

Use of the Rescue Disks from Avast and Avira

Table of contents

1. Introduction	1
2. Alternatives to the rescue disks	3
3. Using Avast Rescue Disk	4
4. Using Avira Antivir Rescue System 18	16
5. Troubleshooting	27

1. Introduction

With the solutions Avast Rescue Disk and Avira Antivir Rescue System, employees of the Forschungszentrum Jülich have two powerful rescue tools ('rescue disks') (also for private use) available to scan Windows and Linux partitions (not Avast) 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 both 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 5-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>).

Both provided 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 the other solution. 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.

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, Trellix (formerly 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 Trellix Stinger:

<https://www.trellix.com/downloads/free-tools/stinger/>

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://learn.microsoft.com/en-us/defender-endpoint/safety-scanner-download?view=o365-worldwide>

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 10/11. It is also only executed when required, so it does not replace a virus scanner.



Quick start guide Microsoft Windows Defender Offline:

<https://learn.microsoft.com/en-gb/defender-endpoint/microsoft-defender-offline>

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/article/1135824/pc-welt-notfall-dvd.html>

3. Using Avast Rescue Disk

An Avast Rescue Disk ISO image can be found on PCSRV at



[\\pcsrv.zam.kfa-juelich.de\public\Notfall-CDs\02-Avast-Antivirus](https://pcsrv.zam.kfa-juelich.de/public/Notfall-CDs/02-Avast-Antivirus)

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

There are two ISO files in this directory: `rescuedisk_UEFI.iso` for systems with UEFI (Unified Extensible Firmware Interface) and `rescuedisk_BIOS.iso` for systems with BIOS (Basic Input/Output System). Select the iso file that applies to your system.



If you are unsure which case applies to the system to be examined, start with the UEFI variant for systems built after 2006, otherwise with the BIOS variant. If there are problems (e.g. does not start or drives are not recognized), then try the other.

If there are still problems, you can try to deactivate `<Secure Boot>` in the UEFI menu and to adjust the UEFI/BIOS mode (`<Legacy>`).

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



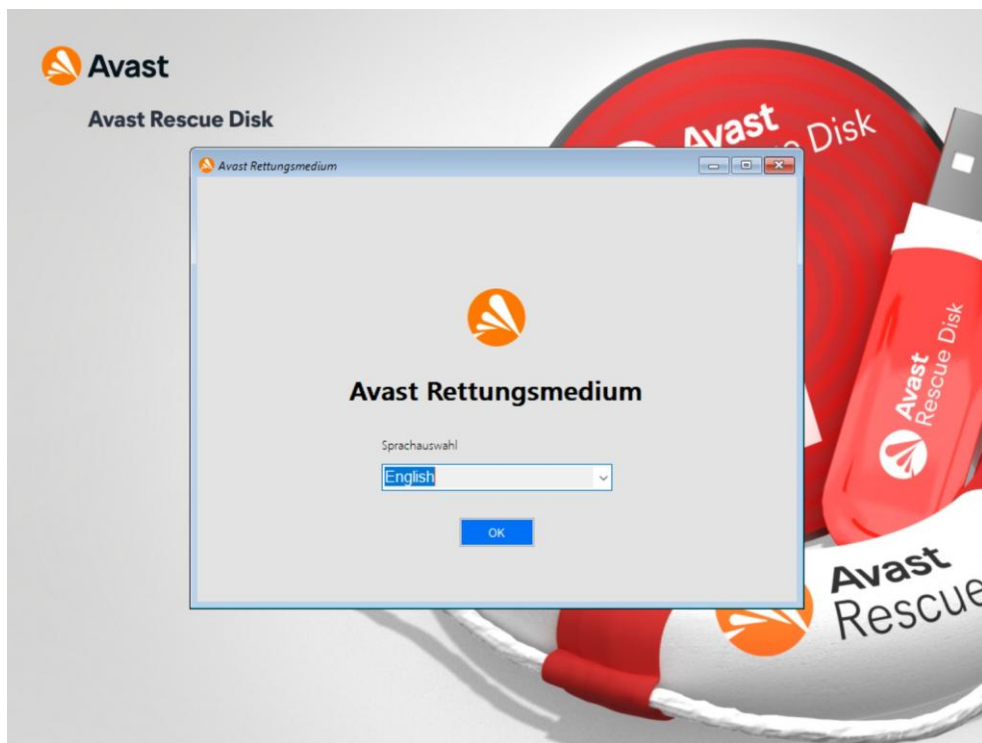
Download Rufus Portable:

<https://rufus.ie/en/>




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.

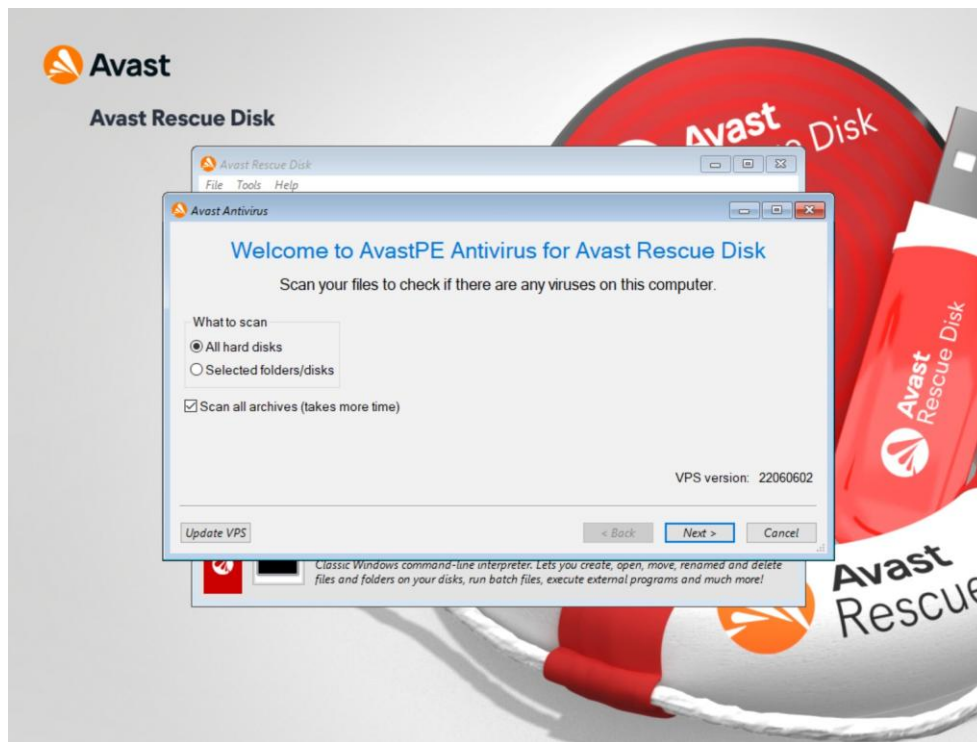
After a short wait, you'll be asked which screen language you want to use to run the Rescue Disk. Select the desired language and click <OK>.



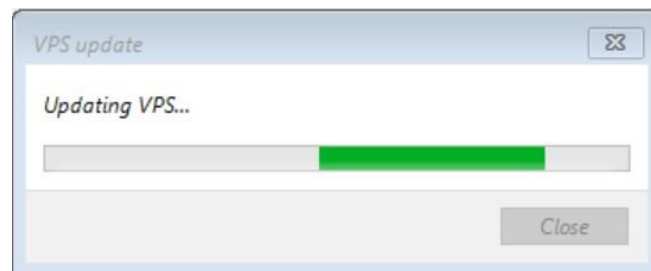
The start screen of Avast Rescue Disk will appear.



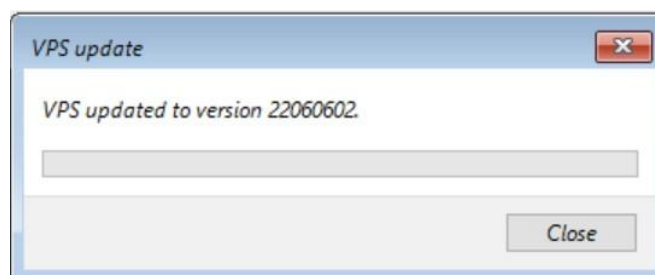
Start by clicking the  (AvastPE Antivirus) button to bring up the virus scanner.



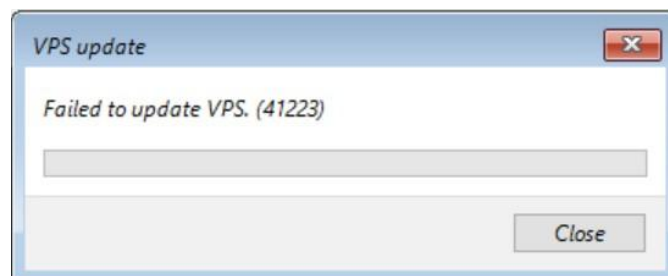
First update the virus pattern definitions by clicking on <Update VPS>. During the update process, which can take several minutes, you will see this message:



If the update was successful, the following message appears, which you can confirm with <Close>.



However, if the update fails, you will see the following message:



The error code shown here (41223) means that the Avast update server could not be reached. The system to be examined is probably not connected to the public network; fix the problem

and try again after clicking <Close>. If necessary, refer to the notes in Chapter 5-Troubleshooting.

An examination without updating the virus pattern definitions is possible, but only of limited use.



If the system is connected to the network via WiFi when you receive this error message, try connecting to a wired connection instead.



If you receive an error code other than 41223, you can resolve this to a specific error message via a Google search and try to correct the problem accordingly. For example, use the search term

Avast error code xxxxx

You are back on the start screen of the virus scanner. You can now decide whether all hard disks (partitions) found in the system should be examined (click on <all hard disks>), or whether you want to limit the search area (click on <selected folders/disks>).

If you are unsure whether and in what form it makes sense to limit the search area, have all partitions examined.

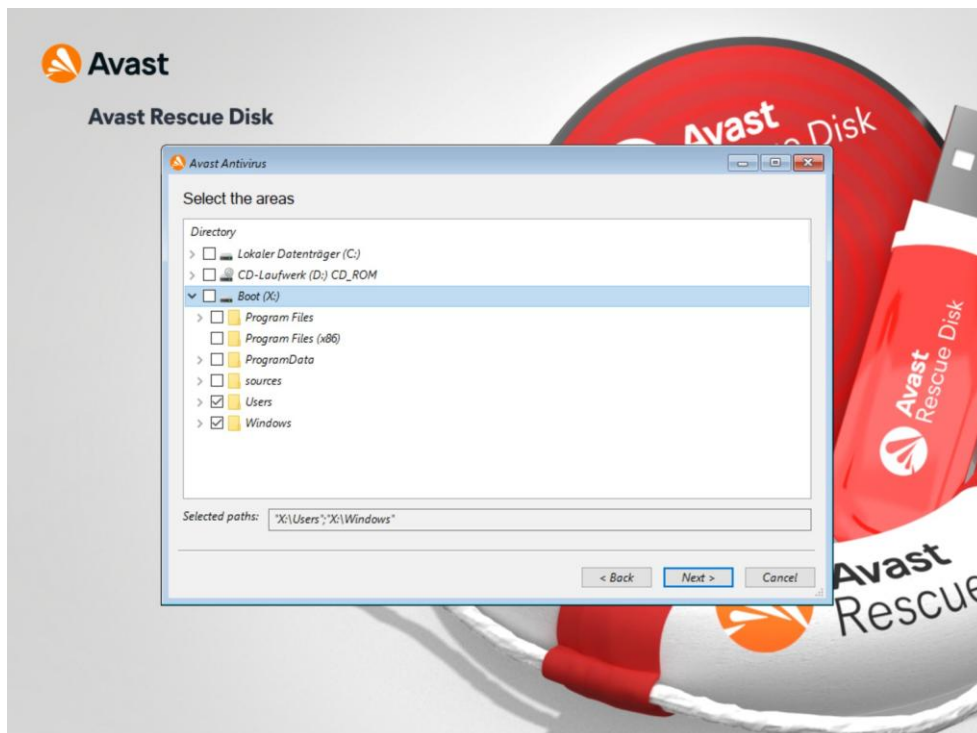


Bootable partitions should definitely be examined.

Also enable the <scan all archives (takes more time)> option to fully scan compressed files.

Click on <Next> or <Select> (if you have selected a limited examination).

In the case of a limited examination, you will now see the following window in which you can make the selection:

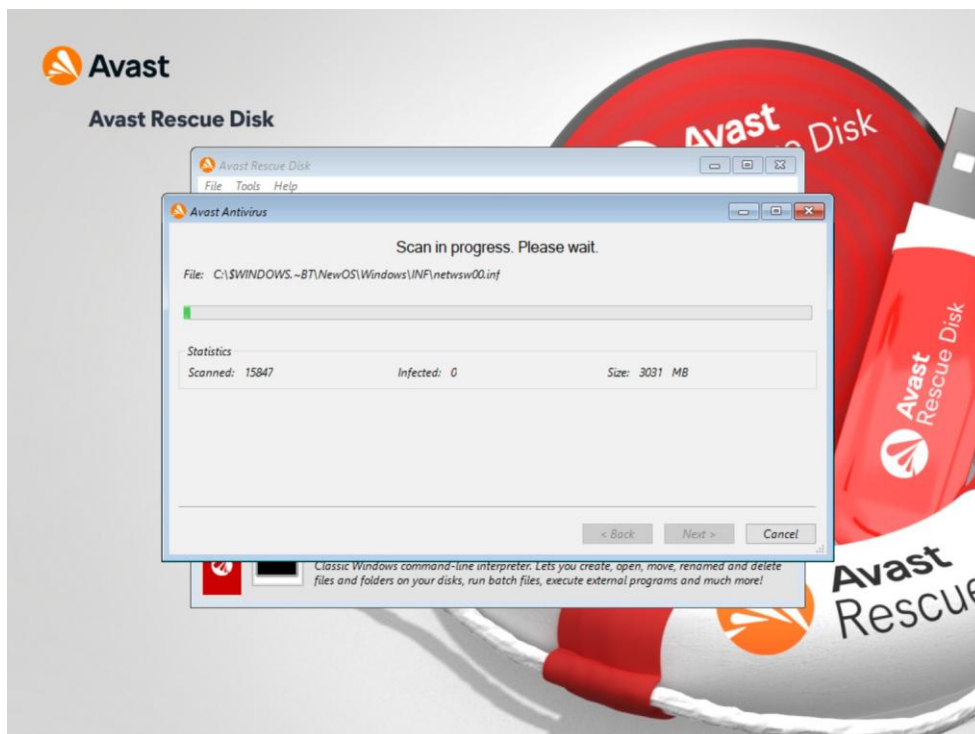


Under <Directory> you will first see all recognized drives and partitions. By clicking on the arrow symbols you can open the directory tree of a drive and navigate through the various directory levels. Mark all directories to be examined by activating the preceding checkbox.

In the example above, on drive X: the Users and Windows directories (and their subdirectories) would be examined.

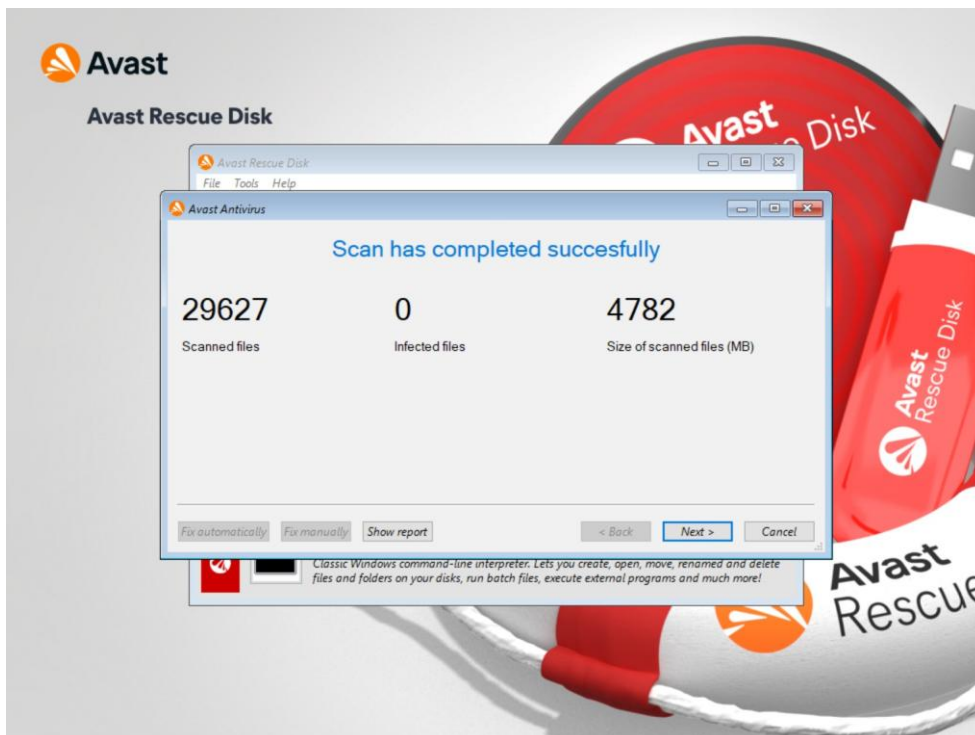
After selecting all objects to be examined, click on <Next>.

The selected examination will now start, which you can end prematurely (if necessary) by clicking on <Cancel>:

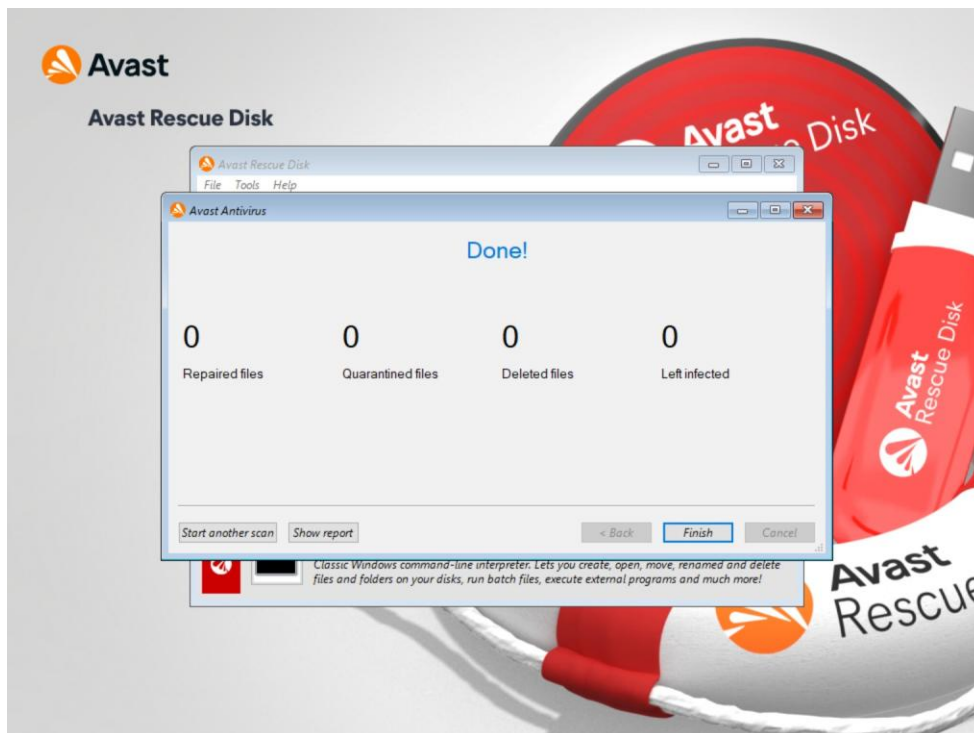


In the <Statistics> area, next to the <Infected:> entry, you can see how many infections have already been found.

If the scan completes without finding any malware, you will receive the following message:

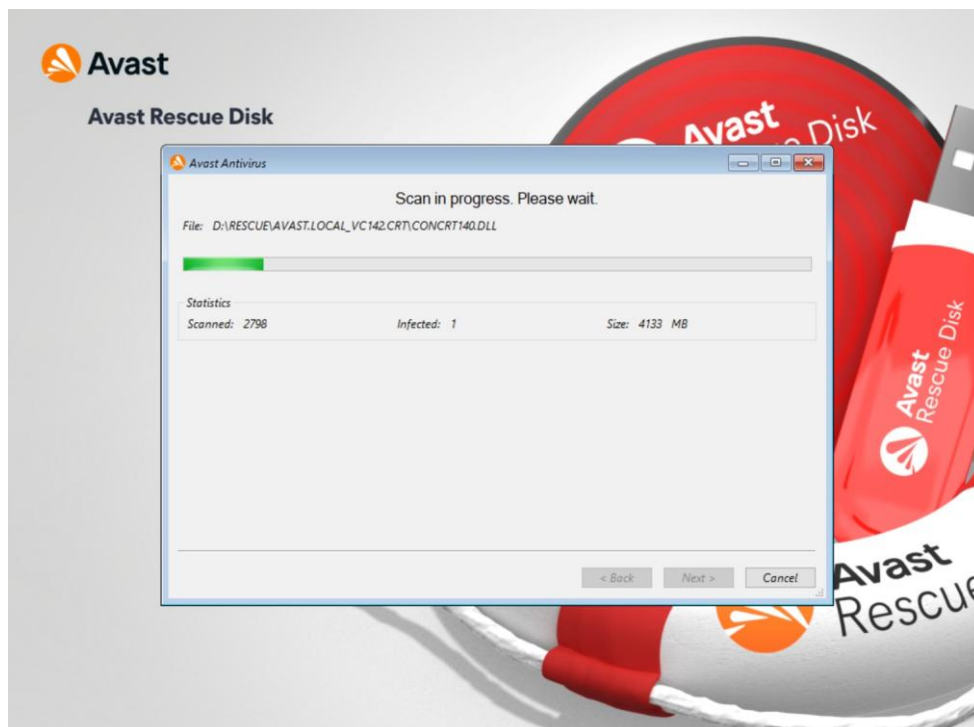


The <Infected files> counter shows 0; click <Next>.

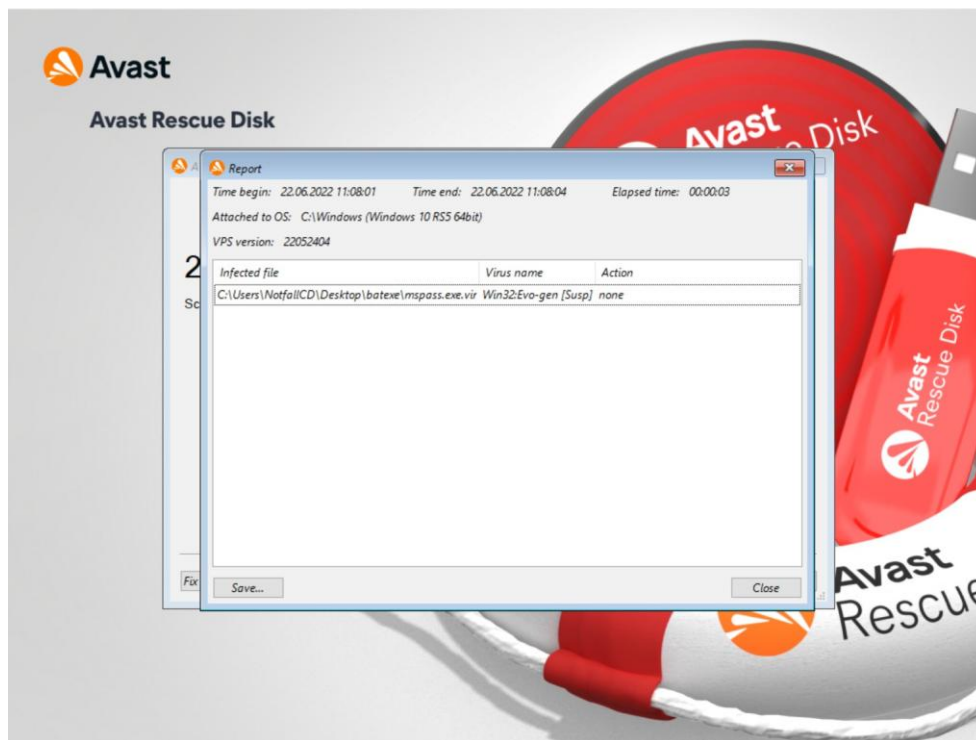


If you would like to have the result checked by another scan (e.g. by examining other drives), select <Start another scan> to return to the start screen of the virus scanner. Otherwise, select <Finish> to return to the Rescue Media main menu.

If, on the other hand, malware infections are found, the field <Infected:> is increased accordingly during the scan:

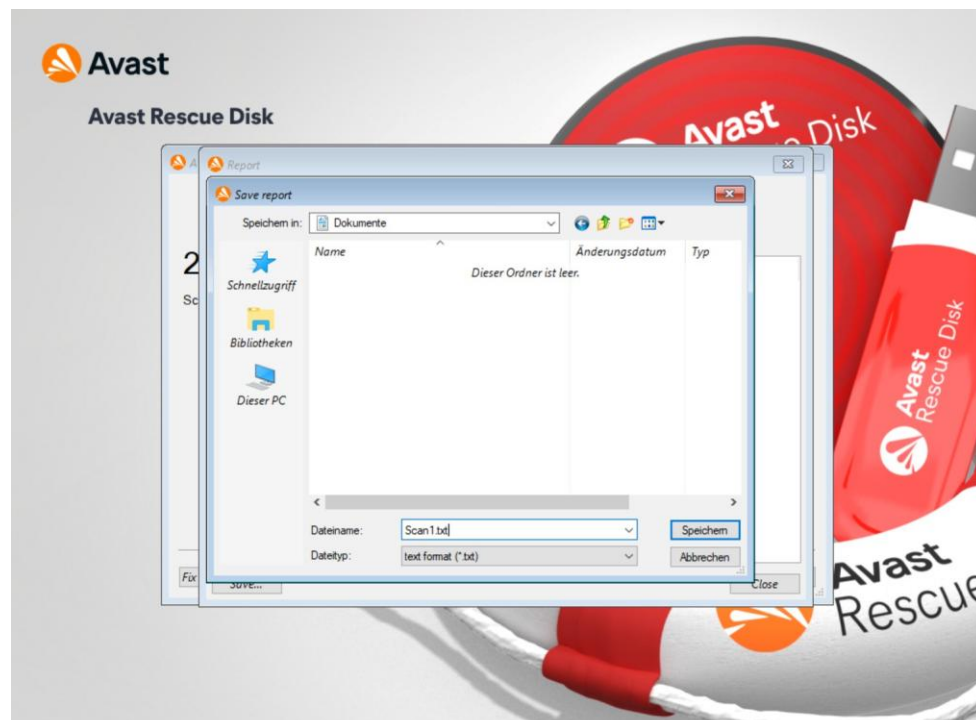


After the scan is complete, a summary of the infection(s) found will appear:



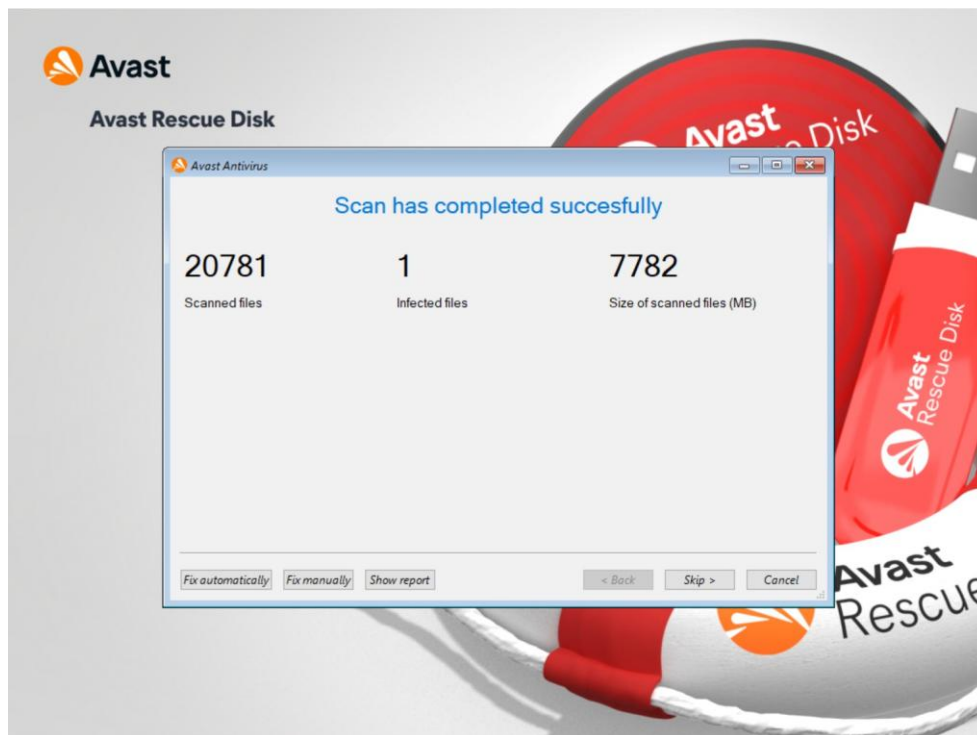
In the above example, a Trojan horse of the type Win32:Evo was found in the file `mypass.exe`, stored under the path shown under <Infected file> and no further action was taken on this file (<Action> = <none>). In the case of several infections, further entries can be found in this overview.

If you wish, you can now save the content of this view as a text file by selecting <Save...>.



Select the desired storage location and enter any file name, the information will be stored in a txt file.

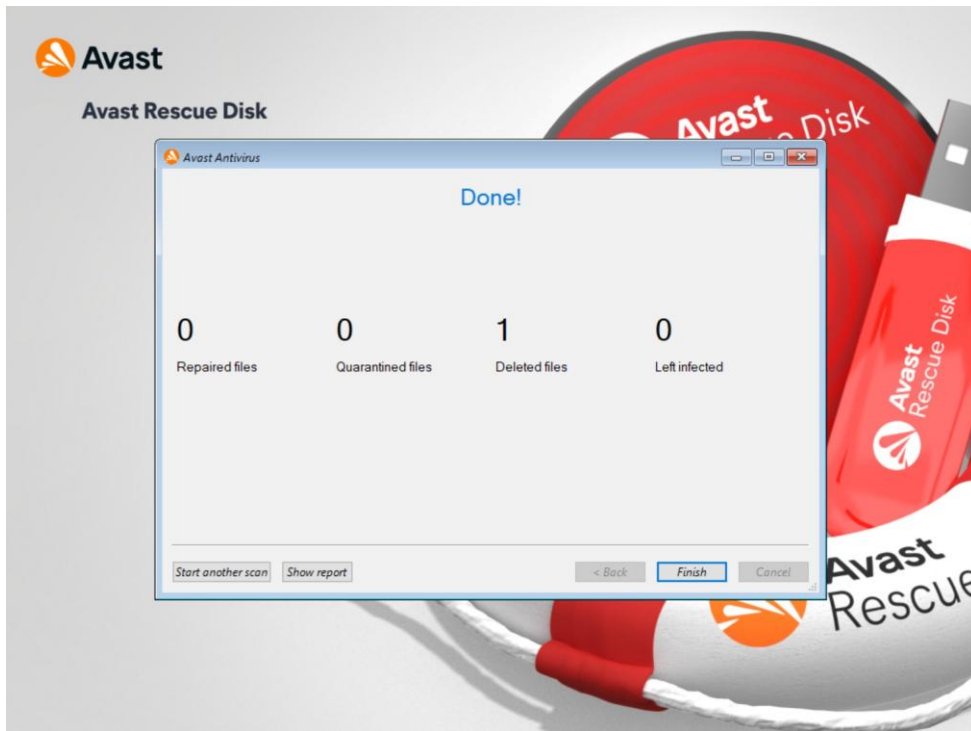
Now close the Report view with <Close>. You get to this view with a summary of the investigation:



Now make the following selection:

- Using `<Fix automatically>`, the rescue disk tries to repair all infected files, i.e. the virus is deleted, but the file remains. Files that cannot be repaired are deleted.
- With `<Fix manually>` you can decide how each file should be handled (repair attempt or delete).
- Use `<Show report>` to return to the previous report view.
- Nothing is done with `<Skip>`, you come to the final screen of the current investigation. The infections found remain unchanged!
- With `<Cancel>` you return directly to the main menu of the rescue disk without further action. The infections found remain unchanged!

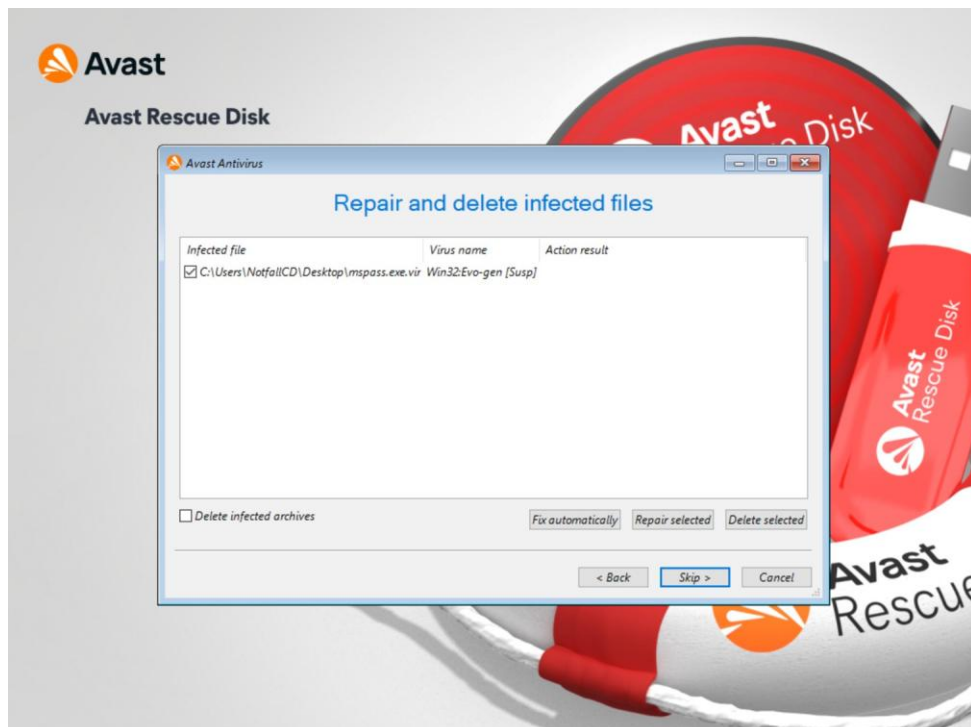
After you have selected `<Fix automatically>`, the rescue disk will deal with any infection it finds automatically and without further notification. After completing the measures, you will receive a summary of the results:



In the example above, one file was deleted (<Deleted files> = 1) because it could not be repaired (<Repaired files> = 0). There are no other known infections left (<Left infected> = 0).

With <Finish> you get back to the main menu of the rescue disk.

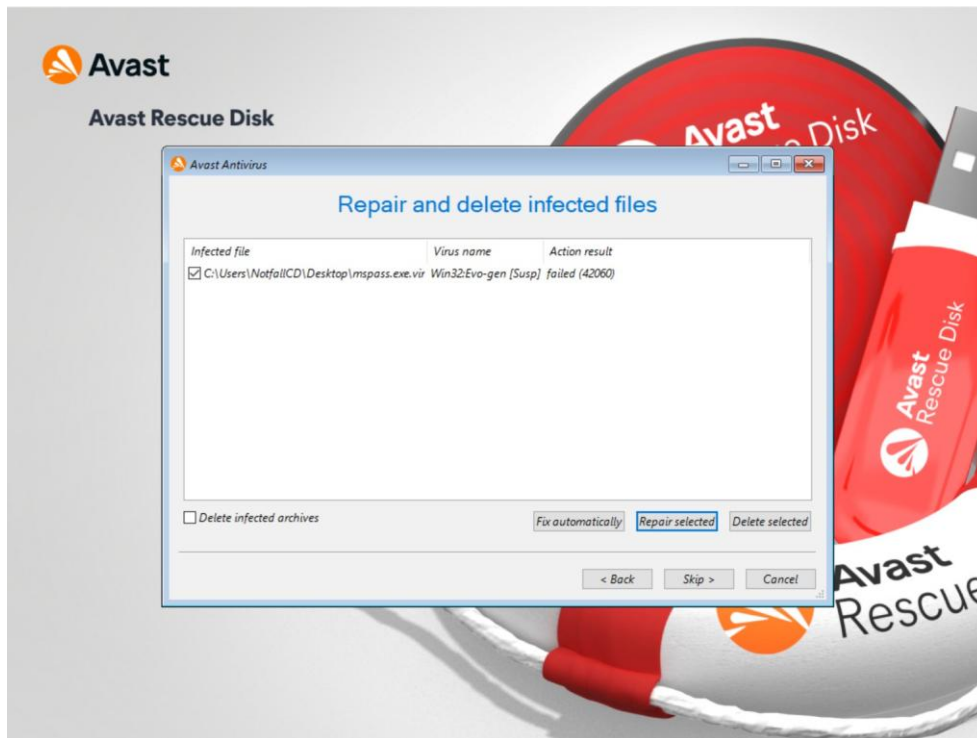
With <Fix manually> you have the same options (repair or delete) using the <Repair selected> and <Delete selected> buttons:



Activate the checkboxes in front of the file names (for multiple infections) for all files that should be subjected to the same treatment and select the desired action. Nothing is done with <Skip>.

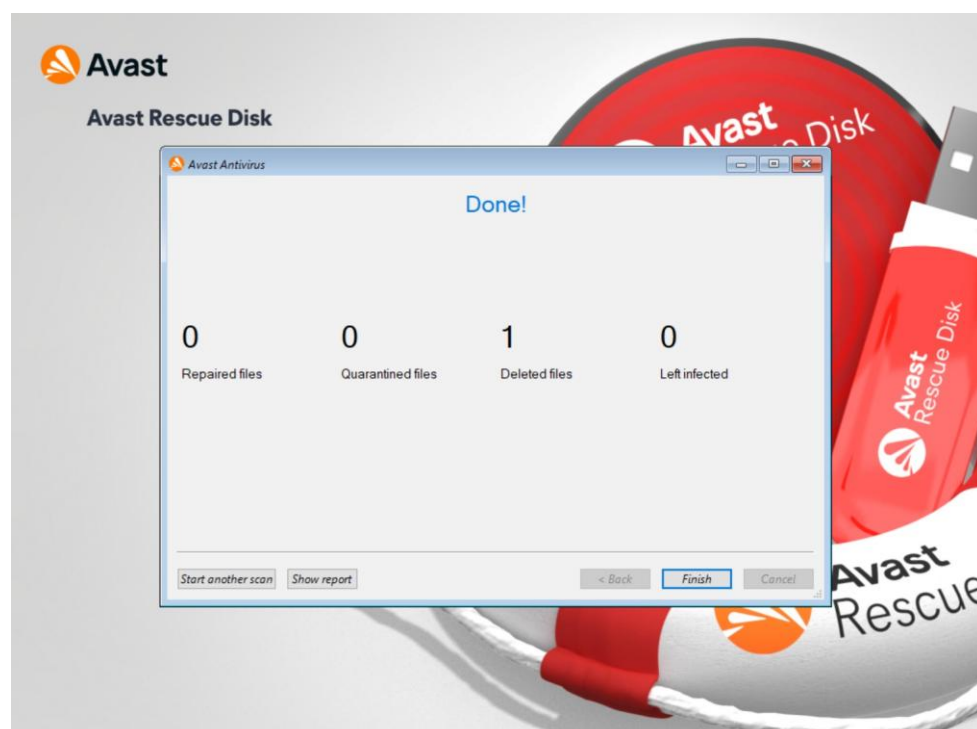
If required, also activate the <Delete infected archives> checkbox.

If you select <Repair selected> and the repair attempt fails, you will get the following message (<Action result> = failed (*Errorcode*)):



In this case, the only option is to delete the file. If the deletion was successful, you will see the entry deleted under <Action result>.

After completing all necessary actions, select <Skip> to see the final screen of the investigation:



Here is a list of how many files were repaired, deleted and left infected during this scan. Close this view with <Finish> to return to the main menu of the rescue disk.



Here you have the following options:

- Start a new scan (<AvastPE Antivirus>),
- open a browser window, e.g. to search for virus names or error codes (<AvastPE Browser>),
- open a system view similar to Windows Explorer (<AvastPE Commander>),
- open an editor of the Windows registry (<Registry Editor>),
- open a Windows command line (<Command-line Tool>),
- restart the system (<File> menu, then <Restart>) and
- switch off the system (<File> menu, then <Shut down>).



The Windows registry editor is recommended for advanced users only, improper changes can seriously damage the operating system.

4. 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](https://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 Avira Antivir Rescue System by creating a bootable USB stick from the ISO image. Use suitable third-party software for this purpose; The Avira 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/en/>



Download UNetbootin:

<https://unetbootin.github.io/>

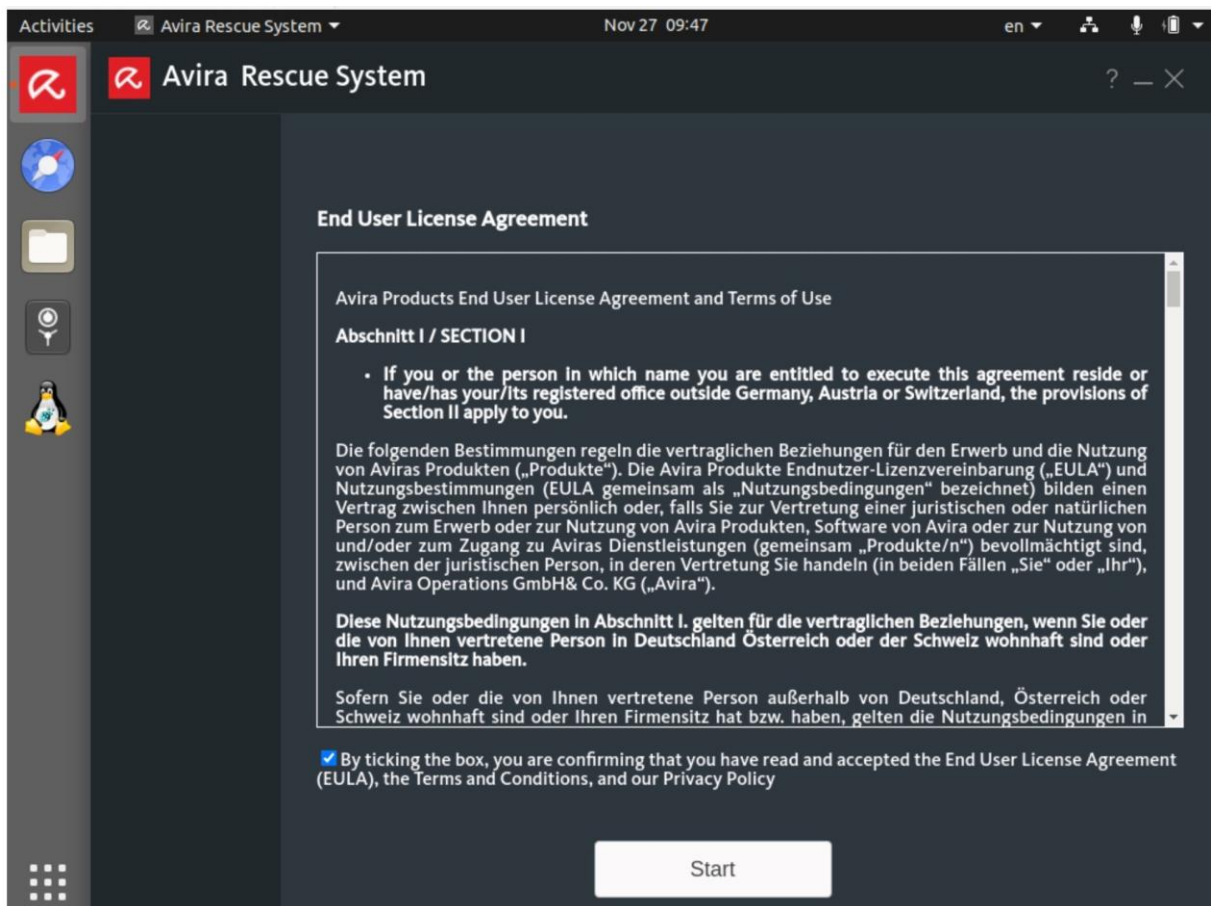


Alternatively, you can burn the ISO image as a CD / DVD and restart the affected system from this. To do so, use the software available at your institute or the <Burn disc image> function integrated in Windows 10.

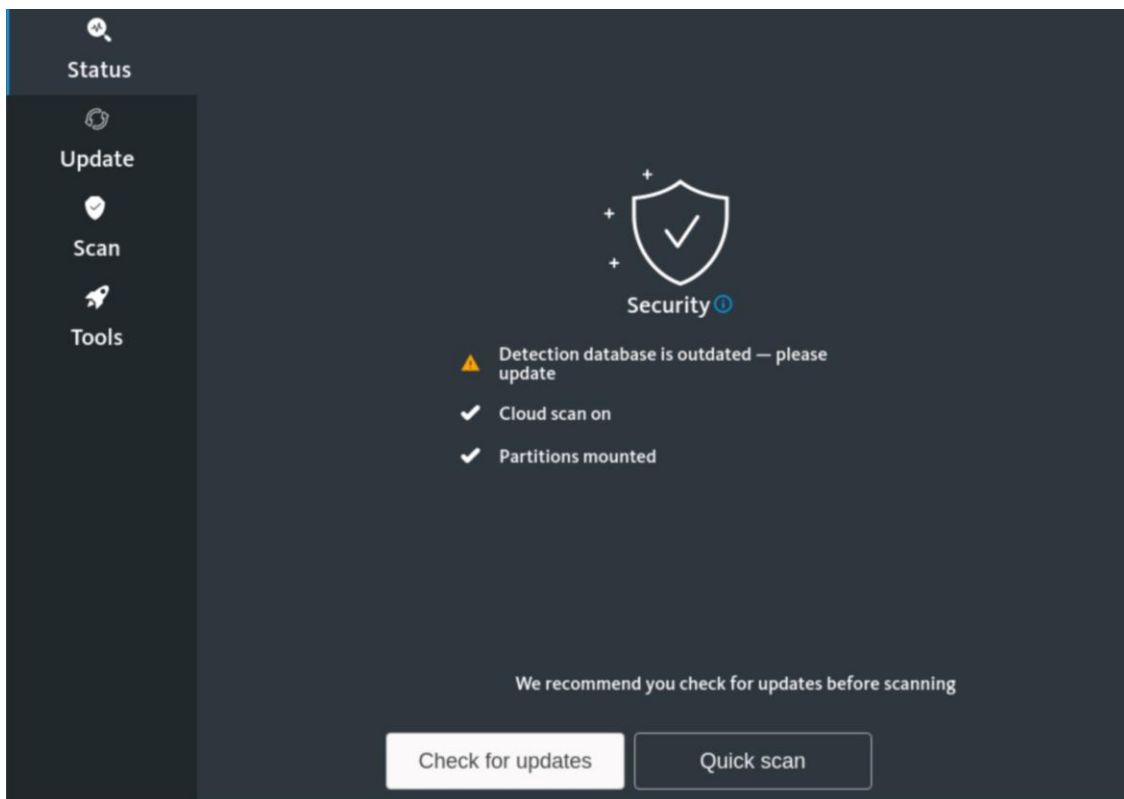
First the boot screen of the Avira Rescue System appears. Select the desired language with the <↑> and <↓> keys and confirm with <Return>.



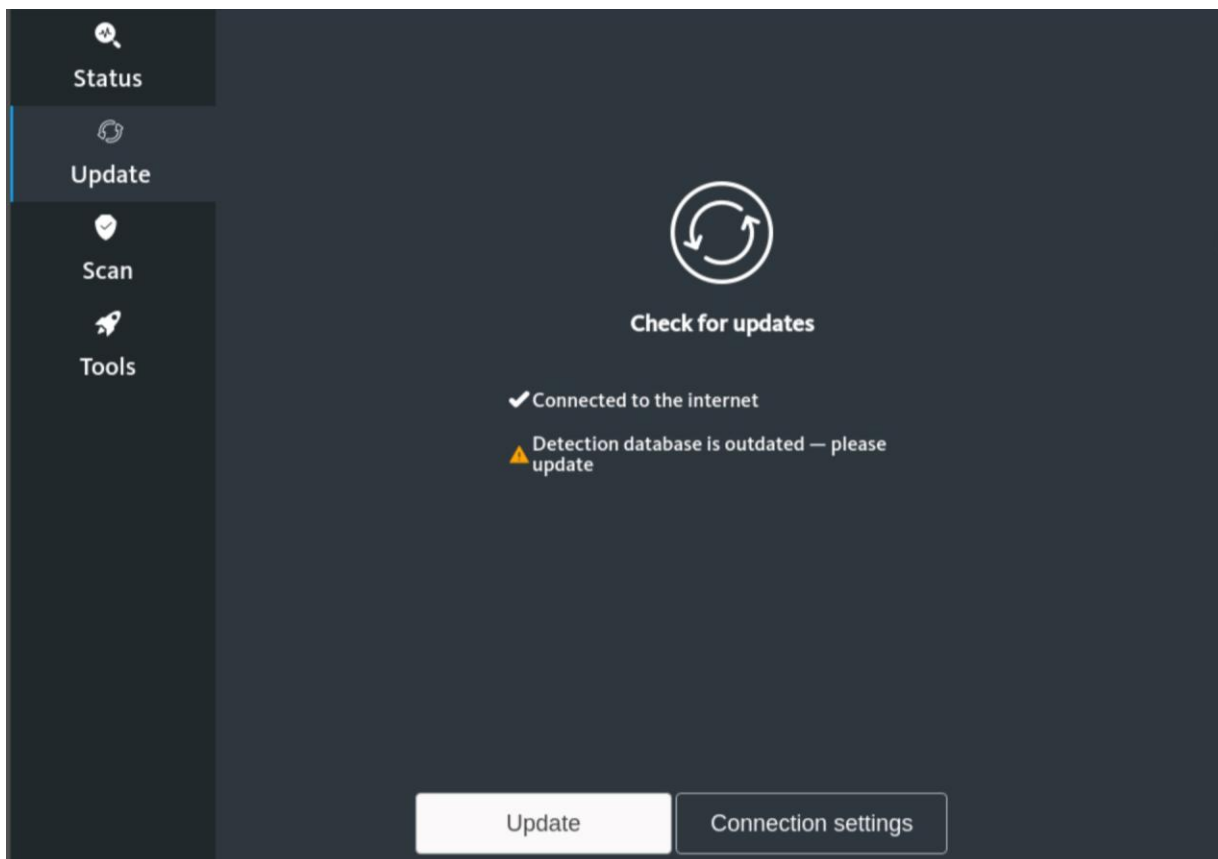
After the boot process, the license agreement is displayed first.



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

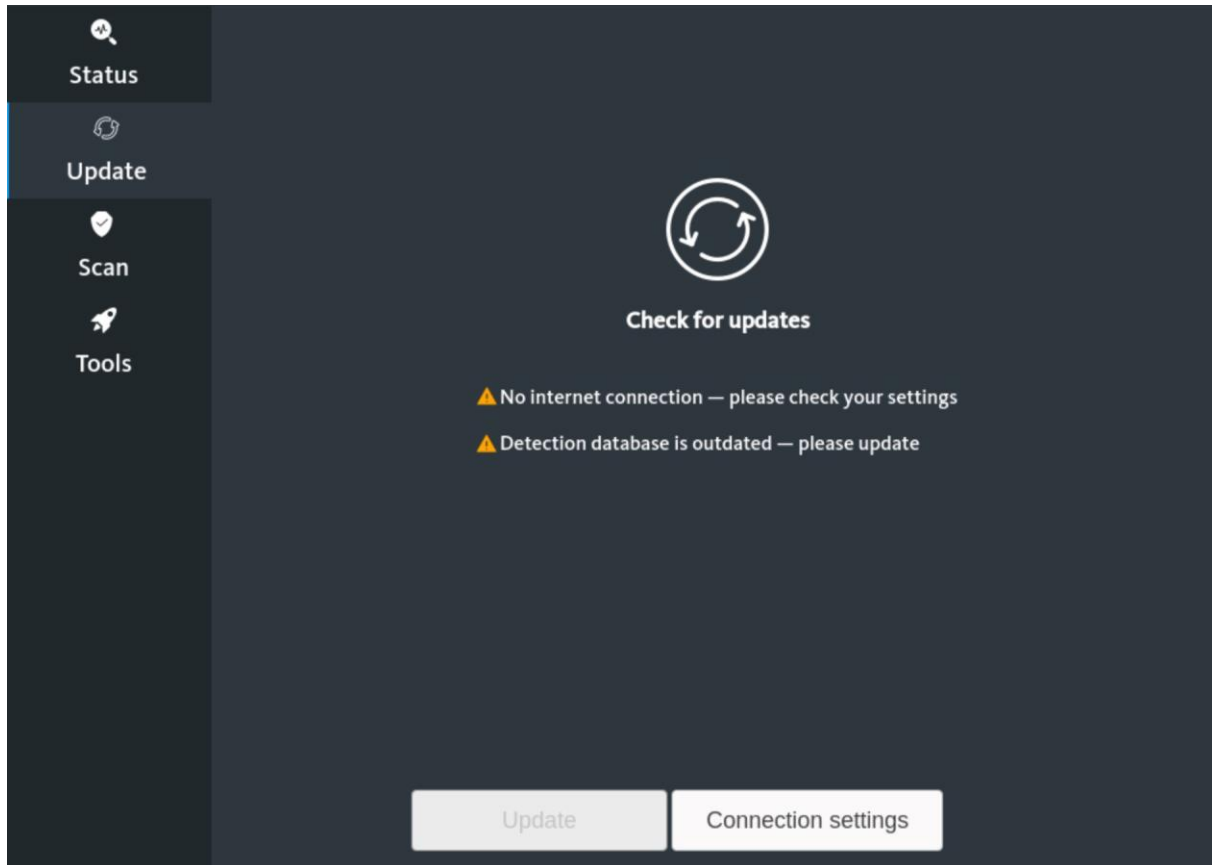


You are informed that the virus pattern definitions are out of date. So click on <Check for updates> to update them. The system can be checked without an update, but this approach is not recommended.



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>.

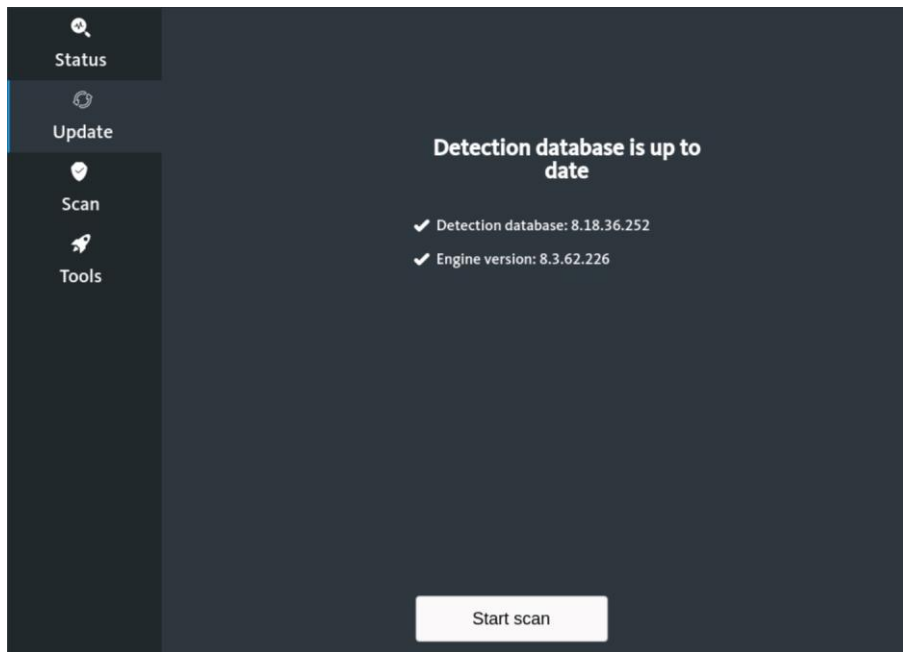
If, on the other hand, you receive the following message <No internet connection...>, the system is not connected to the public network and the <Update> button is inactive. Correct the problem and click <Status> to return to the last step.



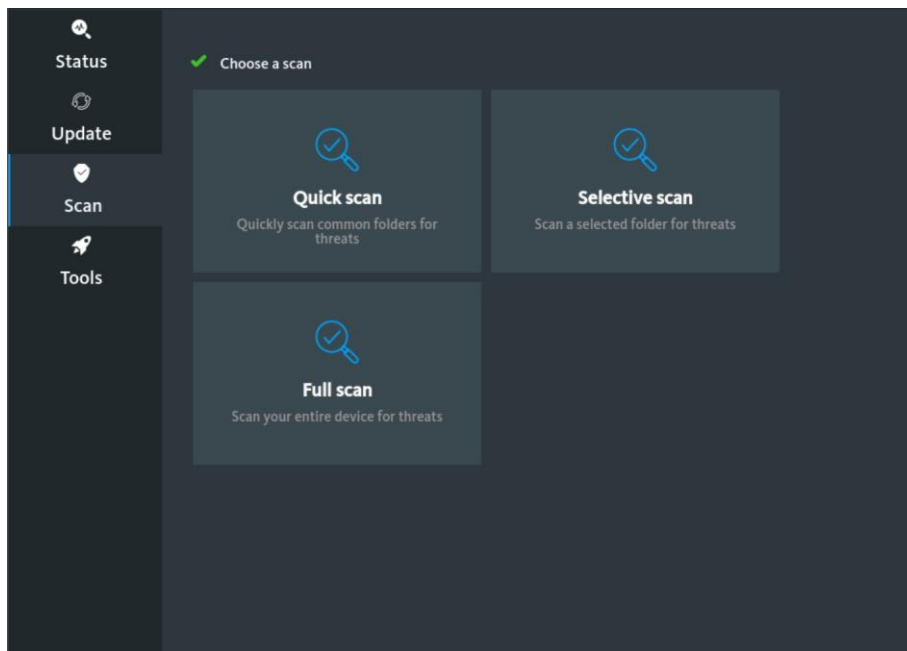
If necessary, take a look at Chapter 5 - Troubleshooting and restart the rescue disk so that the automatic network detection can be carried out again.

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

After clicking on <Update> the update is executed and the message <Updating...> appears. After a while, the following screen will inform you of the successful completion:

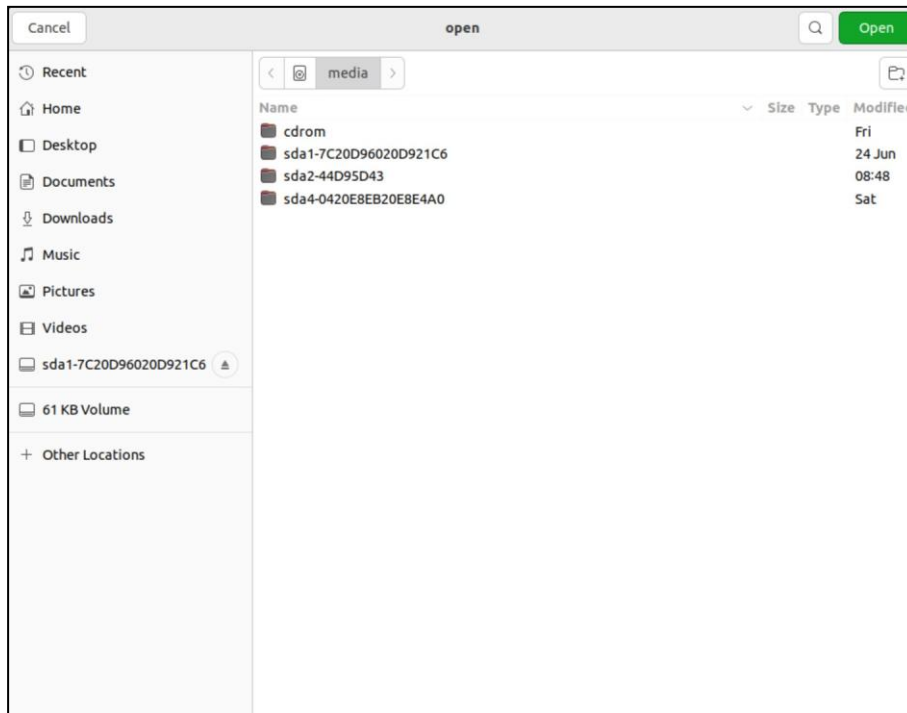


Click on <Start scan>.



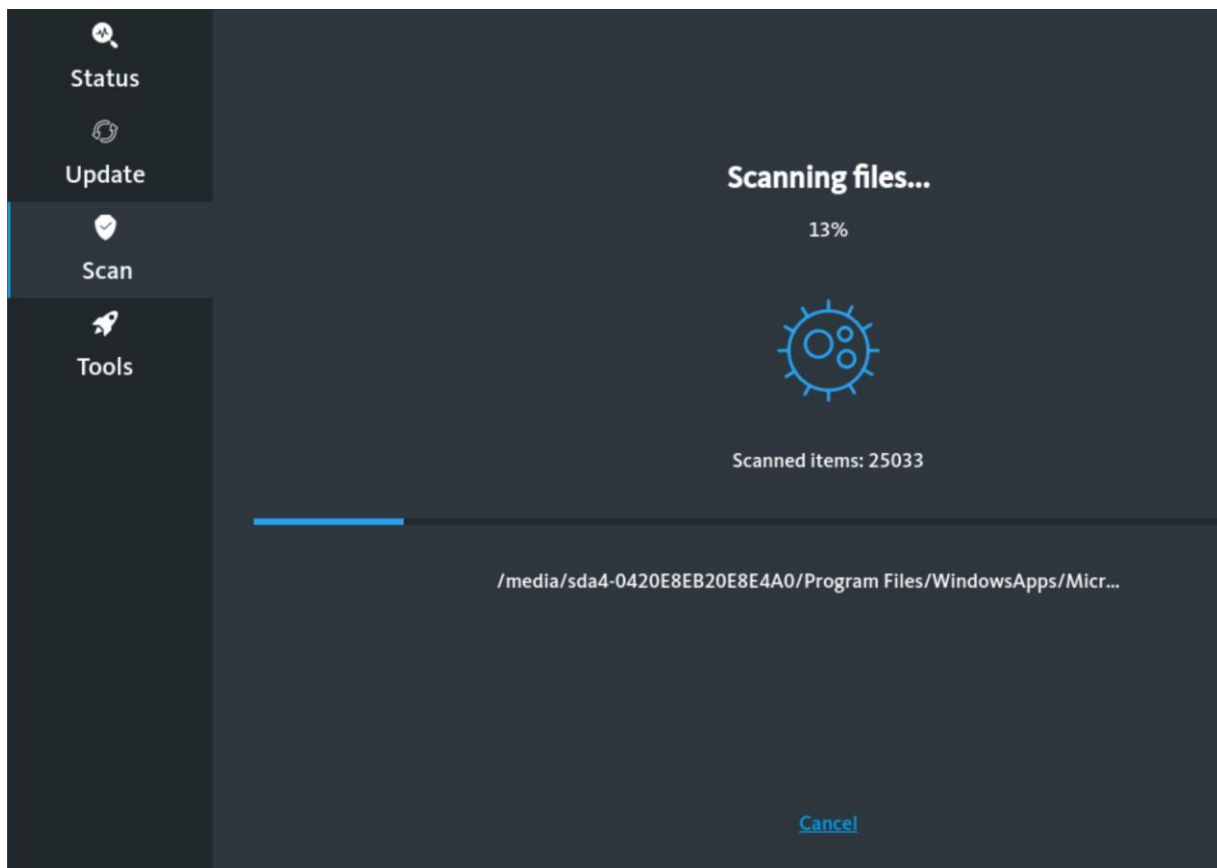
You can now choose between a full scan of the system (<Full scan>) or a scan restricted to certain folders (<Selective scan>). The latter should only be used if the threat has already been restricted to specific directories in advance. If it doesn't, choose the full scan.

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

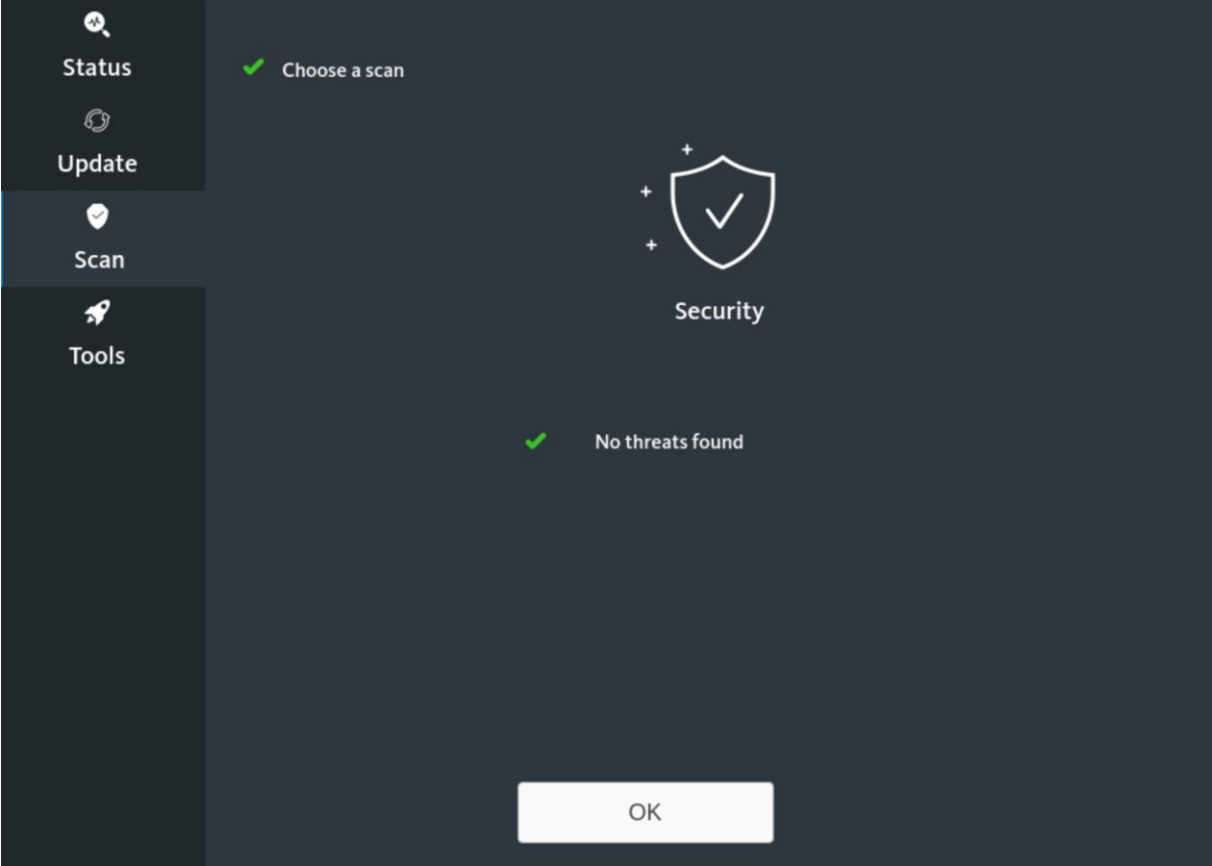


Find the folders or drives to be checked and mark them. You can use the <Ctrl> key to mark several entries in the current view. After clicking on <Open> the check begins.

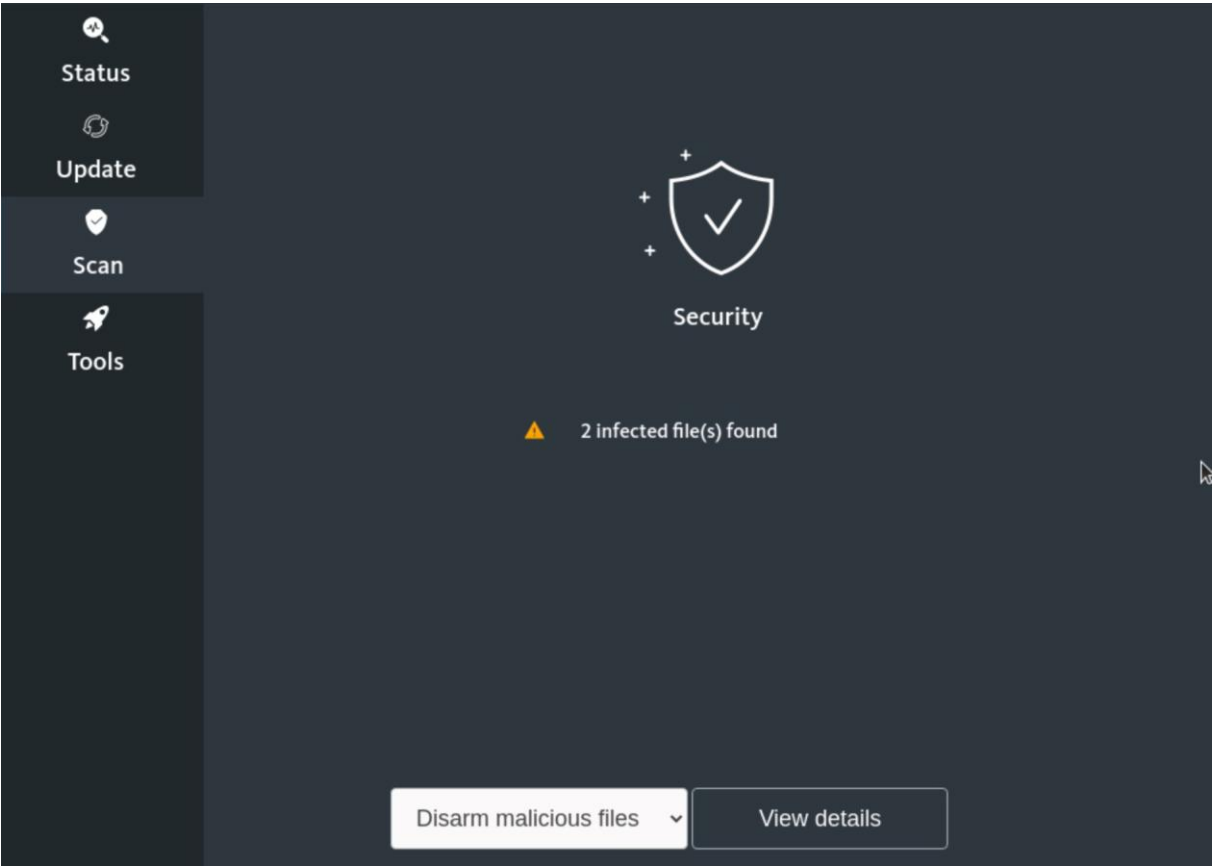
If, on the other hand, you have selected the full check, it will start immediately without any further notification. During the check the screen looks like this, it can be interrupted with <Cancel>.



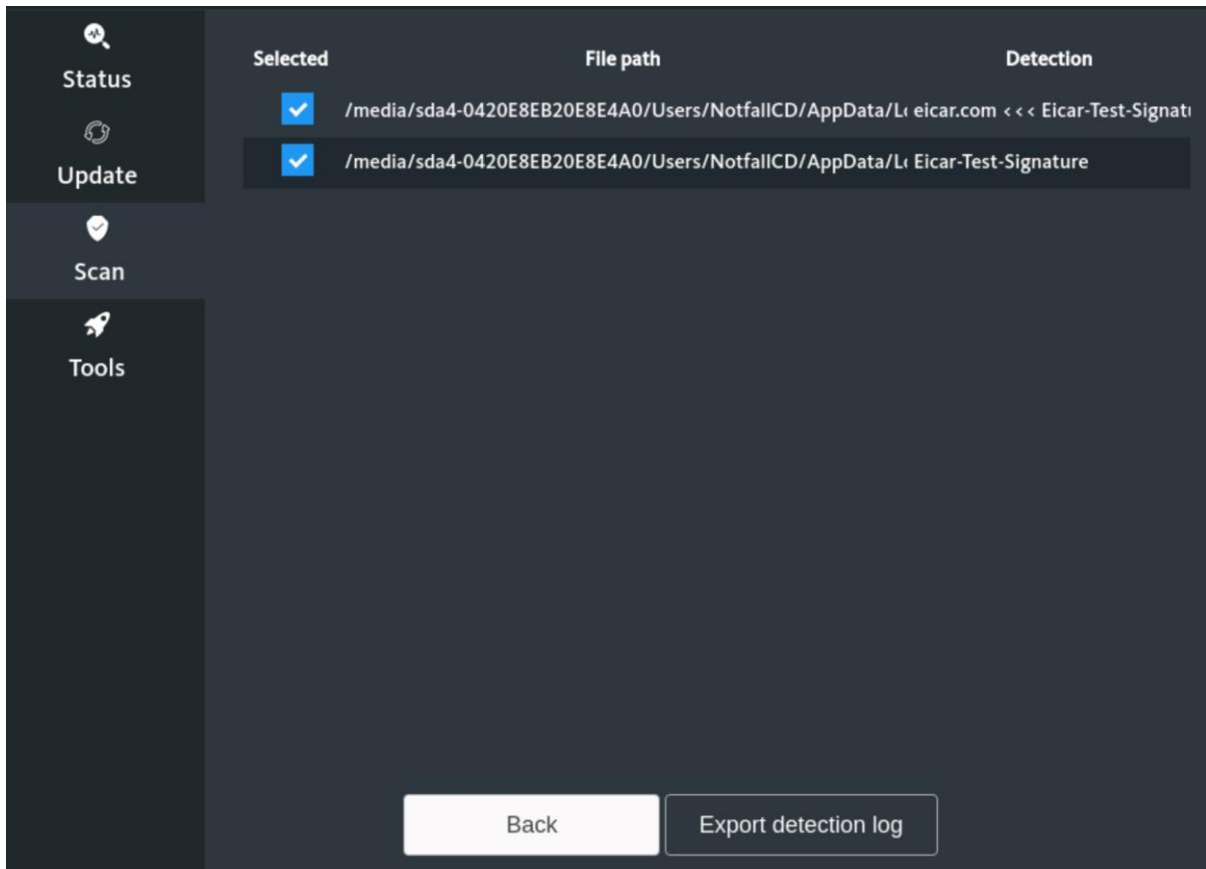
After completing the test, you will receive the following message if no infections were found. Clicking on <OK> takes you back to the main view of the <Scan> section.



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



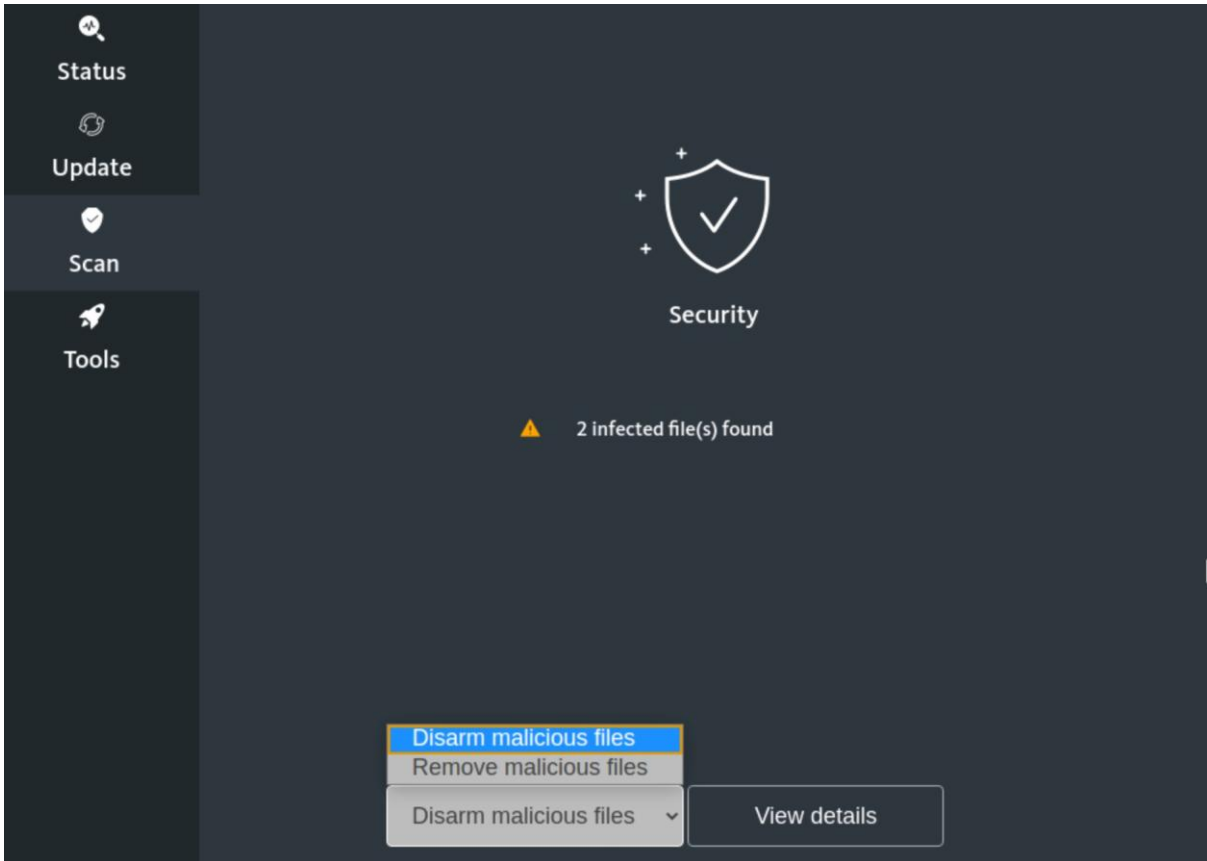
Click on <View details> to get more detailed information about the objects found.



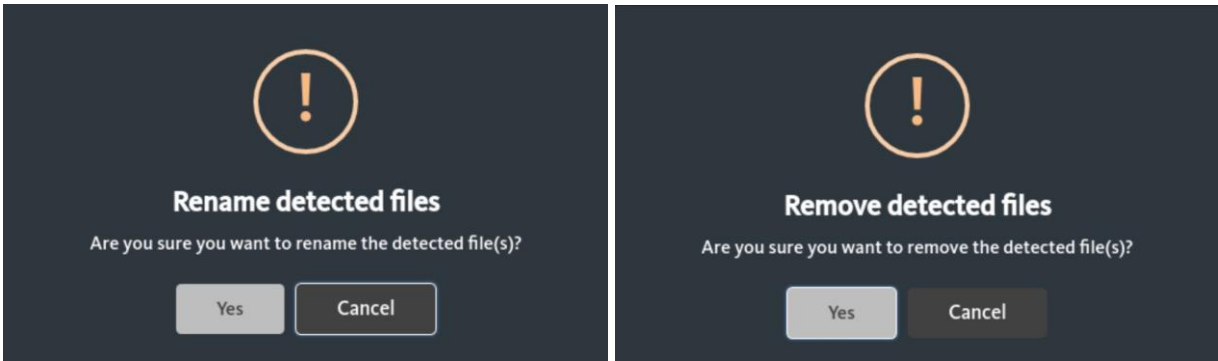
If desired, you can save the information on the system or connected media by clicking on <Export detection log>. An Explorer view appears in which you select the storage location and click <OK>.

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:

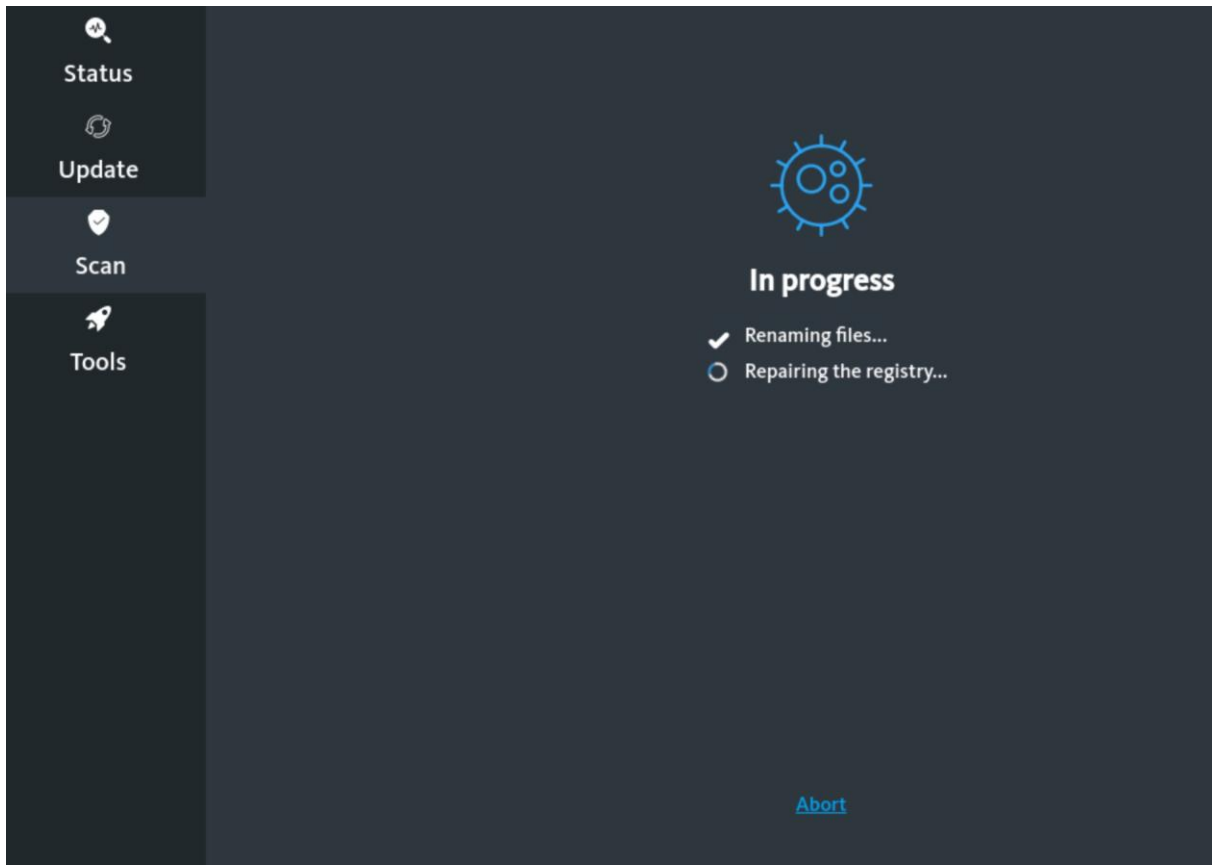
- Disarm malicious files: The infected files are not deleted, only renamed so that they are no longer loaded the next time the system is started. This is useful for files that are (could) still be needed.
- Remove malicious files: The infected files will be deleted. Select this option only if you are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



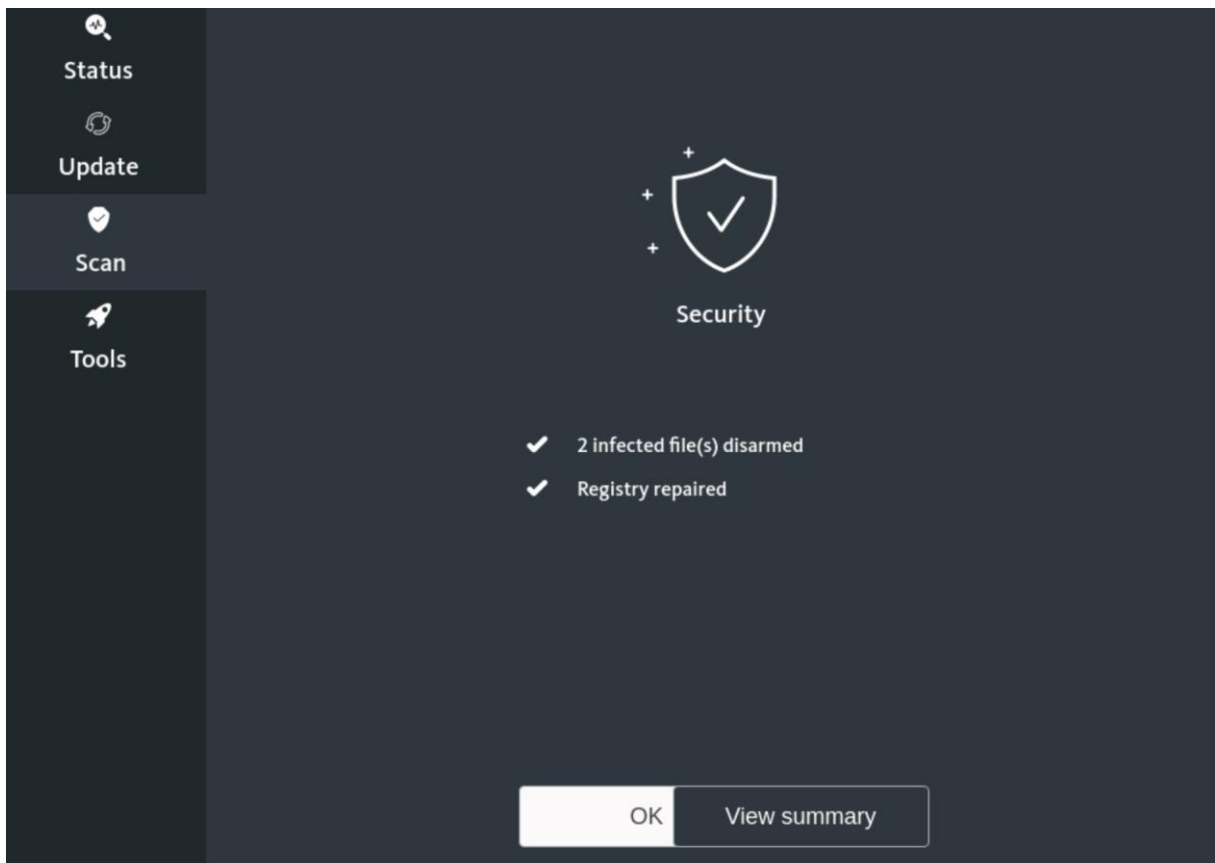
Click on your choice. In both cases you will still be asked to confirm the action:



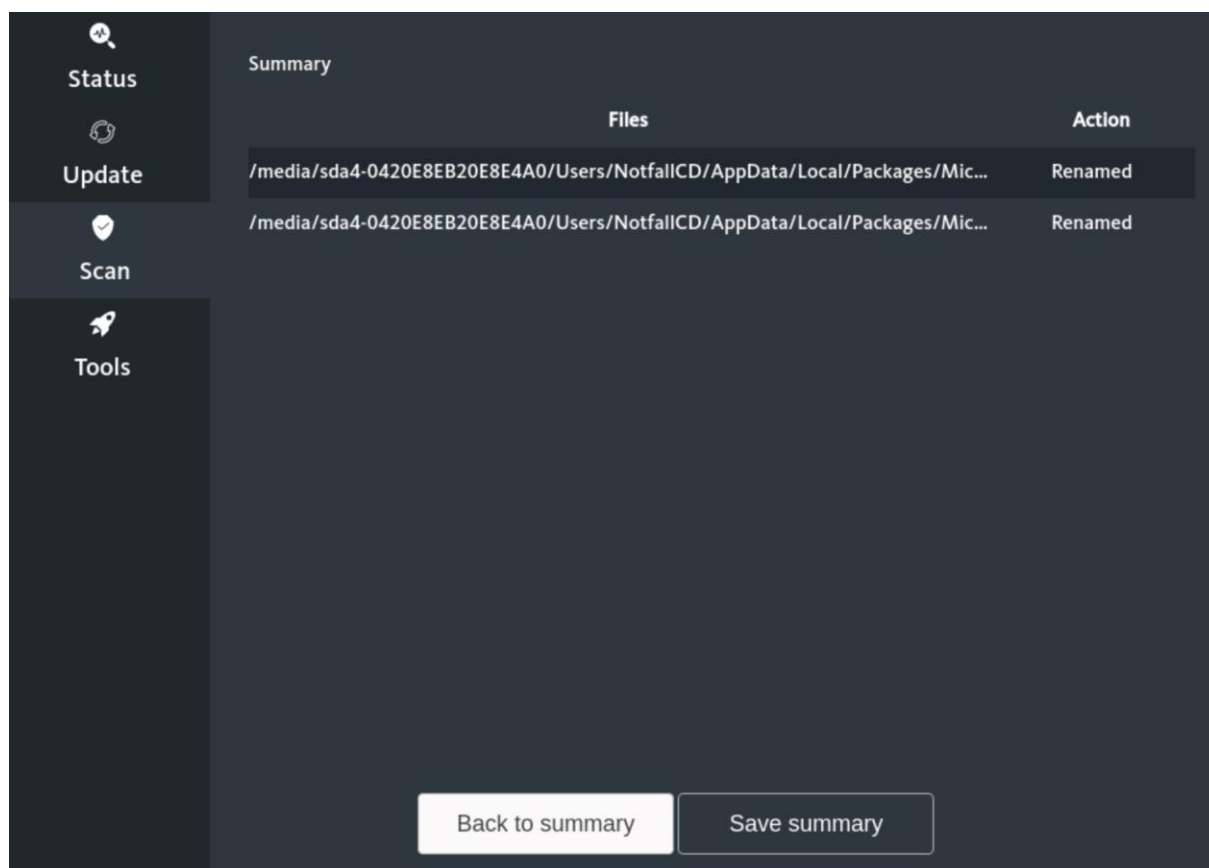
After clicking on <Yes> the action is carried out. During this time you will see the following screen:



After successful completion you will see this message:




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



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>.

5. 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.