SoftControl

ATM Client 6.1.398

User guide

Dear user!

ARUDIT SECURITY, LLC thanks you for choosing SoftControl ATM Client. Specialists of the company do their best to make sure our software both meets the highest requirements in a field of information protection and is easy use. We hope you find SoftControl ATM Client helpful.

COPYRIGHT

LIABILITY LIMIT

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

ARUDIT SECURITY, LLC, 2024
Postal address:
127106 Russia, Moscow
Novovladykinsky passage, house 8, building 3
ARUDIT SECURITY, LLC
Tel:
+7 499 201-55-12
Fax:
+7 499 201-55-12
E-mails:
Customer service: support@safensoft.com
Sales team: sales@safensoft.com
Website: safensoft.com

Contents

1. Introduction

1.1 Purpose

SoftControl ATM Client (hereafter referred to as SoftControl SysWatch) is designed for protection of Microsoft® Windows®-controlled computers against unauthorized data 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 or 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 'whitelist');

- 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, it is possible to carry out remote centralized management of the program, configuring and monitoring of the protection state on the end devices 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	Important information.
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 SysWatch installation directory>	Fields with specific names to be replaced with actual values.
Appendix 7	Links to internal resources (document sections) with the page numbers, 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;
- **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 prevention techniques-based measures designed to prevent harmful effects.
Prevention techniques	The advanced data protection technologies that are 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 code, but track the potentially dangerous actions the object performs. Therefore, the tools of proactive protection do not require the bases of malicious code and their updates that are necessary for traditional protections.
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

Term	Description
	code (signature) in the database.
Control policy	A complete set of **activity control rules**.
Activity control rule	A set of conditions that determine an application's activity and how SoftControl SysWatch reacts to this activity.
System profile	A database that is stored locally on the **client host** and contains the checksums of the **executable modules**. The profile is the result of the SoftControl SysWatch automatic setup (profile gathering).
Application in the profile	An application with its checksum in the **system profile**.
Tracked application	An application that has run on the **client host** and that SoftControl SysWatch has detected during its operation, after the installation.
Trusted application	**Tracked application** from the **trusted execution zone**.
Restricted application	**Tracked application** from the **restricted execution zone**.
Blocked application	**Tracked application** from the **blocked execution zone**. SoftControl SysWatch blocks such applications on the client host.
Execution zone (trusted, restricted, blocked)	Separate **control policy** that applies to the subset of **tracked applications**. There are three execution zones on each **client host**: trusted, restricted, and blocked zones. Any **tracked application** belongs to one of these zones.
Installer	The application that SoftControl SysWatch has heuristically detected as software designed to install other software; otherwise, it is the application that the user has marked as an installer. The installer gives certain privileges for a process to run (see below 'Software update mode').
Software update mode	An application launch mode that places the application and all PE files it has created or modified, to the system profile. The child processes of the application inherit the software update mode.
V.I.P.O. (Valid Inside Permitted Operations)	User account with restricted rights (a limited set of system privileges and no access to system objects). The account is used to arrange the 'sandbox' when running the applications and provides additional protection from possible harmful actions of the applications that are not entirely trustworthy. Only **restricted applications** can run under the V.I.P.O. account.
PE file	An executable file of the PE format (Portable Executable). The format is used in Microsoft® Windows® operating systems for executable files (EXE), dynamic link libraries (DLL) and some other types of files.
Client host	A computer (a workstation, a server, a self-service terminal) with the installed SoftControl SysWatch.

2. How SoftControl SysWatch works

SoftControl SysWatch supports two protection methods: the system profile and the control policy. The profile's purpose is to preserve the integrity of the OS and all its components including software that has been installed by the user. The control policy is a set of activity control rules. It detects the activity of the applications and determines how SoftControl SysWatch reacts to this activity. The control policy allows managing the access to system resources.

The system profile (automatic setup[43]) is created when SoftControl SysWatch runs for the first time. By default, it is supposed that the computer you are installing SoftControl SysWatch on does not contain any malware. All applications that have been already installed on the computer are added to the system profile.

Activity control rules determine the application execution zones[59] (trusted, restricted, or blocked). After the profile gathering, all applications in the profile are assigned to the trusted zone.

The user performs detailed SoftControl SysWatch setup[48] after the profile gathering. This includes selecting the mode to handle the security incidents (manually[56] or automatically[55]) and specifying the activity control rules.

The profile works as follows (see figure below[54]). When an application tries to run, SoftControl SysWatch checks whether it is in the system profile. If the application is in the profile, it runs according to the activity control rules[68] specified for it. SoftControl SysWatch blocks the applications from the blocked zone. If the application is not in the profile SoftControl SysWatch considers it potentially harmful. The actions SoftControl SysWatch then performs depend on the selected settings.

When an installer runs, SoftControl SysWatch checks whether it has a valid digital signature. SoftControl SysWatch allows the installers with valid digital signatures to run. For signed installers, SoftControl SysWatch can additionally check whether the digital signature certificate is in the whitelist[66] specified by the user.

When an unsigned installer or an installer with invalid digital signature runs, SoftControl SysWatch operates in the same way as when an application that is not in the profile runs. Running the installers and executing the scripts are restricted when:

- the installer or script has no digital signature;
- the installer or script has a digital signature with an expired certificate, and there is no signed timestamp;

- the installer or script has a digital signature from an unknown vendor or from a vendor whose digital signature has been stolen by a violator;
- the certificate of the digital signature is not in the whitelist.

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

The control policy works as follows. For the applications that are not blocked (trusted and restricted zones), access rules apply that are common within each zone. The rules manage the access to file system, system registry and external devices, as well as network activity, process privileges and inter-process interaction. Besides, custom rules [65] can be assigned to each application. All activity control rules [68] that are valid for a zone apply to the installers as well.

Applications from the restricted zone can be assigned [64] special 'V.I.P.O.' account with restricted rights. The V.I.P.O. account:

- has a limited set of system privileges;
- cannot access system resources according to the OS policies (because it is a guest account);
- does not allow the user to load libraries that have no digital signatures and that are not in the profile.

Running applications under the the V.I.P.O. account provides additional system protection from potentially harmful operations.

3. Hardware and software requirements

3.1 SoftControl SysWatch system requirements

Table 3. Minimal system requirements

OS[1]	CPU frequency	RAM size	HDD free space
Client operating systems:			150MB + extra 120MB or more for antivirus database updates
Microsoft® Windows® XP (SP2) *32-bit*[2,3]	800MHz	512MB	
Microsoft® Windows® XP (SP3) *32-bit*[2,3]	800MHz	512MB	
Microsoft® Windows® XP (SP2) *64-bit*[2,3]	800MHz	512MB	
Microsoft® Windows® XP Embedded (SP2) *32-bit*[2,3]	800MHz	256 МБ	
Microsoft® Windows® XP Embedded (SP3) *32-bit*[2,3]	800MHz	256 МБ	
Microsoft® Windows® Embedded for Point of Service 1.0 *32-bit*[2]	800MHz	256 МБ	
Microsoft® Windows® 7 (SP1) *32-bit*[4]	1GHz	1GB	
Microsoft® Windows® 7 (SP1) *64-bit*[4]	1GHz	2GB	
Microsoft® Windows® 8 *32-bit*	1GHz	1GB	
Microsoft® Windows® 8 *64-bit*	1GHz	2GB	
Microsoft® Windows® 8.1 *32-bit*	1GHz	1GB	
Microsoft® Windows® 8.1 *64-bit*	1GHz	2GB	
Microsoft® Windows® 10 *32-bit*	1GHz	1GB	
Microsoft® Windows® 10 *64-bit*	1GHz	2GB	
Microsoft® Windows® 10 IoT Enterprise *32-bit*	1GHz	1GB	
Microsoft® Windows® 10 IoT Enterprise *64-bit*	1GHz	2GB	
Microsoft® Windows® 11 *64-bit*	1GHz	4GB	
Server operating systems:			
Microsoft® Windows® Server 2003 (SP2) *32-bit*[2,3]	800MHz	512MB	
Microsoft® Windows® Server 2003 (SP2) *64-bit*[2,3]	800MHz	512MB	
Microsoft® Windows® Server 2003 R2 (SP2) *32-bit*[2,3]	800MHz	512MB	
Microsoft® Windows® Server 2003 R2 (SP2) *64-bit*[2,3]	800MHz	512MB	
Microsoft® Windows® Server 2008 R2 *64-bit*[4,5]	1.4GHz	512MB	
Microsoft® Windows® Server 2012 *64-bit*[5]	1.4GHz	512MB	
Microsoft® Windows® Server 2012 R2 *64-bit*[5]	1.4GHz	512MB	
Microsoft® Windows® Server 2016 *64-bit*[5]	1.4GHz	2GB	
Microsoft® Windows® Server 2019 *64-bit*[5]	1.4GHz	2GB	
Microsoft® Windows® Server 2022 *64-bit*[5]	1.4GHz	2GB	

Notes:

1. All popular platforms with the above-mentioned operating systems are supported.
2. Visual C++ 2008 SP1 Redistributable Package x86 (including for 64-bit OSs).
3. Additional operations may be required for Windows XP and Windows Server 2003 (see

Updating SoftControl SysWatch and antivirus bases on Windows XP 137).

4. Update KB3033929 or equivalent (support of the SHA-256 algorithm for digital signature verification).
5. Only desktop installation options are supported.

4. Installing and setting up SoftControl SysWatch

SoftControl SysWatch can be installed on the client hosts locally[14], as well as by one of the remote centralized[18] 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[31] SoftControl SysWatch on SoftControl Service Center.

4.1 Local installation

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

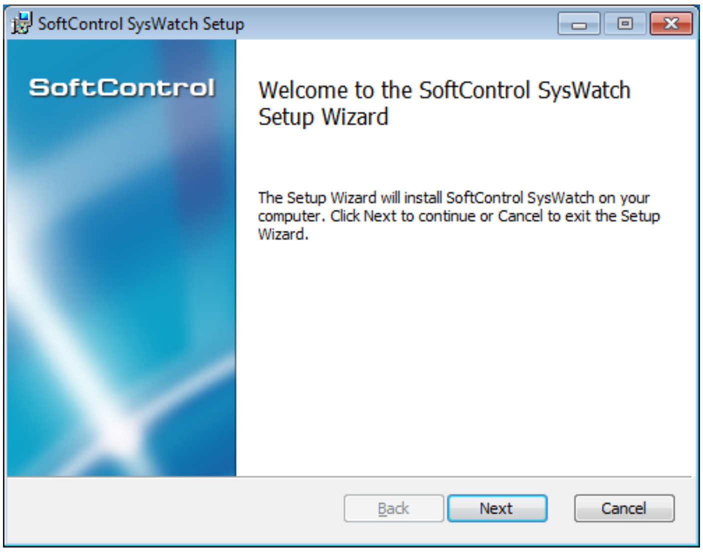
You can install SoftControl SysWatch locally in the following ways.

- standard mode (via GUI)[14];
- silent mode[17];
- silent mode with the help of configuration file[18].

4.1.1 Installing the component in standard mode

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

2) Click **Next** in the **SoftControl SysWatch Setup** window (fig. Running the installer[14]).



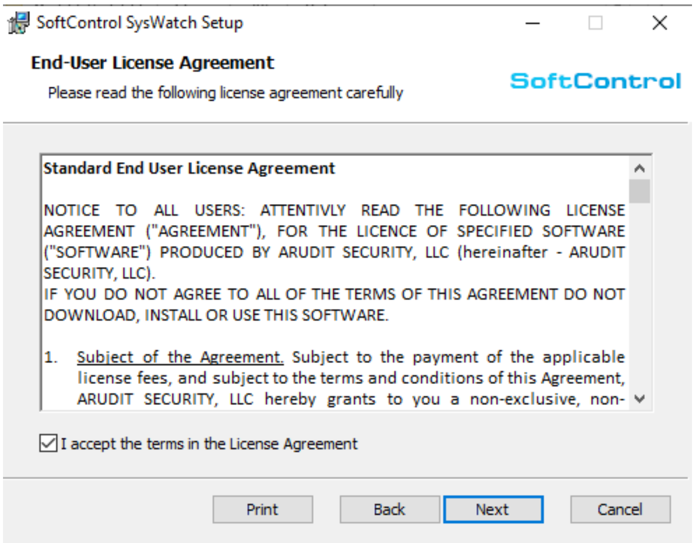
Welcome to the SoftControl SysWatch Setup Wizard

The Setup Wizard will install SoftControl SysWatch on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

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 15).



SoftControl SysWatch Setup

End-User License Agreement

Please read the following license agreement carefully

Standard End User License Agreement

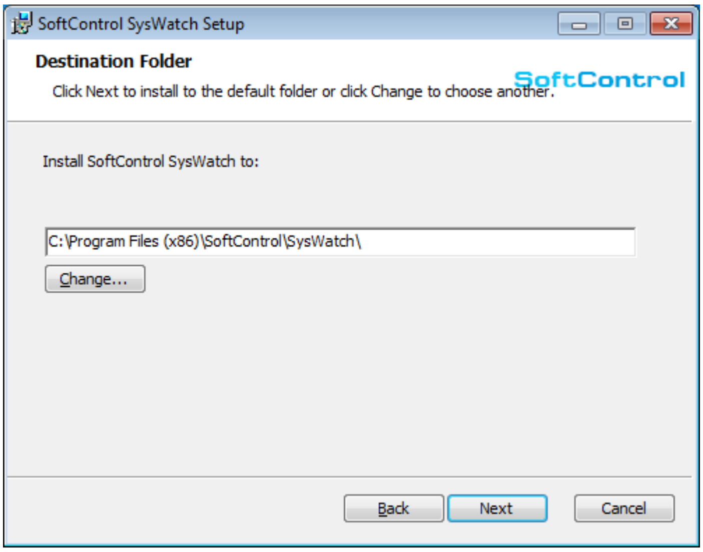
NOTICE TO ALL USERS: ATTENTIVLY READ THE FOLLOWING LICENSE AGREEMENT ("AGREEMENT"), FOR THE LICENCE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY ARUDIT SECURITY, LLC (hereinafter - ARUDIT SECURITY, LLC).
IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

1. Subject of the Agreement. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, ARUDIT SECURITY, LLC hereby grants to you a non-exclusive, non-

☑ I accept the terms in the License Agreement

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 15).



SoftControl SysWatch Setup

Destination Folder

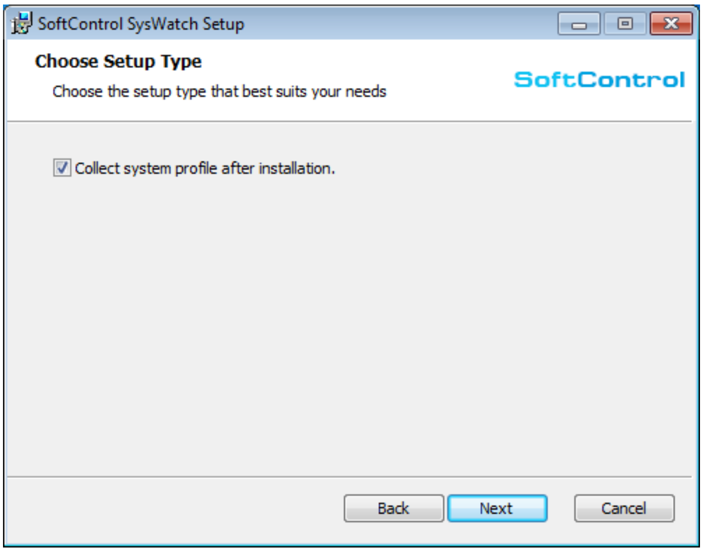
Click Next to install to the default folder or click Change to choose another.

Install SoftControl SysWatch to:

C:\Program Files (x86)\SoftControl\SysWatch\

Figure 3. Installation path

5) By default, SoftControl SysWatch starts gathering system profile after installation (fig. Enabling profile collection 15). As the process takes some time, you can deselect the option and run profile gathering later (see section Run on demand 46).


SoftControl SysWatch Setup

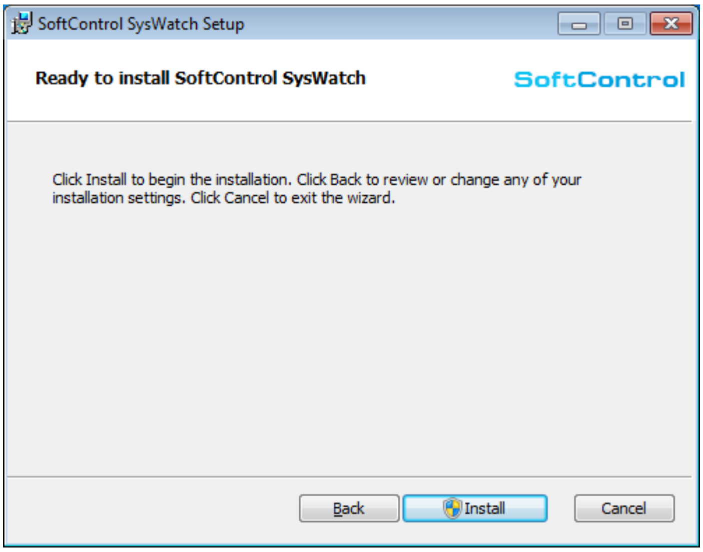
Choose Setup Type

Choose the setup type that best suits your needs

☑ Collect system profile after installation.

Figure 4. Enabling profile collection

6) Click **Install** (fig. Ready to install 16).

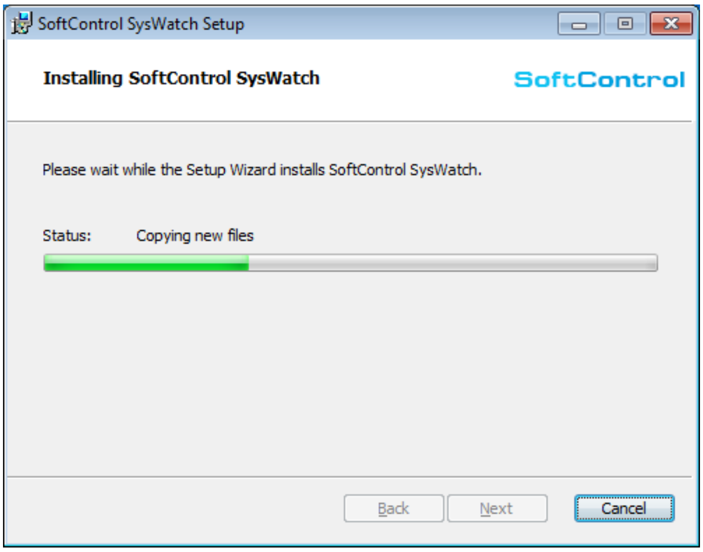

SoftControl SysWatch Setup

Ready to install SoftControl SysWatch

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Figure 5. Ready to install

7) Wait until installation completes (fig. Installation progress 16).



SoftControl SysWatch Setup

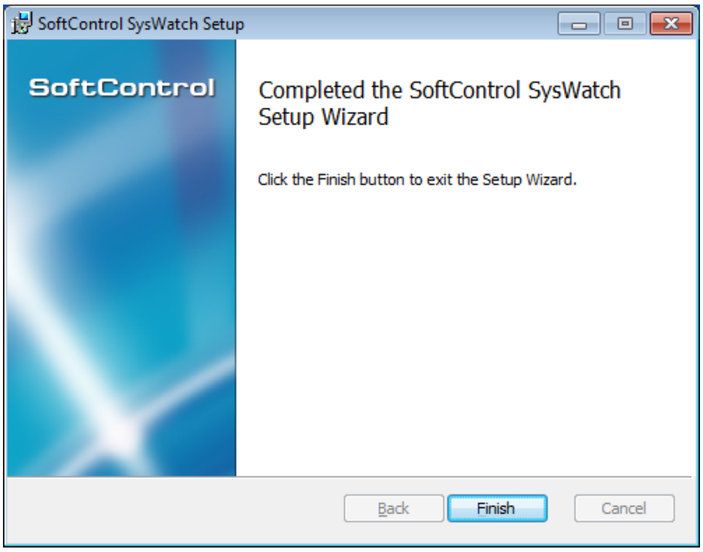
Installing SoftControl SysWatch

Please wait while the Setup Wizard installs SoftControl SysWatch.

Status: Copying new files

Figure 6. Installation progress

8) After the **Completed the SoftControl SysWatch Setup Wizard** message is displayed, click **Finish** (fig. Installation completes 17).



SoftControl SysWatch Setup

Completed the SoftControl SysWatch Setup Wizard

Click the Finish button to exit the Setup Wizard.

Figure 7. Installation completes

4.1.2 Installing the component in silent mode

Important: All steps require administrator privileges.

1) Copy the *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\SysWatch.msi" /quiet
```

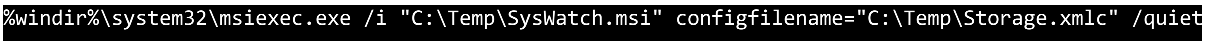
In case of success, msiexec.exe will finish operation with exit code 0. Otherwise, the exit code will have a different value. See https://docs.microsoft.com/ru-ru/windows/win32/msi/error-codes for details.

4.1.3 Installing the component in silent mode with the help of configuration file

Important: All steps require administrator privileges.

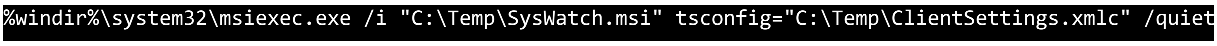
1) During silent installation, you can apply custom configuration (previously exported program settings[111]; *Storage.xmlc* in the example below) or configuration file with the settings of connection to the controlling server[41] (*ClientSettings.xmlc*), while keeping the default settings for the rest of configuration. Copy the *SysWatch.msi* installation package and the required configuration file to the `C:\Temp` directory of a client host (create the directory in advance).
2) Run Windows command prompt and enter the following command:

   for the configuration file with custom settings:



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

   for the configuration file with the connection settings:



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

   Note: In this case, SoftControl SysWatch switches to the Service Center management mode[40] automatically after installation.

In case of success, msiexec.exe will finish operation with exit code 0. Otherwise, the exit code will have a different value. See https://docs.microsoft.com/ru-ru/windows/win32/msi/error-codes for details.

4.2 Remote installation

Remote SoftControl SysWatch installation implies centrally managed installation of client applications on 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[19];

- via the remote installation utility 28;
- via third party administrative tools 31.

4.2.1 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 19).

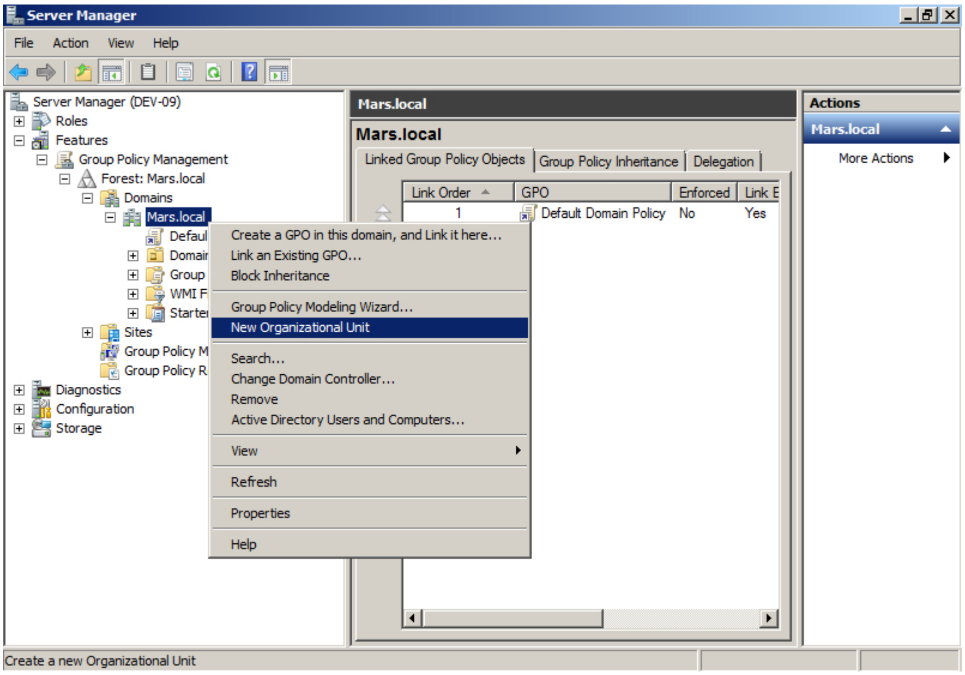
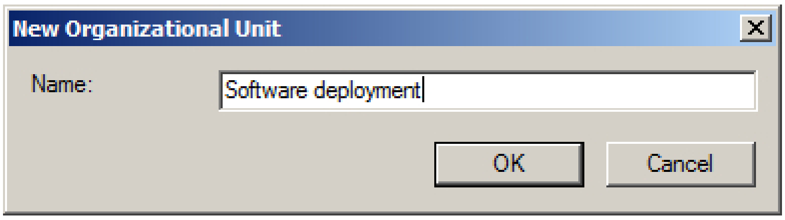


Figure 8. Creating new domain organizational unit

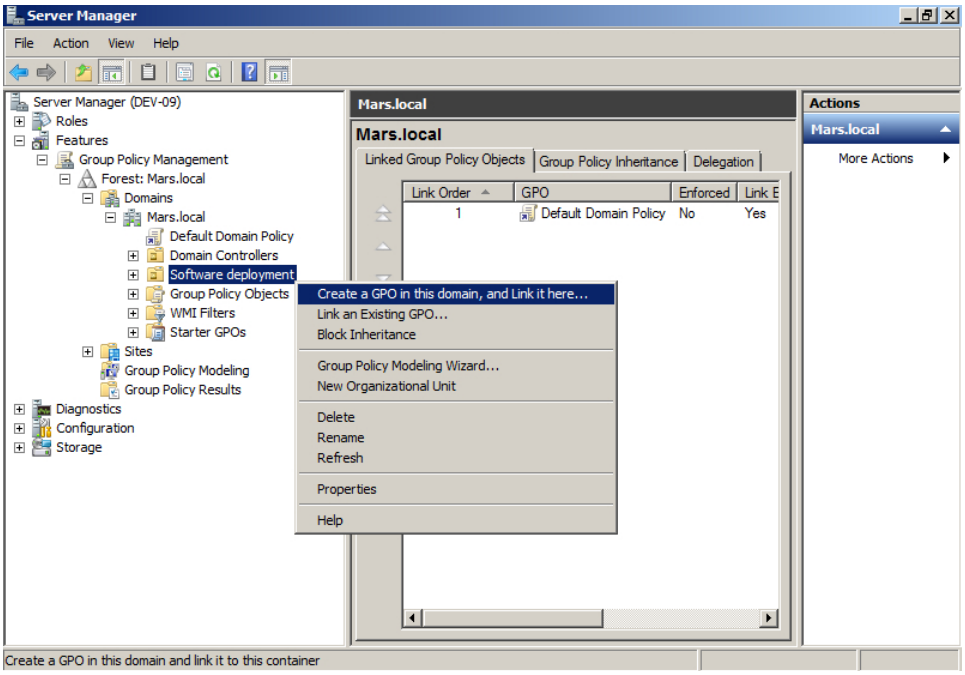
3) Enter **Name** of the unit in the **New Organizational Unit** dialog box and click **OK** (fig. Specifying the name of the organizational unit 19).


New Organizational Unit

Name: Software deployment

Figure 9. Specifying the name of the organizational unit

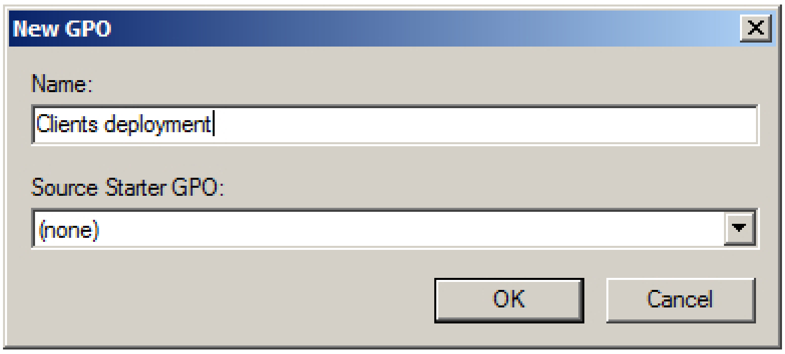
4) Invoke context menu of the created organizational unit in the **Features** → **Group policy Management** → **Forest: <domain name>** → **Domains** → **<domain name>** section and select **Create a GPO in this domain, and Link it here** (fig. Creating a new object of the group policy 20).



Create a GPO in this domain and link it to this container

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 20).



Name:
Clients deployment

Source Starter GPO:
(none)

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 21).

7) Go to the **Computer configuration** → **Policies** → **Software Settings** → **Software installa-**

tion 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 21).

8) Select the *SysWatch.msi* installation package which is in the network source available to the client hosts you need to install the applications to, and click **Open** (fig. Selecting the installation package 21).

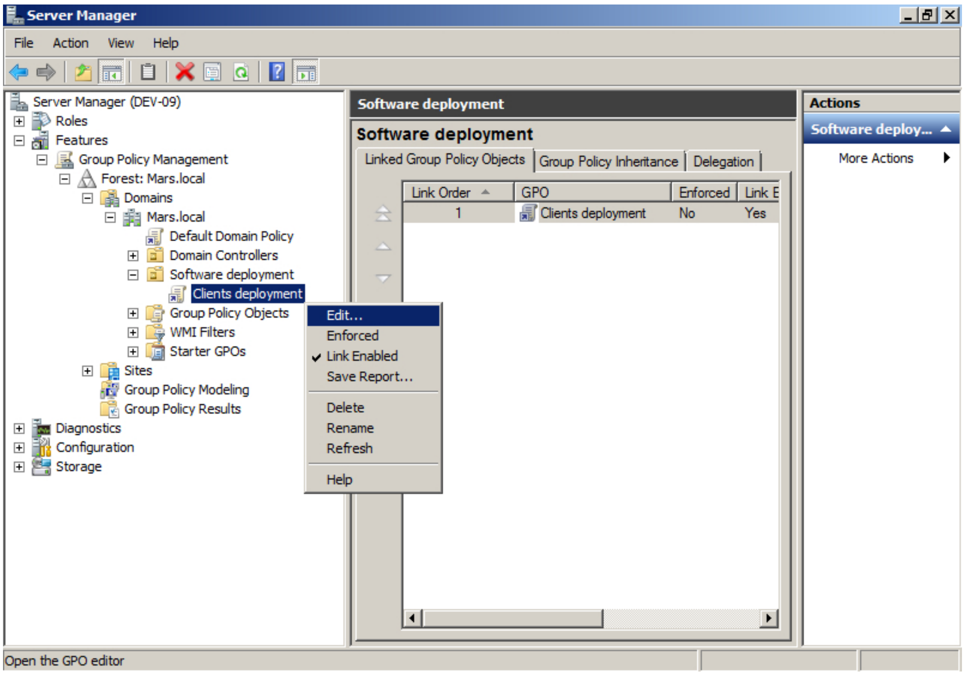


Figure 12. Modifying group policy object

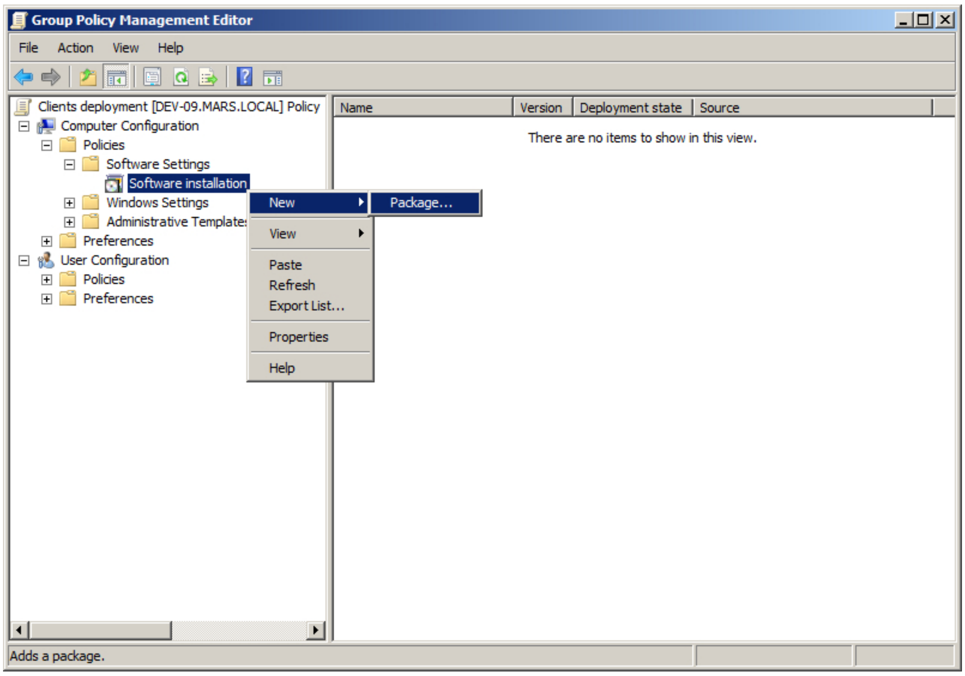
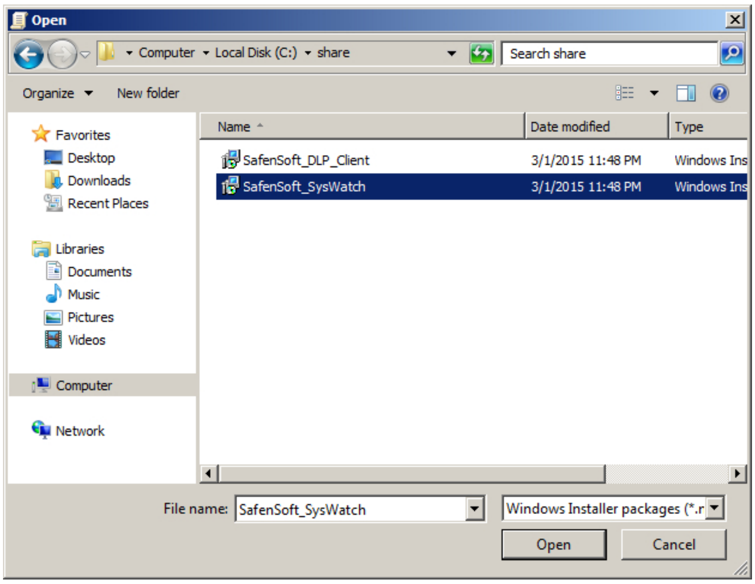


Figure 13. Adding new installation package



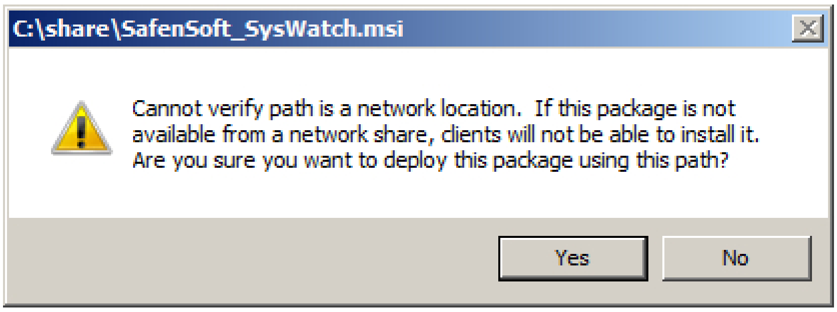
Name	Date modified	Type
SafenSoft_DLP_Client	3/1/2015 11:48 PM	Windows Ins
SafenSoft_SysWatch	3/1/2015 11:48 PM	Windows Ins

File name: SafenSoft_SysWatch

Windows Installer packages (*.r

Figure 14. Selecting the installation package

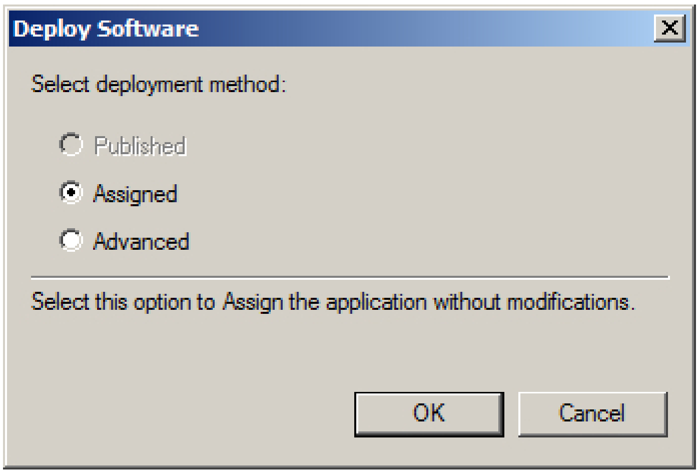
9) If an alert is displayed, make sure that the selected installation package is available for the remote client hosts via network, and click **Yes** (fig. Alert when selecting the location of the installation package 22).


C:\share\SafenSoft_SysWatch.msi

Cannot verify path is a network location. If this package is not available from a network share, clients will not be able to install it. Are you sure you want to deploy this package using this path?

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 22).



Deploy Software

Select deployment method:

○ Published

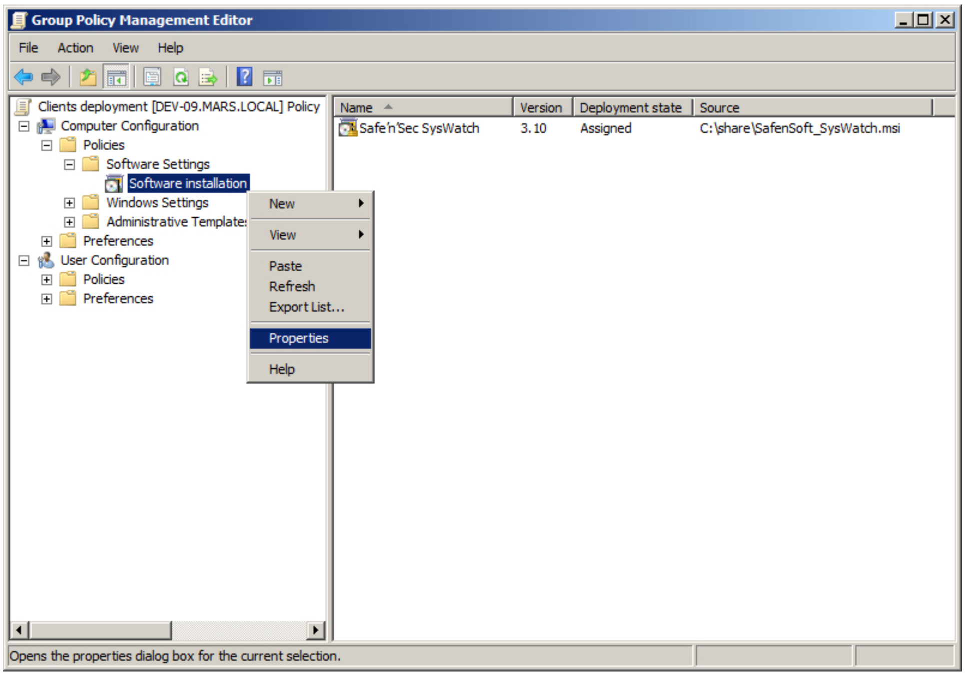
● Assigned

○ Advanced

Select this option to Assign the application without modifications.

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[23]).



Group Policy Management Editor

- Clients deployment [DEV-09.MARS.LOCAL] Policy
  - Computer Configuration
    - Policies
      - Software Settings
        - Software installation
      - Windows Settings
      - Administrative Template:
    - Preferences
  - User Configuration
    - Policies
    - Preferences

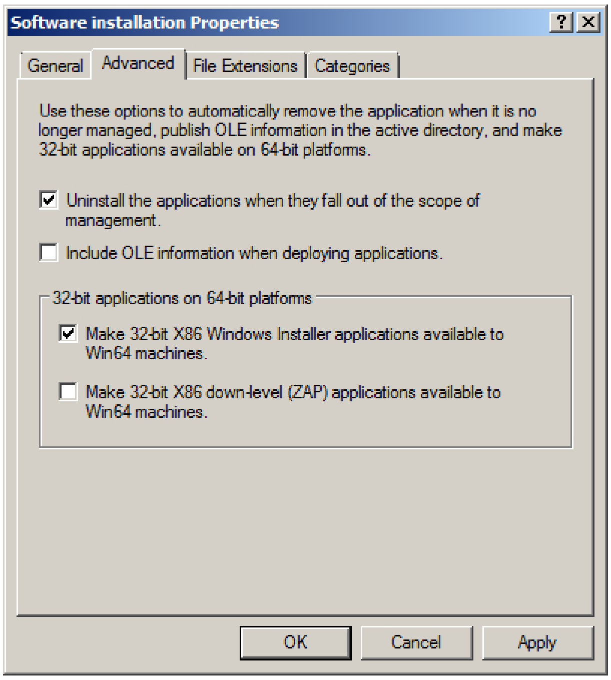
Name	Version	Deployment state	Source
Safe'n'Sec SysWatch	3.10	Assigned	C:\share\SafenSoft_SysWatch.msi

Opens the properties dialog box for the current selection.

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[24]).

To apply changes, click **OK**.



Use these options to automatically remove the application when it is no longer managed, publish OLE information in the active directory, and make 32-bit applications available on 64-bit platforms.

☑ Uninstall the applications when they fall out of the scope of management.

□ Include OLE information when deploying applications.

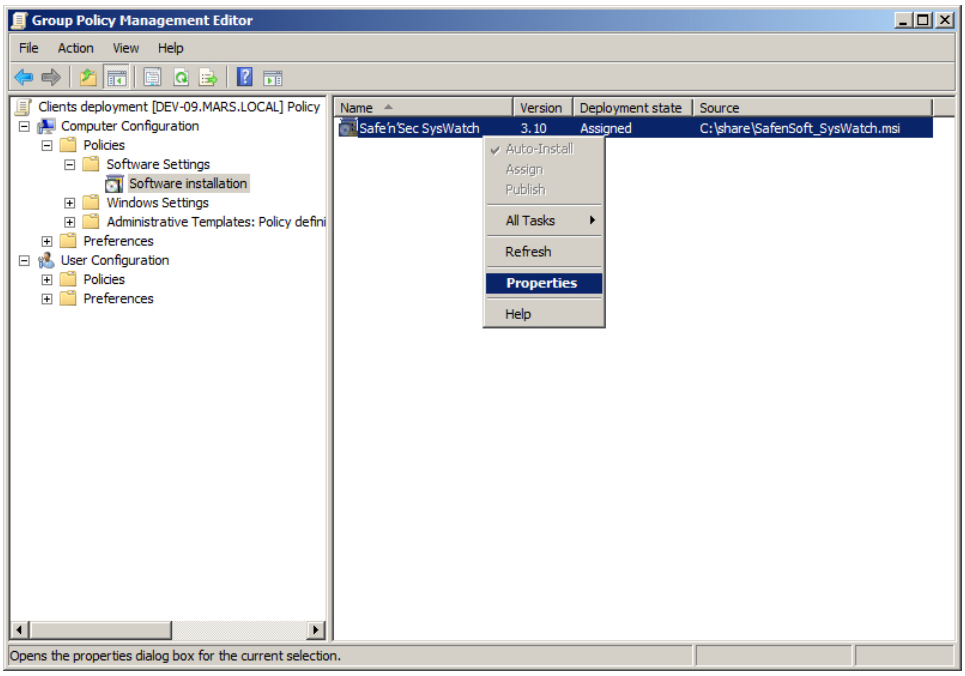
32-bit applications on 64-bit platforms

☑ Make 32-bit X86 Windows Installer applications available to Win64 machines.

□ Make 32-bit X86 down-level (ZAP) applications available to Win64 machines.

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[24]).

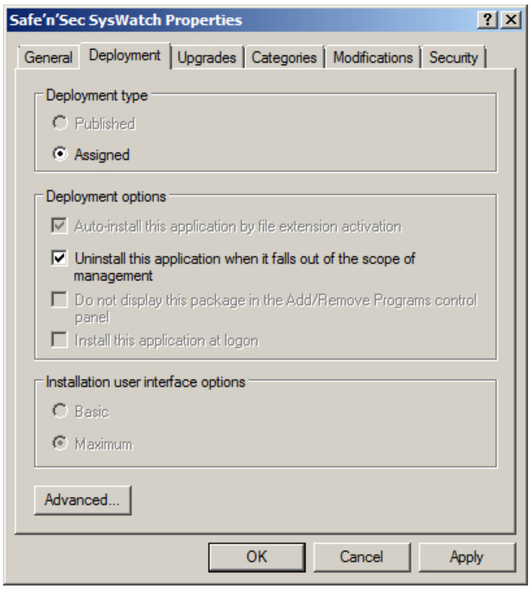


Name	Version	Deployment state	Source
Safe'n'Sec SysWatch	3.10	Assigned	C:\share\SafenSoft_SysWatch.msi

Opens the properties dialog box for the current selection.

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[25]).



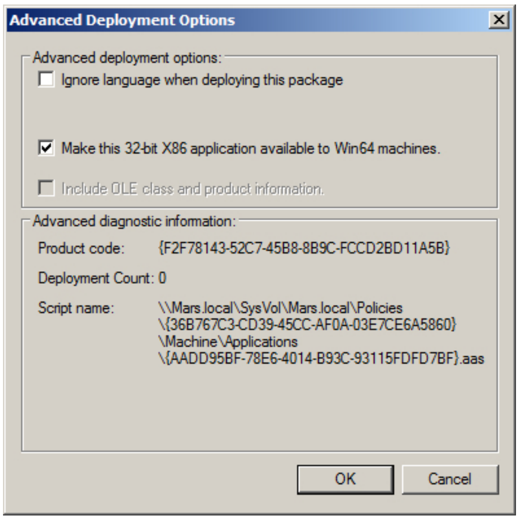
Deployment type
○ Published
● Assigned

Deployment options
☑ Auto-install this application by file extension activation
☑ Uninstall this application when it falls out of the scope of management
□ Do not display this package in the Add/Remove Programs control panel
□ Install this application at logon

Installation user interface options
○ Basic
● Maximum

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[25]). To apply changes, click **OK** in both settings window.



Advanced deployment options:
□ Ignore language when deploying this package
☑ Make this 32-bit X86 application available to Win64 machines.
□ Include OLE class and product information.

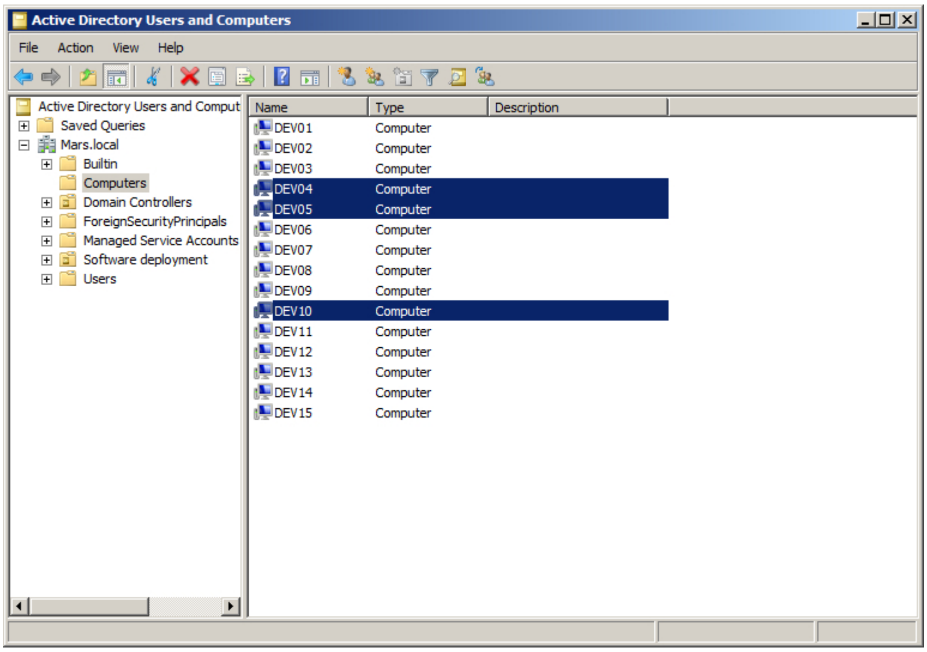
Advanced diagnostic information:
Product code: {F2F78143-52C7-45B8-8B9C-FCCD2BD11A5B}
Deployment Count: 0
Script name: \\Mars.local\SysVol\Mars.local\Policies\{36B767C3-CD39-45CC-AF0A-03E7CE6A5860}\Machine\Applications\{AADD95BF-78E6-4014-B93C-93115FDFD7BF}.aas

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.

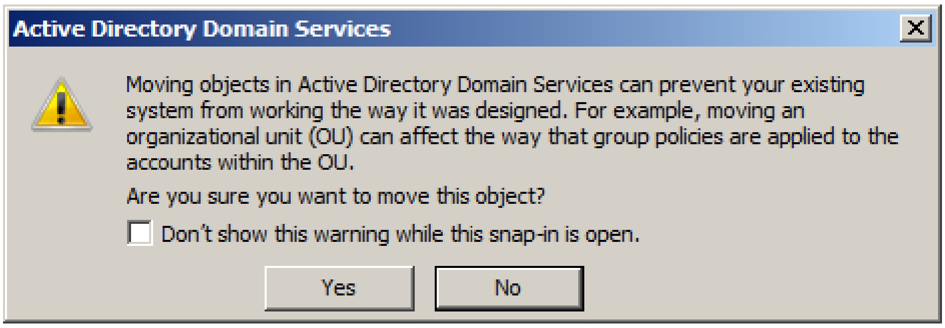
16) Expand the **<domain name>** section and select the **Computers** section (fig. List of the domain hosts 26).



Name	Type	Description
DEV01	Computer	
DEV02	Computer	
DEV03	Computer	
DEV04	Computer	
DEV05	Computer	
DEV06	Computer	
DEV07	Computer	
DEV08	Computer	
DEV09	Computer	
DEV10	Computer	
DEV11	Computer	
DEV12	Computer	
DEV13	Computer	
DEV14	Computer	
DEV15	Computer	

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 26).



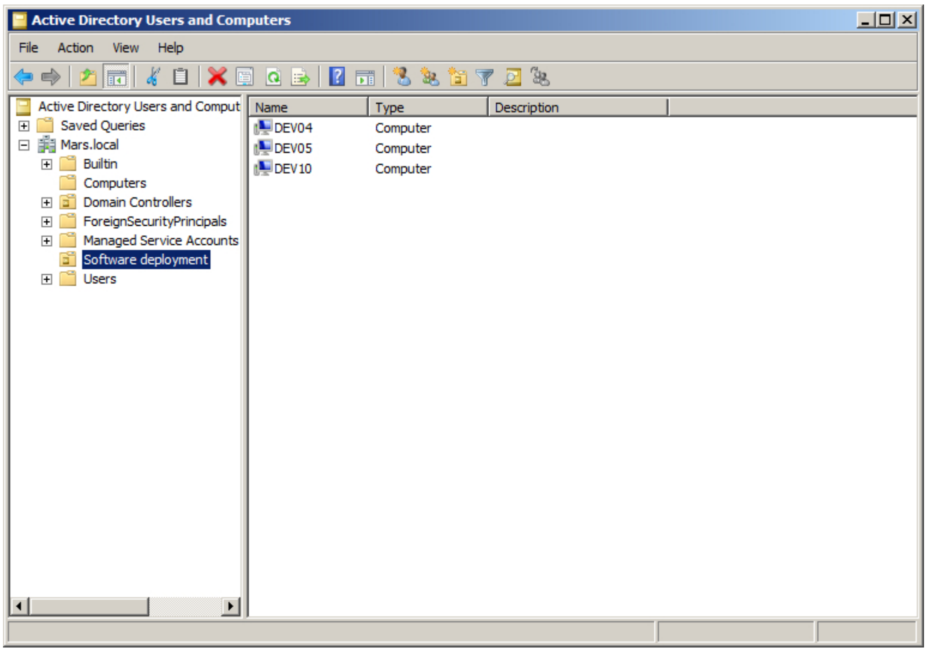
Moving objects in Active Directory Domain Services can prevent your existing system from working the way it was designed. For example, moving an organizational unit (OU) can affect the way that group policies are applied to the accounts within the OU.

Are you sure you want to move this object?

□ Don't show this warning while this snap-in is open.

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 26).



Active Directory Users and Comput
- Saved Queries
- Mars.local
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Managed Service Accounts
  - Software deployment
  - Users

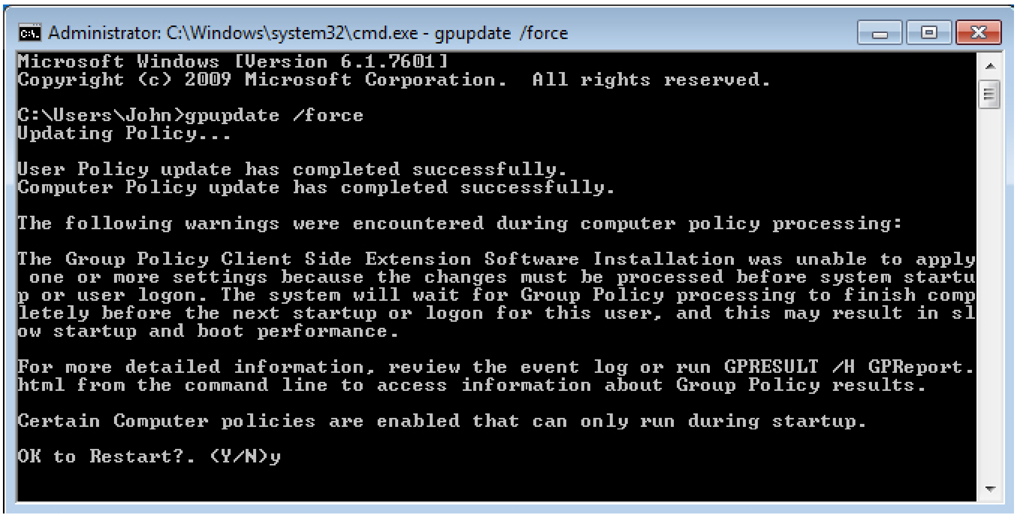
Name	Type	Description
DEV04	Computer	
DEV05	Computer	
DEV10	Computer	

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[27]).


Administrator: C:\Windows\system32\cmd.exe - gpupdate /force

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\John>gpupdate /force
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.

The following warnings were encountered during computer policy processing:

The Group Policy Client Side Extension Software Installation was unable to apply
 one or more settings because the changes must be processed before system startu
p or user logon. The system will wait for Group Policy processing to finish comp
letely before the next startup or logon for this user, and this may result in sl
ow startup and boot performance.

For more detailed information, review the event log or run GPRESULT /H GPReport.
html from the command line to access information about Group Policy results.

Certain Computer policies are enabled that can only run during startup.

OK to Restart?. (Y/N)y
```

Figure 25. Updating the group policy manually

4.2.2 Installing via the remote installation utility

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 intended for remote installation of the ARUDIT SECURITY, LLC client components. Download the utility here: `http://updates.safensoft.com/<license_number>/39/TOOLS/srvrimp.exe`.

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

Installation conditions

- User account with full administrator rights 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 Accounts** → **Change 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** op-

tion in the **HomeGroup Connections** section.

8) Click **Save changes**.

- Inbound 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)** rule 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 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 is necessary to send automatic request for registration 31 to the SoftControl Server after the installation completes. If the file is in the utility

Option	Description
	execution folder, you can specify only the file name (without the quotes).
--hostnames=<name 1> <name 2>... <name N>	List of 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>
```

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>*.

4.2.3 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.

4.3 Registration on the server

SoftControl SysWatch is a client component and can operate 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[40] mode in the program settings.
2) Apply encrypted configuration file[41] with connection to the server settings.
3) Approve registration in SoftControl Admin Console on the **Clients** tab (see the 'SoftControl Service Center administrator's guide' document).

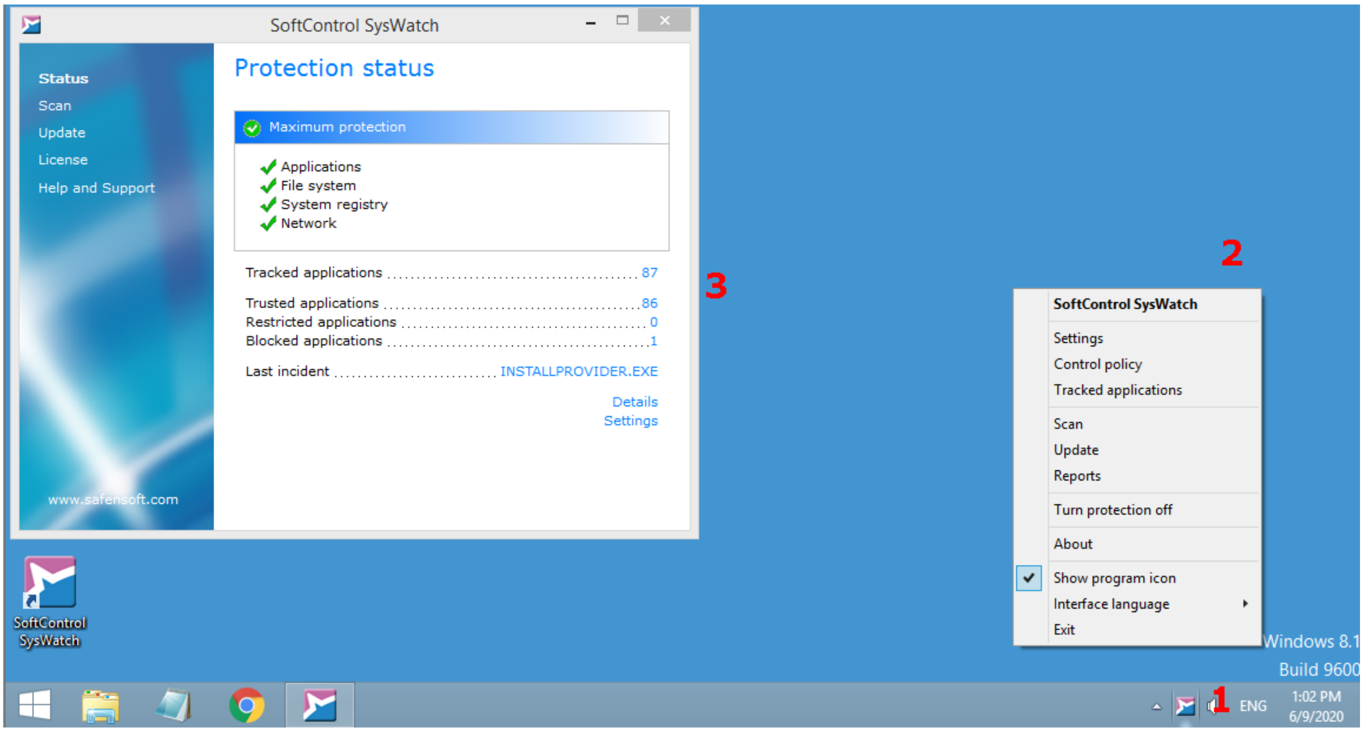
5. Working with SoftControl SysWatch locally

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

5.1 SoftControl SysWatch interface

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

- Program icon in the taskbar notification area [32] (item 1 in fig. below [32]);
- Context menu [33] (item 2 in fig. below [32]);
- Control panel [34] (item 3 in fig. below [32]).


SoftControl SysWatch

Protection status

Maximum protection
- ✓ Applications
- ✓ File system
- ✓ System registry
- ✓ Network

Tracked applications 87
Trusted applications 86
Restricted applications 0
Blocked applications 1
Last incident .... INSTALLPROVIDER.EXE

Windows 8.1
Build 9600

1:02 PM
6/9/2020

Figure 26. Elements of the program GUI

5.1.1 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).

Icon	Program status
	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[33] and the control panel[34]:

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

5.1.2 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[33], while table 6 lists the description of the items.

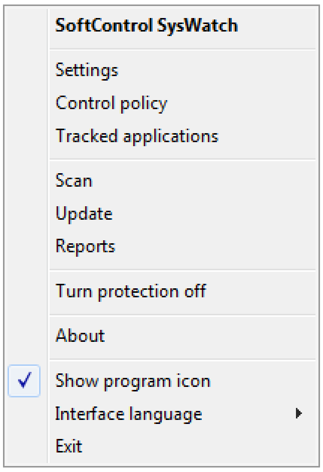


Figure 27. SoftControl SysWatch context menu

Table 6. Description of the SoftControl SysWatch context menu items

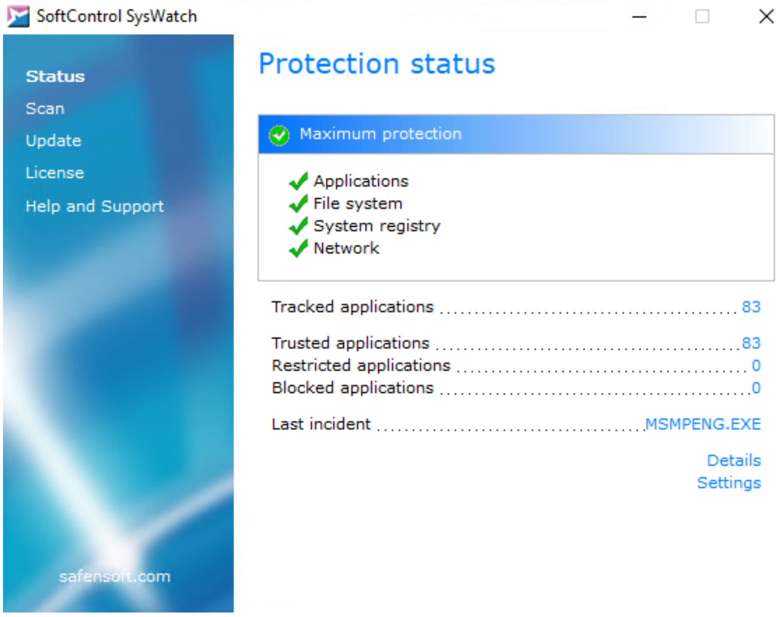
Menu item	Action
SoftControl SysWatch	Open the **Status** tab of the program's control panel.
Settings	Open program settings.
Control policy	Open the **Common rules** tab of the **Control policy** window to view and modify the rules of the applications' access to computer resources and devices, as well to view and modify the rules of network activity.
Tracked applications	Open the **Tracked 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).

5.1.3 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 34). See sections Applications activity control 48 and Control policy 68 for details on this tab.

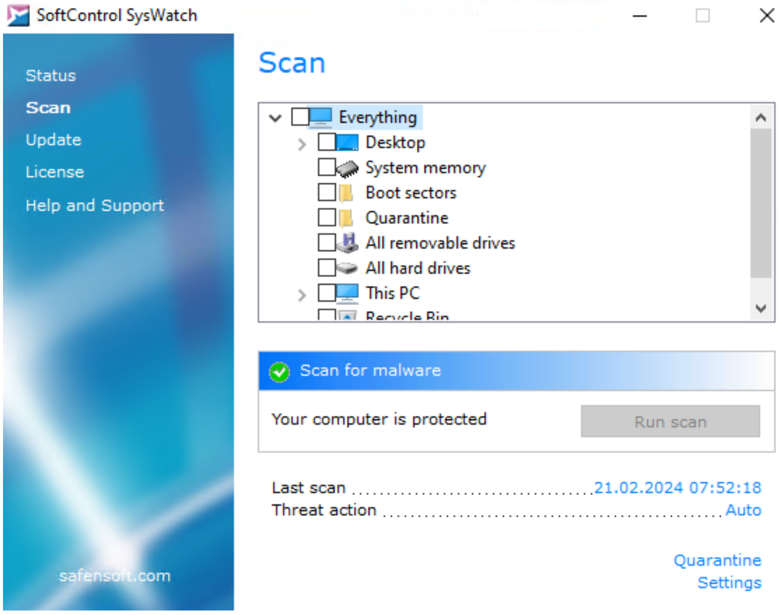


✓ Applications
✓ File system
✓ System registry
✓ Network

Tracked applications 83
Trusted applications 83
Restricted applications 0
Blocked applications 0
Last incident .... MSMPENG.EXE

Figure 28. The 'Status' tab

The **Scan** tab contains the tree of objects to be checked by antivirus on request (fig. The 'Scan' tab 34). See section Antivirus scanning 92 for details.



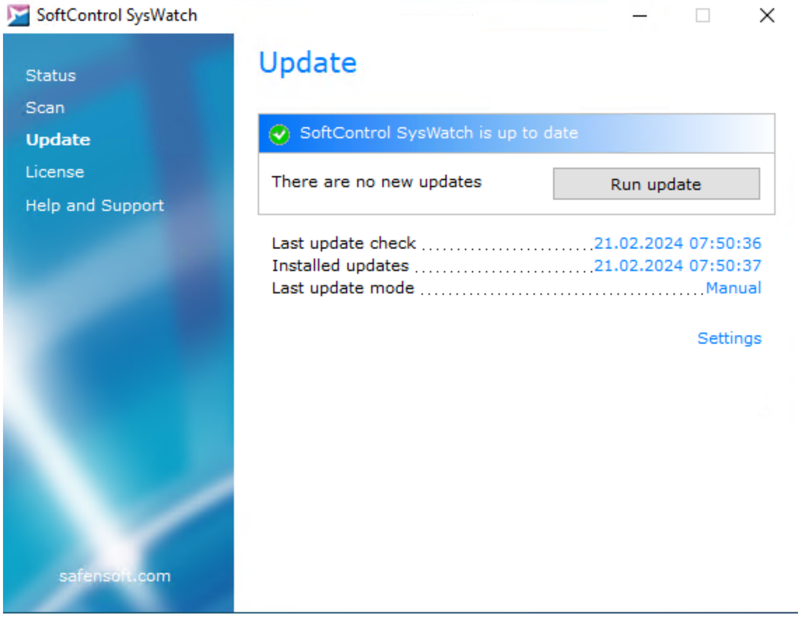
Scan for malware

Your computer is protected

Last scan 21.02.2024 07:52:18
Threat action ....Auto

Figure 29. The 'Scan' tab

The **Update** tab indicates whether any updates of software modules and antivirus bases (114) are available (fig. The 'Update' tab (35)).



SoftControl SysWatch is up to date

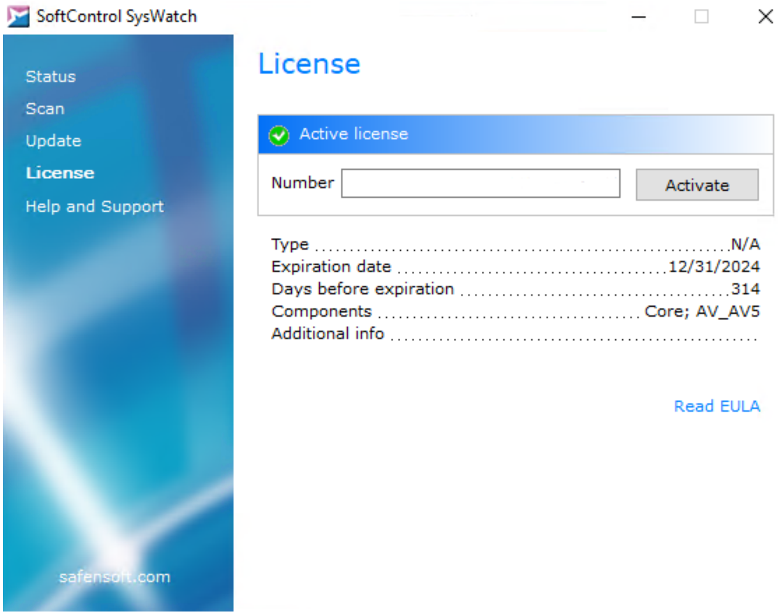
There are no new updates

Last update check 21.02.2024 07:50:36
Installed updates 21.02.2024 07:50:37
Last update mode ....Manual

Figure 30. The 'Update' tab

The **License** tab contains information on the license key (42) that the program uses and the program components (fig. The 'License' tab (35)).

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. The tab is shown in fig. The 'Help and Support' tab (36).



License

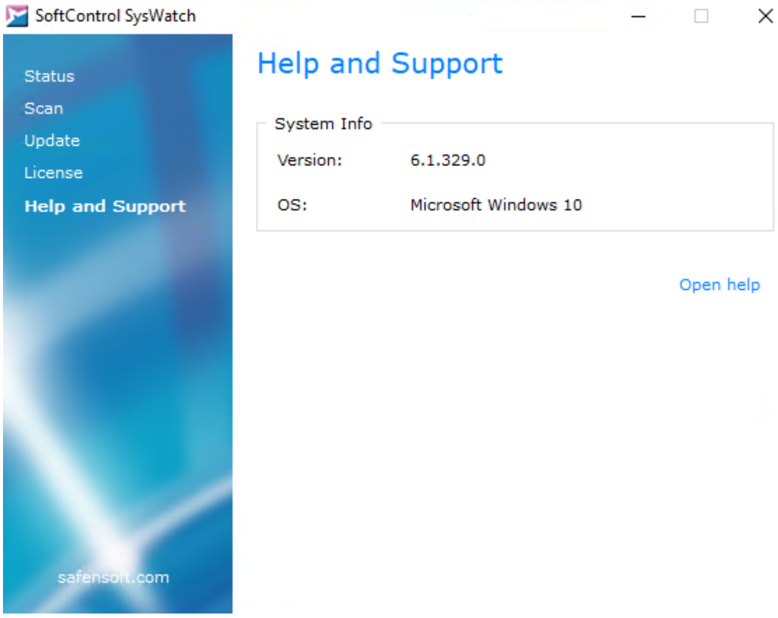
☑ Active license

Number ______ Activate

Type .... N/A
Expiration date 12/31/2024
Days before expiration 314
Components .... Core; AV_AV5
Additional info ....

Read EULA

Figure 31. The 'License' tab



Help and Support

System Info

Version: 6.1.329.0

OS: Microsoft Windows 10

Open help

Figure 32. The 'Help and Support' tab

5.1.4 Interface settings

Setting up the interface

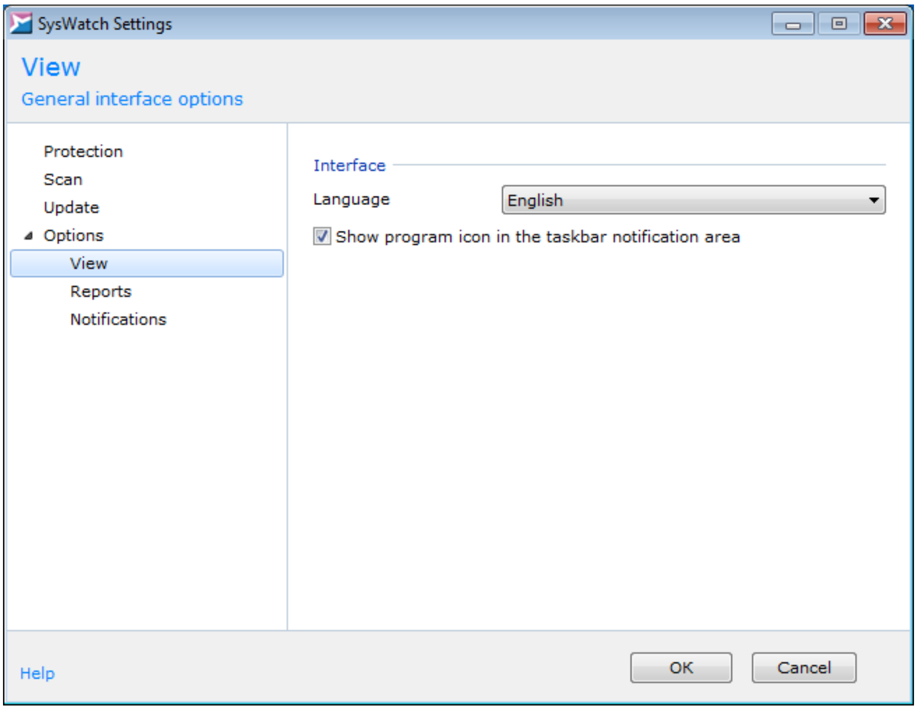
To view and modify SoftControl SysWatch GUI parameters, open program settings and select **Options** → **View** (fig. Interface settings 37).

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

- **English**;

- **Русский** (Russian).

Check **Show program icon in the taskbar notification area** to show the icon[32].



SysWatch Settings

View

General interface options

Interface

Language: English

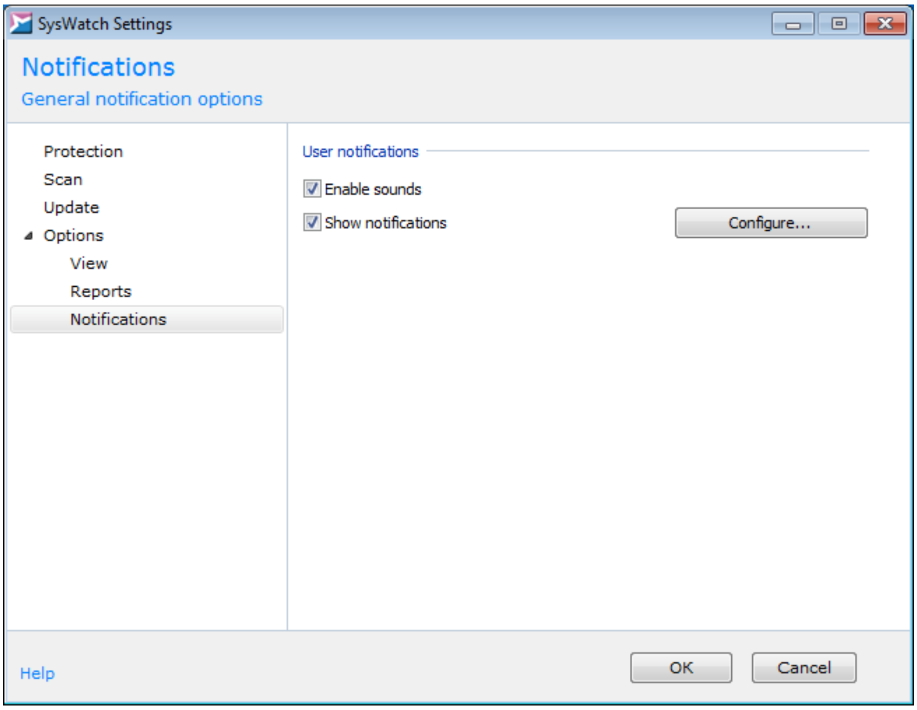
☑ Show program icon in the taskbar notification area

Figure 33. Interface settings

If you uncheck **Show program icon in the taskbar notification area**, you won't be able to open the context menu. To open the control panel in this case, you will have to click twice on the SoftControl SysWatch icon on your desktop.

Setting up local notifications

To specify how the SoftControl SysWatch user is notified about the incidents and the program state, open program settings and select **Options** → **Notifications** (fig. Local notifications settings[37]).


SysWatch Settings

Notifications

General notification options

User notifications

☑ Enable sounds

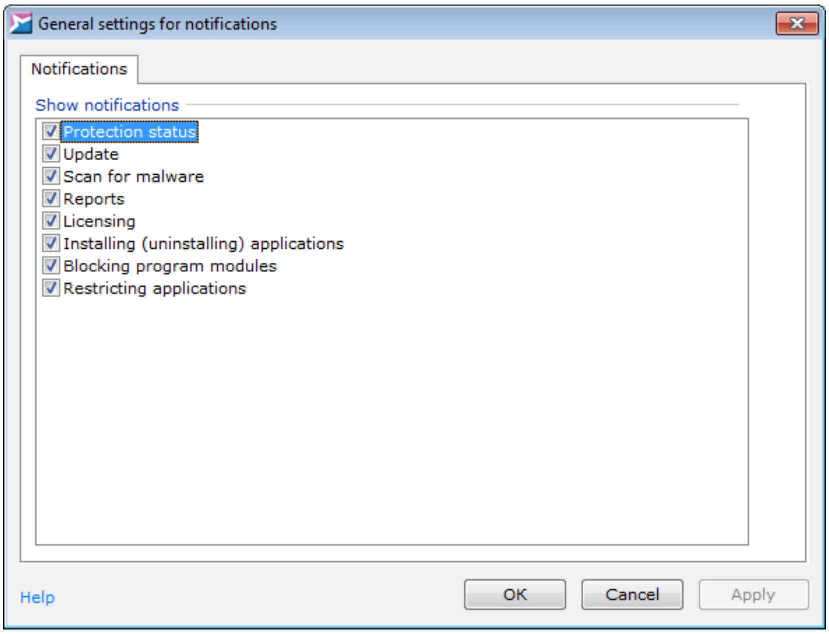
☑ Show notifications

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[38]):

- ❑ **Protection status**;
- ❑ **Update**;
- ❑ **Scan for malware**;
- ❑ **Reports**;
- ❑ **Licensing**;
- ❑ **Installing (uninstalling) applications**;
- ❑ **Blocking program modules**;
- ❑ **Restricting applications**.



General settings for notifications

Notifications

Show notifications

- ☑ Protection status
- ☑ Update
- ☑ Scan for malware
- ☑ Reports
- ☑ Licensing
- ☑ Installing (uninstalling) applications
- ☑ Blocking program modules
- ☑ Restricting applications

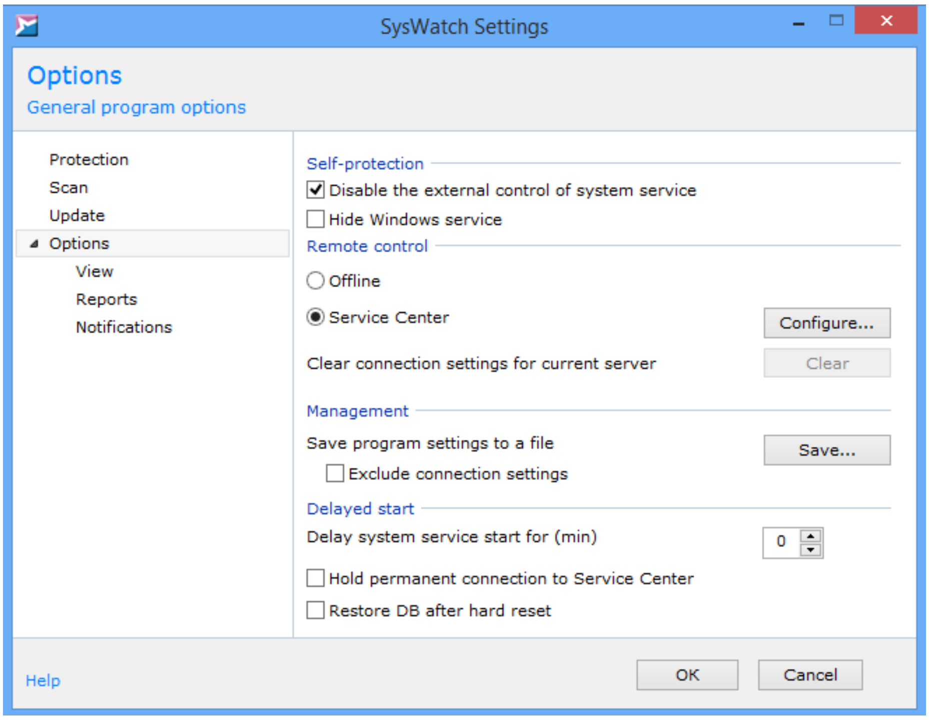
Figure 35. Selecting event types for notifications

Click **OK** to apply changes.

5.2 Management modes

SoftControl SysWatch can be managed in the following modes.

- Stand-alone mode [40];
- Remote control from the server [40].



SysWatch Settings

Options

General program options

- Protection
- Scan
- Update
- Options
  - View
  - Reports
  - Notifications

Self-protection

☑ Disable the external control of system service

□ Hide Windows service

Remote control

○ Offline

● Service Center

Clear connection settings for current server

Management

Save program settings to a file

□ Exclude connection settings

Delayed start

Delay system service start for (min) 0

□ Hold permanent connection to Service Center

□ Restore DB after hard reset

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 **Options** section (fig. Setting up the program parameters [39]). Click **OK** to apply changes.

5.2.1 Stand-alone mode

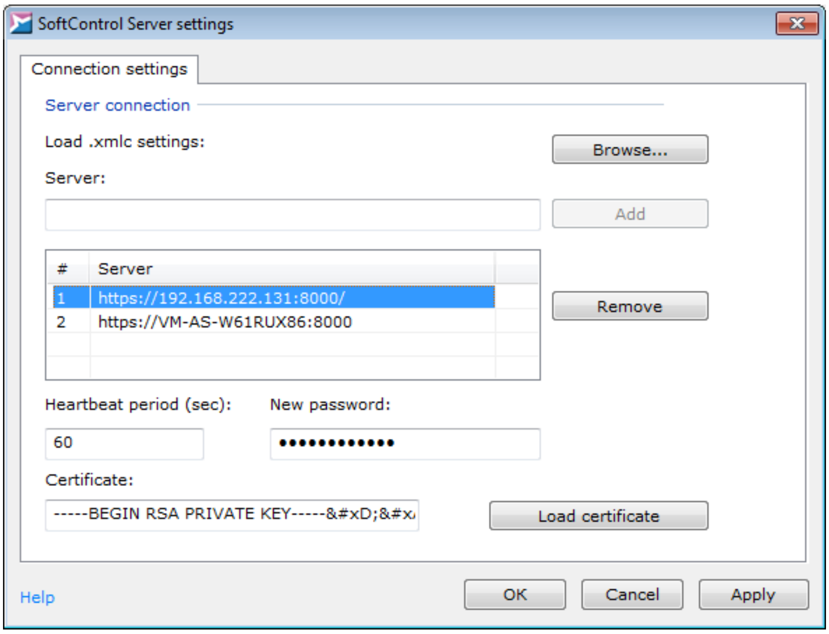
When SoftControl SysWatch operates in the stand-alone mode, the local user sets up the program, runs tasks and processes the incidents with the help of SoftControl SysWatch GUI.

To set this mode, select **Offline** in the program settings (fig. Setting up the program parameters [39]).

5.2.2 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 [39]) and click **Configure** to open the window with the server connection settings (fig. Server connection parameters [40]).



Server connection

Load .xmlc settings:

Server:

#	Server
1	https://192.168.222.131:8000/
2	https://VM-AS-W61RUX86:8000

Heartbeat period (sec): 60

New password: ••••••••••••

Certificate: -----BEGIN RSA PRIVATE KEY-----&#xD;&#x

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 [40]).
3) In the displayed window, select the *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 [40]).

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 [42]). 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 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:

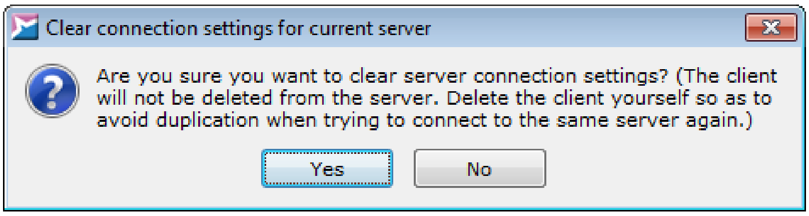
- **Heartbeat period** is the interval between SoftControl SysWatch requests to the controlling server (in seconds);

- **New Password** is the password for SoftControl SysWatch authentication on the controlling server, with the certificate specified 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 **Options** section of the program settings (fig. Setting up the program parameters 39). Select **Yes** in the displayed window (fig. Warning while cleaning the connection settings 42).

SoftControl SysWatch automatically switches to the offline mode after you clear the settings. 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.


Clear connection settings for current server

Are you sure you want to clear server connection settings? (The client will not be deleted from the server. Delete the client yourself so as to avoid duplication when trying to connect to the same server again.)

Figure 38. Warning while cleaning the connection settings

5.3 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-AV4 or AV-AV5) is an extra component that searches for viruses, trojan programs and other malicious objects.

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.

	Note: 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 control panel 34, 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 with the exception that it is not possible to update software modules and antivirus bases. Besides, installing msi packages is not allowed if application activity control is enabled (the **Applications** field in the **Protection status** area is ticked off, see fig. Common protection settings 44).

Two months after the key expires, SoftControl SysWatch displays the corresponding messages on top of other windows. The message is displayed every hour for 10 seconds.

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.

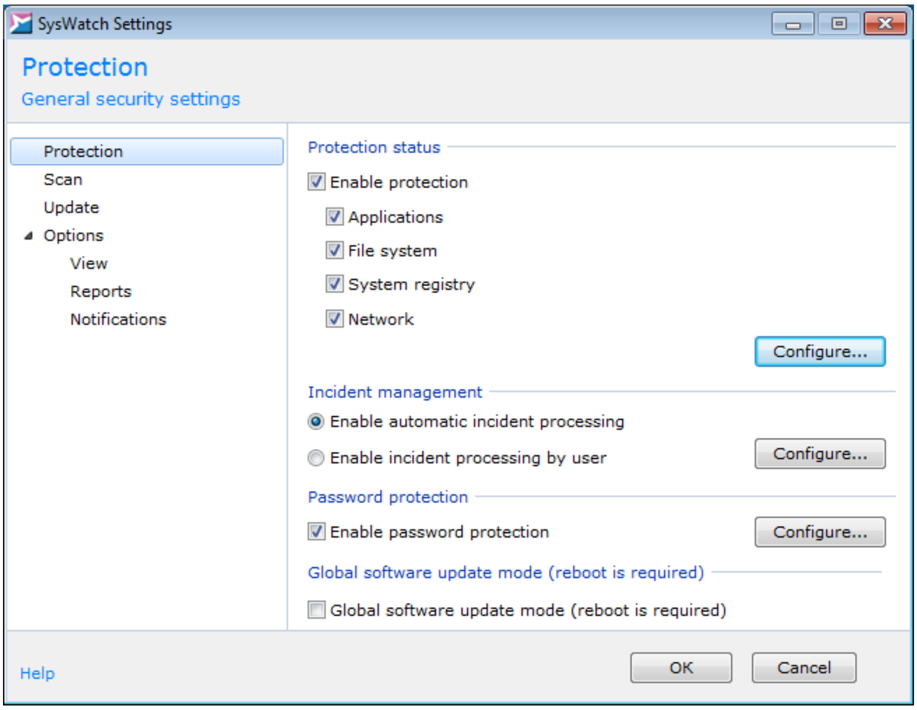
5.4 Automatic setup (profile gathering)

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. The exception is when the **Collect system profile after installation** option is deselected (see fig. Enabling profile collection 15). 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 the 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.

5.4.1 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]).



SysWatch Settings

Protection
General security settings

Protection status
☑ Enable protection
☑ Applications
☑ File system
☑ System registry
☑ Network

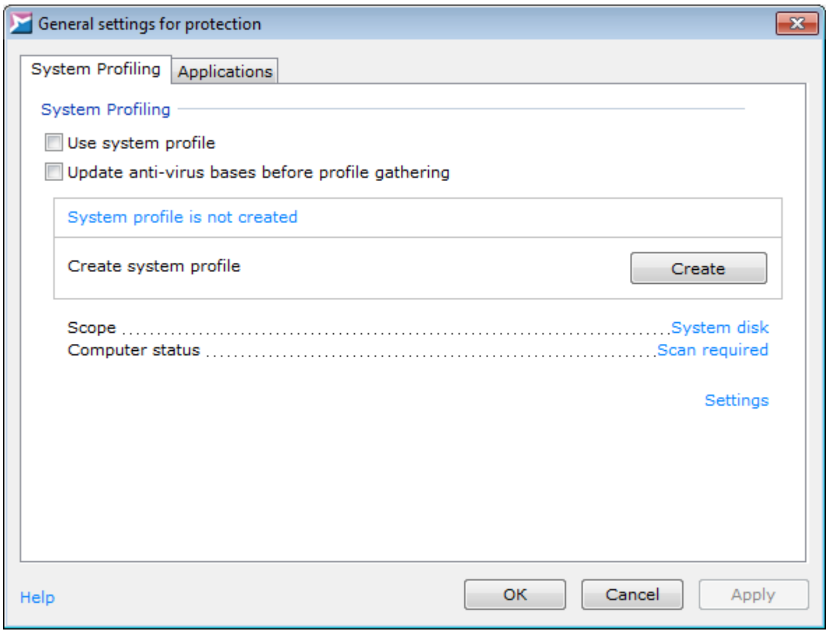
Incident management
● Enable automatic incident processing
○ Enable incident processing by user

Password protection
☑ Enable password protection

Global software update mode (reboot is required)
□ Global software update mode (reboot is required)

Figure 39. Common protection settings

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



General settings for protection

System Profiling
□ Use system profile
□ Update anti-virus bases before profile gathering

System profile is not created

Create system profile

Scope .... System disk
Computer status .... Scan required

Figure 40. Profile gathering window

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

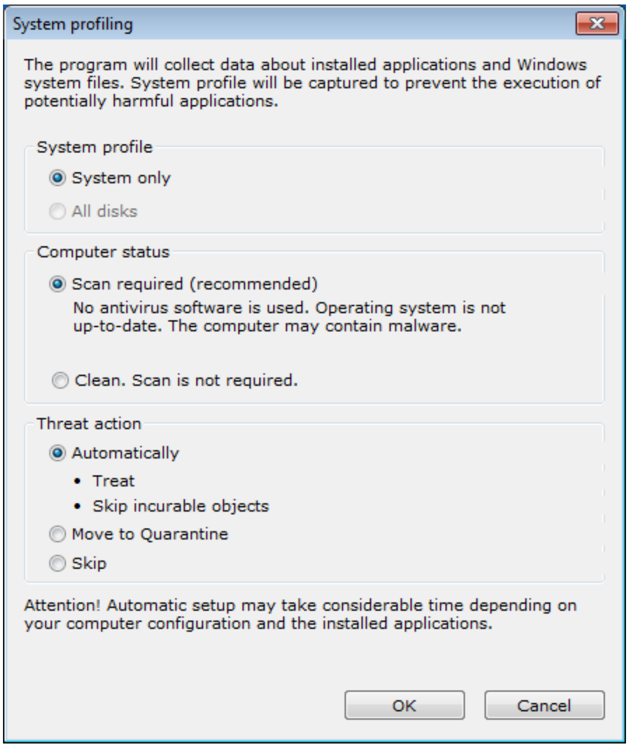
○ **Scan required**

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.

○ **Clean. Scan is not required**

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

Full automatic setup requires more system resources and time than automatic setup without antivirus scanning.



System profiling

The program will collect data about installed applications and Windows system files. System profile will be captured to prevent the execution of potentially harmful applications.

System profile

● System only

○ All disks

Computer status

● Scan required (recommended)

No antivirus software is used. Operating system is not up-to-date. The computer may contain malware.

○ Clean. Scan is not required.

Threat action

● Automatically

- Treat
- Skip incurable objects

○ Move to Quarantine

○ Skip

Attention! Automatic setup may take considerable time depending on your computer configuration and the installed applications.

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):

○ **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**

Do not perform any operations with the infected object.

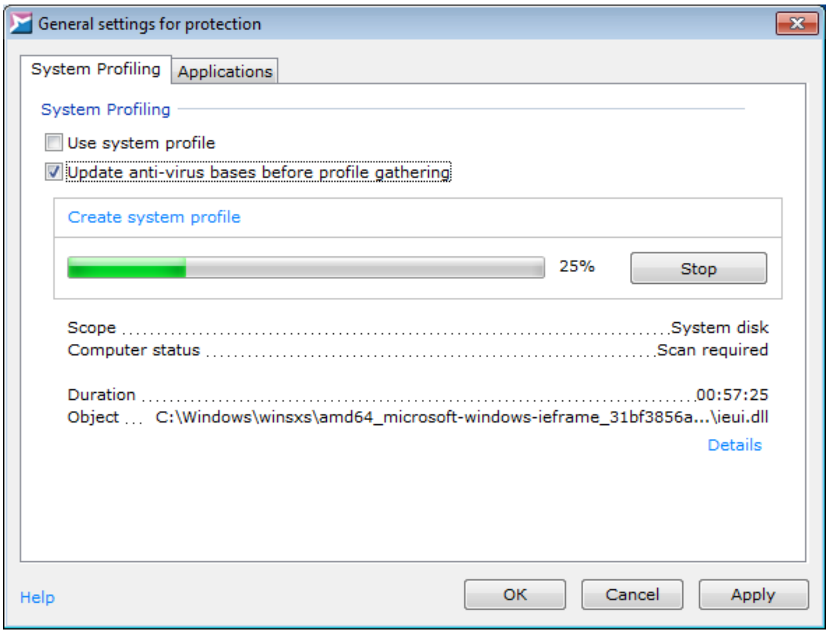
5.4.2 Run on demand

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]).

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]).



□ Use system profile

☑ Update anti-virus bases before profile gathering

25%

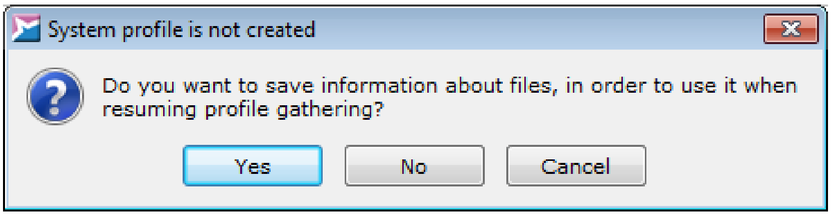
Scope .... System disk
Computer status .... Scan required

Duration 00:57:25
Object ... C:\Windows\winsxs\amd64_microsoft-windows-ieframe_31bf3856a...\ieui.dll

Details

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.



System profile is not created

Do you want to save information about files, in order to use it when resuming profile gathering?

Figure 43. Choosing how to interrupt profile gathering

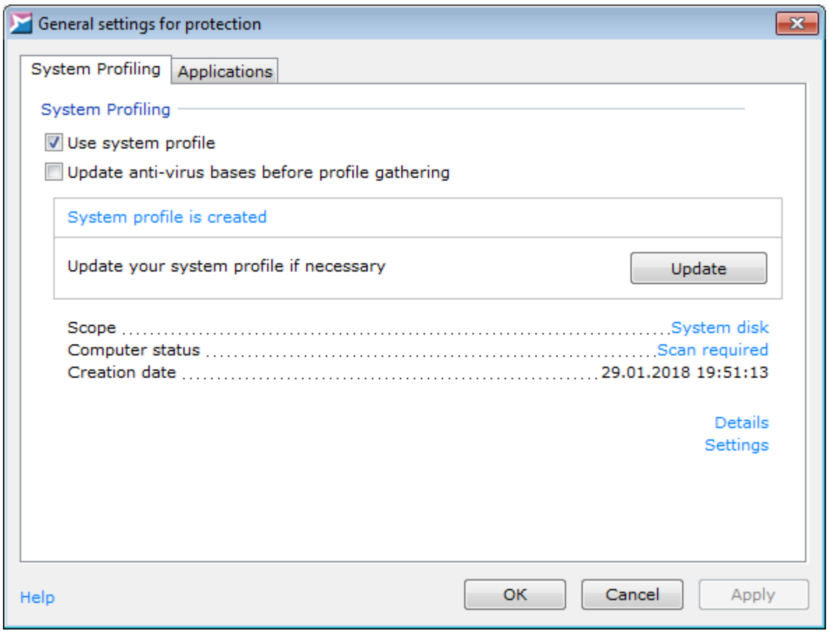
If the *safensec.exe* system service is interrupted during automatic setup, SoftControl SysWatch automatically resumes profile gathering after the service runs again. If the user stops profile gathering with the help of the corresponding button, SoftControl SysWatch does not resume profile gathering 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 system profile** checkbox is ticked off: the program enters the standard mode.

We do not recommend that you deselect **Use system profile** because this turns off the monitoring of PE files.

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[47]).



System Profiling

☑ Use system profile

☐ Update anti-virus bases before profile gathering

System profile is created

Update your system profile if necessary

Scope .... System disk
Computer status .... Scan required
Creation date 29.01.2018 19:51:13

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 47), 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 47).

5.5 Detailed SoftControl SysWatch setup

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

- Running non-profile application;
- Running unsigned installer;
- Control policy violation;
- Loading untrusted DLL;
- Running script engine;
- Modification of PE file by non-installer.

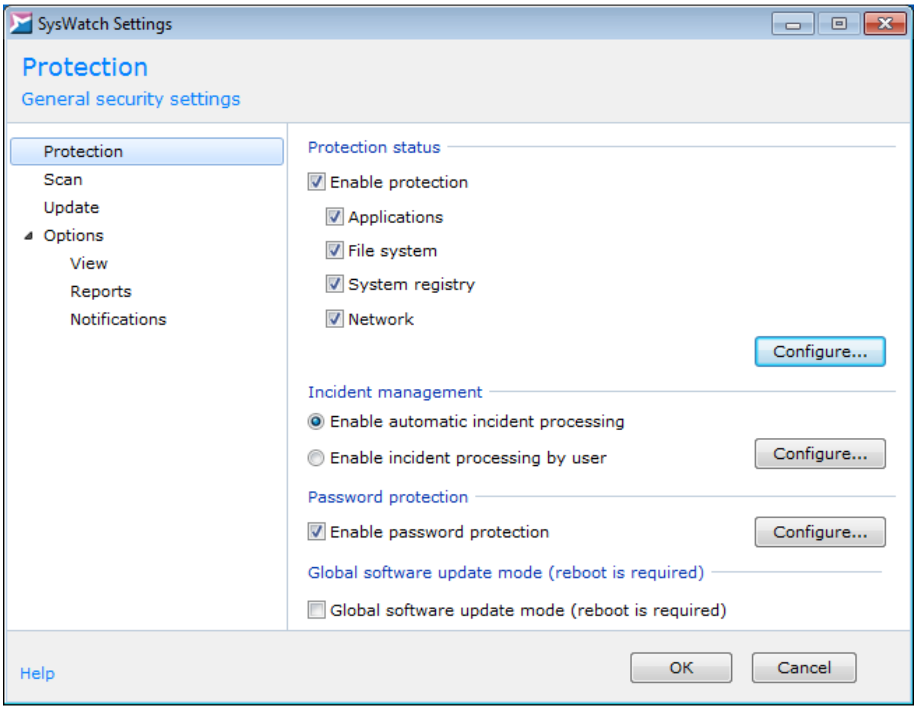
Table 8 lists possible actions for the each category of incidents.

Table 8. **Possible actions when incidents occur**

Incident	Actions
Running non-profile application 56	• **Execute in the restricted mode** The application runs in the isolated environment ('sandbox') under the V.I.P.O. user account with limited permissions. The application is not added to the system profile but is moved to the restricted zone instead. The application can download child modules that are not added to the system profile either. Even if this application is harmful and it installs some extra components, SoftControl SysWatch prevents them from loading. • **Scan and execute in the restricted mode** The application runs in the restricted mode, if no malicious code has been found during the antivirus scanning. Otherwise, the application is blocked. • **Execute in the software update mode** The application runs under current user account without restrictions. The application and all its child modules are moved to the system profile and to the trusted execution zone. • **Scan and execute in the software update mode** The application runs in the software update mode, if no malicious code has been found during the antivirus scanning. Otherwise, the application is blocked. • **Block** The application is blocked.
Running unsigned installer 58	• **Install** The installer runs under current user account without restrictions. The application and all its child modules are moved to the system profile and to the trusted zone after installation. • **Scan and install** The installer runs in the software update mode, if no malicious code has been found during the antivirus scanning. Otherwise, the installer is blocked. • **Install in the restricted mode** The installer runs in the isolated environment ('sandbox') under the V.I.P.O. user account with limited permissions. The installer is not added to the system profile. • **Scan and install in the restricted mode** The installer runs in the restricted mode, if no malicious code has been found during the antivirus scanning. Otherwise, the installer is blocked. • **Block** The installer is blocked.
Control policy violation 68	• **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** 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**

Incident	Actions
	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.
Loading untrusted DLL 52	• **Allow** Allow loading without restrictions. • **Block** Block loading.
Running script engine 51	• **Allow** Allow script engine running without restrictions. • **Block** Block script engine running.
Modification of PE file by non-installer 52	• **Allow** Allow modification of a portable executable file. • **Block** Block modification.

Current protection status and the list of the monitoring scopes are displayed in the **Status** tab of the program's control panel 34. The tab also displays statistics about the total number of applications SoftControl SysWatch has registered, the number of applications in each of the execution zones 59 and the name of the application that caused the last incident. By default, monitoring is established over all control scopes (the *Maximum protection* status is displayed). You can enable or disable monitoring for each of the scopes by left-clicking the scope name. The overall protection status then changes to *Limited protection* if you disable monitoring for at least one scope, and to *Computer is not protected* if you disable monitoring for all scopes. These features are duplicated in the program settings in the **Protection** section (fig. General protection settings 50). SoftControl SysWatch monitors the applications' activity when the **Applications** scope is ticked off.



Protection

General security settings

Protection status

☑ Enable protection

☑ Applications

☑ File system

☑ System registry

☑ Network

Configure...

Incident management

● Enable automatic incident processing

○ Enable incident processing by user

Configure...

Password protection

☑ Enable password protection

Configure...

Global software update mode (reboot is required)

☐ Global software update mode (reboot is required)

Figure 45. General protection settings

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

- activity control options 51;
- handling the application start incidents 54;
- application execution zones 59;
- properties of certain applications 61;
- whitelist of certificates 66.

5.5.1 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. General protection settings 50), and go to the **Applications** tab of the **General settings for protection** window (fig. Activity control options 53).

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

□ **Save activity history for untracked applications and installers**:

Automatically enable the activity history saving option 64 when an application that is not in the profile or an unsigned installer runs for the first time.

□ **Disable execution of scripts**:

Block the execution of untrustworthy scripts by the interpreters (except for the scripts that are signed with a digital signature from the whitelist of certificates[66]). The following processes are blocked:

– wscript.exe (Microsoft ® Windows Based Script Host);

– cscript.exe (Microsoft ® Console Based Script Host);

– java.exe (Java™ Platform SE binary);

– javaw.exe (Java™ Platform SE binary);

– javaws.exe (Java™ Web Start Launcher).

In order to block specific processes, we recommend that you create the appropriate Control policy rules[68].

Note. If you select **Allow** for **Running script engine** in the **Incident management** section, the script execution will not be disabled. The event will be logged.

❑ **All script engines are located in the system directory**:

Only processes started from a system directory (`C:\Windows\System32` or `C:\Windows\SysWOW64`) are blocked.

This option becomes active if **Disable execution of scripts** is checked.

❑ **Enable dll module control (reboot is required)**:

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

DLL module control works as follows. When an exe file tries to load a dll library, SoftControl SysWatch checks whether the library has a digital signature. If the library is signed and the digital signature certificate is considered trusted by Windows, SoftControl SysWatch allows the library to load, even if the library is not in the profile. If the library has no digital signature, SoftControl SysWatch checks whether it is in the profile. If the library is in the profile, SoftControl SysWatch allows it to load; otherwise, SoftControl SysWatch blocks it.

Note 1. Libraries that do not have an entry point (resource-only libraries without executable code) cannot be blocked.

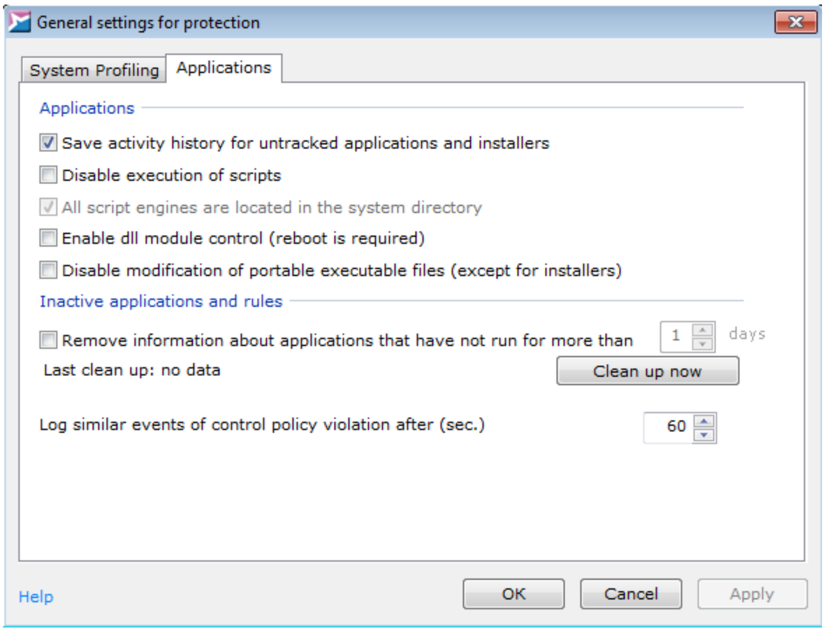
Note 2. If you select **Allow** for **Loading untrusted DLL** in the **Incident management** section, the loading will not be blocked. The event will be logged.

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

Block modification of the executable files (exe, dll, etc.) by all applications except for the applications that work in the software update mode. The options allows reducing the risks of the system integrity violation.

Note. If you select **Allow** for **Modification of PE file by non-installer** in the **Incident man-**

agement section, the file modification will not be blocked. The event will be logged.



Applications

☑ Save activity history for untracked applications and installers

□ Disable execution of scripts

☑ All script engines are located in the system directory

□ Enable dll module control (reboot is required)

□ Disable modification of portable executable files (except for installers)

Inactive applications and rules

□ Remove information about applications that have not run for more than 1 days

Last clean up: no data

Log similar events of control policy violation after (sec.) 60

Figure 46. Activity control options

To delete entries about inactive applications from the SoftControl SysWatch database, tick off the **Remove information about applications that have not run for more than** checkbox in the **Inactive applications** area and specify the required number of days. To delete data immediately, click **Clean up now**. To save information about the application activity, tick **Save application history since** (see figure below[64]).

To modify the period of time after which SoftControl SysWatch starts logging similar events, specify the required value in the **Log similar events of control policy violation after (sec.)** field (60 seconds by default). Control policy violation events are considered *similar* and are not logged if the following conditions are met at the same time.

- the following parameters coincide for the events:
  - activity types;
  - programs that are the sources of the incidents;
  - the files being controlled;
  - process identifiers (PIDs);
- period of time after the previous event has been added is less than the specified value.

The text log contains information about how many similar events have been skipped.

SoftControl SysWatch features the global software update mode to support the execution of the multistage installers. When this mode is active, all applications run as installers and are added to the profile (education mode). All modifications of the PE files are added to the profile as well. To enable the mode, open the **Protection** section of the program settings, tick off **Global software update mode (reboot is recommended)** (fig. General protection settings[50]) and restart the system. Besides, you can manage the global software update mode in silent mode, with the help of the additional changetpsmode utility[112].

To prevent SoftControl SysWatch from adding malicious code to the profile, we recommend that you only use the **Global software update mode** option on 'clean' systems, where all software has been installed from a master image.

To disable the mode, deselect **Global software update mode (reboot is recommended)** and restart the system.

5.5.2 Handling the application start incidents

Figure below[54] shows how SoftControl SysWatch reacts when applications that are not in the profile run on the client host.

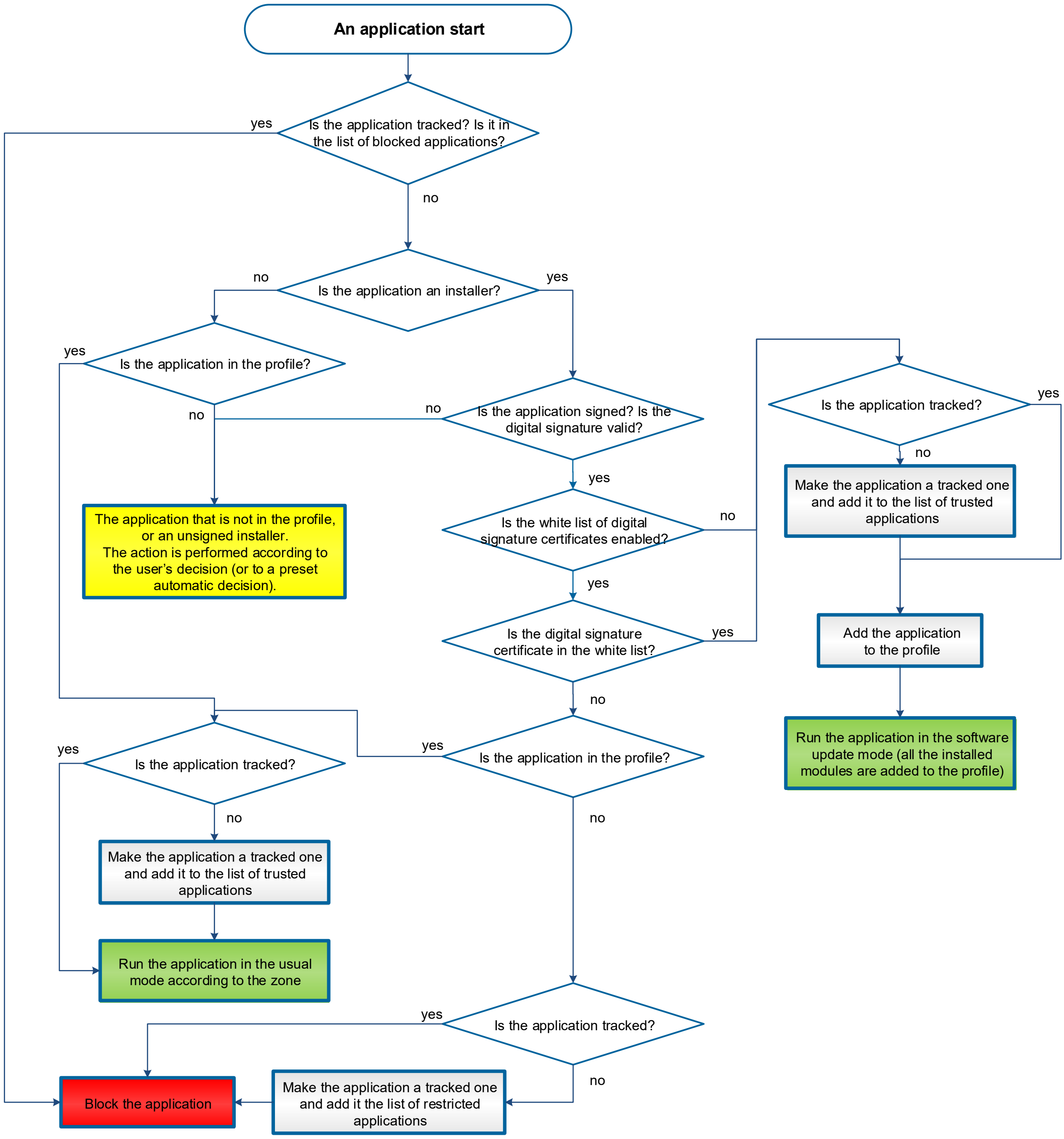
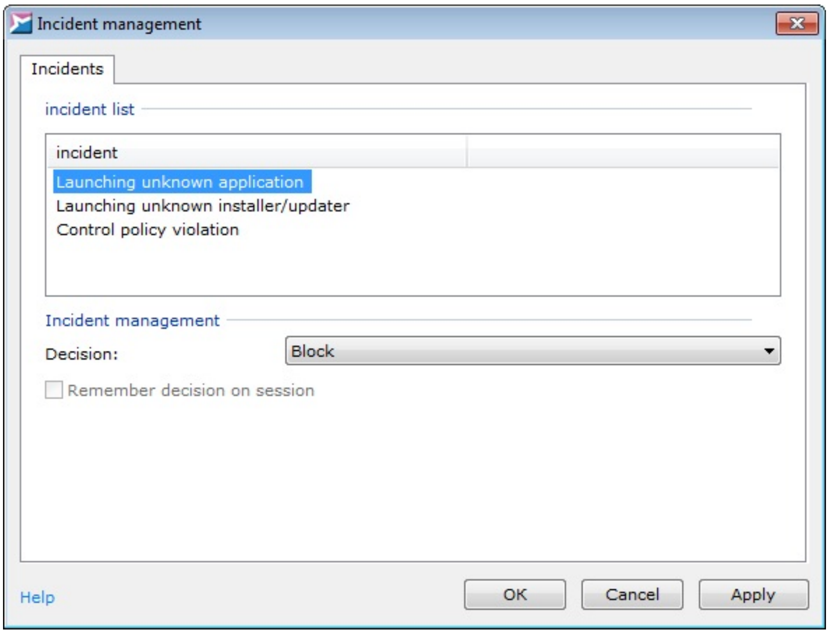

An application start
Is the application tracked? Is it in the list of blocked applications?
yes
no
Is the application an installer?
no
yes
Is the application in the profile?
yes
no
Is the application signed? Is the digital signature valid?
no
yes
The application that is not in the profile, or an unsigned installer.
The action is performed according to the user's decision (or to a preset automatic decision).
Is the white list of digital signature certificates enabled?
no
yes
Is the digital signature certificate in the white list?
yes
no
Is the application tracked?
yes
no
Make the application a tracked one and add it to the list of trusted applications
Add the application to the profile
Run the application in the software update mode (all the installed modules are added to the profile)
Is the application tracked?
yes
no
Make the application a tracked one and add it to the list of trusted applications
Run the application in the usual mode according to the zone
Is the application in the profile?
yes
no
Is the application tracked?
yes
no
Block the application
Make the application a tracked one and add it the list of restricted applications

Figure 47. How SoftControl SysWatch handles the start of an application that is not in the profile

The final *decision* (fig. above [54]) 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 to the **Protection** section of the program settings, switch **Incident management** to **Enable automatic incident processing** and click **Configure** (fig. General protection settings [50]). Select the required event type in the **Incident list** of the **Incidents management** window (fig. Setting up the incident processing[56]), 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[49].


Incident management

Incidents

incident list

incident
Launching unknown application
Launching unknown installer/updater
Control policy violation

Incident management

Decision: Block

□ Remember decision on session

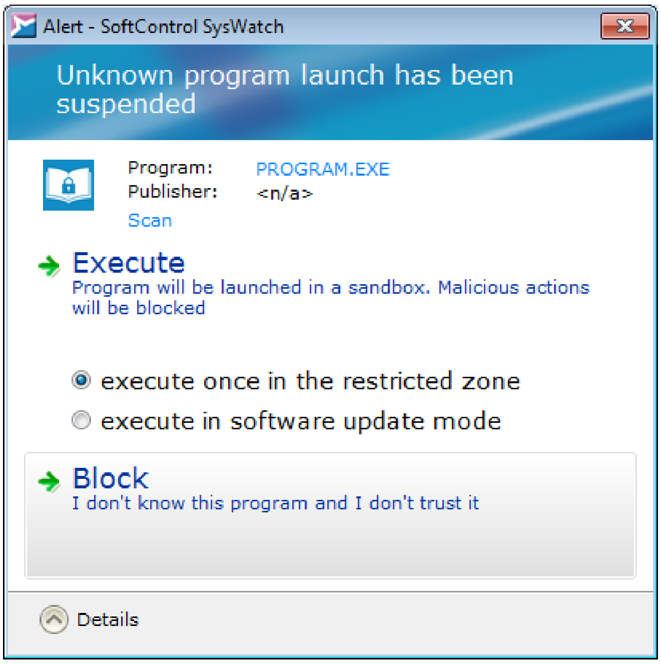
Figure 48. Setting up the incident processing

- **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[50]).

Running non-profile application

Fig. Warning for a non-profile application[56] shows the warning that is displayed when an application that is not in the profile runs.



Alert - SoftControl SysWatch

Unknown program launch has been suspended

Program: PROGRAM.EXE
Publisher: <n/a>
Scan

Execute
Program will be launched in a sandbox. Malicious actions will be blocked

● execute once in the restricted zone
○ execute in software update mode

Block
I don't know this program and I don't trust it

Details

Figure 49. Warning for a non-profile application

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

- Application description area. The area contains information about the non-profile application: the name, the vendor, and the antivirus scan[92] result (you can check the application before you make the decision by clicking the **Scan** link and selecting **Scan...** in the context menu).
- Action selection area. The area contains possible actions when the non-profile application runs:
  - → **Execute**
    - ○ **execute in the restricted mode** – execute the application in the isolated environment ('sandbox') under the V.I.P.O. user account with limited permissions;
    - ○ **execute in the software update mode** – execute the application and add it to the system profile.

> We recommend that you select this action only if you are sure that it will not harm the system.

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

> 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.

Running unsigned installer

Fig. Warning for an unsigned installer[58] shows the warning that is displayed when an unsigned installer runs.

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

- Installer description area. The area contains information about the unsigned installer: the name, the vendor, and the antivirus scan[92] result (you can check the installer before you make the decision by clicking the **Scan** link and selecting **Scan...** in the context menu).
- Action selection area. The area contains possible actions when an unsigned installer runs:

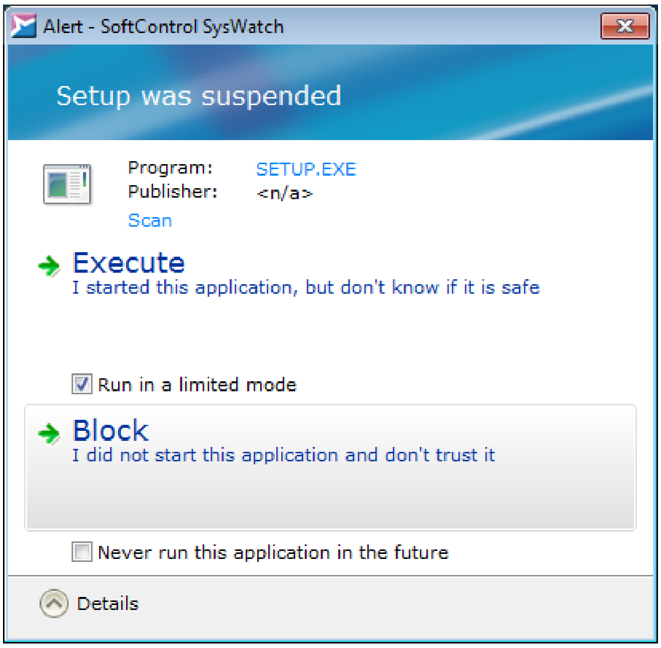
→ **Execute** – run the installer and add it and all the installed modules to the system profile;

> We recommend that you select this action only if you are sure that it will not harm the system.

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

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

> 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.



Alert - SoftControl SysWatch

Setup was suspended

Program: SETUP.EXE
Publisher: <n/a>
Scan

Execute
I started this application, but don't know if it is safe

☑ Run in a limited mode

Block
I did not start this application and don't trust it

☐ Never run this application in the future

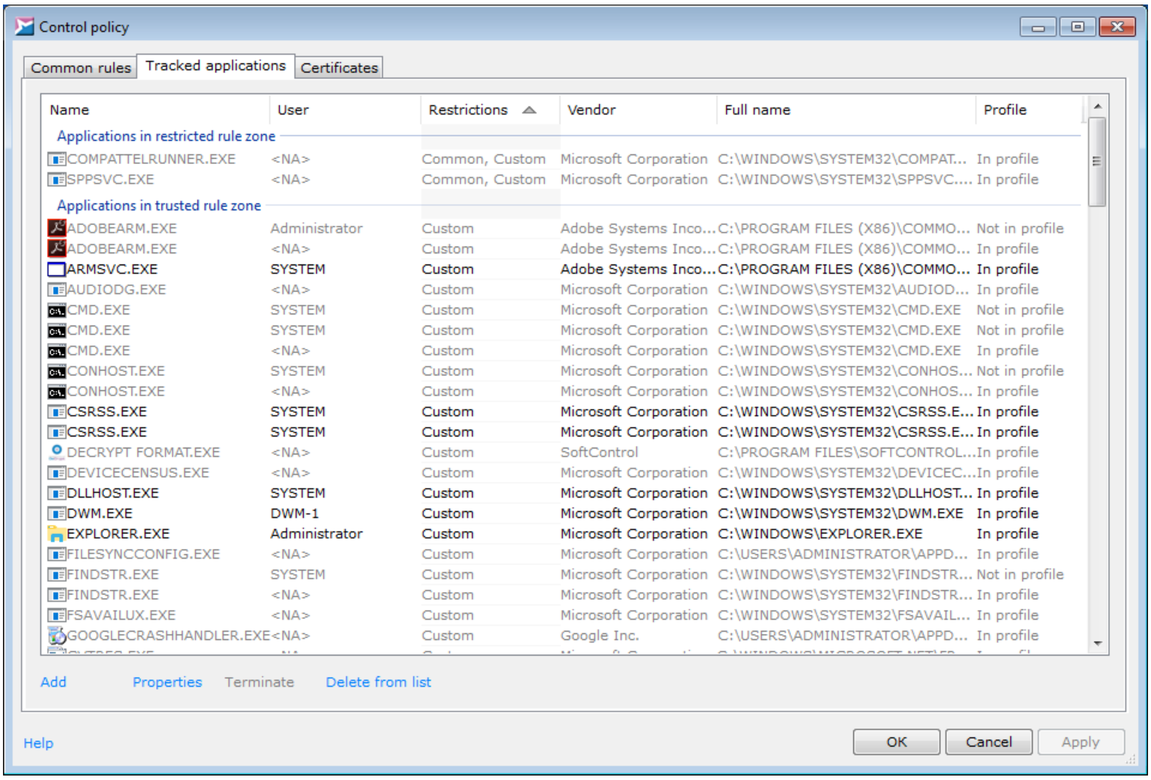
Details

Figure 50. Warning window for unsigned installer

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

5.5.3 Application execution zones

To view and modify the distribution of the applications among the execution zones, select **Tracked applications** in the SoftControl SysWatch context menu [33]. The **Tracked applications** tab of the **Control policy** window displays all applications registered by SoftControl SysWatch after it was installed (fig. Processes and applications [59]).



Name	User	Restrictions	Vendor	Full name	Profile
Applications in restricted rule zone					
COMPATTELRUNNER.EXE	<NA>	Common, Custom	Microsoft Corporation	C:\WINDOWS\SYSTEM32\COMPAT...	In profile
SPPSVC.EXE	<NA>	Common, Custom	Microsoft Corporation	C:\WINDOWS\SYSTEM32\SPPSVC....	In profile
Applications in trusted rule zone					
ADOBEARM.EXE	Administrator	Custom	Adobe Systems Inco...	C:\PROGRAM FILES (X86)\COMMO...	Not in profile
ADOBEARM.EXE	<NA>	Custom	Adobe Systems Inco...	C:\PROGRAM FILES (X86)\COMMO...	In profile
ARMSVC.EXE	SYSTEM	Custom	Adobe Systems Inco...	C:\PROGRAM FILES (X86)\COMMO...	In profile
AUDIODG.EXE	<NA>	Custom	Microsoft Corporation	C:\WINDOWS\SYSTEM32\AUDIOD...	In profile
CMD.EXE	SYSTEM	Custom	Microsoft Corporation	C:\WINDOWS\SYSTEM32\CMD.EXE	Not in profile
CMD.EXE	SYSTEM	Custom	Microsoft Corporation	C:\WINDOWS\SYSTEM32\CMD.EXE	Not in profile
CMD.EXE	<NA>	Custom	Microsoft Corporation	C:\WINDOWS\SYSTEM32\CMD.EXE	In profile
CONHOST.EXE	SYSTEM	Custom	Microsoft Corporation	C:\WINDOWS\SYSTEM32\CONHOS...	Not in profile
CONHOST.EXE	<NA>	Custom	Microsoft Corporation	C:\WINDOWS\SYSTEM32\CONHOS...	In profile
CSRSS.EXE	SYSTEM	Custom	Microsoft Corporation	C:\WINDOWS\SYSTEM32\CSRSS.E...	In profile
CSRSS.EXE	SYSTEM	Custom	Microsoft Corporation	C:\WINDOWS\SYSTEM32\CSRSS.E...	In profile
DECRYPT FORMAT.EXE	<NA>	Custom	SoftControl	C:\PROGRAM FILES\SOFTCONTROL...	In profile
DEVICECENSUS.EXE	<NA>	Custom	Microsoft Corporation	C:\WINDOWS\SYSTEM32\DEVICEC...	In profile
DLLHOST.EXE	SYSTEM	Custom	Microsoft Corporation	C:\WINDOWS\SYSTEM32\DLLHOST...	In profile
DWM.EXE	DWM-1	Custom	Microsoft Corporation	C:\WINDOWS\SYSTEM32\DWM.EXE	In profile
EXPLORER.EXE	Administrator	Custom	Microsoft Corporation	C:\WINDOWS\EXPLORER.EXE	In profile
FILESYNCCONFIG.EXE	<NA>	Custom	Microsoft Corporation	C:\USERS\ADMINISTRATOR\APPD...	In profile
FINDSTR.EXE	SYSTEM	Custom	Microsoft Corporation	C:\WINDOWS\SYSTEM32\FINDSTR...	Not in profile
FINDSTR.EXE	<NA>	Custom	Microsoft Corporation	C:\WINDOWS\SYSTEM32\FINDSTR...	In profile
FSAVAILUX.EXE	<NA>	Custom	Microsoft Corporation	C:\WINDOWS\SYSTEM32\FSAVAIL...	In profile
GOOGLECRASHHANDLER.EXE	<NA>	Custom	Google Inc.	C:\USERS\ADMINISTRATOR\APPD...	In profile

Figure 51. Tracked 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 application identifier in the system.
- **Status** is the application state:
  - **Running** means the active process; the application is currently running (the name is in black color);
  - inactive process; the application isn't currently running (the name is in gray color).
- **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**;
  - **Profile is off**;
  - **Profile is not created**;
  - **File not found**.

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 [61] 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 [47], right-click the required application to invoke the context menu and select one of the options:

- **Add to profile**;
- **Remove from profile**.

This option is only available if both of the following options are ticked off: **Use system profile** (fig. Profile gathering window [44]) and **Applications** in the **Protection status** area (fig. Common protection settings [44]).

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

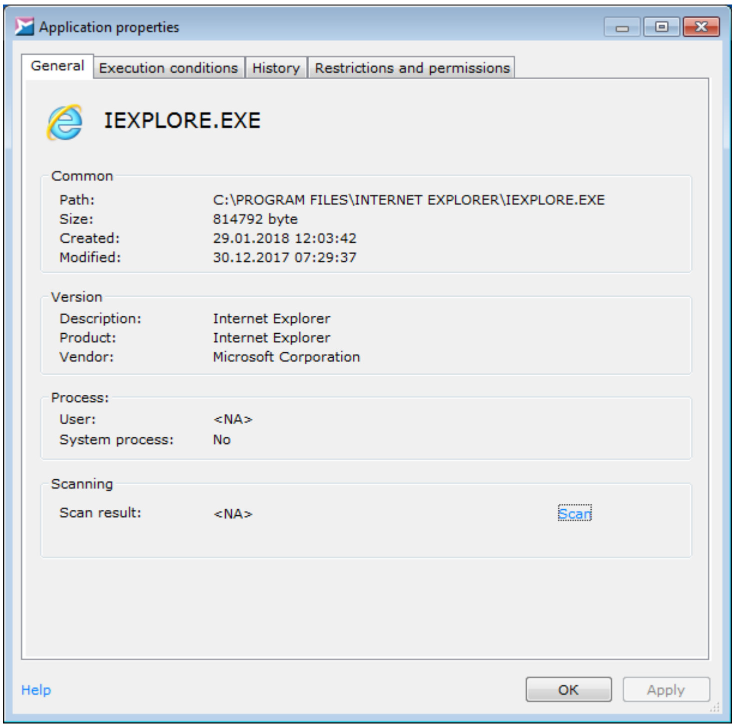
If the application is running, you can interrupt the process by selecting the required application from the list and clicking **Terminate**. To **Delete application file on reboot**, invoke the context menu and select the corresponding command.

5.5.4 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 application context menu on the Processes and applications [59] 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 62).



IEXPLORE.EXE

Common
Path: C:\PROGRAM FILES\INTERNET EXPLORER\IEXPLORE.EXE
Size: 814792 byte
Created: 29.01.2018 12:03:42
Modified: 30.12.2017 07:29:37

Version
Description: Internet Explorer
Product: Internet Explorer
Vendor: Microsoft Corporation

Process:
User: <NA>
System process: No

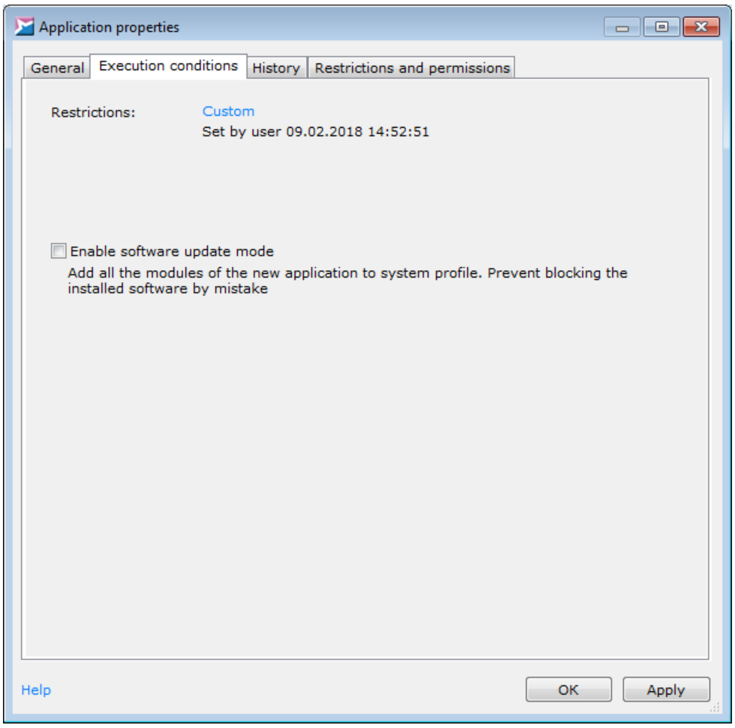
Scanning
Scan result: <NA> Scan

Figure 52. General information about the application

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

Specifying execution conditions

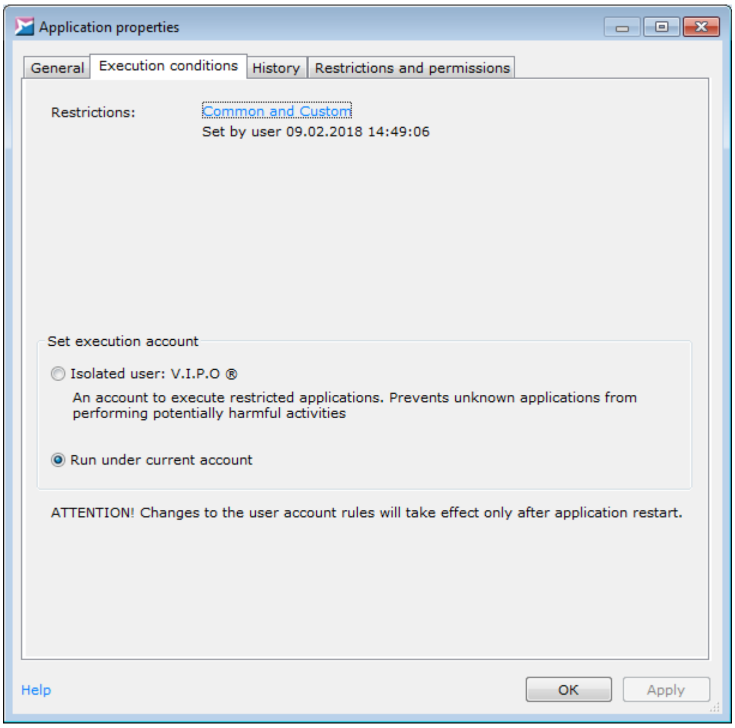
To view and modify the current execution conditions of the application, go to the **Execution conditions** tab of the **Application properties** window (fig. Application execution conditions: trusted applications 63 and Application execution conditions: restricted applications 63).



Restrictions: Custom
Set by user 09.02.2018 14:52:51

□ Enable software update mode
Add all the modules of the new application to system profile. Prevent blocking the installed software by mistake

Figure 53. Application execution conditions: trusted applications



Restrictions: Common and Custom
Set by user 09.02.2018 14:49:06

Set execution account

○ Isolated user: V.I.P.O ®
An account to execute restricted applications. Prevents unknown applications from performing potentially harmful activities

● Run under current account

ATTENTION! Changes to the user account rules will take effect only after application restart.

Figure 54. Application execution conditions: restricted applications

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 **Enable software update mode** option is selected, all program modules are added to the system profile. To activate the option, tick off the corresponding checkbox. The option is only available for trusted applications.

The **Set execution account** switch is responsible for selecting the user account which the application runs under (for restricted applications only):

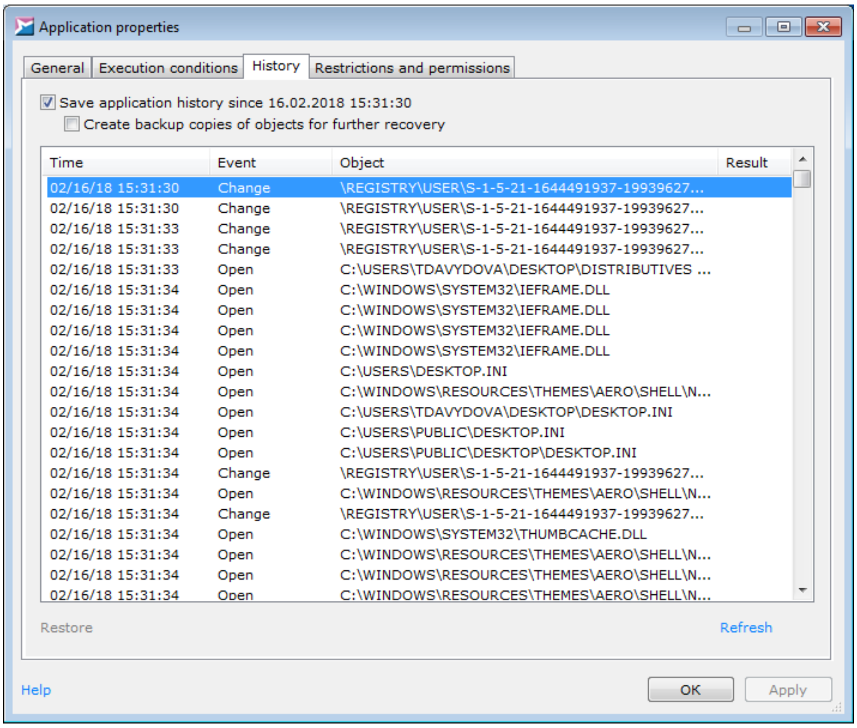
- ○ **Run under current account**: execute the application under current user account;
- ○ **Isolated user: V.I.P.O. ®**: execute the application from the restricted zone under the V.I.P.O. user account with restricted rights.

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 64).

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**.



☑ Save application history since 16.02.2018 15:31:30
□ Create backup copies of objects for further recovery

Time	Event	Object	Result
02/16/18 15:31:30	Change	\REGISTRY\USER\S-1-5-21-1644491937-19939627...	
02/16/18 15:31:30	Change	\REGISTRY\USER\S-1-5-21-1644491937-19939627...	
02/16/18 15:31:33	Change	\REGISTRY\USER\S-1-5-21-1644491937-19939627...	
02/16/18 15:31:33	Change	\REGISTRY\USER\S-1-5-21-1644491937-19939627...	
02/16/18 15:31:33	Open	C:\USERS\TDAVYDOVA\DESKTOP\DISTRIBUTIVES ...	
02/16/18 15:31:34	Open	C:\WINDOWS\SYSTEM32\IEFRAME.DLL	
02/16/18 15:31:34	Open	C:\WINDOWS\SYSTEM32\IEFRAME.DLL	
02/16/18 15:31:34	Open	C:\WINDOWS\SYSTEM32\IEFRAME.DLL	
02/16/18 15:31:34	Open	C:\WINDOWS\SYSTEM32\IEFRAME.DLL	
02/16/18 15:31:34	Open	C:\USERS\DESKTOP.INI	
02/16/18 15:31:34	Open	C:\WINDOWS\RESOURCES\THEMES\AERO\SHELL\N...	
02/16/18 15:31:34	Open	C:\USERS\TDAVYDOVA\DESKTOP\DESKTOP.INI	
02/16/18 15:31:34	Open	C:\USERS\PUBLIC\DESKTOP.INI	
02/16/18 15:31:34	Open	C:\USERS\PUBLIC\DESKTOP\DESKTOP.INI	
02/16/18 15:31:34	Change	\REGISTRY\USER\S-1-5-21-1644491937-19939627...	
02/16/18 15:31:34	Open	C:\WINDOWS\RESOURCES\THEMES\AERO\SHELL\N...	
02/16/18 15:31:34	Change	\REGISTRY\USER\S-1-5-21-1644491937-19939627...	
02/16/18 15:31:34	Open	C:\WINDOWS\SYSTEM32\THUMBCACHE.DLL	
02/16/18 15:31:34	Open	C:\WINDOWS\RESOURCES\THEMES\AERO\SHELL\N...	
02/16/18 15:31:34	Open	C:\WINDOWS\RESOURCES\THEMES\AERO\SHELL\N...	
02/16/18 15:31:34	Open	C:\WINDOWS\RESOURCES\THEMES\AERO\SHELL\N...	

Figure 55. Application activity history

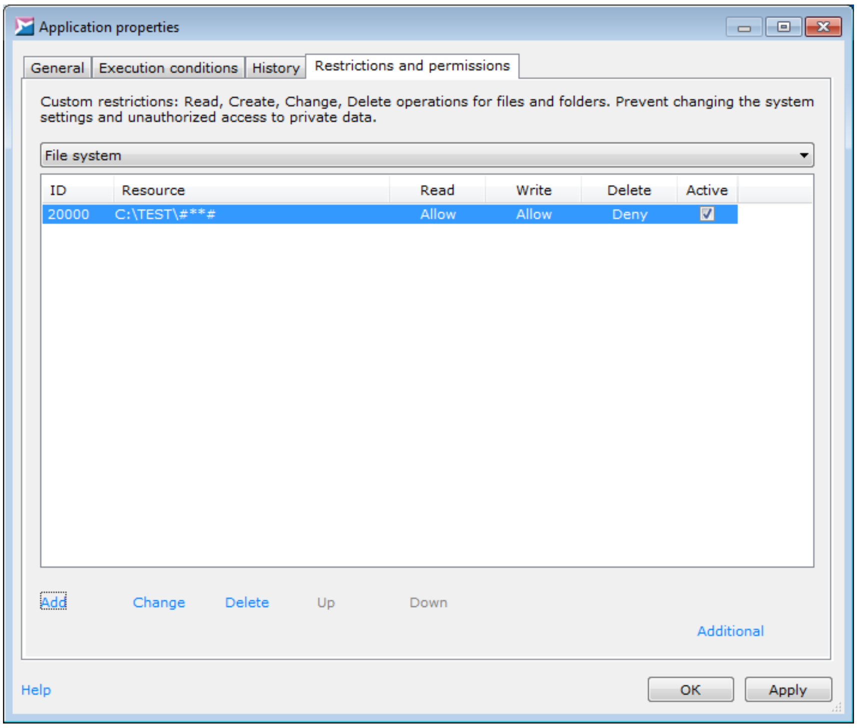
Specifying custom rules

To specify custom rules, go to the **Restrictions and permissions** tab of the **Application properties** window (fig. Custom restrictions of the application 65) 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 68;
- permissions to access system registry 73;
- network activity rules 81;
- process privileges 86.



Custom restrictions: Read, Create, Change, Delete operations for files and folders. Prevent changing the system settings and unauthorized access to private data.

File system

ID	Resource	Read	Write	Delete	Active
20000	C:\TEST\#**#	Allow	Allow	Deny	☑

Figure 56. 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.

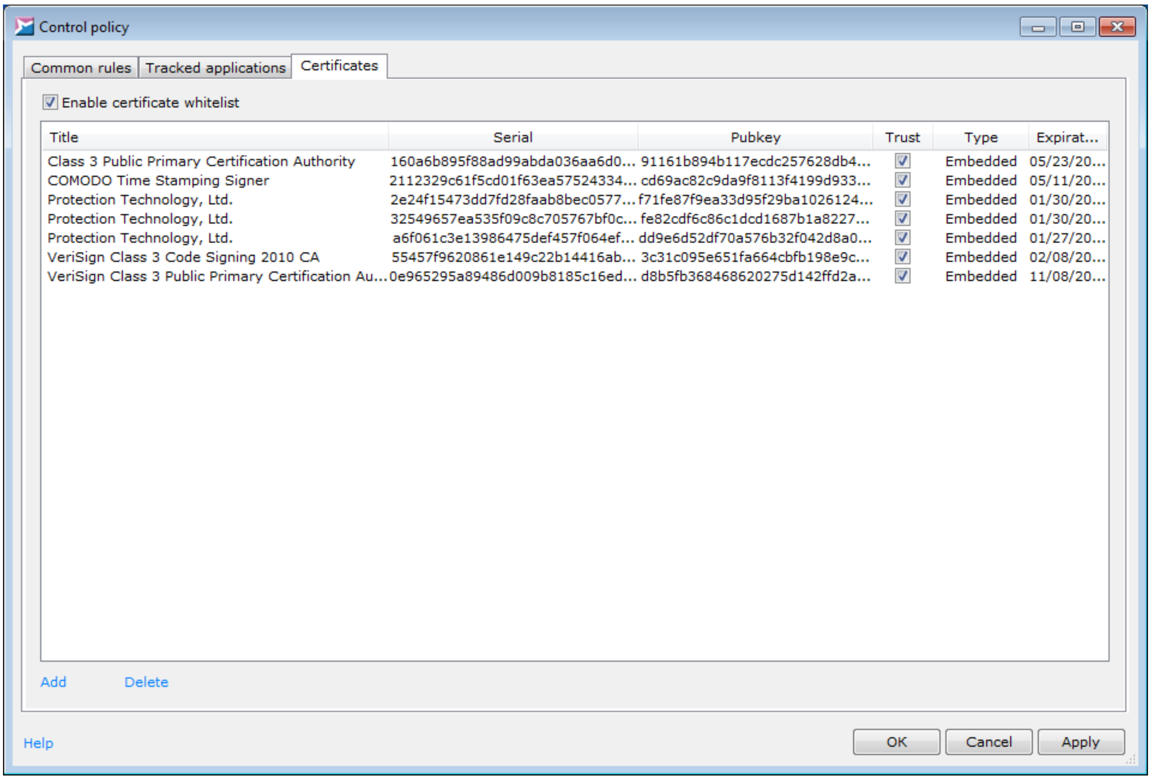
A standard set of custom restrictions can be included to the SoftControl SysWatch package; this set is created by the company experts as a result of the analysis of the application's actions.

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

5.5.5 White list of certificates

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

1) Select **Tracked applications** in the SoftControl SysWatch context menu (33) and go to the **Certificates** tab of the **Control policy** window (fig. The whitelist of certificates (66)).



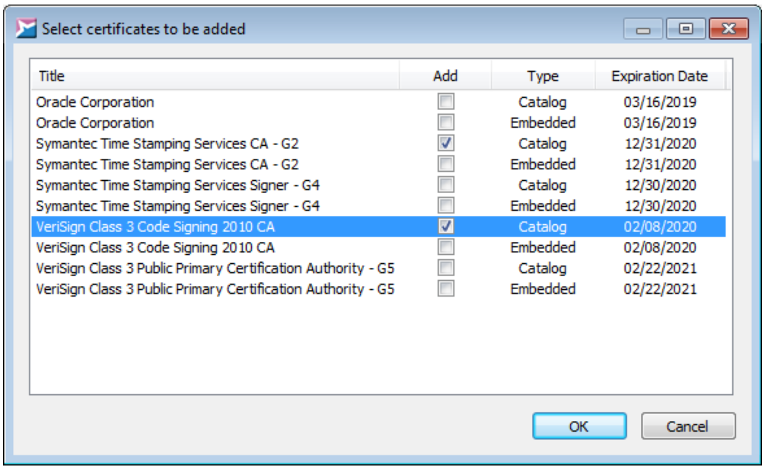
☑ Enable certificate whitelist

Title	Serial	Pubkey	Trust	Type	Expirat...
Class 3 Public Primary Certification Authority	160a6b895f88ad99abda036aa6d0...	91161b894b117ecdc257628db4...	☑	Embedded	05/23/20...
COMODO Time Stamping Signer	2112329c61f5cd01f63ea57524334...	cd69ac82c9da9f8113f4199d933...	☑	Embedded	05/11/20...
Protection Technology, Ltd.	2e24f15473dd7fd28faab8bec0577...	f71fe87f9ea33d95f29ba1026124...	☑	Embedded	01/30/20...
Protection Technology, Ltd.	32549657ea535f09c8c705767bf0c...	fe82cdf6c86c1dcd1687b1a8227...	☑	Embedded	01/30/20...
Protection Technology, Ltd.	a6f061c3e13986475def457f064ef...	dd9e6d52df70a576b32f042d8a0...	☑	Embedded	01/27/20...
VeriSign Class 3 Code Signing 2010 CA	55457f9620861e149c22b14416ab...	3c31c095e651fa664cbfb198e9c...	☑	Embedded	02/08/20...
VeriSign Class 3 Public Primary Certification Au...	0e965295a89486d009b8185c16ed...	d8b5fb368468620275d142ffd2a...	☑	Embedded	11/08/20...

Figure 57. The whitelist of certificates

2) Tick off the **Enable whitelist of certificates** checkbox to activate the whitelist.

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, including three certificates by Protection Technology, Ltd. 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 67).



Title	Add	Type	Expiration Date
Oracle Corporation	□	Catalog	03/16/2019
Oracle Corporation	□	Embedded	03/16/2019
Symantec Time Stamping Services CA - G2	☑	Catalog	12/31/2020
Symantec Time Stamping Services CA - G2	□	Embedded	12/31/2020
Symantec Time Stamping Services Signer - G4	□	Catalog	12/30/2020
Symantec Time Stamping Services Signer - G4	□	Embedded	12/30/2020
VeriSign Class 3 Code Signing 2010 CA	☑	Catalog	02/08/2020
VeriSign Class 3 Code Signing 2010 CA	□	Embedded	02/08/2020
VeriSign Class 3 Public Primary Certification Authority - G5	□	Catalog	02/22/2021
VeriSign Class 3 Public Primary Certification Authority - G5	□	Embedded	02/22/2021

Figure 58. Selecting the certificates to add

4) Tick off the **Trust** column for the added certificates (fig. The whitelist of certificates[66]).

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 whitelist of certificates[66]).

6) To apply changes, click **OK** or **Apply** (fig. The whitelist of certificates[66]).

If the application is signed by several digital signatures, and at least one of the signatures has a certificate in the whitelist, then SoftControl SysWatch allows the application to run. The feature is supported in Windows 8 and newer operating systems.

5.5.6 Activity control rules

Current protection status and the list of the control scopes are displayed in the **Status** tab of the program's control panel[34]. 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:

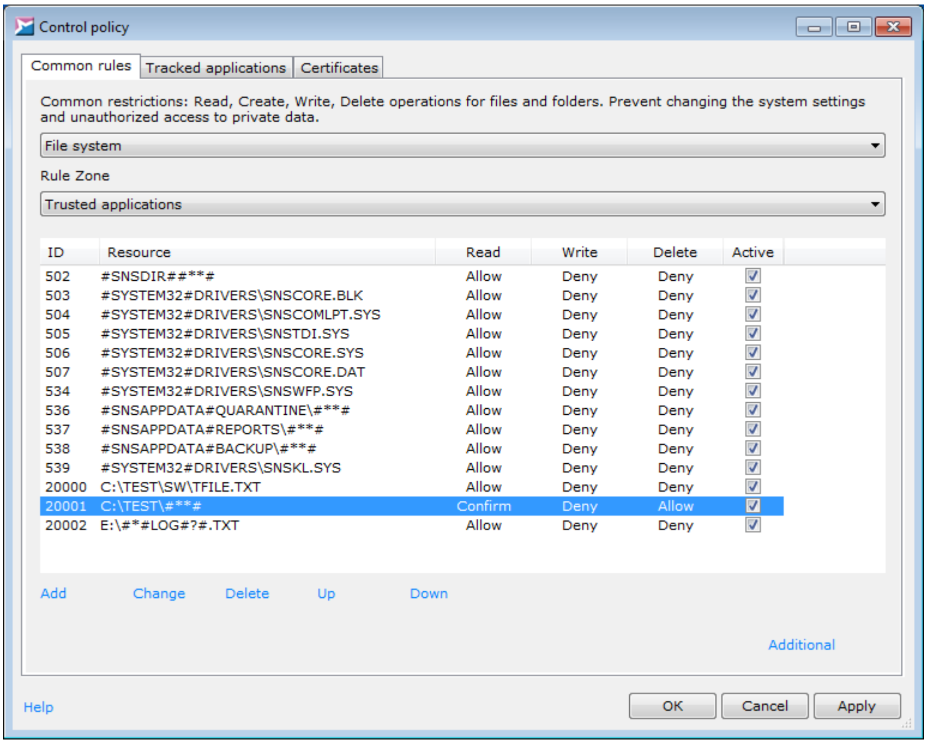
- permissions to access file system[68];
- permissions to access system registry[73];
- permissions to access devices and ports[78];
- network activity[81];
- process privileges[86];
- interprocess interaction[89].

5.5.6.1 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[33], 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[68]).



Common restrictions: Read, Create, Write, Delete operations for files and folders. Prevent changing the system settings and unauthorized access to private data.

File system

Rule Zone

Trusted applications

ID	Resource	Read	Write	Delete	Active
502	#SNSDIR##**#	Allow	Deny	Deny	☑
503	#SYSTEM32#DRIVERS\SNSCORE.BLK	Allow	Deny	Deny	☑
504	#SYSTEM32#DRIVERS\SNSCOMLPT.SYS	Allow	Deny	Deny	☑
505	#SYSTEM32#DRIVERS\SNSTDI.SYS	Allow	Deny	Deny	☑
506	#SYSTEM32#DRIVERS\SNSCORE.SYS	Allow	Deny	Deny	☑
507	#SYSTEM32#DRIVERS\SNSCORE.DAT	Allow	Deny	Deny	☑
534	#SYSTEM32#DRIVERS\SNSWFP.SYS	Allow	Deny	Deny	☑
536	#SNSAPPDATA#QUARANTINE\#**#	Allow	Deny	Deny	☑
537	#SNSAPPDATA#REPORTS\#**#	Allow	Deny	Deny	☑
538	#SNSAPPDATA#BACKUP\#**#	Allow	Deny	Deny	☑
539	#SYSTEM32#DRIVERS\SNSKL.SYS	Allow	Deny	Deny	☑
20000	C:\TEST\SW\TFILE.TXT	Allow	Deny	Deny	☑
20001	C:\TEST\#**#	Confirm	Deny	Allow	☑
20002	E:\#*#LOG#?#.TXT	Allow	Deny	Deny	☑

Figure 59. 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.

Example: the rule with the **ID** 20001 which is shown in fig. Control policy for the file system 68, overrides the action of the rule with the **ID** 20000 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 added to the end of the string, the rule affects only the root directory files);

##** - the mask replaces any number of characters (if the mask is added to 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).

Example: the rule with the **ID** 20020 (*E:\#*#log#?#.txt*) is shown in fig. Control policy for the file system[68]; 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.

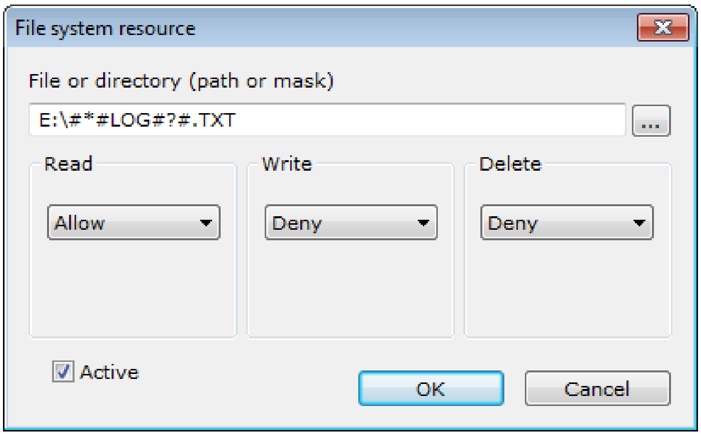
Creating a rule

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. Creating a rule for the file system object[70]). Note that space characters are valid characters. If a rule ends in a space character and the source path does not have it, the rule will fail. In existing rules, space characters are displayed as dots.

You can specify local folders as well as network folders. When you create a rule for network folders, the path is specified as follows: \\<*server_name*>\<*folder_name*>. You can use the **#**#** mask instead of \\. In this case, SoftControl SysWatch checks both network and local folders. Besides, you can specify IP address of the computer with the network folder.

ℹ If you specify the computer's IP address in the rule, the rule is only valid when the user enters IP address to access the folder. It is not valid when the user enters the network path. Therefore, if you need to monitor the folders that the users access by both IP address and network path, create separate rules for each of the notations.



E:\#*#LOG#?#.TXT

Read: Allow
Write: Deny
Delete: Deny

☑ Active

Figure 60. Creating a rule for the file system object

When you add a folder via the explorer, the **#*#** mask[69] 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[70] of the rule.

Moving a rule between zones

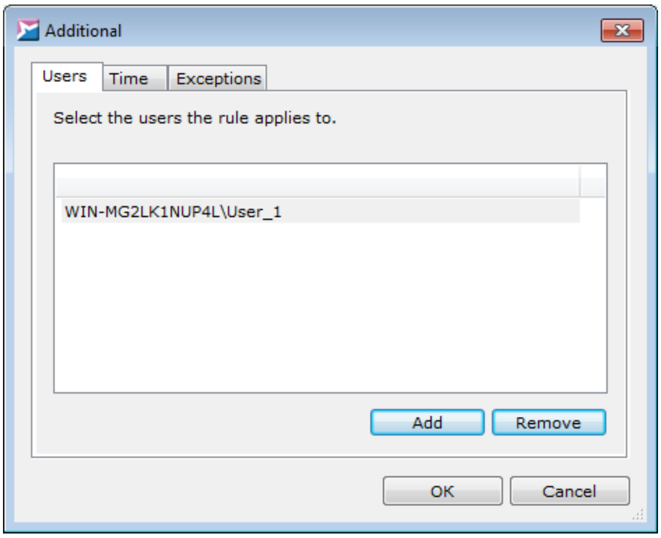
If you need to move a rule to the list for the applications from another execution zone, invoke the rule context menu and select one of the options:

- **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, security groups, and built-in security principals that the rule applies to (fig. Selecting user accounts[72]). By default, the rules apply to all the users.

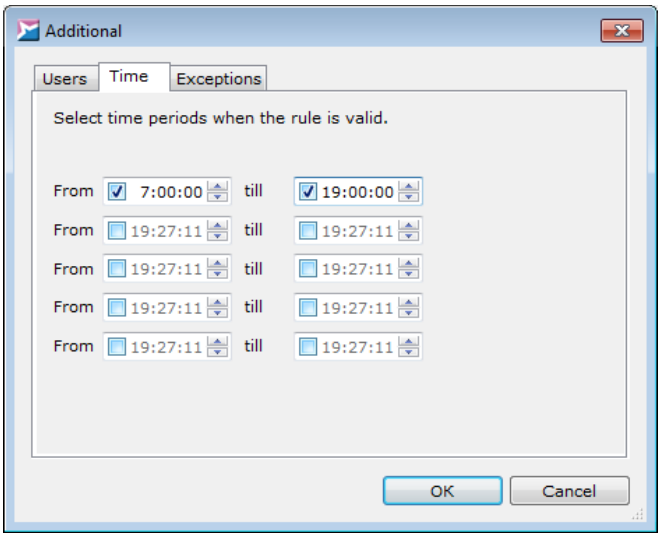


Select the users the rule applies to.

WIN-MG2LK1NUP4L\User_1

Figure 61. Selecting user accounts

- **Time** – on this, tab you can specify time intervals when the rule is valid (fig. Specifying time intervals[72]).



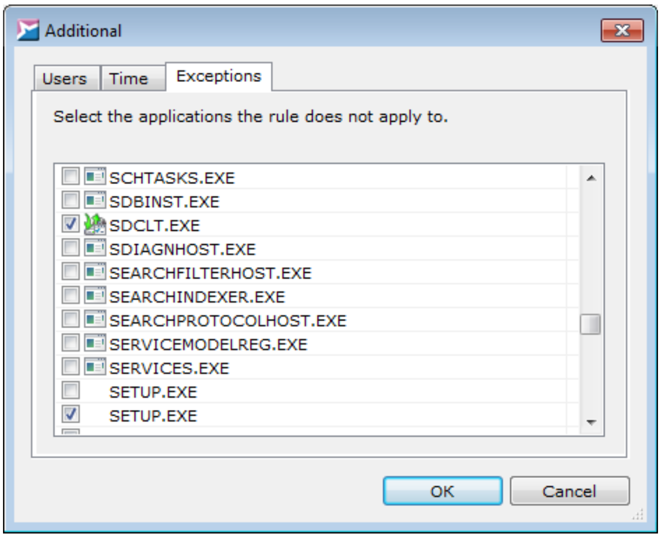
Select time periods when the rule is valid.

From ☑ 7:00:00 till ☑ 19:00:00
From □ 19:27:11 till □ 19:27:11
From □ 19:27:11 till □ 19:27:11
From □ 19:27:11 till □ 19:27:11
From □ 19:27:11 till □ 19:27:11

Figure 62. 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).

- **Exceptions** – on this tab, you can select applications the rule does not apply to (fig. Selecting applications - the exceptions[73]).



Additional

Select the applications the rule does not apply to.

- □ SCHTASKS.EXE
- □ SDBINST.EXE
- ☑ SDCLT.EXE
- □ SDIAGNHOST.EXE
- □ SEARCHFILTERHOST.EXE
- □ SEARCHINDEXER.EXE
- □ SEARCHPROTOCOLHOST.EXE
- □ SERVICEMODELREG.EXE
- □ SERVICES.EXE
- □ SETUP.EXE
- ☑ SETUP.EXE

Figure 63. 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[65] 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.

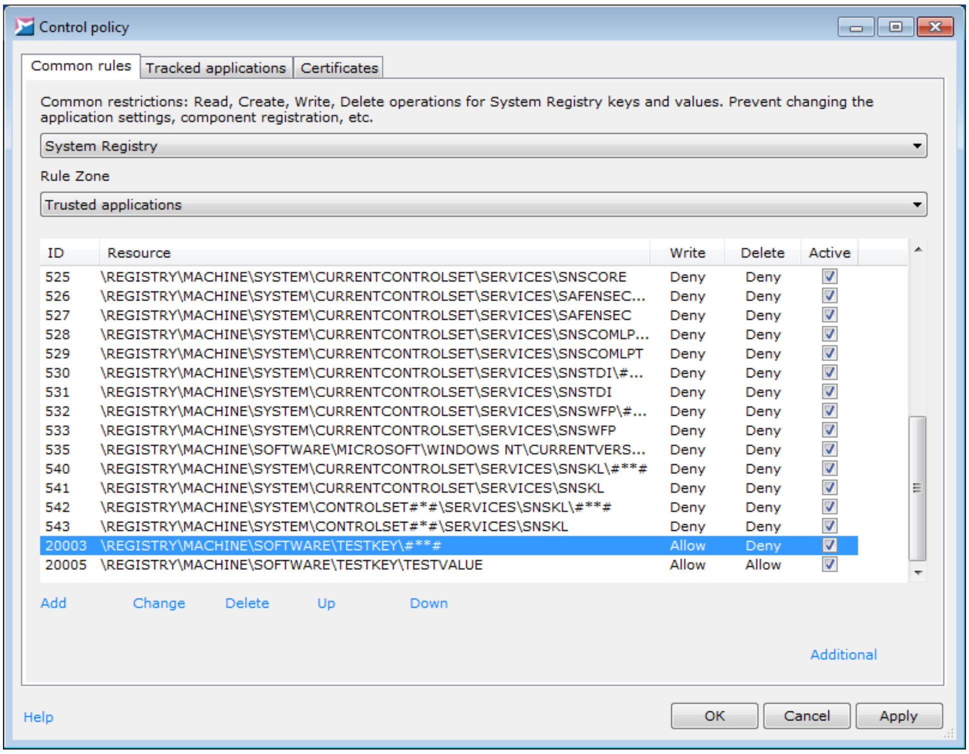
To apply changes, click **OK** or **Apply**.

5.5.6.2 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[33], 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[74]).



Common restrictions: Read, Create, Write, Delete operations for System Registry keys and values. Prevent changing the application settings, component registration, etc.

System Registry

Rule Zone

Trusted applications

ID	Resource	Write	Delete	Active
525	\REGISTRY\MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\SNSCORE	Deny	Deny	☑
526	\REGISTRY\MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\SAFENSEC...	Deny	Deny	☑
527	\REGISTRY\MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\SAFENSEC	Deny	Deny	☑
528	\REGISTRY\MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\SNSCOMLP...	Deny	Deny	☑
529	\REGISTRY\MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\SNSCOMLPT	Deny	Deny	☑
530	\REGISTRY\MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\SNSTDI\#...	Deny	Deny	☑
531	\REGISTRY\MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\SNSTDI	Deny	Deny	☑
532	\REGISTRY\MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\SNSWFP\#...	Deny	Deny	☑
533	\REGISTRY\MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\SNSWFP	Deny	Deny	☑
535	\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERS...	Deny	Deny	☑
540	\REGISTRY\MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\SNSKL\#**#	Deny	Deny	☑
541	\REGISTRY\MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\SNSKL	Deny	Deny	☑
542	\REGISTRY\MACHINE\SYSTEM\CONTROLSET#*#\SERVICES\SNSKL\#**#	Deny	Deny	☑
543	\REGISTRY\MACHINE\SYSTEM\CONTROLSET#*#\SERVICES\SNSKL	Deny	Deny	☑
20003	\REGISTRY\MACHINE\SOFTWARE\TESTKEY\#**#	Allow	Deny	☑
20005	\REGISTRY\MACHINE\SOFTWARE\TESTKEY\TESTVALUE	Allow	Allow	☑

Figure 64. 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** 20005 which is shown in fig. Control policy for the system registry[74], overrides the action of the rule with the **ID** 20003 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 masksto 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 added to the end of the string, the rule affects only key values);

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

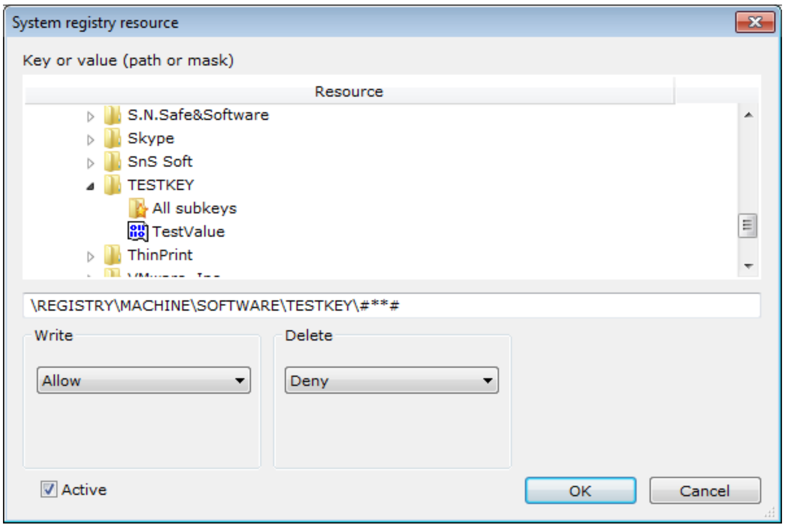
#?# - the mask replaces exactly one character (any character).

Example: the rule with the **ID** 20003 (*\REGISTRY\MACHINE\SOFTWARE\TESTKEY\*#**#) is shown in fig. Control policy for the system registry[74]; 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[75]). Note that space characters are valid characters. If a rule ends in a space character and the source path does not have it, the rule will fail. In existing rules, space characters are displayed as dots.



\REGISTRY\MACHINE\SOFTWARE\TESTKEY\#**#

Write: Allow

Delete: Deny

☑ Active

Figure 65. 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 condi-

tion.

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[75] of the rule.

Moving a rule between zones

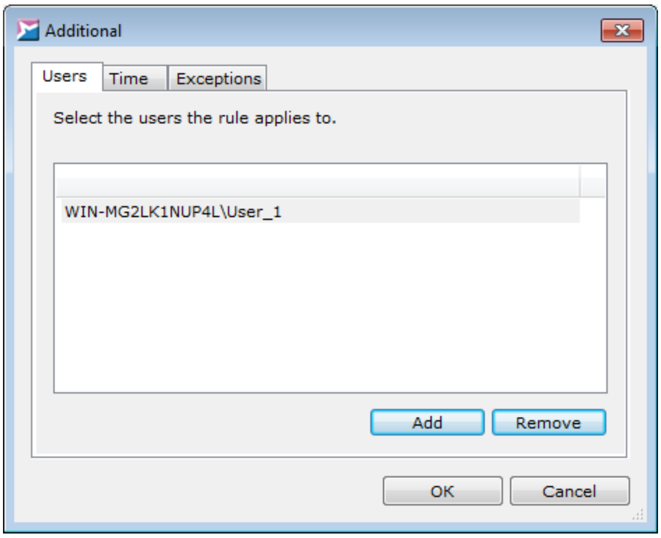
If you need to move a rule to the list for the applications from another execution zone, invoke the rule context menu and select one of the options:

- **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, security groups, and built-in security principals that the rule applies to (fig. Selecting user accounts[76]). By default, the rules apply to all the users.

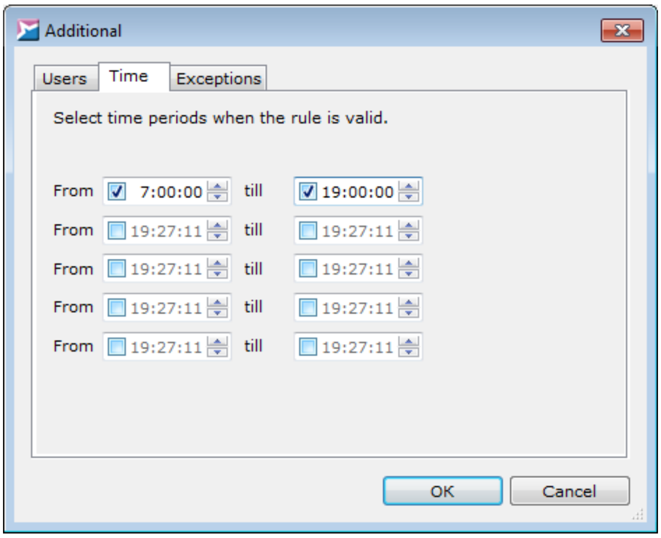


Select the users the rule applies to.

WIN-MG2LK1NUP4L\User_1

Figure 66. Selecting user accounts

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



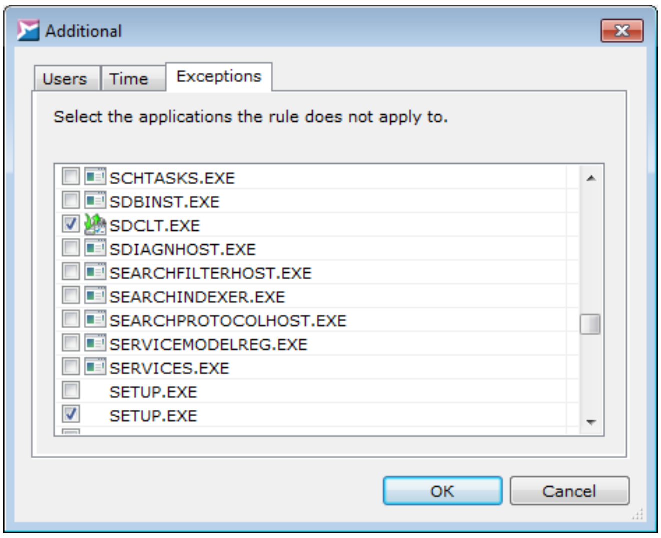
Select time periods when the rule is valid.

From ☑ 7:00:00 till ☑ 19:00:00
From □ 19:27:11 till □ 19:27:11
From □ 19:27:11 till □ 19:27:11
From □ 19:27:11 till □ 19:27:11
From □ 19:27:11 till □ 19:27:11

Figure 67. 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).

- **Exceptions** – on this tab, you can select the applications the rule does not apply to (fig. Selecting applications - the exceptions 77).



Select the applications the rule does not apply to.

□ SCHTASKS.EXE
□ SDBINST.EXE
☑ SDCLT.EXE
□ SDIAGNHOST.EXE
□ SEARCHFILTERHOST.EXE
□ SEARCHINDEXER.EXE
□ SEARCHPROTOCOLHOST.EXE
□ SERVICEMODELREG.EXE
□ SERVICES.EXE
□ SETUP.EXE
☑ SETUP.EXE

Figure 68. 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 65 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 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.

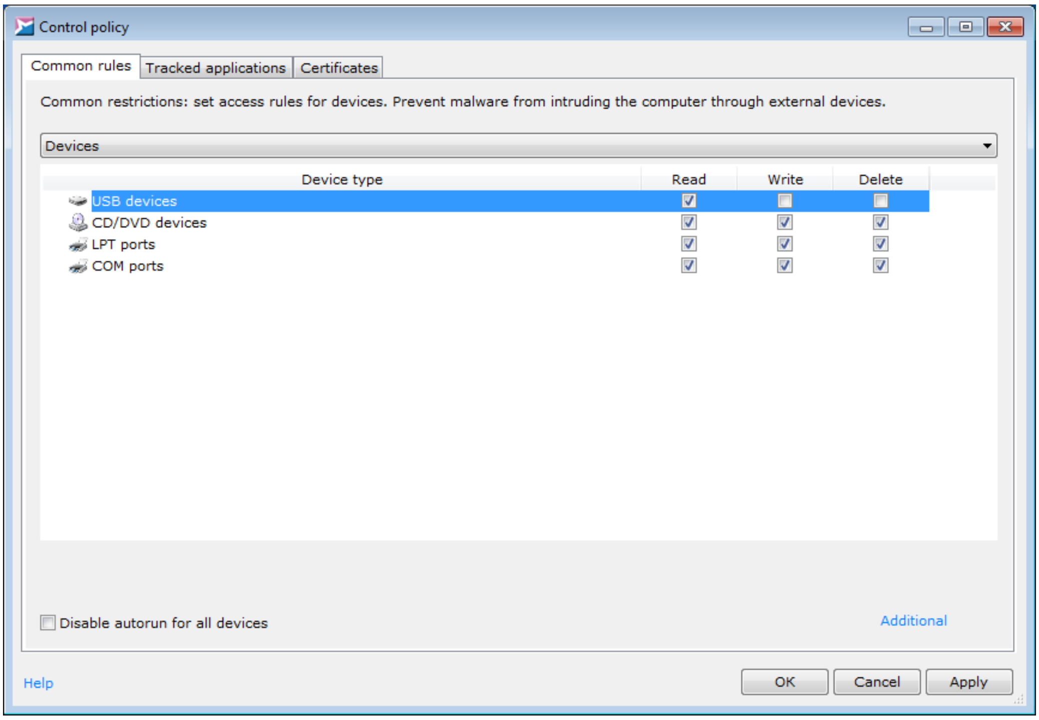
To apply changes, click **OK** or **Apply**.

5.5.6.3 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(33), 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(78)).



Common restrictions: set access rules for devices. Prevent malware from intruding the computer through external devices.

Devices

Device type	Read	Write	Delete
USB devices	☑	□	□
CD/DVD devices	☑	☑	☑
LPT ports	☑	☑	☑
COM ports	☑	☑	☑

□ Disable autorun for all devices

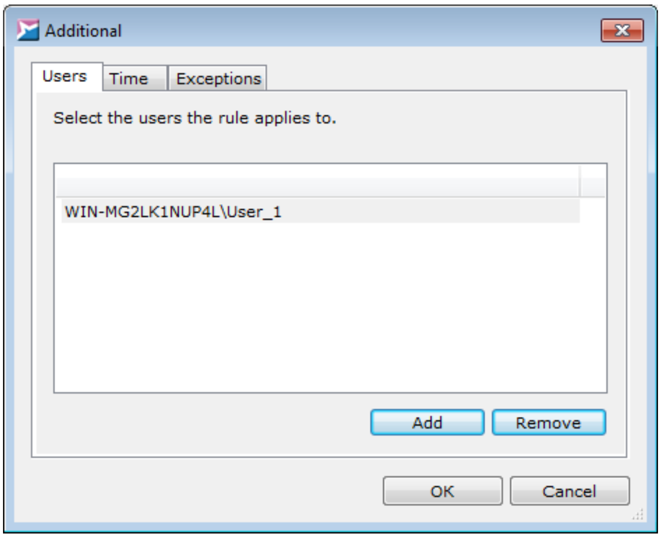
Figure 69. Control policy for devices and ports

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, security groups, and built-in security principals that the rule applies to (fig. Selecting user accounts 79).

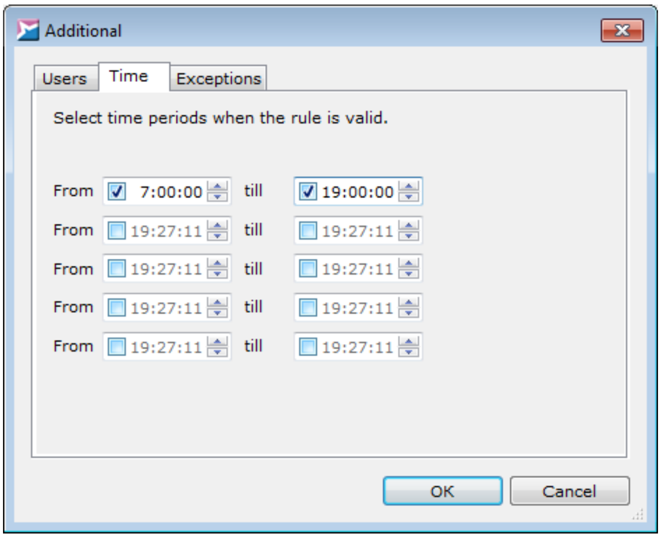


Select the users the rule applies to.

WIN-MG2LK1NUP4L\User_1

Figure 70. Selecting user accounts

- **Time** – on this tab, you can specify time intervals when the rule is valid (fig. Specifying time intervals 80).



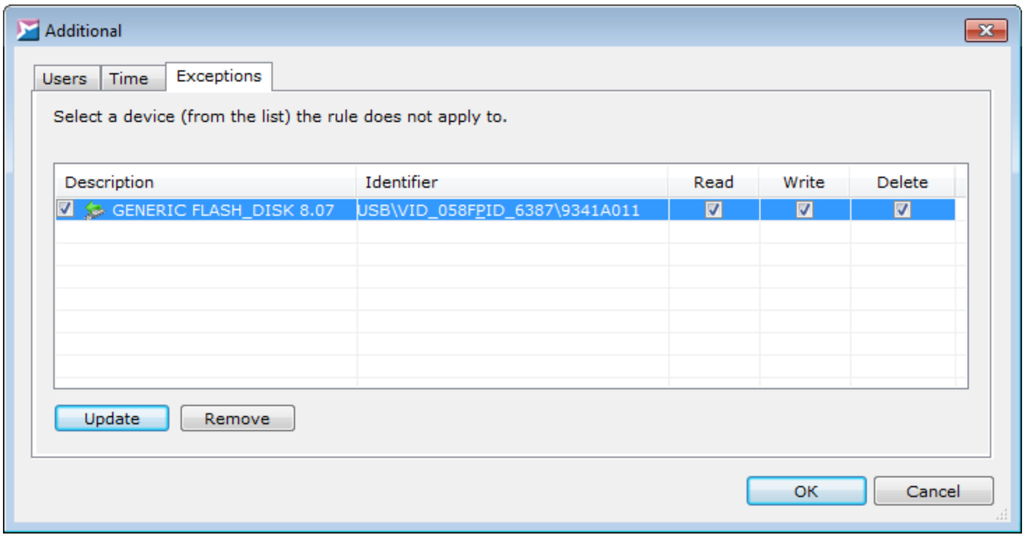
Select time periods when the rule is valid.

From ☑ 7:00:00 till ☑ 19:00:00
From □ 19:27:11 till □ 19:27:11
From □ 19:27:11 till □ 19:27:11
From □ 19:27:11 till □ 19:27:11
From □ 19:27:11 till □ 19:27:11

Figure 71. 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).

- **Exceptions** – on this tab, you can specify certain devices the rule does not apply to (fig. Selecting USB devices - the exceptions 80).



Select a device (from the list) the rule does not apply to.

Description	Identifier	Read	Write	Delete
☑ GENERIC FLASH_DISK 8.07	USB\VID_058FPID_6387\9341A011	☑	☑	☑

Figure 72. Selecting USB devices: the exceptions

In the USB devices 'whitelist', 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 whitelist, 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).

> 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).

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

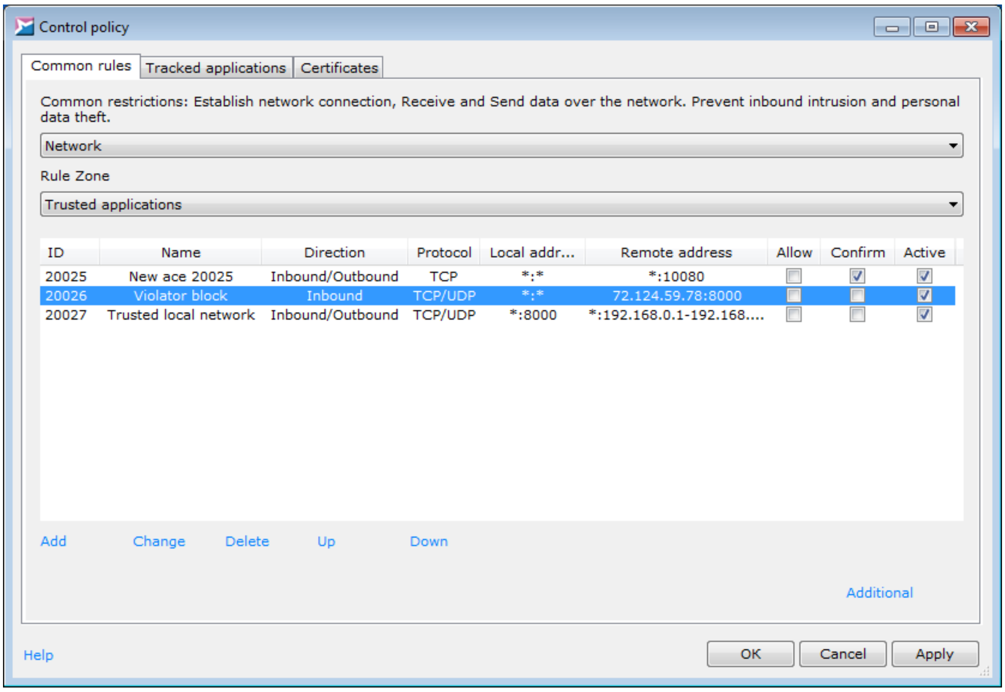
To apply changes, click **OK** or **Apply**.

5.5.6.4 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](33), 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](82)).



Common restrictions: Establish network connection, Receive and Send data over the network. Prevent inbound intrusion and personal data theft.

Network

Rule Zone

Trusted applications

ID	Name	Direction	Protocol	Local addr...	Remote address	Allow	Confirm	Active
20025	New ace 20025	Inbound/Outbound	TCP	*:*	*:10080	□	☑	☑
20026	Violator block	Inbound	TCP/UDP	*:*	72.124.59.78:8000	□	□	☑
20027	Trusted local network	Inbound/Outbound	TCP/UDP	*:8000	*:192.168.0.1-192.168....	□	□	☑

Figure 73. 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[83], 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[83], then the * character is displayed before the *:* sign. If the **Any port** option is selected, then the * character is displayed after the *:* sign.

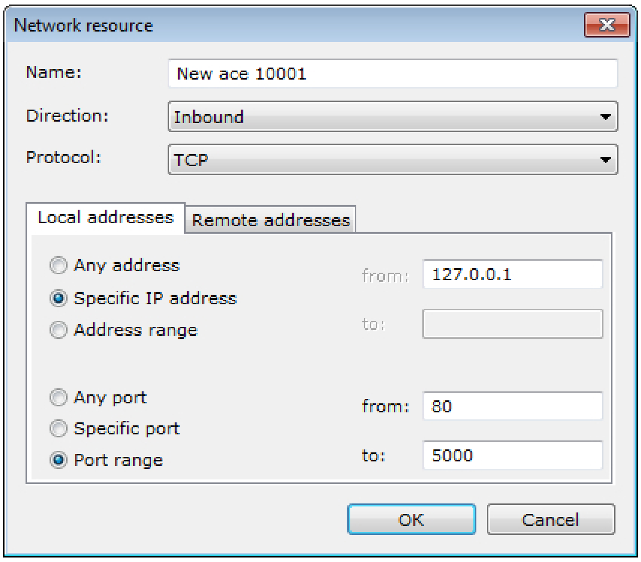
Allowing or blocking the network connection with the specified parameters is managed by the checkbox in the **Allow** column. If it is assumed that the user[84] processes the application network activity incidents, tick off the **Confirm** checkbox. You can enable or disable the rule with the help of 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[83]).

Click **OK** to add the created rule to the list.



Network resource

Name: New ace 10001

Direction: Inbound

Protocol: TCP

○ Any address
● Specific IP address
○ Address range

from: 127.0.0.1
to:

○ Any port
○ Specific port
● Port range

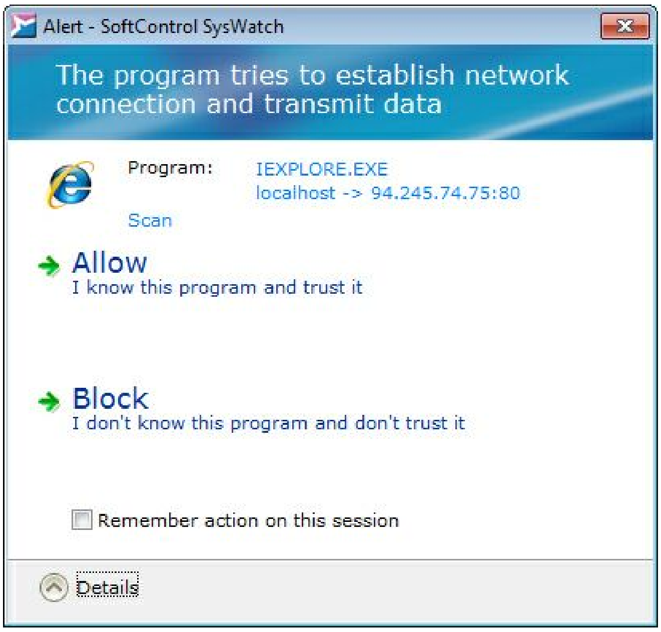
from: 80
to: 5000

Figure 74. 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[84].



Alert - SoftControl SysWatch

The program tries to establish network connection and transmit data

Program: IEXPLORE.EXE
localhost -> 94.245.74.75:80

Scan

Allow
I know this program and trust it

Block
I don't know this program and don't trust it

□ Remember action on this session

Figure 75. 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[92] result (you can check the application before you make the decision, if the antivirus scanner and the corresponding program license[42] 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 for 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 [83] of the rule.

Moving a rule between zones

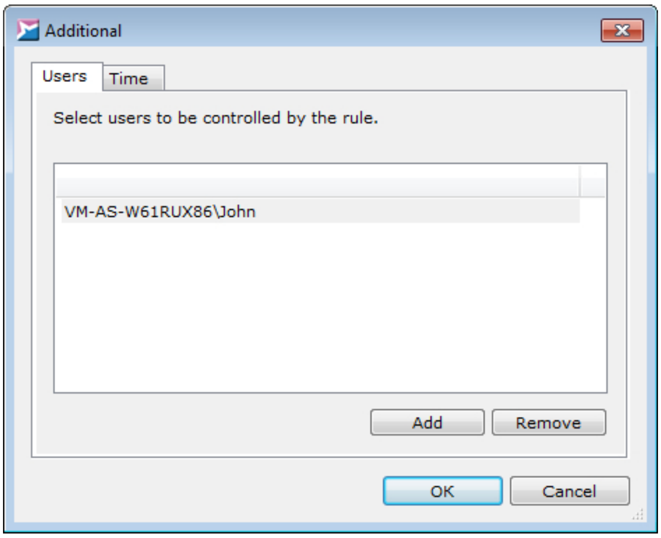
If you need to move a rule to the list for the applications from another execution zone, invoke the rule context menu and select one of the options:

- **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, security groups, and built-in security principals that the rule applies to (fig. Selecting user accounts [85]). By default, the rules apply to all the users.

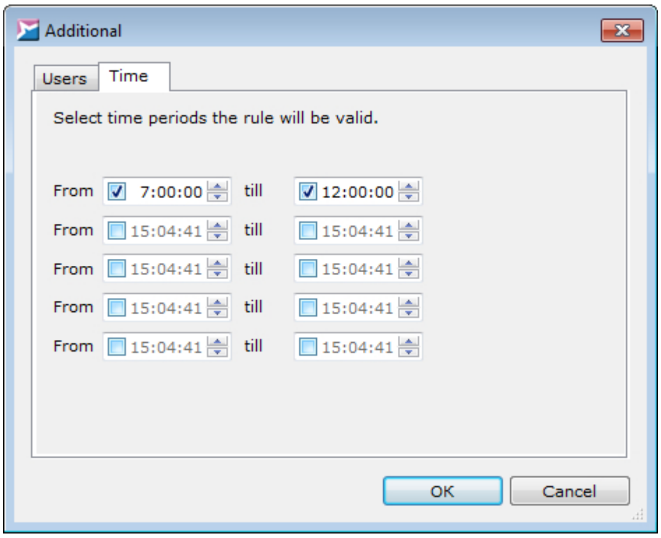


Select users to be controlled by the rule.

VM-AS-W61RUX86\John

Figure 76. Selecting user accounts

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



Select time periods the rule will be valid.

From	☑ 7:00:00	till	☑ 12:00:00
From	□ 15:04:41	till	□ 15:04:41
From	□ 15:04:41	till	□ 15:04:41
From	□ 15:04:41	till	□ 15:04:41
From	□ 15:04:41	till	□ 15:04:41

Figure 77. 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.

Deleting a rule

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

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

5.5.6.5 Specifying process privileges

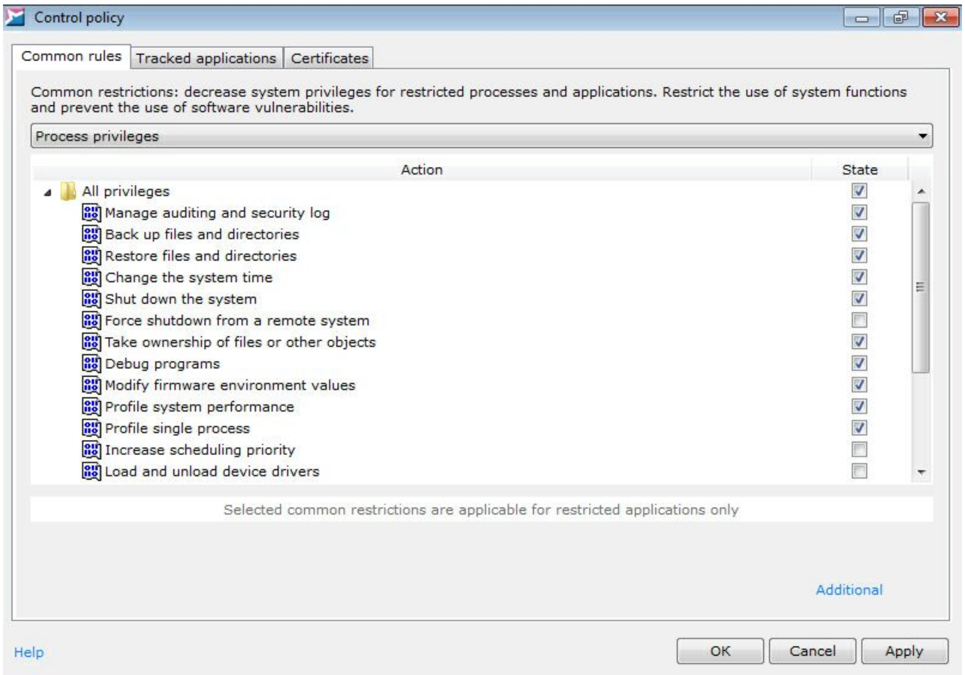
The **Process privileges** scope allows you to restrict the use of Windows privileges by the processes:

- Manage auditing and 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 single process;
- Increase scheduling priority;
- Load and unload device drivers;
- Create a pagefile;
- Adjust memory quotas for a process;
- Bypass traverse 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[33], 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[87]). For description of the privileges and how they are applied, see section Supplemental information[135].



Common restrictions: decrease system privileges for restricted processes and applications. Restrict the use of system functions and prevent the use of software vulnerabilities.

Process privileges

Action	State
All privileges	☑
Manage auditing and security log	☑
Back up files and directories	☑
Restore files and directories	☑
Change the system time	☑
Shut down the system	☑
Force shutdown from a remote system	□
Take ownership of files or other objects	☑
Debug programs	☑
Modify firmware environment values	☑
Profile system performance	☑
Profile single process	☑
Increase scheduling priority	□
Load and unload device drivers	□

Selected common restrictions are applicable for restricted applications only

Figure 78. Control policy for the process privileges

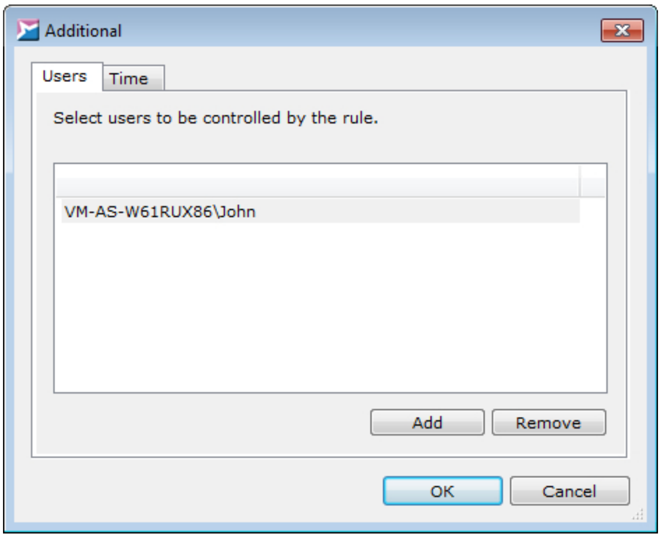
Creating a rule

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 of 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, security groups, and built-in security principals that the rule applies to (fig. Selecting user accounts 88). By default, rules apply to all the users.

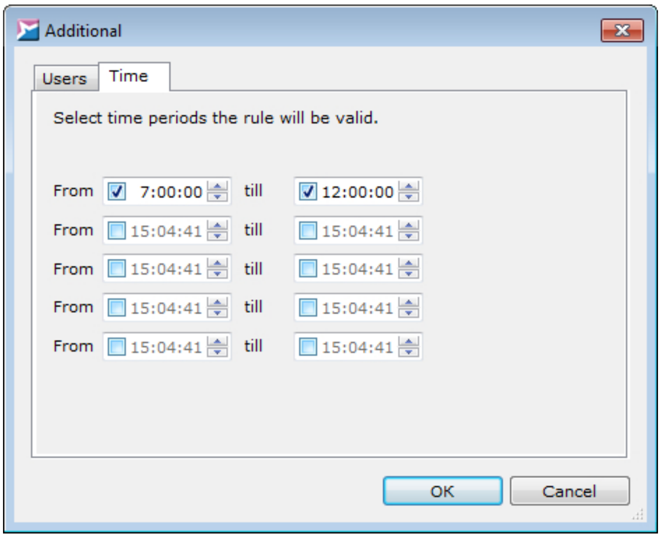


Select users to be controlled by the rule.

VM-AS-W61RUX86\John

Figure 79. Selecting user accounts

- **Time** – on this tab, you can specify time intervals when the rule is valid (fig. Specifying time intervals 88).



Select time periods the rule will be valid.

From ☑ 7:00:00 till ☑ 12:00:00
From □ 15:04:41 till □ 15:04:41
From □ 15:04:41 till □ 15:04:41
From □ 15:04:41 till □ 15:04:41
From □ 15:04:41 till □ 15:04:41

Figure 80. 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).

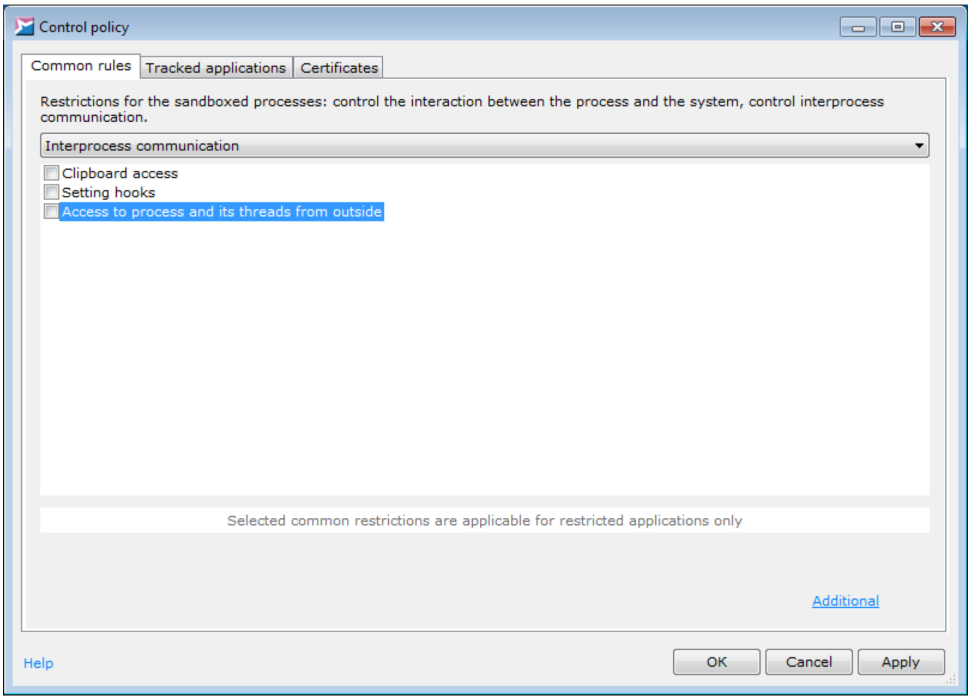
Click **OK** to save the specified additional parameters.

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

5.5.6.6 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;
- Accessing the process and its threads from the outside.



Restrictions for the sandboxed processes: control the interaction between the process and the system, control interprocess communication.

Interprocess communication

□ Clipboard access
□ Setting hooks
□ Access to process and its threads from outside

Selected common restrictions are applicable for restricted applications only

Figure 81. 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[33], switch to the **Common rules** tab of the **Control policy** window and select **Interprocess communication** from the drop-down list (fig. Control policy for the interprocess communication[89]).

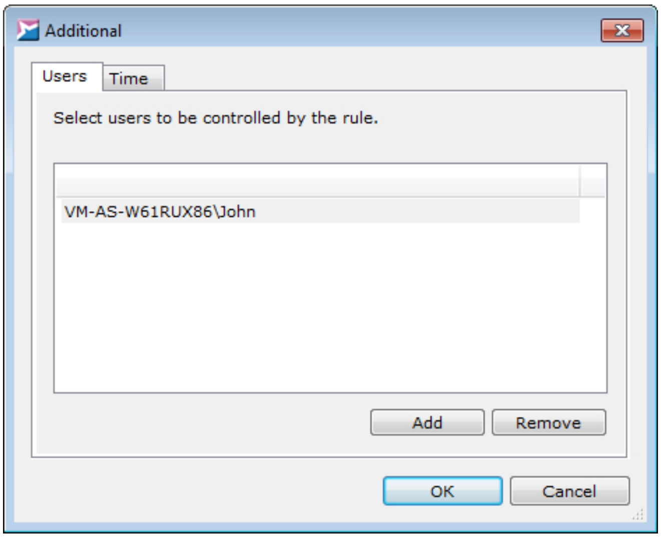
Creating a rule

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, security groups, and built-in security principals that the rule applies to (fig. Selecting user accounts[90]). By default, rules apply to all the users.

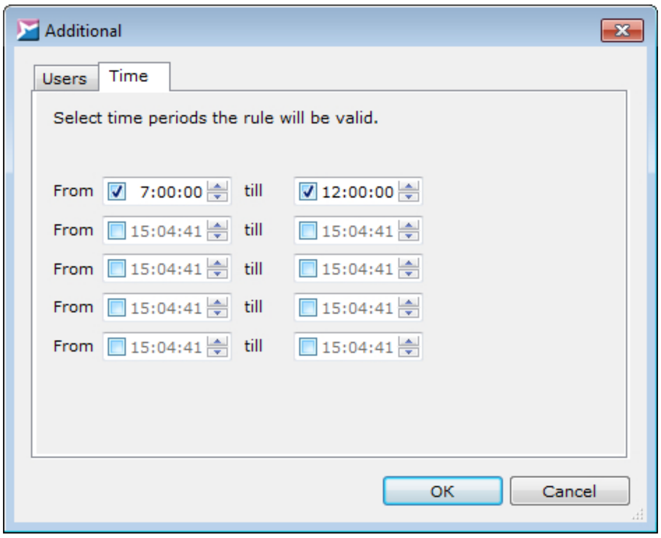


Select users to be controlled by the rule.

VM-AS-W61RUX86\John

Figure 82. Selecting user accounts

- **Time** – on this tab you can specify time intervals when the rule is valid (fig. Specifying time intervals 91).



Select time periods the rule will be valid.

From ☑ 7:00:00 till ☑ 12:00:00
From □ 15:04:41 till □ 15:04:41
From □ 15:04:41 till □ 15:04:41
From □ 15:04:41 till □ 15:04:41
From □ 15:04:41 till □ 15:04:41

Figure 83. 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**.

5.6 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[48]. 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[42] 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.

To make the search for malicious code efficient, you need to update[114] the antivirus bases regularly. We recommend that you set up daily updates[114]. 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[93].
2) Specify the objects in the scan scope[97], 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[97].
4) On the basis of the scan results[98], make a decision regarding the detected threats if they have not been neutralized.

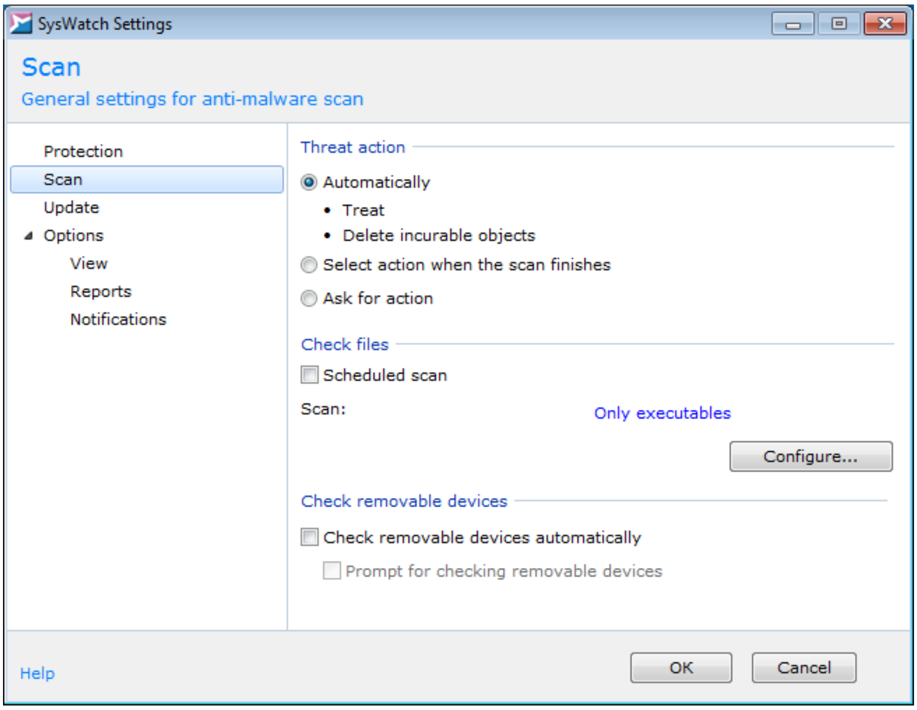
We recommend that you perform scan:

- Immediately after SoftControl SysWatch installation, if there is no other antivirus software previously installed in the system.
- Each time when the application activity control[48] is disabled, while external storage

devices (USB, CD, DVD etc.) are used or Internet connection is established.

5.6.1 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. Setting up check parameters[93]).



SysWatch Settings

Scan

General settings for anti-malware scan

- Protection
- Scan
- Update
- Options
  - View
  - Reports
  - Notifications

Threat action

● Automatically
- Treat
- Delete incurable objects

○ Select action when the scan finishes

○ Ask for action

Check files

□ Scheduled scan

Scan: Only executables

Configure...

Check removable devices

□ Check removable devices automatically

□ Prompt for checking removable devices

Help

OK

Cancel

Figure 84. 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:

○ **Automatically**:

- **Treat**

  Neutralize the infected object.

- **Delete incurable objects**

  Delete the infected object if it cannot be treated.

○ **Select action when the scan finishes**

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

○ **Ask for 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.

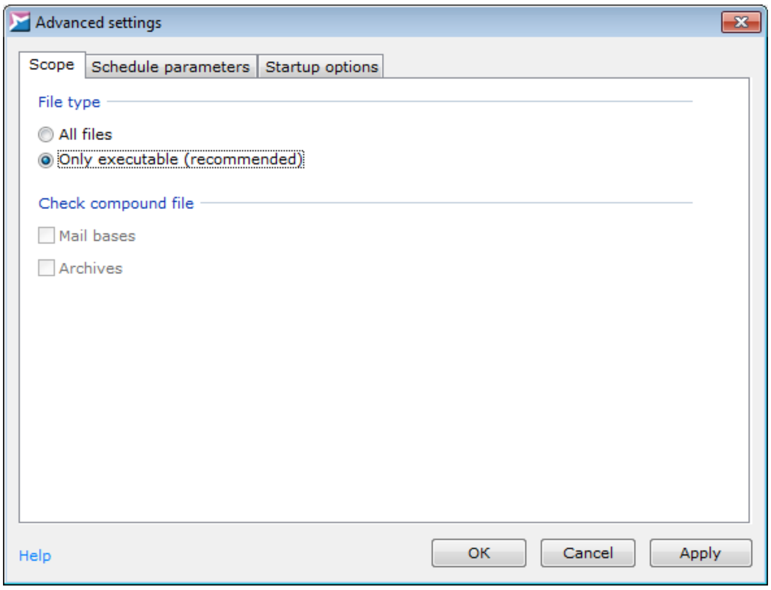
There are the following options on the **Scan scope** tab of the **Advanced settings** window (fig. Check scope settings[94]):

○ **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.).


Advanced settings

Scope | Schedule parameters | Startup options

File type
○ All files
● Only executable (recommended)

Check compound file
□ Mail bases
□ Archives

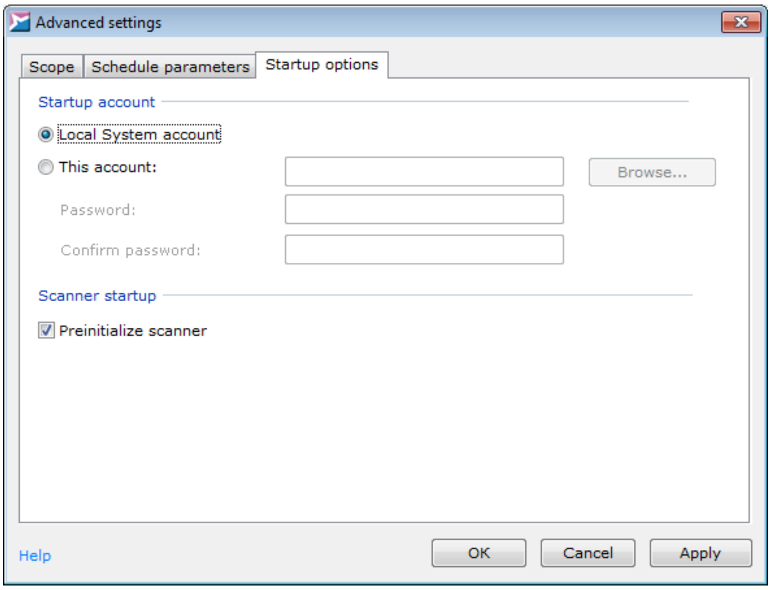
Figure 85. Check scope settings

Select user account to perform the scan, on the **Startup options** tab (fig. Additional check parameters[94]):

○ **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.



Startup account

● Local System account

○ This account:

Password:

Confirm password:

Scanner startup

☑ Preinitialize scanner

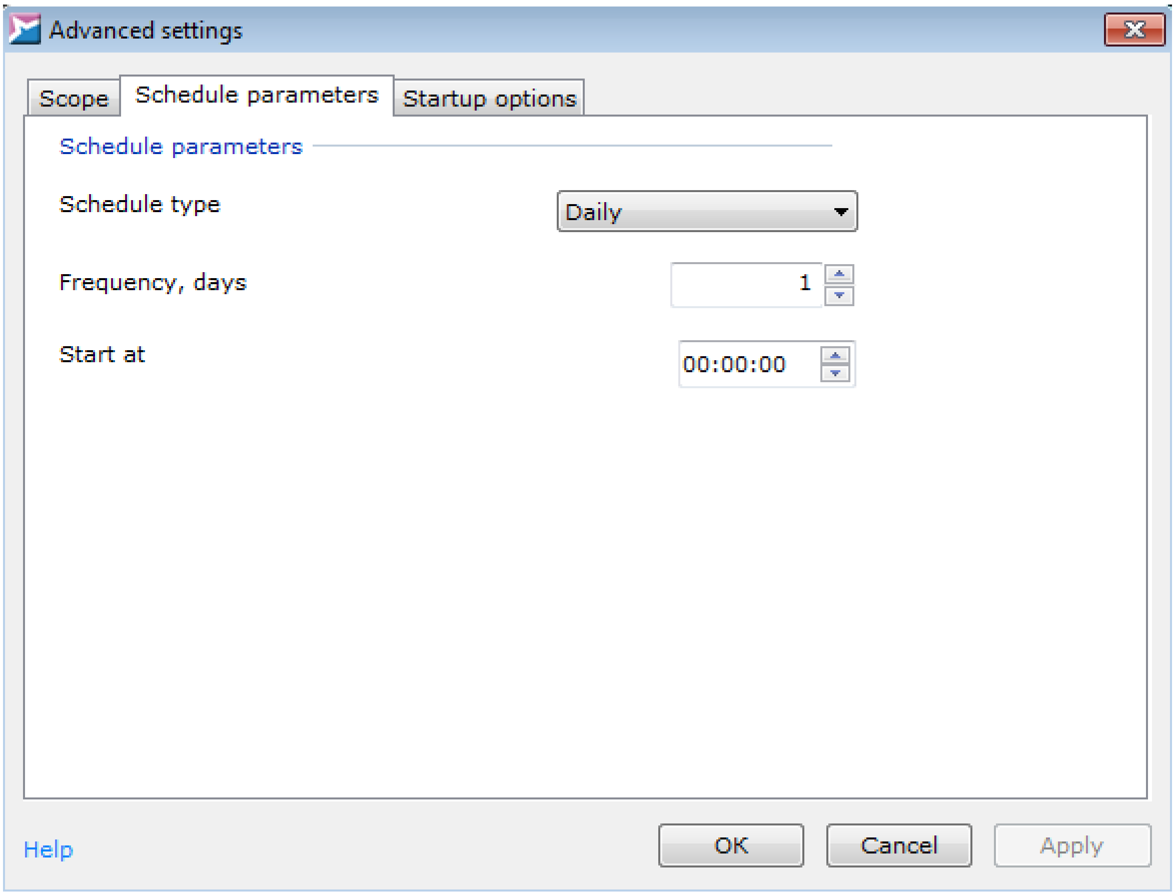
Figure 86. Additional check parameters

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

Settings up scan schedule

Condition: Only when SoftControl SysWatch is controlled from the server remotely[40].

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


Advanced settings

Schedule parameters

Schedule type: Daily

Frequency, days: 1

Start at: 00:00:00

Figure 87. 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. Scan schedule parameters[95]).

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**.

5.6.2 Run on demand

In order to select a scan area and run the check, go the **Scan** tab of the SoftControl SysWatch control panel 34 .

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

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

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.

We recommend that you rescan objects on quarantine after the antivirus base update 114 completes.

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

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 93 .

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[112].

Viewing scan report

To view detailed information about the check during the scan process, click **Details**. To open scan report[101] after the scan completes, click the link with the date and time of last check in the **Last scan** string.

5.6.3 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[93].

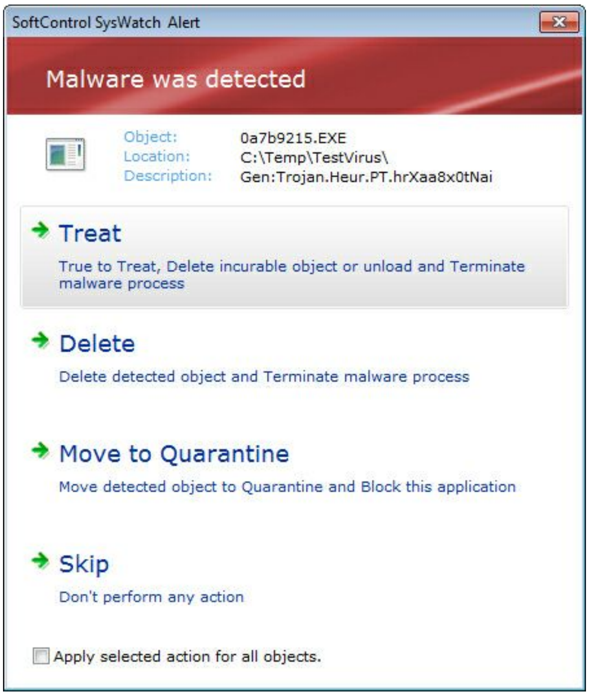
Selecting an action for a certain threat

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[98].

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.



SoftControl SysWatch Alert

Malware was detected

Object: 0a7b9215.EXE
Location: C:\Temp\TestVirus\
Description: Gen:Trojan.Heur.PT.hrXaa8x0tNai

Treat
True to Treat, Delete incurable object or unload and Terminate malware process

Delete
Delete detected object and Terminate malware process

Move to Quarantine
Move detected object to Quarantine and Block this application

Skip
Don't perform any action

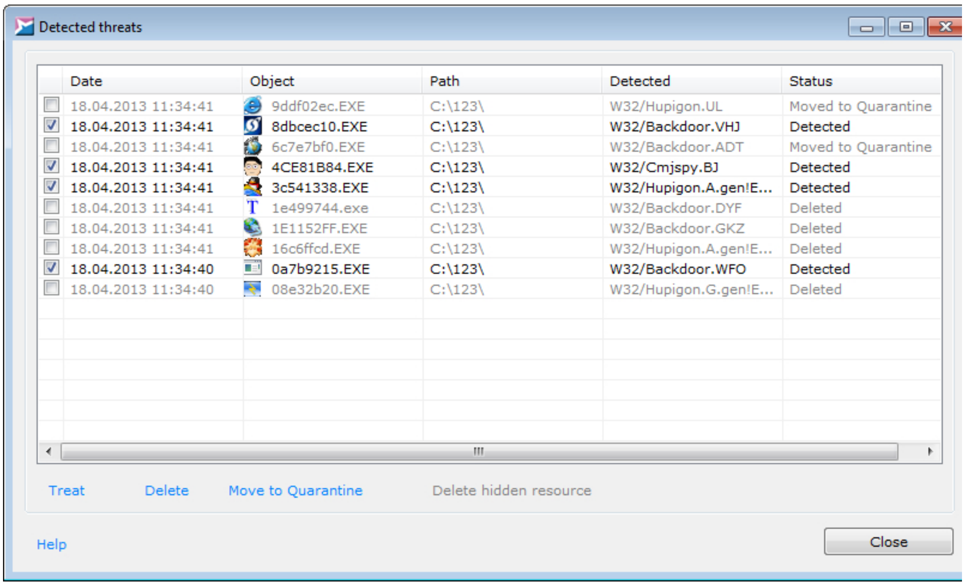
□ Apply selected action for all objects.

Figure 88. 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. It is shown in fig. Window with the detected threats[99].



Detected threats

	Date	Object	Path	Detected	Status
□	18.04.2013 11:34:41	9ddf02ec.EXE	C:\123\	W32/Hupigon.UL	Moved to Quarantine
☑	18.04.2013 11:34:41	8dbcec10.EXE	C:\123\	W32/Backdoor.VHJ	Detected
□	18.04.2013 11:34:41	6c7e7bf0.EXE	C:\123\	W32/Backdoor.ADT	Moved to Quarantine
☑	18.04.2013 11:34:41	4CE81B84.EXE	C:\123\	W32/Cmjspy.BJ	Detected
☑	18.04.2013 11:34:41	3c541338.EXE	C:\123\	W32/Hupigon.A.gen!E...	Detected
□	18.04.2013 11:34:41	1e499744.exe	C:\123\	W32/Backdoor.DYF	Deleted
□	18.04.2013 11:34:41	1E1152FF.EXE	C:\123\	W32/Backdoor.GKZ	Deleted
□	18.04.2013 11:34:41	16c6ffcd.EXE	C:\123\	W32/Hupigon.A.gen!E...	Deleted
☑	18.04.2013 11:34:40	0a7b9215.EXE	C:\123\	W32/Backdoor.WFO	Detected
□	18.04.2013 11:34:40	08e32b20.EXE	C:\123\	W32/Hupigon.G.gen!E...	Deleted

Figure 89. 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 (34). You can view the list of the threats and actions applied to them, in the **Detected threats** window (fig. Window with the detected threats (99)).

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 control panel (34).

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 control panel (34).

5.7 Reports

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

- Text logs (101);
- Registering the events in Windows Management Instrumentation (WMI) (104).

5.7.1 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 application activity 48 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 control policy 68 violation and their parameters: the name, activity type, account, the program which is the source of the incident, the file being controlled, the solution, and the number of similar events that have been skipped (see above 53);
  - UID of the rule where the control policy 68 has been violated;
  - the name of the settings received from the server.
- **Profile gathering** log with the following data:
  - profile gathering 43 scope;
  - the list of the checked objects;
  - profile gathering 43 results.
- **Scan** log with the following data:
  - scan scope 97;
  - settings for the response to a threat 93;
  - scan results 98.
- **Update** log with information about the installed program updates 114.

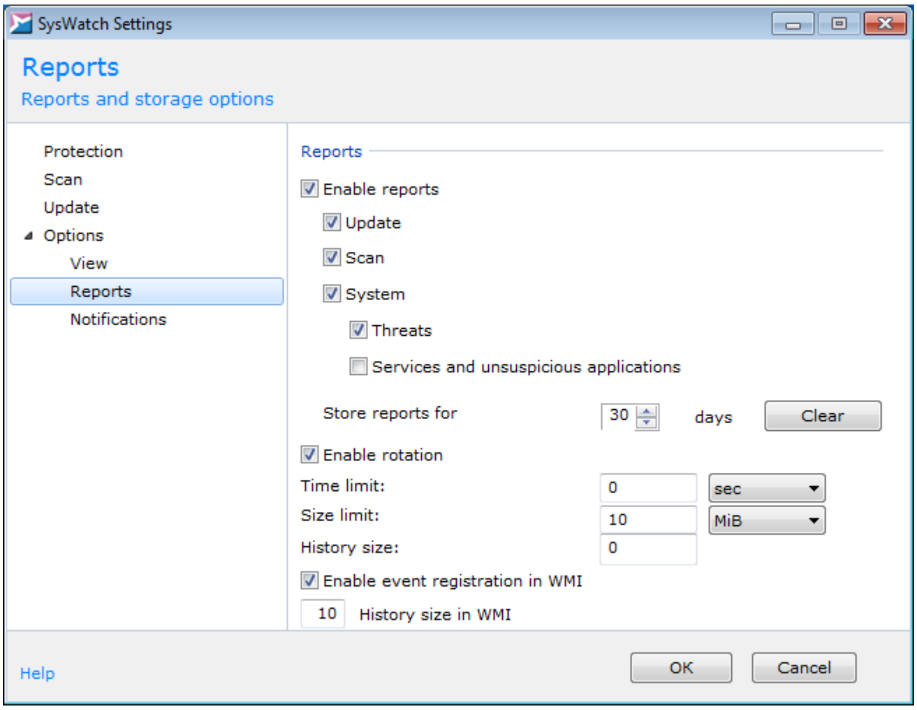
Setting up report generating parameters

To view and modify the log parameters, open program settings and select **Options** → **Reports** (fig. Specifying the report parameters 102).

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

- □ **Update**;
- □ **Scan**;
- □ **System**:
  - □ **Threats**;
  - □ **Services and unsuspicious applications**.

Tick off **Services and unsuspicious applications** to enable the recording of events when the services start and stop. The services that have started before the *safensec.exe* system service are marked as *was started before* in the reports.



Reports

☑ Enable reports

☑ Update

☑ Scan

☑ System

☑ Threats

☐ Services and unsuspicious applications

Store reports for 30 days

☑ Enable rotation

Time limit: 0 sec

Size limit: 10 MiB

History size: 0

☑ Enable event registration in WMI

10 History size in WMI

Figure 90. Specifying the report parameters

Specify the number of days during which the event history is stored, in the **Store reports for** counter. To delete all report files, click **Clear**.

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**.

The rotation of the latest report (by time and by size) and the deletion (clean up) of all the report files work independently. For example, let us set the **Do not store reports longer than** option to 10 days, the **Time limit** option to 1 day, and the **History size** option to 1. Then files of the following type are created each day: *<report type>_<dd.mm.yy>_ <hh.mm.ss.mmm>.txt* and *<report type>_<dd.mm.yy>_<hh.mm.ss.mmm>.txt.1*. Once a day, the *<report type>_<dd.mm.yy>_<hh.mm.ss.mmm>.txt.1* file is deleted, the extension of the *<report type>_<dd.mm.yy>_<hh.mm.ss.mmm>.txt* file changes to *.txt.1*, and a new *<report type>_<dd.mm.yy>_<hh.mm.ss.mmm>.txt* file is created which the subsequent events are logged to.

However, if the computer or the *safensec.exe* system service has been restarted during the specified period (one day in this case), a new *<report type>_<new_date>_ <hh.mm.ss.mmm>.txt* file is created. The next day, a new *<report type>_<new_date>_ <hh.mm.ss.mmm>.txt.1* file is created. The rotation of the reports described above is then applied only to these two files. The *<report type>_<dd.mm.yy>_<hh.mm.ss.mmm>.txt* and *<report type>_<dd.mm.yy>_<hh.mm.ss.mmm>.txt.1* files are stored without changes for 10 days and are then deleted.

Viewing the reports

To view text logs, select **Reports** in the SoftControl SysWatch context menu[33]. 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.

5.7.2 Registering the events in WMI

SoftControl SysWatch can log aggregated information about the events and program status directly to the WMI objects. 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.

A 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	
	• *Network Control* – 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 on its own can switch *SystemScan* to the following status only:

- *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 **Options** → **Reports** (fig. Specifying the report parameters 102).

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

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**.

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 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.

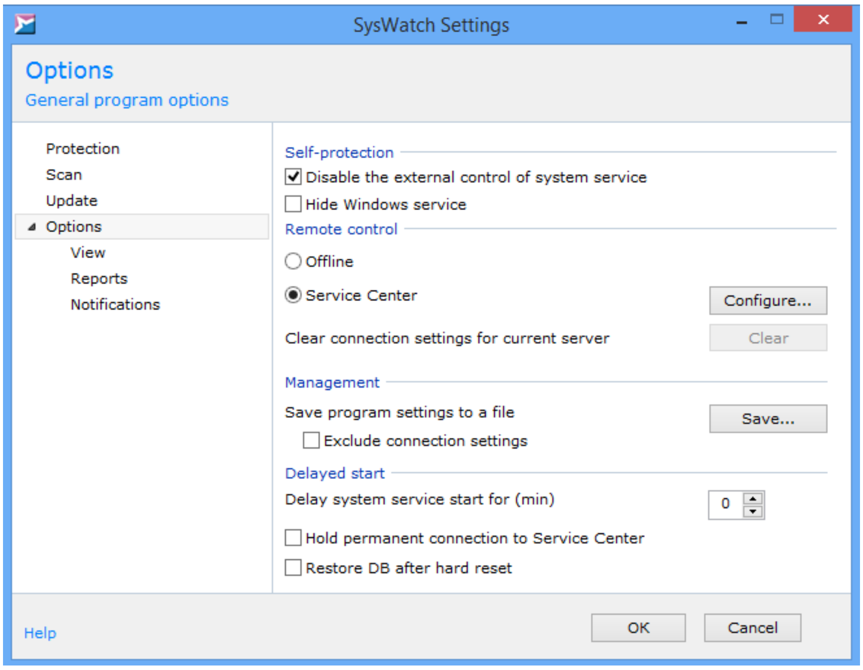
5.8 Setting up general program parameters

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

- system service self-protection (106);
- password protection (108);
- delayed start of the system service (109);
- DB restoration after hard reset (110).

5.8.1 Self-protection of the system service

To enable self-protection of the SoftControl SysWatch system service (*safensec.exe*), select the **Options** 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 (106)).



SysWatch Settings

Options

General program options

- Protection
- Scan
- Update
- Options
  - View
  - Reports
  - Notifications

Self-protection

☑ Disable the external control of system service

□ Hide Windows service

Remote control

○ Offline

● Service Center [Configure...]

Clear connection settings for current server [Clear]

Management

Save program settings to a file [Save...]

□ Exclude connection settings

Delayed start

Delay system service start for (min) 0

□ Hold permanent connection to Service Center

□ Restore DB after hard reset

Help [OK] [Cancel]

Figure 91. Setting up the program parameters

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

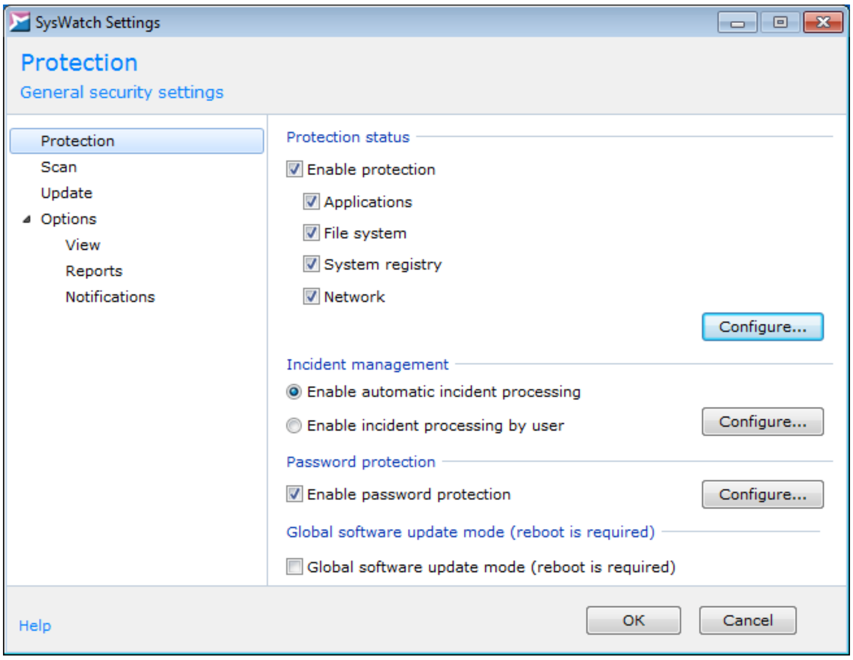
Tick off **Hide Windows service** if the SoftControl SysWatch system service (*safensec.exe*) should be hidden from the Windows **Services** snap-in. This way, managing the system service with any OS tools becomes impossible.

Note: hiding the system service does not work on Windows XP.

To apply changes, click **OK**.

5.8.2 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[108]).



Protection status
☑ Enable protection
☑ Applications
☑ File system
☑ System registry
☑ Network

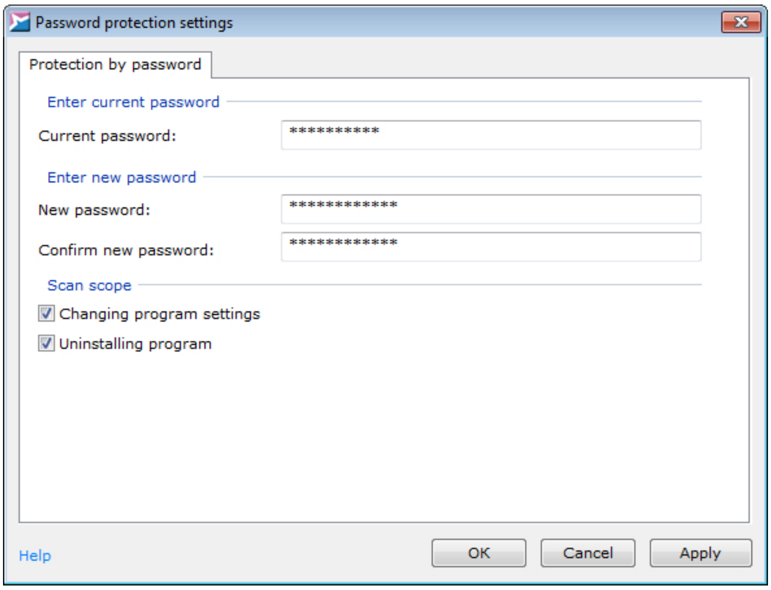
Incident management
● Enable automatic incident processing
○ Enable incident processing by user

Password protection
☑ Enable password protection

Global software update mode (reboot is required)
□ Global software update mode (reboot is required)

Figure 92. 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[108]):



Enter current password
Current password: ***********

Enter new password
New password: ************
Confirm new password: ************

Scan scope
☑ Changing program settings
☑ Uninstalling program

Figure 93. Setting up password protection

❑ Changing the settings

request the password when accessing SoftControl SysWatch control panel[34] and settings.

- ❑ **Uninstalling the program**

  request the password when uninstalling[124] SoftControl SysWatch.

The password should be at least 7 characters long.

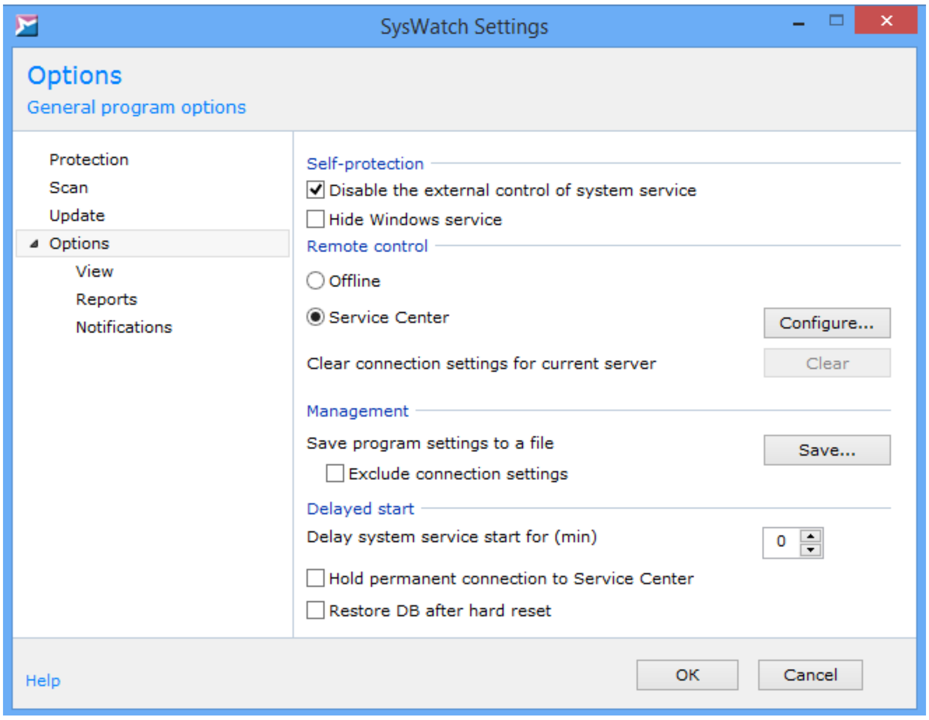
To confirm changes, click **OK** in both settings window.

5.8.3 Delayed start of the system service

In SoftControl SysWatch, you can specify the interval for the delayed start of the 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 **Options** section of the program settings and specify **Delay system service start for (min)** in the **Delayed start** area (fig. Setting up the program parameters[109]).

When SoftControl SysWatch system service restarts next time, its loading is delayed for the specified value. To confirm changes, click **OK**.



SysWatch Settings

Options
General program options

Self-protection
☑ Disable the external control of system service
□ Hide Windows service

Remote control
○ Offline
● Service Center
Clear connection settings for current server

Management
Save program settings to a file
□ Exclude connection settings

Delayed start
Delay system service start for (min): 0
□ Hold permanent connection to Service Center
□ Restore DB after hard reset

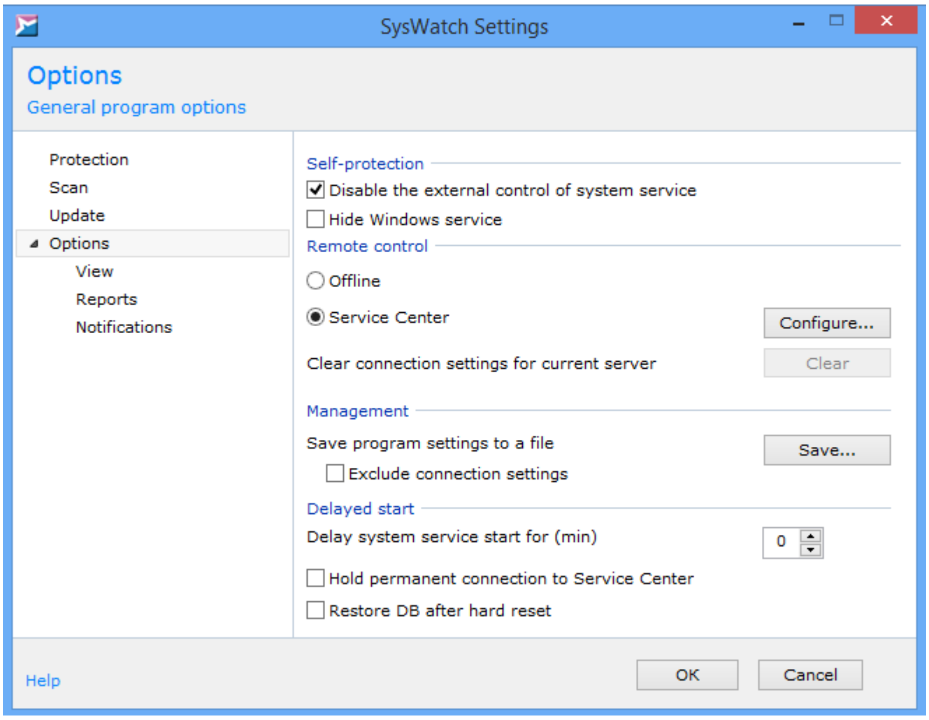
Figure 94. Setting up the program parameters

If the protection is turned off, all applications (both in the profile and outside of it) are given permission to run until the system service starts.

Tick off **Hold permanent connection to Service Center** if you need to maintain connection to SoftControl Service Center in real time.

5.8.4 DB restoration after hard reset

SoftControl SysWatch backs up the database at startup, when new settings arrive from the server, or when you change settings locally. If you wish to restore the database from the most recent copy in case of a hard reset, check **Restore DB after hard reset** in **Options** (fig. Setting up the program parameters[110]).



Self-protection

☑ Disable the external control of system service

□ Hide Windows service

Remote control

○ Offline

● Service Center

Clear connection settings for current server

Management

Save program settings to a file

□ Exclude connection settings

Delayed start

Delay system service start for (min) 0

□ Hold permanent connection to Service Center

□ Restore DB after hard reset

Figure 95. Setting up the program parameters

5.9 Saving and restoring the settings

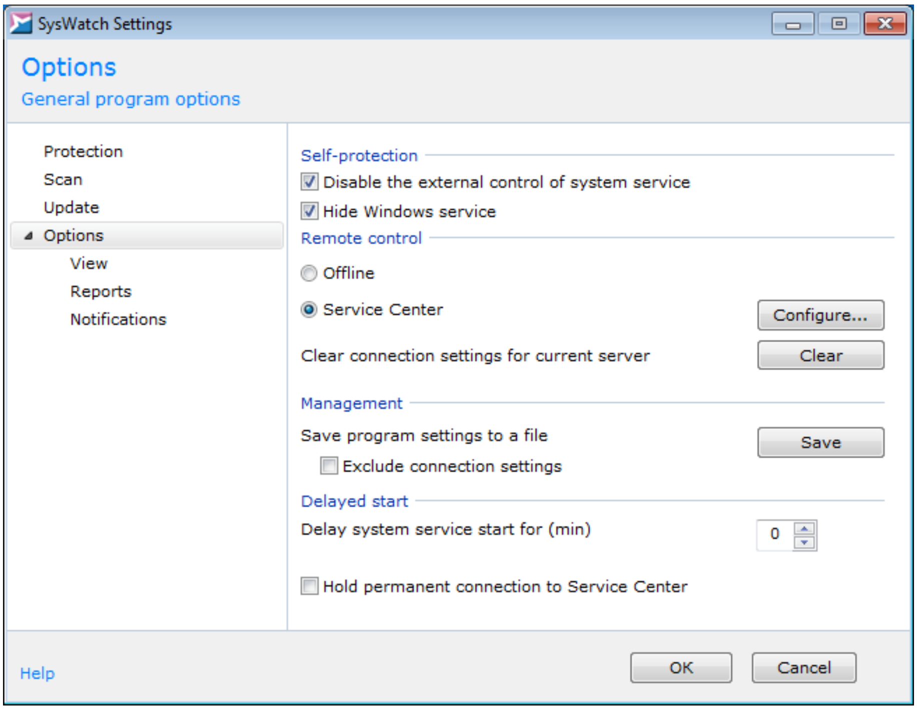
You can export full SoftControl SysWatch configuration, including customized control policies, the whitelist of certificates and current program password, to the main configuration file[111]. You can use this file to install the program in silent mode on other client hosts (to clone the program from a sample protected object) and to remove the program in silent mode.

5.9.1 Exporting main configuration file

To save current settings of SoftControl SysWatch, open the **Options** section of the program settings and click **Save** in the **Management** area (fig. Setting up the program parameters[111]). 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[113].



Self-protection

☑ Disable the external control of system service

☑ Hide Windows service

Remote control

○ Offline

● Service Center

Clear connection settings for current server

Management

Save program settings to a file

□ Exclude connection settings

Delayed start

Delay system service start for (min) 0

□ Hold permanent connection to Service Center

Figure 96. Setting up the program parameters

6. SoftControl SysWatch advanced features

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

6.1 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 ARUDIT SECURITY, LLC company on 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 112;
- snsdumpsetting 113.

6.1.1 changetpsmode

The *changetpsmode.exe* utility is designed to manage the global installation mode 48 and to run the antivirus scanning 92 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+311FKIrNqIGIqkxXGfZWXb) 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 101. Attention: to correctly run silent mode scanning, you should observe the specified command syntax. If you want to perform several checks, run a new check only after

Option	Action
	the previous one completes.

6.1.2 snsdumpsetting

The *snsdumpsetting.exe* utility is intended for exporting the main configuration file[111] 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).

7. 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.

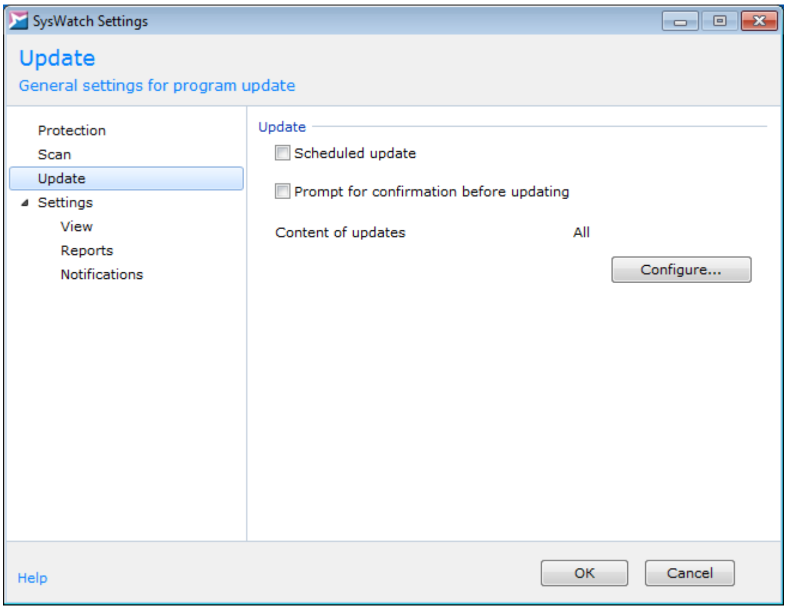
Necessary actions to update SoftControl SysWatch are described below:

- update options 114;
- update in standard mode 117.

If the update source is unavailable, perform the update in manual mode 118.

7.1 Update options

To set up the update parameters, open the **Update** section of the program settings (fig. Update options 114).



SysWatch Settings

Update

General settings for program update

Update

□ Scheduled update

□ Prompt for confirmation before updating

Content of updates All

Figure 97. Update options

Setting up update source and components

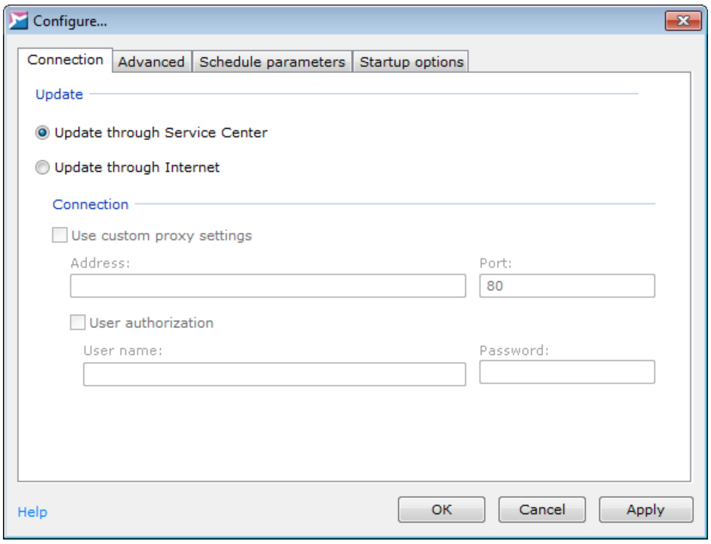
The **Content of updates** string lists the components to be updated. To configure the contents and other update options, click **Configure**.

Select the update method on the **Connection** tab of the **Configure...** window (fig. Selecting the update method 115):

- **Update through Service Center**: update via the intranet update server (in case of remote control from the server 40);

- **Update through Internet**: update via ARUDIT SECURITY, LLC server available via the Internet.

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.



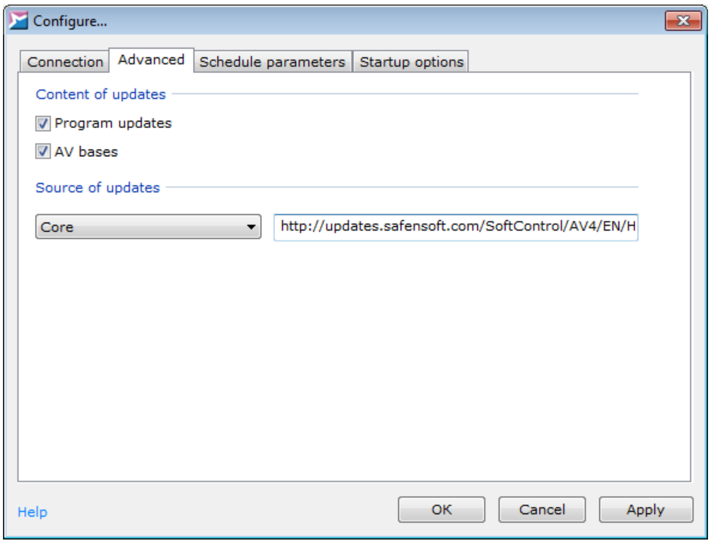
Update
● Update through Service Center
○ Update through Internet

Connection
□ Use custom proxy settings
Address:
Port: 80
□ User authorization
User name:
Password:

Figure 98. Selecting the update method

Select the required components to update on the **Advanced** tab of the **Configure...** window (fig. Selecting components to update[115]):

- ❑ **Program updates**;
- ❑ **AV bases**.



Content of updates
☑ Program updates
☑ AV bases

Source of updates
Core
http://updates.safensoft.com/SoftControl/AV4/EN/H

Figure 99. Selecting components to update

SoftControl SysWatch uses the addresses from the **Source of updates** area to update the proactive protection core and antivirus bases that are available according to the license[42]. You can edit these addresses in the corresponding field if necessary.

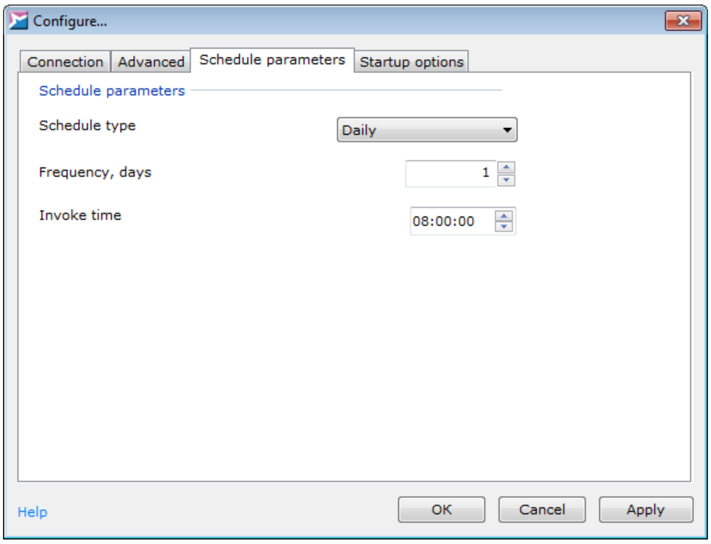
To apply settings, click **OK** or **Apply**.

Setting up the update schedule

Condition: only for remote control from the server[40].

To enable automatic **Scheduled update**, tick off the corresponding option. If you need to **Prompt for confirmation before 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 **Frequency, days** counter and the start time in the *hh:mm:ss* format in the **Invoke time** field (fig. Parameters of scheduled update[116]).



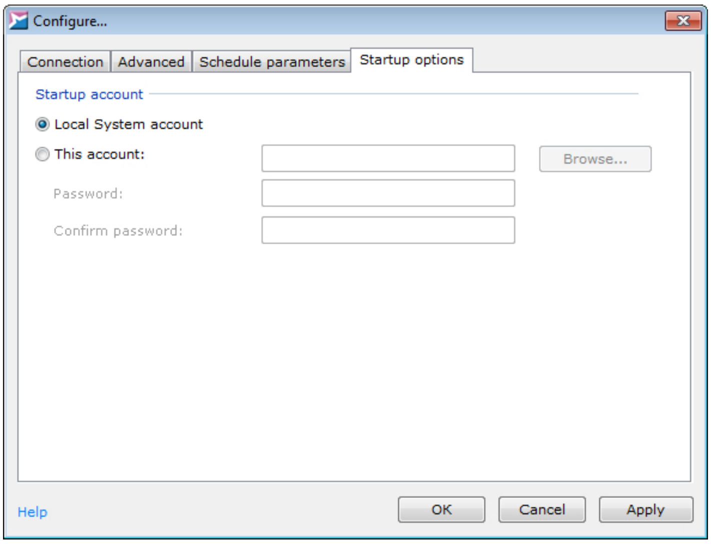
Schedule type: Daily
Frequency, days: 1
Invoke time: 08:00:00

Figure 100. 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. Setting up user account to perform the update[116]):



Startup account

● Local System account

○ This account:

Password:

Confirm password:

Figure 101. 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.

7.2 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[115]).

Updating program modules on demand

Click **Run update** in the **Update** section of the SoftControl SysWatch control panel[34]. 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[34]. 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 newupdates* 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[116], 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[101] after the update completes, click the link with the date and time of the last check, in the **Last update check** string.

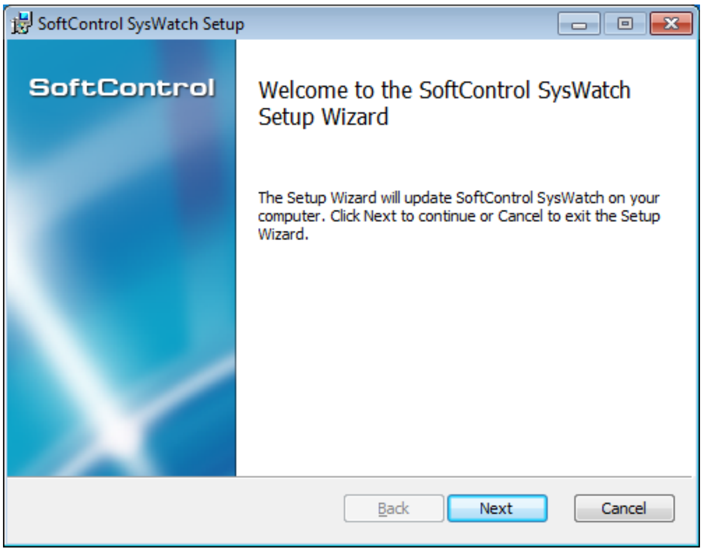
The **Installed updates** string displays the date and time the last update. The **Update mode** string indicates how the last update has been started (on demand or on schedule).

7.3 Updating the component manually

Updating program modules manually in standard mode

1) Run the *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[118]).

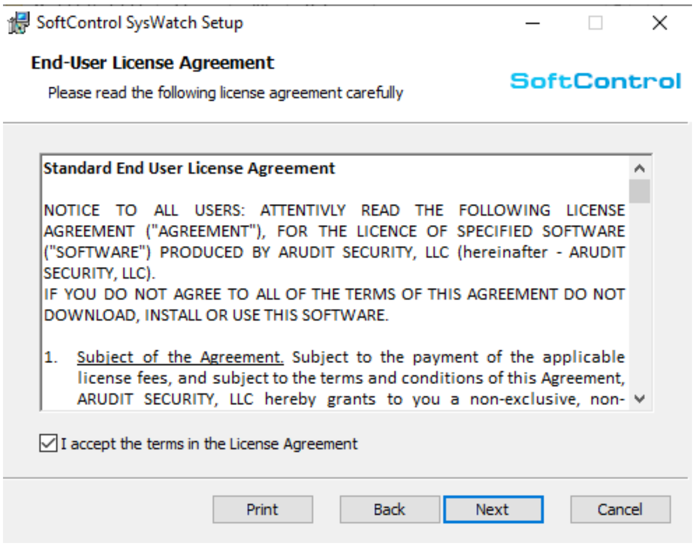


Welcome to the SoftControl SysWatch Setup Wizard

The Setup Wizard will update SoftControl SysWatch on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Figure 102. Running the update

3) If you accept the terms, select **I accept the terms in the License Agreement** and click **Next** (fig. License agreement[119]).



End-User License Agreement

Please read the following license agreement carefully

Standard End User License Agreement

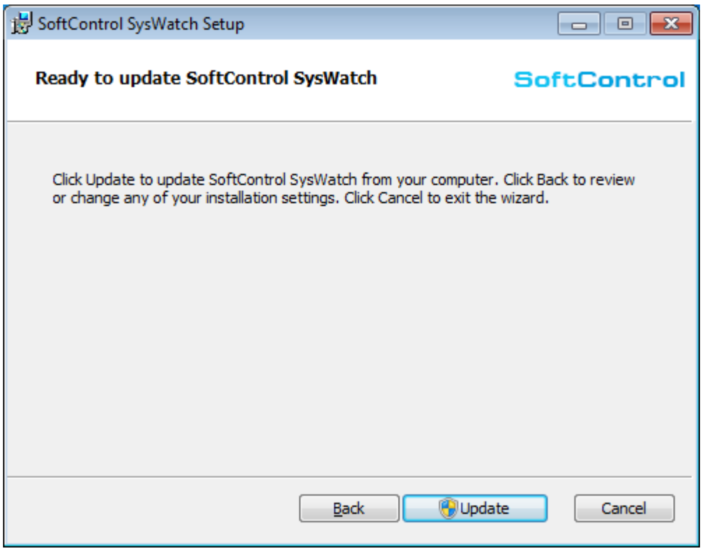
NOTICE TO ALL USERS: ATTENTIVLY READ THE FOLLOWING LICENSE AGREEMENT ("AGREEMENT"), FOR THE LICENCE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY ARUDIT SECURITY, LLC (hereinafter - ARUDIT SECURITY, LLC).
IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

1. Subject of the Agreement. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, ARUDIT SECURITY, LLC hereby grants to you a non-exclusive, non-

☑ I accept the terms in the License Agreement

Figure 103. License agreement

4) Click **Update** (fig. Ready to update[119]).



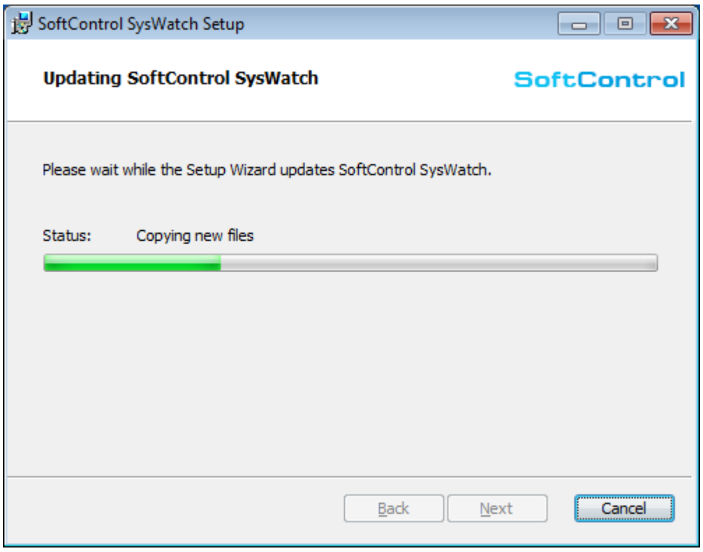
SoftControl SysWatch Setup

Ready to update SoftControl SysWatch

Click Update to update SoftControl SysWatch from your computer. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Figure 104. Ready to update

5) Wait until the update completes (fig. Updating progress (120)).



SoftControl SysWatch Setup

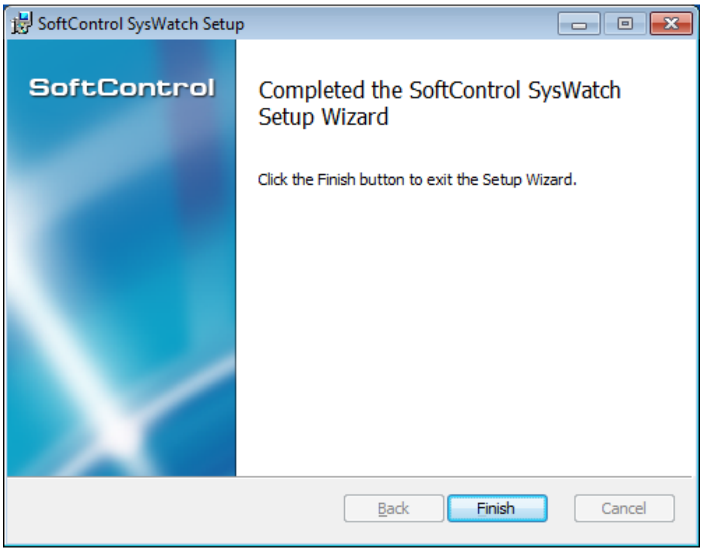
Updating SoftControl SysWatch

Please wait while the Setup Wizard updates SoftControl SysWatch.

Status: Copying new files

Figure 105. Updating progress

6) After the **Completed the SoftControl SysWatch Setup Wizard** message is displayed, click **Finish** (fig. Update completes (120)).



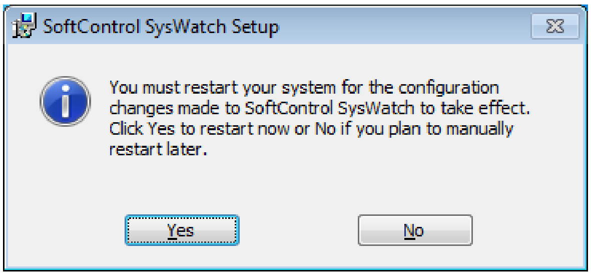
SoftControl SysWatch Setup

Completed the SoftControl SysWatch Setup Wizard

Click the Finish button to exit the Setup Wizard.

Figure 106. 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[121]).



SoftControl SysWatch Setup

You must restart your system for the configuration changes made to SoftControl SysWatch to take effect. Click Yes to restart now or No if you plan to manually restart later.

Figure 107. Requesting system restart

Updating program modules manually in silent mode

Important: all steps require administrator privileges.

1) Copy the *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\SysWatch_Patch.msi" /quiet
```

After the update completes, system restarts automatically.

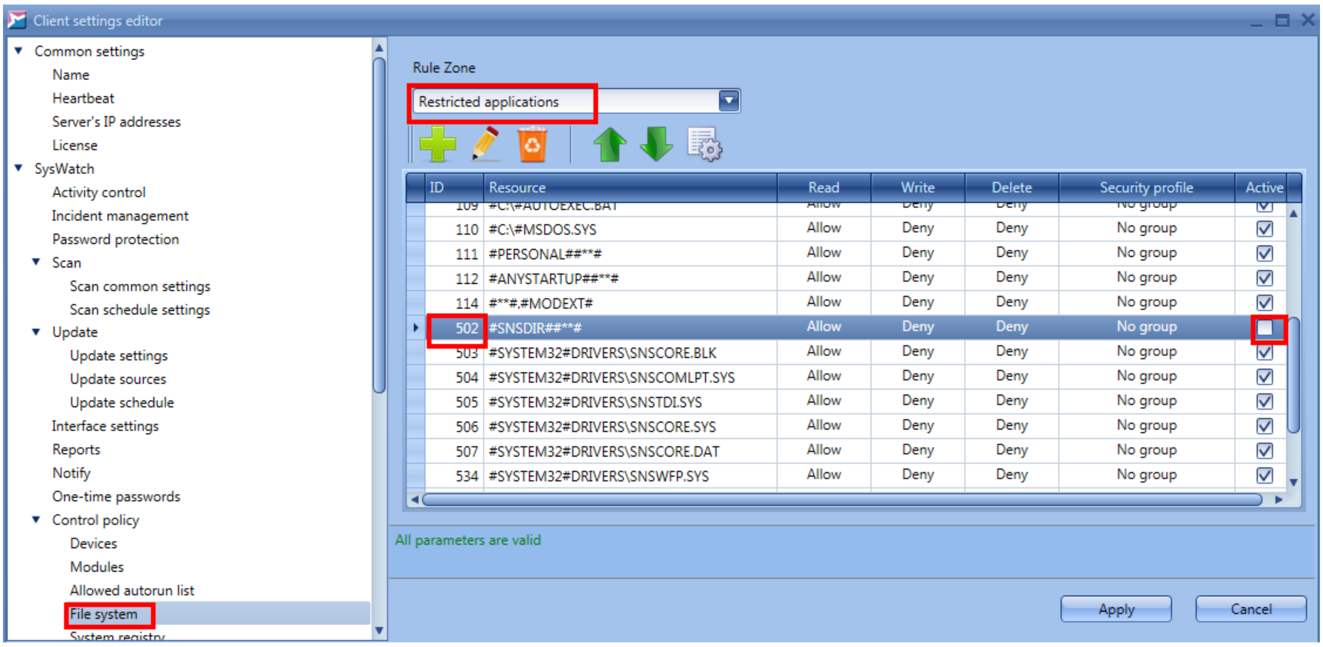
Updating antivirus bases manually

To update antivirus bases manually, perform the following steps:

1) Update the antivirus bases on the test device by any means available to you.

2) Copy the new contents of the folder with the antivirus bases (e.g., `<SoftControl SysWatch installation directory>\Plugins\AV\Av4` for AV4) to an external storage medium.

3) Uncheck rule 502 in client settings (**Control policy –> File system**) for both rule zones (**Restricted applications** and **Trusted applications**). Save the settings under a new name and apply them to the organizational unit of the device that you wish to update antivirus bases on.

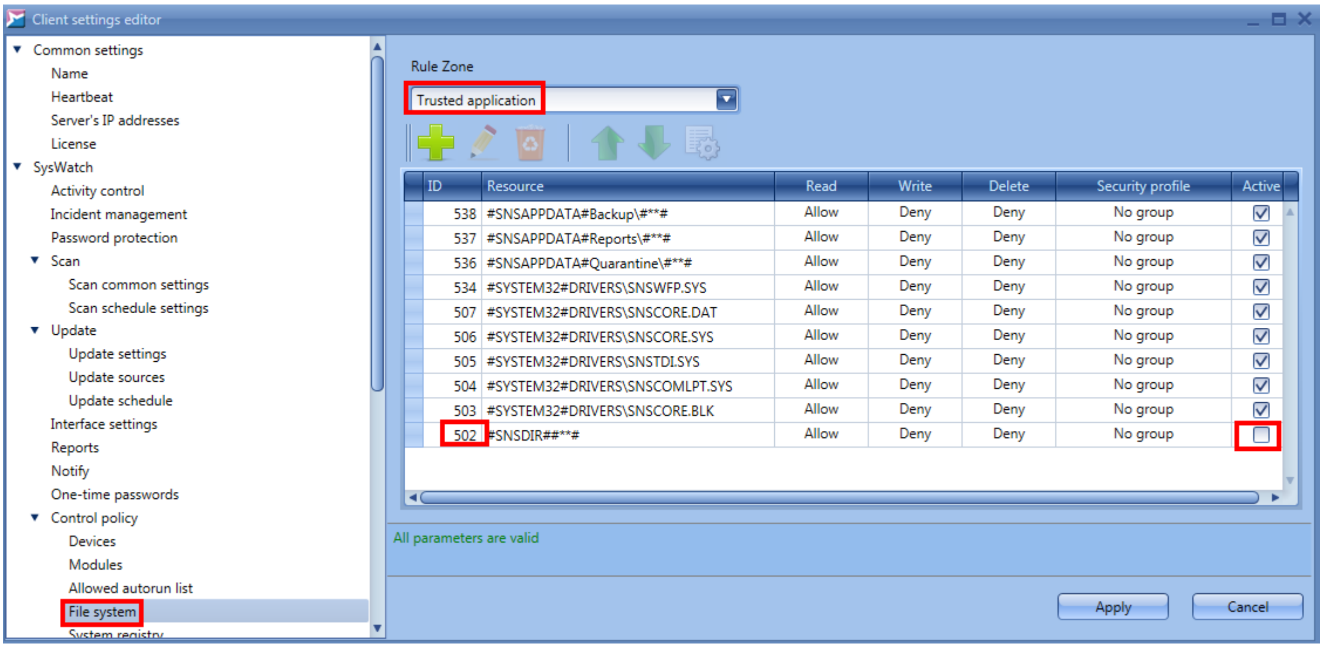


Rule Zone: Restricted applications

ID	Resource	Read	Write	Delete	Security profile	Active
109	#C:\#AUTOEXEC.BAT	Allow	Deny	Deny	No group	☑
110	#C:\#MSDOS.SYS	Allow	Deny	Deny	No group	☑
111	#PERSONAL##**#	Allow	Deny	Deny	No group	☑
112	#ANYSTARTUP##**#	Allow	Deny	Deny	No group	☑
114	#**#.#MODEXT#	Allow	Deny	Deny	No group	☑
502	#SNSDIR##**#	Allow	Deny	Deny	No group	□
503	#SYSTEM32#DRIVERS\SNSCORE.BLK	Allow	Deny	Deny	No group	☑
504	#SYSTEM32#DRIVERS\SNSCOMLPT.SYS	Allow	Deny	Deny	No group	☑
505	#SYSTEM32#DRIVERS\SNSTDI.SYS	Allow	Deny	Deny	No group	☑
506	#SYSTEM32#DRIVERS\SNSCORE.SYS	Allow	Deny	Deny	No group	☑
507	#SYSTEM32#DRIVERS\SNSCORE.DAT	Allow	Deny	Deny	No group	☑
534	#SYSTEM32#DRIVERS\SNSWFP.SYS	Allow	Deny	Deny	No group	☑

All parameters are valid

Figure 108. Uncheck rule 502 in client settings. Restricted applications



Rule Zone: Trusted application

ID	Resource	Read	Write	Delete	Security profile	Active
538	#SNSAPPDATA#Backup\#**#	Allow	Deny	Deny	No group	☑
537	#SNSAPPDATA#Reports\#**#	Allow	Deny	Deny	No group	☑
536	#SNSAPPDATA#Quarantine\#**#	Allow	Deny	Deny	No group	☑
534	#SYSTEM32#DRIVERS\SNSWFP.SYS	Allow	Deny	Deny	No group	☑
507	#SYSTEM32#DRIVERS\SNSCORE.DAT	Allow	Deny	Deny	No group	☑
506	#SYSTEM32#DRIVERS\SNSCORE.SYS	Allow	Deny	Deny	No group	☑
505	#SYSTEM32#DRIVERS\SNSTDI.SYS	Allow	Deny	Deny	No group	☑
504	#SYSTEM32#DRIVERS\SNSCOMLPT.SYS	Allow	Deny	Deny	No group	☑
503	#SYSTEM32#DRIVERS\SNSCORE.BLK	Allow	Deny	Deny	No group	☑
502	#SNSDIR##**#	Allow	Deny	Deny	No group	□

All parameters are valid

Figure 109. Uncheck rule 502 in client settings. Trusted applications

4) Copy the folder with the antivirus bases from the external storage medium to the corresponding directory (for *AV4*, it is <`SoftControl SysWatch installation directory>\Plugins\AV\Av4`) on the device for which you are updating antivirus bases (and overwrite the existing files).

5) Check rule 502 in client settings for both rule zones (**Restricted applications** and **Trusted applications**) and apply the settings to the organizational unit of the device you are updating antivirus bases on.

8. Removing SoftControl SysWatch

SoftControl SysWatch can be uninstalled from the client hosts either locally 124 or in one of the remote centralized 125 methods.

8.1 Local uninstallation

You can remove SoftControl SysWatch locally in the following ways.

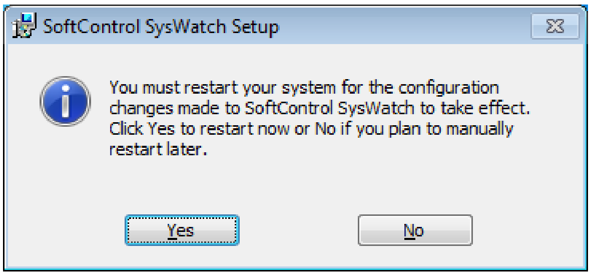
- standard mode (via GUI) 124;
- silent mode 124.

8.1.1 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. Requesting system restart 124).



SoftControl SysWatch Setup

You must restart your system for the configuration changes made to SoftControl SysWatch to take effect. Click Yes to restart now or No if you plan to manually restart later.

Figure 110. Requesting system restart

8.1.2 Uninstalling the component in silent mode

Important: all steps require administrator privileges.

1) Copy the *SysWatch.msi* installation package (or *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\SysWatch.msi" /quiet
```

After the program is removed, system restarts automatically.

8.2 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.

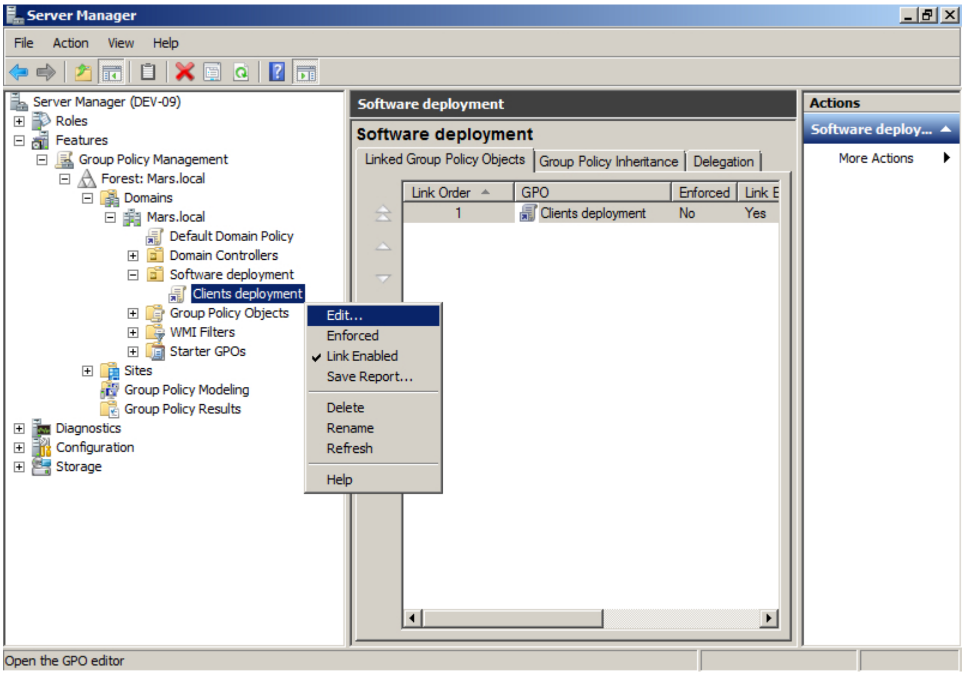
- via domain group policy 125;
- via third party administrative tools 127.

8.2.1 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 19 group policy object for the client application deployment (**Clients deployment**), and select **Edit** (fig. Modifying a group policy object 125).

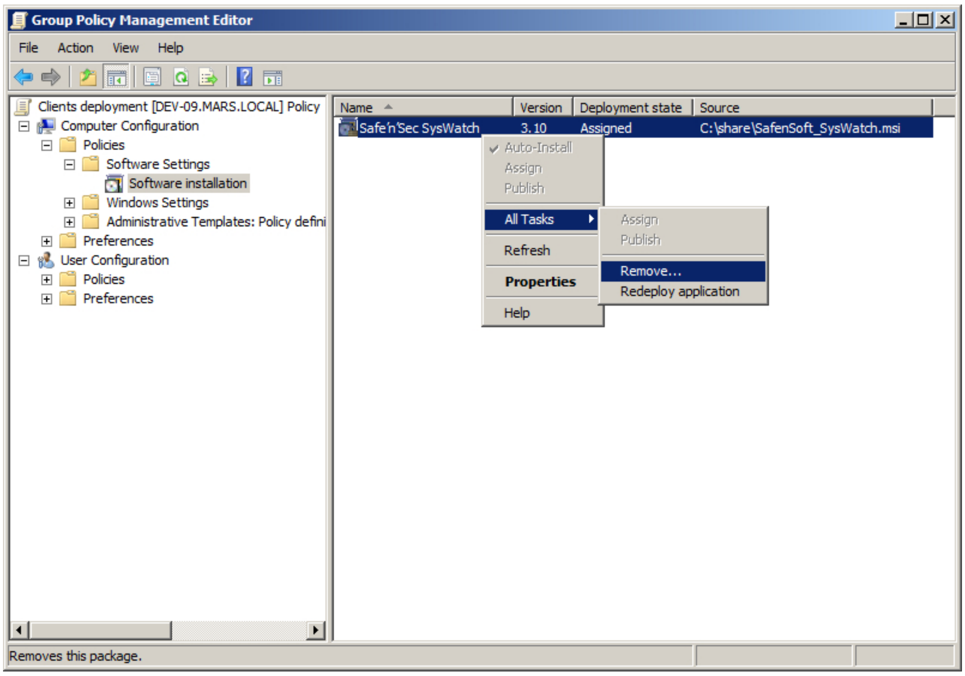


Link Order	GPO	Enforced	Link E
1	Clients deployment	No	Yes

Figure 111. Modifying a group policy object

3) Select the **Computer configuration** → **Policies** → **Software Settings** → **Software installa-**

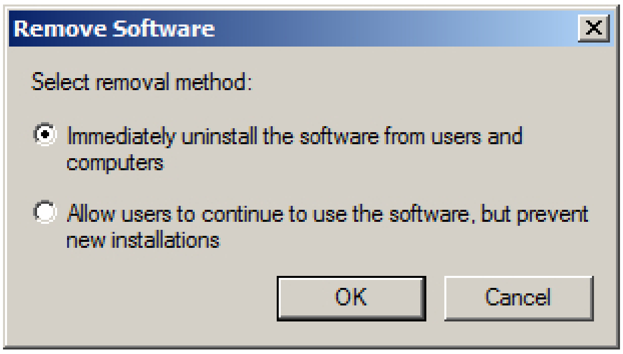
tion section in the displayed **Group Policy Management Editor** snap-in window, select the application to remove from the list of applications, invoke its context menu and select **All tasks** → **Remove** (fig. Invoking the application removal task[126]).



Name	Version	Deployment state	Source
Safe'n'Sec SysWatch	3.10	Assigned	C:\share\SafenSoft_SysWatch.msi

Figure 112. 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[126]).



Remove Software

Select removal method:

● Immediately uninstall the software from users and computers

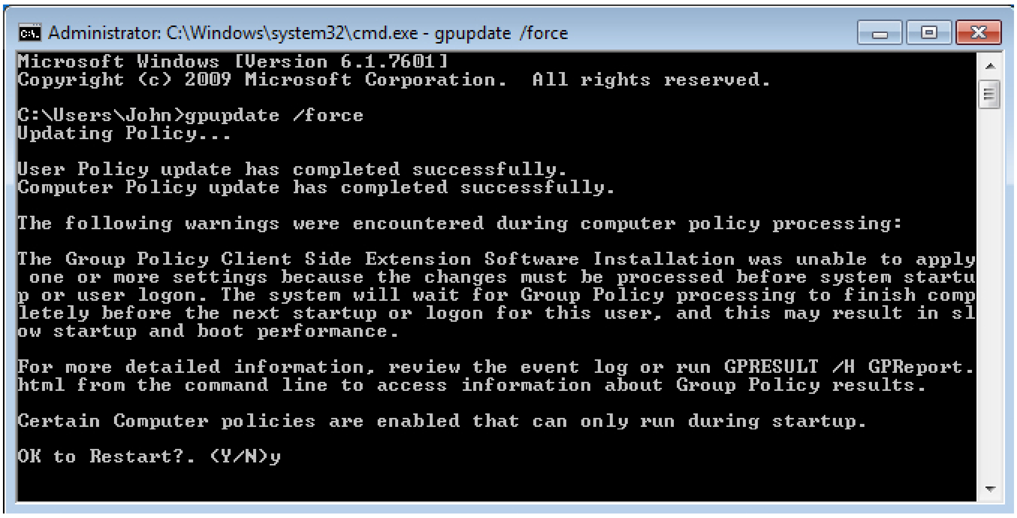
○ Allow users to continue to use the software, but prevent new installations

Figure 113. 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[127]).


Administrator: C:\Windows\system32\cmd.exe - gpupdate /force

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\John>gpupdate /force
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.

The following warnings were encountered during computer policy processing:

The Group Policy Client Side Extension Software Installation was unable to apply
 one or more settings because the changes must be processed before system startu
p or user logon. The system will wait for Group Policy processing to finish comp
letely before the next startup or logon for this user, and this may result in sl
ow startup and boot performance.

For more detailed information, review the event log or run GPRESULT /H GPReport.
html from the command line to access information about Group Policy results.

Certain Computer policies are enabled that can only run during startup.

OK to Restart?. (Y/N)y
```

Figure 114. Updating the group policy parameters manually

8.2.2 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.

9. Customer support

If you have any questions concerning the installation, setting up and operation of SoftControl ATM Client, please contact our 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 anti-virus software.

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

- Dr.Web® Antivirus 129.

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. Selecting the main settings of the program 129).

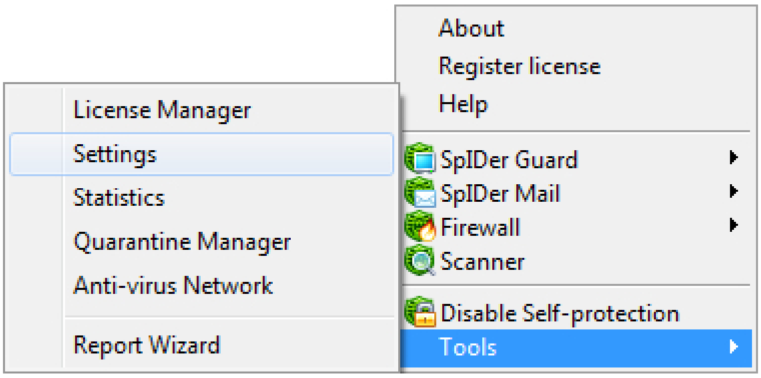
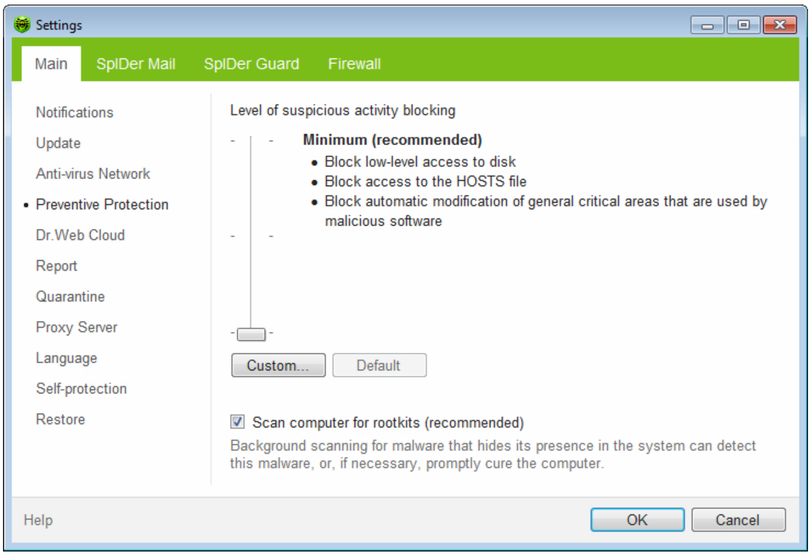


Figure 115. Selecting the main settings of the program

2) Open the **Preventive Protection** section of the **Main** category and click **Custom** to open the detailed settings (fig. Preventive protection settings 129).



Notifications
Update
Anti-virus Network
- Preventive Protection
Dr.Web Cloud
Report
Quarantine
Proxy Server
Language
Self-protection
Restore

Level of suspicious activity blocking

Minimum (recommended)

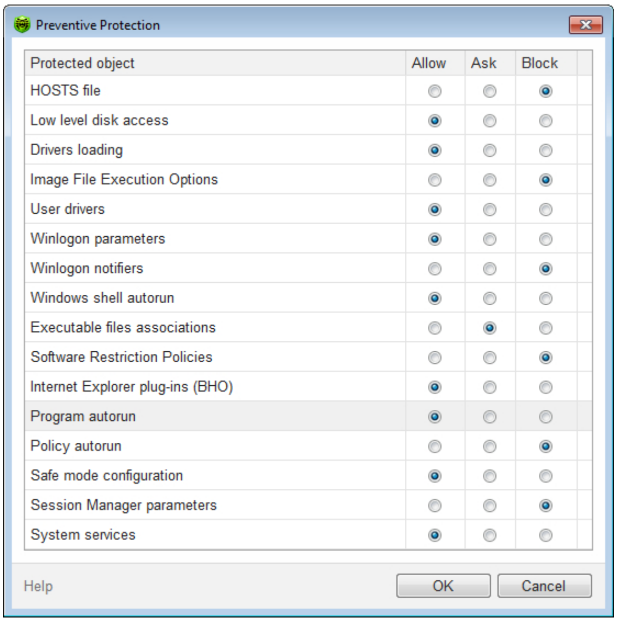
- Block low-level access to disk
- Block access to the HOSTS file
- Block automatic modification of general critical areas that are used by malicious software

☑ Scan computer for rootkits (recommended)

Background scanning for malware that hides its presence in the system can detect this malware, or, if necessary, promptly cure the computer.

Figure 116. Preventive protection settings

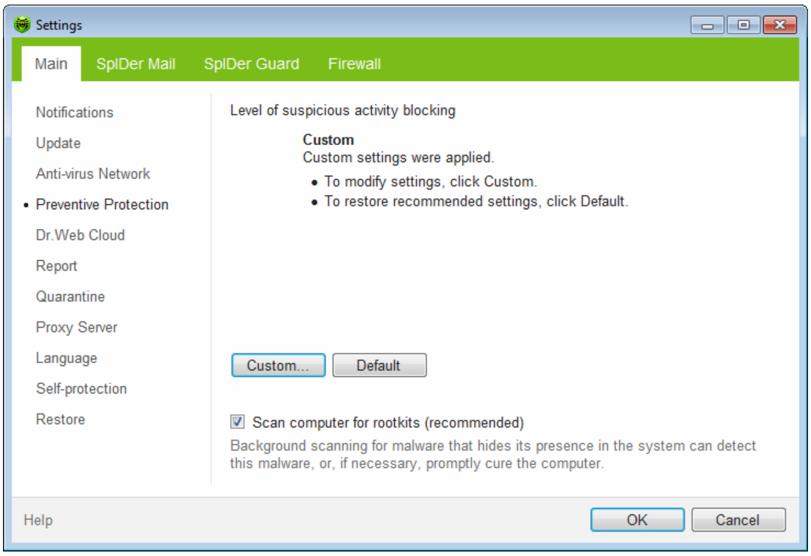
3) Move the **Program autorun** and **Safe mode configuration** switches to the **Allow** state and click **OK** (fig. Custom settings for preventive protection 130).



Protected object	Allow	Ask	Block
HOSTS file	○	○	●
Low level disk access	●	○	○
Drivers loading	●	○	○
Image File Execution Options	○	○	●
User drivers	●	○	○
Winlogon parameters	●	○	○
Winlogon notifiers	○	○	●
Windows shell autorun	●	○	○
Executable files associations	○	●	○
Software Restriction Policies	○	○	●
Internet Explorer plug-ins (BHO)	●	○	○
Program autorun	●	○	○
Policy autorun	○	○	●
Safe mode configuration	●	○	○
Session Manager parameters	○	○	●
System services	●	○	○

Figure 117. Custom settings for preventive protection

4) Confirm the changes in the main settings window by clicking **OK** (fig. Preventive protection settings 130).



Settings

Main | SpIDer Mail | SpIDer Guard | Firewall

- Notifications
- Update
- Anti-virus Network
- • Preventive Protection
- Dr.Web Cloud
- Report
- Quarantine
- Proxy Server
- Language
- Self-protection
- Restore

Level of suspicious activity blocking

Custom
Custom settings were applied.

- To modify settings, click Custom.
- To restore recommended settings, click Default.

Custom... | Default

☑ Scan computer for rootkits (recommended)

Background scanning for malware that hides its presence in the system can detect this malware, or, if necessary, promptly cure the computer.

Help | OK | Cancel

Figure 118. Preventive protection settings

5) Turn off the SpIDer Guard protection component by selecting the **SpIDer Guard** → **Disable** item in the context menu (fig. Disabling SpIDer Guard[131]).

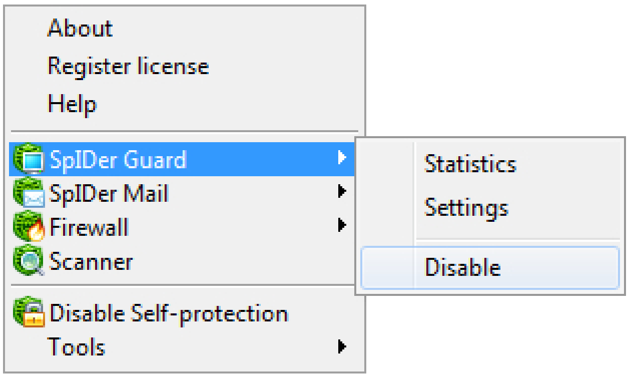
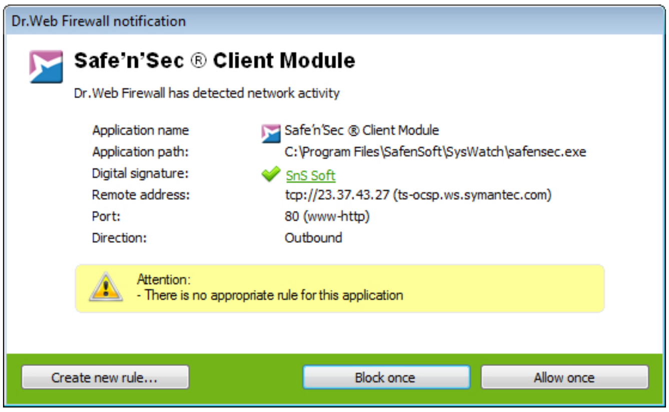


Figure 119. Disabling SpIDer Guard

6) Run SoftControl SysWatch installation[14].

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. Dr.Web® Firewall notification[131], Creating a rule in Dr.Web® Firewall[132]).



Dr.Web Firewall notification

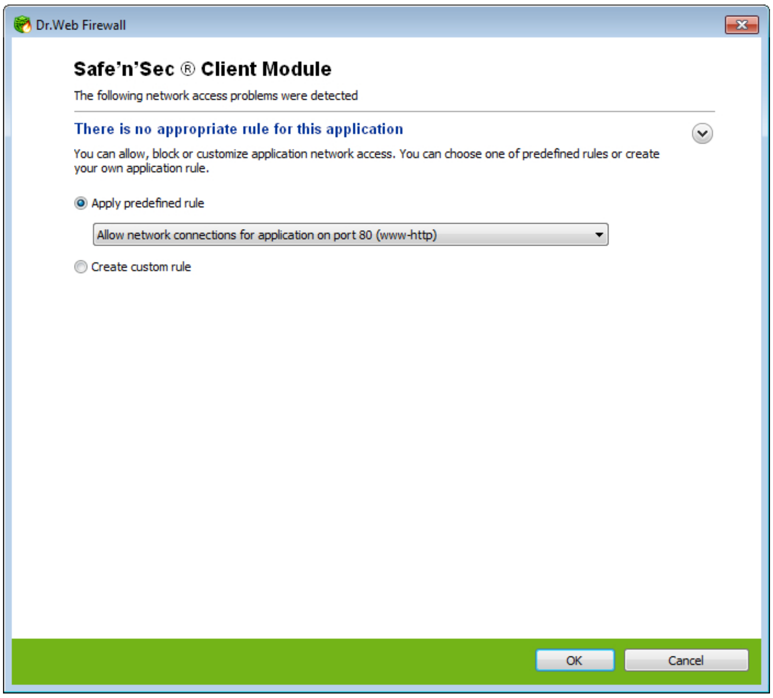
Safe'n'Sec ® Client Module

Dr.Web Firewall has detected network activity

Application name	Safe'n'Sec ® Client Module
Application path:	C:\Program Files\SafenSoft\SysWatch\safensec.exe
Digital signature:	✓ SnS Soft
Remote address:	tcp://23.37.43.27 (ts-ocsp.ws.symantec.com)
Port:	80 (www-http)
Direction:	Outbound

Attention:
- There is no appropriate rule for this application

Figure 120. Dr.Web® Firewall notification



Safe'n'Sec ® Client Module

The following network access problems were detected

There is no appropriate rule for this application

You can allow, block or customize application network access. You can choose one of predefined rules or create your own application rule.

● Apply predefined rule

Allow network connections for application on port 80 (www-http)

○ Create custom rule

Figure 121. 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. SpIDer Guard settings [132]).

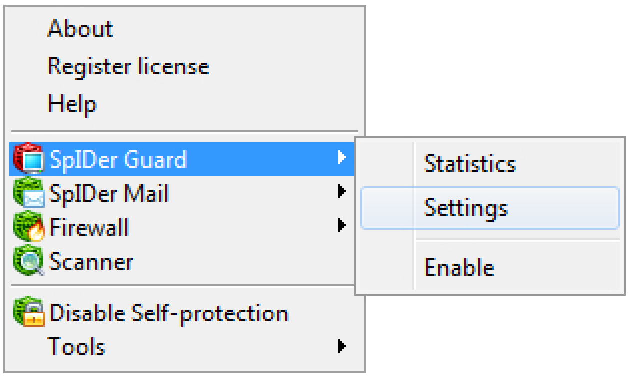
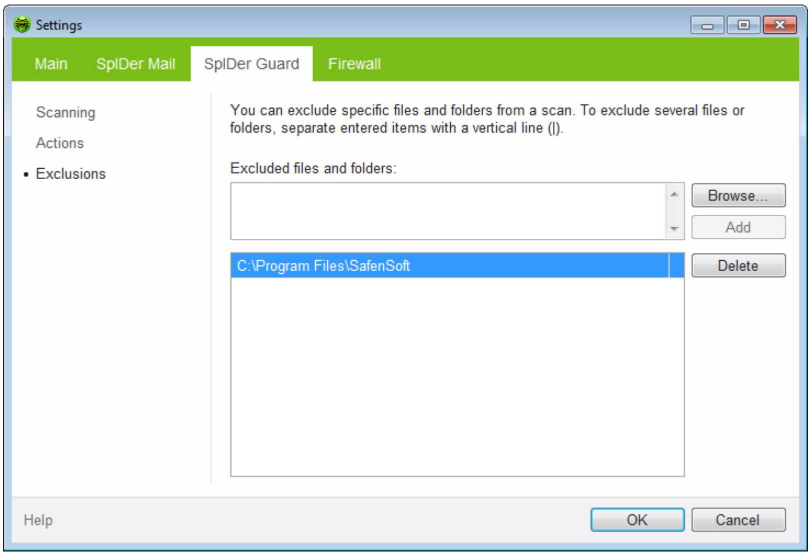


Figure 122. SpIDer Guard settings

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. Adding SpIDer Guard exclusions[133]). Click **OK** to apply changes.



You can exclude specific files and folders from a scan. To exclude several files or folders, separate entered items with a vertical line (|).

Excluded files and folders:

C:\Program Files\SafenSoft

Figure 123. Adding SpIDer Guard exclusions

11) Turn on the SpIDer Guard protection component by selecting the **SpIDer Guard** → **Enable** item in the context menu (fig. Enabling SpIDer Guard[133]).

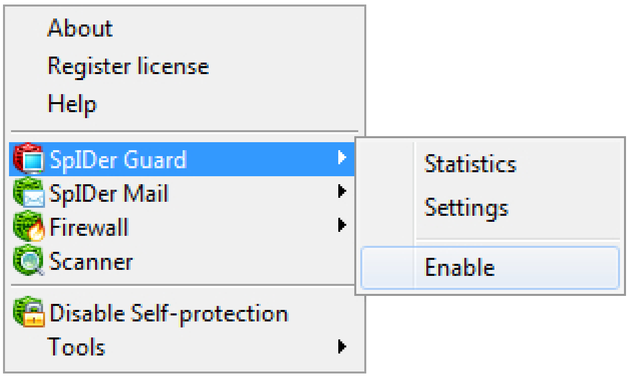


Figure 124. Enabling SpIDer Guard

12) Open the list of processes[59] of SoftControl SysWatch and select **Enable software up-**

date mode in the properties[61] of all the Dr.Web® modules.

11. Supplemental information

11.1 Process privileges

Table 13 describes Windows privileges that the processes use (see also https://msdn.microsoft.com/ru-ru/library/windows/desktop/bb530716(v=vs.85).aspx and https://docs.microsoft.com/en-us/windows/device-security/auditing/event-4704).

Table 13. Process privileges

Privilege	Description
Manage auditing and security log	Required to generate audit-log entries. With this privilege, the user can add entries to the security log.
Back up files and directories	Required to perform backup operations. This privilege causes the system to grant all read access control to any file, regardless of the access control list (ACL) specified for the file. Any access request other than read is still evaluated with the ACL. With this privilege, the user can bypass file and directory, registry, and other persistent object permissions for the purposes of backing up the system.
Restore files and directories	Required to perform restore operations. This privilege causes the system to grant all write access control to any file, regardless of the ACL specified for the file. Any access request other than write is still evaluated with the ACL. With this privilege, the user can bypass file, directory, registry, and other persistent objects permissions when restoring backed up files and directories. Additionally, this privilege enables you to set any valid user or group SID as the owner of a file.
Change the system time	Required to modify the system time. With this privilege, the user can change the time and date on the internal clock of the computer. Users that are assigned this user right can affect the appearance of event logs. If the system time is changed, events that are logged will reflect this new time, not the actual time that the events occurred.
Shut down the system	Required to shut down a local system.
Force shutdown from a remote computer	Required to shut down a system using a network request.
Take ownership of files or other objects	Required to take ownership of an object without being granted discretionary access. With this privilege, the user can take ownership of any securable object in the system, including Active Directory objects, files and folders, printers, registry keys, processes, and threads.
Debug programs	Required to debug and adjust the memory of a process owned by another account. With this privilege, the user can attach a debugger to any process or to the kernel. Developers who are debugging their own applications do not need this user right. Developers who are debugging new system components need this user right. This user right provides complete access to sensitive and critical operating system components.
Modify firmware environment values	Required to modify the nonvolatile RAM of systems that use this type of memory to store configuration information.
Profile the system perform-	Required to gather profiling information for the entire system.

Privilege	Description
ance	With this privilege, the user can use performance monitoring tools to monitor the performance of system processes.
Profile single process	Required to gather profiling information for a single process. With this privilege, the user can use performance monitoring tools to monitor the performance of non-system processes.
Increase scheduling priority	Required to increase the base priority of a process. With this privilege, the user can use a process with Write property access to another process to increase the execution priority assigned to the other process. A user with this privilege can change the scheduling priority of a process through the Task Manager user interface.
Load and unload device drivers	Required to load or unload a device driver. With this privilege, the user can dynamically load and unload device drivers or other code in to kernel mode. This user right does not apply to Plug and Play device drivers.
Create a pagefile	Required to create a paging file. With this privilege, the user can create and change the size of a pagefile.
Adjust memory quotas for a process	Required to increase the quota assigned to a process.
Bypass traverse checking	Required to receive notifications of changes to files or directories. This privilege also causes the system to skip all traversal access checks. It is enabled by default for all users.
Remove a computer from the docking station	Required to undock a laptop. With this privilege, the user can undock a portable computer from its docking station without logging on.
Perform volume maintenance tasks	Enables volume management privileges. Required to run maintenance tasks on a volume, such as remote defragmentation.
Impersonate a client after authentication	Required to impersonate. With this privilege, the user can impersonate other accounts.
Create global objects	Required to create named file mapping objects in the global namespace during Terminal Services sessions. This privilege is enabled by default for administrators, services, and the LocalSystem account.

11.2 SoftControl SysWatch traffic

There are three sources of SoftControl SysWatch traffic:

1) HTTPS overhead,

2) Logs from client device,

3) Updates (client module and antivirus bases).

HTTPS overhead

HTTPS overhead traffic amounts to 3.7 KB per heartbeat. (Heartbeat is the client component parameter that specifies the period when a client component connects to the SoftControl Server component.)

To estimate monthly traffic generated by HTTPS overhead, you can use the following formula: `T1=3.7*30*24*3600/heartbeat value [seconds]`. The result will be measured in KBs per month.

Logs from client device

Traffic generated for one event amounts to approximately 500 bytes. You can use the number of events to estimate the traffic amount generated by logs on a standard device within 24 hours, as well as the required database capacity.

Updates

Client module updates

One update amounts to 30 MB. New updates are released 3–4 times a year.

Antivirus base updates

The first update after installation amounts to 60 MB. Following updates generate 400 to 1,300 KB daily (depending on new antivirus bases released).

11.3 Sources

Sources of supplemental information are presented in table 14.

Table 14. Supporting documentation

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

11.4 Updating SoftControl SysWatch and antivirus bases on Windows XP

Depending on Service Pack, Windows XP either does not support new certificates at all or supports them not completely. It is related to the fact that newer algorithms (SHA-256) were used for generating the certificates.

To ensure that SoftControl products are updated properly, perform the operations described in this section for the update modules.

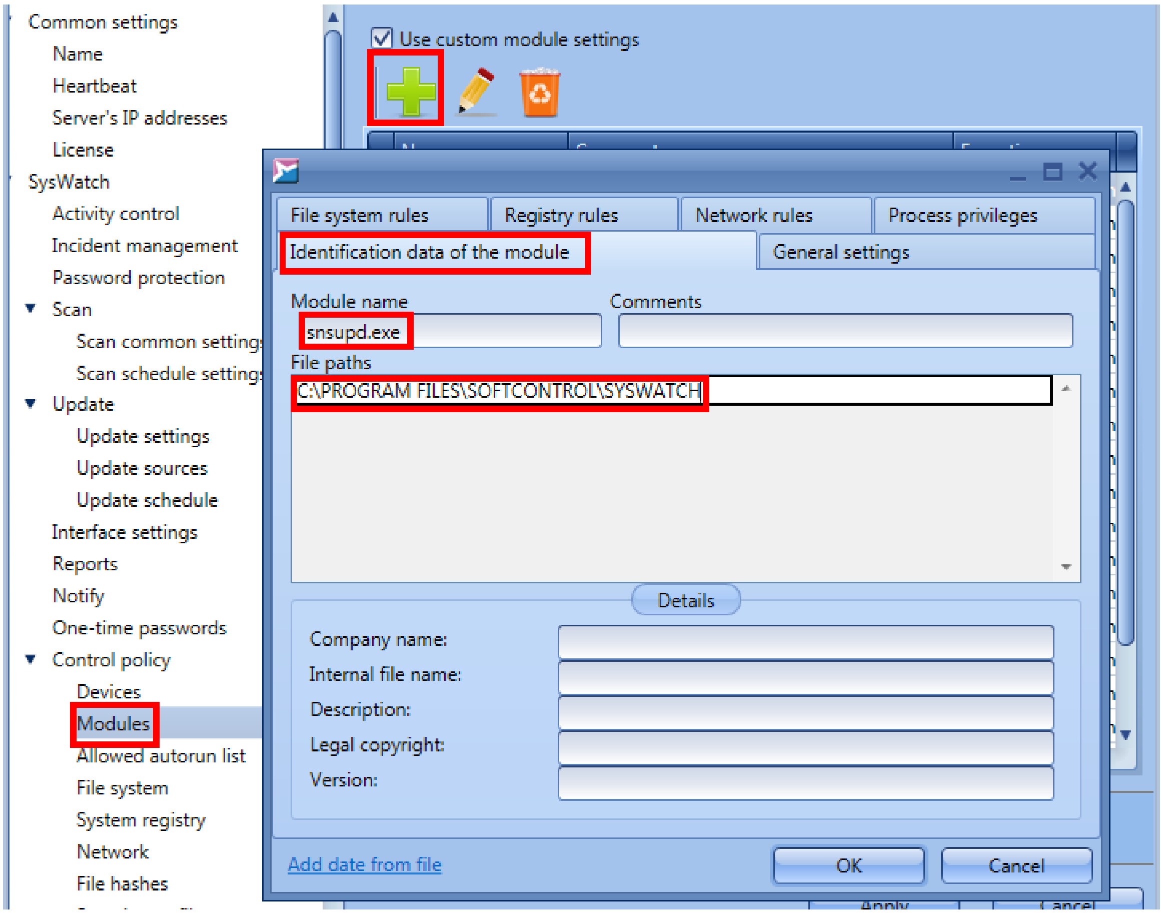
Follow steps in this section to ensure proper update of the SoftControl SysWatch application and antivius bases on 32-bit Windows XP.

Note. If you install version 5.1.79 or later of SoftControl SysWatch and it is the first installation of the application on your computer, these actions are not required: all updates will be performed properly. For SoftControl DLP and SoftControl SysCmd, you do not need to perform instructions from this section if you have version 6.0.95 or later.

1. Open the client settings editor in SoftControl Admin Console.
2. Go to **Modules**.
3. Click on ➕.
4. On **Identification data of the module** tab, enter the module name (the name of the executable file) and its path according to the table below.

Table 15. Update modules

Component for updating	Module name	Path
SoftControl SysWatch	snsupd.exe	`C:\PROGRAM FILES\SOFTCONTROL\SYSWATCH\`
SoftControl SysCmd	upd.exe	`C:\Program Files\SoftControl\SysCmd\Updater`
SoftControl DLP Client	upd.exe	`C:\Program Files\SafenSoft\DLP Client\Updater`



☑ Use custom module settings

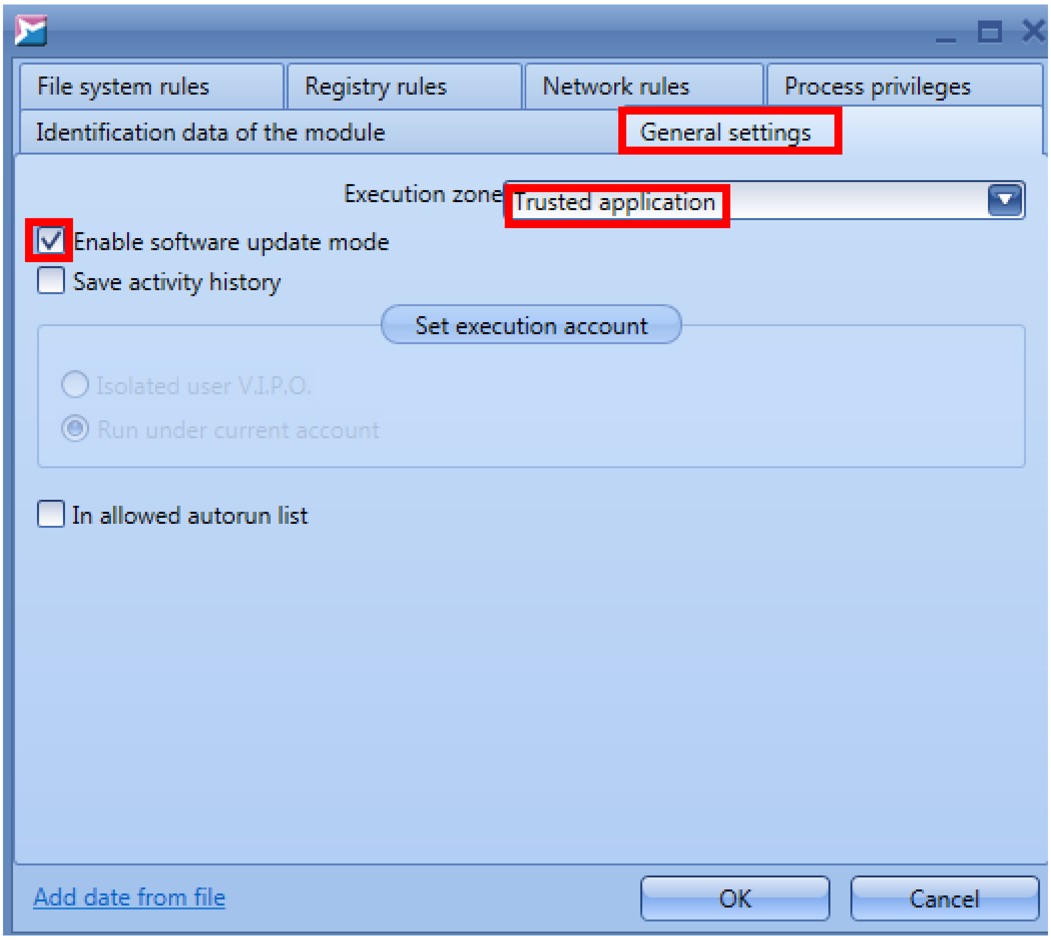
Module name: snsupd.exe

File paths: C:\PROGRAM FILES\SOFTCONTROL\SYSWATCH

Figure 125. Setting up an update module (for SoftControl SysWatch)

5. On **General settings** tab, select **Trusted application** execution zone and check **Enable soft-**

ware update mode.



Execution zone Trusted application

☑ Enable software update mode

□ Save activity history

○ Isolated user V.I.P.O.

● Run under current account

□ In allowed autorun list

Figure 126. Adding the module to trusted applications

6. Click **OK**.

7. Save the client settings under a new name and apply them to the organizational unit of the clients that require updating.

If you are setting up updating for SoftControl SysWatch, now you can create a task to update the antivirus bases or wait for a scheduled update.