Kaspersky Removal Tool 2011

Virus Removal Tool is a utility designed to remove all types of infections from your computer. It implies effective algorithms of detection used by Kaspersky Anti-Virus and AVZ.

- Kasperksy Rescue Disk 10
- Common information
- Viruses and solutions
- Virus-fighting utilities

Knowledge Base | Downloads & Info | System Requirements

Kaspersky Removal Tool 2011

Topic List

← Back to "Work with program" section

Search This Product Search

Article ID: 6187 127

How to configure automatical scan in Kaspersky Virus Removal Tool 2011

Applies To

- Kaspersky Removal Tool 2011

You can modify the following **Autoscan** parameters in **Kaspersky Virus Removal Tool 2011:**

- **Scan scope** – the list of scanned objects and their location.
- **Security level** – set of parameters applied by the program to perform autoscan and disinfection.
- **Actions** – you can specify an action to be performed on threats detected during Autoscan.

*The configured **Autoscan** settings are saved during the current session of the program, as the program is deleted as soon as the main program window is closed.*

How to modify scan scope in Kaspersky Virus Removal Tool 2011

In order to modify the scan scope, perform the following actions:

1. **Launch** Kaspersky Virus Removal Tool 2011.
2. Go to the **Settings** tab marked with an asterisk image.
3. Select the **Scan scope** section.
4. Create the required scan scope by checking the necessary objects you wish to scan. Add other files and folders by clicking on the **Add** button.

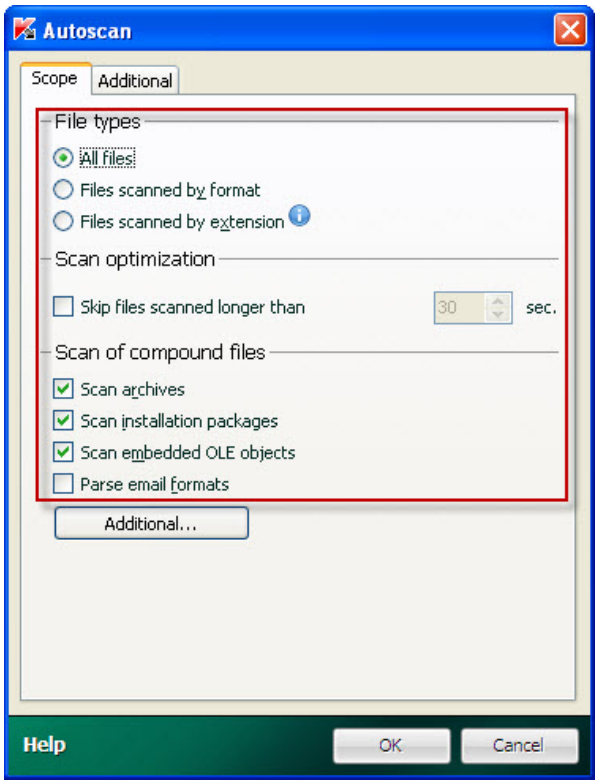
How to modify security level in Kaspersky Virus Removal Tool 2011

In order to change the **Autoscan** security level in **Kaspersky Virus Removal Tool 2011**, perform the following actions:

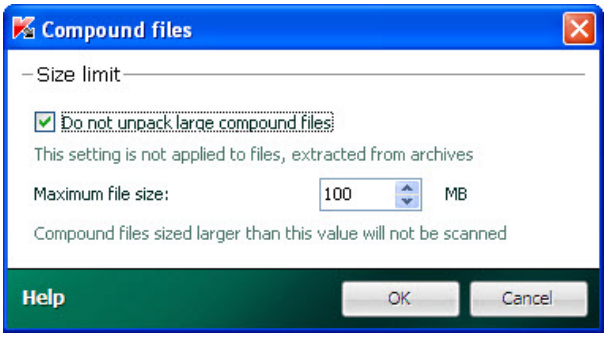
1. **Launch** Kaspersky Virus Removal Tool 2011.
2. Go to the **Settings** tab.
3. Select the **Security level** section.
4. Move the vertical slider to set the desired security level:
   - ***High*** *– if you work in the dangerous environment and the probability of computer infection is very high.*
   - ***Recommended*** *– this level provides optimal balance between security and system efficiency.*
   - ***Low*** *– this security level should be set if the probability of computer infection is low. The number of files to scan is reduced, but additional system resources become available.*

To modify settings of the security level, perform the following actions:

1. On the **Security level** tab click on the **Settings** button.
2. In the **Automatic scan** window on the **Scope** tab specify the required settings:
   - ***All files***. *With this option, all objects will be scanned without exception*
   - ***Files scanned by format*** *- this option scans only potentially infected files – files which viruses can intrude. Before searching for viruses in an object, its internal header is analyzed for the file format (**txt, doc, exe,** etc.).*
   - ***Files scanned by extension***. *In this case, the program only scans potentially infected files (for example, files with extension **.com, .exe, .sys, .bat, .dll** and etc.), and in doing so, the file format is determined by extension.*
   - ***Skip files scanned longer than***. *Check this option and enter the maximum scan time for an object. Then, if this time is exceeded, this object will be removed from the scan queue*
   - ***Scan archives*** *– scan **.rar, .arj, .zip, .cab, .lha, .jar, and .ice** archives.*
   - ***Scan installation packages*** *- scan installation packages of programs.*
   - ***Scan embedded OLE objects****– scan objects embedded in files (for example, Excel spreadsheets or a macros).*
   - ***Parse e-mail formats*** *– scan e-mail files and e-mail databases.*

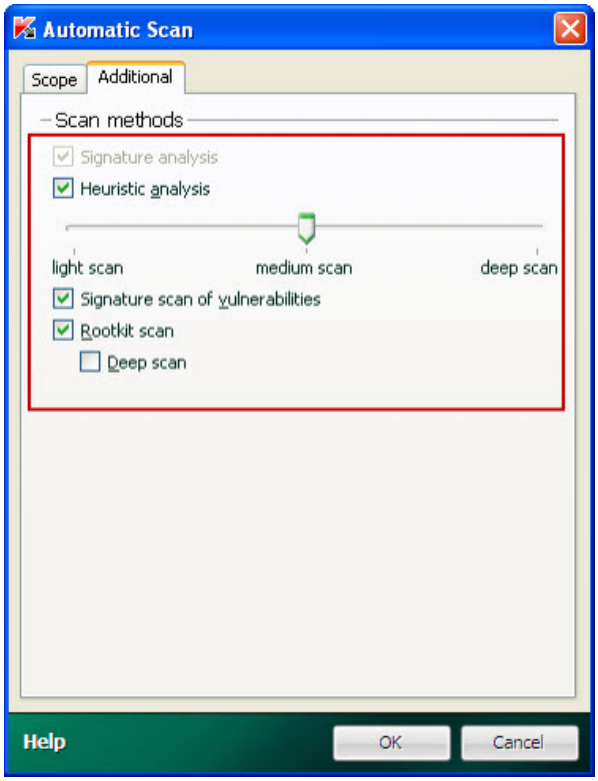


   - *By clicking on the **Additional**... button, the **Compound files** window opens where you define scan parameters of compound files:*
     - ***Do not unpack large compound files***. *Check this option and enter the maximum size for an object. Then, if this size is exceeded, this object will be removed from the scan queue.*



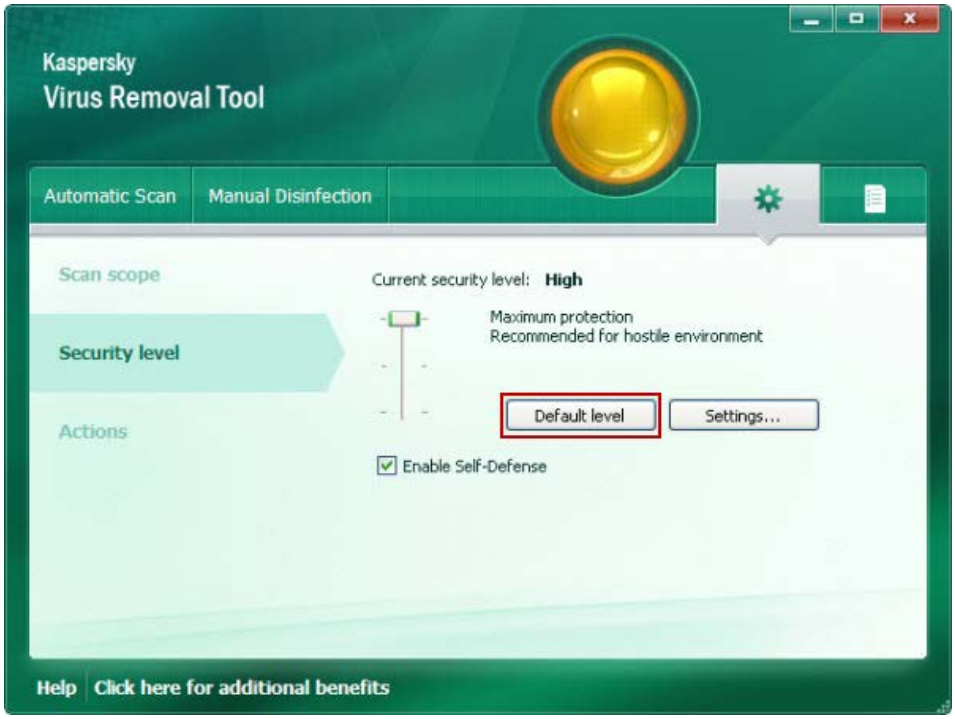
3. On the **Additional** tab select the scan methods:
   - ***Signature analysis*** *– this scan method detects threats based on the database, which contains descriptions of known threats and methods for eradicating them. This method is enabled by default and cannot be disabled.*

- ***Heuristic analysis*** *– a method to detect new malicious programs by the actions they produce in the operating system. The heuristic analyzer can be set to one of the following scan levels:* ***Light scan, Medium scan, High scan****.*
- ***Signature scan of vulnerabilities -*** *enables scan and detection of vulnerabilities of your system, based on databases (signatures) created by* ***Kaspersky Lab's*** *specialists.*
- ***Rootkit scan*** *– enables scan and detection of the utilities which hide actions of malicious programs in the operating system.*
- ***Deep scan*** *– enables more detailed/extended scan of the utilities which hide actions of malicious programs in the operating system.*



4. In the **Automatical scan** window click the **OK** button to save the changes.

To restore the **Security level** settings to the default level recommended by **Kaspersky Lab** experts, click the **Default level** button.



How to change reaction to threat in Kaspersky Virus Removal Tool 2011

In order to change the program reaction to a threat detected during **Automatic scan**, perform the following actions:

Launch Kaspersky Virus Removal Tool 2011.

Go to the **Settings** tab.

Select the **Action** section.

In the right part of the window select the variant:

- ***Prompt on detection***. *In this case a user is instantly prompted for an action upon threat detection.*
- ***Select action***. *You can select the following automatic actions (if no variant is selected, the program will only write the information about detected threats to a report):*
  - **Disinfect** (if a threat can be disinfected, for example, file virus which infected legal software)
  - **Delete, if disinfection fails** (threats which cannot be disinfected are automatically deleted).

Did the provided info help you? Yes No