

ESET SysRescue Live

User Guide

[Click here to download the most recent version of this document](#)



Contents

1.	ESET SysRescue Live	3
2.	Creating ESET SysRescue Live media.....	3
2.1	Creating an ESET SysRescue Live USB using a CD/DVD.....	5
3.	Starting ESET SysRescue Live.....	6
4.	Using ESET SysRescue Live.....	7
4.1	On-demand scan	8
4.1.1	ThreatSense Engine Setup.....	10
4.2	Update.....	12
4.3	What is a potentially unwanted application?.....	13
4.4	Tools.....	13
4.4.1	Log files	13
4.4.2	Protection statistics.....	13
4.4.3	Quarantine.....	13
4.4.4	Submit file for analysis.....	13
4.4.5	ESET Live Grid.....	14
4.5	Preferences	14
4.6	Program menu.....	15
5.	How to exit ESET SysRescue Live.....	16
6.	Erasing ESET SysRescue Live Live media.....	16
7.	Bomgar and TeamViewer	17
8.	About Desktop environment.....	17
8.1	Network.....	19
8.2	Data Backup.....	20
9.	Troubleshooting.....	20

ESET SysRescue Live

Copyright ©2017 by ESET, spol. s r. o.

ESET SysRescue Live was developed by ESET, spol. s r. o.
For more information visit www.eset.com.

All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.

ESET, spol. s r. o. reserves the right to change any of the described application software without prior notice.

Worldwide Customer Support: www.eset.com/support

REV. 3/14/2017

1. ESET SysRescue Live

ESET SysRescue Live is a free utility that allows you to create a bootable rescue CD/DVD or USB Drive. You can boot an infected computer from your rescue media to scan for malware and clean infected files.

The main advantage of ESET SysRescue Live is the fact that it runs independent of the host operating system, but has direct access to the disk and file system. This makes it possible to remove threats that under normal operating conditions might be impossible to delete (for example, when the operating system is running, etc.).

2. Creating ESET SysRescue Live media

Rescue media must be created on a Windows platform to run ESET SysRescue Live. This can be done using the ESET Live USB Creator.

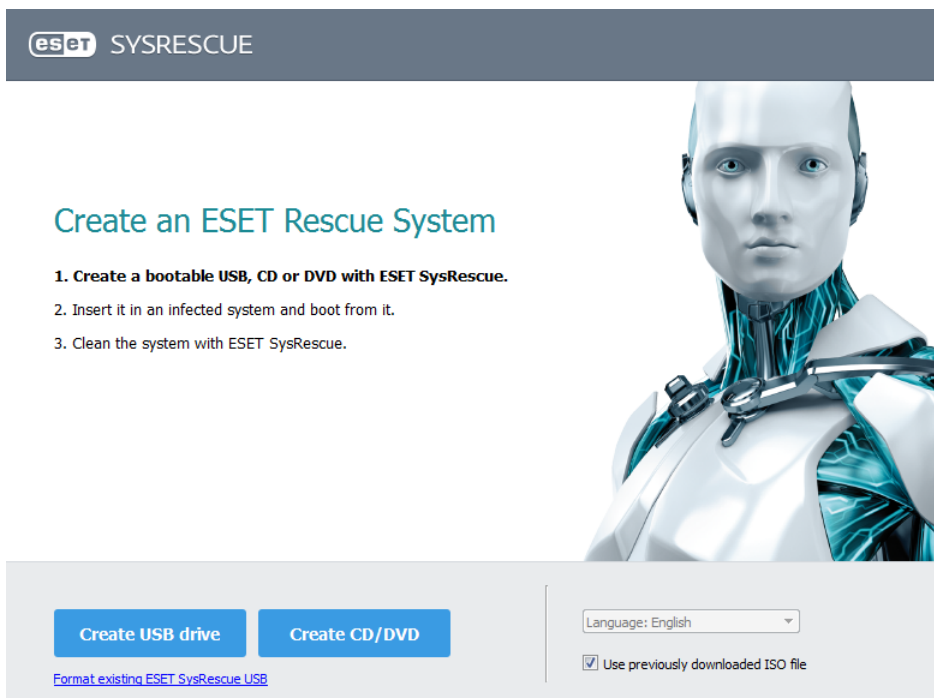
Warning: If you are using portable media (for example, a USB flash drive) as the destination for your rescue disc, any existing data on that media will be erased.

USB drive has to be of at least 1GB size.

To create rescue media, please follow these instructions:

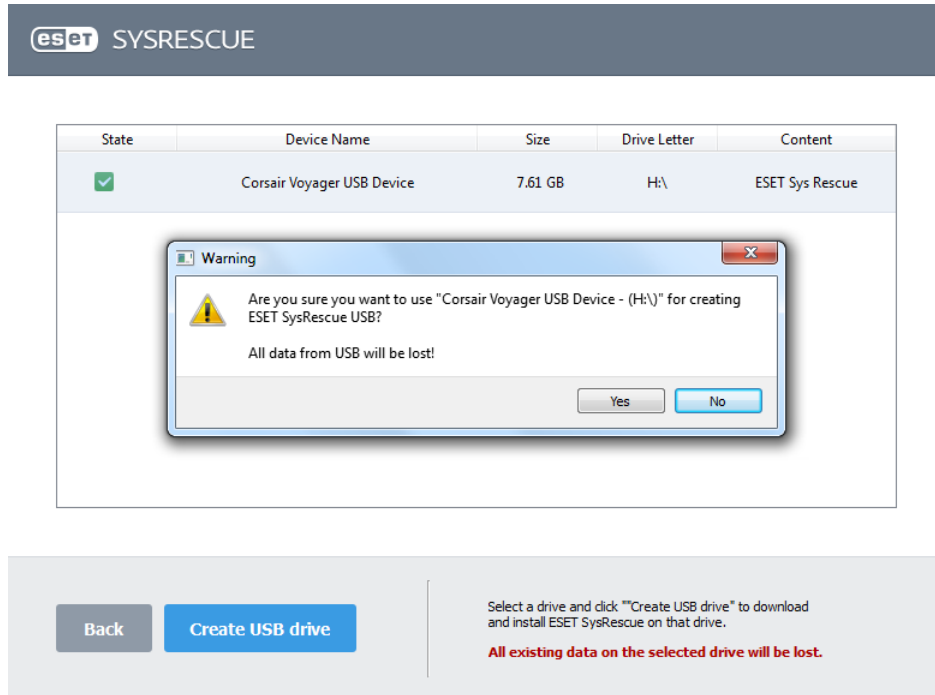
1. Download ESET Live USB Creator from the [ESET website](#). Additional files will be downloaded during installation on a portable device.
2. Run ESET Live USB Creator and select **Create USB drive** or **Create CD/DVD**.

Figure 1 – ESET Live USB Creator



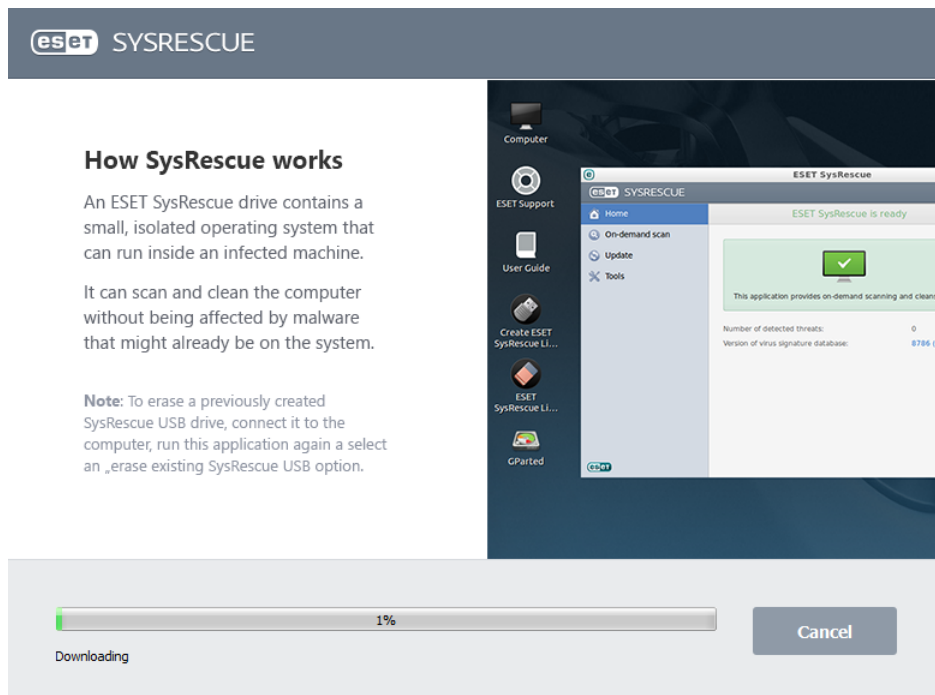
3. Select the type of media you want to create and confirm the operation.

Figure 2 – ESET Live USB Creator



4. Wait until ESET SysRescue Live gets installed on your portable device you have chosen in the previous step.

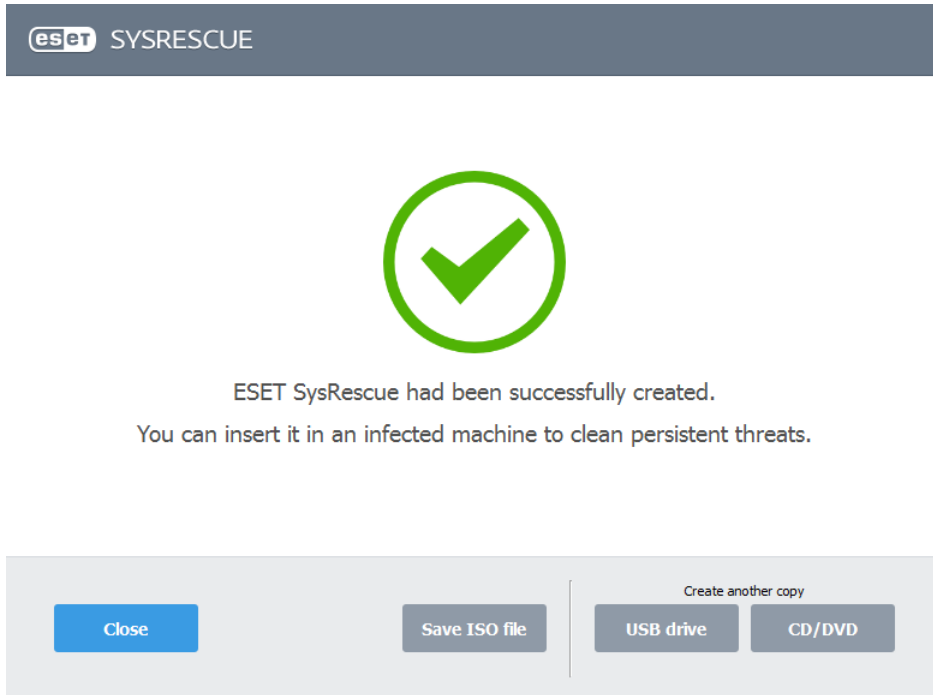
Figure 3 – Creating ESET SysRescue Live



5. The message "ESET SysRescue has been successfully created." will be displayed when ESET SysRescue Live installation is complete.

If you want to create another rescue disc at a later time, we recommend that you use **Save ISO file**. During rescue disc creation, select the check box next to **Use previously downloaded ISO image** to access your saved ISO file.


Figure 4 – ESET SysRescue Live has been created



6. When your ESET SysRescue Live media is ready, remove it from your computer and store it in a safe place. You can now use ESET SysRescue Live on an infected machine.

2.1 Creating an ESET SysRescue Live USB using a CD/DVD

Alternatively, the bootable ESET SysRescue Live disk can also be installed on a USB flash drive directly from a [ESET SysRescue Live environment](#).

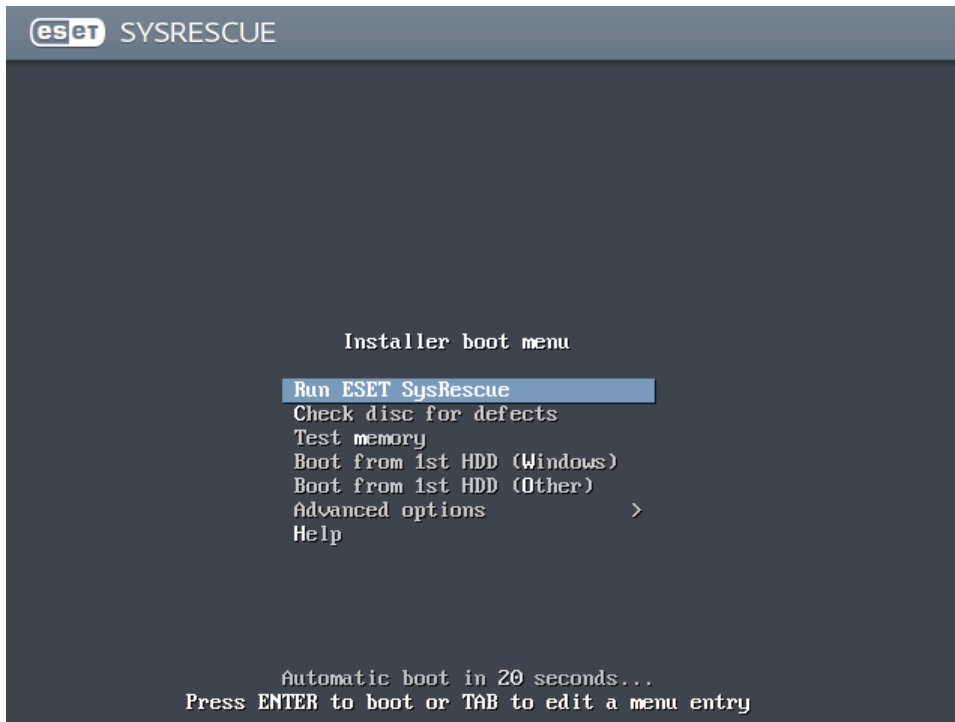
To install ESET SysRescue Live on a USB flash drive, insert a USB flash drive into the PC and click  **Create ESET SysRescue Live USB** icon on the Desktop. Select a USB device from the list and click **OK** to perform the installation and then follow the installation steps.

3. Starting ESET SysRescue Live

For ESET SysRescue Live to function properly, your computer must allow booting from removable media. You can modify boot priority settings in the BIOS, which is usually accessed by pressing one of the function keys (F8-F12) or the ESC key during startup. Instructions for accessing the BIOS are typically displayed on-screen during startup.

A splash screen will be displayed when you boot ESET SysRescue Live from removable media. By default, there is an automatic 30-second timeout during ESET SysRescue Live startup. The timeout can be interrupted by pressing any key.

Figure 5 – ESET SysRescue Live splash screen



The main menu is comprised of the following options:

- **Run ESET SysRescue** – Boots the ESET SysRescue Live environment with your selected language.
- **Check disc for defects** – Checks the integrity of the CD/DVD/USB removable media. If the disk check returns errors, it is possible that the rescue image is damaged. In this case, you will need to recreate rescue media as described in the Installation steps.
- **Test memory** – Runs a stand-alone memory diagnostic tool (Memtest86+) and performs a test on the computer's physical memory to detect memory failure. Use this tool if you experience system malfunctions.
- **Boot from first hard disk** – Choose this option if you want to start your operating system normally.

The function keys F1-F4 are useful if you want to specify special booting parameters. The following options are available:

- **F1 Help** – Displays help content for ESET SysRescue Live's splash screen.
- **F2 Language** – Allows you to select your master language, which will be used for the splash screen and after starting the system.
- **F3 Keymap** – Allows you to adjust your keyboard layout.
- **F4 Other Options** – Allow you to modify Linux kernel parameters.
- **ESC** – Close any opened windows. Allows you to switch to text mode (recommended for advanced users only).

4. Using ESET SysRescue Live

After starting up, ESET SysRescue Live will ask you to read and agree to the ESET License Agreement. Select whether to use [Live Grid](#) (1), set your preference for detection of [Potentially unwanted applications](#) (2), and then click **I Accept the Terms in the License Agreement** (3) to acknowledge your acceptance of the End-User License Agreement.

Figure 6 – ESET SysRescue and License agreement

License Agreement

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 NOTICE: Prior to download, installation, copy or use please read the below terms of the product application. BY DOWNLOAD, INSTALLATION, COPY OR USE OF THE PRODUCT YOU EXPRESS YOUR CONSENT TO THESE TERMS AND CONDITIONS.

End User License Agreement for Software Use.

This agreement on software use (the "Agreement") executed by and between ESET, spol. s r. o., with its seat at Einsteinova 24, 851 01 Bratislava, registered in the Commercial Register of the District Court Bratislava I, Section Sro, Insertion No 3586/B, BIN: 31 333 535 (the "Provider") and you, a physical or legal person, (the "End User") entitles you to use the Software defined in Article 1 hereof. The Software defined in Article 1 hereof may be stored on a CD-ROM or DVD medium, sent via electronic mail, downloaded from the Internet, downloaded from servers of the Provider or obtained from other sources under the terms and circumstances

Live Grid

Please select one of the options **1**

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

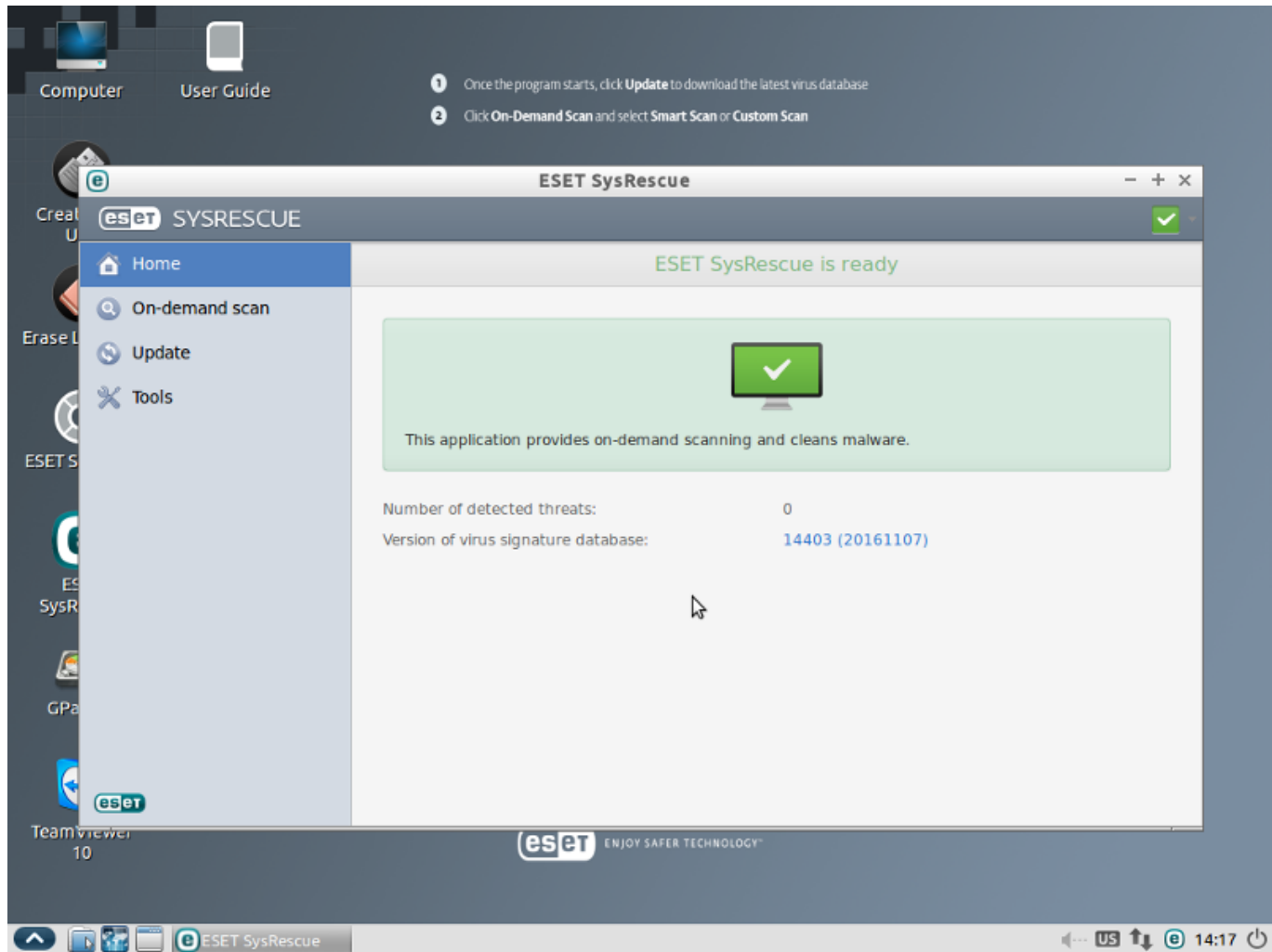
Please select one of the options **2**

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.

Decline and shutdown I accept the terms of the License Agreement **3**

After confirming your acceptance of the License Agreement, the main program window will be displayed.

Figure 7 – ESET SysRescue and Desktop after starting up

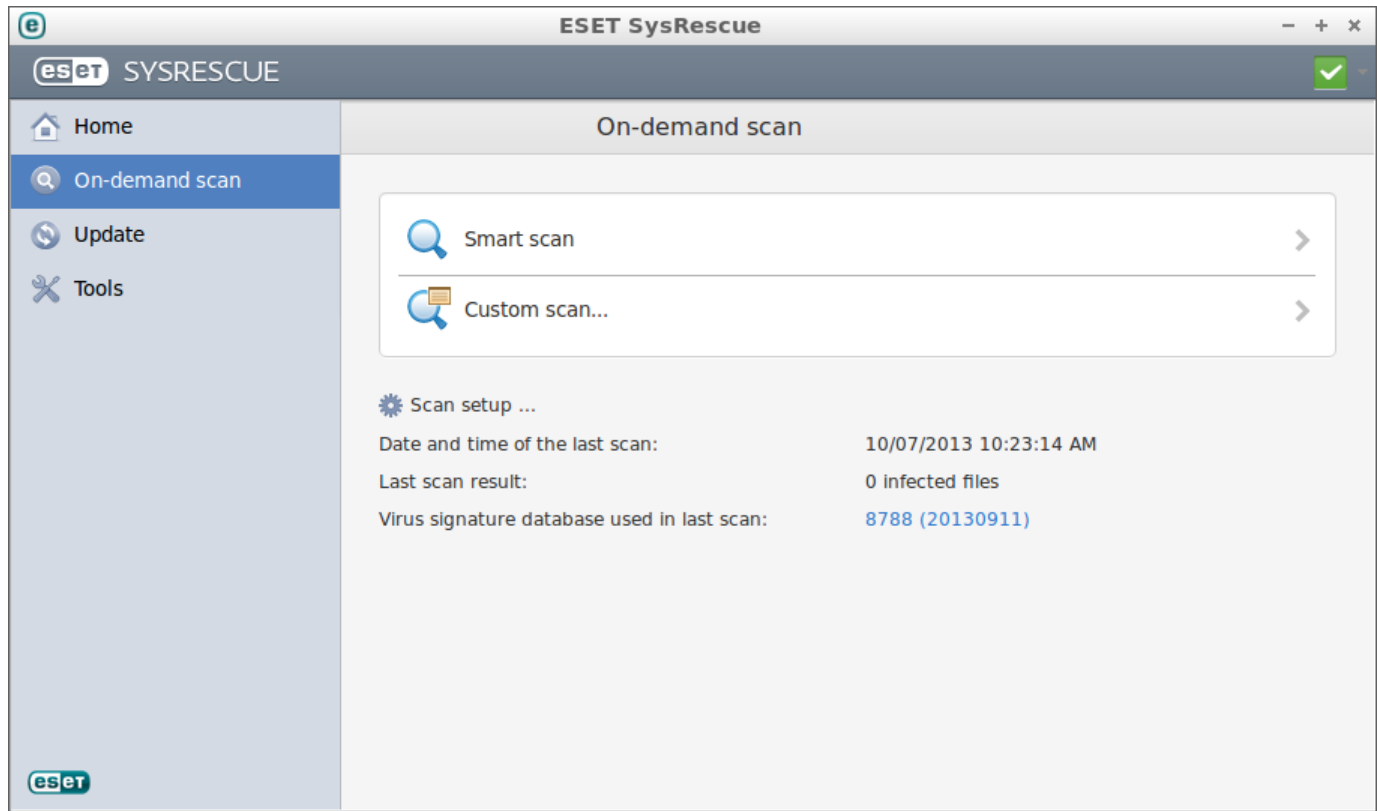


4.1 On-demand scan

ESET SysRescue is able to scan and clean both Linux and Windows partitions, such as ext3, ext4, reiserfs, vfat (fat32) or ntfs. The following scanning options are available:

- **Smart scan** – allows you to quickly launch a computer scan and clean infected files with no need for user interaction. Its main advantage is easy operation without any prior scanning configuration.
- **Custom scan** – is an optimal solution if you want to specify scanning parameters, such as scan targets and scanning methods. The advantage of a Custom scan is the ability to configure the parameters in detail.

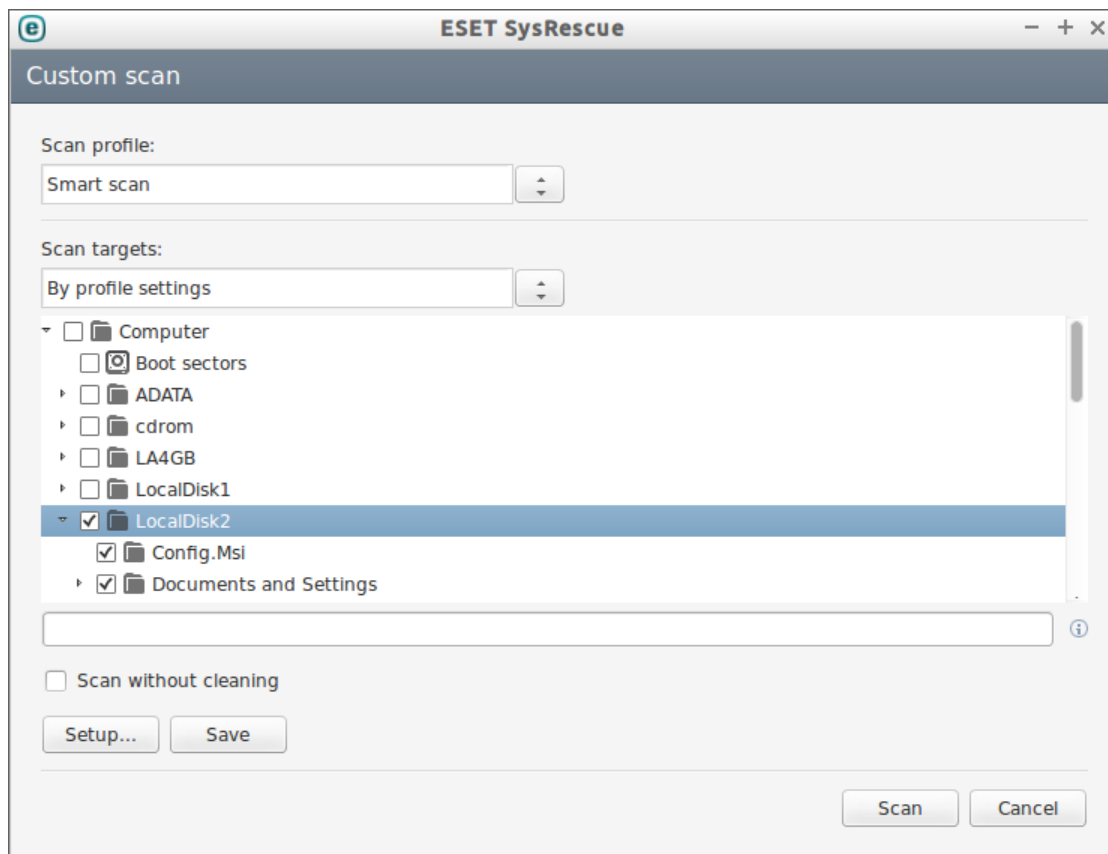
Figure 8 – ESET SysRescue On-demand scan



Note: Both scanning options are configured to scan the */media* folder that includes mounted discs.

When performing a Custom scan, you can select one of the default scan profiles or click **Setup...** to modify scanning parameters or select specific scan targets. Select **Scan without cleaning** if you do not want to perform cleaning actions against any threats discovered by the scan.

Figure 9 – Scan targets



4.1.1 ThreatSense Engine Setup

The ThreatSense engine setup options allow you to specify several scan parameters:

- File types and extensions that are to be scanned
- The combination of detection methods used
- Levels of cleaning, etc.

The **Objects** section allows you to define which computer files will be scanned for infiltrations:

- **Files** – provides scanning of all common file types (programs, pictures, audio, video files, database files, etc.).
- **Symbolic links** – (On-demand scanner only) scans special type of files that contain a text string that is interpreted and followed by the operating system as a path to another file or directory.
- **Email files** – scans special files where email messages are contained.
- **Mailboxes** – scans user mailboxes in the system. Incorrect use of this option may result in a conflict with your email client.
- **Archives** – provides scanning of files compressed in archives (.rar, .zip, .arj, .tar, etc.).
- **Self-extracting archives** – scans files that are contained in self-extracting archive files.
- **Runtime packers** – unlike standard archive types, runtime packers decompress in memory, in addition to standard static packers (UPX, yoda, ASPack, FGS, etc.).
- **Boot sectors** – Scans boot sectors for the presence of viruses in the master boot record.

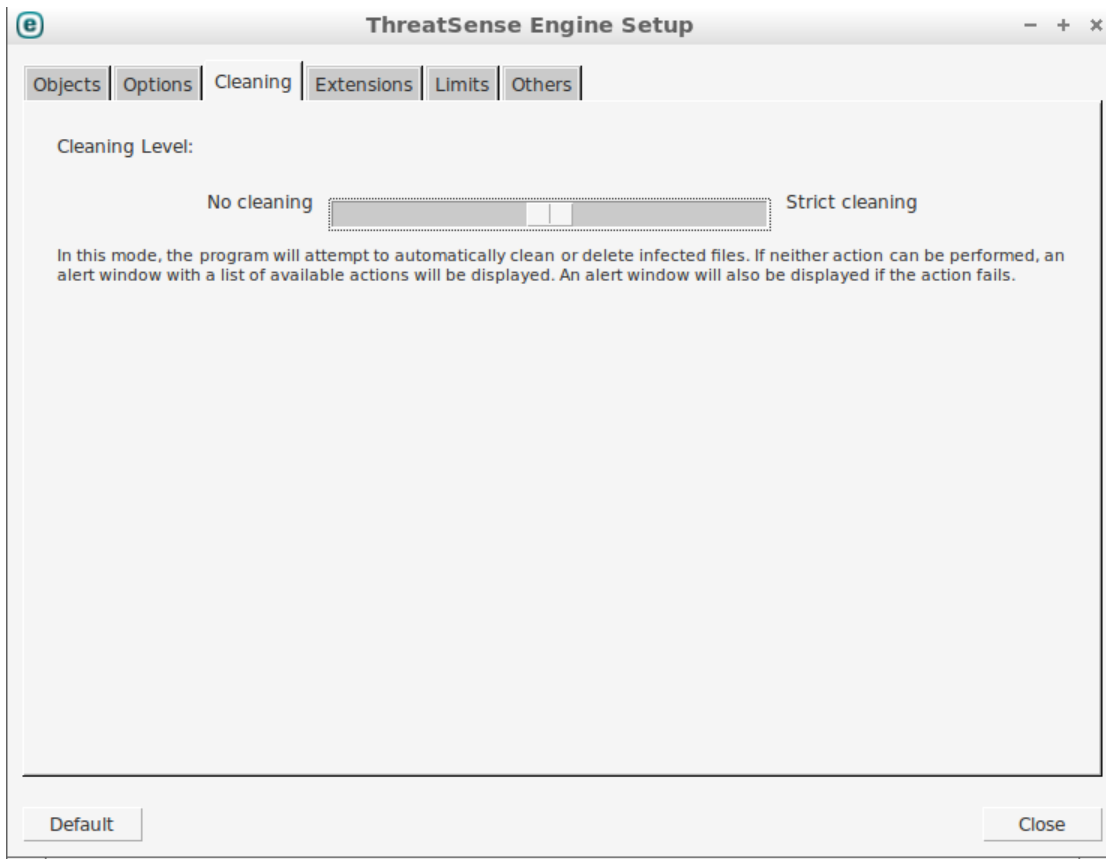
In the **Options** section, you can select the methods used during a scan of the system for infiltrations:

- **Heuristics** – Heuristics use an algorithm that analyzes the (malicious) activity of programs. The main advantage of heuristic detection is the ability to detect new malicious software that did not previously exist, or was not included in the list of known viruses (virus signatures database).
- **Advanced heuristics** – Advanced heuristics utilize a unique heuristic algorithm, developed by ESET, optimized for detecting computer worms and trojan horses written in high-level programming languages. The program's detection ability is significantly higher as a result of advanced heuristics.
- [Potentially unwanted applications](#) – These applications are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require consent for installation.
- **Potentially unsafe applications** – these applications refer to commercial, legitimate software that can be abused by attackers, if it was installed without user's knowledge. The classification includes programs such as remote access tools, which is why this option is disabled by default.

The **Cleaning** settings determine the manner in which the scanner cleans infected files. There are 3 levels of cleaning:

- **No cleaning** – Infected files are not cleaned automatically. The program will display a warning window and allow you to choose an action.
- **Standard cleaning** – The program will attempt to automatically clean or delete an infected file. If it is not possible to select the correct action automatically, the program will offer a choice of follow-up actions. The choice of follow-up actions will also be displayed if a predefined action could not be completed.
- **Strict cleaning** – The program will clean or delete all infected files (including archives). The only exceptions are system files. If it is not possible to clean them, you will be offered an action to take in a warning window.

Figure 10 – ThreatSense engine parameters setup



The **Extensions** settings allow you to define the types of files to be excluded from scanning. An extension is the part of the file name delimited by a period that defines the type and content of the file.

By default, all files are scanned regardless of their extension. Any extension can be added to the list of files excluded from scanning. Using the **Add** and **Remove** buttons, you can enable or prohibit scanning of desired extensions.

Excluding files from scanning is sometimes necessary if scanning of certain file types prevents the proper function of a program that is using the extensions. For example, it may be advisable to exclude the .log, .cfg and .tmp extensions.

The **Limits** section allows you to specify the maximum size of objects and levels of nested archives to be scanned.

- **Maximum Size** – Defines the maximum size of objects to be scanned. The antivirus module will scan only objects smaller than the size specified. We do not recommend changing the default value, as there is usually no reason to modify it. This option should only be changed by advanced users who have specific reasons for excluding larger objects from scanning.
- **Maximum Scan Time** – Defines the maximum time allotted for scanning an object. If a user-defined value has been entered here, the antivirus module will stop scanning an object when that time has elapsed, whether or not the scan has finished.
- **Maximum Nesting Level** – Specifies the maximum depth of archive scanning. We do not recommend changing the default value of 10; under normal circumstances, there should be no reason to modify it. If scanning is prematurely terminated due to the number of nested archives, the archive will remain unchecked.
- **Maximum File Size** – This option allows you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. If scanning is prematurely terminated because of this limit, the archive will remain unchecked.

If you want to disable scanning of folders controlled by the system (`/proc` and `/sys`), select **Exclude system control folders from scanning** option (this option is not available for startup scan).

Use the **Others** tab to define other parameters of the ThreatSense Engine.

- **Enable Smart optimization** – The most optimal settings are used to ensure the most efficient scanning level, while simultaneously maintaining the highest scanning speeds. The various protection modules scan intelligently, making use of different scanning methods while applying them to specific file types. Smart Optimization is not rigidly defined within the product. The ESET Development Team is continuously implementing new changes, which then get integrated into ESET SysRescue via regular updates. If Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the particular module are applied when performing a scan.
- **Scan alternative data streams** – Alternate data streams used by the file system are file and folder associations that are invisible from ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternative data streams.
- **Preserve last access timestamp** – Select this option to keep the original access time of scanned files instead of updating it (for example for use with data backup systems).

4.2 Update

The ability to update the virus signature database is an essential feature of ESET SysRescue. We recommend that you update the program prior to starting a Computer scan.

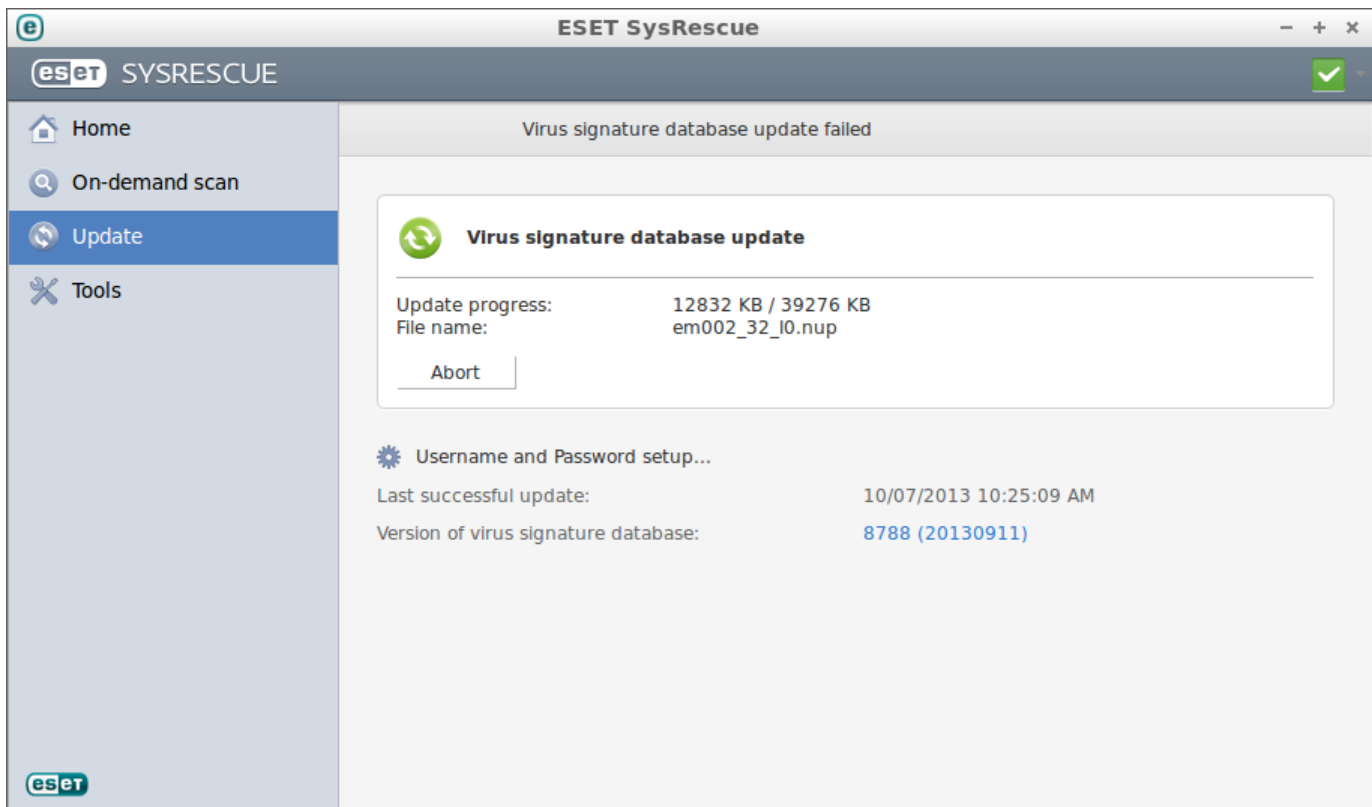
By clicking **Update** from the main menu, you can view the current update status, including the date and time of the last successful update, as well as whether an update is needed. To begin the update process manually, click **Update virus signature database**.

If an update fails, check the internet connection in the [Network Connection settings](#) located in the **Preferences** menu at the bottom left of the screen.

Under normal circumstances, when updates are downloaded properly, the message *"Virus signature database is up to date"* will appear in the **Update** window.

The Update window also contains information about the virus signature database version. This numeric indicator is an active link to the ESET website, where all signatures added during a given update are listed.

Figure 11 – Update screen



Note: Since ESET SysRescue is a free tool, a username and password are not required for automatic updates of the virus signature database. However, if you wish to use a different update server, you can set server details in **Preferences (F5) > Update** by clicking **Edit**.

4.3 What is a potentially unwanted application?

Potentially unwanted applications (PUAs) are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require consent before installation. If they are present on your computer, your system behaves differently (compared to the state before their installation). The most significant changes are:

- New windows you haven't seen previously (pop-ups, ads),
- Activating and running of hidden processes,
- Increased usage of system resources,
- Changes in search results,
- Application communicates with remote servers.

4.4 Tools

4.4.1 Log files

The Log files contain information about all important program events that have occurred, and provide an overview of detected threats. Logging is an essential tool for system analysis, threat detection and troubleshooting. Logging is performed actively in the background with no user interaction.

When Advanced mode is enabled, you can click **Tools > Log files** from the main menu to view log files. Select the desired log type using the **Log** drop-down menu at the top of the window. The following logs are available:

- **Events** – This option is designed for system administrators and users to solve problems. All important actions performed by ESET SysRescue are recorded in the Event logs.
- **On-demand scan** – Results of all completed scans are displayed in this window. Double-click any entry to view details of a specific On-demand scan.

4.4.2 Protection statistics

To view a graph of statistical data related to ESET SysRescue's protection modules, click **Tools > Protection statistics**. The **Antivirus and Antispyware Protection Statistics Graph** displays the number of infected and cleaned objects. Below the statistics graphs, you can see the number of total scanned objects, latest scanned object and the statistics timestamp. Click **Reset** to clear all statistics information.

4.4.3 Quarantine

The main task of the quarantine is to safely store infected files. Files should be quarantined if they cannot be cleaned, if it is not safe or advisable to delete them, or if they are being falsely detected by ESET SysRescue.

You can choose to quarantine any file. This is advisable if a file behaves suspiciously but is not detected by the antivirus scanner. Quarantined files can be submitted to the ESET Threat Lab for analysis.

To restore a quarantined file to its original location, select it and click **Restore**. You can also restore any file listed in the quarantine by right-clicking it and selecting **Restore** from the context menu. The context menu also offers the option **Restore to** which allows you to restore a file to a location other than the one from which it was deleted.

4.4.4 Submit file for analysis

The file submission dialog enables you to send a file or a site to ESET for analysis and can be found under **Tools > Submit sample for analysis**. If you find a suspicious file on your computer or a suspicious site on the Internet, you can submit it to the ESET Virus Lab for analysis. If the file turns out to be a malicious application or website, its detection will be added to an upcoming update.

Alternatively, you can submit the file by email. If you prefer this option, pack the file(s) using RAR/ZIP, protect the archive with the password "infected" and send it to samples@eset.com. Please remember to use a descriptive subject and enclose as much information about the file as possible (for example, the website you downloaded it from).

NOTE: Before submitting a file to ESET, make sure it meets one or more of the following criteria:

- the file is not detected at all
- the file is incorrectly detected as a threat

You will not receive a response unless further information is required for analysis.

4.4.5 ESET Live Grid

The ESET Live Grid Early Warning System keeps ESET immediately and continuously informed about new infiltrations. The bidirectional ESET Live Grid Early Warning System has a single purpose – to improve the protection that we can offer you. There are two options:

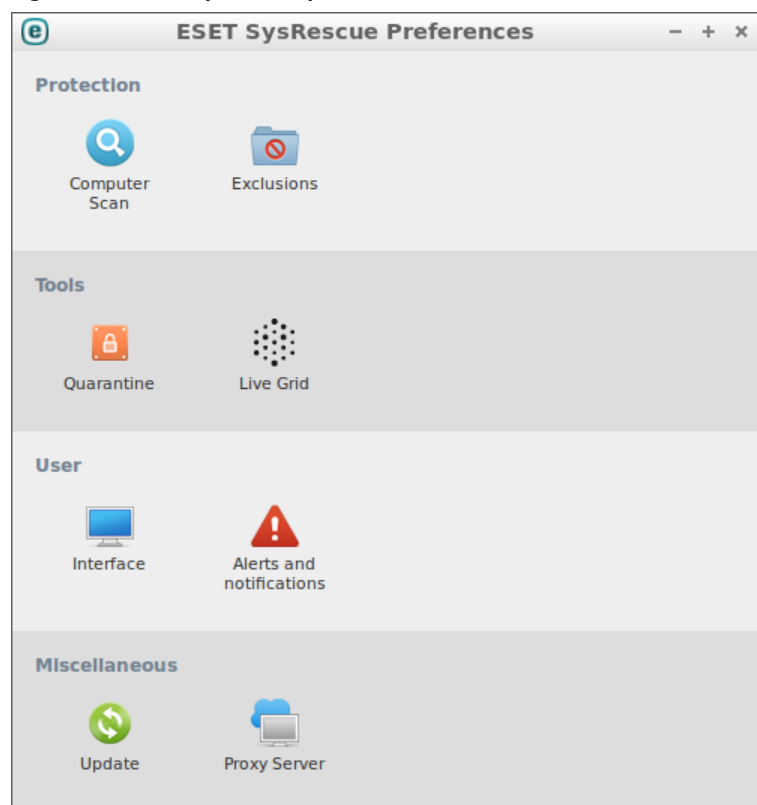
- You can choose not to enable ESET Live Grid Early Warning System. You will not lose any functionality in the software, but, in some cases, ESET SysRescue Live may respond faster to new threats than virus signature database update.
- You can configure the ESET Live Grid Early Warning System to submit anonymous information about new threats and where the new threatening code is contained. This file can be sent to ESET for detailed analysis. Studying these threats will help ESET update its database of threats and improve the program's threat detection ability.

ESET Live Grid Early Warning System setup is accessible from the Advanced Setup window, under **Tools > ESET Live Grid**. Select **Enable ESET Live Grid** to enable it and then click **Setup...** next to the Advanced Options heading.

4.5 Preferences

To access preferences for ESET SysRescue, click main menu in the top right corner of the main window and select **Preferences...** or press **F5**.

Figure 12 – ESET SysRescue preferences



The following options are available:

Computer Scan – Select scanning parameters, select a scan profile or create a new one, adjust [ThreatSense engine parameter setup](#) (options such as file extensions you wish to control, detection methods used, etc.) or choose **Scan targets**, folders and files you wish to scan.

Exclusions – Exclusions enable you to exclude files and folders from scanning. To ensure that all objects are scanned for threats, we recommend only creating exclusions when it is absolutely necessary. However, there are situations where you may need to exclude an object, for example large database entries that would slow your computer during a scan or software that conflicts with the scan.

Quarantine – Enable/disable scanning of quarantined files after every update.

Live Grid – Enable/disable [ESET Live Grid](#), submission of suspicious files and anonymous statistics or add exclusion filters in **Advanced setup**.

Interface – Adjust user interface of ESET SysRescue. Users can enable standard menu, hide tooltips or show hidden files in this section.

Alerts and notifications – Select which notifications should be displayed in **Advanced Setup**, disable all notifications, adjust time after they disappear or change full screen mode settings.

Update – Select an update server, change your username or password, disable update notifications or clear the update cache.

Note: Since ESET SysRescue is a free tool, a username and password are not required for automatic updates of the virus signature database. However, if you wish to use a different update server, you can set server details in **Preferences (F5) > Update** by clicking **Edit**.

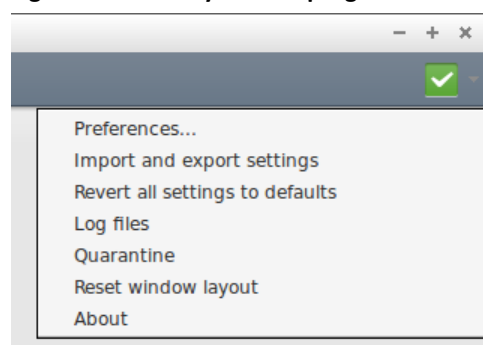
Proxy Server – If you use a proxy server to control Internet connections on a system using ESET SysRescue, the proxy server details must be specified in this section. For more information, please see [Network](#).

Click **Default** to reset settings or click **Show all** to return to the Preferences menu in every section.

4.6 Program menu

To access the program menu, click the protection status icon in the upper right corner of the ESET SysRescue main window.

Figure 13 – ESET SysRescue program menu



Preferences – Select this option to adjust options of ESET SysRescue.

Import and Export settings – Use archive files to store the configuration. Import and export settings are useful if you need to back up your current configuration of ESET SysRescue in order to use it later. The export settings option is also convenient for users who want to use their preferred configuration of ESET SysRescue on multiple systems; they can easily import the configuration file to transfer the desired settings.

Revert all settings to default – Reset all changes made from the start of the system.

Log files – The Log files contain information about all important program events that have occurred and provide an overview of detected threats. For more information please read more in the [Log files](#) section.

Quarantine – Add, restore and delete quarantined objects.

Reset window layout – Reset window size and position to default.

About – Show the product version of ESET SysRescue. Click **More information** in the **About ESET SysRescue** window to show information about program modules and components.

5. How to exit ESET SysRescue Live

To exit ESET SysRescue Live, click system menu  > **Logout** and then choose **Reboot**, or **Shutdown**.

Warning: Local filesystem partitions are mounted as read-write by default. We recommend that you do not perform a force reboot or shutdown to avoid possible data loss.

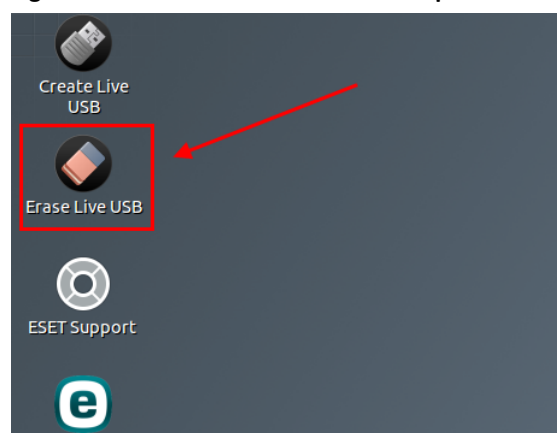
6. Erasing ESET SysRescue Live Live media

Use this utility to restore your USB flash drive to its original state. Ensure that your USB flash drive is plugged into the computer. Two methods of cleaning are available:

1. Cleaning ESET SysRescue in the ESET SysRescue Live environment

Double-click the  **ESET SysRescue Live Live USB Cleaner** icon (available on your Desktop) and follow the instructions in the wizard.

Figure 14 – Live USB Cleaner on Desktop

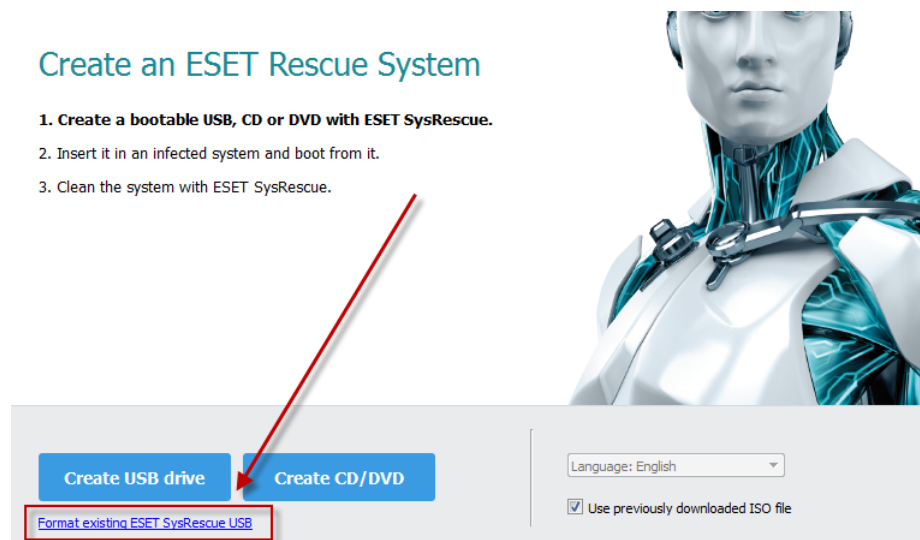


Note: This method of cleaning is only possible if you are running ESET SysRescue Live from a CD/DVD.

2. Cleaning ESET SysRescue Live using ESET Live USB Creator

1. Download and run [ESET Live USB Creator](#) on a Windows platform.
2. Click **Format existing ESET SysRescue Live USB**.
3. Select your ESET SysRescue Live media and confirm the **Erase USB drive** operation.

Figure 15 – Location of the formatting option




Note: Cleaning is only available when ESET SysRescue Live data is stored on a USB flash drive. This prevents destruction of data on other USB flash drives. If you are working in Windows, you will only be able to format the first USB partition (disk), because ESET SysRescue Live creates three Linux-specific partitions.

7. Bomgar and TeamViewer

In the case of a difficult technical problem (for example, you are unable to perform a rescue operation on your computer because of a virus), you can use *TeamViewer* or *Bomgar* proprietary software to enable remote control, desktop sharing, online meetings and file transfers between your computer and ESET Customer Care.

Important: These service may not be available in your country. Contact your local [ESET Customer Care](#) office for more details.

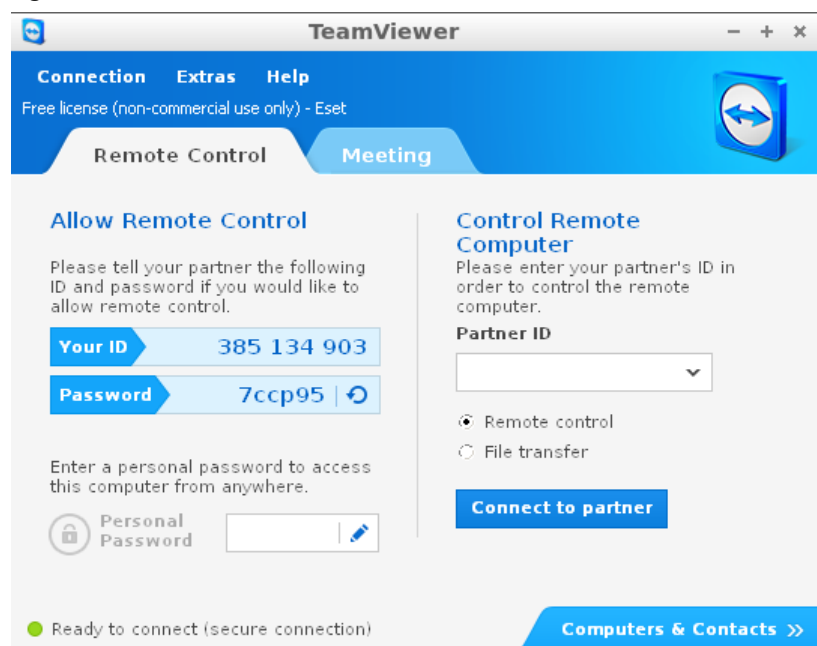
To open a new Bomgar session, please follow these steps:

1. Run Bomgar in the ESET SysRescue Live [desktop environment](#). Click system menu  in the bottom left corner, then navigate to **Internet** and select **Bomgar Support**.
2. Contact your local ESET Customer Care via telephone during operational hours.
3. When prompted, enter a session key you have received from ESET Customer Care.

To open a new TeamViewer session please follow these steps:

1. Run TeamViewer in the ESET SysRescue Live [desktop environment](#). Click system menu  in the bottom left corner, then navigate to **Internet** and select **TeamViewer**.

Figure 16 – TeamViewer



2. Make sure that **Ready to connect (secure connection)** is displayed.
3. Contact your local ESET Customer Care via telephone during operating hours.
4. When prompted, you have to tell **Your ID** and the **Password** in order to create a new TeamViewer remote session.

After your problem is resolved, an ESET support engineer will disconnect the remote session on your computer.

8. About Desktop environment

ESET SysRescue Live runs under GNU Linux OS. The desktop LXDE session environment makes it lightweight and fast.

The package system APT (Debian package management utility) allows you to install potentially useful packages, for example applications or drivers.

If you are an experienced Linux administrator, you can use *LXTerminal* console to perform the necessary operations under root privileges (you must enter `sudo` before each console command), such as *fsck* for file-system check, *fdisk* (console version), or *GParted* (graphic user interface version) to open the partition manager.


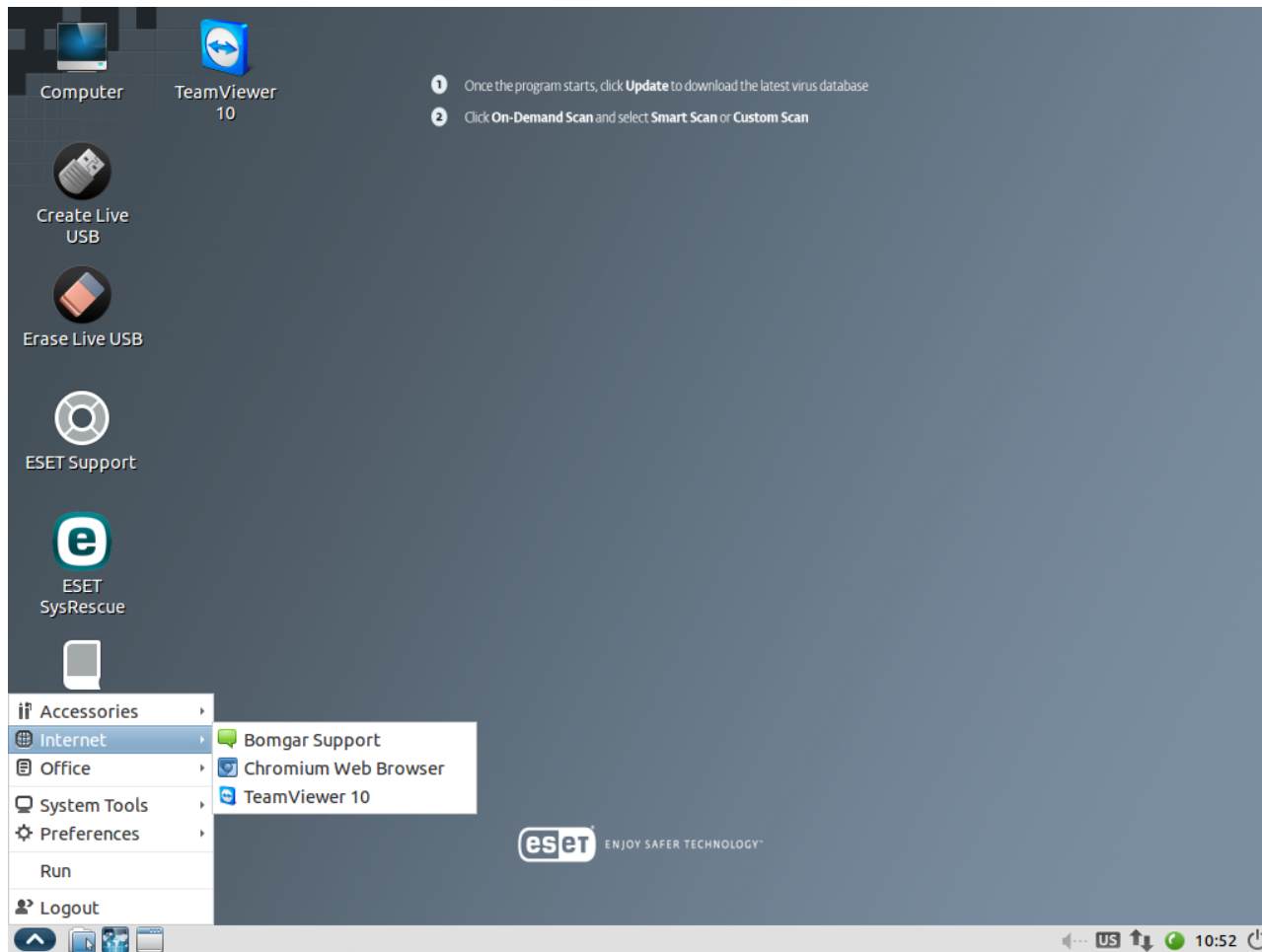
To access the Internet, use the integrated Chromium web browser by clicking system menu  > **Internet** > **Chromium Web Browser**.

Figure 17 – Desktop environment overview



Note: In the ESET SysRescue Live environment, applications may take longer to load, particularly if you are running them from a CD/DVD.

8.1 Network

If you are connected to the Internet, you will most likely obtain the IP address automatically from DHCP server.

Use the **Network Connections** tool to modify network properties:


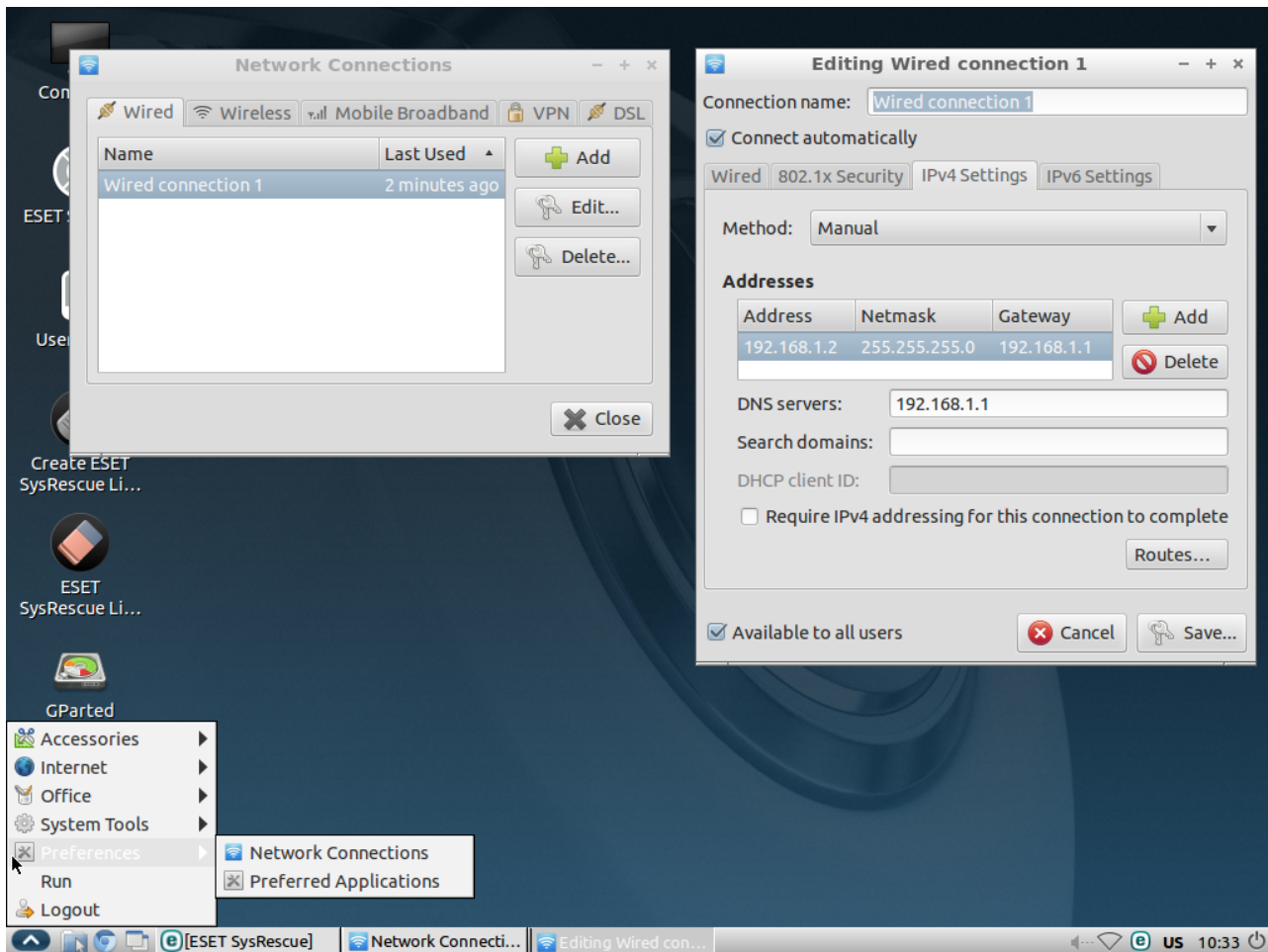
1. Click system menu  in the bottom left corner.
2. Navigate to **Preferences** and select **Network Connections**.
3. To change network settings, select your network connection and click **Edit**.
4. The **Editing Wired connection** window will open. Select the **IPv4 Settings** tab.
5. Change **Method** to **Manual** and enter the required data in the **Address**, **Netmask**, **Gateway** and **DNS servers** fields.
6. Click **Save** and reconnect the network.

Figure 18 – Network Connections



A working Internet connection is required for ESET SysRescue Live to receive virus signature database updates.

If a proxy server is used to control the Internet connection of a system where ESET SysRescue Live is installed, you must specify proxy server details. To do so, press **F5** to open the **Preferences** window and select Proxy server in the **Miscellaneous** section.

Figure 19 – ESET SysRescue Proxy Server configuration



8.2 Data Backup

ESET SysRescue Live can back up your data and system information to a USB flash drive.

Important: Before you remove the USB drive from your computer, right-click it in **File Manager** and select **Unmount Volume**.


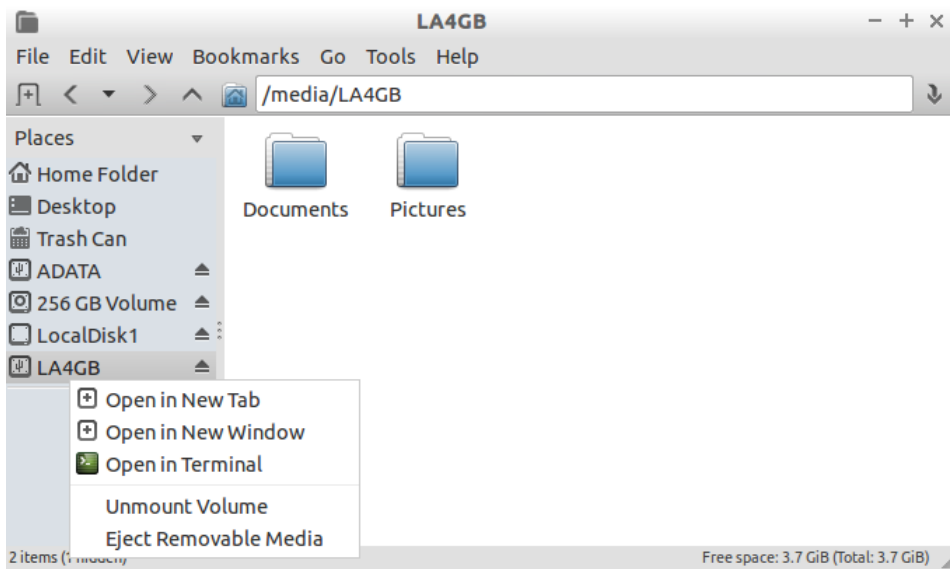
Click system menu , navigate to **Accessories** and select **File Manager**. Browse for and copy the desired files to your USB drive.

Figure 19 – File Manager



9. Troubleshooting

Following instructions may help you to resolve common ESET SysRescue Live issues.

I cannot run ESET SysRescue Live from my removable media

For ESET SysRescue Live to function properly, your computer must allow booting from removable media. You can modify boot priority settings in the BIOS, which is usually accessed by pressing one of the function keys (F8-F12) or the ESC key during startup. Instructions for accessing the BIOS are typically displayed on-screen during startup.

Unable to perform a virus signature database update


If an update fails, check the internet connection in the [Network Connection settings](#) located in the **Preferences** menu at the bottom left of the screen.

I do not know my username or password

Since ESET SysRescue is a free tool, a username and password are not required for automatic updates of the virus signature database.

ESET SysRescue window does not start after booting up

ESET SysRescue window should start automatically under normal circumstances. If not, try to run the ESET SysRescue GUI manually using *LXTerminal*.

1. Click system menu  in the bottom left corner.
2. Navigate to **Accessories** and select **LXTerminal**.
3. Run the following commands in the console:

```
killall esets_gui  
/opt/eset/esets/bin/esets_gui
```

I cannot scan a partition on my hard disk

The complete list of supported filesystems by ESET SysRescue Live can be found in the following folder:

```
/lib/modules/$(uname -r)/kernel/fs
```

Click  **ESET Support** on your Desktop, or visit [our Knowledgebase](#) if you still cannot resolve your issue.