SecuPerts - First Aid Kit

Table of Contents

1 What is the SecuPerts - First Aid Kit?

The "SecuPerts - First Aid Kit" is a separated operating system which can either be run from DVD or from an USB flash drive. It offers various repair tools, anti-virus software and the ability to save data when Windows itself can longer be started.

- **Virus scan:** Malicious software such as viruses or malware are often the cause of recurring crashes and system instability. A virus scan will check your computer for these issues and also tries to solve them.
- **Data backup and recovery:** Does your computer have problems recognizing a hard drive? The data recovery has the possibility to save data even from corrupted hard drives. Backing up your data is also not a problem.
- **Network and internet:** The built-in internet browser allows you to use the internet anonymously. Your normal operating system remains unaffected, thereby espionage and malicious software stand no chance.
- **Wipe hard drive:** Before you sell or dispose your hard drive, the data should be removed first. Simple deletion of the files doesn't grant the wanted result. The SecuPerts - First Aid Kit however makes sure that no file will be left on the hard drive.
- **USB installation:** If your device does not offer an optical drive, such as e.g. netbooks, the SecuPerts - First Aid Kit can still be used. Simply install the software on an USB flash drive and you can boot it from there.
- **Remote maintenance:** If you are stuck in finding the problem of your system you can use the remote maintenance options to let a friend assist you with troubleshooting the issues.
- **Workspace:** The integrated desktop mode can be used as a workstation, where you can find various programs like media player, e-mail clients and internet browser.

2 Booting process

The "SecuPerts - First Aid Kit" can be started using a bootable DVD or USB flash drive. If you do not have an optical drive, you can also use a USB flash drive. The creation of a bootable USB flash drive requires an optical drive for one time. You could use a friends drive for this (more details under "USB installation").

The First Aid Kit should start automatically. If this is not the case, you may need to change the boot order of your system. You can achieve this by pressing one of the following buttons on startup (depending on your system): *F2, F8, F9, F10, F11, F12, Alt, Esc,* or *Tab*. Afterwards you can select the medium you are using from a menu. If this does not work you may need to change the boot order in the BIOS manually.

2.1 Access BIOS

Start the computer's BIOS immediately after booting your PC. The method for starting it differs depending on the model of the motherboard. The required key combination will usually appear during the startup process. Common keyboard shortcuts that need to be pressed directly after system startup are *Delete, F2, F10*, and *Esc*. Netbooks usually require an additional press of *Ctrl* and *Alt.* If none of these combinations work, you should do a Google search with the term 'BIOS access for [your board]'.

2.2 Change boot order

The BIOS interface usually has a button named 'Boot', 'Boot Settings' or 'Boot Options'. Maybe you have to go to advanced options first. After you found the correct option, you can select your DVD or USB drive as the first boot device.

2.3 Start from UEFI PCs

Newer versions of Windows (Windows 8 and above) usually use the BIOS successor UEFI ("Universal Extensible Firmware Interface") in combination with "Secure Boot". SecuPerts - First Aid Kit also uses such a signed loader.

If the setup does not start automatically you can start it manually from windows. Open the "Modern UI" in the PC settings. Then, click on "General" and "Restart Now". In the appearing menu select "Using a Device" as your setup media.

Answer the question whether adding the hash value of the file is permitted with "Yes". Repeat this step for the file "LINUX.EFI". Now you can close the hashtool with "Exit" and start the "CDI forensics system". This procedure has to be performed only one time. Afterwards, the hash values are stored permanently.

2.4 SecuPerts - First Aid Kit does not boot

The SecuPerts - First Aid Kit is based on the Linux system 'LessLinux'. It supports a variety of hardware configurations. In rare cases it may happen that just your system is not supported. You can try those fixes if you are affected:

- Restart your PC in 'Legacy only mode. Users with Windows 8 or higher should reactivate 'UEFI only' after they are done.
- Try to use the available boot parameters, which can be reached through the menu item 'Safe Start' in the boot menu.

3 SecuPerts - First Aid Kit boot menu

The "SecuPerts - First Aid Kit" usually starts from the boot menu screen. You can proceed by either pressing the *Enter* key or automatically after 30 seconds. Sometimes a few parameters have to be changed. These can be accessed via the menu item 'Safe Start'.

3.1 Boot menu

- **Boot SecuPerts - First Aid Kit:** Directly starts First Aid Kit.
- **Safe startup:** Adjust various boot parameters.
- **Boot from 1st harddisk:** Exit the boot menu and start your normal operating system.

3.2 Safe startup

- **Go back:** Closes parameter selection and returns to the boot menu.

- **Start with default settings**: System start without any changes.
  - Start SecuPerts - First Aid Kit (default settings): The same as starting from the boot menu.
  - Start SecuPerts - First Aid Kit (no copy to RAM): If your system does not have that much RAM you can use this option.

- **Start with safe settings:** Boots the system under consideration of possible driver problems.
  - Safe ACPI settings + VESA graphics 1024x768: Boots the system with a resolution of 1024x768. It also affects the energy management. Use this option if you have any problems with your graphic drivers.
  - Safe ACPI settings + VESA graphics auto: Boots the system with the most compatible resolution using the VESA protocol. It also affects the energy management.

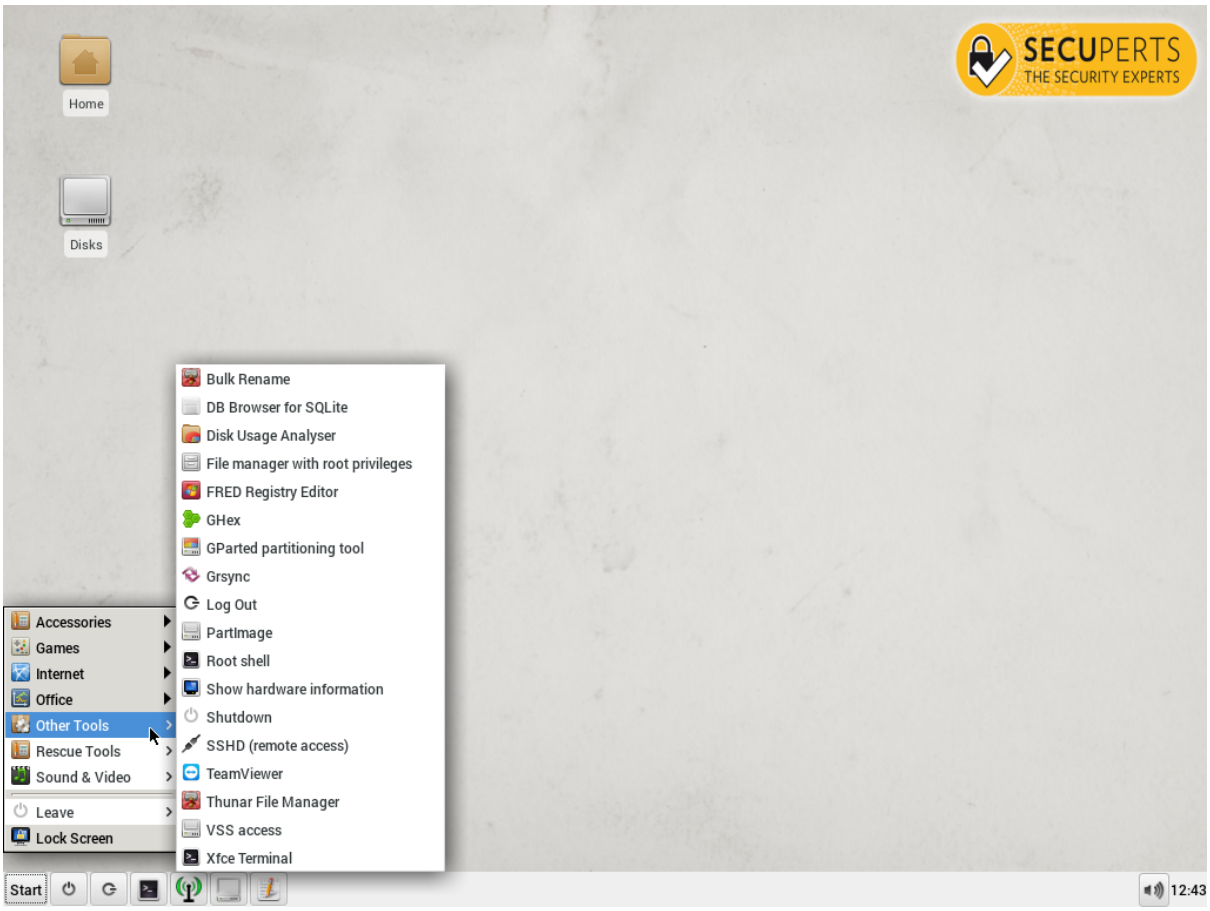
- Safe ACPI settings + Xorg graphics auto: Boots the system with the most compatible resolution using the Xorg protocol. It also affects the energy management.
- VESA graphics 1024x768: Boots the system with a fixed resolution of 1024x768.
- VESA graphics auto: Boots the system with the most compatible resolution using the VESA protocol.

- **Allow remote access (VNC or SSH):** Here you can remote maintain your computer. This should only be used in a known environment.
  - Unsafe remote VNC + local GUI: Allows you to see what is currently done at your computer.
  - Unsafe remote VNC + no local GUI: Disables visual representaton as if your graphic card would not be working anymore.
  - Reverse VNC + local GUI: Allows remote maintenance in an own window. The target computer has to be set up for this.
  - Reverse VNC + no local GUI: Allows remote maintenance in an own window. The target computer has to be set up for this. Disables visual representaton as if your graphic card would not be working anymore.

4 Start screen

After finishing the startup process of the SecuPerts - First Aid Kit you have to accept the license agreement. You are now seeing the start screen, where the most important tools like 'Backup your data', 'Recover lost files' and 'Search for viruses' etc. are located.

The screen icon in the upper right corner leads you to the desktop mode, where you have access to even more tools like office software, browser, an e-mail client or a data explorer. If you are an experienced you user you can also find more recovery tools and the Linux command line. You should not make use of these functions, if you are not experienced enough.



- **Start menu:** Here you can find a variety of office, internet and multimedia software, as well as the previously mentioned recovery tools.

  - Accessories: Access network shares, Archive Manager, Calculator, DB Browser for SQLite, File Manager, FileZilla, Install additional software, Install to USB drive, KeePassX, Midnight Commander, Mount CIFS or WebDAV shares, Mousepad, Screenshot, Share drives, Start VNC server, Terminal Emulator, TrueCrypt, Virtual Keyboard, WiFi Accesspoint
  - Games: Chess. Five or More, Mahjonggm, Mines, Nibbles, Quardapassel, Robots, Swell Foop
  - Internet: Email client, Instantbird (Messenger), Web Browser, Wicd Network Manager
  - Office: AbiWord (Notepad), Document Viewer (for PDFs), Gnumeric Spreadsheet
  - Other Tools: Bulk Rename, DB Browser for SQLite, Disk Usage Analyser, File manager with root privileges, FRED Registry Editor, GHex, GParted partitioning tool, Grsync, Log Out, PartImage, Root shell, Show hardware information, Shutdown, SSHD (remote access), TeamViewer, Thunar File Manager, VSS access, Xfce Terminal
  - Rescue Tools: Check SMART, Clone hard disk, Convert disk to VM image, Create rescue image, Disk shredder, Find lost partitions, QPhotoRec, Reset password, Reset windows shell, Resotore lost files, Xfburn
  - Sound & Video: Audacious, Audio Mixer, Brasero, Ristretto Image Viewer, VLC Media Player, Xfburn

- **Shutdown:** Shuts down the system after a confirmation.
- **Switch to assistant:** Returns to the start screen.
- **Xfce Terminal:** Opens the Linux terminal.
- **Wicd Network Manager:** Check current internet connection.

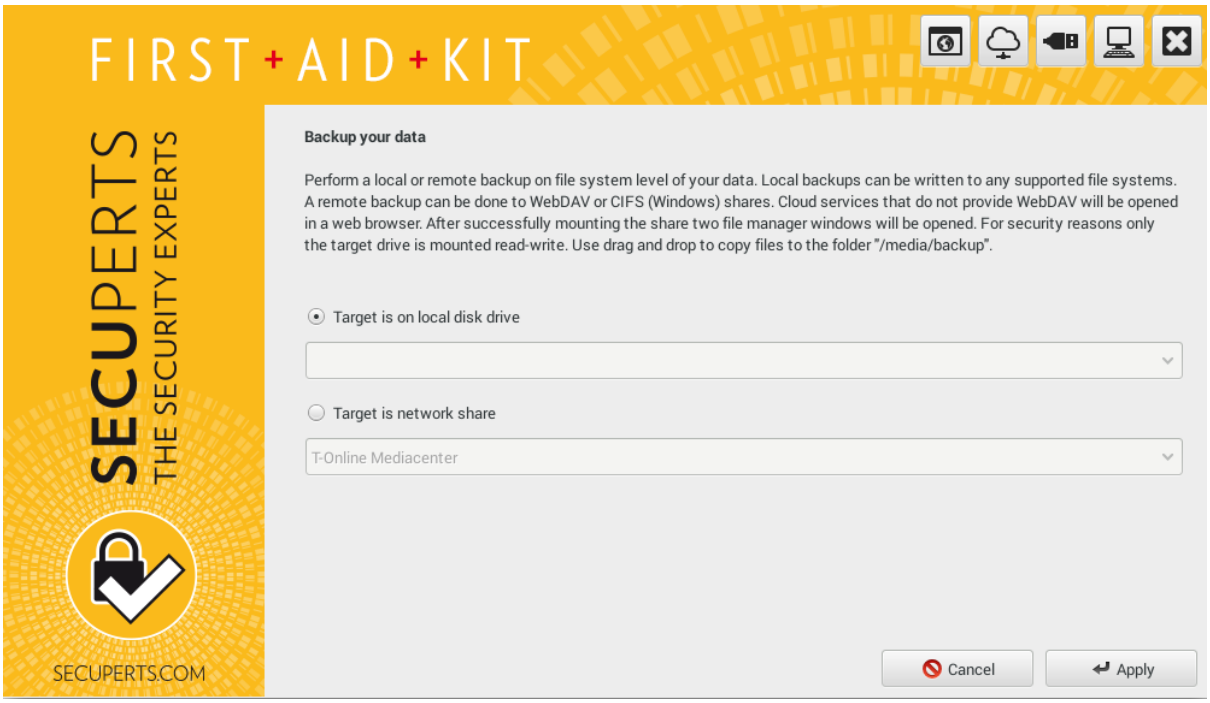
- **Disks:** Displays currently available drives
- **Mousepad:** Opens a text editing software.
- **Sound mixer**: Adjust the system volume.

5 Start screen tools

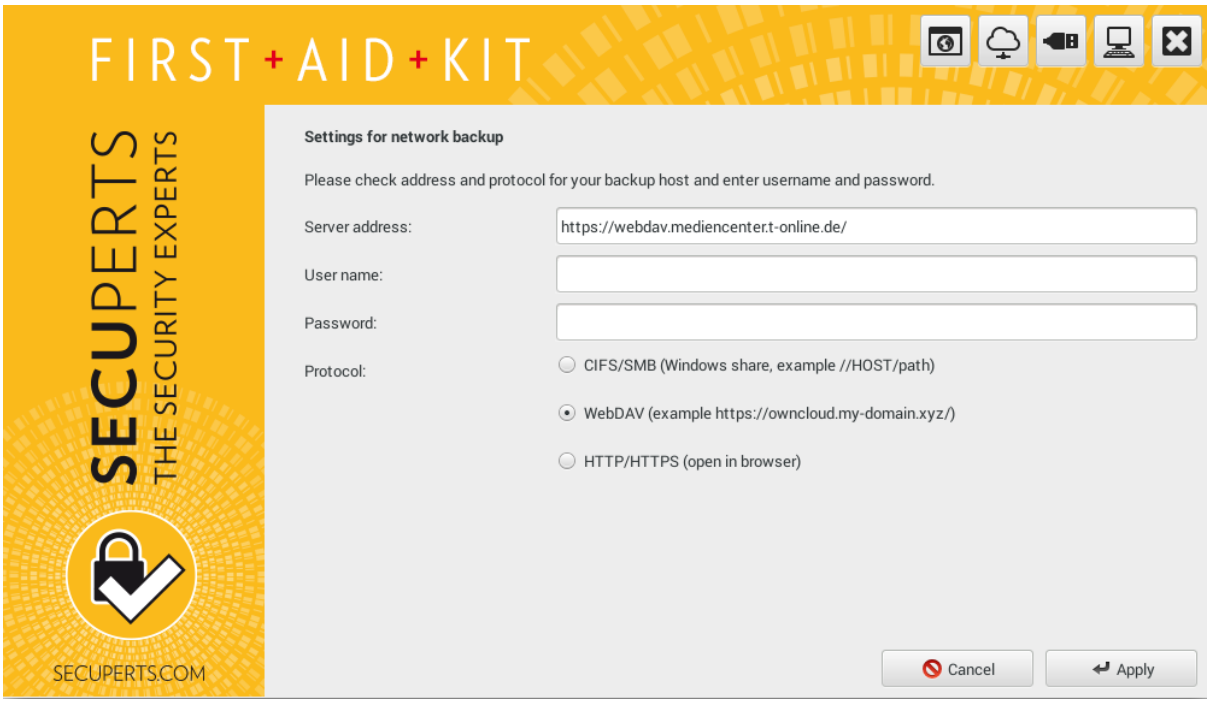
5.1 Backup your data

The tool 'Backup your data' offers two different ways to backup your data:

Target is a local drive
If you want to backup data to an external hard drive you have to choose this option. The internal hard drives will be marked as read-only, the external ones as writeable. This leads to more safety with your data. Two explorers will open. They behave similar to the windows explorer. Just move your desired files via drag and drop to the targeted drive.



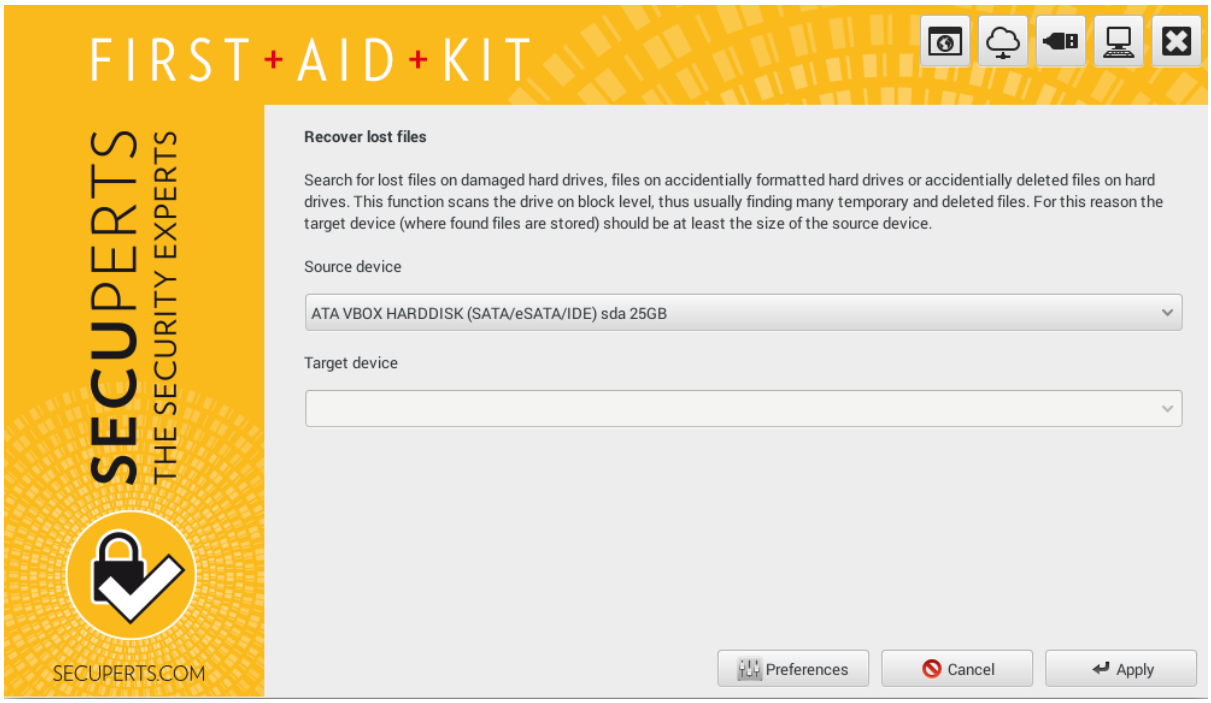
Target is a network drive
If you don’t have an external hard drive you can also save the files to cloud storage. Here you can choose between a variety of different services. In the following window you have to log into the chosen service, so the SecuPerts - First Aid Kitis able to connect to it. Internet plans usually offer far less upload speed than download speed. The backup may take a while, sometimes even multiple hours. It is advised to only save small amounts of data to cloud services.



5.2 Recover lost files

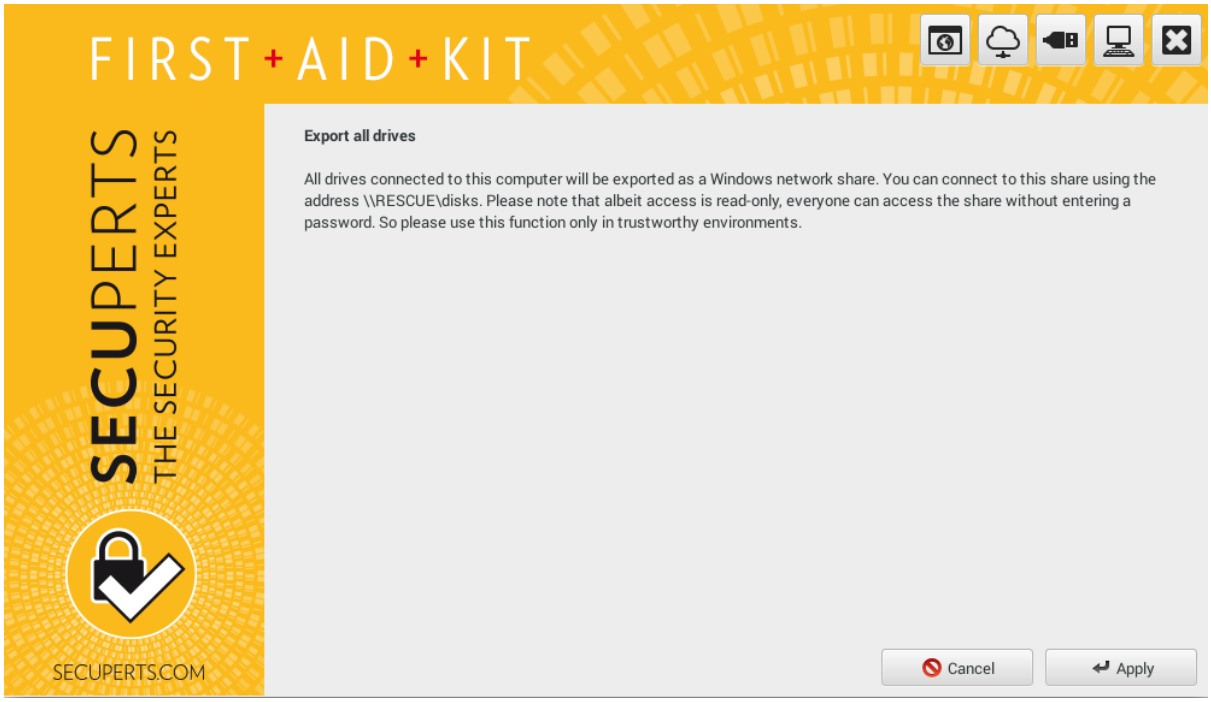
With 'Recover lost files' you may recover accidentally deleted files. Even files from damaged hard drives could sometimes be saved. The tool will not, unlike 'Backup your data', need a completely functioning hard drive. The search for data is independent form the system and will be performed on a block level, so even files from formatted hard drives can be recovered. The tool finds many deleted and temporary files. The target device should be at least as big as the drive you want to recover.

Inside the settings menu you can decide which file types should be recovered. Only searching for part of the files leads to reduced search times. You can also choose to sort the found files. Pictures will be sorted after used camera and the date it was taken, music will be sorted after interpreter, album and title. The files have to be analyzed for this, which leads to overall higher search times.



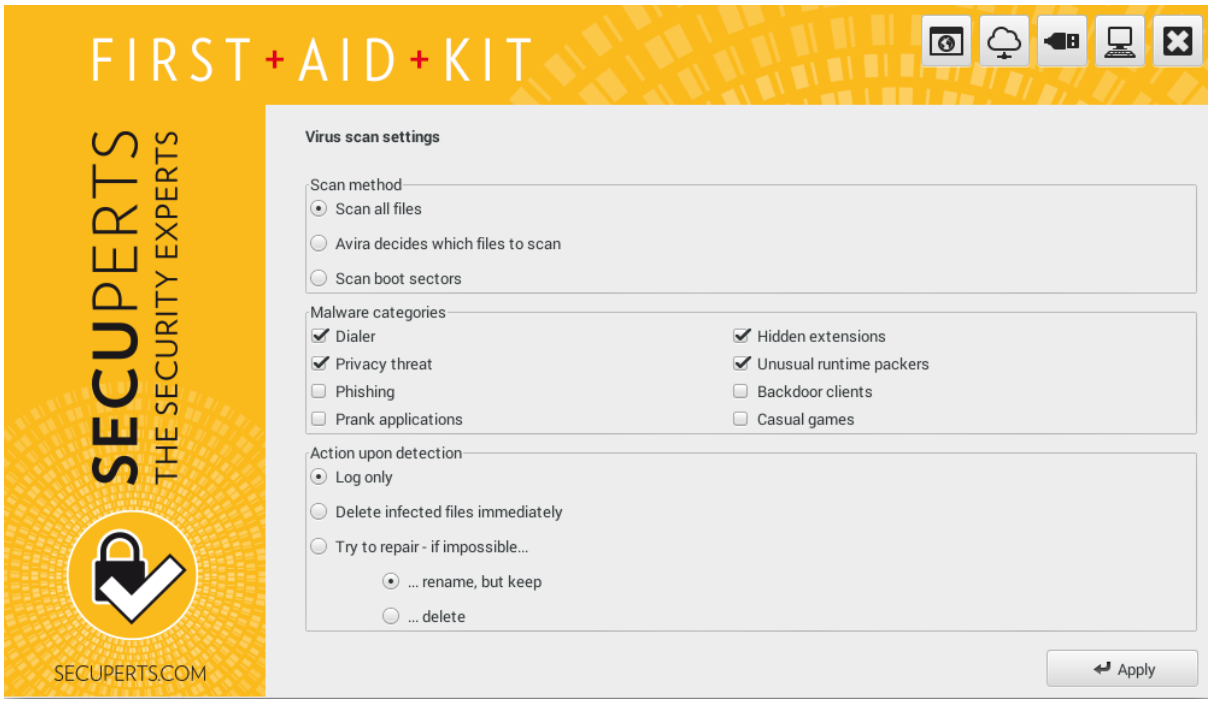
5.3 Export all drives

If you have neither access to an external hard drive or cloud storage you can access the data through a different computer. This option shares the internal hard drives in the local network to allow you to copy the files from one computer to another. Please be aware that this process is not locked through a password. You should only be using this tool in a safe environment.



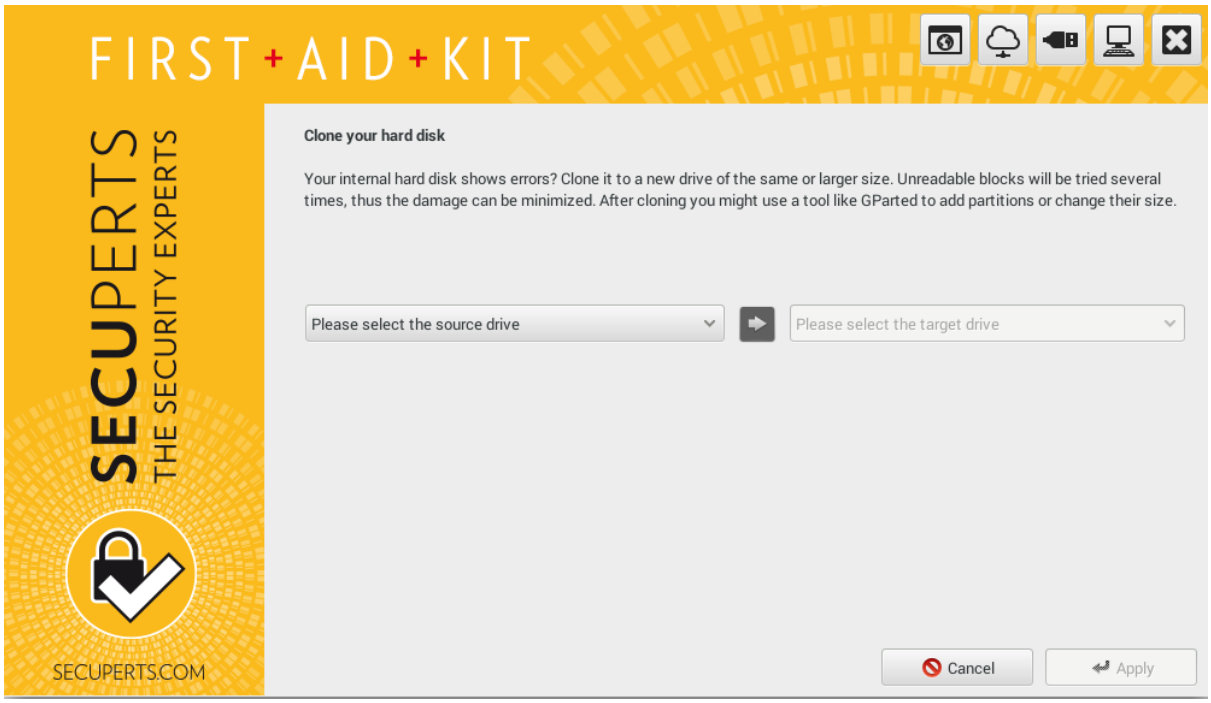
5.4 Search for viruses

The entry 'Search for viruses' is in fact the Avira anti-virus software. The SecuPerts - First Aid Kit is a separated closed system and can possibly find malicious software, which escaped a virus scan on a windows system. It also offers a variety of customization options. You can, e.g. choose which types should be searched for and what the software should do with the found files. After you are finished with the settings, you can select a target device and start the search.



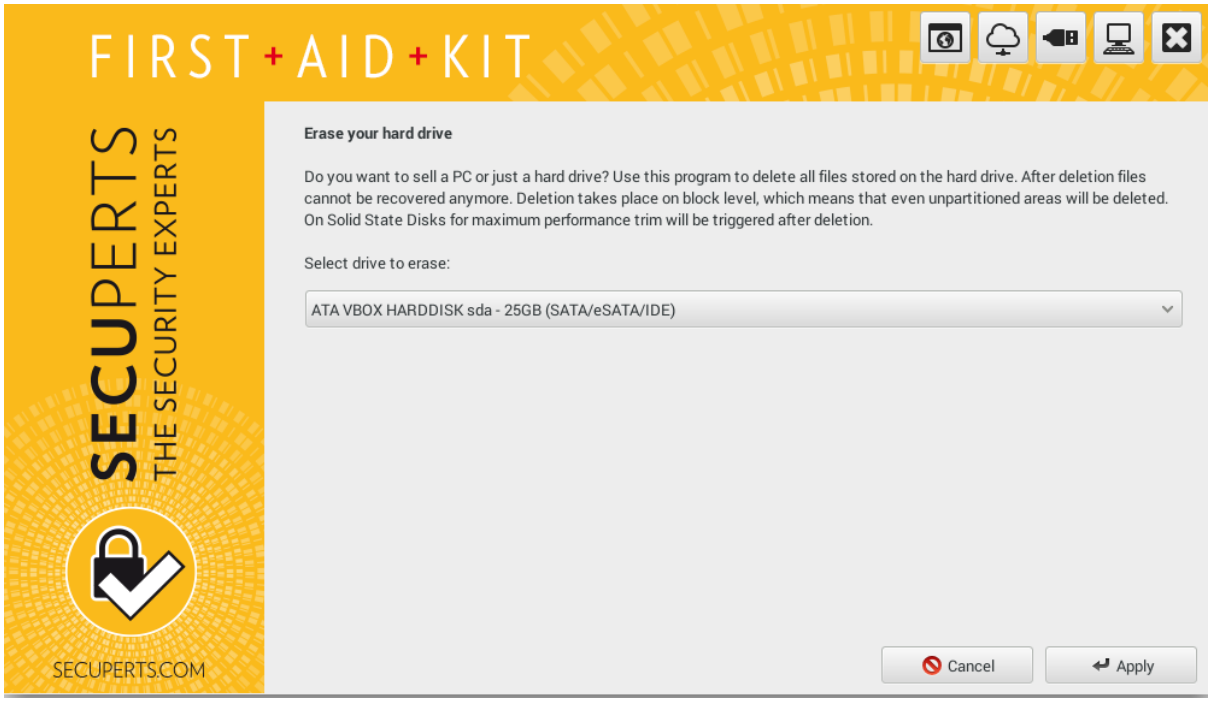
5.5 Clone your hard disk

This tool allows you to completely clone a hard drive. Even minor defects of an old drive are not a problem. The drive you want to clone to needs to have at least the amount of free space as the old one has. After the cloning process has finished, you have to use the tool 'GParted' in the desktop mode to extend the partition to its normal size.



5.6 Erase your har drive

If you want so sell or throw a hard drive away you need to remove all its data first. Just deleting it is often not enough because some files will still be left. This tool allows you to completely wipe a hard drive. After this, you can no longer retrieve any data from the device.



5.7 USB installation

If your SecuPerts - First Aid Kit is located on a CD or DVD you can create a bootable USB flash drive through the button in the upper right corner. It is also possible, in contrast to the DVD version, to get updates with the USB flash drive. It also saves virus signatures, so don't have to reload them after each restart. It is advised to use a stick with at least 8 gigabyte.

You can also install it on an external hard drive, but they are sometimes not bootable. You can ping the boot from the DVD, if this is the case. Be aware that all files will be deleted during the installation. You should back them up first.

6 Desktop mode tools

6.1 Special features of the data structure

The SecuPerts - First Aid Kit is based on a Linux system. It differs from windows in many aspects. The biggest one is the organization of the files.

Windows uses drives with corresponding letters where folders and files are located. Linux uses a root directory, where those things are located under "dev" The root directory has the following structure:

- **/bin:** Directories with basic shell-commands, comparable to DOS.
- **/boot:** Files which are needed for the boot.
- **/dev:** Hardware like hard drives will be displayed here.
- **/home/username:** Private files for normal users.
- **/media:** Removable media like CD/DVD/BD-Drives and USB sticks.
- **/mnt:** Directory for mounted file systems.
- **/opt:** Directory for manually installed software.

- **/root:** Directory for personal data from the administrator.
- **/svr:** Files for services like FTP and HTTP.
- **/tmp:** Temporary files.
- **/usr:** Static and read-only files.
- **/var:** Files which are created during usage of the system.

6.2 Mount

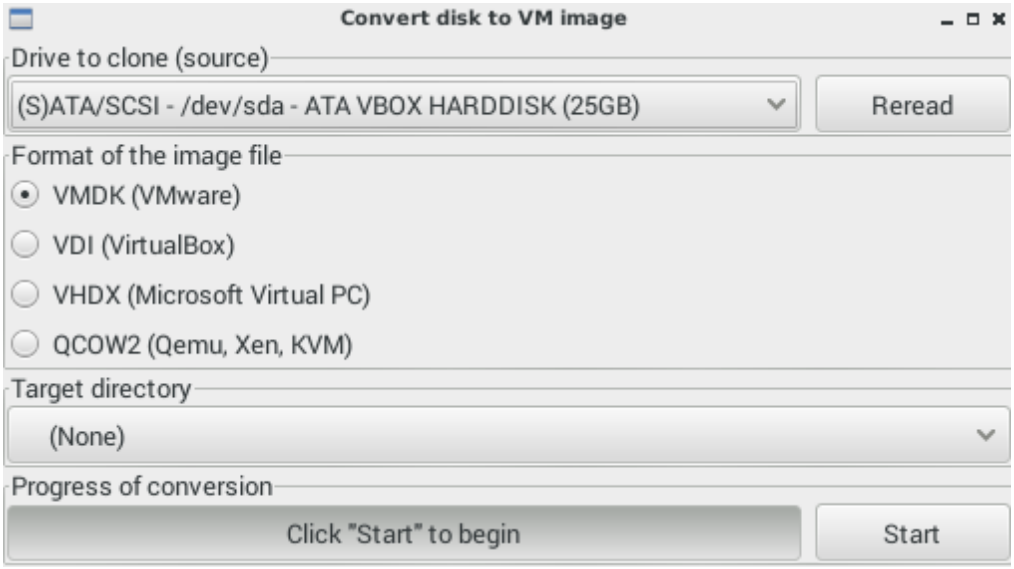
Existing drives will not be automatically mounted during startup. It as to be done manually. The drives are located under "/dev" and are named "/sdaX", where X is a number. If you want to open such a directory and can't see any files it has not been mounted yet.

To mount a drive you have to switch to the desktop mode first. Now start the disk tool which displays all current drives. After this click on "bind partition (sdax, ntfs)". The drive will now be mounted. The button "Show content" reveals an explorer. The option "writeable?" allows you to edit and delete files.

A drive will stay mounted until you remove it manually. To unmount it you have to right-click on the device entry and select the option "disconnect".

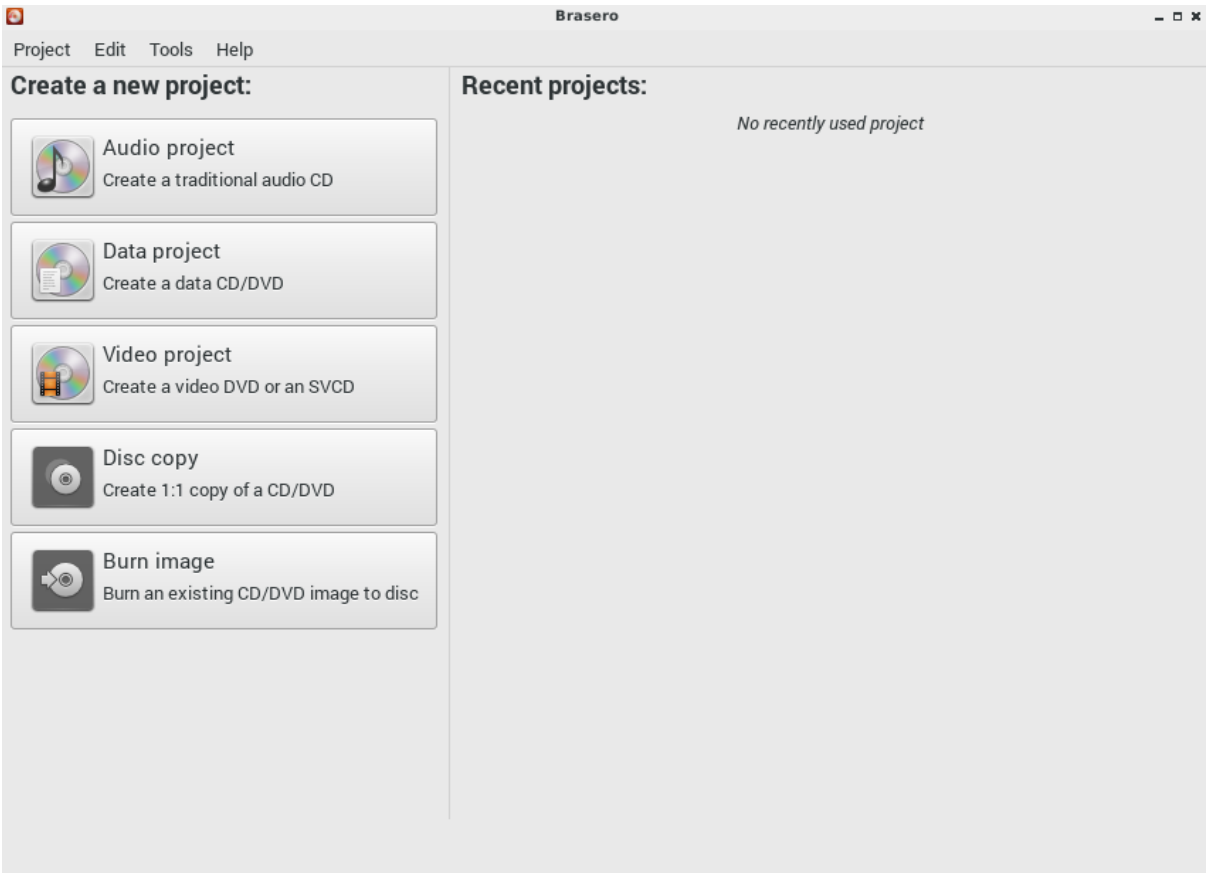
6.3 Backup drive

The tool "VM Image" allows you to back up a whole hard drive incl. partitioning. The created file will be a bit smaller than the original device because only occupied space will be considered for the process. The hard drive has to be undamaged.



6.4 Burn data

The desktop mode offers two different software to burn data, Xfburn and Brasero. You can either burn a completely new CD or copy an existing one. You have also the possibility to create an .iso file. This can be used to create a copy at a later time. If you want to rewrite a RW-CD, you have to use Xfburn.



6.5 Reset password

To reset your windows password start the tool "Reset password" inside the desktop mode. It removes your current password, so that you can get access to your system again. Afterwards you can choose a new password. Since Windows 8 it is possible to use a Microsoft-Live-Account to log into Windows. This cannot be resetted with the tool, you have to proceed as following:

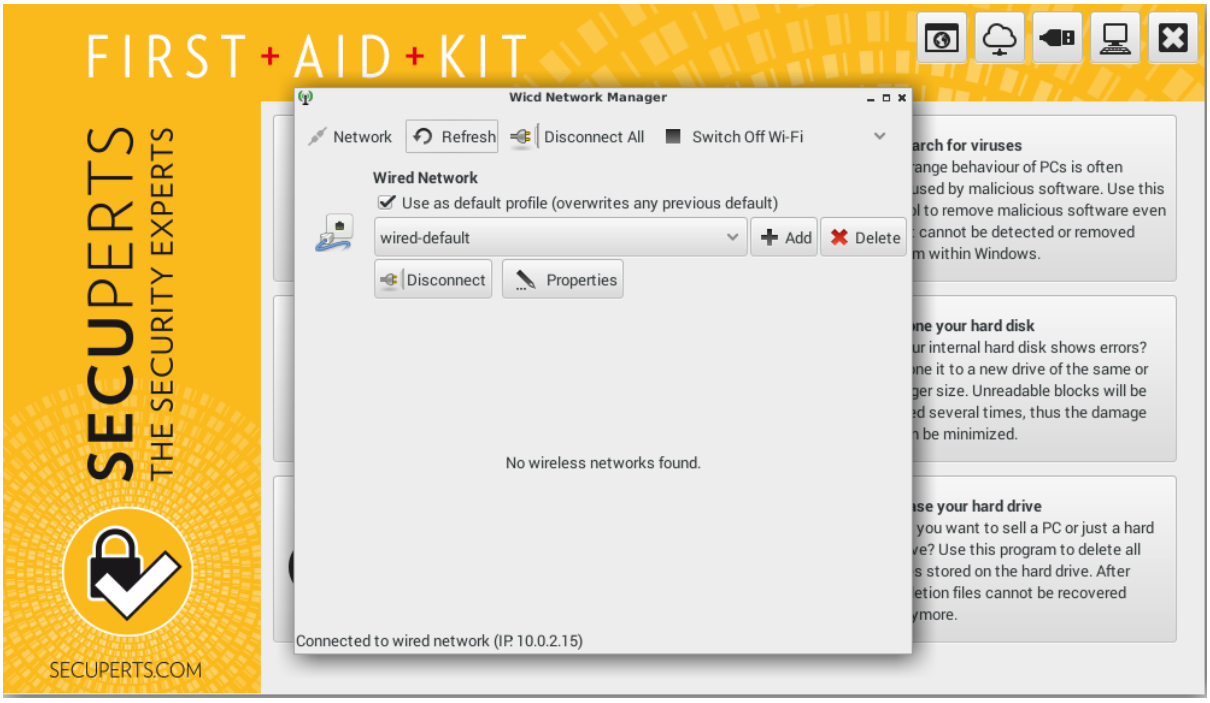
- Start the internet browser of the First Aid Kit, which is located in the start menu inside the desktop mode.
- Type in the following address: "http://login.live.com".
- Click on the button named "Lost access to your account?".
- Now type in the data of your Microsoft account and the captcha.
- In the next dialog select the option "Send link to reset password to my e-mail-address".
- You can receive the e-mail through the e-mail-client inside the desktop mode.
- If you don’t have access to your e-mail address, you can also select the option "I can’t use any of these options", where you can type in another address.

7 Network and internet

The SecuPerts - First Aid Kit works as a separated system. For a wired connection it will find the internet connection automatically. W-LAN needs to be set up manually. You can do this through cloud button in the upper right corner. It will open the "Wicd Network Manager".

If you have a device to use W-LAN with, you will be shown all the available connections. Now you can

either directly connect or choose a password inside the properties.



7.1 Connect network drives

The integrated internet browser allows you to connect to network drives. It can be accessed through its address. The address for a NAS in your local network for example is structured like this: "cifs://12.34.56.78/share".

If you have problems connecting to a network drive you should ask your system administrator or go to the support site of your provider. Alternatively the browser can be used to browse the internet without any dangers. To gain anonymity you could use a proxy like "https://cyberghostvpn..com/proxy".

8 Remote maintanance

The SecuPerts - First Aid Kit offers two different ways to remotely maintain your PC. Both can be accessed through the start menu inside the desktop mode.

- **Teamviewer:** Offers possibility to remotely maintain through the internet. Your PC will get an ID and password you can share to get help from friends or other persons.
- **VNC:** If you only want to use the remote maintenance locally you can use this tool. It is not protected by a password, so use it only in safe environments.

9 Applicaton examples

9.1 Mobile office

The SecuPerts - First Aid Kit has all the necessary components to be used as a mobile office. This is also useful if you do not have access to your computer. Simply start the desktop mode and go to the office section in the start menu. Here you will find all the important software for every day office work. The tools are a text editor, spreadsheet software and a PDF reader. The entry "Internet" also offers an E-Mail client and an internet browser.

9.2 Problems while starting windows

If your Windows does not start or you no longer have access to it, you can often use SecuPerts - First Aid Kit to fix the problems. There are many different reasons for the problems which all need different treatment to solve them. Some of these will be explained now:

If your system freezes often or it needs unusually long to boot, it can help check your drive for possible errors. Open the tool "Check SMART" located under the start menu inside the desktop mode. Then, select a hard drive you want to get checked. If errors are found you should replace the hard drive if possible. A previous backup of the data is recommended.

If no errors are found there may be missing files, which are required to boot Windows. This can be solved using a Windows-Repair. Is can be started from a Windows-Installation-DVD. Select "Computer repair options" from a started installation DVD. After reaching the options select "Windows Repair" and click on "Next". Another click on "System repair" starts the process. If this does not work the first time you may need to repeat it several times.

9.3 Data backup

You can also use the SecuPerts - First Aid Kit to relatively easy to back up personal files from the windows folder "My Documents". First of all start the tool "disks" inside the desktop mode. Now include a drive with your installed windows installation and uncheck the option "writable?". Depending on the used windows version, there are different ways to access the folder "My Documents".

In Windows XP the folder is located under "Documents and Settings > Username". Since Windows 7 the folder is located under "Users > Username". After you have found the correct folder, select it and press *Ctrl + C*. Now connect a disk on which you want the data to be saved to. Simply select it inside the tool "disks" with the option "writeable?" activated. After reaching the target directory press *Ctrl + V* to save the data.

9.4 Rescue partition

The tool "Find lost partitions" allows you to recover accidentally deleted partitions. It is located under Rescue tools inside the desktop mode. After clocking on "Create" you can choose your desired drive with the arrow keys. The process will start after hitting *Enter.* Pressing *Enter + Y* will reveal deleted partitions. Select the desired partition and check the option "Write". To confirm your selection press *Enter* followed by *Enter + Y* . If all has been done correctly the partition will appear after a restart.