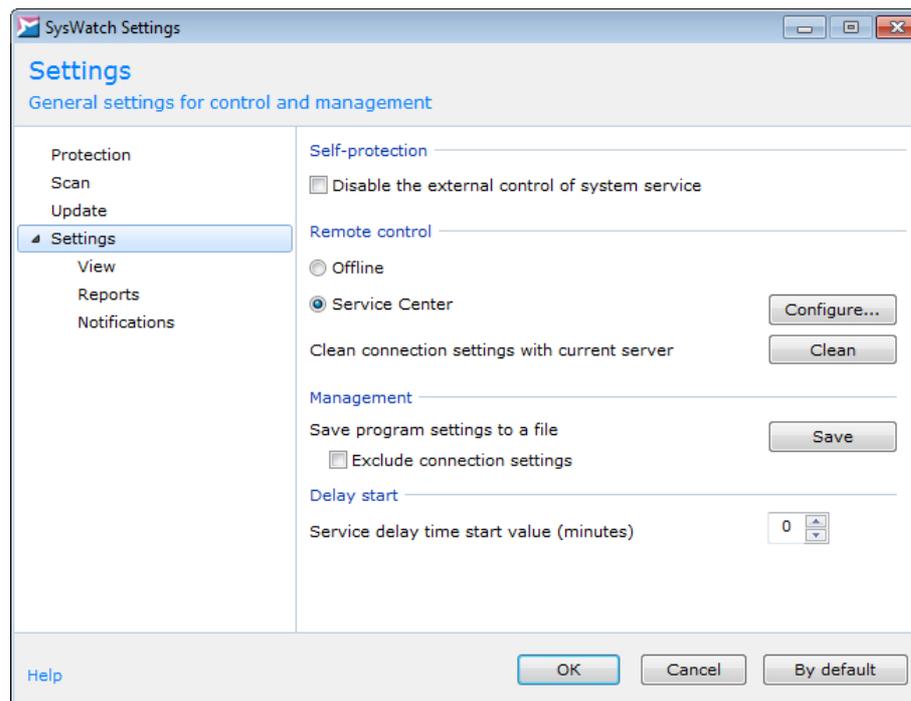
Figure 93. Setting up the program parameters

4.11. Saving and restoring the settings

You can export full SoftControl SysWatch configuration, including customized control policies, the white list of certificates and current program password, to the main configuration file[104]. You can use this file to install the program in silent mode on other client hosts (to clone the program from a sample protected object) and to remove the program in silent mode.

4.11.1. Exporting main configuration file

To save current settings of SoftControl SysWatch, open the **Settings** section of the program settings and click **Save** in the **Management** area (fig. Setting up the program parameters[105]). If the configuration should be unloaded without the server connection settings, tick off **Exclude connection settings** before saving.

View and modify (if necessary) the name of the backup settings file (generated automatically) in the dialog box, specify the path to save the file, select the *XMLC* file type and click **Save**. By default, after the main configuration file is generated, the program encrypts it and saves it to the standard SoftControl SysWatch repository. The repository also contains the *configs.xmlc* and *default.xmlc* files to restore program settings and the default control policy, respectively.

Apart from the standard way to export the main configuration file with the help of GUI, you can

perform this operation with the help of the additional [snsdumpsetting command line utility](#)[107].
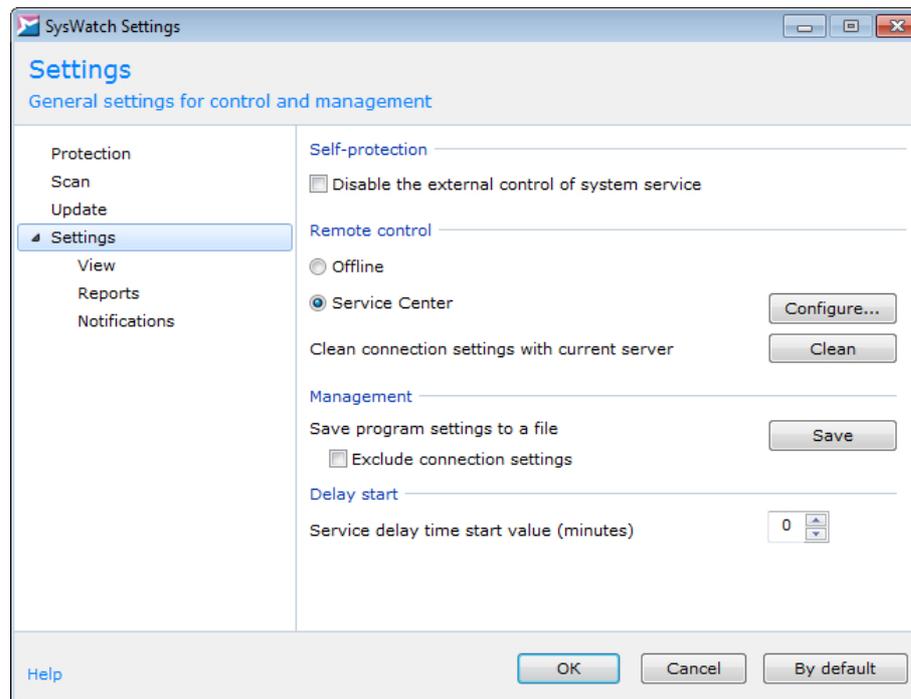

Figure 94. Setting up the program parameters

5. SoftControl SysWatch enhanced capabilities

This section contains the instructions on how to work with the enhanced SoftControl SysWatch functions locally.

5.1. Extra utilities

Extra utilities can be included to the SoftControl SysWatch package. The utilities allow you to use additional SoftControl SysWatch functions. Utilities are provided by the SAFE 'N SEC Corporation company by request.

The utilities run from the OS command line. These utilities can be useful particularly for remote administration of the protected client hosts with the help of the IT infrastructure management tools (for example, MS SCCM).

Below is the description of the utilities:

- changetpsmode [106];
- snsdumpsetting [107].

5.1.1. changetpsmode

The *changetpsmode.exe* utility is designed to manage the global installation mode [49] and to run the antivirus scanning [87] in silent mode.

Command line options for the utility are described in table 11.

Table 11. changetpsmode options

Option	Action
-e <password>	Enable global installation mode. The utility password (GRkNVCOLzyz+311FKlrNqlGlqkxXGfZWXb) is not registered in SoftControl SysWatch reports.
-d	Disable global installation mode.
-s "<object 1>" "<object 2>"..."<object N>"	Run the antivirus scanning of the specified objects in silent mode, where *<object N>* is a full path to the checked object (HDD, a folder or a single file). RAM antivirus scanning is performed automatically when running the check with any path. Silent mode scanning uses the **Automatically** threat action. The results are available in the scan log [96]. Attention: to correctly run silent mode scanning, you should observe the

Option	Action
	specified command syntax. If you want to perform several checks, run a new check only after the previous one completes.

5.1.2. snsdumpsetting

The *snsdumpsetting.exe* utility is intended for exporting the main configuration file[104] in silent mode.

Command line options for the utility are described in table 12.

Table 12. snsdumpsetting options

Option	Action
"<path to the file>\<file name>"	Export SoftControl SysWatch configuration to the file with the specified name (without the extension) in the specified path (if the path is not specified, the utility uses its location as a path by default).

5.2. Using configuration file to edit settings

An alternative way to modify SoftControl SysWatch settings is to use the configuration files[108]. Besides the main configuration file that contains all the program settings, you can use the configuration file only with those parameters that you want to change. To do so, do the following:

1) Create an empty XML file with a random name. Open it in any text editor, for example, in Notepad.

2) Enter the contents of the following type:

```
<Storage>
  <Settings>
    <element 1>
    ...
    <element N>
  </Settings>
</Storage>
```

<element 1>...<element N> are certain elements and their attributes used to modify the program settings described in the corresponding sections:

- automatic setup parameters[108];
- text log parameters[109];
- parameters of registering events in WMI[109].

3) Save the file with the UTF-16 encoding. If you edit the file in Notepad, select Unicode

when you save the file.

5.2.1. Applying configuration file

To apply the configuration file that contains the program settings, do the following:

1) Disable <u>file system protection</u> [65] in the SoftControl SysWatch <u>control panel</u> [32].

2) Copy the configuration file to the *Data* folder of the SoftControl SysWatch installation folder.

3) Enable <u>file system protection</u> [65] in the SoftControl SysWatch <u>control panel</u> [32].

4) Reboot the system for the settings to take effect.

5.2.2. Automatic setup parameters

Configuration *XML* file with automatic setup parameters has the contents of the following type:

```
<Storage>
  <Settings>
    <Setting overwrite="1" key="AutoSetupWizard" type="0" value="<value>"/>
    <Setting overwrite="1" key="EnableAutoSetup" type="0" value="<value>"/>
    <Setting overwrite="1" key="AutoSetupDelay" type="0" value="<value>"/>
  </Settings>
</Storage>
```

Table 13 lists the element keys (the *key* attribute) and their values (the *value* attribute).

Table 13. Keys and the corresponding values of the elements

Key	Function	Value	Description
AutoSetupWizard	Automatic setup status.	0	automatic setup has not been performed
		1	automatic setup has been performed
EnableAutoSetup	Automatic setup run.	0	disabled
		1	enabled
AutoSetupDelay	Delay of the automatic setup relatively to the start of the *safensec.exe* system service.	time	time interval in milliseconds

The encrypted configuration file with the automatic setup parameters can be used for <u>installation in silent mode with the help of the configuration file</u> [15], if it is required to disable profile gathering or delay it after SoftControl SysWatch finishes installation.

5.2.3. Text log parameters

Configuration *XML* file with the text log parameters has the contents of the following type:

```
<Storage>
  <Settings>
    <Setting overwrite="1" key="LogRotateEnable" type="0" value="<value>"/>
    <Setting overwrite="1" key="LogRotateTime" type="3" value="<value>"/>
    <Setting overwrite="1" key="LogRotateSize" type="3" value="<value>"/>
    <Setting overwrite="1" key="LogRotateHistorySize" type="3" value="<value>"/>
  </Settings>
</Storage>
```

Table 14 lists the element keys (the *key* attribute) and their values (the *value* attribute) and the corresponding program GUI elements.

Table 14. Keys and the corresponding values of the elements

Key	GUI element	GUI element status	Additional GUI element status	Value
LogRotateEnable	the **Enable rotation** flag	deselected	-	0
		selected	-	1
LogRotateTime	the **Time limit** field	the specified value	sec	corresponds directly to the GUI element status
LogRotateSize	the **Size limit** field	the specified value	B	corresponds directly
LogRotateHistorySize	the **History size** field	the specified value	-	corresponds directly

5.2.4. Parameters of registering events in WMI

Configuration *XML* file with the parameters of the registering the events in WMI has the contents of the following type:

```
<Storage>
  <Settings>
    <Setting overwrite="1" key="WmiLogEnable" type="0" value="<value>"/>
    <Setting overwrite="1" key="WmiLogLimit" type="0" value="<value>"/>
  </Settings>
</Storage>
```

Table 15 lists the element keys (the *key* attribute) and their values (the *value* attribute) and the corresponding program GUI elements.

Table 15. Keys and the corresponding values of the elements

Key	GUI element	GUI element status	Additional GUI element status	Value
WmiLogEnable	the **Enable events registration in WMI** flag	deselected	-	0

Key	GUI element	GUI element status	Additional GUI element status	Value
		selected	-	1
WmiLogLimit	the **History size in WMI** field	the specified value	-	corresponds directly to the GUI element status

6. Updating SoftControl SysWatch

When SoftControl SysWatch is installed, modifications and new features may already be available for it, and antivirus bases may be out of date. We recommend that you update SoftControl SysWatch right after you install it.

Necessary actions to update SoftControl SysWatch are described below:

- update options [111];
- update in standard mode [114].

If the update source is unavailable, perform the update in manual mode [115].

6.1. Update options

To set up the update parameters, open the **Update** section of the program settings (fig. Update options [111]).
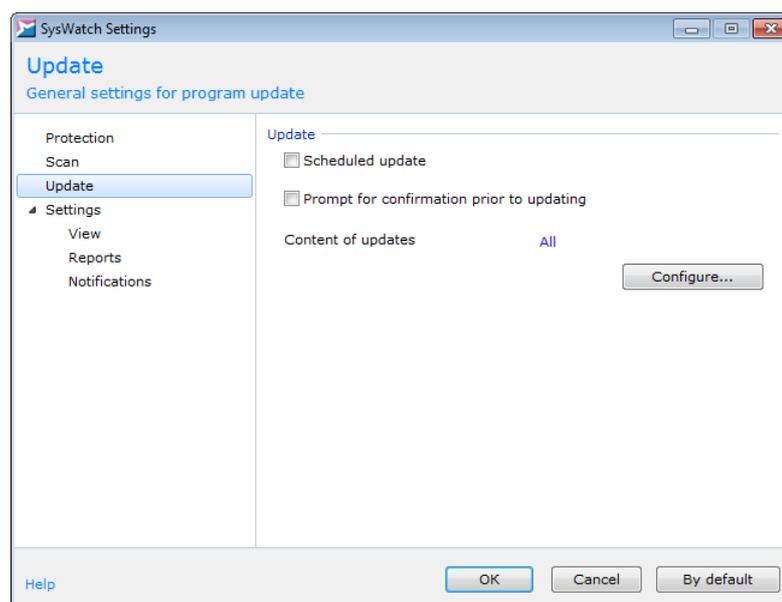
Figure 95. Update options

▽ **Setting up update source and components**

The **Content of updates** string lists the components to be updated. To configure the contents and other update options, click **Configure**.

Select the update method on the **Connection** tab of the **Configure...** window (fig. Selecting the update method [112]):

- ○ **Update through Service Center** – update via the intranet update server (in case of remote control from the server [38]);

○ **Update through Internet** – update via SAFE 'N SEC Corporation server available via internet or LAN.

If you use proxy server to connect to the update server, tick off **Use custom proxy settings** and specify the required settings in the **Connection** area.
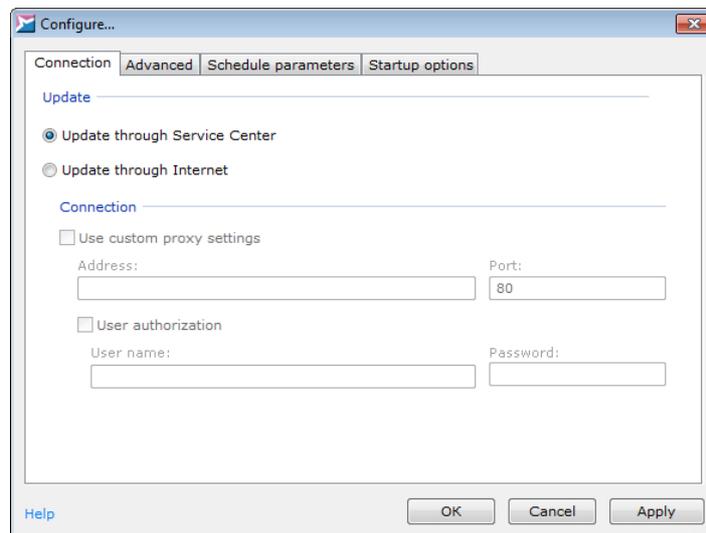
Figure 96. Selecting the update method

Select the required components to update on the **Advanced** tab of the **Configure...** window (fig. <u>Selecting components to update</u> [112]):

❑ **Program updates**;

❑ **AV bases**.
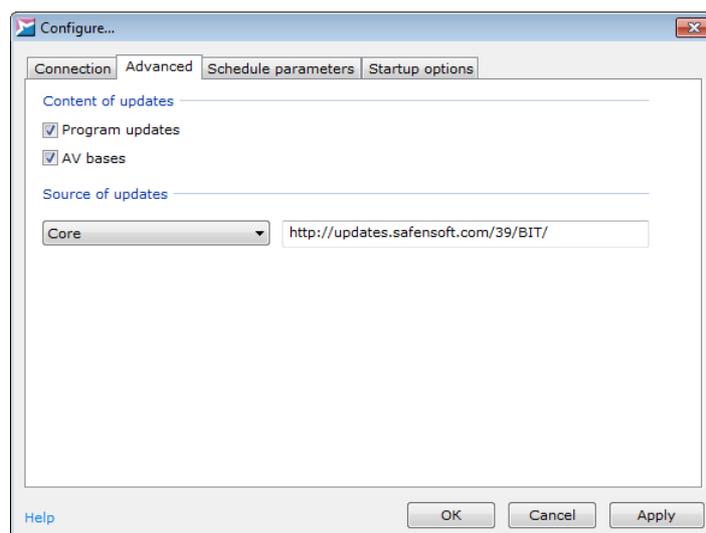
Figure 97. Selecting components to update

%SW%> uses the addresses from the **Source of updates** area to update the proactive protection core and antivirus bases that are available according to the <u>license</u> [40] . You can

edit these addresses in the corresponding field if necessary.

To apply settings, click **OK** or **Apply**.

▽ Setting up the update schedule

Condition: only for <u>remote control from the server</u>⁽³⁸⁾.

To enable automatic **Scheduled update**, tick off the corresponding option. If you need to **Prompt for confirmation prior to updating**, tick off the corresponding checkbox to show the dialog box with the confirmation of the operation. To set up update on schedule parameters, click **Configure**.

Open the **Schedule parameters** tab of the **Configure...** window, specify the the frequency of the task in the **Days frequency** counter and the start time in the *hh:mm:ss* format in the **Invoke time** field (fig. <u>Parameters of scheduled update</u>⁽¹¹³⁾).
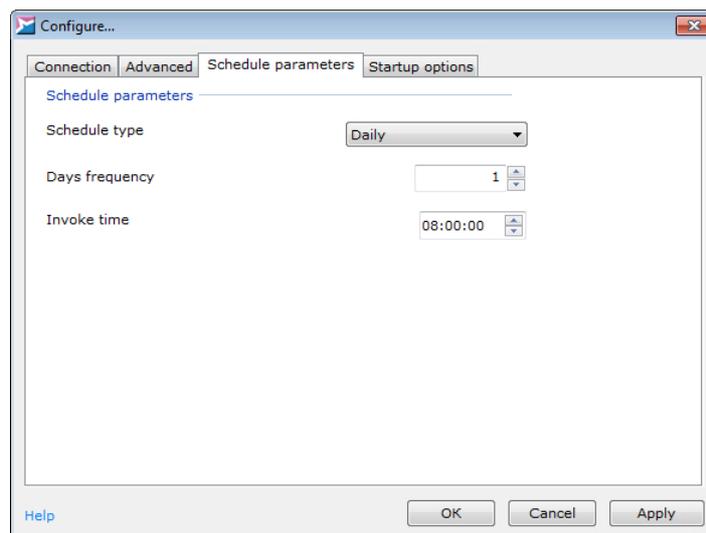
Figure 98. Parameters of scheduled update

To apply settings, click **OK** or **Apply**.

▽ Setting up user account

Specify the user account should be used to perform the update, on the **Startup options** tab of the **Configure...** window (fig. <u>Setting up user account to perform the update</u>⁽¹¹³⁾):
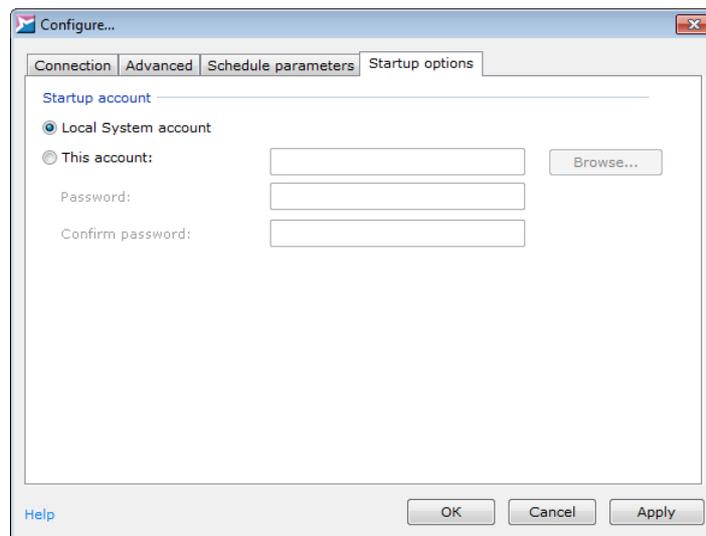
Figure 99. Setting up user account to perform the update

○ **Local System account**;

○ **This account:** specify the credentials.

To apply settings, click **OK** or **Apply**.

Click **OK** to apply the changes.

6.2. Updating the component in standard mode

You can update the program modules and antivirus either simultaneously or separately (tick off the corresponding fields in the update options [112]).

▽ **Updating program modules on demand**

Click **Run update** in the **Update** section of the SoftControl SysWatch control panel [32]. If SoftControl SysWatch detects program modules that are newer than the installed ones, it downloads the modules from the update server and installs them. To complete the update, you should reboot the system after the updates are installed.

If *There are no new updates* status is displayed, the latest version of the program is installed.

The administrator can also perform the update on demand from the SoftControl Admin Console management console. For detailed description of the remote update on demand, see 'SoftControl Service Center administrator's guide'.

▽ **Updating antivirus bases on demand**

Click **Run update** in the **Update** section of the SoftControl SysWatch control panel [32]. If SoftControl SysWatch detects signature databases that are newer than those available on the computer, it downloads the databases from the update server.

If *There are no new updates* status is displayed, antivirus bases are up-to-date.

The administrator can also perform the update on demand from the SoftControl Admin Console management console. For detailed description of the remote update on demand, see 'SoftControl Service Center administrator's guide'.

▽ **Update on schedule**

Scheduling the updates is performed by the local user of SoftControl SysWatch in the corresponding program settings [113], or remotely by the administrator from SoftControl Admin Console. For detailed description of the remote update scheduling, see 'SoftControl Service Center administrator's guide'.

In this mode, SoftControl SysWatch checks for updates at the source specified in the settings, with a certain frequency. If SoftControl SysWatch detects program modules or signature databases that are newer than those available on the computer, it downloads them from the update server runs the installation. To complete the update, you should reboot the system after the program modules are installed.

▽ **Viewing the update report**

To view the detailed information about the update during the process, click **Details**. To open the update report [96] after the update completes, click the link with the date and time of the last check, in the **Last update check** string.

The **Installed updates** string displays the date and time the last update. The **Update mode** string indicates how the last update has been started (on demand or on schedule).

6.3. Updating the component manually

▽ **Updating program modules manually in standard mode**

1) Run the *SoftControl_SysWatch_Patch.msi* installation package of the version you want to update to.

2) Click **Next** in the **SoftControl SysWatch Setup** window (fig. Running the update [115]).

Figure 100. Running the update

3) If you accept the terms, select **I accept the terms in the License Agreement** and click

Next (fig. License agreement[116]).
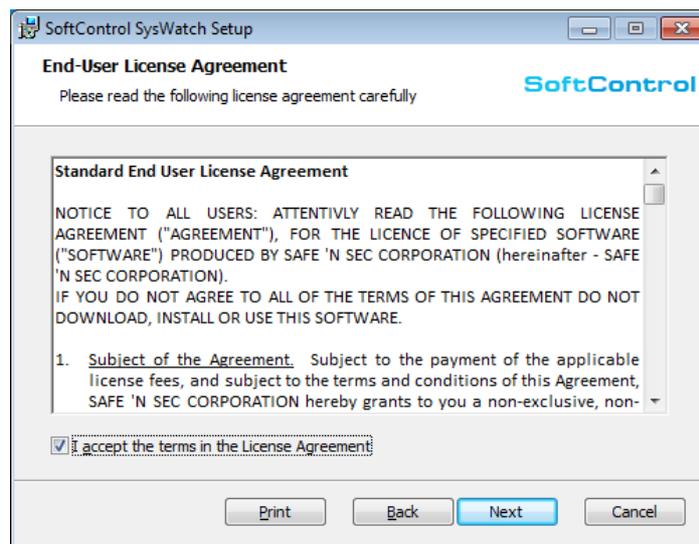
Figure 101. License agreement
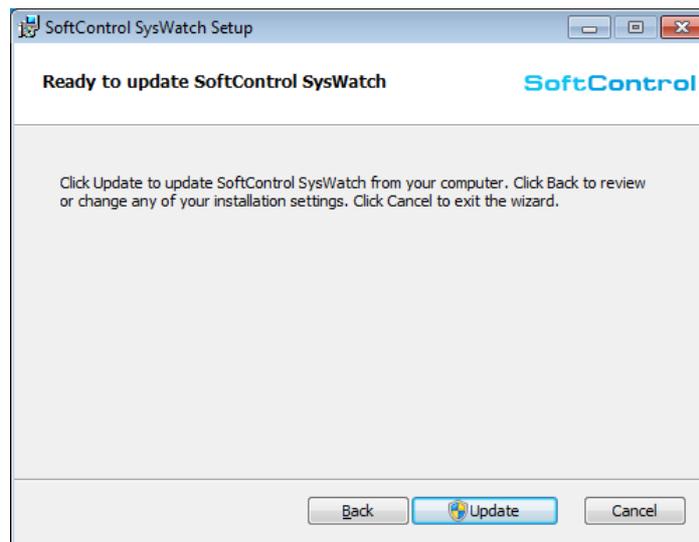
4) Click **Update** (fig. Ready to update[116]).

Figure 102. Ready to update

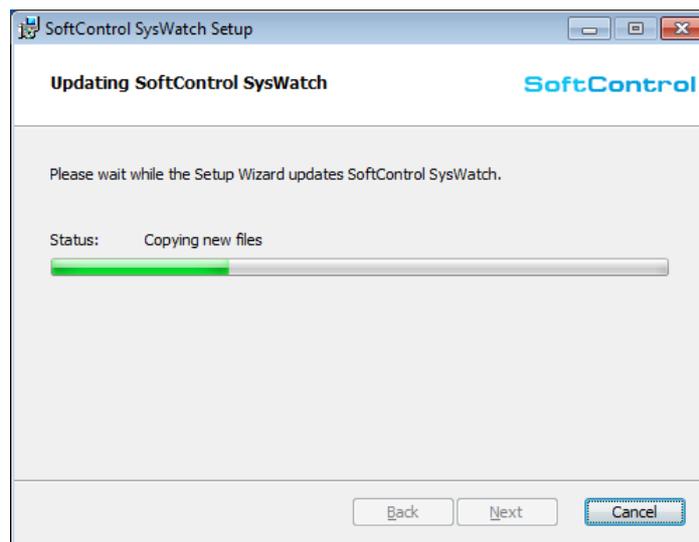5) Wait until the update completes (fig. Updating progress[117]).

Figure 103. Updating progress

6) After the **Completed the SoftControl SysWatch Setup Wizard** message is displayed, click **Finish** (fig. Update completes[117]).
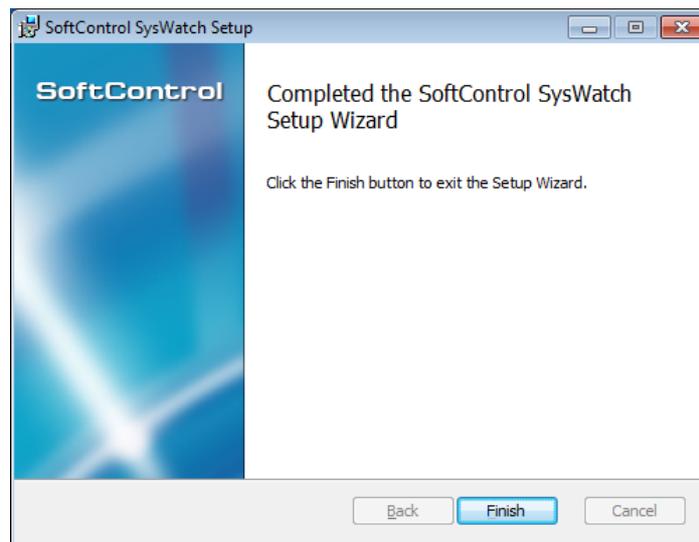
Figure 104. Update completes

7) Select **Yes** in the dialog box that suggests system reboot. The system is then restarted to complete the updates (fig. Requesting system restart[118]).
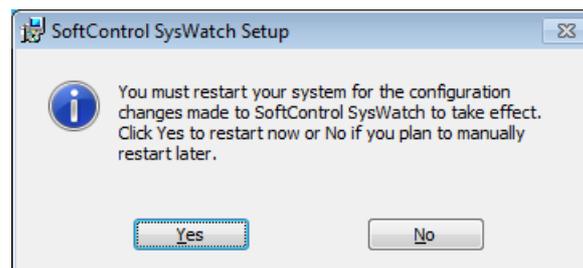
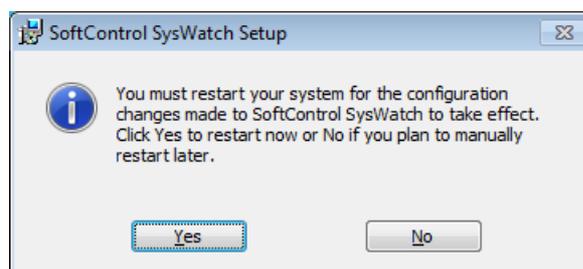**Figure 105. Requesting system restart**

▽ **Updating program modules manually in silent mode**

Important: all steps require administrator privileges.

1) Copy the *SoftControl_SysWatch_Patch.msi* installation package of the version you want to update to the `C:\Temp` directory of the client host.

2) Run Windows command prompt and enter the following command:

```
%windir%\system32\msiexec.exe /i "C:\Temp\SoftControl_SysWatch_Patch.msi" /quiet
```

After the update completes, system is rebooted automatically.

▽ **Updating antivirus bases manually**

To update antivirus bases manually, copy a new archive of the bases (with the replacing option) to the following SoftControl SysWatch folder on the client host:

  o for the *Bitdefender* scanner:

```
<SoftControl SysWatch installation directory>\Plugins\AV\Bitdefender
```

o for the *Kaspersky antivirus* scanner:

```
<SoftControl SysWatch installation directory>\Plugins\AV\KAV
```

o for the *Commtouch antivirus* scanner:

```
<SoftControl SysWatch installation directory>\Plugins\AV\Commtouch
```

o for the *Avira* scanner:

```
<SoftControl SysWatch installation directory>\Plugins\AV\Avira
```

7. Removing SoftControl SysWatch

SoftControl SysWatch can be uninstalled from the client hosts either <u>locally</u>[120] or in one of the <u>remote centralized</u>[121] methods.

7.1. Local uninstallation

You can remove SoftControl SysWatch locally in the following ways.

- <u>standard mode (via GUI)</u>[120];
- <u>silent mode</u>[120];
- <u>silent mode with the help of the configuration file</u>[121].

7.1.1. Uninstalling the component in standard mode

1) For Microsoft® Windows® XP, Microsoft® Windows® Server 2003: go to Windows Control Panel → **Add or Remove Programs** → **Change or Remove Programs**, select *SoftControl SysWatch* and click **Remove**.

   For Microsoft® Windows® 7, Microsoft® Windows® Server 2008, Microsoft® Windows® 8, Microsoft® Windows® Server 2012: go to Windows Control Panel → **Programs** → **Programs and Features**, select *SoftControl SysWatch* and click **Uninstall**.

2) Select **Yes** in the dialog box that suggests system reboot. The system is then restarted to complete uninstallation (fig. <u>Requesting system restart</u>[120]).

Figure 106. Requesting system restart

7.1.2. Uninstalling the component in silent mode

<u>Important</u>: all steps require administrator privileges.

1) Copy the *SoftControl_SysWatch.msi* installation package (or *SoftControl_SysWatch_Patch.msi* if the update was performed) of the current version to the c:

`\Temp` directory of the client host.

2) Run Windows command prompt and enter the following command:

```
%windir%\system32\msiexec.exe /x "C:\Temp\SoftControl_SysWatch.msi" /quiet
```

After the program is removed, system is rebooted automatically.

7.1.3. Uninstalling the component in silent mode with the help of configuration file

Purpose: You can use this method to remove SoftControl SysWatch when program removal is password protected [102] and you need to remove the program in silent mode (without entering password via the interface)

Important: all steps require administrator privileges.

1) Copy the *SoftControl_SysWatch.msi* installation package (or *SoftControl_SysWatch_Patch.msi* if the update was performed) of the current version and the configuration file with the exported program settings [104] (*Storage.xmlc*) to the `C:\Temp` directory of the client host.

2) Run Windows command prompt and enter the following command:

```
%windir%\system32\msiexec.exe /x "C:\Temp\SoftControl_SysWatch.msi" configfilename="C:\Temp\Storage.xmlc" /quiet
```

After the program is removed, system is rebooted automatically.

7.2. Remote uninstallation

Remote uninstallation of SoftControl SysWatch implies centrally managed removal of client applications from a group of hosts integrated into a network.

You can uninstall SoftControl SysWatch remotely in the following ways.

- via domain group policy [121];
- via third party administrative tools [124].

7.2.1. Uninstalling via domain group policy

Note: Microsoft® Windows® Server 2008 R2 is used as an example.

1) Open the **Server Manager** snap-in from the **Administrative Tools** section of the **Start** menu in the OS of the domain controller.

2) Go to the **Features → Group policy Management → Forest: <domain name> → Domains**

→ **<domain name>** section, expand the **Software deployment** organizational unit, invoke context menu of the previously created [16] group policy object for the client application deployment (**Clients deployment**), and select **Edit** (fig. Modifying a group policy object [122]).
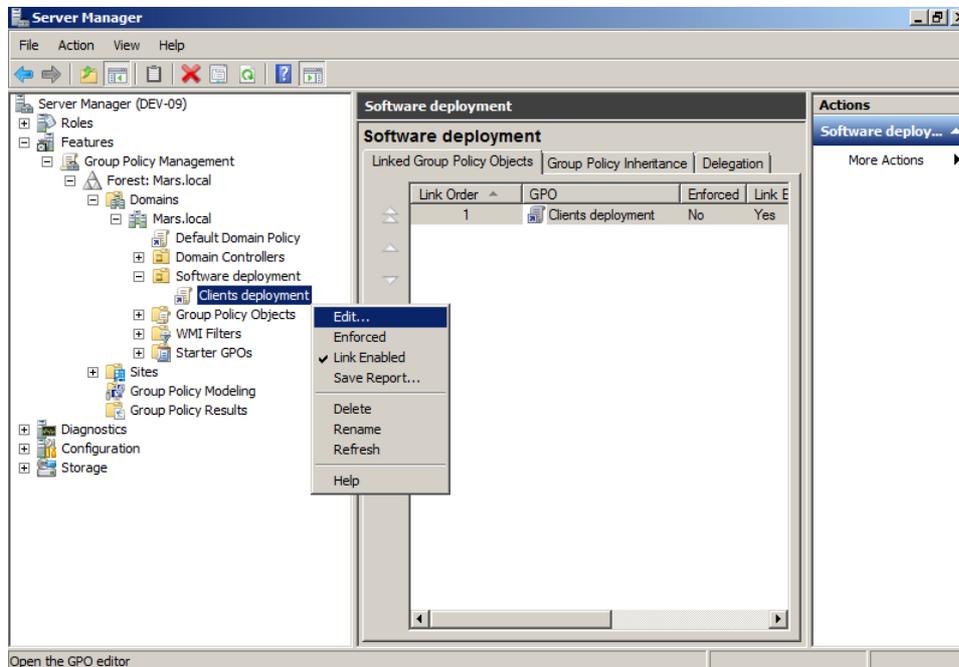
Figure 107. Modifying a group policy object

3) Select the **Computer configuration** → **Policies** → **Software Settings** → **Software installation** section in the displayed **Group Policy Management Editor** snap-in window, select the application to remove from the list of applications, invoke its context menu and select **All tasks** → **Remove** (fig. Invoking the application removal task [122]).
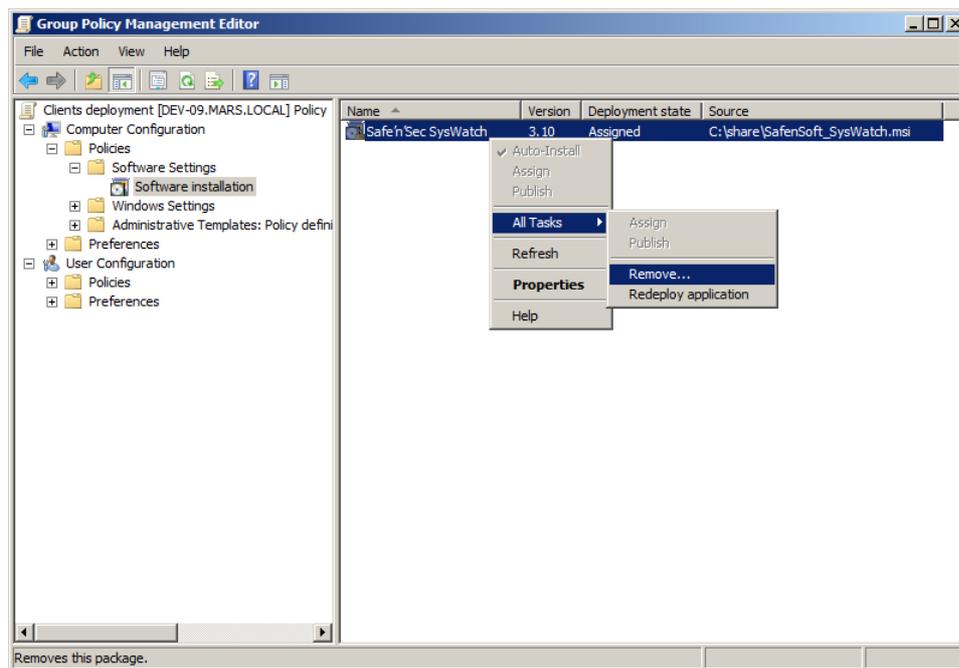
Figure 108. Invoking the application removal task

4) Select **Immediately uninstall the software from users and computers** in the **Remove Software** dialog box and click **OK** (fig. Selecting the removal method [123]).
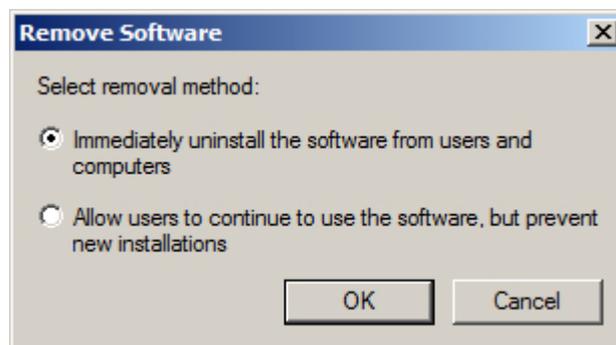
Figure 109. Selecting the removal method

5) After the period of the group policy update expires (the parameter depends on the Active Directory settings), the created policy is applied to the client hosts. The selected applications are removed after the client hosts are rebooted. To apply the created group policy immediately, run Windows command prompt with administrator privileges on a client host and enter the following command:

```
gpupdate /force
```

After the command executes, confirm system reboot by the *Y* command to apply the updated group policy (fig. Updating the group policy parameters manually [123]).

Figure 110. Updating the group policy parameters manually

7.2.2. Uninstalling via third party administrative tools

As with the installation, to to uninstall SoftControl SysWatch remotely you can use third-party IT infrastructure management systems. In this case, the removal method is selected depending on the specific system and the software removal methods that are used in this system.

8. Supplemental information

8.1. Sources

Sources of supplemental information are presented in table 16.

Table 16. Supporting documentation

Name	Description
SoftControl Service Center administrator's guide	Working with the SoftControl Server and SoftControl Admin Console administrative tools.

9. Customer support

If you have any questions concerning the installation, setting up and operation of SoftControl Endpoint Client, please contact our round-the-clock customer support by e-mail support@safensoft.com.

10. Appendix

10.1. Compability with other information security software products

SoftControl SysWatch is a proactive protection tool, and it can be used with most third-party antivirus software.

This chapter describes additional settings that are required to enable SoftControl SysWatch to work with the following products.

- Dr.Web® Antivirus [127].

10.1.1. Dr.Web® Antivirus

For SoftControl SysWatch to install correctly and operate on the system with the installed Dr.Web® Antivirus, you need to perform the following operations.

1) Invoke the Dr.Web® Antivirus context menu by clicking its icon in the Windows notification area and select **Tools** → **Settings** (fig. 111).
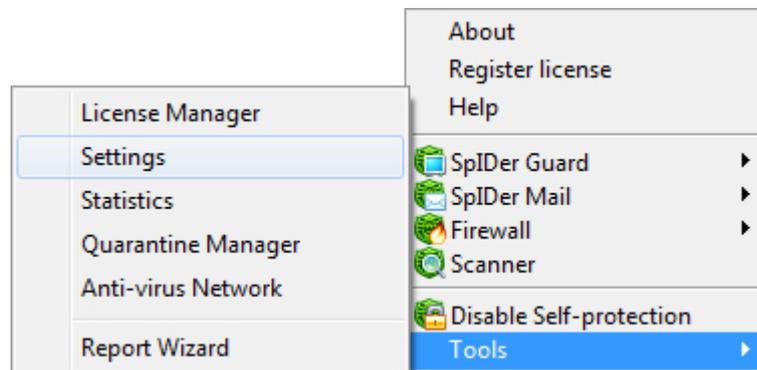
Figure 111. Selecting the main settings of the program

2) Open the **Preventive Protection** section of the **Main** category and click **Custom** to open the detailed settings (fig. 112).
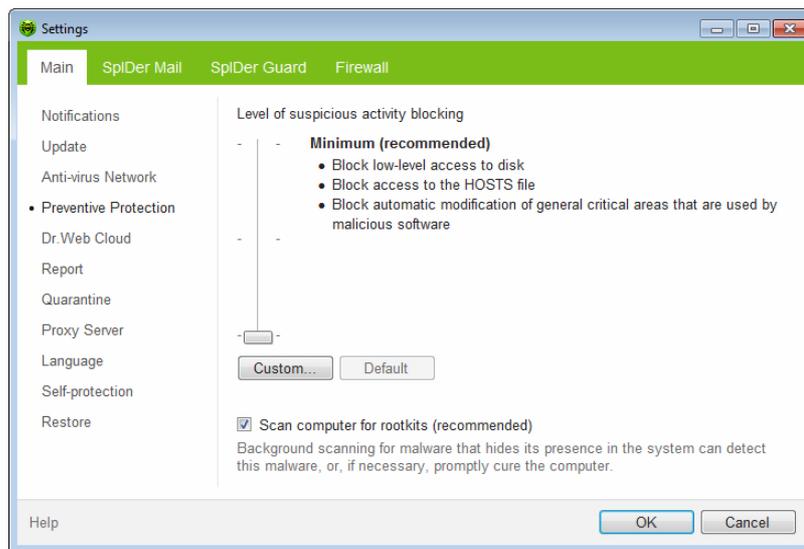
Figure 112. Preventive protection settings

3) Move the **Program autorun** and **Safe mode configuration** switches to the **Allow** state and click **OK** (fig. 113).
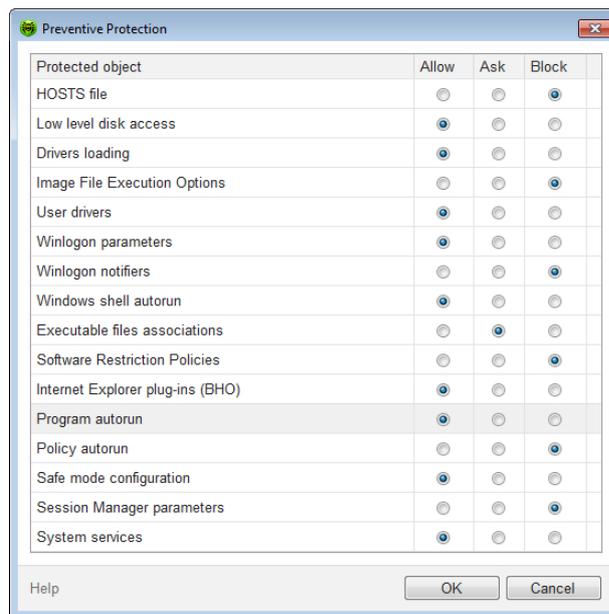

Figure 113. Custom settings for preventive protection

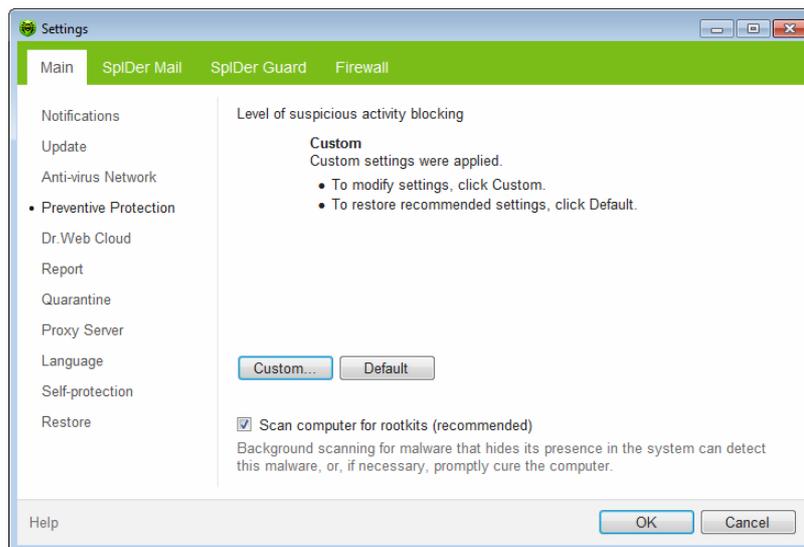4) Confirm the changes in the main settings window by clicking **OK** (fig. 114).

Figure 114. Preventive protection settings

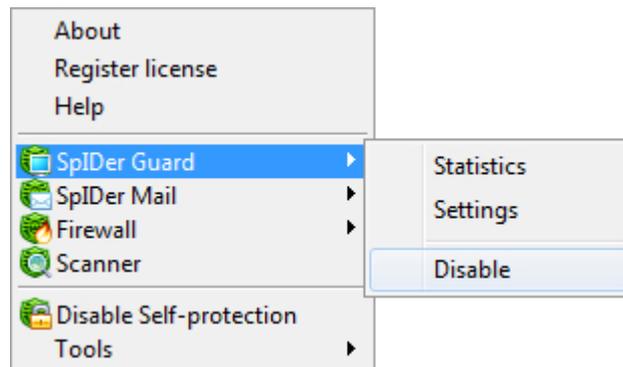5) Turn off the SpIDer Guard protection component by selecting the **SpIDer Guard** → **Disable** item in the context menu (fig. 115).

Figure 115. Disabling SpIDer Guard

6) Run SoftControl SysWatch installation [11].

7) Dr.Web® Firewall displays a notification about the detected network activity during installation. Create a rule that enables outbound connections on 80 port (the HTTP protocol) by clicking **Create new rule**. Confirm the **Apply predefined rule** option by clicking **OK**. (fig. 116, 117).
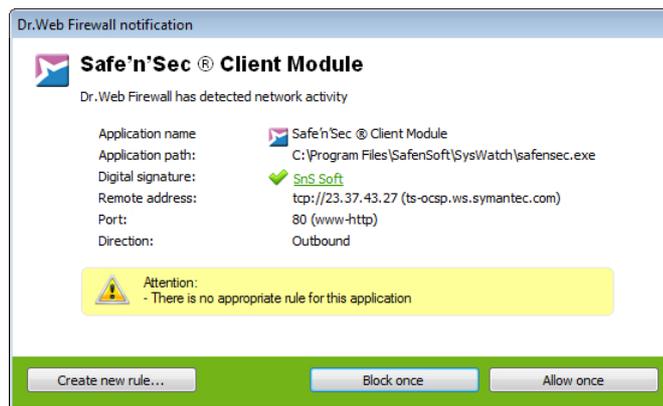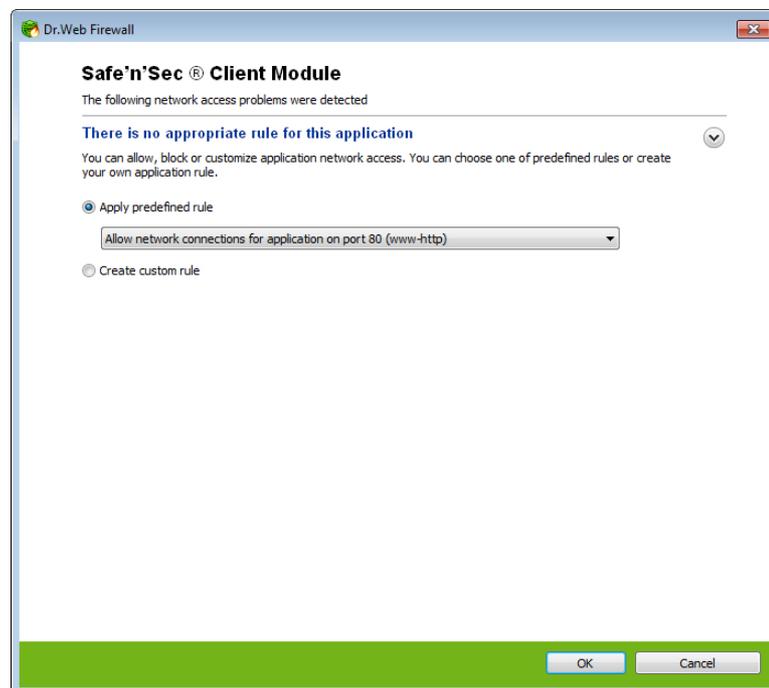
Figure 116. Dr.Web® Firewall notification

Figure 117. Creating a rule in Dr.Web® Firewall

8) Wait until the system profile gathering [43] completes (it runs after the installation). We recommend that you do not perform any operations on the computer during profile gathering.

9) Open the SpIDer Guard component settings by selecting the **SpIDer Guard** → **Settings** item in the context menu (fig. 118).
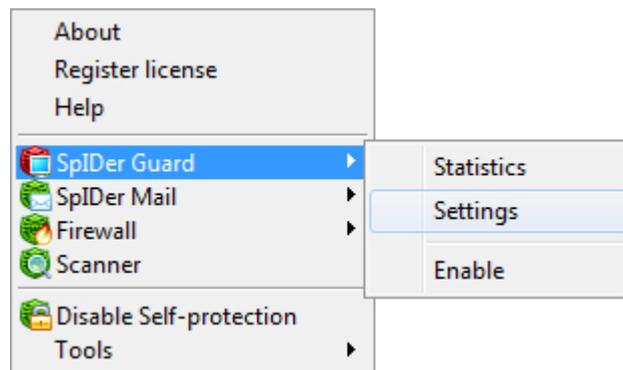
Figure 118. SpIDer Guard settings

10) Open the **Exclusions** section of the **SpIDer Guard** category, select SoftControl SysWatch installation directory by clicking **Browse** and **Add** it to the excluded folders (fig. 119). Click **OK** to apply changes.
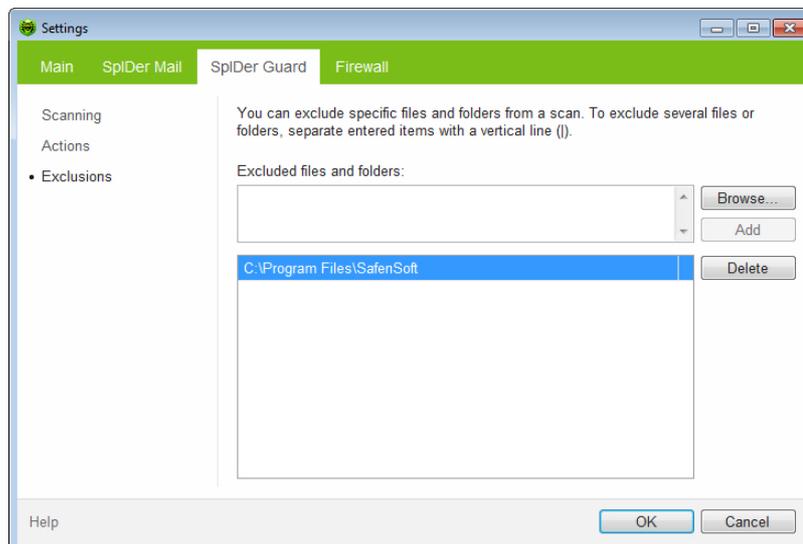

Figure 119. Adding SpIDer Guard exclusions

11) Turn on the SpIDer Guard protection component by selecting the **SpIDer Guard** → **Enable** item in the context menu (fig. 120).
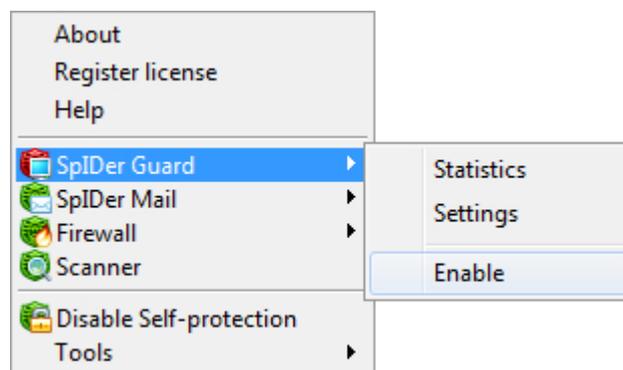

Figure 120. Enabling SpIDer Guard

12) Open the list of processes [56] of SoftControl SysWatch and specify the **Turn on install**

mode option in the properties [59] of all the Dr.Web® modules.