



Premier protection against viruses, hackers and spam

Kaspersky® Security

for Microsoft Exchange Server 2003

Kaspersky® Security for Microsoft Exchange Server 2003 is a solution that protects users of corporate mail systems against viruses and unsolicited mail (spam).

Electronic mail has become a major channel for malware distribution. Virus outbreaks cause companies significant financial damage by undermining the integrity and confidentiality of information. In addition, companies face considerable loss of working hours by their employees, who daily have to delete tens and hundreds of unwanted messages from their mailboxes. The extra traffic caused by unwanted mail also has to be paid for.

Kaspersky® Security for Microsoft Exchange Server 2003 provides antivirus scanning of incoming and outgoing messages and mail stored on the server, as well as messages in common folders. It also helps mail system users to block unwanted mail using spam recognition technologies in addition to technologies provided by Microsoft.

PRINCIPAL ADVANTAGES

Advanced technologies for protection against viruses and spam. In addition to its proven antivirus technologies that ensure high detection rates of malicious programs, the product makes use of SpamTest™ technology to detect unwanted mail.

Two-tier spam filtering. The product filters unsolicited mail in conjunction with Microsoft Exchange 2003 Server / Microsoft Outlook 2003, guaranteeing high spam recognition.

Cost-effectiveness. The software product offers protection against malicious programs and unsolicited mail in one solution, reducing the cost of protecting the mail server and facilitating system administration.

FUNCTIONALITY

Protection against spam

Intelligent spam recognition 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. Mailings can be performed only by senders authorized by the network administrator.

Message classification. The administrator can configure separate processing rules for each unsolicited mail category. This prevents the loss of important information: messages that are known spam can be blocked, suspicious mail is delivered to the Unwanted Mail folder, and formal messages (such as message delivery and message read confirmations) to the Inbox.

Kaspersky® Security

for Microsoft Exchange Server 2003

Antivirus Protection

Real-time 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 any format. In addition, the system administrator can enable antivirus scanning of pass-through mail traffic routed through the Exchange server.

On demand and on schedule background scanning. The application scans folders and messages stored on the server 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 databases, the application can detect and remove not only known malicious software, but potentially hostile programs as well. These include programs that display advertising, data collection programs, dialer programs for automatically establishing connections with pay sites and other utilities that can be used by cybercriminals for their purposes.

Virus outbreak prevention. The application can monitor virus activity and detect outbreaks, allowing the system administrator to take response measures quickly: e.g., launch a scanning task, update databases or increase the system's level of protection. The administrator can be notified of outbreaks by email and, on a local area network, using the Net Send tool.

Backup copying. Before deleting messages, the application saves backup copies, making it possible to restore important information if attempts to cure an object resulted in failure or if a message was erroneously categorized as spam. A broad range of search parameters can be used to make finding objects in the backup storage easier.

Administration

Fine tuning. The administrator can configure the program based on the organization's security policy and hardware capabilities, e.g., select the types of malicious and potentially hostile programs to be detected by choosing standard or extended antivirus databases; adjust the application's performance depending on the mail traffic and the number of users; and, scan only potentially hostile objects by disabling scanning of certain file types.

Database updates. The antivirus database can be updated on demand or automatically on schedule from Kaspersky Lab Internet servers or from the company's local servers which are 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.

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. A report can be stored on the hard drive or sent via email.

Centralized administration. The application is configured and administered via the administration console built into Microsoft Management Console (MMC), a convenient management tool familiar to the administrator, or using Kaspersky® Administration Kit, which can also be used to administer other Kaspersky Lab products.

Fast installation. The interactive installation and configuration mode used by the program by default is appropriate for most systems, making it possible to begin normal operation of the program without spending too much time on installation and configuration.

System Requirements

Hardware requirements

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

Available languages: English, Russian

Product version: 5.5



Contact information

Kaspersky Lab HQ
10 Geroev Panfilovtsev,
Moscow, 125363 Russia
Telephone / Fax:
+7 (095) 797-8700
sales@kaspersky.com

We have local offices in
USA, United Kingdom, Germany,
France, the Netherlands, Poland,
China, Japan and Korea

Visit
<http://www.kaspersky.com/contacts>
for details

Kaspersky Lab products
are available
from our partners listed at
www.kaspersky.com/partners

KASPERSKY Lab
www.kaspersky.com