User Manual

Table of Contents

- WebGuard
- Quarantine
- Scheduler
- Reports
- Events
- Refresh

Extras

- Boot Records Scan
- Detection List
- Configuration

Update

- Start Update
- Product Updates

Help

- Readme
- Contents
- Support
- Load License File
- About Anti-Virus Helix

Configuration

Scanner

- Scan
  - Action for Concerning Files
  - Further Actions
  - Archives
  - Exceptions
  - Heuristic
- Report
  - Reporting

Guard

- Scan
  - Action for Concerning Files
  - Other Actions
  - Exceptions
  - Heuristic
- Report
  - Reporting

MailGuard

- Scan
  - Action on Malware
  - Other actions
  - Heuristic
  - AntiBot
- General
  - Exceptions
  - Cache
- Report
  - Logging
  - Limit Report File

User Manual

Product Information

This section contains all information relevant to the purchase and use of Lavasoft Anti-Virus Helix:

- System requirements
- Licensing

Lavasoft Anti-Virus Helix is a comprehensive and flexible tool you can rely on to protect your computer from viruses, malware, unwanted programs, and other dangers

- Please note the following information:

Note
Loss of valuable data usually has dramatic consequences. Even the best virus protection program cannot provide one hundred percent protection from data loss. Make regular copies (Backups) of your data for security purposes.

Note
A program can only provide reliable and effective protection from viruses, malware, unwanted programs and other dangers if it is up-to-date. Make sure Lavasoft Anti-Virus Helix is up-to-date with automatic updates. Configure the program accordingly.

System Requirements

For Lavasoft Anti-Virus Helix to work properly, the computer system must fulfill the following requirements:

- Computer as from Pentium, at least 266 MHz
- Operating system
  - Microsoft Windows Vista (32- or 64- bit) or
  - Microsoft Windows XP Home or Professional (32- or 64-bit), SP2 recommended, or
  - Microsoft Windows 2000, SP 4 recommended
- At least 192 MB RAM with Windows 2000/XP
- At least 512 MB RAM with Windows Vista
- 40 MB free memory space on the hard disk (more if using the quarantine function)
- 100 MB temporary memory space on the hard disk
- For the installation of Lavasoft Anti-Virus Helix: administrator rights under Windows 2000 and XP

Information for Windows Vista Users

On Windows 2000 and Windows XP, many users work with administrator rights. However, this is not desirable from a security point of view because it is easy for viruses and unwanted programs to infiltrate computers.

For this reason, Microsoft introduced the "User Account Control" with Windows Vista. This

offers more protection for users who are logged in as administrators. Actions which require administrator rights are clearly marked in Windows Vista with an information icon; the user must explicitly confirm the required action. Privileges are only increased and the administrative task carried out by the operating system after this permission has been obtained.

Lavasoft Anti-Virus Helix requires administrator rights for some actions in Windows Vista. If your current user account does not have administrator rights, the Windows Vista dialog of the User Account Control asks you to enter the administrator password. If you do not have an administrator password, you cannot carry out this action.

Licensing

Software License Agreement

Please read the terms and conditions of this license agreement (the "License") before installing the computer software (the "Software"). By installing and using the Software you accept and agree to the terms of this License. This License constitutes the entire agreement concerning the Software between you and Lavasoft AB and it supersedes any prior proposal or representation. If you do not agree with these terms and conditions, promptly un-install the Software and, if you paid for a License, contact your distributor for a refund of the amount that you paid.

The term "Software" includes, and these terms and conditions also apply to, any updates, modifications and upgrades to the Software that you may receive from time to time.

1. License Grant

This License permits you, as purchaser of the Software, to use one copy of the Software solely for your use on one computer per purchased copy of the software, or, for users of Windows® Terminal Server ("WTS"), solely for use by users covered under the WTS License. If you have purchased a 3-seat or 5-seat multi-pack license, you are permitted to use the Software on up to 3 or 5 computers, respectively. The enclosed documentation ("Documentation") may not be copied. You agree that you will not sub-license, assign, transfer, distribute, pledge, lease, rent or share your rights under this License except with prior written permission from Lavasoft AB. You agree that you will not modify, adapt or translate, disassemble, decompile, reverse engineer or otherwise attempt to discover the source code of the Software.

2. Standard Maintenance and Support

All updates and technical support for your purchased Software are free of charge for the licence duration.

3. Lavasoft AB's Rights

You acknowledge and agree that the Software and Documentation (the "Licensed Products") are proprietary products of Lavasoft AB and its licensors under international copyright law and disclosed to you by Lavasoft AB in confidence. You shall take all reasonable steps to safeguard the Licensed Products. Lavasoft AB and its licensors own and retain all copyright-, trademark-,

trade secret- and other proprietary rights in and to the Licensed Products. This License conveys only a non-exclusive and limited right of use to you, revocable in accordance with the terms and conditions of this License. All rights in the Licensed Products not expressly granted in this Agreement are reserved by Lavasoft AB and its licensors.

4. Service Level Agreements

Support services may be purchased under separate agreement with Lavasoft AB.

5. Limited Warranty

Lavasoft AB warrants that for your benefit alone, for ninety (90) days from the day of delivery to you (the "Warranty Period"), the Software media, under normal use in a compatible execution environment, will be free from defects in material and workmanship. Any replacement program will be warranted for the remainder of the original warranty period or thirty (30) days from the date of receipt by you, whichever is longer. In no event may you bring any claim, action or proceeding arising out of the warranty set forth in this Article 4 more than six (6) months after the date on which the breach of warranty occurred.

6. Exceptions to Warranties; Disclaimers

EXCEPT FOR THE ABOVE MENTIONED LIMITED WARRANTY, Lavasoft AB DISCLAIMS ANY AND ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE. Lavasoft AB does not warrant that the Software, its use, operation or your ability to use the Software will be uninterrupted or error-free or that all Software errors will be corrected. The warranty set forth above shall not apply to any defect or problems caused by any defect in any hardware or software used in combination with the Software, or use of the Software in execution environments not specified in the Documentation. Lavasoft AB does not warrant that the Software or service will meet your requirements or that the operation of the Software will be uninterrupted or error free.

Lavasoft AB's limited warranty is void if a breach of the warranty has resulted from (i) accident, corruption or misuse of the Software; or (ii) acts or omissions by someone other than Lavasoft AB.

7. Refund Policy

Lavasoft AB will refund the full price of the Software if the Software is damaged, defective, or does not function properly. A refund will only be received if you notify Lavasoft AB of the refund request within thirty (30) days after the date you purchased the Software.

8. Exclusive Remedies

You agree that if a defect in the Software media appears during the Warranty Period, your exclusive remedy will be, in Lavasoft AB's sole option, to replace the media or to credit the amount paid by you to Lavasoft AB, if any, and terminate this License. The later remedy is subject to the return of all copies of the Licensed Products.

9. Limitations of Liability

In no event shall Lavasoft AB be liable for any damages to you or any other party whether arising out of contract or from tort including loss of data, profits or business, or other special, incidental, exemplary or consequential damages, even if Lavasoft AB has been advised of the possibility of such loss or damages. Lavasoft AB's cumulative liability shall not exceed the license fee paid, if any, for use of this Software and Documentation. This section shall survive termination of this License.

10. Termination

This agreement is in effect until terminated. You may terminate the agreement at any time by destroying all copies of the Software and Documentation and erasing any copies on storage media. The agreement also terminates if you fail to comply with any terms and conditions of this agreement. In such an event, you agree to destroy and erase all copies of the Software and Documentation, and Lavasoft AB will be entitled to all remedies in accordance with applicable law.

11. General

This agreement is governed by the laws of Sweden.

12. Contact

Use of the Software other than for your internal operations on a single computer requires that you enter into a separate license agreement with Lavasoft AB. Please e-mail sales@lavasoft.com for further information.

Installation and Uninstallation

This section contains information relating to the installation and uninstallation of your Lavasoft Anti-Virus Helix:

- Installation: Conditions, Installation Types, Install
- Installation Modules
- Modification Installation
- Uninstallation: Uninstall

Installation

Before installing Lavasoft Anti-Virus Helix, check that your computer fulfills the minimum system requirements.

Note
From Windows XP, Lavasoft Anti-Virus Helix generates a restore point of your computer before installation. This enables you to safely remove Lavasoft Anti-Virus Helix if installation fails. For this to occur, the option **Turn off System Restore** under: "Start | Settings | Control Panel | System | Tab System Restore" must not be marked.
If you want to recover your earlier system, you can do so with the function "Start | Programs | Accessories | System Tools | System Restore". The restore point generated by Lavasoft Anti-Virus Helix is indicated by the Anti-Virus Helix entry.

Installation Types

During installation, you can select a setup type through the installation assistant:

Complete

Anti-Virus Helix is completely installed with all program components. The program files are installed to a given standard folder under `C: \Program Files` .

Custom

You can choose to install individual program components (see the chapter: Installation and Deinstallation - Installation Modules). A destination folder can be selected for the program files to be installed. You can disable creating a desktop icon and program group in the Start menu and predefine a setting for the Win32 file heuristic.

Before Starting Installation

- Close your e-mail program. It is also recommended to end all running applications.
- Make sure that no other virus protection solutions are installed. The automatic protection functions of various security solutions may interfere with each other.
- Establish an Internet connection: an Internet connection is required for the activation of Lavasoft Anti-Virus Helix .

Install

The installation program runs in self-explanatory dialog mode. Every window contains a

certain selection of buttons to control the installation process.

The most important buttons are assigned the following functions:

- **OK:** Confirm action.
- **Abort:** Abort action.
- **Next:** Go to next step.
- **Back:** Go to previous step.

How to install Anti-Virus Helix:

- Start the installation program by double-clicking on the installation file that you have downloaded from the Internet or insert the program CD.
- After a safety message, which acknowledges the producer of the software, the dialog box of the installation program will appear.
- Click **Accept**.
- The dialog box *Welcome...* appears.
- Click **Next**.
- The dialog box *More Threat Categories* appears containing information on basic and advanced protection.
- Click **Next**.
- The dialog box with the license agreement appears.
- Confirm that you accept the license agreement and click **Next**.
- The dialog box *Select installation type* appears.
- Decide whether you want to perform a Complete or a Custom installation.
- Confirm by clicking **Next**

Custom installation

- The dialog box *Choose destination folder* appears.
- Confirm the specified destination directory by clicking **Next**.

- OR -

Use the **Browse** button to select a different destination directory and confirm by clicking **Next**.

- The dialog box *Install components* appears:
- Enable or disable the required components and confirm by clicking **Next**.
- In the following dialog box you can choose to enable the Win32 file heuristic and select low, medium or high detection level.
- Click **Next**.
- In the following dialog box you can choose to create a desktop shortcut and/or a program group in the Start menu.
- Click **Next**.

Continue for full and custom installation.

- The license assistant is opened.

You have the following options to activate Anti-Virus Helix.

- Enter an activation code.

By entering your activation code Lavasoft Anti-Virus Helix is activated with your

license.

- Select the option **Test product**

If you select **Test Product**, an evaluation license will be generated during the activation process. You can test Lavasoft Anti-Virus Helix with its complete range of functions for a certain period of time.

Note
By using the option **Valid hbedv.key license file available** you can load a valid license file. During product activation with a valid activation key, the license file is generated and saved in the program folder of Lavasoft Anti-Virus Helix. Use this option if you have activated a product and want to re-install Lavasoft Anti-Virus Helix without an active Internet connection.

Note
In order to activate Anti-Virus Helix a connection to Lavasoft's servers is established. Under **Proxy settings** you can configure the Internet link by a proxy server.

- Select an activation procedure and click **Next** to acknowledge.

Product activation

- A dialog box will open in order to enter your personal details.
- Enter your details and click **Next**
- Your details will be transmitted to Lavasoft's servers and will be checked. Lavasoft Anti-Virus Helix will be activated with your license.
- Your license data will be displayed in the next window.
- Click **Next**.
- Skip the following chapter "Activate by selecting the option **Valid hbedv.key available** ".

Select the option "Valid hbedv.key available"

- A box will be opened for loading the license file.
- Select the license file hbedv.key with your license data for Anti-Virus Helix and click **Open.**
- Your license data will be displayed in the next window.
- Click **Next.**

Continue after completed activation or loading of the license file

- The program components are installed and started.
- The setup program asks if the *readme.txt* file containing up-to-date information on Lavasoft Anti-Virus Helix should be displayed.
- Agree where appropriate and click **Finish**.
- Confirm the information by clicking **OK**.

Next procedure (varies slightly depending on the operating system):

- The setup program closes the installation and, where appropriate, creates a desktop shortcut.
- The file *readme.txt* is displayed where appropriate.
- You are asked if you want to perform an update.

Note
The latest version of Lavasoft Anti-Virus Helix provides reliable protection from the ever-increasing number of viruses and malware. Perform an update immediately after

installation. After this first update, the Windows Security Centre (XP and Vista) will announce that Lavasoft Anti-Virus Helix is ACTIVATED.

- OR -

- You are asked if you want to restart your computer.

If you want to perform an update:

- Click **Yes** to confirm.
- An update is sought for Lavasoft Anti-Virus Helix via the existing web server connection.
- Lavasoft Anti-Virus Helix then starts an automatic scan of the Windows system directories.

Note
The first scan is particularly important to ensure that your system is free from viruses and malware. Do not cancel the first scan.

If you want to restart your computer:

- Click **Yes** to confirm.
- The computer is restarted.

Modification Installation

You have the option to add or remove individual program components of the current Lavasoft Anti-Virus Helix installation (see Installation and Uninstallation - Installation Modules)

If you wish to add or remove modules of Lavasoft Anti-Virus Helix's installation, you can use the option **Add or Remove Programs** in the **Windows control panel** to **Change/ Remove** programs.

Select Lavasoft Anti-Virus Helix and click **Change**. In the welcome dialog of Lavasoft Anti-Virus Helix select the option **Modify**. You will be guided through the installation changes.

Installation Modules

In a Custom installation or a modification installation, the following installation modules can be selected, added or removed.

- **Anti-Virus Helix**
  This module contains all components required for successful installation of Lavasoft Anti-Virus Helix.
- **Anti-Virus Guard**
  The Anti-Virus Guard runs in the background. It monitors and repairs (when necessary) files during operations such as open, write and copy in on-access mode. Whenever a user carries out a file operation (e.g. load document, execute, copy), Lavasoft Anti-Virus Helix automatically scans the file. Renaming a file does not trigger a scan by Anti-Virus Guard.
- **Anti-Virus MailGuard**
  Anti-Virus MailGuard is the interface between your computer and the e-mail server

from which your e-mail program (mail client) downloads the e-mails. MailGuard is connected as a so-called proxy between the e-mail program and the e-mail server. All incoming e-mails are routed through this proxy, scanned for viruses and unwanted programs and forwarded to your e-mail program. Depending on the configuration, the program processes the affected e-mails automatically or asks the user for a certain action.

- **Anti-Virus WebGuard**
  When surfing the Internet, you are using your web browser to request data from a web server. The data transferred from the web server (HTML files, script and image files, Flash files, video and music streams, etc.) will normally be moved directly into the browser cache for display in the web browser, meaning that an on-access scan as performed by Anti-Virus Guard is not possible. This could allow viruses and unwanted programs to access your computer system. WebGuard is what is known as an HTTP proxy which monitors the ports used for data transfer (80, 8080, 3128) and checks the transferred data for viruses and unwanted programs. Depending on the configuration, the program may process the affected files automatically or prompt the user for a specific action.
- **Rootkit Detection**
  The Rootkit Detection checks whether software is already installed on your computer that can no longer be detected with conventional methods of malware protection after penetrating the computer system.
- **Shell Extension**
  The Lavasoft Anti-Virus Helix Shell Extension generates an entry Scan selected files with Anti-Virus in the context menu of the Windows Explorer (right-hand mouse button). With this entry you can directly scan files or directories.

Uninstallation

If you wish to remove Lavasoft Anti-Virus Helix from your computer, you can use the option **Add or Remove Programs** to **Change/Remove** programs in the Windows Control Panel.

To uninstall Lavasoft Anti-Virus Helix (e.g. in Windows XP and Windows Vista):

- Open the **Control Panel** via the Windows **Start** menu.
- Double click on **Software** (Windows Vista: **Program files**).
- Select **Lavasoft Anti-Virus Helix** and click **Remove**.
- You will be asked if you really want to remove the program.
- Click **Yes** to confirm.
- All components of the program are removed.
- Click on **Finish** to complete uninstallation.
- Where appropriate, a dialog box appears recommending that your computer be restarted.
- Click **Yes** to confirm.
- Lavasoft Anti-Virus Helix is uninstalled, and all directories, files and registry entries for Lavasoft Anti-Virus Helix are deleted when your computer restarts.

Anti-Virus Helix Overview

This section contains an overview of the functionality and operation of Anti-Virus Helix.

- User Interface and Operation
- How to...?

User Interface and Operation

Control Center

The Control Center is designed to monitor the protection status of your computer system and control and operate the protection components and functions of Anti-Virus Helix.

- Starting and ending Control Center
- Control Center operation

The Control Center window is divided into three areas: the **menu bar**, the **navigation area** and the detail window **view**:

- **Menu bar:** In the Control Center menu bar, you can access general program functions and information on Anti-Virus Helix.
- **Navigation area:** In the navigation area, you can easily swap between the individual sections of the Control Center. The individual sections contain information and functions of Anti-Virus Helix's program components and are arranged in the navigation bar according to activity. For example: Activity *Overview* – Section **Status**.

- **View:** This window shows the section selected in the navigation area. In the upper bar of the detail window, you will find buttons to execute functions and actions. Data or data objects are displayed in lists in the individual sections You can sort the lists by clicking in the box to define how to sort the list.

Opening and closing the Control Center

To open the Control Center, the following options are available:

- double click the program icon on your desktop
- via the Anti-Virus Helix program entry in the Start menu | program.
- via the Lavasoft Anti-Virus Helix tray icon.

Close the Control Center via the menu command **Close** in the menu **File** or by clicking on the close tab in the Control Center.

Control Center operation

To navigate in the Control Center

- Select an activity in the navigation bar.
- The activity opens and other sections appear. The first section of the activity is selected and displayed in the View.
- If necessary, click another section to display this in the detail window.

- OR -

- Select a section via the menu *View*.

Note
You can activate the keyboard navigation in the menu bar with the help of the [ALT] key. If navigation is activated, you can move within the menu with the arrow keys. You activate the active menu item with the Return key.

To process data or objects displayed in the detail window:

- highlight the data or object you wish to edit.

To highlight multiple elements (elements in columns), hold down the control key or the shift key while selecting the elements.

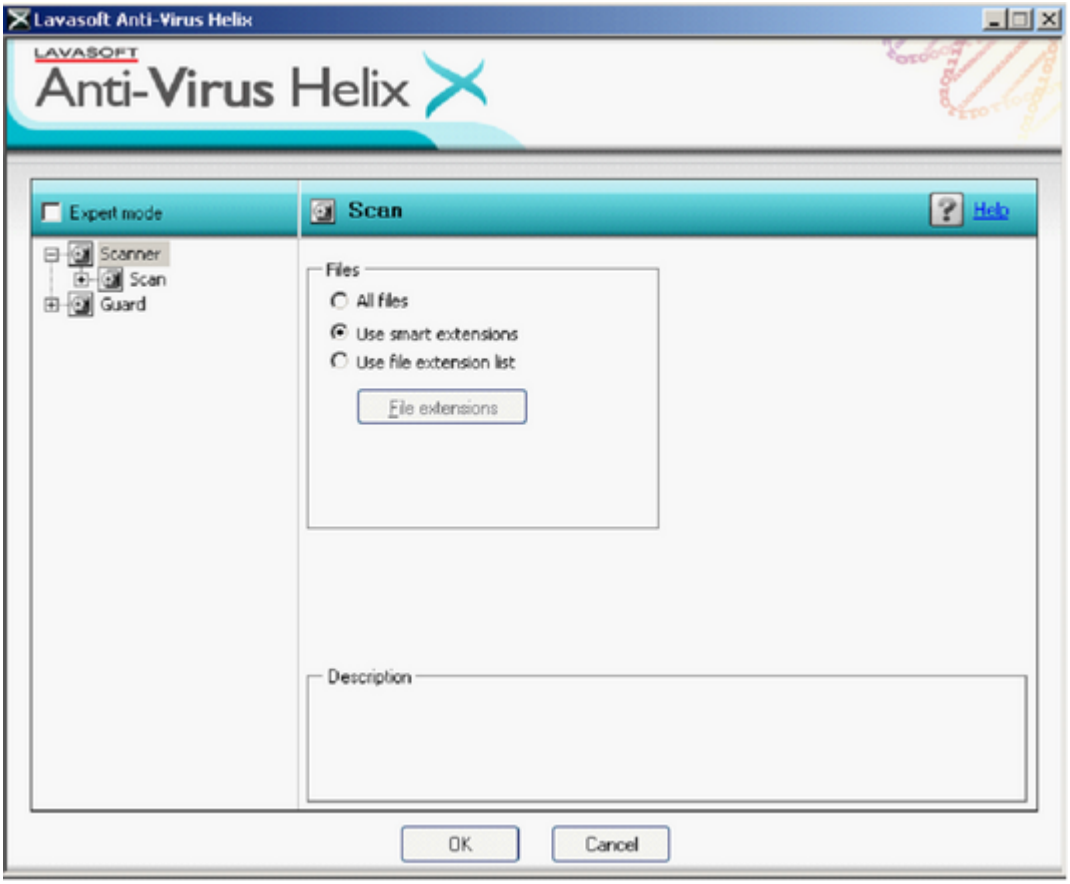
- Click the appropriate button in the upper bar of the detail window to edit the object

---

Configuration

In Lavasoft Anti-Virus Helix Configuration, you can implement settings for Anti-Virus Helix. After installation, Anti-Virus Helix is configured with standard settings, ensuring optimal protection for your computer system. However, your computer system or your specific requirements for Anti-Virus Helix may require that you adapt the protective components of Anti-Virus Helix.

- Accessing Lavasoft Anti-Virus Helix Configuration
- Operating Lavasoft Anti-Virus Helix Configuration



Lavasoft Anti-Virus Helix Configuration opens a dialog box: confirm or delete your configuration settings using the OK or Cancel button. You can select individual configuration sections in the left-hand navigation bar.

Accessing Lavasoft Anti-Virus Helix Configuration

You have several options for accessing the configuration:

- via the Windows control panel.
- via the Windows Security Center - from Windows XP Service Pack 2.
- via the Lavasoft Anti-Virus Helix tray icon.
- in the Lavasoft Anti-Virus Helix Control Center via the menu item Extras | Configuration.
- in the Lavasoft Anti-Virus Helix Control Center via the Configuration button.

Note

If you are accessing Configuration via the **Configuration** button in the Control Center, go to the configuration register of the section which is active in Control Center. Expert mode must be activated to select individual configuration registers. In this case, a dialog appears asking you to activate expert mode.

Lavasoft Anti-Virus Helix Configuration Operation

Navigate in the configuration window as you would in Windows Explorer:

- Click on an entry in the tree structure to display the configuration section in the

detail window
- Click on the plus symbol in front of an entry to expand the configuration section and display configuration subsections in the tree structure.
- To hide configuration subsections, click on the minus symbol in front of the expanded configuration section.

Note
All configuration sections are only displayed in expert mode. Activate expert mode to see all configuration sections Expert mode can be protected by a password which must be defined during activation.

If you want to confirm your configuration settings:
- Click **OK**.
- The configuration window is closed and the settings are accepted.

If you want to finish configuration without confirming your settings:
- Click **Cancel**.
- The configuration window is closed and the settings are discarded.

Tray Icon

After installation, you will see the Anti-Virus Helix tray icon in the system tray of the taskbar:

Central functions of Lavasoft Anti-Virus Helix can be quickly accessed via the context menu of the tray icon. To open the context menu, click on the tray icon with the right-hand mouse button.

How to...?

Anti-Virus Helix Automatic Update

Note
An update job has been pre-selected to update Lavasoft Anti-Virus Helix every 24 hours if an Internet connection is established and available.

To create a job in Anti-Virus Scheduler to update Lavasoft Anti-Virus Helix automatically:
- In the Control Center, select the **Manager :: Scheduler** section.
- Click on the  *Insert new job* icon.
- The dialog box *Name and description of job* appears.
- Give the job a name and, where appropriate, a description.
- Click **Next**.
- The dialog box *Type of job* is displayed.
- Select **Update job** from the list.
- Click **Next**.
- The dialog box *Time of job* appears.
- Select a time for the update:
- **Immediately**
- **Daily**

- **Weekly**
- **Interval**
- **Once**
- **Login**

Note
We recommend that you update Lavasoft Anti-Virus Helix regularly and often, e.g. every 6 hours.

- Where appropriate, specify a date according to the selection.
- Where appropriate, select additional options (availability depends on type of job):
- **Also start job when Internet connection is established**

In addition to the defined frequency, the job is carried out when an Internet connection is set up.
In addition to the defined frequency, the job is carried out when an Internet connection is set up.

- **Repeat job if the time has already expired**

Past jobs are carried out that could not be carried out at the required time, for example, because the computer was switched off.

- Click **Next**.
- The dialog box *Select display mode* appears.
- Select the display mode of the job window:
- **Minimize**: progress bar only
- **Maximize**: Entire job window
- **Hide**: No job window
- Click **Finish**.
- Your newly created job appears on the start page of the **Manager :: Scanner** section with the status activated (check mark).
- Where appropriate, deactivate jobs which are not to be carried out.

Use the following icons to further define your jobs:

 Display properties of the selected job

 Edit selected job

 Delete selected job

---

Start a Manual Update

You have various options for starting a Lavasoft Anti-Virus Helix update manually. When an update is started manually, the virus definition file and search engine are always updated. A product update can only take place if you have activated the option **Download and automatically install product updates** in the configuration under General :: Update

To start a Lavasoft Anti-Virus Helix update manually:

- With the right-hand mouse button, click on the Lavasoft Anti-Virus Helix tray icon in the taskbar.
- A context menu appears.

- Select **Start update**.
- The dialog box *Lavasoft Anti-Virus Helix Updater* appears.

- OR -

- In the Control Center, select the **Overview :: Status** section.
- In the *Last update* field, click on the link **Start update**.
- The Lavasoft Anti-Virus Helix Updater dialog box appears.

- OR -

- In the Control Center, in the **Update** menu, select the menu command *Start update*.
- The Lavasoft Anti-Virus Helix Updater dialog box appears.

Note
We strongly recommend regular automatic updates for Lavasoft Anti-Virus Helix, e.g. every 24 hours.

Note
You can also carry out a manual update directly via the Windows Security Center.

On-Demand Scan: Using a Scan Profile to Scan for Viruses and Malware

A scan profile is a set of drives and directories to be scanned.

The following options are available for scanning via a scan profile:

- Use predefined scan profile

if the predefined scan profile corresponds to your requirements.

- Customize and apply scan profile (manual selection)

if you want to scan with a customized scan profile.

- Create and apply new scan profile

if you want to create your own scan profile.

Depending on the operating system, various icons are available for starting a scan profile:

- In Windows XP and 2000:


This icon starts the scan via a scan profile.

- In Windows Vista:

In Microsoft Windows Vista, the control center only has limited rights, e.g. for access to directories and files. Certain actions and file accesses can only be carried out in the Control Center with extended administrator rights. These extended administrator rights must be granted at the start of each scan via a scan profile.


This icon starts a limited scan via a scan profile. Only directories and files that Windows Vista has granted access rights to are scanned.


This icon starts the scan with extended administrator rights. After confirmation, all directories and files in the selected scan profile are scanned.

To scan for viruses and malware with a scan profile:

- In the Control Center select the **Local protection :: Scanner** section.
- Predefined scan profiles appear.

- Select one of the predefined scan profiles.

-OR-

- Adapt the scan profile *Manual selection*.

-OR-

- Create a new scan profile
- Click on the (Windows XP:  or Windows Vista: ) icon.
- The *Virus Scan Helix* window appears and an on-demand scan is started.
- When the scan is complete, the results are displayed.

If you want to adapt a scan profile:

- In the scan profile, expand **Manual Selection** in the file tree so that all the drives and directories you want to scan are open.
- Click on the + symbol: The next directory level is displayed.
- Click on the - symbol: The next directory level is hidden.
- Highlight the nodes and directories you want to scan by clicking on the relevant box of the appropriate directory level.

The following options are available. Select directories:

- Directory, including sub-directories (black check mark)
- Directory, excluding sub-directories (green check mark)
- Sub-directories of one directory only (grey check mark, sub-directories have black check marks)
- No directory (no check mark)

If you want to create a new scan profile:

- Click on the  **Create new profile** icon.
- The profile *New profile* appears below the profiles previously created.
- Where appropriate, rename the selected profile by clicking on the icon  .
- Highlight the nodes and directories to be saved by clicking on the check box of the respective directory level.

The following options are available. Select directories:

- Directory, including sub-directories (black check mark)
- Directory, excluding sub-directories (green check mark)
- Sub-directories of one directory only (grey check mark, sub-directories have black check marks)
- No directory (no check mark)

On-Demand Scan: Scan for Viruses and Malware Using Drag & Drop

To scan for viruses and malware systematically using Drag & Drop:

- Open Lavasoft Anti-Virus Helix's Control Center.
- Highlight the file or directory you want to scan.
- Use the left-hand mouse button to drag the highlighted file or directory into the *Control Center*.

- The *Virus Scan Helix* window appears and an on-demand scan is started.
- When the scan is complete, the results are displayed.

On-Demand Scan: Scan for Viruses and Malware Via the Context Menu

To scan for viruses and malware systematically via the context menu:

- Click with the right-hand mouse button (e.g. in Windows Explorer, on the desktop or in an open Windows directory) on the file or directoryyou want to scan.
- The Windows Explorer context menu appears.
- Select **Scan selected files with Lavasoft Anti-Virus Helix** in the context menu.
- The *Virus Scan Helix* window appears and the on-demand scan starts.
- When the scan is complete, the results are displayed.

On-Demand Scan: Automatically Scan for Viruses and Malware

To create a job to automatically scan for viruses and malware:

- In the Control Center select **Manager ::** section **Scheduler**.
- Click on the icon 
- The dialog box *Name and description of job* appears.
- Give the job a name and, where appropriate, a description.
- Click **Next**.
- The dialog box *Type of job* appears.
- Select **Scan job**.
- Click **Next**.
- The dialog box *Select profile* appears.
- Select the profile to be scanned.
- Click **Next**.
- The dialog box *Time of job* appears.
- Select a time for the scan:
- **Immediately**
- **Daily**
- **Weekly**
- **Interval**
- **Once**
- **Login**
- Where appropriate, specify a date according to the selection.
- Where appropriate, select the following additional options (availability depends on job type):
- **Repeat job if the time has already expired**

Past jobs are carried out that could not be carried out at the required time, for example because the computer was switched off.

- Click **Next**.

- The dialog box *Select display mode* appears.
- Select the display mode of the job window:
- **Minimize**: progress bar only
- **Maximize**: Entire job window
- **Hide**: No job window
- Click **Finish**.
- The job you have just initiated is shown as activated (check mark) on the start page of the **Manager :: Scheduler** section.
- Where appropriate, deactivate jobs which are not to be carried out.

Use the following icons to further define your jobs:

 View properties of a job

 Modify job

 Delete job

---

On-Demand Scan: Targeted Scan for Active Rootkits

To scan for active rootkits, use the predefined scan profile *Scan for rootkits*.

To scan for active rootkits systematically:

- In the Control Center select the **Local protection :: Scanner** section.
- Predefined scan profiles appear.
- Select the predefined scan profile **Scan for rootkits**.
- Where appropriate, highlight other nodes and directories to be scanned by clicking on the check box of the directory level.
- Click on the (Windows XP:  or Windows Vista: ) icon.
- The *Virus Scan Helix* window appears and an on-demand scan is started.
- When the scan is completed, the results are displayed.

Reacting to Detected Viruses and Malware

For the individual protection components of Anti-Virus Helix, you can define how Anti-Virus Helix reacts to a detected virus or unwanted program in the Configuration under the section *Action for concerning files*.

- **Interactive**

When this option is enabled, if a virus or unwanted program is detected, a dialog box appears in which you can select what to do with the infected object. This option is enabled as the default setting.

- **Automatic**

When this option is enabled, if a virus or unwanted program is detected, no dialog box appears and you cannot select an action. The component reacts in accordance with your predefined settings.

If you have selected the option *Interactive* for your protection components, Lavasoft Anti-Virus Helix gives you the following options for actions to take:

Note

The options displayed depend on the operating system and the module, (Anti-Virus Guard, Anti-Virus Scanner or Anti-Virus MailGuard), that makes the detection.

- **Repair**

The file is repaired.This option is only available if the infected file can be repaired.

- **Move to quarantine**

The file is packaged into a special format (**.qua*) and moved to the Quarantine directory *INFECTED* on your hard disk, so that direct access is no longer possible. Files in this directory can be repaired in Quarantine at a later data or, if necessary, sent to Lavasoft .

- **Delete**

The file is deleted but can be recovered with the appropriate tools (e.g. *Lavasoft UnErase*). This allows the virus signature to be recovered. This process is significantly quicker than *Overwrite and delete*.

- **Overwrite and delete**

The file is overwritten with a default template and then deleted. It cannot be restored.

- **Rename**

The file is renamed with a **.vir* extension. Direct access to these files (e.g. by double-clicking) is therefore no longer possible. Files can be repaired and given their original name at a later time.

- **Deny access**

If this option is enabled, the detection is only entered in the report file.

- **Ignore**

Lavasoft Anti-Virus Helix takes no further action. The infected file remains active on your computer.

Warning

This could result in loss of data and damage to the operating system! Only use the Ignore option in exceptional cases.

- **Take no further action**

Access to the file is blocked.

- **Copy file in quarantine before action**

This option can only be selected if one of the options – Repair, Delete, Overwrite and Delete – is selected.

- **Apply selection to all subsequent detections**

The action selected for this detection is applied to the next detection.

Note

We recommend that you move any suspicious file that cannot be repaired to Quarantine.

You can identify files reported by the heuristic from the designation *HEUR/* or *HEURISTIC/* that prefixes the file name, e.g.: *HEUR/testdatei.**.

If viruses or malware have been found in an archive file, you have the following options:

- Delete the entire archive
- Rename the archive
- Move archive to Quarantine

Note
Individual infected files cannot be deleted from the archive.

Quarantine: Handling Quarantined Files (*.qua)

To handle quarantined files:

- In the Control Center select **Manager :: Quarantine** section.
- Check which files are involved, so that, if necessary, you can reload the original back onto your computer from another location.

If you want to see more information on a file:

- Highlight the file and click on 
- The dialog box *Properties* appears with more information on the file.

If you want to rescan a file:

Scanning a file is recommended if the Lavasoft Anti-Virus Helix virus definition file has been updated and a false positive report is suspected. This enables you to confirm a false positive with a rescan and restore the file.

- Highlight the file and click on 
- The file is scanned for viruses and malware using the on-demand scan settings.
- After the scan, the dialog *Scan statistics* appears which displays statistics on the status of the file before and after the rescan.

To delete a file:

- Highlight the file and click on 

You can also restore the files in Quarantine:

See Quarantine - Restoring Files in Quarantine

Quarantine - Restoring Files in Quarantine

Different icons control the restore procedure, depending on the operating system:

- In Windows XP and 2000:

 This icon restores the files to their original directory.

 This icon restores the files to a directory of your choice.

- In Windows Vista:

In Microsoft Windows Vista, the Control Center only has limited rights, e.g. for access to directories and files. Certain actions and file accesses can only be carried out in the Control Center with extended administrator rights. These extended administrator rights must be granted at the start of each scan via a scan profile.

 This icon restores the files to a directory of your choice.

 This icon restores the files to their original directory. If extended administrator rights are necessary to access this directory, a corresponding request appears.

To restore files in quarantine:

Warning
This could result in loss of data and damage to the computer's operating system! Only use the function *Restore selected object* in exceptional cases. Only restore files that could be repaired by a new scan.

- File rescanned and repaired.
- In the Control Center select **Manager :: Quarantine** section.

Note

E-mails and e-mail attachments can only be restored using the option  if the file extension is *. *eml*.

To restore a file to its original location:

- Highlight the file and click on the (Windows 2000/XP:  , Windows Vista ) icon.

This option is not available for e-mails.

Note

E-mails and e-mail attachments can only be restored using the option  if the file extension is *. *eml*.

- A message appears asking if you want to restore the file.
- Click **Yes**.
- The file is restored to the directory it was in before it was moved to quarantine.

To restore a file to a specified directory:

- Highlight the file and click on 
- A message appears asking if you want to restore the file.
- Click **Yes**.
- The Windows default window for selecting the directory appears.
- Select the directory to restore the file to and confirm.
- The file is restored to the selected directory.

Quarantine - Move Suspicious Files to Quarantine

To move a suspect file to quarantine manually:

- In the Control Center select the **Manager :: Quarantine** section.
- Click on 
- The Windows default window for selecting a file appears.
- Select the file and confirm.
- The file is moved to quarantine.

You can scan files in quarantine with Anti-Virus Scanner: See Quarantine - Handling Quarantined Files (*.qua)

Scan Profile: Amend or Delete File Type in a Scan Profile

To stipulate additional file types to be scanned or exclude specific file types from the scan in a scan profile (only possible for manual selection and customized scan profiles):

- In the Control Center go to the section **Local protection :: Scanner.**
- With the right-hand mouse button, click on the scan profile you want to edit.
- A context menu appears.
- Select **File filter**.
- Expand the context menu further by clicking on the small triangle on the right-hand side of the context menu.
- The entries *Default*, *Scan all files* and *Custom* appear.
- Select **Custom**.
- The *File extensions* dialog box appears with a list of all file types to be scanned with the scan profile.

If you want to exclude a file type from the scan:

- Highlight the file type and click **Delete**.

If you want to add a file type to the scan:

- Highlight the file type.
- Click **Add** and enter the file extension of the file type into the input box.

Use a maximum of 10 characters and do not enter the leading dot. Wildcards (* and ?) are allowed as replacements.

Scan Profile: Create Desktop Shortcut for Scan Profile

You can start an on-demand scan directly from your desktop, without accessing the Lavasoft Anti-

Virus Helix Control Center, via a desktop shortcut to a scan profile. To create a desktop shortcut to the scan profile:

- In the Control Center, go to the section **Local protection :: Scanner.**
- Select the scan profile you want to create a shortcut for.
- Click on the icon  .
- The desktop shortcut is created.

Events: Filter Events

In the Control Center, under **Overview :: Events**, events are displayed that have been generated by Anti-Virus Helix program components. (analogous to the event display of your Windows operating system). The program components are:

- Updater
- Guard
- MailGuard
- Scanner
- Scheduler

The following event types are displayed:

- Information
- Warning
- Error
- Detection

To filter displayed events:

- In the Control Center, select the section **Overview :: Events**.
- Check the box of the program components to display the events of the activated components.

- OR -

Uncheck the box of the program components to hide the events of the deactivated components.

- Check the event type box to display these events.

- OR -

Uncheck the event type box to hide these events.

MailGuard: Exclude E-mail Addresses from Scan

To define which e-mail addresses (senders) are excluded from the MailGuard scan (whitelisting):

- Go to the Control Center and select the section **Online protection :: MailGuard**.
- The list shows incoming e-mail.
- Highlight the e-mail you want to exclude from the MailGuard scan.

- Click on the appropriate icon to exclude the e-mail from the MailGuard scan:


In the future, the selected e-mail address will no longer be scanned for viruses and unwanted programs.

- The e-mail sender's address is included in the exceptions list and no longer scanned for viruses and malware .

Warning
Only exclude e-mail addresses from the MailGuard scan if the senders are completely trustworthy.

Note
You can add other e-mail addresses to the exceptions list or remove e-mail addresses from the exceptions list in the configuration under **MailGuard :: General :: Exceptions**.

Detection

This section contains comprehensive information, arranged according to module, on detection messages. You can also find information on detected viruses and unwanted programs in archives and mailboxes and on detected boot sector viruses.

- Scanner
- Guard
- MailGuard
- WebGuard
- Archive
- Boot sector virus
- Detection in mailbox
- Blocked file
- Rootkits

Scanner

If the option **Interactive** is selected in the configuration of the Scanner in the group **Action for concerning files**, you are asked what is to be done with a detected virus or unwanted program.

Note
If reporting is enabled, the Scanner enters each detection in the Report file.

Name and Path of the Currently Detected Virus or Unwanted Program

The name and path of the currently detected virus or unwanted program is displayed in the middle window of the message.

Options

Note

In Interactive mode, if the detection is a heuristic hit (HEUR/), an unusual runtime compression tool (PCK/) or a file with a hidden file extension (HEUR-DBLEXT/), the only options available are **Move to quarantine** and **Ignore**. In Automatic mode, the detection is automatically moved to quarantine. This restriction prevents detected files, which could be false positives, from being directly removed (deleted) from your computer. The file can be recovered at any time with the aid of the Quarantine Manager.

Repair

If this option is enabled, the Scanner repairs the affected file.

Note

The option **Repair** can only be enabled if a repair of the detected file is possible.

Move to quarantine

If this option is enabled, the Scanner moves the file to quarantine. The file can be restored from the

Quarantine Manager if it is of informative value or - if necessary - sent to the Lavasoft Malware Research Center. Depending on the file, further selection options are available in the Quarantine Manager.

Delete

If this option is enabled, the file is deleted but can be restored if necessary with appropriate tools (e. g. Lavasoft UnErase). The virus pattern can still be detected again. This process is much quicker than *Overwrite and delete.*

Overwrite and delete (Wipe)

If this option is enabled, the Scanner overwrites the file with a default pattern and then deletes it. It cannot be restored.

Rename

If this option is enabled, the Scanner renames the file. Direct access to these files (e.g. by double-clicking) is therefore no longer possible. Files can later be repaired and given their original names.

Ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation. It may cause serious damage on your workstation.

Copy file to quarantine before action

If this option is enabled, the Scanner creates a back-up copy before carrying out the requested action. The back-up copy is saved in quarantine. It can be restored from the Quarantine Manager if it is of informative value or - if necessary - sent to the Lavasoft Malware Research Center. Depending on the file, further selection options are available in the Quarantine Manager.

Apply selection to all following detections

If this option is enabled, the Scanner uses the selected option for all malware detected during the scan.

Alert Message in the Case of a Blocked File

If the required action cannot be carried out by the Scanner in the event of a detection, the file is blocked (this could be the result of another application or of your operating system).

Name and Path of the Currently Detected Virus or Unwanted Program

The name and path of the currently detected virus or unwanted program is displayed in the middle window of the message.

Options

Delete blocked file after restart

When the option is enabled, the blocked file is immediately deleted during the boot process after a restart.

Ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation. It may cause serious damage on your workstation.

Apply selection to all following blocked files

When the option is enabled, the Scanner uses the selected option for all blocked files containing a virus or unwanted program.

Buttons and Links

Button / link	Description
Virus information	With this link - and with an active Internet connection - you can access an Internet page with further information on this virus or unwanted program.
	This page of the online help is opened via this button or link.

Guard

If the option **Interactive** is selected in the configuration of the Guard in the group **Action for concerning files**, you are asked what is to be done with a detected virus or unwanted program.

Name and Path of the Currently Detected Virus or Unwanted Program

The name and path of the currently detected virus or unwanted program is displayed in the middle window of the message.

Options

Note

In Interactive mode, if the detection is a heuristic hit (HEUR/), an unusual runtime compression tool (PCK/) or a file with a hidden file extension (HEUR-DBLEXT/), the only options available are **Move to quarantine, Ignore** and **Deny access**. In Automatic mode, the detection is automatically moved to quarantine. This restriction prevents the detected files, which may be a false alarm, from being directly removed (deleted) from your computer. The file can be recovered at any time with the aid of the Quarantine Manager.

Repair

If this option is enabled, the Guard repairs the affected file.

Note

The option **Repair** can only be enabled if a repair of the detected file is possible.

Move to quarantine

If this option is enabled, the Guard moves the file to quarantine. The file can be restored from the

Quarantine Manager if it is of informative value or - if necessary - sent to the Lavasoft Malware Research Center. Depending on the file, further selection options are available in the Quarantine Manager.

Delete

If this option is enabled, the file is deleted, but can be restored if necessary with relevant tools (e.g. Lavasoft UnErase). The virus pattern can still be detected again. This process is much quicker than *Overwrite and delete.*

Overwrite and delete (Wipe)

If this option is enabled, the Scanner overwrites the file with a default pattern and then deletes it. It cannot be restored.

Rename

If this option is enabled, the Guard renames the file. Direct access to these files (e.g., via double-clicking) is no longer possible. Files can later be repaired and given their original names.

Deny access

If this option is enabled, the Guard only enters the detection in the Report file if the Report function is enabled. In addition, the Guard writes an entry in the Event log when this option is enabled.

Ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation. It may cause serious damage on your workstation.

Buttons and Links

Button / link	Description
Virus information	With this link - and with an active Internet connection - you can access an Internet page with further information on this virus or unwanted program.
Help	This page of the online help is opened via this button or link.

MailGuard: Incoming emails

If the option **Interactive** is selected in the configuration of the MailGuard in the group **Action for concerning files**, you are asked what is to be done with a detected virus or unwanted program. You will receive the warning message, shown below, if a virus is detected in an incoming e-mail.

Sender of E-mail and Name of the Currently Detected Virus or Unwanted Program

The sender of the e-mail and the name of the currently detected virus or unwanted program is displayed in the middle window of the message.

Options

Note

In Interactive mode, if a detection is a heuristic hit (HEUR/), an unusual runtime compression tool (PCK/) or a file with a hidden file extension (HEUR-DBLEXT/), the only options available are **Move to quarantine** and **Ignore**. In Automatic mode, the detection is automatically moved to quarantine. This restriction prevents detected files, which could be false positives, from being directly removed (deleted) from your computer. The file can be recovered at any time with the aid of the Quarantine Manager.

Move to quarantine

If this option is enabled, the e-mail (including all attachments) is moved to quarantine. It can later be delivered via the Quarantine Manager. The affected e-mail is deleted. The body of the text and any attachments are replaced by default text.

Delete

If this option is enabled, the affected e-mail is deleted when a virus or unwanted program is

detected. The body of the text and any attachments are replaced by default text.

Delete attachment

If this option is enabled, the affected attachment is replaced by default text. If the body of the e-mail is affected, it is deleted and replaced by default text. The e-mail itself is delivered.

Move attachment to quarantine

If this option is enabled, the affected attachment is moved to quarantine and then deleted (replaced by default text). The body of the e-mail is delivered. The affected attachment can later be delivered via the Quarantine Manager.

Ignore

If this option is enabled, the affected e-mail is delivered despite detection of a virus or unwanted program.

Warning
Viruses and unwanted programs can penetrate your computer system in this way. Only select this option after careful consideration. Disable the preview in your mail client and never open any attachments by double-clicking.

Buttons and Links

Button / link	Description
Virus information	With this link - and with an active Internet connection - you can access an Internet page with further information on this virus or unwanted program.
	This page of the online help is opened via this button or link.

MailGuard: Outgoing emails

If the option **Interactive** is selected in the configuration of the MailGuard in the group **Action for concerning files**, you are asked what is to be done with a detected virus or unwanted program. The warning message, shown below, is displayed if a virus is detected in an outgoing e-mail.

Sender of E-mail and Name of the Currently Detected Virus or Unwanted Program

The e-mail sender and the name of the detected virus or unwanted program are displayed in the middle window of the message.

Options

Move mail to quarantine (do not send)

If this option is enabled, the e-mail (together with all attachments) is copied to Quarantine and is not sent. The e-mail remains in the outbox of your e-mail client. You will receive an error message in your e-mail program. All other e-mails sent from your e-mail account will be scanned for malware.

Block sending of mails (do not send)

The e-mail is not sent and remains in the outbox of your e-mail client. You will receive an error message in your e-mail program. All other e-mails sent from your e-mail account will be scanned for malware.

Ignore

If this option is enabled, the infected e-mail is sent despite detection of a virus or unwanted program.

Warning

Viruses and unwanted programs can penetrate the computer system of the e-mail recipient in this way.

Buttons and Links

Button / link	Description
Virus information	With this link - and with an active Internet connection - you can access an Internet page with further information on this virus or unwanted program.
Help	This page of the online help is opened via this button or link.

WebGuard

If the WebGuard configuration has the option **Interactive** selected under **Action for infected files**, when a virus or unwanted program is detected, you are prompted as to what should happen to the data transferred from the web server.

URL and Name of the Currently Detected Virus and/or Unwanted Program

The URL and name of the currently detected virus or unwanted program is displayed in the middle window of the message view.

Options

Note

In Interactive mode, if the detection is a heuristic hit (HEUR/), an unusual runtime compression tool (PCK/) or a file with a hidden file extension (HEUR-DBLEXT/), the only options available are **Move to quarantine** and **Ignore**. In Automatic mode, the detection is automatically moved to the quarantine folder. This restriction prevents the detected files, which may be a false alarm, from being directly removed (deleted) from your computer. The file can be recovered at any time with the aid of the Quarantine Manager.

Deny access

The website requested from the web server and/or any data or files transferred are not sent to your web browser. An error message to notify you that access has been denied is displayed in the web browser. WebGuard logs the detection to the report file if the report function is activated.

WebGuard also appends an entry to the event log if the relevant option is enabled.

Move to quarantine

In the event of a virus or malware detection, the website requested from the web server and/or the transferred data and files are moved into quarantine. The affected file can be be restored via the Quarantine Manager if it is of informative value or - if necessary - sent to the Lavasoft Malware Research Center.

Ignore

The website requested from the web server and/or the data and files that were transferred are forwarded on by WebGuard to your web browser.

Alert
This could allow viruses and unwanted programs to access your computer system. Only select this item after careful consideration.

Buttons and Links

Button / link	Description
Virus information	With this link - and with an active Internet connection - you can access an Internet page with further information on this virus or unwanted program.
	This page of the online help is opened via this button or link.

Archive

If the option **Interactive** is selected in the configuration of the Scanner in the group **Action for concerning files**, you are asked what is to be done with a detected virus or unwanted program.

Note
Affected files in an archive are not repaired or deleted!

Name and Path of the Currently Detected Virus or Unwanted Program

The name and path of the archive in which the virus or unwanted program was detected is displayed in the middle window of the message.

Buttons and Links

Button / link	Description
Virus information	With this link - and with an active Internet connection - you can access an Internet page with further information on this virus or unwanted program.
Help	This page of the online help is opened via this button or link.

Boot Sector Virus

If the option **Interactive** is selected in the configuration of the Scanner and the Guard in the group **Action for concerning files**, you are asked what is to be done with a detected virus or unwanted program.

Note
Boot sector viruses are only detected by the Guard. If possible, you can repair the detected boot sector virus with the aid of the Scanner. Alternately, the boot sector virus can be deleted or ignored.

Name and Path of the Currently Detected Virus or Unwanted Program

The name and path of the currently detected virus or unwanted program are displayed in the lower window of the message.

Name and Path of the Currently Detected Virus or Unwanted Program

The name and path of the currently detected virus or unwanted program are displayed in the middle window of the message.

Options

Repair

If this option is enabled, the boot sector virus is repaired.

Delete

If this option is enabled, the boot sector is deleted.

Ignore

If this option is enabled, the boot sector is ignored.

Buttons and Links

Button / link	Description
Virus information	With this link - and with an active Internet connection - you can access an Internet page with further information on this virus or unwanted program.
Help	This page of the online help is opened via this button or link.

Detection in Mailbox

If the option **Interactive** is selected in the configuration of the Scanner and the Guard in the group **Action for concerning files**, you are asked what is to be done with a detected virus or unwanted program.

Note
Affected files in a mailbox are not repaired or deleted!

Information Displayed

The name and path of the mailbox in which the virus or the unwanted program was detected are displayed in the window. In addition, you will receive a message that access to this file is allowed.

Buttons and Links

Button / link	Description
Virus information	With this link - and with an active Internet connection - you can access an Internet page with further information on this virus or unwanted program.
	This page of the online help is opened via this button or link.

Blocked File

If the required action cannot be carried out by the Scanner in the event of a detection, the file is blocked (this may be due to another application or your operating system.)

Name and Path of the Currently Detected Virus or Unwanted Program

The name and path of the detected virus or unwanted program is displayed in the middle window of the message, together with information that access to the file has been blocked.

Options

Delete blocked file after restart

When the option is enabled, the blocked file is immediately deleted during the boot process after a restart.

Ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation. It may cause serious damage to your workstation.

Use selection for all following blocked files

When the option is enabled, the Scanner uses the selected option for all blocked files containing a virus or unwanted program.

Buttons and Links

Button / link	Description
Virus information	With this link - and with an active Internet connection - you can access an Internet page with further information on this virus or unwanted program.
	This page of the online help is opened via this button or link.

Detection of a Rootkit

If the option **Interactive** is selected in the configuration of the Scanner in the group **Action for concerning files**, in the event of detection of a rootkit, you are asked what is to be done.

The Scanner scans for hidden processes, files and registry entries. In addition, a scan is made for hidden malware. The alert message depends on the type of detection of a hidden object and on what further action is selected.

Name and Path of the Currently Detected Malware

The name and path of the currently detected hidden malware is displayed in the middle window of the message.

Options

Copy to quarantine

When the option is enabled, the detection is copied to quarantine.

Move to quarantine

When the option is enabled, the detection is moved to quarantine. You are also informed that a restart of your operating system is necessary to complete the repair process.

Delete

When the option is enabled, the detection is moved to quarantine. You are also informed that a restart of your operating system is necessary to complete the repair process.

Ignore

When the option is enabled, the detection is left as it is.

Name and Path of the Currently Detected Hidden Object

The name and path of the currently detected hidden object are displayed in the middle window of the message.

Options

Ignore

When the option is enabled, the detection is left as it is.

Warning
The hidden object remains active on your computer. It may cause serious damage to your workstation!

Buttons and Links

Button / link	Description
Virus information	With this link - and with an active Internet connection - you can access an Internet page with further information on this virus or unwanted program.
Help	This page of the online help is opened via this button or link.

Scanner

With Lavasoft Anti-Virus Helix, you can carry out manual scans (on-demand scans) for viruses and unwanted programs in several ways.

- **On-demand scan via context menu**
  The on-demand-scan via the context menu (right-hand mouse button - entry **Scan selected files with Anti-Virus**) is recommended if, for example, you wish to scan individual files and directories. Another advantage is that it is not necessary to first start the Lavasoft Anti-Virus Helix Control Center for an on-demand scan via the context menu.
- **On-demand scan via drag & drop**
  When a file or directory is dragged into the program window of the Lavasoft Anti-Virus Helix Control Center, the Scanner scans the file or directory and all sub-directories it contains. This procedure is recommended if you wish to scan individual files and directories that you have saved, for example, on your desktop.
- **On-demand scan via profiles**
  This procedure is recommended if you wish to regularly scan certain directories and drives (e.g. your work directory or drives on which you regularly store new files). You do not need to select these directories and drives again for every new scan; simply select using the relevant profile.

On-demand scan via the Scheduler
The Scheduler enables you to carry out time-controlled scans.

Virus Scan Helix

During an on-demand scan, the status window **Virus Scan Helix** appears, providing you with exact information on the status of the scan.

If the option **Interactive** is selected in the configuration of the Scanner in the group **Action for concerning files**, you are asked what is to be done with a detected virus or unwanted program. If the option **Automatic** is selected, any detections are shown in the Scanner report.

Displayed Information

Status

The following are the various status messages:

- The file is being scanned
- Initialize archive
- Memory released
- File is being unpacked
- Boot sectors are being scanned
- Master boot sectors are being scanned
- The registry is being scanned
- The program will be ended!
- Scan completed

Last object

Name and path of the file that is being scanned or was last scanned.

Last detection

The following are the various messages for the last detection:

- No detection
- Name of the last detected virus or unwanted program

Scanned files

Number of scanned files.

Scanned directories

Number of scanned directories.

Scanned archives

Number of scanned archives.

Time elapsed

Duration of the on-demand scan.

Scanned

Percentage of scan already completed.

Detections

Number of detected viruses and unwanted programs.

Repaired

Number of repaired viruses and unwanted programs.

Deleted

Number of deleted viruses and unwanted programs

Moved

Number of files and unwanted programs placed in quarantine.

Warnings

Number of messages about errors that occurred during the scan.

Buttons and Links

Button / link	Description
Virus information	With this link - and with an active Internet connection - you can access an Internet page with further information on this virus or unwanted program.

	This page of the online help is opened via this button or link.
Stop	The scan process is stopped.
Pause	The scan will be interrupted and can be continued by clicking on the button **Resume**.
Resume	The interrupted scan will be continued.
End	The Scanner is closed.
Report	The report file of the scan will be shown.

Control Center

The Lavasoft Anti-Virus Helix Control Center is an information, configuration and management center. In addition to the sections that can be selected individually, it offers a large number of options that can be accessed from the menu bar.

Menu Bar

All functions of the Lavasoft Anti-Virus Helix Control Center are contained in the menu bar.

File

- **Exit**

View

- **Overview**
  - Status
  - Events
  - Reports
- **Local protection**
  - Scanner
  - Guard
- **Online protection**
  - MailGuard
  - WebGuard
- **Administration**
  - Quarantine
  - Scheduler
- **Update**

Extras

- Boot records scan
- Detection list.
- Configuration

Update

- Start update
- Manual update
- Start product update

Help

- Readme
- Contents
- Support
- Load license file
- About Anti-Virus Helix

Note
You can activate the keyboard navigation in the menu bar with the help of the [ALT] key. If the navigation is activated, you can move within the menu with the arrow keys. Activate the active menu item with the Return key.

Sections

The sections offer you the following options:

- In **Overview** you will find all sections with which you can monitor the functions of Lavasoft Anti-Virus Helix.
- The **Status** section lets you see, at a glance, which Lavasoft Anti-Virus Helix modules are active and provides information on the last update carried out. You can also see whether you own a valid license.
- The **Events** section enables you to view events generated by certain Lavasoft Anti-Virus Helix modules.
- The **Reports** section enables you to view the results of actions executed by Lavasoft Anti-Virus Helix.
- In **Local protection,** you will find the components for checking the files on your computer system for viruses and malware.
- The **Scanner** section enables you to easily configure and start an on-demand scan. Predefined profiles enable you to run a scan with preset default options. In the same way, it is possible to adapt the scan for viruses and unwanted programs to fit your personal requirements. This can be done with the help of manual selection (not saved) or by creating Custom profiles.
- The **Guard** section displays information on scanned files, as well as other statistical data, which can be reset at any time, and enables access to the report file. More detailed information on the last virus or unwanted program detected can be obtained simply at the push of a button.
- In **Online protection** you will find the components to protect your computer system against viruses and malware from the Internet, and against unauthorized network access.
- The **MailGuard** section shows you the e-mails scanned by MailGuard, their properties and other statistical data.
- The **WebGuard** section shows you information on scanned URLs and detected viruses, as well as other statistical data, which can be reset at any time and enables access to the report file. More detailed information on the last virus or unwanted program detected can be obtained simply at the push of a button.
- In **Administration,** you will find tools for isolating and managing suspicious or infected files, and for planning recurring tasks.
- The **Quarantine** section contains the Quarantine manager. This is the central point for files already placed in quarantine or for suspect files which you would like to place in quarantine.
- The **Scheduler** section enables you to configure scheduled scanning and update jobs and to adapt or delete existing jobs.

Buttons and Links

The following buttons and links are available in each section.

Button / link	Shortcut	Description
		This button or link is used to access the corresponding configuration dialog for the section.
	F1	This button or link opens the corresponding online help topic for the section.

File

Exit

The menu item **Exit** in the **File** menu closes the Lavasoft Anti-Virus Helix Control Center.

View

Status

The **Status** section enables you to see, at a glance, whether your computer system is protected and which Lavasoft Anti-Virus Helix modules are active. The **Status** section also provides information about the last update carried out. You can see if you own a valid license, as well.

- Anti-Virus Guard
- Online Protection: Anti-Virus MailGuard, Anti-Virus WebGuard
- Last full system scan
- Last update

Anti-Virus Guard

Information on the current status of Anti-Virus Guard is displayed in this box.

The following options are available:

Icon	Status	Option	Description
	Activated	Deactivate	The Guard service is active, i.e. your system is continually monitored for viruses and unwanted programs. **Note** You can deactivate the Guard service. However, please note that you are no longer protected from viruses and unwanted programs when the Guard is deactivated. All files can pass through the system unnoticed and possibly cause damage.
	Deactivated	Activate	The Guard service is deactivated, i.e. the service is loaded but is not active. **Warning** No scan is carried out for viruses and unwanted programs. All files can pass through the system unnoticed. You are not protected against viruses and unwanted programs. **Note** In order to be protected against viruses and unwanted programs, please click the link **Activate** in the section **Anti-Virus Guard**.
	Service stopped	Start service	The Guard service is stopped. **Warning** No scan is carried out for viruses and unwanted programs. All files can pass through the system unnoticed. You are not protected against viruses and unwanted programs. **Note** In order to be protected against viruses and unwanted programs, please click the link **Start**. The current status should now display **Activated** .

Unknown	Help	This status is displayed when an unknown error occurs. In this case, please contact our Support Center.

Online Protection

Information on the current status of the Anti-Virus services protecting your computer against viruses and malware are displayed in this panel.

Click the + sign to obtain further information on the processes:

- The Anti-Virus MailGuard service checks e-mail and their attachments for viruses and malware.
- The Anti-Virus WebGuard service checks the data that is transmitted and loaded into your Web browser while you are surfing the Internet (monitoring of ports 80, 8080, 3128).

The following options are available:

Icon	Status	Status Process	Option	Description
	OK	Activated	Deactivate	All services for online protection are active. **Note** You can deactivate a service by clicking the link **Deactivate**. **Note** You are no longer fully protected against viruses and malware once a service has been deactivated.
	Limited	Deactivated	Activate	A service is deactivated, i.e. the service has been started but is not active. **Warning** Your computer system is not being fully monitored. There is a possibility that viruses and unwanted programs can access your computer system. **Note** To activate the service, click the link **Activate.**
	Warning	Service stopped	Start service	A service has been stopped or all services for online protection are deactivated. **Warning** Your computer system is not being fully monitored. There is a possibility that viruses and unwanted programs can access your computer system. **Note** Click on the Start link to start the service so that your computer system is monitored. The service is started and activated.
		Unknown	Help	This status is displayed when an unknown error occurs. In this event please contact our Support Center.

Last complete system check

Information on the current status of the last system scan carried out is displayed in this panel. A complete system check means a full check of all local hard drives on your computer.

The following details are displayed:

- Date of last complete system check

The following possibilities are available:

Icon	Status	Option	Explanation
	Date of last update, e.g. 18/07/2007	Check system now	The last complete system check was executed within the last 7 days. **Note** You can execute a complete system check by clicking on the **Check system now** link.
	Date of last update, e.g. 10/07/2007	Check system now	The last complete system check was performed sometime between a week and a month ago. **Warning** The status of the system is insecure. There is a possibility that viruses or unwanted programs have been saved on your computer since the last system check. **Note** To check your computer, please click on the **Check system now** link.
	Not performed	Check system now	No complete system check has been executed since installation. **Warning** The status of the system is unchecked. There is the possibility that viruses or unwanted programs are to be found on your computer. **Note** To check your computer, please click on the link **Check system now**.
	Date of last update, e.g. 10/06/2007	Check system now	The last complete system check was more than a month ago. **Warning** The status of the system is insecure. There is a possibility that viruses or unwanted programs have accessed your computer since the last system check. **Note** To check your computer, please click on the link **Check system now**.

Unknown	Help	This status is displayed when an unknown error occurs. In this case, please contact our Support Center.

Last update

Information on the current status of the last update carried out is displayed in this box.

The following details are displayed:

- Date of the last update

Click on the + icon for more information:

- Version of the installed virus definition file and date created
- Version of the installed search engine and date created

The following options are available:

Icon	Status	Option	Description
	Date of last update, e.g. 18.07.2005	Start update	Your Lavasoft Anti-Virus Helix version has been updated during the last 24 hours. **Note** You can update Lavasoft Anti-Virus Helix to the latest version via the link **Start update**.
	Date of last update, e.g. 15.07.2005	Start update	Since updating, 24 hours have already passed but you are still within the update-reminder-cycle that you chose. This depends on the setting in the configuration. **Note** You can update Lavasoft Anti-Virus Helix to the latest version via the link **Start update**.
	Not executed	Start update	Since installation, no update has been carried out or the update reminder cycle you chose has been exceeded (see Configuration(, meaning no update has been carried out or the virus definition file is older than three days. You can update your Lavasoft Anti-Virus Helix to the latest version via the link **Start update**.
		Not available	No updates are possible when the license has expired.

Product activate until

Information on the current status of your Lavasoft Anti-Virus Helix license is displayed in this box.

Click on the + icon for more information.

The following options are available:

Icon	Status	Option	Meaning
Full Version			
	Validity date of the current license for a full version, e.g. December 31, 2008.	Update	You possess a valid license for Lavasoft Anti-Virus Helix. Use the link **Update** to access the Online Shop of Lavasoft Anti-Virus Helix. There you have the opportunity to adapt your current license to your needs.
	Validity date of the current license for a full version, e.g. December 31, 2008	Update	You possess a valid license for Lavasoft Anti-Virus Helix. The licensing period, however, is thirty days or less. Use the link **Update** to access the Online Shop of Lavasoft Anti-Virus Helix. There you have the option to extend the current license.
	License expired on: e.g. December 31, 2008	Purchase	Your license for Lavasoft Anti-Virus Helix has expired. Use the link **Purchase** to access the Online Shop of Lavasoft Anti-Virus Helix. There you have the option to purchase a valid license. **Warning** If your license has expired, updates are no longer possible. The protective functions of Lavasoft Anti-Virus Helix have been deactivated and can no longer be activated.
Evaluation license			
	Validity date of the evaluation license, e.g. December 31, 2008	Purchase	You have an evaluation license and thus have the option of testing the full range of functions of Lavasoft Anti-Virus Helix for a certain period of time. Use the link **Purchase** to access the Online Shop of Lavasoft Anti-Virus Helix. There you have the option to purchase a valid license.
	Validity date of the evaluation license, e.g. December 31, 2008	Update	You have an evaluation license. The licensing period is thirty or

			less days. Use the link **Update** to access the Online Shop of Lavasoft Anti-Virus Helix. There you have the option to purchase a valid license.
	The evaluation license has expired on: December 12, 2008	Purchase	Your license for Lavasoft Anti-Virus Helix has expired. Use the link **Purchase** to access the Online Shop of Lavasoft Anti-Virus Helix. There you have the option to purchase a valid license. **Warning** If your license has expired, updates are no longer possible. The protective functions of Lavasoft Anti-Virus Helix are deactivated and can no longer be activated.
Demo version			
	Demo version with limited functions	Purchase	You are using a demo version with restricted functions. Updates are not possible. Use the link **Purchase** to access the Online Shop of Lavasoft Anti-Virus Helix. There you have the option to purchase a valid license.

Scanner

The section **Scanner** enables you to easily configure and start an on-demand scan. Predefined profiles enable a scan with already adapted default options. In the same way, it is possible to adapt the scan for viruses and unwanted programs to fit your personal requirements with the help of manual selection or by creating Custom profiles. The required action can be selected either via the icon in the toolbar, via shortcut or via the context menu. Start a scan via the item **Start scan** with a selected profile.

The display and handling of the editable profiles corresponds to that of Windows Explorer. Every folder in the main directory corresponds to one profile. Folders or files to be scanned are selected or can be selected with a check mark in front of the folder or file to be scanned.

- To change directories, double-click on the required directory.
- To change drives, double-click on the required letter of the drive.
- To select folders and drives, you can click on the box in front of the folder or drive icon or select via the context menu.
- You can navigate through the menu structure with the aid of the scroll bar.

Predefined profiles

Lavasoft Anti-Virus Helix offers pre-defined profiles for a scan.
Note
These profiles are read only and cannot be altered or deleted. To adapt a profile to your requirements, select a one-time scan in the folder **Manual selection** or select **Create new profile** to create a Custom profile (which can be saved.)
Note
For predefined profiles, the scanning options of the Files group of the Lavasoft Anti-Virus Helix Configuration are used. You can adapt this setting to your requirements in the Lavasoft Anti-Virus Helix Configuration. Access Lavasoft Anti-Virus Helix Configuration via the Configuration button or link in this section.

Local Drives

All local drives on your system are scanned for viruses or unwanted programs.

Local Hard Disks

All local hard disks on your system are scanned for viruses or unwanted programs.

Removable Drives

All available portable drives on your system are scanned for viruses or unwanted programs.

Windows System Directory

The Windows system directory on your system is scanned for viruses or unwanted programs.

My Documents

The folder "My Documents" on your system is scanned for viruses or unwanted programs.

Active Processes

All current processes are scanned for viruses or unwanted programs.

Scan for Rootkits

The computer is scanned for active rootkits.
Note
In **Interactive** mode, you have several ways of reacting to a detection. In **Automatic mode**, the detection is recorded in the report file.
Note
The rootkit scan is not yet available in 64-bit systems,

Manual selection

Select this folder if you want to adapt the scan to meet your individual requirements. Mark the required directories and files to be scanned.
Note
The profile **Manual selection** is used to scan data without first creating a new profile.

Custom profiles

A new profile can be created via the toolbar, via shortcut or via the context menu.

New profiles can be saved under the name you require and, in addition to the manually controlled scan, are useful for creating time-based scans with the aid of the Scheduler.

Toolbar and Shortcuts

Icon	Shortcut	Description
	F3	Start scan with the selected profile The selected profile is scanned for viruses or unwanted programs.
	F6	Start scan with the selected profile as administrator (This function is only available with Windows Vista. Administrator rights are required to carry out this action.) The selected profile is scanned for viruses or unwanted programs.
	Ins	Create new profile A new profile is created.
	F2	Rename selected profile Gives the selected profile the name you chose.
	F4	Create desktop link for the selected profile Creates a link to the selected profile on the desktop.
	Del	Delete selected profile The selected profile is irretrievably deleted.

Context menu

The context menu for this section can be obtained by selecting a required profile with the mouse and keeping the right-hand mouse button selected.

Start Scan

The selected profile is scanned for viruses or unwanted programs.

Start scan (administrator)

(This function is only available with Windows Vista. Administrator rights are required to carry out this action.)

The selected profile is scanned for viruses or unwanted programs.

Create New Profile

A new profile is created. Select the directories and files that Lavasoft Anti-Virus Helix should scan for you.

Rename Profile

Gives the selected profile the name you chose.

Note

This entry cannot be selected in the context menu if a predefined profile is selected.

Delete Profile

The selected profile is irretrievably deleted.

Note

This entry cannot be selected in the context menu if a predefined profile is selected.

File Filter

- **Standard:** The files are scanned according to the setting in the group Files of Lavasoft Anti-Virus Helix Configuration. This setting can be adapted to your requirements in the Lavasoft Anti-Virus Helix Configuration. Access Lavasoft Anti-Virus Helix Configuration via the button or the link **Configuration**.
- **Scan all files:** All files are scanned irrespective of the setting in the configuration.
- **Custom:** A dialogue window is opened in which all file extensions that are scanned are displayed. Default entries are defined for the extensions. However, entries can be added or deleted.

Note

This entry is only available when the mouse hovers over a checkbox alternative. It is not possible to select the option with pre-defined profiles.

Select

- **With sub-directories:** Everything is scanned in the selected node (black check mark).
- **Without sub-directories:** Only the files are scanned in the selected node (green check mark).
- **Only sub-directories:** Only the sub-directories are scanned in the selected node, not the files which are in the node (gray check mark; sub-directories have a black check mark).
- **No selection:** Selection is cancelled. The currently selected node is not scanned (no check mark).

Note

This entry can only be selected in the context menu when the mouse is over a check box. The option is not available with predefined profiles.

Create Desktop Link

Creates a link to the selected profile on the desktop.

Note

This entry cannot be selected in the context menu if the profile **Manual selection** is selected, as the settings of the Manual selection are not permanently saved.

Guard

The **Guard** section shows information on scanned files, as well as other statistical data, which can be reset at any time, and enables access to the report file. More detailed information on the last virus or unwanted program detected can be obtained simply at the push of a button.

Note

If the Guard service is not started, the boxes of this section are grayed out and cannot be selected. However, the report file of the Guard can be displayed.

Toolbar

Icon	Description
	Display report file The report file of the Guard is displayed.
	Reset statistics data The statistical information in this section is set to zero.

Displayed information

Last File Found

Shows the name and location of the file last found by the Guard.

Last Detection

Shows the name of the last virus or unwanted program found.

Icon / link	Description
	Click on the icon or the link when connected to the Internet to display more detailed information on the virus or unwanted program.

Last File Scanned

Shows the name and path of the file last scanned by the Guard.

Statistics

Number of Files

Shows the number of files scanned so far.

Number of Messages

Shows the number of viruses and unwanted programs found so far.

Number of Deleted Files

Shows the number of files deleted so far.

Number of Repaired Files

Shows the number of files repaired so far.

Number of Moved Files

Shows the number of files moved so far.

Number of Renamed Files

Shows the number of files renamed so far.

MailGuard

The **MailGuard** section shows you all the e-mails scanned by MailGuard, their properties and other statistical data.

Note
If the MailGuard service or the Anti-Virus Helix MailGuard helper service is not started, the boxes in this section are grayed out and cannot be selected. However, the report file of the MailGuard can be displayed.

Note
Exemption of individual e-mail addresses from the malware scan only applies to incoming e-mail. To disable the scanning of outgoing e-mail, deactivate the scan in the configuration under **MailGuard ::Scan**.

Toolbar

Icon	Description
	Display report file The report file of the MailGuard is displayed.
	Display properties of the selected e-mail Opens a dialog window with more information on the selected e-mail.
	Do not scan e-mail address for malware The selected e-mail address will no longer be scanned for viruses and unwanted programs in the future. You can undo this setting in the configuration under **MailGuard:: General :: Exceptions**.
	Delete selected e-mail The selected e-mail is deleted from the Lavasoft Anti-Virus Helix cache. However, the e-mail remains in your e-mail program.
	Reset statistics data The statistical information in this section is set to zero.

Scanned e-mails

This area shows the e-mail scanned by MailGuard.

Icon	Description
	No virus or unwanted program was found.
	A virus or unwanted program was found.

From

Displays the sender address of the e-mail, and shows if the e-mail was received or sent.

Subject

Displays the subject of the e-mail received.

Date/Time

Shows when the e-mail was scanned for spam.

Note
You can obtain further information about an e-mail by double-clicking on the relevant e-mail.

Statistics

E-mail Action

Shows the action carried out when the MailGuard finds a virus or an unwanted program in an e-mail. In Interactive mode, no display is available, as you can select which procedure is to be followed in the event of detection.

Note
You can adapt this setting to your requirements in the Lavasoft Anti-Virus Helix Configuration. The Lavasoft Anti-Virus Helix Configuration is accessed via the button or the link **Configuration**.

Affected Attachments

Shows the action carried out when the MailGuard finds a virus or an unwanted program in an affected attachment. In Interactive mode, no display is available, as you can select which procedure is to be followed in the event of detection.

Note
You can adapt this setting to your requirements in the Lavasoft Anti-Virus Helix Configuration. The Lavasoft Anti-Virus Helix Configuration is accessed via the button or the link **Configuration**.

Number of E-mail

Shows the number of e-mail scanned by MailGuard.

Last Message

Gives the name of the last virus or unwanted program found.

Number of Messages

Displays the number of viruses and unwanted programs previously detected and reported.

Suspicious E-mail

Displays the number of e-mail received containing malware.

Number of E-mail Received

Displays the number of e-mail received.

Number of E-mail Sent

Displays the number of e-mail sent.

WebGuard

The **WebGuard** section shows information on scanned URLs, as well as other statistical data, which can be reset at any time, and enables access to the report file. Detailed information about the last detected virus or unwanted program is available simply at the press of a button.

Toolbar

Icon	Description
	Display report file The report file of the WebGuard is displayed.
	Reset statistics data The statistical information in this section is set to zero.

Displayed information

Last Detected URL

Displays the last URL detected by WebGuard.

Last Detected Virus or Unwanted Program

Gives the name of the last virus or unwanted program found.

Icon/link	Description
	Click on the icon or link to display detailed information about the virus or unwanted program if an Internet connection is present.

Last Scanned URL

Shows the name and path of the last URL checked by WebGuard.

Statistics

Number of URLs

Number of URLs checked so far.

Number of Messages

Shows the number of viruses and unwanted programs found so far.

Number of Blocked URLs

Number of previously blocked URLs.

Number of Ignored URLs

Displays the number of previously ignored URLs.

Quarantine

The **quarantine manager** manages affected objects (files and e-mails). Lavasoft Anti-Virus Helix can move affected objects to the quarantine directory in a special format. It can then no longer be executed or opened.

Note

To quarantine a detected object automatically, select the relevant option for quarantine in the **Lavasoft Anti-Virus Helix Configuration** under Scanner and Guard and MailGuard - **Scan :: Action on detection :: Action on detection** if you are working in **Automatic mode**. Alternatively you can select the relevant option for quarantine in **Interactive mode**.

Toolbar, shortcuts and context menu

Icon	Shortcut	Description
	F2	Rescan object A selected object is scanned again for viruses and unwanted programs. The settings of the on-demand scan are used for this.
	Enter	Properties Opens a dialog window with more information on the selected object.
	F3	Restore object A selected object is restored. This object is then in its original location. **Note** This option is not available for e-mail objects.
 (Windows Vista)		**Warning** Extensive system damage can occur due to viruses and unwanted programs! If you restore files, ensure that only files are restored which were able to be cleaned by another scan. **Note** With Windows Vista, restoration of objects is only possible with administrator rights.
	F6	Restore object to... A selected object can be restored at a location you select. If you select this option, a "Save as" dialog box opens in which you can select where to save the object. **Warning** Extensive system damage can occur due to viruses and unwanted programs!

If you restore files: ensure that only files are restored which were able to be cleaned by another scan.

Ins

Add file

If you regard a file as suspicious, you can add it to the quarantine manager manually with this option.

Del

Delete object

A selected object is deleted from the quarantine manager. The object cannot be restored.

Table

Status

An object placed in quarantine may have the following various statuses:

Icon	Description
	No virus or unwanted program was found; the object is "clean".
	A virus or unwanted program was found.
	If the suspect file was added to the quarantine manager with the option **Add file**, it has this warning icon.

Object Type

Designation	Description
E-mail	The object detected is an e-mail.
File	The object detected is a file.

Restored

See option **Restore object**.

Sent

See option **Send file**.

Detection

Shows the name of the virus or unwanted program detected.

Date/Time

Displays the date and time of the detection.

Engine
Shows the version number of the Lavasoft Anti-Virus Helix search engine.

VDF
Shows the version number of the virus definition file.

Source
Shows the detection location of the virus or unwanted program.

Scheduler

The **Scheduler** gives you the option of creating scheduled scanning and update jobs, and adapting or deleting existing jobs.

You can set Lavasoft Anti-Virus Helix to search for new virus definition files on the Internet server (for example, every 6 hours) and - where appropriate - load and install them. By doing so, you can always keep Lavasoft Anti-Virus Helix up to date without manual effort. You can also set Lavasoft Anti-Virus Helix to scan your computer for viruses and unwanted programs at scheduled times (for example, daily at 22:00.)

Toolbar, shortcuts and context menu

Icon	Shortcut	Description
	Ins	Insert new job Creates a new job. An assistant easily guides you through the necessary settings.
	Enter	Properties Opens a dialog window with more information on the selected job.
	F2	Edit job Opens the assistant to create and alter a job.
	Del	Delete job Deletes the selected jobs from the list.
		Display report file The report file of the Scheduler is displayed.
	F3	Start job Start a marked job from the list.
	F4	Stop job Stops a started and marked job.

Table

Status

Icon	Description
	The job is an update job.
	The job is a scan job.

Name

Name of the job.

Action

Indicates whether the job is a **scan** or an **update** of Lavasoft Anti-Virus Helix.

Frequency

Indicates how often and when the job is started.

Display Mode

The following display modes are available:

- **Invisible:** The job is carried out in the background and is not visible. This applies to scanning jobs and update jobs.
- **Minimize:** The job window only displays a progress bar.
- **Maximize:** The job window is completely visible.

Enable

The job is enabled by checking the box.

Note

If the frequency of the job is set to **Immediately**, the job is started immediately after checking the box. This allows you to restart the job at any time, on demand, by checking the box.

Create jobs with the Scheduler

The Anti-Virus Helix assistant supports you in planning, configuring and creating:

- a timed scan for viruses and unwanted programs
- a timed update of Lavasoft Anti-Virus Helix via the Internet

For both types of jobs you must enter:

- the name and the description of the job
- when the job should be started
- how often the job should be carried out
- the display mode of the job

Frequency of the Job

Immediately	Job is started immediately after ending the Anti-Virus Helix assistant.
Daily	Job is started daily at a certain time, e.g. 22:00.
Weekly	Job is started weekly on a certain day at a certain time, e.g. Tuesday, 16:26.
Interval	Job is carried out at certain intervals, e.g. every 24 hours (minimum scan job: 15 minutes; minimum update job: 15 minutes).
Once	Job is carried out once at a defined time, e.g. on 10.04.04 at 10:04.
Login	Job is carried out at each login of a Windows user.

Start Time of the Job

You can define the weekday, date, time or interval when Lavasoft Anti-Virus Helix should start the job. This is not displayed if you have entered Immediately as the start time.

Depending on the job type, there are the following additional options:

- **Also start job when connecting to Internet (dial-up)**
  In addition to the defined frequency, the job is carried out when an Internet connection is set up.
  This option can be selected with an update job that is to be carried out daily, weekly or at other intervals.
- **Repeat job if the time has already expired**
  Past jobs are carried out that could not be carried out at the required time (for example: because the computer was switched off.) This option can be selected both with an update job and with a scan job that is to be carried out daily, weekly, at intervals or once.

Note
With a scan job, it is possible to select both pre-defined profiles and Custom profiles in the dialog window **Selection of the profile**. The profile **Manual selection** is always carried out with the current selection.on.

Reports

The **Reports** section enables you to view the results of actions executed by Lavasoft Anti-Virus Helix.

Toolbar, shortcuts and context menu

Icon	Shortcut	Description
	Enter	Display report Opens a window in which the result of the selected action is displayed. (For example: the result of a scan.)
	F3	Display report file Displays the report file of the selected report.

F4

Print report file

Opens the Windows print dialog to print the report file.

Del

Delete report(s)

Deletes the selected report and the relevant report file.

Table

Status

Icon	Description
	The action was successfully carried out.
	The action should be checked.
	The update was not successfully carried out.

Action
Shows the action carried out.

Result
Shows the result of the action.

Date/Time
Shows the date and time when the report was created.

Contents of a report for a scan

Scanned Archives
Number of scanned archives.

Deleted
Total number of deleted files.

Scanned Files
Total number of scanned files.

Quarantine
Total number of files placed in quarantine.

Information

Number of information items issued (for example: further information that may arise during a scan.)

Scanned Directories
Total number of directories scanned.

Renamed
Total number of renamed files.

Repaired
Total number of repaired files.

Detections
Total number of viruses and unwanted programs detected.

Warnings
Number of warnings issued (for example: problems that may arise during a scan.)

Overwrite
Total number of overwritten files

Hidden objects
Total number of active rootkits detected

Date of the Scan
Date of the scan.

Start time of the Scan
Start time of the scan

Scanning Time Required
Displays the time in mm:ss format.

Last Detection
Name of the virus or unwanted program last detected.

Scan Status
Shows whether the scan job was completely carried out or aborted.

Events

The **Events** enables you to view the events generated by Lavasoft Anti-Virus Helix modules.

Toolbar, shortcuts and context menu

Icon	Shortcut	Description
	Return	Display selected event Opens a window in which the result of the selected action is

displayed. (For example: the result of a scan.)

 F3

Export selected event(s)

Export a selected event.

 Del

Delete selected event(s)

Deletes the selected event.

Modules

The events of the following modules can be displayed by the event viewer:

Icon	Description
	Scheduler
	Anti-Virus Updater
	Guard
	MailGuard
	Scanner

By checking the box **All**  you can display the events of all available modules. To display only the events of a certain module, check the box next to the required module.

Filter

The following event classification can be displayed by the event viewer.

Icon	Description
	Information
	Alert
	Error
	Detection

By checking the box **Filter**  you can display all events. To display only certain events, check the box next to the required event.

Table

The event list contains the following information:

Icon

The icon of the event classification.

Type

A classification of the event severity: Information, Alert, Error, Detection.

Module

The module that has logged the event. (For example: the Guard which has made a detection.)

Action

Event description of the respective module.

Date/Time

The date and the local time the event occurred.

Refresh

Updates the view of the opened section.

Extras

Boot Records Scan

You can also scan the boot sectors of the drives of your workstation with an on-demand scan. This is recommended, for example, when Lavasoft Anti-Virus Helix finds a virus when scanning individual files or directories with an on-demand scan and you want to make sure that the boot sectors are not affected.

It is possible to select more than one boot sector by keeping the Shift key pressed and selecting the required drives with the mouse.

Note
You can have the boot sectors automatically scanned with an on-demand scan (see Lavasoft Anti-Virus Helix Configuration :: Scanner :: Scan :: Scan boot sectors of selected drives).

Note
Scanning of the boot sectors with Windows Vista is only possible with administrator rights.

Detection List

With this function, the names of the viruses and unwanted programs that Lavasoft Anti-Virus Helix knows are listed. A convenient search function for the names is integrated.

Search for:

Enter a search word or character sequence in this box.

- **Search for character sequence within a name**
  You can enter a consecutive sequence of letters or characters on the keyboard and the marker moves to the first point in the list of names which includes this sequence. This also applies to the middle of a name (example: "raxa" finds "Abraxas").
- **Search from the first character of a name**
  You can enter the initial letter and the following characters on the keyboard and the marker scrolls alphabetically in the list of names (example: "Ra" finds "Rabbit").

If the name or sequence of characters searched for is available, the position found is marked in the list.

Search Forwards

Starts the search forward in alphabetical order.

Search Backwards

Starts the search backward in alphabetical order.

First Match

Moves in the list to the first entry found.

Entries of the Detection List

Under this title, there is a list with names of viruses or unwanted programs that Lavasoft Anti-Virus Helix can recognize. Most entries in this list can also be removed with Lavasoft Anti-Virus Helix. They are listed in alphabetical order (first special characters and numbers, then the letters). Use the scroll bar to scroll up or down in the list.

Configuration

The menu item **Configuration** in the **Extras** menu opens the Lavasoft Anti-Virus Helix Configuration.

Update

Start Update

The menu item **Start update...** in the **Update** menu starts an immediate update. The virus definition file and search engine have been updated. A product update can only take place if you have activated the option **Download and automatically install product updates** in the configuration under General :: Update

---

.

Product Updates

The menu item **Start product update** in the **Update** menu starts a product update. Updating the program files updates the virus definition file and the search engine.

Help

Readme

The menu item **Readme** in the **Help** menu opens the file readme.txt. This file contains important information on every new version of Lavasoft Anti-Virus Helix.

Contents

The menu item **Contents** in the **Help** menu opens the list of contents of the online help of Lavasoft Anti-Virus Helix.

Support

The menu item **Support** in the **Help** menu opens (with an active Internet connection) an information page on http://www.lavasoft.com/support/supportcenter/. There you can see how to contact us in the event of questions or technical problems.

Load License File

The menu item **Load license file** in the **Help** menu opens a dialog to load the license file hbedv.key.

Note
Loading of the license file with Windows Vista is only possible with administrator rights.

The menu item **License management** in the **Help** menu opens the Lavasoft Anti-Virus Helix license assistant. This assistant helps you to easily license or activate Lavasoft Anti-Virus Helix.

Activating the Product

Activate this option if you already have an activation key and have not yet activated Lavasoft Anti-Virus Helix . During the product activation, you are registered as a customer and Lavasoft Anti-Virus Helix is activated with your license. You received the activation key either by e-mail or it has been noted on the product packaging.

Note
The activation of Lavasoft Anti-Virus Helix can be carried out repeatedly with a valid activation key, if this should be required by a new installation of the system.

Testing the Product

Activate this option if you want to test Lavasoft Anti-Virus Helix and have not acquired a license yet. Lavasoft Anti-Virus Helix is activated with an evaluation license.

Note
For product activation or for applying for a test license, you need an active Internet connection. If a connection cannot be established to Lavasoft's servers, check the setting of the firewall used; if and when applicable, a communication via HTTP protocol and Port 80 (web communication) is

required. Please make sure that your firewall does not block incoming and outgoing data. Please check whether you can access the web pages with your web browser.

Valid hbedv.key License File

By using hbedv.key you can load a valid license file. During product activation with a valid activation key, the license key is generated, saved in the program directory of Lavasoft Anti-Virus Helix and loaded. Use this option, if you have activated a product and want to re-install Lavasoft Anti-Virus Helix without an active Internet connection.

Proxy Settings ...

A dialog window will open when you click on this button. If and when required, you can set that you want to establish the Internet connection for product activation by a proxy server.

About Anti-Virus Helix

General

Shows addresses for information on Lavasoft Anti-Virus Helix and for customer support.

Version Information

Shows important version information for files in the Lavasoft Anti-Virus Helix package.

License Information

Shows the license details of the current license and enables licenses to be conveniently obtained, extended, etc. via the Internet.

Configuration

This section contains the information you need to configure Lavasoft Anti-Virus Helix and ensure optimal computer use.

- Configuration Options - Overview
- Expert Mode
- Buttons

The following configuration options are available:

- **Scanner**: Configuration of on-demand scan

Scan options

Actions for concerning files

File scan options

On-demand scan exceptions

On-demand scan heuristics

Report function setting

- **Guard**: On-access scan configuration

Scan options

Actions for concerning files

On-access scan exceptions

On-access scan heuristics

Report function setting

- **MailGuard**: Configuration of MailGuard

Scan options

Actions on malware

MailGuard scan heuristics

MailGuard scan exceptions

Configuration of cache, empty cache

- **WebGuard**: Configuration of WebGuard

Action on detections

Blocked access: unwanted URLs, file types, MIME types

MailGuard scan exceptions

MailGuard heuristics

Report function setting

- **General**

Configuration of e-mail using SMTP

Extended risk categories for on-demand and on-access scan

Password protection for access to Control Center and Lavasoft Anti-Virus Helix Configuration

Security: alert for outdated Anti-Virus Helix, configuration protection, process protection,

Event log configuration

Configuration of report functions

Setting of directories used

Update: configuration of connection to download server, set-up of product updates

Expert Mode

If this option is enabled, you obtain access to all available configuration options for Lavasoft Anti-Virus Helix. If the option is disabled, only greatly simplified setting options are accessible.

Note
Enabling of the expert mode can be protected with a password.

If expert mode is disabled, the following configuration sections are available:

- Scanner :: Scan (with the options: Scan boot sectors of selected drives, Files and Scan memory)
- Scanner :: Scan :: Archives (with the option Scan archives)
- Guard :: Scan (with the options Scan mode, Files, Drives)

Buttons

Button	Description
OK	With this button, you accept the settings in the configuration. Depending on option settings, you must have administrator rights on Windows Vista.
Cancel	With this button, you reject the settings in the configuration.

Scanner

The Scanner section of the Lavasoft Anti-Virus Helix Configuration is responsible for the configuration of the on-demand scan.

Scan

Here you define the basic behavior of the scan routine for an on-demand scan. If you select certain directories to be scanned with an on-demand scan, depending on the configuration, the Scanner scans:

- with a certain scanning power (priority),
- boot sectors and main memory,
- certain or all boot sectors and the main memory,
- all or selected files in the directory.

Files

The Scanner can use a filter to scan only those files with a certain extension (type).

All Files

If this option is enabled, all files are scanned for viruses or unwanted programs, irrespective of their content and file extension. The filter is not used.

Note
If All files is enabled, the button **File extensions** cannot be selected.

Smart Extensions

If this option is enabled, the selection of the files scanned for viruses or unwanted programs is automatically chosen by Lavasoft Anti-Virus Helix. This means that Lavasoft Anti-Virus Helix decides, respective of their content, whether the files are scanned or not. This procedure is somewhat slower than **Use file extension list**, but more secure, since not only on the basis of the file extension is scanned. This option is enabled as the default setting and is recommended.

Note
If Smart Extensions is enabled, the button **File extensions** cannot be selected.

Use File Extension List

If this option is enabled, only files with a specified extension are scanned. All file types that may contain viruses and unwanted programs are preset. The list can be edited manually via the button **File extension**.

Note
If this option is enabled and you have deleted all entries from the list with file extensions, this is indicated with the text "No file extensions" under the button **File extensions**.

File Extensions

With the aid of this button, a dialog window is opened in which all file extensions are displayed that are scanned in **Use file extension list** mode. Default entries are set for the extensions, but entries can be added or deleted.

Note
Please note that the default list may vary from version to version.

Additional Settings

Scan Boot Sectors of Selected Drives

If this option is enabled, the Scanner only scans the boot sectors of the drives selected for the on-demand scan. This option is enabled as the default setting.

Scan Master Boot Sectors

If this option is enabled, the Scanner scans the master boot sectors of the hard disk(s) used in the system.

Ignore Offline Files

If this option is enabled, the direct scan ignores offline files completely during a scan. This means that these files are not scanned for viruses and unwanted programs. Offline files are files that were physically moved by a Hierarchical Storage Management System (HSMS) from the hard disk onto a

tape, for example. This option is enabled as the default setting.

Follow Symbolic Links

If this option is enabled, Scanner performs a scan that follows all symbolic links in the scan profile or selected directory and scans the linked files for viruses and malware. This option is not supported by Windows 2000 and has been deactivated.

Important
The option does not include any shortcuts, but refers exclusively to symbolic links (generated by mklink.exe) or Junction Points (generated by junction.exe) which are transparent in the file system.

Scan for Rootkits Before Scan

If this option is enabled and a scan is started, the Scanner scans the Windows system directory for active rootkits in a so-called shortcut. This process does not scan your computer for active rootkits as comprehensively as the scan profile **Scan for rootkits**, but it is significantly quicker to perform.

Important
The rootkit scan is not yet available on 64-bit systems.

Scan Process

Allow Stopping the Scanner

If this option is enabled, the scan for viruses or unwanted programs can be terminated at any time with the button **Stop** in the window "Virus Scan Helix". If you have disabled this setting, the button **Stop** in the window "Virus Scan Helix" has a gray background. Premature ending of a scan process is not possible. This option is enabled as the default setting.

Scanner Priority

With the on-demand scan, the Scanner distinguishes between priority levels. This is only effective if several processes are running simultaneously on the workstation. The selection affects the scanning speed.

Low

The Scanner is only allocated processor time by the operating system if no other process requires computation time. For example, as long as only the Scanner is running, the speed is maximum. All in all, work with other programs is optimal: the computer responds more quickly if other programs require computation time while the Scanner continues running in the background. This setting is activated by default and is recommended.

Medium

The Scanner is performed with normal priority. All processes are allocated the same amount of processor time by the operating system. Under certain circumstances, work with other applications may be affected.

High

The Scanner has the highest priority. Simultaneous work with other applications is almost impossible. The Scanner will completes its scan at maximum speed.

Action for Concerning Files

You can define actions that the Scanner is to carry out when a virus or unwanted program is detected.

Interactive

When this option is enabled, on detection of a virus or unwanted program during an on-demand scan, a dialog window appears in which you can select what is to be done with the affected file. This option is enabled as the default setting. Further information is available here.

Automatic

If this option is enabled and a virus or unwanted program is detected, no dialogue appears in which an action can be selected. The Scanner reacts according to the settings made by you in this section.

Copy File to Quarantine Before Action

If this option is enabled, the Scanner creates a back-up copy before carrying out the requested primary or secondary action. The back-up copy is saved in quarantine, where the file can be restored if it is of informative value.

Primary action

Primary action is the action carried out when the Scanner finds a virus or an unwanted program. If the option **repair** is selected but a repair of the file involved is not possible, the action selected under **Secondary action** is carried out.

Note
The option **Secondary action** can only be selected if the setting **repair** was selected under **Primary action**.

Repair

If this option is enabled, the Scanner repairs affected files automatically. If the Scanner cannot repair an affected file, it carries out the action selected under Secondary action.

Note
An automatic repair is recommended, but means that the Scanner modifies files on the workstation.

Delete

If this option is enabled, the file is deleted, but can be restored if necessary with relevant tools. This means that the virus pattern could be detected again. This process is much faster than "overwrite and delete".

Overwrite and Delete

If this option is enabled, the Scanner overwrites the file with a default pattern and then deletes it. It cannot be restored.

Rename

If this option is enabled, the Scanner renames the file. Direct access to these files (e.g. with double-click) is therefore no longer possible. Files can later be repaired and given their original names again.

Ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation! It may cause serious damage on your workstation!

Quarantine

If this option is enabled, the Scanner moves the file to the quarantine. These files can later be repaired or - if necessary - sent to the Lavasoft Malware Research Center.

Secondary action

The option **Secondary action** can only be selected if the setting **Repair** was selected under **Primary action**. With this option it can now be decided what is to be done with the affected file if it cannot be repaired.

Delete

If this option is enabled, the file is deleted, but it can be restored if necessary with relevant tools (e. g. Lavasoft UnErase). This means the virus pattern could be detected again. This process is much faster than "overwrite and delete".

Overwrite and Delete

If this option is enabled, the Scanner overwrites the file with a default pattern and then deletes (wipes) it. It cannot be restored.

Rename

If this option is enabled, the Scanner renames the file. Direct access to these files (e.g. by double-clicking) is therefore no longer possible. Files can later be repaired and given their original names.

Ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation. It may cause serious damage on your workstation.

Quarantine

If this option is enabled, the Scanner moves the file to the quarantine. These files can later be repaired or - if necessary - sent to the Lavasoft Malware Research Center.

Further Actions

Acoustic Alert

If this option is enabled, the Scanner plays a sequence of notes in the event of a detection. This option is activated by default.

Wave File

In this input box, you can enter the name and the associated path of an audio file of your choice. If

this box is empty, the default alert sound is played.

The button opens a window in which you can select the required file with the aid of the file explorer.

Test Acoustic Alert

This button is used to test the selected wave file.

Archives

When scanning archives, the Scanner uses a recursive scan. Archives within archives are also unpacked and scanned for viruses and unwanted programs. The files are scanned, decompressed and scanned again.

Scan Archives

If this option is enabled, the selected archives in the archive list are scanned. This option is enabled as the default setting.

All Archive Types

If this option is enabled, all archive types in the archive list are selected and scanned.

Smart Extensions

If this option is enabled, the Scanner detects whether a file is a packed file format (archive), even if the file extension differs from the usual extensions, and scans the archive. However, for this to take place, every file must be opened, which reduces the scanning speed. For example, if a *.zip archive has the file extension *.xyz, the Scanner also unpacks this archive and scans it. This option is enabled as the default setting.

Note
Only archive types marked in the archive list are supported.

Limit Recursion Depth

Unpacking and scanning deeply interlaced archives can require a great deal of computer time and resources. If this option is enabled, you limit the depth of the scan in multi-packed archives to a certain number of packing levels (maximum recursion depth). This saves time and computer resources.

Note
In order to find a virus or an unwanted program in an archive, the Scanner must scan up to the recursion level in which the virus or the unwanted program is located.

Maximum Recursion Depth

In order to enter the maximum recursion depth, the option Limit recursion depth must be enabled. You can either enter the requested recursion depth directly or by means of the right arrow key on the entry field. The permitted values are 1 to 99. The standard value is 20 which is recommended.

Default Values

The button restores the pre-defined values for scanning archives.

Archive List

In this display area you can set which archives the Scanner should scan. For this, you must select the relevant entries.

Exceptions

File Objects to be Omitted for the Scanner

The list in this window contains files and paths that should not be included by the Scanner in the scan for viruses or unwanted programs.

Please enter as few exceptions as possible here and really only files that, for whatever reason, should not be included in a normal scan. We recommend that you always scan these files for viruses or unwanted programs before they are included in this list!

Note
The entries on the list must not result more than 6000 characters in total.

Warning
These files are not included in a scan!

Note
The files included in this list are entered in the report file. Please check the report file from time to time for unscanned files, as perhaps the reason you excluded a file here no longer exists. In this case you should remove the name of this file from this list again.

Input Box

In this input box you can enter the name of the file object that is not included in the on-demand scan. No file object is entered as the default setting.

The button opens a window in which you can select the required file or the required path.
When you have entered a file name with its complete path, only this file is not scanned for infection. If you have entered a file name without a path, all files with this name (irrespective of the path or drive) are not scanned.

Add

With this button, you can add the file object entered in the input box to the display window.

Delete

The button deletes a selected entry in the list. This button is not active if no entry is selected.

Note
If you add a complete partition to the list of the file objects, only those files which are saved directly under the partition will be excluded from the scan, which does not apply for files in sub-directories on the corresponding partition:
Example: File object to be skipped: `D: \ = D: \file. txt` will be excluded from the scan of the Scanner, `D: \folder\file. txt` will not be excluded from the scan.

Heuristic

This configuration section contains the settings for the heuristic of the Lavasoft Anti-Virus Helix search engine.

Lavasoft Anti-Virus Helix contains very powerful heuristic, which can also detect unknown (new) viruses, worms or Trojans. This is done with a comprehensive analysis and examination of the relevant codes for functions that are typical of viruses, worms or Trojans. If the code examined fulfils these characteristic criteria, it is reported as being suspect. However, this does not necessarily mean that the code is in actual fact a virus, a worm or a Trojan; it may also be a false alert. The user has to decide what to do with the relevant code, for example based on his/her knowledge of whether the source containing the suspect code is reliable.

Macrovirus Heuristic

Lavasoft Anti-Virus Helix contains a very powerful macrovirus heuristic. If this option is enabled, all macros are deleted in the event of a repair, alternatively suspect documents are only reported, i.e. you receive an alert. This option is enabled as the default setting and is recommended.

Win32 file Heuristic

Lavasoft Anti-Virus Helix contains a very powerful heuristic for Windows file viruses, worms and Trojans, which can also detect unknown viruses, worms and Trojans. If this option is enabled, here you can set how "aggressive" this heuristic should be. This option is enabled as the default setting.

Low Detection Level

If this option is enabled, Lavasoft Anti-Virus Helix detects fewer viruses, worms or Trojans, the risk of false alerts is low in this case.

Medium Detection Level

This option is enabled as the default setting if you have selected application of this heuristic.

High Detection Level

If this option is enabled, Lavasoft Anti-Virus Helix detects a large number of unknown viruses, worms or Trojans, but you must also expect false positives.

Report

The Scanner has a comprehensive reporting function. You thus obtain precise information on the results of an on-demand scan. The report file contains all entries of the system as well as alerts and messages of the on-demand scan.

Note
So that you can establish what actions the Scanner has carried out when viruses or unwanted programs have been detected, a report file should always be created.

Reporting

Off

If this option is enabled, the Scanner does not report the actions and results of the on-demand scan.

Default

When this option is activated, the Scanner logs the names of the files concerned with their path. In addition, the configuration for the current scan, version information and information on the licensee is written in the report file.

Extended

When this option is activated, the Scanner logs alerts and tips in addition to the default information.

Complete

When this option is activated, the Scanner also logs all scanned files. In addition, all files involved as well as alerts and tips are included in the report file.

Note
If you have to send us a report file at any time (for troubleshooting), please create this report file in this mode.

Guard

The Guard section of the Lavasoft Anti-Virus Helix Configuration is responsible for the configuration of the on-access scan.

Scan

You will normally want to monitor your system constantly. To this end, use the Guard (= on-access scanner). You can thus scan all files that are copied or opened on the computer "on the fly", for viruses and unwanted programs.

Scan Mode

Here the time for scanning of a file is defined.

Scan When Reading

If this option is enabled, the Guard scans the files before they are read or executed by the application or the operating system.

Scan When Writing

If this option is enabled, the Guard scans a file when writing. You can only access the file again after this process has been completed.

Scan When Reading and Writing

If this option is enabled, the Guard scans files before opening, reading and executing and after writing. This option is enabled as the default setting and is recommended.

Files

The Guard can use a filter to scan only files with a certain extension type.

All Files

If this option is enabled, all files – irrespective of their content and their file extension –are scanned for viruses or unwanted programs, i.e. the filter is not used.

Note
If All files is enabled, the button **File extensions** cannot be selected.

Smart Extensions

If this option is enabled, the selection of the files scanned for viruses or unwanted programs is automatically chosen by Lavasoft Anti-Virus Helix. This means that Lavasoft Anti-Virus Helix decides whether the files are scanned or not based on their content. This procedure is somewhat slower than Use file extension list, but more secure, since scanning is not done only on the basis of the file extension.

Note
If Smart Extensions is enabled, the button **File extensions** cannot be selected.

Use File Extension List

If this option is enabled, only files with a pre-defined extension are scanned. All file types that may contain viruses and unwanted programs are pre-defined. The list can be edited manually via the button **File extension**. This option is enabled as the default setting and is recommended.

Note
If this option is enabled and you have deleted all entries from the list with file extensions, this is indicated with the text "No file extensions" under the button **File extensions**.

File Extensions

With the aid of this button, a dialog window is opened in which all file extensions are displayed that are scanned in the **Use file extension list** mode. Default entries are set for the extensions, but entries can be added or deleted.

Note
Please note that the file extension list may vary from version to version.

Archives

Scan Archive

If this option is enabled, archives will be scanned. Compressed files are scanned, then decompressed and scanned again. This option is deactivated by default. Additional settings are available for restricting the scanning of archives and for setting the recursion depth of the scanning. This is recommended if you activate the archive scan.

Note
This option is deactivated by default, since the process puts heavy demands on the computer's performance. It is generally recommended that archives be checked using an on-demand scan.

Maximum Depth of Recursion

When scanning the archives, the Guard can use a recursive scan. This unpacks archives that packed

inside other archives and checks them for viruses and unwanted programs. You can define the recursion depth. Activate this option to do so. Permitted values are 1 to 20. The default value for the recursion depth is 1 and is recommended; all archives that are directly located in the main archive are unpacked and scanned.

Maximum Number of Files

If this option is enabled, you can restrict the scan to a maximum number of files in the archive. Permissible values are between 1 and 99. The default value of 10 files to be scanned is recommended.

Maximum Size (KB)

If this option is enabled, you can restrict the scanner to unpacking only archives below a defined maximum size. Permissible values are between 1 and 9,999 KB. The standard value of 1,000 KB is recommended.

Action for Concerning Files

You can define actions that the Guard is to carry out when a virus or unwanted program is detected.

Interactive

If this option is enabled, a dialog window appears during the on-access scan when a virus or unwanted program is detected in which you can choose what is to be done with the file concerned. This option is enabled as the default setting.

Automatic

If this option is enabled, no dialog box for selecting an action appears following the detection of a virus or unwanted program. The Guard reacts according to the settings you selected in this section.

Copy File to Quarantine Before Action

If this option is enabled, the Guard creates a backup copy before carrying out the requested primary or secondary action. The backup copy is saved in quarantine. It can be be restored via the Quarantine manager if it is of informative value. You can also send the backup copy to the Lavasoft Malware Research Center. Depending on the object, there are more selection possibilities in the quarantine manager.

Primary Action

Primary action is the action carried out when the Guard finds a virus or an unwanted program. If the option **Repair** is selected but a repair of the file involved is not possible, the action selected under **Secondary action** is carried out.

Note
The option Secondary action can only be selected if the option Repair was selected under Primary action.

Repair

If this option is enabled, the Guard repairs affected files automatically. If the Guard cannot repair an affected file, it carries out the action selected under Secondary action.

Note
An automatic repair is recommended, but means that the Guard modifies files on the workstation.

Delete

If this option is enabled, the file is deleted, but can be restored if necessary with relevant tools (e.g. Lavasoft UnErase). This means that the virus patterns could be detected again. This process is much faster than "overwrite and delete".

Overwrite and Delete

If this option is enabled, the Guard overwrites the file with a default pattern and then deletes it. It cannot be restored.

Rename

If this option is enabled, the Guard renames the file. Direct access to these files (e.g. by double-clicking) is therefore no longer possible. Files can later be repaired and given their original names.

Ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation. It may cause serious damage on your workstation.

Deny Access

If this option is enabled, the Guard only enters the detection in the report file if the report function is enabled. In addition, the Guard writes an entry in the event log, if this option is enabled.

Quarantine

If this option is enabled, the Guard moves the file to the quarantine. The files in this directory can later be repaired or - if necessary - sent to the Lavasoft Malware Research Center.

Secondary Action

The option **Secondary action** can only be selected if the option **Repair** was selected under **Primary action**. This option allows you to decide what should be done with the affected file if it cannot be repaired.

Delete

If this option is enabled, the file is deleted, but can be restored, if necessary, with relevant tools (e.g. Lavasoft UnErase). This means that the virus patterns could be detected again. This process is much faster than "overwrite and delete".

Overwrite and Delete

If this option is enabled, the Guard overwrites the file with a default pattern and then deletes it. It cannot be restored.

Rename

If this option is enabled, the Guard renames the file. Direct access to these files (e.g. by doubleclicking) is therefore no longer possible. Files can later be repaired and given their original names again.

Ignore

If this option is enabled, access to the file is allowed and the file is left as it is.

Warning
The affected file remains active on your workstation. It may cause serious damage on your workstation.

Deny Access

If this option is enabled, the Guard only enters the detection in the report file if the report function is enabled. In addition, the Guard writes an entry in the event log, if this option is enabled.

Quarantine

If this option is enabled, the Guard moves the file to the quarantine. The files can later be repaired.

Other Actions

Notifications

Use Event Log

When this option is enabled, an entry is added to the event log for every detection. The administrator can identify detections and react accordingly. This option is enabled by default.

Acoustic Alert

When this option is enabled, the Guard plays a sequence of notes when a detection is made. This setting is enabled by default.

Exceptions

With these options, you can configure exception objects for the Guard (on-access scan). The relevant objects are then not included in the on-access scan. The Guard can ignore file accesses to these objects during the on-access scan via the list of processes to be omitted. This is useful, for example, with databases or back-up solutions.

Processes to be Omitted for the Guard

All file accesses of processes in this list are excluded from monitoring by the Guard.

Input Box

In this box you can enter the name of the process that is not included in the on-access scan. No process is entered as the default setting. The names of the individual process can most easily be obtained via the task manager. You can find the names of all currently active processes under the index card "Processes" of the task manager. Select "your" process and enter its name (found under "Image Name").

Note
You can enter up to 20 processes.

Warning
Only the first 15 characters of the process name (including the file extension) are considered. If there are two processes with the same name, the Guard excludes both processes from the monitoring.

Warning
Please note that all file accesses by processes recorded in the list are excluded from the scan for viruses and unwanted programs. Windows Explorer and the operating system itself cannot be excluded. A corresponding entry in the list is ignored.

Add

With this button, you can add the process entered in the input box to the display window.

Delete

With this button you can delete a selected process from the display window.

File Objects to be Omitted for the Guard

All file accesses to objects in this list are excluded from monitoring by the Guard.

Note
The entries on the list must not contain more than 6,000 characters in total.

Input Box

In this box, you can enter the name of the file object that is not included in the on-access scan. No file object is entered as the default setting.

The button opens a window in which you can select the file object to be excluded.

Add

With this button, you can add the file object entered in the input box to the display window.

Delete

With this button you can delete a selected file object from the display window.

Please observe the following points:

- The file name can only contain the wildcards * (any number of characters) and ? nbsp;(a single character).
- Directory names must end with a backslash, otherwise a file name is assumed.
- The list is processed from top to bottom.
- Individual file extensions can also be excluded (inclusive wildcards).
- If a directory is excluded, all its sub-directories are automatically also excluded.
- The longer the list is, the more processor time is required for processing the list for each access. Therefore, keep the list as short as possible.
- In order to also exclude objects when they are accessed with short DOS file names (DOS name convention 8.3), the relevant short file name must also be entered in the list.

Note
A file name that contains wildcards may not be terminated with a backslash.

For example:

```
C:\Program Files\Application\applic*.exe\
```

This entry is not valid and not treated as an exception!

Note

In case of dynamic drives which are mounted as a directory on another drive, the alias of the operating system for the integrated drive in the list of the exceptions has to be used: e.g. \Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\

If you use the mount point itself, such as C:\DynDrive, the dynamic drive will be scanned nonetheless. You can determine the alias of the operating system to be used from the report file of Guard. To do this, set the protocol function of the Guard to **complete** in the configuration under Guard :: Report. Then access the mounted drive with the activated Guard. You can now read the drive name used from the report file of the Guard. The report file can be accessed in the Control Center under Local protection :: Guard

Examples:

```
C:
C:\
C:\*.*
C:\*
*.exe
*.xl?
*.*
C:\Program Files\Application\application.exe
C:\Program Files\Application\applic*.exe
C:\Program Files\Application\applic*
C:\Program Files\Application\applic?????.e*
C:\Program Files\
C:\Program Files
C:\Program Files\Application\*.mdb
```

Heuristic

This configuration section contains the settings for the heuristic of the Lavasoft Anti-Virus Helix search engine.

Lavasoft Anti-Virus Helix contains very powerful heuristic, which can also detect unknown (new) viruses, worms or Trojans. This is done with a comprehensive analysis and examination of the relevant codes for functions that are typical of viruses, worms or Trojans. If the code examined fulfils these characteristic criteria, it is reported as being suspect. However, this does not necessarily mean that the code is in fact a virus, worm or Trojan. False positives do sometimes occur. The user has to decide what to do with the relevant code based on his/her knowledge of whether the source containing the suspect code is reliable.

Macrovirus Heuristic

Lavasoft Anti-Virus Helix contains a very powerful macrovirus heuristic. If this option is enabled,

all macros are deleted in the event of a repair. Alternatively suspect documents are only reported, i. e. you receive an alert. This option is enabled as the default setting and is recommended.

Win32 File Heuristic

Lavasoft Anti-Virus Helix contains a very powerful heuristic for Windows file viruses, worms and Trojans, which can also detect unknown viruses, worms and Trojans. If this option is enabled, you can set how "aggressive" this heuristic should be. This option is enabled as the default setting.

Low Detection Level

If this option is enabled, Lavasoft Anti-Virus Helix detects fewer viruses, worms or Trojans, the risk of false alerts is low in this case.

Medium Detection Level

This option is enabled as the default setting if you have selected the application of this heuristic.

High Detection Level

If this option is enabled, Lavasoft Anti-Virus Helix detects a large number of unknown viruses, worms or Trojans, but you must also expect false positives.

Report

The Guard has a comprehensive reporting function that can provide the user or the administrator with precise information on the type of malware detected.

Reporting

The scope of content of the report file is defined in this group.

Off

If this option is enabled, the Guard does not create a report. Only refrain from enabling reporting in exceptional cases, for example if you carry out test runs with many viruses or unwanted programs.

Default

If this option is enabled, the Guard adds important information (on the found, alerts and errors) to the report file. Less important information is ignored in order to provide a clear overview. This option is enabled as the default setting.

Extended

If this option is enabled, the Guard also includes less important information in the report file.

Complete

If this option is enabled, the Guard includes all information (file size, file type, date etc) in the report file.

Limit report file

Limit Size to n MB

If this option is enabled, the report file can be limited to a certain size; possible values: 1 to 100 MB. This option is enabled as the default setting, with a value of 1 MB. A tolerance of approximately 50 kilobytes is included in order to minimize load of the computer. If the size of the report file exceeds the pre-defined size by 50 kilobytes, old entries are automatically deleted until the pre-defined size (50 kilobytes) has been reached.

Backup Report File Before Shortening

If this option is enabled, the report file is backed up before being shortened in the report directory.

Write Configuration in Report File

If this option is enabled, the configuration of the on-access scan used is written in the report file.

MailGuard

The MailGuard section of the Lavasoft Anti-Virus Helix Configuration is responsible for the configuration of the MailGuard.

Scan

Use MailGuard to scan incoming e-mail for viruses and malware . Outgoing e-mail can be scanned for viruses and malware by MailGuard. Outgoing e-mails which are spam sent from an unknown bot on your computer can be blocked by MailGuard.

Scan

Scan Incoming E-mail (POP3)

If this option is enabled, incoming e-mail are scanned for viruses, malware and spam.

Scan Outgoing E-mail (SMTP)

If this option is enabled, outgoing e-mail are scanned for viruses and malware. E-mail which are spam sent by unknown bots are blocked.

Action on Malware

This configuration section contains settings for actions performed when MailGuard finds a virus or unwanted program in an e-mail or attachment.

Note
These actions are performed both when a virus is detected in incoming e-mail and outgoing e-mail.

Action for Concerning Files

Interactive

If this option is enabled, a dialog window appears when a virus or unwanted program is detected in an e-mail or attachment in which you can choose what is to be done with the e-mail or attachment concerned. This option is enabled as the default setting.

Show Progress Bar

If this option is enabled, the MailGuard shows a progress bar while downloading e-mail. This can only be enabled if the option **Interactive** has been selected.

Automatic

If this option is enabled, you are no longer notified when a virus or unwanted program is found. The MailGuard reacts according to the settings you selected in this section.

Primary Action

Primary action is the action carried out when the MailGuard finds a virus or an unwanted program in an e-mail. If the option **Ignore e-mail** is selected, it is also possible to select under **Affected attachments** what is to be done if a virus or unwanted program is detected in an attachment.

Delete E-mail

If this option is enabled, the affected e-mail is automatically deleted if a virus or unwanted program is found. The body of the e-mail is replaced by the default text given below. The same applies to all attachments included; these are also replaced by default text.

Isolate E-mail

If this option is enabled, the complete e-mail (including all attachments) is placed in Quarantine if a virus or unwanted program is found. If required, it can later be restored. The affected e-mail itself is deleted. The body of the e-mail is replaced by the default text given below. The same applies to all attachments included; these are also replaced by default text.

Ignore E-mail

If this option is enabled, the affected e-mail is ignored despite detection of a virus or unwanted program. However, you can decide what is to be done with the affected attachment:

Affected Attachments

The option **Affected attachments** can only be selected if the setting **Ignore e-mail** has been selected under **Primary action**. With this option, it is now possible to decide what is to be done if a virus or unwanted program is found in an attachment.

Delete

If this option is enabled, the affected attachment is deleted if a virus or unwanted program is found and replaced by a default text.

Isolate

If this option is enabled, the affected attachment is placed in quarantine and then deleted (replaced by a default text). If required, it can later be restored.

Ignore

If this option is enabled, the attachment is ignored and delivered, despite detection of a virus or unwanted program.

Warning
If you select this option, you have no protection against viruses and unwanted programs by the MailGuard. Only select this after careful consideration. Disable the preview in your e-mail program and never open attachments by double-clicking.

Other actions

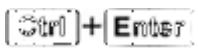
This configuration section contains other settings for actions performed when MailGuard finds a virus or unwanted program in an e-mail or in an attachment.

Note
These actions are performed exclusively when a virus is detected in incoming e-mail.

Default Text for Deleted and Moved E-mail

The text in this box is inserted in the e-mail as a message instead of the affected e-mail message. Please note that you can also format the text in this edit box. You can enter a maximum of 500 characters.

You can use the following key combination for formatting:



inserts a line break.

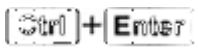
Default

The button inserts a pre-defined default text in the edit box.

Default Text for Deleted and Moved Attachments

The text in this box is inserted in the e-mail as a message instead of the affected attachment. Please note that you can also format the text in this edit box. You can enter a maximum of 500 characters.

You can use the following key combination for formatting:



inserts a line break.

Default

The button inserts a pre-defined default text in the edit box.

Heuristic

This configuration section contains the settings for the heuristic of the Lavasoft Anti-Virus Helix search engine.

Lavasoft Anti-Virus Helix contains very powerful heuristic, which can also detect unknown (new) viruses, worms or Trojans. This is done with a comprehensive analysis and examination of the relevant codes for functions that are typical of viruses, worms or Trojans. If the code examined fulfils these characteristic criteria, it is reported as being suspect. However, this does not necessarily mean that the code is actually a virus, worm or Trojan; it may also be a false alert. The user has to decide what to do with the relevant code based on his/her knowledge of whether the source containing the suspect code is reliable.

Macrovirus Heuristic

Lavasoft Anti-Virus Helix contains a very powerful macrovirus heuristic. If this option is enabled, all macros are deleted in the event of a repair, alternatively suspect documents are only reported, i.e. you receive an alert. This option is enabled as the default setting and is recommended.

Win32 file Heuristic

Lavasoft Anti-Virus Helix contains a very powerful heuristic for Windows file viruses, worms and Trojans, which can also detect unknown viruses, worms and Trojans. If this option is enabled, you can set how "aggressive" this heuristic should be. This option is enabled as the default setting.

Low Detection Level

If this option is enabled, Lavasoft Anti-Virus Helix detects fewer viruses, worms or Trojans. The risk of false alerts is low in this case.

Medium Detection Level

This option is enabled as the default setting if you have selected application of this heuristic. This option is enabled as the default setting and is recommended.

High Detection Level

If this option is enabled, Lavasoft Anti-Virus Helix detects a large number of unknown viruses, worms or Trojans, but you must also expect false positives.

AntiBot

The AntiBot function of MailGuard prevents your computer from becoming part of a botnet and being used to send out spam e-mail. To send spam via a botnet, an attacker usually infects a number of computers with a bot, which then connects to an IRC server, opens a particular channel and waits for the command to send the spam e-mail. To distinguish spam e-mail from an unknown bot from genuine e-mail, MailGuard checks if the SMTP server and e-mail sender for an outgoing e-mail are included in the lists of permitted servers and senders. If this is not the case, the outgoing e-mail are blocked, and the e-mail is not sent. A dialog box appears in which you can choose what to do with the e-mail.

Note
The AntiBot function can only be used if the MailGuard scan of outgoing e-mail is enabled (see the option **Scan outgoing e-mail** under MailGuard :: Scan).

Permitted Servers

All servers in this list are authorized to send e-mail. E-mail sent to these servers are **not** blocked by

MailGuard. If no servers are included in the list, the SMTP server used to send outgoing e-mail is not scanned. If the list is populated, MailGuard blocks e-mail sent to any SMTP server not included in the list.

Input Box

In this box, enter the host name or IP address of the SMTP server you use to send your e-mail

Note
You can find details of the SMTP server used by your e-mail program to send e-mails in your e-mail program under the date the user account was created.

Add

You can use this button to include servers specified in the input box in the list of permitted servers.

Delete

This button deletes a highlighted entry from the list of permitted servers. This button is inactive if no entry is selected.

Delete All

This button deletes all entries from the list of permitted servers.

Permitted Senders

All senders in this list are authorized by MailGuard to send e-mail. E-mail sent from this e-mail address are **not** blocked by MailGuard. If no senders are included the list, the e-mail address used to send outgoing e-mail is not scanned. If the list is populated, MailGuard blocks e-mail from senders not included in the list.

Input Box

Enter your e-mail sender address(es) in this box.

Add

You can use this button to include senders specified in the input box in the list of permitted senders.

Delete

This button deletes a highlighted entry from the list of permitted senders. This button is inactive if no entry is selected.

Delete All

This button deletes all entries from the list of permitted senders.

General

Exceptions

E-mail Addresses Not Scanned

This table shows you the list of e-mail addresses excluded from scanning by Anti-Virus MailGuard (white list).

Note
The list of exceptions is used exclusively by MailGuard with regard to incoming e-mail.

Status

Icon	Description
	This e-mail address will no longer be scanned for malware.

E-mail Address

E-mail that is no longer to be scanned.

Malware

When this option is enabled, the e-mail address is no longer scanned for malware.

Up

You can use this button to move a highlighted e-mail address to a higher position. If no entry is highlighted or the highlighted address is at the first position in the list, this button is not enabled.

Down

You can use this button to move a highlighted e-mail address to a lower position. If no entry is highlighted or the highlighted address is at the last position in the list, this button is not enabled.

Input Box

In this box, enter the e-mail address that you want to add to the list of e-mail addresses not to be scanned. Depending on your settings, the e-mail address will no longer be scanned in future by the MailGuard.

Add

With this button you can add the e-mail address entered in the input box to the list of e-mail addresses not to be scanned.

Delete

This button deletes a highlighted e-mail address from the list.

Cache

The MailGuard cache contains data regarding scanned e-mail that is displayed as statistical data in the Control Center under MailGuard.

Maximum Number of E-mail to be Stored in the Cache

This field is used to set the maximum number of e-mails that are stored by MailGuard in the cache. E-mails are deleted oldest first.

Maximum Storage Period of an E-mail in Days

The maximum storage period of an e-mail in days is entered in this box. After this time, the e-mail is removed from the cache.

Empty Cache

Click on this button to delete the e-mail stored in the cache.

Report

MailGuard includes an extensive logging function to provide the user or administrator with exact information on the type of detection.

Logging

This group allows for the content of the report file to be determined.

Off

If this option is enabled, MailGuard does not create a log. Only turn off the logging function in exceptional cases, such as if you are executing test runs with multiple viruses or unwanted programs.

Default

If this option is enabled, MailGuard records important information (concerning detections, alerts and errors) in the report file, while less important information ignored for improved clarity. This option is enabled as the default setting.

Extended

If this option is enabled, MailGuard also logs less important information in the report file.

Complete

If this option is enabled, MailGuard logs all available information in the report file, including file size, file type, date, etc.

Limit Report File

Limit Size to n MB

If this option in enabled, the report file is restricted to a specific size. Permitted values are between 1 and 100 MB. This option is activated by default with a value of 1 MB. Up to 50 kilobytes of extra space are allowed to minimize the use of system resources. If the size of the log file exceeds the indicated size by more than 50 kilobytes, then old entries are then deleted until the indicated size

minus 50 kilobytes is attained.

Backup Report File Before Shortening

If this option is enabled, the abbreviated report file is saved.

Write Configuration in Report File

If this option is enabled, the MailGuard configuration is recorded in the report file.

WebGuard

The WebGuard section of Lavasoft Anti-Virus Helix's Configuration is used to configure WebGuard.

Scan

Action on Detection

You can define the actions to be carried out by WebGuard when a virus or unwanted program is detected.

Interactive

If this option is enabled, a dialog window appears when a virus or unwanted program is detected during an on-demand scan, in which you can choose what is to be done with the affected file. This option is enabled as the default setting.

Show Progress Bar

If this option is enabled, a desktop notification appears with a download progress bar if a download of website content exceeds a 20 second timeout. This desktop notification is specifically designed for downloading websites with larger data volumes. If you are surfing with WebGuard, website content is not downloaded incrementally in the Internet browser, as it is scanned for viruses and malware before being displayed in the Internet browser. This option is disabled as the default setting.

Automatic

If this option is enabled, no dialog box for selecting an action appears following the detection of a virus or unwanted program. WebGuard reacts according to the settings you define in this section.

Primary action

The primary action is the action carried out when WebGuard finds a virus or an unwanted program.

Deny Access

The website requested by the web server and/or the transferred data and files are not sent to your web browser. An error message about the denial of access is displayed in the web browser. WebGuard logs the detection to the report file if the report function is activated. WebGuard also

appends an entry to the event log if this option is enabled.

Isolate

In the event of a virus or malware being detected, the website requested from the web server and/or the transferred data and files are moved into quarantine. The infected file can be restored via the Quarantine Manager if it is of informative value or - if necessary - sent to the Lavasoft Malware Research Center.

Ignore

The website requested by the web server and/or the transferred data and files are forwarded on by WebGuard to your web browser. Access to the file is permitted and the file is ignored.

Warning
The affected file remains active on your workstation. It may cause serious damage on your workstation.

Locked requests

In **Locked requests** you can specify the file types and MIME types (content types for the transferred data) to be blocked by WebGuard. The Web filter lets you block known phishing and malware URLs. WebGuard prevents the transfer of data from the Internet to your computer system.

File Types / MIME Types to be Blocked by WebGuard (Custom)

All file types and MIME types (content types for the transferred data) in the list are blocked by WebGuard.

Input Box

In this box, enter the names of the MIME types and file types you want WebGuard to block. For file types, enter the file extension, e.g. **.htm**. For MIME types, indicate the media type and, where applicable, subtype. The two statements are separated from one another by a single slash, e.g. **video/mpeg** or **audio/x-wav**.

Note
Files which are already stored on your computer system as temporary Internet files and blocked by WebGuard can be downloaded locally from the Internet by your computer's Internet browser. Temporary Internet files are files saved on your computer by the Internet browser so that websites can be accessed more quickly

Note
The list of blocked file and MIME types is ignored if they are entered in the list of excluded files and MIME types under WebGuard::Scan::Exceptions.

Note
No wildcards (* for any number of characters or ? nbsp for a single character) can be used when entering file types and MIME types.

MIME types: Examples for media types:

- `text` = for text files
- `image` = for graphics files
- `video` = for video files
- `audio` = for sound files
- `application` = for files linked to a particular program

Examples: Excluded file and MIME types

- `application/octet-stream` = application/octet-stream MIME type files (executable files *.bin, *.exe, *.com, *dll, *.class) are blocked by WebGuard.
- `application/olescript` = application/olescript MIME type files (ActiveX script-files *.axs) are blocked by WebGuard.
- `.exe` = All files with the extension .exe (executable files) are blocked by WebGuard.
- `.msi` = All files with the extension .msi (Windows Installer files) are blocked by WebGuard.

Add

With this button, you can add the MIME or file type entered in the input box to the display window.

Delete

This button deletes an entry highlighted in the list. This button is inactive if no entry is selected.

Web Filter

The Web filter is based on an internal database, updated daily, that classifies URLs according to content.

Block Phishing and Malware URLs

If this option is enabled, known phishing and malware URLs are blocked by WebGuard.

Note
The Web filter is ignored for entries in the list of excluded URLs under WebGuard::Scan:: Exceptions.

Exceptions

These options allow you to set exceptions based on MIME types (content types for the transferred data) and file types for URLs (Internet addresses) for scanning by WebGuard. The MIME types and URLs specified are ignored by WebGuard, i.e. that data is not scanned for viruses and malware when it is transferred to your computer system.

MIME Types Skipped by WebGuard

In this field, you can select the MIME types (content types for the transferred data) to be ignored by WebGuard during scanning.

File Types/MIME Types Skipped by WebGuard (Custom)

All MIME types (content types for the transferred data) in the list are ignored by WebGuard during scanning.

Input Box

In this box, you can input the name of the MIME types and file types to be ignored by WebGuard during scanning. For file types, enter the file extension, e.g. z.B. **.htm**. For MIME types, indicate the media type and, where applicable, subtype. The two statements are separated from one another

by a single slash, z.B. **video/mpeg** or **audio/x-wav**.

Note
No wildcards (* for any number of characters or ?nbsp for a single character) can be used when entering file types and MIME types.

Alert
All file types and content types on the exceptions list are downloaded into the Internet browser without further scanning of the blocked access (List of file and MIME types to be blocked in WebGuard::Scan::Blocked access) or by WebGuard. For all entries on the exceptions list, the entries on the list of file and MIME types to be blocked are ignored. No scan for viruses and malware is carried out.

MIME types: Examples for Media Types:

- `text` = for text files
- `image` = for graphics files
- `video` = for video files
- `audio` = for sound files
- `application` = for files linked to a particular program

Examples: Excluded File and MIME Types

- `audio/` = All audio media type files are excluded from WebGuard scans
- `video/quicktime` = All Quicktime sub-type video files (*.qt, *.mov) are excluded from WebGuard scans
- **.** `pdf` = All Adobe PDF files are excluded from WebGuard scans.

Add Rule

The button allows you to copy MIME and file types from the input field into the display window.

Delete

The button deletes a selected entry from the list. This button is inactive if no entry is selected.

URLs Skipped by WebGuard

All URLs in this list are excluded from WebGuard scans.

Input Box

In this box, you can input URLs (Internet addresses) to be excluded from WebGuard scans, e.g. **www.domainname.com/**. Indicate websites with any top-level domain (.com or .net) with a concluding dot: **domainname.**. If you indicate a string without a leading or concluding dot, the string is interpreted as a top-level domain, e.g. **net** for all NET-Domains (www.domain.net).
Note
No wildcards (* for any number of characters or ?nbsp for a single character) can be used when entering URLs.

Warning
All websites on the list of excluded URLs are downloaded into the Internet browser without further scanning by the web filter or WebGuard. For all entries in the list of excluded URLs, the entries in the web filter (see WebGuard::Scan::Blocked access) are ignored. No scan for viruses and malware is carried out. Only trusted URLs should therefore be excluded from WebGuard scans. Make sure no strings are entered with a concluding dot, as all URLs with a corresponding top-level domain are excluded from WebGuard scans.

Add Rule

The button allows you to copy URLs (Internet addresses) from the input field into the display window.

Delete

The button deletes a selected entry from the list. This button is inactive if no entry is selected.

Examples: Excluded URLs

- `www.domainname.com` = All pages from the URL, such as www.domain.com/page/ are excluded from WebGuard scans.
- `domainname.com` = All pages of the URL and all subdomains of the URL are excluded from WebGuard scans; www.domain.com/page/, www.subdomain.domain.com/
- `Lavasoft.` = All websites with the second-level domain Lavasoft are excluded from WebGuard scans: www.Lavasoft.de, www.Lavasoft.com
- `net` = All websites with the .net top-level domain are excluded from WebGuard scans: www.name1.net, www.name2.net

---

Heuristic

This configuration section contains the settings for the heuristic of the Lavasoft Anti-Virus Helix search engine.

Lavasoft Anti-Virus Helix contains very powerful heuristics that can uncover even unknown (new) viruses, worms and Trojans. This occurs through an extensive analysis and investigation of the affected codes for functions typical of viruses, worms or Trojan horses. If the code being scanned exhibits these characteristic features, it is reported as being suspicious. This does not necessarily mean that the code is in fact a virus, worm or Trojan horse. False positives do sometimes occur. The decision on how to handle affected code is to be made by the user, e.g. based on his or her knowledge of whether the source of the code is trustworthy or not.

Macrovirus Heuristic

Lavasoft Anti-Virus Helix contains a highly powerful macrovirus heuristic. If this option is enabled, all macros are deleted if repair is possible. Alternatively, suspect documents may simply be reported, i.e. you will receive an alert. This option is enabled as the default setting and is recommended.

Win32 File Heuristic

Lavasoft Anti-Virus Helix contains a very powerful heuristic for detecting viruses, worms and Trojan horses in Windows. It is also able to detect unknown viruses, worms and Trojans. If this option is activated, you can define how "aggressive" this heuristic should be. This option is activated by default.

Low Detection Level

If this option is enabled, Lavasoft Anti-Virus Helix identifies fewer viruses, worms and Trojan horses, but there is less risk of potential false positives.

Medium Detection Level

This setting is activated by default if you have selected the use of this heuristic.

High Detection Level

If this option is enabled, Lavasoft Anti-Virus Helix identifies a large number of unknown viruses, worms and Trojan horses, but you must also accept that there are likely to be false positives.

Report

WebGuard includes an extensive logging function to provide the user or administrator with exact notes about the type and manner of a detection.

Logging

This group allows for the content of the report file to be determined.

Off

If this option is enabled, then WebGuard does not create a log. It is recommended that you turn off the logging function only in exceptional cases, such as if you are executing trials with multiple viruses or unwanted programs.

Default

If this option is enabled, WebGuard records important information (concerning detections, alerts and errors) in the report file, with less important information ignored for improved clarity. This option is activated by default.

Extended

If this option is enabled, WebGuard logs less important information to the report file as well.

Complete

If this option is enabled, WebGuard logs all available information in the report file, including file size, file type, date, etc.

Limit Report File

Limit Size to n MB

If this option in enabled, the report file is restricted to a specific size. Permitted values are between 1 and 100 MB. This option is activated by default with a value of 1 MB. Up to 50 kilobytes of extra space are allowed to minimise the use of system resources. If the size of the log file exceeds the indicated size by more than 50 kilobytes, old entries are then deleted until the indicated size minus 50 kilobytes is attained.

Write Configuration in Report File

If this option is enabled, the configuration of the on-access scan is recorded in the report file.

General

Email

Lavasoft Anti-Virus Helix can send messages via e-mail. This is done with the Simple Message Transfer Protocol (SMTP).

The messages can be triggered by various events. Transmission of e-mail is supported by the following modules:

- Examination enquiries of suspicious files to the Lavasoft Malware Research Center

Note
Please note that ESMTP is not supported. In addition, an encrypted transfer via TLS (Transport Layer Security) or SSL (Secure Sockets Layer) is currently not possible.

E-mail messages

SMTP Server

Enter the name of the host to be used here - either its IP address or the direct host name.
The maximum possible length of the host name is 127 characters.

For example:

192.168.1.100 or mail.musterfirma.de.

Sender Address

In this input box, enter the e-mail address of the sender. The maximum length of the sender's address is 127 characters.

Authentication

Some mail servers expect a program to verify itself to the server (log in) before an e-mail is sent. Lavasoft Anti-Virus Helix can transmit alerts with authentication to the SMTP server via e-mail.

Use Authentication

If this option is enabled, a user name and a password can be entered in the relevant boxes for login (authentication).

- **User name**: Enter your user name here.
- **Password**: Enter the relevant password here. The password is saved in encrypted form. For security, the actual characters you type in this space are replaced by asterisks (*).

Send test e-mail

When you click on the button, Lavasoft Anti-Virus Helix attempts to send a test e-mail to the sender address to check the data entered.

Extended Threat Categories

Lavasoft Anti-Virus Helix protects you against computer viruses. In addition, you can scan according to the following extended threat categories:

- Backdoor control software (BDC)

- Dialer
- Games (GAMES)
- Joke programs (JOKES)
- Security Privacy Risk (SPR)
- Adware/Spyware (ADSPY)
- Unusual runtime packers (PCK)
- Files with hidden file endings (HEUR-DBLEXT)
- Phishing
- Application (APPL)

By clicking on the relevant box, the selected type is enabled (check mark set) or disabled (no check mark).

Enable All

If this option is enabled, all types are enabled.

Default Values

This button restores the predefined default values.

Note
If a category is disabled, files recognized as being of the relevant program type are no longer indicated. No entry is made in the report file.

Password

You can protect Lavasoft Anti-Virus Helix in different areas with a password. If a password has been issued, you will be asked for this password every time you want to open the protected area.

Enter Password

Enter your required password here. For security reasons, the actual characters you type in this space are replaced by asterisks (*). The password can only have a maximum of 19 characters. Once the password has been issued, the program refuses access if an incorrect password is entered. An empty box means "No password".

Confirm Password

Confirm the password entered above by entering it again. For security reasons, the actual characters you type in this space are replaced by asterisks (*).

Note
Passwords are case-sensitive.

Areas protected by password

Lavasoft Anti-Virus Helix can protect individual errors with a password. By clicking on the relevant box, the password request can be disabled or reactivated for individual areas as required.

Password-protected area	Function
Control Center	If this option is enabled, a password is required to start the Control Center.

Enable / disable Guard	If this option is enabled, the pre-defined password is required to enable or disable the Anti-Virus Guard.
Enable / disable MailGuard	If this option is enabled, the pre-defined password is required to enable/disable the MailGuard.
Enable/disable WebGuard	If this option is enabled, the pre-defined password is required to enable/disable the WebGuard.
Adding and changing jobs	If this option is enabled, a password is required when adding and changing jobs in Scheduler.
Start product updates	If this option is enabled, a password is required to start the product update in the update menu.
Quarantine	If this option is enabled, all possible areas of the quarantine manager protected by a password are enabled. By clicking on the relevant box, the password enquiry can be disabled or enabled again on request for individual areas.
Restore affected objects	If this option is enabled, a password is required to recover an object.
Repairing affected objects	If this option is enabled, a password is required to repair an object.
Properties of affected objects	If this option is enabled, a password is required to display the properties of an object.
Deleting affected objects	If this option is enabled, a password is required to delete an object.
Configuration	If this option is enabled, configuration of Lavasoft Anti-Virus Helix is only possible after entering the pre-defined password.
Enable expert mode	If this option is enabled, a password is required to enable expert mode.
Installation / Uninstallation	If this option is enabled, a password is required for installation or uninstallation of Lavasoft Anti-Virus Helix.

Security

Update

Alert If Last Update Older Than n Day(s)

In this box you can enter the maximum number of days allowed to have passed since the last update of Lavasoft Anti-Virus Helix. If this number is exceeded, a warning is displayed in the Scheduler.

Show Notice if the Signature Database with Detection Patterns is Out of Date

If this option is enabled, you will obtain an alert message if the virus definition file is not up to date. With the help of the alert option, you can configure the temporal interval for an alert message if the last update is older than n day(s).

Protect configuration file against unwanted modifications

Protect Configuration

If this option is enabled, the Lavasoft Anti-Virus Helix Configuration can only be saved with administrator rights.

Warning
This option is only effective if Lavasoft Anti-Virus Helix is installed on an NTFS partition.

Protect Job Files

When this option is enabled, only a user with administrator rights can change existing scanning and update jobs and protect jobs that he or she has created.

Protect processes

Prevent Anti-Virus Processes from Being Terminated

If this option is enabled, the anti-virus processes are protected against unwanted termination by viruses and malware or against 'uncontrolled' termination by a user e.g. via Task Manager. This option is enabled by default.

Important
Protection is not yet available for 64-bit systems!

Directories

Temporary path

In this input box, enter the temporary path with which Lavasoft Anti-Virus Helix works.

Use Default System Settings

If this option is enabled, the settings of the system are used for handling temporary files.

Note
You can see where your system saves temporary files - for example with Windows XP - under: Start | Settings | Control Panel | System | Index card "Advanced" | Button "Environment Variables". The temporary variables (TEMP, TMP) for the currently registered user and for system variables (TEMP, TMP) are shown here with their relevant values.

Use Following Directory

If this option is enabled, the path displayed in the input box is used.

The button opens a window in which you can select the required temporary path.

Default

The button restores the pre-defined directory for the temporary path.

Update

The **Update section** of the Lavasoft Anti-Virus Helix Configuration is responsible for the configuration of the Updater .

Product Updates

Download and Automatically Install Product Updates

If this option is enabled, product updates are downloaded and automatically installed by the Anti-Virus Updater as soon as updates become available. Updates to the virus definition file and search engine always function independently of this setting. The conditions for this option are: complete configuration of the update and an open connection to a download server.

Notification When New Product Updates are Available

If this option is enabled, you will be notified by e-mail when new product updates become available. Updates to the virus definition file and search engine are carried out independently of this setting. The conditions for this option are: complete configuration of the update and an open connection to a download server. You will receive notifications via a desktop popup window and via a warning message from Anti-Virus Updater in the Control Center under Manager ::Scheduler.

Do Not Download Product Updates

If this option is enabled, no automatic product updates or notifications of available product updates by the Anti-Virus Updater are carried out. Updates of the virus definition file and the search engine are always carried out independently of this setting.

Important
An update of the virus definition file and of the search engine is carried out during every update process independent of the settings for the product update (see Updates).

Web server

The update can be performed directly via a web server on the Internet.

Web Server Connection

Use Existing Connection (Network)

This setting is displayed if your connection is used via a network.

Use the Following Connection:

This setting is displayed if you define your connection individually.

The Lavasoft Anti-Virus Helix Updater automatically detects which connection options are available. Connection options which are not available are grayed out and cannot be activated. A dial-up connection can be established manually via a phone book entry in Windows, for example.

- **User:** Enter the user name of the selected account.
- **Password:** Enter the password for this account. For security, the actual characters you type in this space are replaced by asterisks (*).

Note
If you have forgotten an existing Internet account name or password, contact your Internet Service Provider.

Note
The automatic dial-up of the updater through dial-up tools (e.g. SmartSurfer, Oleco, etc.) is currently not available in Lavasoft Anti-Virus Helix.

Terminate a Dial-Up Connection that was Set Up for the Update

If this option is enabled, the RDT connection made for the update is automatically interrupted again as soon as the download has been successfully carried out.

Proxy

Do Not Use a Proxy Server

If this option is enabled, your connection to the web server is not carried out via a proxy server.

Use Windows System Settings

When the option is enabled, the current Windows system settings are used for the connection to the web server via a proxy server.

Use the Following Proxy Server

If your web server connection is set up via a proxy server, you can enter the relevant information here.

Address

Please enter the URL or the IP address of the proxy server you should use to connect to the web server.

Port

Please enter the port number of the proxy server you should use to connect to the web server.

Login Name

Enter your login name for the proxy server here.

Login Password

Enter the relevant password for logging in on the proxy server here. For security, the actual characters you type in this space are replaced by asterisks (*).

Examples:

Address:	proxy.domain.com	Port:	8080
Address:	192.168.1.100	Port:	3128

Events

Limit Maximum Number of Events to n Entries

If this option is enabled, the maximum number of events listed in the event database can be limited to a certain size; possible values: 100 to 10,000 entries. If the number of entered entries is exceeded, the oldest entries are deleted.

Delete Events Older than n Day(s)

If this option is enabled, events listed in the event database are deleted after a certain period of time; possible values: 1 to 90 days. This option is enabled as the default setting, with a value of 30 days.

Do Not Limit Size of Event Database (Delete Events Manually)

When this option has been activated, the size of the event database is not limited. However, in the Control Center under Events, a maximum of 20,000 entries are displayed.

Limit reports

Limit Number of Reports

Limit the Number to n Units

When this option is enabled, the maximum number of reports can be limited to a specific amount. Values between 1 and 300 are permissible. If the specified number is exceeded, then the oldest report at that time is deleted.

Delete All Reports More Than n Day(s) Old

If this option is enabled, reports are automatically deleted after a specific number of days. Permissible values are between 1 and 90 days. This option is enabled by default with a value of 30 days.

Do Not Limit Number of Reports (Manually Delete Reports)

If this option is enabled, the number of reports is not restricted.

Tray Icon

The tray icon in the system tray of the taskbar displays the status of the Guard service.

Entries in the Context Menu

- **Activate Anti-Virus Guard:** enables or disables the Lavasoft Anti-Virus Helix Guard.
- **Start Anti-Virus:** opens the Lavasoft Anti-Virus Helix Control Center.
- **Configure Anti-Virus**: opens the Lavasoft Anti-Virus Helix Configuration.
- **Start update**: starts an update.
- **Help:** opens this online help.
- **Lavasoft on the Internet**: Opens the web portal of Lavasoft Anti-Virus Helix on the Internet. The condition for this is that you have an active connection to the Internet.

Updates

The effectiveness of anti-virus software depends on how up-to-date the program is, in particular the virus definition file and the search engine. To carry out updates, the component Anti-Virus Updater is integrated into Anti-Virus Helix. Anti-Virus Updater ensures that Lavasoft Anti-Virus Helix is always up-to-date and able to deal with the new viruses that appear every day. Anti-Virus Updater updates the following components:

- Virus definition file:

The virus definition file contains the virus patterns of the harmful programs used by Anti-Virus Helix to scan for viruses and malware and repair infected objects.

- Search engine:

The search engine contains the methods used by Anti-Virus Helix to scan for viruses and malware.

- Program files (product update):

Update packages for product updates make extra functions available to the individual program components.

An update checks whether the virus definition file and search engine are up-to-date and, if necessary, implements an update. Depending on the settings in the configuration, the Anti-Virus Updater also carries out a product update or informs you of the product updates available. After an update, Anti-Virus Helix does not have to be restarted.

Note

For security reasons, the Lavasoft Anti-Virus Helix Updater checks whether the Windows host file of your computer was altered to the effect that, for example, the Lavasoft Anti-Virus Helix update URL was manipulated by malware and diverts the Lavasoft Anti-Virus Helix Updater to unwanted download sites. If the Windows host file has been manipulated, this is shown in the Lavasoft Anti-Virus Helix Updater report file.

In the Control Center under Scheduler, you can organize update jobs which are carried out by Anti-Virus Updater at the intervals stipulated. An update job is created by default after installation of Anti-Virus Helix. You also have the option to start an update manually:

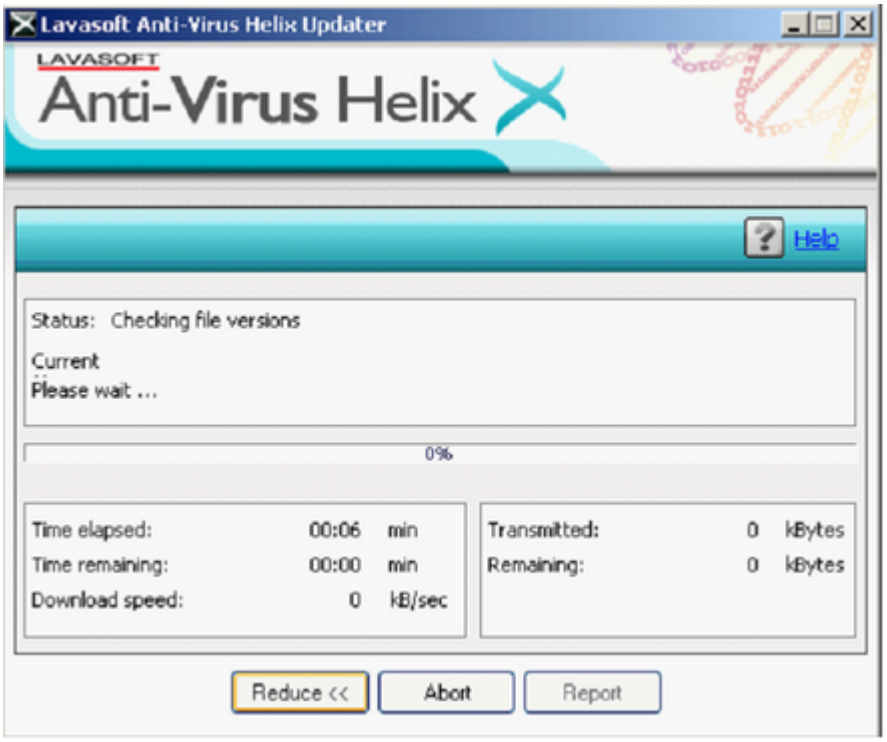
- in the Control Center, in the Update menu and in the Status section
- via the context menu of the tray icon

Updates can be obtained from the Internet via a Web server of the manufacturer. The existing network connection is the default connection to the download servers of Lavasoft. You can change this default setting in Lavasoft Anti-Virus Helix's Configuration under General:: Update.

Updater

The Lavasoft Anti-Virus Helix Updater window opens at the start of an update.

Lavasoft Anti-Virus Helix Updater



Note
For update jobs created in the Scheduler, you can define the display mode for the update window; you can select **Hide**, **Minimize** or **Maximize**.

Note
If you are using a program in full screen mode (e.g. games) and the updater's display mode is set to maximized or minimized, the updater will switch to the desktop. To prevent this, start the updater with the display mode set to hide. In this mode you will no longer be notified about updates by the update window.

Status

Shows how the updater is proceeding.

Current File

Name of the file which is currently being downloaded.

Time Elapsed

Time which has elapsed since starting the download.

Estimated Time Remaining

Time until download is finished.

Download Speed

Speed of download.

Downloaded Bytes

Bytes already downloaded.

Remaining Bytes
Bytes left to download.

Buttons and Links

Button / link	Description
	This page of the online help is opened via this button or link.
Reduce	The display window of the updater will appear in a reduced size.
Enlarge	The display window of the updater will be re-established to its original size.
Abort	The update procedure will be canceled. The updater will be closed.
Close	The update procedure is completed. The display window will be closed.
Report	The report file of the update is displayed.

Index

- S -

- T -

- U -

- V -

- W -