

New Features

Kaspersky[®] Anti-Virus 6.0
for Windows Servers

Contents

1 Introduction	3
2 Antivirus protection	3
3 New services	5

1 Introduction

In this document, we provide an overview of the new features offered in Kaspersky® Anti-Virus 6.0 for Windows Servers, describing the new functions and services available and explanations for how these benefit the user and/or system administrator.

2 Antivirus protection

Protection for the file server launches at the operating system startup, and continues running in the operating memory, scanning all files that are opened, saved or launched by users or other program files. Crucially, our antivirus protection allows the user to designate areas of the computer for on demand scanning. Individual objects (e.g., files, catalogs, disks and removable storage devices) can be singled out for scanning, or alternatively, the system administrator can request a full computer scan. On demand scanning tasks preclude the spread of malicious code that is already present on the computer.

Function	Description
iSwift and iChecker scan acceleration technologies	When on demand scanning is first launched, the program scans all objects. Subsequent scans are carried out only on new and modified files. Acceleration technologies increase the program's performance several times over.
On access mode	<p>The antivirus monitor has several operating modes to choose from. The administrator/user may wish to limit further scanning tasks to avoid repeatedly rescanning the same object needlessly by choosing one of four operating modes.</p> <ol style="list-style-type: none"> 1. Smart mode. The program analyzes the number, type and sequence of operations executed by an object to decide whether it requires scanning. <p>For example, when working with Microsoft Office documents, the program scans files only when they are opened and closed, which is sufficient to detect an infected file. All intermediary operations, such as converting or saving the file, do not trigger scanning.</p> <ol style="list-style-type: none"> 2. On access or modification. 3. On access. 4. On execution. <p>Since repeated and superfluous scans are avoided, this capability heightens the solution's performance.</p>
New algorithm for scanning compound objects	Scanning of compound objects that have complex structures (for example, archives and mail databases) has been optimized saving time and resources.
System restore after infection	After the program has detected and removed a malicious object, it also removes all traces of the object from system files and registry, thus preventing any future problems for the operating system.

Scanning of critical system areas	This task launches a scan of all the areas of the operating system that are most vulnerable to infection. Conducting a scan of startup objects, for instance, can help prevent viruses from being launched when the system is booted and can detect rootkits.
Protection from self-defense	Usually, when a file is used by one application, it is not accessible to other applications. Some malicious programs imitate processes by a legitimate application to prevent the antivirus program from accessing files. Kaspersky Anti-Virus 6.0 for Windows Servers detects these processes by malicious programs.
Scan suspension	When the server experiences peak loads, the application reduces the antivirus system's solution's demand on system resources. Scanning continues in the background mode, which does not impede the user's work with other applications.
Four scan completion modes	The administrator can specify one of four regimes once a scan task has completed: restart, standby, hibernate or shut down. For example, after the administrator has remotely scanned the server, the administrator can put the computer into standby mode to economize energy.
Disinfection of download sectors on the hard disk and removable disks	If hard disk sectors and/or removable storage devices become infected, it is possible to restore them using clean copies that were saved earlier. If copies have not been made, the administrator can simply use a standard version of the download sectors.
Choice of user accounts for scanning	Using the impersonation function, the administrator can launch a scanning task using another user account. This is essential for networks where system administrators have different access privileges. In order to fully scan the file system, an administrator may need to use another user account (which has full access privileges).
Flexible settings for time limits	Conducting a full scan on the server can take quite a long time, since file servers usually contain large quantities of data. This function allows the administrator to specify a start and end time for scanning. Administrators can choose the quietest times for scanning, for example, overnight.
Launching multiple copies of the antivirus engine	When using the application on multi-process servers, it is possible to launch multiple copies of the antivirus engine simultaneously. This option significantly increases the speed of antivirus scanning, since the program can scan a greater number of objects at any given moment.
Distributing load across server processors	When using the solution on multi-processor servers, the administrator can configure the program to only use specified processors. This technology ensures that the solution uses server resources as efficiently as possible. For example, the administrator may choose to exclude the processor that deals with databases from use by the antivirus solution.
Isolation of infected workstations	If a workstation becomes infected, the antivirus solution on the file server temporarily prevents the user from accessing network resources. This gives the administrator time to track down the source of infection and treat the workstation.
Pause button for antivirus scanning	Antivirus scanning can be paused at any time (and resumed as necessary) to prevent the program from rescanning objects needlessly.

3 New services

Function	Description
Centralized administration	The Kaspersky® Administration Kit provides administration tools to remotely and centrally manage all Kaspersky Lab solutions on the network.
iSwift technology	All version 6.0 products from Kaspersky Lab use iSwift technology, which ensures that the program does not rescan files on the computer needlessly. A good example of how iSwift technology can improve the efficiency of the system is a network where Kaspersky Anti-Virus is installed on the server and on workstations. Once a file has been scanned by the antivirus solution on the server, iSwift ensures that it is not scanned again when it arrives on the workstation. Naturally, scanning time is significantly reduced and files are delivered to users with minimal delay.
Configuration Wizard	This tool allows the administrator to configure all of the essential settings for the product during installation (such as security levels, schedules for updates and computer scans, etc.)
Configuration of notifications	The administrator can tailor notifications about events on the network (for instance, when a virus is detected or there is a system conflict), deciding when notifications are sent, the method of delivery and alert sounds.
Self-defense	This new technology makes it difficult for malicious programs to combat the antivirus protection, foiling attempts to shut down antivirus tasks or remove the program from the list of startup objects.
Retaining databases and license keys	When removing the product, the administrator can retain license keys and antivirus databases on the computer for future use.
Installation on infected computers	This component makes it possible to install the antivirus solution even on computers that already have malicious programs active in the operating memory.
Small updates	Updates to the antivirus databases have been reduced in size. Incremental updates amount to no more than several tens of kilobytes.