

Migrating to KAV 6.0 in 20 Minutes or Less

Copyright © 2006 ICE Systems, L.L.C. All rights reserved. 877-332-3250. www.ice-kav.com

Intro

The technical support staff at ICE Systems has created this document to assist existing KAV users in the migration, installation, and configuration of the much anticipated new version of Kaspersky Anti-Virus, KAV 6.0. Using screen prints and detailed step-by-step instructions, ICE Systems is confident that your new installation of KAV 6.0 will go smoothly. We have made suggestions as to how to install and configure KAV 6.0. Our suggestions are by no means requirements, they are intended to assist users who do not wish to spend a lot of time with the configuration of their Anti-Virus program, yet wish to be as thoroughly protected from viruses and other threats as possible. If all of the suggestions in this document are followed you will have a computer fully protected by KAV 6.0 in less than 20 minutes.

In addition to our 20 minute install guide, we have also included as much detail as possible about how to navigate your way through the new program interface, comparing new KAV 6.0 terminology and actions with those from KAV 5.0. Weve also endeavored to introduce some of the coolest new features along with some new popups you man be seeing. We strongly encourage anyone who still has questions after reading this document to please read the official Kaspersky 6.0 documentation.

We have also sprinkled what we call “Performance Tips” throughout the document. Some of these are geared for more advanced users, none of them are required, but they should all be understood by anyone using KAV 6.0. In the event that questions or problems arise during any phase of deployment, our staff of trained network security experts are ready to assist all ICE Systems customers. ICE Systems customers in need of technical support can call 1-877-332-3250.

Installation

One of the first changes you will notice with KAV 6.0 is the new installation file format. Prior versions of Kaspersky installed via a file with an .exe extension, for example the most recent version of KAV Personal 5.0 was installed using the file kav5.0.527_personal.exe. Version 6.0 uses an .msi installation file. As with the .exe installation file the .msi file only requires a double-click of the mouse to initiate the install process. The current version of KAV 6.0 is installed with the file kav6.0en.msi.

You can download the new version at the following web page:

<http://www.ice-kav.com/version6.php>

Look for the KAV 6.0 link at the top of the page, click the link and begin the download of the installation file, (kav6.0en.msi).

Copyright © 2006 ICE Systems, L.L.C. All rights reserved. 877-332-3250. www.ice-kav.com

Once the download is complete you are ready to begin the installation process by double-clicking on the kav6.0en.msi file that you downloaded to your computer.

After clicking the .msi file the installer wizard will begin leading you through the installation process.

Performance Tip: *A new feature of KAV 6.0 is the ability to detect and remove software that is incompatible with KAV 6.0. As current KAV users you likely have KAV Personal 5.0 or KAV Personal Pro 5.0 installed. **You do not have to uninstall or close these programs prior to installing KAV 6.0.** As we will see shortly, KAV 6.0 will detect and remove these programs for you.*

When the installation wizard appears you will be greeted with a welcome message. The message will include the version of product you are installing and ask you to click the Next button when you are done reading the information. The legal agreement will now appear. When you are done reading this click the button indicating that you accept the agreement and then click the Next button. The next window that will appear displays the default location where the product will be installed, C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0\). Click the Next button. You will now see a window asking if you would like a Complete or Custom install. Unless you consider yourself to be a computer expert select Complete. Click the Next button after clicking on the Complete option. You will now see a window like that seen in Figure 1 below:

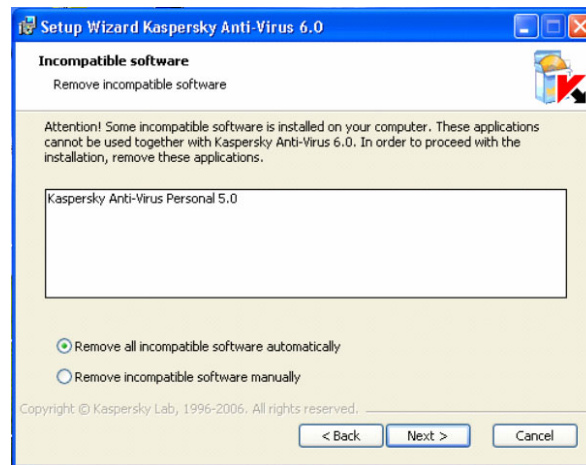


Figure 1 KAV 6.0 does not require pre-existing AV programs to be uninstalled prior to installation. In the image above the installation of KAV 6.0 detected KAV Personal 5.0 and has offered the option to automatically remove it.

After you choose the option to automatically remove all incompatible software and click the Next button, you will see a window prompting you to begin the removal process of KAV 5.0 (or other incompatible software). Click the Install button to continue the process of removing earlier KAV versions. You will see the red “K” in your system tray disappears as KAV 5.0 is uninstalled. Following the uninstallation process you will be prompted to restart your computer.

When your computer is restarted you will notice a small Windows Installer window appear, followed shortly by the Welcome message you saw when you first began the installation process. Again click the Next button. You will notice at this time that no other programs are running; only the installation of KAV 6.0 – this is to ensure that the installation is not affected by other running programs. Following the Welcome message you will see the next four familiar windows: the license agreement (click Agree and Next when done reading), the installation location (click Next to continue), the option for a Complete or Custom install (choose Complete and click Next), and lastly the Install window (click the Install button). A progress bar will appear that tracks the installation. When the installation is complete you will see a message indicating such and be prompted to again restart your computer.

Once your computer is restarted you will see the following window:

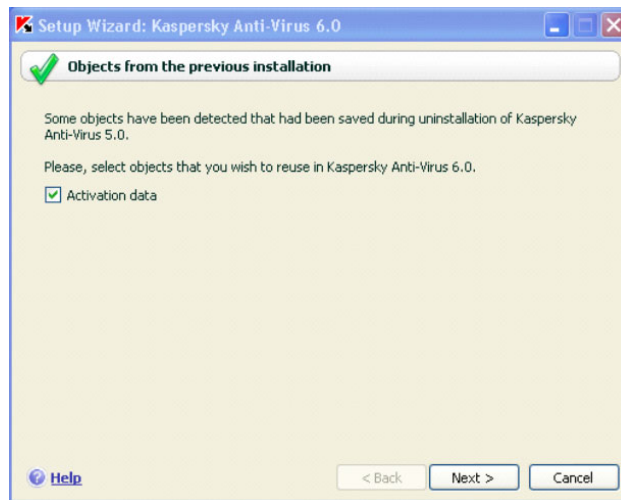


Figure 2 KAV 6.0 will detect and use the license key installed with earlier versions of Kaspersky as long as the key is still valid.

As Figure 2 indicates, your license key that was installed with KAV 5.0 will be detected and used with KAV 6.0 – it will not be removed when KAV 5.0 is automatically uninstalled. After clicking the Next button the details of your license key will be displayed; review the information and click Next when done. The next window to appear will be the Update settings window (see Figure 3 below). By default KAV 6.0 is configured to download updates from the Internet whenever a new set of updates are available. This is different from earlier versions of KAV that were by default set to update every 3 hours. The Update settings window you see will allow you to change the schedule of the update task; ICE Systems suggests you use the default settings.

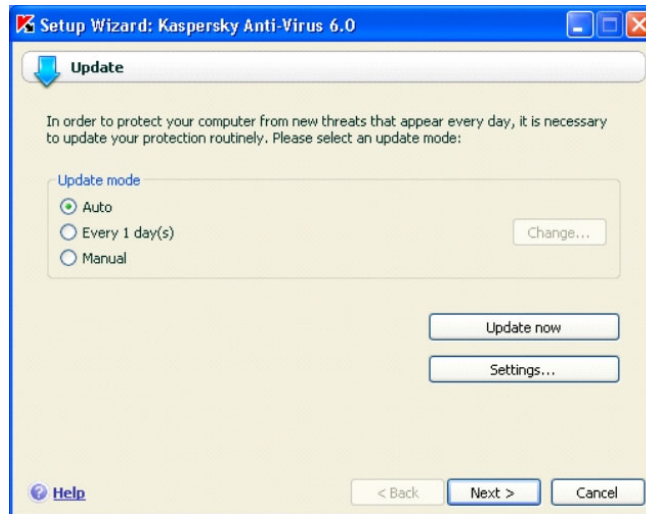


Figure 3 the Update settings window. The default setting, seen above, is Auto meaning that your anti virus definitions will be automatically downloaded when new ones are available. There is no user interaction required for these auto updates to occur.

After you click Next in the Updater settings window the Scan settings window will appear (see Figure 4 below). There are three sections to the Scan settings window.

The first section deals with startup objects. Startup objects are programs or files that are loaded when your computer is booted or turned on. For example if you are an AOL user and AOL starts up automatically whenever your pc is turned on, the files AOL uses will all be scanned when your computer is started or restarted. By default the startup scan is set to run every time your computer starts up. ICE Systems suggests using the default setting for the startup scan. The first time this startup scan runs following the installation of KAV 6.0 it may run for up to five minutes. Unlike earlier versions of the product however, the startup scan with KAV 6.0 will still allow you to access other programs on your computer as the scan runs, without slowing down your system. Subsequent startup scans following the initial one will run in less than one minute – depending on the number of programs configured to start when your pc is turned on and the speed of your computer.

Performance Tip: *The startup scan can be safely disabled as long as your computer has been fully scanned for viruses and Kaspersky file protection has never been turned off while connected to the network. As mentioned above however, the startup scan in KAV 6.0 is not as performance intensive as in earlier versions. To disable the startup scan simply uncheck the box “Run on system startup” that is checked by default.*

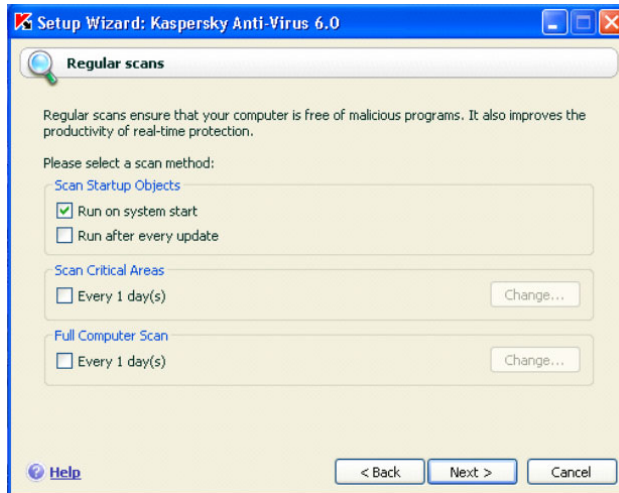


Figure 4 the Scan settings window allows you to configure or disable Startup scans, scans of critical areas, and a full computer scan. By default only the Startup scan is scheduled to run.

The second section of the Scan settings window is the Scan Critical Areas. This scan can be used if necessary to scan areas of your computer that would be most affected if damaged by a virus. The critical area scan is not enabled by default but can be run at anytime. We do not suggest scheduling this task. The full scan we will configure and schedule next scans all of the files included in the Scan Critical Areas scan.

The third section of the Scan settings window is the Full Computer Scan. This scan was previously referred to as the On-Demand scan. By default this task is configured to be ran on-demand as it is not scheduled. If you would like to schedule a full system scan of all files on your computer you can do so by clicking the box “Every 1 day(s)” seen above in Figure 4, followed by the Change button associated with the full scan. After clicking the Change button you will see the window displayed below in Figure 5:

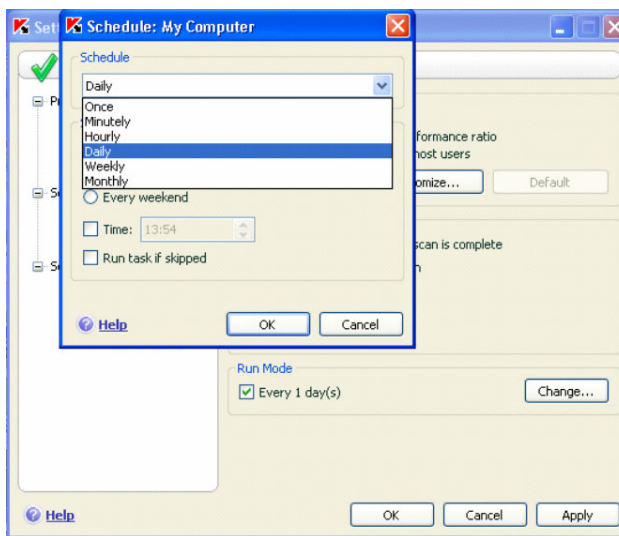


Figure 5 the schedule options for the full scan task.

ICE Systems suggests running a full system scan once a week. Pick a time when you can allow the scan to be the only program running. During the full scan it is normal for your computer to act sluggish – Kaspersky will use as much resources as possible to complete the scan. Most scans will complete in an hour or less, depending on the amount of data stored and the speed of the computer.

Performance Tip: *To decrease the time a full scan takes, prior to starting the scan, delete all files/folders in the following folders:*

C:\Windows\Temp\
C:\Documents and Settings\<<USER>\Local Settings\Temp\
C:\Documents and Settings\<<USER>\Local Settings\Temporary Internet Files\

In the above example <USER> equals the user account you login as.

All of the files and folders in the above folders are temporary files/folders and can be safely deleted. If you get a message indicating that a file can not be deleted because it is in use, simply skip it and delete all of the files/folders that you can. Sometimes it is necessary to boot your pc in Safe Mode in order to delete all files and folders listed above.

Once your weekly scan has been scheduled click the Next button. The Password window is the next screen you will see. If you have a need to password protect KAV 6.0 from others in your home or office this is the window to do it, (see Figure 6 below).

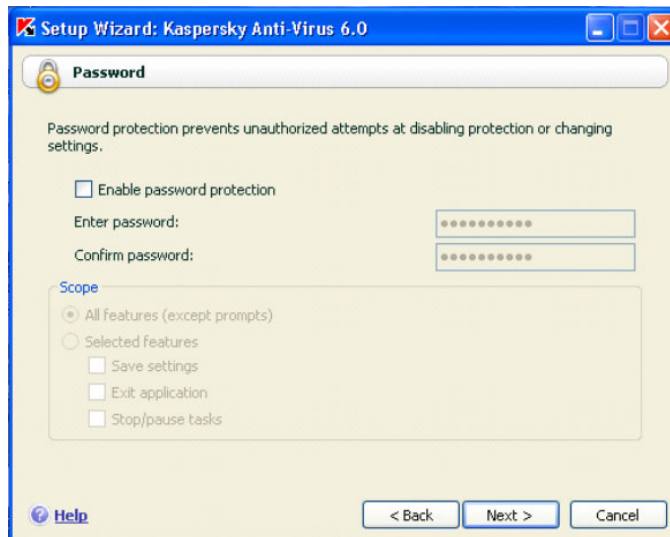


Figure 6 The Password window allows you to password protect your KAV 6.0 installation. You can choose to have all operations password protected or selectively choose which features you want to protect. ICE Systems suggests that if password protection is enabled the “All features” box should be checked.

After configuring or skipping the Password protection screen click Next and the installation process will conclude. You will see another progress bar as the final stages of installation are completed. A final Interactive Protection window will appear as seen in Figure 7:

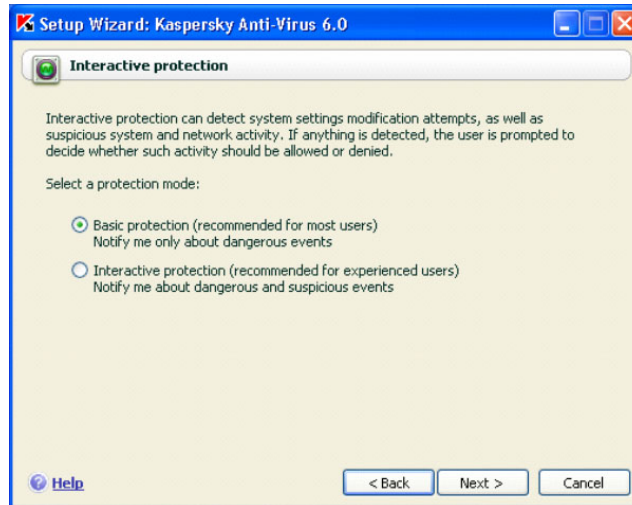


Figure 7 The Interactive Protection window offers choices on the amount of information that is delivered to the end user regarding potential threats. ICE Systems is comfortable leaving this set to the default Basic Protection level.

After selecting Basic Protection click the Next button and the installation is complete. You will be prompted for one last reboot. Following the reboot you should see the small red “K” appear in your system tray. If this K does not immediately appear following your first reboot after installation, do not panic, the K will appear soon after your pc is back up. Check your watch, has 20 minutes elapsed? You are all set, completely protected from the rogues of the internet. At this point the following settings are in place on your computer:

- 1) Automatic updates of your anti-virus database definitions have been configured to run whenever there are new updates available.
- 2) A full system scan has been configured and scheduled to run weekly.
- 3) A startup scan will run whenever your computer is started, scanning all important files needed during the startup process or required for programs configured to run when your computer starts.
- 4) All of your files and incoming email is protected from attacks – even those from yet to be defined viruses.

In short, if you never touch a single thing inside the Kaspersky interface your pc will be safely protected from all threats. If you are satisfied with this you can close the document

and call us when your license is about to expire – thanks for reading, and thanks for using ICE Systems.

If you'd like to learn more please read on....

Program Interface

Overview

Like previous versions of KAV, to open the program interface simply double-click on the red K that appears in your system tray. You can also access the program interface from your Windows Start button by selecting All Programs – Kaspersky Anti Virus 6.0 – Kaspersky Anti Virus 6.0 (yes it is there twice) or by clicking the Start menus KAV 6.0 shortcut item if one is present.

After opening the program interface hover your mouse over some of the items/icons. When you move your mouse over items in the interface you will notice that they are actually links that when clicked reveal additional details about the linked item, usually on the right hand side of the main window. For example when I click the Protection icon/link (see below Figure 8) I see four additional links appear directly below the Protection icon as well as additional information displayed on the right side of the screen.



Figure 8 The new program interface for KAV 6.0. Listed under the Protection link are the four Protection elements. In this image only the Protection icon was selected/clicked.

At the top of the program interface you will notice a large green check mark with the word Settings to the right. Whenever a linked item is selected the settings for that object can be accessed by clicking the Settings link. For example to access the settings options for the scan task we created during installation I would first click the Scan icon, followed by the My Computer icon and then the Settings icon. We will go into detail later about the settings options for all major tasks.

Immediately to the right of the Settings icon you see a Help icon. There is either a help icon or a help link in every window you see in KAV 6.0. When a help icon or link is clicked a window with comprehensive information pertaining to the subject referenced is opened. When in doubt, click on Help.

Below the Settings and Help icons are the symbols for play, pause, and stop. You will see these buttons in any window associated with a task, i.e. scans, updates, email protection, etc. You can use these buttons to selectively start or stop an individual task or entire sets of tasks. Again this will be detailed soon.

Below the play/pause/stop buttons you will find a brief description of the task, a summary of details associated with the task, and statistics for the task. This format is

consistent throughout the interface; you can always find the Help icon or the Settings icon – there are always three sections displayed on the right side of the interface for any task you select as well as the play/pause/stop buttons. It may look different than 5.0, but once you get the hang of it you will like it more. Lets take a brief look at each of the three main sections of the program interface; Protection, Scan, and Service.

Protection

The Protection section in KAV 6.0 deals entirely with what we used to call real-time protection, the protection mechanism that keeps new viruses and other threats from attacking and compromising your computer. Unlike a full or on-demand scan where every file is scanned, real-time protection only scans files as they are created or changed.

When you click on the Protection link or its umbrella icon (please refer to figure 8 above) you will see below it a list of the four Protection tasks that run whenever your computer is started. These tasks are:

- 1) File Anti Virus – This is the traditional real-time file protection. All files newly created or modified are scanned by default.
- 2) Mail Anti Virus – The same as real-time mail protection in v5.0. All incoming email, (except mail delivered via HTTP such as Yahoo, MSN, and HotMail) and attachments will be scanned prior to delivery to your Inbox.
- 3) Web Anti Virus – This feature protects your computer from attacks originating from web sites you access when surfing the net.
- 4) Proactive Defense – This is a super cool feature that allows Kaspersky to protect your computer from new viruses that have not yet been identified by Kaspersky.

All of the above listed Protection tasks **are enabled by default**. You can view statistics and summary information for any of the four Protection tasks by simply clicking the link to the task.

When the Protection icon is clicked, in addition to displaying the above mentioned four tasks, information about the overall system protection status is displayed on the right side of the window. Referring again to Figure 8 above we can see in the Summary section the current date of the AV database definitions as well as the status of all protection tasks – in this case we can see that all protective services are running. The start, pause, and stop buttons in Figure 8 could be used to halt ALL protective services on the system, a dangerous thing to do.

Scan

The Scan section of the program interfaces is the area where all on-demand scans are controlled. An on-demand scan, as opposed to a real-time scan, is a scan initiated by the user (you) on a file, list of files, or all files on your pc, regardless of whether they are new or modified. In KAV 6.0 there are three different types of scans that we can configure and run and they are displayed in the interface under the Scan area as:

- 1) Critical Areas – A Critical Areas scan will scan files and areas of memory that are most critical for the continued operation of your Windows computer.
- 2) My Computer – This scan will scan all files on your computer, including system memory and all other objects included in the critical areas scan and the startup scan.
- 3) Startup Objects – This scan will scan files and system memory used to start your computer, including the files associated with any programs that start automatically whenever you start your pc.

The My Computer scan is the most comprehensive as it includes all items in both the Critical Areas and Startup Objects scan. During installation we configured a full computer or My Computer scan to run once a week at a time convenient for you. The Critical Areas scan includes items scanned in the Startup Objects scan, and finally the Startup Objects scan will scan the smallest subset of objects on your pc. All of these scans can be configured and scheduled – operations that will be covered shortly. The Scan menu from the program interface seen below in Figure 9 displays the Scan-Startup Objects window following the successful completion of the Startup Objects scan:

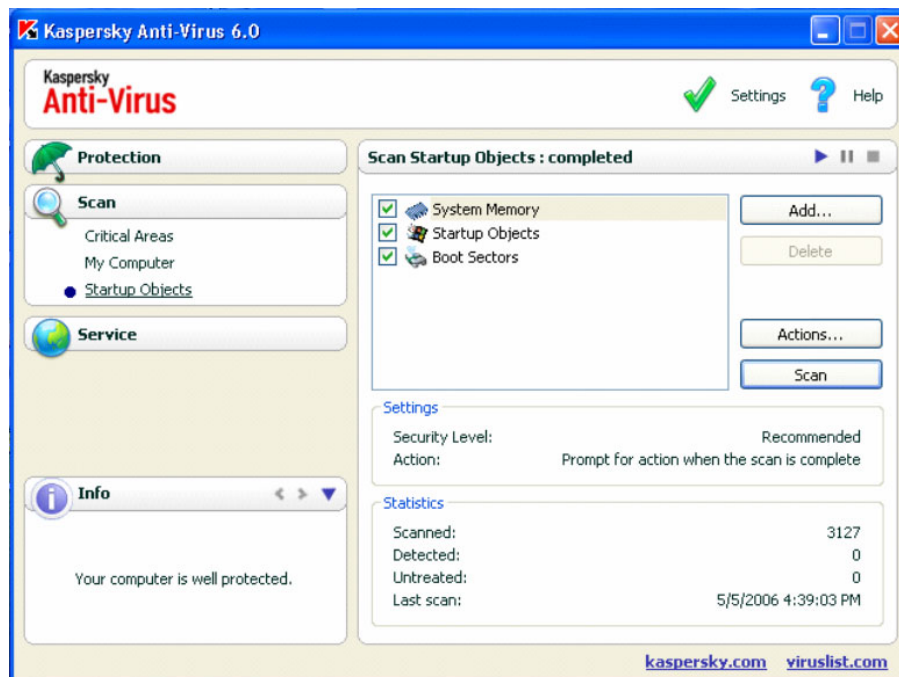


Figure 9 Scan-Startup Objects screen in the program interface.

Service

The third main area of KAV 6.0's program interface is the Service section. After clicking on the icon for Service, the blue globe, you will see a list of four options appear below it:

- 1) Update – The Update section is the area where you can configure and manually run the anti-virus database definitions update. By default the update will run automatically, every time a new set of definitions are available.
- 2) Data Files – The Data Files section is where infected files that have been backed up or quarantined are located. The Reports section of the program can also be accessed from this sub-section. We will cover the Reports section in greater detail later.
- 3) Rescue Disk – A rescue disk is used to recover lost data following a mass infection or other catastrophic computer problem. It is necessary to have PE Builder v3.1.3 or higher installed as well as the Windows XP Service Pack 2 Installation CD. Not an operation for the novice computer user.
- 4) Support – The Support section provides contact information for technical support as well as links to online forums, FAQs, and an option to report bugs (software defects).

Now that you have a general idea of how the program interface is laid out and navigated lets cover how to perform some of the operations we were used to in v5.0 in the new KAV 6.0.

How To?

Kaspersky 6.0, like all of its predecessors, is made up of three main components; real-time scanning, covered in the Protection section, on-demand or full computer scans, covered in the Scan section, and anti virus database updates, covered in the Service section. Lets look at some of the how tos associated with each of these sections. Please note that many of these settings should only be used by experienced computer users.

Protection how to's

How to enable/disable Protection tasks

To disable all Protection tasks select Protection - Settings, and then uncheck the Enable Protection box in the General section at the top of the Settings window. Or you can click the stop button after clicking the Protection icon.

To selectively disable a Protection task select Protection - <desired task> - Settings. Each Protection task has a General section at the top of the Settings window that will allow you to disable and re-enable a specific Protection task. You can also use the play/pause/stop buttons available by just clicking on the task.

How to modify the Protection level

To modify the default protection level select Protection - <desired task> - Settings. The Security level section of the Settings window contains the familiar scroll bar that you can click on and slide to the setting you prefer. The protection level names have changed slightly from v5 to v6. I have listed below first the new KAV 6.0 terms with the old v5.0 equivalents.

High (v6) – Maximum Protection (v5)
Recommended – Recommended
Low (v6) – High Speed (v5)

Each of the first three Protection tasks - Files, Email, and Web all have the same scroll bar. The Proactive Defense task will be covered later.

Performance Tip: *The protection level Low, though less protective than Recommended or High, is more than sufficient protection for computers operated by experienced or expert users. If you are experiencing a noticeable performance drag on your pc following the installation of KAV 6.0 set the protection level to Low.*

How to customize default Protection settings

In addition to changing the default Protection level you can access other settings options for each of the Protection tasks by selecting Protection - <desired task> - Settings - Customize. Each of the first three Protection tasks, File, Email, and Web all have a Customize option in their Settings window with various options appropriate for each task. For example the File Anti Virus task can be customized to scan all files that are accessed instead of only new or modified files. The Email Anti Virus task can be customized to scan only incoming email but to scan all attachments. The Web Anti Virus task offers its own customizable options which are covered in the new features section below.

Performance Tip: *If you have more than one computer in your home network and all of them are protected by Kaspersky, you may get better performance when accessing network shares if you disable the scanning of Network drives in real-time. To do this click the File Anti Virus link, then click the Settings icon. Next, click the Customize button. In the Custom Settings window click the Protection Scope tab and then uncheck the box next to Network Drives.*

How to keep KAV 6.0 from starting when the pc starts

This is an option that should be used by experienced users for troubleshooting purposes only. ICE Systems cannot guarantee the integrity of any computer that starts up without KAV Protective services running. In the event that this option needs to be activated, select Protection - Settings. In the Protection Settings window at the top is a box you can uncheck to keep KAV from starting at system startup.

How to exclude files or folders from real-time protection

Select Protection – Settings - Trusted Zone. Make sure the Exclusions Mask tab is selected in the Trusted Zone window and then click the Add button. In the Exclusion Mask window that opens make sure that only the Object box is selected, and then click the blue, underlined specify link in the Rule description box that appears at the bottom of the small window. You should now see the following:

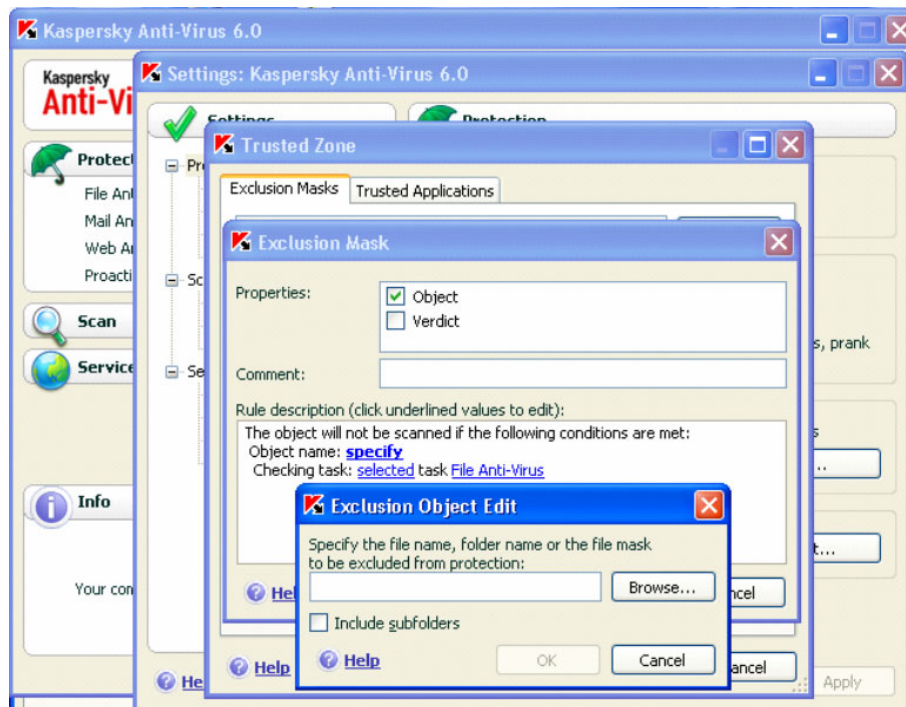


Figure 10 Exclusion mask.

Inside the Exclusion Object Edit window you can either manually type out the path to file or folder you wish to exclude or click the Browse button and use Windows Explorer. If you want to exclude a folder and all folders inside it make sure you click the Include subfolders box. Click the OK button when you are done adding your exclusion. You can now choose which to task to exclude the file(s) or folder(s) from by clicking the blue underlined selected or any link in the Exclusion Mask windows Rule Description section. Clicking selected will toggle the option to any and vice-versa, clicking the blue underlined task name (if selected is chosen) will allow you to choose additional tasks to exclude the file or folders from. When the any option is selected **all tasks, including on-demand scans**, will exclude the selected file(s) or folder(s). After clicking OK in the

Exclusion Mask window you will return to the Trusted Zone window where you can add additional exclusions or modify/delete existing ones.

How to exclude trusted Riskware from real-time protection

Knowing how to exclude trusted riskware (remember WinVNC?) in v5.0 used to be mandatory for many users. Thankfully v6.0 does not falsely detect the same programs it did in version 5.0 – namely the host of VNC products. In the event that KAV 6.0 does detect a program on your computer as Riskware that you do not want detected as such you can add the riskware mask Kaspersky reports to the list of trusted Riskware. For example to exclude all Remote Administration tools from riskware detection you would select Protection – Settings - Trusted Zone, make sure the Exclusion Masks tab is selected and then click the Add button. In the Exclusion Mask window that appears check the box in the Properties section marked Verdict. In the Rule Description section below Properties click the blue, underlined link specify. In the Verdict Type window that appears type *RemoteAdmin.*. Click the OK button and then choose the task or tasks you wish to exclude the RemoteAdmin programs from by clicking the selected or any blue, underlined link just as we did while excluding files and folders from specified tasks. When finished click the OK button again and continue to add new masks or modify/delete existing ones.

How to add Trusted Programs

Kaspersky Anti-Virus can create a list of trusted applications that need not have their file and network activity monitored, suspicious or otherwise. For example, you feel that objects used by Windows Notepad are safe and do not need to be scanned. In other words, you trust the processes of this program. After we successfully add Windows Notepad to the list of trusted programs files used by Notepad will no longer be scanned. Additional trust features are also available which we will cover in a minute.

To add Windows Notepad to the list of trusted applications select Protection - Settings Trusted Zones. In the Trusted Zone window that appears make sure the Trusted Applications tab is selected and then click the Add button. In the Trusted Applications window that appears click the Browse button and first look at the preloaded list of applications by clicking the Applications option that appears – if the program you want to add is not listed, as Notepad is not, click the Browse option and use Windows Explorer to locate the notepad.exe file. After selecting your trusted application you can modify the trust properties of the application via the Properties section. For more information on this subject please refer to the Help option in the Trusted Applications window.

How to save, load, and reset configuration settings

You can save, load or reset configuration associated with the Protection tasks, by selecting Protection – Settings - Settings Manager. The options here are pretty self-explanatory. When you save your config settings they are kept in a file with a .cfg extension, thus when you load a saved config the Settings Manager will look for a file

with a .cfg extension. The reset option is pretty cool. When you select this option you will be confronted with a window that displays various modified sections of the program that you can reset. After selecting what is to be reset the program will reset itself and guide you through the configuration setup as you did when the program was first installed.

How to disable Macro protection

The macro protection module is now found under the Proactive Defense task under the name Office Guard. To disable this feature select Protection – Proactive Defense – Settings. Uncheck the box next to Office Guard to disable macro protection. Customers using MS Access or MS Excel may need to turn this off if they experience poor performance while using these MS Office applications.

Scan how-to's

How to enable and schedule a full scan

Select Scan – My Computer – Settings. At the bottom of the My Computer Settings window is an option called Run Mode. If you click the box Every 1 day(s) the formerly grayed out Change button becomes active. Click the Change button and proceed to schedule your scan.

How to exclude files or folders from the My Computer or any other Scan task

Please see the associated How-to in the Protection section above. Exclusions created via the Protection-Settings-Trusted Zone option can be applied to all tasks - including the Scan tasks.

How to change the default protection level for a scan

Select Scan – <task desired> – Settings. Slide the security level bar to the desired protection level.

How to customize a Scan task and reset settings to default

Select Scan - <task desired> - Settings. In the scan settings window click the Customize button. To reset the task back to default levels, click the Default button next to Customize.

How to customize a scan to only scan new and modified files

Select Scan - <desired task> - Settings – Customize – General. In the Productivity section in the middle of the window click the box next to the option Scan new and changed files only.

How to create uniform scan settings for all scans

Select Scan – Settings. Set the Security level to the desired setting; click the Customize button and select the custom settings you want in place for all scans. When all settings have been configured click the Apply button at the bottom of the Scan Settings window. All scans will now inherit the newly customized settings.

How to disable I-Checker/I-Swift during scans

Select Scan - <task desired> - Settings – Customize – Advanced. Uncheck the features you wish to disable.

How to make sure Outlook .pst files are not scanned

Select Scan – My Computer – Settings – Customize – General. At the bottom of the custom settings window, in the Compound Files section, be sure the Parse email format files box is **not** checked.

Service how-to's

How to schedule updates

By default updates are scheduled to run automatically whenever a new set of definitions are available. If you wanted to schedule the updates to run at a regular interval or to be run manually, select Service – Update – Settings. In the Update settings window click the Manual option if desired or to schedule the task click the Every 1 day(s) option and then click the Change button. Choose the schedule you prefer in the window that appears after clicking the Change button.

How to configure a Proxy server connection for Updates

Select Service – Update – Settings – Customize. Click the Use Proxy option in the Update Configuration window, along with any other required proxy server settings.

How to manually start an Update

Select Service – Update. In the update window on the right side click the Update Now button.

How to add a license key file

Select the Service icon. In the bottom right portion of the Service window you will see license key details. Move your mouse over any portion of the license key details and click. A license key manager window will appear, click the Activate button. If you have a license key file for KAV 6.0 select the option Apply existing license key and click Next. If you have an activation code select the appropriate option and click Next. If you have a key file browse to the location on disk where the key is stored and double click it when located. If you have an activation code enter the information into the form and click Next.

How to enable Email Notifications

A neat new feature of KAV 6.0 is the ability to have email notifications sent to you when certain configurable events occur. To enable email notifications select Service – Settings. In the Service settings window at the top right you will see the Notifications section. Make sure the Enable notifications box is checked and click the Setting button. To configure which events you want email notification for select the Events tab and place a check mark in each box under the email column that wish to receive updates for. After you have selected your events click the Email settings tab and configure the From and To sections. In my test I used the same From and To email address as I was basically emailing myself the notification. Sorry web emailers, (Yahoo, HotMail, MSN) you need an email program that uses pop/smtp in order to use this feature.

From this same area of the interface you can also control what balloon messages (popups) you receive and what events play sounds on your computer when they occur. Figure 11 below shows the Notifications screen.

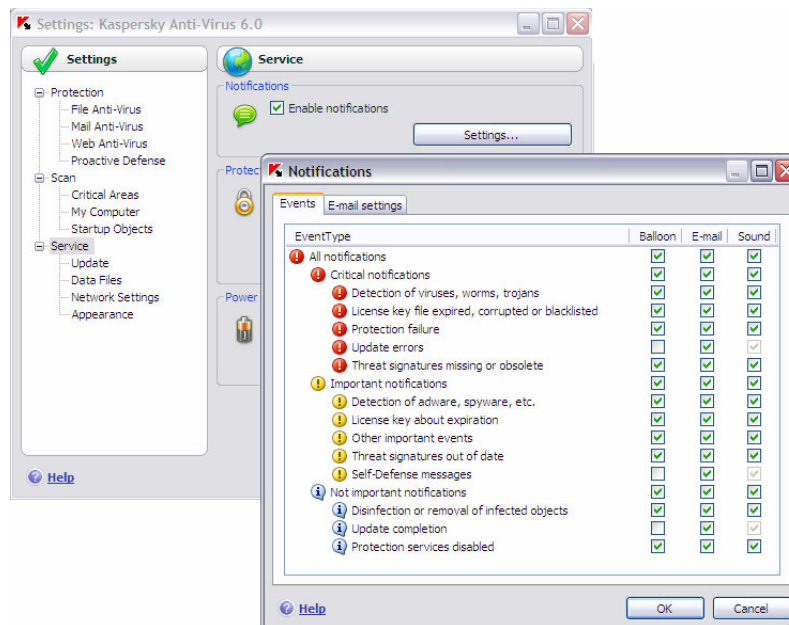


Figure 11 The Notifications option.

New Features, Queer Popups, and Reports

KAV 6.0 is loaded with new features – we will cover as many as possible using a format similar to our How-to section above.

Protection – Web Anti Virus

Earlier versions of KAV had an http scanner built-in but not with the configuration options available in KAV 6.0. To access the Web Anti Virus task settings, select Protection – Web Anti Virus – Settings. You can enable/disable this feature as well as configure the protection level as you did for the Files Anti Virus task. The only thing we should really mention here is that if you are having poor performance while surfing the net, slide the protection level bar to the lowest setting. For details on this feature please refer to the product doc.

Protection - ProActive Defense

Proactive Defense, in addition to housing the module formerly known as macro protection, also is the home of some real cool technology. KAV 6.0 has the ability to detect viruses and other threats prior to the viruses and threats being officially recognized, and before definitions can be created. Because viruses and threats behave in a certain way on your computer, KAV 6.0 can detect this behavior even if no definition for the cause of the behavior is known. For example, most viruses attempt to modify the Registry, especially the area that controls which programs start when the pc is booted. With **Registry Guard** (a subsection of Proactive Defense) enabled, any modification to the area of the Registry that manages startup programs will be blocked, a notification will be delivered to you via a **popup** (see Figures 12 and 13 below) or email and you will be given the option to allow the change or block it.

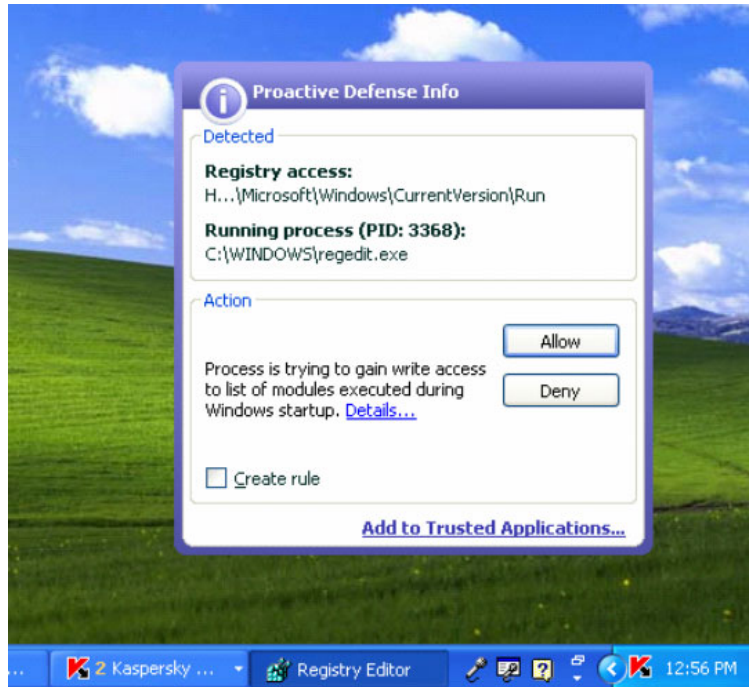


Figure 12 If a virus or other threat attempts to modify the registry, a popup similar to that seen above will appear. Unless you are installing software you should NEVER click the Allow button in the popup. Programs that you choose to install can safely modify the registry and should be allowed.



Figure 13 After clicking the Deny button in the popup seen in Figure 12, the following informational message will be displayed informing you that the process trying to modify your registry has been successfully blocked. By clicking the Details link additional information about the intruder can be collected. Click the blue x in the upper right corner to close the popup.

In addition to the Office Guard and Registry Guard modules, the Proactive Defense feature also includes the Application Activity Analyzer and the Application Integrity Control module.

The Application Activity Analyzer monitors behavior of otherwise safe programs that can be used to do dangerous things. For example, links embedded in emails that open an Internet Explorer window are normally safe – however this is a method that bad guys use to misdirect users to fake websites or sites that might download malicious programs to your computer. More experienced users can safely disable this specific element of the Application Activity Analyzer; new users will want to keep it turned on. With this feature enabled, any access to a web page via an emailed link will cause an alert to be generated, followed by a request to the user to allow or deny the activity. See below figure 12 for an example.

In Figure 14 we can see that an email was sent containing a link to www.espn.com, a known safe site. If the link is sent from a known sender and the link is recognized it of course could be allowed. Anytime you receive links from unknown senders the Deny button should be clicked.

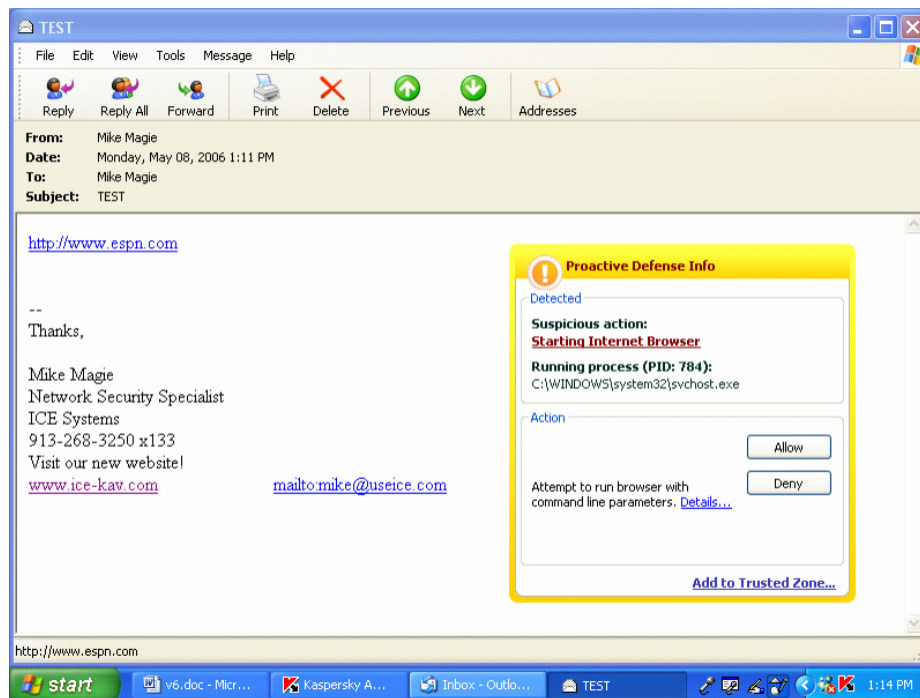


Figure 14 With the Application Activity Analyzer operating with default settings, attempts to access web pages via embedded email links will generate the following popup message.

The last feature included in the Proactive Defense section of the Protection area is the Application Integrity Control module. This element of the Protective Defense section ensures that all applications that are trusted, (Windows programs needed to run in order for the pc to operate correctly) run as they are supposed to. Some viruses will try to embed code in critical Windows files – all known viruses that do this have been identified by Kaspersky, your computer is safe from these. But if a new threat is released that does not have a known definition for cleanup, the Application Integrity Control module will protect you by examining the behavior of otherwise trusted Windows

programs; if they perform operations outside of their normal scope this Application Integrity Control module will whack them off at their knees.

Service – Enable Self Defense

The Enable Self Defense feature protects the Kaspersky program files, registry entries, and memory processes from being deleted or stopped. You can access this feature by selecting Service – Settings, in the Protection section of the Service settings window you will see the box to enable Self Defense. No notification message appears if anyone tries to delete a file or kill a process, but a notification can be configured by clicking the Settings button located in the Notifications section (refer to Figure 11 above).

With our notification configured, any attempts to kill a process or remove a KAV file/registry entry will result in a balloon/popup as seen in Figure 15 below:



Figure 15 This popup appears only after we configured it. Note how the message indicates that there is nothing for us to do.

Service – Disable external service control

This feature simply blocks any remote access tool, such as Windows Remote Desktop or WinVNC, from connecting to and accessing your pc.

Reports

You can access report information for all tasks by clicking on any part of the Statistics section in the program interface for any task. For example if I click on any link in the Statistics section for the Web Anti Virus task I will see report details associated with the Web Anti Virus task, as seen below in Figure 16:

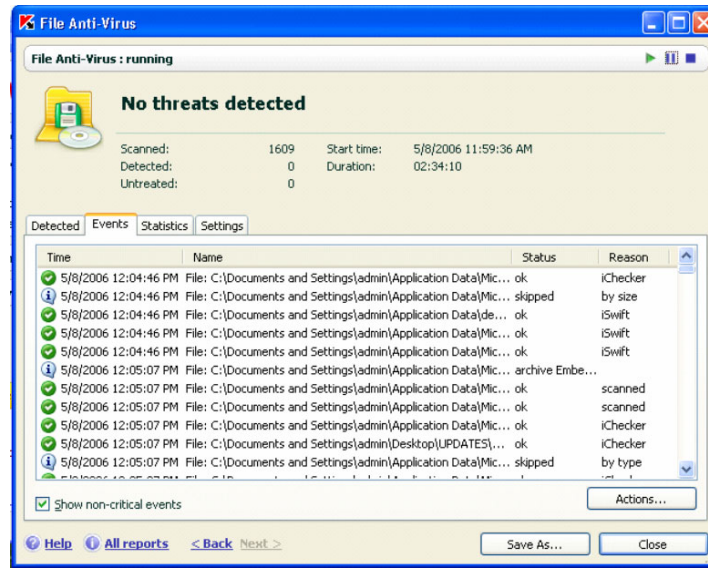


Figure 16

By clicking the Save As button I can save the entire Web Anti Virus report to a text file. If I wanted to see reports for additional tasks I would click the All reports link highlighted in orange at the bottom of the screen. Figure 17 shows the window displayed after clicking the All reports link:

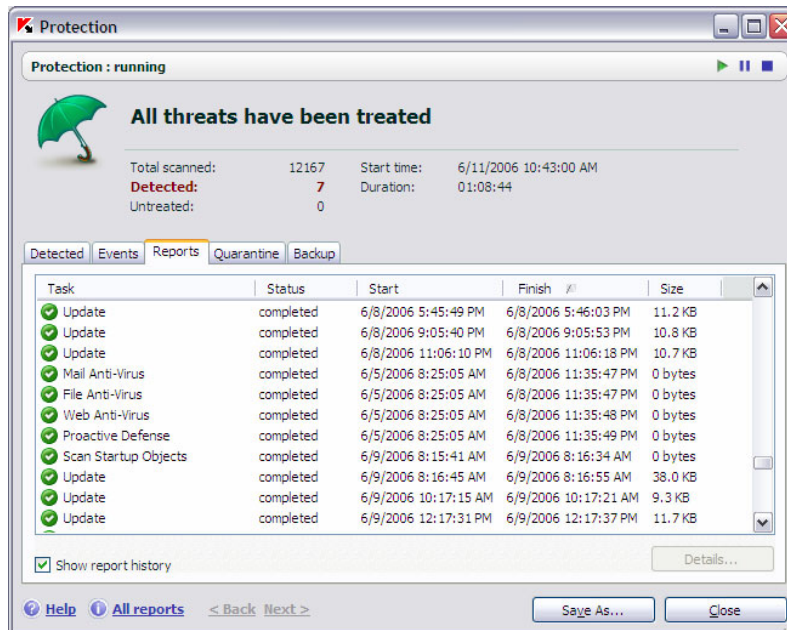


Figure 17 Shows a list of all tasks with associated reports. By double-clicking on any of the listed task items details regarding the task will be displayed.

Conclusion

Hopefully you are better equipped now to navigate your way through the new KAV 6.0 interface. There are a lot of changes in this release as we saw, but with this document, the Kaspersky product documentation and the program's built-in Help option you should be fine.

In the event that you do have a question that is not covered in one of the aforementioned sources please do call, email, or instant message us. We can be reached by phone at 877-332-3250, by email at support@ice-kav.com, or by instant message at www.ice-kav.com, look for the 'Live Chat Online' icon on our home page's upper right corner.