



IKARUS anti.virus Manual



 **IKARUS**
anti.virus
anti.spam

© IKARUS Security Software GmbH
<https://www.ikarussecurity.com>

Page 1 of 60

Index

1. Introduction	4
2. Installing IKARUS anti.virus	5
2.1 System requirements	5
2.2 Installing IKARUS anti.virus	6
2.3 Unattended command line installation	14
2.4 Uninstalling IKARUS anti.virus	17
3. Features of IKARUS anti.virus	19
3.1 Symbols and screens	20
4.1 Guard – Your personal minder	21
4.2 Updating IKARUS anti.virus	23
4.3 Scan - The virus check from IKARUS anti.virus	25
4.3.1 Scan-Settings	29
4.4 Quarantine - what to do when a virus is found?	30
4.4.1 Virus detection warning	30
4.4.2 Virus detected during scan	31
4.4.3 Quarantine	32
5.1 Anti-SPAM	37
5.2 Microsoft-SharePoint protection	38
5.2.1 Performance	39
5.2.2 Installation	40
5.2.3 Functioning	40
4. Settings	46
6.1 Language settings	46
6.2 Logs	47
6.3 Further settings	48
6.3.1 E-Mail	48
6.3.2 Update	49
6.3.3 Dial Up Connection	50
6.3.4 Exclusions	51
6.3.5 Logs	52
6.3.6 Extras	53

6.3.7 Anti-SPAM	54
5. Support	55
7.1 License key	57
6. Further informations	59
8.1 .NET Framework	59
8.2 Licensing Terms	59

1

Introduction

Thank you for choosing IKARUS anti.virus from IKARUS Security Software.

IKARUS anti.virus secures your personal data and PC from all kinds of malware. Additionally, the Anti-SPAM module protects you from SPAM and malware from e-mails. Prevent intrusion and protect yourself against cyber-criminals by choosing IKARUS anti.virus, powered by the award-winning IKARUS scan.engine. It is among the best in the world, detecting new and existing threats every day.

Simple installation, an intuitive user interface and frequent incremental updates of the virus database are just some of the many benefits.

2

Installing IKARUS anti.virus

Here you get the information on how to install and use the IKARUS anti.virus. Each setup step is documented by the fitting screenshot.

2.1 System requirements

For IKARUS anti.virus to run properly, your system must meet the following minimum requirements:

Hardware:

- Processor from 2 GHz (Intel/AMD)
- 2 GB RAM
- Min. 500 MB free storage space
- Display resolution min. 1024 x 575

Operating Systems:

- Windows 7 and higher (32/64 Bit)
- Windows Server 2008 R2 and higher (32/64 Bit)
- Windows Embedded Versions (depending on the configuration)
- Microsoft Outlook 2007 and higher

NOTE: Before installing IKARUS anti.virus, please uninstall other antivirus programs on your computer and then reboot it.

Close all other programs before installing IKARUS anti.virus.

A quick system scan is performed once IKARUS anti.virus have been installed. This will take about 10 minutes.

Please do not cancel the system check after installing the software. This is done for the security of your computer.

2.2 Installing IKARUS anti.virus

We recommend closing all other programs before installing IKARUS anti.virus.

Double-click the "Setup-IKARUS antivirus.exe" file to start the program.

Here are screenshots for the individual installation steps:

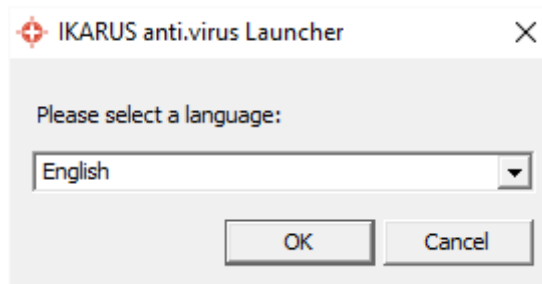


Figure 1: Installation step 1
Select a language

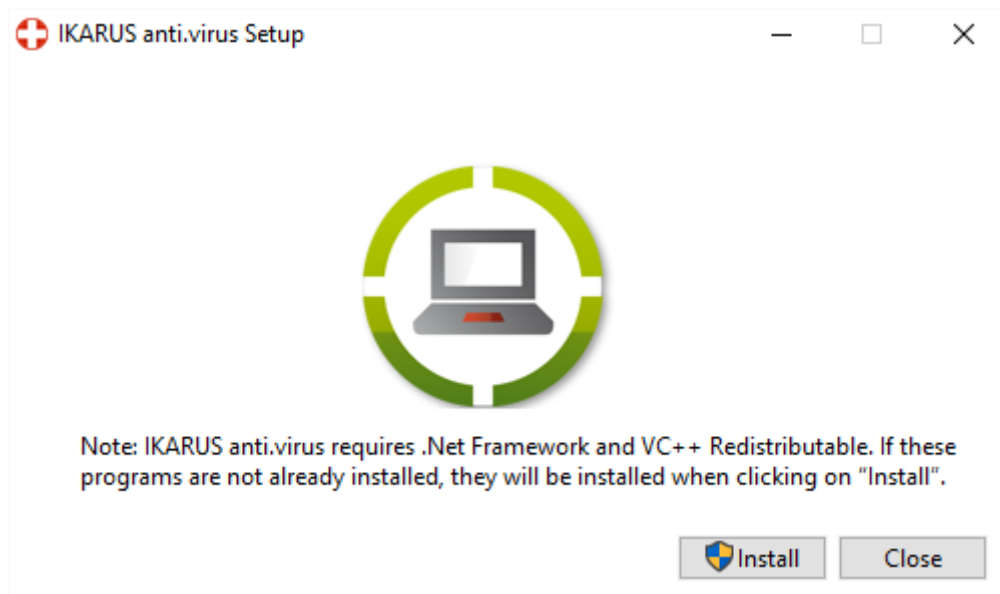


Figure 2: Installation step 2

To start the installation, your PC requires the Microsoft program .NET Framework. If you don't have it, the installation will be done automatically. An existing Internet connection is required.

IKARUS anti.virus checks whether an older version of IKARUS anti.virus is installed.

If this is the case, the older IKARUS anti.virus version must be uninstalled manually. You will probably be asked to restart your computer after uninstalling. Please restart the system, and the installation of IKARUS anti.virus can be started immediately.

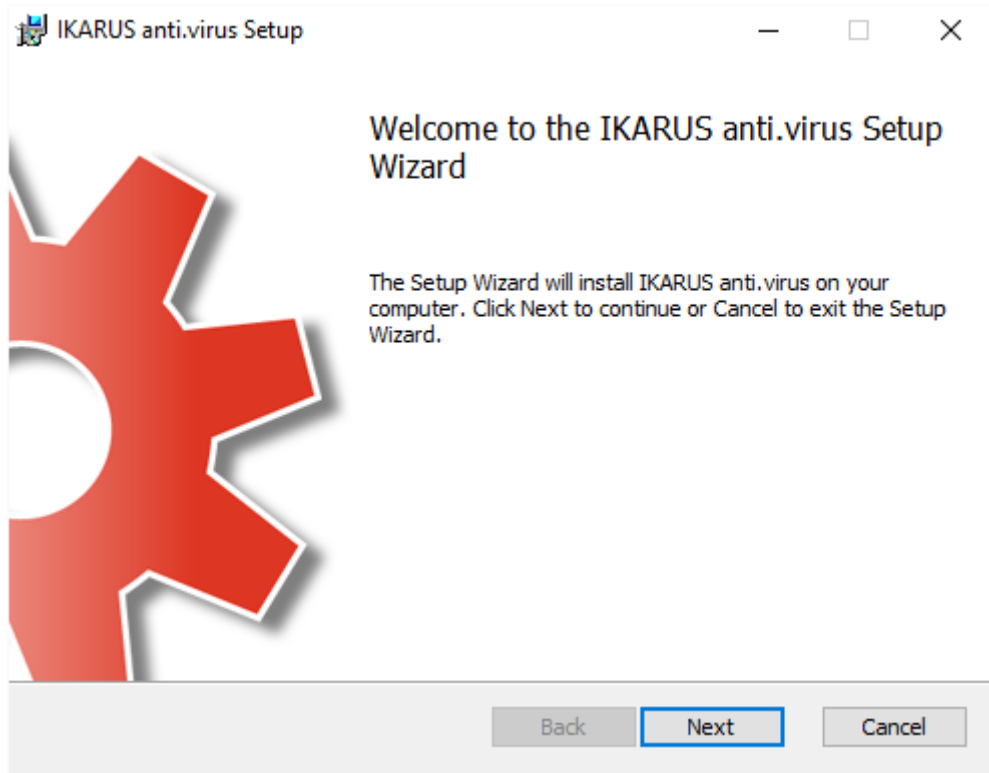


Figure 3: Installation step 3

Follow the installation wizard's instructions to install IKARUS anti.virus.

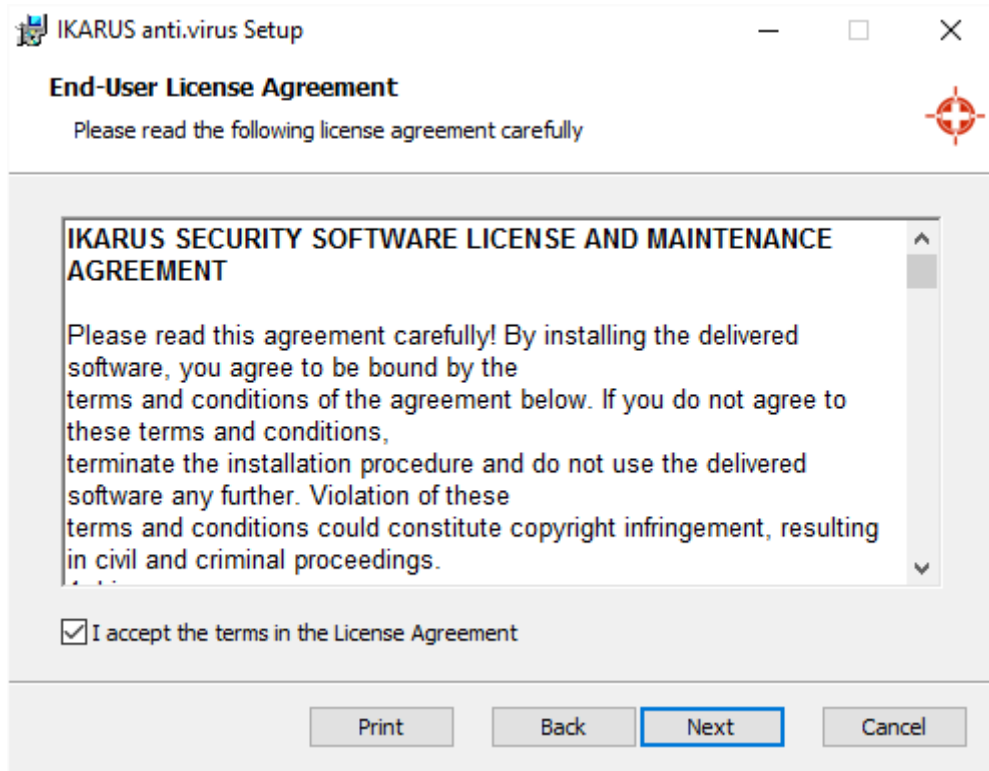


Figure 4: Installation step 4

Please accept the IKARUS license terms to proceed with the installation.

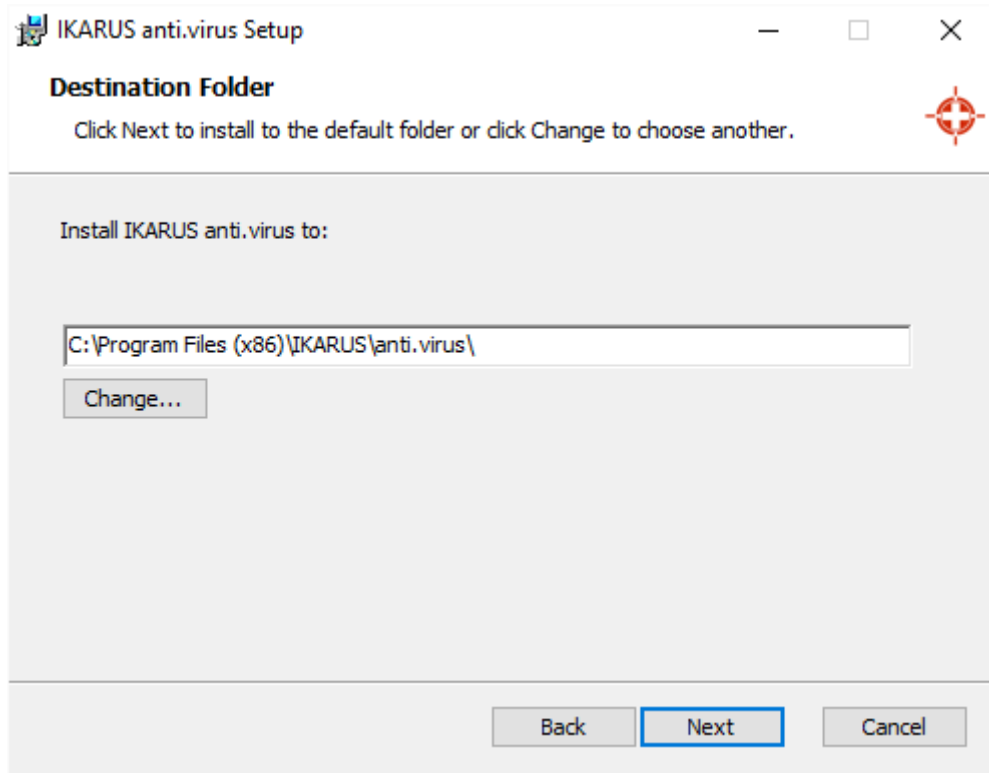


Figure 5: Installation step 5

Select the target directory for the installation of IKARUS anti.virus. We recommend keeping the suggested default folder.

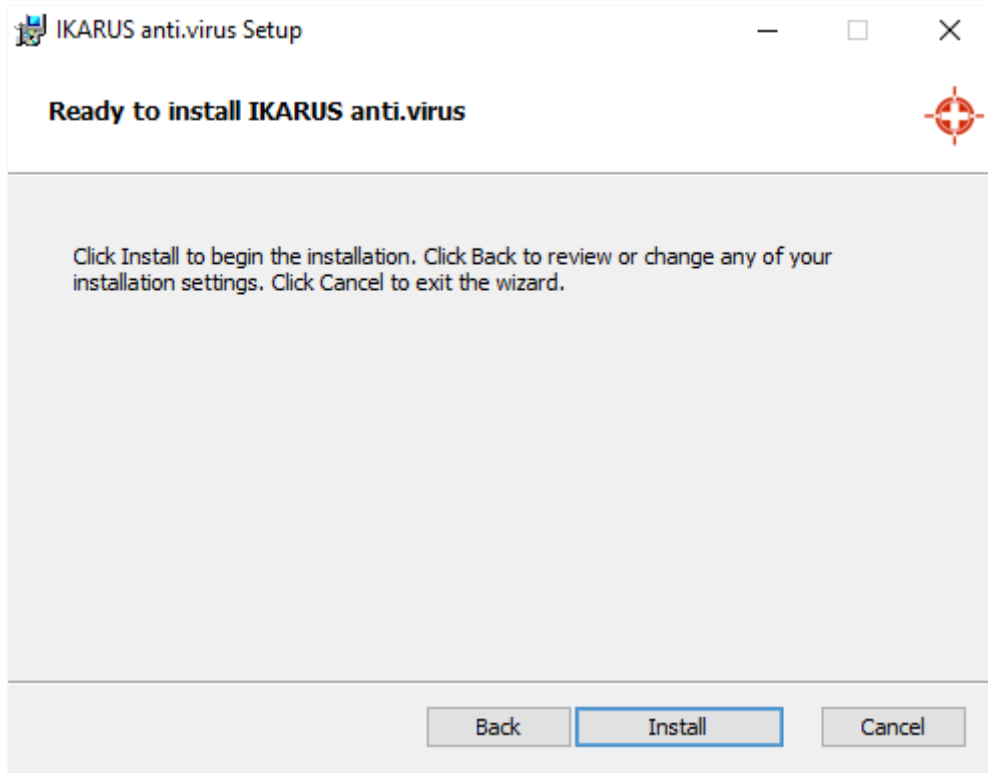


Figure 6: Installation step 6

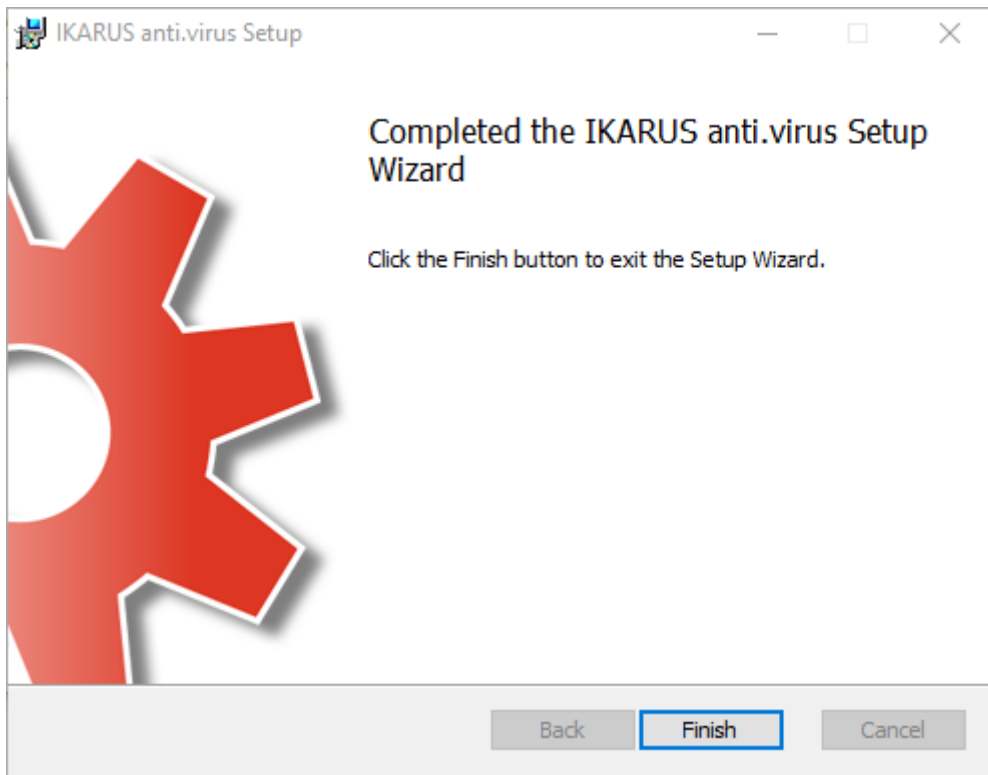


Figure 7: Installation step 7

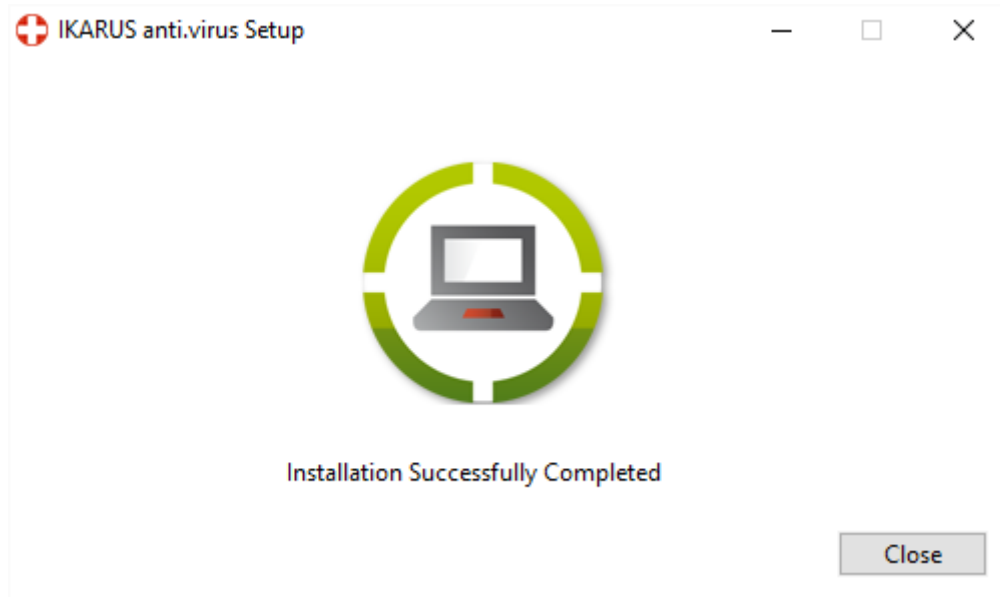


Figure 8: Installation step 8

The installation of IKARUS anti.virus is now complete. We recommend carrying out the quick system check in all cases!

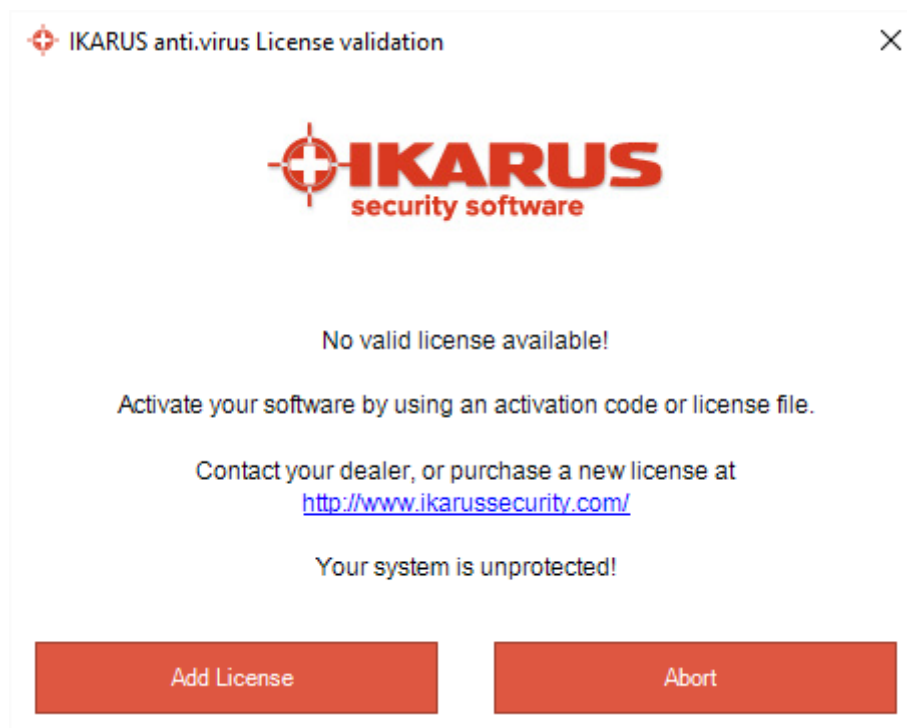


Figure 9

Please enable IKARUS anti.virus using the activation code or license file.

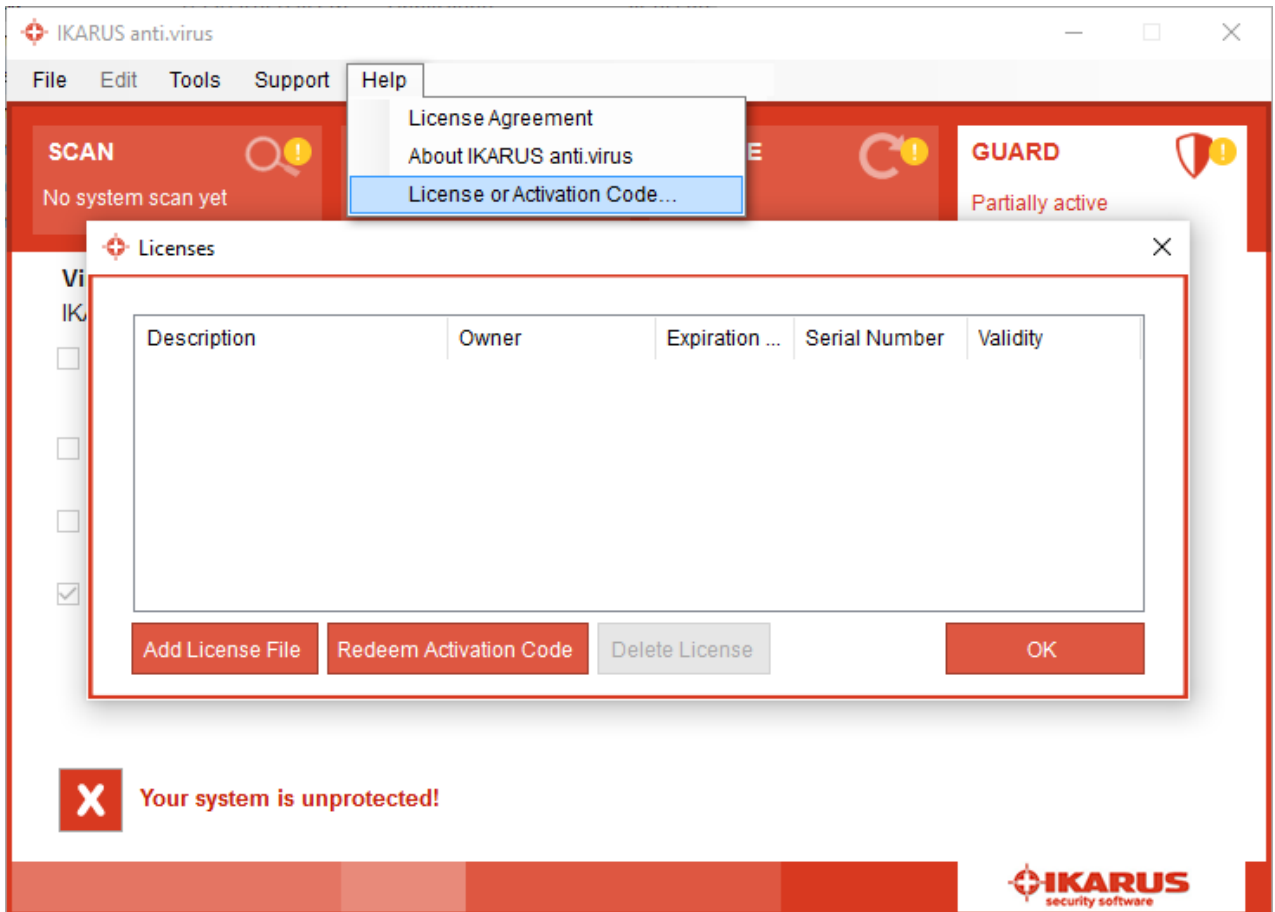


Figure 10

In the "Help" menu item, select "License file or Activation code "

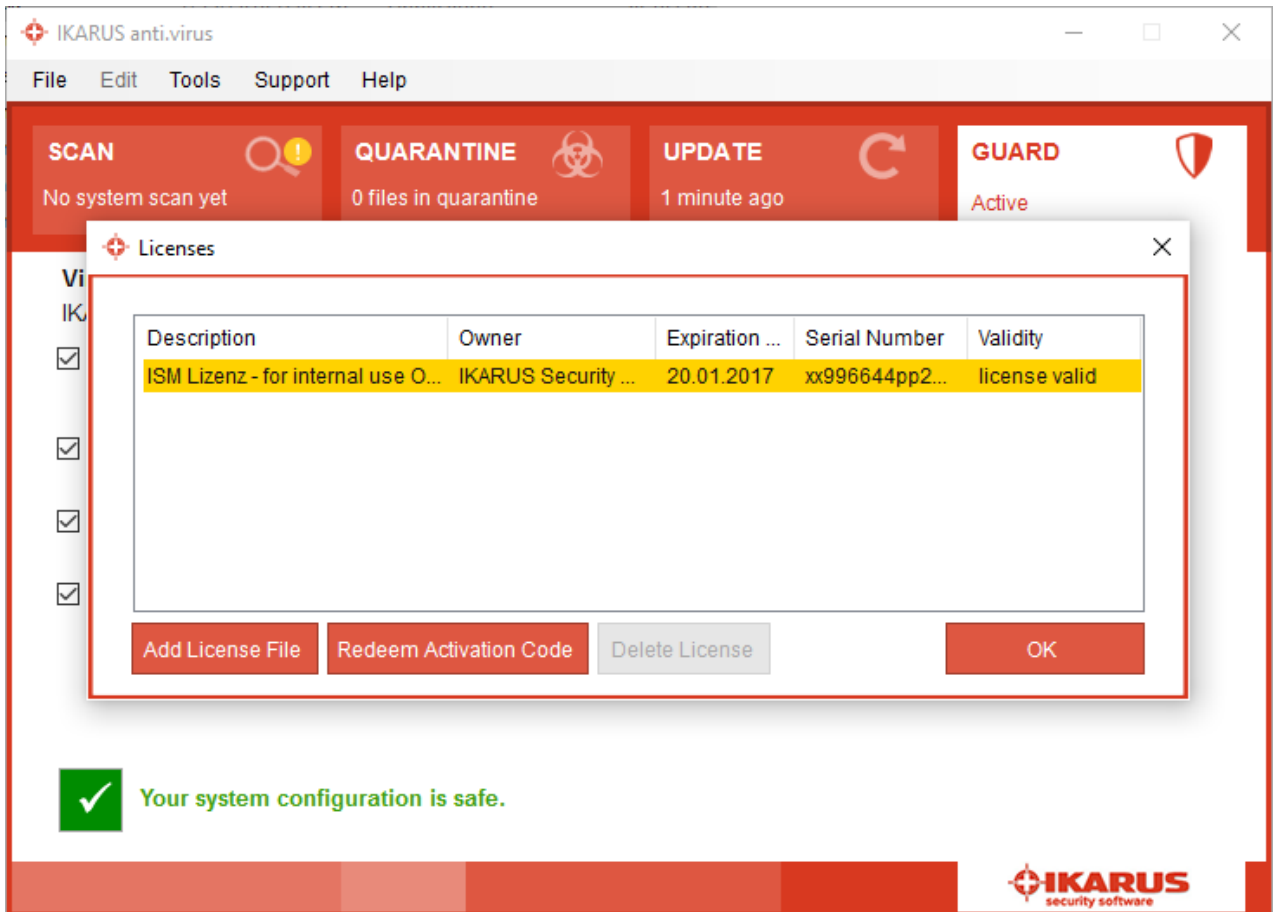


Figure 11
72/5000

Redeem the activation code or install the license file.

2.3 Unattended command line installation

With the unattended installation of the command line (hereinafter referred to as "silent installation") there are further possibilities for configuring IKARUS anti.virus.

IMPORTANT: This kind of installation is possible only with the MSI installers of the IKARUS anti.virus software and is intended exclusively for advanced users and system administrators. Downloads can be found at:

<https://www.ikarussecurity.com/at/downloads/produkte/download-ikarus-antivirus/>

In order to perform a silent installation of IKARUS anti.virus, a CMD window opened with administrative privileges is needed.

The correct syntax for the silent installation is:

```
msiexec /q /l* SetupLog.txt /i SetupProject.msi PROPERTY=VALUE
```

The parameter `/l* SetupLog.txt` is for the log file of the setup and can be omitted.

Instead of `SetupProject.msi` also an absolute path can be provided (e.g. `C:\setup\setup.msi`). If no absolute path is provided, the current folder in the CMD window must be the one containing the setup file. The syntax of `PROPERTY=VALUE` is very important. `PROPERTY` must be written in capital letters. Furthermore no whitespaces are allowed (e.g. `PROPERTY=VALUE`). The order of the properties is not important.

An example for a valid and correct syntax is:

```
msiexec.exe /q /l* setuplog.txt /i SetupProject.msi  
ACCEPTLICENSEAGREEMENT="yes"USEPROXY="yes" PROXY="127.0.0.1:8080"
```

The following properties are currently supported for the silent installation.
(Default values, if property is not set, are written in bold letters).

Mandatory:

The only mandatory property for the silent installation is accepting the license agreements.

`ACCEPTLICENSEAGREEMENT (yes)` - Has to be accepted.

Anti.virus-Settings:

Proxy:

`USEPROXY (yes/no)` - Uses the defined proxy server

`PROXY (Host:Port)` - Defined proxy server

Dependencies:

- `Port= 1 ... 65535`
- `USEPROXY=yes -> PROXY must be set`
- `PROXY is set, USEPROXY not set -> USEPROXY=yes`

Protection:

- WSYSTEM (**yes/no**) - Enable system protection
- WEMAIL (**yes/no**) - Enable mail protection
- WSPAM (**yes/no**) - Enable anti-spam protection
- UPDATE (**yes/no**) - Enable automatic updates

Scan scheduling:

Remark: The default values in bold are only valid if at least one of the following properties is provided. If none are provided, no scheduled scan profile will be created.

- AUTOSCAN (**yes/no**) - Enable automatic scheduled scan
- SCANTYPE (**quick/standard/full**) - Scan type for the automatic scan
- DAILY (**yes**) - Interval for automatic scan
- WEEKLY (**0-6**) - Interval for automatic scan (0=Sunday), 5default
- MONTHLY (**1-31**) - Interval for automatic scan
- SCANHOUR (**xx:xx**) - Time for automatic scan (17:00default)

Dependencies:

- Choose one of the scan intervals (**DAILY, WEEKLY, MONTHLY**)
- **DAILY** accepts only "yes", other parameters lead to an error message
- If one of the properties is provided, the other will be assigned default values. E.g.:
 - ➔ SCANTYPE="standard"
 - AUTOSCAN="yes"
 - WEEKLY="5"
 - SCANHOUR="17:00"

Existing files:

The following existing files can be provided for the silent installation. If not provided, the setup will use the default ones.

The files can be provided independently from each other.

CONFIG (path)	Path to an existing guardx.conf. E.g.: CONFIG="C:\mydir" If provided, the properties of "Anti.virus-Settings" will be ignored.
VDB (path)	Path to an existing t3sig.vdb. E.g.: VDB="C:\mydir"
T3 (path)	Path to an existing t3.dll. E.g.: T3="C:\mydir"
T3_W64 (path)	Path to an existing t3_w64.dll. E.g.: T3_W64="C:\mydir"
SDB (path)	Path to an existing antispam.sdb. E.g.: SDB="C:\mydir"

Installation behaviour:

The following properties can change the behaviour during and after the installation.

INSTALLFOLDER (path)	Install path for the installation. If not provided, default one will be used. Automatically ends with anti.virus. E.g.: "C:\myfolder" will be used as "C:\myfolder\anti.virus" for installation.
UPDATENOW (yes/no)	Perform an update after the setup is finished.
LICENSE (path)	Absolute path to the license file. E.g.: LICENSE="C:\mydir\license.ikkey"
CLOSEOUTLOOK (yes/no)	Determines whether Outlook should be closed automatically if opened during the installation. Remark: There will be no user interaction.

Error messages:

If the installation fails, the cause for it can be determined from the created log file.

To determine whether the installation failed because of a wrong property syntax, you should look in the log file for "Error 0x80004005".

E.g.: If the user agreements have not been accepted, you would find the following line in the log files:

"Error 0x80004005: In order to install IKARUS anti.virus you must accept the license agreement. Please provide the property `ACCEPTLICENSEAGREEMENT="yes"` in order to install the product."

Additional information regarding the silent installation:

[https://msdn.microsoft.com/en-us/library/aa367988\(VS.85\).aspx](https://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx)

2.4 Uninstalling IKARUS anti.virus

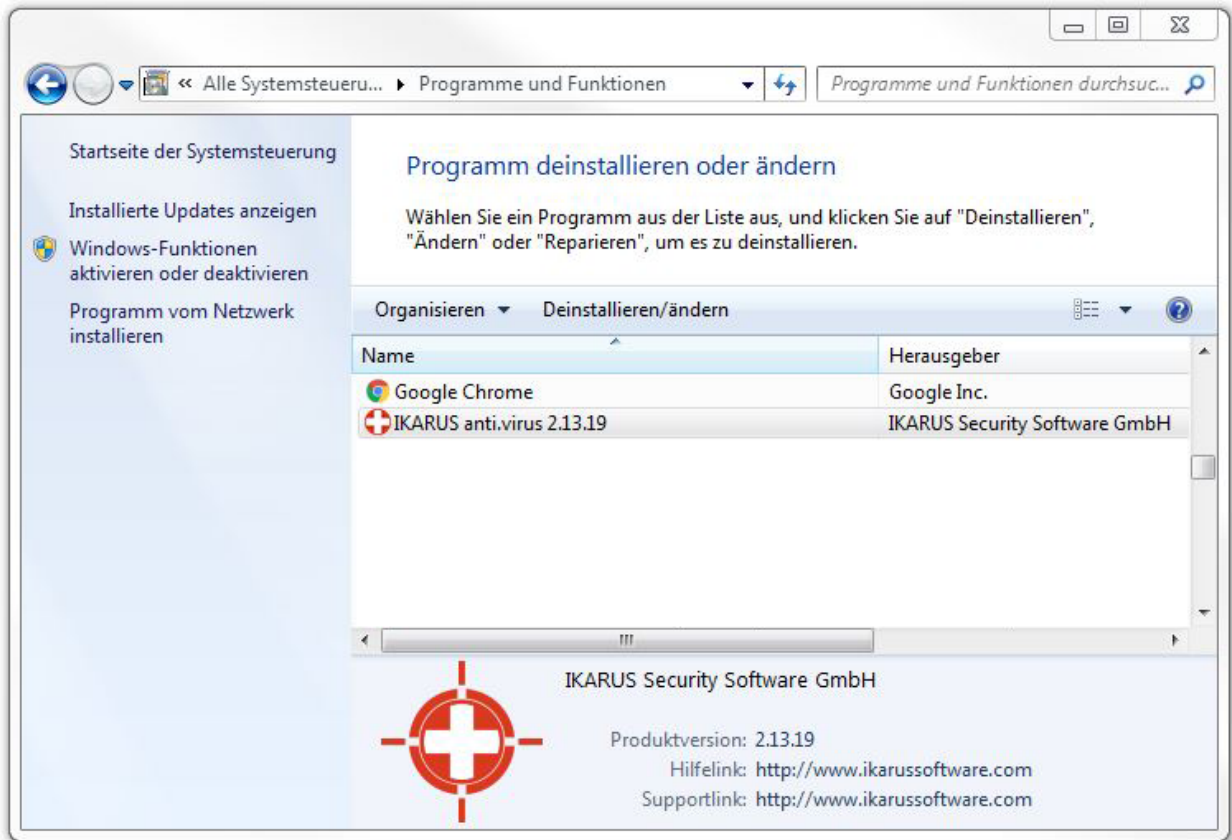


Figure 12: Start Uninstalling IKARUS

To uninstall IKARUS anti.virus, go to the Control Panel and open "Programs and features". Search IKARUS anti.virus

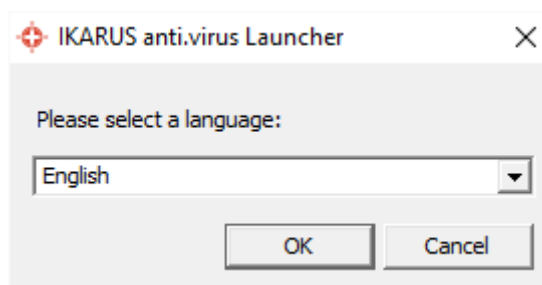


Figure 13: Uninstalling step 2

Select a language

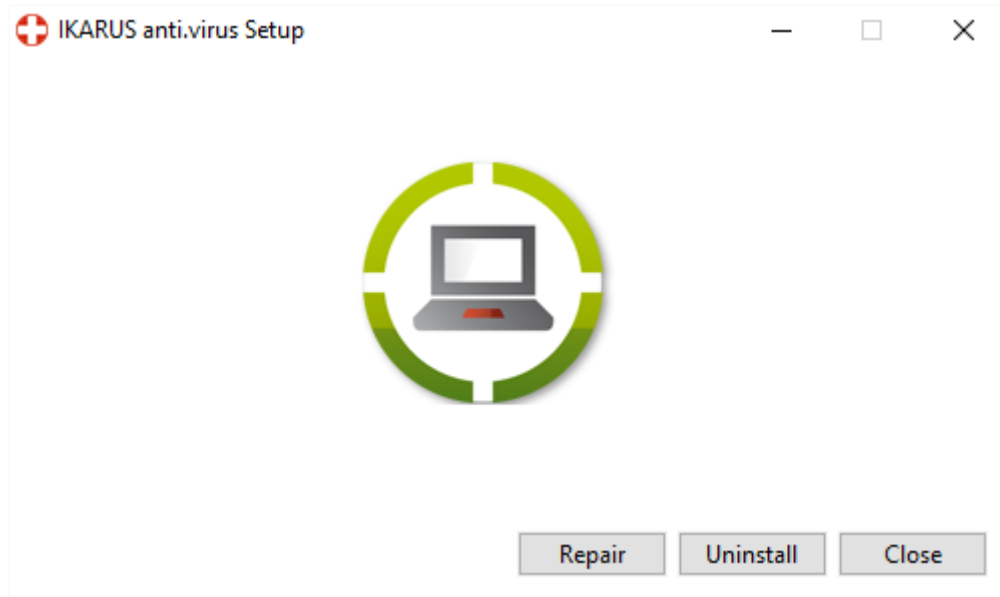


Figure 14: Uninstalling step 3
Choose the Option „Uninstall“.

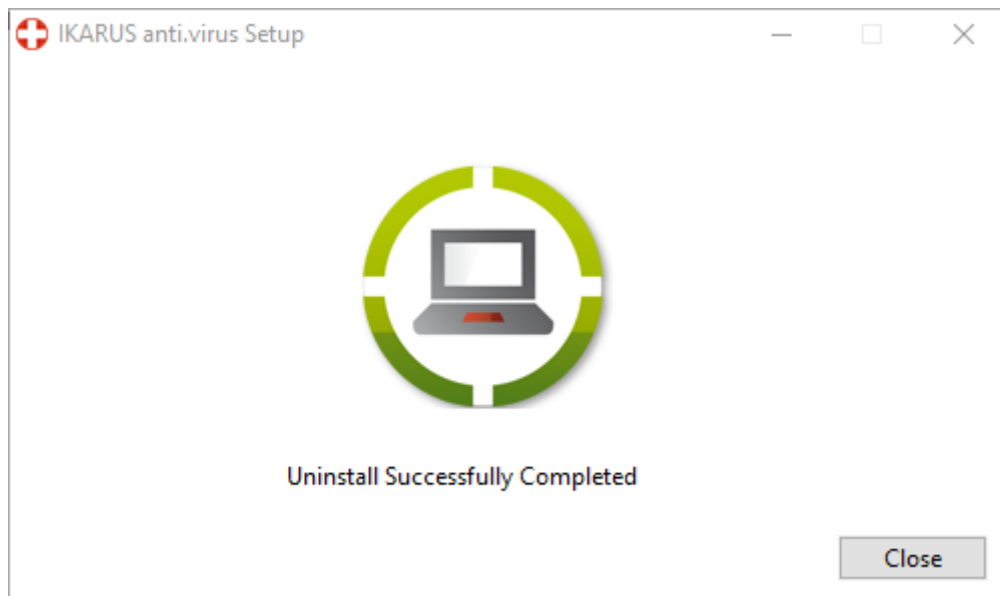


Figure 15: Uninstalling step 4
After the procedure has finished, an appropriate note will appear. At the same time, you will be asked to restart your computer. It is recommended to proceed the restart as soon as possible.









Features of IKARUS anti.virus

Main features on IKARUS anti.virus:

- Powered by the IKARUS scan.engine for solid detection
- Incremental updates (every 4 hours) incl. Program updates
- Comprehensive virus scanning
- Microsoft SharePoint monitoring
- E-Mail monitoring (Outlook) with Anti-SPAM feature
- Available languages: German, English, Russian, Italian, Croatian
- Compatible with IKARUS security.manager – the central management console for business networks
- Scheduled On-demand scanning profiles
- Fast On-Access Scan
- Submit suspicious files to the IKARUS lab for further analysis
- Quarantine feature with different clean up possibilities
- Enable “Guard” option for pro-active virus and SPAM protection
- Password protection for settings
- Resource saving operation
- Flexible licensing - 1/2/3/5 years

3.1 Symbols and screens

Now take the time to familiarize yourself with the symbols used in IKARUS anti.virus.

Symbol	Description
	You can find the standard symbol at the bottom right of your screen in the taskbar. *
	Double-click on the symbol and the configuration screen for IKARUS anti.virus opens automatically. When moving the cursor over the symbol, the pop-up shown below will appear for a few seconds on your screen. You can also open IKARUS anti.virus here too. Simply click the required function (Scan, Update or Guard). This provides you with all the information on whether IKARUS anti.virus is running properly, when the last update was performed, when the last scan took place and whether all components of the virus protection are activated. If all three fields are white, everything is working OK. *
	When this window appears, you can see which area is affected by the warning. In the example, one component of the guard is disabled, i.e. part of the scanning function is disabled. *
The appearance of the symbol in the taskbar may change and has different meanings accordingly.	
	The white cross set to a red background indicates that everything is OK, the virus protection is set to its highest level and the software is fully updated. IKARUS anti.virus is on and monitoring your PC.
	This symbol indicates that one of the three components (Scan, Update or Guard) is not set to the highest security level available in IKARUS anti.virus.
	When the symbol pulsates in size (like a heartbeat), this indicates that IKARUS anti.virus is currently being updated.
	A rotating symbol shows that a scan is currently being performed.
	If the symbol for IKARUS anti.virus appears like this, a virus has been found. In this case, follow the instructions under 4.4, What to do when a virus is found -

Overview IKARUS anti.virus symbols

Symbole, deren Beschreibung mit * markiert ist entfallen ab Windows 10

The four main features

4.1 Guard – Your personal minder

Guard is the monitoring component in IKARUS anti.virus. To achieve the highest level of protection against malicious software, tick all of the available checkboxes. If required, you can reduce the level of protection by unchecking one or more checkboxes.

ATTENTION: IKARUS anti.virus only offers full virus protection when all options are selected and enabled!

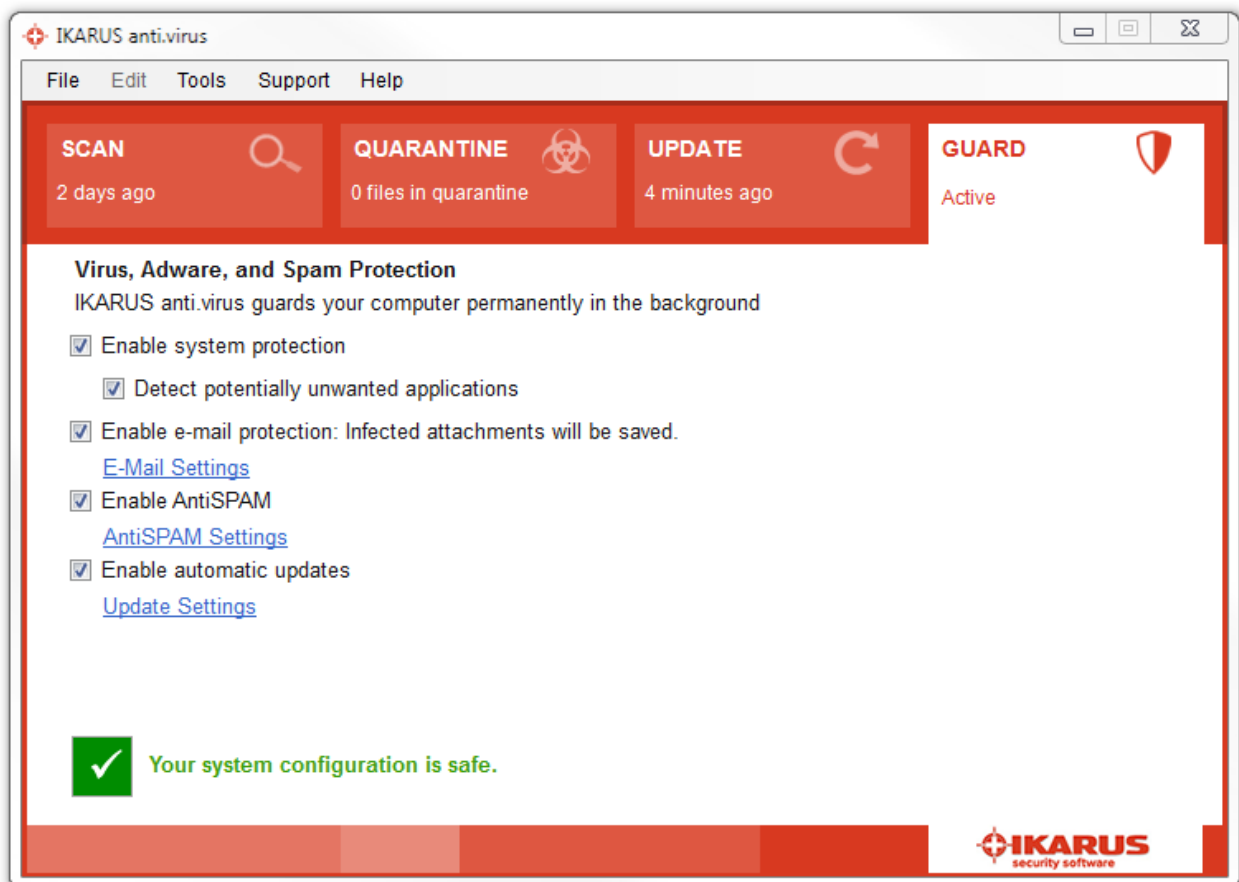


Figure 16: Guard

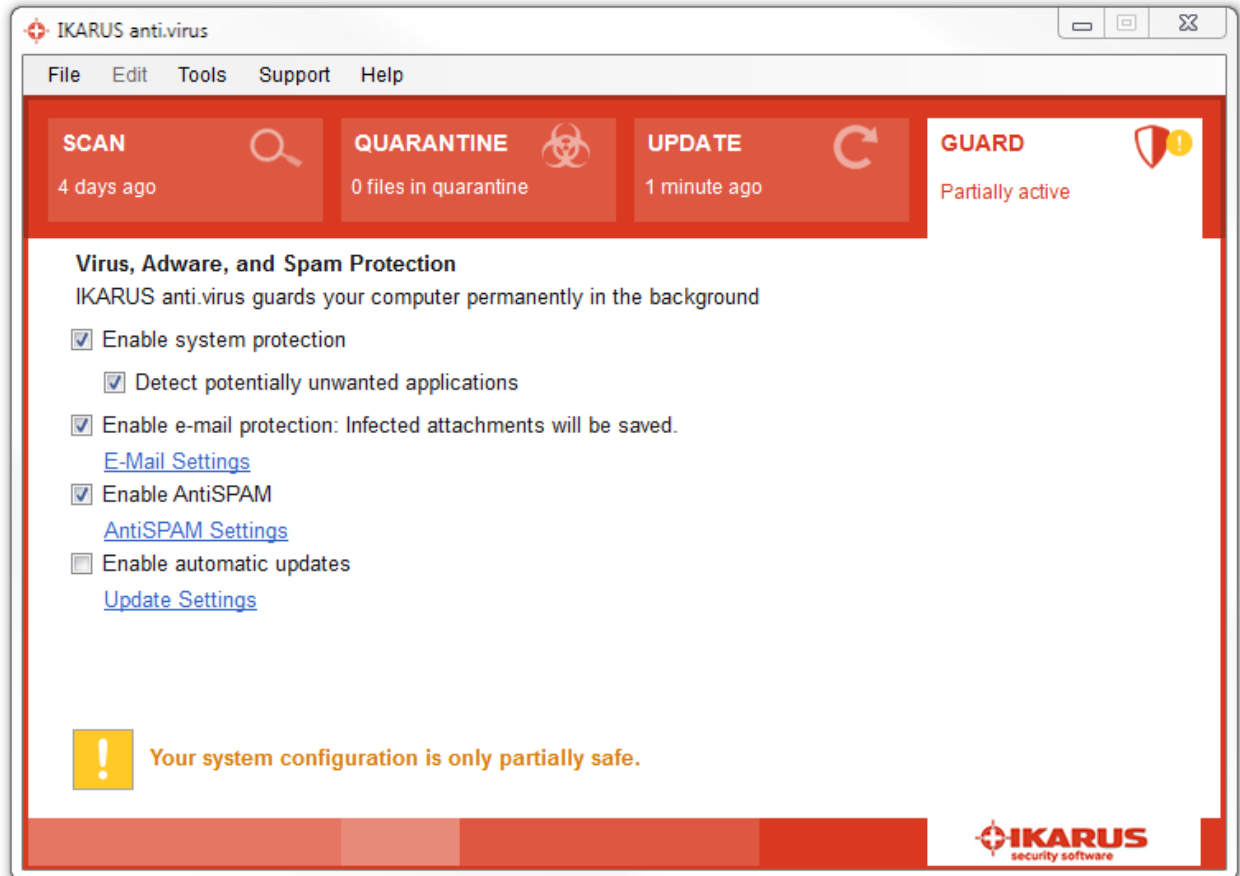


Figure 17: Guard - partly activated

You will also see a yellow symbol and the message “Your system is partly safe configured.” appears. IKARUS anti.virus is then no longer able to provide you full protection.

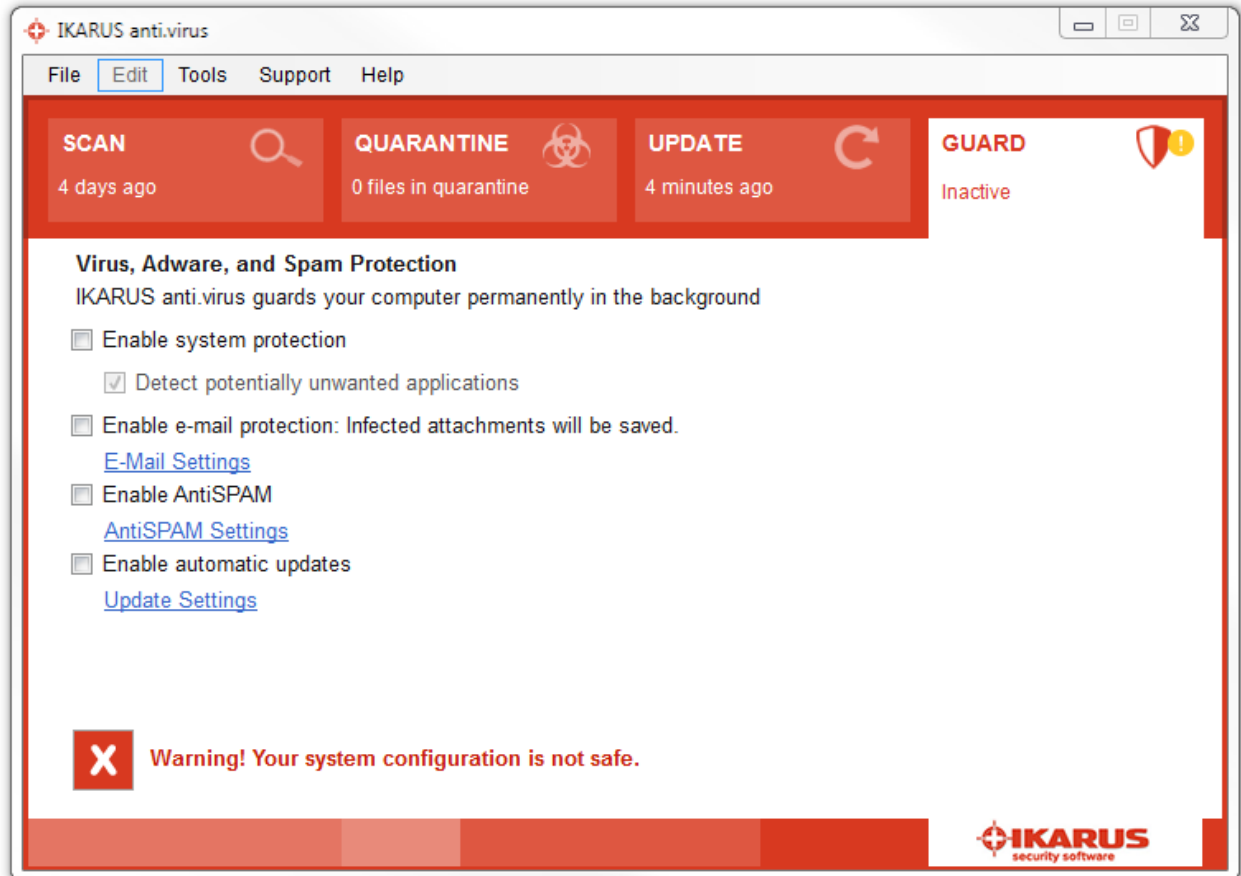


Figure 18: Guard not activated

If the Symbol turns to red your system protection is turned off and the status message is “Warning! Your system configuration is not safe.”.

If one or more areas are excluded from the scan, the appearance of the IKARUS anti.virus symbol in the taskbar will change to indicate this.

4.2 Updating IKARUS anti.virus

Your software can only provide reliable protection against viruses, worms, spyware and Trojan horses if it is up-to-date.

IKARUS anti.virus therefore contains an automatic update feature. Every 20 minutes, it checks for new updates. These are then automatically installed. The program connects to the internet if no connection is currently available.

If you do not use your computer for a long period of time, IKARUS anti.virus automatically download the latest updates when you start your PC.

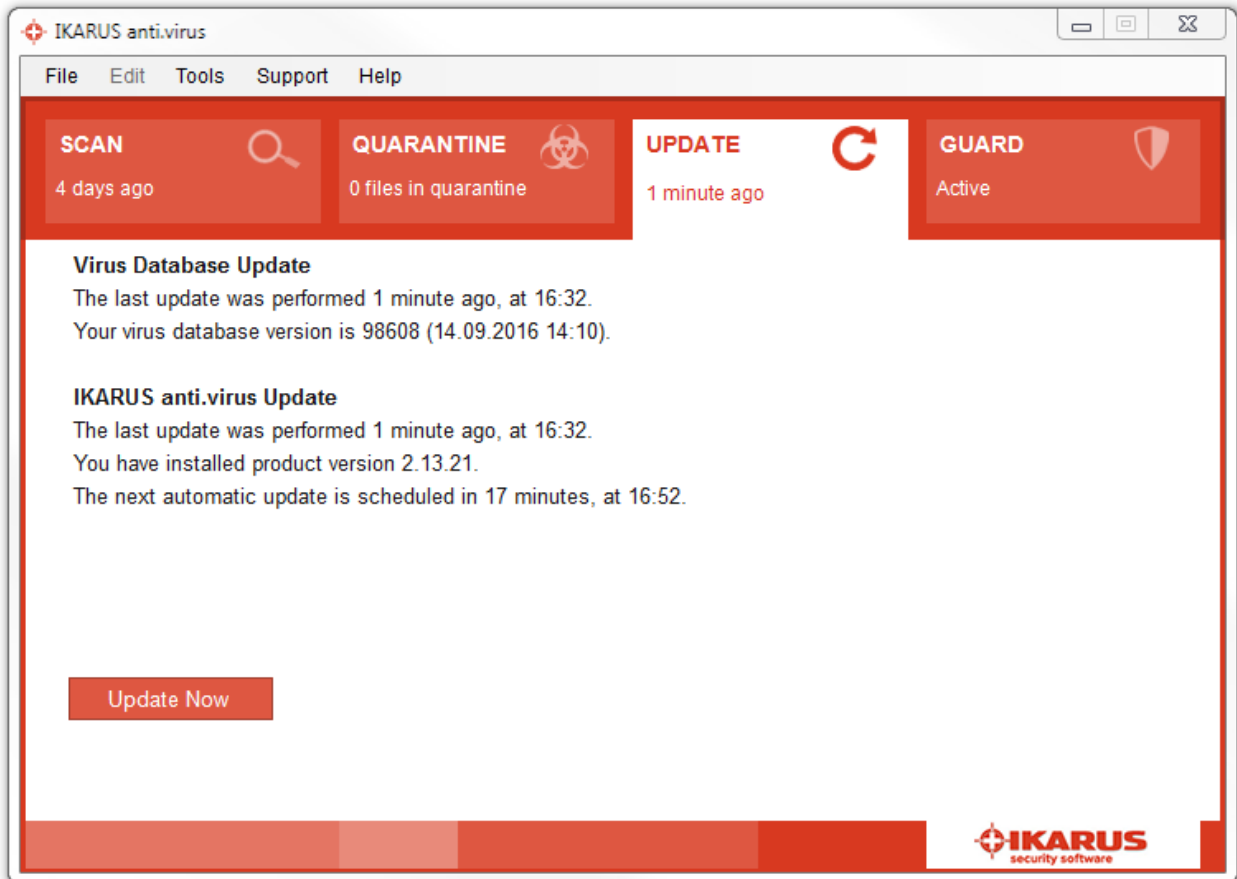


Figure 19: Update

There are two types of updates in IKARUS anti.virus: virus database updates and updates to IKARUS anti.virus itself.

Virus databases (or VDB for short) updates ensure that new malicious software is detected. The updates to IKARUS anti.virus are program updates that add new features or functions. Press 'Update now' to check for new updates.

If the latest updates are already installed, 'All up to date' will appear.

4.3 Scan - The virus check from IKARUS anti.virus

You can configure the scan to be performed automatically or start the scan manually in IKARUS anti.virus. You can manage and add as many scans as required.

Preset scans:

- **Fast System Scan:** Here, the Windows installation directory is scanned. Most malicious programs such as viruses and Trojan horses are located in this directory, and can be quickly and readily detected.
- **System Partition:** With this option, IKARUS anti.virus scans the drive where your operating system is installed. All archives, directories, folders and files on this drive are scanned by IKARUS anti.virus.
- **Entire Computer:** IKARUS anti.virus scans all drives on your computer.
- **Removable Media:** All external drives such as USB sticks and CD ROM drives are scanned.

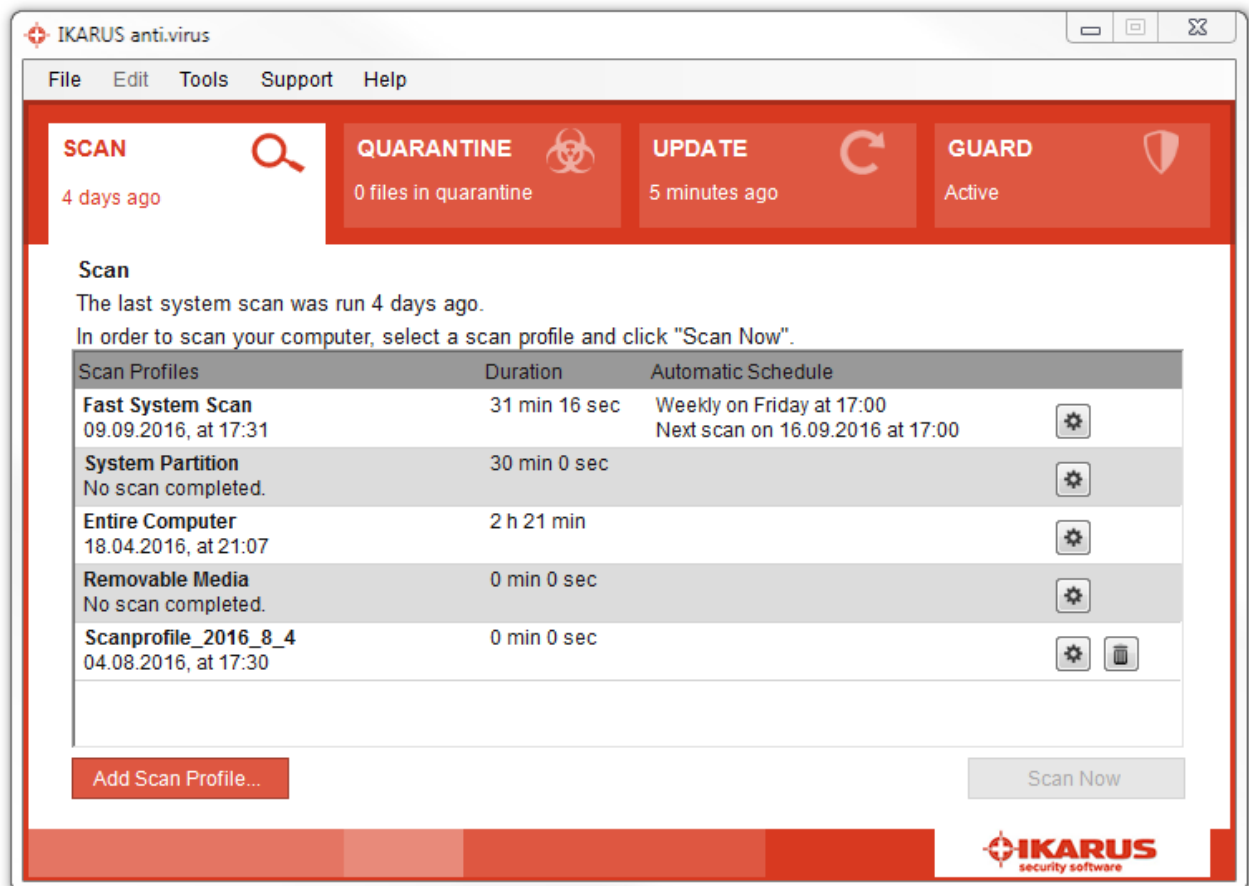


Figure 20: Scan

Individual scans are configured by pressing "Add Scan Profile".

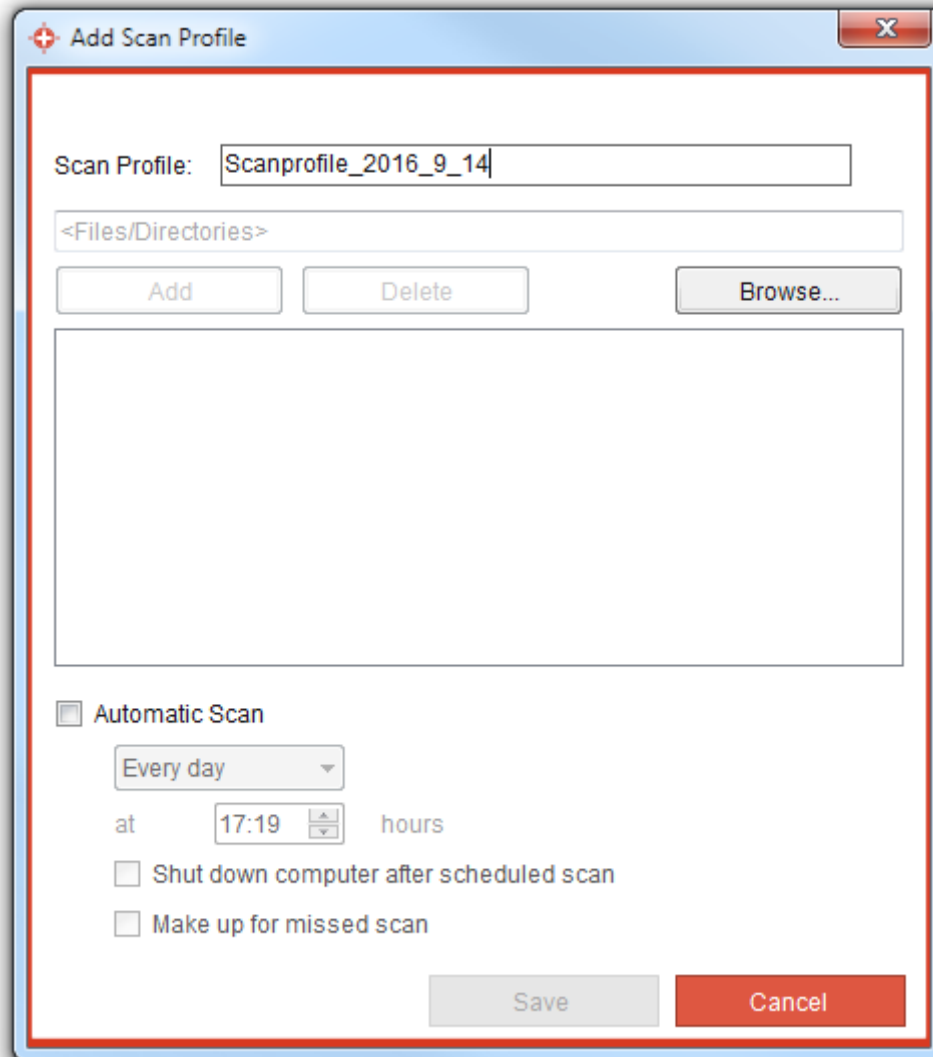


Figure 21: Add Scan Profile

You can enter any name for the scan. Press “Browse” to select the folder, files etc. that you wish to scan. You may also set the program to perform an automatic scan where required.

The automatic scan can be scheduled for any time (e.g. every Friday at 12pm) and only scans the areas selected by the user.

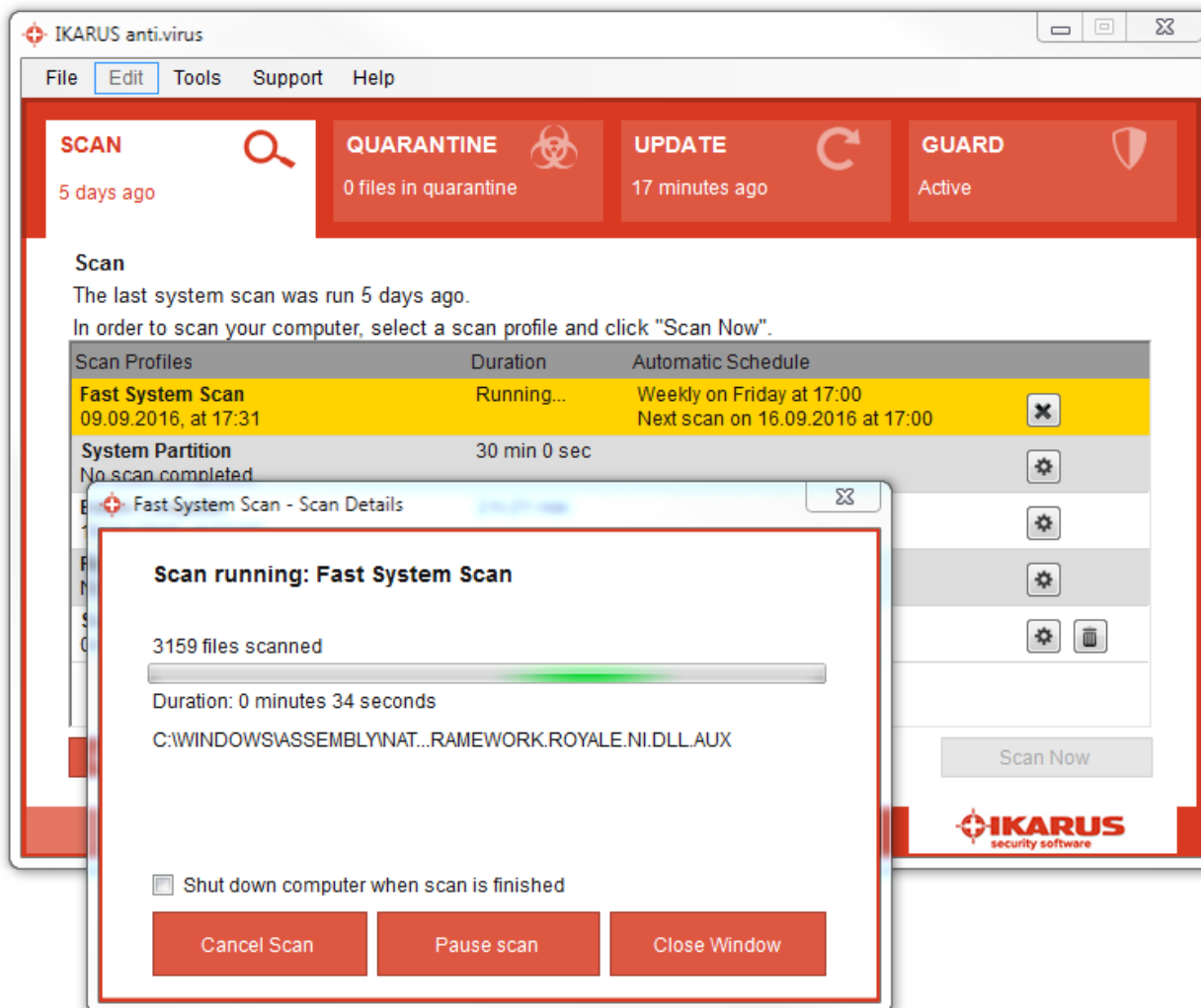


Figure 22: Scan running

To start a scan, press 'Scan Now'.

You can stop or cancel a scan at any time.

The status bar and remaining time indicator provide information on how the scan is progressing.

If the scan is completed and no viruses were detected, you can press 'close window' to return to the main window.

If a virus was detected, please click to Section '4.4 Quarantine - what to do when a virus is found' - and read the information provided there.

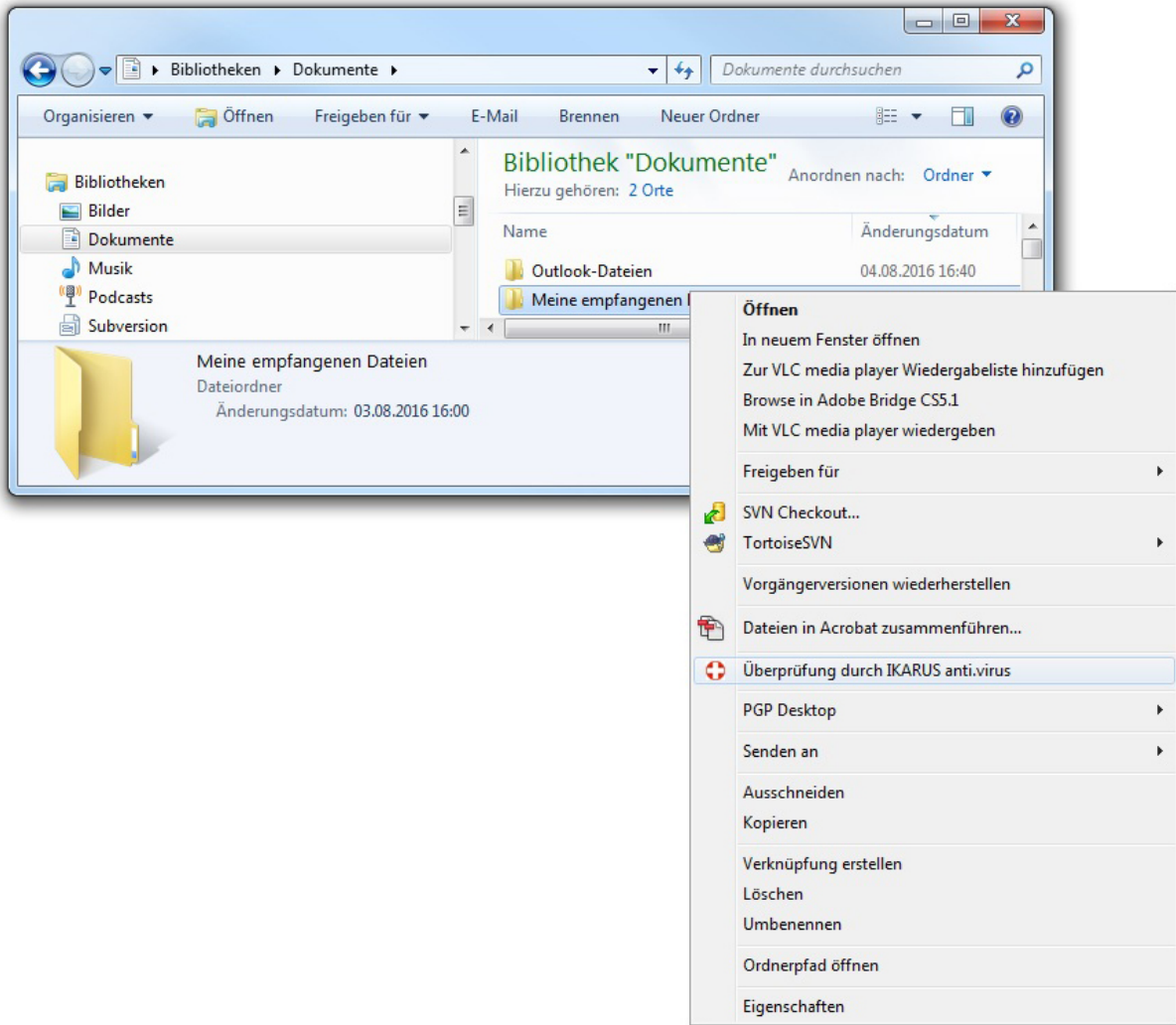


Figure 23: Start IKARUS anti.virus Scan via Explorer

Another way to start a scan is to right-click on a drive, file or folder in Windows Explorer and select “IKARUS anti.virus scan”.

4.3.1 Scan-Settings

Click scan settings in the scan window or in the menu to go to the exclusions tab.

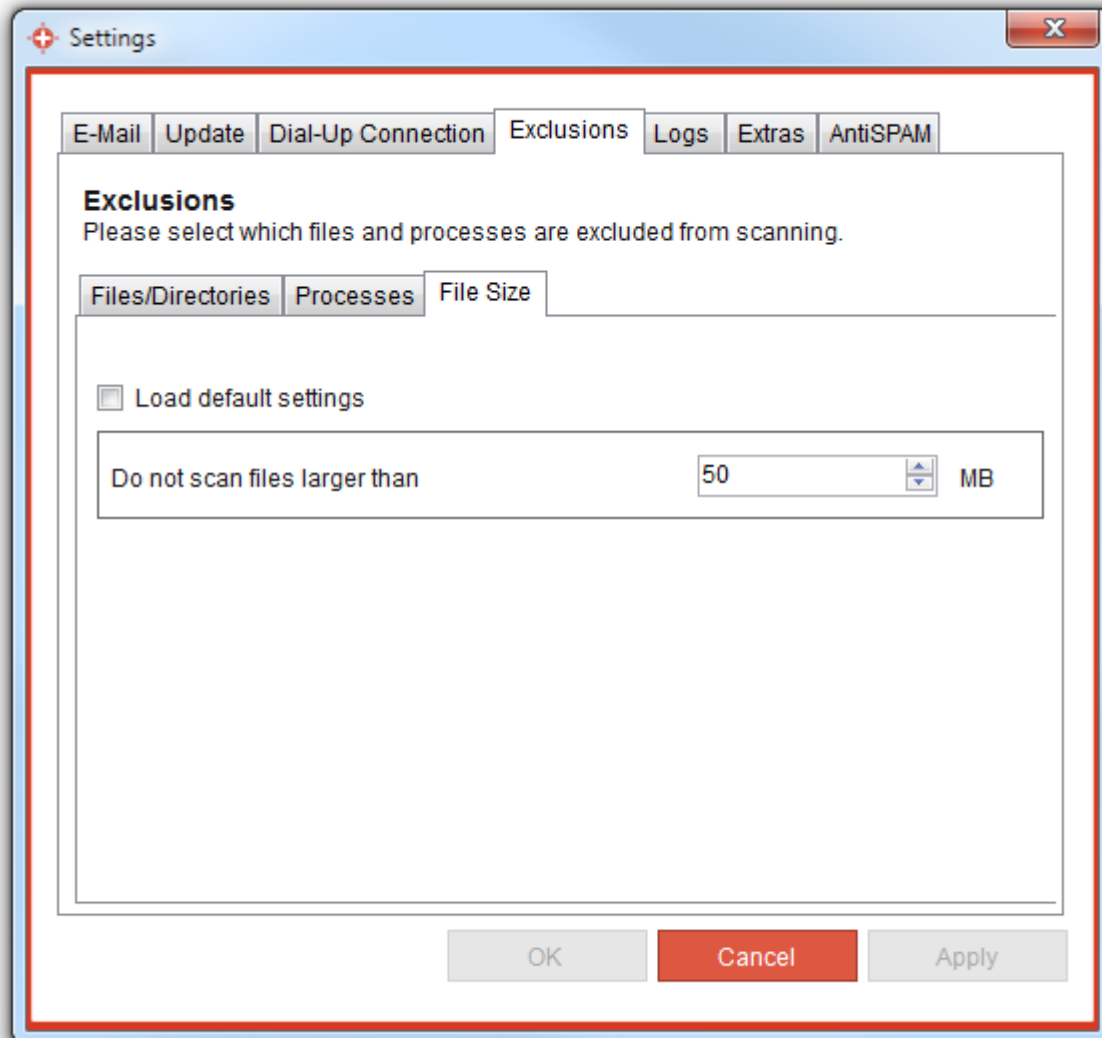


Figure 24: Exclusions




In this tab, you can specify which files and processes are not scanned by IKARUS anti.virus. It is also possible to limit the scan to files of a certain size or smaller.

4.4 Quarantine - what to do when a virus is found?

Read here how to manage infected files in the quarantine of IKARUS anti.virus and what possibilities you have to remove a virus from your system.

4.4.1 Virus detection warning

When a virus is detected, IKARUS anti.virus provides the following warnings:

Warnings	
 <p>IKARUS anti.virus - virus found</p> <p>IKARUS anti.virus found a virus(EICAR-ANTIVIRUS-TESTFILE) in the attachment eicar.apk, the attachment was removed from the e-mail.The file was saved as ..\quarantine\files\4.vir.</p> <p>OK</p>	 <p>ENG 11:00 US 03/13/2014</p>
<p>When an infected e-mail arrives in your inbox, IKARUS anti.virus detects the malicious program. A window will now appear on your screen, where IKARUS anti.virus notifies you that a virus was found and it was moved to the quarantine directory.</p>	<p>The yellow IKARUS anti.virus icon is shown in the taskbar.</p>
<p>IKARUS anti.virus has scanned this mail for viruses, trojans and other malware. The e-mail was INFECTED.</p> <p>eicar.apk -> infected (EICAR-ANTIVIRUS-TESTFILE) attachment removed. The file(..\quarantine\files\4.vir) was saved.</p>	 <p>IKARUS anti.virus</p> <p>SCAN UPDATE GUARD</p> <p>Virus 8 minutes ago Active</p> <p>Your system may be infected! Virus found!</p>
<p>In the infected email, the following text is shown when a virus is detected.</p>	<p>The information panel with the red bar shows a warning message in the scan window.</p>

Warnings when a virus is found

4.4.2 Virus detected during scan

When a scan is automatically or manually started and a virus is detected, this is indicated as follows:.

- As described above, the yellow IKARUS anti.virus icon appears in the Windows taskbar and a warning is shown in the information panel.
- In the 'Scan Details' windows, you will see the message 'infected files found' during and after the virus scan.
- The Quarantine tab opens automatically when the scan is completed.

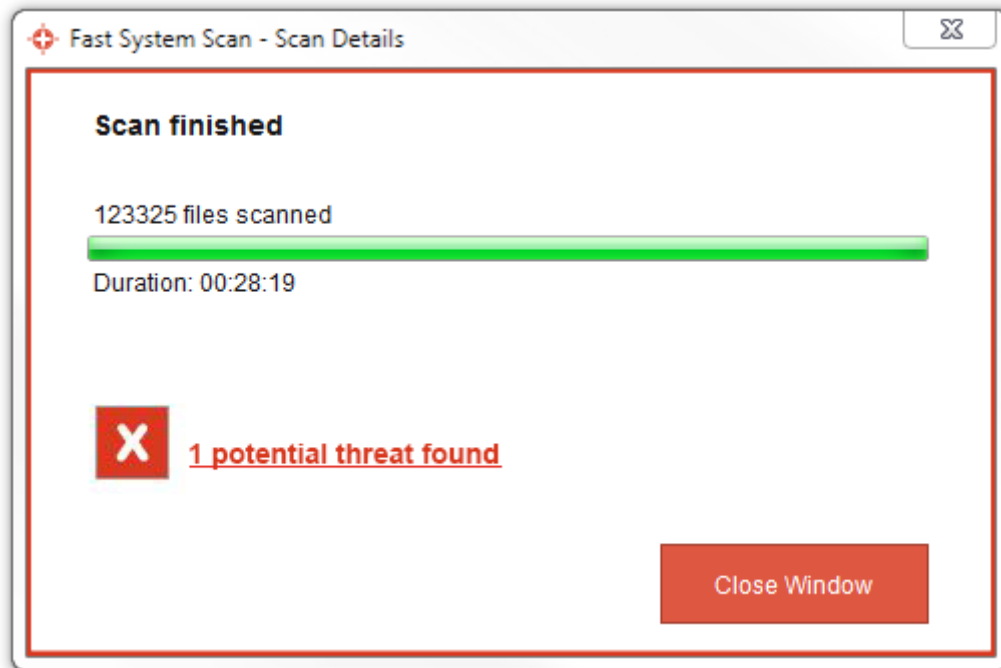


Figure 25: Scan finished – 1 potential threat found

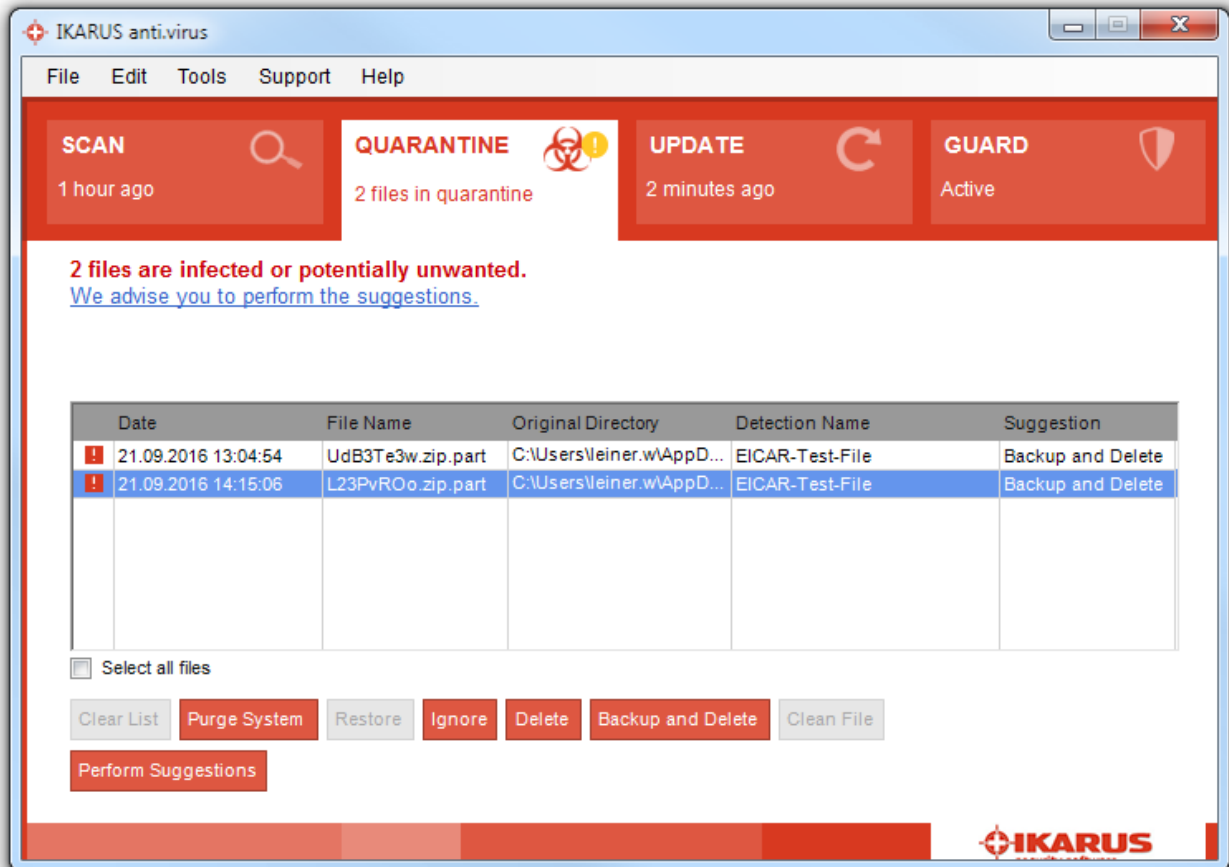


Figure 26: Quarantine – Virus found

4.4.3 Quarantine

Any viruses detected by IKARUS anti.virus are automatically moved to quarantine. Once the virus is 'quarantined', it no longer represents a threat to your system.

Once the infected file is moved to quarantine, all access to it is denied. From this point on, the file does not represent a threat to your computer.

The Quarantine tab contains all the information you require on the virus and about ways to remove it. You can also start any of the functions in the Quarantine tab from the toolbar or in the menu under "Edit".

The Quarantine tab in IKARUS anti.virus offers numerous options for configuring what actions to take when a virus or infected file is detected.

IKARUS anti.virus also suggests the best action to take in each case.

Press 'Suggestion' to carry out the actions proposed by the program.

You can also select a different option if you do not wish to follow the recommendation provided by IKARUS anti.virus:

- **Purge System:** Alle infizierten Dateien werden in die Quarantäne verschoben.
- **Ignorieren:** Die als infiziert erkannte Datei wird temporär freigegeben. Das bedeutet, dass diese Datei bis zum Neustart des Services (d.h. normalerweise bis zum Neustart des PCs) nicht mehr gemeldet wird. Dies ermöglicht Ihnen wieder den Zugriff auf diese Datei. Nach einem Neustart Ihres PCs finden Sie die Datei jedoch wieder in der Quarantäne. Nach Betätigen des Buttons werden Sie außerdem gefragt, ob Sie die infizierte Datei an IKARUS zur Analyse schicken möchten (anonym oder mit E-Mail-Adresse zur Rückmeldung)
- **Löschen:** Die markierte Datei wird in die Quarantäne verschoben.
- **Sichern und löschen:** Die infizierte Datei wird in die Quarantäne verschoben. Gleichzeitig wird eine Sicherungskopie der Datei in Ihrem IKARUS anti.virus-Verzeichnis belassen. Der Eintrag in der Quarantäne wird danach hellgrau. Wenn gewünscht, können Sie die Datei durch Klick auf den Button „Zurück verschieben“ wiederherstellen.
- **Datei bereinigen:** Wenn möglich, wird nur das Virus selbst aus der infizierten Datei entfernt. Die Datei selbst bleibt dabei bestehen und wird nicht gelöscht. Dateien, die im Grunde nur aus einem Virus bestehen, werden zur Gänze gelöscht.
- **Liste löschen:** Entfernt die Einträge aus der Quarantäneliste. Mehr als 7 Tage alte Einträge werden automatisch aus der Liste entfernt.

In IKARUS anti.virus, you can check the quarantine list to see which viruses have already been detected, if any were deleted, or what actions were taken when they were detected.

Entries that appear in black indicate that a virus is in quarantine and no action has been taken. Now decide what action to take or follow the recommendations provided by IKARUS anti.virus.

Entries shown in grey indicate that a virus was deleted or saved to a back-up file. You can remove these entries from the list at any time by pressing 'Clear list'.

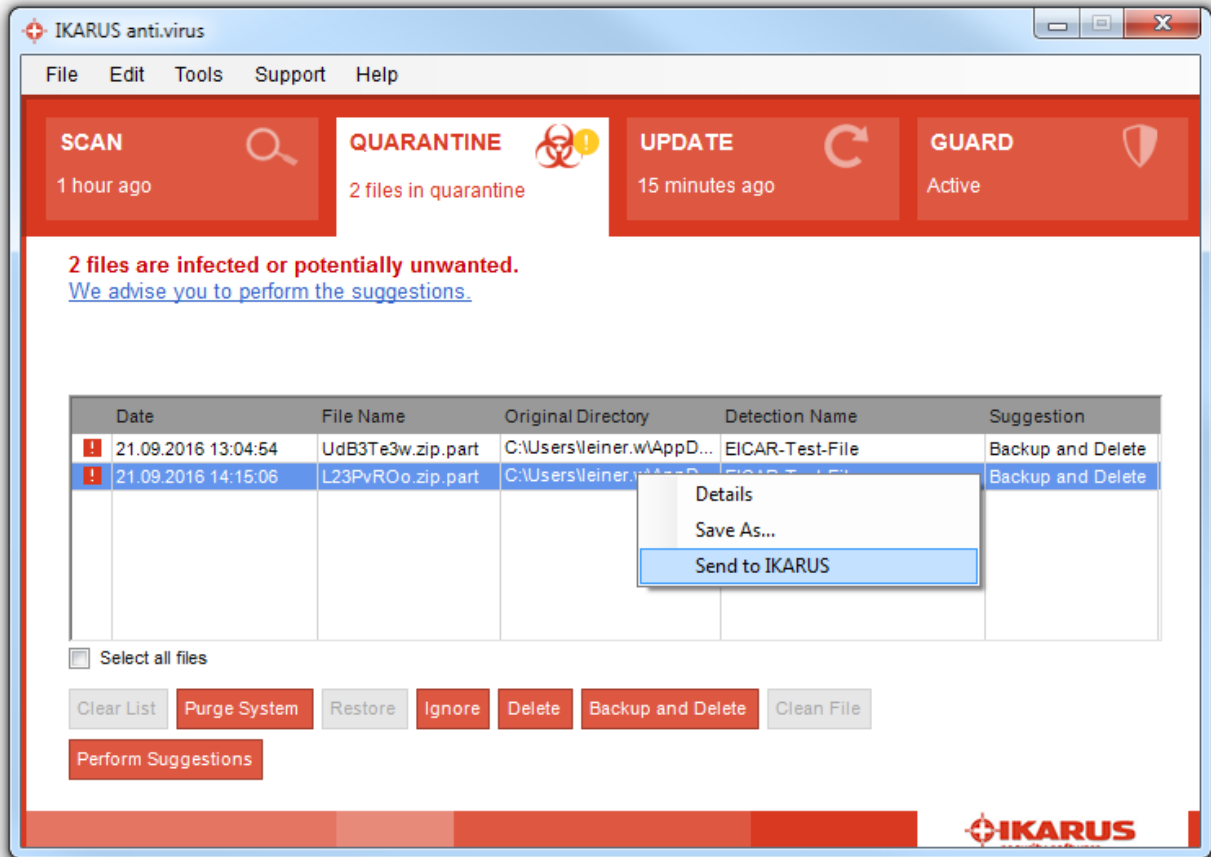


Figure 27: Right-click on the virus

If the cursor is on a virus entry in the quarantine list, you can now right-click the item. A pop-up window now appears where you can specify what actions are to be taken.

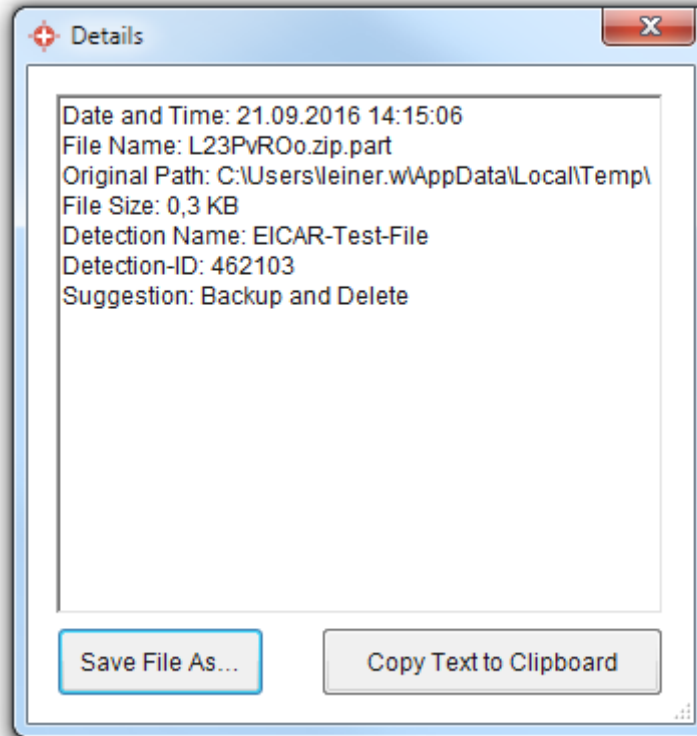


Figure 28: Virus information

To get more information on any virus in the quarantine list, simply double-click on the file name or the original directory.

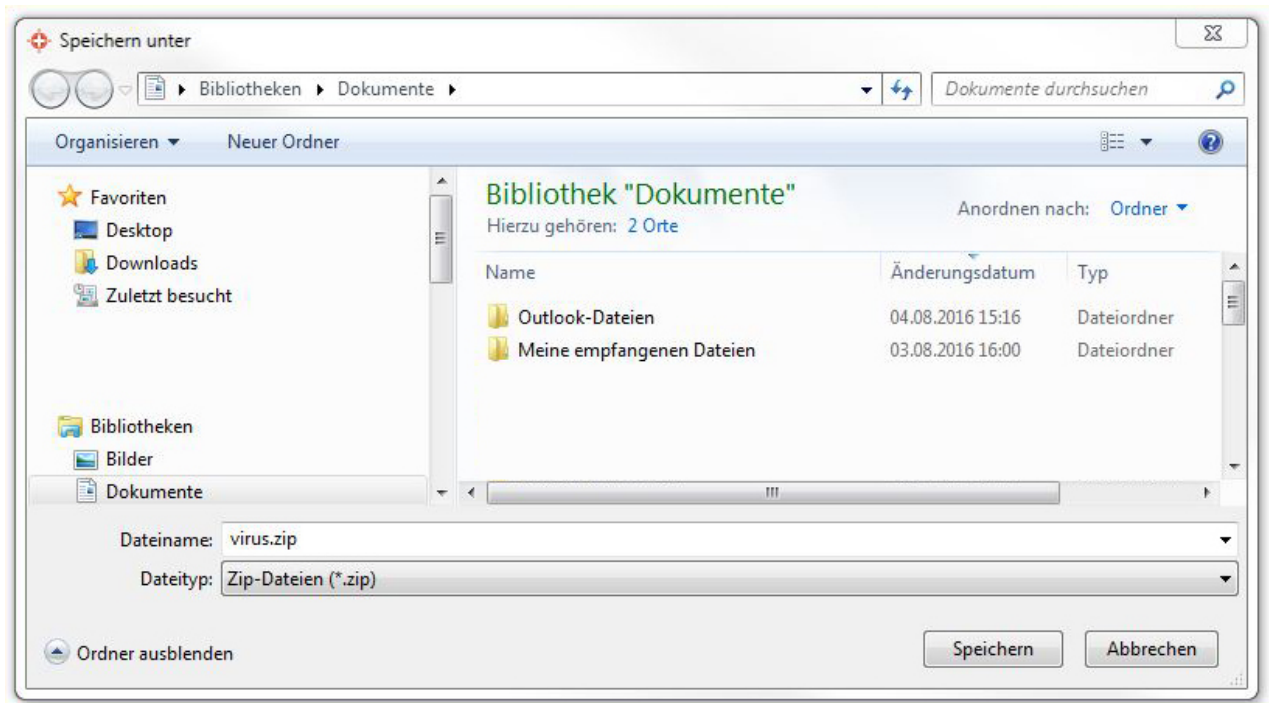


Figure 29: Save virus

If you right-click on "Save as..." a "virus.zip" will be generated and you can send it to IKARUS via mail.

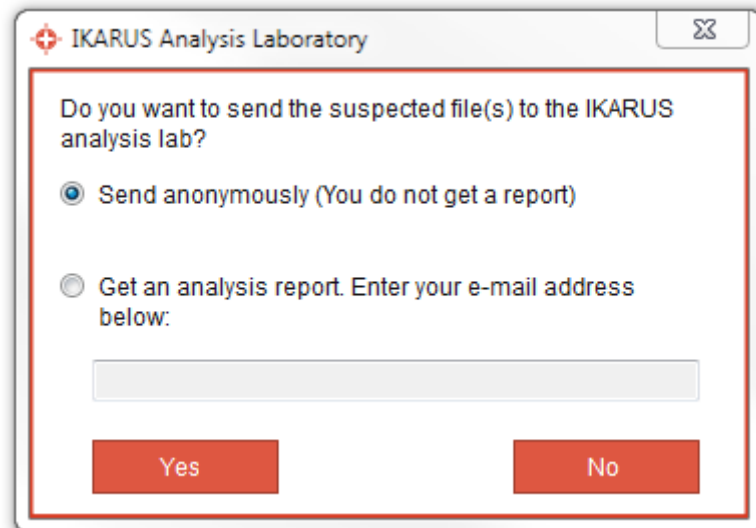


Figure 30: Send virus to IKARUS

To do this automatically just use the function “send to ikarus”. You can do this wether anonymous or with your E-Mail adress to receive further informations from IKARUS.

5

Additional features

5.1 Anti-SPAM

The IKARUS Anti-SPAM Module lets you filtering e-mails, which are received via Outlook, Outlook Express or Windows Mail. To activate the Spam protection just click on the option "Activate Anti-SPAM" in the settings of IKARUS anti.virus.

After the next IKARUS update the Anti-SPAM Module is activated.

To adjust the spam assessment click on the yellow and red controls (yellow stands for "Possible SPAM", red for "SPAM").

To edit the default setting (3/7) click on the row (above "Possible SPAM"; above "SPAM") on the colour labelling.

For e-mails which are marked as SPAM, you can choose between the two options "Mark mail" (add the word "SPAM" to the subject of the e-mail) and "Move mail" (the e-mail gets transferred in the Junk-folder from the mail client).

"Possible SPAM" mails will always be tagged in the mail subject and will stay in the inbox folder of your mail- client.

In the "Advanced SPAM protection" you are able to configure your own spam filter, with possibility to define spam rules for sender, recipient, subject and content of e-mails.

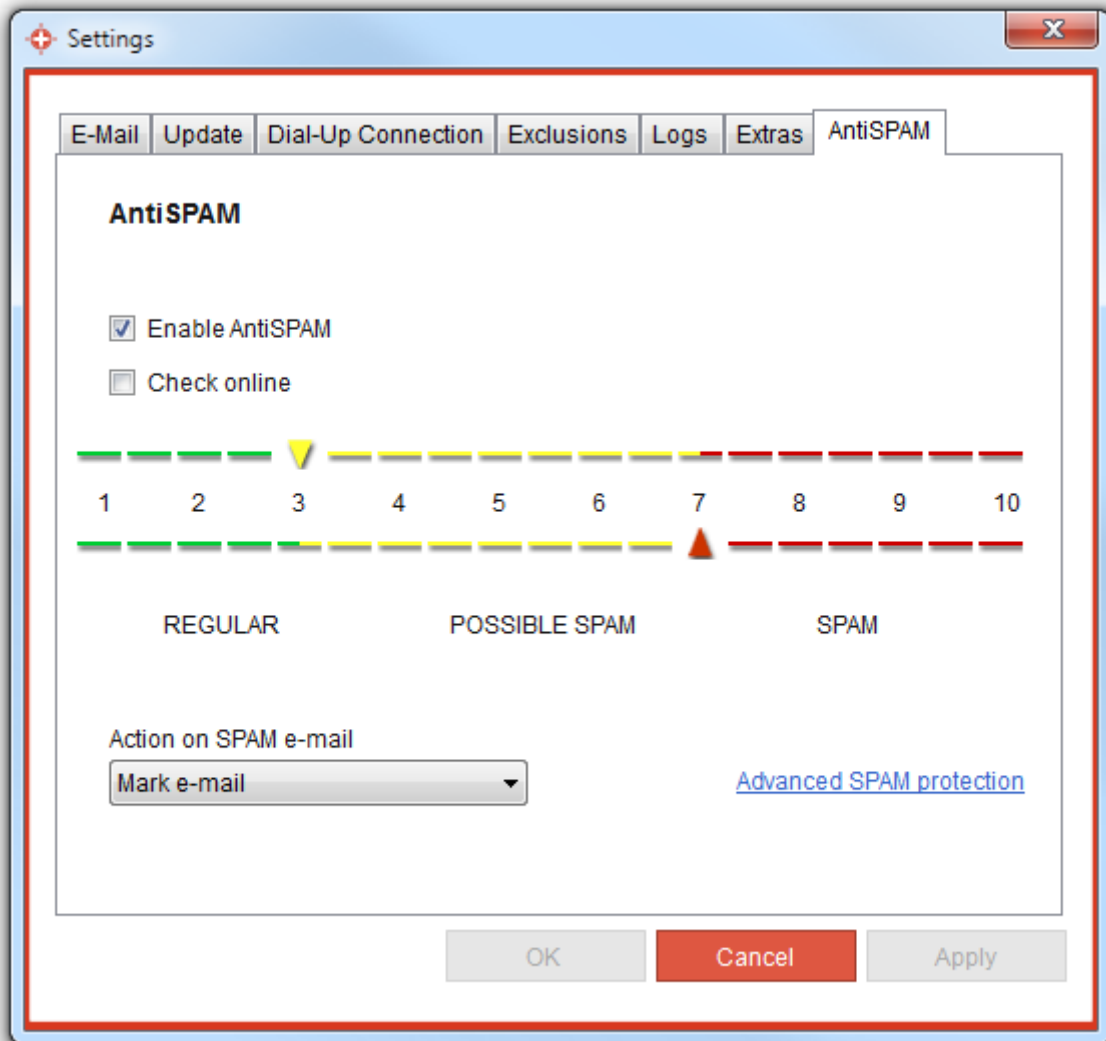


Figure 31: Anti-SPAM settings

Durch Bewegen der Regler nach links oder rechts können Sie die Einstellungen verändern.

5.2 Microsoft-SharePoint protection

This chapter describes how to use IKARUS anti.virus as an anti-virus-plugin for Microsoft SharePoint and addresses advanced users or administrators.

If SharePoint is not installed on your computer, this chapter is not relevant to you.

5.2.1 Performance

IKARUS anti.virus can be used as an anti-virus-plugin for Microsoft SharePoint. The protection covers to components:

- Uploaded files are scanned and the upload is interrupted if a virus is detected.
- Downloaded files are scanned and the download is interrupted if a virus is detected.

<p>Antivirus Settings</p> <p>Specify when you want documents stored in document libraries and lists to be virus scanned, and whether you want your virus scanner to attempt to clean infected documents.</p>	<p><input checked="" type="checkbox"/> Scan documents on upload</p> <p><input checked="" type="checkbox"/> Scan documents on download</p> <p><input type="checkbox"/> Allow users to download infected documents</p> <p><input type="checkbox"/> Attempt to clean infected documents</p>
<p>Antivirus Time Out</p> <p>You can specify how long the virus scanner should run before timing out. If server response time is slow while scanning, you may want to decrease the number of seconds.</p>	<p>Time out duration (in seconds):</p> <p><input type="text" value="300"/></p>
<p>Antivirus Threads</p> <p>You can specify the number of execution threads on the server that the virus scanner may use. If server response time is slow while scanning, you may want to decrease the number of threads allowed for virus scanning.</p>	<p>Number of threads:</p> <p><input type="text" value="5"/></p>

Figure 32: AntiVirus Settings for Microsoft SharePoint

The interface of IKARUS anti.virus offers you the possibility to activate or deactivate the whole protection of Microsoft SharePoint. The plugin itself is controlled in the administration panel of Microsoft SharePoint. Please note that the option “Attempt to clean infected documents” is not supported by IKARUS anti.virus und will therefore show no impact.

IMPORTANT: The IKARUS anti.virus Plugin requires a 64-bit operating system and SharePoint Server Version 2007 or higher.

5.2.2 Installation

Install IKARUS anti.virus as described in chapter 2. IKARUS anti.virus recognizes if Microsoft SharePoint is already installed but you still have to restart Microsoft IIS after finishing the installation procedure. You also have to restart Microsoft IIS after uninstalling IKARUS anti.virus to finish the registration of the Plugin.

Please note that the installation will only succeed if you do not have installed any other anti-virus software that supports Microsoft SharePoint.

For the clients that connect to your SharePoint, no further configuration is required!

5.2.3 Functioning

Following the standard setting of SharePoint and IKARUS anti.virus, every file that is up- or downloaded will be scanned. If the file is not infected, end users on client computers will not notice anything of this process and will be able to go on working undisturbed.

If IKARUS anti.virus detects a virus, the running process will be stopped and the user will be informed over a dialogue box in the current browser window.



Figure 33: Notification about a detected virus when uploading

The figure shows the dialogue box that will be shown to the end user if IKARUS anti.virus has detected a virus within the uploading file.



Figure 34: Notification about a detected virus when downloading

These figure shows the dialogue box that appears if IKARUS anti.virus has detected a virus in a file that is being downloaded and if the option "Scan documents on download" is active and "Allow users to download infected documents" is deactivated.

SharePoint allows the server-administrator to activate or deactivate the scan of uploading and downloading files separately. If one these options is deactivated, IKARUS anti.virus will no longer carry out the virus-scans. Both options, to scan files on download or on upload, will be shown in the IKARUS anti.virus user interface as additional information – but it can only be changed directly in the administration panel of SharePoint.

IKARUS anti.virus offers the possibility to deactivate the surveillance of SharePoint completely. In that case, neither up- or downloads will be scanned.

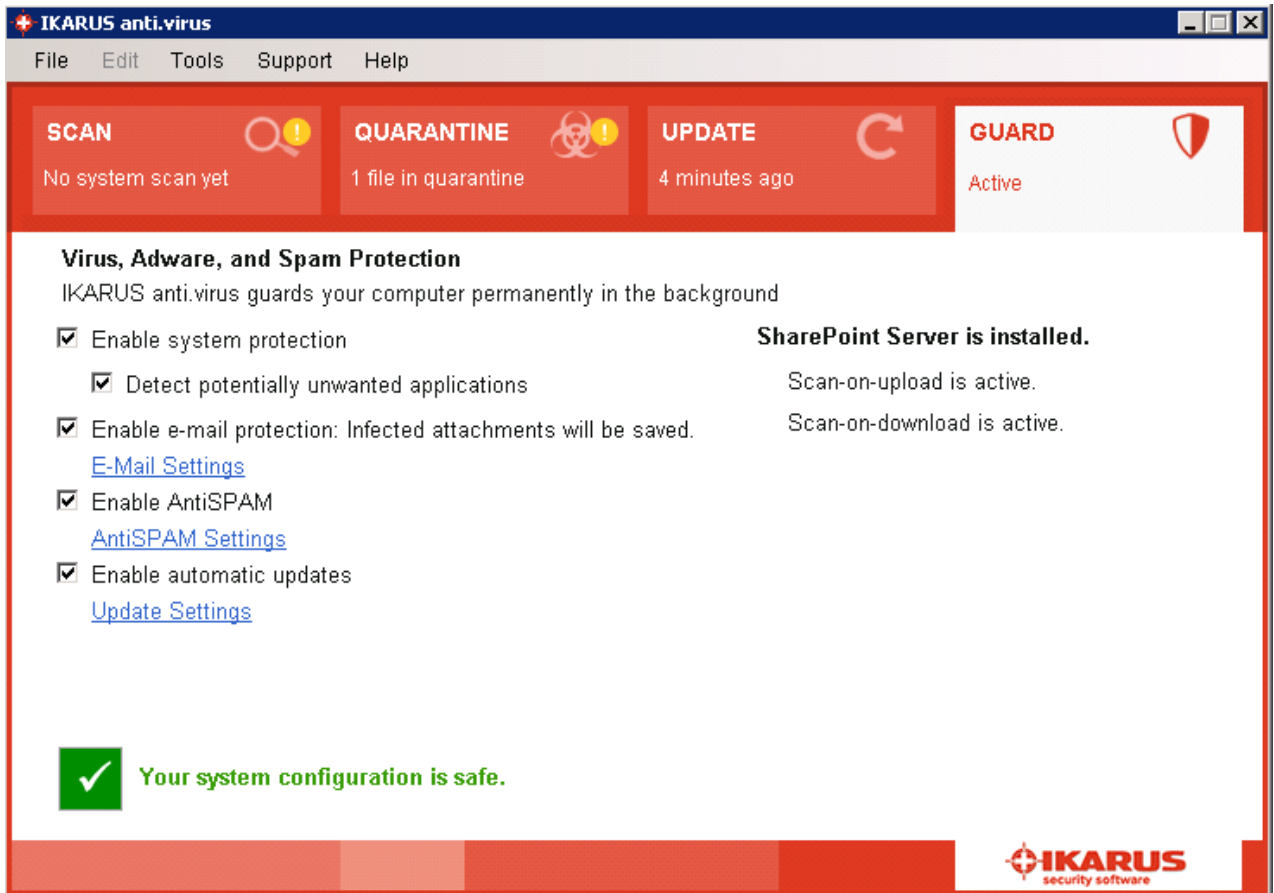


Figure 35: Sharepoint-Settings IKARUS anti.virus

This figure shows the checkmark with the note “Monitor SharePoint Server” that can be set or deleted to control the protection of SharePoint. Below the current status of the up- und download-scanning is shown.

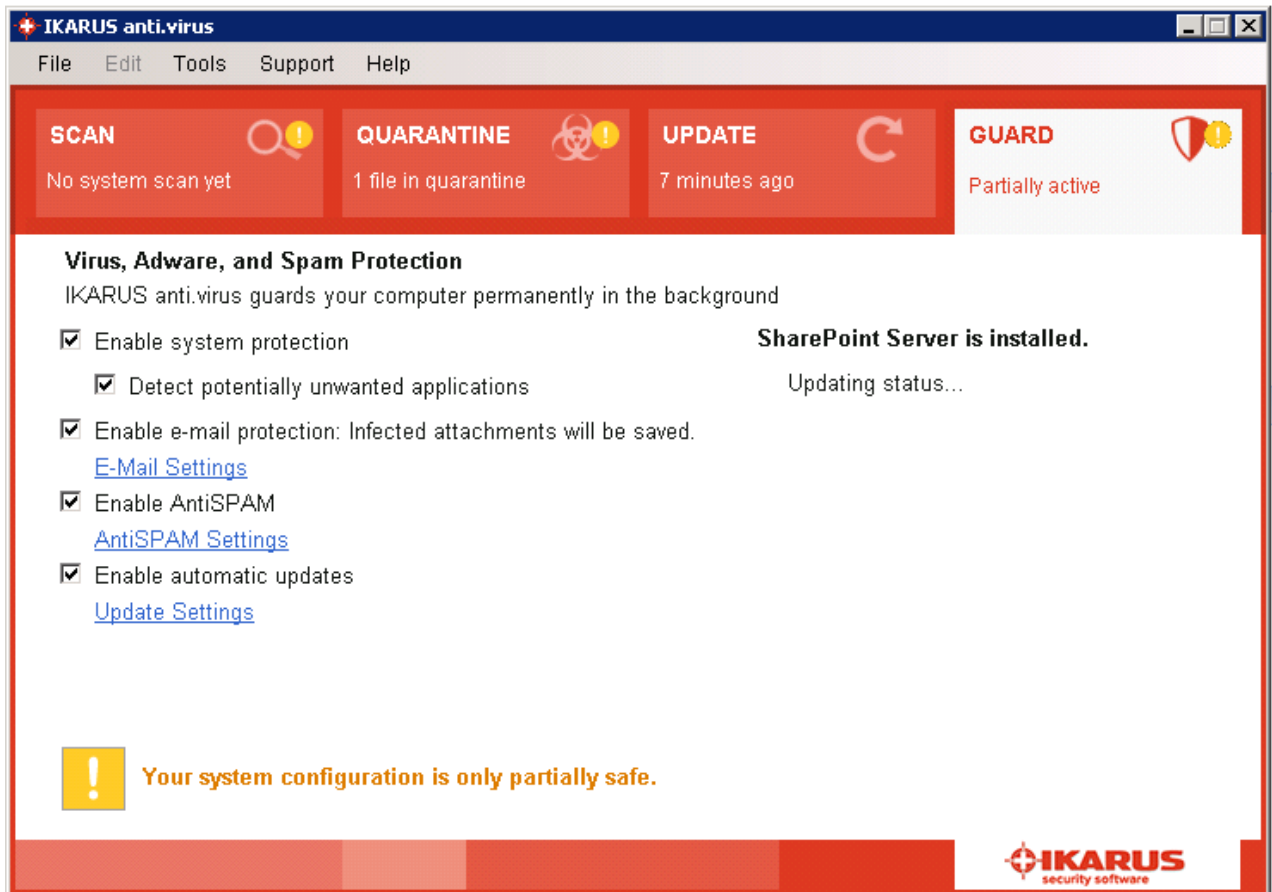


Figure 36: Sharepoint-Settings – Updating status

It might take a few moments until the settings have been checked: In that case you will see the note “Updating status ...” as shown in this image.

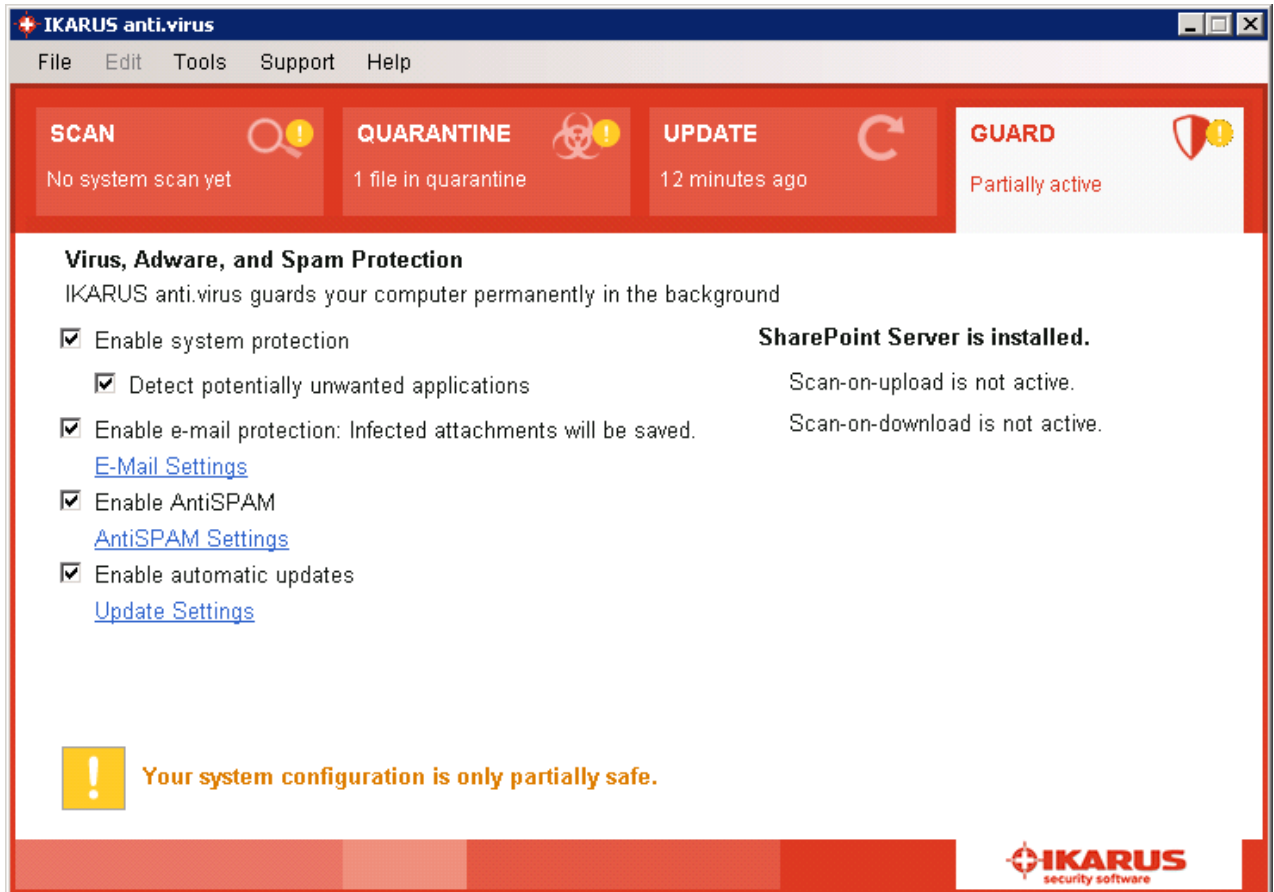


Figure 37: Sharepoint-protection disabled

This image shows that the information of the up- and downloading status disappears if SharePoint protection is deactivated, Then the system protection is not completely safe configured which will be shown by displaying the warning symbol and the status "Your system is partly safe configured".

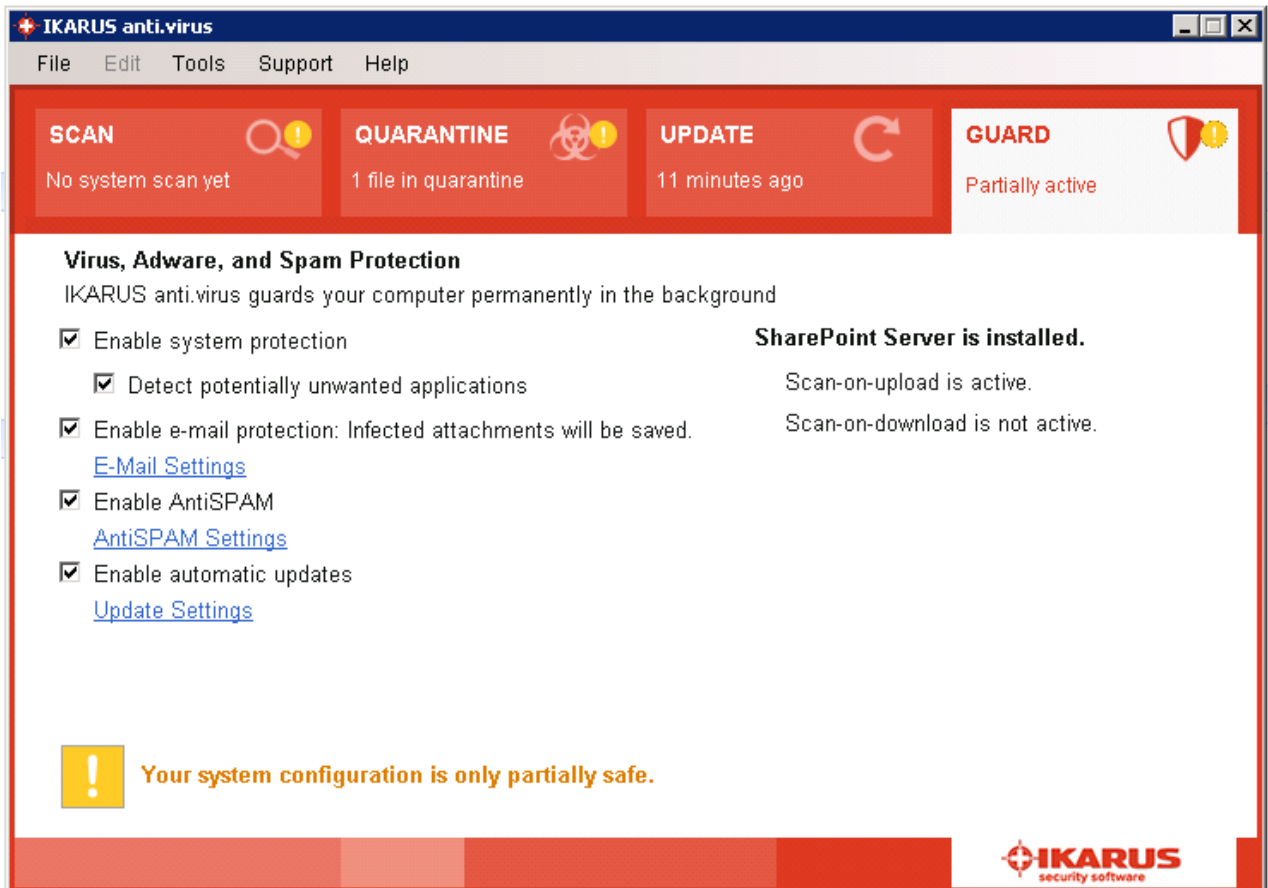


Figure 38: Sharepoint-protection not complete

Derselbe Gesamtsystemstatus ist auch dann gegeben, wenn in der Administrationsoberfläche von SharePoint zumindest eine der beiden Optionen für Upload- oder Download-Scanning deaktiviert ist.

Sollten mit IKARUS anti.virus unerwartete Probleme auftreten, können keine SharePoint-Dateien gescannt werden. In diesem Fall werden aus Sicherheitsgründen der Upload und Download komplett unterbunden, so fern die jeweilige Scan-Option am SharePoint aktiviert ist. Für den SharePoint-Endbenutzer am Clientrechner äußert sich dieses Problem in folgender Fehlermeldung: „installed virus scanner is currently unavailable. If the problem persists, contact your administrator.“

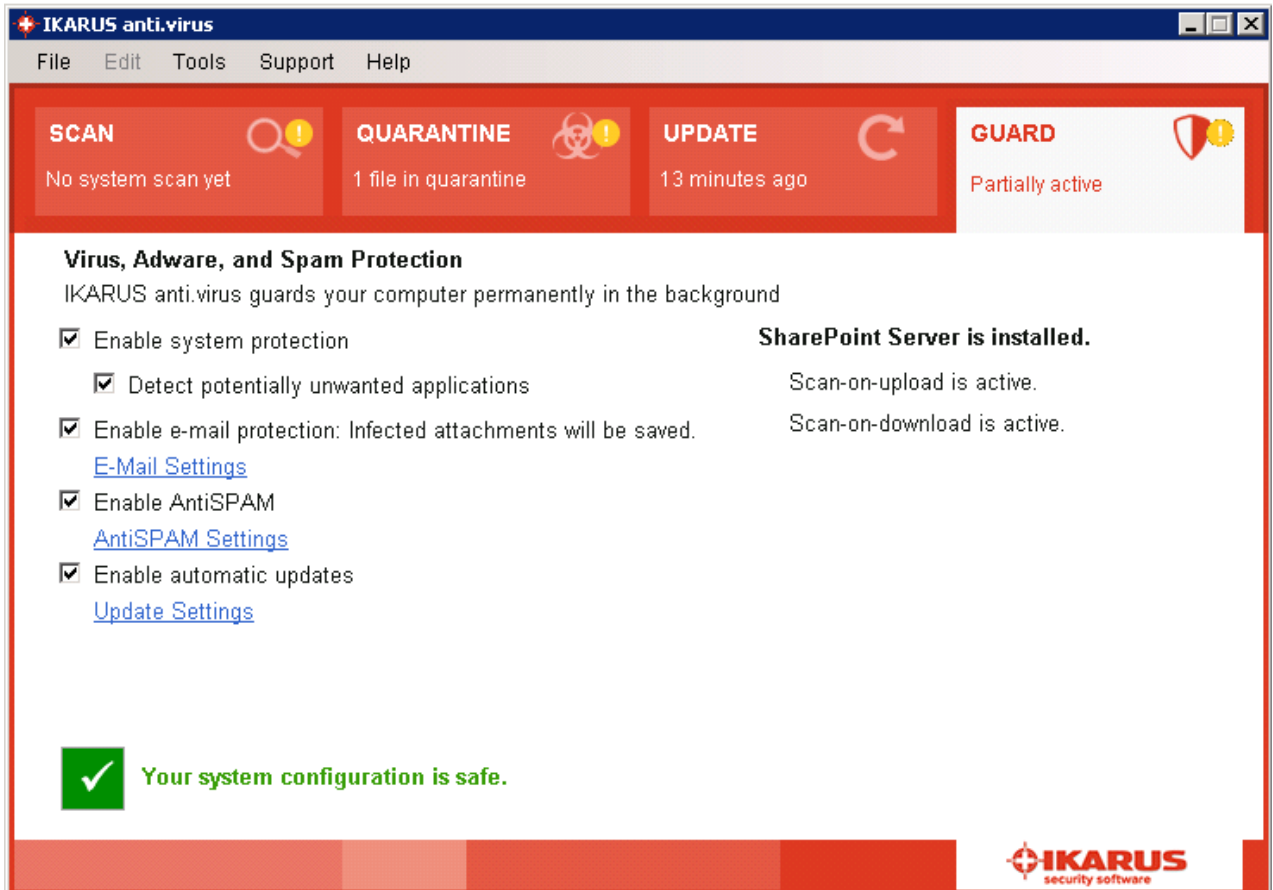


Figure 39: SharePoint-protection complete

6.1 Language settings

Several interface languages are available in IKARUS anti.virus. The software determines the right language (based on your computer settings) during the installation process.

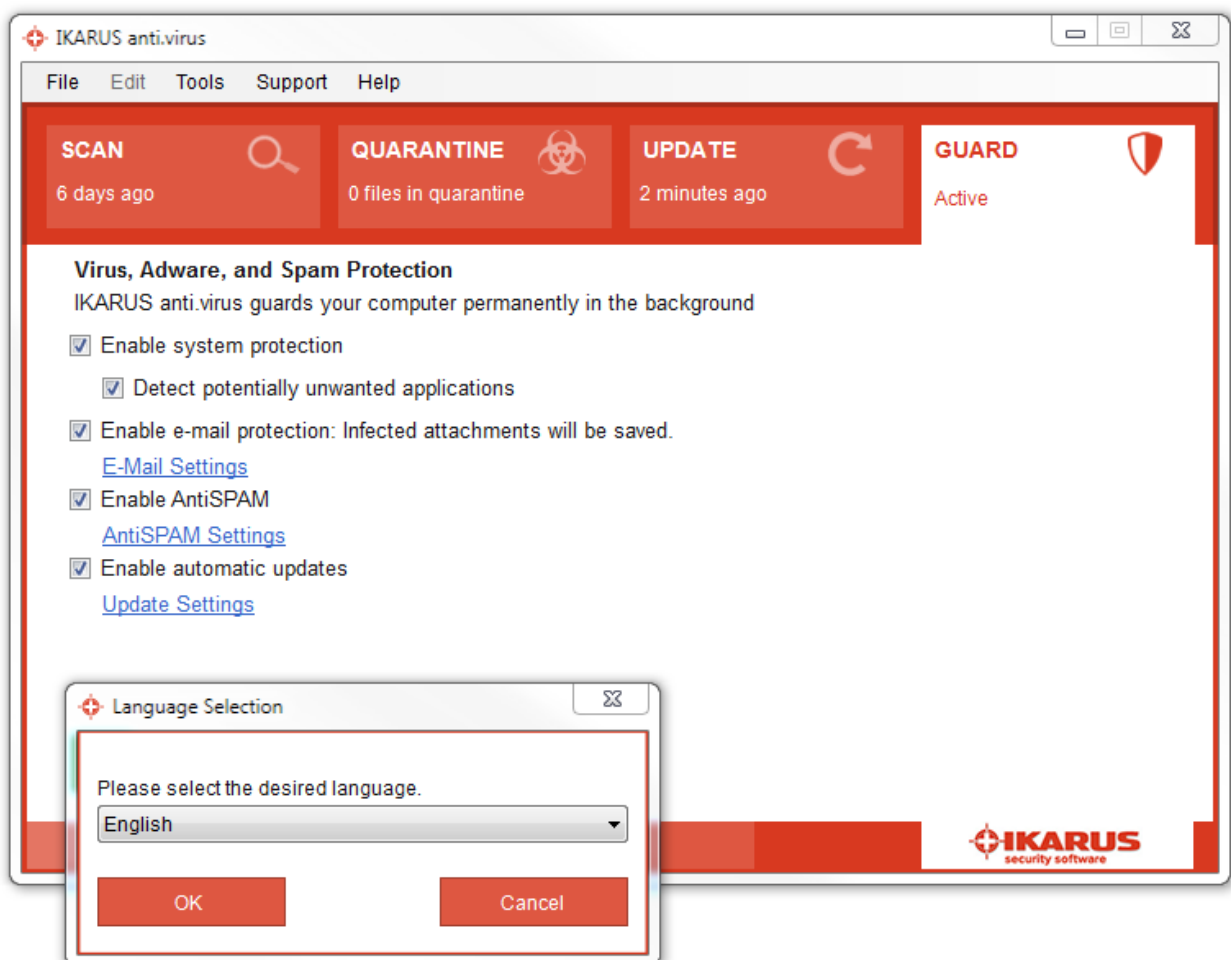


Figure 40: Language settings

The window for changing the language settings is opened under 'Tools' > 'Language' in the menu.

IKARUS anti.virus supports the following languages:

- German
- English
- Croatian
- Italian
- Russian

6.2 Logs

Under „Tools/Logs” you can specify which logs are shown for which actions. In the log window, the previous actions carried out by utilities are displayed.

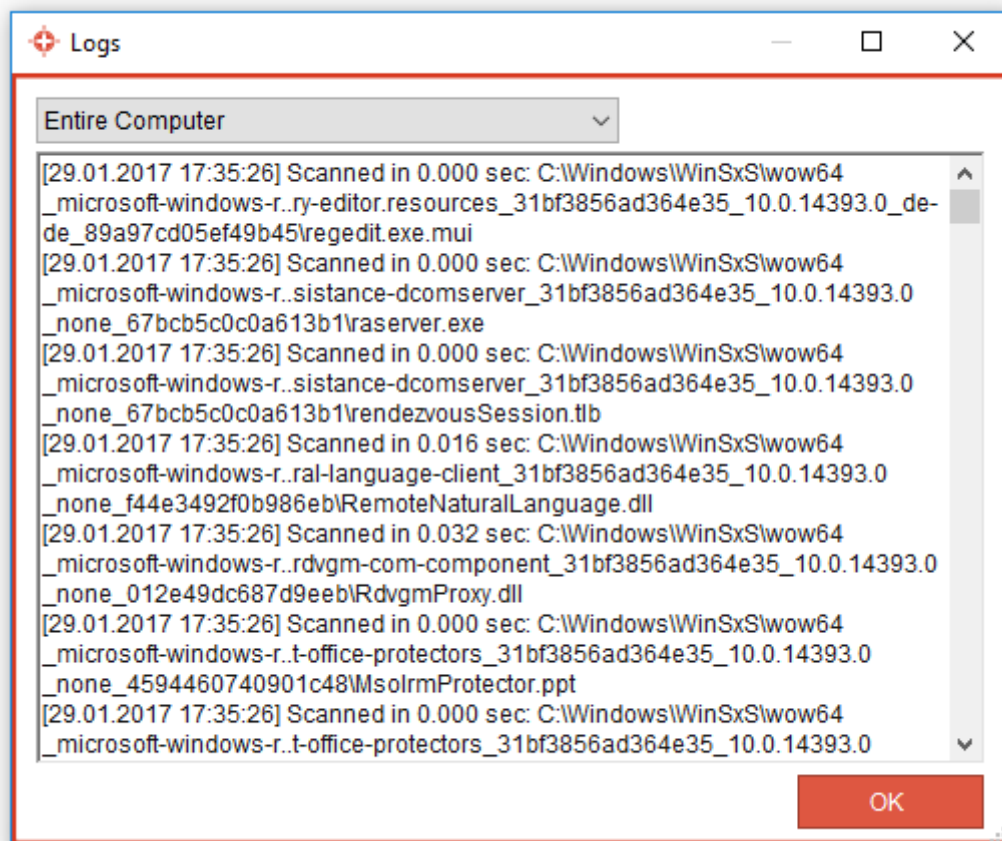


Figure 41: Logs of performed actions

These logs come in particularly handy when you need to get in touch with the IKARUS support hotline (see section 7). You can also view and check the logs to see which actions were performed by IKARUS anti.virus.

6.3 Further settings

IKARUS anti.virus bietet Ihnen im Menü „Extras/Einstellungen“ einen Dialog zur Konfiguration an. In dem Dialog sind die Einstellungsmöglichkeiten über Registerkarten nach Themenbereichen gegliedert.

6.3.1 E-Mail

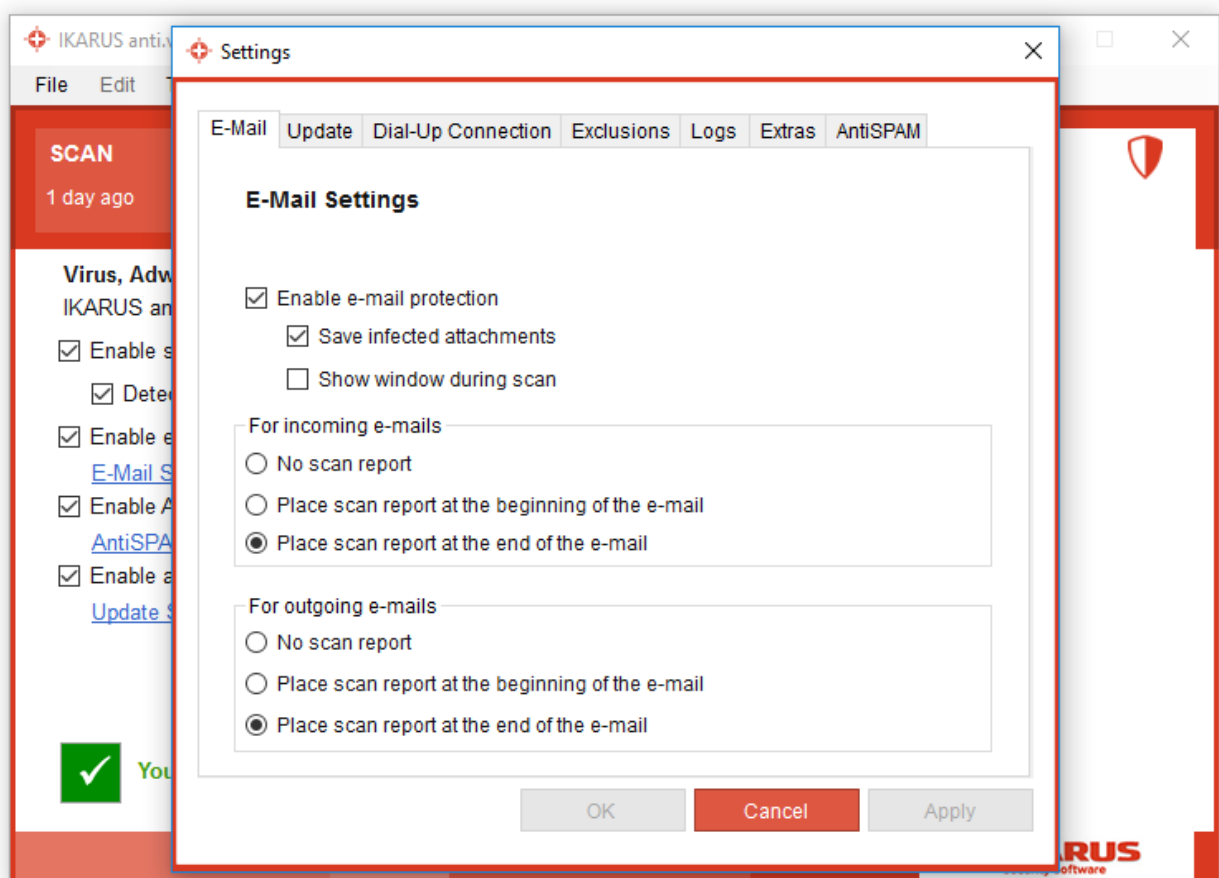


Figure 42: E-Mail Einstellungen

In the Email tab, you can enable and configure e-mail scanning.

6.3.2 Update

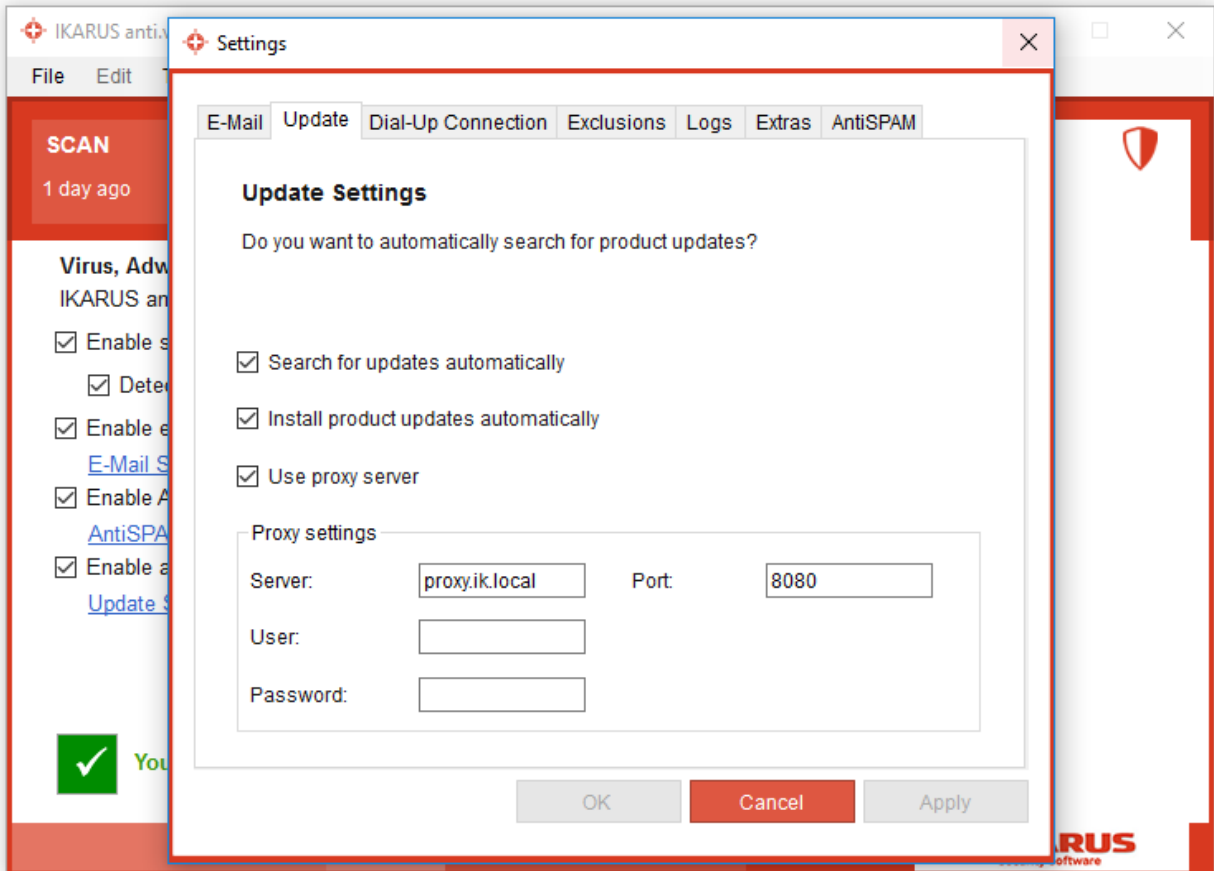


Figure 43: Update-settings

The Update tab shows the different options available for the update function.

6.3.3 Dial Up Connection

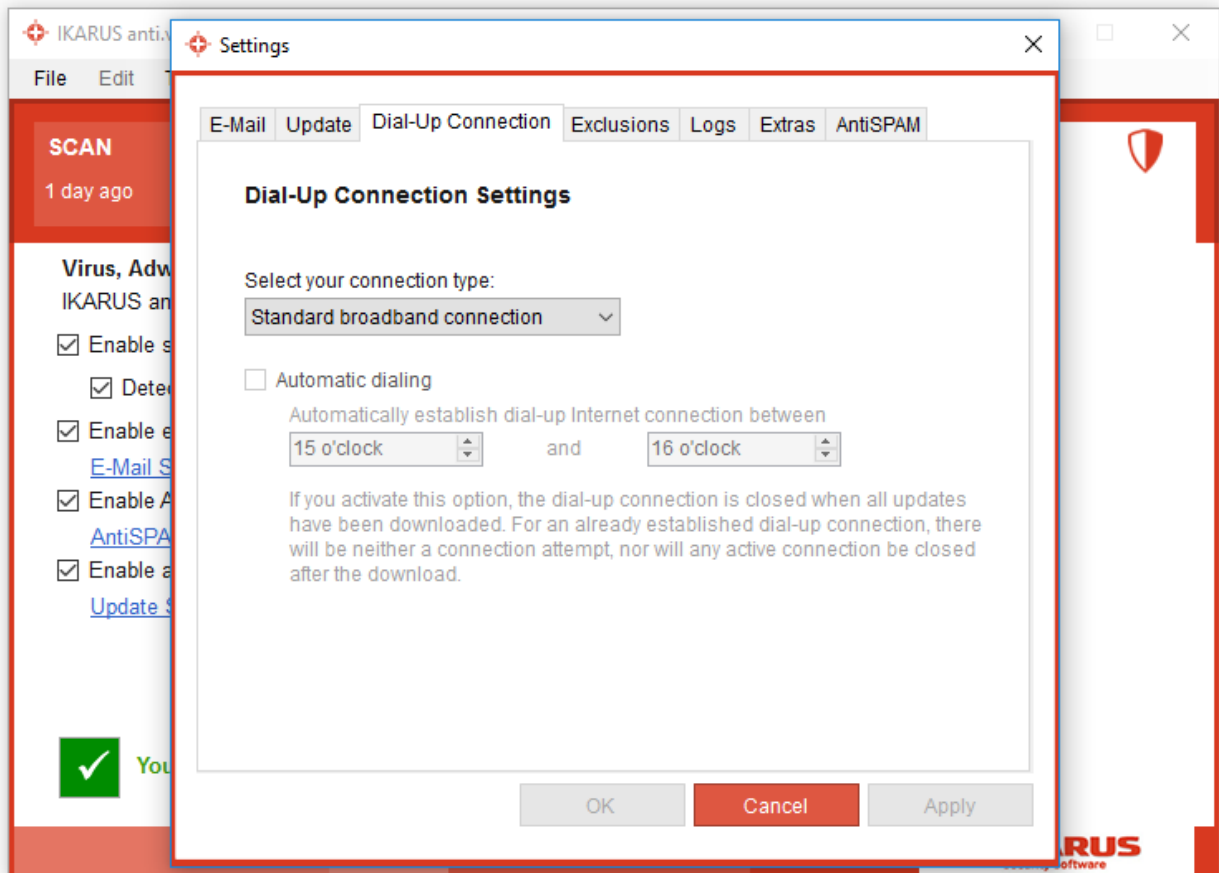


Figure 44: Dial Up Connection-Settings

The Modem connection tab is used to set the autodial function for updating IKARUS anti.virus. You can specify a period of time during which Auto Update can automatically dial and connect to the internet (if dial-up connection is selected).

6.3.4 Exclusions

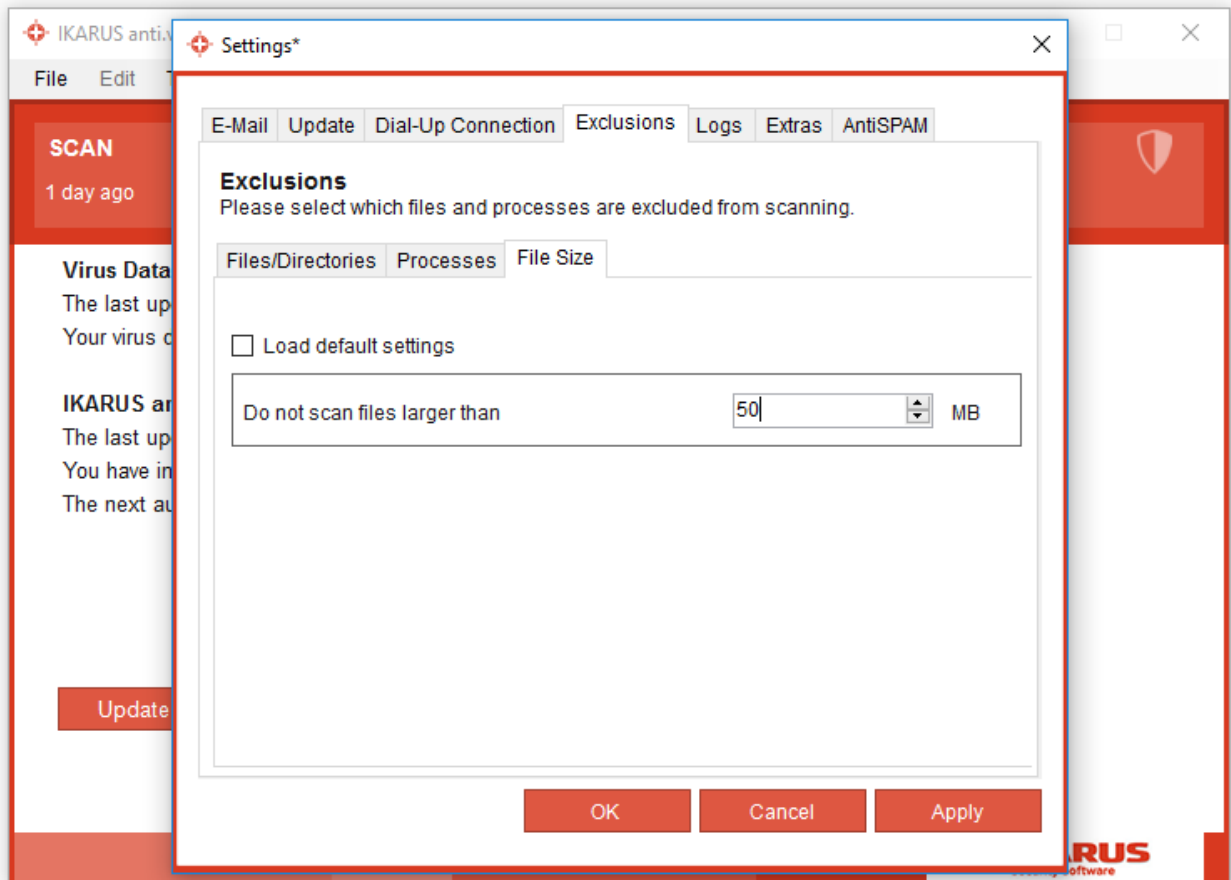


Figure 45: Exclusions-Settings

On the Exclusions tab you can select which files and process are excluded from the IKARUS anti.virus scan. This may be quite useful in cases where you wish to exclude a service from the scan that is already using a good amount of the system resources (mp3 or holiday photos), or if you do not want one specific directory to be scanned.

6.3.5 Logs

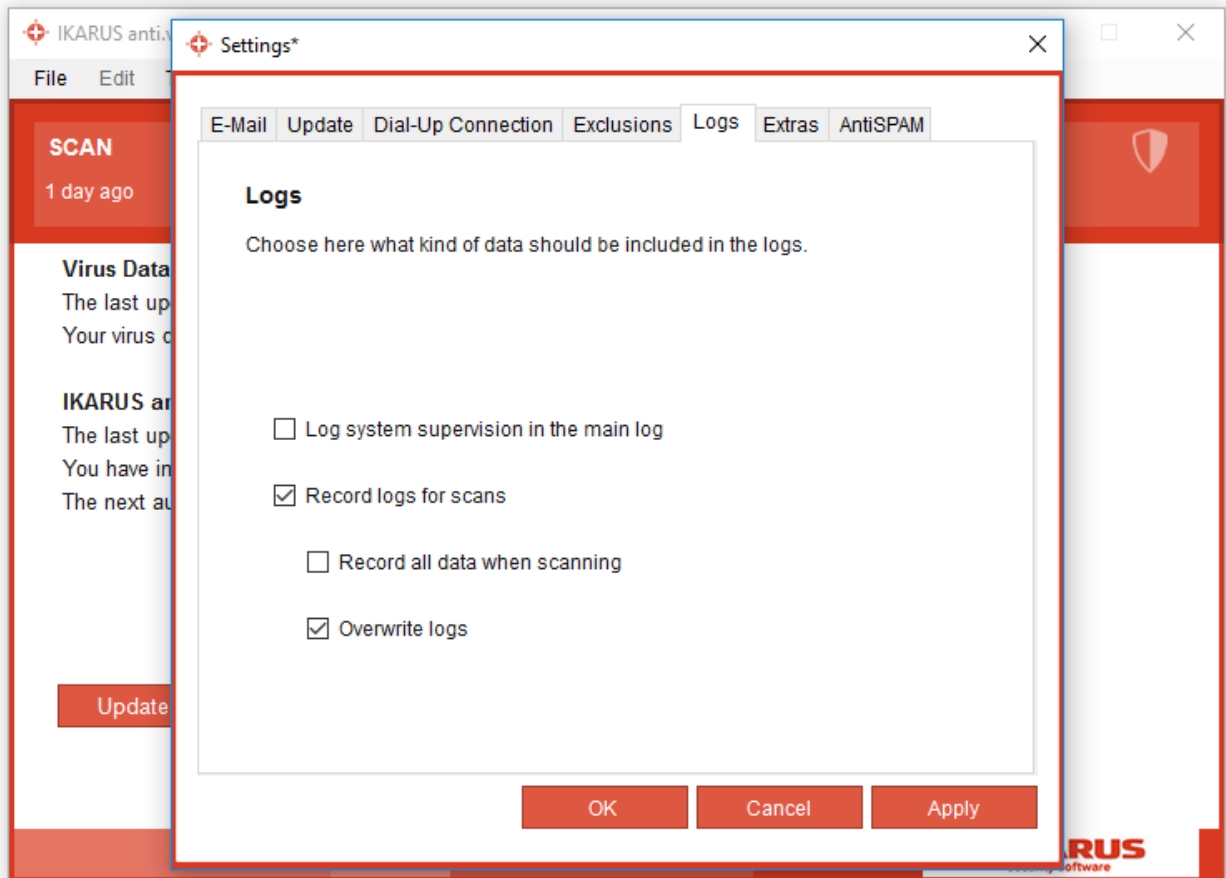


Figure 46: Logs-Settings

Select what actions are to be logged by IKARUS anti.virus on the 'Logs' tab.

6.3.6 Extras

In the 'Extras' tab, you can specify additional settings:

- You can specify that system monitoring is to be reactivated when your PC reboots.
- You can participate on the Quality Insurance Program. IKARUS receives statistic informations from your system to enforce the virus detection. Please recognize the License Agreement in section 8.3 for that.
- Since IKARUS anti.virus 2.2 exists the possibility to set a password protection. If this is activated, settings can only be edited after entering the password. This option is helpful if you as administrator of the computer want to prevent that non-authorized users can edit the settings. This password protection is also for enabling/disabling the System protection.

Press 'Restore Default Settings" to reset IKARUS anti.virus to its original settings following installation. All previously changes to the settings are reset.

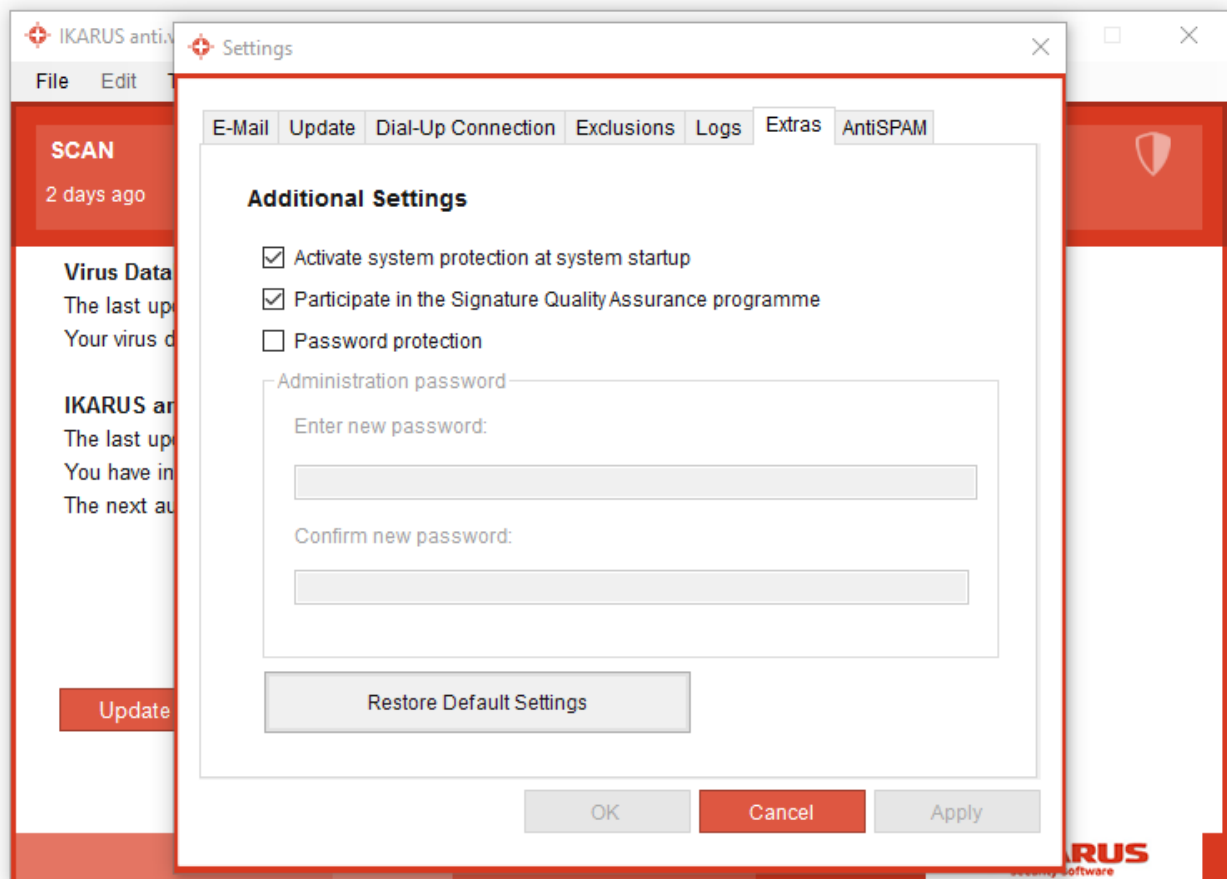


Figure 47: Extras-Settings

6.3.7 Anti-SPAM

The Anti-Spam Module lets you organize the settings for your personal mail filter of IKARUS IKARUS anti.virus. Find more information about the Anti-SPAM Module at section 5.1 of this manual.

7

Support

For inquiries and consultation with IKARUS it is helpful to obtain detailed informations about the installed version of IKARUS anti.virus or the virus database (VDB).

To make the process as fast and efficient as possible, there are several ways to get in touch with us and send us information regarding questions you have on IKARUS anti.virus.

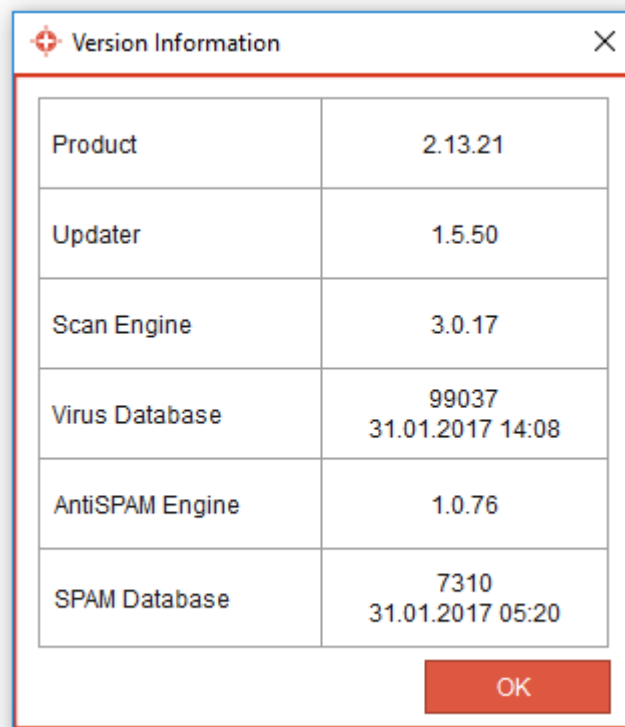


Figure 48: Support – Version information

Go to Support in the menu bar to quickly view the current version number of your IKARUS anti.virus. You will need this information when contacting our support team.



Figure 49: Support – Contact

You can also view the contact details in IKARUS anti.virus. When you write an email to this address, it is automatically sent to us with the vital version information.

Under “Support” – “Save Support Info” in the menu, you can compile the most support information and send it to us as a zip file.

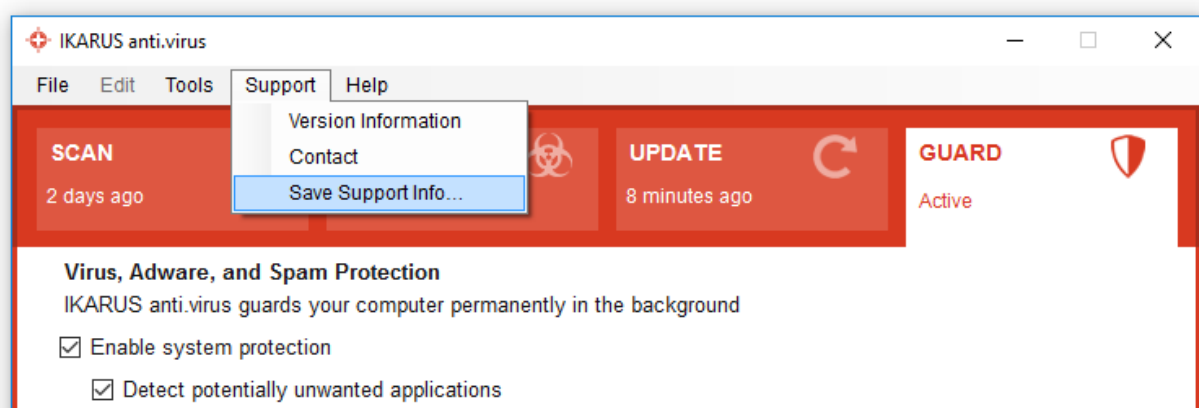


Figure 50: Support-Info

7.1 License key

The IKARUS anti.virus program comes with a special license key. This governs the length of your license and the number of installed users.

You automatically receive the license key when you purchase IKARUS anti.virus or sending the registration form to IKARUS via product activation.

Under Help in the menu, you can check, delete, add or archive your license keys.

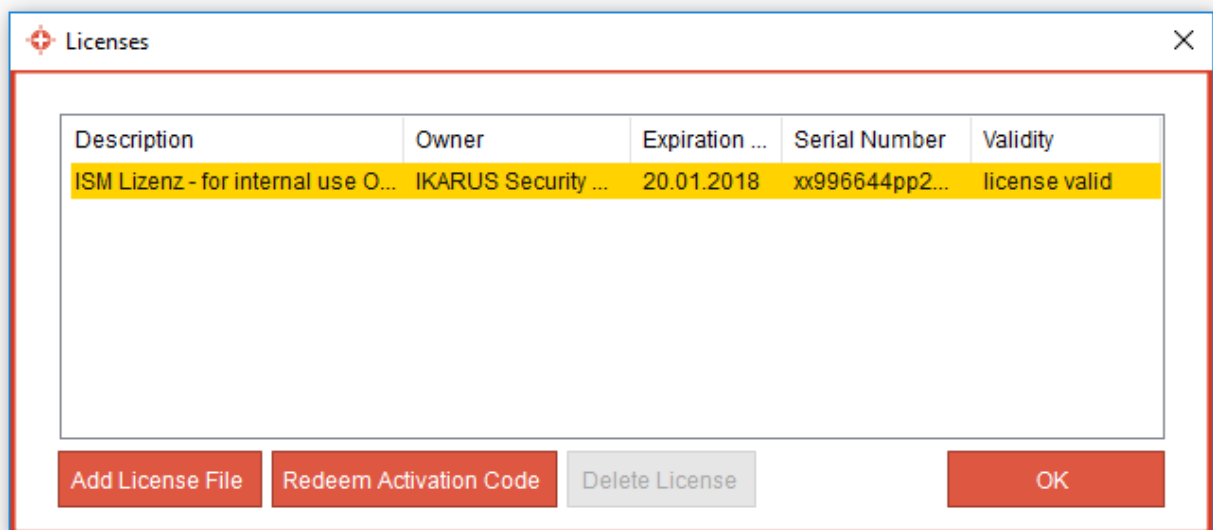


Figure 51: IKARUS anti.virus Licenses

It is also possible to manage multiple license keys in cases, for instance, where a license key is set to expire soon and you have already received the new one. IKARUS anti.virus automatically selects the right key.

Please contact our support team if you cannot find your license key or you did not receive one.

If you have an activation key, please fill in your personal data and send the registration to IKARUS to receive a license key for IKARUS anti.virus, which will be imported into the software automatically.

Redeem Activation Code [X]

Please fill out the required fields.
We need your data so that we can provide free support as long as your product is licensed.

Activation Code:*	<input type="text"/>	Last Name:*	<input type="text"/>
Gender:*	<input checked="" type="radio"/> Male <input type="radio"/> Female	First Name:*	<input type="text"/>
Company:	<input type="text"/>	House Number:*	<input type="text"/>
Street:*	<input type="text"/>	City:*	<input type="text"/>
Postal Code:	<input type="text"/>		
Country:*	Austria ▼		
E-Mail:*	<input type="text"/>	Phone:	<input type="text"/>

* These fields are required for a successful registration!

Figure 52: Activate the software via activation code

8

Further informations

Please get here information about the necessary Microsoft NET Framework, the adaption of personal firewalls and the licensing terms of IKARUS Security Software GmbH.

8.1 .NET Framework

.NET Framework is required to display IKARUS anti.virus' graphical interface. If this program is already in- stalled on your computer, the installation of IKARUS anti.virus will be completed without interruption. If, however, this program is not already installed on your computer, this will be either automatically installed from the installation CD or, if you are not installing the program from a CD, it will be downloaded from the Microsoft website.

.NET Framework is freeware from Microsoft. There are no license fees and it requires no registration.

8.2 Licensing Terms

The actual EULA you can find also under <https://www.ikarussecurity.com/eula/>

IKARUS Security Software GmbH

Blechturm-gasse 11
1050 Vienna
Austria

Telefon: +43 (0) 1 58995-0
Fax: +43 (0) 1 58995-100
office@ikarus.at
<https://www.ikarussecurity.com>

IKARUS Security Software Support Kontakt

Phone: +43 (0) 1 58995-400
Support times: Monday - Thursday: 8 am – 6 pm Uhr (CET)
Friday: 8 am – 3 pm (CET)

E-Mail: support@ikarus.at

IKARUS Security Software Sales Contact

Phone: +43 (0) 1 58995-500
E-Mail: sales@ikarus.at