SafenSoft SysWatch

PERSONAL

User Manual

SafenSoft

Content

1 Introduction

Dear SafenSoft customer,

Thank you for choosing **SafenSoft SysWatch®** to protect your computer. Our experts have worked hard to ensure the software meets the highest standards of information security, and we believe that **SafenSoft SysWatch®**, when installed and used in accordance with the documentation, will protect your system against malware and other threats, both external and internal.

If you have any comments or questions about the software, please don't hesitate to send them to us at support@safensoft.com.

1.1 What's new in SafenSoft SysWatch

All **SafenSoft** products are subject to continuous improvement. Listed and described below are the new and improved features included in **SafenSoft SysWatch v.3.6**.

Feature	Benefits
New: Script execution control	Detection and prevention of any scripting language launch.
Improved: Auto adjust	Automatic creation of trusted applications list in background mode minimizes the need for additional adjustments and enables "out-of-the-box" protection.
Improved: Alerting system	Alerts provide timely information about all endpoint activity, enabling effective reactions to attempts to breach security policies.
Improved: Application activity history and rollback to remove unwanted changes	For every application, the entire activity history and shadow copies of the changed/deleted files can be created to provide the ability to roll back unwanted changes.
Improved: Application launch control	Granular application launch control settings allow precise controls and prevent unknown processes from launching, so damage cannot occur.
Improved: Automatic incident processing	Automatically blocks malicious application activity to adjust security levels as needed.
Improved: Core integrity engine	Primary algorithms have been improved to deliver better performance and greater efficiency.

1.2 How it works

The main purpose of the **SafenSoft SysWatch** protection system is to preserve the integrity of the operating system and all its components as installed at the original build, as well as applications installed at a later date.

Immediately after installation, **SafenSoft SysWatch** activates in Simple Mode, which provides control over the launch of unknown applications. Simple Mode is based on the detection of new executable modules in the system. The decision as to whether to allow the new application to launch is made based on the degree of confidence in the unknown application and on internal **SafenSoft SysWatch** logic regarding executable modules.

To reduce the number of alerts on unknown application launches, and for more effective protection, **SafenSoft SysWatch** carries out an automatic adjustment the first time it is run, creating the basic System Profile. After the automatic adjustment is successfully completed, **SafenSoft SysWatch** activates the **Extended Mode**.

Unknown applications (applications that are not included in the System Profile) may be launched and activated only in a secure environment (sandbox), during the current operating system session, and only if the application is launched by the authorized user of the system. Only the authorized user may determine whether to add a new application to the System Profile as a trusted application, launching it in **Install Mode.**

Trusted applications that are potentially dangerous (web browsers, instant messengers, and P2P clients, for example), can be launched in a sandbox. To launch potentially dangerous applications with restrictions, the Execution Conditions can be changed in the Application Properties window.
When the user attempts to launch a new application, **SafenSoft SysWatch** issues a notification that the application is unknown and offers the following options:

- **Execute Application**. The application is launched in a secure environment (sanbox) and allowed to load additional executable modules not present in the system profile. If the application is malicious, it will still be allowed to execute, even to install additional components into the operating system. But when the system is restarted, the malware will be unable to execute as it is not present in the System Profile, thus preventing any damage or the transmission of infective code.

- **Run in Install Mode**. In this case, **SafenSoft SysWatch** registers all the new components installed by the application in the System Profile. The application and its components are granted rights to start in future.

- **Block Application**.

By default, only those modules that reside on a local hard drive are included in the System Profile. Those executable modules distributed as application resources, archives, and the like will not be registered initially. In order for such applications to work properly, they should be launched them in Install Mode - applications and all their components are considered safe and added to the System Profile.

1.3 System requirements

Operating System	Hardware requirements
• Microsoft Windows XP Home Edition (SP 3) • Microsoft Windows XP Professional Edition (SP 3) • Microsoft Windows XP Professional x64 Edition (SP3)	• Intel Pentium x86/x64, 300 MHz or compatible • 256 MB RAM or more • At least 150 MB free disk space
• Microsoft Windows Vista Home Basic x86/ x64 (SP1) • Microsoft Windows Vista Home Premium x86/x64 (SP1) • Microsoft Windows Vista Business x86/x64 (SP1) • Microsoft Windows Vista Ultimate x86/x64 (SP1)	• Intel Pentium x86/x64, 800 MHz or compatible • 512 MB RAM or more • At least 150 MB free disk space
• Microsoft Windows 7 Home Basic x86/x64 • Microsoft Windows 7 Home Premium x86/ x64 • Microsoft Windows 7 Professional x86/x64 • Microsoft Windows 7 Ultimate x86/x64	• Intel Pentium x86/x64, 800 MHz or compatible • 512 MB RAM or more • At least 150 MB free disk space

2 Installing SafenSoft SysWatch

Before installing **SafenSoft SysWatch,** ensure you have the latest version of the product.
You can download the latest version here: **http://products.safensoft.com/SafenSoft_SysWatch_Personal.exe**

The installation program is implemented as a standard Windows wizard. Each window contains a set of buttons to control the installation process. These buttons and their actions are:

- **Next** – accept the action and move to the next step in the installation process

- **Back** – return to the previous step in the installation process.
- **Cancel** – cancel the installation.
- **Finish** – complete the application installation procedure.

Let us take a closer look at each step of the installation procedure.

Step 1. To install **SafenSoft SysWatch** on your computer, run the installer (the file with the .exe extension) named **SafenSoft_SysWatch_Personal.exe**

Step 2. Choose your language from the list and click **OK**.

Step 3. Wait until **SafenSoft SysWatch** extracts its installation files.

Step 4. In the **Welcome to the Install Wizard for SafenSoft SysWatch** windows click **Next**.

Step 5. The License Agreement. If you accept its terms, click "I accept the terms in the license agreement" and then click the **Next** button. The application installation will continue.

Step 6. Specify the folder in which **SafenSoft SysWatch** will be installed. The default location: **C:\Program Files\SnS Soft\Safe'n'Sec Client**

You can specify another folder, by clicking the **Browse** button, and selecting the required folder in the standard folder selection window, or by entering the path to it in the text entry field. To proceed with the installation, click the **Next** button.

Step 7. To start the actual software installation, click the **Install** button.

Step 8. When you see the **InstallShield Wizard Completed** window, click the **Finish** button to finish the installation process.

3 Application Interface

The **SafenSoft SysWatch** is straightforward and easy-to-use. This section describes the basic features in detail.

3.1 Notification area icon

Immediately after installing **SafenSoft SysWatch**, the application icon will appear in the Microsoft Windows taskbar notification area.

This icon indicates the program's operational status. It also shows the protection status and whether any basic functions are currently active.

 - protection is enabled;

 - protection is disabled;

 - automatic adjustment is being performed;

 - update is in progress;

 - computer is being scanned.

The icon also provides quick access to the basic components via the SysWatch interface: the context menu and the main window.

- The Context menu is opened by right-clicking on the application icon.
- To open the SafenSoft SysWatch control panel, double click on the application icon.

3.2 Context menu

The Context menu is opened by right-clicking on the application icon in the notification area. You can run tasks and quickly access **SafenSoft SysWatch** settings from the context menu.

The **SafenSoft SysWatch** context menu contains the following items:

- **SafenSoft SysWatch** – open main window (Control panel)
- **Settings** – view and change the program's parameters.
- **Activity Policy** - change the application activity policies.
- **Processes and applications** - view and change the application parameters.
- **Scan** – select objects and start a scan for malicious code.
- **Update** – download and install application updates if available.
- **Reports** – view system, update, scan and system profile creation reports.
- **Turn protection off/on** - change the status of the protection.
- **About** - view information about **SafenSoft SysWatch** .
- **Show program icon** - toggle visibility of the program's icon in the notification area.
- **Interface language** – change the language used in the program interface.
- **Exit** - shut down the SysWatch interface. Note that the protection will continue to run.

3.2.1 SafenSoft SySWatch

- **SafenSoft SysWatch**. – open main window (Control panel)

Actions

▼ Open Control panel

1. Right-click on the application icon in the notification area to open context menu. Then choose **SafenSoft SysWatch** to open control panel.

3.2.2 Settings

The Application settings window provides quick access to general **SafenSoft SysWatch** settings:

- **Protection** – settings for application activity control, learning mode, and automatic incident processing
- **Scan** – settings for malware scanning and actions to be performed on malware detected.
- **Update** - change application update settings.
- **Settings** – system service control, remote application control, backup and restore settings, preinitialize antivirus scanner.
- **View** –change interface language and visibility of notification area icon.
- **Reports** – report generation management.
- **Notifications** – settings for application notifications.

Actions

▼ Open Application settings window

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.
2. **SafenSoft SysWatch** settings window will be opened.

3.2.2.1 Protection

When **SafenSoft SysWatch** is installed the following protection parameters are set by default:

- **Enable protection** – Enabled
  - **Applications** – Enabled
  - **File system** – Enabled

- **System registry** – Enabled
- **Network** – Enabled

- **Automatic processing of incidents** – Disabled
- **Password protection** - Disabled

Actions

Disable protection

1. Right-click on the application icon in the notification area to open context menu. Then chose **Settings** to open application settings window.
2. Uncheck **Enable protection** and click **OK** to disable protection of all controlled areas.

or

3. Uncheck appropriate control areas and click **OK** to disable protection of these areas only.

Enable automatic processing of incidents

Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open Application settings window.

1. Check **Enable automatic processing of incidents** and click **Configure.**

2. Under **Incidents** tab you can set automatic decisions on different incidents.

Following types of incidents are available:

- **Launching unknown application** - attempt to launch any application which was not installed before system profile creation. Exception is made for installers with certificate from trusted Certificate Authority.
- **Launching unknown installer/updater** – attempt to launch any installer without certificate from trusted Certificate Authority or with expired certificate.
- **Control policy violation** – any violations of application activity policies by applications with adjusted activity restrictions (access to file system, registry etc.).

Following decisions on Launching unknown application are available:

- **Execute in a limited mode** – launch application in a sandbox.
- **Scan and execute in a limited mode after** – scan and launch application in a sandbox if no malicious code was detected.
- **Execute in install mode -** launch application and add to system profile as trusted.

- **Scan and execute in install mode after -** scan and launch application if no malicious code was detected. Add application to system profile as trusted.
- **Block** – prevent application from launching

Following decisions on Launching unknown installer/updater are available:

- **Install** – launch installer/updater and add all new modules to the system profile as trusted.
- **Scan and install after** – scan and launch installer/updater if no malicious code was detected. Add all new application's modules to system profile as trusted.
- **Install in a limited mode -** launch installer/updater in a sandbox.
- **Scan and install in a limited mode after -** scan and launch installer/updater in a sandbox if no malicious code was detected.
- **Block–** prevent installer from launching

Following decisions on control policy violation are available:

- **Allow** – operation which is not allowed by the SysWatch's control policy will be permitted.
- **Scan and allow after -** operation which is not allowed by the SysWatch's control policy will be permitted, if no malicious code was detected.
- **Block -** operation which is not allowed by the SysWatch's control policy will be blocked.
- **Block and Kill application -** operation which is not allowed by the SysWatch's control policy will be blocked and the process initiated this operation will be stopped.

You can also set additional parameters:

Delayed decision – in case of an incident, automatic decision will be made after the delay, if no manual decision were made.

Remember decision on session - in case of an incident, automatic decisions on application's operations will be made until it will be stopped (applicable for Control policy violation only).

Decide on the administering computer - applicable for corporate products only. Decision will be made by the administrator remotely via management console - Admin Explorer.

Enable password protection

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.
2. Check **Enable password protection** and click on **Configure** button.
3. In the field **Current Password** enter the password you set before.

   NOTE:

   *If you didn't set password for SafenSoft SysWatch leave **Current Password** field blank.*

4. Enter new password and confirm it in appropriate fields – **New password** and **Confirm new**

password.

5. Check actions to SafenSoft SysWatch to be protected with password: **Changing program settings, uninstalling program** and click **Ok** button.

NOTE:

Now whenever any user on your computer attempts to perform the actions you selected, SafenSoft SysWatch will always request a password.

3.2.2.1.1 System Profile Creation

In order to ensure the best possible protection, **SafenSoft SysWatch** automatically creates and adjusts System Profiles the first time it is run. If the computer is restarted or switched off before the end of this automatic adjustment process, it will continue from the point at which it was stopped when the system is powered back on. After the automatic adjustment is successfully completed, **SafenSoft SysWatch Extended Mode** is activated, which enables you to:

- **Classify** all installed applications into trusted/known and potentially harmful/unknown categories.
- **Execute** unknown applications in a sandbox and automatically block any malicious activities.
- **Reduce** the need for user interaction when a decision needs to be made about an application launch.

System Profile creation consists of the following steps:

- **Update** automatic adjustment components via the Internet. If an Internet connection is unavailable, existing components are used.
- **Search and collect information** about all executable files (exe, com, dll, etc.)
- **Identification of executable files**
- **Define rules** for application execution:
  - **Trusted** or **known** application
  - **Restricted** application.
  - **Blocked** application (execution is prohibited).
  - **Scan application files** for malware

Running in Extended Mode, **SafenSoft SysWatch** tracks new or unknown applications (those not present in the **System Profile**), blocks harmful actions, and notifies of any suspicious activities.

NOTE

*The time taken to create the System Profile depends on the amount of software installed on the system. It is recommended that you **minimize** the SysWatch interface to the Windows task bar and continue to work while this process is completed*

NOTE

You can update the System Profile as necessary. For example, the profile should be updated whenever a significant change is made to the system, such as attaching an external storage device that contains executable files. Simply update then System Profile when the device is connected; after the update is completed, the applications on the storage device will be considered known and trusted.

IMPORTANT

*Do not install or update software during an automatic adjustment, as SysWatch will be unable to add new or changed software to the System Profile. You can update or add new software to the System Profile by launching it in **install mode**.*

Actions

- Cancel automatic adjustment
  1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.
  2. In **Protection Status section** click on **Configure** button to open **General Settings for Protection** window.
  3. Choose **System Profiling** tab and click on Stop button while system profiling is running.
  4. SysWatch will ask whether you wish to continue the automatic adjustment later or not.
  5. Click **Yes** if you would like to continue profile creation in future or **No** if you would like to create profile from very beginning in future.

- Update System Profile
  1. In the General Settings for Protection window, choose the System Profile tab.
  2. For Scope, select Disks to create the System Profile or Add files and folders to include them in the existing system profile.

3. Click the Update button.

3.2.2.1.2 Applications

In the **Applications** tab you can change following settings:

- Save activity history of unknown applications on the first run.
- Disable script engine to block JavaScripts and VBScripts from running.

NOTE

If the **dll modules control** is enabled, all the processes from the list below will be blocked. Hence all the js, vbs, java bytecode which are executed by these interpreters will be blocked from running.

- **wscript.exe** - Microsoft ® Windows Based Script Host
- **cscript.exe** - Microsoft ® Console Based Script Host
- **java.exe** - Java(TM) Platform SE binary
- **javaw.exe** - Java(TM) Platform SE binary
- **javaws.exe** - Java(TM) Web Start Launcher

- Enable dll modules control (system restart is required).

NOTE

Dll modules control means the control of the libraries (*.dll) or the drivers (*.sys), which are loaded by the process or operating system.

Dll modules control in the Simple Mode:

SafenSoft SysWatch checks availability of the libraries (drivers) loaded by the process (system) in the blacklist. If the libraries (drives) are present in the blacklist they will be blocked.

Dll modules control in the Extended Mode :

SafenSoft SysWatch checks availability of the libraries (drivers) loaded by the process (system) in the checksums database. If the checksums of the libraries (drives) are not present in the database or differs from the checksums stored in the database, they will be blocked.

- Set automatic removal of the information about rarely launched applications

- Remove information about rarely launched applications

Actions

▼ Save activity history of unknown applications on the first run

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.

2. In **Protection Status** section click on Configure button to open **General Settings for Protection** window.

3. Choose **Applications** tab and check **Save activity history of unknown applications on the first run**.

4. Click on **Ok** button.

▼ Disable script engine

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.

2. In **Protection Status** section click on **Configure** button to open **General Settings for Protection** window.

3. Choose **Applications** tab and check **Disable script engine**.

4. Click on **Ok** button.

▼ Enable dll modules control

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.

2. In **Protection Status** section click on **Configure** button to open **General Settings for Protection** window.

3. Choose **Applications** tab and check **Enable dll modules control**. Click on **Ok** button.

4. To Enable dll modules control the system must be restarted.

▼ Remove information about rarely launched applications

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.

2. In **Protection Status** section click on **Configure** button to open **General Settings for Protection** window.

3. Choose **Applications** tab and click on **Clean up now** button.

4. Click on **Ok** button.

▼ Set automatic removal of the information about rarely launched applications

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.

2. In **Protection Status** section click on **Configure** button to open **General Settings for Protection** window.

3. Choose **Applications** tab and check **Remove information about the application does not run more than** and set the number of days.

4. Click on **Ok** button.

3.2.2.1.3 Incidents

In the **Incidents** tab you can set different variants of **SafenSoft SysWatch** decisions when appropriate incident appears.

Following types of incidents are available:

- **Launching unknown application** - attempt to launch any application which was not installed before system profile creation. Exception is made for installers with certificate from trusted Certificate Authority.
- **Launching unknown installer/updater** – attempt to launch any installer without certificate from trusted Certificate Authority or with expired certificate.
- **Control policy violation** – any violations of application activity policies by applications with adjusted activity restrictions (access to file system, registry etc.).

Following decisions on **Launching** unknown application are available:

- **Execute in a limited mode** – launch application in a sandbox.
- **Scan and execute in a limited mode after** – scan and launch application in a sandbox if no malicious code was detected.
- **Execute in install mode** - launch application and add to system profile as trusted.
- **Scan and execute in install mode after** - scan and launch application if no malicious code was detected. Add application to system profile as trusted.
- **Block** – prevent application from launching

Following decisions on **Launching unknown installer/updater** are available:

- **Install** – launch installer/updater and add all new modules to the system profile as trusted.
- **Scan and install after** – scan and launch installer/updater if no malicious code was detected. Add all new application's modules to system profile as trusted.
- **Install in a limited mode** - launch installer/updater in a sandbox.
- **Scan and install in a limited mode after** - scan and launch installer/updater in a sandbox if no malicious code was detected.
- **Block** – prevent installer from launching

  Following decisions on control policy violation are available:

- **Allow** – operation which is not allowed by the SysWatch's control policy will be permitted.
- **Scan and allow after** - operation which is not allowed by the SysWatch's control policy will be permitted, if no malicious code was detected.
- **Block** - operation which is not allowed by the SysWatch's control policy will be blocked.
- **Block and Kill application** - operation which is not allowed by the SysWatch's control policy will be blocked and the process initiated this operation will be stopped.

You can also set additional parameters:

- **Delayed decision** – in case of an incident, automatic decision will be made after the delay, if no manual decision were made.
- **Remember decision on session** - in case of an incident, automatic decisions on application's operations will be made until it will be stopped (applicable for Control policy violation only).
- **Decide on the administering computer** - applicable for corporate products only. Decision will be made by the administrator remotely via management console - Admin Explorer.

Actions

▼ Enable automatic processing of incidents

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open Application settings window.

2. Check **Enable automatic processing of incidents** and click **Configure**.

3. Under **Incidents** tab you can set automatic decisions on different incidents.

4. Click on **Ok** button when changes are done.

3.2.2.2 Scan

When SafenSoft SysWatch is installed the following anti-malware scan parameters are set by default (if the scanner is available in the product):

- **Threat action** – Treat, Delete incurable objects
- **Check files** – Only executable files
- **Advanced check** - Use digital signatures: Enabled
- **Check removable devices automatically** – Disabled
- **Startup account** – Local system account
- **Scanner startup** – Preinitialize scanner: Disabled

Actions

▼ Set automatic scan of the removable devices

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open Application settings window.

2. Select **Scan** section of the Application settings window.

3. Set **Check removable devices automatically** and **Prompt for checking removable devices** if it is necessary.

4. Click on **Ok** button to apply changes.

▼ Set manual selection of the action on detected threat

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open Application settings window.

2. Select **Scan** section of the Application settings window.

3. Set **Select action when the scan finishes** to view all found threats or **Ask action** to be asked on every single threat during the scanning.

4. Click on **Ok** button to apply changes.

- Set file types to be scanned for malicious code and scan methods

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open Application settings window.

2. Select **Scan** section of the Application settings window.

3. Click **Configure** button under **Check files** section to open **Advanced settings** window.

4. In the **Advanced settings** windows set **All files**, check **Mail bases** and **Archives**, check **Use digital signatures** and **Use heuristics** for slower, but more comprehensive scan.

5. Click on **Ok** button in **Advanced settings** windows and in **Application settings** window to apply changes.

- Set scanner startup parameters

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open Application settings window.

2. Select **Scan** section of the Application settings window.

3. Click **Configure** button under **Check files** section to open **Advanced settings** window.

4. Choose **Startup options** tab in Advances settings window.

5. Set scanner startup account if you don't like to run scanner under Local system account (default).

6. Check **Preinitialize scanner** for faster scanning (requires more RAM). Scanner will be loaded to RAM at system startup.

7. Click on **Ok** button in **Advanced settings** windows and in Application settings window to apply

changes.

3.2.2.3 Update

When **SafenSoft SysWatch** is installed the following update parameters are set by default:

- **Update automatically** – Enabled
- **Prompt for confirmation prior to updating** – Disabled
- **Check for updates** – Once a day
- **Content of updates** – All:
    - **Use default proxy settings** – Disabled. Your web browser parameters are used for Internet connection.
    - **Credentials** – Local system account.
- **Notifications** – Settings for application notifications.

Actions

▼ Change automatic update settings

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.

2. Select **Update** section of the Application settings window.

3. In **General settings for program update** window you can Disable/Enable automatic updates, Enable/Disable confirmation before update, set periodicity of automatic updates and set program components to be updated (Program or AV bases).

4. Click on **Ok** button to apply changes.

▼ Change Internet connection settings for automatic update task

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.

2. Select **Update** section of the Application settings window.

3. In **General settings for program update** window click **Configure** button.

4. In the **Advanced settings** window select **Connection** tab.

5. Check **Use default proxy settings** then enter **Address** and **Port** number (80 by default). Enter **User name** and **Password**, if authorization is required.

6. Click on **Apply** button to apply changes or click on **Ok** button to apply changes and close window.

▼ Set credentials for automatic update task

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.

2. Select **Update** section of the Application settings window.

3. In **General settings for program update** window click **Configure** button.

4. In the **Advanced settings** window select **Startup options** tab.

5. Set account for automatic updates, if you don't like to run updates under Local system account (default).

6. Click on **Apply** button to apply changes or click on **Ok** button to apply changes and close window.

3.2.2.4 Settings

When **SafenSoft SysWatch** is installed the following parameters are set by default:

- **Self-protection** – Disabled
- **Remote control** – Disabled
- **Check for updates** – Once a day
- **Backup** of the default program settings and application control policy is created. If you create new control rules or change other **SafenSoft SysWatch** settings which prevent system from working correctly, you can restore default settings.

In the **Settings** section of the **Application Settings** window you can:

- **Backup/restore** program settings including application control policies.
- **Enable/Disable external control** of the **SafenSoft SysWatch** system service (self-protection).
- **Change settings for remote control** of **SafenSoft SysWatch** (available for corporate products only).

Actions

▼ Save program settings to a file (backup program settings)

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.

2. Select **Settings** section of the main Application settings window.

3. Click on **Save** button.

4. In the **Save As** window choose the destination folder where the backup copy of all settings will be saved.

5. Select file type (**xml** or encrypted **xmlc** format) and click on **Save** button.

6. Click **Ok** button in the **General settings** for control and management window.

- Restore program settings from a file

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.

2. Select **Settings** section of the main Application settings window.

3. Click on **Restore** button.

4. Choose the backup file you have saved before or default backup file and click on **Open** button.

5. Click on **Ok** button in the **SysWatch backup and restore** window.

6. Click **Ok** button in the **General settings for control and management** window.

- Enable/Disable external control of the SysWatch system service (self-protection).

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.

2. Select **Settings** section of the main Application settings window.

3. Check **Disable the external control of the system service** and click **Ok** button.

NOTE

If you checked **Disable the external control of the system service**, you can't stop or block execution of SafenSoft SysWatch with help of:

- Task manager
- Services (services.msc)
- Net stop command
- Taskkill command

3.2.2.4.1 View

When **SafenSoft SysWatch** is installed the following parameters are set by default:

- **Show program icon in in the taskbar notification area** – Enabled
- **Language**: the language you have selected during **SafenSoft SysWatch** installation

Действия

Hide program icon

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.
2. Select **View** section of the main Application settings window.
3. Uncheck the **Show program icon in the taskbar notification area** checkbox.
4. Click on the **OK** button to apply changes.

Change interface language

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open Application settings window.
2. Select **View** section of the main Application settings window.
3. Select language from drop-down menu.
4. Click on the **OK** button to apply changes.

3.2.2.4.2 Reports

When **SafenSoft SysWatch** is installed the following parameters are set by default:

- Enable reports – All
- Do not store reports longer than – 14 days
- Check for updates – Once a day

SafenSoft SysWatch creates following reports:

- **System** report contains data about the program's execution, exceptions and warnings on activity policy violation. A text file with the name system_date_time.txt template is created each time the program starts.
- **Update** contains data regarding the update process. A text file with the name update_date_time.txt template is created each time an update process starts.

- **Scan** report contains data regarding the scanning process (if antivirus scanner is included in the product). A text file with the name scan_date_time.txt is created each time a scan starts.
- **Profile** report contains data about system profile creation. A text file with the name profile_date_time.txt is recreated each time the profile is created or updated.

All the reports are saved to the:

C:\Documents and Settings\All Users\Application Data\S.N.Safe&Software\Safe'n'Sec\Reports (for Windows XP)

C:\Users\All Users\S.N.Safe&Software\Safe'n'Sec\Reports (for Windows Vista, Windows 7)

Actions

Disable reports

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.

2. Select **Reports** section of the main Application settings window.

3. Uncheck the **Enable reports** checkbox.

or

4. Uncheck a checkbox of a required type of reports. **SafenSoft SysWatch** will stop creating reports of the specified type.

Change how long reports are to be kept

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.

2. Select **Reports** section of the main Application settings window.

3. Specify the number of days reports are to be kept in the corresponding field.

Remove all reports

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.

2. Select **Reports** section of the main Application settings window.

3. Click the **Clean up** button and **OK** button in **Delete** reports window

or

4. Delete all files from the

C:\Documents and Settings\All Users\Application Data\S.N.Safe&Software\Safe'n'Sec\Reports (for

Windows XP)

C:\Users\All Users\S.N.Safe&Software\Safe'n'Sec\Reports (for Windows Vista, Windows 7)

▼ View reports

1. Right-click on the application icon in the notification area to open context menu. Then choose **Reports** to open Reports folder.

2. In the **Reports** folder you can find following report types:
   - **System**
   - **Update**
   - **Scan**
   - **Profile**
3. To view the report double click on it.

3.2.2.4.3 Notifications

When **SafenSoft SysWatch** is installed the following parameters are set by default:

- **Sounds** - Enabled
- **Show Notifications** – Enabled

When the program generates an event it displays special notification windows. Depending on the seriousness of an event a notification can be one of the following types:

- **Protection status** - indicates that protection status has changed or there are errors in protection components.
- **Update** - indicates that errors in program update process are thrown.
- **Scan for malware** - indicates that new threats have been detected or there are errors in the scanning process.
- **Reports** - used when automatically deletes reports.
- **Licensing** - used to notify you about the state of the license or when the license expires.
- **Application installation (uninstallation)** – indicates installation, update or uninstallation of any application with digital certificate
- **Program modules blocking** – indicates that application has been blocked automatically or by user's decision
- **Message from administrator** - used in corporate products only
- **Restricting applications** – indicates that the application was launched with restrictions: in the sandbox or custom rules are applied.

Actions

▼ Disable notifications

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.

2. Select **Notifications** section of the main Application settings window.

3. Uncheck the **Show notifications** checkbox.

or

4. To disable showing a notification of a specific origin click on Configure button and uncheck the corresponding checkbox.

5. Click on OK button to apply changes.

▼ Disable sounds

1. Right-click on the application icon in the notification area to open context menu. Then choose **Settings** to open application settings window.

2. Select **Notifications** section of the main Application settings window.

3. Uncheck the **Enable sounds** checkbox.

4. Click on **OK** button to apply changes.

3.2.3 Activity policy

- **Activity policy** – open application activity policies window.

Actions

▼ Open application activity policies window

1. Right-click on the SysWatch icon in the notification area to open the Context menu. Then choose **Activity policy** to open the application activity policies window.

3.2.4 Processes and applications

- **Processes and applications** – open the settings for the Processes and applications window.

Actions

▼ Open the Processes and applications window

1. Right-click on the application icon in the notification area to open context menu. Then choose **Processes and applications** to open settings for processes and applications window.

3.2.5 Scan

- **Scan** – select objects and start a scan for malicious code (if antimalware scanner is available).

Actions

▼ Run antimalware scan

1. Right-click on the application icon in the notification area to open context menu. Then choose **Scan** to select objects and start scan for malicious code.

2. Check object to be scanned and click on **Run scan** button.

3.2.6 Update

- **Update** – download and install SysWatch updates if available.

Actions

▼ Check for updates and install if available

1. Right-click on the application icon in the notification area to open context menu. Then choose **Update** item.

2. Click on **Run update** button.

3. Click on **Details** link while updating to view the report.

4. Update report will be opened

3.2.7 Reports

- **Reports** – view system, update, scan and system profile creation reports.

Actions

▼ View reports

1. Right-click on the application icon in the notification area to open context menu. Then choose **Reports** to open Reports folder.

2. In the Reports folder you can find following report types:
   - **System**
   - **Update**
   - **Scan**
   - **Profile**

3. To view the report double click on it.

3.2.8 Turn protection off

- **Turn protection off/on** - change the protection status.

IMPORTANT

New applications installed or launched when protection is turned off will not be added to the system profile automatically and will be considered as unknown applications when protection is re-activated.

Actions

- Turn protection off

1. Right-click on the program icon in the notification area to open the Context menu. Then choose **Turn protection off** to disable protection.

- Turn protection on

1. Right-click on the application icon in the notification area to open context menu. Then choose **Turn protection on** to enable protection.

3.2.9 About

- **About** - view information about the version of **SafenSoft SysWatch**, installed on this computer.

Actions

- Open the About SafenSoft SysWatch window.

1. Right-click on the application icon in the notification area to open context menu. Then choose **About** item.

2. About **SafenSoft SysWatch** windows will be opened.

3.2.10 Show program icon

- **Show program icon** - toggle the visibility of the SysWatch icon in the Windows notification area.

Actions

- Hide program icon

1. Right-click on the program icon in the notification area to open the Context menu. Then choose the **Show program icon** to uncheck it.

- Show program icon

1. Double click on the **SafenSoft SysWatch** shortcut at the desktop or launch it via Start menu.

2. Click on **Settings** link at the Protection Status window of the Control panel.

3. Check **Show program icon in the taskbar notification area** and click **OK** to apply changes.

3.2.11 Interface language

- **Interface language** – change the language of the SysWatch interface.

Actions

▼ Change the interface language

1. Right-click on the application icon in the notification area to open context menu. Then choose **Interface language** item and select the language.

3.2.12 Exit

- **Exit** - shut down the SysWatch user interface. Note that the protection continues to be in effect.

Actions

▼ Close thel user interface

1. Right-click on the application icon in the notification area to open context menu. Then choose **Exit** item. Note that the protection module will still be running.

3.3 Control panel

The Control panel is the main **SafenSoft SysWatch** window and contains the following sections:

- **Status** - displays protection status and allows protection settings to be changed.
- **Scan** - enables antimalware scanning to be activated and managed.
- **Update** - enables the management of program updates and settings.
- **License** - displays the legal information about the SysWatch license for this machine, program activation, and license renewal.

- Help and Support - contains information about the version of the **SafenSoft SysWatch**, installed on this machine and enables users to send an inquiry to SafenSoft technical support.

3.3.1 Protection status

The **Status** section displays the current SysWatch protection status:

- **Computer is protected -** all protection areas are under control.
- **Partial protection** - at least one of the protection areas is out of compliance with SysWatch protection requirements.
- **Unprotected** - SysWatch protection is disabled.

To change the protection status, click the appropriate link:

- **Applications** to enable/disable application launch control
- **File system** to enable/disable file system protection.
- **System registry** to enable/disable system registry protection.
- **Network** to enable/disable protection of network connections.

The lower part of the window contains information about application activities and allows changes to be made to the application activity control settings by clicking on it:

- **Registered applications** - total number of trusted, restricted, and blocked applications.
- **Trusted applications** - the number of trusted applications. The trusted application list is generated automatically after automatic adjustment or manually, when the system profile is updated or applications are launched in install mode.
- **Restricted applications** - the number of applications added to Restricted Applications group manually and, unknown applications launched in the sandbox.
- **Blocked applications** - the number of applications that were blocked. A blocked application will be prevented from launching as long as the application area is enabled.
- **Last incident** - the last application which attempted to violate control policy or was otherwise blocked from launching.

Actions

▼ Turn off protection

1. Click the **Settings** link at the bottom of the Control Panel **Status** section.

2. Uncheck the **Enable Protection** checkbox in the SysWatch Settings window and click **OK** to save the changes

3.3.2 Scan

The **Scan** section displays information relating to the last malware scan and enables the scanner's settings to be changed. This is only available if your SysWatch license includes the optional antimalware scanner:

- **Scan** has not been performed indicates that a malware scan has never been performed on this computer.
- **Computer is checked and protected** – the last scan either did not reveal any malware or all detected threats have been neutralized.
- **Untreated threats exist** - during the last scan malware was detected which has not yet been neutralized. The next step should be to update the program and rescan it or manually neutralize the untreated threats using the detected threats list.
- **Scan data is obsolete** indicates that more than 5 days have passed since the last scan, and so a new system scan should be initiated.
- **Scan is unavailable** indicates that the antimalware scanner is not available in the product or it is has not been activated. In order to activate the scanner, enter the appropriate license key and reactivate the program.
- **Last scan** displays detailed information from the last antimalware scan.
- **Threat action** specifies what the antimalware scanner should do when a threat is detected:
    - **Automatically -** treat infected object or delete it if treatment is not possible.
    - **Select action when the scan finishes –** request what should be done to infected objects after the scan is complete.
    - **Ask action** - request a decision as to what should be done with a malicious object each time the object is detected during a scan.
- **Settings** enables scan settings to be changed.
- **Quarantine** displays a list of objects to quarantine.

Actions

▼ Run antimalware scan

1. Specify one or more objects in the Scan section of the Control panel.

2. Click the **Run scan** button.

3. To view the state of the scan at any time click the **Details** link.

Scan report will be opened.

▼ View scan report

1. Click the **Last scan** link in the Scan section of the Control panel.

2. Scan report will be opened.

3.3.3 Update

The **Update** section displays information about the last update and allows changes to be made to the update settings:

- **SafenSoft SysWatch is out of date** - no update routine has ever taken place or more than 5 days have passed since the last update. The program should be updated.
- **SafenSoft SysWatch is up to date** - the program is up-to-date.
- **Updates are unavailable** the program has not been not activated or the license has expired. In order to perform a program update, a license key should be provided and the program activated or the license renewed.
- **Last search for updates** - detailed information about the last search for available updates.
- **Updates installed** displays details about the last updates installed.
- **Startup mode** specifies when the update routine starts:
  - **Automatic** - the update routine should start automatically.
  - **On demand -** the update routine should start on demand.
- **Settings** enables the update settings to be changed.

Actions

▼ Run update

1. Click the **Run update** button in the **Update** section of the Control panel.

2. To view the status of the update process, click the **Details** link.

3. TXT file with the update report will be opened.

▼ View update report

1. Click the **Installed updates** link in the **Update** section of the Control panel.

2. TXT file with the update report will be opened

3.3.4 License

The **License** section displays information regarding the SafenSoft license key for this machine.

- **Active license** - the program has been activated and is fully functional.
- **License will expire soon** - the license will expire in less than 5 days.
- **License has expired** - the license has expired and program functionality is now limited. The license should be renewed as soon as possible.
- **License not found** - the program does has not been activated. A license key should be provided and the program activated.

License type

  - **Commercial license** - the scope of the license key is defined at the time of purchase or renewal. When the key expires, the license can be renewed and the program reactivated.
  - **Trial license** - a free license key issued for the purpose of evaluating the program. Trial license keys cannot be renewed.

- **License expiration date** - the license key expiration date.
- **License validity term (days)** - the number of days for which the license key is valid.
- **Protection components** - program modules activated with this license key:
  - **SafenSoft SysWatch Core (Core)** is the core proactive protection component in **SafenSoft SysWatch.**
  - **SafenSoft SysWatch Rootkit Detector (RD)** - the component responsible for rootkit detection.
  - **Antivirus (AV) -** an optional component for detecting malware: viruses, trojans, worms, and other malware.
  - **Antispyware (AS)** - an optional component for detecting spyware.
- **Restrictions** specifies the limitations in functionality that take effect on license key expiration:
  - **Update** indicates that program updating is disabled.
- **Read EULA** - display the end user license agreement.
- **Renew / Buy license** links to the company's online store to purchase a new license key.

Actions

- Activate program

  1. Provide the license key in the **Number** field and click the **Activate** button.

  2. If an Internet connection is available, the program will automatically activate

  or

  3. In case no Internet connection is available the program will suggest **Manual activation** option.

  4. You will be suggested to contact the Support service by phone and provide them with the serial number and hardware code.

  5. Type the license key obtained from the Support service in the **Number** field and click on **Activate** button.

- Renew license

  1. Click the **Buy license** button if you use trial version or Renew License if you use commercial version. You will be navigated to the company's online store.

  2. Choose an appropriate product in the store.

3.3.5 Help and support

The **Help and support** section describes the information needed to request technical support:

- **SafenSoft SysWatch** version.
- **SafenSoft SysWatch** update version.
- Operating System and version.
- Open help
- Search Internet knowledge base
- Request support via e-mail
- Request support via web form

Actions

- Open help

  1. Choose the **Help and support** section of the Control Panel.
  2. Click the **Open help** link.

- Search Internet knowledge base

  1. Choose **Help and support** section of the Control Panel.
  2. Click the **Search Internet knowledge base** link to find information in SafenSoft's online knowledge base.

- Send support request
  1. To send a request to the Support service, establish Internet connection.
  2. Choose **Help and support** section of the Control Panel.
  3. Click the **Support request (recommended)** link to send your request by e-mail.
  4. Enter User Data and request description and click on **Forward** button.
  5. Check the data to be sent: Settings and program info, processes, Windows system information. Attach screenshot or file with the detailed description if it is necessary and click on **Forward** button.
  6. Click on **Finish** button to send the e-mail to SafenSoft Support team.

- Send support request using web form
  1. To send a request to the Support service, establish Internet connection.
  2. Choose **Help and support** section of the Control Panel.
  3. Click the **Send support request (web form)** to open SafenSoft's website.
  4. Enter user data and request description and click on **Send** button.

4 Getting started

SafenSoft SysWatch default settings provide good basic protection immediately after installation.

It is possible that the computer might have been infected before **SafenSoft SysWatch** was installed. For this reason, a full scan to detect and treat existing malware infections is performed automatically during the automatic adjustment process, if you have a version of the software that includes an antimalware scanner. Otherwise, third-party antimalware should be used to scan the computer before installing **SafenSoft SysWatch**.

Because we are continuously improving the software **SafenSoft SysWatch** will automatically check for updates and install them before the automatic adjustment process begins. The same applies to antimalware signature update files, if that capability is included with your version of the software.

As soon as these steps have been taken, the program is ready.

4.1 Program activation

The functionality available in **SafenSoft SysWatch** functionality is determined by the license type installed on this computer. The license key is provided at the time of purchase; the following components are available for use as soon as **SafenSoft SysWatch** is installed:

- **SafenSoft SysWatch Core (Core)** which is the primary proactive protection component.
- **SafenSoft SysWatch Rootkit Detector (RD),** which is the primary component responsible for detecting rootkits.
- **Antivirus (AV)** is an optional additional component that scans for viruses, trojans, worms, and other malware.
- **Antispyware (AS)** is an optional additional component that scans for spyware.

When the license key expires, the product will remain fully functional, but program and antimalware signature updates will not be available, we cannot guarantee that the antimalware scanner will continue to be effective after the SafenSoft **SafenSoft SysWatch** license key has expired.
To continue to get the full value of the **SafenSoft SysWatch** protection and take advantage of new features and improvements, the license key should be renewed promptly. A week before the **SafenSoft SysWatch** license expires, the program will notify you, and thereafter each time the program is started up, another reminder message will be displayed.

There are two ways to activate the program:
Automatic activation - enter the serial number and the program will automatically validate the key and activate itself.
Manual activation - you will need to provide the serial number and hardware code to SafenSoft technical support by phone or e-mail. You will receive the license key by phone or e-mail, so you can then manually activate the program.
The serial number consists of a sequence of digits separated by hyphens, which must be entered into a series of blocks with no spaces. The serial number must be entered using the Roman alphabet.If the program was purchased in a box, the serial number will be printed on the setup disk envelope.

Actions

▼ Activate program

1. Provide the license key in the Number filed and click on the **Activate** button.

2. In case Internet connection is available the program will automatically get activated

   or

3. In case no Internet connection is available the program will suggest Manual activation option.

4. You will be suggested to contact the Support service by phone and provide them with the serial number and hardware code.

5. Type the license key obtained from the Support service in the Number field and click on the **Activate** button.

4.2 Program update

Because we are continually improving the product, changes and new features may already be available at the time the software is installed. Additionally, the signature database accompanying the antimalware scanner (if included in the product) will need to be updated immediately upon installation. **SafenSoft SysWatch** will automatically check for updates and install them before the automatic adjustment process begin.

Actions

- Change automatic update settings

  1. Click on the **Update** section of the Control Panel. Then click on the **Settings** link to open the Update section of the Application settings window.

  2. In the **General settings for program update** window, you can Disable/Enable automatic updates, Enable/Disable confirmation before update, set frequency of automatic updates, and set program components to be updated (program and signature databases).

  3. Click **Ok** to apply the changes.

- Change Internet connection settings for automatic updates

  1. Click on **Update** section of the Control Panel. Then click on **Settings** link to open **Update** section of the Application settings window.

  2. In **General settings for program update** window click Configure button.

  3. In the **Advanced settings** window select **Connection** tab.

  4. Check **Use default proxy settings** then enter **Address** and **Port** number (80 by default). Enter **User**

name and **Password**, if authorization is required.

5. Click on **Apply** button to apply changes or click on **Ok** button to apply changes and close window.

▼ Set credentials for automatic updates

1. Click on **Update** section of the Control Panel. Then click on **Settings** link to open **Update** section of the Application settings window.

2. In **General settings for program update** window click **Configure** button.

3. In the **Advanced settings** window select **Credentials** tab.

4. Set account for automatic updates, if you don't like to run updates under Local system account (default).

5. Click on **Apply** button to apply changes or click on **Ok** button to apply changes and close window.

4.3 Scan

It is possible that your computer might have been infected with malware before **SafenSoft SysWatch** was installed. For this reason, a full scan to detect and neutralize any existing malware is be performed automatically during the automatic adjustment process, if an antimalware scanner is included with your version of the product. Otherwise, a third-party antimalware scanner should be used to run a complete scan before installing **SafenSoft SysWatch**.

The antimalware scanner uses the following components to detect and neutralize malicious code:

- **Antivirus databases** - signatures of known viruses, worms, Trojans and other malware.
- **Antispyware databases** - signatures of known spyware.
- **The Rootkit Detector** - searches for hidden malicious objects (rootkits). A rootkit is a program or set of programs used to hide malicious activities, or attacks on the operating system. A rootkit injects itself into the operating system and disguises its existence and the existence of processes, folders, and registry keys that relate to other malicious programs described in the rootkit's configuration file.

The antimalware scanner compares the object it scans against records in its databases; if a match is found, it marks the object as malicious. This is a often described as signature-based analysis. In order to detect hidden resources, all the running processes and system hooks are checked.

In order to perform a scan, it is necessary to:

- Include objects to be scanned in the protection scope. Any of the following objects can be

scanned: file system objects (logical drives and files), system memory, bootable sectors, etc. By default all objects are included in the scope.

- The scan results require a decision to be made regarding any the threats found, that have not been neutralized.

Scans should be performed as follows:

Immediately after installing SafenSoft SysWatch no other antimalware was previously installed.

Any time the application activity control is disabled and external storage (USB, CD, DVD, etc) has been used or an Internet connection has been established.

NOTE

In order to be able to use the anti-virus and antispyware databases you must be using a licensed copy of a version of SafenSoft SysWatch that includes antimalware.

IMPORTANT

For effective malware scanning, the signature databases should be updated daily. The simplest way to ensure this happens is to set up a daily automatic update.

Actions

▼ Run scan

1. Specify one or more objects in the Scan section of the Control panel.
2. Click **Run scan**.
3. To check the progress of the scan, click the **Details** link.

▼ Stop scan

1. Click the **Stop scan** button in the Scan section of the Control panel. Note that the scan cannot be stopped until after initialization is complete.
2. To examine the state of the scan click the **Details** link.

▼ View scan report

1. Click the **Last scan** link in the Scan section of the Control panel.
2. A scan report in text format will be opened.

▼ Manually select the action on detected threat

1. Open the **Program properties** window from the program's Context menu and select the **Scan** section.

or

Click the **Settings** link in the Scan section of the Control panel.

2. Set **Select action when the scan finishes** to view all detected threats, or **Ask action** to make a decision about each threat uncovered during the scan.

3. Start scan.

▼ Scan all files/search for unknown threats

1. Open the **Program properties** window from the program's Context menu and select the **Scan** section.

or

Click the **Settings** link in the Scan section of the Control panel.

2. In the Advanced settings windows, set **All files**, check **Mail bases** and **Archives**, check **Use digital signatures** and **Use heuristics** for a slower, but more comprehensive scan.

3. Start scan.

▼ Search for rootkits

1. Open the **Program settings** window from the program's context menu and select the **Scan** section.

or

Click the **Settings** link in the Scan section of the Control panel.

2. Check the **Search for hidden resources** checkbox.

3. Start scan.

▼ Set scanner startup parameters

1. Click on **Update** section of the Control Panel. Then click on **Settings** link to open **Update** section of the Application settings window.

2. Click on **Configure** button under **Check files** section to open **Advanced settings** window.

3. Choose **Startup options** tab in Advances settings window.

4. Set scanner startup account if you don't like to run scanner under Local system account (default).

5. Check **Preinitialize scanner** for faster scanning (requires more RAM). Scanner will be loaded to RAM at system startup.

6. Click on **Ok** button in Advanced settings windows and in Application settings window to apply changes.

4.3.1 Objects

You can specify the following objects to be scanned:

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

  It is recommended a system memory scan is performed each time daily and whenever a new process not started by you appears.

- **Bootable sectors** - scan the hard drive's boot sectors.
- **Objects in quarantine** - scan objects moved to quarantine should be scanned.

  It is recommended objects in quarantine be scanned after each program update is completed.

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

  It is recommended to scan removable drives whenever you plan to read or write files from or to such drives or run a program from a removable drive.

- **All hard drives** - scan all file system objects on all hard drives.
- **My computer** - scan all file system objects on the computer.
- **Trash** - scan all deleted objects.
- **My documents** - scan your documents.
- **Desktop** - scan all file system objects on the desktop.

Actions

▼ Run scan

1. Specify one or more objects in the **Scan** section of the Control panel.
2. Click the **Run scan** button.
3. To examine the state of the scan click the **Details** link.

▼ View scan report

1. Click the Last scan link in the Scan section of the Control panel.
2. TXT scan report will be opened

4.3.2 Scan results

When a malicious object is detected **SafenSoft SysWatch** determines the type (virus, worm, Trojan, spyware, etc.) and takes one of the following actions:

- **Treats** or **Deletes** the infected object if treatment is impossible.

- **Postpones** treatment of infected objects detected until the scan is complete. **SafenSoft SysWatch** provides a list of detected threats on scan completion and will request a decision on action to take for each object detected.
- **Asks action** each time a threat is detected:
  - **Treat** - to treat the threat or delete it if treatment is not possible, or terminate a malicious process.

    It is recommended this action is performed if your data or any of your applications have been modified by a malicious program.
  - **Delete** - to delete an infected file and terminate a malicious process.

    It is recommended this action is performed when a malicious program is detected.
  - **Move to quarantine** - to move an infected object to a special folder and block it from execution.

    This action is recommended whenever you suspect SafenSoft SysWatch has found a malicious object.
  - **Skip** - to take no action regarding the object.

Actions

▼ View detected threats

1. A list of all threats detected is available only after a scan is complete. It also contains a log of all infected objects found since **SafenSoft SysWatch** was installed.

2. Click the **Detected** link in the **Scan** section of the Control panel.

3. The window with detected threats will be opened.

▼ View scan report

1. Click the **Last scan** link in the **Scan** section of the Control panel.

2. A scan report in text format will be opened.

▼ Change the action on detected threat

1. Open the **Program properties** window from the program's context menu and select the **Scan** section.

or

2. Click the **Settings** link in the Scan section of the Control panel.

3. Set **Select action when the scan finishes** to view all found threats or **Ask action** to be asked on every single threat during the scanning.

4. Start scan.

4.3.3 Detected Threats

The **Detected threats** list contains information about malicious objects found, along with the actions taken on those objects:

- **Date** - the date and time when a malicious object was found.
- **Object** - the name of the object and its path:
  - File name.
  - Process name in memory.
  - Boot sector.
- **Path** - the full path to the object.
- **Detected** - the name of the malicious object.
- **Status** - the status of the object:
  - **Detected** - malicious object has been detected.
  - **Treated** - malicious object has been disinfected.
  - **Deleted** - malicious object has been deleted.
  - **Moved to quarantine** - malicious object has been moved to the quarantine folder.
  - **Cannot be treated** - the object cannot be disinfected.

    It is recommended the object be deleted manually.
  - **Cannot be deleted** - an error has occurred when deletion was attempted.

    In this instance, it is recommended the process be terminated and the object blocked .
  - **Cannot move to quarantine** - an error occurred when an attempt was made to move the object to quarantine folder.

    In this instance it is recommended that the process be terminated and the object blocked .

Treat - to treat the object.

Delete - to delete malicious objects.

Move to quarantine - to move the malicious objects to a special quarantine folder.

NOTICE

The list of *Detected Threats* is available only after the scan is completed. The list contains the entire history of all threats detected from the time **SafenSoft SysWatch** was installed.

Actions

▼ Manually treat detected threats

1. Check detected objects in the **Detected Threats** window.
2. Click the **Treat**, **Delete** or **Move to Quarantine** links to ensure the appropriate action is taken regarding the detected threat.

▼ Send detected threats to technical support for analysis

1. Select objects in the **Detected Threats** list.
2. Select the **Send** command from the list's Context menu. The program will create an e-mail with the information required by SafenSoft technical support and open it in the default e-mail client.
3. Send the e-mail.

5 Settings

SafenSoft SysWatch is designed to deliver operating system and application consistency by preserving the integrity of all system components.

SysWatch protection comprises:

- **Application launch control** - protects all executable software on the system by detecting any unauthorized activation attempt and preventing the process from launching before damage can occur.
- **Sandboxing** - specially-designated user account for potentially dangerous software provides system-level privilege controls to block malicious software activity.
- **Application activity control** - controls how different applications can access files and folders, registry keys, external devices, and network resources. User-driven rules can be created to control application activity.

System protection is performed in accordance with application control policy, which defines what rules will be applied to which applications.

SafenSoft SysWatch offers the following proactive protection settings:

Application control policy
Protection scope
Managing applications and processes

5.1 System Profile Creation

In order to ensure the best possible protection, **SafenSoft SysWatch** automatically creates and adjusts System Profiles on the first run. If the computer is restarted or switched off before the end of the automatic adjustment, it will continue from the point at which it was stopped when the system is powered back on. After the automatic adjustment is successfully completed, **SafenSoft SysWatch Extended Mode** is activated, which enables you to:

- **Classify** all installed applications into trusted/known and potentially harmful/unknown categories.
- **Execute** unknown applications in a sandbox and automatically block any malicious activities.
- **Reduce** the need for user interaction when a decision needs to be made about an application launch.

System Profile creation consists of the following steps:

- **Update** automatic adjustment components via the Internet. If an Internet connection is unavailable, existing components are used.
- **Search and collect information** about all executable files (exe, com, dll, etc.)
- **Identification of executable files**
- **Define rules** for application execution:
  - **Trusted** or **known** application
  - **Restricted** application.
  - **Blocked** application (execution is prohibited).
- **Scan application files** for malware

Running in Extended Mode, **SafenSoft SysWatch** tracks new or unknown applications (those not present in the **System Profile**), blocks harmful actions, and notifies you of any suspicious activities.

NOTE

*The time taken to create the System Profile depends on the amount of software installed on the system. It is recommended that you **minimize** the* **SafenSoft SysWatch** *interface to the Windows task bar and continue to work while this process is completed*

NOTE

You can update the System Profile if necessary. For example, the profile should be updated whenever a significant change is made to the system, such as attaching an external storage device that contains executable files. Simply update System Profile when the device is connected; after the update is completed, the applications on the storage device will be considered known and trusted.

IMPORTANT

Do not install or update software during an automatic adjustment, as SysWatch will be unable to add new or changed software to the System Profile. You can update or add new software to the System Profile by launching it in installation mode.

Actions

- Cancel automatic adjustment

  1. In the **General Settings for Protection** window, open the **System Profile** tab while automatic adjustment is in progress.

  2. Click the **Stop** button.

  3. **SafenSoft SysWatch** will ask whether you wish to continue the automatic adjustment later or not.

- Update System Profile

  1. In the **General Settings for Protection** window, open the **System Profile** tab.

  2. For **Scope**, select **Disks** to create the System Profile or add files and folders to be added to the existing profile.

  3. Click the **Update** button.

5.2 Application control policy

System protection is provided according to the application activity policy.

Application control policy – a set of rules which determines the activity controls for each applications.

Activity control rule – a set of conditions that describe an application's activities and actions that **SafenSoft SysWatch** takes when such activities occur.

Activity control rules can be applied to the following groups of applications:

- All
- Trusted
- Restricted

Trusted applications are identified basing on digital signature from a trusted Certification Authority, presence in the Windows catalog (CATalog file), and the **SafenSoft SysWatch** application white list

(system profile). Applications can be designated trusted manually by launching them in Install Mode.

Restricted applications are those applications that have been removed from Trusted manually, or unknown applications that are not present in the system profile.

The proactive protection technologies used in the application activity control allow the program to rapidly neutralize new threats before damage can occur. **SafenSoft SysWatch** delivers effective protection and without the need for signature updates. Your computer will be protected against zero-day threats and application vulnerabilities before security patches and application updates are released.

The Application control policy window consists of:

- Common rules
- Processes and applications

5.2.1 Protection scope

The **Common Rules** tab in the **Application control policy** window contains information about the general rules

imposed on all applications when resource (files, folder, system registry, etc.) or device access is detected. These rules are grouped into following categories:

- File system
- System registry
- Network
- Process privileges
- Devices
- Interprocess interaction

A default set of rules is included with the program, developed by **SafenSoft SysWatch**'s experts as a result of analyzing malicious code behavior.

Actions

▼ Block access to file object

1. Choose **Activity policy** in the Context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **File system** protection scope from the drop-down list.

3. Select a file system object in the tree and
   - Check the **Read** checkbox in order to protect the file from reading by applications. This will automatically block changing and deletion of the file.
   - Check the **Write** checkbox to protect the file object from creation and altering by applications.
   - Check the **Delete** checkbox to protect the file object from being deleted.

4. Right click in the Use for column to change the group of applications which will be affected by the activity control rule:
   - **All** – the rule will be applied to all applications
   - **Trusted** – the rule will be applied to known/trusted applications, which are present in the system profile
   - **Restricted** - the rule will be applied to potentially dangerous – restricted or unknown applications, which are not present in the system profile

5. Right click in the **Use for** column and choose **Additional** item.

6. Change following settings in the Additional window:
   - **Users** – select the users to be controlled by this rule
   - **Time** – set time periods for the rule to be active. The rule will be active at all times by default
   - **Exceptions** – select the applications to be excluded from the rule

7. Click on **OK** button in the **Additional** window to save changes

8. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

▼ Block access to a System registry object

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **System registry** protection scope from the drop-down list.

3. Select a file system object in the tree and

- Check the **Read** checkbox in order to protect the selected system registry object from being read by applications. This will automatically preventing changing or deletion of the system registry object.
- Check the **Write** checkbox to protect the selected system registry object from new entry creation or alteration by applications.
- Check the **Delete** checkbox to protect the selected system registry object from being deleted.

4. Right click in the **Use for** column to change the group of applications which will be affected by the activity control rule:

- **All** – the rule will be applied to all applications
- **Trusted** – the rule will be applied to known/trusted applications, which are present in the system profile
- **Restricted** - the rule will be applied to potentially dangerous – restricted or unknown applications, not present in the system profile

5. Right click in the **Use for** column and choose **Additional** item.

6. Change following settings in the **Additional** window:

- **Users** – select the users to be controlled by the rule
- **Time** – set time periods for the rule to be active. The rule will be active at all times by default
- **Exceptions** – select the applications to be excluded from the rule

7. Click on **OK** button in the **Additional** window to save changes

8. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

▼ Create new Network rule

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Network** protection scope from the drop-down list.

3. Click the **Add** button.

4. Enter a name of the network rule into the **Name** field.

5. Specify the direction of data transfer from the **Direction** drop-down list. The default value is **Inbound/Outbound**.

6. Specify the network protocol from the **Protocol** drop-down list. The default value is **TCP/UDP**.

7. Define the **Local** IP address or an address range in the appropriate fields. The default value is **Any address**.

8. Define the **Remote** IP address or an address range in the appropriate fields. The default value is **Any address**.

9. Click on the **OK** button to save the rule.

10. Change following settings in the **Additional** window:
    - **Users** – select the users to be controlled by the rule
    - **Time** – set time periods for the rule to be active. The rule will be active at all times by default

11. Click on **OK** button in the Additional windows to save changes

12. In the list of network rules uncheck the **Allow** checkbox next to the rule created to block connection to the specified network resource.

13. In the list of network rules check the **Confirm** checkbox to be prompted each time **SafenSoft SysWatch** is going to restrict application's network activity.

14. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

▼ Change Network rule

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Network** protection scope from the drop-down list.

3. Select an appropriate network rule from the list.

4. Click the **Edit** button.

5. Change the rule and click on the **OK** button to save changes.

6. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

▼ Remove Network rule

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Network** protection scope from the drop-down list.

3. Select an appropriate network rule from the list.

4. Click the **Delete** button.

5. Click on the **OK** button to confirm deletion.

6. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

▼ Block any network activity for restricted applications

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Network** protection scope from the drop-down list.

3. Select the **Any network activity** network rule from the list and uncheck the **Allow** checkbox next to it.

4. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

▼ Deny access to USB devices and set exceptions

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Devices** protection scope from the drop-down list.

3. Select the **USB Devices** from the list and uncheck the

- Uncheck the **Read** checkbox to protect the selected USB device from being read by applications. This will automatically prevent change or deletion of the files and folders stores on the USB device.
- Uncheck the **Write** checkbox to protect the selected USB device from new file and folder creation and the alternation of existing data by applications.
- Uncheck the **Delete** checkbox to protect files and folders stored on the selected USB device from being deleted.

4. Click on **Additional** link.

5. Change following settings in the **Additional** window:

- **Users** – select the users to be controlled by the rule
- **Time** – set time periods for the rule to be active. The rule will be active at all times by default
- **Exceptions** – select devices to be excluded from the rule. You can additionally allow/deny **Read**, **Write** and **Delete** access for the excepted device.
- **Update** – update the list of USB devices attached to the computer
- **Remove** - remove the selected device from the list of excepted devices

6. Click on **OK** button in the Additional window to save changes

7. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

▼ Disable autorun for all devices

1. Choose **Activity policy** in the Context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Devices** protection scope from the drop-down list.

3. Check **Disable autorun for all devices**.

4. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

- Disable access to CD/DVD devices

1. Choose **Activity policy** in the Context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Devices** protection scope from the drop-down list.

3. Select the **CD/DVD Devices** from the list and uncheck the **Read**, **Write**, **Delete** checkboxes.

4. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

- Disable access to LPT ports

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Devices** protection scope from the drop-down list.

3. Select the **LPT Ports** from the list and uncheck the **Read**, **Write**, **Delete** checkboxes.

4. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

- Disable access to COM ports

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Devices** protection scope from the drop-down list.

3. Select the **COM Ports** from the list and uncheck the **Read, Write, Delete** checkboxes.

4. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

- Hide unrestricted resources

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **File System** or **System Registry** protection scope from the drop-down list.

3. Uncheck the **Show objects without access restrictions** checkbox.

4. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

▼ Enable access to the clipboard by applications run under V.I.P.O. limited user

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Interprocess Interaction** protection scope from the drop-down list.

3. Check **Clipboard access** checkbox

4. Click on the **Additional** link.

5. Change following settings in the **Additional** window:
   - **Users** – select the users to be controlled by the rule
   - **Time** – set time periods for the rule to be active. The rule will be active at all times by default

6. Click on **OK** button in the Additional window to save changes

7. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

▼ Decrease Windows privileges for restricted processes and applications

1. Choose **Activity policy** in the Context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Interprocess Interaction** protection scope from the drop-down list.

3. Select a privilege in the list and uncheck the checkbox at the **State** column.

4. Click on **Additional** link.

5. Change following settings in the Additional window:
   - **Users** – select the users to be controlled by the rule
   - **Time** – set time periods for the rule to be active. The rule will be active at all times by default

6. Click on **OK** button in the Additional window to save changes

7. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

5.2.1.1 File System

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

- **Reading** a file or a folder.
- **Creating or Changing** a file or a folder.
- **Deleting** a file or a folder.

Masks (asterisks) can be used to create activity control rules for the file system objects of the same type or with similar names. Using masks you can easily filter the data to be protected.

Actions

▼ Block access to the objects on the C:\ drive using file mask

1. Choose **Activity policy** in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **File system** protection scope from the drop-down list.

3. Expand Drive C:\ tree and select **No masks (press Ins to add the mask)** parameter.

4. To set access rules for the group of objects with similar names or with same extension, Press **Ins (Insert)** button and enter the regular expression for the full file or folder name (including path to the object). Following masks can be used:

#*# - replaces any number of characters, except '\'
##** - replaces any number of characters
#0# - equivalent to the comparison with zero byte
#?# - replaces 1 character

5. For example, to set access rules for all files on the drive C:\ which have **log** in the file name and have .TXT extension: Press **Ins (Insert)** button and add following mask: **#**#log#**#.TXT**

NOTE

For the created mask:

- Check the **Read** checkbox in order to protect all TXT files from reading by applications. This

will automatically block changing and deletion of the TXT files.

- Check the **Write** checkbox to protect all TXT files from creation and altering by applications.
- Check the **Delete** checkbox to protect all the TXT files from being deleted.

6. Right click in the **Use for** column to change the group of applications which will be affected by the activity control rule:

- **All** – the rule will be applied to all applications
- **Trusted** – the rule will be applied to known/trusted applications, which are present in the system profile
- **Restricted** - the rule will be applied to potentially dangerous – restricted or unknown applications, which are not present in the system profile

7. Right click in the **Use for** column and choose **Additional** item.

8. Change following settings in the **Additional** window:

- **Users** – select the users to be controlled by the rule
- **Time** – set time periods for the rule to be active. The rule will be active at all times by default
- **Exceptions** – select applications to be excluded from the rule

7. Click on **OK** button in the Additional window to save changes

8. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

Block access to file object

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **File system** protection scope from the drop-down list.

3. Select a file system object in the tree and

- Check the **Read** checkbox in order to protect the file from reading by applications. This will automatically block changing and deletion of the file.
- Check the **Write** checkbox to protect the file object from creation and altering by applications.
- Check the **Delete** checkbox to protect the file object from being deleted.

4. Right click in the **Use for** column to change the group of applications which will be affected by the activity control rule:

- **All** – the rule will be applied to all applications
- **Trusted** – the rule will be applied to known/trusted applications, which are present in the system profile
- **Restricted** - the rule will be applied to potentially dangerous – restricted or unknown applications, which are not present in the system profile

5. Right click in the **Use for** column and choose **Additional** item.

6. Change following settings in the Additional window:

- **Users** – select users to be controlled by the rule
- **Time** – set time periods for the rule to be active. The rule will be active all the time by default
- **Exceptions** – select applications to be not affected by the rule

7. Click on **OK** button in the Additional window to save changes

8. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

5.2.1.2 System Registry

The **System Registry** protection scope covers the creation of rules controlling access to the Windows System Registry:

- **Reading** keys and values.
- **Creating** or **changing** keys and values.
- **Deleting** keys and values.

Actions

▼ Block access to a System Registry object

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **System registry** protection scope from the drop-down list.

3. Select a file system object in the tree and
   - Check the **Read** checkbox in order to protect the selected system registry object from reading by applications. This will automatically block changing and deletion of the system registry object.
   - Check the **Write** checkbox to protect the selected system registry object from new entries creation and altering by applications.
   - Check the **Delete** checkbox to protect the selected system registry object from being deleted.

4. Right click in the **Use for** column to change the group of applications which will be affected by the activity control rule:
   - **All** – the rule will be applied to all applications
   - **Trusted** – the rule will be applied to known/trusted applications, which are present in the system profile
   - **Restricted** - the rule will be applied to potentially dangerous – restricted or unknown applications, which are not present in the system profile

5. Right click in the **Use for** column and choose **Additional** item.

6. Change following settings in the Additional window:
   - **Users** – select the users to be controlled by the rule
   - **Time** – set time periods for the rule to be active. The rule will be active at all times by default
   - **Exceptions** – select applications to be excluded from the rule

7. Click on **OK** button in the **Additional** window to save changes

8. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

5.2.1.3 Network

The **Network** protection scope covers the creation of access rules for restricted applications with regard to network resources:

- **Creating** network connections.
- **Transferring** data to a remote computer.
- **Receiving** data from a remote computer.

A network rule includes the following information:

Name specifies the name of the rule.

Direction - specifies the direction of a network connection from the perspective of the connection originator:

- **Inbound** – indicates that the connection has been initiated by the remote computer.
- **Outbound** – indicates that the connection has been initiated by the local computer.
- **Inbound/Outbound** - bidirectional coverage.

Protocol - specifies the name of the protocol used to establish the connection:

- **TCP**
- **UDP**
- **TCP/UDP** - either protocol.

Local address - specifies the IP address or range of IP addresses for the local computer. *.* covers any available local network address.

Remote address - specifies the IP address or a range of IP adresses for the remote computer.

Actions

▼ Create new Network rule

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Network protection** scope from the drop-down list.

3. Click the **Add** button.

4. Enter a name of the network rule into the **Name** field.

5. Specify the direction of data transfer from the **Direction** drop-down list. The default value is **Inbound/Outbound.**

6. Specify the network protocol from the **Protocol** drop-down list. The default value is **TCP/UDP**.

7. Define the **Local** IP address or an address range in the appropriate fields. The default value is **Any address**.

8. Define the **Remote** IP address or an address range in the appropriate fields. The default value is **Any address.**

9. Click on the **OK** button to save the rule.

10. Change following settings in the **Additional** window:

- **Users** – select the users to be controlled by the rule
- **Time** – set time periods for the rule to be active. The rule will be active at all times by default

11. Click on **OK** button in the Additional windows to save changes

12. In the list of network rules uncheck the **Allow** checkbox next to the rule created to block connection to the specified network resource.

13. In the list of network rules check the **Confirm** checkbox to be prompted each time SafenSoft SysWatch is going to restrict application's network activity.

14. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

Change Network rule

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Network protection** scope from the drop-down list.

3. Select an appropriate network rule from the list.

4. Click the **Edit** button.

5. Change the rule and click on the **OK** button to save changes.

6. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

Remove Network rule

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Network protection** scope from the drop-down list.

3. Select an appropriate network rule from the list.

4. Click the **Delete** button.

5. Click on the **OK** button to confirm deletion.

6. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

▼ Block any network activity for restricted applications

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Network protection** scope from the drop-down list.

3. Select the **Any network activity** network rule from the list and uncheck the **Allow** checkbox next to it.

4. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

5.2.1.4 Devices

The **Devices** protection scope covers the creation of rules to control access to certain devices:

- **USB devices**
- **CD/DVD drives**
- **COM ports**
- **LPT ports**

Actions

▼ Deny access to USB devices and set exceptions

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Devices** protection scope from the drop-down list.

3. Select the **USB Devices** from the list and uncheck the

    • Uncheck the **Read** checkbox in order to protect the selected USB device from reading by

applications. This will automatically block changing and deletion of the files and folders stores on the USB device.

• Uncheck **Write** checkbox to protect the selected the selected USB device from new files and folders creation and altering existing data by applications.

• Uncheck the **Delete** checkbox to protect files and folders stored on the selected USB device from being deleted.

4. Click on **Additional** link.

5. Change following settings in the **Additional** window:

- **Users** – select the users to be controlled by the rule
- **Time** – set time periods for the rule to be active. The rule will be active at all times by default
- **Exceptions** – select the devices to be excluded from the rule. You can additionally allow/deny **Read**, **Write** and **Delete** access for the excepted device.
- **Update** – update the listed of USB devices attached to computer
- **Remove** - remove the selected USB device from the list of excepted devices

6. Click on **OK** button in the Additional window to save changes

7. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

Disable autorun for all devices

1. Choose **Activity policy** in the Context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Devices** protection scope from the drop-down list.

3. Check **Disable autorun for all devices.**

4. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

Disable access to CD/DVD drives

1. Choose **Activity policy** in the Context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Devices** protection scope from the drop-down list.

3. Select the **CD/DVD Devices** from the list and uncheck the **Read**, **Write**, **Delete** checkboxes.

4. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

- Disable access to LPT ports

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Devices** protection scope from the drop-down list.

3. Select the **LPT Ports** from the list and uncheck the **Read**, **Write**, **Delete** checkboxes.

4. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

- Disable access to COM ports

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Devices** protection scope from the drop-down list.

3. Select the **COM Ports** from the list and uncheck the **Read**, **Write**, **Delete** checkboxes.

4. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

5.2.1.5 Process Privileges

The **Process Privileges** protection scope enables the reduction of Windows privileges for restricted processes and applications.

You can disable following Windows privileges for the restricted processes and applications:

- Manage auditing and security logs
- Back up files and directories
- Restore files and directories
- Change system time

- Shut down 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
- Create a pagefile
- Adjust memory quotas for a process
- Bypass traverse checking
- Remove computer from docking station
- Perform volume maintenance tasks
- Impersonate a client after authentication
- Create global objects

Actions

▼ Reduce Windows privileges for restricted processes and applications

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Process Privileges** protection scope from the drop-down list.

3. Select a privilege in the list and uncheck the checkbox at the **State** column.

4. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

5.2.1.6 Interprocess interaction

The **Interprocess Interaction** protection scope allows restrictions for sandboxed processes to be disabled, both: the processes which are run under V.I.P.O. limited user (for restricted applications) and those are run under Safe'n'Sec limited user (for trusted applications).

After **SafenSoft SysWatch** installation, the following restrictions are set for the processes run under V.I.P.O. limited user:

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

For the processes run under Safe'n'Sec limited user restriction is set for trusted applications:

- Access to the process and its threads from outside

Actions

▼ Enable access to the clipboard by applications run as restricted application under V.I.P.O. limited user

1. Choose **Activity policy** item in the context menu.

2. Switch to **Common rules** tab in the **Application control policy** window. Select the **Interprocess Interaction** protection scope from the drop-down list.

3. Check Clipboard access checkbox

4. Click on the **Additional** link.

5. Change following settings in the Additional window:
   - **Users** – select users to be controlled by the rule
   - **Time** – set time periods for the rule to be active. The rule will be active all the time by default

6. Click on **OK** button in the **Additional** window to save changes

7. Click on **OK** or **Apply** button in the Common rules tab to save new rule and to update Application control policy.

5.2.2 Processes and applications

The Processes and applications section in the Application control policy window contains information about all applications run on the computer during or after the **SafenSoft SysWatch** installation:

Name - specifies the name of an application (read from the version info of the application) or the name of a file.

Status - specifies the status of an application:

- **Black** - indicates that the application is currently executing.
- **Gray** - indicates that the application is currently not running.

Restrictions - specifies the set of restrictions imposed on the application.

- **Custom** – applicable for a particular application
- **Common** - applicable for a group of applications. Common rules can be created for All, Trusted, or Restricted applications and certain applications can be excluded from the rules.
- **All blocked** - specifies that the execution and all actions by the application are blocked.

Vendor - determines the producer of the application (read from the version info of the application).

Full name - determines the name and the path to the installation directory of the application (read from the version info of the application).

Actions

Block application

1. Choose **Processes and applications** in the context menu.

2. Specify one or more applications in the list and select the **Block execution** Item of the context menu.

3. Click on **OK** or **Apply** button to save the changes.

IMPORTANT

Please, be careful blocking execution of an application. If you block execution of a system service or process it may lead to Windows inoperability.

Add new application

1. Choose **Processes and applications** item in the context menu.

2. Click the **Add** link and specify an application in the **Open file** dialogue.

3. Click on **OK** or **Apply** button to save the changes. The application will be added to the restricted applications.

Move application to Trusted

1. Choose **Processes and applications** item in the context menu.

2. Specify one or more applications in the list and right click on them.

3. From the context menu select the **Trust to application** item (or **Move to trusted** for the group of applications).

4. Click on **OK** or **Apply** button to save the changes.

Open application properties window

1. Choose **Processes and applications** item in the context menu.

2. Select application and click on the **Properties** link or right-click and select **Application properties**

from the context menu.

- Delete application from Trusted

1. Choose **Processes and applications** item in the context menu.

2. Specify one or more applications and from the context menu select the **Delete application from Trusted** item.

3. The application will be moved to restricted applications.

- Delete application from list

1. Choose **Processes and applications** item in the context menu.

2. Specify one or more inactive applications in the list and click the **Delete from list** link.

NOTE

When you delete application from list, all the structures related to this application will be removed from **SafenSoft SysWatch**'s database (custom rules for this application, execution conditions etc.).

- Delete application file on reboot

1. Choose **Processes and applications** item in the context menu.

2. Specify required application in the list and right click on it.

3. From the context menu select the **Delete application file on reboot** item.

- Terminate application

1. Choose **Processes and applications** item in the context menu.

2. Specify the active application in the list and click the **Terminate** link.

Please, be careful specifying applications for termination. Terminating system processes may lead to Windows restart.

5.2.2.1 Application properties

This section covers the following application properties:

General
Execution conditions
History
Restrictions and permissions

Actions

- Change execution conditions

1. Choose **Processes and applications** item in the context menu.

2. Select an application from the list, right-click on it and choose the **Application properties** item.

3. In the **Execution conditions tab** under restriction section you can set following parameters:

For the Trusted application

Block application – the application will be moved to Blocked

Delete application from Trusted the application will be moved to Restricted

For Restricted application

Block application

Trust to application – the application will be moved to Trusted

For Blocked application

Allow application – the application will be moved to Restricted

Trust to application

4. Click on **OK** button in the Application properties window.

- Scan application for malicious code

1. Choose **Processes and applications** item in the context menu.

2. Select an application from the list, right-click on it and choose the **Application properties** item.

3. In the **General tab** under Scanning section click the **Scan** link and select **Scan** from the context menu.

- Save application activity history

1. Choose **Processes and applications** item in the context menu.

2. Select an application from the list, right-click on it and choose the **Application properties** item.

3. In the **History tab** check Save activity history checkbox.

4. Check the **Create backup copies of objects for further recovery** checkbox to create backup copies of all file system and system registry objects which were changed or deleted by the application.

5. Click on **OK** button in the Application properties window

- Recover changed objects

1. Choose **Processes and applications** item in the context menu.

2. Select an application from the list, right-click on it and choose the **Application properties** item.
3. In the **History** tab select file system or system registry objects in the list and click the **Restore** link.

4. Click on **OK** button in the Application properties window.

5.2.2.1.1 General properties

The **General tab** in the **Application properties** window contains information about an application's executable file and the restrictions assigned to that file:

Path - specifies the full path to the executable file of the application.
Size - specifies the size of the file in bytes.
Created - specifies the date and time when the file was created.
Modified - specifies the date and time when the file was last changed.
Description - provides the description text from the file's version info.
Product - provides product's name (read from the file's version info).
Vendor - specifies the name of the company that produced the application (read from the file's version).
User - specifies that restrictions were manually assigned.
System process - specifies whether it is a system process or not.
Scan results - contains information about the most recent antimalware scan of the application (if the antimalware scanner and appropriate license are installed).

Actions

▼ Scan application for malicious code

1. Choose **Processes and applications** item in the context menu.

2. Select an application from the list, right-click on it and choose the **Application properties** item.

3. In the **General tab** under Scanning section click the **Scan** link and select **Scan** from the context menu.

5.2.2.1.2 Execution conditions

On the **Execution conditions tab** under **Application properties** the following parameters may be changed:

For a Trusted application

Block application – the application will be moved to Blocked

Delete application from Trusted - the application will be moved to Restricted

Turn on Install mode – all the application's modules (including new ones) will be added to the system profile

Set execution account

Limited user – the application will be launched in a sandbox for trusted, but potentially dangerous, applications. Potentially dangerous application activity will be blocked.

Current account – the application will be launched outside the sandbox.

For Restricted application

Block application – the application will be moved to Blocked

Trust application – the application will be moved to Trusted

Turn on Install mode – all the application's modules (including new ones) will be added to the system profile. The application will be moved to Trusted.

Set execution account

Isolated user (set by default) - the application will be launched in a sandbox. Potentially dangerous application activity will be blocked.

Current account – the application will be launched outside the sandbox.

For Blocked application

Allow application – the application will be moved to Restricted

Trust application - the application will be moved to Trusted

Turn on Install mode – all the application's modules (including new ones) will be added to the system profile. The application will be moved to Trusted

Actions

▼ Change execution conditions

1. Choose **Processes and applications** item in the context menu.

2. Select an application from the list, right-click on it and choose the **Application properties** item.

3. In the **Execution conditions tab** under restriction section you can set following parameters:

For the Trusted application

Block application – the application will be moved to Blocked

Delete application from Trusted the application will be moved to Restricted

For Restricted application

Block application

Trust to application – the application will be moved to Trusted

For Blocked application

Allow application – the application will be moved to Restricted

Trust to application

4. Click on **OK** button in the **Application properties** window.

▼ Turn on Install mode

1. Choose **Processes and applications** item in the context menu.

2. Select an application from the list, right-click on it and choose the **Application properties** item.

3. In the **Execution conditions tab** check **Turn on Install mode** checkbox.

4. Click on **OK** button in the Application properties window.

▼ Set Limited execution account

1. Choose **Processes and applications** item in the context menu.

2. Select an application from the list, right-click on it and choose the **Application properties** item.

3. In the **Execution conditions tab** set **Limited User**.

4. Click on **OK** button in the **Application properties** window.

5.2.2.1.3 Activity History

The **History tab** section in the **Application properties** window contains information about application activities they relate to file resource and System Registry access:

Time - specifies the date and time of an event.

Event - contains a description of the event:

Execute - specifies when the application started.

Stop - specifies when the application stopped.

Read - indicates that the application has read a file or System Registry object.

Change - indicates that the application has created or changed a file or a System Registry object. The changed objects can be restored.

Delete - indicates that the application has deleted a file or a System Registry object. The deleted objects can be restored.

Object - specifies the name of the file or System Registry object.

Result - specifies the result of restoring a changed object:

Restored - indicates that the object has successfully been restored.

Recovery error - indicates that the object cannot be restored.

The **SafenSoft SysWatch** stores backup copies of modified objects in the *<Installation directory>\History folder*.

Actions

Save application activity history

1. Choose **Processes and applications** item in the context menu.
2. Select an application from the list, right-click on it and choose the **Application properties** item.
3. In the **History tab** check **Save activity history** checkbox.
4. Check the **Create backup copies of objects for further recovery** checkbox to create backup copies of all file system and system registry objects which were changed or deleted by the application.
5. Click on OK button in the Application properties window.

Recover changed objects

1. Choose **Processes and applications** item in the context menu.
2. Select an application from the list, right-click on it and choose the **Application properties** item.
3. In the **History tab** select file system or system registry objects in the list and click the **Restore** link.
4. Click on **OK** button in the **Application properties** window.

5.2.2.1.4 Restrictions and Permissions

The **Restrictions and Permissions** tab in the **Application properties** window contains information about **Custom** rules that control an application when it accesses computer resources and devices. These rules are grouped into the following categories:

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

Custom rules take precedence over **Common** rules. It is the **Custom** rules that are evaluated first. The product may be shipped with a predefined set of rules established by the company's experts as a result of examining behavior of the given application.

NOTE

The process of changing Custom rules for an application is exactly the same as the process for changing Common rules.

Actions

▼ Change custom rules for the application

1. Choose **Processes and applications** from the Context menu.

2. Select an application from the list, right-click on it, and choose **Application properties**.

3. In the **Restrictions and Permissions tab,** under the restriction section rules can be set for:
   - File system access
   - System registry access
   - Network access
   - Process privileges

4. Click on **OK** in the **Application properties** window.

6 Alerts

SafenSoft SysWatch controls all activities of all applications installed on the computer and notifies the user about each policy or rules violation or an unknown application launch attempt. This section describes **SafenSoft SysWatch** alerts:

Unknown application launch

Unknown installer launch

Actions

Allow unknown application launch

1. Launch new application.

2. **SafenSoft SysWatch** suspends the launch and pops up an Alert window.

3. If you are sure that the application is safe, set **Execute in install mode** and click the **Execute** button.

   The application and all its modules will be added to the system profile as Trusted.

NOTE

You can scan the application for malicious code from the Alert Window. Click the **Scan** link to check the application (if antimalware scanner and appropriate license are available).

IMPORTANT

If you are not sure that the application is safe, set **Execute in a limited mode** and click on the **Execute** button to launch the application in a sandbox. The application will be launch under Isolated user account, the malicious activity will be blocked.

Block launch of unknown application

1. In case of unknown application launch is attempted, **SafenSoft SysWatch** suspends the launch and pops up Alert window.

2. If you don't know what application is launching or don't trust it, click on the **Block** button, to block the launch.

Allow launch of unknown installer

1. Launch the setup program for the new application.

2. **SafenSoft SysWatch** suspends the launch and pops up an Alert window.

3. Uncheck the **Run in limited mode** checkbox and click the **Execute** button. All the installer modules will be added to the system profile as Trusted.

Block launch of unknown installer and remember this selection

1. In case of unknown installer launch is attempted, **SafenSoft SysWatch** suspends the launch and pops up Alert window.

2. If you don't know what installer is launching or don't trust it, check **Never run this application in future** and click on the **Block** button, to block the launch

6.1 Unknown application launch

Unknown application – any application that is not present in the **SafenSoft SysWatch** system profile, other than installers with a digital signature from a trusted Certification Authority.

When the launch of an unknown application is attempted, **SafenSoft SysWatch** suspends the launch and pops up an Alert window.
The Alert window has 2 parts:

- **Application description**. Information about the unknown application is shown: name, vendor, antimalware scan result (if antimalware scanning is supported by your SafenSoft SysWatch license).
- **Available actions**. Available actions that can be performed on the application are shown:

  Execute in limited mode – application will be launched in a sandbox.

  Execute in install mode – application and all its modules will be added to the system profile as Trusted.

  Block – block application from launching. This option is recommended for any applications you don't trust or for unauthorized launch attempts by those applications.

NOTE

If no decision is made within 5 minutes of the Alert window appearings, the application will be blocked automatically.

NOTE

The Alert window may not appear, if Automatic processing of incidents is enabled. It is necessary to set **Delayed Decision** in the **Incident management** window for the Alert window to appear in the case of security incidents.

Actions

▼ Allow launch of unknown application

1. Launch new application.

2. **SafenSoft SysWatch** suspends the launch and pops up an Alert window.

3. If you are sure that the application is safe, set **Execute in install mode** and click the **Execute** button. The application and all its modules will be added to the system profile as Trusted.

NOTE

You can scan the application for malicious code from the Alert Window. Click the **Scan** link to check the application (if antimalware scanner and appropriate license are available).

IMPORTANT

If you are not sure that the application is safe, set **Execute in a limited mode** and click on the **Execute** button to launch the application in a sandbox. The application will be launch under Isolated user account, the malicious activity will be blocked.

▼ Block launch of unknown application

1. In case of unknown application launch is attempted, **SafenSoft SysWatch** suspends the launch and pops up Alert window.

2. If you don't know what application is launching or don't trust it, click on the **Block** button, to block the launch.

6.2 Unknown installer launch

Unknown installer – any setup program that does not contain a digital signature from a trusted Certification Authority or that has an expired digital signature.

If an unknown installer launch is attempted, **SafenSoft SysWatch** suspends the launch and pops up an Alert window. The Alert window has 2 parts:

- **Installer description**. Information about the unknown installer is shown: name, vendor, antimalware scan result (if antimalware scanning is supported by your SafenSoft SysWatch license).
- **Available actions**. Available actions that can be performed on the installer are shown:

  Execute – the installer and all its modules will be added to the system profile as Trusted.

  Execute with checked **Run in limited mode** – installer will be launched in a sandbox, all malicious activity will be blocked.

  Block – block installer from launching. This option is recommended for the applications you don't trust or for unauthorized launch attempts by those applications.

  Block with checked **Never run this application in future** - block installer from launching and remember the choice.

NOTE

If no decision is made within 5 minutes of the Alert window appearing, the installer will be blocked automatically

NOTE

The Alert window may not appear, if Automatic processing of incidents is enabled.
It is necessary to set **Delayed Decision** in **the Incident management** window for the Alert window to

appear in the case of security incidents.

NOTE

If the installer has a valid digital signature from a trusted Certification Authority, it will be executed in Install mode automatically.

Actions

- Allow launch of unknown installer

1. Launch the setup program for the new application.

2. **SafenSoft SysWatch** suspends the launch and pops up an Alert window.

3. Uncheck the **Run in limited mode** checkbox and click **Execute.** All the installer modules will be added to the system profile as Trusted.

- Block launch of unknown installer and remember this selection

1. In case of unknown installer launch is attempted, **SafenSoft SysWatch** suspends the launch and pops up Alert window.

2. If you don't know what installer is launching or don't trust it, check **Never run this application in future** and click on the **Block** button, to block the launch.

7 Glossary

- **Blocked Applications**

Applications not permitted to launch. In the SysWatch Processes and applications window, they are grouped under Blocked Applications.

- **Common Rules**

Rules for application activity control, set up for a group of applications: Trusted, Restricted, or All.

- **Custom Rules**

Rules for application activity control, set up for one particular application. Custom rules are processed after Common rules, so Custom Rules can apply exceptions to the Common rules.

- **Extended Mode**

Fully functional protection mode, based on the system profile and techniques used in Simple mode.

- **File Mask**

Masks (asterisks) can be used to create activity control rules for the file system objects of the same type or with similar names. Regular expression for the full file or folder name (including path to the object) can be created using following masks:
#*# - replaces any number of characters, except '\'
#**# - replaces any number of characters
#0# - equivalent to the comparison with zero byte
#?# - replaces 1 character

- **Install Mode**

Launch application and add to system profile as a trusted application

- **Isolated User**

VIPO sandbox, more restricted than the Safe'n'Sec sandbox, and used to launch unknown or restricted applications

- **Known Applications**

Applications that have been added to the system profile

- **Limited Mode**

Launch application in a sandbox, under a VIPO (restricted) user account

- **Limited User**

Safe'n'Sec sandbox used for known, trusted, but potentially dangerous applications

- **Restricted Applications**

Applications that are present in the system profile, but not included to the Trusted group, or unknown applications that are not present in the system profile. In the SysWatch Processes and applications window, both are grouped under Restricted Applications

- **Simple Mode**

Used immediately after installation, before the system profile is created, to protect the system during auto adjust (system profile creation)

- **System Profile**

Database containing all the information needed to identify an application and its modules

- **Trusted Applications**

Applications added to the system profile and run outside the sandbox. In the SysWatch Processes and applications window, Trusted Applications are grouped under Known, Trusted Applications

- **Unknown Applications**

Applications that have not been added to the system profile

- **Unknown Installer**

Installer with an expired digital signature or no digital signature from a trusted CA

8 SafenSoft

SafenSoft was founded in 2006 when the Proactive Computer Security department of StarForce, a leader in the field of digital content copyright protection software, decided to branch out.

Now SafenSoft is a leading developer of cutting edge information-security software solutions developed from the ground up to provide proactive protection.

The SafenSoft approach to security has its roots in digital rights management, where the goal is to preserve the integrity of the system rather than try to identify every malicious action attempted on that system. The technology behind this process, VIPO (Valid Inside Permitted Operations), is a unique and highly-effective architecture that efficiently monitors and processes all system activity for unexpected and/or unauthorized activities.

SafenSoft technology focuses on securing networks through system and application integrity, coupled with profile-based access controls. The company's founders experienced at first hand the increasing inability of signature-based security solutions to keep up with the pace of malware development through their work with leading traditional antimalware developers, and knew there had to be a better way. The resulting SafenSoft products deliver both proactive protection against internal threats and comprehensive data leak prevention solution.

SafenSoft technology is used by some of the world's largest banks to protect their ATM networks. SafenSoft SysWatch can deliver the same security standards to your business and home computers.

Contacts

Website	http://www.safensoft.com
Technical support service	support@safensoft.com
Sales Department	sales@safensoft.com