

Avira Rescue System

HowTo

Table of contents

1. Introduction	3
2. System Requirements	4
3. Product availability	4
4. Product features	5
5. Using the Rescue System.....	6
5.1 The BIOS setup	6
5.2 Booting the PC with the Rescue System.....	6
5.3 Configuration of the Rescue System.....	7
5.4 Options of the Rescue System	7
6. Restoring renamed files	11
7. Editing the Windows registry	11
8. TeamViewer - Avira support assistance.....	14

1. Introduction

The Avira Rescue System is a product that is able to scan, repair and undo changes of a Windows system that malware might have done in particular to the registry.

The new Rescue System is based on an adapted Ubuntu 12.04 LTS desktop system and runs on that platform as an independent application. Thus, it provides support for a broad range of hardware and drivers and should run on a large number of systems available on the market or used by customers.

The Rescue System is a wizard-based product and therefore easy to use for any inexperienced consumer. The product offers also the possibility to scan and disinfect an operating system via the command line, unfortunately the repair option is not supported in this mode.

The product allows additionally Avira support to remotely access a customer's machine and assist him in repairing his system.

The product scans, disinfects and repairs following operating systems:

- Windows XP
- Windows Vista
- Windows 7
- Windows 8 desktop systems

Note

The product scans and disinfects as well Linux Systems but is not able to repair them.

The product does not support multi-boot scenarios and the product does not scan and repair:

- Boot sectors
- Encrypted files
- Partitions

The product supports the languages English and German and can be [downloaded](#) from the Avira Homepage.

The Avira Rescue System is a free-of-charge product that comes with an inbuilt product license that runs for 12 months. If the license runs out, the user is requested to download another version from the Avira Homepage.

2. System Requirements

To ensure that the product is working properly, make sure to comply with the following requirements:

- 1 GB RAM
- 700 MHz CPU
- CD/DVD drive
- VGA 800x600 (recommended)
- Internet Connection (recommended)

Note

Currently the Avira Rescue System can mount dynamic disks as simple volumes, volume sets, stripe sets, spanned volumes, striped volumes and RAID volumes (Redundant Arrays of Inexpensive Disks), as well as virtual hard disks (VHD). But those are mounted with incorrect drive letters.

3. Product availability

The Avira Rescue System is available as an *ISO* file and as a *EXE* file. The *EXE* file has a CD-Burner included. Both the *ISO* and the *EXE* file can be downloaded from the Avira Homepage.

After downloading the *ISO* file of the Avira Rescue System, you have to burn the file onto a CD that should be provided in a bootable form while being copied.

Note

If you want to save the *ISO* file to an USB stick, please follow the instructions of the [Avira Knowledge Base](#).

After you have created a bootable CD, you have to boot your computer with the CD and start the Avira Rescue System. The Avira Rescue System can help you to restore your system after a serious crash or an infection.

4. Product features

- **Dash home**
This option includes a repository of several applications and is divided into 4 main categories: *Recent Apps*, *Installed Apps*, *Folders* and *Search Music Collection*
- **The Avira Rescue System Wizard**
The Wizard helps scanning the system for threats and repairs the system in case of damage
- **Contact Avira Support**
If any problems occur during the repair and there is need for technical assistants do not hesitate to contact the support section of Avira
- **Start Team Viewer**
This option helps to establish a remote desktop connection with an Avira expert
- **Start Avira Registry Editor**
The Avira Registry Editor allows you to modify registry keys and value data
- **Firefox Web Browser**
The implemented web browser helps you to get in contact with the internet
- **Home Folder**
Within this option you can explore the folders of your system
- **GParted Partition Editor**
The Partition Editor mounts your system partition and helps editing and modifying the partition
- **Terminal**
The integrated Terminal helps to restore manually renamed files in case of a mistaken detection
- **System Settings**
This option contains a repository for *User* and *Hardware* settings

5. Using the Rescue System

If you created your bootable media successfully, you have to boot as next your PC via the Rescue System CD.

5.1 The BIOS setup

In case your computer does not boot from the CD drive, you may have to change the boot priority of your BIOS (Basic Input Output System). This function can be configured in the setup options of the computer's BIOS. To access the BIOS, press several times the setup key during the start up process of your Windows system.

Note

The setup key differs with each PC. On some computers, the name of the key used to access the setup functions is displayed on your screen during the start up process. The most frequent keys are: Del, F2, F12, F1, F8, Esc, ...

Once you enter the computer's BIOS, use the arrow keys to navigate to the Boot section. Move the item CD/DVD / CD-ROM Drive between the entries "Removable Devices" and "Hard Drive".

Save the changes and restart the computer.

5.2 Booting the PC with the Rescue System

- **The Welcome screen**

Once the Avira Rescue System has booted, the Ubuntu® based live system opens the EULA (End User License Agreement) that has to be accepted to open the Avira Rescue System application with its Welcome screen.

If you do not accept this license agreement, you can not use the Avira Rescue System, but you may still use the functionalities available on the Ubuntu desktop.

On startup of the GUI, the product checks for an Internet connection that is required to perform an update of the detection technology. If no connection is found, the user will be prompted to establish one via the displayed link.

Note

If there is no internet connection available the product will use the detection (engine and vdf) that is part of the ISO file.



The Welcome area of the Avira Rescue System explains the three scan and repair functions of the Wizard. The Avira Rescue System will not delete infected files but renames detections to `.rend` files, in order to make them still accessible.

5.3 Configuration of the Rescue System

The Avira Rescue System is pre-configured, the Wizard uses an inbuilt configuration that is not available to the user to make sure that the scan and repair always delivers the best possible results and facilitate the use of the product. Any individual configuration by the user is not supported.

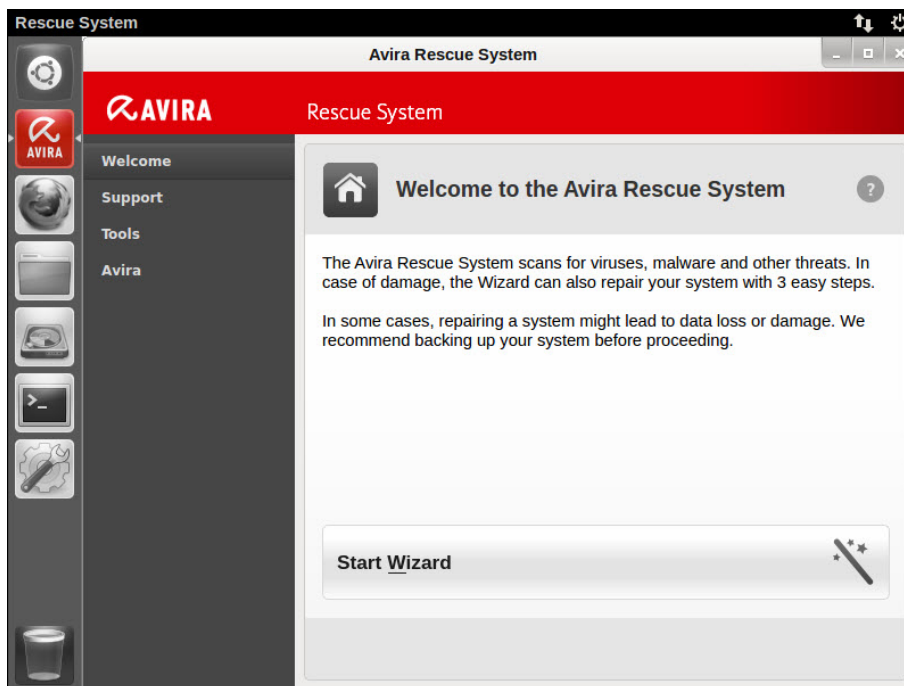
5.4 Options of the Rescue System

• Start Wizard

The Wizard of the graphical application helps you to scan and repair your system. The Wizard guides you step-by-step through important functions of the rescue system.

The Wizard consists of 3 pages:

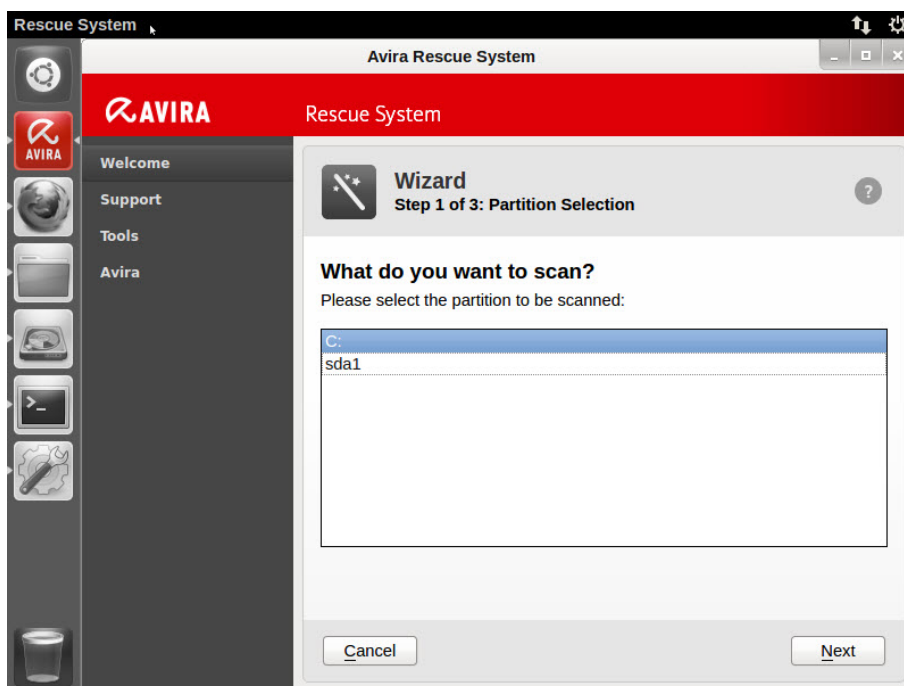
- Partition Selection
- Scan and repair
- Result Summary



• Partition Selection

To optimize the scan and repair performance the user first selects the specific partition he wants to scan and repair. All partitions (NTFS or FAT formatted) found on the system are automatically mounted and displayed.

Multi-select of partitions is not supported, partitions have to be scanned one by one.



The product detects if a system is in hibernation mode (NTFS only, hibernation on FAT systems is not supported). Partitions of hibernated systems are mounted read-only. You may trigger a scan on hibernated partitions, but detected threats will not be removed and the system will not be repaired. Moreover, you can not use the Avira Registry Editor as long as your system is in hibernation mode.

The user can then choose to:

- restart his system and finish the hibernation mode manually
- have the Rescue System finish the hibernation mode for him
- start scanning and decide when a suspicious file is detected

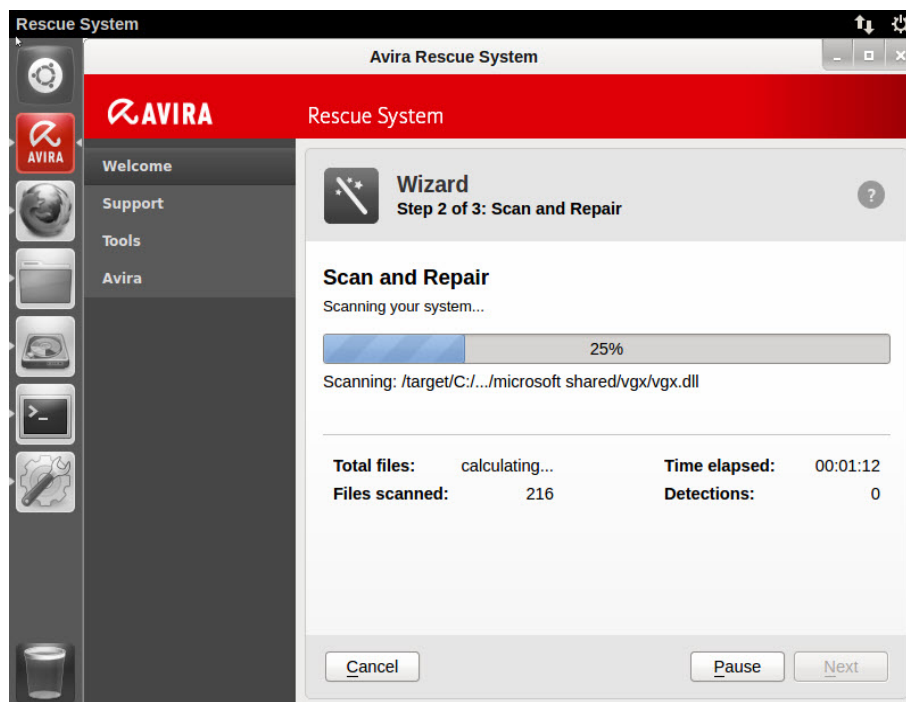
Note

The Avira Rescue System can exit the hibernation mode first and then starts the scan. Please note that exiting the hibernation mode may lead to loss of data.

If the required partition is selected click on **Next** to start the "Scann and Repair" process.

• Scan and Repair

The "Scan and Repair" area displays a progress bar during the scanning process. In the first instance, the scanner updates the Virus Definition File (VDF) and the scan engine. If no Internet connection is established, the scanner searches for infections with the VDF and engine versions found on the ISO file.



During the scan process the total number of files to be scanned is calculated. Depending on the amount of compressed files, such as .zip and .rar archives, the scan process may take some time. The scan engine uses a recursive scan: Archives in archives are also unpacked and scanned for viruses and unwanted programs. The files are scanned, decompressed and scanned again. This process reduces the scanning speed.

Suspicious files that are detected during the scan, are automatically renamed so as to render them harmless. There is a command line tool available to undo the renaming for all files, or specific files should there be a false positive among them.

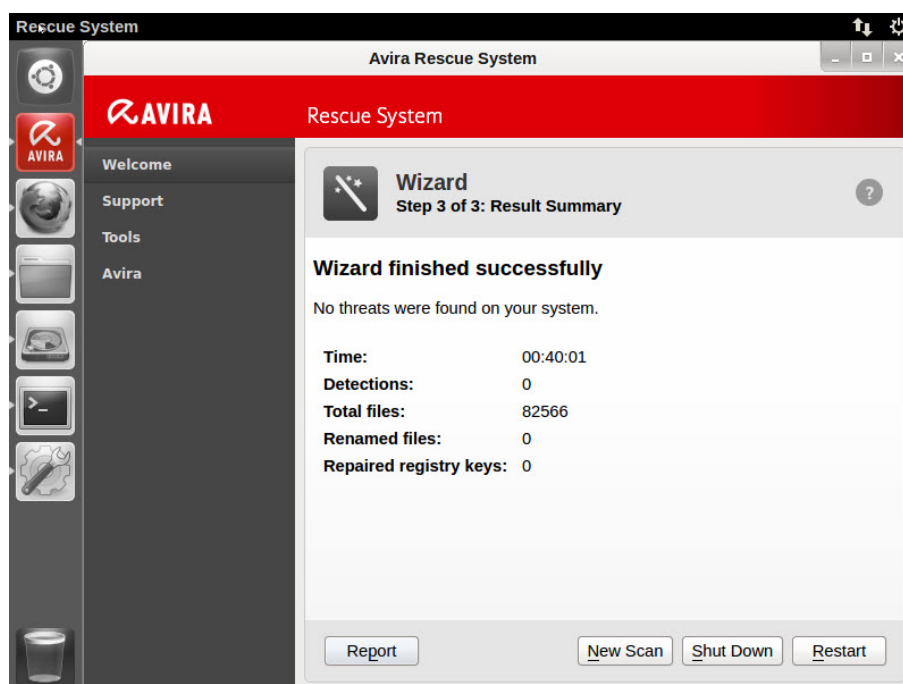
The repair is done as an integral part of the scanning and must not be started separately by the user. Click **Next** to see the result of the scanning process after the scan is completed.

After the scan and repair is finished the user can start a new scan, restart his system or shut down his system.

• Result Summary

The Results area shows whether your system was completely cleaned and repaired. By clicking the **Report** button, details about the detections will be displayed.

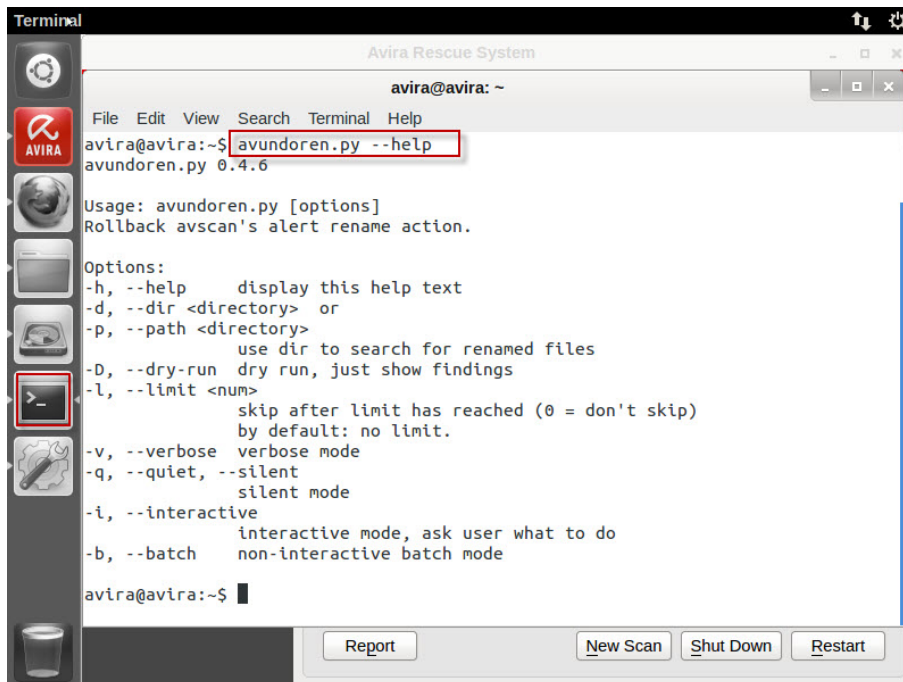
The results of a finished scan and repair run can also be displayed as an HTML report which can be printed out.



6. Restoring renamed files

The Avira Rescue System renames possible detections to `.rend` files. You can restore these files to regain access. Therefore, open the Terminal in the side bar and enter the command `avundoren.py` and press **Enter**.

To see all options of the `avundoren.py` command, enter the following line:
`avundoren.py --help`



```
Terminal
Avira Rescue System
avira@avira: ~
File Edit View Search Terminal Help
avira@avira:~$ avundoren.py --help
avundoren.py 0.4.6

Usage: avundoren.py [options]
Rollback avscan's alert rename action.

Options:
-h, --help          display this help text
-d, --dir <directory> or
-p, --path <directory>
                    use dir to search for renamed files
-D, --dry-run      dry run, just show findings
-l, --limit <num>
                    skip after limit has reached (0 = don't skip)
                    by default: no limit.
-v, --verbose      verbose mode
-q, --quiet, --silent
                    silent mode
-i, --interactive
                    interactive mode, ask user what to do
-b, --batch        non-interactive batch mode

avira@avira:~$
```

The Avira Rescue System displays a list of information about the files:

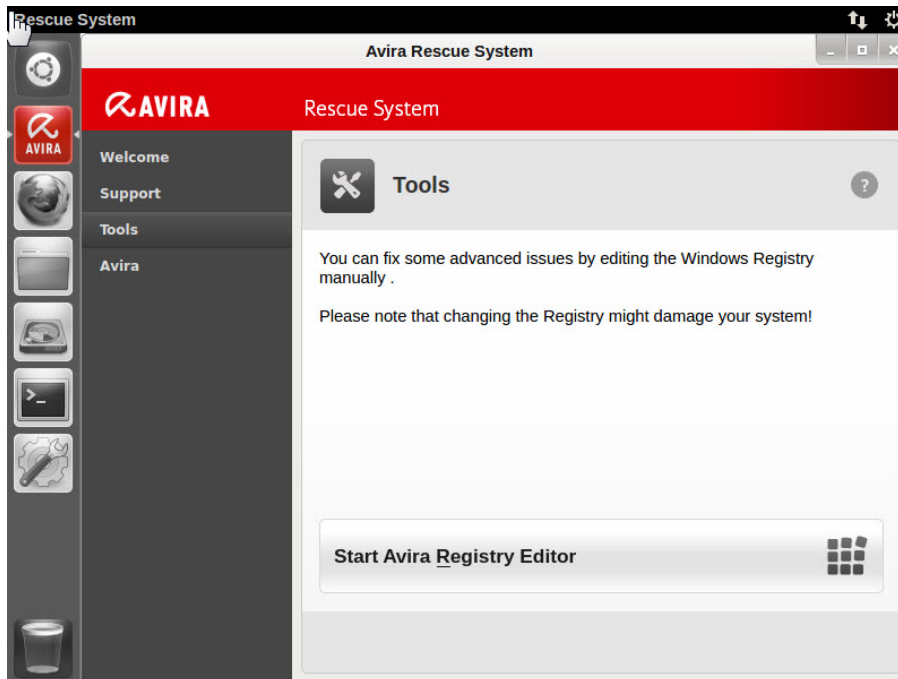
- File type
- File scan info
- File path
- Alarm
- Alarm-URL

Please navigate through the list entries and confirm the restore of files by entering `yes` where you are prompted. Enter `no` if you do not want to restore a file.

7. Editing the Windows registry

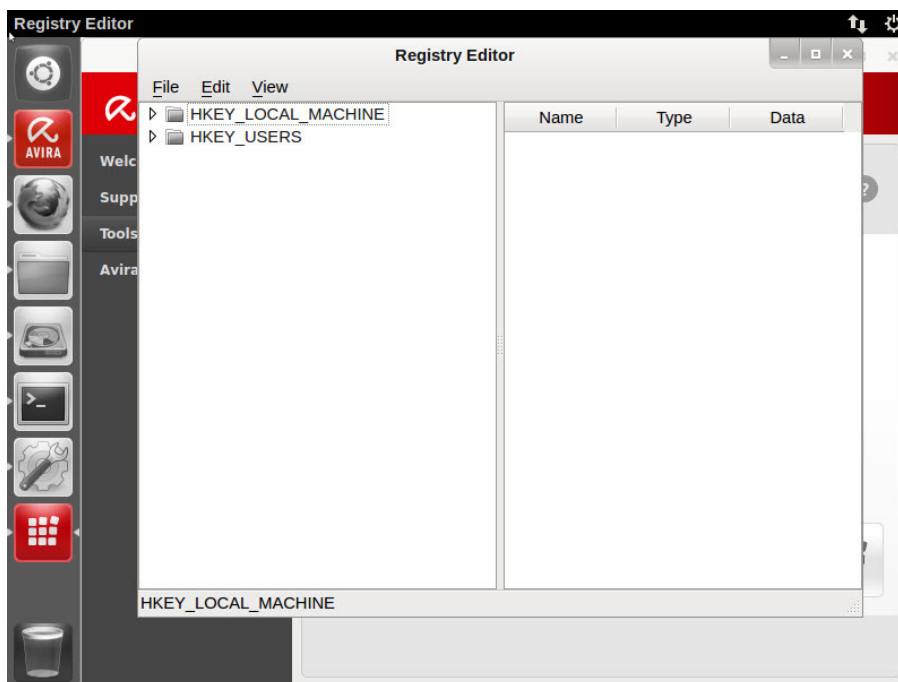
The product is able to access the registry of a local Windows system. This is needed for the inbuilt repair functionality. But the registry access is also available via the GUI to allow manual editing of the registry. This registry editor is developed by Avira and covers the main features as provided by the Windows Registry Editor.

To edit various configuration settings of your Windows system, you can open the graphical interface of the Avira Registry Editor. (*Avira/Tools/Start Avira Registry Editor*)



The Avira Registry Editor allows you to create, delete, edit and rename registry keys, subkeys, values and value data.

By default the *HKEY_LOCAL_MACHINE* and the *HKEY_USERS* hives are displayed.



Note

Change entries of the Windows registry only, if you are an expert user. Editing the registry may damage your Windows system.

We recommend to backup the registry first before making any changes. Each incorrect modification of the registry might occur serious problems. In case any problem occurs afterwards, you can restore the registry at any time.

Note

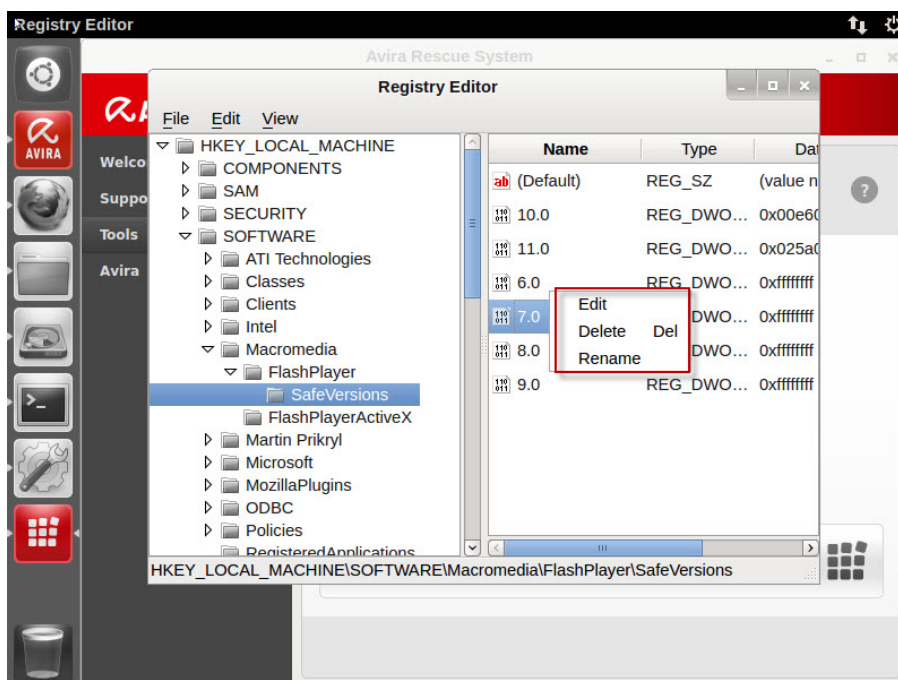
For more information about how to back up and restore the registry, click the following link to view the article in the [Microsoft Knowledge Base](#).

The following task contains steps that tell you how to modify the registry.

In the side bar of the application click on *Tools > Start Avira Registry Editor*. The Avira Registry Editor table displays the *Name*, the *Type* and the *Data* of the value.

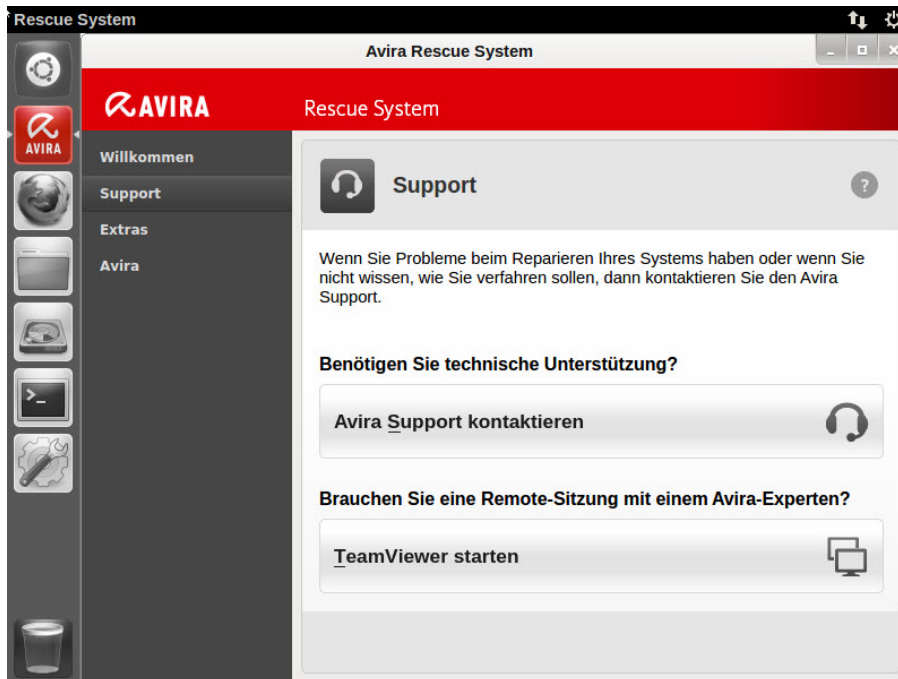
Right-click the entry you want to edit:

- Edit, delete or rename the name of a value
- Confirm a value removal
- Create new key types
- Create different kind of data values



8. TeamViewer - Avira support assistance

The Avira Rescue System offers the Avira branded Teamviewer client that allows users to have their machine remote connection and repaired by the "Avira Support". Therefore, click on **Support** in the side bar. You have two options to contact the Avira Support department.



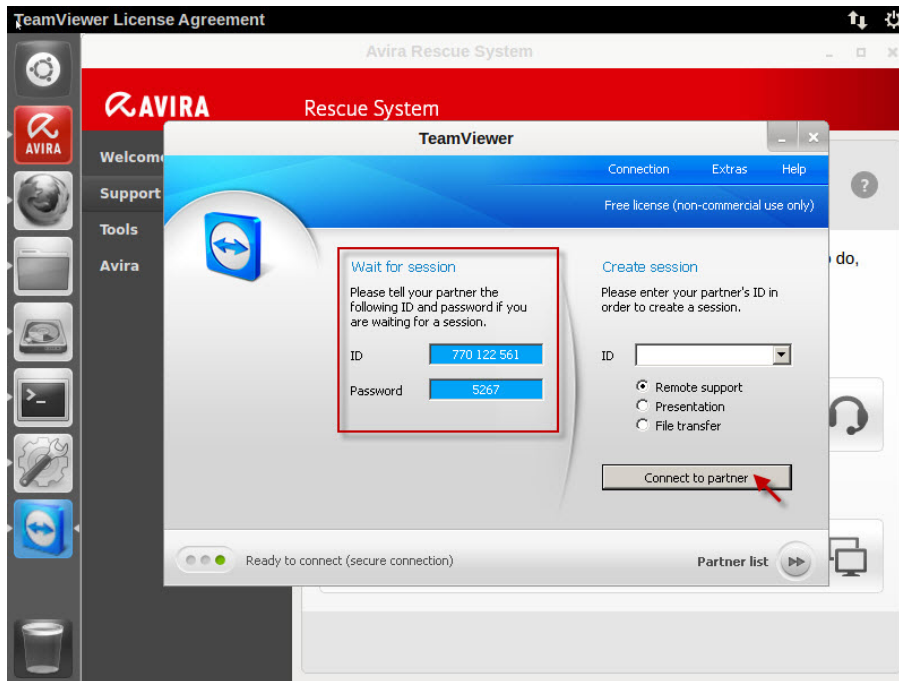
- Click on **Contact Avira Support** and access the Avira Support website. Thereafter, choose between different offers to find help
- Click **Start TeamViewer** and establish a remote connection to let an Avira expert have a look at your system.

If you decide to get help via the TeamViewer click on **Start TeamViewer** and **Accept the TeamViewer Disclaimer**.

- Dial the number of the [Avira Support hotline](#), considering if you have a Free or Paid product version
- Tell the Avira support expert the *ID* and the *password* displayed
- The Avira support expert will remotely log in to your computer and control your mouse while explaining the action performed

Note

Please do not interfere in trying to use the mouse by your own while the expert is working on your system.



This manual was created with great care. However, errors in design and contents cannot be excluded. The reproduction of this publication or parts thereof in any form is prohibited without previous written consent from Avira Operations GmbH & Co. KG.

Issued Q3-2013

Brand and product names are trademarks or registered trademarks of their respective owners. Protected trademarks are not marked as such in this manual. However, this does not mean that they may be used freely.



live free.™