

for Microsoft Windows

Kaspersky Lab Corporate Products

KASPERSKY Lab

CONTENTS

Kaspersky Lab: experts in data security 3

Advanced Technologies by Kaspersky Lab 4

Corporate Network Protection Today 5

Protection for File Servers and Workstations

Kaspersky® Anti-Virus for Windows Workstations 9

Kaspersky® Anti-Virus for Windows File Server 11

Corporate Mail Protection

Kaspersky® Security for Microsoft Exchange Server 2003 15

Kaspersky® Anti-Virus for Microsoft Exchange Server 2000/2003 17

Protection for Internet Traffic

Kaspersky® Anti-Virus for Microsoft ISA Server 21

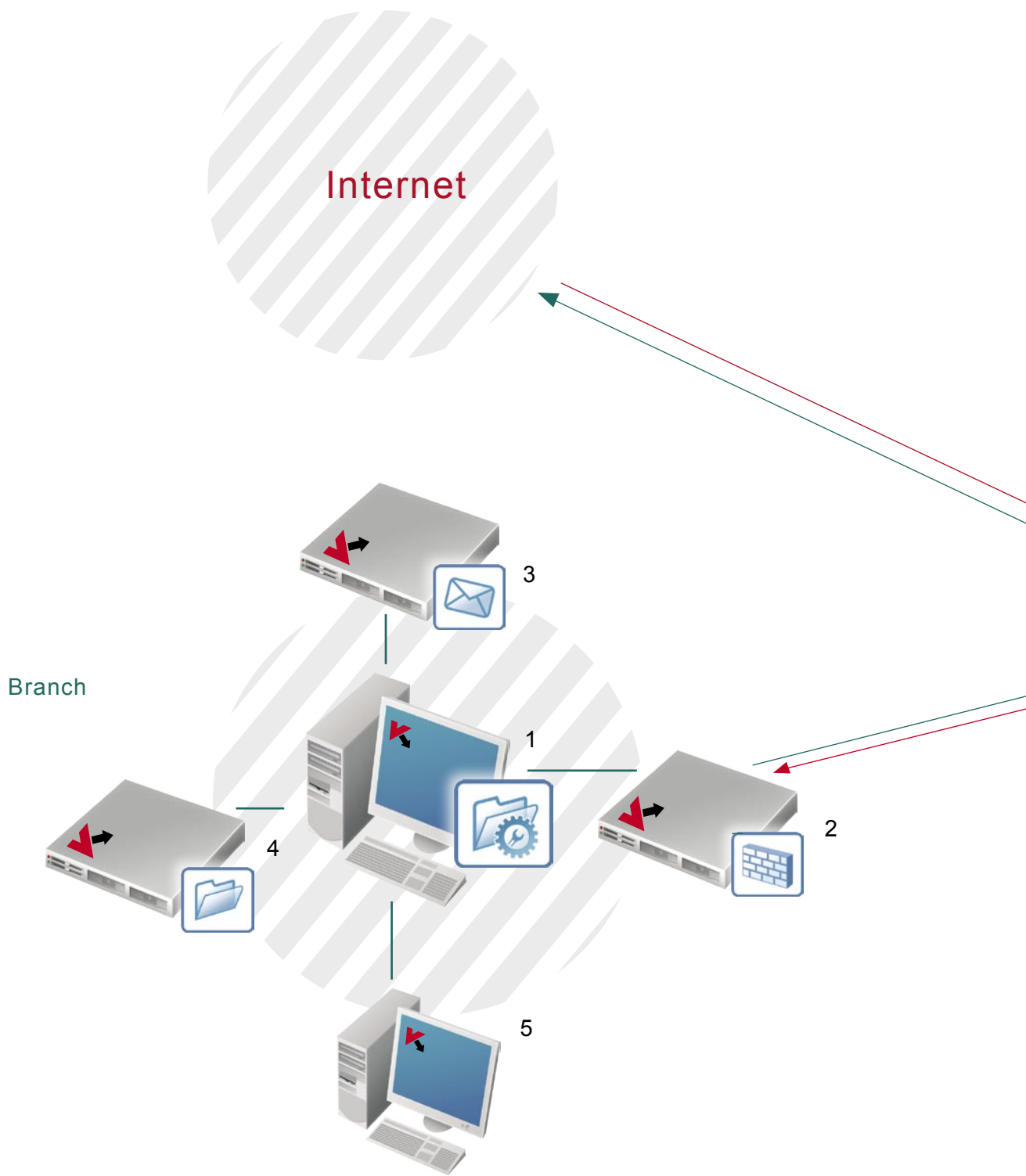
Protection of Mobile Devices

Kaspersky® Security for PDA 25

Centralized Administration System

Kaspersky® Administration Kit 29

Services 31



- 1 Kaspersky Administration Kit
- 2 Kaspersky Anti-Virus for Microsoft ISA Server
- 3 Kaspersky Security for Microsoft Exchange Server 2003 or Kaspersky Anti-Virus for Microsoft Exchange Server 2000/2003

Kaspersky Lab: experts in data security

Kaspersky Lab is an acknowledged leader in developing protection against viruses, spyware, adware, spam and hacker attacks.

In over a decade and a half of fighting viruses and other IT threats, we at Kaspersky Lab have amassed knowledge and experience that allows us to foresee trends in malware development. This is the main advantage we bring to our services and products. We are always one step ahead of our competitors in offering our customers the best protection possible.

Kaspersky Lab customers have access to a wide range of additional services guaranteeing complete conformity with all business requirements. We design, implement and support enterprise-wide antivirus systems. Our customers receive hourly antivirus database updates and we offer our users round-the-clock technical support in several languages.

The quality of Kaspersky Lab products is confirmed by certificates issued by leading hardware and software vendors, including Microsoft, IBM, Intel, Novell and others.

Advanced Technologies by Kaspersky Lab

Kaspersky Lab developed many of the technologies which are in place in contemporary antivirus solutions. These technologies are available in our own products, as well as our technology partners' products: F-Secure (Finland), G-Data (Germany), Sybari (US), Blue Coat (US), Clearswift (UK), Astaro (Germany), Alcatel (France), ZyXEL (Taiwan), and BlackSpider (UK).


Kaspersky Lab's antivirus technologies combine high detection rates for malicious code with minimal false positives, ensuring effective protection against all known virus threats and offering complete security for important information. A distinctive feature of Kaspersky Lab's antivirus engine is its ability to recognize and scan for viruses in a broad range of archived and compressed file formats. The heuristic analyzer, intrusion prevention system (IPS) and behavior blocker provide proactive protection against even the newest malicious code. Hourly updates keep the antivirus databases and engine up-to-date.

The effectiveness of the company's antivirus technologies has been confirmed numerous times by independent testing labs, which regularly compare the most popular antivirus products on the market. Kaspersky Lab has to its credit such well known awards and certificates as the VB100% awarded by Virus Bulletin, an authoritative industry magazine, Checkmark awarded by the British West Coast Labs, ICSA Certified by ICSA Labs, a research laboratory, and many others.

Corporate Network Protection Today

One of the main criteria used to assess how effectively a company's network infrastructure is protected against electronic threats is whether the protection covers all network nodes. This is due to the variety of ways in which unwanted guests can penetrate a local area network, as well as the growing sophistication of these attacks. Setting up an integrated antivirus system requires implementing a complex set of procedures, including installation of the appropriate software on Internet gateways and workstations, mail and file servers, ensuring control of mobile user activity and setting up centralized administration of the antivirus system. This helps ensure high response speed and reliable protection against external as well as internal electronic threats.

One of the more significant trends in the development of the information security industry is the use of different vendor solutions on one network. Although no existing antivirus technology guarantees absolute protection against malicious code, combining products developed by different vendors and based on different antivirus protection technologies allows a company to increase its level of protection against contemporary cyber threats.



The days when hackers acting on their own posed the main threat to corporate networks are long gone. Today, this is a business just like developing software to protect networks. Under such conditions corporate information systems need full scale protection. Keeping antivirus protection up to date is the best defense. This is why new threat response speed is becoming an ever more important criterion for choosing an antivirus solution.

Kaspersky Lab offers companies a complete product line that includes products that provide comprehensive protection of all nodes on a corporate network: solutions that provide antivirus scanning of the mail and web traffic, file servers and workstations, as well as centralized administration tools. The company releases antivirus database updates every hour and leads the market in new threat response speed.

ΚΑΣΠΕΡΙΚΥ lab

PROTECTION
for FILE SERVERS
& WORKSTATIONS

Kaspersky® Anti-Virus for Windows Workstations

Kaspersky® Anti-Virus for Windows Workstations is an integrated solution that protects workstations against viruses and malicious programs and supports centralized administration.

FEATURES

Effective antivirus protection

Scanning of all files and drives

The application scans all files for viruses as they are executed, created or modified. The program also performs antivirus scans of data on local and network drives on demand – set by the user or administrator.

Email scanning

The program automatically scans all incoming and outgoing email for viruses and disinfects incoming mail. The program can also scan databases of various email clients on demand and disinfect Microsoft Outlook and Outlook Express email databases.

Protection against potentially hostile programs

When using extended antivirus databases, the application provides protection not only against malicious software, but against potentially hostile programs as well. These include utilities used to remotely monitor and control victim computers (e.g., spyware), programs that automatically establish modem connections with pay sites (e.g., dialers), etc.

Proactive protection of Microsoft Office applications

The Office Guard™ module monitors all macros executed in Microsoft Office documents and blocks any suspicious action.

Backup copies

Copies of infected objects can be saved in a backup storage prior to treatment making it possible to restore important information if treatment of an object results in an error.

Performance Optimization

Optimization for Intel Centrino for mobile PCs

If the Internet connection is disrupted or broken while downloading an update, the process will be automatically resumed when connection resumes and the portion already downloaded by the user will be automatically saved and will not need to be downloaded again. The solution is designed to save battery power and cancels on schedule scanning of the computer if battery power is low.

List of trusted processes

By creating a list of trusted processes, the administrator can exclude some processes from antivirus scanning, thereby reducing system load.

PROTECTION FOR FILE SERVERS & WORKSTATIONS

Flexible Administration

Centralized control

The program is installed on workstations and administered using Kaspersky® Administration Kit. The application is used to configure the parameters of antivirus scanning for individual computers, create groups of workstations and define security policies for these groups, create reports on the system's operation, update antivirus databases, etc.

Notification and reporting

The administrator is notified by email or using the NetSend utility of network events related to the antivirus program's operation (such as the detection of a virus). Detailed reports provide comprehensive information on the status of antivirus protection and results of the application's operation for a specified time period.

Antivirus database updates

Updating of the antivirus database and program components on workstations is performed centrally, using Kaspersky Administration Kit. Depending upon configuration, updates are performed automatically or on demand, over the Internet from dedicated Kaspersky Lab servers or from specified local update servers.



Kaspersky Anti-Virus for Windows Workstations meets a series of Intel technical requirements and is designed to use Intel Centrino technology for mobile PCs to its best advantage: lower power consumption without sacrificing performance is achieved by suspending or postponing antivirus scanning; antivirus databases update automatically; and network traffic is reduced, since only the missing parts of updates are downloaded whenever the Internet connection is lost or interrupted.



The Designed for Microsoft Windows XP logo attests to the product's high quality and its faultless operation on Windows XP. Kaspersky Anti-Virus for Windows Workstations supports standard Windows installation procedures, removal and operation of software, computer-sharing capabilities (user sessions). The application does not result in system conflicts and is characterized by a high level of stability.

SYSTEM REQUIREMENTS

Microsoft Windows 98/Me/NT Workstations 4.0 with Service Pack 6 installed:

- Intel Pentium 133 MHz or higher for Windows 98/NT;
- Intel Pentium 150 MHz or higher for Windows Me;
- At least 32 MB RAM available;
- 50 MB of free space on the hard drive;

Microsoft Windows 2000 Professional with Service Pack 2 installed:

- Intel Pentium 133 MHz or higher;
- At least 64 MB RAM available;
- 50 MB of free space on the hard drive;

Microsoft Windows XP Home Edition and XP Professional:

- Intel Pentium 300 MHz or higher;
- At least 128 MB RAM available;
- 50 MB of free space on the hard drive.

Product version: 5.0

Available languages: English, French, German & Russian

Kaspersky® Anti-Virus for Windows File Server

Kaspersky® Anti-Virus for Windows File Server provides reliable antivirus protection for data servers running Windows NT Server 4.0, Windows 2000 Server and Windows Server 2003 (including the x64 Enterprise Edition).

FEATURES

Effective antivirus protection

Full-scale antivirus protection

The application protects the server's file system against malicious programs in real time. The administrator can also request more in-depth virus scans of the system.

Superior technologies

Kaspersky Anti-Virus for Windows File Server can detect viruses in archived and compressed files in over 1.200 formats and cure files in ZIP, ARJ, CAB and RAR archive formats. The program also provides protection against script viruses that penetrate computers via Internet browsers and email clients.

Choice of protection level

The system administrator can adjust the application's operating mode from maximum system performance to maximum user protection, depending upon the stringency of the company's security policy and the current virus situation.

Virus outbreak prevention

The application monitors virus activity, detects virus attacks, and gives the administrator a choice of rapid responses, e.g., launching a scan, updating databases or increasing the system's level of protection.

High Performance

Antivirus scanning optimization

The intelligent technologies iChecker™ and iStream™ enhance the application's performance and reduce the amount of RAM required for its operation.

Selection of trusted processes

The administrator can also increase the application's performance by excluding those processes from scanning that do not pose any potential threat, such as backup copying of data, hard disk defragmentation, etc.

PROTECTION FOR FILE SERVERS & WORKSTATIONS

Flexible administration

Centralized installation and management

Kaspersky Administration Kit is a centralized management system designed to remotely install and configure applications on several file servers simultaneously using the administrator's console installed on the administrator's machine.

Notifications and reports

The application can notify the administrator of events in the antivirus program's operation by creating entries in the Windows system log and the Kaspersky Administration Kit event log, as well as using email alerts and the NetSend tool. The centralized administration system enables the administrator to view different types of HTML reports on the status of antivirus protection for specified time periods.

Antivirus database updates

The antivirus database and program modules on file servers can be updated centrally using Kaspersky Administration Kit. Depending upon the configuration, updating is performed automatically or on demand, over the Internet from dedicated Kaspersky Lab servers or from specified local update servers. The program chooses the least loaded update server. If the connection is broken, only the remaining part of an antivirus database needs to be downloaded when the connection is restored.



Kaspersky Anti-Virus for Windows File Servers has been tested by VeriTest for compliance with Microsoft technical requirements and is approved for use on servers running Microsoft Windows Server 2003 Standard Edition. The application is fully compliant with security, reliability and stability standards for server applications and comes with highly qualified technical support. Kaspersky Anti-Virus for Windows File Servers was the first Russian application to be Certified for Microsoft Windows Server 2003 Standard Edition.



The CheckMark certificate awarded by West Coast Labs, an independent test lab, guarantees antivirus security when working with any data. Kaspersky Anti-Virus for Windows File Servers is one of the few products that successfully passed West Coast Labs testing in three categories: Anti-Virus Level 1, Anti-Virus Level 2 and Trojan. The program correctly identified all malicious programs in the test collection without any false positives and successfully performed the treatment.

SYSTEM REQUIREMENTS

Supported operating systems:

- Microsoft Windows NT 4.0 Server (with Service Pack 6a or higher)
- Microsoft Windows 2000 Server (with Service Pack 2 or higher)

- Microsoft Windows 2000 Advanced Server (with Service Pack 2 or higher)
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64

Product version: 5.0

Available languages:

English, French, German & Russian

PROTECTION for CORPORATE MAIL

Kaspersky® Security for Microsoft Exchange Server 2003

Kaspersky® Security for Microsoft Exchange Server provides antivirus scanning of incoming and outgoing messages and mail stored on the server, as well as messages in shared folders. It also helps mail system users to block unwanted mail by using intelligent spam recognition technologies in addition to technologies provided by Microsoft.

FEATURES

Reliable Protection against Spam

Intelligent technologies

The application scans all messages that are transferred to the Microsoft Exchange Server via the SMTP protocol for spam attributes based on filtering by formal attributes (e.g., email and IP addresses, message size, headers, etc.). It also analyzes message contents and attachments using intelligent technologies, including unique graphical signatures, which help detect spam in image form.

Mass mailing prevention

The product prevents the unauthorized use of the mail server by monitoring and blocking mass mailing attempts from computers within the organization.

Effective Antivirus Protection

Real time and on demand scanning

The program scans for and removes all types of viruses, worms, Trojans and other malicious programs from incoming and outgoing mail, including attachments in nearly all formats. Messages stored on the server are scanned in the background, ensuring that all objects are processed using the latest version of the antivirus databases without any noticeable increase in server load.

Detection of potentially hostile programs

When using the extended antivirus protection mode, the application can detect and remove not only known malicious code, but potentially hostile programs as well. These include programs that display advertising (i.e., adware), data collection programs (i.e., spyware) and other utilities that can be used by cyber criminals for their purposes.

Virus outbreak prevention

The application can monitor virus activity and detect outbreaks, allowing the system administrator to take action quickly – e.g., launch a scan, update databases or increase the system's level of protection.

Flexible Administration

Fine tuning

The administrator can adjust the application's performance depending on mail traffic and the number of users, and scan only potentially hostile objects by disabling scanning of certain file types.

Detailed reports

The system administrator can control the operation of the application and the antivirus protection status using descriptive HTML reports or by viewing the Windows event log. The frequency with which reports are generated and the information to be included in reports is configured by the system administrator.

Centralized administration

The application is configured and administered via the administration console built into the Microsoft Management Console (MMC), a convenient management tool familiar to administrators, or using the Kaspersky Administration Kit.

Automatic updates

The antivirus database can be updated centrally, using the Kaspersky Administration Kit. Depending upon configuration, updating is performed automatically or on demand over the Internet from Kaspersky Lab servers or from local update servers specified by the administrator. Some modules of the antivirus engine and linguistic analyzer can also be updated together with the databases. Antivirus and spam recognition databases can be updated separately.

SYSTEM REQUIREMENTS

Hardware requirements

- CPU: Intel Pentium 300 MHz or higher;
- 256 MB of RAM available (recommended); and,
- 50 MB free disk space for the installation of the application (not including disk space required for backup storage and other service folders).

Software requirements

- Requirements for Microsoft Exchange Server 2003 Enterprise Edition protected by the solution:
- Microsoft Windows 2000 Server with Service Pack 4 or higher installed / Microsoft Windows 2000 Advanced Server with Service Pack 4 or higher installed / Microsoft Windows Server 2003 Standard Edition or higher / Microsoft Windows Server 2003 Enterprise Edition or higher;
 - Microsoft Exchange Server 2003 Enterprise Edition or higher.

Requirements for Microsoft Exchange Server 2003 Standard Edition protected by the solution:

- Microsoft Windows 2000 Server with Service Pack 4 or higher installed / Microsoft Windows 2000 Advanced Server with Service Pack 4 or higher installed / Microsoft Windows Server 2003 Standard Edition or higher / Microsoft Windows Server 2003 Enterprise Edition or higher;
- Microsoft Exchange Server 2003 Standard Edition or higher.

Requirements for the computer used for system administration:

- Microsoft Windows 2000 with Service Pack 4 or higher installed / Microsoft Windows XP / Microsoft Windows 2003 and MMC version 1.2 or higher.

Product version: 5.5

Available languages:

English, French, German & Russian

Kaspersky® Anti-Virus for Microsoft Exchange Server 2000/2003

Kaspersky® Anti-Virus for Microsoft Exchange Server is a high performance scalable solution designed to protect mail system users against malicious code. The application's seamless integration with the Microsoft Exchange Server ensures effective detection and removal of viruses, creating a reliable barrier to their penetration onto the corporate network.

FEATURES

Effective Antivirus Protection

Real time scanning of email messages

The application scans incoming and outgoing messages for viruses in real time. All message elements, such as attachments (including archived and compressed), embedded OLE objects and attached messages are scanned. Depending upon the application's configuration, infected objects are treated or deleted.

Antivirus scanning of email databases

The program is capable of removing viruses from messages received prior to the program's installation and, after antivirus databases are updated, from previously scanned messages. Such scanning can be performed in the background or from time to time, according to a schedule set by the administrator.

Virus outbreak prevention

The virus outbreak recognition mechanism enables the administrator to take any necessary measures to strengthen the antivirus protection of the mail server. When the predefined virus activity threshold is reached the network administrator is notified by email or using the NetSend tool.

Backup copying of objects

Backup copying makes it possible to restore information if an attempt to treat infected objects results in an error and to send such objects for analysis to Kaspersky Lab experts. User defined filters facilitate searching for objects in the backup storage.

High Performance and Scalability

Performance optimization

The administrator can configure the application based on traffic volume and type and the hardware characteristics of the server (amount of RAM, performance, number of CPUs, etc.). Up to eight different objects can be scanned in parallel in RAM, each up to 1 MB.

Scalability

When running on multiprocessor systems, the application is scaled according to the number of processors installed on the server protected. Several copies of the antivirus engine can be launched to increase the application's performance.

Flexible Administration

Ease of administration

The application is administered using a plugin for Microsoft Management Console (MMC). During installation the program runs with the optimal settings recommended by Kaspersky Lab specialists. The administrator can customize the application's settings either locally or remotely.

Flexible reporting

Reports on the status of antivirus protection are regularly generated based on predefined templates either automatically or on the administrator's demand. Logging of events in the Windows application log and the program's own logs provides a complete diagnosis of Kaspersky Anti-Virus.

Automatic updates

The antivirus database and program modules are updated automatically or on demand, over the Internet from dedicated Kaspersky Lab servers or from local update servers.

SYSTEM REQUIREMENTS

Requirements for Microsoft Exchange 2000 Server Enterprise Edition protected by the solution:

- Microsoft Windows Server 2000 / Microsoft Windows 2000 Advanced Server with Service Pack 4 or higher installed
- Microsoft Exchange 2000 Server Enterprise Edition with Service Pack 2 or higher installed

Requirements for Microsoft Exchange 2000 Server Standard Edition protected by the solution:

- Microsoft Windows Server 2000 / Microsoft Windows 2000 Advanced Server with Service Pack 4 or higher installed
- Microsoft Exchange 2000 Server Standard Edition with Service Pack 2 or higher installed

Requirements for Microsoft Exchange Server 2003 Enterprise Edition protected by the solution:

- Microsoft Windows Server 2000 with Service Pack 4 or higher installed / Microsoft Windows 2000 Advanced Server with Service Pack 4 or higher installed / Windows Server 2003 Standard Edition / Windows Server 2003 Enterprise Edition
- Microsoft Exchange Server 2003 Enterprise Edition

Requirements for Microsoft Exchange Server 2003 Standard Edition protected by the solution:

- Microsoft Windows Server 2000 with Service Pack 4 or higher installed / Microsoft Windows 2000 Advanced Server with Service Pack 4 or higher installed / Windows Server 2003 Standard Edition / Windows Server 2003 Enterprise Edition
- Microsoft Exchange Server 2003 Standard Edition

Requirements for the computer used for system administration:

- Microsoft Windows 2000 with Service Pack 4 or higher installed / Microsoft Windows XP / Microsoft Windows 2003 with MMC version 1.2 or higher
- Active Directory Service Interfaces (ADSI) 2.5 or Active Directory Client Extensions (Microsoft Windows 2000 or higher automatically meets this requirement)

Hardware requirements

- CPU: Intel Pentium 300 MHz or higher;
- 256 MB RAM available;
- 20 MB free space on the hard drive for installation of the application (not including disk space required for backup storage and other service folders).

Product version: 5.5
Available languages: English, French, German & Russian

PROTECTION for INTERNET TRAFFIC

Kaspersky® Anti-Virus for Microsoft ISA Server

Kaspersky® Anti-Virus for Microsoft ISA Server filters Internet traffic entering local area networks and blocks infected objects. The application can run on server arrays and offers flexible centralized administration of settings on all servers in the array.

FEATURES

Integrated Protection against Viruses and Malicious Code

Real time antivirus scanning

The program scans data traffic transferred via the Microsoft ISA Server and removes all types of viruses. Objects scanned by the solution include archived and compressed files in over 1.200 formats. Data in ZIP, CAB, RAR and ARJ archives can be disinfected. A unique heuristic analyzer detects unknown viruses for which signatures have not yet been added to the database.

Automatic selection of installation mode

The set of data filters to be installed (HTTP, FTP or web filter) is determined automatically during installation of Kaspersky Anti-Virus. The selection of filter types depends on the current operating mode of Microsoft ISA Server: Firewall, Proxy or Integrated.

Protection against potentially hostile programs¹

Extended databases can be used to detect not only malicious software, but also potentially hostile programs, such as programs used to remotely monitor and control victim computers (i.e., spyware), programs that automatically establish modem connections with pay sites (i.e., dialers), etc.

Performance Optimization

Launching several copies of the antivirus engine

Kaspersky Anti-Virus for Microsoft ISA Server is capable of scanning large volumes of data without reducing the server's performance. Up to 32 copies of the program's antivirus engine (depending upon the number of CPUs installed on the server) can be launched and run simultaneously.

Trusted objects and servers

The administrator can exclude from scanning certain object types that do not pose any potential threat in order to reduce server load. Traffic received from servers included by the administrator in the "trusted" list can also be excluded from antivirus scanning.

Optimization for Intel Xeon

The product is optimized for computers with Intel Xeon² processors used in dual-processor servers.

Flexible Management and Administration

Centralized management

The application can be managed either locally or remotely, using the Microsoft Management Console or Kaspersky Administration Kit³. The administrator can configure the parameters for all servers in an array, define security policies for user groups, view reports on the application's operation and update antivirus databases.

Notification and reporting

The administrator supervises the program's operation by viewing Windows and Microsoft ISA Server system logs, as well as the Kaspersky Anti-Virus log, in which event types specified by the administrator are recorded. The administrator can also define events following which the system will send notifications by email and, within a local area network, using the NetSend tool.

Automatic updates

The antivirus database and program modules can be updated centrally, using the Kaspersky Administration Kit. Depending upon configuration, updating is performed automatically or on demand, over the Internet from Kaspersky Lab dedicated servers or from local update servers specified by the administrator.



Kaspersky Anti-Virus for Microsoft ISA Server 2000/2004 Enterprise Edition is optimized for Xeon processors in order to fully benefit from the high performance and scalability of modern 64-bit and multiple-processor servers based on the Intel Xeon technology. The software product complies with a range of requirements, including support for such functions as processor performance optimization and multithreading.



Kaspersky Anti-Virus for Microsoft ISA Server 2000/2004 Enterprise Edition was developed with the technical requirements of Microsoft in mind. This enabled the product to successfully pass VeriTest testing. The product correctly operates on servers running Microsoft Internet Security and Acceleration Server 2000/2004 Enterprise Edition, without negatively affecting the system's stability and configuration and without limiting the functionality of Microsoft ISA Server.

SYSTEM REQUIREMENTS

Kaspersky Anti-Virus for Microsoft ISA Server 2000 Standard Edition

Software requirements:

- Microsoft Internet Security and Acceleration Server 2000 with Service Pack 1 installed on the following platforms:
- Microsoft Windows Server 2003 Standard / Enterprise Edition
- Microsoft Windows 2000 Server with Service Pack 3 or higher.
- Microsoft Windows 2000 Advanced Server with Service Pack 3 or higher

Hardware requirements:

- Intel Pentium II 300 MHz or higher
- 256 MB of RAM available
- At least 20 MB of free space on the hard drive for installation of the application

- At least 200 MB of free space on the hard drive for temporary storage of data prior to antivirus scanning

Product version: 5.1

Kaspersky Anti-Virus for Microsoft ISA Server 2000/2004 Enterprise Edition

Software requirements:

- Microsoft Internet Security and Acceleration Server 2000/2004 Enterprise Edition with the latest Service Pack installed on the following platforms:
- Microsoft Windows Server 2003 Standard / Enterprise Edition
- Microsoft Windows 2000 Server with Service Pack 4 or higher
- Microsoft Windows 2000 Advanced Server with Service Pack 4 or higher

Hardware requirements:

- Intel Pentium II 300 MHz
- 256 MB of RAM available
- At least 50 MB of free space on the hard drive for installation of the application
- At least 200 MB of free space on the hard drive for temporary storage of data prior to antivirus scanning

Product version: 5.6 / 5.5
Available languages:
English & Russian

^{1,2,3} For Microsoft ISA Server Enterprise Edition only

KASPERSKY lab

PROTECTION for MOBILE DEVICES

Kaspersky® Security for PDA

Kaspersky® Security for PDA is designed to protect pocket-size computers (PDAs) and smartphones against viruses and unauthorized data access.

FEATURES

Solution for Microsoft Smartphone

Memory and memory card scanning

Kaspersky Anti-Virus for Microsoft Smartphone can be used to scan both the device memory and memory extension cards for viruses. Antivirus scanning is launched upon user demand. If a virus is detected, the program can delete the infected object.

Automatic Updates

Databases are updated manually by copying the antivirus database file downloaded from Kaspersky Lab's Internet server to a specified folder in the smartphone's memory.

Solution for Pocket PC-based PDAs

Antivirus protection for PDAs

The Kaspersky Anti-Virus component monitors all attempts to access file system objects and databases on the PDA in real time, e.g., during PC synchronization, wireless data exchanges with other devices and when receiving email. The program can also perform full antivirus scans of the PDA and objects on connected memory extension cards. If a virus is detected, the program can delete the infected object and save a backup copy.

Automatic updates

The antivirus database can be updated on demand or automatically according to a user defined schedule from Kaspersky Lab Internet servers or from a specified local folder on the PDA.

Cryptographic protection of data

The DataSafe component protects confidential data against unauthorized access by encrypting information. The user selects an encryption algorithm and sets an access password for the object. The application encrypts data "on the fly" — that is, information is decrypted every time it is accessed and encrypted as it is saved.

Solution for Palm OS-based PDAs

Antivirus protection for PDAs

Files can be scanned for viruses during PC synchronization or when receiving data from another device using any method, including via the infrared port or Bluetooth, or when launching applications.

Memory card scanning

The program can scan objects for viruses in the device's memory and on connected memory extension cards upon user demand. If an infected object is detected, the program can automatically or upon user demand delete the infected object or record the event in the scan report file.

Automatic updates

The antivirus database can be updated on user demand or automatically on a predefined schedule by synchronizing with another PDA or PC. The program for downloading updates from Kaspersky Lab's Internet servers to the personal computer is supplied with Kaspersky Security for PDA.

Protection against unauthorized access

The DataSafe component protects confidential data by encrypting the information stored on the PDA and blocking access to the device. It is impossible to use the PDA and gain access to the data without knowing the password set by the user.

SYSTEM REQUIREMENTS

Pocket PC-based PDAs:

- ARM / XScale family processor;
- Microsoft Pocket PC 2002/2003 operating system;
- At least 600 KB of available RAM;
- At least 550 KB available disk space.

Palm OS-based PDAs:

- Operating system: Palm OS 3.x, 4.x, 5.x. E.g., Palm III, Palm m10x, Palm m50x, Tungsten T (T2,T3), Sony TG-50;
- At least 100 KB of available RAM.

Windows CE-based smartphones:

- ARM / XScale family processor;
- Microsoft Smartphone 2002 / Windows Mobile 2003 for Smartphone operating system;
- At least 100 KB available RAM;
- At least 100 KB available disk space.

A personal computer is required for the installation of Kaspersky Security for PDA. The PC should meet the following requirements:

- Operating system: Windows 98/ME/NT 4/2000/XP;
- Computer synchronization software installed;
- For Pocket PC: Microsoft ActiveSync;
- For Palm OS: Palm Desktop, HotSync;
- Connection cradle for synchronization with the PC.

Product version: 5.5
Available languages: English & German

CENTRALIZED ADMINISTRATION SYSTEM

Kaspersky® Administration Kit

Kaspersky® Administration Kit is a powerful and flexible tool enabling enterprises to create integrated antivirus systems based on Kaspersky Lab secure content management solutions. Kaspersky Administration Kit has been specifically developed for companies of any size and complexity. It provides centralized management of antivirus protection on even the most complex networks that have tens of thousands of nodes and support remote offices and mobile users.

PRODUCT PHILOSOPHY

Versatility and scalability

Kaspersky Administration Kit enables effective management of antivirus protection on hierarchical networks of any complexity and configuration. Communication between administrative servers and clients is enabled on networks using dedicated lines, VPN, firewalls and proxy servers.

Administration from a single location

Without leaving their work place, network administrators can deploy antivirus protection, set application parameters, keep antivirus databases and program modules fully updated, continuously monitor system status and respond effectively to critical situations.

Continual control

Data on administration servers and client computers (including laptops) is regularly synchronized to update security policies and download tasks from the server. This also ensures that the administrator receives up-to-the-minute information on network incidents, even to remote locations.

Minimal disruption to user work

Administrators can perform all tasks related to deploying and maintaining antivirus protection on corporate networks remotely, without having to disrupt end user work. This ensures that the installation, set up and operation of the antivirus application has hardly any impact on end users.

Security

Kaspersky Administration Kit provides a whole new level of security. It is now possible to configure role and task definitions for administrators, audit their activities and exchange information on the administrative network through a protected SSL connection. By operating the antivirus program in non-interactive mode, administrators can ensure that users do not make local changes to application settings that could put their system at risk.

Ease of use for administrators

The system is administered via the Microsoft Management Console (MMC), which is a familiar tool for network administrators. A choice of wizards is available to simplify integration and set up of the program. There is also the option of making backup copies of the database and the application settings, which saves the administrator time when re-installing the program. Moreover, full-color graphic reports make for easy reading.

FEATURES

Remote installation of applications

The program supports various installation scenarios. Creation and maintenance of server hierarchies and administrative groups is performed automatically, using the Active Directory service or IP address range.

Centralized administration

Configuration of application parameters on all network nodes (including remote users) and updating of antivirus databases and program modules is performed centrally, from the administrator's work place.

Monitoring the status of antivirus protection

In addition to email, administrators can select other types of responses to events in the system. Storage areas for suspicious and infected files implemented as distributed databases with centralized administration offer additional flexibility when processing such objects.

TRAINING AND SUPPORT

Product training

The company offers its corporate clients a training course and product certification. The course trains system administrators to design, deploy and maintain antivirus protection based on Kaspersky Lab products.

Free technical support

Kaspersky Lab customers can receive free technical support in English, French, German or Russian by telephone or email.

SYSTEM REQUIREMENTS

Software requirements:

- MSDE 2000 with Service Pack 3 (supplied) or Microsoft SQL Server 2000 with Service Pack 3;
- Windows 2000 with Service Pack 1 or higher; Windows XP with Service Pack 1 or higher, Windows 2003 Server; Windows NT4 with Service Pack 6a, Microsoft Management Console version 1.2 or higher (only for the administration console).

Hardware requirements:

- Intel Pentium III 800 MHz or faster (for the administration console Intel Pentium II 400 MHz or faster);
- 128 MB of RAM (64 MB for the administration console);
- 400 MB of free (available) disk space (10 MB for the administration console).

Applications supported: Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows File Servers, and Kaspersky Anti-Virus for Microsoft ISA Server

Product version: 5.0

Available languages: English & Russian

Services

Supporting services comprise an essential component of Kaspersky Lab's products and solutions. Registered users are provided with hourly antivirus database updates, free product updates and round-the-clock technical support. A range of additional services are available to corporate customers.

Regular database updates are crucial for ensuring the effective operation of Kaspersky Lab products. Currently, antivirus database updates are released hourly and antispam databases are updated every 20 minutes. During virus outbreaks or epidemics, Kaspersky Lab issues more frequent updates and disinfection solutions to help users prevent infection.

Additionally, users of Kaspersky Lab products can contact the company's 24-hour technical support service. Support is available via telephone and email in English, French, German and Russian.

Anyone visiting the Kaspersky Lab website can scan any file on their computer for viruses online. Before purchasing any program, users can download a free trial version and try it on their computers. During global virus outbreaks the company releases free disinfection utilities which are available to the general public.

In addition to software, Kaspersky Lab offers information support. The Virus Encyclopedia contains detailed descriptions of malicious programs of all kinds and the company's newsletters keeps users updated on the latest virus outbreaks.

Kaspersky Lab supports its enterprise level information security products with a range of additional services. Each corporate client's needs are addressed on an individual basis. Services provided to such customers include examining and analyzing the corporate network, installation of an antivirus system, training of the customer's staff and maintenance of the security system installed.

Contact Information



● **Kaspersky Lab HQ**
Science and Technology Park
1st Volokolamsky Proezd, 10/1
Moscow 123060
Russian Federation
www.kaspersky.com
Email: sales@kaspersky.com
Tel. +7 495 797 8700

● **Kaspersky Lab USA**
300 Unicorn Park
Woburn MA 01801 USA
www.kaspersky.com
Email: info@us.kaspersky.com
Tel. +1 781 503 1800

● **Kaspersky Lab Japan**
Iwamoto Bldg. 4F 3-2-3
Iwamoto-cho 101-0032
Chiyoda-ku Tokyo Japan
www.kaspersky.co.jp
Email: sales@kaspersky.co.jp
Tel. +81 3 5687 7839

● **Kaspersky Lab UK**
Culham Innovation Centre
D5 Culham Science Centre
Abingdon OX14 3DB
United Kingdom
www.kaspersky.co.uk
Email: sales@kasperskylab.co.uk
Tel. +44 (0) 870 0113461

● **Kaspersky Lab Germany**
Steinheilstraße 13
85053 Ingolstadt
Germany
www.kaspersky.de
Email: info@kaspersky.de
Tel. +49 (0) 841 98 18 90

● **Kaspersky Lab France**
Immeuble l'Européen
ZAC Rueil 2000
2, Rue Joseph MONIER
92 500 Rueil Malmaison
France
www.kaspersky.fr
Email: info@fr.kaspersky.com
Tel. +33 8205 888 612

● **Kaspersky Lab Benelux**
Havensingel 1A
5211 TX's-Hertogenbosh
The Netherlands
www.kasperskylab.nl
Email: sales@bnl.kaspersky.com
Tel. +31 (0) 73 615 4860

● **Kaspersky Lab Poland**
Ul. Krotka 27A 42-200
Czestochowa Poland
www.kaspersky.pl
Email: info@kaspersky.pl
Tel. +48 34 368 18 14

● **Kaspersky Lab China**
Suite A504-505
U-Space Mall, No. 8
Guang Qu Men Wai Street
Chaoyang District
Beijing 100022 China
www.kaspersky.cn
Email: sales@kaspersky.com.cn
Tel. +86 10 5861 2570

● **Kaspersky Lab Korea**
Flour 8, Plaza 654 Building,
654-3 Yuksam-dong,
Kangnam-ku Seoul 135-080
South Korea
www.kasperskylab.co.kr
Email: sales@kasperskylab.co.kr
Tel. +82 2 508 8789

Kaspersky® Anti-Virus and Kaspersky® are registered trademarks of Kaspersky Lab, Ltd.
Other brands and products are trademarks of their respective holder(s).

Copyright © 2006 Kaspersky Lab, Ltd. All rights reserved.

Intel, the Intel logo, Centrino, the Centrino logo, Xeon, and Xeon Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.