FORSCHUNGSZENTRUM JÜLICH GmbH

Jülich Supercomputing Centre
D-52425 Jülich, Tel. (02461) 61-6402

Network Service Desk, Tel. (02461) 61-6440

Technical Information

FZJ-JSC-TKI-0419
Dr. Frank Mohr, JSC-KS
01.12.2021

Use of the Rescue Disks from ESET, Kaspersky and Avira

Table of contents

1. Introduction

With the solutions ESET SysRescue, Kaspersky Rescue Disk 2018 and Avira Antivir Rescue System, employees of the Forschungszentrum Jülich have three powerful rescue tools (‘rescue disks’) (also for private use) available to scan Windows and Linux partitions for malware. Any infections should be identified and removed.

For all solutions appropriate update procedures are given to guarantee daily updated virus signatures. It is strongly recommended that such an update be carried out before the actual examination, so that the rescue disks can develop their full potential.

With all three solutions, the provided ISO images can be used in form of a USB stick or burned as a CD / DVD. For the sake of simplification, the term rescue disks will be used in the following.

In principle, no guarantee can be given that the rescue disks work correctly with all existing hardware and software combinations or that the update procedures work with all available network adapters. If problems arise, some tips are listed in the respective instructions and in

Chapter 6-Troubleshooting; you can get in touch with your PC support as well as the JuNet hotline on extension 6440.

On many hardware platforms, especially newer ones, the UEFI settings have to be adjusted so that the rescue disks work correctly. This is briefly discussed in the respective chapters. It is generally helpful to deactivate `<Secure Boot>` in the event of problems. The UEFI / BIOS mode may also have to be selected correctly (`<Legacy>`).

All three solutions cannot examine encrypted partitions. A partition to be examined must therefore first be decrypted manually by the user before the rescue disks are used. Advanced users will find instructions on the World Wide Web on how some of the common encryption techniques can be individually added to the rescue disks; this is not discussed further in this TKI.

In addition, no guarantee can be given that any infection can be correctly identified and cured. If a system is reported by a rescue disk as not or no longer infected, this should be confirmed by at least one of the other solutions. Systems that have been infected are no longer trustworthy, even if rescue tools report successful removal. Depending on the circumstances, a re-examination or even a new installation is advisable in the medium term.

JSC recommends the usage of such solutions with following priority: First ESET SysRescue, then Kaspersky Rescue Disk 2018 and finally Avira Antivir Rescue System.

2. Alternatives to the rescue disks

A few alternatives to the rescue disks should also be mentioned, which can assist the user of a suspicious system. This is particularly helpful in the case of hardware conflicts that prevent the use of the rescue media.

First of all, McAfee Stinger is mentioned, which (in contrast to the rescue disks) is used directly on the Windows desktop of the system to be checked. The virus database includes the viruses classified as highly threatening at the time, so Stinger must always be downloaded up-to-date.

Download McAfee Stinger:

https://downloadcenter.mcafee.com/products/mcafee-avert/stinger/stinger32.exe

The Microsoft Safety Scanner is also a tool that can be used directly on the desktop of a suspicious Windows system if the local virus scanner is no longer trusted. In the event of a specific threat, it can be downloaded free of charge and used for 10 days.

Download Microsoft Safety Scanner and short introduction:

https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download

Windows Defender Offline also comes from Microsoft, which can scan for malware in the event of a suspected infection and is already integrated into Windows 10. It is also only executed when required, so it does not replace a virus scanner.

Quick start guide Microsoft Windows Defender Offline:

https://support.microsoft.com/en-us/windows/help-protect-my-pc-with-microsoft-defender-offline-9306d528-64bf-4668-5b80-ff533f183d6c

Finally, reference is made to the PC-Welt Rescue DVD, which, in addition to several virus scanners, also contains other administration tools for Windows, e.g. hardware diagnostics, data recovery and backups.

Download PC-Welt Rescue-DVD [german]:

https://www.pcwelt.de/downloads/PC-WELT-Notfall-DVD-3890747.html

3. Using ESET SysRescue

An ESET SysRescue ISO image can be found on PCSRV at

🔗 \\pcsrv.zam.kfa-juelich.de\public\Notfall-CDs\01-ESET-SysRescue

This image is updated regularly (which, however, does not replace the daily updates of the virus signatures).

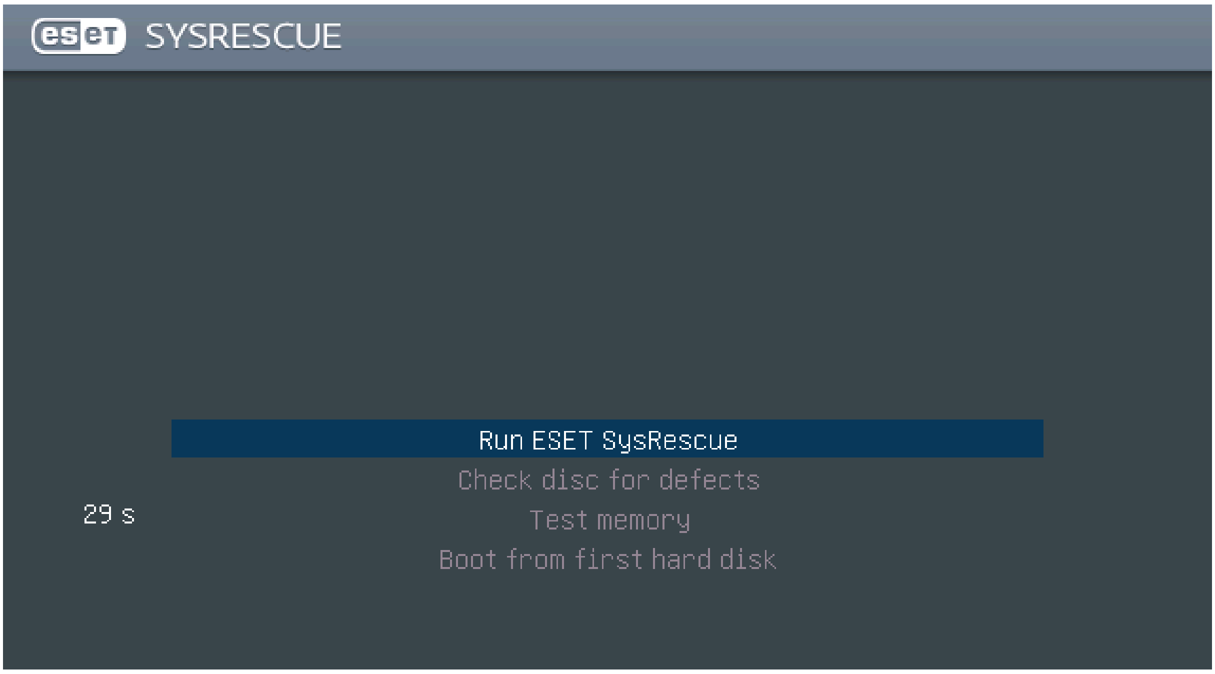
⚠ Depending on the hardware configuration, ESET SysRescue can only run on EFI / UEFI systems if you deactivate `<Secure Boot>` in the system setup and set the UEFI mode to `<Legacy>` or `<Legacy only>`.

Start the affected system with ESET SysRescue by creating a bootable USB stick from the ISO image. Use suitable third-party software for this purpose; The ESET image was successfully tested e.g. with Rufus Portable. Note that the previous contents of the USB stick will be deleted.

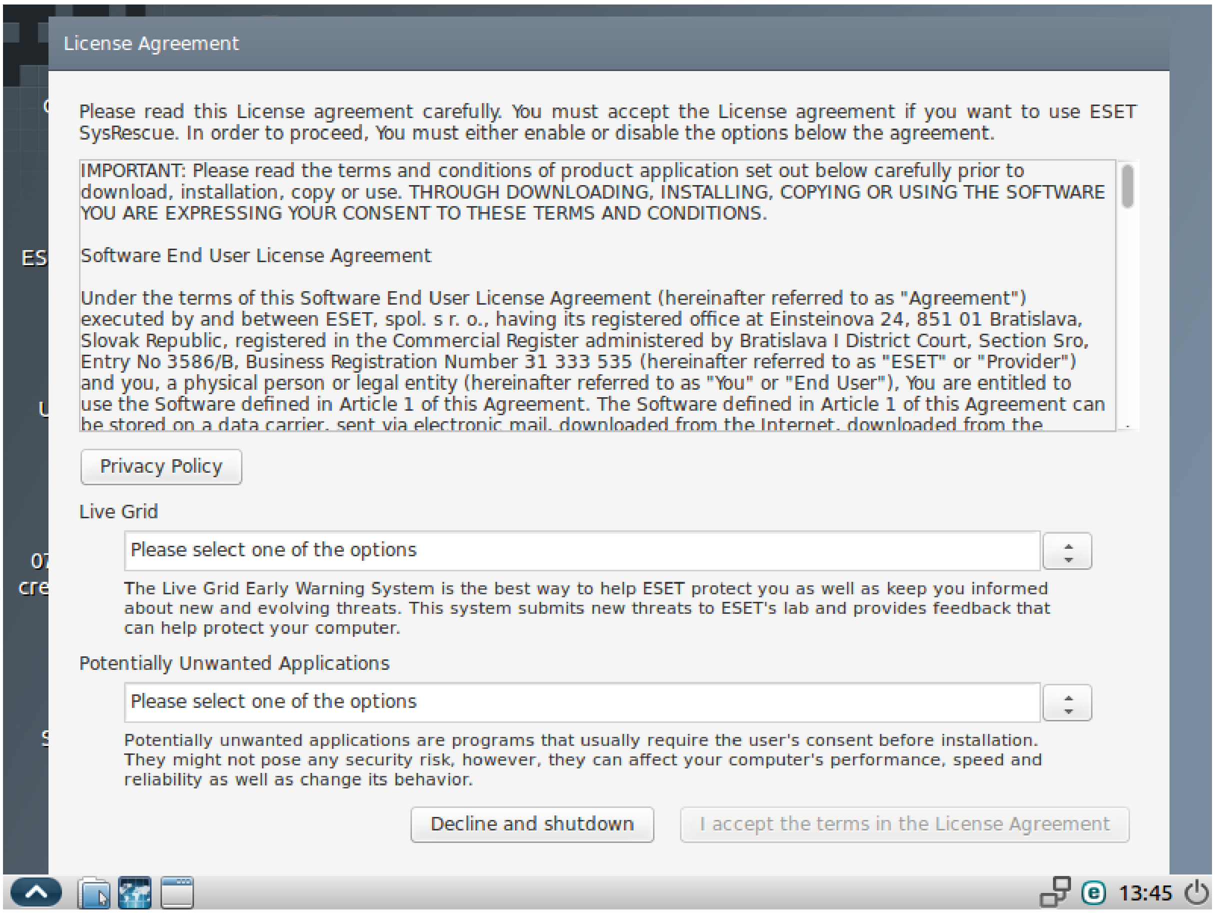
🔗 Download Rufus Portable:
https://rufus.ie/de/

⚠ Alternatively, you can burn the ISO image as a CD / DVD and restart the affected system from this. To do so, use the software available at your institute or the `<Burn disc image>` function integrated in Windows 10.

The boot menu of the rescue disk appears:



Normally you can simply confirm `<Run ESET SysRescue>` with `<Return>`. If you make no entry, the boot process starts automatically after 30 seconds.



Please read this License agreement carefully. You must accept the License agreement if you want to use ESET SysRescue. In order to proceed, You must either enable or disable the options below the agreement.

IMPORTANT: Please read the terms and conditions of product application set out below carefully prior to download, installation, copy or use. THROUGH DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS.

Software End User License Agreement

Under the terms of this Software End User License Agreement (hereinafter referred to as "Agreement") executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number 31 333 535 (hereinafter referred to as "ESET" or "Provider") and you, a physical person or legal entity (hereinafter referred to as "You" or "End User"), You are entitled to use the Software defined in Article 1 of this Agreement. The Software defined in Article 1 of this Agreement can be stored on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the

Live Grid

Please select one of the options

The Live Grid Early Warning System is the best way to help ESET protect you as well as keep you informed about new and evolving threats. This system submits new threats to ESET's lab and provides feedback that can help protect your computer.

Potentially Unwanted Applications

Please select one of the options

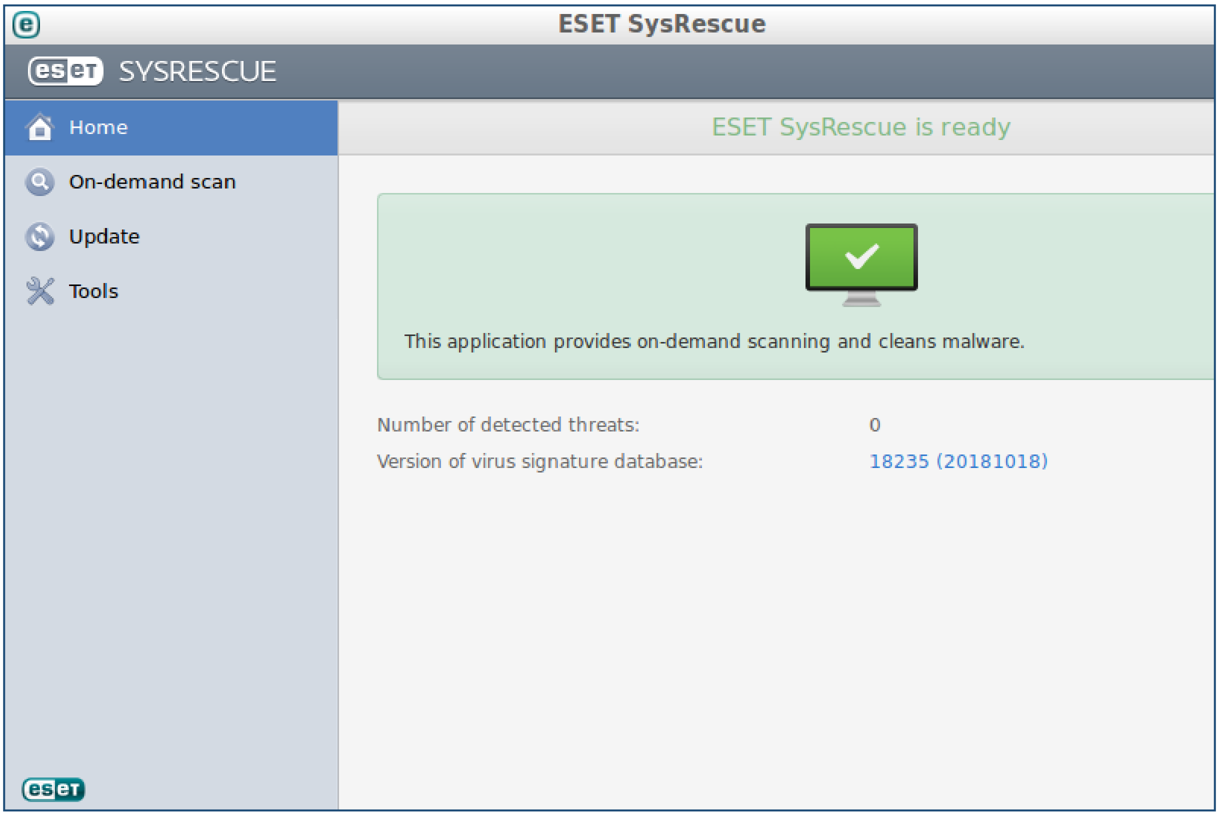
Potentially unwanted applications are programs that usually require the user's consent before installation. They might not pose any security risk, however, they can affect your computer's performance, speed and reliability as well as change its behavior.

Wait until the rescue disk has loaded all the necessary files and settings. The license agreement is displayed first; to be able to confirm this, you have to choose two options:

Live Grid: If you select <Enable Live Grid Early Warning System>, information about malware found will be sent to the manufacturer to improve the early detection of new threats. If you do not want this, select <Disable ...>, the emergency CD is fully functional even without it.

Potentially Unwanted Applications: If you select <Enable ...>, the rescue disk also checks for programs that are not malware in the strict sense, but can reduce the confidentiality and performance of your system. This affects e.g. certain advertising measures or spyware. If you do not consider the check necessary, select <Disable ...>, the check for malware takes place normally.

After selecting both fields, you can confirm the license agreement using <I accept the terms in the License Agreement>. The main menu of the rescue disk appears.



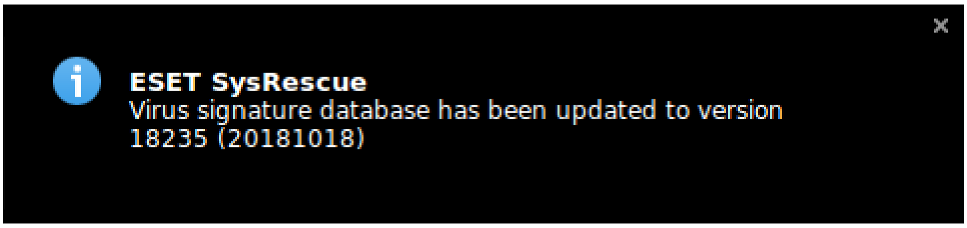
ESET SysRescue is ready

This application provides on-demand scanning and cleans malware.

Number of detected threats: 0

Version of virus signature database: 18235 (20181018)

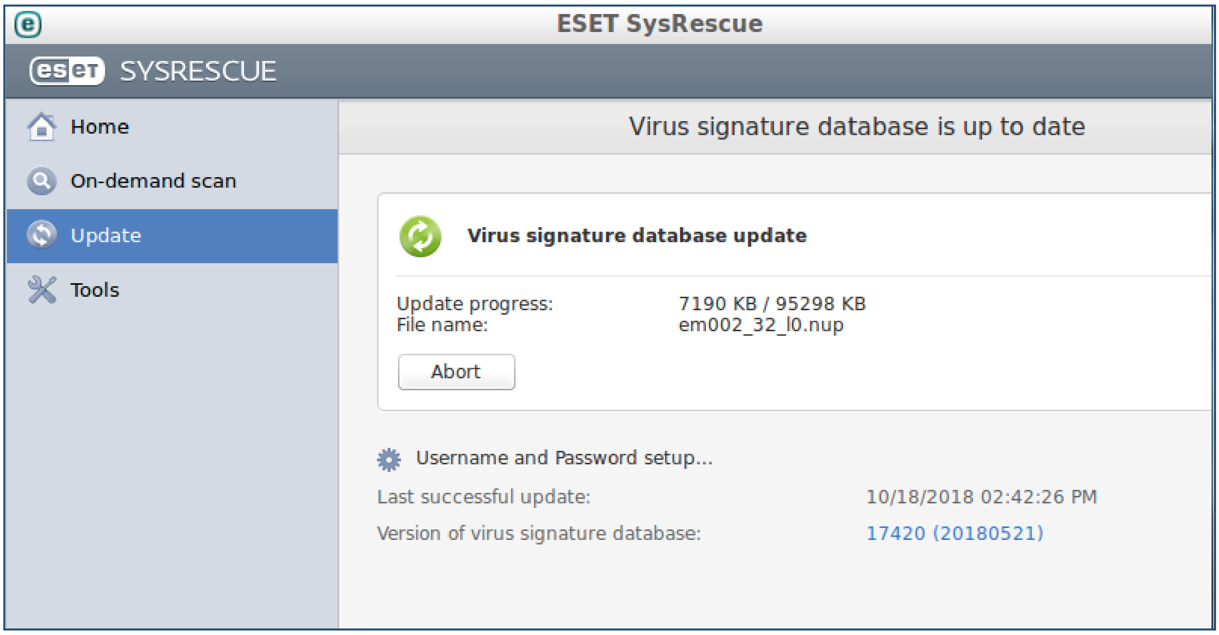
If you are connected to the public network, you may already receive the following message that the virus pattern definitions have been updated successfully:



ESET SysRescue
Virus signature database has been updated to version 18235 (20181018)

In this case you do not have to carry out any further updates, you can continue using the rescue disk directly below.

However, if you have not yet seen such a message, click on `<Update>` in the main menu. If you get the following view, there is a connection to the public network and an update is in progress:



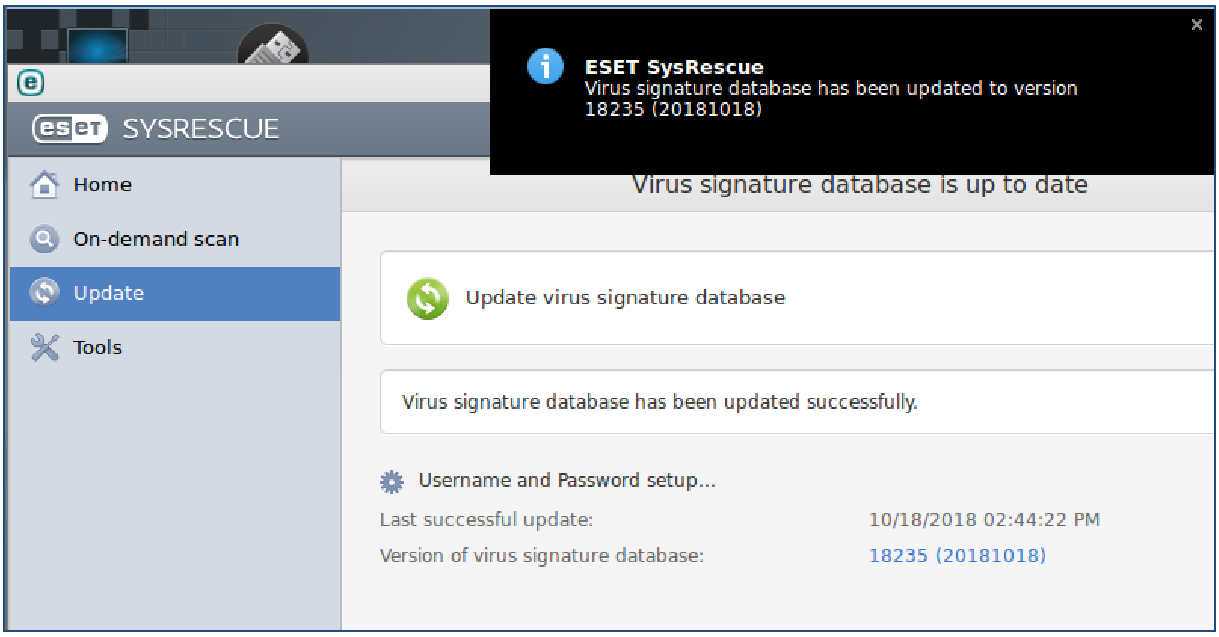
Virus signature database is up to date

Virus signature database update

Update progress: 7190 KB / 95298 KB
File name: em002_32_l0.nup

Last successful update: 10/18/2018 02:42:26 PM
Version of virus signature database: 17420 (20180521)

In this case, you have to wait until the update is completed and the following message appears:



ESET SysRescue
Virus signature database has been updated to version 18235 (20181018)

Virus signature database is up to date

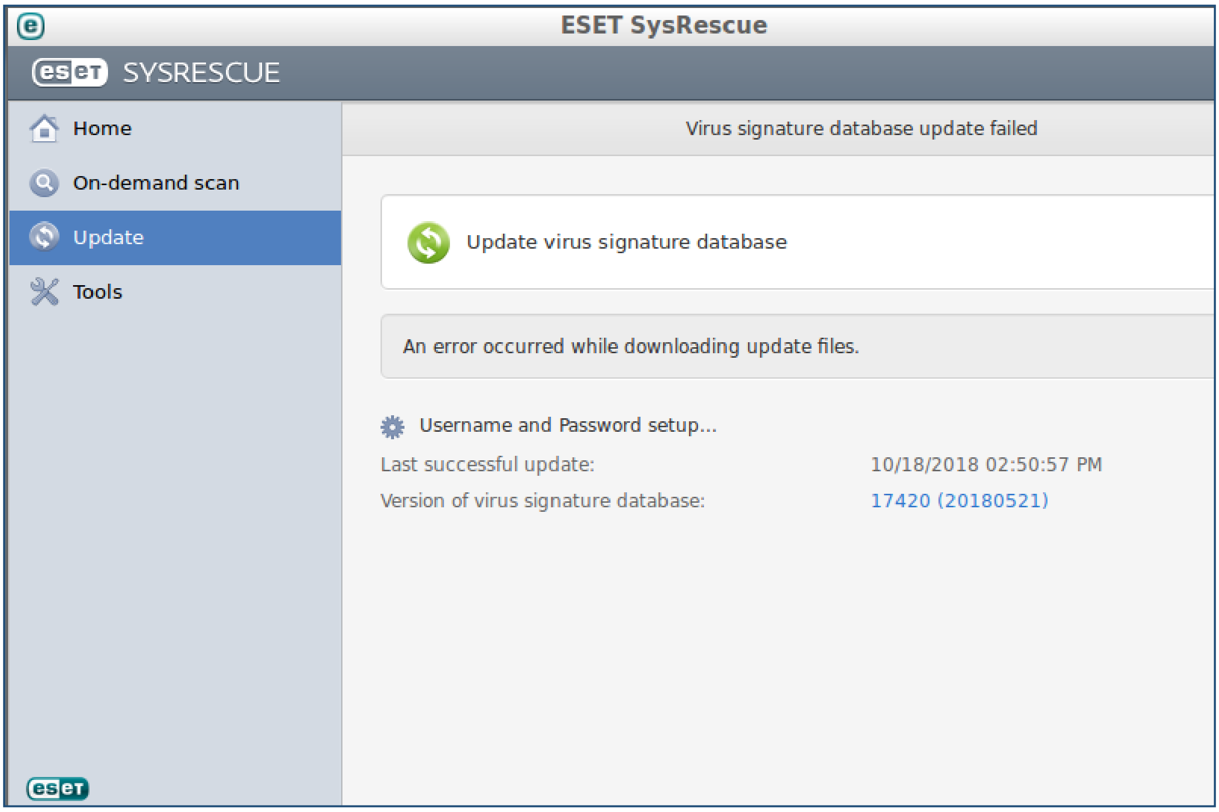
Update virus signature database

Virus signature database has been updated successfully.

Last successful update: 10/18/2018 02:44:22 PM
Version of virus signature database: 18235 (20181018)

You can then continue to use the rescue disk.

If, on the other hand, you receive the message `"An error occured while downloading update files."`, the virus pattern definitions could not be updated successfully.



Virus signature database update failed

Update virus signature database

An error occurred while downloading update files.

Username and Password setup...

Last successful update: 10/18/2018 02:50:57 PM

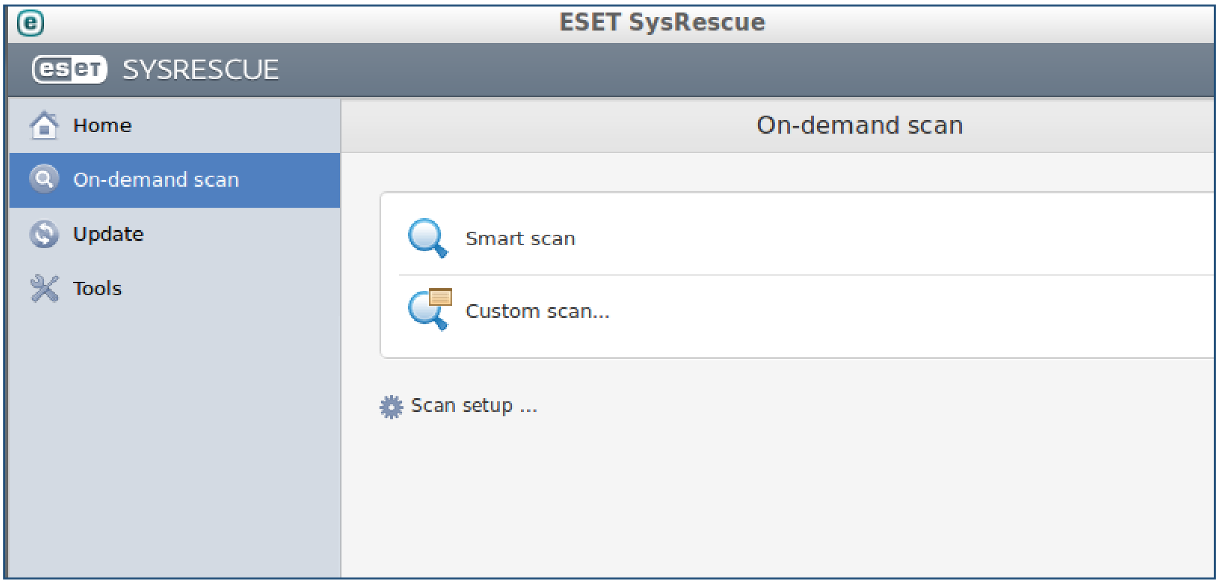
Version of virus signature database: 17420 (20180521)

At the time of the update attempt, there was probably no connection to the public network. Correct the problem and try again by clicking on `<Update virus signature database>`. If necessary, refer to the tips in Chapter 6 - Troubleshooting.

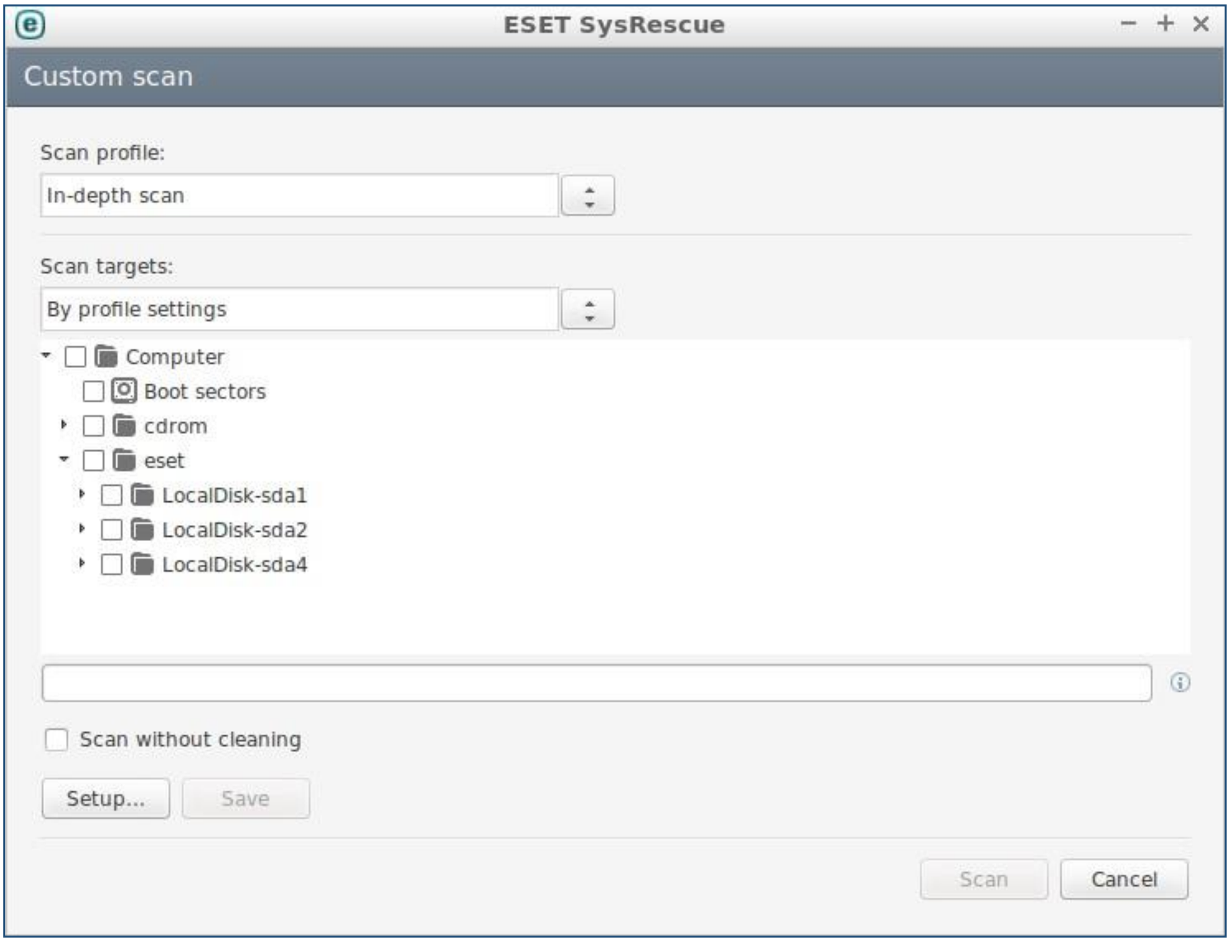
⚠ Advanced users can try to configure the network connection manually by selecting ⌃, then `<Preferences>` and `<Network Connections>` in the main menu.

The rescue disk can also be used without a live update, but the detection of current threats is very limited extent, since the virus pattern definitions are outdated.

After the update, click on `<On-demand scan>` in the main menu.



Click <Custom scan…> to perform a full, high-intensity scan of the system. Alternatively, you can also use <Smart scan> to perform a faster scan, which in return is only carried out at a lower intensity. We therefore recommend the custom scan, to which the following screenshots also refer.



Custom scan

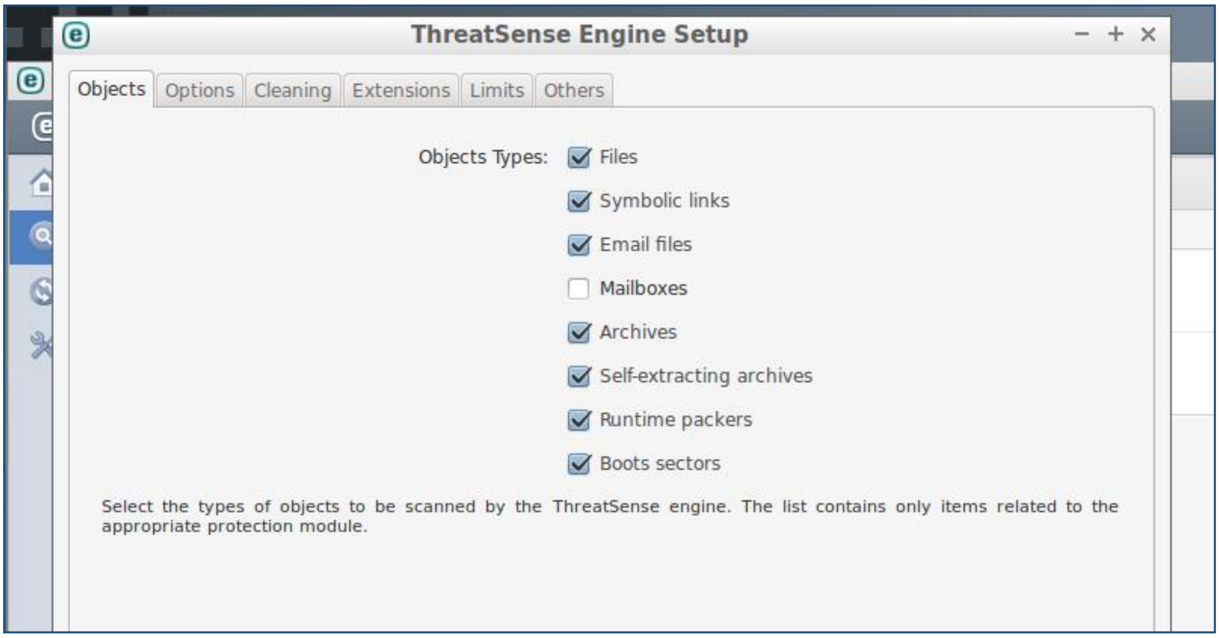
Scan profile: In-depth scan

Scan targets: By profile settings

- □ Computer
  - □ Boot sectors
  - □ cdrom
  - □ eset
    - □ LocalDisk-sda1
    - □ LocalDisk-sda2
    - □ LocalDisk-sda4

□ Scan without cleaning

Make sure that the `<In-depth scan>` option is set in the `<Scan profile:>` field, select it, if necessary. The high-intensity scan is now preset and you do not have to enter any further information. Alternatively, you can also view and change the scan parameters by clicking on `<Setup ...>`:



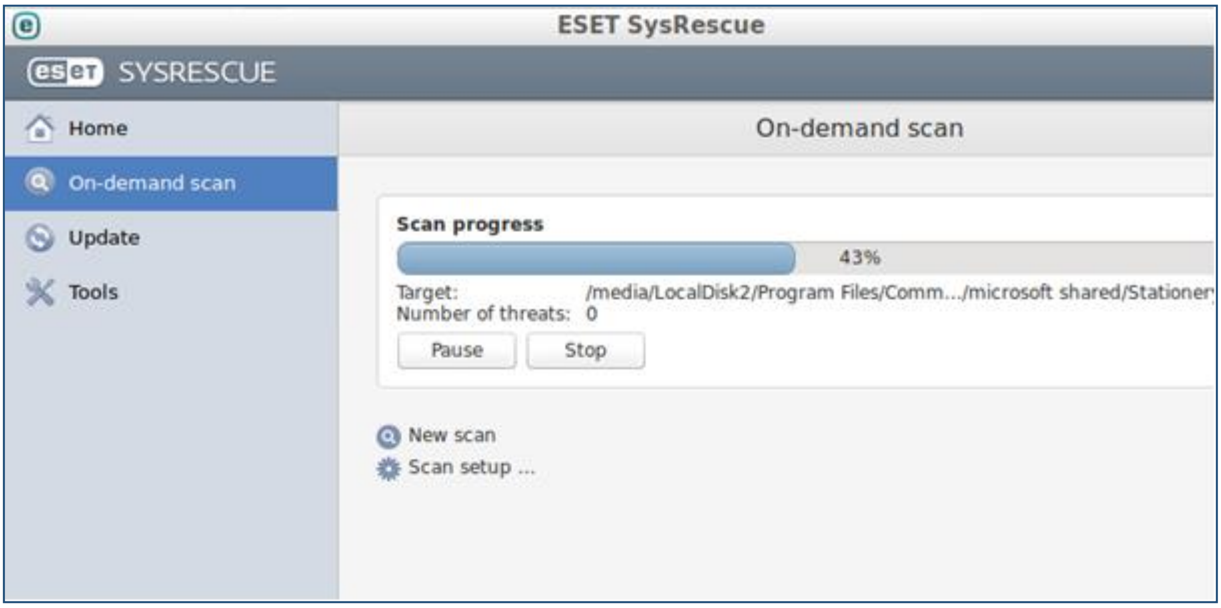
Objects Types:
- ☑ Files
- ☑ Symbolic links
- ☑ Email files
- □ Mailboxes
- ☑ Archives
- ☑ Self-extracting archives
- ☑ Runtime packers
- ☑ Boots sectors

Select the types of objects to be scanned by the ThreatSense engine. The list contains only items related to the appropriate protection module.

Leave this view with `<OK>`, if open. Now select in the previous view all drives (`LocalDisk ...`) that are to be checked from the rescue disk. If you are unsure which drives might be infected, select all drives.

> ⚠ In any case, also activate the check of the boot sectors (`<Boot sectors>`).

After selecting the drive, click `<Scan>`. The examination of the system begins.



Scan progress

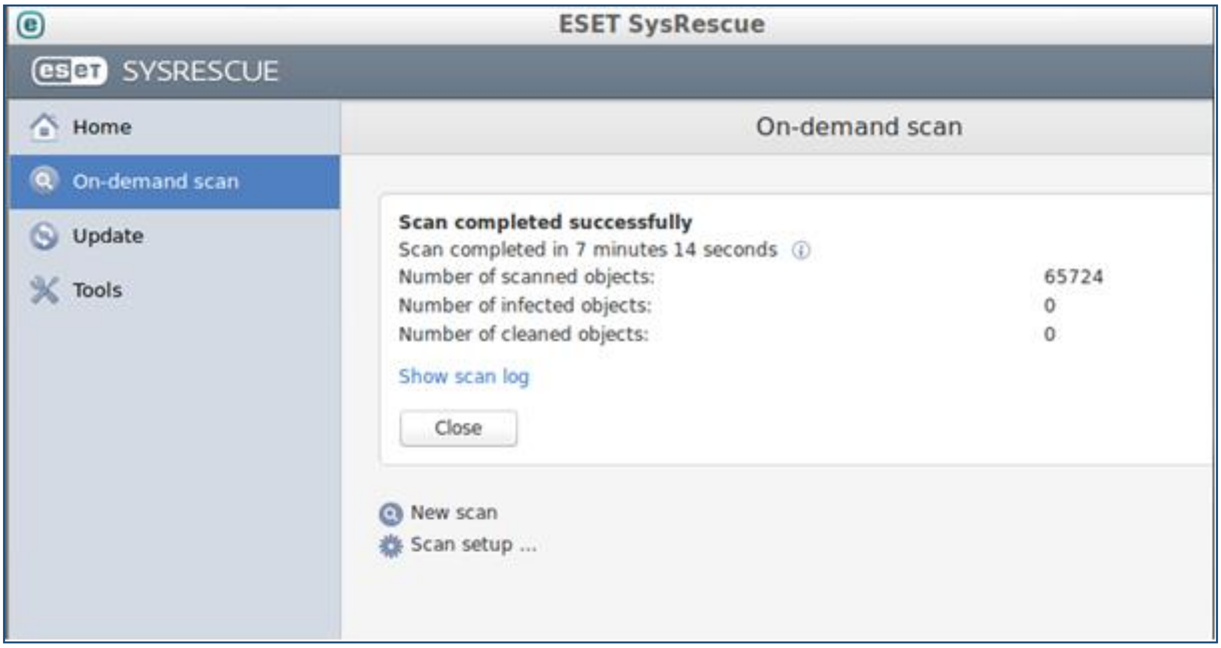
43%

Target: /media/LocalDisk2/Program Files/Comm.../microsoft shared/Stationer

Number of threats: 0

With <Pause> and <Stop> the running scan can be interrupted or stopped. In the Number of threats: field you will find an indication of how many (possible) infections have already been found.

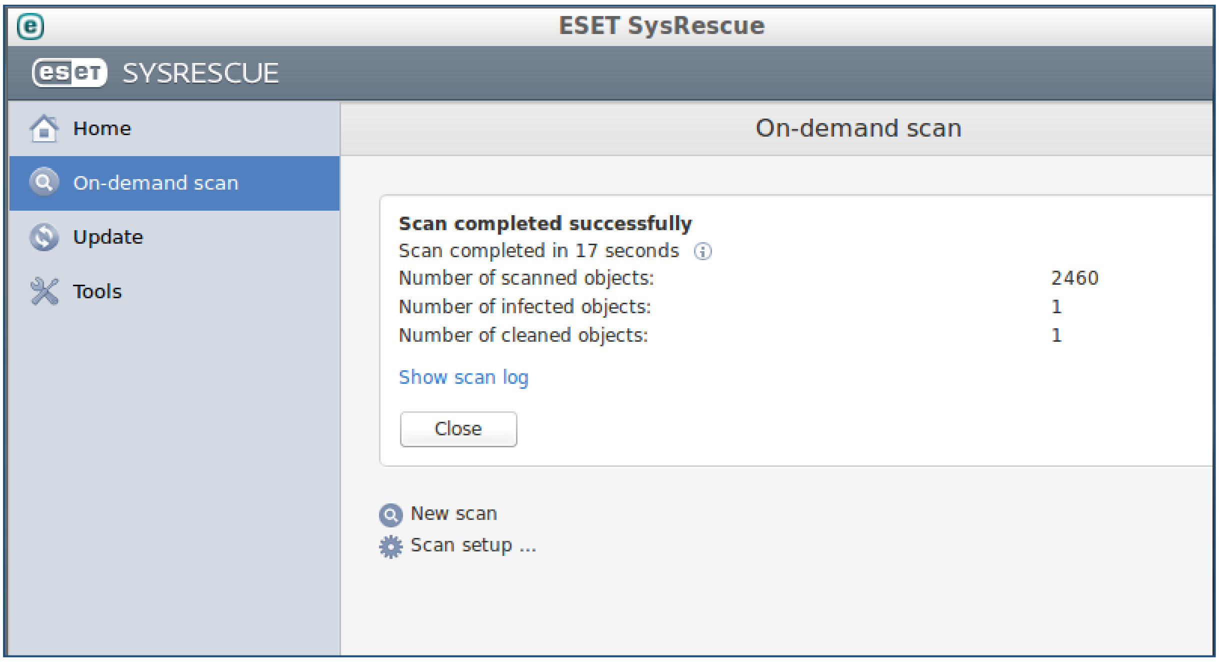
After completing the scan, you will receive a summary. If no threats were found, the number of infected objects and number of cleaned objects are both 0.



Scan completed successfully
Scan completed in 7 minutes 14 seconds

```
Number of scanned objects:     65724
Number of infected objects:    0
Number of cleaned objects:     0
```

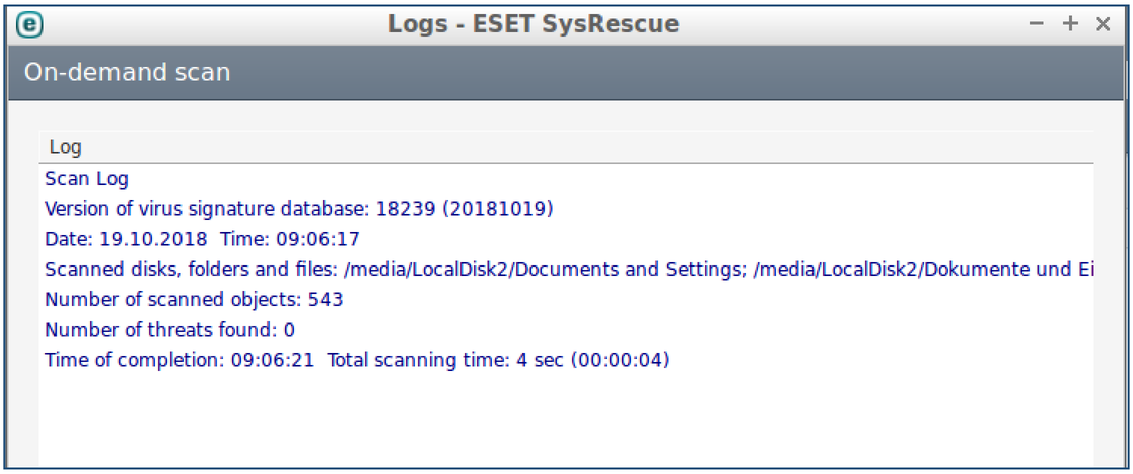
However, if threats were found, these values count accordingly:



Scan completed successfully
Scan completed in 17 seconds

```
Number of scanned objects:     2460
Number of infected objects:    1
Number of cleaned objects:     1
```

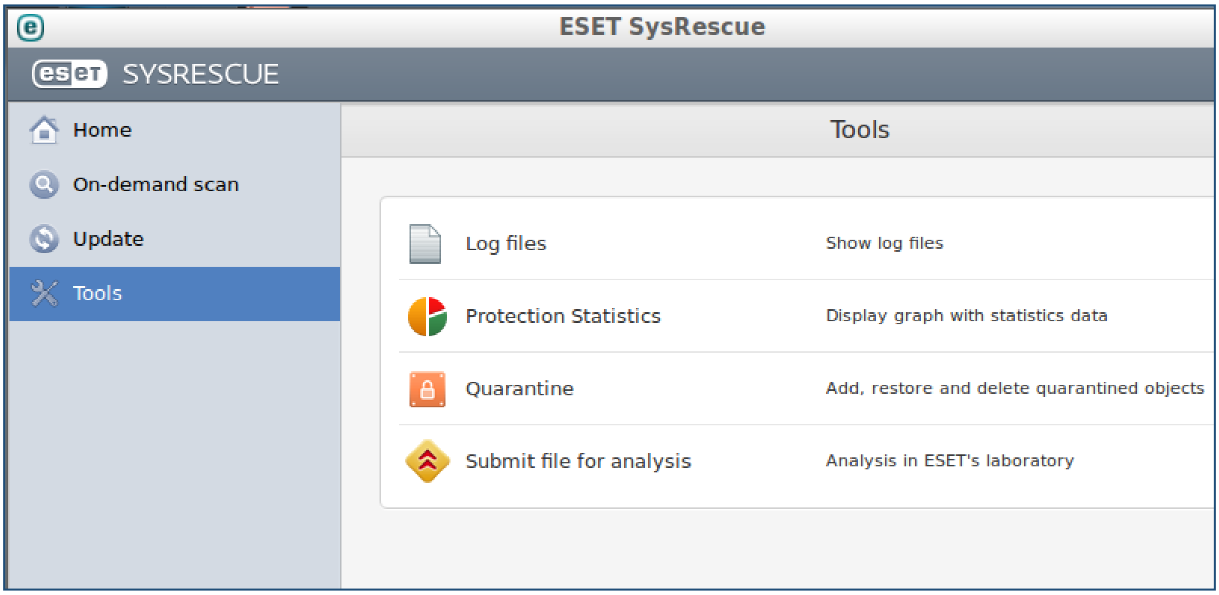
By clicking on <Show scan log>, you can display information about the finds:



```
Scan Log
Version of virus signature database: 18239 (20181019)
Date: 19.10.2018  Time: 09:06:17
Scanned disks, folders and files: /media/LocalDisk2/Documents and Settings; /media/LocalDisk2/Dokumente und Ei
Number of scanned objects: 543
Number of threats found: 0
Time of completion: 09:06:21  Total scanning time: 4 sec (00:00:04)
```

Leave this view with <Close>. In the previous view, you can now change the scan parameters using <Scan setup…> and then initiate a new scan using <New scan>, if necessary.

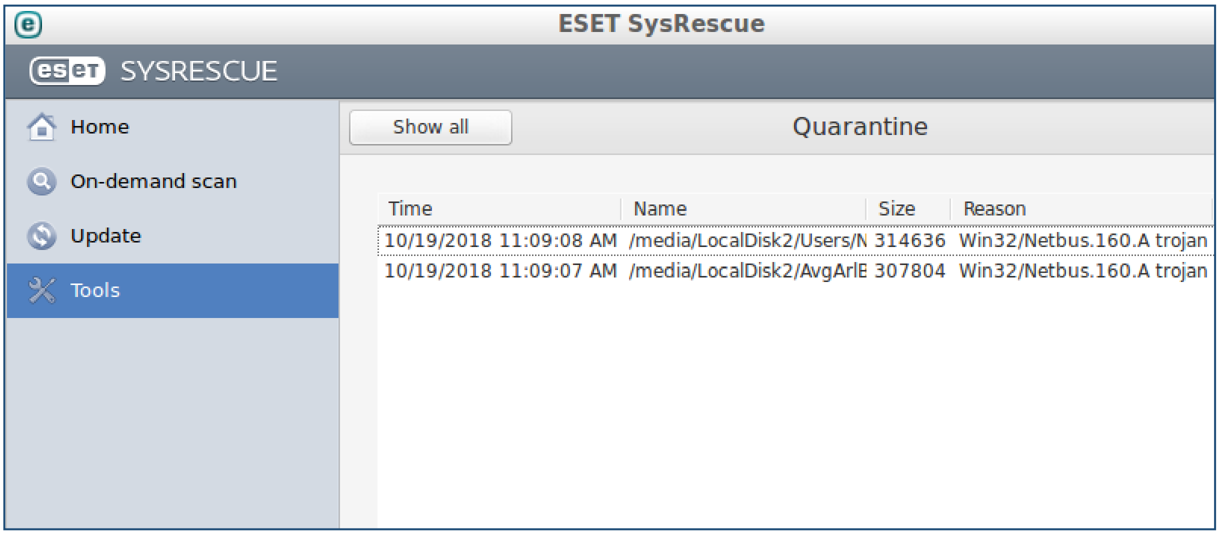
Please be also aware of the available tools in the main menu:



Log files	Show log files
Protection Statistics	Display graph with statistics data
Quarantine	Add, restore and delete quarantined objects
Submit file for analysis	Analysis in ESET's laboratory

<Log files> offers the possibility to display the results of all scans of the current session. <Protection Statistics> shows the scan results in a diagram. With <Submit file for analysis> you can send a suspicious file to ESET for diagnosis; however, this works only, if you have activated the Live Grid Early Warning System when confirming the license agreement.

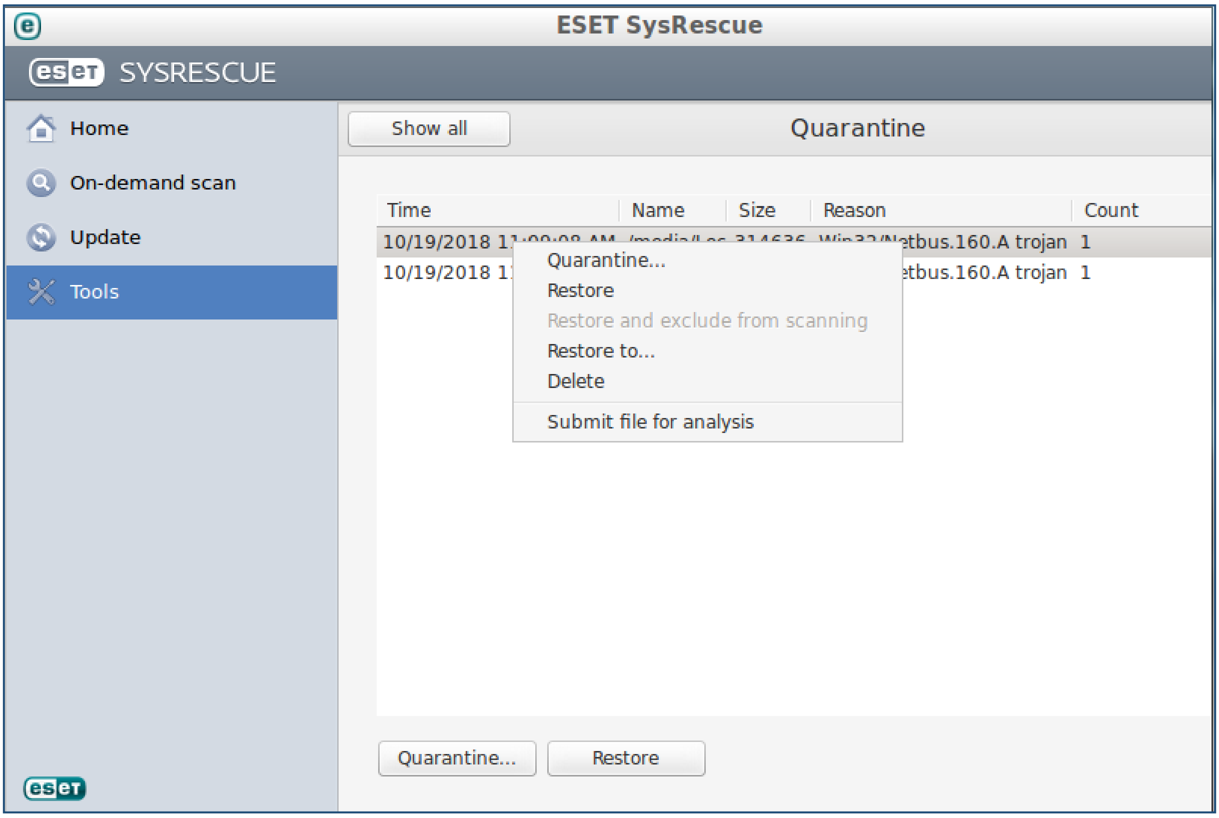
All threats found are first moved to a quarantine folder by ESET SysRescue, you can generate an overview with <Quarantine>:



Time	Name	Size	Reason
10/19/2018 11:09:08 AM	/media/LocalDisk2/Users/N	314636	Win32/Netbus.160.A trojan
10/19/2018 11:09:07 AM	/media/LocalDisk2/AvgArlE	307804	Win32/Netbus.160.A trojan

Two infections were found in the example shown above. In the columns you will find the discovery time (Time), path and file name (Name), the file size (Size), a brief description of the infection (Reason, here a Trojan horse of the type Netbus.160.A) and the number (Count) of discoveries.

You can right-click to open a context menu for each entry in the list:



Time	Name	Size	Reason	Count
10/19/2018 11:09:08 AM	/media/Loc	314636	Win32/Netbus.160.A trojan	1
10/19/2018 1			tbus.160.A trojan	1

With <Quarantine…> you can move the file from the predefined quarantine area to any other directory. With <Delete> you delete the file permanently.

Use <Restore> to restore the suspicious file in its original directory unchanged. Of course, you should only do this if the file can be considered safe. With <Restore to…> the suspicious file is restored in a directory of your choice.

<Submit file for analysis> transfers the file to ESET for further analysis. However, this works only, if you have activated the Live Grid Early Warning System when confirming the license agreement (see above).

After completion of the examination, you can exit the rescue disk by clicking ⏻ and shutdown (<Shutdown>) or reboot (<Reboot>).

4. Using Kaspersky Rescue Disk 2018

A Kaspersky Rescue Disk 2018 ISO image can be found on PCSRV at

`\\pcsrv.zam.kfa-juelich.de\public\Notfall-CDs\02-Kaspersky-Rescue-Disk-2018`

This image is updated regularly (which, however, does not replace the daily updates of the virus signatures).

Start the affected system with Kaspersky Rescue Disk by creating a bootable USB stick from the ISO image. Use suitable third-party software for this purpose; The ESET image was successfully tested e.g. with Rufus Portable and UNetbootin. Note that the previous contents of the USB stick will be deleted.

Download Rufus Portable:

`https://rufus.ie/de/`

Download UNetbootin:

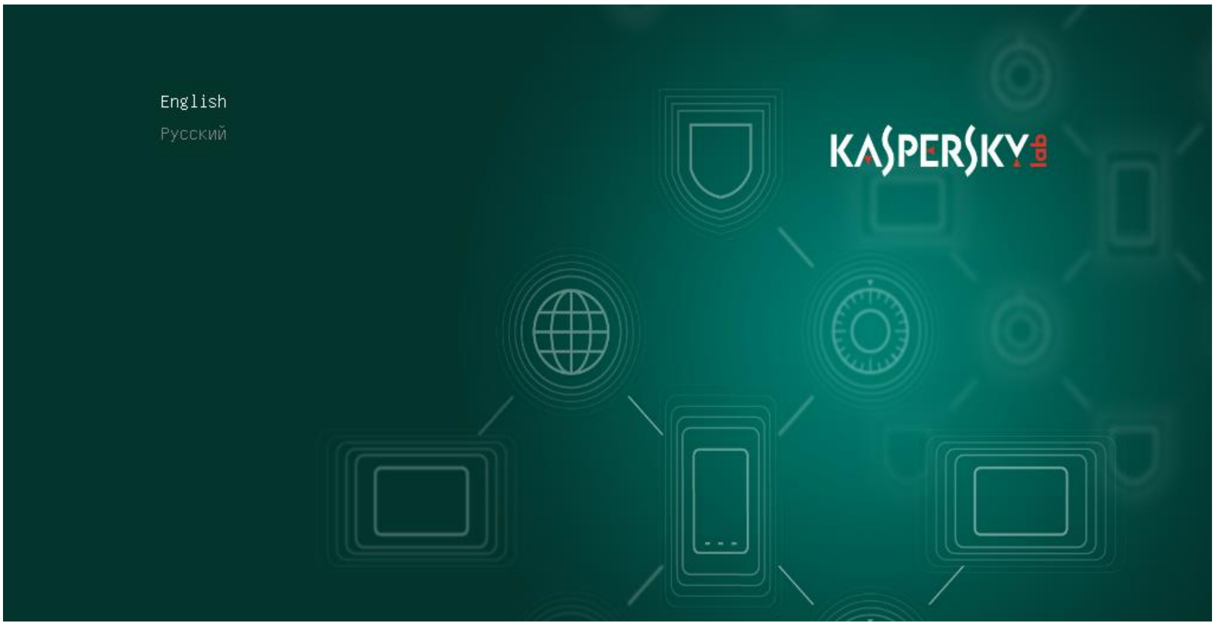
`https://unetbootin.github.io/`

Alternatively, you can burn the ISO image as a CD / DVD and restart the affected system from this. To do so, use the software available at your institute or the <`Burn disc image`> function integrated in Windows 10.

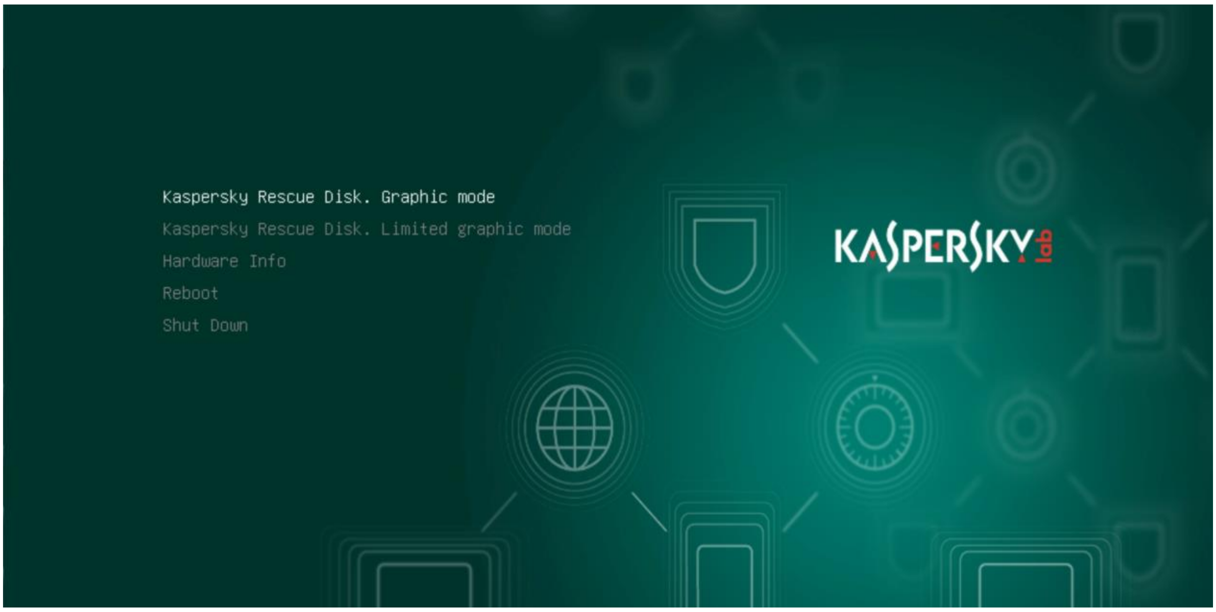
If you would like more detailed information on creating the USB stick, you can find it here:

`https://support.kaspersky.com/14226`

In the first screen you can select the desired language with the <⬇> and <⬆> keys and confirm with <`Return`>.



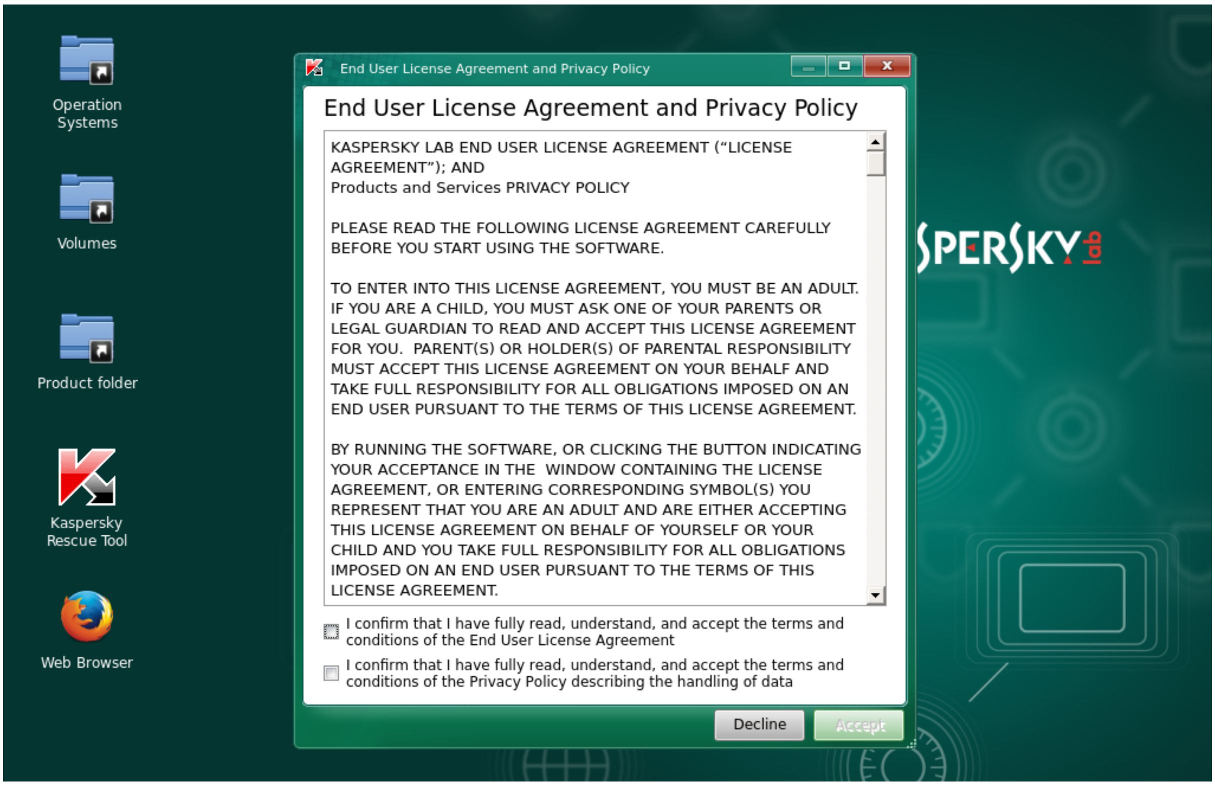
Start the actual Rescue Disk by confirming `<Kaspersky Rescue Disk. Graphic Mode>`.


Kaspersky Rescue Disk. Graphic mode
Kaspersky Rescue Disk. Limited graphic mode
Hardware Info
Reboot
Shut Down
KASPERSKY lab

⚠ If problems should arise in graphic mode, try restarting the rescue disk in `<Limited graphic mode>`. The operation of the rescue disk is identical in both cases.

The rescue disk is now booted, which can be associated with a waiting time of a few minutes, especially on virtual machines.

The Rescue Disk 2018 user interface appears and the license conditions are displayed.



End User License Agreement and Privacy Policy

KASPERSKY LAB END USER LICENSE AGREEMENT (“LICENSE AGREEMENT”); AND
Products and Services PRIVACY POLICY

PLEASE READ THE FOLLOWING LICENSE AGREEMENT CAREFULLY BEFORE YOU START USING THE SOFTWARE.

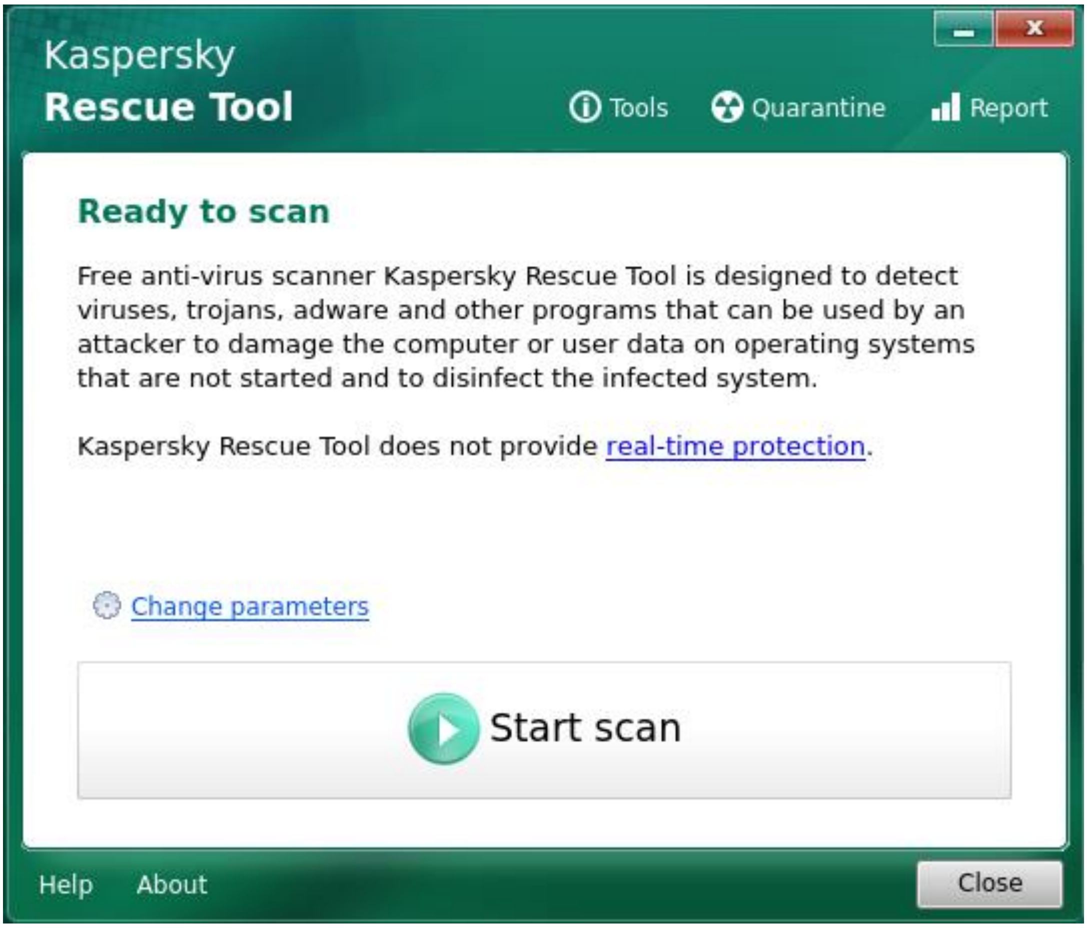
TO ENTER INTO THIS LICENSE AGREEMENT, YOU MUST BE AN ADULT. IF YOU ARE A CHILD, YOU MUST ASK ONE OF YOUR PARENTS OR LEGAL GUARDIAN TO READ AND ACCEPT THIS LICENSE AGREEMENT FOR YOU. PARENT(S) OR HOLDER(S) OF PARENTAL RESPONSIBILITY MUST ACCEPT THIS LICENSE AGREEMENT ON YOUR BEHALF AND TAKE FULL RESPONSIBILITY FOR ALL OBLIGATIONS IMPOSED ON AN END USER PURSUANT TO THE TERMS OF THIS LICENSE AGREEMENT.

BY RUNNING THE SOFTWARE, OR CLICKING THE BUTTON INDICATING YOUR ACCEPTANCE IN THE WINDOW CONTAINING THE LICENSE AGREEMENT, OR ENTERING CORRESPONDING SYMBOL(S) YOU REPRESENT THAT YOU ARE AN ADULT AND ARE EITHER ACCEPTING THIS LICENSE AGREEMENT ON BEHALF OF YOURSELF OR YOUR CHILD AND YOU TAKE FULL RESPONSIBILITY FOR ALL OBLIGATIONS IMPOSED ON AN END USER PURSUANT TO THE TERMS OF THIS LICENSE AGREEMENT.

□ I confirm that I have fully read, understand, and accept the terms and conditions of the End User License Agreement

□ I confirm that I have fully read, understand, and accept the terms and conditions of the Privacy Policy describing the handling of data

Activate both checkboxes in the lower area and click on <`Accept`>. The Kaspersky Rescue Tool window appears.

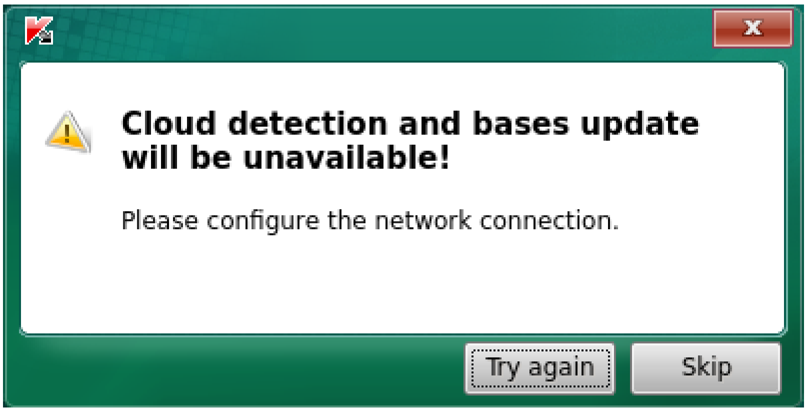


Ready to scan

Free anti-virus scanner Kaspersky Rescue Tool is designed to detect viruses, trojans, adware and other programs that can be used by an attacker to damage the computer or user data on operating systems that are not started and to disinfect the infected system.

Kaspersky Rescue Tool does not provide real-time protection.

If, however, the following message appears, there is no connection to the public network, which is why the virus pattern definitions could not be updated.

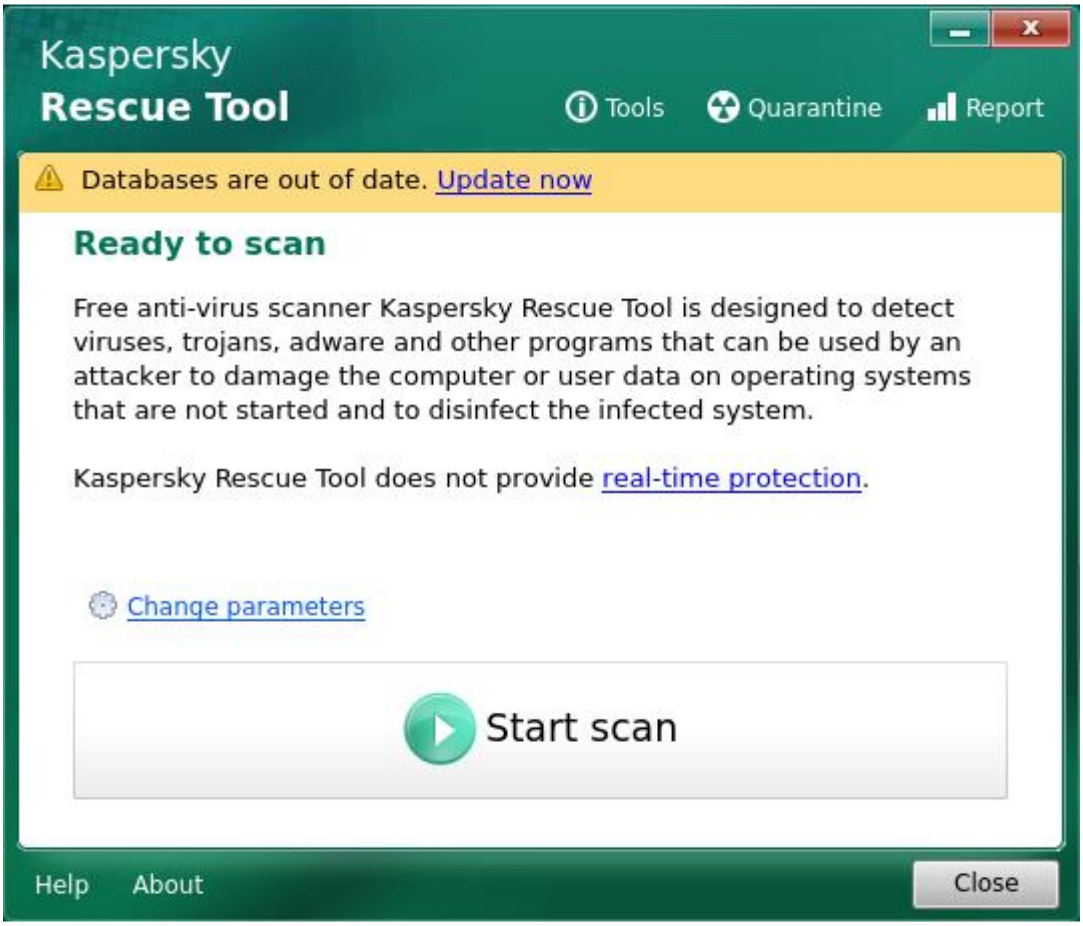


Cloud detection and bases update will be unavailable!

Please configure the network connection.

⚠ If the update process was not completed correctly, refer to Chapter 6-Troubleshooting and restart the rescue disk so that the network detection is carried out again.
Advanced users can try manual configuration using the on-board tools in the user interface.

Depending on the age of the virus pattern definitions, you will receive a yellow message in the main window of the Kaspersky Rescue Tool, alerting you that the virus database is no longer up to date:



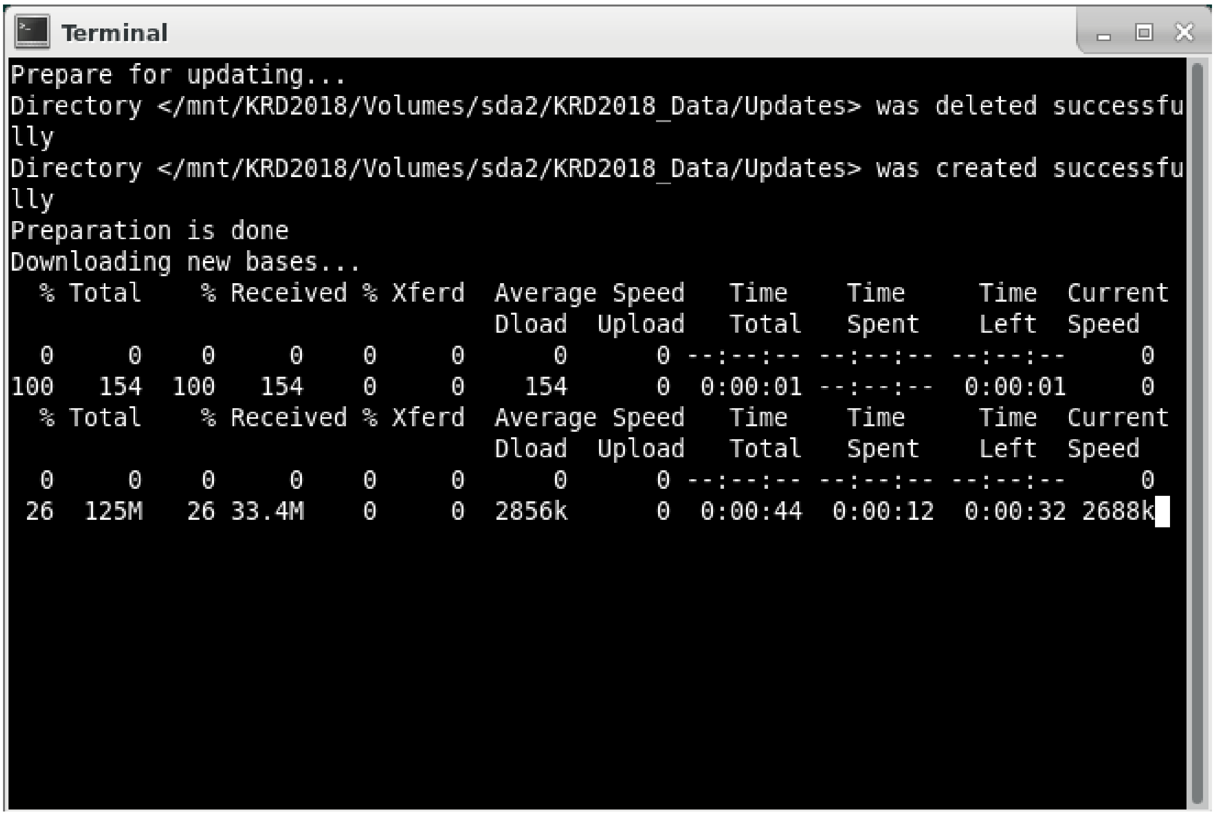
Databases are out of date. Update now

Ready to scan

Free anti-virus scanner Kaspersky Rescue Tool is designed to detect viruses, trojans, adware and other programs that can be used by an attacker to damage the computer or user data on operating systems that are not started and to disinfect the infected system.

Kaspersky Rescue Tool does not provide real-time protection.

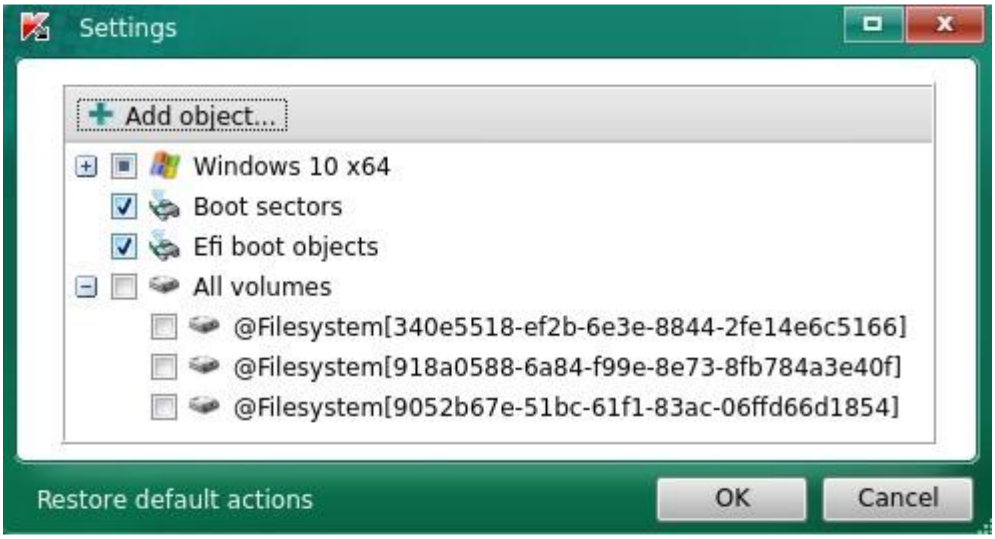
In this case, click on <`Update now`> (if you have not received such a message, just skip this step). An online update of the virus pattern definitions is carried out, which of course can only work with an active connection to the public network, see above. A terminal window with the current status appears during the update process:



```
Prepare for updating...
Directory </mnt/KRD2018/Volumes/sda2/KRD2018_Data/Updates> was deleted successfu
lly
Directory </mnt/KRD2018/Volumes/sda2/KRD2018_Data/Updates> was created successfu
lly
Preparation is done
Downloading new bases...
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
100   154  100   154    0     0    154      0  0:00:01 --:--:--  0:00:01     0
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
 26  125M   26 33.4M    0     0  2856k      0  0:00:44  0:00:12  0:00:32 2688k
```

After successful completion, the rescue disk returns to the main view, you may have to confirm the license agreement again.

Select <`Change parameters`> in the main view. In the next dialog, expand all entries using the <**+**> buttons.



- [+] ■ Windows 10 x64
  - ☑ Boot sectors
  - ☑ Efi boot objects
- [−] □ All volumes
  - □ @Filesystem[340e5518-ef2b-6e3e-8844-2fe14e6c5166]
  - □ @Filesystem[918a0588-6a84-f99e-8e73-8fb784a3e40f]
  - □ @Filesystem[9052b67e-51bc-61f1-83ac-06ffd66d1854]

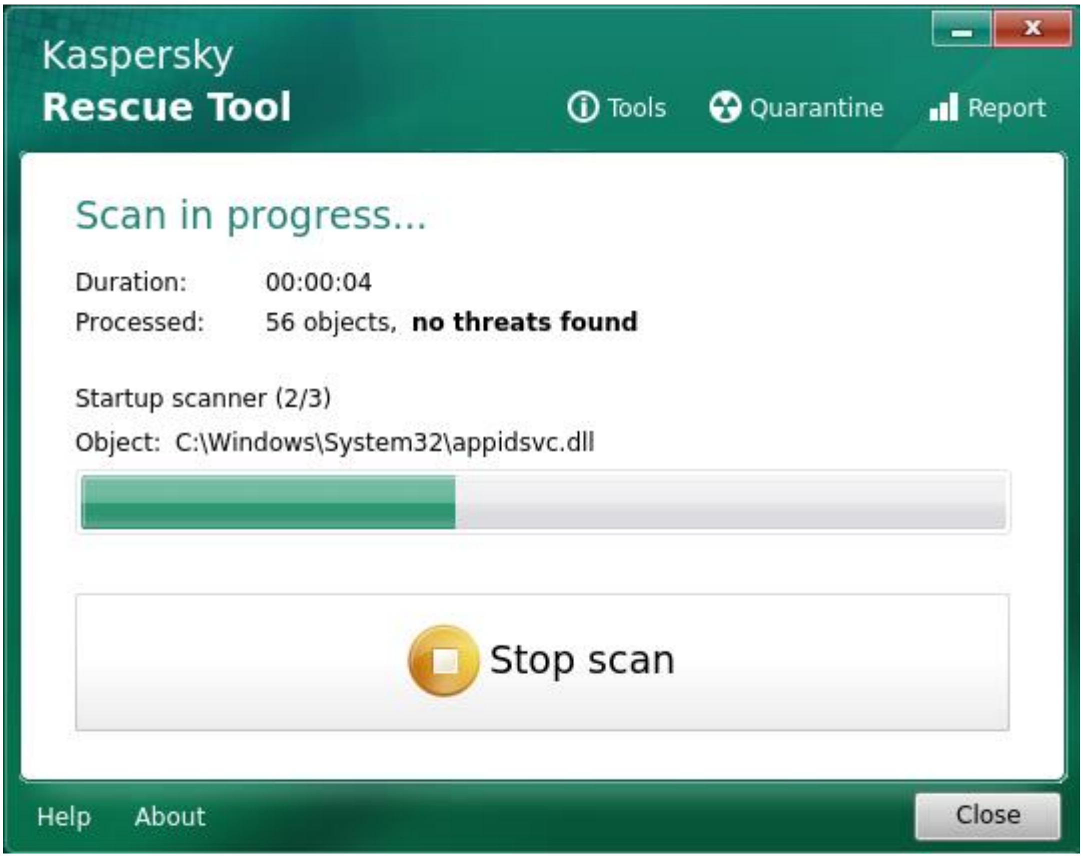
In the example shown above, the rescue disk recognizes a Windows 10 installation ("Windows 10 x64") and three drives or partitions.

You can now select which objects are to be examined: main memory (fileless objects), autostart objects (startup objects), the system drive (system drive) and boot sectors (boot sectors, Efi boot objects). In the lower area you can also select and deselect entire hard disks or partitions. Depending on the system configuration, not all of the items shown here may be listed.

Select all entries or partitions that could be infected and should be checked. If you are not sure which ones to choose, select all the entries listed.

⚠ Bootable partitions should definitely be included. Also select the entries <Boot sectors> and <Efi boot objects>.

Confirm your selection with <OK>. Back in the main view of the Kaspersky Rescue Tool, you can now start the actual examination with <Start Scan>. During the exam, the screen looks like this:



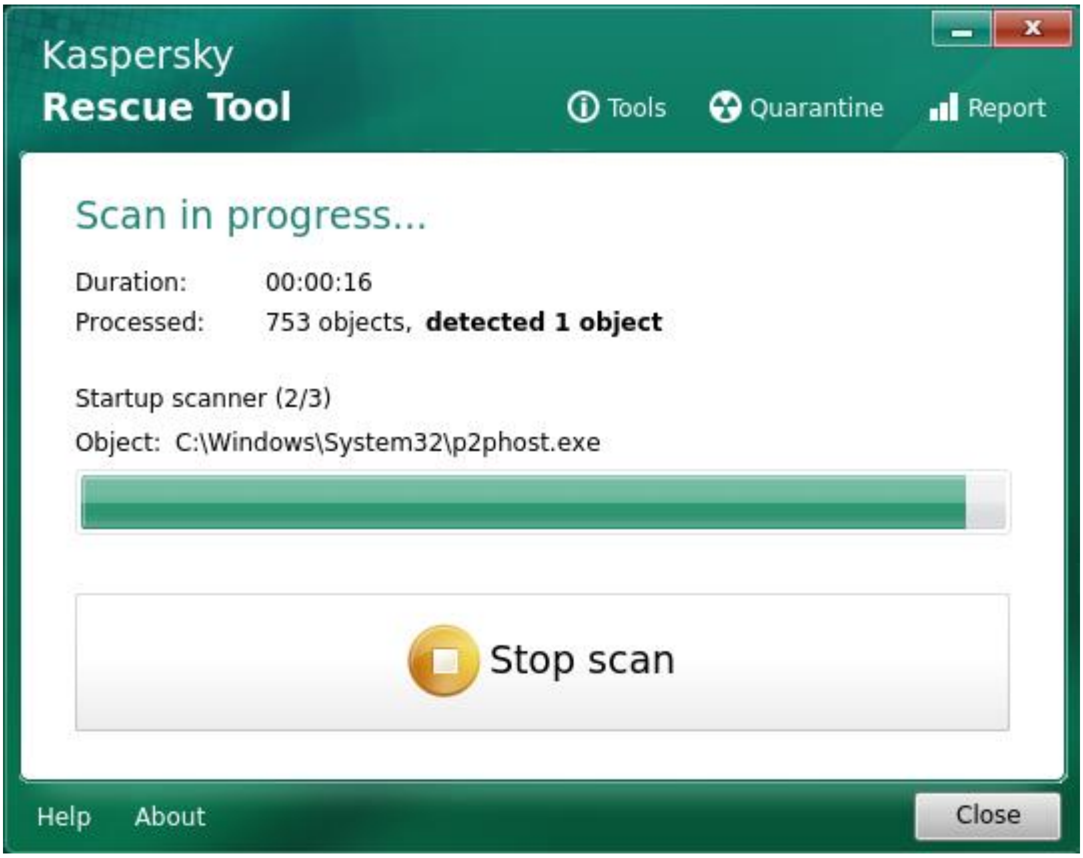
Scan in progress...

Duration: 00:00:04
Processed: 56 objects, **no threats found**

Startup scanner (2/3)
Object: C:\Windows\System32\appidsvc.dll

With <Stop scan> the examination can be ended prematurely.

The note no threats found indicates that no suspicious files have been found so far; otherwise the message detected 1 object (or higher) can be found here.



Scan in progress...

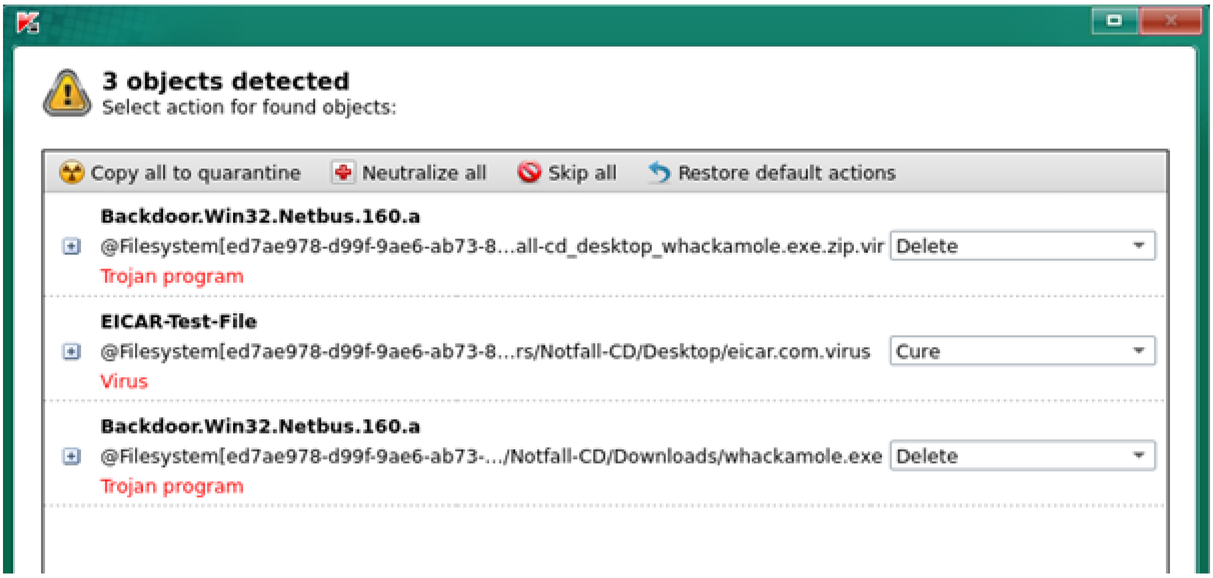
Duration: 00:00:16

Processed: 753 objects, **detected 1 object**

Startup scanner (2/3)

Object: C:\Windows\System32\p2phost.exe

After the investigation has completed, a summary will be displayed if suspicious items have been found. If none have been found, the Kaspersky Rescue Tool returns to the main view without further notification.



3 objects detected

Select action for found objects:

Backdoor.Win32.Netbus.160.a
@Filesystem[ed7ae978-d99f-9ae6-ab73-8...all-cd_desktop_whackamole.exe.zip.vir Delete
Trojan program

EICAR-Test-File
@Filesystem[ed7ae978-d99f-9ae6-ab73-8...rs/Notfall-CD/Desktop/eicar.com.virus Cure
Virus

Backdoor.Win32.Netbus.160.a
@Filesystem[ed7ae978-d99f-9ae6-ab73-.../Notfall-CD/Downloads/whackamole.exe Delete
Trojan program

In the example shown, three infections have been found. The generated output displays the name of the malware, e.g. `Backdoor.Win32.Netbus.160.a`, followed by the file name and path and the malware type, e.g. Trojan horse.

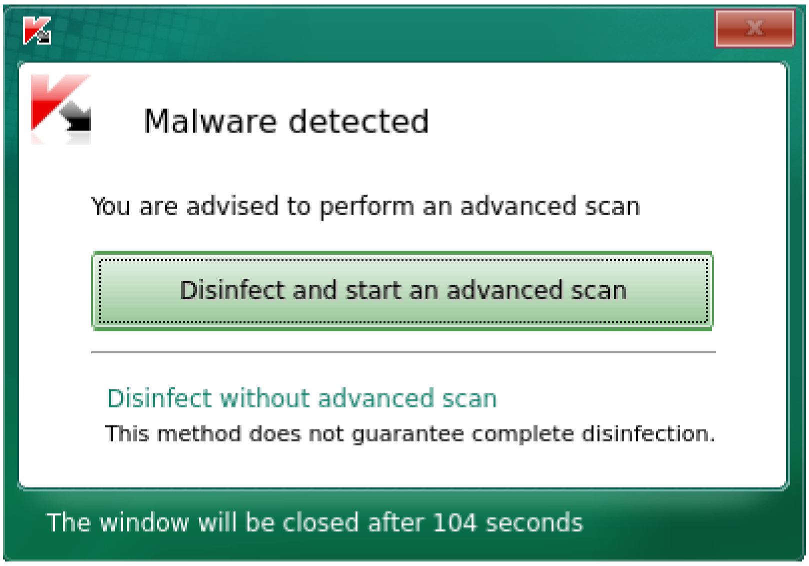
In the selection field behind each list entry, the Rescue Tool suggests an action on how to deal with the infection. The following actions are possible:

<`Skip`>: Ignore, no further action.
<`Cure`>: The Rescue Tool tries to remove the infection from the file, keeping it intact.
<`Delete`>: The infected file is deleted.
<`Copy to quarantine`>: The infected file is moved to a quarantine area so that it is no longer activated at future system starts.

The user can now set an individual action for each list entry. Otherwise, the buttons in the upper area can also be used to select a uniform action for all list entries: <`Copy all to quarantine`> for the quarantine area, <`Neutralize all`> for healing / deletion (depending on whether healing is possible) and <`Skip all` > to ignore. The actions proposed by the Rescue Tool can be restored using <`Restore default actions`>.

Confirm your selection with <`Continue`>.

Depending on the threats found, the rescue disk suggests performing a more intensive, significantly more time-consuming scan, what is recommended. To do this, select <`Disinfect and start an advanced scan`>; if you do not want to do this, you can skip this step with <`Disinfect without advanced scan`>.



Malware detected

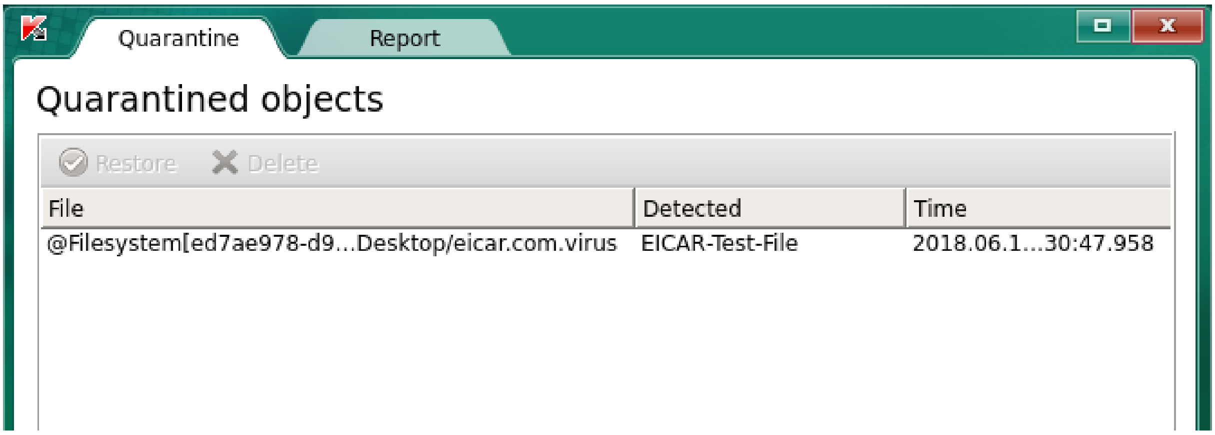
You are advised to perform an advanced scan

Disinfect and start an advanced scan
Disinfect without advanced scan

This method does not guarantee complete disinfection.

The window will be closed after 104 seconds

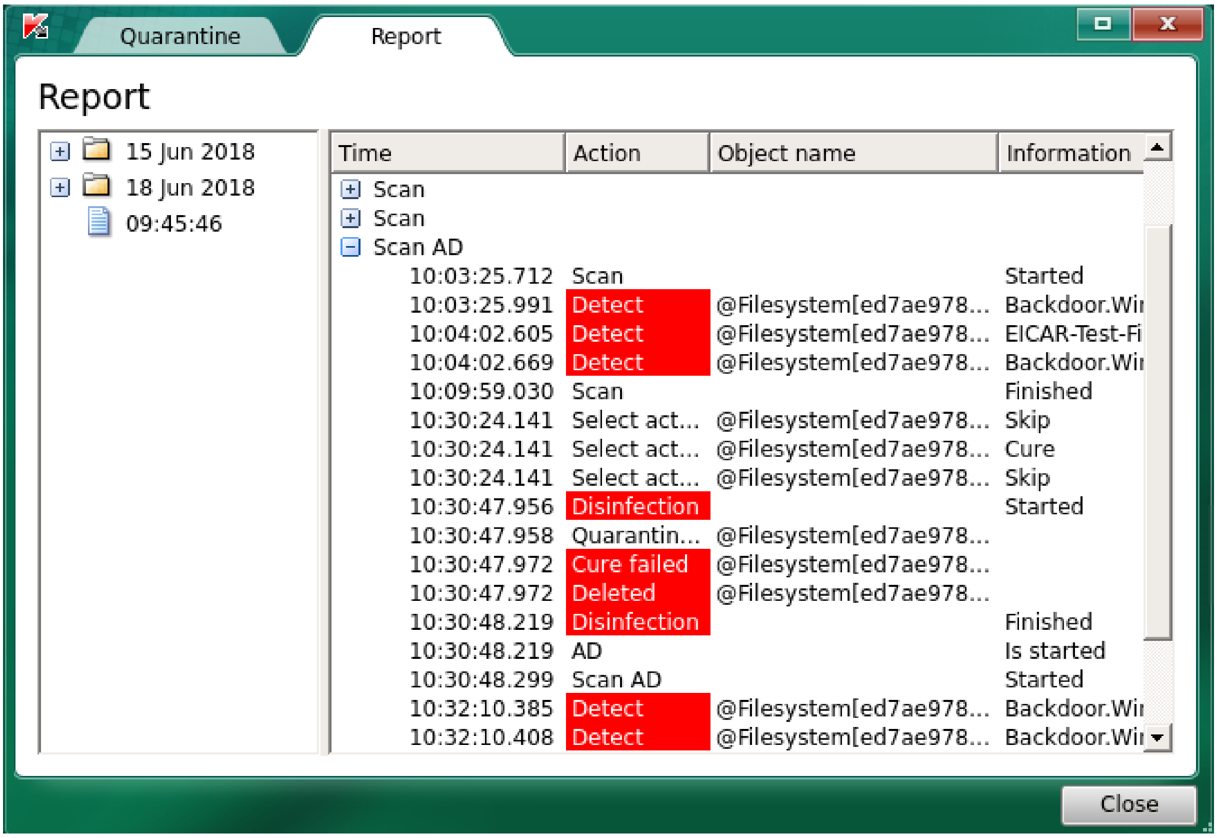
After the selected actions have been carried out, the rescue disk returns to the main view. By clicking on <Quarantine> you will get an overview of the files in the quarantine area:



Quarantined objects

File	Detected	Time
@Filesystem[ed7ae978-d9...Desktop/eicar.com.virus	EICAR-Test-File	2018.06.1...30:47.958

By clicking on <Report> you can generate an overview of all scan processes. chosing the <+> button further information can be displayed. Now you can see which actions the rescue disk has carried out and whether they have been successful.



Report

- 15 Jun 2018
- 18 Jun 2018
- 09:45:46

Time	Action	Object name	Information
Scan			
Scan			
Scan AD			
10:03:25.712	Scan		Started
10:03:25.991	Detect	@Filesystem[ed7ae978...	Backdoor.Wi
10:04:02.605	Detect	@Filesystem[ed7ae978...	EICAR-Test-Fi
10:04:02.669	Detect	@Filesystem[ed7ae978...	Backdoor.Wi
10:09:59.030	Scan		Finished
10:30:24.141	Select act...	@Filesystem[ed7ae978...	Skip
10:30:24.141	Select act...	@Filesystem[ed7ae978...	Cure
10:30:24.141	Select act...	@Filesystem[ed7ae978...	Skip
10:30:47.956	Disinfection		Started
10:30:47.958	Quarantin...	@Filesystem[ed7ae978...	
10:30:47.972	Cure failed	@Filesystem[ed7ae978...	
10:30:47.972	Deleted	@Filesystem[ed7ae978...	
10:30:48.219	Disinfection		Finished
10:30:48.219	AD		Is started
10:30:48.299	Scan AD		Started
10:32:10.385	Detect	@Filesystem[ed7ae978...	Backdoor.Wi
10:32:10.408	Detect	@Filesystem[ed7ae978...	Backdoor.Wi

In the example above, at the time index 10:30:47.972 failed to attempt a healing, leading to deletion of the infected file.

To stop using the rescue disk, click and select <Leave>. Then choose between <Restart> and <Shut Down> for switching off the machine.

5. Using Avira Antivir Rescue System 18

An Avira Antivir Rescue System ISO image can be found on PCSRV at

\\pcsrv.zam.kfa-juelich.de\public\Notfall-CDs\03-Avira-Antivir

This image is updated regularly (which, however, does not replace the daily updates of the virus signatures).

⚠ Depending on the hardware configuration, Avira Antivir can only run on EFI / UEFI systems if you deactivate `<Secure Boot>` in the system setup and set the UEFI mode to `<Legacy>` or `<Legacy only>`.

Start the affected system with Kaspersky Rescue Disk by creating a bootable USB stick from the ISO image. Use suitable third-party software for this purpose; The ESET image was successfully tested e.g. with Rufus Portable and UNetbootin. Note that the previous contents of the USB stick will be deleted.

Download Rufus Portable:

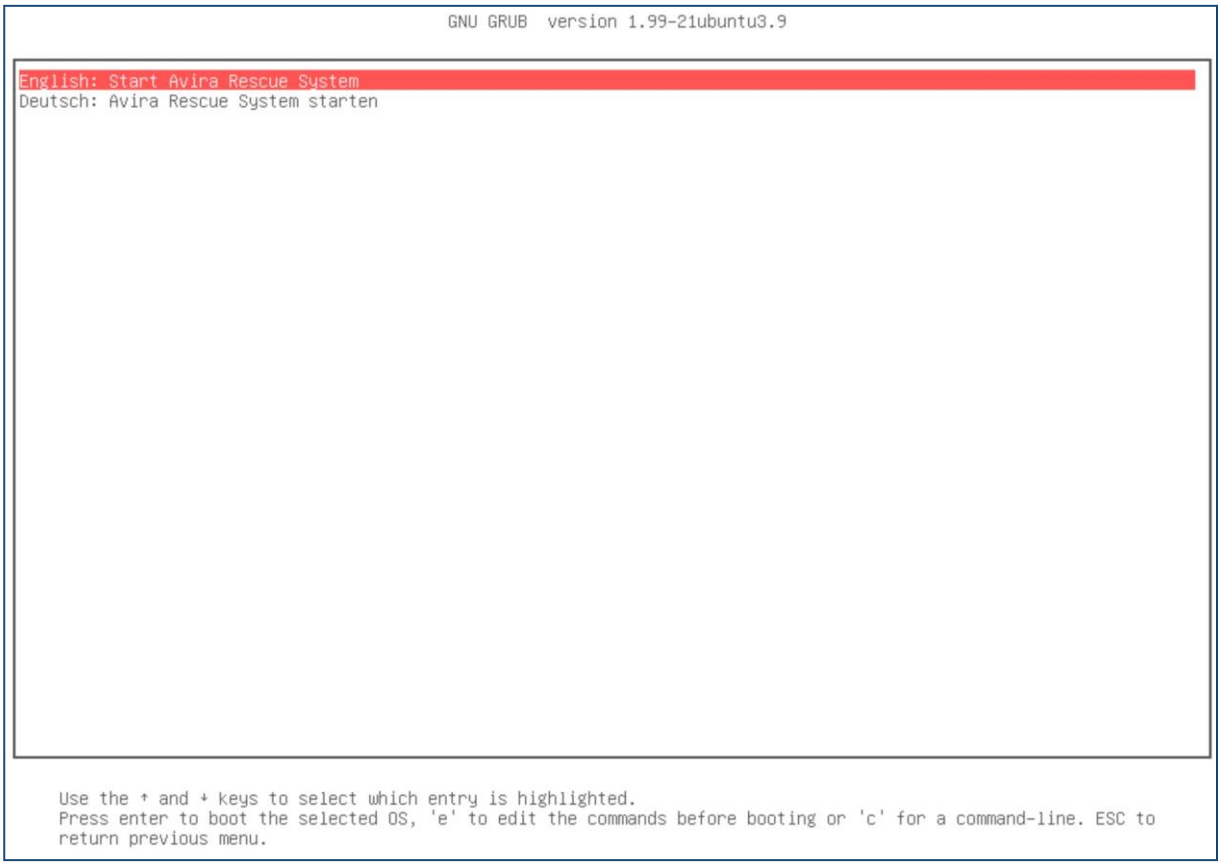
https://rufus.ie/de/

Download UNetbootin:

https://unetbootin.github.io/

⚠ Alternatively, you can burn the ISO image as a CD / DVD and restart the affected system from this. To do so, use the software available at your institute or the `<Burn disc image>` function integrated in Windows 10.

First the boot screen of the Avira Rescue System appears. Select the desired language with the <↑> and <↓> keys and confirm with `<Return>`.

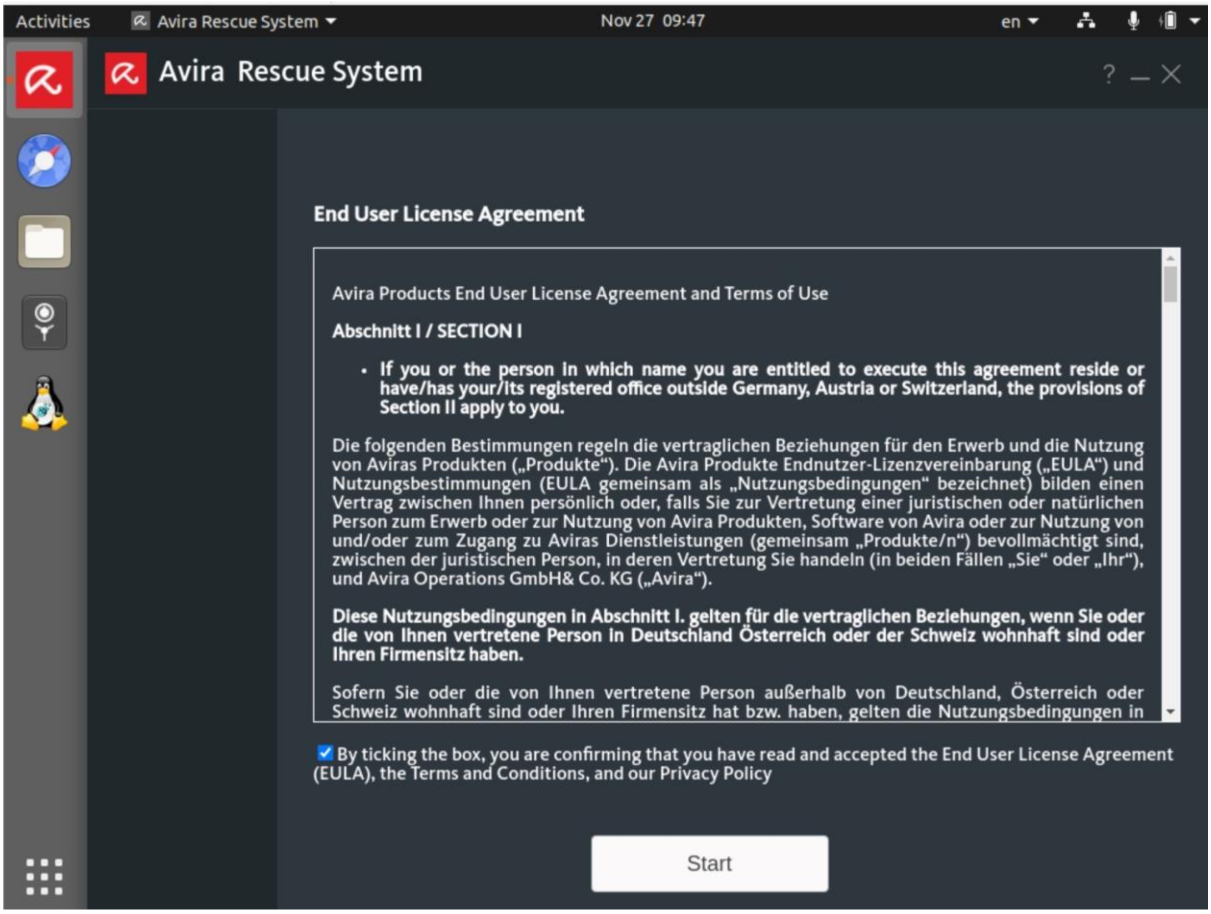


```
                         GNU GRUB  version 1.99-21ubuntu3.9

English: Start Avira Rescue System
Deutsch: Avira Rescue System starten

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the commands before booting or 'c' for a command-line. ESC to
    return previous menu.
```

After the boot process, the license agreement is displayed first.



End User License Agreement

Avira Products End User License Agreement and Terms of Use

Abschnitt I / SECTION I

- **If you or the person in which name you are entitled to execute this agreement reside or have/has your/its registered office outside Germany, Austria or Switzerland, the provisions of Section II apply to you.**

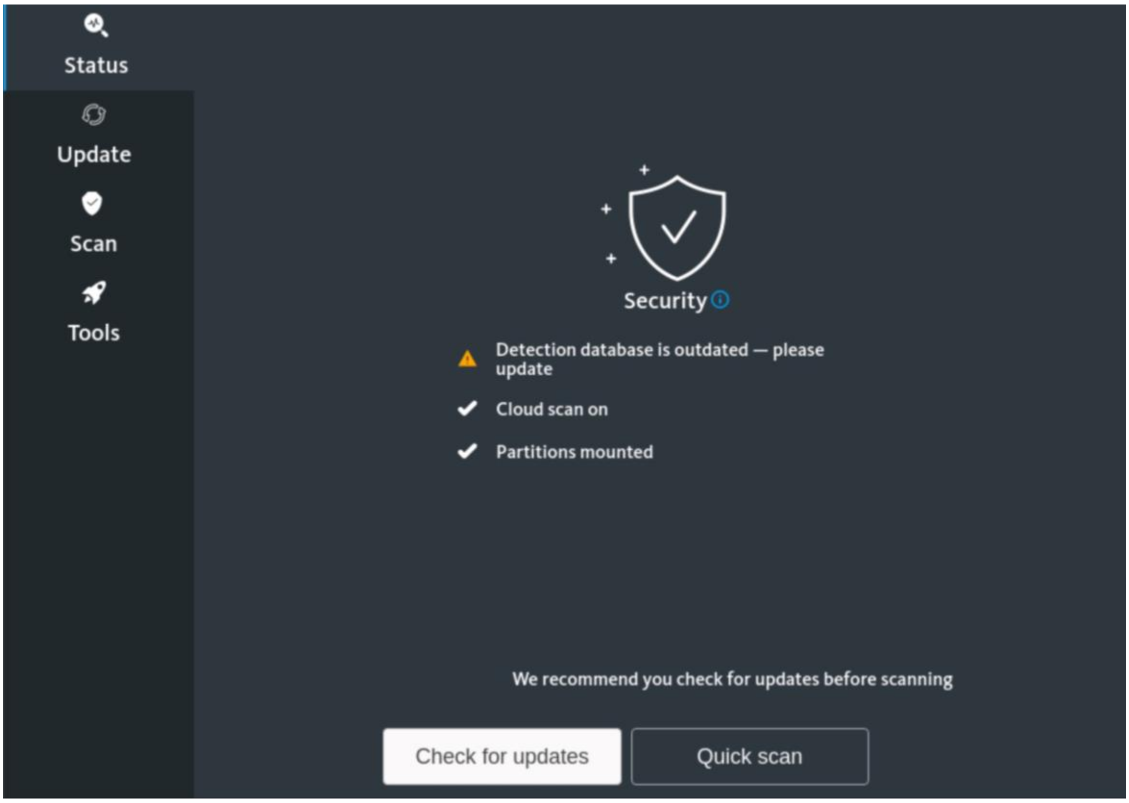
Die folgenden Bestimmungen regeln die vertraglichen Beziehungen für den Erwerb und die Nutzung von Aviras Produkten („Produkte“). Die Avira Produkte Endnutzer-Lizenzvereinbarung („EULA“) und Nutzungsbestimmungen (EULA gemeinsam als „Nutzungsbedingungen“ bezeichnet) bilden einen Vertrag zwischen Ihnen persönlich oder, falls Sie zur Vertretung einer juristischen oder natürlichen Person zum Erwerb oder zur Nutzung von Avira Produkten, Software von Avira oder zur Nutzung von und/oder zum Zugang zu Aviras Dienstleistungen (gemeinsam „Produkte/n“) bevollmächtigt sind, zwischen der juristischen Person, in deren Vertretung Sie handeln (in beiden Fällen „Sie“ oder „Ihr“), und Avira Operations GmbH& Co. KG („Avira“).

Diese Nutzungsbedingungen in Abschnitt I. gelten für die vertraglichen Beziehungen, wenn Sie oder die von Ihnen vertretene Person in Deutschland Österreich oder der Schweiz wohnhaft sind oder Ihren Firmensitz haben.

Sofern Sie oder die von Ihnen vertretene Person außerhalb von Deutschland, Österreich oder Schweiz wohnhaft sind oder Ihren Firmensitz hat bzw. haben, gelten die Nutzungsbedingungen in

☑ By ticking the box, you are confirming that you have read and accepted the End User License Agreement (EULA), the Terms and Conditions, and our Privacy Policy

Activate the checkbox in the lower area of the screen (<By ticking the box…>) and click on <Start>.



Security

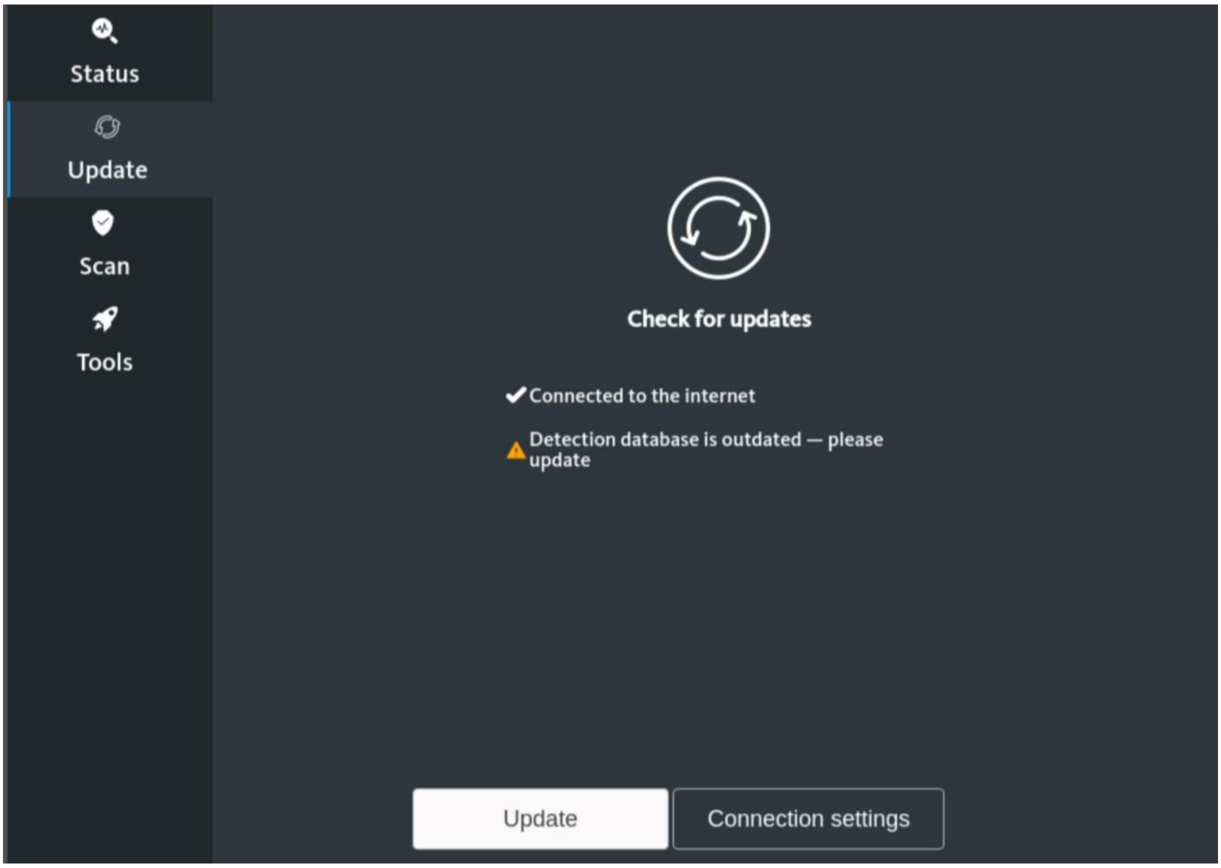
⚠ Detection database is outdated — please update

✓ Cloud scan on

✓ Partitions mounted

We recommend you check for updates before scanning

You are informed that the virus pattern definitions are out of date. So click on <Check for updates> to update them. The system can be checked without an update, but this approach is not recommended.



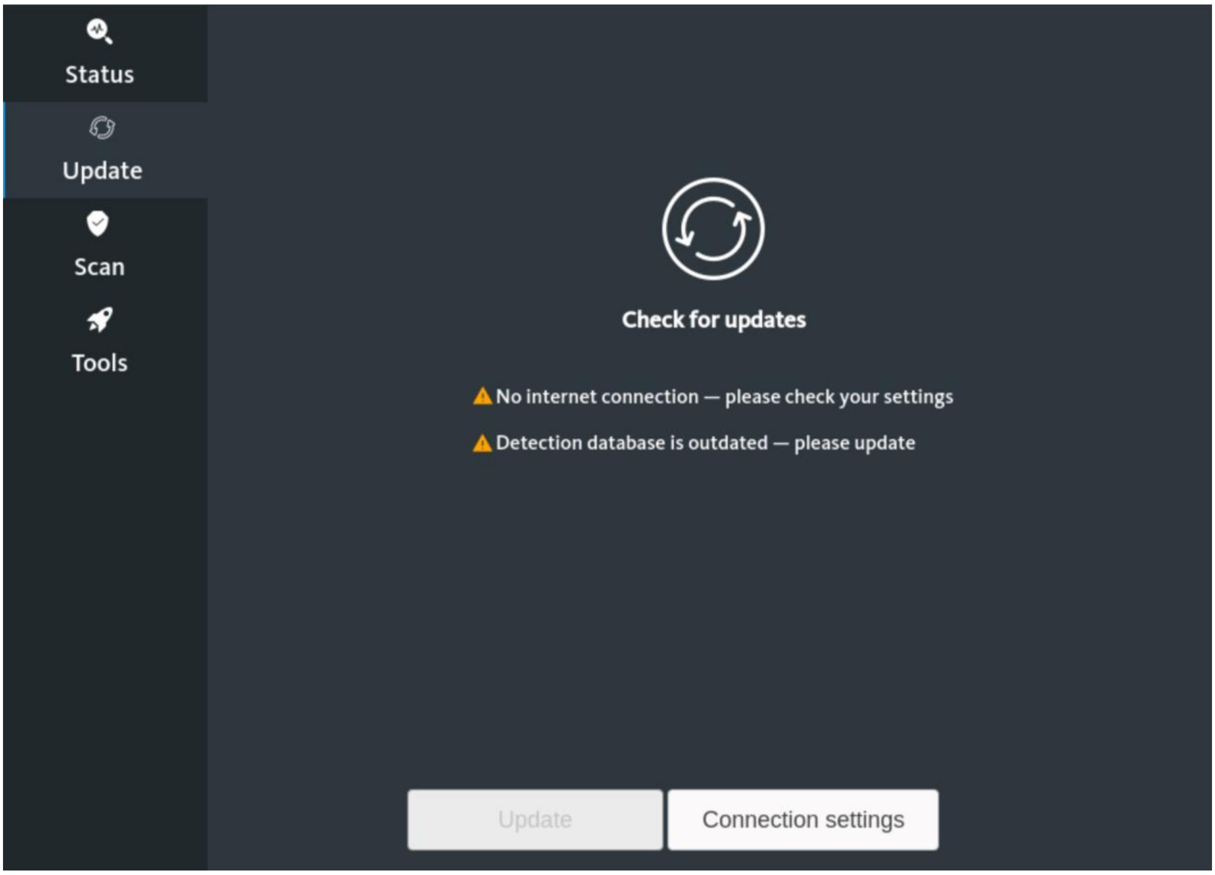
Check for updates

✓ Connected to the internet

⚠ Detection database is outdated — please update

If the message shown above <✓ Connected to the internet> appears, the system is connected to the public network and an update can be carried out. To do this, click on <Update>.

If, on the other hand, you receive the following message <No internet connection…>, the system is not connected to the public network and the <Update> button is inactive. Correct the problem and click <Status> to return to the last step.



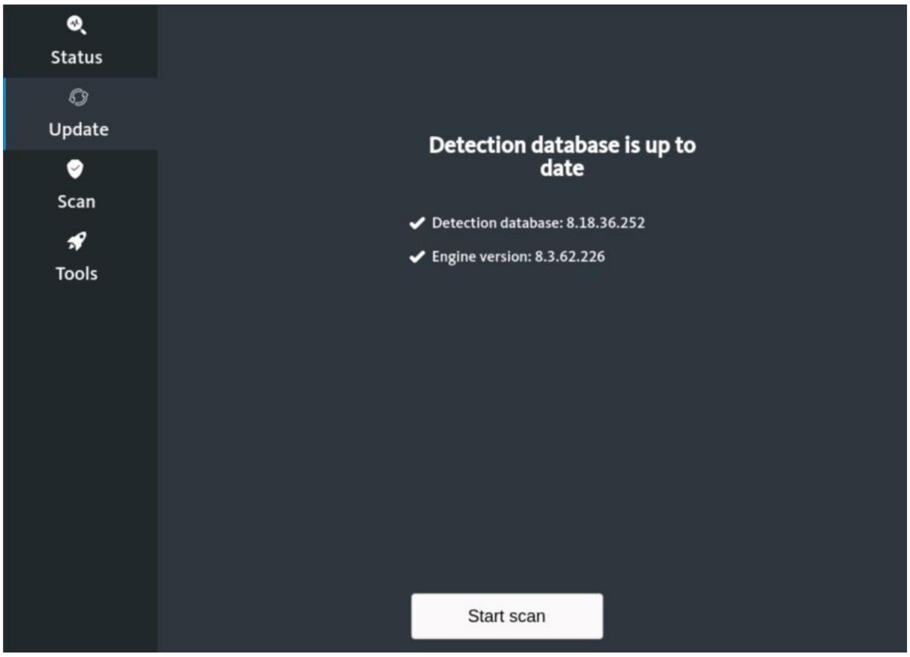
⚠ No internet connection — please check your settings

⚠ Detection database is outdated — please update

If necessary, take a look at Chapter 6 - Troubleshooting and restart the rescue disk so that the automatic network detection can be carried out again.

Advanced users can try a manual configuration of the network connections via <Connection settings>.

After clicking on <Update>, this is carried out in the background without issuing a separate message about this. After a while, the following screen will inform you of the successful completion:

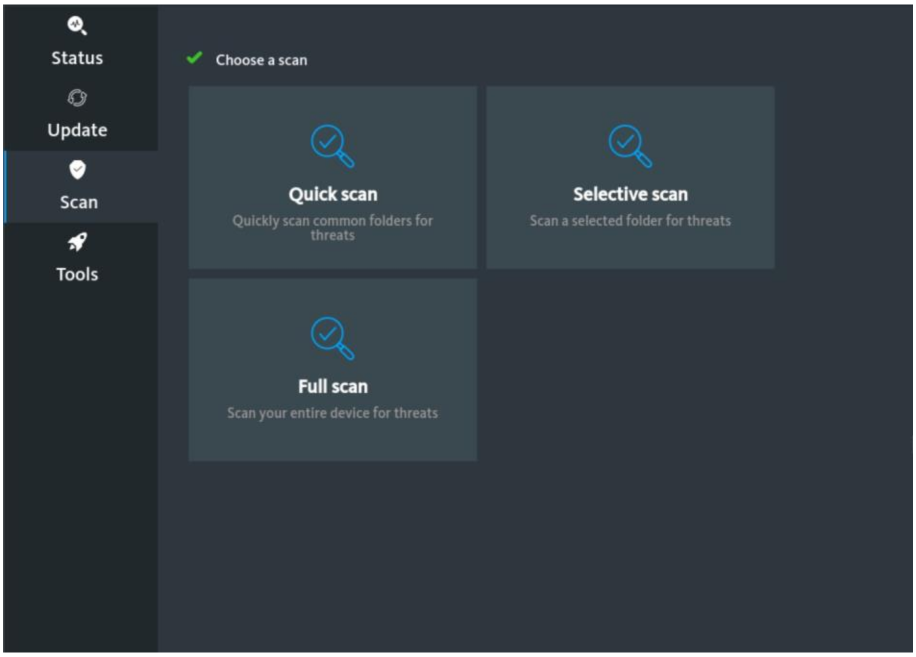


Detection database is up to date

✓ Detection database: 8.18.36.252

✓ Engine version: 8.3.62.226

Click on <Start scan>.



✓ Choose a scan

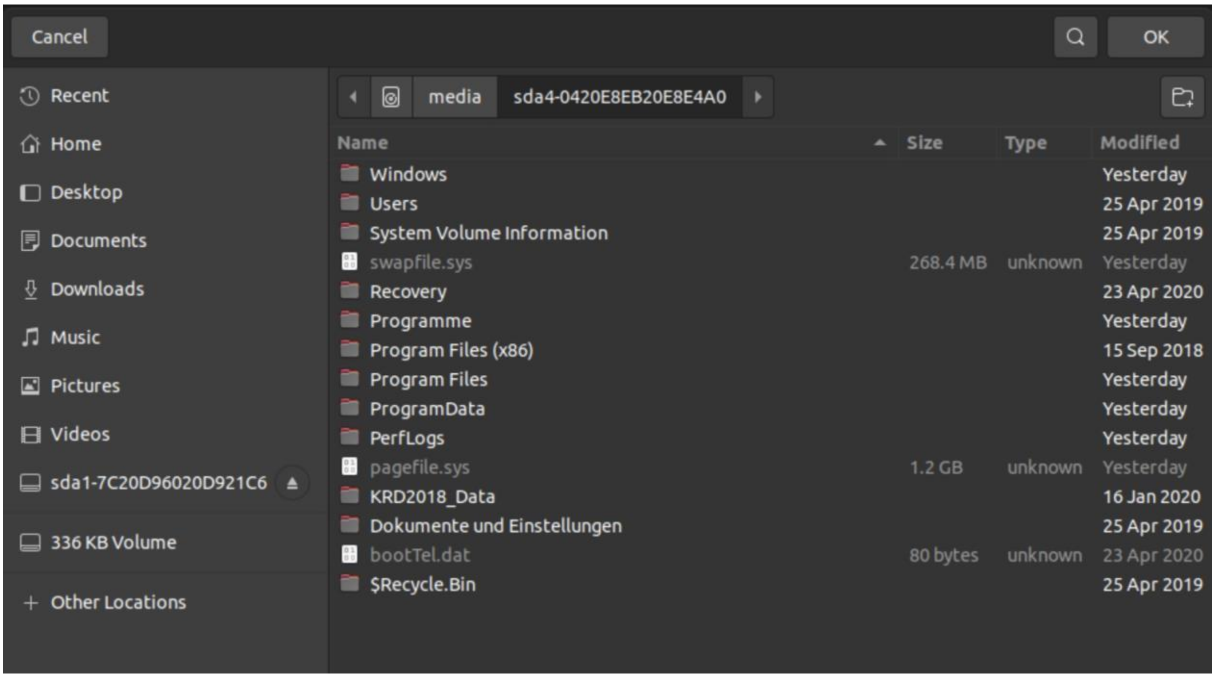
Quick scan: Quickly scan common folders for threats

Selective scan: Scan a selected folder for threats

Full scan: Scan your entire device for threats

You can now choose between a full scan of the system (<Full scan>) or a scan restricted to certain folders (<Selective scan>). The latter should only be used if the threat has already been restricted to specific directories in advance. If it doesn't, choose the full scan.

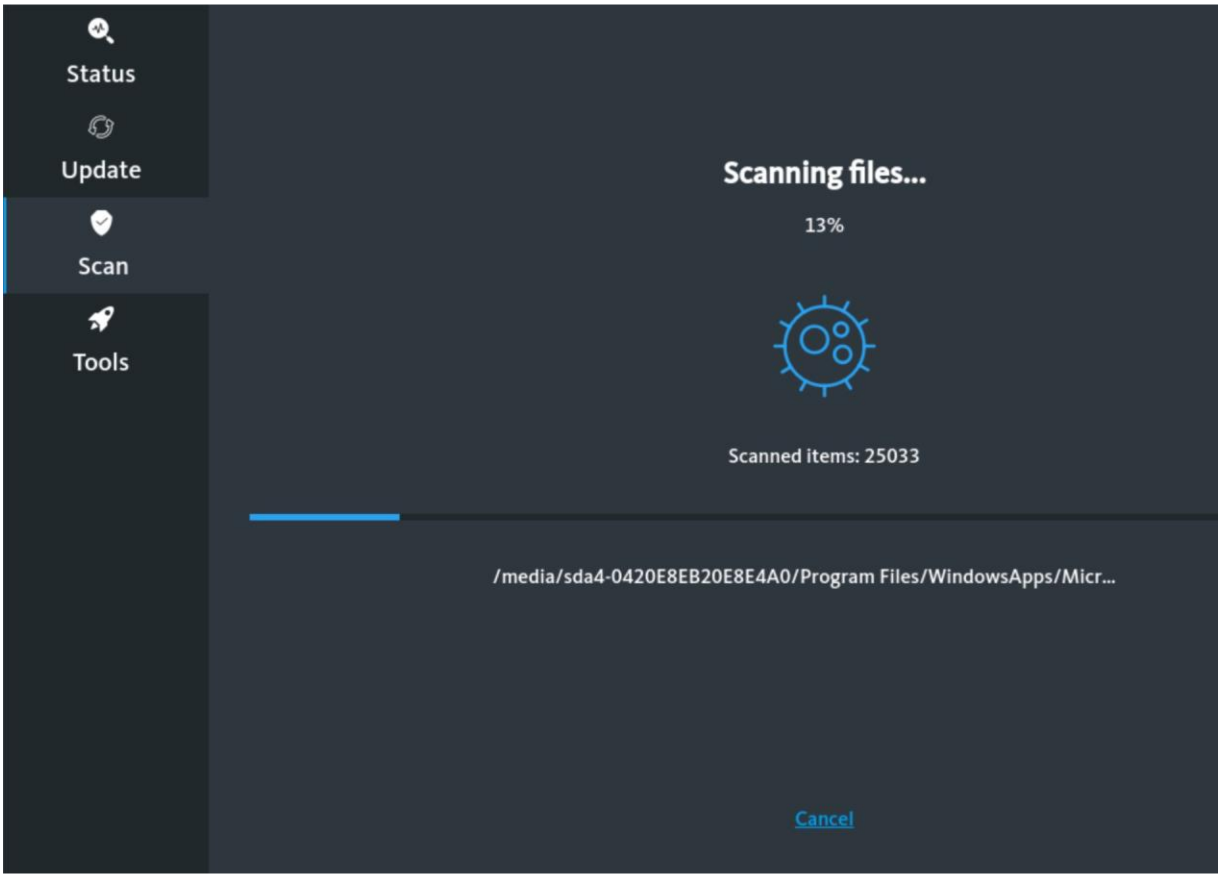
If you have selected <Selective scan>, you will now see an Explorer view, the directory tree corresponding to the structure of Linux systems:



Name	Size	Type	Modified
Windows			Yesterday
Users			25 Apr 2019
System Volume Information			25 Apr 2019
swapfile.sys	268.4 MB	unknown	Yesterday
Recovery			23 Apr 2020
Programme			Yesterday
Program Files (x86)			15 Sep 2018
Program Files			Yesterday
ProgramData			Yesterday
PerfLogs			Yesterday
pagefile.sys	1.2 GB	unknown	Yesterday
KRD2018_Data			16 Jan 2020
Dokumente und Einstellungen			25 Apr 2019
bootTel.dat	80 bytes	unknown	23 Apr 2020
$Recycle.Bin			25 Apr 2019

Find the folders or drives to be checked and mark them. You can use the <Ctrl> key to mark several entries in the current view. After clicking on <OK> the check begins.

If, on the other hand, you have selected the full check, it will start immediately without any further notification. During the check the screen looks like this, it can be interrupted with <Cancel>.



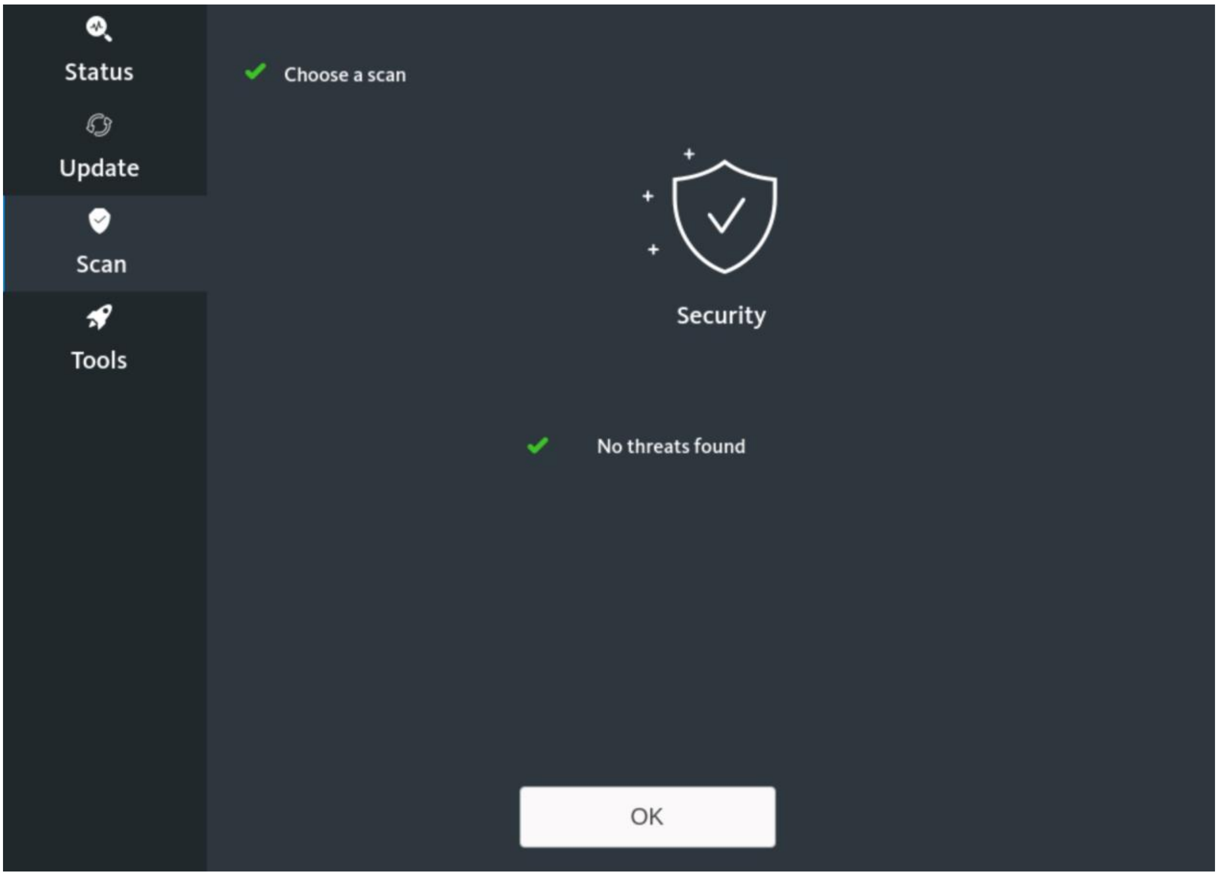
Scanning files...

13%

Scanned items: 25033

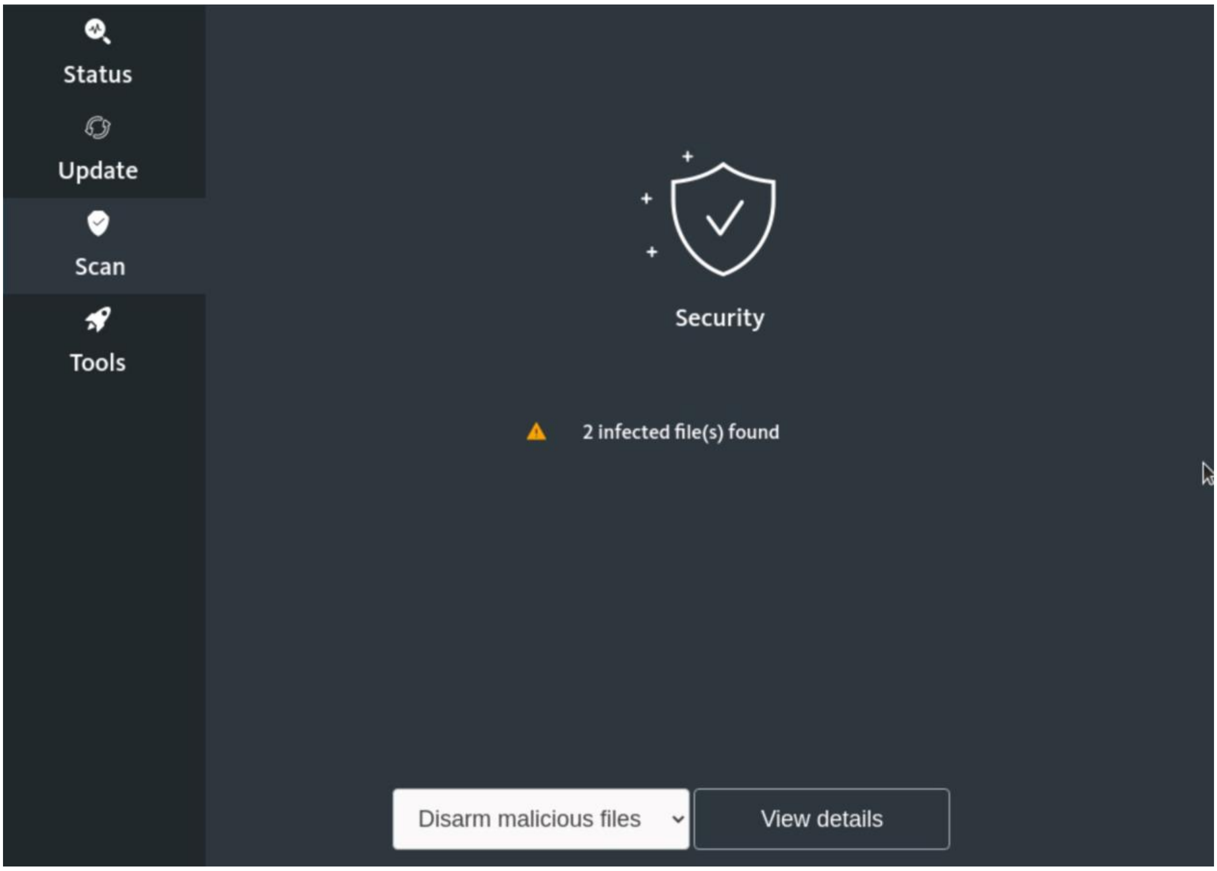
/media/sda4-0420E8EB20E8E4A0/Program Files/WindowsApps/Micr...

After completing the test, you will receive the following message if no infections were found. Clicking on <OK> takes you back to the main view of the <Scan> section.



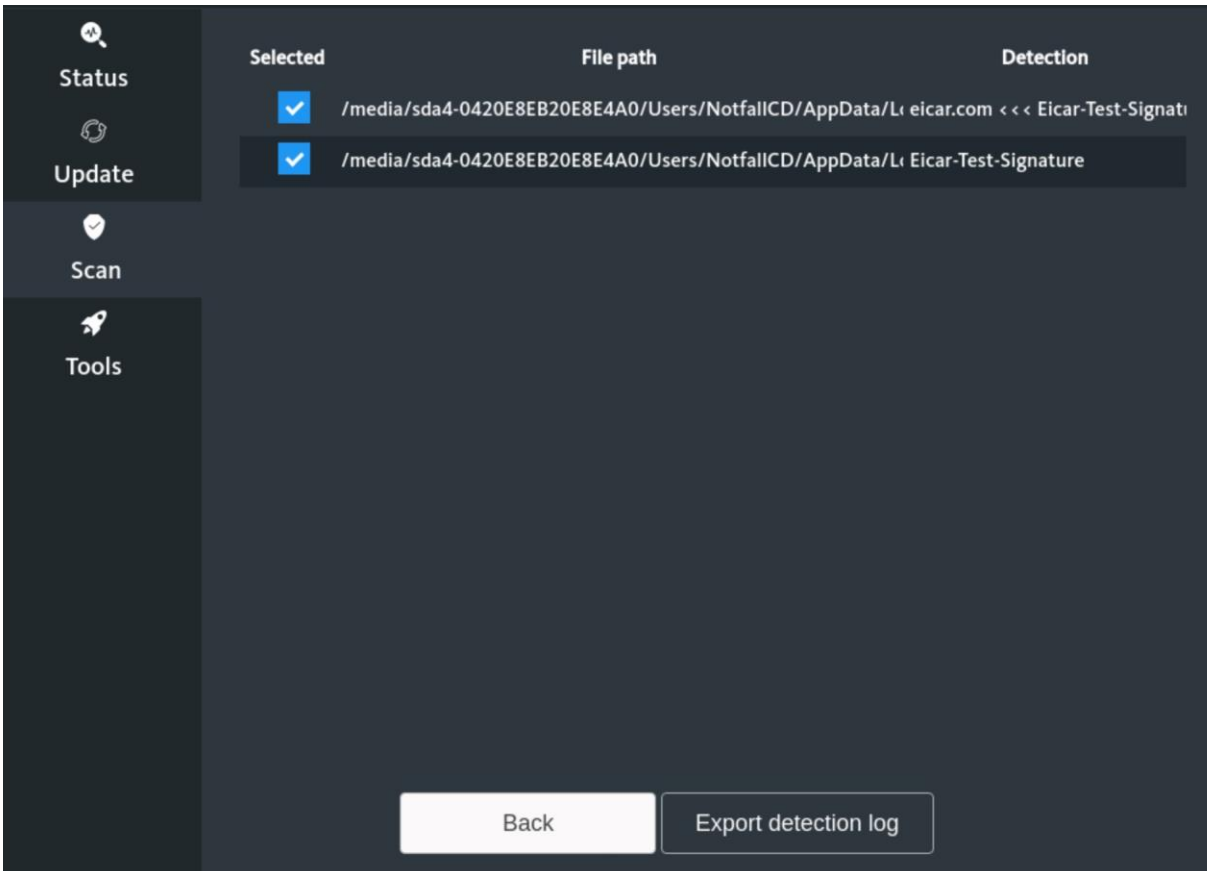
✓ No threats found

If, on the other hand, infections were found, you will receive a message like this:



⚠ 2 infected file(s) found

Click on <View details> to get more detailed information about the objects found.

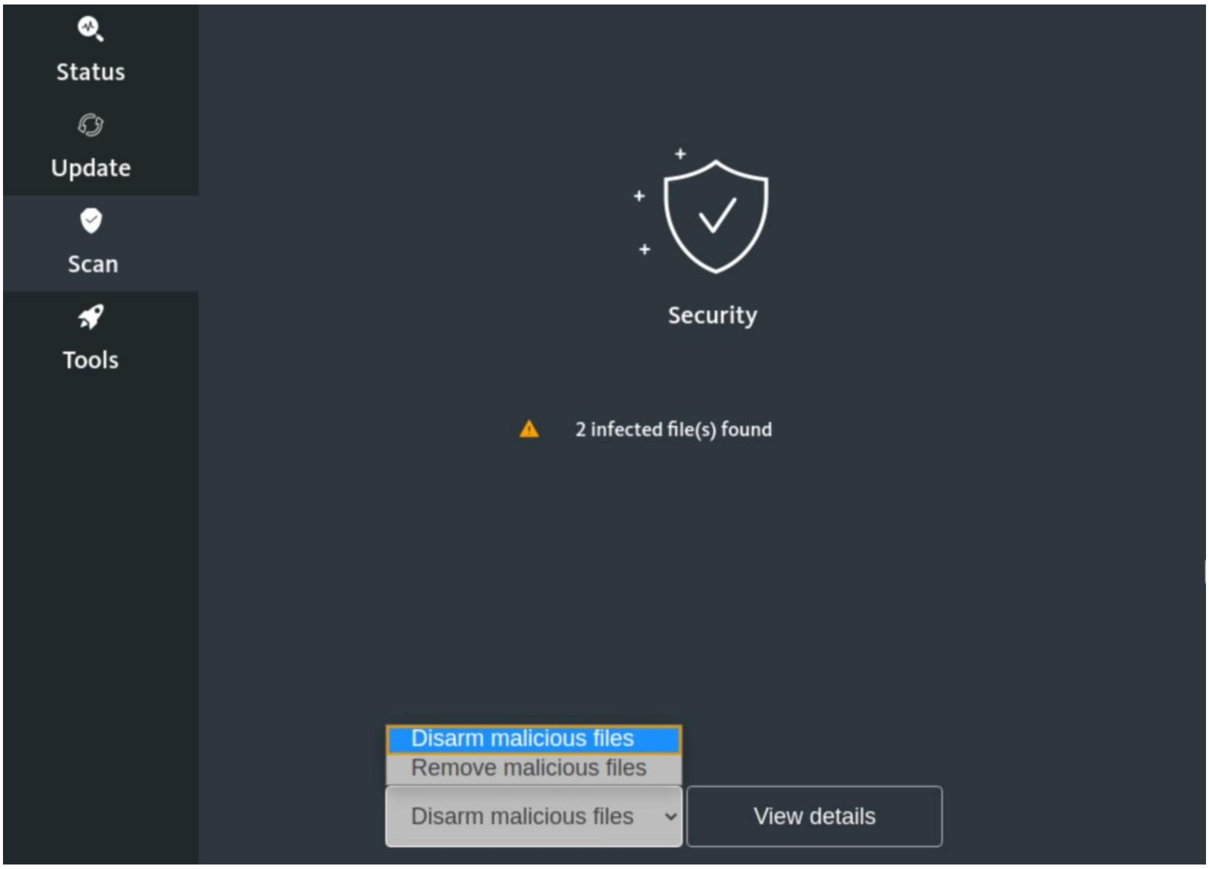


Selected	File path	Detection
☑	/media/sda4-0420E8EB20E8E4A0/Users/NotfallCD/AppData/L	eicar.com <<< Eicar-Test-Signat
☑	/media/sda4-0420E8EB20E8E4A0/Users/NotfallCD/AppData/L	Eicar-Test-Signature

⚠ If desired, you can save the information on the system or connected media by clicking on `<Export detection log>`. An Explorer view appears in which you select the storage location and click `<OK>`.

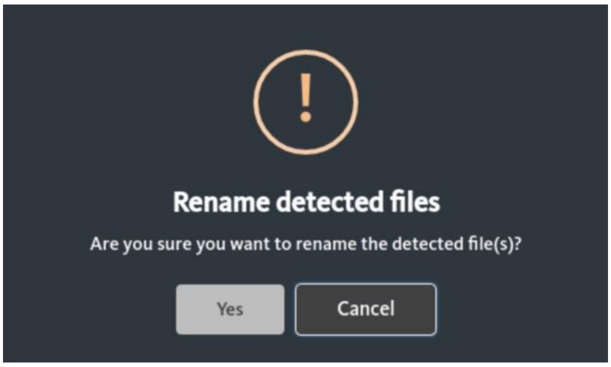
Select `<Back>` to go back to the last view. Click on `<Disarm malicious files>` to display the two options of what to do with the infections found:

- `Disarm malicious files`: The infected files are not deleted, only renamed so that they are no longer loaded the next time the system is started. This is useful for files that are (could) still be needed.
- `Remove malicious files`: The infected files will be deleted. Select this option only if you are certain that the files are no longer needed.



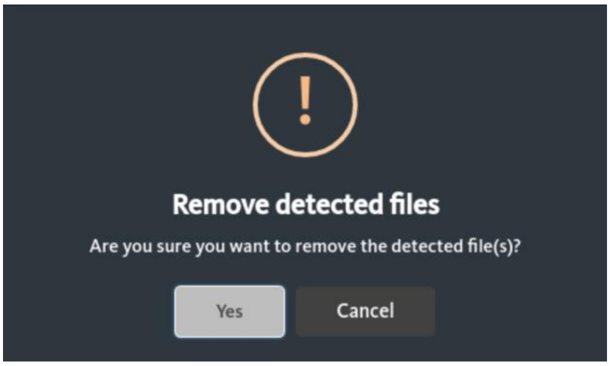
⚠ 2 infected file(s) found

Click on your choice. In both cases you will still be asked to confirm the action:



Rename detected files

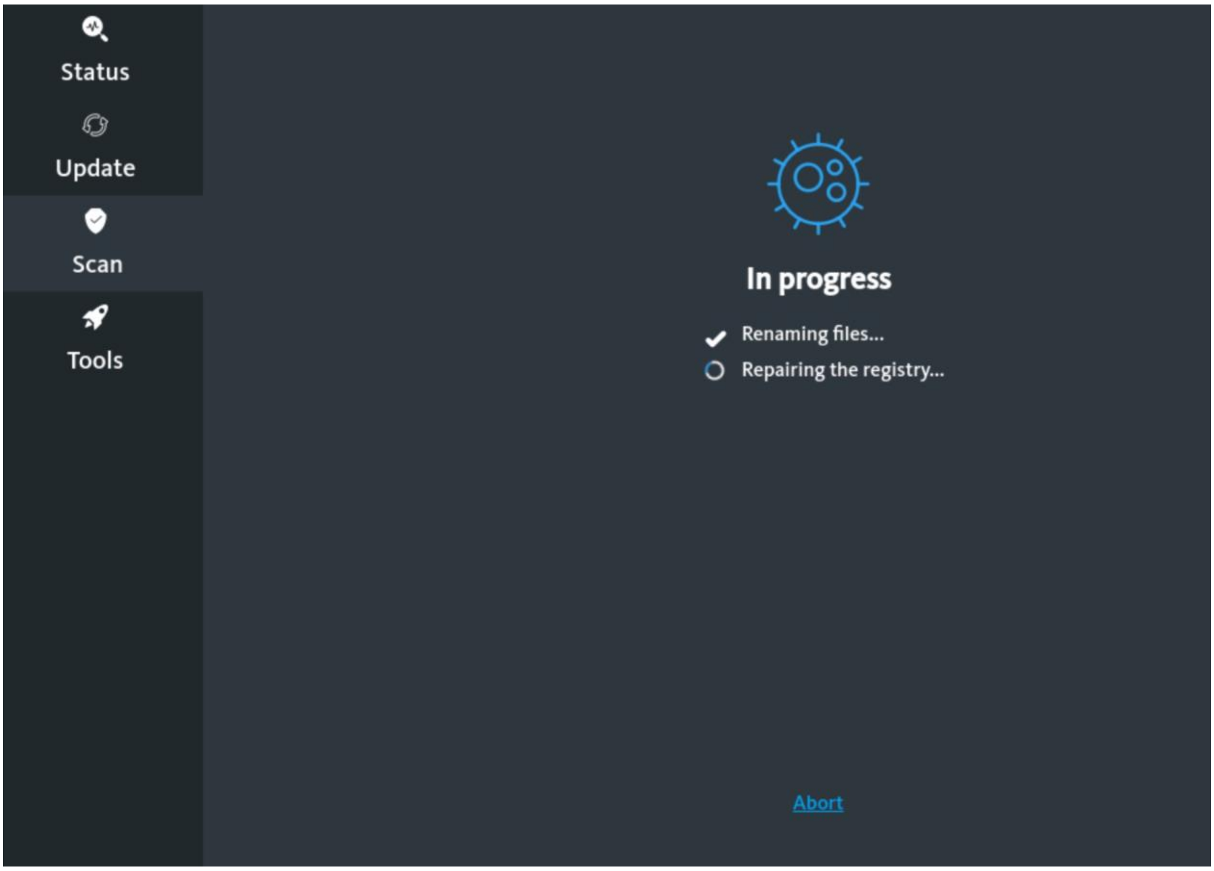
Are you sure you want to rename the detected file(s)?



Remove detected files

Are you sure you want to remove the detected file(s)?

After clicking on `<Yes>` the action is carried out. During this time you will see the following screen:

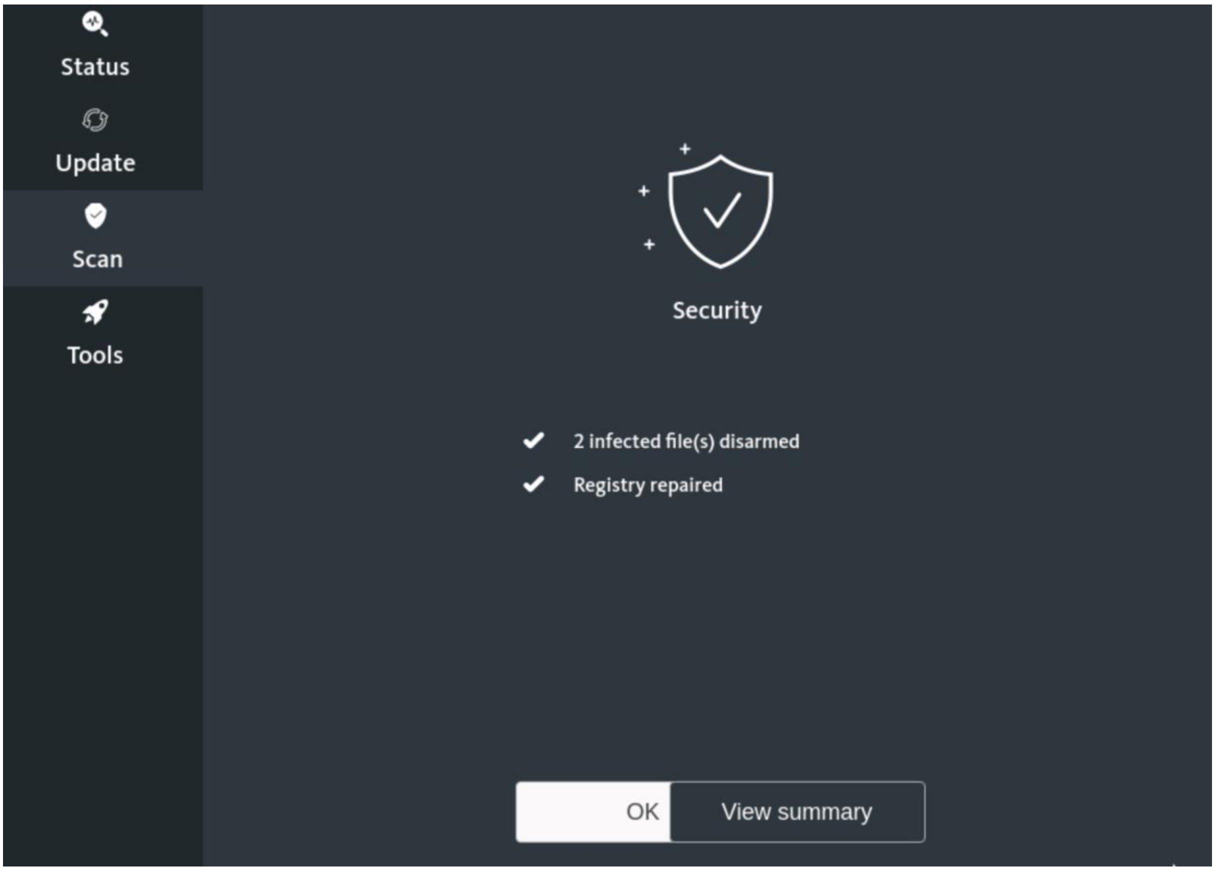


In progress

✓ Renaming files...

○ Repairing the registry...

After successful completion you will see this message:

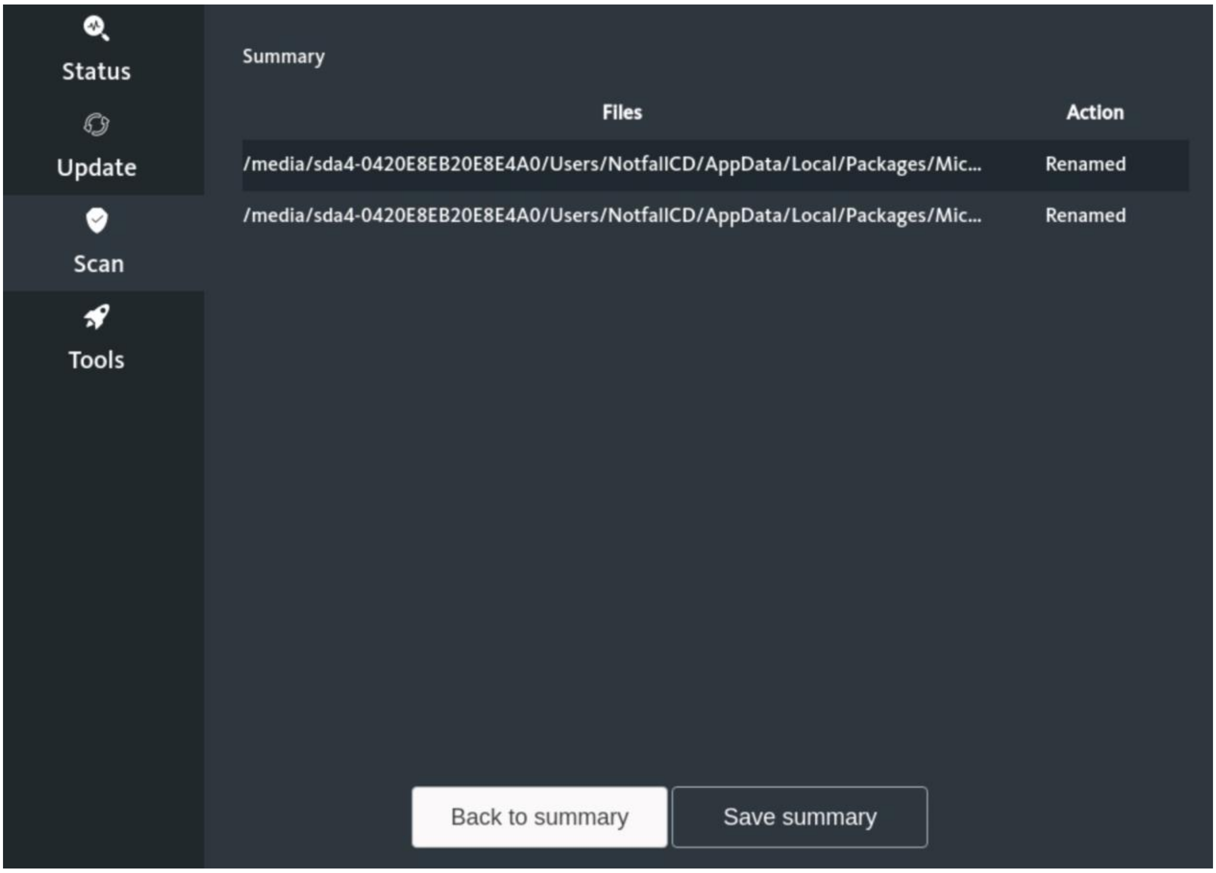


Security

✓ 2 infected file(s) disarmed

✓ Registry repaired

With <View summary> you can display a summary that corresponds to the already known view of the infections found:



Summary

Files	Action
/media/sda4-0420E8EB20E8E4A0/Users/NotfallCD/AppData/Local/Packages/Mic...	Renamed
/media/sda4-0420E8EB20E8E4A0/Users/NotfallCD/AppData/Local/Packages/Mic...	Renamed

You can also save this information on the system using <Save summary>, as has already been explained above.

With <Back to summary> you get back to the last view. Click on <OK> there to return to the main view of the <Scan> section.

Now run additional scans as needed by repeating the steps shown.

If you want to stop using the Avira Rescue System, click on the symbol ▾ in the upper right corner and select <Power Off / Log Out>, then <Power Off ...> and finally <Power Off> or <Restart>.

6. Troubleshooting

If the internet connection is not working correctly, please check the following points (the order in which they are listed is not binding, it is rather a case-specific decision here):

- The network adapter used must be selected correctly; the rescue disks select the adapter automatically. Some WLAN adapters and USB-based solutions may not be recognized correctly; therefore, if possible, connect the affected device for the duration of the update process using an internal network card via a wired connection.

- With permanently integrated network adapters, make sure that they are activated in the BIOS or UEFI. With retrofitted network cards, make sure that the slot / connection used is activated in the BIOS or UEFI.

- Check whether the system is actually connected to a data socket with access to the public network. In the case of experimental networks, etc. this is usually not the case!

- For the correct functioning of the update process, the affected system ideally has to obtain its network configuration from the DHCP server (or otherwise be configured manually). If the system is blocked for JuNet use due to the infection, an update process is therefore not possible. In this case, contact the JuNet hotline on phone extension 6440.

- Note that the use of KVM switches when using the rescue disks can lead to problems with the screen display. In this case, connect the PC directly to a monitor for the duration of the measures.

If these measures do not lead to success either, contact your IT support, IT service provider or the JuNet hotline (6440).

It is still possible to continue using the various rescue disks without an update, but the probability is limited that possible infections with malware can be detected and eliminated.