Ad-Aware\textsuperscript{11}
Product Manual

Fast antivirus engine that works alongside our legendary anti-spyware technology in one superfast security solution.

Advanced malware protection built upon our legendary anti-spyware and antivirus technology that shields you against the latest cyber threats and real-time web-filtering technology that safeguards your PC against phishing attacks and online scams.
# Table of Contents

Product Information ................................................................................................................................. 4
Ad-Aware Features ................................................................................................................................. 4
System Requirements ............................................................................................................................. 5
Copyright .................................................................................................................................................. 6
Installation and Uninstallation .................................................................................................................. 7
Ad-Aware Install ...................................................................................................................................... 7
Ad-Aware Uninstall ............................................................................................................................... 20
Ad-Aware Overview ............................................................................................................................... 24
User Interface and Operation .................................................................................................................... 24
Status Bar ................................................................................................................................................ 26
Using Ad-Aware .................................................................................................................................... 28
Configuring Settings ............................................................................................................................... 28
  Real-Time Protection .......................................................................................................................... 28
  Web Protection .................................................................................................................................... 30
    Anti-Phishing .................................................................................................................................... 31
    Parental Control .............................................................................................................................. 31
    Predefined Sets ............................................................................................................................... 33
    Custom Settings .............................................................................................................................. 35
    Security Code .................................................................................................................................. 37
Email Protection ...................................................................................................................................... 40
Network Protection ............................................................................................................................... 42
  Advanced Settings ............................................................................................................................. 43
    Application Rules ............................................................................................................................ 45
    Adapter Settings ............................................................................................................................. 48
Scanning System .................................................................................................................................... 51
  About Scan ......................................................................................................................................... 51
  Running a Scan ................................................................................................................................. 52
  Quarantined Items .............................................................................................................................. 58
Reports .................................................................................................................................................... 59
Scheduling Scans ..................................................................................................................................... 61
Creating Exclusion List ........................................................................................................................... 62
Updating Definitions ............................................................................................................................... 64
Ad-Aware Settings .................................................................................................................................. 65
  System Notifications (Gaming Mode) ............................................................................................... 66
  System Reset ...................................................................................................................................... 67
Ad-Aware Command Line Scanner .....................................................................................................................................................92

How To ................................................................................................................................................................................................75

Scan .................................................................................................................................................................................................96
Download Definitions .....................................................................................................................................................................94
Action List .......................................................................................................................................................................................93
Find Ad-Aware Command Line Scanner with Command Prompt ..................................................................................................92
Start Command Prompt as Administrator ......................................................................................................................................92
Get Help ..........................................................................................................................................................................................88

Ad-Aware Command Line Scanner .....................................................................................................................................................92
Getting Started .................................................................................................................................................................................92
Start Command Prompt as Administrator ......................................................................................................................................92
Find Ad-Aware Command Line Scanner with Command Prompt ..................................................................................................92
Action List .......................................................................................................................................................................................93
Download Definitions .....................................................................................................................................................................94
Scan..................................................................................................................................................................................96
    Quick Scan .....................................................................................................................................................................................96
    Full Scan....................................................................................................................................................................................98
    Custom Scan ...........................................................................................................................................................................99
    Scan Boot Sectors .................................................................................................................................................................102
Delete Action .............................................................................................................................................................................104
Quarantine Action ....................................................................................................................................................................106
Disinfect Action .......................................................................................................................................................................108
Specify Scan Result Path ..........................................................................................................................................................110
Product Information ..................................................................................................................................................................112
Definitions Information ..............................................................................................................................................................113
Check for Product Updates..........................................................................................................................................................114
Product Information

Welcome to Ad-Aware 11!

Ad-Aware is a security solution that allows you to combat stealthy online threats and the latest advancements by cyber criminals. Ad-Aware protects you from malware that secretly takes control of your computer, resulting in aggressive advertising pop-ups, sluggish computer activity and even identity theft through stolen private information. Ad-Aware allows you to root out hazardous content on your system, clearly identify the threat level, and gives you the ability to remove or block harmful applications and processes, so that your private information remains right where it should – under your control. With Ad-Aware, you can keep an eye on your credit file activity and monitor a potential fraud. Ad-Aware provides complete malware protection against viruses, spyware, trojans, rootkits, blended malware, hijackers, keyloggers, and other potential cyber threats, giving you the power to protect your online security and privacy – so that you can use the Internet how, when, and where you want.


Please follow the guidelines set forth in this most recent edition of the Manual to facilitate the work with Ad-Aware.

Ad-Aware Features

Ad-Aware is an easy-to-use and effective anti-malware and anti-virus Lavasoft product comprising high-class technologies which give you an unequalled protection against various kinds of viruses and malware.

Learn about the Ad-Aware key features:

**Scan Computer** (Free, Personal, Pro, Total)

Completely and correctly scans your computer for malicious software like blended malware, trojans, worms, backdoors, rootkits, hijackers, and invasive software like password stealers, monitoring tools, keyloggers and other applications that transmit private or personally identifiable information.

**Real-Time Protection** (Free, Personal, Pro, Total)

Constantly watches the vulnerable areas of the computer and reacts to suspicious activity in real time. Monitors the change, deletion or modification of the files and also the execution and loading of programs and DLLs.

**Gaming Mode** (Free, Personal, Pro, Total)
Suspends the security alerts, system scans and auto-updates without compromising the security, allowing you to work or play with no interruptions or strain on system resources.

**Web Protection** (Personal, Pro, Total)

Internet filter and parental control software for your PC. It offers a security against a wide range of web-based threats, including the entry of malware, phishing, pharming and intrusions.

**Email Protection** (Pro, Total)

Protects against e-mail-borne threats by scanning both the content and the attachment of all incoming and outgoing emails against potentially malicious content.

**Network Protection** (Pro, Total)

Effectively filters network traffic, prevents malicious behavior, protects running processes and filters web content.

**Parental Control** (Total)

Helps you filter inappropriate content by restricting access to the Internet. Allows blocking your child from accessing adult-oriented websites.

System Requirements

You may install the Ad-Aware antivirus only on computers running the following operating systems:

- Windows XP with Service Pack 3 (32-bit), Service Pack 2 (64-bit)
- Windows Vista with Service Pack 2 (32- & 64-bit)
- Windows 7 with Service Pack 1 (32- & 64-bit)
- Windows 8, 8.1 (32- & 64-bit)

4.5 or higher version of Microsoft Windows Installer is required for installation of Ad-Aware antivirus.

Your computer must meet the following system requirements in order to run the application effectively.
Minimum system requirements:
1.8 GB available free hard disk space (at least 800 MB on the system drive)
800 MHz processor
1 GB of memory (RAM)

Recommended system requirements:
2.8 GB available free hard disk space (at least 800 MB on the system drive)
Intel CORE Duo (1.66 GHz) or equivalent processor
Memory (RAM): 1 GB for Windows XP and 1.5 GB for Windows Vista, Windows 7 and Windows 8

Copyright
To get full information about the Ad-Aware program:

- On the floating panel, click the Info icon.

With the dialog displayed, learn more about the program.

To close the dialog, click a little cross in the upper right-hand corner of the dialog or just click in the content pane.
Installation and Uninstallation

Ad-Aware Install

Ad-Aware Uninstall

Ad-Aware Install

The installation process of Ad-Aware allows you to select the nature of installation that suits your needs the best:

- Default Install: An intelligent installation mode that automatically determines what to install for optimal configuration adapted to your PC.

- Compatible Install: Installation as a second line of defense if you already have another antivirus on the PC. Ad-Aware then enhances a protection by defaulting to Compatible Mode, adding a second layer of protection.

Moreover, you have an option to install Safe Browsing Add-on and select an application language.

You can install the application in less than ten steps. Time to get started!

Step 1

To start the installation, locate and click the link to download a file.

Step 2

When prompted, save the installer file.

Step 3

Once the download is complete, go to the downloaded path and double-click the installation file to launch an Ad-Aware Web Installer.

The Ad-Aware Web Installer downloads and runs the Ad-Aware Updater.
The Ad-Aware Updater does not run if you have a version of Windows Installer earlier than 4.5. Mostly, Windows XP users can face the problem. Your system is updated automatically. Wait until the installation process is completed. Afterwards, the Ad-Aware Updater automatically runs.

Step 4

Follow the prompts within the installer to complete the installation of Ad-Aware.

1. Start by selecting the language you prefer to use for the installation process from the drop-down combo box at the right of the dialog displayed.

In addition, you can change the default application installation directory by clicking the Browse button.

Warning: You are not allowed to manually type the directory into the text box.

With the screen, you can also create a desktop icon by selecting the corresponding check box.
2. We strongly recommend to read the **End-User License Agreement** carefully before downloading, installing and using Ad-Aware. To read the antivirus software document, click a corresponding link on the screen:
3. Then select an install type depending on your needs:

- Select the **Install as a second line of defense only** check box to install the application as a second line of defense if you already have another antivirus on the PC or you prefer to use the Scan Computer option only.

- Click **Start Install** to install the application with default settings. The default destination folder to install the application is `C:\Program Files\Lavasoft\Ad-Aware Antivirus`.

**Compatible Install**

Once you select the **Install as a second line of defense only**, the following message box displays:
Click **Yes** to accept the prompt. The **Start Install** button is replaced with the **Compatible Install** button.
Once you click **Compatible Install**, the installation continues and no drivers are installed. If any Ad-Aware drivers were installed earlier, they are removed.

If an incompatible program is detected, Ad-Aware antivirus installation as a 2nd line of defense starts. No drivers are installed. If any Ad-Aware drivers were installed earlier, they are removed.

If the prompt is accepted and no incompatible program is detected, the installation continues and no drivers are installed. If any Ad-Aware drivers were installed earlier, they are removed.

**Default Install**

Once you click **Start Install**, you are proposed to install additional download for your browser: **Safe Browsing Add-on**.

If you have the download already installed on your PC, Ad-Aware Antivirus installation starts immediately by clicking **Start Install**.

The **Start Install** button is not available if Ad-Aware has detected any incompatible software. Then you have only an option to install Ad-Aware in the Compatible mode.
4. You can install an additional download for your browser both for Compatible and Default install: *Safe Browsing Add-on*. On the screen that displays, select a preferred option(s) and click **Next** to proceed.

If you do not want to install the toolbar, make *Lavasoft SecureSearch* your browser’s default search provider or set new tabs and homepage as *Lavasoft SecureSearch*, click **Skip**, or unselect corresponding check boxes, and then click **Next**.

*Ad-Aware Browsing Protection, which blocks phishing and malware sites, is installed together with Ad-Aware Antivirus as a standalone module. It is present in the Programs and Features list in Control Panel.*

5. You can see the *Ad-Aware* installation process in progress.
6. Afterwards, the *Ad-Aware Service* is initialized.
7. **Definition Files** then start downloading.
If you skip the step, definition files continue downloading in the background. To see the downloading process, launch the application after its installation.

8. Once Definition Files are downloaded, they are applied.
9. After applying *Definition Files*, your computer is scanned for viruses. A quick automatic scan starts.
If you skip the step, a quick scan is performed in the background. To see the scanning process, launch the application after its installation.

10. **Congratulations!** The *Ad-Aware* application has been successfully installed on your PC.
11. To complete the installation, you must restart your computer. With the screen displayed, click **Reboot Now**.

Your computer reboots and *Ad-Aware* is completely installed.

*If you have installed *Ad-Aware* in the **Compatible** mode, reboot is not required.*
Ad-Aware Uninstall

To uninstall Ad-Aware, first make sure the application is closed.

1. Click the Start button on your computer (left-hand side of the screen).

2. Click Control Panel in the Start Menu.

3. Double-click Add or Remove Programs / Click Programs, and then click Programs and Features. Select Ad-Aware Antivirus from the list and then click Uninstall.

*The programs installed are typically listed in an alphabetical order.*

4. With the dialog box displayed, click Remove to proceed.

5. With the message box displayed, confirm your decision to uninstall the program by clicking Yes.
6. You can see the uninstalling process in progress.
7. To complete the uninstalling process, click **Reboot Now**.
If you have installed Ad-Aware in the **Compatible** mode, reboot is not required.
Ad-Aware Overview

User Interface and Operation

Status Bar

User Interface and Operation

You can operate the Ad-Aware application via the following program interface elements:

1. **Caption panel**
   On the panel, you can see the program name. Use the Minimize and Close buttons to minimize or hide the application to the taskbar, or close the application. You may use the caption panel to move an application window by grabbing the title bar and dragging.

2. **Header**
   On the panel, you can see the program version and status bar indicating that computer is protected, at risk or threats are detected.

3. **Left menu**
   The menus purpose is to supply a common housing for the main application features. Click the menu element of your choice to access the required menu section.

4. **Breadcrumbs**
   Breadcrumbs are a navigation and effective visual aid that indicates your location within the application’s hierarchy. It allows you to keep track of your locations within Ad-Aware.
   Breadcrumbs reduce the number of actions you need to take to get to a higher-level screen, and they improve the find ability of the application's sections and screens.

5. **Back button**
   Gives you a way to return to the previous screen.

6. **Content pane**
   Once you click the menu element of your choice on the Left menu, a corresponding menu section opens.

7. **Floating panel**
To make the floating panel visible, click or move your pointer over the bottom edge of the application window for the panel to make it expanded. On the panel, you can see a logo and the following icons: alerts, info and help.
Status Bar

The Status Bar reports you the program functionality as well as helps monitoring all updates and promotional offers. To facilitate comprehensive monitoring result estimation, the status bar acquires a corresponding color. The following is an explanation of each computer status:

**Protected (Blue)** indicates the following:

- No threats are found.
- The Real-Time Protection and Email Protection features are enabled. The Definitions are up to date and the automatic threat definition updates are enabled.

**At risk (Orange)** indicates the following:

- Threat Definitions are out of date or the automatic threat definition updates are disabled or both.
- System scan date is too old or has never been performed.

**Protection Inactive (Red)** indicates that the Real-Time Protection feature is disabled.

To get a summary on problems found, open the Home screen. You can see a list of problems under the Notifications block.
Click View All to access the Notification center screen and learn more about problems.

Click Options next to the problem to apply one of the following actions:

1. Fix problem now (recommended)
2. Remind me later
3. Ignore (not recommended)
Using Ad-Aware

Configuring Settings

You can set and configure the Ad-Aware application features from the feature screen.

To access a specific feature screen, on the left menu, click the required menu element:

- Real-Time Protection
- Web Protection
- Email Protection
- Network Protection

When you start using your copy of Ad-Aware, make sure any other antivirus software is not installed on your PC. If you have other antivirus programs installed and run on your computer, a message box appears when you try to activate a feature of Ad-Aware which requires additional components to be installed: Real-Time Protection, Web Protection, Email Protection, and Network Protection.

To avoid compatibility issues, we strongly recommend uninstalling the software indicated in the message box appearing when you try to turn on the feature.

If not, you can continue with installing additional components to enable the feature.

With the message box displayed, click the Continue button, and then click the Ok button to start the installation process for enabling the feature you want to activate and configure. Be aware that this gives no guarantee against any further conflicts that may occur.

Real-Time Protection

The Real-Time Protection feature provides an automatic protection which monitors computer systems for suspicious activity such as malicious objects in real-time. While you are working with files, the Real-Time Protection is on in the background without causing noticeable strain to your computer system.

⚠️ If Real-Time Protection is turned on, ensure that you do not run another real-time protection software. If there is another real-time software running, the two programs running together may adversely affect your system performance.

⚠️ If Ad-Aware has detected any incompatible software, you need to install additional components to enable Real-Time Protection. For the purpose, click the slider and then continue installing additional components.

To set and configure the Real-Time Protection feature, proceed through the steps listed below:

2. Click the slider next to **Real-Time Protection** to enable **Real-Time Protection**. At a time, the **Scan local files** and **Scan network files** features are enabled as well.

Alternatively, on the **Home** screen, click the slider next to **Real-Time Protection** to enable the feature.

You can disable the **Scan local files** feature or the **Scan network files** feature separately by clicking a corresponding slider. With that, the **Real-Time Protection** feature remains enabled.

If a local or network file is detected as a suspicious one, that file is added to **Quarantine**.
Web Protection

The web is the number one source of malware and the threats which get more varied and sophisticated every day. The *Web Protection* feature allows blocking the latest web threats and keep you safe from malicious sites. It implies an Internet filter and parental control for your computer.

To set and configure the *Web Protection* feature, proceed through the steps listed below:

1. On the left menu, click **Web Protection**. The *Web Protection* screen opens.

2. Click the slider next to **Web Protection** to enable *Web Protection*. At a time, the *Anti-Phishing* feature is enabled as well.

   *By clicking the slider, you activate the Ad-Aware Browsing Protection to be protected from phishing and malware.*

Alternatively, on the *Home* screen, click the slider next to **Web Protection** to enable the feature.
If Ad-Aware has detected any incompatible software, you need to install additional components to enable Web Protection. For the purpose, click the slider and then continue installing additional components.

To enable the Parental Control feature, click Activate Parental Control or click the slider next to Parental Control.

You can disable the Anti-Phishing feature or the Parental Control feature separately. With that, the Web Protection feature remains enabled.

**Anti-Phishing**

The Anti-Phishing feature helps keeping you safe online. It attempts to identify phishing content contained in websites and prevent fraudulent websites from masquerading as other legitimate web sites.

Once you turn on Anti-Phishing, the feature warns you when a page you visit has been reported as a "phishing" page and shows you a message.

**Parental Control**

The Parental Control feature monitors and tracks your child's online activity blocking dangerous sites. It is a good web filtering for parents looking to protect their kids from inappropriate or adult websites at home by setting content restrictions.

To enable the Parental Control feature, proceed through the steps listed below:

1. On the left menu, click Web Protection.

2. On the Web Protection screen, click the slider next to Parental Control.

3. To access the Parental Control Settings screen, click Advanced Settings.

4. On the Parental Control Settings screen, use the drop-down combo box to select a predefined set to block specific content.
If you want to create your own restrictions, proceed through the steps listed below:

1. In the drop-down combo box, select the **Custom** option.
2. In the **Custom Settings** block, click **Change Settings**.
3. With the **Custom Parental Control** screen, customize your set and/or create your own exclusion list to allow a specific web site if a category it belongs to is blocked.
For your convenience, we have created predefined sets to block specific web content. To learn more about these sets, see the table below:

<table>
<thead>
<tr>
<th>Set</th>
<th>Adults (21 and over)</th>
<th>Young Adults (under 21)</th>
<th>Teen (under 18)</th>
<th>Children Permissive (under 12)</th>
<th>Children Restrictive (under 12)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adult/Sexual</td>
<td></td>
<td></td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Pornography</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Mature Content</td>
<td></td>
<td></td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Online Dating</td>
<td></td>
<td></td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Computers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Web Proxy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Hacking</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Search Engines</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>File Sharing</td>
<td></td>
<td></td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Scams</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Regional TLDS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Video</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Cultures/Society</td>
<td></td>
<td></td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Religious</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Drugs/Alcohol/Tobacco use or abuse</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Drugs</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Narcotics</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Fraud/Illegal Activities/Cheating</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Illegal</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Hate</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Fraud/Illegal Activities/Cheating</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Games/Gambling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Games</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Casual Games</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Online Games</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Computer Games</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Gambling</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Health &amp; Medical</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Health</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>News</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tabloids</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Blogs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>News</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Web Content &amp; Social Networking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Videos Online</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Photos Online</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shopping</td>
<td></td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online Shop</td>
<td></td>
<td>+</td>
<td></td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>Online Pay</td>
<td></td>
<td>+</td>
<td></td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>Violence</td>
<td></td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Violent Cartoons</td>
<td></td>
<td>+</td>
<td></td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>Weapons</td>
<td></td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Custom Settings

Ad-Aware allows you to create your own set of restrictions to block access to specific sites. With that, you can create an exclusion list to allow a specific web site to be accessed if a category it belongs to is blocked.

Before settings customization, make sure the Parental Control feature is enabled.

To customize settings, proceed through the steps listed below:

1. With the Web Protection screen, click the slider next to Parental Control.

2. In the Parental Control block, click Advanced Settings.

3. On the Parental Control Settings screen, select Custom from the drop-down combo box.

4. With the Custom Settings block, click Change Settings.

5. With the Custom Parental Control screen, in the Customize slide box, select a category to customize by clicking the required caption. With the category expanded, select a check box to specify a subcategory.

![Custom Parental Control Screen](image.png)
6. Click the *Exclusions List* caption, to expand the slide box. With the *Exclusions List* slide box expanded, click the *Add URL* button to add the URL of the website from blocked category that you want allow access.

7. With the dialog box displayed, type the URL and then click *Add*. The URL is now displayed in the list.

To remove the URL from the list, select the check box it corresponds to and then click *Remove*. 
Security Code

To create a security code for the Parental Control feature, proceed through the steps listed below:

1. On the left menu, click Web Protection.

2. On the Web Protection screen, click the slider next to Parental Control.

3. In the Parental Control block, click Advanced Settings.

4. On the Parental Control Settings screen, click Insert your security code or click the slider next to Security pin.

5. With the message box displayed, type a 4 digit pin number, and then click the Submit button.

6. Type your email address to help retrieving your pin if you forget it or use the wrong one. Click the Submit button.

We strongly recommend complete the procedure by indicating your retrieval email. If you do not indicate the email for any reason and hide the application to the system tray, the message box for typing your retrieval email address is closed. Thus we cannot help retrieving your pin if you forget it or use the wrong one.
7. With the confirmation message box, click the **Close** button. The *Parental Control Login* is now enabled.

*Information: Once you have enabled the security code, you are asked to type your 4 digit pin each time you try to enable/disable the Parental Control or Web Protection feature and to access Advanced Settings of Parental Control.*

To customize security code settings, proceed through the steps listed below:

1. With the *Web Protection* screen, in the *Parental Control* block, click *Advanced Settings*.

2. With the message box displayed, type the security code, and then click the **Submit** button.

If you forgot your pin number, with the message box displayed, click **Forgot your key? Click here to resend it to retrieval email**. Your 4 digit pin is now sent to the email address you have indicated as a retrieval one. If you cannot find it in your Inbox, please check your Spam and Junk folders.

*Information: The retrieval email contains 4 digit pin presented as pictures. Make sure the feature to show pictures is enabled in your email client. Please remember the digits and type them to the corresponding fields in the message box.*
3. With the Parental Control Settings screen, click Change your security code, to type your new 4 digit pin with a message box displayed. Once you are done, click Submit.

4. With the confirmation message box, click the Close button. Your security code is now changed.

5. Click Change your retrieval email address, to type your new email address with a message box displayed. Once you are done, click Submit.

6. With the confirmation message box, click the Close button. Your retrieval email address is now changed.
The **Email Protection** feature allows you to shield email from malware, spam, and viruses filtering inbound messages. Once **Email Protection** is on, your email is automatically scanned behind the scenes.

To set and configure the **Email Protection** feature, proceed through the steps listed below:

1. On the left menu, click **Email Protection**. The **Email Protection** screen opens.

2. Click the slider next to **Email Protection** to enable **Email Protection**.

Alternatively, on the **Home** screen, click the slider next to **Email Protection** to enable the feature.

If Ad-Aware has detected any incompatible software, you need to install additional components to enable **Email Protection**. For the purpose, click the slider and then **continue** installing additional components.
Use the **Protection Level** drop-down combo box to select a level of the protection:

- Aggressive
- Normal
- Permissive

*Email Protection is available only for desktop email clients that use POP3/SMTP mail servers.*
Network Protection

Our two-way firewall complements and enhances the protection offered by your typical router and provides more robust security by monitoring which applications are attempting to send data out (outgoing traffic).

To set and configure the Network Protection feature, proceed through the steps listed below:


![Network Protection Screen](image)

2. Click the slider next to Network Protection to enable Network Protection.

Alternatively, on the Home screen, click the slider next to Network Protection to enable the feature.

If Ad-Aware has detected any incompatible software, you need to install additional components to enable Network Protection. For the purpose, click the slider and then continue installing additional components.

3. Click Advanced Settings to configure settings for Network Protection.
Advanced Settings

You can set and configure advanced settings for the Network Protection feature from the Advanced Settings screen.

To access the Advanced Settings screen, on the Network Protection screen, click Advanced Settings.

Here you can manage the following settings:

- **Internet connection sharing.** Click the slider to enable the protection of your internet connection from being shared without your consent.
- **Block port scans.** Click the slider to enable blocking hackers from scanning your computer ports.
- **Monitor process changes.** Click the slider to enable monitoring all process changes in applications and adapters for which you have created rules.
- **Default action.** Use the drop-down combo box to select a default action (Allow or Deny) to be applied to any program or zone, or both for which no rule has been created yet.
- **Application Rules.** Click the link to manage operations applied to your applications.
- **Adapter Settings.** Click the link to manage adapter(s) available on your PC.
Default action. Use the drop-down combo box to select a default action (Allow, Deny or Prompt). Allow and Deny actions are applied to any program or zone, or both for which no rule has been created yet. If the Prompt action is selected, you are prompted to apply Allow or Deny action for any application, when it is trying to access network/internet.

Once Allow or Deny action is applied, the corresponding application rule is automatically created. When the application accesses network/internet next time, you are not prompted again.
On the Application Rules screen, you can configure access to your network from applications installed on your PC by creating your own rules.

To access the Application Rules screen, on the Advanced Settings screen, click Manage in the Application Rules block.

Here you can add, edit or remove rules to be applied to the applications installed on your PC.

To add a rule, click Add. With the Add Rule screen displayed, specify the required parameters and click Save.
- **Program Path**: Click **Browse** and select the application the rule applies to.

- **Local Address**: Select the **Any** check box if you want to allow or deny traffic for any local address. If you clear the check box, the **IP** and **Port** text boxes become available for specifying the parameters. You are allowed to type only one value for **IP** address, and several values separated by a comma or a range of values using dash for **Port**.

- **Remote Address**: Select the **Any** check box if you want to allow or deny traffic for any remote address. If you clear the check box, the **IP** and **Port** text boxes become available for specifying the parameters. You are allowed to type several values separated by a comma for **IP** address, and several values separated by a comma or a range of values using dash for **Port**.
• **Protocol**: Select the **Any** radio button to include all IP protocols. Select the **TCP** radio button to enable two hosts to establish a connection and exchange streams of data. TCP - Transmission Control Protocol - guarantees data and guarantees delivery of packets in the same order they have been sent. Select the **UDP** radio button to use User Datagram Protocol that is an IP-based transport designed for high performance. It is often used by games and other video-based applications. Select the **Other** radio button and indicate a number to represent a specific IP protocol (other than TCP and UDP).

• **Direction**: Select from the drop-down combo box the traffic direction the rule applies to.
  - **Outbound** means that the rule applies only for the outgoing traffic.
  - **Inbound** means that the rule applies only for the incoming traffic.
  - **Both** means that the rule applies in both directions.

• **IP Version**: Select from the drop-down combo box suitable IP address format: IPv4, IPv6, or Any.

• **Permission**: Select from the drop-down combo box an option to allow or deny application access to the network or Internet under the specified circumstances.

To edit a rule, select it in the application rules list, and then click **Edit**. With the **Add Rule screen** displayed, modify the parameters previously set, and click **Save**.

To delete a rule, select it in the application rules list, and then click **Remove**.
On the **Adapter Settings** screen, you can manage adapter settings.

To access the **Adapter Settings** screen, on the **Advanced Settings** screen, click **Manage** in the **Adapter Settings** block.

Here you can see adapter(s) found on your PC. To edit an adapter, click **Edit** next to it. The **Adapters** screen opens:
To add a zone, click **Add**. With the dialog displayed, type IP address and select an action (Allow or Deny), and then click **Save**.

To edit a zone, select it in the zone list, and then click **Edit**. With the **Add Zone** screen displayed, modify the parameters previously set, and click **Save**.

To delete a zone, select it in the zone list, and then click **Remove**.
In addition, you can specify a *Stealth* mode status. On the drop-down combo box, select an option of your choice:

- **On**: your computer is invisible from both the local network and the Internet.
- **Off**: anyone from the local network or the Internet can ping and detect your computer.
- **Remote**: your computer cannot be detected from the Internet. Local network users can ping and detect your computer.
Scanning System

About Scan

Scanning is considered to be a process of reading drives on your PC to detect threats with further quarantining or removing those threats. You can specify areas or files or both to be scanned on your computer.

The following scopes of a scan process are supported by the *Ad-Aware Antivirus* application:

**Quick Scan**

A *Quick Scan* is the fastest and easiest way to scan commonly affected areas of your computer. It saves your time in detecting active malware by taking just a fraction of the system resources needed by a regular virus scan. This option performs a fast scan of your system and checks only running processes in memory, susceptible registry keys, and cookies.

**Full Scan**

A *Full Scan* performs a thorough scan process on your computer checking all its areas.

**Custom Scan**

A *Custom Scan* is a network audit based on parameters, which you configure: running processes, registry files, cookies, and particular drives and folders, etc.
Running a Scan

You can run:

- quick scan
- full scan
- custom scan

To perform a scan of any type, on the left menu, click **Scan Computer**. With the screen displayed, click an option of your choice:

- **Quick Scan** to launch a quick scan.
- **Full Scan** to launch a full scan.

Alternatively, to run a quick scan, on the Home screen, click the Scan button.

To perform a **Custom Scan**, proceed through the steps listed below:

1. On the left menu, click **Scan Computer**.
2. With the screen displayed, click the **Custom Scan**.
3. On the **Custom Scan Settings** screen, specify scan option(s), as needed, by selecting corresponding check box(es).
4. To select a drive/a folder/a file to scan, click the **Add** button and specify a drive/a folder/a file to be scanned.
5. To remove an item from the **Paths** section, select the check box and click the **Remove** button.
6. Once you are done, click **Start Scan** to launch a custom scan.

You can start the **Context Menu** scan. For the purpose, right-click one or more files or folders from Windows Explorer, and then click **Scan with Ad-Aware** to run a scan.
Once you start scanning, the balloon appears notifying you that the Context Menu scan has been started. Click the View details link to open the application on the Scan Computer screen.

Your selected scan begins to run. A scan progress screen displays. You can view the progress of the scan. Pause the scan by clicking the Pause button. To resume the scan after a pause, click the Resume button. If you want to cancel scanning, click the Stop button.

After the scan is performed or canceled, and no threats are found, Ad-Aware Antivirus opens the Scan Complete screen.
If you have performed a Quick Scan, the Scan Complete screen always displays even if any threats were found. If any threat is found during the Quick Scan, it is automatically deleted.

If risks are found, the Scan Summary screen displays the detected risks with the recommended clean actions (Quarantine, Ignore, Delete, or Disinfect). At a point in time when a threat is detected, a balloon appears with a corresponding notification.

To apply an action to a threat, select the required clean action from the drop-down combo box next to this threat.

The action applied to each threat by default is Quarantine.

To apply an action to all threats, select an option of your choice from the drop-down combo box next to the Clean button.

The action applied to all threat by default is Recommended that implies Quarantine.
Click the *Clean* button to start cleaning the risks based on the set action. You can view the progress of the cleaning process. Pause cleaning files by clicking the *Pause* button. To resume cleaning after a pause, click the *Resume* button. If you want to cancel cleaning, click the *Stop* button.
If no action is applied to risks found, Scan Summary displays each time you navigate to the Scan Computer screen or try perform a new scan.

Once the risks are cleaned, the Scan Complete screen displays the summary and details of the scan. Your computer is now clean of viruses and malware.
With the Scan Complete screen, you can view report by clicking the corresponding command button.

If the risks are quarantined, disinfected or deleted, message appears for users of Free Antivirus. It shows the exact number of blocked threats and gives an opportunity to visit Lavasoft official page on Facebook, to write a review on CNET or to buy Ad-Aware Pro version for discounted price. After following one of the links within the message box, it does not appear next time.
Quarantined Items

The Quarantine contains potentially harmful items detected by the Ad-Aware Antivirus application which you can further remove from your computer. It is a safe place for storing threats, malware and/or infected files that could not be disinfected. You have an option to restore a quarantined item back to your computer in its original location as well as permanently delete a quarantined item from your computer.

To access the quarantined items, proceed through the steps listed below:

1. On the left menu, click Scan Computer.
2. With the screen displayed, click the View Quarantined Files link available in the Quarantined Files block.

To restore a risk from the quarantine list, select a check box next to the threat and click the Restore button.

To delete a quarantined item from your computer, select a check box next to the threat you wish to delete and click Delete Selected. The item is permanently removed from your computer.

To view a full path the threat is located at, point the threat path.

To delete all quarantined items from your computer, click Delete All.

To view a full path the threat is located at, point the threat path.
Ad-Aware Antivirus creates a scan report after each manual or automated scan you perform.

To access the Scan Report List screen, proceed through the steps listed below:

1. On the left menu, click Scan Computer.
2. With the scan screen displayed, click the View Report List link available in the Report List block.

You can delete a report from the list. Select a check box next to this report, and then click the Delete button.

To view detailed information on a scan report, click Details in the report line. The Scanned Report Details screen displays.
Details are presented in the Report Details table. Here you can see three slide boxes: Overview, Scan Result, and Objects Detected. Each slide box contains specific report details. To expand a slide box, click in the slide box caption.

In addition, you are allowed to download a report as an XML file. For the purpose, click Download Report.
Scheduling Scans

You can schedule the scan process to run it periodically. It is very useful to keep your computer free from malware on a regular basis.

To enable the *Automated Scan* option and configure the schedule options, proceed through the steps listed below:

1. On the left menu, click **Scan Computer**.
2. With the screen displayed, scroll down until reaching the **Automated Scan** block, and then click the slider to turn on the automated scan and then click the **Edit Schedule** link to start configuring the schedule options.
3. With the screen displayed, specify the scheduling parameters listed below:
   - Frequency period to scan computer (*Daily*, *Weekly*, and *Monthly*). For the Weekly and Monthly parameters, select additionally day(s).
   - **Scan type** (*Quick* or *Full*).
   - Scan time.

You can disable the *Automated Scan* option by clicking the slider next to **Automated Scan** on the **Scan Computer** screen.
Creating Exclusion List

Create your *Exclusion List* of files if you want them to be excluded from the scan process and the real-time protection.

To access the *Manage Exclusions* screen, proceed through the steps listed below:

1. On the left menu, click *Scan Computer*.
2. With the screen displayed, click the *Manage Exclusions* link available in the *Manage Exclusions* block.

The *Manage Exclusions* screen opens:

With the *Manage Exclusions* screen, you can perform the following actions:

- add an item (path/extension) to the list;
- remove an item from the list.

To add a path to be excluded, click the **Add** button. With the *Open* dialog box displayed, select the path you want to add to the exclusion list, and then click **Open**.
To add an extension to be excluded, click the **Add** button. With the dialog box displayed, type an exclusion in the following format: *exe*, and then click **Add**.

![Enter Exception Type](image)

To remove an item, both a path and an extension, specify it in the list by selecting a corresponding check box and then click **Delete**.
Updating Definitions

Ad-Aware Antivirus uses continuously updated definitions to protect you from all sorts of malware. It is important to keep Ad-Aware Antivirus updated regularly.

To enable and configure the Update Definitions feature, proceed through the steps listed below:

1. On the left menu, click Scan Computer.
2. With the screen displayed, in the Definition Files block, click the Modify Settings link.
3. With the Definition Files Settings screen, click the slider to turn on the automatic download of definitions and then specify the frequency period (from 1 hour to 24 hours) for new threat definition to be checked.
4. To update threat definitions manually, click Check for updates.
Ad-Aware Settings

You can set and configure all of the *Ad-Aware* settings from the *App Management* screen.

To access the *App Management* screen, on the left menu, click **App Management**. Here you can manage the following settings:

- Gaming Mode
- System Reset
- Notification Center
- Ignored Notifications
- Language
- Activate
- Update
System Notifications (Gaming Mode)

If you do not want to receive any pop-up notifications about threats available, etc. while playing a game, activate the Gaming Mode.

To enable the Gaming Mode, proceed through the steps listed below:


2. In the System Notifications (Gaming Mode) block, click the slider to enable the feature.
System Reset

If you want to restore Ad-Aware to default settings, proceed through the steps listed below:

1. On the left menu, click **App Management**. The **App Management** screen opens.

   ![App Management Screen](image.jpg)

   2. In the **System Reset** block, click **Reset All**.

   *If you have the **Security pin** option for the **Parental Control** feature enabled, you are asked to type 4 digit pin number when attempting to reset all settings to default.*
Notification Center

To access a Notification Center, proceed through the steps listed below:

1. On the left menu, click **App Management**.
2. With the screen displayed, click the **View** link under the **Notification Center** block.

Alternatively, on the **Home** screen click the **View All** link in the **Notifications** block, or click the bell icon on the **floating panel**.

With the screen displayed, you can see a list of problems detected.

To learn details about the problem found, click **Learn more** underneath the problem summary. The screen with the detailed problem description and recommendations how to solve the problem opens.
Use the drop-down combo box to perform one of the following actions on the item: **Fix It Now (recommended)**, **Remind me later**, or **Ignore (not recommended)**.

Select **Fix problem now (recommended)** to fix the problem immediately. Afterwards, the problem is not available in the list.

Select **Remind me later** to clear the problem. You are reminded about it after 48 hours.

Select **Ignore (not recommended)** to move the item to the **Ignored List**.

On the **Notification Center** screen, click **Options** next to the problem to select one of the following actions on the context menu: **Fix problem now (recommended)**, **Remind me later**, or **Ignore (not recommended)**.
Ignored Notifications

If you want to manage notifications, proceed through the steps listed below:

1. On the left menu, click **App Management**. The **App Management** screen opens.

   ![App Management Screen](image)

   - Click **Ignored Notifications**
   - Click **Manage**

2. In the **Ignored Notifications** block, click **Manage**.

With the **Ignored Notifications** screen displayed, you can see the list of actions you have ignored/working with Notification Center.

To remove an action from the list, select the check box it corresponds to and then click **Remove**.
You are not notified about problems listed in the Ignored List. In order to restore the problem(s) to the Notification Center, select the item(s) and click on "Remove" from the list button.

- Automatic Definition Update is disabled
To use Ad-Aware in your preferred language, proceed through the steps listed below:

1. On the left menu, click **App Management**. The **App Management** screen opens.

2. In the **Language** block, select one of the supported languages from the drop-down combo box.
Notifications and Balloons

To keep you informed about the Ad-Aware Antivirus program’s activity, notifications as well as balloons display for the following events:

1. Threat is detected during the scanning process. Click View details to navigate to the Scan Computer screen.

2. Threat is detected in real time.

The balloon shows the action applied to the treat found (quarantine) and a threat path. The full path to the treat is provided in a tooltip.

3. The scan (Context Menu or automatic) starts. Click View details to navigate to the Scan Computer screen.

4. Update for the application, or an additional download, or both, is available. Click Click here to update now to navigate to the Home screen.

5. Special offer is available. Click View details to navigate to the Home screen.
Tray Application

Double-click the *Ad-Aware Tray Application* in the system tray to access the *Ad-Aware*’s main user interface.

Right-click the *Ad-Aware Tray Application* to open a context menu which includes the options shown below.

**Open Ad-Aware**

Opens the *Ad-Aware* program.

**Disable/Enable Ad-Aware features**

Disables/Enables *Ad-Aware features*. Click the required feature to disable/enable it. A feature set available in the list depends on your current [version](#) of *Ad-Aware*.

**Quick Scan**

Runs a [Quick scan](#).

The **Quick Scan** command is replaced by one of the following statuses depending on a process being currently performed:

- **Scanning...**: when a scan of any type is being performed.
- **Scan Paused**: when a scan of any type is paused.
- **Cleaning...**: when a selected action is applied to threat(s) found.
- **Clean Paused**: when a cleaning procedure is paused.
- **See Scan Results**: when a scan of any type is finished and threats are found.

Clicking a status on the tray context menu opens a [Scan Computer](#) screen.
How To

Register Ad-Aware

You can register your copy of the Ad-Aware application. The purpose of the registration is to give you a possibility to access and use Ad-Aware Free Antivirus+ for one-year period. In addition, registering your copy ensures that you receive product support, product update information, and other benefits. Completing the registration requires only a few minutes. Personal information (a full name and an email address) is required if you decide to register.

When you launch the application you have not activated yet for the first time after its installation, the following dialog appears. To start registering, click Register Now.

In addition, you can open the dialog box for further registration by clicking the Get an activation key here link in the Activate message box if your copy of Ad-Aware has not been activated yet or the activation period has been expired.

With the screen you advance to, click Upgrade Now to get Ad-Aware Pro Security. Otherwise, click Activate to continue with the registration.
1. With the dialog displayed, type your name and email address in the corresponding fields. Then select the “I have read and agree to Lavasoft Privacy Policy” check box and click the Submit button to proceed.

If you want to receive our newsletter on relevant information about security threats as well as promotional offers from Lavasoft, select the Yes, sign-me to the Lavasoft newsletter check box.
2. Once you are done with submitting a registration form, an email with your activation key is sent to this address.

In addition, you have an option to change your email address or resend activation to the email address you have indicated when submitting, just click a link of your choice in the dialog displayed.
Afterwards, copy the activation key you have received by email in the form and then click the **Activate** button to start using **Ad-Aware Free Antivirus+** for one-year period.

If you want to postpone activation, click **Do it Later**.
To activate *Ad-Aware Antivirus*, proceed through the steps below:

1. On the left menu, click **App Management**.
2. With the **App Management** screen displayed, scroll down until reaching the **Account Settings** block.
3. Click **Add a key**.
4. With the message box displayed, type your activation key and then click the **Submit** button.

*We recommend copying and pasting the key from your email into the field to avoid any mismatch.*
You are notified once the activation key is accepted. To continue, click **Close this window**.
If you launch the application for the first time after installation, and you have not activated your copy of Ad-Aware yet, the following message box appears:
The message box is accessed by clicking the Get an activation key here link in the Activate message box if your copy of Ad-Aware has not been activated yet or the activation period has been expired.

With the message box displayed, type your activation key and then click the Activate button.

We recommend copying and pasting the key from your email into the field to avoid any mismatch.

You are notified once the activation key is accepted. To continue, click Close.
Renew License

You can renew license for your copy of Ad-Aware, when it is about to expire.

The **Your Ad-Aware version is about to expire** notification appears on the *Home* screen.

![Ad-Aware notification](image)

Alternatively, you can access this notification from the *Notification Center* screen.

Select **Renew Now** from the drop-down combo box to start the process of renewal. Lavasoft web page will be opened in the web browser where you can purchase a new license.

Select **Remind me later** to be reminded about expiration after 48 hours.
Update Ad-Aware

If a new version of the application is available on our server, you can see a prompt to update the program on the Home screen. The notification becomes available when you launch Ad-Aware.

When the program is hidden to the system tray or minimized to the taskbar, Ad-Aware opens on the Home screen informing you that the program update is available. Moreover, if Ad-Aware displays any screen, but not Home, the screen shows each time updates are available.

![New updates are checked for availability every hour.](image)

To get the latest version of the application, proceed through the steps listed below:

1. Click the Update Now button. Lavasoft update web page opens in your default web browser.

2. Locate and click the link to download the update file.
3. When prompted, save the installer file.
4. Once the download is complete, go to the downloaded path and double-click the update file to launch an Ad-Aware Web Installer. The Ad-Aware Web Installer downloads and runs the Ad-Aware Updater.
5. Once the update process is complete, click **Close** or a little cross in the upper right-hand corner of the following screen. The *Ad-Aware antivirus* updater closes and the *Ad-Aware antivirus* desktop application starts.
If you update Ad-Aware from v. 9.6/10.x to v. 11, you are prompted to uninstall the older version. Follow the on-screen instructions until the process is complete. Once uninstall completes, PC reboot is required. After Windows start up, Ad-Aware Web Installer launches. Afterwards, proceed through the steps of Ad-Aware install beginning with step 4.

If you remove the older version manually through the Control Panel, after PC reboot proceed through the steps of Ad-Aware install from the very beginning.
Upgrade Ad-Aware

At Lavasoft, we believe that every computer user must have the power to control their individual privacy and security when they use the Internet. That is why we offer Ad-Aware Free Antivirus+, a proactive malware removal tool that allows users to combat today’s toughest cyber threats. Ad-Aware Free Antivirus+ features real-time anti-malware protection, rootkit protection, and community-driven initiatives to ensure that you have the power to protect yourself online.

Ad-Aware Personal Security is a paid upgrade of our Ad-Aware Free Antivirus+ version and builds upon the malware protection offered in our free product. Ad-Aware Personal Security adds a powerful web-filter that protects users against phishing attacks and online scams.

Ad-Aware Pro Security is a paid upgrade of our Ad-Aware Free Antivirus+ version and provides a line-of-defense against the most extreme forms of malware and cyber threats. It adds a powerful two-way firewall, an email protection engine, advanced web protection as well as our most advanced detection and threat blocking algorithms.

Ad-Aware Total Security is a paid upgrade of our Ad-Aware Free Antivirus+ version which above all adds a parental control feature to filter out all bad content.

To take advantages of using the full functionality of the product, we propose to upgrade the program. All you have to do is buy an upgrade key from Lavasoft:

1. On the left menu, click App Management.
2. With the App Management screen displayed, scroll down until reaching the Account Settings block.
3. In the Account Settings block, click Renew.
4. With the message box displayed, type your activation key and then click the Submit button.

<table>
<thead>
<tr>
<th>Ad-Aware Free Antivirus+</th>
<th>Upgrade to Ad-Aware Personal Security</th>
<th>Upgrade to Ad-Aware Pro Security</th>
<th>Upgrade to Ad-Aware Total Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Computer</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Application Management</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Real-Time Protection</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Gaming Mode</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Web Protection</td>
<td></td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Email Protection</td>
<td></td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Network Protection</td>
<td></td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Ignored Notifications</td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Parental Control</td>
<td></td>
<td></td>
<td>+</td>
</tr>
</tbody>
</table>
Navigate Ad-Aware

To navigate Ad-Aware, use the following elements of user interface:

- **Left menu**: click the element on the left menu to go to the corresponding screen.
- **Breadcrumbs**: click the element of the breadcrumbs to go to the corresponding screen.
- **Back button**: click the back button (blue arrow) to go to the previous screen.

Get Help

If you have any questions about Ad-Aware antivirus or experience some problems while using it, there are several online resources that can help you find prompt and effective answers.

To get access to the online support, proceed through the steps listed below:

1. On the left menu, click **App Management**.
2. In the **Technical Support** block, click **Get Support**.
3. With the **Support Center** screen, in the **Frequently Asked Questions** block, click **View Frequently Asked Questions** to check common questions, answers and to get better understanding of Ad-Aware antivirus.
4. In the **Identity Protection** block, click **Go to Identity Protection** to get protection against identity theft.
5. In the **Lavasoft Forums** block, click **Go to Lavasoft Forums** to post your questions or description of issues on the support forum.
6. In the **Software Manual** block, click **View Software Manual** to open the user guide containing detailed instructions with screenshots and explaining how to use Ad-Aware antivirus.
You also can access the Support Center screen by clicking ? icon from the floating panel.

If you are unable to resolve the issue using online resources, you can contact Lavasoft Customer Support team.

To send a message to an agent, proceed through the steps below:

1. With the Support Center screen, in the Contact Support block, complete the submission form:
   - enter your name;
   - enter your email address;
   - select a subject;
   - enter description of the problem you are experiencing.
We strongly recommend indicate your valid email address. It will guarantee that you will be contacted by Customer Support agent.

2. Click Send.

3. With the confirmation message box, click Close. You will be contacted by Lavasoft Customer Support within 12-24 hours during working days.

By default Ad-Aware log files from your computer are attached to your message. This data is required for technical assistants to evaluate an issue and provide you with a prompt and correct reply.
Ad-Aware Command Line Scanner

Getting Started

To start working with *Ad-Aware Command Line Scanner*, proceed through the steps listed below:

1. Download the archived AdAwareCommandLineScanner file depending on your operating system type: 32-bits or 64-bits.
2. Unpack the archive file into a directory of your choice on the machine where you perform the installation.

Start Command Prompt as Administrator

To start a command prompt as an administrator, proceed through the steps listed below. To complete the procedure, you must be a member of the Administrators group.

1. Click the **Start** button, click **All Programs**, click **Accessories**, and then click.
2. Right-click **Command Prompt**, and then click **Run as administrator**.

   *If the User Account Control dialog opens, make sure the action prompted in the dialog corresponds to the one you are performing, and then click Yes.*

Or Click **Start**. In the **Start Search** box, type **cmd**, and then press **CTRL+SHIFT+ENTER**.

   *If the User Account Control dialog opens, make sure the action prompted in the dialog corresponds to the one you are performing, and then click Yes.*

Find Ad-Aware Command Line Scanner with Command Prompt

As soon as Command Prompt starts, you need to go to the location where AdAwareCommandLineScanner_xxx_11.0.xxxx.0 has been unpacked.

1. At a command prompt, type `cd \` to return to C:\, and then press ENTER.
2. If you extract CommandLineScanner files to the root directory of your hard drive C:, type first letters of the file name (for example, "ad"), and then press the TAB key or type the full name.
3. If you extract CommandLineScanner files to any folder on your hard drive C:
o type "cd" before typing the folder name, and then press ENTER;

OR

o type "cd" and first letters of the folder name (for example, "ad"), press the TAB key;

OR

o type the full path.

4. Once you open the AdAwareCommandLineScanner_xxx_11.0.xxxx.0 folder, type first letters of the file name (for example, "ad"), press the TAB key or type the full name.

Action List

To view a list of actions that Ad-Aware Command Line Scanner can do, proceed through the steps listed below:

1. With Command Prompt, type first letters of the AdAwareCommandLineScanner.exe file name (for example, "ad"), and then press the TAB key or type the full name.
2. Then type "--help" and press ENTER.
Download Definitions

To start working with Ad-Aware Command Line Scanner, you need to download definitions.

To download definitions, proceed through the following steps:

1. With Command Prompt, type first letters of the AdAwareCommandLineScanner.exe file name (for example, "ad"), and then press the TAB key or type the full name.
2. Then type "--updatedefs" and press ENTER.

3. You can see the definition downloading process. It takes some time, wait for this process to be finished.
Once definitions are downloaded, you can continue working with Ad-Aware Command Line Scanner.
To start a Quick scan, proceed through the following steps:

1. With Command Prompt, type first letters of the AdAwareCommandLineScanner.exe file name (for example, "ad"), and then press the TAB key or type the full name.
2. Then type "--quick" and press ENTER.
After a Quick scan completes, you can see a path where results can be found. By default, scan results are stored in the Scan Results folder within the AdAwareCommandLineScanner_xxx_11.0.xxxx.0 folder as an .xml file. Its name represents a scan type, date and time.

If threats are detected, the information about those threats is prompted. No action is applied automatically.
Full Scan

To start a Full scan, proceed through the following steps:

1. With Command Prompt, type first letters of the AdAwareCommandLineScanner.exe file name (for example, "ad"), and then press the TAB key or type the full name.
2. Then type "--full" and press ENTER.

After a Full scan completes, you can see a path where results can be found. By default, scan results are stored in the Scan Results folder within the AdAwareCommandLineScanner_xxx_11.0.xxxx.0 folder as an .xml file. Its name represents a scan type, date and time.

If threats are detected, the information about those threats is prompted. No action is applied automatically.
Custom Scan

To start a Custom scan, proceed through the following steps:

1. With Command Prompt, type first letters of the Ad Aware CommandLineScanner.exe file name (for example, "ad"), and then press the TAB key or type the full name.
2. Then type "--custom" and a path of the folder/file (including folder/file name) that you want to scan, and press ENTER.

   To scan the drive, should be indicated as follows: C:\\

To scan a folder, should be indicated as follows: C:\folder name
To scan a file, should be indicated as follows: C:\folder name\file name.

After a Custom scan completes, you can see a path where results can be found. By default, scan results are stored in the Scan Results folder within the AdAwareCommandLineScanner_xxx_11.0.xxxx.0 folder as an .xml file. Its name represents a scan type, date and time.
If threats are detected, the information about those threats is prompted. No action is applied automatically.
Scan Boot Sectors

To scan boot sectors, proceed through the following steps:

1. With Command Prompt, type first letters of the AdAwareCommandLineScanner.exe file name (for example, "ad"), and then press the TAB key or type the full name.
2. Then type '--boot' and press ENTER.

Once boot sectors are scanned, you can see a path where results can be found. By default, scan results are stored in the Scan Results folder within the AdAwareCommandLineScanner_xxx_11.0.xxxx.0 folder as an .xml file. Its name represents a scan type, date and time.
If threats are detected, the information about those threats is prompted. No action is applied automatically.

```xml
<?xml version="1.0"?>
<Summary>
  <ScanInfo EndTime="20130905T142321.678236" StartTime="20130905T142321.366236" ScanType="Boot"/>
  <ScanPaths/>
  <DefectedObjects/>
</Summary>
```
Delete Action

If you want to delete all threats detected during a scan process of any type, proceed through the steps below:

1. With Command Prompt, type first letters of the AdAwareCommandLineScanner.exe file name (for example, "ad"), and then press the TAB key or type the full name.
2. Then specify a scan type ("--quick", "--full", "--custom" or "--boot"), for the custom scan specify a path of the folder/file (including folder/file name) that you want to scan, then type "--delete" and press ENTER.
C:\windows\system32>cd \n
C:\my downloads>cd AdAwareCommandLineScanner_x64_11.0.***.0

C:\my downloads\AdAwareCommandLineScanner_x64_11.0.***.0>AdAwareCommandLineScanner.exe --full --delete
Quarantine Action

If you want to quarantine all threats detected during a scan process of any type, proceed through the steps below:

1. With Command Prompt, type first letters of the AdAwareCommandLineScanner.exe file name (for example, "ad"), and then press the TAB key or type the full name.
2. Then specify a scan type ("--quick", "--full", "--custom" or "--boot"), for the custom scan specify a path of the folder/file (including folder/file name) that you want to scan, then type "--quarantine" and press ENTER.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>cd \
C:\>cd "My downloads"
C:\My downloads>cd AdAwareCommandLineScanner_x64_11.0.xxx.0
C:\My downloads\AdAwareCommandLineScanner_x64_11.0.xxx.0>AdAwareCommandLineScanner.exe --full --quarantine
Disinfect Action

If you want to disinfect all threats detected during a scan process of any type, proceed through the steps below:

1. With Command Prompt, type first letters of the AdAwareCommandLineScanner.exe file name (for example, "ad"), and then press the TAB key or type the full name.
2. Then specify a scan type ("--quick", "--full", "--custom" or "--boot"), for the custom scan specify a path of the folder/file (including folder/file name) that you want to scan, then type "--disinfect" and press ENTER.
The disinfect action is recommended to be applied to infected boot sectors.

If an infected file cannot be disinfected, it is deleted.
Specify Scan Result Path

To specify a path for scan results, proceed through the steps below:

1. With Command Prompt, type first letters of the AdAwareCommandLineScanner.exe file name (for example, "ad"), and then press the TAB key or type the full name.
2. Then specify a scan type ("--quick", "--full", "--custom" or "--boot"), for the custom scan specify a path of the folder/file (including folder/file name) that you want to scan.
3. Type "--scan-result< path >".

   If you want to save scan result on any drive without specifying its name, type "<Drive name> :\"

4. Press ENTER.

The file is saved on the specified drive. It is an .xml file. Its name represents a scan type, date and time.
If you want to save scan result on the specified folder, type "< Drive name > :\folder name\file name" and then Press ENTER.
Product Information

To view information on the product, proceed through the following steps:

1. With Command Prompt, type first letters of the AdAwareCommandLineScanner.exe file name (for example, "ad"), and then press the TAB key or type the full name.
2. Then type "--product-info" and press ENTER.
Definitions Information

To view information on definitions, proceed through the following steps:

1. With Command Prompt, type first letters of the AdAwareCommandLineScanner.exe file name (for example, "ad"), and then press the TAB key or type the full name.
2. Then type "--definitions-info" and press ENTER.
Check for Product Updates

To check for the product updates, proceed through the following steps:

1. With Command Prompt, type first letters of the AdAwareCommandLineScanner.exe file name (for example, "ad"), and then press the TAB key or type the full name.
2. Then type "--updateapp" and press ENTER.

If any updates are available, you can see a link from where you can download a new version.

If there is no new version available, you are notified that you use the latest version.